情報セキュリティ白書

Information Security White Paper

2022

ゆらぐ常識、強まる脅威：想定外にたちむかえ

IPA 独立行政法人情報処理推進機構
Information-technology Promotion Agency, Japan

「情報セキュリティ白書2022」の刊行にあたって

2021 年も新型コロナウイルス変異株による感染拡大が継続しました。米欧では対策緩和の方針がとられましたが、ワクチン接種やそれに基づく移動許可等の可否について多くの議論を呼びました。日本は、厳しい規制の中で東京 2020 オリンピック・パラリンピック競技大会を無観客で開催、成功させましたが、その後も規制はゆるまず、テレワーク等の新しい業務形態が定着していきました。

この間、重要な組織やインフラを狙った攻撃も続きました。特に目立ったのがランサムウェア被害です。米国では 2021 年 5 月にエネルギー事業者が攻撃を受け、米国東部の石油供給が一時ストップしました。国内では 7 月に食品事業者がバックアップデータまで暗号化され、事業再開が遅れました。10 月には病院が攻撃を受けて診療に支障が出ました。2022 年 2 月には製造事業者が攻撃を受け、納入先の事業者の生産に影響が出ました。昨年の巻頭言で申し上げたとおり、こうした攻撃は巧妙化しており、システムの脆弱性やサプライチェーンを介して侵入し、情報を盗んで二重の脅迫を行う等、深刻な脅威となっています。一方脆弱性については、テレワークで活用が進んだ VPN 等の対策がまだ十分でなく、12 月には広範囲の Web システムに影響を及ぼす Log4j の脆弱性が報告されました。こうした懸念もあり、2022 年の 10 大脅威では修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）が初めてランクインしました。テレワークや DX 推進等によって生活や業務の各場面でデジタル化が進む中、安全で信頼できると思っていた機器やシステムに脆弱性が見つかり、ゼロデイ攻撃され、生活の一部が突然立ち行かなくなるかもしれない、そういう時代を私達は迎えつつあります。

更に 2021 年後半以降のウクライナ危機は、「まさかこのような事態が起こるとは」を私達に痛切に感じさせました。ロシアとウクライナの紛争は、情報セキュリティの視点からは、三つの点が特に注目されます。一つ目は、紛争が武力とサイバー空間上の攻防が組み合わされたハイブリッドな戦いであること。二つ目は、ネット等で配信される紛争関連情報が急増し、その信頼性の見極めが難しいこと。最後は、サイバー空間の攻防において、民間組織や個人が簡単に当事者になってしまうこと。私達は国家間の分断や物的な流通分断のリスクに加え、虚偽の情報に誘導される、サイバー攻撃の対象になる、等のリスクに直面することとなりました。

半年前まで想定できなかったこうした状況に私達はどう対応すればよいでしょうか。申し上げてきたことの繰り返しになりますが、リスク対応の基本が大切であると思います。情報セキュリティに関しては、機器やシステムの脆弱性をなくすこと、このサービスが止まったときにどうするか、の想像力を持つことは大変重要です。また虚偽の情報に惑わされないために、様々なソースの情報を参照し、視野を広く持つことも大切になるでしょう。本白書が、多くの方々に広く利用され、新しい生活や働き方のリスクに対する意識を高め、備えを実践するための一助となることを祈念します。

2022年7月

独立行政法人情報処理推進機構（IPA）

理事長　富田達夫

目次

コラム

情報セキュリティ白書

序章

2021年度の情報セキュリティの概況

2020年から世界中で流行した新型コロナウイルス感染症については、日本・米国・欧州ではワクチン接種が進み、感染者の増減はあるものの、経済活動は徐々に以前の状態に戻りつつある。国内では、感染拡大防止対策として実施されたテレワークやオンライン会議等が新しい働き方として定着しつつある。こうした業務の見直し、デジタル化は、組織におけるDX（デジタルトランスフォーメーション）の推進を後押しする形となっている。

2021年はランサムウェアの手口が巧妙化して被害が拡大し、サプライチェーンに関連したインシデントや脆弱性を狙った攻撃も引き続き発生した。警察庁によれば、2021年下期の被害報告件数は2020年下期の4倍となった。また、2021年7月の製粉会社、10月の病院の事案では、バックアップデータも暗号化されたために早期復旧が困難であった。データ保管方法の見直しや復旧計画の重要性が再確認された。

攻撃経路として、海外拠点、海外子会社、取引先が攻撃され、被害を受ける事案も多くみられた。2021年10月の医薬品メーカの情報漏えい事案は海外拠点が攻撃対象であった。2022年2月の自動車部品会社へのランサムウェア攻撃では、部品供給先の自動車メーカの工場が1日停止した。サプライチェーン全体のセキュリティ強化が求められている。情報漏えい事案としては、マッチングアプリや大手製菓製造会社への不正アクセスにより合わせて300万件以上の大量の個人情報が流出した。

ソフトウェアの脆弱性を悪用した攻撃も継続して報告された。2021年に報告された脆弱性としては、VPN製品、Microsoft Exchange Serverの脆弱性、多くの製品やソフトウェアで使用されるJavaベースのロギングライブラリApache Log4jの脆弱性等、影響範囲が広く、攻撃により大きな被害が予想されるものが目立った。このほか、2021年初頭に欧州司法機関の一斉テイクダウンにより沈静化したウイルス「Emotet（エモテット）」の感染が再拡大し、2022年に入り注意喚起された。

セキュリティ政策面では、国内では2021年9月に「サイバーセキュリティ戦略」が閣議決定された。同戦略では「DX with Cybersecurity」として、デジタル社会の進展と併せてサイバーセキュリティ確保の取り組み推進が重要とされた。また同月にデジタル庁が発足、政府のIT基盤とセキュリティの整備を統括することとなった。サプライチェーンセキュリティについては、経済産業省がサプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）等を継続的に推進した。

米国では、重要インフラやライフラインに関わる制御システムへの攻撃が相次ぎ、水道や浄水場等の制御システムへの攻撃、石油供給事業者へのランサムウェア攻撃が報告された。米国Biden政権は重要インフラのセキュリティ対策強化を打ち出し、これを受けた米国国立標準技術研究所（NIST）は、重要ソフトウェア調達におけるセキュリティガイドライン策定、消費者向けIoT製品のラベリング制度の検討等を実施した。NISTはまたサプライチェーンセキュリティに関する官民連携イニシアティブ（NIICS）の設置、サプライチェーンリスク管理の標準ガイド（NIST SP800-161）の改訂を進めた。今後の動向が注目される。

欧州では、欧州ネットワーク・情報セキュリティ機関（ENISA）が主導し、重要インフラに関するサイバーセキュリティ準拠法の改訂案（NIS2 Directive）審議、あるいは域内の製品・サービスのセキュリティを担保するサイバーセキュリティ認証スキーム（EUCC scheme V1.1.1）の構築等を中心としてセキュリティ政策を推進した。また欧州委員会は2021年4月、AI利用リスクへの対処に関する法案を公表した。同法は罰則を伴う初のAI利用規格として注目される。

このように、各国とも重要インフラやサプライチェーンへのセキュリティ対策強化を進めてきたが、2021年後半以降はウクライナ情勢が悪化、2022年2月のロシアのウクライナ侵攻により、世界は新たな緊張に直面している。この紛争は、武力とサイバー攻撃・防御あるいはサイバー空間での情報戦が組み合わさったハイブリッドな戦いが特徴であり、サイバー空間上では政府に加えて民間組織・個人が参画する、というまったく新たな状況が生まれている。政府の安全保障政策・サイバーセキュリティ政策は言うまでもなく、企業や個人がこのリスクへの対応、例えば、親ロシア系ハッカーの攻撃への備え、紛争に関連する情報の信頼度の見極め等をどうするべきか、が問われている。

2021 年度の情報セキュリティの概況

	主な情報セキュリティインシデント・事件	主な情報セキュリティ政策・イベント
2021 年　4 月	● VPN 製品「Pulse Connect Secure」ゼロデイ攻撃発生（1.2.5） ● ファーストフードチェーン店でランサムウェア被害（1.2.8） ● マッチングアプリが不正アクセスを受け約 171 万件の個人情報流出（1.2.8、3.3.2）	■ 経済産業省「サイバーセキュリティ体制構築・人材確保の手引き」（第 1.1 版）改訂（2.1.2、2.3.1） ■ 欧州委員会「Artificial Intelligence Act」（AI 法）提出（3.4.2）
5 月	● 米石油供給事業者へのサイバー攻撃、身代金 500 万ドル相当を支払いか（3.4.1）	■ サプライチェーンセキュリティ強化を目指した米国大統領令 EO 14028 発表（3.4.1） ■ EU 域内のセキュリティ認証スキーム（EUCC scheme V1.1.1）公開（3.4.2）
6 月	● 無線通信機器メーカ、2017 年に不正アクセス確認から 3 年以上報告せず（1.2.8） ● 電子部品メーカの再委託先社員が取引先情報約 3 万件、従業員関連情報約 4 万件を不正持ち出し（1.2.8）	■ 総務省「スマートシティセキュリティガイドライン（第 2.0 版）」公開（2.1.3）
7 月	● 大手製粉会社がサイバー攻撃を受けシステム障害（1.2.2） ● IT 管理ツールをランサムウェア攻撃に悪用（1.1.1）	■ NISC「政府機関等のサイバーセキュリティ対策のための統一基準（令和3年度版）」公開（2.1.1） ■ 総務省「ICT サイバーセキュリティ総合対策 2021」公開（2.1.3）
8 月	● ProxyShell の脆弱性を公表(1.2.5)	■ IPA「サイバーセキュリティ経営可視化ツール」公開（2.1.1） ■ NIST が「サプライチェーンセキュリティに関する官民を推進する国家イニシアティブ」を設置（3.4.1）
9 月		■ デジタル庁発足（2.1.1） ■ NISC「サイバーセキュリティ戦略」「サイバーセキュリティ 2021」決定（2.1.1）
10 月	● 徳島の町立病院でランサムウェアの被害発生（1.2.2） ● 医薬品メーカの国内外の拠点に不正アクセス（1.2.8）	■ NISC、第 14 回「日・ASEAN サイバーセキュリティ政策会議」開催（2.2.1） ■ Ransom Disclosure Act 米国議会に提出（3.4.1）
11 月	● 大手眼鏡販売チェーン持株会社で約 1 億円のビジネスメール詐欺被害（1.2.3） ● Emotet（エモテット）の攻撃活動再開（1.2.6）	■ NISC「クラウドを利用したシステム運用に関するガイダンス」公開（2.1.1、3.3.4） ■ CISA が既知の脆弱性悪用に関する重大リスクの削減に関する運用指令を公開（3.4.1）
12 月	● ロギングライブラリ Apache Log4j の任意のコード実行の脆弱性に関する注意喚起（1.1.1、1.3.2） ● スマホ決済のキャンペーン関係識別情報 13 万 3,484 件が GitHub 上で閲覧可能になっていたと発表（1.2.8）	■ 米 Biden 大統領が国防授権法に署名、アジア大平洋地域やウクライナ・NATO への関与を強化（3.4.1）
2022 年　1 月	● 決済サービス事業者不正アクセスによる情報漏えい公表（1.2.8）	
2 月	● ロシアがウクライナに侵攻（3.4.1） ● CISA、FBI がウクライナで使用された破壊的ウイルスに関し注意喚起（3.4.1）	■ NIST「ソフトウェアサプライチェーンセキュリティガイダンス」、NIST SP800-218 Ver.1.1 公開（3.4.1）
3 月	● 自動車部品会社がサイバー攻撃を受け、自動車メーカが国内工場停止（1.2.2） ● 大手製菓製造会社への不正アクセス（1.2.8） ● 複数の自治体で利用するクラウドが踏み台となり約 91 万件の迷惑メール発信（3.3.2）	■ CISA がウクライナ関連攻撃対策サイト「SHIELDS UP」を公開（3.4.1） ■ 総務省「地方公共団体における情報セキュリティポリシーに関するガイドライン」改訂版等公開（2.1.3）

※ 2021年度の主な情報セキュリティインシデント・事件、及び主な情報セキュリティ政策・イベントを示している。標的型攻撃、ランサムウェア被害、ビジネスメール詐欺、DDoS 攻撃、Web 改ざん、フィッシング等の攻撃や被害は通年で発生している。表中の数字は本白書中に掲載している項目番号である。特に注目されたもののみを挙げた。他のインシデントや手口と対策、及び政策・イベント等については本文を参照していただきたい。

第1章
情報セキュリティインシデント・脆弱性の現状と対策

2021年もテレワークやDX推進の取り組みが進む中、国内外でランサムウェアやサプライチェーン攻撃による大きな被害が続いた。Emotetの感染再拡大、影響と深刻度が大きいApache Log4jの脆弱性等も話題となった。

本章では、国内外で発生した主なインシデントの概要と攻撃の手口や対策の状況、脆弱性の動向等について解説する。

1.1 2021年度に観測されたインシデント状況

本節では2021年度に観測された世界と日本における情報セキュリティインシデントの発生状況について概説する。

1.1.1 世界における情報セキュリティインシデント状況

世界における情報セキュリティインシデントの発生状況について、主に以下の情報セキュリティ関連の報告書を参照し概説する。

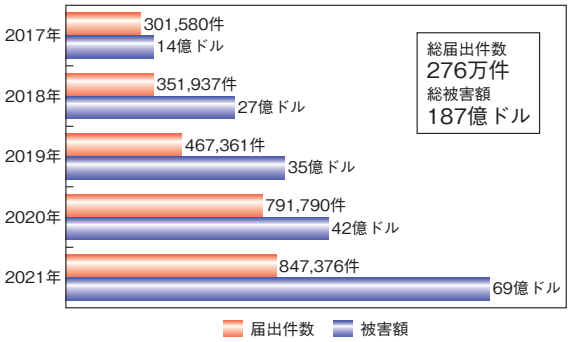
- 米国連邦捜査局（FBI：Federal Bureau of Investigation）：Internet Crime Report 2021※1
- Anti-Phishing Working Group, Inc（APWG）：Phishing Activity Trends Reports※2
- Verizon Communications Inc.（以下、Verizon社）：2022 Data Breach Investigations Report※3
- 日本アイ・ビー・エム株式会社（以下、IBM社）：IBM X-Force 脅威インテリジェンス・インデックス2022※4

(1) 広い範囲に影響を与えるサプライチェーンに対するインシデント

FBIによると、サイバー犯罪の件数と被害額は過去5年間増加を続け、2021の年間被害額は69億ドルとなった（図1-1-1）。

中でも、2021年は広範囲に影響を及ぼしたサプライチェーンに関わるインシデントが注目された。ここでは5件の事例を紹介する。

2021年5月、米Colonial Pipeline Companyがランサムウェアによるサイバー攻撃を受け、米国東海岸の燃料輸送が6日間にわたり停止し、多数のガソリンスタンドで売り切れや油価の高騰等、社会に大きな影響を与えた※5（「3.4.1 (1) (b) Colonial Pipeline事案とその対応」参照）。



■図1-1-1　サイバー犯罪の届出件数と被害額の推移
（出典）FBI「Internet Crime Report 2021」を基にIPAが編集

2021年の3月と8月に相次いで発見されたMicrosoft Exchange ServerのProxyLogon※6及びProxyShell※7の脆弱性においては、最も攻撃に晒されやすいインターネットに接続されたExchange Serverの総数が40万台以上にわたっていると報告された※8（「1.2.5 (2) Microsoft製品の脆弱性を対象とした攻撃」「3.4.1 (1) (a) Microsoft Exchange Server事案とその対応」参照）。

2021年12月には、Apache Log4jの任意のコードが実行される脆弱性（CVE-2021-44228）がアナウンスされた※9。Apache Log4jはApache Software Foundationが開発したオープンソースのJavaベースのロギングライブラリである。発見された脆弱性のCVSS（Common Vulnerability Scoring System）による深刻度は、最大値の10.0（レベルⅢ（危険））であった。影響を受ける最初のバージョンのリリースが2013年と古く、システムを開発する際に、開発者がこのモジュールを組み

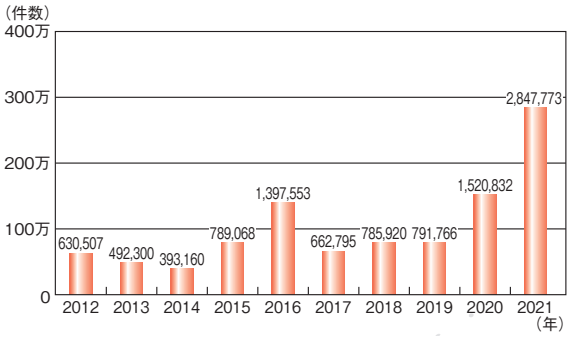
込むことが可能だったため、ソフトウェアの使用者が、Log4j が組み込まれていること自体を把握していなかったり、どのバージョンが組み込まれているかを把握することも困難だったりと、混乱が生じた（「3.1.2（1）（a）Log4Shell」参照）。

2020 年から続いた米 SolarWinds Worldwide, LLC. のネットワーク監視ソフト「Orion」の侵害による大規模な攻撃により、米政府機関を始め、同社顧客の 1 万 8,000 社が影響を受けた[※10]。このインシデントは、同社の正規アップデートファイルに悪意のあるウイルスが組み込まれた、サプライチェーン攻撃によるものであった（本インシデントに関係した米国の政策については「3.4.1 米国の政策」参照）。

2021 年 7 月には、米 Kaseya Limited の IT 管理ツール「VSA」がサイバー攻撃を受け、ランサムウェアを拡散する攻撃に悪用された。その結果、1,500 社近くの会社がランサムウェアによる攻撃を受けた可能性があると Kaseya Limited は発表している[※11]。

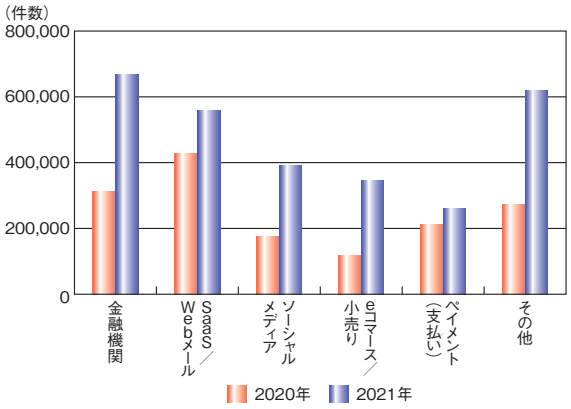
(2) フィッシングの傾向

APWG によると、2021 年の届け出されたフィッシングサイトの総数は約 284 万 8,000 件で、2020 年と比較して 87% 増と大幅に増加し、過去 10 年で最多となった（図 1-1-2）。



■図 1-1-2　世界における届け出されたフィッシングサイト件数
（出典）APWG「Phishing Activity Trends Reports」を基に IPA が作成

業種別のフィッシングサイト件数では、2021 年には、「金融機関」が 23.5%、「SaaS ／ Web メール」が 19.6%、「ソーシャルメディア」が 13.8% と続いている。2017 年から 2020 年までトップ 3 に入っていた「ペイメント（支払い）」は 9.2% と、全体に占める割合は減った。ただし、各業種別の件数を 2020 年と比較すると上記業種はいずれも増加しており、「ペイメント（支払い）」以上に件数が増加した業種が多かったに過ぎないことが分かる（図 1-1-3）。なお、フィッシングサイトの国内の傾向については「1.1.2 (3) フィッシングによる被害」を参照されたい。

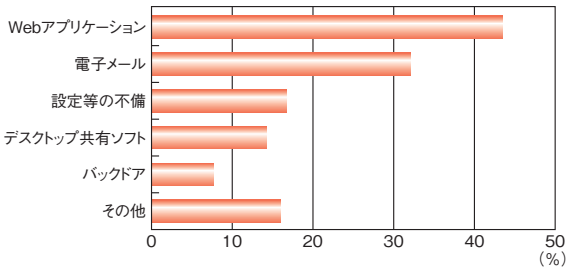


■図 1-1-3　業種別のフィッシングサイト件数（2020 年と 2021 年の比較）
（出典）APWG「Phishing Activity Trends Reports」を基に IPA が作成

(3) 情報漏えいインシデントの状況

Verizon 社によると、2021 年に同社が分析した 2 万 3,896 件のインシデントのうち、情報漏えい／侵害の件数は 5,212 件であり、2 万 9,207 件のインシデントのうち 5,258 件だった 2020 年[※12] に比べ、インシデント件数が 18.1% 減ったものの、情報漏えい／侵害の件数はほぼ横ばいだった。

情報漏えい／侵害の侵入手口では、「Web アプリケーション」の侵害が最も多く、「電子メール」「設定等の不備」「デスクトップ共有ソフト」と続いている（図 1-1-4）。



■図 1-1-4　情報漏えい／侵害の侵入手口（2021 年、n=3,279）
（出典）Verizon 社「2022 Data Breach Investigations Report」を基に IPA が編集

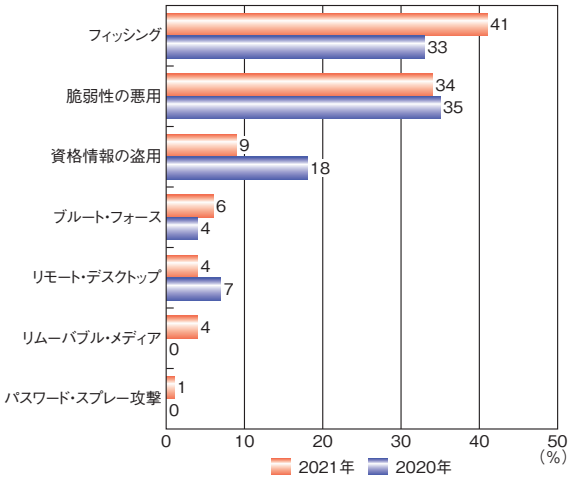
情報漏えい／侵害の 82% において、窃取された認証情報の利用、フィッシング、特権の誤用、ヒューマンエラー等、人的要因が関与していたという。

また、システムへの侵入インシデントの 62% がサプライチェーンを介して発生したという。

(4) 脆弱性とランサムウェアによる被害

IBM Security X-Force Incident response によって

観測された感染手口の内訳では、「フィッシング」と「脆弱性の悪用」が合わせて 75% と 2020 年に続いて多い。また、2021 年には、「リムーバブル・メディア」や「パスワード・スプレー攻撃※13」といった項目も新たに登場している（図 1-1-5）。



■図 1-1-5　上位の感染手口（2021 年と 2020 年の比較）
（出典）IBM 社「IBM X-Force 脅威インテリジェンス・インデックス 2022」を基に IPA が編集

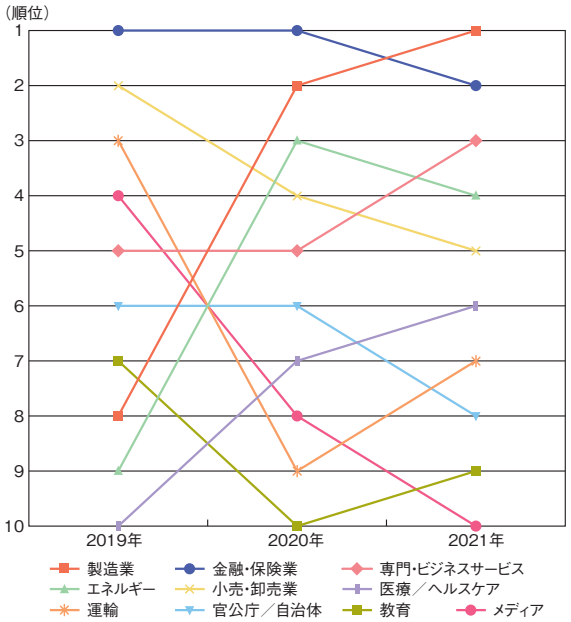
2021 年に頻繁に悪用された脆弱性の上位を表 1-1-1 に示す。2020 年には上位 10 件中 4 件※14 が 2 年以内に公表された脆弱性であったが、2021 年には上位 10 件中 8 件が 2 年以内に公表されたものとなった。

	CVE No.	内容
1	CVE-2021-34523	Microsoft Exchange server の ProxyLogon の脆弱性
2	CVE-2021-44228	Apache Log4j ライブラリの脆弱性
3	CVE-2021-26857	Microsoft Exchange Server におけるリモートでコードを実行される脆弱性
4	CVE-2020-1472	Netlogon の特権昇格の脆弱性
5	CVE-2021-27101	Accellion における SQL インジェクションの影響を受ける脆弱性
6	CVE-2020-7961	Liferay Porta におけるリモートでコードを実行される脆弱性
7	CVE-2020-15505	MobileIron におけるリモートでコードを実行される脆弱性
8	CVE-2018-20062	ThinkPHP におけるリモートでコードを実行される脆弱性
9	CVE-2021-35464	ForgeRock Access Management（OpenAM）におけるリモートでコードを実行される脆弱性
10	CVE-2019-19781	Citrix ADC および Citrix Gateway における任意のコードを実行される脆弱性

■表 1-1-1　2021 年に最も頻繁に悪用された上位の脆弱性
（出典）IBM 社「IBM X-Force 脅威インテリジェンス・インデックス 2022」を基に IPA が作成

この中でも Apache Log4j の脆弱性は 2021 年 12 月と比較的新しく報告されたものであるが、広く利用されているライブラリであるため、このように頻繁に悪用される結果になったと考えられる。

IBM 社によると 2021 年に攻撃の対象となった業種は、2020 年まで 1 位だった「金融・保険業」が 2 位となり、代わって「製造業」が初めて首位となった。また、2019 年の順位と比較すると「製造業」のほか、「エネルギー業」「医療／ヘルスケア」も順位が大きく上昇している（図 1-1-6）。

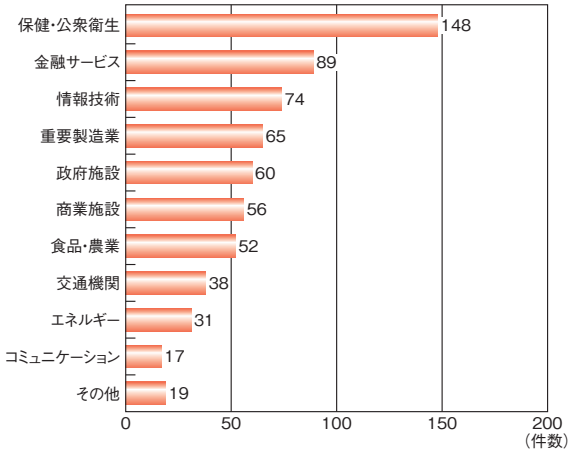


■図 1-1-6　最も頻繁に攻撃対象となった業界の順位（上位 10 業種）
（出典）IBM 社「IBM X-Force 脅威インテリジェンス・インデックス 2022」を基に IPA が作成

一方、FBI によると、ランサムウェア被害の届出件数と被害額は 2020 年には 2,474 件、29.1 万ドル※15 だったのに対し、2021 年には 3,729 件、49.2 万ドルと大幅に増加した。ランサムウェアの被害を受けた業界は、「保健・公衆衛生」が最も多く、「金融サービス」「情報技術」「重要製造業」が続いている（次ページ図 1-1-7）。

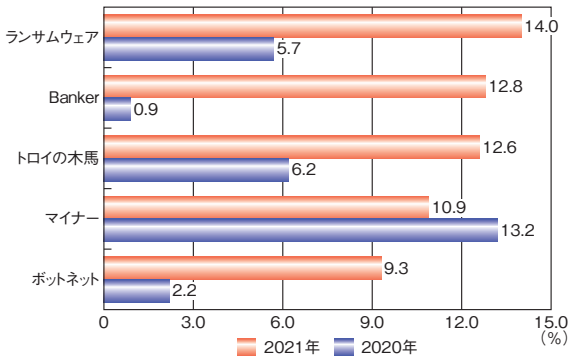
(5) Linux を狙うウイルス

Linux を狙うウイルスは年々増加しているが、IBM Security X-Force 脅威インテリジェンス・インデックスのパートナーである Intezer Labs の分析によると、ウイルス※14 のコードの多くが再利用されている場合は革新性は低く、独自のバリエーションが多い場合は革新性が高い、という方法論に基づく指標を用いて、固有のコードを持つ Linux 環境のウイルスの割合を調査した結果、2021 年は 2020 年よりはるかに固有のコードを持つウイル



■図 1-1-7　産業別ランサムウェア被害の届出件数
(出典)FBI「Internet Crime Report 2021」を基に IPA が編集

スの割合が高くなったと報告している（図 1-1-8）。更に、Linux のウイルスが増加している理由は、クラウドの利用増加に伴い、そこで運用される OS として Linux の比率が高いためと分析している。



■図 1-1-8　固有のコードを持つ Linux を狙うウイルス
（2021 年と 2020 年の比較）
(出典)IBM 社「IBM X-Force 脅威インテリジェンス・インデックス 2022」を基に IPA が編集

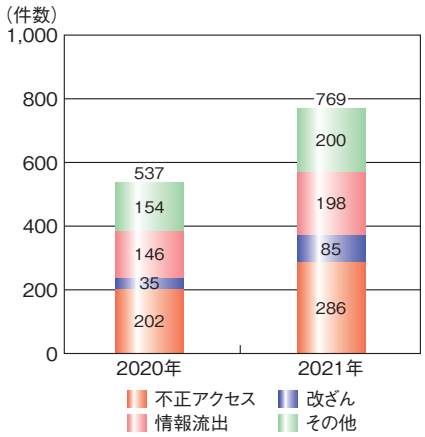
1.1.2 国内における情報セキュリティインシデント状況

国内における情報セキュリティのインシデント発生状況について、主に以下の資料を参照して概説する。

- 三井物産セキュアディレクション株式会社（以下、MBSD 社）による集計情報※17
- 一般社団法人 JPCERT コーディネーションセンター（JPCERT/CC：Japan Computer Emergency Response Team Coordination Center）：インシデント報告対応レポート※18
- フィッシング対策協議会：月次報告書※19
- 警察庁：令和 3 年におけるサイバー空間をめぐる脅威の情勢等について※20-1

(1) 情報セキュリティインシデントの発生状況

MBSD 社によれば 2021 年の情報セキュリティインシデントの種類別報道件数は全体で 769 件となり、2020 年の 537 件から 43.2% 増であった（図 1-1-9）。割合が最も多いのは「不正アクセス」で、37.2% であった。前年比では、「不正アクセス」が 141.6%、「改ざん」が 242.9%、「情報流出」が 135.6%、「その他」が 129.9% であった。



■図 1-1-9　情報セキュリティインシデントの種類別報道件数
(出典)MBSD 社による集計情報を基に IPA が作成

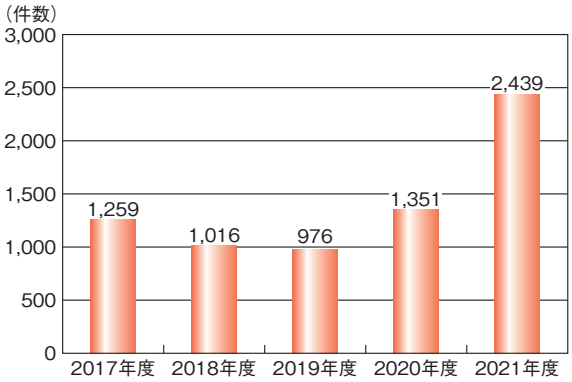
(2) Web サイト改ざんによる被害

2021 年 4 月 1 日から 2022 年 3 月 31 日までに JPCERT/CC へ報告された Web サイト改ざん件数は 2,439 件で前年比 180.5% と急増し、過去 5 年間では最多となった（図 1-1-10）。

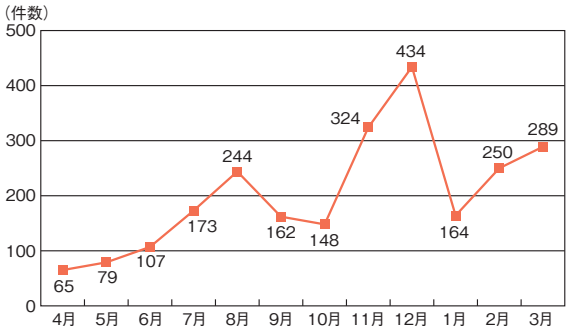
月別では 12 月が 434 件、四半期別では 2021 年 10 ～ 12 月が 906 件で最も多かった（次ページ図 1-1-11）。

(3) フィッシングによる被害

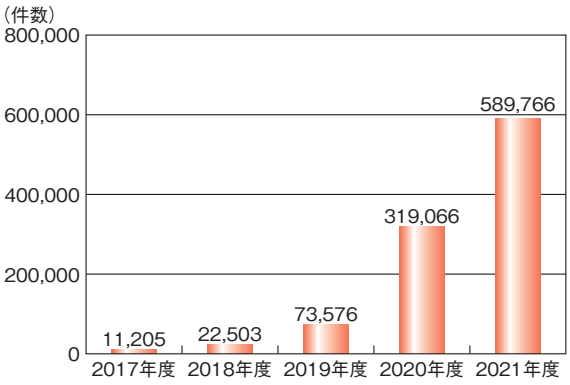
フィッシング対策協議会への 2021 年度の報告件数は



■図 1-1-10　Web サイト改ざん年度別件数推移（2017 ～ 2021 年度）
(出典)JPCERT/CC「インシデント報告対応レポート」（2017 年 4 月 1 日～ 2022 年 3 月 31 日）を基に IPA が作成



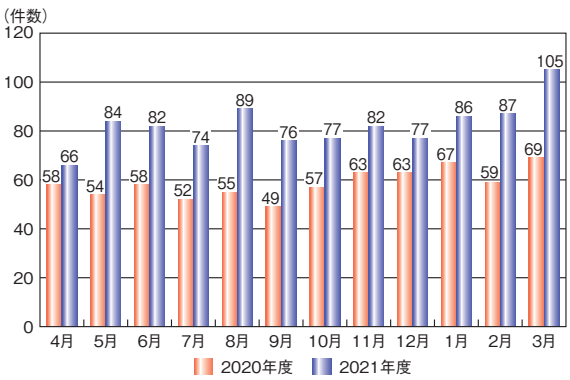
■図 1-1-11　Web サイト改ざん月別件数推移（2021 年度）
（出典）JPCERT/CC「インシデント報告対応レポート」（2021 年 4 月 1 日～ 2022 年 3 月 31 日）を基に IPA が作成



■図 1-1-12　年度別フィッシング報告件数（2017 ～ 2021 年度）
（出典）フィッシング対策協議会「月次報告書」（2017 年 4 月～ 2022 年 3 月）を基に IPA が作成

58 万 9,766 件で前年比 185% であった（図 1-1-12）。2020 年度の件数はその前の過去 3 年に比べて突出していたが、2021 年度は更にそれを上回り、2017 年度と比べると 52 倍以上に上る報告件数であった。この増加の内訳を悪用されたブランド数で見ると、2021 年度の各月ブランド数は 2020 年度の同月を 1.1 倍から 1.6 倍程度上回っていた（図 1-1-13）。

月によってブランドの変動はあるが、2020 年度は毎月上位四つのブランドで報告件数の約 9 割を占めていた[※20-2]。例えば「Amazon」「Apple」「LINE」「楽天」「三井住友カード」等である。しかし 2021 年度は悪用されるブランドが多岐にわたり、2020 年度のように特定のブランドが集中して悪用される傾向とは異なっている。



■図 1-1-13　悪用されたブランド数の比較（2020 年度、2021 年度）
（出典）フィッシング対策協議会「月次報告書」（2020 年 4 月～ 2022 年 3 月）を基に IPA が作成

表 1-1-2 は 2021 年度に悪用された各月の上位五つのブランドである。報告件数全体に占める割合は 2020 年度に比べ低下している。8 割を超過したのは 2021 年 4 月のみで、それ以降は 6 割から 7 割台半ばで推移し、2022 年 2 月、3 月には 6 割を切った。この傾向は上位の特定ブランド以外にも多くのブランドが悪用されたことが要因である。表 1-1-3（次ページ）は月間 1,000 件以上が報告されたブランドの数と全体に占める割合をまとめたものである。2020 年度の各月は上位 4 ブランドで約 9 割を占めていたが、2021 年 9 月以降は 10 以上のブランドで全体の約 8 割を占め、多種多様なブランドが悪用されていることがうかがえる。

警察庁によれば、フィッシングを主な手口とする「インターネットバンキングに係る不正送金」は、2019 年に被

	4 月	5 月	6 月	7 月	8 月	9 月
全件に占める割合	81.2%	76.6%	71.4%	67.8%	65.8%	64.0%
1 位	Amazon	Amazon	Amazon	Amazon	Amazon	Amazon
2 位	楽天	楽天	楽天	三井住友カード	三井住友カード	ETC 利用照会サービス
3 位	三菱 UFJ ニコス	三井住友カード	エムアイカード	楽天	エポスカード	イオンカード
4 位	三井住友カード	イオンカード	三井住友カード	イオンカード	イオンカード	三井住友カード
5 位	JCB	JCB	エポスカード	VISA	PayPay 銀行	コロナワクチンナビ
	10 月	11 月	12 月	1 月	2 月	3 月
全件に占める割合	66.6%	67.7%	74.0%	67.6%	56.6%	55.0%
1 位	Amazon	Amazon	Amazon	Amazon	Amazon	Amazon
2 位	メルカリ	メルカリ	メルカリ	メルカリ	メルカリ	メルカリ
3 位	三井住友カード	三井住友カード	三井住友カード	JCB	JCB	えきねっと
4 位	ETC 利用照会サービス	楽天	ETC 利用照会サービス	三井住友カード	—	—
5 位	楽天	ETC 利用照会サービス	JCB	—	—	—

■表 1-1-2　悪用された上位ブランド名と報告全件に占める割合
（出典）フィッシング対策協議会「月次報告書」（2021 年 4 月～ 2022 年 3 月）を基に IPA が作成

	9月	10月	11月	12月	1月	2月	3月
ブランド数	10	11	9	12	10	10	18
全件に占める割合	81.6%	83.2%	79.2%	88.4%	82.9%	74.2%	88.7%

■表 1-1-3　報告件数が月間 1,000 件を超過したブランド数と報告件数全体に占める割合
（出典）フィッシング対策協議会「月次報告書」（2021 年 9 月～ 2022 年 3 月）を基に IPA が作成

害額約 25 億 2,100 万円に達していたが、2021 年までに被害額は約 3 分の 1 に減少したという。一方、図 1-1-12（前ページ）のとおりフィッシングの報告件数は増加の一途をたどっている。

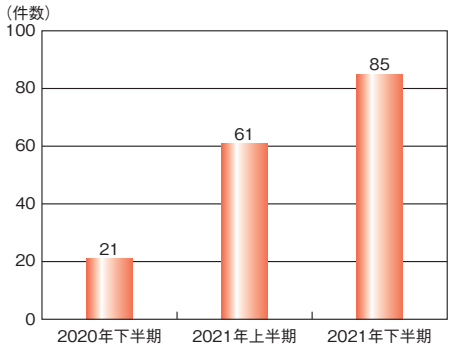
一般財団法人日本サイバー犯罪対策センター（JC3：Japan Cybercrime Control Center）によれば、2021 年は銀行を装ったフィッシングサイトの割合は少なく、ネット通販等の e コマース、通信事業者、クレジットカード会社等を装ったフィッシングサイトが多数を占めているという。「インターネットバンキングに係る不正送金」の被害額が減少している一方で、ネット通販等のクレジットカード情報を窃取するフィッシングサイトの割合が大きくなったことが、クレジットカード不正利用の被害額が増加している要因の一つと考えられるという。銀行等の金融機関から、クレジットカード情報や各種 EC サイトのアカウント情報へとフィッシングのターゲットが変化してきていることから、同センターは一層の警戒が必要あるという※20-3。

トレンドマイクロ株式会社（以下、トレンドマイクロ社）のレポートにおいても、誘導先となるフィッシングを含む詐欺サイトは、銀行等金融機関やクレジットカード関連のほか、モバイル決済、暗号資産取引所、生命保険、携帯通信会社、給付金・ワクチン等コロナ関連、水道等の公共料金支払い等、多岐に及ぶとしている。その要因として、これまでもサイバー犯罪における常套手段として用いられてきた詐欺手法が、コロナ禍における支払い・決済手段としてのインターネット需要の高まりにより、広く一般のインターネット利用者を狙う攻撃の中で拡大し、2021 年はその傾向が顕著化したとしている※20-4。

(4) 国内被害が拡大したランサムウェアについて

ランサムウェアについては、国内外で「二重恐喝」（窃取したデータを暗号化するだけでなく、金銭を支払わなければ、そのデータを公開すると二重に脅す手口。「二重の脅迫」とも呼ばれる）による被害の拡大や、産業制御システムに影響を及ぼすようなウイルスが引き続き確認されているほか、国内の医療機関等重要インフラ事業者が標的となり、市民生活にまで重大な影響を及ぼす事案も発生している。

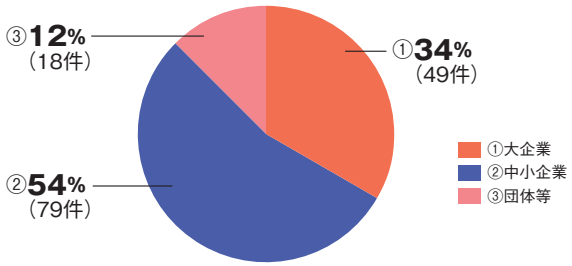
警察庁に報告された国内のランサムウェアによる被害の報告件数は、2020 年下半期 21 件から 2021 年上半期 61 件、同下半期 85 件と急激に増加した（図 1-1-14）。



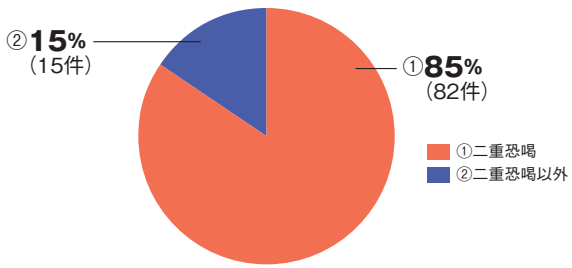
■図 1-1-14　企業・団体等におけるランサムウェア被害の報告件数の推移
（出典）警察庁「令和 3 年におけるサイバー空間をめぐる脅威の情勢等について」を基に IPA が編集

2021 年中にランサムウェア被害を警察に報告した企業に対し警察庁が行ったアンケート調査によると、企業・団体等の被害件数 146 件のうち、54% が「中小企業」であった（図 1-1-15）。また、金銭の要求が確認できたのはそのうち 97 件であり、「二重恐喝」による要求は 85% を占めたという（図 1-1-16）。

警察庁は被害のあった 146 件に対して、「復旧に要し



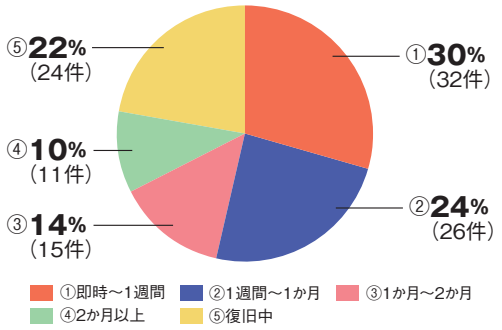
■図 1-1-15　被害企業・団体等の件数及び割合（n=146）
（出典）警察庁「令和 3 年におけるサイバー空間をめぐる脅威の情勢等について」を基に IPA が編集



■図 1-1-16　被害の手口別件数及び割合（n=97）
（出典）警察庁「令和 3 年におけるサイバー空間をめぐる脅威の情勢等について」を基に IPA が編集

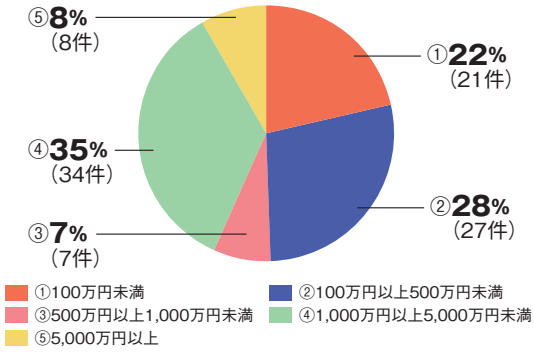
た期間」「調査・復旧費用の総額」「感染経路」についてアンケートを実施し、123 件の回答が得られた。

「復旧に 1 ケ月以上要した」のは、有効回答 108 件のうち 26 件、24% であった（図 1-1-17）。ランサムウェアの被害に遭うと、その後の事業継続に少なからず影響を及ぼすことが分かる。



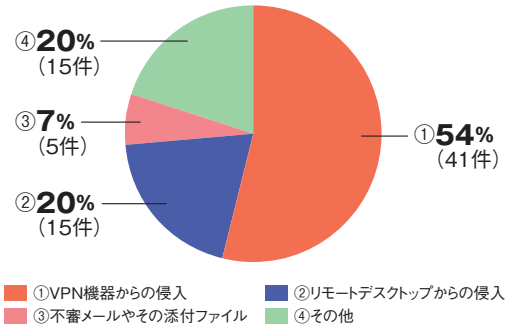
■図 1-1-17　復旧に要した期間（n=108）
（出典）警察庁「令和 3 年におけるサイバー空間をめぐる脅威の情勢等について」を基に IPA が編集

「調査・復旧費用の総額」で最多だったのは、有効回答 97 件のうち 34 件で 35% を占めた「1,000 万円以上～ 5,000 万円未満」であった（図 1-1-18）。被害に遭った企業・団体にとって、調査・復旧費用が重荷になっていると推察される。



■図 1-1-18　調査・復旧費用の総額（n=97）
（出典）警察庁「令和 3 年におけるサイバー空間をめぐる脅威の情勢等について」を基に IPA が編集

感染経路では、「VPN 機器からの侵入」が 54% と最も多く、「リモートデスクトップからの侵入」は 20% であった。一方で従来認識されていた「不審メールやその添付ファイル」を経由した侵入は 7% であり、テレワークの急速な拡大等に伴い生じた脆弱性を突いて攻撃している傾向が見受けられる（図 1-1-19）。



■図 1-1-19　感染経路（n=76）
（出典）警察庁「令和 3 年におけるサイバー空間をめぐる脅威の情勢等について」を基に IPA が編集

VPN やリモートデスクトップを感染経路としたランサムウェアは、新型コロナウイルス感染拡大で定着したリモートワークにより顕在化した脅威である。今後もリモートワークがゼロになることはなく、一般的なビジネス環境として活用が続くと考えられる。感染被害を引き起こさないためにも、企業・組織では脆弱性対策等の基本的対策のほか、万が一侵入された場合に備えた対策の充実が求められる（ランサムウェアの手口や対策については「1.2.2 ランサムウェア攻撃」参照）。

COLUMN

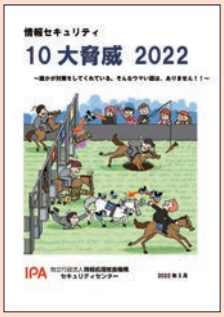
知ってる人は知っている、知らない人は多分ぜんぜん知らない 情報セキュリティの10大脅威

IPAが毎年、発表している情報セキュリティ10大脅威（表1）。2022年版では組織の7位に「修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）」が初ランクインしましたが、トップ10にランクインする顔ぶれは例年大きく変わることはありません。「毎年ほぼ同じ顔ぶれ」ということは残念ながら、これらの脅威はずっと、私たちの身近に存在し続けていると言えます。

表1 情報セキュリティ10大脅威 2022「個人」・「組織」向け脅威の順位

「個人」向け脅威	順位	「組織」向け脅威
フィッシングによる個人情報等の詐取	1	ランサムウェアによる被害
ネット上の誹謗・中傷・デマ	2	標的型攻撃による機密情報の窃取
メールやSMS等を使った脅迫・詐欺の手口による金銭要求	3	サプライチェーンの弱点を悪用した攻撃
クレジットカード情報の不正利用	4	テレワーク等のニューノーマルな働き方を狙った攻撃
スマホ決済の不正利用	5	内部不正による情報漏えい
偽警告によるインターネット詐欺	6	脆弱性対策情報の公開に伴う悪用増加
不正アプリによるスマートフォン利用者への被害	7	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）
インターネット上のサービスからの個人情報の窃取	8	ビジネスメール詐欺による金銭被害
インターネットバンキングの不正利用	9	予期せぬIT基盤の障害に伴う業務停止
インターネット上のサービスへの不正ログイン	10	不注意による情報漏えい等の被害

しかし、これらの脅威について一般のパソコン利用者の認知度を調査してみると、「ランサムウェア」が30.9%、「標的型攻撃」が26.8%、「ビジネスメール詐欺」が26.8%と決して高くはありません。最も認知度が高い脅威である「フィッシング」でも56.7%と、過半数を超えた程度です[i]。この認知度をどうとらえるかは人それぞれだと思いますが、職場やプライベートでインターネットの利用が不可避となる中、脅威を理解し、その対策を実践するのは、「ニューノーマルな生活の知恵」ではないでしょうか？　IPAは情報セキュリティの脅威とその対策が国民に広く浸透、理解されることを願っています。



「情報セキュリティ10大脅威 2022」解説書及び社内教育や研修に使える「情報セキュリティ10大脅威 2022」簡易説明資料（スライド形式）、関連するIT用語を解説した「知っておきたい用語や仕組み」は以下のURLからダウンロードできます。また、「情報セキュリティ10大脅威の活用法」も以下のURLで公開していますので併せてご活用ください。

https://www.ipa.go.jp/security/vuln/10threats2022.html

i　IPA：2021年度 情報セキュリティの倫理と脅威に対する意識調査－【脅威編】－
https://www.ipa.go.jp/security/economics/ishikichousa2021.html〔2022/5/23確認〕

1.2 情報セキュリティインシデント別の手口と対策

本節では、インシデント別の発生状況と、具体的な事例について述べる。また、2021 年度に確認されたサイバー攻撃の手口を中心に解説する。

1.2.1 標的型攻撃

標的型攻撃とは、ある特定の企業・組織や業界等を狙って行われるサイバー攻撃の一種である。ウイルスメールやフィッシングメールを不特定多数の相手に無差別に送り付ける攻撃とは異なり、標的型攻撃は、特定の企業・組織や業界が持つ機密情報の窃取やシステム・設備の破壊・停止といった、明確な目的を持って行われる。また、標的型攻撃は長期間継続して行われることが多く、攻撃者が標的とする組織（以下、標的組織）の内部に長期間潜伏して活動するという特徴も持つ。

IPA では、過去の事例等から、標的型攻撃の流れを五つの段階に分類している（図 1-2-1）。

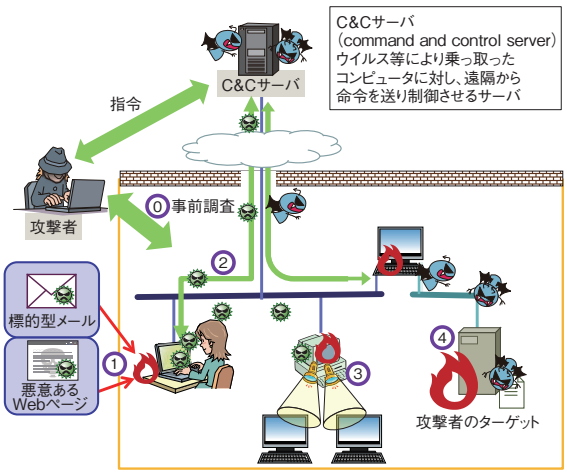
「事前調査段階」では、標的組織や業界の情報を収集する。公開されている情報を収集するだけでなく、標的組織と他の組織とのメールの盗聴等により必要な情報を収集することもある。

次の「初期潜入段階」では、「事前調査段階」で得られた情報を基に、標的組織の端末へのウイルス感染を試みる。海外拠点や取引先組織といった、いわゆるサプライチェーン上のセキュリティの弱い部分を狙う手口に加え、VPN 製品や公開サーバ等のインターネットとの境界にある装置の脆弱性を悪用し、侵入する手口もある。標的組織の人間に対し、ウイルスを仕込んだファイルが添付された、あるいは悪意のある URL リンクが記載された標的型攻撃メールを送り付ける手口も依然として確認されている。また、悪意のある Web サイトを閲覧しただけで、ウイルスに感染してしまうドライブ・バイ・ダウンロード攻撃が用いられることもある。

「初期潜入段階」で標的組織の内部に侵入した攻撃者は、「攻撃基盤構築段階」へと移り、標的組織内のパソコンを遠隔操作するため、遠隔操作ウイルス（RAT: Remote Access Trojan）に感染させることを試みる。この際、遠隔操作を長期的かつ継続的に行うため、複数の RAT に感染させる場合もある。このとき、より隠密性の高いウイルス（ファイルレスマルウェア※22 等）を使うケースも確認されている。

次の「システム調査段階」では、「攻撃基盤構築段階」で感染させた RAT を使用して、組織内ネットワークの攻撃に必要なウイルスやツールを送り込む。これらのウイルスやツールを用いて、組織内ネットワークの調査、管理者権限の奪取、目的とする情報の探索等を行う。このとき、侵入したパソコン等に標準でインストールされているアプリケーションが悪用されることもある。

「攻撃最終目的の遂行段階」では、攻撃者は、目的とする情報の窃取等を行う。海外の事例では、情報の窃取ではなく、国家間の政治的主張等を目的とした攻撃も確認されている※23。



⓪［事前調査段階］
標的組織を攻撃するための情報を収集する。

①［初期潜入段階］
標的型攻撃メールや、Webサイト閲覧を通してウイルスに感染させる。

②［攻撃基盤構築段階］
侵入したPC内でバックドアを作成し、外部のC&Cサーバと通信を行い、新たなウイルスをダウンロードする。

③［システム調査段階］
情報の存在箇所特定や情報の取得を行う。
攻撃者は取得情報を基に新たな攻撃を仕掛ける。

④［攻撃最終目的の遂行段階］
攻撃専用のウイルスをダウンロードして、攻撃を遂行する。

■図 1-2-1　標的型攻撃の流れ
（出典）IPA「標的型サイバー攻撃の脅威と対策※21」を基に編集

(1) 国内の標的型攻撃事例

本項では、2021 年度に確認された 2 件の標的型攻撃の事例を紹介する。

(a) ショートカットファイルを悪用した攻撃

JPCERT/CC のレポート※24 によると、2021 年 7 月から 9 月の間に、暗号資産交換業者を狙ったと考えられる

標的型攻撃の報告が寄せられたという。この攻撃は、標的組織に対し、ファイル共有を装ったメールが送られてくることから始まる。メールの本文中には URL リンクが記載され、URL リンクをクリックさせることで不正なショートカットファイルを格納した圧縮ファイルをダウンロードさせようとする。ショートカットファイルには、JavaScript ファイルをダウンロードして実行するコマンドが含まれており、最後には本命のウイルスに感染させられる。この攻撃手口は、2019 年 7 月に JPCERT/CC が公開した国内外の暗号資産に関連する組織を狙った攻撃キャンペーンと類似しているという※25。このキャンペーンでは、圧縮ファイルには、パスワードが設定された囮の文書とショートカットファイルが格納されている。ショートカットファイルには「パスワード.txt.lnk」のように二重拡張子で拡張子を偽装したファイル名が付けられており、囮の文書のパスワードを確認しようとショートカットファイルを開いてしまうと、攻撃が進行し、最終的には本命のウイルスに感染させられる※26。

手口が類似していることから、同じ攻撃者が継続して標的型攻撃を行っているものと思われる。

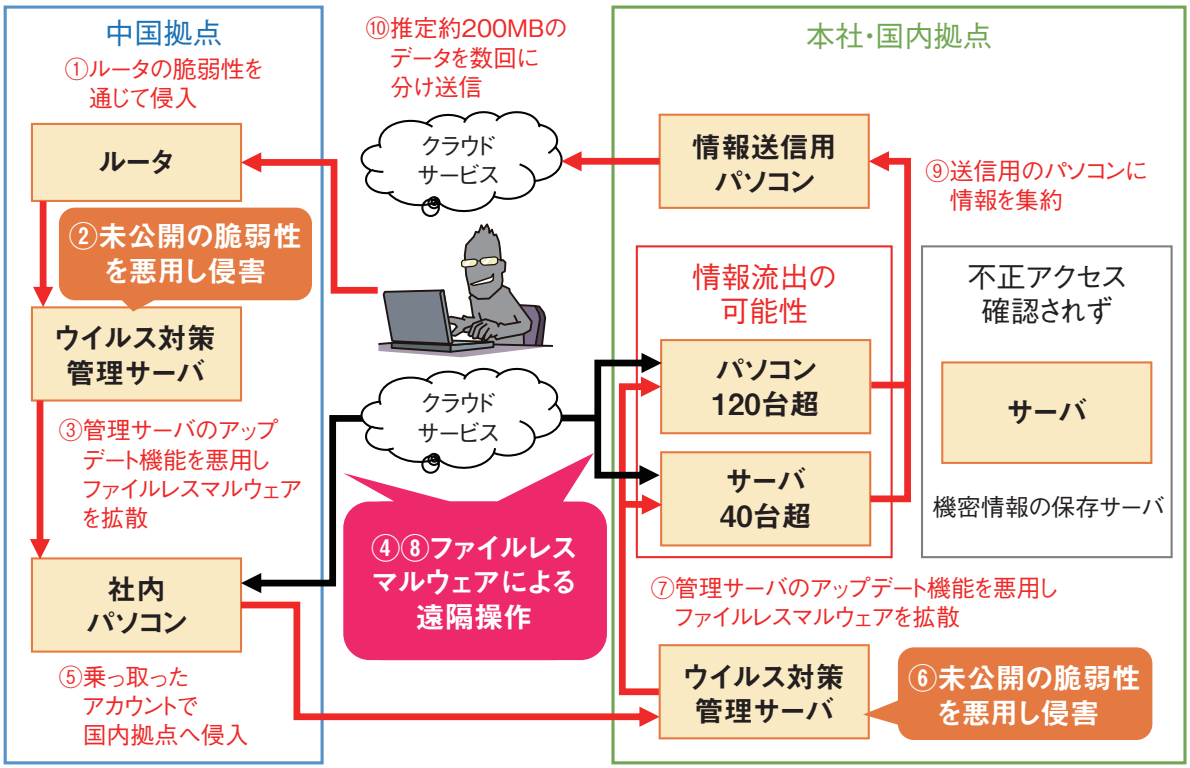
(b) 国内企業の海外拠点を狙った未公開の脆弱性を悪用した標的型攻撃

2019 年 6 月に三菱電機株式会社の国内拠点の端末のセキュリティソフトが不審な挙動を検知し、社内ネットワークが外部から不正アクセスを受けていたことが、同社プレスリリースにて 2020 年 1 月に公表された※27。2020 年 2 月に公表された第 3 報によると、中国にある海外拠点への侵入を発端とした標的型攻撃と考えているとのことであった※28。

2021 年 12 月、防衛省は、本件により流出した可能性のある防衛関連のデータファイル約 2 万件のうち、安全保障に影響を及ぼす恐れのあるデータファイルは 59 件であるとの調査結果を公表した※29。三菱電機株式会社も同時期に、第 4 報として本件により流出した可能性のある防衛関連の一部のデータの管理不備について、防衛省より注意・指導を受けたとの内容を公表した※30。

図 1-2-2 は、公表された資料を基に、システム構成の概略と攻撃経路を図示したものである。

本事例では、攻撃者は最初にルータの脆弱性を悪用し、中国拠点の社内ネットワークに侵入し、中国拠点のウイルス対策管理サーバ（以下、管理サーバ）へ未公開の脆弱性※32 を悪用した攻撃を行い、同サーバを侵害した。次に、管理サーバのパターンファイルアップデート機能を利用して拠点内の端末にファイルレスマルウェアを拡散した。感染した端末を大手クラウドサービス上に構築したサーバから遠隔操作し、中国拠点と同じ手口で日



■図 1-2-2　標的型攻撃の事例概要
（出典）三菱電機株式会社「不正アクセスによる個人情報と企業機密の流出可能性について（第 3 報）※28」及び piyolog「ログ消去もされていた三菱電機の不正アクセスについてまとめてみた※31」を基に IPA が編集

本国内の管理サーバを経由して国内の端末へ感染を拡大していった。

本事例では、セキュリティ対策が強固な日本国内のネットワークへ侵入するための足掛かりとして、中国拠点が狙われたものと思われる。攻撃者は中国拠点の管理サーバへの攻撃において、送信元アドレスを詐称し、特定を困難にしていたという。また、ファイルレスマルウェアの利用や不正通信先に大手クラウドサービスを利用するといった、ウイルス対策製品等で検知しづらい手法が用いられていた。更に、未公開の脆弱性を悪用するゼロデイ攻撃が行われていたため、侵入を完全に防ぐことは困難であったと言える。他のサイバー攻撃と同様に、侵入を前提とした多層的なセキュリティ対策を実施し、速やかに攻撃を発見し対応できる体制を整備しておくことが望ましい。

(2) 標的型攻撃の傾向

日本国内の企業・組織を対象とした標的型攻撃は、2011 年に複数の重工業メーカ等が標的となった事例以降、継続的に発生している。

「1.2.1 (1) 国内の標的型攻撃事例」で紹介したように、海外関連組織を足掛かりとした攻撃も確認されており、海外を含む企業グループ全体でセキュリティ対策を講じていく必要がある。

初期潜入段階で用いられる手口としては、2020 年と同様に、標的型攻撃メールのみならず、テレワークの普及で利用が拡大した VPN 製品や外部からアクセス可能なサーバ等の脆弱性管理の不備を突く事例が報告されている。

一方、海外の事例では、重要インフラ組織や防衛・政府機関を標的とした攻撃が報告されている※33。今後日本の組織が攻撃されることも予想されるため、業種や規模にかかわらず、常に対策を講じておくことが重要である。

(3) 標的型攻撃の手口（初期潜入段階）

初期潜入段階における、代表的な標的型攻撃の手口を以下に示す。

なお、記載する手口はこれまでに確認されているものの一部であり、業務形態や IT 環境・セキュリティ対策の変化に応じて、攻撃者も手口を変化させていくことが予想されるため、新たな手口への注意も重要である。

(a) 標的型攻撃メール

標的型攻撃メールは、標的とする企業・組織・業界でよく用いられる言葉を使用し、メールの信憑性を高めることで、添付ファイルの実行または悪意のあるファイルのダウンロードを行わせるというソーシャルエンジニアリングの手口である。

攻撃者はメールの信憑性を高めるため、標的とする企業に関係する組織や官公庁が公表している情報等から、その業界特有の用語や関係者の情報を「事前調査段階」で集め、それを件名、本文、署名、添付ファイル名や内容等に利用するケースが過去に確認されている。

(b) サプライチェーン・海外拠点等への攻撃

「1.2.1 (1) (b) 国内企業の海外拠点を狙った未公開の脆弱性を悪用した標的型攻撃」や「情報セキュリティ白書 2021※34」の「1.2.1 (1) 国内の標的型攻撃事例」で紹介したように、標的となる組織のネットワークやシステムを直接狙うのではなく、取引先企業や海外拠点、または海外の子会社を初期潜入の標的にした攻撃の手口が確認されている。

これは、取引先企業が小規模の組織であるとセキュリティ対策が脆弱であったり、また海外拠点・組織に対しては国内のセキュリティガバナンスが効きにくかったりする傾向が強いためである。攻撃者は事前調査段階で、標的組織のネットワークやサプライチェーン全体を見渡し、そのうちの脆弱な箇所を侵入のための足掛かりとしている。

(c) VPN 製品や公開サーバ等の脆弱性を悪用した攻撃

米国政府機関によると、攻撃者は標的組織への侵入経路として、SSL-VPN 製品の脆弱性を利用している可能性があると報告されている※35。

また、Web サイトやユーザ向けシステム等、公開サーバの脆弱性を悪用した攻撃による被害も確認されている。特に近年、脆弱性情報が公開された後、その脆弱性を悪用した攻撃方法が作成されるまでの時間や、その攻撃方法が悪用されるまでの時間が短くなっている傾向がある※36。修正プログラムが作成される前に攻撃され、被害が発生してしまうこともある。

(4) 標的型攻撃の手口（攻撃基盤構築段階）

攻撃基盤構築段階における、最近確認している具体的な手口を紹介する。

(a) 感染の永続化

攻撃者は、標的組織内での活動を継続して行うため、

端末の起動時にRATが自動的に実行されるよう、レジストリの改変やタスクスケジューラの登録等を行う。このとき、ファイルレスマルウェアを用いることで、セキュリティソフト等による検知を避けようとする手口が確認されている※37。

(b) 組織内での侵害範囲拡大

前述の国内企業の海外拠点を狙った事例のように、セキュリティソフトのアップデート機能等、標的組織のシステムやアプリケーションソフトが持つファイルの共有・配布機能を悪用して組織内で侵害範囲を拡大する手口が確認されている。

(c) 感染端末と攻撃者のサーバとの通信

感染端末と攻撃者のサーバとの通信においては、通信先（攻撃者のサーバ）のIPアドレスやドメインを頻繁に変えるほか、前述の事例のように、大手クラウドサービスを通信先として悪用することで、正規の通信であるかのように見せかけ、セキュリティソフト等での検知を逃れようとする手口が確認されている。また、通信内容を暗号化したり、一見無害な画像データの中に命令を埋め込むステガノグラフィ技術を用いたりすることで、命令を隠ぺいする手口も確認されている※38。

(5) 標的型攻撃への対策

標的型攻撃の傾向や手口に記載したとおり、攻撃者は多種多様な手口で、計画的かつ巧妙に攻撃を遂行する。このため、ある対策を取れば完全に防御できるということはなく、多層的防御が必要である。組織の規模や業種により取り得る対策は異なるが、情報資産を守るためには、あらゆる可能性を考慮し、対策の検討と選別、実施を行うことが重要である。以下に、その例を示す。

(a) 利用者の意識向上

利用者の意識向上を目的とした対策例を以下に示す。

- 不審メールに対する注意力の向上

  標的型攻撃では、標的組織に関連する人物のメールアカウントを攻撃者が悪用してメールを送信するものや、組織や業界固有の用語等をメール本文中で用いて自然な文章を装ったもの等、受信者を騙すために巧妙な手口が使われることが多い。しかし、標的型攻撃メールがすべて精巧に作られているわけではない。そのため、組織としては、利用者へ不審メールに対する注意力向上に向けた教育や注意喚起を実施することが重要である。また、利用者が不審な点がないか注意し、不用意な添付ファイルの開封や、本文URLリンクのクリック、及びメールへの返信をしないことは、有効な対策である。添付ファイルを開いてしまい、不審と感じるメッセージやダイアログが表示された場合や、表示されたメッセージの意味が分からない場合はその指示に従わずに、企業のシステム管理部門へ連絡することが望ましい。

- SNSを悪用した手口の周知

  攻撃者はSNSを悪用し、求人や共通の趣味等、個人への関心を装って攻撃対象者に近づき、信頼関係を構築する。そして、悪意のあるファイルやURLリンクを送り、それを開かせることで初期潜入の経路を開拓することがある。

  個人の環境でSNS等の利用を制限することは難しいが、このようなケースがあることを周知し、利用者の警戒意識を高めることは有効である。また組織内の業務環境では、個人によるSNSの利用を制限することが望ましい。

- 標的型攻撃メール訓練等の実施

  擬似的な標的型攻撃メールを利用者に送信して、そのメールへの対応を行う訓練（標的型攻撃メール訓練）の実施も利用者の意識向上に有効である。訓練を通じて、不審メールを受信した場合に着目すべき箇所の再確認や、不審メールを受信した際、あるいは受信したメールの添付ファイルを開いてしまった（ウイルスに感染した）際に必要となる対処の再確認を行う。必要となる対処には、組織内の不審メール届出窓口への連絡も含まれる。不審メールを開封したことを責めず、利用者に報告してもらい、情報を共有することが重要である。また、利用者が不審メールを未読のまま削除するだけでは不十分であり、報告が必要であると理解してもらうことも重要である。

  このような訓練を定期的に行うことで、利用者の対応能力を維持・向上させる。また、具体的な攻撃手口を利用者に周知することも対応能力の向上に有効である。

(b) 組織としての対応体制の強化

組織として攻撃に対応していくための体制の強化を図る対策例を以下に示す。

- CSIRT設置と運用

  利用者が標的型攻撃メール等の不審なメールを受信した際に、連絡すべき窓口が組織内に周知されていることは重要である。また、組織外から連絡を受けて

標的型攻撃の被害に気付くことも考えられるため、外部からの連絡を受ける窓口を設けることも重要となる。このような、組織内部・外部との適切な連絡体制の整備やセキュリティインシデントが発生した際の調査・分析、セキュリティの教育・啓発活動の実施等を行う組織・体制のことをCSIRT（Computer Security Incident Response Team）と呼ぶ。セキュリティインシデントの未然防止、またはインシデント発生時の迅速な対応を行うために、CSIRTやそれに準ずる体制を組織内に設置することは有効な手段である※39。

- インシデントの発生を想定した事前準備
  組織内にCSIRT等の体制を整えるだけではなく、実際にセキュリティインシデントが発生した際、事業を継続できるように事業継続計画（BCP：Business Continuity Plan）に情報セキュリティの観点を組み込み、運用しておくとよい。
  CSIRT向けの取り組みでは、他組織で発生したインシデントや自組織で起こり得るインシデントを基にシナリオを作成し、インシデントの発生を想定して演習を行うことが望ましい。これは、組織全体の対応力・回復力（サイバーレジリエンス）の強靭化に有効である。
- 流行している攻撃の手口や対策の組織内共有
  今後も引き続き、標的型攻撃によるセキュリティインシデントが、被害を受けた組織から公表され、また各報道機関やセキュリティベンダがその手口や対策を発表していくことが想定される。
  これらの情報をCSIRT等が定期的に収集し、自組織において同様の脅威となり得るか確認し、必要であれば自組織の対策に組み込むことは重要である。具体的には、攻撃者の侵入手口が特定機器の脆弱性を突いたものであれば、自組織のシステムに該当する機器や脆弱性がないか確認し、修正プログラムが適用されていなければ適用する。標的型攻撃メールにより攻撃が行われたのであれば、社内にそのメールの特徴を周知することで、類似した攻撃メールによる被害が発生しないようにすることが望ましい。
- 海外拠点・サプライチェーンを意識したセキュリティ対策の強化
  前述のとおり、攻撃者はセキュリティ対策が脆弱な海外拠点や海外子会社、取引先企業を初期潜入の標的にする傾向がある。このため、海外拠点・サプライチェーンを意識したセキュリティ対策の強化が求められている。
  具体的には、海外拠点においても国内拠点と同様にセキュリティポリシーが策定・周知され、またセキュリティリスクの可視化と、改善や対策活動が行われることが望ましい。実施する際は、所在地の法制度や労働慣行の違い等も把握して、国内と同一の対策が取れない場合は代替策を考える必要がある。
  また、国内・海外を問わず取引先等とは、セキュリティ対策状況や連絡体制を共有し、セキュリティインシデント発生時の連携を容易にすることで、サプライチェーンを狙った標的型攻撃にいち早く対処可能となる。

（c）システムによる対策

システムによる対策例を以下に示す。

- 不審メールを警告する仕組みの導入
  組織のメールシステムでメール受信時に、送信者（From）メールアドレスの偽装や、フリーメールアドレスの利用、悪用されやすい添付ファイルの拡張子やファイルタイプ、メール内のURLリンク先の情報等を検知し、必要に応じて利用者に警告することで、利用者に不審メールであると気付く機会を与えることが可能である。
  また、添付ファイル付きメールの受信時やインターネット上のファイルダウンロード時には、ウイルス検査はもちろん、サンドボックス上で動的にファイル解析を行うことも有効である。なお、オンラインで提供されるサンドボックスを利用する際は、ファイルをアップロードすることで意図せず情報漏えいにつながる危険性があるため、十分な注意が必要である。
  加えて、セキュリティインシデント発生に備え、不審メールを確保できる仕組みを導入することが望ましい。不審メールをいつでも調査可能にしておくことで、影響範囲等の解析が可能となり、解析結果を組織全体で活用し対策を取ることができる。
- 適切な修正プログラムの適用
  システムの脆弱性を悪用する標的型攻撃に備え、IT資産管理システム等を活用し、組織内のすべてのサーバ・パソコン等に適切に修正プログラムが適用できる仕組みを作ることが望ましい。
  特に今回紹介した手口のように、初期潜入段階ではインターネットに公開されたサーバやVPN製品等の脆弱性が狙われる傾向がある。これらの製品は、システム環境によってはすぐに修正プログラムを適用できない場合もある。また、脆弱性情報が公開されたら速やかに対応することが望ましいが、その時点で修正プログラムが提供されていないこともある。その場合、ベン

ダから一時的な回避策が提示されていれば適用を検討する、提示されていなければ当該システムを一時的に停止する等の対応が有効である。修正プログラムを適用する場合、検証環境でテストし、問題がなければ本番環境に適用する等の対応が必要となることもあるため、適用するシステムを想定して、どのように対応していくか、事前に計画を立てておくことが望ましい。運用中のシステムの脆弱性対策を外部へ委託する場合、委託先と協議の上、事前に具体的な実施内容を取り決めておくことが重要である。

- 通常業務で使わないファイルの実行・ソフトウェアの利用防止
  利用者が通常の業務では使わないであろうファイルやソフトウェアについては、あらかじめ、システムやポリシーで制御することが望ましい。具体的には、利用者の環境で実行可能なファイルの種類やソフトウェアを許可リスト化しておくことで、ウイルスへの感染を防止する。許可リストのみによる制限の実施が難しい場合は、利用者の環境で実行することが望ましくないファイルの種類やソフトウェアを特定し禁止リスト化する。
  例えば、悪用されることの多いPowerShellやJavaScript等のスクリプトファイル（拡張子が.ps1や.js等のファイル）のような、業務で使用しないであろうファイルの実行を禁止することが有効である。
- セキュリティ対策の再チェック
  2021年度も新型コロナウイルスの流行は収束しておらず、テレワークを目的としたVPN製品等のシステムの導入や、システム構成または設定の変更等が継続して行われた。しかし、適切なセキュリティ設計や設定が行われていなかったり、セキュリティ設定をあえて緩和したりすることで、脆弱な箇所が発生するケースもあったと思われる。
  そのようなケースを認識している場合には、改めてセキュリティ対策が現状のままでよいか再検討することが望ましい。
- ネットワーク構成の変化に合わせた対策
  働き方の多様化により、仕事場を従来の職場に限定せず、在宅でも可能にする勤務形態や、BYOD（Bring Your Own Device）端末の業務利用の広まりにより、これまでのような組織内ネットワークとインターネットの境界におけるセキュリティ対策だけでは、侵害を防ぐことが難しくなってきている。そのため、パソコンや携帯端末等の業務端末（エンドポイント）において不審な挙動を監視し、攻撃活動の抑え込みを行うEDR（Endpoint Detection and Response）製品の導入等も有効な対策である。EDR製品は、すべてのウイルス等に対して万能ではないものの、ファイルレスマルウェアや未知のマルウェア等の検知・対策にも有効である可能性がある。またクラウドの利用等によって、業務情報を自社システム外に保管するケースも増えてきており、データそのものへのセキュリティ対策（暗号化やDLP（Data Loss Prevention）等）を検討することも有効である。

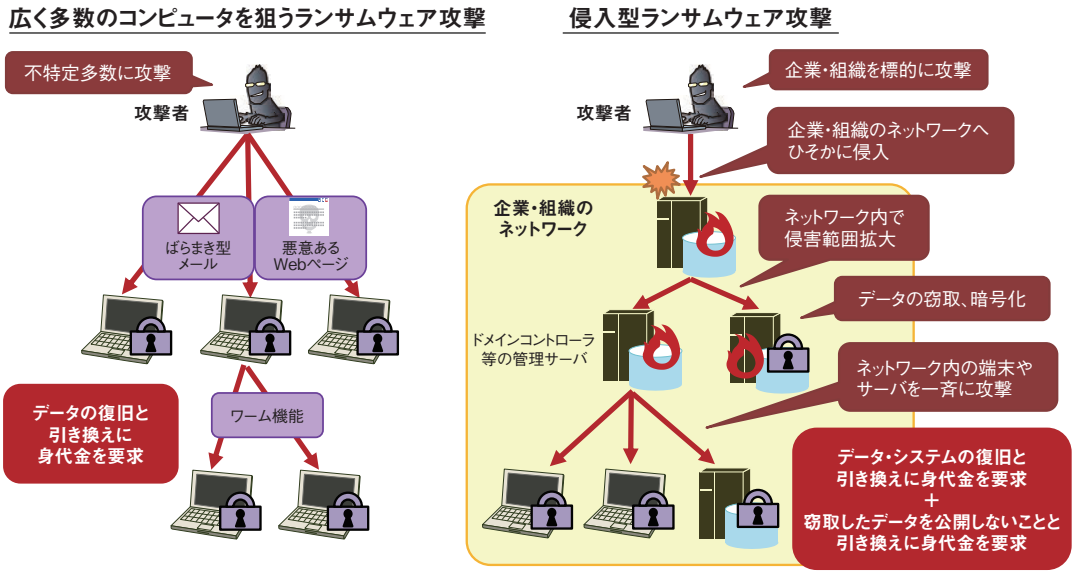
以上のように、利用者のセキュリティリテラシーの向上、インシデント発生時に適切に対応できる組織体制の構築、システムによる各種対策等、複数の観点を組み合わせ、多層的に対策を実施していくことが標的型攻撃への対策として重要である。

1.2.2 ランサムウェア攻撃

ランサムウェアとは「ransom」（身代金）と「software」（ソフトウェア）を組み合わせた造語で、パソコンやネットワーク接続された共有フォルダ等に保管されたファイルを暗号化することや、画面をロックすること等により、パソコンやファイルを使用不可にするウイルスの総称である。使用不可の状態から復旧することと引き換えに身代金を支払うように促すメッセージを表示することから、ランサムウェアと呼ばれている。本項では、ランサムウェアを使用したサイバー攻撃を「ランサムウェア攻撃」と呼ぶ。

ランサムウェア攻撃には、大きく分けて次の2種類がある（次ページ図1-2-3）。

- 広く多数のコンピュータを狙うランサムウェア攻撃
  ばらまき型メール、悪意のあるWebサイトからのダウンロード、脆弱性の悪用等で、広く不特定多数のコンピュータをランサムウェアに感染させようとする攻撃。2017年に多くの感染が確認された「WannaCry」と呼ばれるランサムウェアでは、感染拡大の方法として、脆弱性を悪用したワーム（自己複製）機能の手口が用いられた。
- 侵入型ランサムウェア攻撃
  攻撃者自身が様々な攻撃方法を駆使し、企業・組織のネットワークへひそかに侵入し、システムの侵害範囲を拡大しつつ、大量のデータをランサムウェアによって暗号化する等、事業継続に関わるような被害を与える攻撃。組織の内部ネットワークへの侵入手口には標的型攻撃と同様の攻撃技術が使われる。海外では「human-operated ransomware attacks（人手によ



■図 1-2-3　ランサムウェア攻撃の手口のイメージ
（出典）IPA「【注意喚起】事業継続を脅かす新たなランサムウェア攻撃について※40」を基に編集

るランサムウェア攻撃）」とも言われる。侵入型ランサムウェア攻撃では、データの復旧のために金銭を要求するだけでなく、データを窃取し、身代金を支払わない場合、データを公開するといった脅迫も行うことがある（「二重の脅迫」と呼ばれる）。

(1) ランサムウェア攻撃の傾向

従来の主流は「広く多数のコンピュータを狙うランサムウェア攻撃」であったが、2018※41 ～ 2019 年※42 ごろから「侵入型ランサムウェア攻撃」や「二重の脅迫」が観測され始めた。2020 年には、複数の日本企業・組織の被害が報道され、IPA※40 と内閣サイバーセキュリティセンター（NISC：National center of Incident readiness and Strategy for Cybersecurity）※43 が同攻撃の手口について注意喚起を行っている。

また、警察庁の公表した資料※44 によると、2020 年下期の企業・団体等におけるランサムウェア被害の報告件数が 21 件であったものが、2021 年上期は 61 件、2021 年下期は 85 件と急増した。2022 年 2 月にも、自動車部品会社である小島プレス工業株式会社がランサムウェア攻撃を受けたことにより、トヨタ自動車株式会社が国内全工場（14 工場 28 ライン）を 3 月 1 日に丸 1 日停止させるという被害が出ている※45。これらのことから、今後も日本の企業・組織が攻撃対象となる状況は続くと予想されるため、注意が必要である。

なお、ランサムウェア攻撃は 2015 年前後から高度に組織化・分業化※46 の動きも見られており、ランサムウェア（ウイルス）の開発、攻撃の実行、及び身代金の回収を別の攻撃者が分担して行う等のシステムが成立している。そのため、高度な技術を持たなくても、簡単に攻撃が行える状況となっており、多くの企業・組織が攻撃対象となり得る。

侵入の手口については、2021 年も継続して、VPN 製品※47 や Windows のリモートデスクトップサービス※48 の設定不備、あるいは脆弱性を悪用する手口が確認されている。従って、VPN 製品やリモートデスクトップサービスが攻撃者に狙われていることを認識し、対策を講じる必要がある。

(2) ランサムウェア攻撃の被害事例

2021 年度に公表された事例から次の 2 件を紹介する。両事例ともにバックアップデータまで暗号化されて復旧が困難となり、被害が大きくなった。バックアップデータをオフラインで保存する等、暗号化されることのない状態でバックアップデータを管理することの重要性が示唆される。

(a) 国内病院の被害事例

2021 年 10 月 31 日、徳島県つるぎ町の町立半田病院は、ランサムウェアに感染した事実を公表した。報道※49 を基に被害状況や攻撃の手口を紹介する。

公表当日の 0 時半ごろ、同病院の電子カルテのデータが暗号化され、患者約 8 万 5,000 人分の記録が参照できなくなったほか、受付・診察・会計まで、すべての IT システムがダウンした。また、病院内のプリンタから大量に文章が印刷された。内容は「身代金を払わなければ、盗んだデータを公開する」といった旨の英語の脅迫

文であったという。

同病院では電子カルテのデータをバックアップサーバに保存していたが、バックアップサーバもランサムウェアにより暗号化されたため、システムの復旧が困難となった。同病院によると、バックアップサーバは災害時にメインサーバが壊れた場合の予備として用意していたもので、サイバー攻撃から守る仕組みにはなっていなかったという。

同病院は、電子カルテ復旧のため身代金の支払いも検討したが、身代金を支払ってもデータが復旧する保証がないこと等から、支払わないことを決め、約2億円をかけ新システムを構築することにした。しかしながら、窃取された可能性のある電子カルテ等の個人情報は、今後も流出のリスクが残存することとなった。

同病院では、少なくとも約4,000枚のカルテを手書きで作り直したが、過去の治療歴を正確に把握できなかったことや、新規患者や救急搬送の受け入れを停止せざるを得ない状況になったこと等、2022年1月4日の全面再開まで約2ヵ月間、病院の機能低下を強いられた。同病院は13の診療科を持ち、1日約300人が通院する県西部の主要な病院であったため、多くの通院者にも影響が生じた。

本事例は「Lockbit2.0」と呼ばれる攻撃者グループによるものと報じられている。システムログが攻撃者によって消去されていたため、攻撃者やウイルスの侵入経路は明らかになっていないが、同病院では脆弱性のあるVPN製品をテレワークで使用していたと報道されており、VPN製品を起点に不正アクセスされて「侵入型ランサムウェア攻撃」と「二重の脅迫」の被害に遭った可能性がある。

(b) 国内企業の被害事例

大手製粉会社である株式会社ニップンは、2021年7月9日に公表したシステム障害について、サイバー攻撃による被害であったことを2021年8月16日に公表した[※50]。それによると、2021年7月7日未明から同社グループの大部分のサーバ及び一部の端末に対し、同時多発的にデータが暗号化されるサイバー攻撃が発生したという。また、同社サーバへの不正アクセスにより、企業情報及び個人情報が一部流出した可能性があるとのことだ。同社では事業継続計画を策定していたが、災害時や単体のシステム障害を想定しており、本件のように同時多発的な攻撃を受けることは想定外だったとしている。

同社ではバックアップデータも暗号化されたため、サーバの早期復旧が難しく、通常は財務システムに自動入力される帳票を手作業で作成することになった。また、被害状況の調査、全面的なネットワーク環境の見直し、サーバの再構築等に時間を要することから、2021年度の第1四半期及び第2四半期の決算をそれぞれ延期せざるを得ない状況となった。

本事例は状況から「侵入型ランサムウェア攻撃」及び「二重の脅迫」、もしくはそれに類する攻撃を受けた可能性がある。また、同時多発的に全部または一部のデータを暗号化されたことから、攻撃者が1台ずつランサムウェアに感染させたとは考えにくい。ドメインコントローラのような管理サーバ経由でランサムウェア感染等が行われた可能性も考えられる。

(3) 侵入型ランサムウェア攻撃の手口

前述の被害事例からも分かるように、「侵入型ランサムウェア攻撃」は企業・組織にとって脅威である。ここではその手口について紹介する。

「侵入型ランサムウェア攻撃」は、次の(a)～(e)の五つのステップに分けられる。

(a) ネットワークへの侵入

「侵入型ランサムウェア攻撃」は、攻撃者が企業・組織のネットワークへ侵入するところから始まる。ネットワークへの侵入手口として次のようなものがある。

- ウイルスメールによる侵入
  攻撃者は、企業・組織へ遠隔操作ウイルス等を添付したメールや、遠隔操作ウイルス等をダウンロードさせるURLリンクを記載したメールを送り付ける。受信者が不用意に添付ファイル等を開くことで、遠隔操作ウイルス等に感染させられ、パソコンが乗っ取られる。攻撃者は、そのパソコンを足掛かりとして組織内ネットワークへ侵入する。
- インターネットを経由した侵入
  攻撃者は、企業・組織がインターネット上に公開しているリモートデスクトップサービスやVPN製品を調査し、アクセス制御、認証に関する設定、パスワードの強度が不十分であれば、認証を突破して侵入する。
- 脆弱性を悪用した侵入
  攻撃者は、企業・組織が使用しているVPN製品等に残存する脆弱性を悪用して侵入する（「1.2.5 (1) VPN製品の脆弱性を対象とした攻撃」参照）。

(b) ネットワーク内の侵害範囲拡大

攻撃者は、企業・組織のネットワークへの侵入に成功した後、データの窃取やランサムウェアの感染範囲を広

げる目的で、ネットワーク内で侵害範囲拡大を行う。標的型攻撃同様、ネットワーク構成の把握や管理者権限の奪取を行い、これらの情報を基にして、機微情報等が保存されているパソコンやサーバ、ドメインコントローラ等の管理サーバ、バックアップ用のサーバ等に侵入すると考えられる。ドメインコントローラの一種である Active Directory サーバを掌握されると、グループポリシーによるウイルスの配信が可能となるため、組織内のパソコンやサーバのデータが一斉に暗号化される危険性がある。

(c) データ窃取

データの窃取は、攻撃者が「二重の脅迫」を狙っている場合に行われる。遠隔操作ウイルスを使用する等、攻撃者自身の操作によって、データの探索・収集、攻撃者のサーバやクラウドストレージへのアップロード等が行われる。

(d) データの暗号化・システム停止

攻撃者は身代金を得るために企業・組織のデータをランサムウェアで暗号化し、事業継続に関わる重要なシステムの停止を狙う。また、バックアップデータ等による業務復旧を妨害するため、「1.2.2 (2) ランサムウェア攻撃の被害事例」のように、ネットワーク経由で到達可能であれば、それらのデータも暗号化する可能性がある。

データを暗号化する際に OS の標準機能を使って暗号化する等、セキュリティ製品では検知されない機能を悪用した事例もある。例えば、Windows OS の標準機能である BitLocker を悪用してディスク全体を暗号化する事例が確認されている※51。

(e) 窃取したデータの公開

窃取したデータの公開は、攻撃者が「二重の脅迫」を狙っている場合に行われる。公開方法としては、攻撃者がインターネットやダーク Web 上に設置した、データ公開のための Web サイト（以下、リークサイト）での公開や、オークション形式での販売が挙げられる。攻撃者は窃取したデータをリークサイトで公開する際に、被害者への身代金支払いの圧力を高めるため、窃取したデータを一度にすべて公開するのではなく、一部だけ公開し、指定した期日までに身代金を支払わないと、徐々に公開するデータの範囲を広げるといった声明を出す場合がある。

身代金の交渉には電子メールのほかに、攻撃者が特定サイト内のチャットで個別にやり取りを要求する事例もある※52。

(4) 広く多数のコンピュータを狙うランサムウェア攻撃の手口

「広く多数のコンピュータを狙うランサムウェア攻撃」も依然として確認されており、感染させる手口は以下の (a) ～ (f) の六つが考えられる。なお、これらはランサムウェアに限らず、他のウイルスの感染経路となる可能性がある。

(a) ばらまき型メールによる感染

ばらまき型メールを介して、添付ファイルを開封させる方法や、メール本文の悪意のある URL リンクへ誘導し、「(b) Web サイトからの感染」の手口を使用する方法により、ランサムウェアに感染させる。

(b) Web サイトからの感染

悪意のある Web サイトからダウンロードしたファイルの実行によって感染させる。また、悪意のある Web サイトだけでなく、企業の正規の Web サイトが改ざんされて感染源となる場合もある。

(c) 脆弱性の悪用による感染

更新されていない端末等の OS の脆弱性を悪用し、リモートコードの実行や遠隔操作等で感染させる。また、悪意のある Web サイトにアクセスした際に、端末のソフトウェアの脆弱性を調査して攻撃する「エクスプロイトキット」というツールによって、ランサムウェアに感染させる※53。

(d) ワーム機能による感染

LAN に接続された端末にワーム（自己複製）機能を持つランサムウェアが感染すると、ワーム機能によりネットワークを介して他の端末にもランサムウェアを感染させる。

(e) 不正アプリによる感染

ゲームやセキュリティソフトを装った偽のアプリ（不正アプリ）のインストールによってランサムウェアに感染させる。パソコンだけでなく、スマートフォンやタブレットもランサムウェア感染のリスクがある。

(f) USB メモリ経由による感染

攻撃者が用意した USB メモリからランサムウェアに感染させる。例えば、攻撃者が差出人を偽装した郵送物に USB メモリが入っており、その USB メモリを接続した端末がランサムウェアに感染した事例がある※54。

(5) ランサムウェア攻撃への対策

ここではランサムウェア攻撃に対して、特に重要と考えられる対策について説明する。

(a) セキュリティソフトの導入

セキュリティソフトの導入は「侵入型ランサムウェア攻撃」及び「広く多数のコンピュータを狙うランサムウェア攻撃」双方で有効である。新しいウイルスを検知・駆除するために、セキュリティソフトは最新の状態に保つことも重要となる。ただし、「侵入型ランサムウェア攻撃」では、使用されるウイルスが標的の企業・組織向けにカスタマイズされている場合もあり、セキュリティソフトでは検知しにくい可能性もあるため、他の対策も併用することが望ましい。

(b) 攻撃メール対策

攻撃メール対策は、「侵入型ランサムウェア攻撃」及び「広く多数のコンピュータを狙うランサムウェア攻撃」双方で有効である。攻撃メール対策には、メールのフィルタ機能や、セキュリティ装置等を用いて不審なメールの検知・隔離を行うシステムによる対策や、従業員への教育、啓発、訓練による対策等がある。また、メール利用者一人ひとりが、「身に覚えのないメールの添付ファイルは開かない、怪しいリンクはクリックしない」という意識を持つことが大切である。

(c) 不正アプリ対策

「広く多数のコンピュータを狙うランサムウェア攻撃」で使われる不正アプリは、主に非公式なアプリストアから配布される。改ざんされた Web サイト等では「ソフトウェアアップデート」や「システムエラー」の画面を表示して非公式のアプリストアへ誘導するため、これらの表示が出た場合は、ブラウザを閉じることで対処する。また、公式のアプリストアにも不正アプリが紛れ込んでいる場合があるため、注意が必要である。提供元が不明な信頼できないアプリのインストールをしないことが大切である。

(d) 脆弱性対策

脆弱性を悪用したウイルス感染やネットワークへの侵入を防ぐために、パソコンやサーバの OS 及び利用ソフトウェア、ネットワーク機器のファームウェア等を常に最新の状態に保つことは「侵入型ランサムウェア攻撃」及び「広く多数のコンピュータを狙うランサムウェア攻撃」双方で有効である。インターネットを経由して企業・組織内のネットワークに接続するための VPN 装置が攻撃者によく狙われるため、企業・組織では特に注意が必要である。また、脆弱性が公開されてから、その脆弱性が悪用されるまでの期間が短くなっていることから、公開された脆弱性に迅速に対応できるよう体制や計画を整えておくことが大切である。

(e) 企業・組織のネットワークへの侵入対策

「侵入型ランサムウェア攻撃」は、攻撃者が企業・組織内のネットワークへ侵入することから始まる。そのため、次のような侵入対策を行うことが重要である。

- 攻撃対象領域の最小化
  インターネットからアクセス可能な、意図的に公開するサーバやネットワーク機器等を最小限にするとともに、アクセス可能なプロトコルやサービスも最小限にする。また、誤ってインターネットに公開している機器等がないか確認を行う。更に、それらの機器が乗っ取られる可能性を考慮し、そこからアクセス可能な範囲を限定する。例えば、不用意にリモートデスクトップサービスをインターネット上に公開しない、業務に必要なサーバ等をインターネット上に公開する場合は、どの機器を公開しているか等の管理を行う、といった対策が挙げられる。
- アクセス制御と認証
  企業・組織外からアクセス可能な機器等を最小限にした上で、それらが攻撃者に不正に操作されないよう、適切なアクセス制御と認証を行う必要がある。例えば、運用上、機器へのアクセスが国内からのみであれば、海外の IP アドレスからのアクセスを遮断するといった対策が考えられる。また、多要素認証のような強固な認証方式を使用して、認証を突破しにくくすることや、アクセスや認証のログを取得、監視して、不審な行為や攻撃の検知を試みることも有効である。
- 拠点間ネットワークのセキュリティ強化
  ランサムウェア攻撃に限らず、自組織で複数の拠点をネットワークで接続している場合、例えば十分にセキュリティ対策ができていない防御の弱い海外拠点から侵入され、組織の中枢が侵害される場合がある（「1.2.1 (1) (b) 国内企業の海外拠点を狙った未公開の脆弱性を悪用した標的型攻撃」参照）。必要に応じ、拠点間のアクセス制御の強化も検討する。

(f) ネットワーク内の侵害範囲拡大への対策

「侵入型ランサムウェア攻撃」を受けた場合、企業・

組織のネットワーク内における不審な活動を検知し、攻撃の早期発見と対応につなげる。統合ログ管理、内部ネットワーク監視、エンドポイント監視といった仕組み（製品等）を活用し、ネットワークのスキャン、通常発生しない不正な通信や認証の試行、無許可のユーザアカウント作成等の操作、無許可のプログラム設置・実行、イベントログの削除、シャドウコピーの削除等の攻撃者の活動を検知する。

被害者は、データの暗号化やシステム停止を受けて初めて、攻撃を受けていることを認識する場合があるが、データの暗号化等がされてからの対策・対応は困難であるため、より早期の検知を可能にすることが望ましい。

(g) バックアップからの復旧

「侵入型ランサムウェア攻撃」への対策として重要なことは、データの保護のみならず、「システムの再構築を含めた復旧計画」を事前に策定し、バックアップからの復旧を可能にしておくことである。「1.2.2 (2) ランサムウェア攻撃の被害事例」にもあるように、企業・組織のパソコンやサーバ等がバックアップも含めて一斉に暗号化される可能性がある。こうした状況に備え、事業継続に重要なデータやシステムのバックアップデータをオフラインで管理するほか、必要に応じて業務継続やシステムの再構築に必要なリソース等を考慮した復旧計画を策定しておくことが大切である。

(h) データの窃取と公開への対策

「侵入型ランサムウェア攻撃」によりデータが窃取され、意図せず公開される脅威への対策として、IRM（Information Rights Management）[※55] 等の活用や、ネットワーク分離が挙げられる。IRM を活用し、データが窃取されても被害を限定的な範囲に留める。また、ネットワーク分離では、例えば、メールの送受信や Web 閲覧等で使用する一般的な業務用のネットワークと機密情報等を取り扱うネットワークを分離する。こうすることで、攻撃者に業務用のネットワークに侵入されたとしても、機密情報等を取り扱うネットワークには到達されないようにする。ただし、ネットワーク分離は運用コストや利便性に著しい影響があるため、機密情報等の重要性やリスクを踏まえて実施を検討する必要がある。

(i) インシデント対応

ランサムウェア攻撃の被害を受けてしまった際のインシデント対応はケースバイケースとなるが、「侵入型ランサムウェア攻撃」は、侵入の手口が標的型攻撃と同様のため、対応も全体的に標的型攻撃と同様となる（「1.2.1 (5) (b) 組織としての対応体制の強化」参照）。インシデント対応の一般的な進め方について、JPCERT/CC がマニュアル[※56] を公開しているため、参照いただきたい。また、データ暗号化と身代金要求への対応については JPCERT/CC が侵入型ランサムウェア攻撃を受けた際の FAQ[※57] についても公開しているため、こちらも参照いただきたい。

ランサムウェア攻撃のインシデント対応において、留意すべき点として、「ステークホルダーとのコミュニケーションができる体制作り」がある。ランサムウェア攻撃では、一般のインシデントと異なり、業務停止や顧客・取引先の情報漏えいが発生し、自組織内に閉じたインシデントで終わらない傾向がある。ステークホルダーとの適切で素早い連絡・調整を含む、経営層を含めた体制作りが必要である。

1.2.3 ビジネスメール詐欺（BEC）

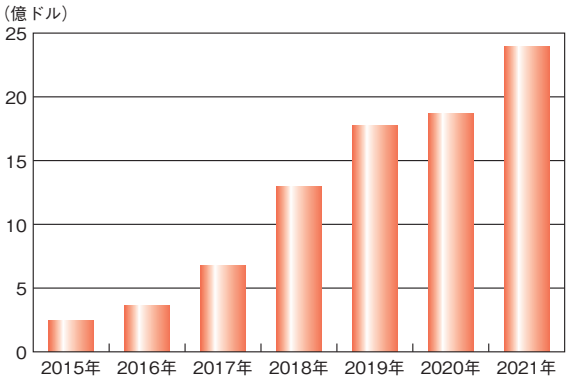
ビジネスメール詐欺（BEC：Business Email Compromise）は、巧妙な騙しの手口を駆使した偽のメールを企業・組織に送り付け、従業員を騙して送金取り引きに関わる資金を詐取する等の金銭被害をもたらすサイバー攻撃である。偽のメールを送るための前段階として、企業の従業員や取引先のメールアカウント情報を狙うため、フィッシング攻撃や情報を窃取するウイルスが使用されることもある。

本項では、2021 年度に公表されたビジネスメール詐欺の状況、事例を紹介し、その巧妙な手口と対策について解説する。

(1) ビジネスメール詐欺の被害状況

FBI のインターネット犯罪苦情センター（IC3：Internet Crime Complaint Center）が 2022 年 3 月に公開した年次報告書[※58] によると、2021 年度に報告されたビジネスメール詐欺の被害総額は、前年比約 1.3 倍の約 23 億 9,600 万ドル（未遂を含む）となっている。また、2015 年から 2021 年までに発生した被害総額の推移をグラフで表すと、被害額が増加傾向にあることから、ビジネスメール詐欺の脅威がより深刻なものになっていることが分かる（次ページ図 1-2-4）。

また、トレンドマイクロ社の報告によれば、同社のセキュリティ製品がビジネスメール詐欺と判定・検出したメール



■図 1-2-4　ビジネスメール詐欺の被害総額推移
（出典）IC3 年次報告書を基に IPA が作成

の件数が、2021 年の 1 月から 9 月にかけて徐々に増加しているという。特に 7 月から 9 月においては、検出数が約 5 万件と、新型コロナウイルス拡大前の 2019 年の同時期と比較して、約 3.5 倍になったとしている※59。また、国際的なフィッシング対策の非営利団体である APWG の報告によると、2021 年 5 月に、給与振込口座を変更させる手口が電信送金を利用する手口を上回り、増加したという※60。

一方で、世界の法執行機関等がビジネスメール詐欺の容疑者を逮捕・起訴する事例も多数公表されている。2021 年の 6 月から 9 月までの 4 ヵ月間に行われた「HAECHI-II」と呼ばれる国際的な取り締まりでは、ビジネスメール詐欺等に関わっていた 1,003 人を逮捕し、金銭の詐取等に悪用されていた約 2,350 件の口座を凍結させ、約 2,700 万ドルの資金を押収することに成功したという※61。また、「情報セキュリティ白書 2021」の「1.2.3（1）ビジネスメール詐欺の被害状況」で紹介した、国際刑事警察機構（ICPO：International Criminal Police Organization、INTERPOL とも呼ばれる）やナイジェリア警察等が行った共同調査による逮捕事例に関連し、2022 年 1 月、同じ犯罪組織のメンバーと見られる 11 人の容疑者が新たに逮捕された。逮捕された容疑者の一人は、自身のパソコン上に攻撃対象と思われる 80 万件以上のアカウント情報を所持していたという※62。そのほか、米国司法省（U.S. Department of Justice）の発表※63 によれば、ビジネスメール詐欺等を行い、少なくとも 100 人の被害者から 1,700 万ドル以上の金銭を詐取した 33 人の容疑者が逮捕されたほか、欧州においても、ビジネスメール詐欺等に関わっていたとされる 106 人の容疑者が逮捕されている※64。

（2）2021 年度に報道された事例の概要

2021 年度においても国内外で金銭被害に遭った事例が多数確認されている。国内で発生した事例としては、大手眼鏡販売チェーンの持株会社である株式会社ビジョナリーホールディングスの子会社の株式会社 VISIONIZE に対し、取引先関係者をかたった人物から仕入代金の送金を促すメールが送られ、当該子会社が約 1 億円を送金してしまったという※65。また、国内企業の海外子会社で発生した事例では、加賀電子株式会社の海外子会社が悪意の第三者による虚偽の送金指示に騙され、約 5 億円の資金を流出させてしまったという※66。海外で発生した事例では、韓国の航空関連企業である韓国航空宇宙産業に対し、取引先企業のメールアカウントを乗っ取った攻撃者が担当者になりすまして、口座を変更したという旨の偽メールを送ってきたという。当該企業の担当者は、そのメールを取引先企業からの正規のメールだと思い込み、約 16 億ウォンを送金してしまったという※67。

一方で、詐取された金銭を回収できた事例もあった。米国ミネソタ州レッドウッドフォール市で起きた事例では、同市が消防車の売買に関する担当者をかたった攻撃者とやり取りし、約 120 万ドルを送金してしまったが、調査の過程で資金が見つかったため、同市へと返還されることになったという※68。

（3）IPA が情報提供を受けた事例の概要

IPA では、実際に試みられたビジネスメール詐欺の事例を基に、2017 年 4 月、2018 年 8 月に続き、2020 年 4 月に第三報として注意喚起を行った。また、サイバー情報共有イニシアティブ（J-CSIP：Initiative for Cyber Security Information Sharing Partnership of Japan）の運用状況レポートでも事例を公開している。

IPA が情報提供を受けたビジネスメール詐欺事例のうち、J-CSIP の運用状況レポートにて 2021 年度に公開した事例の概要を表 1-2-1（次ページ）に示す。なお、このうちの 1 件（表 1-2-1 の項番 3）については、金銭的被害が確認されている。残り 8 件については、メールの受信者等が不審であることに気付いたため、被害を防ぐことができている。

（4）IPA が情報提供を受けた事例

ここでは、IPA が 2021 年度に公開したビジネスメール詐欺事例の中から特筆すべき表 1-2-1（次ページ）の項番 3 と 8 について紹介する。

項番	事例概要	被害の有無	備考
1	2021 年 1 月、国内企業の取締役になりすました攻撃者から、海外グループ企業の担当者に対してビジネスメール詐欺が試みられた。	なし	「サイバー情報共有イニシアティブ（J-CSIP）運用状況［2021 年 1 月～ 3 月］[※69]」に記載
2	2021 年 2 月、取引先ではない海外企業の担当者になりすました攻撃者から、国内企業の担当者に対し、偽の口座への支払いを要求するメールが送られた。	なし	同上
3	2021 年 4 月、国内企業の海外関連企業（請求側）と、海外取引先企業（支払側）との取り引きにおいて、請求側企業の担当者になりすました攻撃者から、偽の口座への振り込みを要求するメールが送られ、支払側企業の担当者が送金した。	あり	「サイバー情報共有イニシアティブ（J-CSIP）運用状況［2021 年 4 月～ 6 月］[※70]」に記載
4	2021 年 5 月、国内企業の役員になりすました攻撃者から、当該企業の複数の担当者に対して、同一内容の偽メールを送り付けるビジネスメール詐欺が試みられた。	なし	同上
5	2021 年 6 月、国内企業の役員になりすました攻撃者から、当該企業の複数の担当者に対して、英語と日本語で書かれた偽メールを送り付けるビジネスメール詐欺が試みられた。	なし	同上
6	2021 年 8 月、国内企業の海外関連企業の役員になりすました攻撃者から、当該企業の担当者に対して、ビジネスメール詐欺が試みられた。	なし	「サイバー情報共有イニシアティブ（J-CSIP）運用状況［2021 年 7 月～ 9 月］[※71]」に記載
7	2021 年 9 月、国内企業（支払側）と、海外取引先（請求側）との取り引きにおいて、請求側企業の担当者になりすました攻撃者から、偽の口座への振り込みを要求するメールを送り付けるビジネスメール詐欺が試みられた。	なし	「サイバー情報共有イニシアティブ（J-CSIP）運用状況［2021 年 10 月～ 12 月］[※72]」に記載
8	2021 年 10 月、国内企業の代表取締役になりすました攻撃者から、当該企業の複数の役員に対して、約 2 時間の間に 17 通の偽メールを送り付けるビジネスメール詐欺が試みられた。	なし	同上
9	2021 年 10 月、国内企業の役員になりすました攻撃者から、当該企業の人事部門の担当者に対して、ビジネスメール詐欺が試みられた。	なし	同上

■表 1-2-1　IPA が情報提供を受け 2021 年度に公開したビジネスメール詐欺事例の概要

また、「情報セキュリティ白書 2020」の「1.2.2 (4) (b) CEO を詐称する一連の攻撃」で紹介した事例、及び、注意喚起の第三報の「『日本語化』された CEO 詐称の攻撃」で紹介した事例について、引き続き、多数の情報提供を受けたため、それぞれの概要を紹介する。なお、攻撃メールに見られる特徴等に関しては、表 1-2-1 の「備考」に記載した各レポートを参照いただきたい。

(a) 偽の口座への振り込みを要求する攻撃事例

本事例は、2021 年 4 月、J-CSIP の参加組織（国内企業）の海外関連企業（A 社：請求側）と、その海外取引先企業（B 社：支払側）との間で取り引きを行っている中、A 社の担当者になりすました攻撃者から、偽の口座への振り込みを要求するメールが送られたものである。B 社の担当者が攻撃者の用意した偽の口座へと送金を行ってしまったため、金銭的な被害が発生した。

この手口は、IPA が 2017 年 4 月に公開した注意喚起[※73] で紹介しているビジネスメール詐欺の五つのタイプのうち、「タイプ 1:取引先との請求書の偽装」に該当する。

今回の事例では、やり取りされたメールはすべて英文であり、詐欺の過程において、次の手口が使われた。

- A 社と B 社のやり取りへ介入
- 正規のメールアドレスに似せた偽の詐称用ドメインの悪用
- メールの転送設定によるメールの盗聴

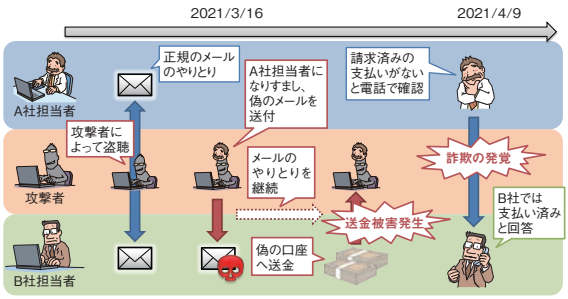
(ア) A 社と B 社のやり取りへ介入

A 社（海外関連企業）と、B 社（海外取引先）との間で、取り引きに係るビジネスメールをやり取りしている中、2021 年 3 月 16 日に攻撃者から B 社の担当者へ偽のメールが送られた。その後、B 社担当者と攻撃者間で複数回メールのやり取りを継続したと見られるが、詳細は情報提供外のため不明である。そのやり取りの中で、B 社担当者は攻撃者が用意した偽の口座へ支払いをしてしまったため、金銭的被害が発生した。

攻撃に関係したメールのやり取りを図 1-2-5（次ページ）に示す。

その後、2021 年 4 月 9 日に A 社から B 社へ、請求中の支払いがないため連絡をしたところ、B 社からは支払い済みであると回答を受けたことで事案が発覚した。B 社では偽の口座への振り込みの取り消し対応を行っており、当該口座は凍結されたとのことだが、送金した資金が回収できたかは不明である。

なお、本件で攻撃者が用意した偽の口座は、同時期



■図 1-2-5　攻撃者とのやり取り
（出典）IPA「サイバー情報共有イニシアティブ（J-CSIP）運用状況［2021年４月～６月］」

に本件とは別のビジネスメール詐欺と思われる詐欺行為でも悪用されていたことが判明している。攻撃者が、被害者を騙して振り込ませる口座を、複数の犯罪に使い回していることは推測されていたが、実際に複数の会社に対するビジネスメール詐欺が関係していたということが本事例をとおして確認された。

ビジネスメール詐欺にて確認した偽の口座情報を、銀行や警察等と連携することで、攻撃者の口座を凍結し、別の企業等に行われているビジネスメール詐欺の被害を未然に防げる可能性がある。攻撃者の口座が判明した際は、速やかに銀行や警察等へ連絡することを検討いただきたい。

（イ）正規のメールアドレスに似せた偽の詐称用ドメインの悪用

攻撃者からＢ社の担当者へ送られた偽メールでは、Ａ社の正規のドメインに似通った「詐称用ドメイン」がメールの送信に使用されていた。詐称用ドメインは、最初の攻撃メールが送られた当日（2021 年３月 16 日）に新規に取得され、図 1-2-6 に示すように、正規のドメイン名を１文字変更したものであった。

【本物のメールアドレス】alice @ abccompany-a . com
【偽物のメールアドレス】alice @ abcccompany-a . com
（「c」を一文字追加）

※実際に悪用されたものとは異なる。

■図 1-2-6　Ａ社の詐称用ドメインの例（Ｂ社へ送られた偽メールで使われたドメインの例）
（出典）IPA「サイバー情報共有イニシアティブ（J-CSIP）運用状況［2021年４月～６月］」

（ウ）メールの転送設定によるメールの盗聴

攻撃者は何らかの方法でＢ社の Microsoft 365 のメールアカウントへ不正アクセスし、正規のＡ社の担当者から送られたメールを攻撃者の元へ転送するように設定していた。この設定を行うことで、攻撃者はＢ社が利用していたメールサービスに定期的にログインすることなく、Ａ社とＢ社のやり取りを盗み見ることが可能となっていたと見られる。

（b）経営者をかたる日本語の攻撃事例

本事例は、2021 年 10 月、J-CSIP の参加組織（国内企業）の複数の役員に対し、同社の代表取締役になりすました攻撃者から、約２時間の間に 17 通の偽のメールが送られたと情報提供があったものである。

攻撃者から送られた偽のメールは日本語であり、機密事項について助けが必要だという内容で、受信者に返信を依頼するものであった。メールの下部には実在する日本の弁護士事務所の弁護士から連絡があったように見せかける偽の内容が記載されていた。

本事例で、攻撃者から送られたメールを図 1-2-7 に示す。

■図 1-2-7　実在する代表取締役と弁護士を詐称する日本語のメール
（出典）IPA「サイバー情報共有イニシアティブ（J-CSIP）運用状況［2021年 10 月～ 12 月］」

本メールの送信者のメールアドレスには、日本の金融庁のドメインに似た偽のメールアドレスも記載されており、この偽のメールアドレスへ返信されるように細工されていた。また、同報先（CC）には、弁護士のメールアドレスをかたった偽のメールアドレスが設定されており、あたかも

弁護士にも同報されているかのように見せかけていた。

このメールについては、IPA が 2018 年 8 月に公開した注意喚起の続報※74 のレポート事例 1 と同じ手口であり、継続して類似した攻撃が行われているものと推測される。

普段英語のメールでやり取りを行わないような企業や組織であっても、日本語で書かれた偽のメールが着信する可能性があるため、引き続き注意が必要である。

(c) CEO を詐称する一連の攻撃

2021 年においても、CEO（Chief Executive Officer）詐欺について継続して情報提供があった。更に IPA で J-CSIP 外の情報等を含め独自に調査を行ったところ、複数の類似するメール検体を入手した。

本項では、これら二つの CEO 詐欺について説明する。

- 複数組織へ行われた CEO を詐称する一連の攻撃
- 「日本語化」された CEO 詐欺の攻撃

複数組織へ行われた CEO を詐称する一連の攻撃については、2021 年に 34 件の情報提供を受け、これまでに 207 件のメール検体を入手している。本攻撃は、2019 年 7 月以降継続して観測しており、国内外の複数の組織を対象として行われた痕跡を確認している。メールの件名や内容は時期ごとに変化が見られるが、メールのヘッダ情報に類似する点があり、一連の攻撃は同一の攻撃者によるものと推測している。また、本攻撃メールについては、米国のセキュリティベンダが公開しているレポートと同様の手口であることを確認している※75。

「日本語化」された CEO 詐欺の攻撃については、2021 年に 15 件の情報提供を受け、これまでに 68 件のメール検体を入手している。本攻撃は、2019 年 11 月以降継続して観測しており、国内外の複数の組織を対象として行われた痕跡を確認している。メールの件名や内容は一部に変化が見られるが、ほぼ同じ内容のメールであり、メールのヘッダ情報や、「SendGrid」や「SMTP2GO」というメールサービスを使用する場合がある等類似する点があり、一連の攻撃は同一の攻撃者によるものと推測している。

これら二つの CEO 詐欺は、特定の組織や業種を狙うものではなく、多くの業種に対して試みられたことを確認している。このため、業種に関わらず、今後も継続して国内外の組織に対して攻撃が行われる可能性があり、注意が必要である。

(5) ビジネスメール詐欺の騙しの手口

ビジネスメール詐欺で用いられる騙しの手口は様々である。詳細は「情報セキュリティ白書 2020」の「1.2.2 (5) ビジネスメール詐欺の騙しの手口」にて、実際に使われた具体的な手口を紹介しているため、そちらを参照いただきたい。

なお、攻撃者は被害者から金銭を詐取するために、手口を多様に組み合わせて巧妙に攻撃を仕掛ける場合や、「新型コロナウイルスによる影響のため、通常の取引手続きではない方法で支払ってほしい」等と時流に沿った口実を使って被害者を騙そうとする等、手口を新しくしながら攻撃を行っていることを認識しておく必要がある。

(6) ビジネスメール詐欺への対策

ビジネスメール詐欺への対策を以下にまとめる。日頃からビジネスメール詐欺への意識を高め、組織内の送金チェック体制や監視体制、被害に遭ったときの迅速な対応体制を整えておくことが重要である。

また、JPCERT/CC や株式会社マクニカ、PwC の報告書等も、対策・対応について記載されており、そちらも活用いただきたい※76。

(a) ビジネスメール詐欺の周知徹底と情報共有

ビジネスメール詐欺は、企業間のビジネス活動がメールに依存している点を悪用した巧妙な騙しの手口であり、その手口を知らなければ、被害を防止することは困難である。ビジネスメール詐欺におけるなりすましは外部企業との取り引きだけでなく、グループ会社同士の取り引きにおいても発生している。このため、海外関連企業を含む全グループ企業の全従業員に対して詐欺の手口について周知徹底し、ビジネスメール詐欺への意識を高めておくことが重要である。特に、最高財務責任者（CFO：Chief Financial Officer）や経理部門等の金銭を取り扱う担当者が、ビジネスメール詐欺の脅威についてよく理解し、送金前に攻撃に気付くことができれば、金銭的な被害を未然に防ぐ可能性が高まる。

また、メールに普段とは異なる言い回しや表現の誤りがあった、突然送信エラーメールを受信するようになった等、不審な兆候が見られた場合、CSIRT 等の社内の適切な部門に報告できる体制を整え、その情報を組織内外で共有することも重要である。ビジネスメール詐欺は、自組織だけではなく、取引先にも被害が及ぶことがあり、取引先と情報を共有することにより、サプライチェー

ン全体でビジネスメール詐欺への耐性を高めることができる。もし、自組織を詐称したビジネスメール詐欺を確認した場合や自組織が被害に巻き込まれた場合は、取引先や、警察、金融機関へ報告し、同様の攻撃に対する注意喚起を行うといった体制を整えておくことで、更なる被害拡大を防ぐことが可能となる。

(b)電子署名等によるなりすまし防止

ビジネスメール詐欺は、メールのやり取りにおいて本物の担当者になりすますことで攻撃を成立させる。そのため、取引先と連携した対策として、請求書等の重要情報をメールで送受信する際は電子署名を付ける等の手段で、なりすましを防止する対策が有効である。

(c)送金処理のチェック体制強化

ビジネスメール詐欺の被害を防止するためには、送金時のチェック体制を強化することが最も重要である。金銭を取り扱う担当者は、通常と異なる対応（役員等権威ある立場からの通常の手順とは異なる支払い依頼や、企業間取り引きにおいて別の口座への突然の変更依頼、見積価格の修正、支払方法の変更、急なメールアドレス変更等）を求められた場合は、ビジネスメール詐欺を疑い、別の担当者とダブルチェックを行うことや、信頼できる方法で入手した連絡先に、電話やFAX等のメール以外の手段で事実を確認するといった、二重三重のチェックを行う体制とすることが必要である。

(d)攻撃に使われるメールアドレスへの対策

ビジネスメール詐欺において、攻撃者がメールを偽装する方法は様々であるが、偽のメールだと気付かず返信してしまった場合でも、送信先や返信先に設定されているメールアドレスに注意していれば、攻撃と見抜ける可能性があった事例が多く見られるため、送信前にメールアドレスが正しいかどうか、落ち着いて確認していただきたい。

ビジネスメール詐欺で使われるメール偽装の手口として、フリーメールを悪用する場合や、自組織のドメイン名に似せた詐称用のドメインを取得し、そのドメインのメールアドレスを用いて攻撃を行う場合がある。フリーメールや自組織外のメールアドレスから着信したメールについて、件名や本文にその旨の警告を表示するメールシステムを採用すれば、従業員がそれらのメールを見分けやすくなる。なお、このようなメールシステムを利用していても、取引先の企業でフリーメールをビジネスに使っている場合や、攻撃者が取引先等のドメイン名に似せた詐称用のドメインを取得し、そのドメインのメールアドレスを用いる場合等、正しいメールと偽のメールの区別がつきにくい場合があるため、注意が必要である。また、送信元（Fromヘッダ）を正しい送信者のメールアドレスに偽装し、返信先（Reply-Toヘッダ）を攻撃者のメールアドレスにする手口もあり、送信元（Fromヘッダ）と返信先（Reply-Toヘッダ）が異なる際に警告を表示する機能があるメールシステムを導入することも対策として有効である。

(e)フィッシング・ウイルス・不正アクセス対策

ビジネスメール詐欺を行う攻撃者は、攻撃に至る前に、何らかの方法でメールのやり取りを盗み見ている場合がある。その方法として、フィッシング攻撃によるメールアカウントの詐取、ウイルス感染等によるメールの内容やメールアカウント情報の窃取、メールサーバやメールアカウントへの不正アクセス等がある。そのため、基本的なフィッシング対策・ウイルス対策・不正アクセス対策を徹底していただきたい。

特に、Microsoft 365やGoogle Workspace（旧称、G Suite）等のようなクラウド型サービスを利用している場合は、多要素認証等を活用し、第三者による不正ログインを防ぐことが重要である。

また、攻撃者によってメールアカウントが乗っ取られ、利用者本人が行っていない転送設定やフォルダの振り分け設定がされている等、不正利用の兆候があった場合には、Microsoft社等より該当アカウントへの対処方法※77が公開されているため、そちらを参照いただきたい。

1.2.4 DDoS攻撃

DDoS（Distributed Denial of Service）攻撃とは、Webサーバ等の攻撃対象に対して複数の送信元から同時に大量のパケットを送信することで、攻撃対象のリソースに負荷をかけ、サービス運用を妨害する攻撃である。

本項では、2021年度に確認されたDDoS攻撃について事例と対策を解説する。

(1)DDoS攻撃の動向

セキュリティベンダによると、2021年上半期に全世界で確認されたDDoS攻撃は、過去最多となる540万回で、前年同期と比較して11%増加した※78。2020年以降、DDoS攻撃は急激に増加しているが、これは、新型コロナウイルスの世界的蔓延とロックダウン等の影響に

より、多くの日常的な活動がオンラインに移行したことで、潜在的な攻撃対象が増加したことが原因である可能性が高いとされる※79。

ここでは、2021 年度における、DDoS 攻撃に関する主だった事例を紹介する。

(a)リフレクション攻撃の事例

通信プロトコルの中には、リクエストよりもレスポンスのデータサイズが大きくなるものがある。攻撃者がそのような仕様を悪用し、送信元を攻撃対象のアドレスに偽装したリクエストを大量に送信することで、増幅されたレスポンスが攻撃対象のアドレスに宛てて送信される。攻撃対象は、大量のデータを受信することになり、処理能力の限界を迎え、サービスのパフォーマンス低下や停止を起こす。このような DDoS 攻撃は「リフレクション攻撃」と呼ばれる。

リフレクション攻撃では、外部に公開されている UDP (User Datagram Protocol)※80を用いて通信を行うサービス (以下、UDP サービス) を悪用した攻撃が多く観測されている。UDP サービスを悪用した攻撃では、UDP の以下の三つの特徴が悪用される。

①要求パケットの送信元 IP アドレスを確認しない。このため、送信元を偽装しやすい。
②要求パケットの長さよりも応答パケットの長さが大きくなる増幅効果(Amplification)がある。
③ UDP サービスを提供するサーバ(以下、UDP サーバ)へ行われたリクエストは、応答パケットとして、送信元ホスト (攻撃においては送信元に偽装された攻撃対象のホスト)へ反射(Reflection)される。

UDP サービスが DDoS 攻撃に悪用されると、①の特徴により攻撃元の特定が難しく、②③の特徴を悪用することで、送信するデータ量を数十倍から数百倍に増幅させた攻撃が可能となる。また、インターネット上からアクセス可能な UDP サーバへの通信そのものは正常であるため、攻撃が行われていることを把握し対応を行うには、後述の「1.2.4 (3) (b) 攻撃に加担しないための対策」が必要となる。

UDP サービスを悪用したリフレクション攻撃は、2021 年も定常的に確認されており、11 月には、Microsoft Azure のアジアユーザを対象とした、3.47Tbps(テラビット／秒)という過去最大規模の DDoS 攻撃が行われた※81。この事例では、大規模な DDoS 攻撃の兆候を検知した時点で、その攻撃に対する緩和策を既に Microsoft 社が構築・実施していたために被害は発生しなかったが、このようなリフレクション攻撃の頻度と規模は近年ますます増加している。

(b) オリンピック期間中に確認された DDoS 攻撃

CDN (Content Delivery Network)※82 事業者により、東京 2020 オリンピック・パラリンピック競技大会の競技開始後の日本国内への DDoS 攻撃の件数が、通常時の 10 倍以上に増加したとする調査データが公開された※83。

オリンピック・パラリンピックの開催中は、開催国へのサイバー攻撃が集中することがこれまでも観測されており、東京 2020 オリンピック・パラリンピック競技大会でも、攻撃が集中することが予測されていた。本大会では、組織委員会や関係機関が、開催前から攻撃への対策を強化すると宣言する等、事前に対策に乗り出していたこともあり、大会の開催期間中に運営に支障が出るような被害は生じなかった。

(2) DDoS 攻撃を行うボットネットの拡大

DDoS 攻撃には、ボットネットと呼ばれる攻撃用ネットワークが使用される場合がある。ボットネットは、攻撃者が乗っ取った多数のコンピュータ、ネットワーク機器、IoT 機器等と、それらに対して遠隔で指令を送信するための C&C サーバで構成されている。攻撃者が C&C サーバを介して、ボットネットに攻撃指令を送信することで、ボットネットを構成する機器が一斉に攻撃を行う。ボットネットを構成する機器のほとんどは組織や家庭で利用されているもので、サービスやソフトウェアの脆弱性を悪用されたりウイルスに感染させられたりした結果、制御を奪われた機器である。

攻撃者は、より多くの機器を乗っ取るため、アップデートを繰り返すことで、最新の悪用手法等を取り入れ、様々なターゲットに対して攻撃を繰り返しながらボットネットを拡大させ、大規模な DDoS 攻撃等を実行する。

2021 年 6 月末ごろから、IoT 機器を悪用して DDoS 攻撃を仕掛ける「Mēris」と呼ばれるボットネットが新たに観測された※84。Mēris による攻撃トラフィックは、2016 年に猛威を振るった IoT マルウェアである Mirai※85 にて観測されたものの約 3 倍規模に相当し、Cloudflare, Inc. では 1,720 万 rps (リクエスト／秒) という大規模な DDoS 攻撃が確認されている※86。

このようなボットネットは、攻撃ツールとして、DDoS 代行サービスを通じて有償で貸し出されることがある。拡大

したボットネットが DDoS 代行サービスに使用され、攻撃者がそれを購入することで比較的手軽に悪用できることが、大規模な DDoS 攻撃が発生しやすくなる要因となっている。

(3) DDoS 攻撃への対策

DDoS 攻撃への対策では、DDoS 攻撃の被害に遭った場合の対策に加えて、管理または所有する機器が乗っ取られ、DDoS 攻撃に加担することを防ぐための対策も求められる。これらの対策について解説する。

(a) DDoS 攻撃の被害に遭った場合の対策

DDoS 攻撃によって送られてくる通信データを遮断し、サービスを提供するサーバやネットワークのリソースを保護する対策が必要である。正常なアクセスと DDoS 攻撃によるアクセスを、どのように切り分けるかが対策のポイントとなる。以下に、具体的な対処方法を挙げる。

- アクセスログや通信ログ等を確認し、攻撃が特定の IP アドレスから行われていると判断できる場合は、当該 IP アドレスからのアクセスを遮断する。
- 国内からのアクセスを主に想定しているサイトでは、海外の IP アドレスからのアクセスを一時的に遮断することを検討する。
- 攻撃者が攻撃元の IP アドレスや攻撃方法を定期的に変更してくる場合があるため、継続して監視を行い、攻撃方法に合わせた対策を実施する。
- 攻撃の頻度や、攻撃対象サイトの重要性によっては、ISP 事業者が提供する DDoS 攻撃対策サービスやセキュリティベンダ等が提供する DDoS 攻撃対策製品の利用を検討する。
- 組織内で対処しきれない程、大規模な攻撃や執拗な攻撃を受けている場合は、ISP 事業者との対策協議等の連携や警察等への通報を実施する。

(b) 攻撃に加担しないための対策

自組織や個人で使用する機器が DDoS 攻撃に悪用されないように、セキュリティソフトを導入したり、適切な設定をしたりといった対策が必要である。また企業においては、自組織の機器を悪用された場合に、それを早期に検知できるように通信の監視を行うといった対策も推奨する。以下に、具体的な対処方法を挙げる。

- IoT 機器の OS やファームウェアを最新の状態に保ち、脆弱性の悪用により制御を奪われることを防ぐ。
- パスワードが初期設定のままの機器が存在しないか確認し、存在した場合は適切なパスワードに変更する。パスワードが初期設定のままの機器は、攻撃者により容易に侵入され、制御を奪われてしまう可能性がある。
- 外部と接続しているネットワーク機器や IoT 機器をとおして組織内の他の機器に対して感染拡大を試みるウイルスも確認されているため、インターネットに直接接続していない機器においても脆弱性対策等を行う。
- 組織内で稼働しているプリンタ等の機器や、自組織が外部で管理している Web カメラや気象センサー等の機器を洗い出し、DDoS 攻撃に悪用される可能性があるサービスやソフトウェアが適切に運用されていることを確認する。具体的には、これらのサービスやソフトウェアが稼働する機器に関して、OS を始め、各サービス等が脆弱性を含むバージョンで稼働していないことや、DDoS 攻撃に悪用される設定になっていないことを確認する。また、それらのサービスを組織内のみで利用している場合でも、意図せずインターネット上に公開していないかを確認する。
- 組織内の機器の外向きの通信を監視し、異常な通信を確認した場合は、攻撃の踏み台となっている可能性がある。そういった機器は、ウイルス感染等が生じていないか調査し、対処を行う。自組織での対処が困難な場合は関係当局やセキュリティベンダ等への相談を検討する。

1.2.5 ソフトウェアの脆弱性を悪用した攻撃

2021 年度は、2020 年度に引き続き VPN 製品の脆弱性を狙った攻撃が多く報告された。また、多くの利用者がいる Microsoft 製品や、多数の IoT 製品に影響があるとされる脆弱性も報告された。

本項では、これらの脆弱性を悪用した攻撃の状況と対策について解説する。

(1) VPN 製品の脆弱性を対象とした攻撃

VPN は、専用のネットワーク回線を仮想的に構築することで、物理的に離れている拠点のネットワーク間を、あたかも同一のネットワークであるかのように接続する技術である。拠点のネットワークと離れた場所にあるパソコン等を安全に接続するために、VPN は使用される。

2021 年度は、新型コロナウイルス感染拡大防止のため、2020 年度に引き続きテレワークが強く推奨された影響もあり、VPN 製品の脆弱性を悪用した攻撃数が依然として高い水準で推移した※87。また、VPN 製品の新

たな脆弱性が相次いで発見され、脆弱性が解消されていない製品を狙った攻撃も多数報告された。

(a) 攻撃事例

2021 年 2 月 に、SonicWall, Inc. 製 SonicWall SMA100 シリーズの SSL-VPN 機能に関して、SQL インジェクション※88 の脆弱性（CVE-2021-20016※89）が公表された。

この脆弱性は、SSL VPN ポータルに存在する。攻撃者は、細工したリクエストをポータルに送信することで、認証を必要とせずに SQL 文を実行し、認証やセッションに関連する情報にアクセスできる可能性があった。

2021 年 1 月 22 日、同社は当該脆弱性を悪用したと思われる標的型攻撃を観測し、1 月下旬より調査を進めていることを公表した。当該脆弱性が悪用された事例として、FiveHands ランサムウェアへの感染等がある※90。

また、2021 年 5 月に Pulse Secure, LLC. は、同社の VPN 製品である Pulse Connect Secure に発見された複数の脆弱性を解消する定例外の修正プログラムを公開した※91。解消された脆弱性のうち、CVE-2021-22893※92 については、悪用による被害が確認された。

この脆弱性を悪用されると、認証されていない攻撃者により、解放済みメモリ使用の脆弱性（Use After Free）を悪用され、当該製品上のライセンスサーバの Web サービスを経由して任意のコードを実行される可能性がある。また、認証を回避され、製品上に Web シェル※93 を設置されることで、システムが永続的に侵害される可能性がある。

これらの VPN 製品は、脆弱性を解消したバージョンのソフトウェアが配布されるまでに数週間から 1 ヵ月程の期間を要しており、脆弱性情報の公開後、当該脆弱性を悪用した攻撃の事例が報告されている。

これは、脆弱性情報の公開当初はソフトウェアの修正プログラムが公開されていなかったことに加え、修正プログラムを適用したとしても、適用前に脆弱性を悪用され、認証情報を不正に取得されていた場合、攻撃者が窃取した認証情報により不正アクセスできてしまうことが要因として挙げられる※94。

(b) 脆弱性を狙った攻撃への対策

脆弱性が発見されると攻撃者に狙われ、被害が発生してしまう可能性があるため、新たな脆弱性が公開された際は、迅速な対応が求められる。

そのためには、事前の準備が重要である。自らが保有または利用するシステムについて、構成管理を適切に行い、システムを構成するソフトウェア等の脆弱性に関する情報収集を日々行う必要がある。また、事前に対策の実施手順を整えておき、脆弱性の対応を遅延なく着実に実施することが重要である。

対策の実施手順として、以下に示す内容をあらかじめ定めておくことを推奨する。

- 利用しているソフトウェア等の脆弱性情報の収集方法
- 脆弱性が確認された場合の対応方法
- 脆弱性の緊急度や深刻度に応じた対応の優先度
- 他部署やベンダ等への連絡の要否基準

このような実施手順の準備に加え、侵害されている痕跡が存在するかの確認や攻撃を受けてしまった場合の対応を定めておくことを推奨する。

なお、近年の VPN 製品の需要の高まりから、古い製品を利用する必要に迫られることも考えられる。その際は、ベンダからサポートを受けられる状態であることを確認し、必要な修正プログラムを適用して既知の脆弱性を解消してから利用することが望ましい。

(2) Microsoft 製品の脆弱性を対象とした攻撃

2021 年度も 2020 年度に引き続き、Microsoft 製品の脆弱性を狙った攻撃が多数報告されている。本項では、Microsoft Exchange Server の脆弱性を狙った事例を紹介する。

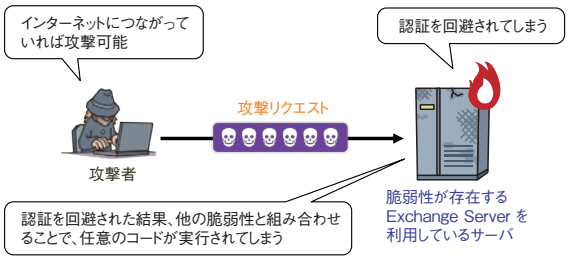
(a) 攻撃事例

Microsoft Exchange Server は、Microsoft 社が開発したメールサーバ及びグループウェアである。

ここでは、2021 年 3 月に公開された「ProxyLogon」と呼ばれる脆弱性（CVE-2021-26855※95 等）と、同年 8 月に公開された「ProxyShell」と呼ばれる脆弱性（CVE-2021-34473※96 等）を悪用した攻撃について解説する。

- ProxyLogon の脆弱性

  この脆弱性は、Exchange Server のプロキシアーキテクチャに認証の不備があることに起因する。攻撃者は、脆弱性が存在する Exchange Server を導入したサーバの 443 番ポートに対して細工したリクエストを送信する。脆弱性が存在すると、認証を回避して管理者になりすますことが可能となり、他の脆弱性と組み合わせることで、任意のコードが実行される（次ページ図 1-2-8）。
- ProxyShell の脆弱性



■図 1-2-8　ProxyLogon の脆弱性を悪用した攻撃イメージ

ProxyShell の脆弱性も、ProxyLogon の脆弱性と同様に、クライアントアクセスサービスに認証の不備があることに起因する。当該脆弱性により、攻撃者が標的となる Exchange Server に対し、細工したリクエストを送信することで、バックエンドサーバの任意の URL へアクセスできる。また、他の脆弱性と組み合わせることで、任意のファイルを上書きして Web シェルを設置すること等ができるとされている。

2021 年 1 月、ProxyLogon を悪用され、攻撃対象のサーバで認証を回避し、メール情報を窃取される事例が報告されている※97。

(b) 脆弱性を狙った攻撃への対策

脆弱性を狙った攻撃による被害を防ぐため、修正プログラムが公開されたら、利用者は速やかにアップデートを実施することが求められる。また、事前に対策の実施手順を整えておくことを推奨する（「1.2.5 (1) (b) 脆弱性を狙った攻撃への対策」参照）。

(3) IoT 製品を対象とした攻撃

2021 年度も、多数の IoT 製品に影響を与える脆弱性が公開されている。本項では、「NAME:WRECK」と呼ばれる脆弱性を紹介する。

(a) 多数の IoT 製品に影響する脆弱性

2021 年 4 月 12 日、米国のサイバーセキュリティ企業である Forescout Technologies, Inc. 及びイスラエルのサイバーセキュリティ企業である JSOF Ltd. より、「NAME:WRECK」と呼ばれるゼロデイ※98 の脆弱性群に関する情報が公開された※99。NAME:WRECK は、TCP/IP スタック※100 に DNS プロトコルのメッセージ圧縮機能を持つ FreeBSD や Nucleus NET 等の IoT 機器向けの OS やソフトウェアライブラリに発見された 9 個の脆弱性の総称である。これらの脆弱性が悪用された場合、攻撃者により、IoT 製品を経由して外部からネットワークに侵入され、ブロードキャストによって、ネットワーク内の脆弱性がある機器の制御を奪取されたり、サービス妨害等を引き起こされたりする可能性があるという。

当該製品は、医療機器や制御システム等の組み込み機器で広く利用されていることから、少なくとも 1 億台の機器が影響を受ける可能性があるとされる※101。

今後も、NAME:WRECK の脆弱性が解消されていない IoT 製品を狙った攻撃が発生する可能性があり、対策が必要である。

(b) IoT 製品を対象とした攻撃への対策

前述の NAME:WRECK のような脆弱性の存在を踏まえて、IoT 製品を安全に保つためには、以下の対策が必要となる。

- 製品開発者が行うべき対策
  - IPA や JPCERT/CC 等の各組織が公開している IoT 製品の開発ガイドライン等を基に、企画・設計等を含めたすべての開発工程で実施すべきセキュリティ対策を明確にする（ガイドラインについては「3.2.4 (1) IoT 関連セキュリティガイド等の改訂・新規発行」参照）。
  - 製品で使用する部品の調達に関し、契約等において脆弱性対処の項目を含める。
  - 製品出荷後に修正プログラムによりアップデートが実施できるように製品に更新機能等を組み込む。
  - 製品に関する脆弱性が発見・報告された場合、速やかに修正プログラムを公開する。
  - 安全に運用するための注意点等の情報を製品利用者に提供する。
- 製品利用者が行うべき対策
  - 製品開発者が提供する安全に運用するための注意点やアップデート方法等の情報を確認した上で利用する。
  - 攻撃者に脆弱性を悪用されるリスクを低減するため、製品を利用するにあたって問題がなければ、インターネットから直接 IoT 製品にアクセスできないようにする。
  - 脆弱性情報を収集する。具体的には、IPA が公開している「JVN iPedia※102」や、IPA から送付されるセキュリティ対策情報のメールニュース、製品開発者の Web サイトで公開される情報等を定期的に確認する。
  - 製品開発者が修正プログラムを公開した場合、速やかに修正プログラムを適用する。

1.2.6 ばらまき型メールによる攻撃

特定の組織や個人ではなく、不特定多数の一般利用者を狙った、ウイルス感染を目的としたメールを本項では「ばらまき型メール」と呼ぶ。

2015 年 10 月ごろより、国内で日本語のばらまき型メールによる攻撃が多く観測されるようになった※103。2021 年においても、件名やメール本文が受信者とは関係のないメール、実在の組織をかたったメール、一見すると業務に関係のありそうな件名や本文のメール、「正規のメールへの返信」を装ったメール等を確認している。ばらまき型メールでウイルスに感染させる手口としては、添付ファイルやメール本文中の URL を用いる手法が存在する。メールの添付ファイルには実行ファイル、脆弱性を悪用する Office 文書ファイル、Office アプリケーションのアドインファイル等を確認している。また、マクロ付きの Office 文書ファイル、これらのファイルを圧縮した形式のファイルについても継続的に確認している。ばらまき型メールによってウイルスに感染すると、感染した端末の情報窃取や遠隔操作、ランサムウェアへの感染等につながるため注意が必要である。

IPA では、2019 年、2020 年に日本国内で多くの感染被害が発生した「Emotet」と呼ばれるウイルスへの感染を狙うばらまき型メール（以下、Emotet のばらまき型メール）を、2021 年 11 月に再度観測した。Emotet のばらまき型メールは、2021 年 1 月に欧州刑事警察機構（Europol）により Emotet の攻撃基盤（ウイルスをばらまいたり、感染したマシンを操作したりするための機器等）がテイクダウン（停止）された※104 ため、世界中で 2021 年 2 ～ 10 月の間、確認されていなかった。しかし、Emotet のばらまき型メールが再度観測されたことから、攻撃者はテイクダウンされた攻撃基盤とは別の攻撃基盤を用意し、Emotet のばらまき型メールを送信している可能性がある。国内では、2022 年 2 ～ 3 月にかけて、企業・組織における Emotet 感染が急増していると報告されている※105。このほか、Emotet 以外のウイルスに感染させるばらまき型メールについては、2021 年をとおして観測されている。

本項では、2021 年度に国内で観測された日本語のばらまき型メールによる攻撃で使用されたメール偽装の手口やウイルス感染の手口について解説する。

(1) 正規のメールと誤認させる手口

攻撃者が、ばらまき型メールの受信者に正規のメールと誤認識させるために使う手口について解説する。

(a) 正規のメールへの返信、転送、及び再送を装う手口

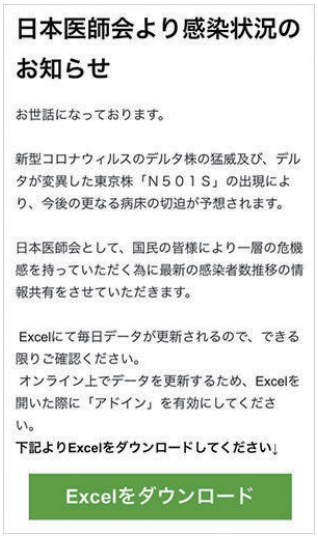
IPA では、正規のメールへの返信、転送、及び再送を装うばらまき型メール（以下、正規のメールへの返信等を装うメール）を観測している。このばらまき型メールでは、攻撃対象者が過去にメールのやり取りをしたことのある、実在する相手の氏名、メールアドレス、メールの内容等が流用され、その相手からの返信、転送、及び再送のメールを装っている。

この手口のばらまき型メールは 2018 年 11 月から観測されており※106、次の方法によってメールが送信される。

- ウイルスに感染した端末から窃取した情報を基に、メール送信用のボットネットから、別の相手に対して正規のメールへの返信等を装うメールをばらまく方法※107。
- 攻撃者がメールアカウントへ不正アクセスし、そのメールアカウントで受信していた正規のメールへの返信等を装うメールをばらまく方法
- あらかじめ窃取したメール情報を用いて正規のメールへの返信等を装うメールをばらまく方法

(b) メール受信者の興味・関心を惹く題材を悪用する手口

IPA では、受信者の興味・関心を惹く題材をメールの件名・本文に記載するばらまき型メールを継続して観測している。2020 年 12 月にはクリスマスや賞与を題材と



■図 1-2-9　新型コロナウイルスを題材としたばらまき型メールの例
（出典）公益社団法人日本医師会「【注意喚起】日本医師会を騙る不審メールの流通について※108」

したばらまき型メールを、2021 年 1 月には緊急事態宣言を題材としたばらまき型メールを観測していた。その後、2021 年 7 ～ 10 月には請求書を題材としたばらまき型メールを、2021 年 9 月には図 1-2-9（前ページ）のように新型コロナウイルスを題材としたばらまき型メールを観測した。これらの手口から、攻撃者は日本国内のメール受信者の興味・関心を惹く題材を選んで継続的に攻撃を行っていると言える。

(c) 実在の組織をかたった手口

実在する組織をかたるばらまき型メールも観測されている。図 1-2-9（前ページ）や図 1-2-10 のように、実在する組織をかたり、あたかもその組織からの連絡であるかのように送信元や本文を偽装したメールが送信される。この手口も継続して使われているため、引き続き注意が必要である。

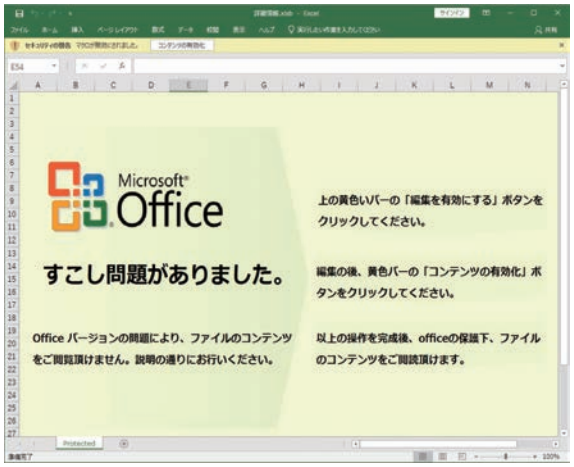
■図 1-2-10　実在する企業をかたるばらまき型メールの例

(2) ウイルスに感染させる手口

攻撃者がばらまき型メールを用いてウイルスに感染させる手口を解説する。

(a) マクロ付きの Office 文書ファイルを使用する手口

この手口では、マクロ付きの Word、Excel、PowerPoint といった Office 文書ファイル内の悪意あるマクロが動作することでウイルスに感染させる。マクロ付き Word、Excel ファイルには、Microsoft 社や Office 等のロゴとともに、「文書ファイルを閲覧するには操作が必要である」という趣旨の記述と「Enable Editing」（編集を有効にする）ボタンと「Enable Content」（コンテンツの有効化）ボタンのクリックを促す指示が書かれているものがあることを確認している。2020 年 9 月まではこれらの記述は英語のみであったが、IPA では 2020 年 10 月以降、日本語で指示が記載された Word ファイルや Excel ファイルを確認している。2021 年 4 月にも図 1-2-11 に示すように、Excel ファイルを使用し、ウイルスに感染させようとするばらまき型メールを確認している※109。



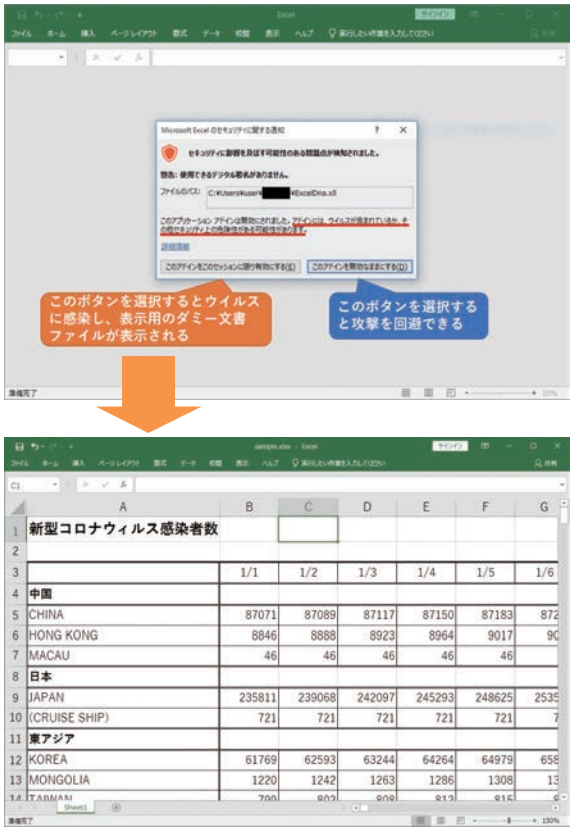
■図 1-2-11　日本語で記載されている Excel ファイルの例

(b) Excel アドインファイルを使用する手口

Excel アドイン（拡張子が .xll）のファイルを悪用する手口を確認している※110。この手口ではファイルを開くと、図 1-2-12（次ページ）のように、警告ウィンドウが表示される。警告ウィンドウで、利用者が「このアドインをこのセッションに限り有効にする」を選択すると、表示用のダミー文書ファイルが表示され、最終的にウイルスに感染する。

(c) パスワード付きの ZIP ファイルを使用する手口

パスワード付きの ZIP ファイルが添付され、そのパスワードがメール本文に記載されているばらまき型メールを確認している。ZIP ファイルを解凍すると、マクロ付きの Word ファイルが出力され、利用者がそのファイルを開いて「コンテンツの有効化」ボタンをクリックすることでウイルスに感染する。添付ファイルが暗号化されていることから、メール配送中のセキュリティ製品や、セキュリティサービス、セキュリティソフトによる検知や検疫をすり抜け、受信者のもとに攻撃メールが届いてしまう確率が高い。この手口自体は 2019 年 12 月ごろから使われているが、2021 年度も継続的に使われており、引き続き注意が必要である。



■図 1-2-12　Excel アドインのファイルを開いたときに表示される警告ウィンドウとダミー文書ファイルの例

(d) メール本文中の URL リンクを使用する手口

この手口ではメール本文中に URL リンクが記載されており、URL リンクをクリックしてアクセスすると、悪意のあるマクロ付き Office 文書ファイルや PDF 閲覧ソフトを装ったウイルスファイル等をダウンロードさせる Web サイトへ誘導される※111。Office 文書ファイルをダウンロードした場合、前述の「(a) マクロ付きの Office 文書ファイルを使用する手口」を用いてウイルスに感染させる。また、PDF 閲覧ソフトを装うウイルスファイルについては、脆弱性を悪用し更に別のウイルスに感染させることを確認している※112。URL リンク先は、攻撃者が用意したサーバである場合や、Microsoft OneDrive、Google Drive 等のクラウドストレージの場合もある。この手口は新しいものではないが 2021 年度も継続して使われており、引き続き注意が必要である。

(3) ばらまき型メールへの対策

ばらまき型メールの攻撃者は、ウイルスに感染させる確率を上げるために様々な工夫を凝らし、新たな手口を取り入れて攻撃している。そのため利用者はセキュリティソフトの活用、スパムメール対策、メール受信者自身による防御等の対策を実施し、多層的な防御を行うことが重要である。

(a) 一般利用者における対策

次に示す対策は、ばらまき型メール以外の攻撃に対しても有効であり、徹底することを推奨する。

- セキュリティソフトを導入する
  メール受信者がウイルスメールであると判断できずに添付ファイル等を開いてしまったとしても、セキュリティソフトが検知・検疫し、被害を免れる可能性がある。セキュリティソフトは導入するだけでなく、常に最新の状態に保つことも重要である。
- 不用意にメールや添付ファイル内の指示に従わない
  身に覚えのないメールの添付ファイルを開かないことや、本文中の URL リンクにアクセスしないことが重要である。また、受信したメールに疑問や不審を抱いた場合は、送信元となっている企業や組織の公式サイトでばらまき型メールに関する注意喚起が公開されていないかを確認するほか、当該メールの送付有無を問い合わせる。受信メールの真偽が分からない段階では、メールへの返信、添付ファイルを開くこと、及び本文中に記載されている URL へのアクセスは避けるべきである。また、添付ファイルを開いたときに、警告ウィンドウが表示された場合、その警告の意味が分からないのであれば、操作を中断し、システム管理部門等へ報告・相談を行うことを推奨する。
- OS やソフトウェアのバージョンを常に最新に保つ
  適宜、修正プログラムを適用し、既知の脆弱性を解消しておくことで、脆弱性を悪用した攻撃が成功する確率を下げることができる。
- Office 文書ファイルを開いたときに保護ビューの解除やマクロの有効化を行わない
  正規のものであると確信の持てない Word、Excel、PowerPoint 等のファイルを何らかの方法で入手して開いたときに、マクロやセキュリティに関する警告が表示された場合は、不用意に「編集を有効にする」ボタンや「コンテンツの有効化」ボタンをクリックしない。また、Word、Excel、PowerPoint 等の設定でマクロの自動実行を無効化する。業務等でマクロを使わないと分かっている場合にはマクロ機能自体を無効化するといった対策も有効である。

(b) 企業・組織における対策

企業・組織におけるばらまき型メールに対する対策は、「1.2.1 (5) 標的型攻撃への対策」で述べている内容と基

本的には同じである。不審なメールを受信した際の報告窓口を設けることや、利用者に対してウイルス感染を想定した訓練と教育を行うといった組織的な取り組みのほか、システムの対策として、不審なメールを解析する仕組みを確立する、適切な修正プログラムを適用する、特定のファイル形式について実行許可・禁止の設定を行う、使用しない特定のファイル形式のファイルが添付されたメールは受信を拒否する、使用しないクラウドサービスへのアクセスを禁止するといった対策が重要である。

また、公開されているばらまき型メールに関する注意喚起情報を組織内で共有し、同様の攻撃による被害を受けないようにすることも重要である。なお、企業や大学、個人等からも、ばらまき型メールに関する注意喚起が出されているため、これらの情報を収集し、活用することが望ましい。

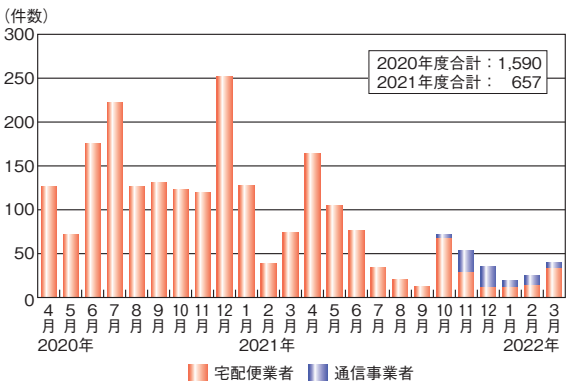
1.2.7 個人をターゲットにした騙しの手口

2021 年度は、手口の種類は増えてはいないが、手口の細かい部分で変化し続けているのが特徴と考えられる。

SMS（Short Message Service）の手口では、通信事業者をかたる SMS が出現した。一時期減少していた暗号資産を要求する脅迫メールの手口では、文面がより日本語らしくなったこともあり、本物と信じたという相談が増加している。Web からの騙しの手口では、2020 年度末から登場した Web ブラウザの通知機能を悪用する手口の相談が増加している。

(1) 変化が続く SMS の手口

2021 年度も、偽 SMS の手口に関する相談は継続して寄せられているが、従来の手口である宅配便業者をかたる SMS に加えて、通信事業者をかたった偽 SMS が登場した（図 1-2-13）。

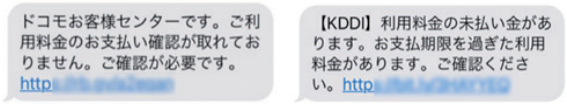


■図 1-2-13　偽 SMS に関する月別相談件数推移（2020～2021 年度）

これを受けて 2021 年 12 月、IPA では「安心相談窓口だより※113」に通信事業者をかたった手口の説明を追加し、注意喚起を行った。

(a) 通信事業者を装う SMS

2021 年 10 月ごろより、利用料金の支払いが確認できない等の偽の SMS 文面から URL をタップさせようとする手口の相談が多くなった。通信事業者は、当初、株式会社 NTT ドコモ（以下、NTT ドコモ）をかたっていたが、au（KDDI 株式会社）をかたるものも登場した（図 1-2-14）。



■図 1-2-14　通信事業者をかたる偽 SMS の例

(ア) 手口

この手口は、「利用料金に未払いがある」という通信事業者を装った SMS を送り付け、SMS 内のリンクから偽サイトへ誘導する。リンクをタップした後の手口は変化を続けている。以下は、2022 年 1 月時点の確認内容である。

偽サイトにアクセスしてしまうと、アクセスしたスマートフォンが Android OS 端末（以下、Android）であるか、iPhone や iPad 等の iOS 端末（以下、iPhone）であるかによって、この後遭遇する手口が異なる。

①Android を狙った手口の詳細

SMS の URL をタップすると、「システム警告」という画面が出て、「XXXセキュリティ」というアプリのバージョンアップを促されるが、これは不正なアプリをダウンロードさせようとしているものである（図 1-2-15）。

ダウンロードしただけでは被害にはつながらないが、

■図 1-2-15　KDDI セキュリティのアップデートをかたる例

ファイルをタップし、不正なアプリをインストールすると、被害につながる。

なお、偽のセキュリティアプリの名前は、かたる通信事業者に合わせ、au の場合は、「KDDI セキュリティ」、NTT ドコモの場合は、「NTT セキュリティ」となる。

不正なアプリのインストールが終わった後、正規のセキュリティアプリの削除に誘導される場合がある（図 1-2-16）。

■図 1-2-16　セキュリティアプリ（あんしんセキュリティ）を削除させる例

削除される正規のセキュリティアプリは次の三つを確認している。

- あんしんセキュリティ（NTT ドコモ）
- 安心ネットセキュリティ（KDDI 株式会社）
- マカフィーモバイルセキュリティ（マカフィー株式会社）

②iPhone を狙った手口の詳細

iPhone を狙った手口は、以下の三つを確認している。

- 不正なアプリをインストールさせる手口

  SMS の URL のタップにより構成プロファイルをダウンロードさせ、偽のセキュリティアプリをインストールさせる（図 1-2-17）。

  構成プロファイルは主に通信事業者等が iPhone の設定を一括して行うために利用されるが、この手口では正規のアプリストアである Apple Store 以外から不正なアプリをインストールさせるためにダウンロードさせたものと考えられる。

- フィッシングサイトに誘導し、アカウント認証情報とクレジットカード情報を入力させる手口

  SMS の URL をタップすると、Apple Store アカウントに異常があったというポップアップメッセージが出て、メッセージをタップすると、Apple Inc. を装ったフィッシングサイトが表示される。

- フィッシングサイトに誘導し、アカウント情報とギフト券番号を入力させる手口

  au を装ったフィッシングサイトに誘導された場合は、au ID とパスワードを入力すると、未払い料金を請求する偽のメッセージと偽の請求額が表示される（図 1-2-18）。

■図 1-2-17　構成プロファイルをダウンロードさせ、不正なアプリをインストールさせる手口

（出典）一般財団法人日本サイバー犯罪対策センター「通信事業者を装ったフィッシング（不正アプリに注意）※114」を基に IPA が編集

■図 1-2-18　未払い料金を請求する偽のメッセージと偽の請求額が表示される画面

NTT ドコモを装ったフィッシングサイトに誘導された場合は、d アカウント ID とパスワードを入力すると、未払い料金を請求する偽のメッセージと偽の請求額が表示される。ログインページが出ず、偽の請求額が表示される場合もある。

（イ）被害

手口に遭遇した端末が、Android か iPhone であるかによって被害が異なる。

①Android における被害

Android における被害として、以下が確認されている。

- スマートフォンが攻撃の踏み台にされ、不特定多数の宛先（自身のアドレス帳にはない電話番号）へ、偽SMSを勝手に送信された。
- スマートフォンから、アドレス帳の内容、SMSメッセージ等を窃取され、以下のように悪用された。
  - 通信事業者が提供するキャリア決済サービスにおいて、身に覚えのない請求が発生した。
  - フリーマーケットサービス、後払い決済サービス、その他のアカウントサービス等のアカウントを勝手に作成され、不正使用された。
- セキュリティアプリが削除され、セキュリティ対策が機能しなくなった。

② iPhoneにおける被害

iPhoneにおける被害として、以下が確認されている。

- 不正なアプリをインストールさせられた。

  不正なアプリを起動すると、ネットワーク暗証番号を入力させる画面が出て、入力した情報が詐取された。
- フィッシングサイトに誘導し、アカウント認証情報とクレジットカード情報を入力させられた。

  フィッシングサイトで情報を入力した場合は、その情報を不正使用される可能性がある。次のような相談が寄せられている。
  - Apple ID、パスワード、Apple ID確認コードを入力したところ、不正ログインされた。
  - 電話番号とキャリア決済サービスの認証コードを入力したところ、身に覚えのない請求が発生した。
  - 電話番号と認証コードを入力したところ、フリーマーケットサービス等にアカウントを勝手に作成された。
- フィッシングサイトに誘導し、アカウント情報とギフト券番号を入力させられた。

  「利用料金の未払い金があります。」という偽の画面から先へ進むと、ギフトカードで料金を支払うように誘導され、ギフトカードのシリアル番号を入力した場合は、購入したギフトカードの額面（金額）が相手に渡ってしまう（図1-2-19）。

■図1-2-19　ギフトカード番号の入力に誘導される画面

（ウ）対処

手口に遭遇した端末が、Androidか iPhoneであるかによって対処が異なる。

①Androidにおける対処

不正なアプリをインストールした場合の対処は、「情報セキュリティ白書2021」の「1.2.7（3）（a）（ウ）対処」を参照いただきたい。なお、正規のセキュリティアプリを削除してしまった場合は、セキュリティアプリの再インストールが必要である。また、セキュリティアプリの初期設定が必要な場合がある。

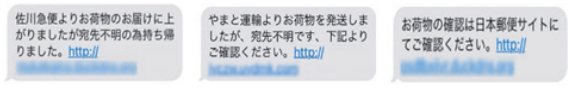
②iPhoneにおける対処

不正なアプリをインストールした場合の対処は、以下のとおりである。

- 不正なアプリのインストールによる、スマートフォン本体への影響範囲は不明なため、アンインストールだけではなく、スマートフォンの初期化を推奨する。
- 不正なアプリにネットワーク暗証番号を入力した場合は、ネットワーク暗証番号を変更する。
- 上記以外の対処は、「情報セキュリティ白書2021」の「1.2.7（3）（a）（ウ）対処」を参照いただきたい。

（b）宅配便業者を装うSMS

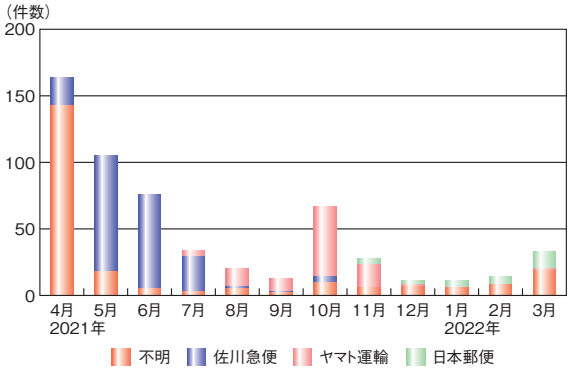
本件に関する相談は、2017年から確認されている。この手口は、当初佐川急便株式会社（以下、佐川急便）をかたるものであったが、2020年8月ごろからは、事業者名が記載されないものが登場し、2021年度は、かたる宅配便業者や不正なアプリの名前が変わる等、継続的に変化している（図1-2-20）。



■図1-2-20　宅配便業者をかたるSMSの例

2021年4月から佐川急便をかたるSMSによる相談が増加し、8月ごろからはヤマト運輸株式会社をかたるSMSの相談へ、更に11月からは日本郵便株式会社をかたるSMSの相談へと変化している。相談件数自体は減少傾向にある（次ページ図1-2-21）。

2021年5月初旬ごろから、再配達受付サイトを装っ



■図 1-2-21　宅配便業者をかたる SMS の件数推移（2021 年度）

た偽サイトに誘導し、運転免許証等の本人確認書類の写真を詐取する新たな手口に関する相談が増加した。IPA は「安心相談窓口だより※115」で、2021 年 6 月に注意喚起を行った。

以下では、この新たな手口について説明する。従来の Android 端末に不正なアプリをインストールさせる手口や、iPhone での偽のサイトに誘導する手口については、「情報セキュリティ白書 2021」の「1.2.7 (3) (a) 宅配便の不在通知を装う SMS」を参照いただきたい。

(ア) 手口

下記のような宅配便の不在通知を装った偽 SMS が送られてくる。偽 SMS に記載されている URL をタップすると、佐川急便を装った再配達受付の偽サイトに誘導される（図 1-2-22）。

■図 1-2-22　偽の不在通知 SMS から本人確認書類を詐取する手口

この手口は、従来の宅配便業者をかたる手口と異なり、Android も iPhone も同じ手口なのが特徴である。

偽サイトに記載されている指示に従い「電話番号」「本人確認書類（マイナンバーカード、運転免許証、パスポート）の写真」「メールアドレス」を入力すると、それらの情報が相手に伝わってしまうと考えられる。

(イ) 被害

入力した電話番号やメールアドレス宛に、不審な SMS や迷惑メールが届く可能性が考えられる。しかしながら、運転免許証、マイナンバーカード、パスポートの写真が悪意の第三者に渡った場合の被害については分かっていない。

(ウ) 対処

どのような対処が必要かについては、詐取された本人確認書類によって、以下の窓口等に相談することを検討いただきたい。

- 運転免許証の場合、住所地を管轄する警察署
- マイナンバーカード、パスポートの場合、交付元の各自治体

(c) SMS の手口の変化への対策

通信事業者は、SMS を送信する場合の電話番号やアドレス、内容について公式サイトで説明を行っている。宅配便業者は、SMS で連絡することはないとサイトで案内している場合が多い。公式サイト等の確かな情報源を使って確認していただきたい。特に SMS に記載されている URL には注意が必要である。また、送信元情報は偽装される場合もある。SMS を安全に利用するためには、受信しても即座に反応せず、真偽の判断を行っていただきたい。

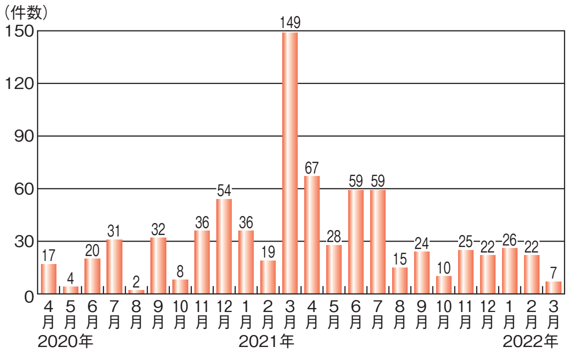
なお、2022 年 3 月から、各通信事業者が SMS を悪用したフィッシング詐欺への対策を開始した。NTT ドコモは、危険と判断したサイトの URL 等が含まれる SMS を自動で拒否する設定の自動適用を開始した※116。KDDI 株式会社は、迷惑メッセージブロック機能アプリの無償提供を開始し※117、ソフトバンク株式会社は迷惑 SMS 対策機能の提供を順次行っている※118。通信事業者が提供している機能を利用した対策を併せて行っていただきたい。

(2) 暗号資産を要求する脅迫メールの手口

この手口については 2018 年度より相談があり、2019

年度末以降は減少していたが、2020 年度末から 2021 年 7 月にかけて相談が増加した(図 1-2-23)。

従来は、外国語を日本語に直訳したような翻訳調の文面が多かったが、2020 年度末からは翻訳調ではなく顔文字を入れる等の日本語らしい文面のメールも登場したため、受信件数の増加に加えて、内容を信じて不安になり相談することが増えたと考えられる。



■図 1-2-23 暗号資産を要求する脅迫メールについての相談件数の推移(2020 ～ 2021 年度)

(a)手口

脅迫メールの文面は変化を続けているが、盗んだ情報や盗撮したという動画を知人や動画サイトにばらまかれたくなければ、制限時間内に Bitcoin (ビットコイン) 等の暗号資産を送金するよう要求する手口は変わっていない。

盗んだとする情報がメールに記載・添付されていた事例や、支払いに応じなかったために情報がばらまかれた事例等は確認されていない。このことから、根拠のない内容で脅迫していると推測される。

①脅迫メールの文面の変化

過去から継続している脅迫メールの文面としては、ハッカーを名乗り、パソコンに「トロイの木馬ウイルスをインストールした」(図 1-2-24)、「ハッキング」した、という文面がある。

過去の文面と比較して、以下のような変化が観測された。

- ハッキングしたという内容は同様だが、スマートフォンを対象として、「あなたのモバイルストレージについてデータ侵害がありましたことをお知らせいたします。」という文面も登場した。
- パソコンやスマートフォンの中の情報から友人、知人に情報をばらまくというのが定番であったが、2021 年 12 月ごろから、盗撮した動画を動画サイトで公開するという脅迫の手口も登場した。

Re:悪いお知らせがあります。

数ヶ月前にあなたのデバイスにアクセスしました。
その後、あなたの活動を監視するようになりました。
私は、あなたがインターネットにアクセスするために使っているすべての機器のOSにトロイの木馬ウイルスをインストールしました。このソフトウェアは、あなたのデバイス上のすべてのコントローラにアクセスすることができます。
あなたの情報、データ、写真、閲覧履歴をすべて私のサーバーにアップロードしました。
あなたのすべてのデータ、メッセンジャー、ソーシャルネットワーク、メール、チャット履歴、連絡先にアクセスできます。
私のウイルスはシグネチャを更新し、ウイルス対策ソフトからは見えないようになっています。
あなたの情報を集めているうちに、あなたがアダルトサイトの大ファンで、中毒性のある動画を楽しみながら見ていることがわかりました。
あなたがオナニーをしてオーガズムに達するという、あなたの汚いシーンをなんとか録画しました。
少しでも疑問があれば、私が数回クリックするだけで、すべての動画が知り合いに表示されます。
また、あなたの通信簿や個人的な写真、すべての秘密のデータをインターネット上に掲載することもできます。
あなたの評判を永遠に台無しにしてしまうかもしれません。
あなたが好きなビデオの仕様を考えると（よくわかっていると思いますが）、それはあなたにとって本当の意味での災難となるでしょう。
このように解決しましょう。あなたが私に 109931 円
(JPY)（送金時の為替レートでビットコイン換算）を送金してくれれば、私はこの汚れをすぐに取り除きます。その後は、お互いのことを忘れてしまいます。
また、お客様のデバイスからすべてのマルウェアを無効にして削除することをお約束します。
私はいつも約束を守ります。
ここに私のビットコインウォレットがあります： bc1qd0ggud54qfun6jkx0n38rfyfgvf9mzrtkpy8x3
このメールを開いた瞬間から3日間の猶予があります。
送金がない場合は、あなたのビデオと詳細情報がインターネット上に公開され、すべての人とあなたの愛する人が見ることができます。
あなたの評判を永遠に台無しにします。
私を探そうとしないでください。
警察やその他のセキュリティ機関に連絡しようとすると、あなたの詳細が公表されてしまいます。
私はあなたの秘密をたくさん知っています。 [redacted]
自分の評価を意識する。

■図 1-2-24 脅迫メールの例

②自然な日本語の文面

当初この手口はもっぱら英語の文面を用いていたが、その後機械翻訳されたと思われる日本語の文面が送られるようになり、2021 年度には自然な日本語の文面の脅迫メールが登場した。顔文字が入っているものもある(図 1-2-25)。元になる文面は英語と思われるが、翻訳ソフトの翻訳精度が上がってきたためではないかと考えられる。

Subject: アカウントからのお支払い。未払いがあります

こんにちは！
残念ながら凶報がございます。数ヶ月前、あなたがインターネット閲覧に利用しているデバイスへのアクセス権を取得しました。
さらに、あなたのインターネット活動の追跡も行いました。

下記は、それまでに至る経緯です。
以前、ハッカーから複数のメールアドレスへのアクセス権を購入しました（最近では、オンライン上で簡単に購入することが可能です）。
よって苦労することなく、あなたのメールアカウント（[redacted]）にログインしています。
あなたのデバイスにアクセスしてから１週間以内に、メールに利用されているデバイスのオペレーティングシステム全てにトロイの木馬ウイルスをインストールしました。実際、この操作はかなり単純です（なぜなら、あなたが受信メールをクリックしたからです）。スマートな物事は何でもかなり単純なのでしょう。(´▽`)

～～～～～～～ 以下 省略 ～～～～～～～～～～～～～～～～～～～～～～～～～～～～～～～～

■図 1-2-25 自然な日本語の脅迫メールの例

(b)対処

当該メールが複数回届くため、パソコンやスマートフォンからの情報窃取が、事実ではないかと信じ始めて相談される場合や、メールソフトやメールサービスの「迷惑メールフォルダ」に振り分けられている脅迫メールを確認して心配になり相談されることが多くなった。メールが届いた場合は、メールを削除するだけで問題ない。

メールの送信元が、メール受信者自身のアドレスになっている場合があるが、送信元アドレスは技術的に詐称が可能であり、迷惑メールのフィルタリングを回避することや、あたかもメールアカウントをハッキングしたと信じさせることが目的と考えられる。また、現在使用しているパスワードが書かれていた場合は、すぐにパスワードを変更し、併

せて、そのパスワードを使っていたサービスへの不正ログインがないか確認することを推奨する。

(3) 世の中の関心に乗じる手口

2021 年度も、新型コロナウイルスの感染が続き、経済や社会に様々な影響が出ているが、関心の高かった予防接種に関する内容が、フィッシングメールの手口に使われた。

(a) 手口

2021 年 2 月より、新型コロナウイルスワクチンの先行接種が開始され※119、高齢者の接種に続いて、対象年齢が順次下げられていったが、予約が取りづらい状況にあった。これに乗じて、8 月ごろから、新型コロナワクチン接種に関するフィッシングが登場し、「大規模接種センターの予約サイト案内」をかたるフィッシングメールに関する相談があった。IPA でフィッシングサイトを確認したところ、各種個人情報、クレジットカード情報を詐取する画面に誘導されることが分かり（図 1-2-26）、注意喚起を行った※120。また、厚生労働省※121 や、国民生活センター※122 からも注意喚起が行われた。

■図 1-2-26　コロナワクチン接種の偽サイト

2020 年度は「新型コロナウイルス感染症緊急経済対策」として家計支援のため、1 人あたり 10 万円が支給された「特別定額給付金」に関するものが多かったが、2021 年度も、特別定額給付金に関する通知を装うフィッシングが、フィッシング対策協議会より報告されている（図 1-2-27）。

(b) 対処

新型コロナワクチン接種に関しては、「新型コロナウイルスを題材とした攻撃メールについて※119」という注意喚起が厚生労働省より出され、注意喚起が行われている。

■図 1-2-27　特別定額給付金の支給をかたるメール
（出典）フィッシング対策協議会「特別定額給付金に関する通知を装うフィッシング（2021/08/24）※123」を IPA にて編集

総務省は、特別定額給付金について、政府からメール等で知らせることはないと説明している※124。

今後も、新型コロナウイルスに関して、様々な手口が登場することが想定されるが、対処は他の不審メールやフィッシングメールへの対応と同様である。本物かどうか判断に迷った場合は、公式サイト等、確かな情報源を使って確認し、以下の対処を行う。

- 添付ファイルを開かない。
- 記載の URL から Web サイトにアクセスしない。
- 記載の電話番号に電話をしない。
- 返信しない。

Web サイトについては、見た目だけでは本物のサイトか偽のサイトかは、判断できにくくなっているため、メールに記載された URL から Web サイトにアクセスする以外の方法で運営者に確認するほか、フィッシング詐欺事例等がないかをインターネットで検索する等の対処を行う。

(4) 悪質化する Web ブラウザによる手口

パソコンやスマートフォンでインターネット閲覧中に、突然別の Web サイトに遷移し、画面が切り替わったり、スマートフォンにポップアップが表示されたりすることで、「偽のセキュリティ警告」や「アプリ誘導」の手口に遭遇することがある。

2020 年度末から 2021 年度にかけては、Web ブラウザの通知機能を悪用した手口によって誘導される相談が多くなってきた。

(a) 偽のセキュリティ警告

主にパソコンで Web サイト閲覧中に、突然警告音とともに、「ウイルスに感染している」等の警告画面が表示されたことをきっかけに、画面に表示された電話番号に電話をしてしまい、遠隔操作に誘導され被害に遭ってしまったという相談が 2021 年度も続いている。IPA は 2021 年 11 月、「安心相談窓口だより※125」で改めて注意喚起を行った。

警告画面を出す手口に変化は少ないが、コンビニエンスストアでプリペイドカードを購入させ、その番号を伝えることによりサポート費用と称したお金を支払わせる手口の相談が多くなった。

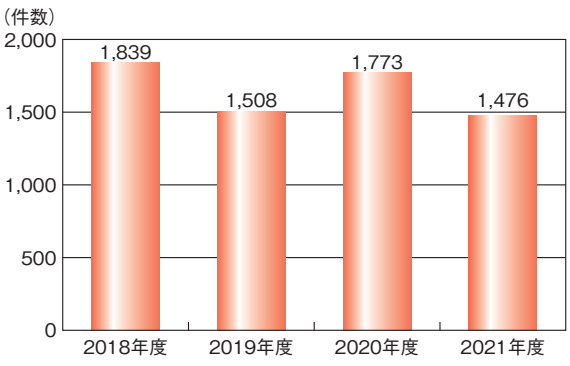
コンビニエンスストアのプリペイドカード売り場に注意喚起の表示がされるようになったが、被害が続いている。テレビやインターネットのニュース等でもこの手口が報道され、手口についての認識は広がっていると考えられるが、実際に遭遇すると、この手口に遭っていることに気が付かなかったという相談者も多い。

2022 年 1 月に、この手口で犯人が初めて逮捕されたとの報道があった。被害は 400 件以上でサポート費用と偽って銀行口座に振り込ませていたという※126。この報道の後も、相談件数は減らないため、この手口を用いる攻撃者は多く存在していると考えられる。

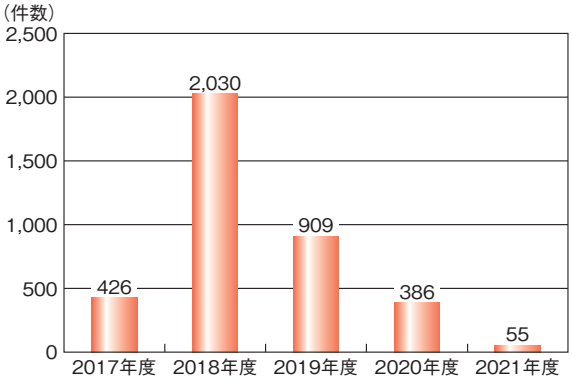
2021 年度に IPA の安心相談窓口に寄せられた相談件数は、有償サポート契約に誘導される「偽警告」(別名、サポート詐欺)が 1,476 件(図 1-2-28)、有償ソフトウェアの購入に誘導される「偽セキュリティソフト」が 55 件であった(図 1-2-29)。「偽セキュリティソフト」の購入に誘導する手口は減少している。

(ア) 手口

インターネット閲覧中の Web ブラウザ画面上に、本物に見せかけたセキュリティ警告を表示して、解決のため



■図 1-2-28　偽警告に関する年度別相談件数



■図 1-2-29　偽セキュリティソフトに関する年度別相談件数

に記載してある電話番号に電話をかけさせようとする。そのため、様々な誇大表現で危険性を訴えかけ、冷静な判断を妨げるよう仕組んでいると考えられる。

この手口は以下の①から④の流れとなる場合が多い。

①偽のセキュリティ警告画面が表示される

偽のセキュリティ警告画面の表示は以下のようになる場合が多い。

- 警告の画面が次々と重なって開く

  警告画面がいくつも重なって開き、しかも警告が全画面表示で固定されて「閉じるボタン」が隠されてしまい、画面を閉じることができない事例が多い(図 1-2-30)。

■図 1-2-30　警告画面が次々と全画面で開く画面の例

- 実在する企業やサービスのロゴ等が表示される

  Microsoft 社、マカフィー株式会社等の企業名やロゴ(次ページ図 1-2-31)、また Windows の標準機能からの警告を偽った表示が、繰り返し表示される。

- サポート窓口の電話番号が表示される

  問い合わせ先の電話番号が、繰り返し表示される。特に Microsoft 社のサポート窓口をかたる事例を多く確認している(次ページ図 1-2-32)。

②警告音やアナウンスが流れる

画面上の偽の警告表示に加えて、けたたましい警告

■図 1-2-31　実在する企業やサービスのロゴ等が表示された画面の例

■図 1-2-32　サポート窓口の電話番号が表示された画面の例

音や、テクニカルサポートを名乗る「ウイルス感染」等の警告アナウンスが大音量で延々と流れる。

③オペレーターが電話対応する

警告画面に記載されている電話番号に電話をかけると、オペレーターが状況を聞き、ウイルスに感染している等と言い、遠隔操作用ソフトウェアをダウンロードさせインストールをさせようとする。更に遠隔操作によって、パソコンに様々な画面を表示させ、危険性をあおり、有償サポート契約を勧める。

- 相手の反応を見ながら、「月契約」「年間契約」「永久契約」等の契約期間を説明し、期間に合わせて、数万～10万円程度の代金を提示することが多い。
- 入力フォームに住所・氏名等の個人情報の入力をさせることがある。
- デスクトップのアイコンを非表示にしたり、パソコン起動時に新たにパスワードの入力を必要にしたりする等、勝手にパソコンの設定を変更し、元に戻すために契約しろと要求する悪質な手口も確認している。

④サポート代金のプリペイドカードを繰り返し購入させる

2021年度は、購入したプリペイドカードのコードを伝えると「コードが間違っていてブロックされた」等と言い、繰り返しプリペイドカードを購入させ、複数回支払わせる例が増え、90万円を支払ったという相談事例もあった。

(イ)対処

パソコンの画面については、Webブラウザを閉じるだけで問題はない。通常の操作で画面を閉じることができない場合は、Windowsであれば、タスクマネージャーからWebブラウザを終了する、Macであれば、「強制終了」ウィンドウからWebブラウザを終了する、という方法で対処できる。また、どちらのOSの場合も、パソコンを再起動することでも対処できる。

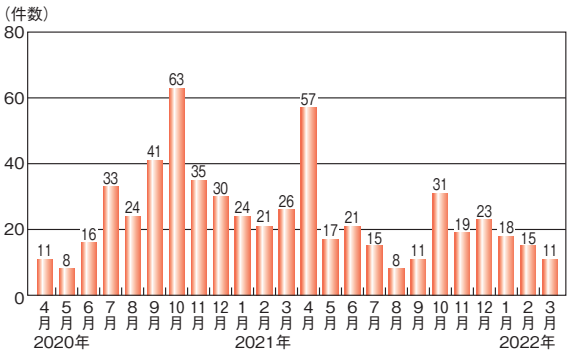
パソコンに遠隔操作用ソフトウェアをインストールしてしまった場合は、アンインストールする。

電話口のオペレーターに詳細不明のソフトウェアをインストールさせられた場合は、より安全な対応として、当該ソフトをインストールする前の状態にシステムを戻すことや、パソコンを初期化することを推奨する。

契約については、消費生活センター等※127に相談する。プリペイドカードでの支払いについては返金が困難な場合が多い。また、Microsoft社では、当該手口に関する専用ページ※128で手口や事例を紹介し、被害報告も受け付けているため、活用を検討いただきたい。

(b)アプリ誘導

主にスマートフォンで、Webサイト閲覧中に「ウイルスに感染している」等の根拠のない警告画面を表示して騙す手口の相談が続いている(図1-2-33)。

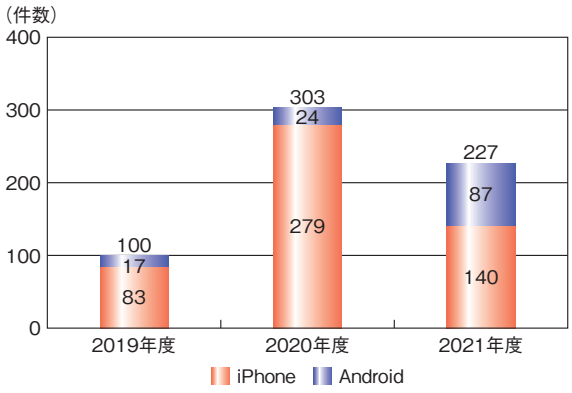


■図 1-2-33　アプリ誘導に関する相談件数(2020～2021年度)

手口の変化は少なく、インターネット閲覧中に偽の警告から誘導される事例が多い。

2020年度は、iPhoneカレンダースパムからこの手口に誘導されたため、iPhoneの相談が多かったが、2021年度は、Androidの相談が増えているのが特徴である(次ページ図1-2-34)。

以下では、Androidの場合の手口、対処を中心に説明する。



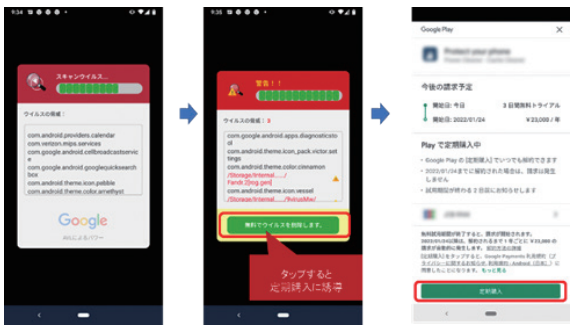
■図 1-2-34　アプリ誘導の端末別の年度別相談件数推移

(ア)手口

「あなたのスマホはウイルスに感染している可能性がある」「下のボタンをタップし無料で推奨セキュリティアプリをインストールして実行し、ウイルスを削除」というように、偽の警告画面を表示して公式ストア上のアプリを入手するよう誘導する手口である(図 1-2-35)。

■図 1-2-35　偽のセキュリティ警告から公式ストアのアプリへ誘導する流れの例(Android の場合)

「サブスクリプション詐欺」を目的として、自動継続課金※129 に誘導することが目的と考えられ、アプリインストール後の初回起動時にウイルススキャンをしているかのような表示をしてウイルスを検出したと偽り、定期購入に誘導するものも登場した(図 1-2-36)。



■図 1-2-36　偽のウイルス検知画面から定期購入へ誘導する流れの例(Android の場合)

無料アプリだと誤解して承認してしまうと、無料期間は3日間から1週間程度であることが多く、無料試用期間の終了後に意図しない利用料金が発生することになる。

(イ)対処

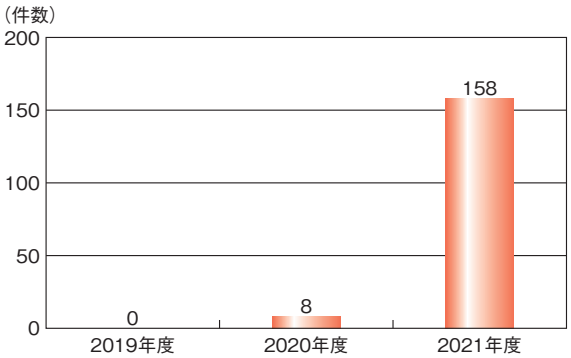
偽のセキュリティ警告が表示された場合は、Web ブラウザのタブを閉じる、または、Web ブラウザを終了し閲覧履歴を削除することで対処できる。

アプリをインストールしてしまった場合は、不要であればアンインストールをする。アンインストールだけでは自動継続課金は解約されないので、自動継続課金の登録を取り消す必要がある。Android の場合は定期購入の解約(図 1-2-37)、iPhone の場合はサブスクリプションの解約も実施する。

■図 1-2-37　定期購入の解約手順(Android 11 の場合)

(c)Web ブラウザの通知機能の悪用

2020 年度後半から、2021 年度にかけて、パソコンやスマートフォンで Web ブラウザを起動中に、「『コンピュータが危険にさらされている』『携帯をクリーンアップしてください』 等のメッセージが繰り返し表示された」、またその表示画面から「不審なセキュリティソフトの購入や、不審なスマートフォンアプリのインストールに誘導された」といった相談が急増した(図 1-2-38)。IPA は 2021 年 3 月、「安心相談窓口だより※130」で注意喚起を行った。



■図 1-2-38　Web ブラウザ通知機能の悪用の相談件数推移

(ア)手口

Web ブラウザの通知機能※131 を悪用し偽の通知を表示させ、不審サイトに誘導する手口である。以下の①から③の流れとなる場合が多い。

①サイト上で Web ブラウザの通知を許可するように誘導される

検索サイトで表示されたサイトにアクセスする等でサイトに訪れた人に Web ブラウザ通知の許可ボタンを表示し、アクセスした人に「許可」を押させようとする(図 1-2-39)。その際、reCAPTCHAv2 認証※132 を装った画面を表示して、「許可」ボタンを押させようと誘導する(図 1-2-40)。

■図 1-2-39 「許可」ボタンへの誘導事例(Android の場合)

■図 1-2-40 reCAPTCHAv2 認証を装った「許可」ボタンへの誘導事例(パソコンの場合)

② Web ブラウザ起動中に偽の通知が表示される

図 1-2-39 や、図 1-2-40 等の画面で「許可」を押してしまうと、当該不審サイトの通知許可が Web ブラウザに登録されてしまう。その後、Web ブラウザを起動中等に「パソコンがウイルス感染した」「スマートフォンをクリーンアップしてください」(図 1-2-41) 等の通知が表示

■図 1-2-41 スマートフォンに表示される通知表示事例(Android の場合)

■図 1-2-42 パソコンのデスクトップ右下に出現する通知表示事例

される。

パソコンではセキュリティベンダや、Windows のロゴを勝手に使用したと思われる通知がデスクトップの右下に表示される事例を確認している(図 1-2-42)。

これらの通知は根拠のない偽の内容であり、不安をあおって不審サイトに誘導する目的であると考えられる。

③通知表示をクリックすると不審なサイトに誘導される

通知表示をクリックすると、様々な不審サイトに誘導される。パソコンの場合、「偽のセキュリティ警告」が表示されるサイトや、「セキュリティソフト購入サイト」に誘導される。スマートフォンの場合、「不審アプリのインストール誘導サイト」が表示される事例を確認している。

(イ)対処

Web ブラウザ通知機能の悪用そのものへの対処、Web ブラウザ通知機能を悪用された結果起こった事象への対処、それぞれの対処方法について述べる。

① Web ブラウザの通知の削除方法

Web ブラウザに登録した通知許可を削除することで、通知表示を止めることができる。各 Web ブラウザ操作方法の詳細は、「安心相談窓口だより※128」や、パソコン・スマートフォンメーカのサポート情報、各 Web ブラウザのヘルプページを参照いただきたい。

②誘導された不審サイトで操作を行った場合

誘導された不審サイトの手口に応じて、以下の対処を行う。

- 偽のセキュリティ警告に誘導された場合
  「1.2.7(4)(a)偽のセキュリティ警告」に記載した対処を行う。
- セキュリティソフト購入サイトに誘導された場合
  マカフィー株式会社と思われるサイトに誘導された場合は、マカフィー株式会社の Web ページにある、「マカフィーを装う偽のポップアップ通知と問題の解消方法について※133」を参照して対処いただきたい。誤って製品等を購入した場合については、「一般的な FAQ※134」を参照いただきたい。
- 不審アプリのインストールサイトに誘導された場合
  「1.2.7(4)(b)アプリ誘導」に記載した対処を行う。

(5) 騙しの手口への対策

情報セキュリティへの意識の高まりを攻撃者に逆手にとられ、「ウイルス感染」や「トロイの木馬」「ハッキングした」等という文言を信じてしまい、被害に遭っていることが多いと考えられる。

日頃からしっかりとセキュリティ対策を行うことによって、不審な SMS やメール、端末への通知が来ても、いったん立ち止まり、対応を確認することができるので、過剰な心配をせず攻撃者に付け込まれないようにすることができると考える。

対策の例としては、以下のものがある。

- 使用している端末やアプリのアップデートを常日頃行う。
- サービスの利用にあたって、可能な場合は必ず多要素認証を設定する。
- 不審なメールや SMS、サイト等で目にした情報の真偽は、確かな情報源で確かめる。
- 判断に迷ったら、身に覚えのない内容のメールや画面に表示された電話番号の相手ではなく、信頼できる相手に相談する。

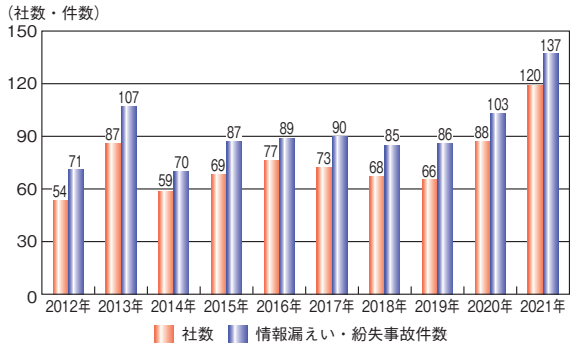
以上に加えて、日頃から最新情報を入手して手口を知ることが、騙しの手口への重要な対策となると考える。

1.2.8 情報漏えいによる被害

2021 年度も、多数の情報漏えい被害が発生している。本項では、外部からの不正アクセス、操作ミス等の過失、内部者の故意による持ち出し、不適切な情報の取り扱い等を主な要因とする情報漏えい被害について述べる。

(1) 2021 年の情報漏えいの概況

2022 年 1 月に株式会社東京商工リサーチ（以下、東京商工リサーチ社）が公開した上場企業の個人情報漏えい・紛失事故の調査結果※135 によると、2021 年に個人情報の漏えい・紛失事故を公表した上場企業は 120 社（2020 年※136 は 88 社）、事故件数は 137 件（2020 年は 103 件）、漏えいした個人情報は 574 万 9,773 人分（2020 年は 2,515 万 47 人分）に達した。漏えいした個人情報は大幅に減少しているが、公表した社数、事故件数ともに東京商工リサーチ社が調査を開始した 2012 年以降で最多となった（図 1-2-43）。



■図 1-2-43　漏えい・紛失事故の年次推移
（出典）東京商工リサーチ社「上場企業の個人情報漏えい・紛失事故は、調査開始以来最多の 137 件 574 万人分（2021 年）※135」を基に IPA が編集

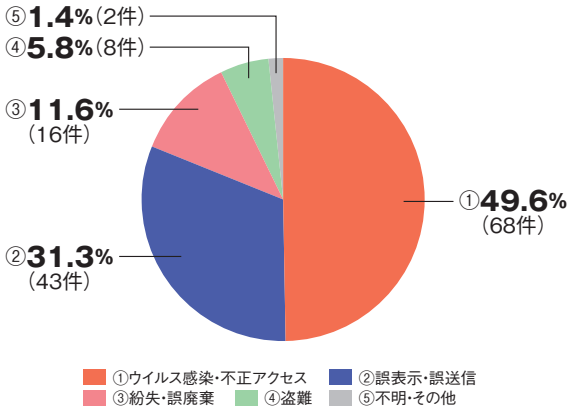
2021 年の情報漏えい・紛失事故 137 件のうち、原因として最も多かったのは「ウイルス感染・不正アクセス」の 68 件、構成比 49.6%（2020 年は 51 件、構成比 49.5%）、次いで「誤表示・誤送信」が 43 件、構成比 31.3%（2020 年は 32 件、構成比 31.0%）となっており、構成比の変化は小さいが、件数がともに 10 件以上増えており、過去最多となった要因になっている（次ページ図 1-2-44）。

(2) 不正アクセスによる情報漏えい

不正アクセスの手口は年々巧妙化しており、システムの脆弱性を利用したものや、対策が不十分な委託先、システム等、様々な原因から不正アクセスが発生している。

(a) 不正アクセスによる大量の情報流出事例

株式会社ネットマーケティングの事例※137 では、同社の運営する恋活・婚活マッチングアプリ「Omiai」から 171 万 1,756 件の年齢確認書類画像データが流出した。年齢確認書類画像データは法令で義務付けられた本人



■図 1-2-44　情報漏えい・紛失事故件数の原因別割合
(出典)東京商工リサーチ社「上場企業の個人情報漏えい・紛失事故は、調査開始以来最多の 137 件　574 万人分(2021 年)」を基に IPA が編集

確認に使用しており、運転免許証、健康保険証、パスポート、マイナンバーカード（表面）等が含まれていた。その他に登録されていた個人情報の流出は確認されていない(「3.3.2(2)不正アクセスに起因するインシデント」参照)。

森永製菓株式会社の事例※138-1では、同社運営のWeb サイト「森永ダイレクトストア」(旧「天使の健康」)の顧客 164 万 8,922 人分の個人情報(氏名や住所、連絡先等）が流出した可能性があると公表した。脆弱性が残存していたネットワーク機器への攻撃により侵入され、一部のデータは利用できない状態となった。

カジュアルウェア専門店株式会社ライトオンの事例では、公式オンラインショップに不正アクセスがあり、会員登録フォームより入力された個人情報（氏名や生年月日、性別、住所、電話番号、メールアドレス等）24 万 7,600 件が流出した※138-2。

臨床試験に関する業務を受託する株式会社リニカルの事例※139では、日本、台湾、欧州の同社拠点のサーバに対して不正アクセスがあり、犯行グループから窃取したとするデータに対して身代金を要求する脅迫メッセージがあった。日中韓台の採用応募者や株主情報等約 9 万 6,000 件、日欧中韓台の社員情報・人事情報約 12 万 5,000 件及び臨床試験関連文章や営業データ等が流出した可能性が判明した。

映像技術・マイクロ波・無線通信技術の専門メーカである株式会社ユピテルの事例※140では、同社は 52 万 8,563 件のデータ、会員情報 40 万 5,576 件が 2017 年 10 月に流出していたことを 2021 年 6 月に公表した。2017 年当時は不正アクセスを確認するも情報流出の痕跡は認められなかったため公表しなかったが、2021 年 5 月にサーバからハッキングした顧客情報を持っているとして、犯人と見られる人物から金銭を要求する脅迫メールが同社に届き、記載されたリンク先で上記情報を確認したという。

(b)不正アクセスによる情報流出への対策・対処

不正アクセスの事前対策については、「1.2.1 (5) 標的型攻撃への対策」を参照いただきたい。不正アクセスを認識した場合、情報流出の有無の調査に時間を要することが多い。情報漏えいは企業・組織の信頼を失墜させる可能性があり、流出の事実が確認できるまでは公表を避けたいと考える企業もある。しかし、不正アクセスが検知された段階で公表することにより、類似の攻撃によるインシデントの未然防止や早期検知に貢献できる。また流出が確認された場合は、情報の悪用による二次被害を防げる可能性がある。そのため、企業・組織は早期に公表、あるいは関連機関への報告を行い、調査を継続して経過を伝えることが重要である。なお、2020 年 6 月に公布され、2022 年 4 月より全面施行された「個人情報の保護に関する法律等の一部を改正する法律案」では、情報が漏えいした場合の個人情報保護委員会等への報告や本人への通知が、一定条件のもとで義務化された(「2.8.1 個人情報保護法改正」参照)。

情報流出の有無について調査でも判明しない場合は、不正アクセス対策を強化するとともに、定期的に流出した情報が悪用されていないかを確認することが必要である。

個人情報については、必要以上に保有しないことも重要である。前述の株式会社ネットマーケティングの事例では、会員情報の保管期間を一律で退会後 10 年間としていたが、被害後、年齢確認書類画像データは提出後 72 時間で自動削除、その他の個人データは退会後 90 日間と変更し、他の安全対策とともに運用を開始した。

(c)SQL インジェクション攻撃による情報流出事例

株式会社メタップスペイメントの事例※141では、決済情報等を格納した三つのデータベースに不正アクセスされ、そのうちの一つであるトークン方式クレジットカード決済情報データベースから最大 46 万 395 件のクレジットカード情報(カード番号、有効期限、セキュリティコード)が流出した可能性がある。本事例では SQL インジェクション攻撃と不正ファイル（バックドア）の設置が確認されている。同社の収納代行システムを利用する団体では、一部のカード決済機能の停止、チケット販売や新規入会停止等の影響が出た※142。

SQL インジェクション攻撃による情報の流出では、他に

も中学受験関連サービスを提供する株式会社日能研※143から最大28万106件、翻訳ソフトウェア事業等を展開するロゴヴィスタ株式会社※144から約12万8,000件、株式会社石橋楽器店※145から9万8,635件、自社ブランド製品の企画、開発を行うビーズ株式会社※146から2万3,435件のメールアドレスが、宅配クリーニングサービスのWebサイトを運営する株式会社ヨシハラシステムズ※147から5万8,813件のクレジットカード情報が流出した可能性があると公表されている。

(d) SQLインジェクション攻撃による情報流出への対策

SQLインジェクションは過去10年以上にわたり問題であり続けている。IPAでは2008年に「SQLインジェクション攻撃に関する注意喚起※148」、2017年に「SQLインジェクションをはじめとしたウェブサイトの脆弱性の再点検と速やかな改修を※149」と題する注意喚起を行っている。IPAが公開している「ウェブ健康診断仕様※150」「安全なウェブサイトの作り方※151」等を参照して、対策を検討いただきたい。

(e) ランサムウェア攻撃による情報流出事例

日本サブウェイ合同会社の事案※152では、ランサムウェア攻撃により、約30万件のサブクラブカード会員番号、約8万人分の顧客情報(誕生日、都道府県、職業等)、約1万人分の個人情報(名前、結婚歴、誕生日、性別、住所、職業、電話番号、職歴、メールアドレス、収入情報、銀行口座情報、自動車運転免許、国籍、クレジット歴、パスポート/ID、賞罰歴、ユーザネーム等)、64名の顧客情報(名前、年齢、電話番号)に不正アクセスされた恐れがあると公表している。

行政機関の公共事業を受託するランドブレイン株式会社の事例※153では、不正アクセスした攻撃者が、サーバ上の二つのファイルを開封した痕跡があり、データの暗号化、ファイルの作成が確認された。しかし、情報流出を示唆する明確な痕跡は確認されず、情報流出はないと判断したという。攻撃に用いられたランサムウェアは、「Crypt3r」「Ghost」「Phantom」「Vjiszy1lo」といった別名でも知られる「Cring」であることが判明した※154。

同じく公共事業を受託する株式会社オリエンタルコンサルタンツホールディングスの事例※155では、同社はグループ会社数社の複数のサーバがランサムウェア攻撃を受け、サーバ内の委託業務関連データの多くが暗号化され、外部流出した可能性があると公表した。流出の可能性のある情報には、千葉県、東京都、群馬県、滋賀県、埼玉県、岡山県等※156の建築関連の委託業務の図面や資料、関係者の個人情報等が含まれているが、どの情報が流出したかの特定には至っていない。同社は2021年9月期(2020年10月1日～2021年9月30日)の連結業績について、復旧に向けた関連費用として約7億5,000万円の特別損失を計上する見込みを発表した※157。

その他のランサムウェアの被害と対策については「1.2.2 ランサムウェア攻撃」を参照いただきたい。

(f) 委託先のシステムが不正アクセスされたことによる漏えい事例

富士通株式会社の事例※158では、同社はプロジェクト情報共有ツール「ProjectWEB」に不正アクセスがあり、保存していた情報の一部が不正に閲覧またはダウンロードされたと公表した。同社がプロジェクト運営に際し、委託元を含む関係者との情報共有にProjectWEBを利用しており、被害のあった顧客は行政機関(NISC、外務省、国土交通省、総務省等)や重要インフラ企業(成田国際空港株式会社等)等142に及んだ。閲覧またはダウンロードされた情報には、システムに関する情報(システムを構成する機器類の情報等)、プロジェクト関連資料(体制図、打合せメモ、作業項目一覧、進捗管理表、社内事務手続きの資料等)、顧客・関係者の個人情報(氏名・メールアドレス等)が含まれていたという。同社は、脆弱性を悪用した第三者がIDとパスワードを窃取し、外部から不正アクセスを行ったとしている。NISCは政府機関等、重要インフラ事業者等に向けて、同種ツールに対する不正アクセス対策の確認について注意喚起※159を行った。同社はProjectWEBの利用を停止し、その後の調査でProjectWEBに複数の脆弱性が存在していたこと、多要素認証を採用していなかったこと、不正アクセスを早期に検知する仕組みが十分でなかったこと等を認めた。

株式会社ジーアールの事例※160では、同社が運営する「オムニECシステム」に不正アクセスがあり、顧客情報やクレジットカード情報が流出した。クレジットカード会社から同システムを利用する流通大手企業に情報流出の懸念があると同社に連絡があり、発覚した。同システムは、小売店や製造販売会社のサービスのデジタル統合に利用されており、影響を受けた11社※161が被害を公表した。漏えいした情報は11社合わせて40万件以上に及ぶ。この事例の攻撃手法はクロスサイト・スクリプティングだったと報じられている。

(g) 委託先のシステムへの不正アクセス対策・対処

複数の企業・組織が利用するシステムやサービスに対する不正アクセスは、影響範囲が広く、システムやサービスの提供事業者は、不正アクセス対策と流出した情報を特定する調査に時間を割かれる。利用各社は情報流出の可能性について報告を受けた場合、すぐに、二次被害を防ぐための対応と当該システムやサービスの利用継続を検討しなければならない。情報流出被害がなかった委託元企業・組織も、システムやサービスの運用停止、改修等の影響を受ける可能性がある。システムやサービスの委託にあたっては日頃から保管を委託する情報の種類、量、保管状態等を確認し、この情報が流出あるいは利用できない状態となった場合の対応策についても検討しておくことが望ましい。

(3) 過失による情報漏えい

認定個人情報保護団体である一般財団法人日本情報経済社会推進協会（JIPDEC）が 2021 年 10 月に公表した「（2020 年度）『個人情報の取扱いにおける事故報告集計結果』[※162]」によると、2020 年度は 939 のプライバシーマーク付与事業者から 2,644 件の事故報告があった。事故の発生原因としては「誤送付」が 62.3%（2019 年度は 59.5%）と最も多く、「紛失」が 14.9%（2019 年度は 16.6%）、「その他漏えい」が 17.2%（2019 年度は 17.5%）となっている。「誤送付」の中でも「メール誤送信」は過去 5 年間で最も多く、764 件に達している。これに対し、「宛名間違い」「封入ミス」「FAX 誤送信」等の紙媒体を伴う報告は減少しており、テレワークの導入等により、通信及び連絡手段が変化したことによるものと推測している。

(a) 過失による情報漏えい事例

日本年金機構の事例[※163]では、同機構は年金振込通知書の印刷誤りにより愛知県、三重県、和歌山県、奈良県、福岡県、山形県、富山県、静岡県、岐阜県の合わせて 97 万 5,065 件の受給者に、本人と別の受給者の情報が記載されたはがきを送付したと公表した。原因は、印刷業務を委託したサンメッセ株式会社での印刷工程の作業ミスであったが、その後の調査により、仕様書どおりの環境で作業せず同機構に虚偽の報告をしていた、出力設定に誤りがないことを確認する仕組みがなかった、仕様書に定められている宛名と記載情報の突合作業をしていなかった等、作業ミスの防止対策が実施されていなかったことが分かった[※164]。年金振込通知書の再作成・発送やお詫び状の送付等費用はサンメッセ株式会社が負担し、同社は 2022 年 3 月期第 2 四半期において 2 億 3,000 万円の特別損失を計上した[※165]。

LINE 株式会社の事例[※166-1]では、同社は LINE VOOM（旧タイムライン）において、システム移行時の設定ミスにより「友だち」の公開範囲の設定が適切に機能せず、利用者が非公開と設定した「友だち」が公開先リストに誤って含まれる不具合があったと公表した。この不具合により、約 111 万アカウント（国内約 84 万アカウント）において非公開投稿が誤って表示されたほか、非公開の「友だち」が「LINE 友だち」に追加されたアカウントは約 911 万アカウント（国内約 764 万アカウント）に上るという。

LINE Pay の事例[※166-2]では、LINE 株式会社がサービス利用ユーザのアカウント合計 13 万 3,484 件（うち国内ユーザは 5 万 1,543 件）のキャンペーン関係の識別情報（識別子・加盟店管理番号、キャンペーン情報）が GitHub 上で外部閲覧可能な状態にあったと公表した。同社の委託先であるグループ会社の従業員が、ポイント付与漏れの調査を行うプログラム及び対象となる決済に関する情報を無断で GitHub 上にアップロードしてしまい、閲覧できる状態であったという。部外者から GitHub の情報へのアクセスが 11 件あったことが確認され、流出対象となったユーザに通知を行った。

(b) 過失による情報漏えいへの対策

情報の取り扱いに人が介在する状況においては、過失による情報漏えい被害を完全に防ぐことは難しい。事故事例に基づく教育等で担当者の意識向上を図ることに加え、重要な情報の取り扱いルールを設け、運用を徹底する、適宜見直す等で、過失の発生機会をできる限り削減する体制づくりが望まれる。うっかりミスを減らすために、ダブルチェック等の対策が取られることも多いが、新型コロナウイルス対策、あるいは、省人化・自動化のため、1 人で業務することも増えており、業務フローの見直しも含めたリスク低減策が必要である。また、業務を委託している場合は、ルール順守状況の点検や成果物の確認等を委託元の責任として実施することも大切である。

(4) 内部不正による情報漏えい

IPA が実施した「企業における営業秘密管理に関する実態調査 2020[※167]」では、営業秘密の漏えい原因は「中途退職者」が 36.3% と最も多く、2016 年の調査から 7.7 ポイント上昇していた。同調査によれば、うっかりミス

は減少したが確信犯的な内部不正は増加しており、継続している傾向がうかがえる。

(a) 内部不正による情報漏えい事例

株式会社村田製作所の事例※168では、同社は委託先である日本アイ・ビー・エム株式会社の再委託先の中国法人 IBM Dalian Global Delivery Co., Ltd. の社員が同社の取引先情報 3 万 555 件、同社の従業員関連情報 4 万 1,905 件を含むプロジェクト管理データを許可なく業務用パソコンへダウンロードし、更にこれらのデータを中国国内クラウドストレージサービスの個人アカウントへアップロードしていたと公表した。再委託先の社内監視システムのセキュリティアラートにより検知された。

回転ずし大手「かっぱ寿司」を経営するカッパ・クリエイト株式会社の事例※169では、同社は代表取締役が競合する株式会社はま寿司（以下、はま寿司）の営業秘密を不正に取得したとして、不正競争防止法違反で警視庁から捜査され、はま寿司により告訴がなされたことを公表した。代表取締役は、同社の顧問となる以前は、はま寿司の親会社である株式会社ゼンショーホールディングスに勤めており、元同僚からはま寿司の日次売上データ等の送付を数回にわたって受けていた。

株式会社ハウスドゥ住宅販売の事例※170では、元従業員が 2021 年 1 月に同社を退職する際、所属部門に保管されていた顧客情報を持ち出した。同社は元従業員を不正競争防止法違反で刑事告訴し、愛知県警察による捜査で不正な持ち出しが判明した。

(b) 内部不正による情報漏えいへの対策

IPA では、2022 年 4 月に「組織における内部不正防止ガイドライン※171」第 5 版を公開した。内部不正による情報セキュリティ事故を防止するための幅広い対策を掲載しており、参照いただきたい（「2.8.2 内部不正防止対策の動向」参照）。

(5) 不適切な情報の取り扱い

紙媒体を含めた情報の不適切な管理による漏えいも継続している。

(a) 不適切な情報の取り扱い事例

日本郵便株式会社の事例※172では、投資信託取り引き及び国債取り引きに関する「金融商品仲介補助簿」の社内紛失が全郵便局 1 万 9,816 局のうち 6,389 局（32.2%）で確認され、合わせて顧客約 7 万 2,000 人分と公表された。また「金融商品仲介補助簿」以外の書類を確認した結果、176 局で約 14 万 2,000 人分を紛失していた。「金融商品仲介補助簿」は法令上 7 年保存（社内規則上は 10 年保存）と定められていたが、大多数の郵便局において保存期間の認識相違や保存箱の入れ間違い等により、誤って廃棄してしまったという。

金沢信用金庫の事例※173では、同金庫は為替関係帳票、ATM ジャーナル、住宅ローン稟議書、伝票等の書類を保管していた文書箱合わせて 11 箱、延べ 55 万 1149 件の顧客情報の所在が不明であることを公表した。保存期限を経過した書類を廃棄（裁断）した際、誤ってこれらも廃棄（裁断）した可能性が高いと考えられている。

トヨタ自動車株式会社の事例※174では、同社が提供する顧客向け Web サイト認証サービス「TOYOTA/LEXUS の共通 ID」の ID 発行のため、本人の同意を得ずに顧客情報を登録していた。同社の販売店である福岡トヨペット株式会社において、同事象が発覚し、全国 257 社で同様の事例がないか調査した結果、27 社、5,797 人分の個人情報（名前、生年月日、性別、住所、電話番号、コネクテッドサービス契約車両の所有情報）が本人の同意を得ずに登録されていたという。このような個人情報の不適切な取り扱いの背景には、同社から販売店に同 ID の発行を推奨する活動を行っていたことがあるとされる。同様に、株式会社 SUBARU※175においても本人の同意を得ずに新規会員登録が行われていた。

新生銀行グループの事例※176では、株式会社新生銀行並びに新生フィナンシャル株式会社は複数の業務委託先に対して Web 解析や広告媒体事業に関するデータを提供する際、提供対象ではないデータが誤って含まれていたと公表した。同行において、Web 解析を目的に、業務委託先等のうち 1 社から還元を受けたデータを検証したところ、新生銀行グループの株式会社アプラスから提供したデータに、提供すべきでない ID・パスワードが含まれていたことから、同グループ内において類似の事象が発生していないか調査を実施した。その結果、七つの事案において延べ 8,875 件のデータが誤って業務委託先及び広告媒体会社 10 社に提供されていた。提供されたデータにはメールアドレス、住所、氏名、生年月日、会員番号、カード番号、カード暗証番号、金融機関と口座情報等が含まれていた。

株式会社新生銀行の別の事例※177では、同行は吸収分割契約によりマネックス証券株式会社へ承継する投資信託保護預かり口座の情報を提供する際、無関係の

口座情報 1,469 件を誤って提供したことを公表した。提供された情報には個人情報（マイナンバー、氏名、生年月日、口座番号）、法人情報（法人番号、法人名、口座番号）が含まれていた。

(b) 不適切な情報の取り扱いへの対策

個人情報や営業秘密情報等の取り扱いについては、法改正やガイドラインの整備が進んでおり、社内ルールへの取り込みや周知徹底のために従業員への教育等を継続して行う必要がある。

COLUMN

子どもへの情報リテラシー教育のために

IPA では、情報セキュリティの基礎知識に加えて情報リテラシーの向上を目指し、「インターネット安全教室」という講義形式のセミナーを実施しています。対象は、「インターネットを利用するすべての方」で、子どもからシニア世代まで幅広く受講いただいています。受講された学校の先生から、「生徒の自宅での情報端末管理は各家庭に任せている」という声があり、家庭での情報リテラシー教育も重要なことを改めて認識しました。

インターネット利用開始時に誰に使い方を教えてもらったかを尋ねたところ、保護者と回答した割合が最も多かったという家庭教育の重要性を示す調査結果[i]があります。SNS をめぐるトラブルや情報流出等の事故を防ぐためには、判断能力が十分に備わっていない子どもに任せきりにせず、保護者との日頃のコミュニケーションを通じた学びが不可欠です。

子どもに情報端末を持たせるとき、保護者側が何らかのルールを設ける場合が多いものの、その内容は利用する時間・場所、利用料金や利用するサイトに関するものが多く[ii]、ID・パスワードの管理といったセキュリティ寄りの内容はやや不足しているように思われます。GIGA スクール構想で一人一台の情報端末が配布され、オンライン教育も当たり前のものとなった今、子どもにとって、インターネットを安全に利用するための情報セキュリティはより身近なものとなり、保護者自身も意識を高めていくことが重要です。

IPA では、Web サイト「#今こそ考えよう 情報モラル・セキュリティ[iii]」上で、対象者層ごとに適したコンテンツを紹介しています。更に、一般社団法人日本教育情報化振興会では、「ネット社会の歩き方[iv]」で、冊子・シミュレーション教材等を公開しています。ぜひ、これらの資料を活用しましょう。

一方、情報リテラシー啓発に携わる教育委員会の委員等からは、「保護者に啓発したいけれども、なかなかセミナーの場に参加していただけない」という声が聞かれました。今後、保護者層へ訴求していくためには、学校や公的機関による従来の情報提供の形に加えて、情報リテラシー分野をより敷居の低いのものとするため、TV アニメ化もされた漫画「はたらく細胞[v]」にみられるような、擬人化したキャラクターやストーリーをきっかけに、保護者・子どもが共に楽しみながら学べる新しいコンテンツ等も求められているのかもしれません。

i　総務省：2020 年度 青少年のインターネット・リテラシー指標等に係る調査結果　https://www.soumu.go.jp/main_content/000746185.pdf〔2022/5/23 確認〕
ii　内閣府：令和 2 年度 青少年のインターネット利用環境実態調査（PDF 版）　https://www8.cao.go.jp/youth/youth-harm/chousa/r02/net-jittai/pdf-index.html〔2022/5/23 確認〕
iii　https://www.ipa.go.jp/security/keihatsu/imakoso/〔2022/5/23 確認〕
iv　http://www2.japet.or.jp/net-walk/〔2022/5/23 確認〕
v　株式会社講談社：はたらく細胞　https://shonen-sirius.com/series/sirius/saibou/〔2022/5/23 確認〕

1.3 情報システムの脆弱性の動向

本節では、ソフトウェア製品の脆弱性の動向や、ソフトウェア製品及びWebアプリケーションの脆弱性対策について概説する。

1.3.1 JVN iPediaの登録情報から見る脆弱性の傾向

IPAは、脆弱性対策情報データベース「JVN iPedia※102」に、国内外のソフトウェア製品の脆弱性対策情報を収集し、蓄積している。このデータベースに登録されている脆弱性対策情報から、ソフトウェアに関する脆弱性の特徴を統計的に確認することができる。本項では、2021年12月までに登録されたJVN iPediaの脆弱性対策情報の傾向を分析する。

(1) JVN iPediaへの登録状況

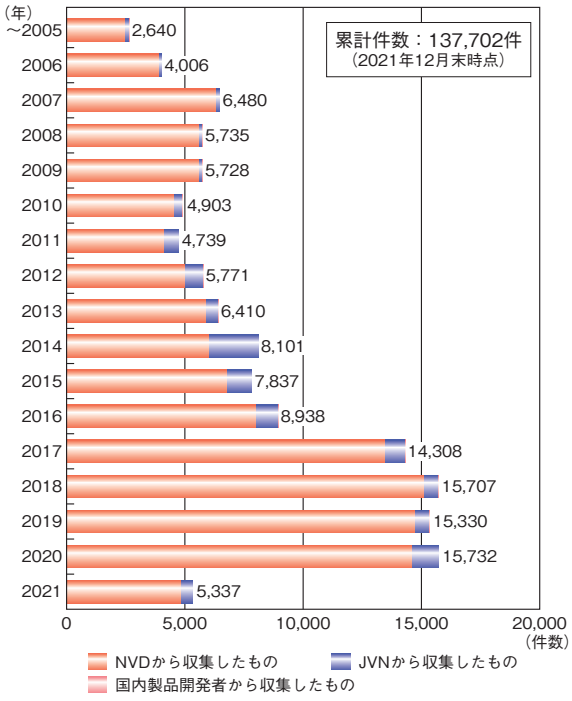
JVN iPediaは、国内外で利用されているソフトウェア製品の脆弱性対策情報を、以下の三つの公開情報から収集・蓄積しており、2007年4月25日から公開している。

- 脆弱性対策情報ポータルサイトJVN※178で公表した脆弱性対策情報
- 国内のソフトウェア開発者が公開した脆弱性対策情報
- 米国国立標準技術研究所（NIST：National Institute of Standards and Technology）の脆弱性データベース「NVD※179」で公開された脆弱性対策情報

(a) JVN iPediaの登録件数の推移

JVN iPediaに登録している情報を、製品ベンダやセキュリティ関連企業が脆弱性情報を公表した年別※180にまとめると、2011年を境にしてNVDから収集した脆弱性対策情報の登録件数がおおむね増加傾向となっており、2018年以降は1万5,000件を超えている。なお、2021年の登録件数は12月末時点で5,337件であるが、脆弱性対策情報の公開からJVN iPediaへの登録までタイムラグがあるため、2021年の登録数も最終的には2020年と同程度になる見込みである（図1-3-1）。2017年以降、NVDに公開される脆弱性の件数が大幅に増加した理由としては、脆弱性を登録するための共通脆弱性識別子CVE（Common Vulnerabilities and Exposures）※181の採番機関（CNA：CVE Numbering Authority）※182が増加したことが一因として挙げられる。The MITRE Corporation※183によると、2016年12月に47社※184だったCNAは、2021年12月には209社※185と約4.4倍となった。この増加したCNAによって、多くの脆弱性にCVEが付与され、NVDに公開される脆弱性の件数増加につながった可能性がある。

一方、JVNから収集した脆弱性情報は、2020年に公表されたものが1,120件で、2019年の594件から2倍近くになったが、2021年は再び減少し、半数以下の496件となった。また、国内製品開発者から公表された脆弱性対策情報は、毎年数十件の登録であり、2021年は12件であった。



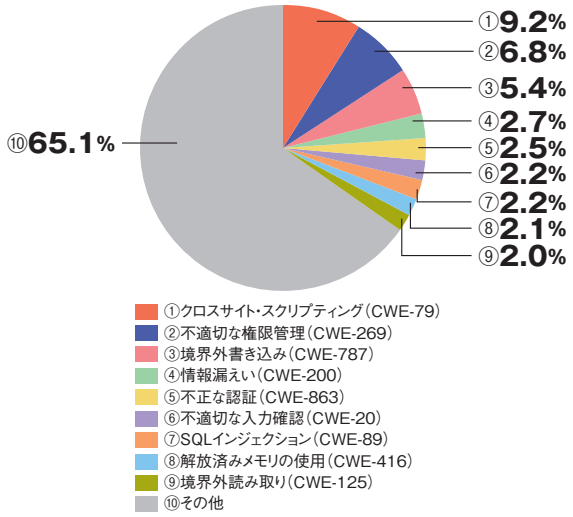
■図1-3-1 JVN iPedia登録状況（公表年別）
（出典）JVN iPediaの登録情報を基にIPAが作成

JVN iPediaは、発見された脆弱性の種類を識別するための共通脆弱性タイプ一覧（CWE：Common Weakness Enumeration）※186を脆弱性対策情報に付与して登録を行っている。2021年に登録したCWEの割合は「クロスサイト・スクリプティング」が9.2%と最も高く、「不適切な権限管理」が6.8%、「境界外書き込み」が5.4%、「情報漏えい」が2.7%と続いている（次ページ図1-3-2）。

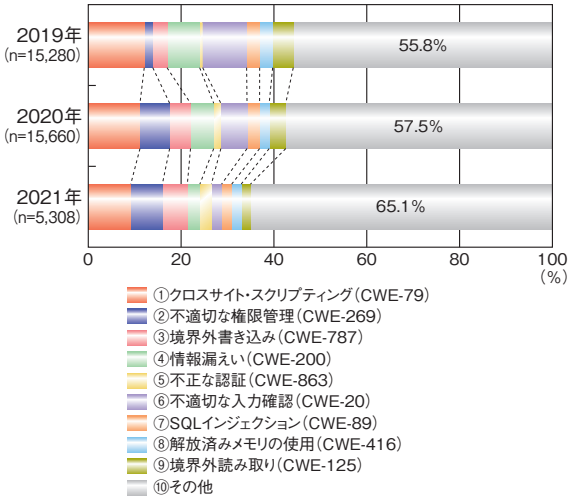
最も件数の多かった「クロスサイト・スクリプティング」に分類される脆弱性を悪用されると、偽のWebサイトへ

誘導され、情報が漏えいしたりする恐れがある。

2019 年以降の CWE 別割合を年別に見ると、上位 5 種では、「クロスサイト・スクリプティング」「情報漏えい」の割合が減少傾向にあり、「不適切な権限管理」「境界外書き込み」「不正な認証」の割合は増加傾向である（図 1-3-3）。一方で、上位 9 種と、10 位以下をまとめた「その他」の割合を見ると、上位 9 種については「不適切な入力確認」を始め、2020 年に比べて減少したものが多い。これに対して、「その他」の割合が 2021 年は 65.1%と 2020 年の 57.5%から増加している。この増加の一因としては、JVN iPedia の情報の収集元である NVD において、近年 CWE を細分化して採番する傾向があることが挙げられる。このため、これまで 9 種の CWE に分類されていた脆弱性の一部が「その他」に分類され、



■図 1-3-2　JVN iPedia における脆弱性対策情報の CWE 別割合（2021 年、n=5,308）
（出典）JVN iPedia の登録情報を基に IPA が作成



■図 1-3-3　JVN iPedia における脆弱性対策情報の CWE 別割合（2019 ～ 2021 年）
（出典）JVN iPedia の登録情報を基に IPA が作成

「その他」の採番が増えたと考えられる。

(b) JVN iPedia の登録情報の深刻度

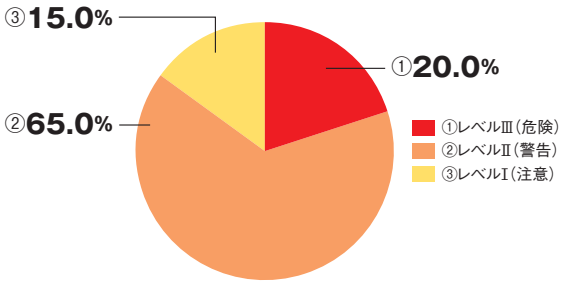
JVN iPedia は、オープンで汎用的な脆弱性評価手法である CVSS（Common Vulnerability Scoring System：共通脆弱性評価システム）[※187] を用いて、脆弱性の深刻度を公開している。なお、JVN iPedia では CVSS v2 及び CVSS v3 の二つのバージョンの情報を公開しているが、本項では CVSS v2 を基に統計処理を行っている。

深刻度には、CVSS v2 の基本評価基準（BM：Base Metrics）を基に評価した基本値によるレベルI、レベルII、レベルIIIの 3 段階があり、数値が大きい程深刻度が高い。

深刻度のレベルごとに想定される影響は以下である。

- 深刻度 レベルIII（危険）：基本値 7.0 ～ 10.0
  リモートからシステムを完全に制御されたり、大部分の情報が漏えいしたりする等の影響が想定される。
- 深刻度 レベルII（警告）：基本値 4.0 ～ 6.9
  一部の情報が漏えいしたり、サービス停止につながったりする等の影響が想定される。
- 深刻度 レベルI（注意）：基本値 0.0 ～ 3.9
  深刻度レベルII相当の影響があるが、攻撃するには複雑な条件を必要とする。

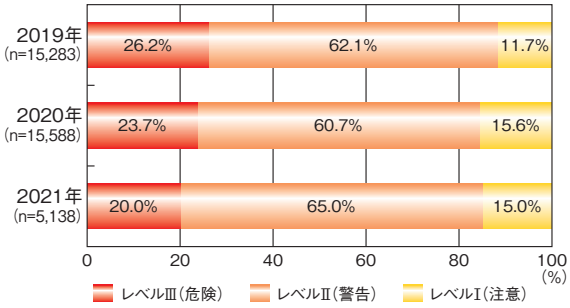
2021 年に登録された脆弱性対策情報を深刻度のレベル別で分類すると、レベルIIIが 20.0%、レベルIIが 65.0%、レベルIが 15.0%となっており、一部の情報漏えいやサービス停止につながるレベルII以上の脆弱性が全体の 8 割以上を占めている（図 1-3-4）。



■図 1-3-4　JVN iPedia における脆弱性対策情報のレベル別割合（2021 年、n=5,138）
（出典）JVN iPedia の登録情報を基に IPA が作成

2019 年以降の深刻度のレベル別割合を年別に見ると、レベルII以上の脆弱性の割合は 2019 年が 88.3%、2020 年が 84.4%と減少したが、2021 年は 85.0%とほぼ横ばいであった。更に 2021 年を 2020 年と比較すると、

最も深刻度が高いレベルⅢに該当する脆弱性の割合が3.7%減少し、レベルⅡの脆弱性の割合はその分増加している（図 1-3-5）。これは、比較的レベルⅡに分類されることが多い「不正な認証（CWE-863）」の脆弱性が増加したことや、全体の 65.1%を占める「その他」の脆弱性がレベルⅡに分類されることが多かったことが一因と考えられる。



■図 1-3-5　JVN iPedia における脆弱性対策情報のレベル別割合（2019 ～ 2021 年）
（出典）JVN iPedia の登録情報を基に IPA が作成

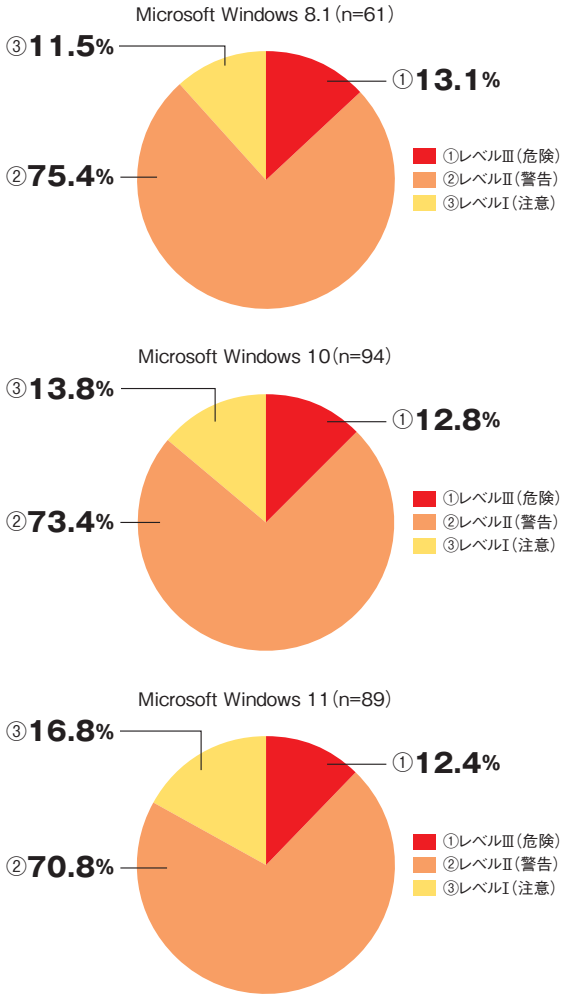
製品開発者は、ソフトウェアの企画・設計・製造段階からセキュアコーディング※188 を含めたセキュリティ対策を講じる等、脆弱性による被害を未然に防ぐための対応が必要となる。また、製品の利用者にも、日頃から新たに公開される脆弱性対策情報に注意を払い、脆弱性が公開された場合には製品を最新バージョンにアップデートする等の対応が求められる。

(2) Microsoft Windows 11 の脆弱性について

Microsoft 社より、Windows 11 が 2021 年 10 月 5 日（日本時間）にリリースされた。本製品は Windows 10 の後継バージョンとして注目を集め、無償でアップグレードできるため、徐々に利用者が増えている。同社は、Windows 11 は様々な新機能に加え、「何も信頼しない」を前提に対策を講じるゼロトラストの考え方を取り入れる等、セキュリティ面も強化したとしている※189。

その一方で、Windows 11 において既に多くの脆弱性が公開されている。リリースから 2021 年 12 月末までに、89 件の Windows 11 の脆弱性対策情報が JVN iPedia に登録された。その中には、深刻度の高い脆弱性も含まれている。図 1-3-6 は、2021 年第 4 四半期（10 月 1 日～ 12 月 31 日）に JVN iPedia へ登録された、現在 Microsoft 社でサポートされている Windows 8.1、Windows 10、Windows 11 の脆弱性対策情報の深刻度のレベル別割合である。

Windows 11 においては、脆弱性の深刻度が最も高



■図 1-3-6　JVN iPedia に登録された Microsoft Windows 製品の脆弱性対策情報の深刻度のレベル別割合（2021 年 10 ～ 12 月）
（出典）JVN iPedia の登録情報を基に IPA が作成

いレベルⅢが 12.4%、次に高いレベルⅡが 70.8%、レベルⅠが 16.8%である。レベルⅢ及びレベルⅡにあたる脆弱性が全体の 8 割以上を占めており、Windows 8.1、Windows 10 と比較して深刻度のレベル別割合に大きな差は見られなかった。このことから、2022 年以降も Windows 11 の脆弱性対策情報は、これまでの Windows OS と同様の傾向で公開されると見られる。

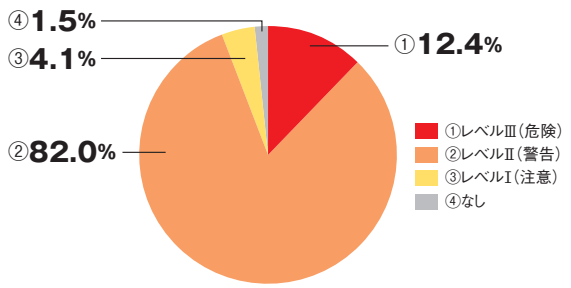
これらの脆弱性を解消し安全に Windows 11 を利用するためには、利用者は従来の Windows 製品と同様に Microsoft 社から公開される修正プログラムを速やかに適用することが推奨される。IPA においても、同社から月例の修正プログラムが公開された際、重要なセキュリティ情報として注意喚起情報を公開しており、特に脆弱性攻撃が確認されている場合は緊急対策情報として発信している。

(3) Apache HTTP Server の脆弱性について

2021 年 10 月に、Apache Software Foundation から Apache HTTP Server の脆弱性 CVE-2021-41773 の情報が公開され、IPA を始め複数の公的機関から脆弱性の悪用が確認されたとして注意喚起が発信された※190。本脆弱性はドキュメントルート外のファイルにアクセスされる恐れのあるパストラバーサルの脆弱性で、これを悪用されるとリモートから不正にファイルを操作される恐れがあった。脆弱性の深刻度を示す CVSS v2 基本値は 4.3※191 でレベルⅡにあたり、特別高い数値ではなかった。しかし、複数の実証コードが公開され、国内での攻撃が確認されたこともあり、脆弱性の影響を受けるバージョンを利用している組織は対策が求められた。

また、CVE-2021-41773 の修正版としてリリースされたバージョンの Apache HTTP Server にも、数日で別のパストラバーサルの脆弱性 CVE-2021-42013 が存在することが明らかになった。本脆弱性の CVSS v2 基本値は 7.5※192 で、レベルⅢに分類された。CVE-2021-41773 と同様に本脆弱性も実証コードの公開が確認され、また、CVE-2021-41773 の修正版のリリース直後に発見された脆弱性ということもあり、ネット記事等にも掲載され※193、広く注目された。

Apache HTTP Server は Apache Software Foundation がオープンソースソフトウェアとして提供している Web サーバ用のプログラムである。本製品の脆弱性対策情報は、JVN iPedia に 2021 年末までの累計で 194 件登録されている。図 1-3-7 はその深刻度別割合を示したものである。脆弱性の深刻度が最も高いレベルⅢが 12.4%、次に高いレベルⅡが 82.0%、レベルⅠが 4.1% となっており、脆弱性を悪用された場合の影響が大きい、レベルⅢ及びレベルⅡでほぼ占められている。



■図 1-3-7　JVN iPedia に登録された Apache HTTP Server の脆弱性対策情報のレベル別割合(2007 年 4 月～ 2021 年 12 月、n=194)
(出典)JVN iPedia の登録情報を基に IPA が作成

Apache HTTP Server のように広く利用されているソフトウェアは、脆弱性情報が公開されると攻撃者の注目も集まり、攻撃に悪用される恐れがある。利用者においては、継続的に脆弱性情報を収集し、修正プログラムが公開された場合は速やかに対応することが求められる。

(4) 今後の展望

JVN iPedia へ登録された脆弱性対策情報の累計件数は、2021 年 12 月末時点で 13 万件を超えている。2017 年以降は毎年 1 万件前後の脆弱性対策情報が登録されており、2022 年以降も同程度の件数が登録されていくものと考えられる。

2021 年は、2020 年に引き続き新型コロナウイルス感染への対応を迫られる年であった。対応の施策として、この間急速にテレワークの普及が進んだが、これに伴いテレワーク機器の脆弱性等を狙った攻撃も報告された※194。テレワーク対応のため急遽導入した機器については、業務の早期開始を重視した結果、脆弱性の管理がされていない等セキュリティに対して十分対応できないという課題が明らかになり、機器の運用管理の見直しが必要になった。

一方、2019 年の「情報処理の促進に関する法律の一部を改正する法律案」の閣議決定※195 等をきっかけに、DX (デジタルトランスフォーメーション) の考え方が注目されるようになり、組織においては業務の DX 化が求められるようになった。2022 年はテレワークに伴う業務のデジタル化が加速し、更に DX 導入が進展すると考えられる。これに伴い、AI (Artificial Intelligence：人工知能) や IoT 機器等を活用して DX 化を推進する様々な機器やソフトウェア、サービスが提供されると考えられる。このような DX 対応の機器やソフトウェアの導入にセキュリティ研究者や攻撃者が関心を持ち、新たな脆弱性を発見し、JVN iPedia 等の脆弱性対策情報データベースにおいて登録が増えることも予想される。

DX 化を推進する機器やソフトウェアの新たな脆弱性が発見されれば、それを狙った攻撃が増えると想定される。一方で、テレワーク対応機器の導入においては既知の脆弱性が放置され、被害が出た等の事例があり、DX 化を推進するための機器やソフトウェアの導入についても同様の問題が懸念される。これを防ぐために、導入した機器を構成するソフトウェア及びそのバージョンの把握、当該バージョンが影響を受ける脆弱性情報等の定期的な入手、アップデート対応等、基本的な脆弱性対策を適切に行っていくことを強く推奨する。その中の当該バージョンが影響を受ける脆弱性情報等の定期的な入手の一つの手段として、JVN iPedia をぜひ活用し

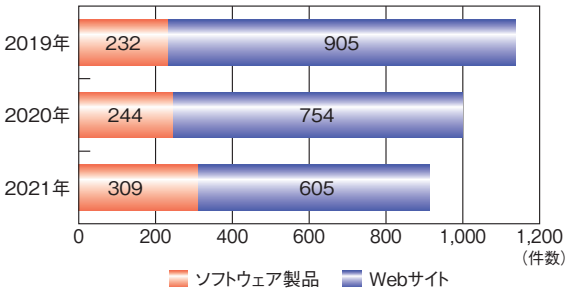
ていただきたい。

1.3.2 早期警戒パートナーシップの届出状況から見る脆弱性の動向

ソフトウェア製品や Web アプリケーション（以下、Web サイト）※196 の脆弱性を悪用した攻撃による情報漏えい、及び Web サイト改ざん等の被害は、2021 年も引き続き発生している。

社会的に大きな影響を与える恐れのある脆弱性については、開発者以外に関係機関から注意喚起等が出されることがある。例えば、2021 年 12 月には、多くの製品やソフトウェアで使用され、任意のコードが実行可能な Java ベースのロギングライブラリ Apache Log4j の脆弱性について、IPA 以外にも NISC 等複数機関から注意喚起※197 が出された。

「情報セキュリティ早期警戒パートナーシップ※198」（以下、パートナーシップ）では、脆弱性関連情報の届出※199 を受け付けているが、2021 年に届出された件数は、ソフトウェア製品が 309 件、Web サイトが 605 件、合計 914 件であった（図 1-3-8）。

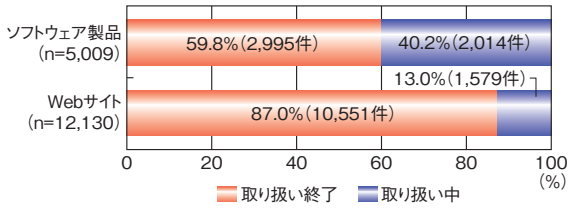


■図 1-3-8　脆弱性関連情報の種類別届出状況（2019 ～ 2021 年）
（出典）パートナーシップの届出状況を基に IPA が作成

2021 年のソフトウェア製品及び Web サイトの総届出件数（914 件）と、2020 年の件数（998 件）を比較すると、約 8% 減少している。なお、2021 年のソフトウェア製品と Web サイト個々の件数を 2020 年の件数と比較すると、ソフトウェア製品の届出は約 27% 増加、Web サイトの届出は約 20% 減少した。

パートナーシップ開始時点（2004 年 7 月 8 日）からの届出件数を累計すると、ソフトウェア製品は 5,009 件、Web サイトは 1 万 2,130 件となり、2021 年 12 月末時点での合計が 1 万 7,139 件に上る。これらの届出のうち IPA での取り扱いが終了※200 した届出件数は、ソフトウェア製品 2,995 件（59.8%）、Web サイト 1 万 551 件（87.0%）である（図 1-3-9）。

パートナーシップには、製品開発者と連絡が取れず進



■図 1-3-9　脆弱性関連情報の種類別取り扱い終了状況
（2021 年末までの累計）
（出典）パートナーシップの届出状況を基に IPA が作成

展が望めない届出（調整不能案件）を公表する手続きとして、公表判定委員会※201 がある。2021 年は、公表判定委員会の判定の結果、10 件の調整不能案件を JVN で公表した（「1.3.2 (1) (c) 公表判定委員会の判定による JVN 公表」参照）。

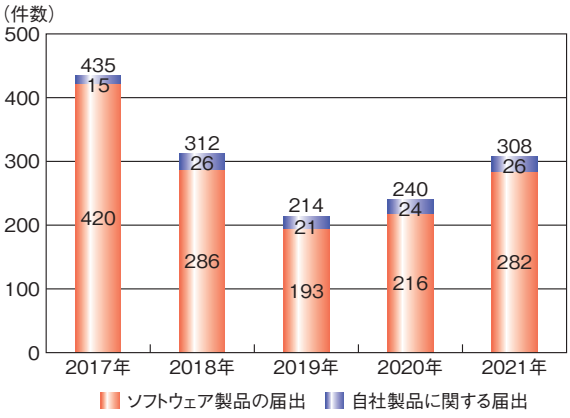
(1) ソフトウェア製品の脆弱性

2021 年のソフトウェア製品の脆弱性の状況を、パートナーシップへの届出件数や製品開発者による対策の取り組み状況等から解説する。

(a) 2021 年のパートナーシップの届出受付動向

2021 年にパートナーシップで受け付けたソフトウェア製品の届出（不受理 1 件を除く）は、308 件であった。

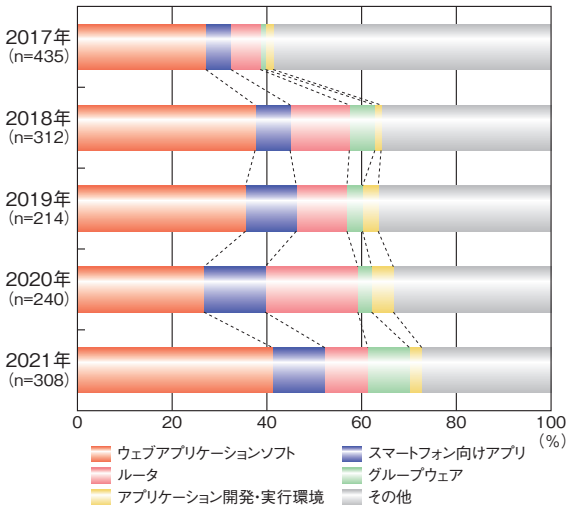
図 1-3-10 は、2017 年から 2021 年までのソフトウェア製品の届出受付数（不受理を除く）を示している。届出受付数は、2017 年の 435 件から 2019 年の 214 件まで減少したが、2020 年は 240 件、2021 年は 308 件と増えてきている。2021 年のソフトウェア製品の届出のうち、製品開発者による自社製品に関する届出は、308 件中 26 件であった。



■図 1-3-10　ソフトウェア製品の届出受付数（2017 ～ 2021 年）
（出典）パートナーシップの届出状況を基に IPA が作成

図 1-3-11（次ページ）は、同期間の製品の種類別の届出受付数の割合を示している。2021 年に割合が大き

く増加したものは「ウェブアプリケーションソフト※202」と「グループウェア」であった。「ウェブアプリケーションソフト」は41.2%と直近5年で最も大きな割合となっている。また、「グループウェア」は前年の2.9%から約3倍の8.8%になった。

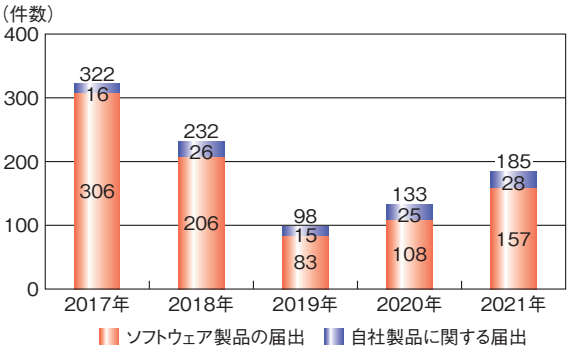


■図1-3-11　製品種類別のソフトウェア製品の届出受付数の割合（2017～2021年）
（出典）パートナーシップの届出状況を基にIPAが作成

(b) 2021年のJVN公表の動向

パートナーシップに届出のあった脆弱性の対策情報のうち2021年にJVN公表に至った件数は、185件であった。

図1-3-12は、届出のうち2017年から2021年までのJVN公表数を示している。2017年から2019年までJVN公表数は減少していたが、2020年からは一転して増加している。また2021年に公表した自社製品に関する届出は28件であった。



■図1-3-12　届出されたソフトウェア製品のうちJVN公表した件数（2017～2021年）
（出典）パートナーシップの届出状況を基にIPAが作成

2021年は、Webサイト構築に使用されるCMS（Content Management System）の脆弱性に関するJVN公表が31件あった。

CMSは、Webサイトのコンテンツの作成・管理に使用されるソフトウェア製品である。CMSの特徴として、「プラグイン」と呼ばれる拡張ソフトウェア製品を導入することで、機能の拡張が容易であることが挙げられる。CMSとプラグインを利用することで、Webサイトの運営者に専門知識がなくても、自組織のニーズに合わせたWebサイトの作成・管理が可能となる。代表的なCMSとしてはWordPressやMovable Type、EC-CUBE等が挙げられる。

2021年にJVNに公表したEC-CUBEに関連した対策情報を見ると、EC-CUBE本体だけでなく、プラグインも含めて脆弱性が発見されており（表1-3-1）、8件中6件がクロスサイト・スクリプティングの脆弱性であった。

項番	JVN番号	件名
1	JVN#97554111	EC-CUBEにおけるクロスサイトスクリプティングの脆弱性
2	JVN#79254445	複数のETUNA製 EC-CUBE用プラグインにおけるクロスサイトスクリプティングの脆弱性
3	JVN#57524494	複数のイーシーキューブ製EC-CUBE用プラグインにおける複数のクロスサイトスクリプティングの脆弱性
4	JVN#95292458	EC-CUBEにおける複数のクロスサイトスクリプティングの脆弱性
5	JVN#57942445	EC-CUBEにおけるアクセス制限不備の脆弱性
6	JVN#46313661	EC-CUBE用プラグイン「一覧画面（受注管理）項目変更プラグイン」におけるクロスサイトスクリプティングの脆弱性
7	JVN#23406150	EC-CUBE用プラグイン「注文ステータス一括変更プラグイン」におけるクロスサイトスクリプティングの脆弱性
8	JVN#75444925	EC-CUBE 2系における複数の脆弱性

■表1-3-1　2021年にJVN公表した「EC-CUBE」に関連した脆弱性対策情報
（出典）JVNを基にIPAが作成

公表した脆弱性の中でも、影響が大きいものとしてJVN#97554111※203がある。これは、EC-CUBE本体にクロスサイト・スクリプティングの脆弱性が存在したため、EC-CUBEを用いて作成したECサイトにおいて、攻撃者が特定の入力欄にスクリプトを入力することにより、ECサイト管理者のWebブラウザ上で任意のスクリプトが実行される可能性がある、というものであった。また、この脆弱性を悪用した攻撃が確認されており、実際にクレジットカード情報が流出したため注意喚起が出された※204。

CMSの脆弱性対策としては、CMS本体やそのプラ

グインを、常に最新の状態に維持（アップデート）することが重要である。アップデートをするためには、JVN や製品開発者の Web サイト等を確認し、脆弱性対策情報やアップデート情報が新たに公表されていないか定期的に確認しなければならない。また、開発・サポートが終了したプラグインについては、使用をやめる必要がある。

このようなアップデート情報の確認やアップデートの適用作業等が負担となる場合には、Web サイトの運用・保守作業を委託することや、CMS 本体を、自動アップデート機能を持つクラウド版に置き換えることも一つの方策となる。

(c) 公表判定委員会の判定による JVN 公表

パートナーシップでは、原則として、製品開発者の合意のもとで、脆弱性対策情報を JVN で公表しているが、届出の中には、製品開発者との連絡が取れない等の様々な理由により、公表に向けての調整が難航してしまう調整不能案件が存在する。

製品利用者が被害を受ける可能性を低減するため、IPA では、調整不能案件の脆弱性情報について、公表が適当か否かを判定する第三者委員会である「公表判定委員会」を組織している。

2021 年には、同委員会での判定に基づき、10 件の脆弱性情報を JVN に公表した（表 1-3-2）。JVN での調整不能案件の公表は 2020 年の 9 件に続き、2 年連続となった。また、公表した 10 件のうち 9 件は、深刻度の 3 段階レベルのうちレベルⅡの「警告」と判断され、残りの 1 件はレベルⅠの「注意」と判断された。

公表した脆弱性は、いずれも製品開発者と連絡が取れないことを理由に調整不能となったもので、アップデート等の対策は提供されていない。また、IPA において届出情報を基に製品を検証しており、脆弱性が存在することが確認されている。利用者には脆弱性を回避する対策として、製品の使用をやめることが求められる。

項番	JVN 番号	深刻度	件名
1	JVN#97370614	警告	マガジンガーZにおけるクロスサイトスクリプティングの脆弱性
2	JVN#12559271	警告	影舞におけるクロスサイトスクリプティングの脆弱性
3	JVN#42220311	警告	影舞におけるクロスサイトスクリプティングの脆弱性
4	JVN#11438679	注意	影舞におけるクロスサイトリクエストフォージェリの脆弱性
5	JVN#93207949	警告	Click Ranker におけるクロスサイトスクリプティングの脆弱性
6	JVN#37179202	警告	Yomi-Search におけるクロスサイトスクリプティングの脆弱性
7	JVN#83042295	警告	Yomi-Search におけるクロスサイトスクリプティングの脆弱性
8	JVN#94705238	警告	Yomi-Search におけるクロスサイトスクリプティングの脆弱性
9	JVN#68244135	警告	rNote におけるクロスサイトスクリプティングの脆弱性
10	JVN#55833077	警告	yappa-ng におけるクロスサイトスクリプティングの脆弱性

■表 1-3-2　2021 年に JVN 公表した調整不能案件
（出典）JVN を基に IPA が作成

(d) 製品開発者の脆弱性対策に関する取り組み

IPA とともにパートナーシップを運営している JPCERT/CC は、インシデント報告や脆弱性報告で顕著な貢献をした報告者を顕彰するための「ベストレポーター賞※205」を 2021 年に制定し、同年に初の贈呈を実施した。

同賞の脆弱性報告部門では、トレンドマイクロ社が製品開発者の脆弱性対応の取り組みとして、社内外で発見された自社製品の脆弱性について、その悪用の有無を含め多数報告し、脆弱性情報流通に対して前向きに対処、協力している姿勢が評価され受賞した。

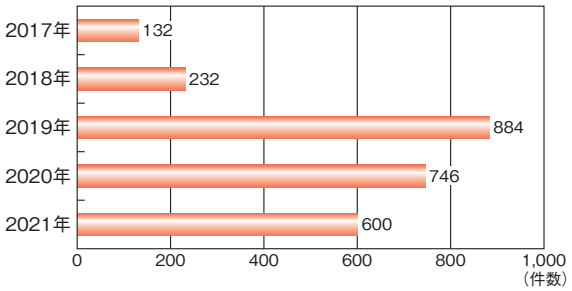
パートナーシップでは、製品開発者からの自社製品の脆弱性の届出も受け付けているが、2021 年の自社製品の届出は 26 件と多くない。

製品開発者から自社製品の脆弱性について報告が増えることで、製品開発者側での公表や JVN での公表も増え、より多くの利用者に対策情報が認識されるようになり、脆弱性悪用の被害が低減することが今後期待される。

(2) Web サイト※196 の脆弱性

2021 年にパートナーシップで受け付けた Web サイトの届出（不受理 5 件を除く）は、600 件であった。

図 1-3-13 は、2017 年から 2021 年までの Web サイトの届出受付数（不受理を除く）を示している。前年を大きく上回る 2019 年の 884 件をピークに、2020 年より届出

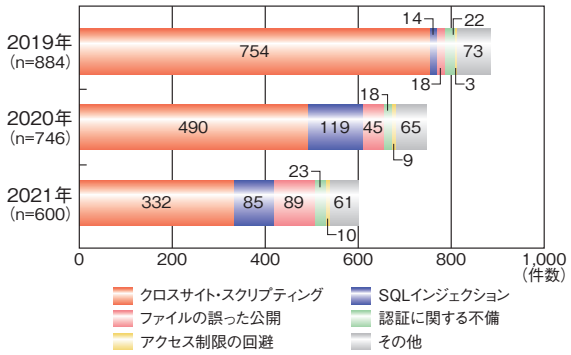


■図 1-3-13　Web アプリケーションの不受理を除いた届出件数（2017 ～ 2021 年）
（出典）パートナーシップの届出状況を基に IPA が作成

は減少してきている。

(a) パートナーシップから見る 2021 年の届出の傾向

図 1-3-14 は、2019 年から 2021 年までの脆弱性の種類別の届出受付数（不受理を除く）を示している。2020 年では届出全体に対する割合が多かった「クロスサイト・スクリプティング」と「SQL インジェクション」は、2021 年では減少した。他方、2021 年に増加したものに、「ファイルの誤った公開」がある。この脆弱性の 2021 年届出数は 89 件であり、2020 年の 45 件と比較すると 2 倍に増加した。これは、2004 年の制度開始から 2021 年までの間で当該脆弱性に関して最も多い件数である。



■図 1-3-14　脆弱性種類別の Web アプリケーションの届出受付数（2019 ～ 2021 年）
（出典）パートナーシップの届出状況を基に IPA が作成

「ファイルの誤った公開」は 2018 年当時からあり、決して少なくない。そのため同年の第 4 四半期の「ソフトウェア等の脆弱性関連情報に関する届出状況[※206]」では「機密情報の意図しない公開に注意」と題して、Web サイト運営者に注意を促していた。

しかしながら、その後も数の増減はあるもののパートナーシップには毎年一定数届出されている。前述のとおり、2021 年はこれまでで最多であり、依然としてこの脆弱性が残存する Web サイトが多数あると考えられる。

(b)「ファイルの誤った公開」の脆弱性の現状

「ファイルの誤った公開」とは、Web サイトの管理・運用においてアクセス制限等の設定不備により、意図せずファイルにアクセスされてしまう問題であり、このファイルに保存されている管理者権限のアカウントやパスワードが外部に流出すると、第三者に悪用され被害が深刻化する等の脅威が発生する。ディレクトリ・トラバーサルのようなソフトウェアの設計に起因する問題とは異なり、基本的には Web サイト運営者による不適切な運用の問題に起因する。

パートナーシップでは、このような問題についても、脆弱性の一種と定義し取り扱っている。

2021 年のパートナーシップに届出があった「ファイルの誤った公開」の主な要因は、CMS のような「ウェブアプリケーションソフト」を初期設定のまま使用し構築した問題であった。それにより Web サイトでは、公開領域に機密情報が含まれるファイルが生成、配置される作りとなっていた。

上記は「ウェブアプリケーションソフト」の仕様であり、この仕様に気が付かずそのまま運用していたため、意図せず機密情報が含まれるファイルが誰でもアクセスできるようになっており、その多くは検索エンジンから特定のキーワードで検索することにより、アカウント情報を含む機密情報が公開状態にあることを容易に知ることができたというものであった。

(c) Web サイト運営者に求められる対策

前述のとおり、「ファイルの誤った公開」の届出では、「ウェブアプリケーションソフト」の仕様を確認しないまま利用していたため、非公開にすべきファイルが公開されているという届出が多数を占めていた。

まず、Web サイト運営者は「ウェブアプリケーションソフト」の現状の設定を確認していただきたい。併せて、IPA が公開している「安全なウェブサイトの運用管理に向けての 20 ヶ条[※207]」や「Web サーバからのファイル流出対策[※208]」等を参考にして、非公開にすべきファイルが公開されていないか、設定やファイルの配置場所等を見直すことも必要である。

なお、Web サイト運営者が自組織で確認できない場合は、セキュリティベンダに脆弱性診断を依頼する等の対応が考えられる。

問題を確認した場合は、公開しているファイルを速やかに非公開設定にする。加えて、漏えいが疑われる情報は、検索エンジンでキャッシュされている場合があるため、各検索エンジンを運営する事業者へ問題となったページやファイルのキャッシュ情報の削除を依頼する等の対応を検討いただきたい。

また、クロスサイト・スクリプティングや SQL インジェクション等の脆弱性についても、未だに多くの届出がある。Web サイト運営者は、ページの新規追加や変更を行う際に、IPA が公開している「ウェブ健康診断仕様[※150]」「安全なウェブサイトの作り方[※151]」等を参照して、運営する Web サイトの現状を確認し、対策や見直しを検討いただきたい。

COLUMN

多様化する「だまし」の手口に対抗するには

IPAの「情報セキュリティ安心相談窓口」には日々様々な相談が寄せられています。中でも、「偽サイトや不審サイトにアクセスして、大事な情報をサイトに入力した」「不審なアプリをサイトからインストールした」という相談が多く寄せられています。

そのような偽サイトや不審サイトへの誘導方法としては、メールやSMSを不特定多数にばらまく手法が従来の代表的な手口です。しかし、最近では、それ以外の方法により偽サイトや不審サイトへ誘導する手口の相談も増えており、「だまし」の手口が多様化しているといえる状況です。例えば、「スマートフォンのカレンダー機能」「SNSのメッセージ機能」「ブラウザの通知機能」等を悪用して、ユーザが利用する端末に不審なURLを送り付ける手口も確認しています。これらのどの手口においても、基本的にはURLリンクをタップ／クリックすることで被害につながります。URLをタップ／クリックさえしなければ被害につながることはありません（図1）。

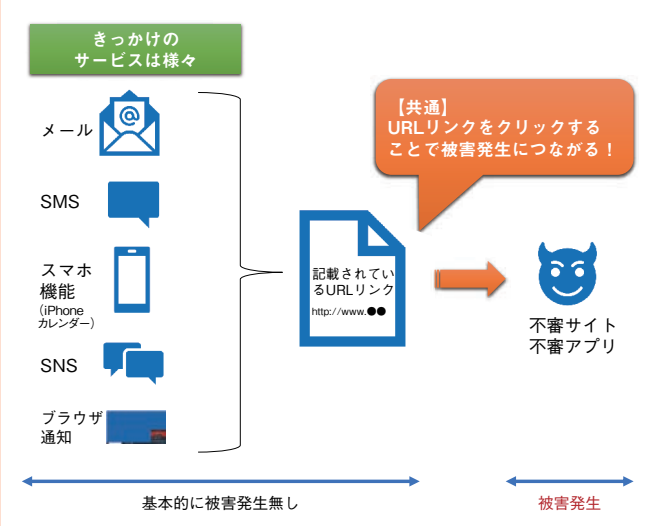


図1　URLリンクからの被害発生のイメージ

これらの手口があることを知っていれば、実際にそのような場面に遭遇しても、怪しいことに気が付き、被害の発生を防げる可能性が高まります。そのため情報セキュリティ安心相談窓口では、以下の情報発信を行っています。

- 「Twitter安心相談窓口公式アカウント」（https://twitter.com/IPA_anshin）では新たな手口が確認された場合に速やかに情報を提供しています。
- 「安心相談窓口だより」（https://www.ipa.go.jp/security/anshin/mgdayoriindex.html）では確認された手口と対処、被害に遭わないための対策等を分かりやすく詳細に説明しています。

「だまし」の手口に引っかからないように、「Twitter公式アカウント」をフォローして、「安心相談窓口だより」を定期的にチェックしてください。

※ 1　https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf〔2022/5/17 確認〕
※ 2　https://apwg.org/trendsreports/〔2022/5/17 確認〕
※ 3　https://www.verizon.com/business/resources/reports/dbir/〔2022/5/27 確認〕
※ 4　https://www.ibm.com/security/jp-ja/data-breach/threat-intelligence/〔2022/5/17 確認〕
※ 5　CNN.co.jp：米首都のガソリンスタンド、8割が売り切れ　パイプライン停止の影響続く　https://www.cnn.co.jp/business/35170841.html〔2022/5/17 確認〕
※ 6　Microsoft 社：Microsoft Exchange Server のリモートでコードが実行される脆弱性 CVE-2021-26855　https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26855〔2022/5/17 確認〕
※ 7　Microsoft 社：Microsoft Exchange Server のリモートでコードが実行される脆弱性 CVE-2021-34473　https://msrc.microsoft.com/update-guide/ja-jp/vulnerability/CVE-2021-34473〔2022/5/17 確認〕
NIST：CVE-2021-34523 Detail　https://nvd.nist.gov/vuln/detail/CVE-2021-34523〔2022/5/17 確認〕
NIST：CVE-2021-31207 Detail　https://nvd.nist.gov/vuln/detail/CVE-2021-31207〔2022/5/17 確認〕
※ 8　Orange Tsai：ProxyLogon is Just the Tip of the Iceberg, A New Attack Surface on Microsoft Exchange Server!　https://i.blackhat.com/USA21/Wednesday-Handouts/us-21-ProxyLogon-Is-Just-The-Tip-Of-The-Iceberg-A-New-Attack-Surface-On-Microsoft-Exchange-Server.pdf〔2022/5/17 確認〕
※ 9　JVN iPedia：JVNDB-2021-005429 Apache Log4j における任意のコードが実行可能な脆弱性　https://jvndb.jvn.jp/ja/contents/2021/JVNDB-2021-005429.html〔2022/5/17 確認〕
※ 10　Solar Winds Worldwide, LLC.：SolarWinds Security Advisory　https://www.solarwinds.com/ja/sa-overview/securityadvisory〔2022/5/17 確認〕
※ 11　Reuters：Kaseya ransomware attack sets off race to hack service providers -researchers　https://www.reuters.com/technology/kaseya-ransomware-attack-sets-off-race-hack-service-providers-researchers-2021-08-03/〔2022/5/17 確認〕
Kaseya Limited：Incident Overview & Technical Details　https://helpdesk.kaseya.com/hc/en-gb/articles/4403584098961-Incident-Overview-Technical-Details〔2022/5/17 確認〕
※ 12　Verizon 社：2021 Data Breach Investigations Report　https://www.verizon.com/business/resources/reports/2021-data-breach-investigations-report.pdf〔2022/5/27 確認〕
なお、本文に記載した 2020 年のインシデント件数である 2 万 9,207 件は、7 万 9,635 件のうちの適格性の基準を満たした件数である。
※ 13　パスワード・スプレー攻撃：同じパスワードを使って複数のアカウントへのログインを試みる攻撃手法。ログイン制御が施されているシステムに対して、同じアカウントへの複数回のログイン試行を回避できる。
※ 14　IBM 社：X-Force 脅威インテリジェンス・インデックス 2021 エグゼクティブ・サマリー　https://www.ibm.com/downloads/cas/98Z6YYG6〔2022/5/17 確認〕
※ 15　FBI：Internet Crime Report 2020　https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf〔2022/5/17 確認〕
※ 16　「マルウェア」等の用語を混在して使用すると、読者を混乱させる可能性があるため、本白書では特に断りのない限り、または文献引用上の正確性を期す必要のない限り、総称して「ウイルス」と表現する。
※ 17　MBSD 社のご厚意により、ご提供いただいた集計情報を本白書では掲載している。
※ 18　https://www.jpcert.or.jp/ir/report.html〔2022/5/16 確認〕
※ 19　フィッシング対策協議会：月次報告書 一覧　https://www.antiphishing.jp/report/monthly/〔2022/5/16 確認〕
※ 20-1　https://www.npa.go.jp/publications/statistics/cybersecurity/data/R03_cyber_jousei.pdf〔2022/5/16 確認〕
※ 20-2「情報セキュリティ白書 2021」（https://www.ipa.go.jp/security/publications/hakusyo/2021.html〔2022/5/16 確認〕）の「1.1.2 (3) フィッシングによる被害」(p.13) 参照。
※ 20-3　JC3：フィッシングターゲットの変遷　https://www.jc3.or.jp/threats/topics/article-430.html〔2022/5/16 確認〕
※ 20-4　トレンドマイクロ社：2021 年年間セキュリティラウンドアップ　https://resources.trendmicro.com/jp-docdownload-form-m449-web-2021-annualsecurityreport.html〔2022/5/16 確認〕
※ 21　https://www.ipa.go.jp/security/event/2013/isec-semi/documents/2013videosemi_targeted_cyber_attacks_v1.pdf〔2022/4/18 確認〕
※ 22　ファイルレスマルウェア：ウイルス本体をディスクドライブ上に直接格納せず、悪意あるコードを PowerShell 等のツールに読み込ませることで、メモリ上で実行・動作するタイプのウイルスのこと。
※ 23　ITmedia NEWS：ベラルーシのハクティビスト、ロシア軍阻止目的で国鉄にランサムウェア攻撃と声明　https://www.itmedia.co.jp/news/articles/2201/25/news080.html〔2022/4/18 確認〕
※ 24　JPCERT/CC：JPCERT/CC インシデント報告対応レポート〔2021 年 7 月 1 日～ 2021 年 9 月 30 日〕　https://www.jpcert.or.jp/pr/2021/IR_Report20211014.pdf〔2022/4/18 確認〕
※ 25　JPCERT/CC：短縮 URL から VBScript をダウンロードさせるショートカットファイルを用いた攻撃　https://blogs.jpcert.or.jp/ja/2019/07/shorten_url_lnk.html〔2022/4/18 確認〕
※ 26　NTT セキュリティ株式会社：標的型攻撃グループ CryptoMimic の攻撃手法の変化について　https://insight-jp.nttsecurity.com/post/102gpur/cryptomimic〔2022/4/18 確認〕
※ 27　三菱電機株式会社：不正アクセスによる個人情報と企業機密の流出可能性について　https://www.mitsubishielectric.co.jp/news/2020/0120-b.pdf〔2022/4/18 確認〕
※ 28　三菱電機株式会社：不正アクセスによる個人情報と企業機密の流出可能性について（第 3 報）　http://www.mitsubishielectric.co.jp/news/2020/0212-b.pdf〔2022/4/18 確認〕
※ 29　防衛省：三菱電機株式会社に対する不正アクセスによる安全保障上の影響に関する調査結果について　https://www.mod.go.jp/j/press/news/2021/12/24c.pdf〔2022/4/18 確認〕
※ 30　三菱電機株式会社：不正アクセスによる個人情報と企業機密の流出可能性について（第 4 報）　http://www.mitsubishielectric.co.jp/news/2021/1224.pdf〔2022/4/18 確認〕
※ 31　https://piyolog.hatenadiary.jp/entry/2020/01/20/172436〔2022/4/18 確認〕
※ 32　報道によると Trend Micro ウイルスバスター法人向け製品の脆弱性を悪用されたとのこと。当時は未公開であったが、2022 年時点では修正パッチが提供されている。
ZDNet：Two Trend Micro zero-days exploited in the wild by hackers　https://www.zdnet.com/article/two-trend-micro-zero-days-exploited-in-the-wild-by-hackers/〔2022/4/18 確認〕
※ 33　TechCrunch：US says Iran-backed hackers are now targeting organizations with ransomware　https://techcrunch.com/2021/11/17/cisa-iran-hackers-ransomware/〔2022/4/18 確認〕
Security Affairs：China-linked APT used Pulse Secure VPN zero-day to hack US defense contractors　https://securityaffairs.co/wordpress/117060/apt/pulse-secure-vpn-zeroday-attacks.html〔2022/4/18 確認〕
※ 34　IPA：情報セキュリティ白書 2021　https://www.ipa.go.jp/security/publications/hakusyo/2021.html〔2022/4/18 確認〕
※ 35　Cybersecurity and Infrastructure Security Agency（CISA）：FBI-CISA Joint Advisory on Exploitation of Fortinet FortiOS Vulnerabilities　https://www.cisa.gov/uscert/ncas/current-activity/2021/04/02/fbi-cisa-joint-advisory-exploitation-fortinet-fortios〔2022/4/18 確認〕
※ 36　IPA：IPA 脆弱性対策コンテンツリファレンス　https://www.ipa.go.jp/files/000051352.pdf〔2022/4/18 確認〕
※ 37　INTERNET Watch：カスペルスキー、マルウェア「LODEINFO」の亜種が観測されたと発表　https://internet.watch.impress.co.jp/docs/news/1374019.html〔2022/4/18 確認〕
※ 38　シスコシステムズ合同会社：侵害された Web サイトを使用した新しいキャンペーンで ObliqueRAT が復活　https://gblogs.cisco.com/jp/2021/03/talos-obliquerat-new-campaign/〔2022/4/18 確認〕
※ 39　一般社団法人日本コンピュータセキュリティインシデント対応チーム協議会：What's CSIRT？　https://www.nca.gr.jp/imgs/CSIRT.pdf〔2022/4/18 確認〕
※ 40　IPA：【注意喚起】事業継続を脅かす新たなランサムウェア攻撃について　https://www.ipa.go.jp/security/announce/2020-ransom.html〔2022/4/18 確認〕
※ 41　株式会社 FFRI セキュリティ：標的型ランサムウェアの脅威　https://www.ffri.jp/blog/2020/06/2020-06-29-Targeted-ransomware-threat.htm〔2022/4/18 確認〕
※ 42　株式会社カスペルスキー：ランサムウェアを操る脅迫犯、盗んだデータを公開　https://blog.kaspersky.co.jp/ransomware-data-disclosure/26862/〔2022/4/18 確認〕
※ 43　NISC：ランサムウエアによるサイバー攻撃について【注意喚起】　https://www.nisc.go.jp/pdf/policy/infra/ransomware20201126.pdf〔2022/4/18 確認〕
※ 44　警察庁：令和3年におけるサイバー空間をめぐる脅威の情勢等について　https://www.npa.go.jp/publications/statistics/cybersecurity/data/R03_cyber_jousei.pdf〔2022/4/18 確認〕
※ 45　日本経済新聞：ハッカーに狙われたトヨタの部品　小島プレスがなぜ　https://www.nikkei.com/article/DGXZQOUC0319Y0T00C22

A3000000/〔2022/4/18 確認〕
※ 46 トレンドマイクロ社：闇市場とサイバー犯罪：「RaaS」ランサムウェアのサービス化 https://blog.trendmicro.co.jp/archives/17416〔2022/4/18 確認〕
※ 47 トレンドマイクロ社：ランサムウェア「Cring」の被害が国内で拡大、VPN 脆弱性を狙い侵入 https://blog.trendmicro.co.jp/archives/27830〔2022/4/18 確認〕
※ 48 ESET：ESET サイバーセキュリティ脅威レポート 2021 年第 2 三半期版を公開 ～侵入口として悪用される RDP/ オリンピック期間中の動向も～ https://www.eset.com/jp/blog/threat-report/2021-t2/〔2022/4/18 確認〕
※ 49 NHK：病院がサイバー攻撃を受けたとき 消えた電子カルテの衝撃 https://www3.nhk.or.jp/news/special/sci_cul/2021/11/special/story_20211119〔2022/4/18 確認〕
MBS：サイバー攻撃と戦った公立病院の 2 か月間『電子カルテが暗号化』過去の検査結果も病歴もわからず ... 手書き対応にも苦労 https://www.mbs.jp/4chantv/news/kodawari/article/2022/01/087200.shtml〔2022/4/18 確認〕
MBS：【特集】サイバー攻撃と戦った公立病院の2か月間『電子カルテが暗号化』過去の検査結果も病歴もわからず ... 手書き対応にも苦労（2021 年 1 月 6 日） https://www.youtube.com/watch?v=eb8RLIlaBn4〔2022/4/18 確認〕
MBSD：ランサムウェア「LockBit2.0」の内部構造を紐解く https://www.mbsd.jp/research/20211019/blog/〔2022/4/18 確認〕
日本経済新聞：身代金払わず 2 億円で新システム 徳島サイバー被害病院 https://www.nikkei.com/article/DGXZQOUE25C3L0V21C21A1000000/〔2022/4/18 確認〕
※ 50 株式会社ニップン：ウィルス攻撃感染被害によるシステム障害発生のお知らせ https://www.nippn.co.jp/topics/detail/__icsFiles/afieldfile/2021/07/09/20210709system.pdf〔2022/4/18 確認〕
株式会社ニップン：システム障害発生のお知らせ（続報） https://www.nippn.co.jp/topics/detail/__icsFiles/afieldfile/2021/08/16/20210816.pdf〔2022/4/18 確認〕
株式会社ニップン：2022 年 3 月期第 1 四半期報告書の提出期限延長に関する承認申請書提出のお知らせ https://www.nikkei.com/nkd/disclosure/tdnr/d2a0bf/〔2022/4/18 確認〕
ITmedia NEWS：ニップン、前例ないサイバー攻撃で延期した 1Q 決算は増収増益に 影響は「引き続き調査中」 https://www.itmedia.co.jp/news/articles/2110/29/news202.html〔2022/4/18 確認〕
ITmedia NEWS：日本の製粉大手に「前例ない」大規模攻撃 大量データ暗号化 起動不能、バックアップもダメで「復旧困難」 https://www.itmedia.co.jp/news/articles/2108/17/news121.html〔2022/4/18 確認〕
※ 51 NTT Com DD 株式会社：予測不能に進化し続けるネットワークの脅威 – 最近のランサムウェアとマルウェアはどんなもの? https://nttcdd.jp/blog/2107/〔2022/4/18 確認〕
※ 52 トレンドマイクロ社：ランサムウェア攻撃後に予期される身代金交渉の実状を解説 https://blog.trendmicro.co.jp/archives/30035〔2022/4/18 確認〕
※ 53 Avast Software s.r.o.：Magnitude Exploit Kit: Still Alive and Kicking https://decoded.avast.io/janvojtesek/magnitude-exploit-kit-still-alive-and-kicking/〔2022/4/18 確認〕
※ 54 Gigazine：ランサムウェア入り USB メモリを送りつける詐欺が増加中、データを暗号化して使用不能にし元に戻すための身代金を要求する手口 https://gigazine.net/news/20220111-cyber-criminals-mailing-usb-drives-ransomware/〔2022/4/18 確認〕
※ 55 IRM：業務で使用する文書ファイル等を暗号化し、閲覧や編集等を制限する仕組み。
※ 56 JPCERT/CC：インシデントハンドリングマニュアル https://www.jpcert.or.jp/csirt_material/files/manual_ver1.0_20211130.pdf〔2022/4/18 確認〕
※ 57 JPCERT/CC：CSIRT：侵入型ランサムウェア攻撃を受けたら読む FAQ https://www.jpcert.or.jp/magazine/security/ransom-faq.html〔2022/4/18 確認〕
※ 58 被害金額については、2015 ～ 2021 年の年次報告書（IC3：Annual Reports https://www.ic3.gov/Home/AnnualReports〔2022/4/18 確認〕）を参照した。
※ 59 トレンドマイクロ社：電子メールサービスの特性を悪用する様々なビジネスメール詐欺の手口を解説 https://blog.trendmicro.co.jp/archives/29272〔2022/4/18 確認〕
日本経済新聞：ビジネスメール詐欺が急増、トレンドマイクロ調べ https://www.nikkei.com/article/DGXZQOUC09CGM0Z01C21A2000000/〔2022/4/18 確認〕
※ 60 APWG：Phishing Activity Trends Reports 2nd Quarter 2021 https://docs.apwg.org/reports/apwg_trends_report_q2_2021.pdf〔2022/4/18 確認〕
※ 61 INTERPOL：More than 1,000 arrests and USD 27 million intercepted in massive financial crime crackdown https://www.interpol.int/News-and-Events/News/2021/More-than-1-000-arrests-and-USD-27-million-intercepted-in-massive-financial-crime-crackdown〔2022/4/18 確認〕
※ 62 INTERPOL：Nigerian cybercrime fraud: 11 suspects arrested, syndicate busted https://www.interpol.int/News-and-Events/News/2022/Nigerian-cybercrime-fraud-11-suspects-arrested-syndicate-busted〔2022/4/18 確認〕
※ 63 The Record：US arrests 33 BEC scammers linked to Nigerian crime syndicate https://therecord.media/us-arrests-33-bec-scammers-linked-to-nigerian-crime-syndicate/〔2022/4/18 確認〕
※ 64 Europol：106 arrested in a sting against online fraudsters https://www.europol.europa.eu/newsroom/news/106-arrested-in-sting-against-online-fraudsters〔2022/4/18 確認〕
※ 65 株式会社ビジョナリーホールディングス：当社子会社における資金流出事案の発生並びに特別損失の計上に関するお知らせ https://ssl4.eir-parts.net/doc/9263/tdnet/2092784/00.pdf〔2022/5/19 確認〕
※ 66 加賀電子株式会社：当社米国子会社における資金流出事案について https://www.taxan.co.jp/jp/ir/upload_file/tdnrelease/8154_20210319481006_P01_.pdf〔2022/4/18 確認〕
※ 67 dongA.com：KAI, 해커 일당에 16 억원 '피싱사기' 당해… "후속 조치 협조" https://www.donga.com/news/Society/article/all/20210618/107504131/1/〔2022/4/18 確認〕
※ 68 KNUJ Radio：City of Redwood Falls victim of bank wire scam over fire truck; funds recovered https://knuj.net/2021/06/19/city-of-redwood-falls-victim-of-bank-wire-scam-over-fire-truck-funds-recovered/〔2022/4/18 確認〕
※ 69 https://www.ipa.go.jp/files/000090633.pdf〔2022/4/18 確認〕
※ 70 https://www.ipa.go.jp/files/000092808.pdf〔2022/4/18 確認〕
※ 71 https://www.ipa.go.jp/files/000094117.pdf〔2022/4/18 確認〕
※ 72 https://www.ipa.go.jp/files/000095766.pdf〔2022/4/18 確認〕
※ 73 IPA：ビジネスメール詐欺「BEC」に関する事例と注意喚起 https://www.ipa.go.jp/files/000058478.pdf〔2022/4/18 確認〕
※ 74 IPA：【注意喚起】偽口座への送金を促す"ビジネスメール詐欺"の手口（続報） https://www.ipa.go.jp/security/announce/201808-bec.html〔2022/4/18 確認〕
※ 75 Agari：Cosmic Lynx: A Russian Threat Hits the BEC Scene https://www.agari.com/email-security-blog/cosmic-lynx-russian-bec/〔2022/4/18 確認〕
※ 76 JPCERT/CC：ビジネスメール詐欺の実態調査報告 https://www.jpcert.or.jp/research/BEC-survey.html〔2022/4/18 確認〕
株式会社マクニカ：ビジネスメール詐欺の実態と対策アプローチ 第 1 版 https://www.macnica.net/security/report_02.html〔2022/4/18 確認〕
PwC：Business-Email-Compromise-Guide https://github.com/PwC-IR/Business-Email-Compromise-Guide/blob/main/PwC-Business_Email_Compromise-Guide.pdf〔2022/4/18 確認〕
※ 77 Microsoft 社：侵害された電子メールアカウントへの対応 https://docs.microsoft.com/ja-jp/microsoft-365/security/office-365-security/responding-to-a-compromised-email-account?view=o365-worldwide〔2022/4/18 確認〕
Microsoft 社：アカウントが侵害されたかどうかを Office 365 する方法 https://docs.microsoft.com/ja-jp/office365/troubleshoot/sign-in/determine-account-is-compromised〔2022/4/18 確認〕
FireEye：Obscured by Clouds：Office 365 攻撃の洞察と Mandiant Managed Defense の調査方法 https://www.fireeye.com/blog/jp-threat-research/2020/07/insights-into-office-365-attacks-and-how-managed-defense-investigates.html〔2022/4/18 確認〕
Google LLC：ハッキングまたは不正使用された Google アカウントを保護する https://support.google.com/accounts/answer/6294825?hl=ja〔2022/4/18 確認〕
※ 78 NetScout Systems, Inc.：ISSUE 7: FINDINGS FROM 1H 2021 NETSCOUT THREAT INTELLIGENCE REPORT https://www.netscout.com/sites/default/files/2021-10/SECIG_015_EN-2101-Threat_Report_SP_Infographic.pdf〔2022/4/18 確認〕
※ 79 株式会社カスペルスキー：＜Kaspersky サイバー脅威調査：2020 年第 2 四半期の DDoS 攻撃＞新型コロナウイルスの流行下、DDoS 攻撃数は前年同期比の 3 倍に。人々の外出機会の減少が影響 https://www.kaspersky.co.jp/about/press-releases/2020_vir18092020〔2022/4/18 確認〕
※ 80 UDP（User Datagram Protocol）：インターネットで標準的に使われているプロトコルの一種。接続のチェックが不要なコネクションレスなサービスに利用される。

※ 81 Microsoft 社：Azure DDoS Protection—2021 Q3 and Q4 DDoS attack trends https://azure.microsoft.com/en-us/blog/azure-ddos-protection-2021-q3-and-q4-ddos-attack-trends/〔2022/4/18 確認〕
※ 82 CDN（Content Delivery Network）：Web コンテンツを配信するために最適化されたネットワーク。オリジナルの Web コンテンツを格納するサーバである「オリジンサーバ」、代理で Web コンテンツを配信する「キャッシュサーバ」などから構成される。
※ 83 INTERNET Watch：オリンピック開始後、DDoS 攻撃が 10 倍超に増加。Cloudflare がトラフィック動向を発表 https://internet.watch.impress.co.jp/docs/news/1341736.html〔2022/4/18 確認〕
※ 84 GIGAZINE:史上最大規模の DDoS 攻撃を行う「Mēris ボットネット」が出現 https://gigazine.net/news/20210910-meris-botnet/〔2022/4/18 確認〕
※ 85 Mirai：IoT 機器に感染してボットネットを構成し、サイバー攻撃に悪用するウイルス。2016 年に史上最大規模の DDoS 攻撃を引き起こした。ソースコードが公開されていたため、様々な亜種が出現している。
※ 86 Cloudflare, Inc.：Cloudflare が 1720 万 RPS（記録上最大規模）の DDoS 攻撃を防御 https://blog.cloudflare.com/ja-jp/cloudflare-thwarts-17-2m-rps-ddos-attack-the-largest-ever-reported-ja-jp/〔2022/4/18 確認〕
※ 87 トレンドマイクロ社：2021 年年間セキュリティラウンドアップ https://resources.trendmicro.com/jp-docdownload-form-m449-web-2021-annualsecurityreport.html〔2022/4/19 確認〕
※ 88 SQL インジェクション：SQL 文の組み立てにおいて、利用者からの入力情報を基に細工された SQL 文を埋め込まれると、データベースを不正に操作されてしまう脆弱性。
※ 89 SonicWall, Inc.：CONFIRMED ZERO-DAY VULNERABILITY IN THE SONICWALL SMA100 BUILD VERSION 10.X https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0001〔2022/4/19 確認〕
※ 90 FBI：CU-000154-MW: Fivehands-HelloKitty FLASH Cord Final (002) https://www.ic3.gov/Media/News/2021/211029.pdf〔2022/4/19 確認〕
※ 91 Pulse Secure, LLC.：SA44784 - 2021-04: Out-of-Cycle Advisory: Multiple Vulnerabilities Resolved in Pulse Connect Secure 9.1R11.4 https://kb.pulsesecure.net/articles/Pulse_Secure_Article/SA44784/〔2022/4/19 確認〕
※ 92 JPCERT/CC：Pulse Connect Secure の脆弱性（CVE-2021-22893）に関する注意喚起 https://www.jpcert.or.jp/at/2021/at210019.html〔2022/4/19 確認〕
※ 93 Web シェル：Web サーバに不正にアップロードされるバックドアプログラム。
※ 94 Palo Alto Networks, Inc.：ランサムウェアギャング REvil：Kaseya VSA 攻撃の背後にいる攻撃グループを理解する https://unit42.paloaltonetworks.jp/revil-threat-actors/〔2022/4/19 確認〕
※ 95 Microsoft 社：Microsoft Exchange Server Vulnerabilities Mitigations – updated March 15, 2021 https://msrc-blog.microsoft.com/2021/03/05/microsoft-exchange-server-vulnerabilities-mitigations-march-2021/〔2022/4/19 確認〕
※ 96 Microsoft 社：April 2021 Update Tuesday packages now available https://msrc-blog.microsoft.com/2021/04/13/april-2021-update-tuesday-packages-now-available/〔2022/4/19 確認〕
※ 97 Volexity：Operation Exchange Marauder: Active Exploitation of Multiple Zero-Day Microsoft Exchange Vulnerabilities https://www.volexity.com/blog/2021/03/02/active-exploitation-of-microsoft-exchange-zero-day-vulnerabilities/〔2022/4/19 確認〕
※ 98 ゼロデイ：脆弱性が発見・報告された日から、その脆弱性を解消するための手段が確立するまでの期間のこと。
※ 99 Forescout Technologies, Inc.：NAME:WRECK https://www.forescout.com/research-labs/namewreck/〔2022/4/19 確認〕
※ 100 TCP/IP スタック：IoT 機器のファームウェア等に追加されるネットワーク機能を提供するためのライブラリ。
※ 101 Forescout Technologies, Inc.：NAME:WRECK: Breaking and fixing DNS implementations https://www.forescout.com/resources/namewreck-breaking-and-fixing-dns-implementations/〔2022/4/19 確認〕
※ 102 https://jvndb.jvn.jp/〔2022/4/19 確認〕
※ 103 IPA：【注意喚起】特定の組織からの注文連絡等を装ったばらまき型メールに注意 https://www.ipa.go.jp/security/topics/alert271009.html〔2022/4/18 確認〕
※ 104 Europol：World's most dangerous malware EMOTET disrupted through global action https://www.europol.europa.eu/media-press/newsroom/news/world's-most-dangerous-malware-emotet-disrupted-through-global-action〔2022/4/18 確認〕
※ 105 IPA：「Emotet（エモテット）」と呼ばれるウイルスへの感染を狙うメールについて https://www.ipa.go.jp/security/announce/20191202.html〔2022/4/18 確認〕
JPCERT/CC：マルウェア Emotet の感染再拡大に関する注意喚起 https://www.jpcert.or.jp/at/2022/at220006.html〔2022/4/18 確認〕
※ 106 IPA：サイバー情報共有イニシアティブ（J-CSIP）運用状況［2018 年 10 月～ 12 月］ https://www.ipa.go.jp/files/000071273.pdf〔2022/4/18 確認〕
※ 107 JPCERT/CC：マルウエア Emotet の感染活動について https://www.jpcert.or.jp/newsflash/2019112701.html〔2022/4/18 確認〕
※ 108 https://www.med.or.jp/nichiionline/article/010228.html〔2022/4/18 確認〕
※ 109 Mal-Eats：日本を狙う新たな攻撃キャンペーン Campo の全体像 https://mal-eats.net/2021/05/10/campo_new_attack_campaign_targeting_japan/〔2022/4/18 確認〕
※ 110 IPA：サイバー情報共有イニシアティブ（J-CSIP）運用状況［2021 年 7 月～ 9 月］ https://www.ipa.go.jp/files/000094117.pdf〔2022/4/18 確認〕
デジタルアーツ株式会社：見慣れない XLL ファイル（Excel アドイン）を使う攻撃に要注意! https://www.daj.jp/webtopics/102/〔2022/4/18 確認〕
※ 111 IPA:「Emotet（エモテット）」と呼ばれるウイルスへの感染を狙うメールについて https://www.ipa.go.jp/security/announce/20191202.html〔2022/4/18 確認〕
※ 112 BleepingComputer：Microsoft fixes Windows AppX Installer zero-day used by Emotet https://www.bleepingcomputer.com/news/Microsoft/Microsoft-fixes-windows-appx-installer-zero-day-used-by-emotet/〔2022/4/18 確認〕
※ 113 IPA：安心相談窓口だより 宅配便業者に加えて通信事業者をかたる偽ショートメッセージサービス（SMS）が増加中 https://www.ipa.go.jp/security/anshin/mgdayori20211222.html〔2022/4/18 確認〕
※ 114 https://www.jc3.or.jp/threats/examples/article-409.html〔2022/4/18 確認〕
※ 115 IPA：安心相談窓口だより 安易に運転免許証など本人確認書類の写真を送信しないで! https://www.ipa.go.jp/security/anshin/mgdayori20210623.html〔2022/4/18 確認〕
※ 116 NTT ドコモ：フィッシング詐欺を未然に防ぐ「危険 SMS 拒否設定」の提供を開始＜2022 年 1 月 13 日＞ https://www.nttdocomo.co.jp/info/news_release/2022/01/13_00.html〔2022/4/18 確認〕
NTT ドコモ：SMS 拒否設定 https://www.docomo.ne.jp/info/spam_mail/sms/〔2022/4/18 確認〕
※ 117 KDDI 株式会社：迷惑メッセージブロック機能を au・UQ mobile・povo 向けに提供 https://news.kddi.com/kddi/corporate/newsrelease/2022/03/16/5928.html〔2022/4/18 確認〕
※ 118 ソフトバンク株式会社：迷惑 SMS 対策機能を提供開始 https://www.softbank.jp/corp/news/press/sbkk/2022/20220113_02/〔2022/4/18 確認〕
※ 119 厚生労働省：新型コロナウイルスワクチンの接種の実施について https://www.mhlw.go.jp/stf/newpage_16799.html〔2022/4/18 確認〕
※ 120 IPA（情報セキュリティ安心相談窓口 Twitter アカウント）：https://twitter.com/IPA_anshin/status/1432190641866358784〔2022/4/18 確認〕
※ 121 厚生労働省：新型コロナウイルスを題材とした攻撃メールについて https://www.mhlw.go.jp/stf/newpage_09393.html〔2022/4/18 確認〕
※ 122 厚生労働省：新型コロナワクチン接種の予約を案内する怪しいメールに注意!ー国がコロナワクチン接種に関連して金銭やクレジットカード番号を求めることはありませんー https://www.kokusen.go.jp/news/data/n-20210902_7.html〔2022/4/18 確認〕
※ 123 https://www.antiphishing.jp/news/alert/kyufukin_20210824.html〔2022/4/18 確認〕
※ 124 総務省：特別定額給付金の給付を騙ったメールに対する注意喚起 https://www.soumu.go.jp/menu_kyotsuu/important/kinkyu02_000438.html〔2022/4/18 確認〕
※ 125 IPA：安心相談窓口だより 偽のセキュリティ警告に表示された番号に電話をかけないで! https://www.ipa.go.jp/security/anshin/mgdayori20211116.html〔2022/4/18 確認〕
※ 126 朝日新聞：PC 画面に「ウイルス感染」偽の警告…「サポート詐欺」容疑で初逮捕 https://www.asahi.com/articles/ASQ1L3G76Q1LUTIL001.html〔2022/4/18 確認〕
※ 127 独立行政法人国民生活センター：全国の消費生活センター等 http://www.kokusen.go.jp/map/〔2022/4/18 確認〕
※ 128 Microsoft 社：テクニカル サポート詐欺から身を守る https://support.microsoft.com/ja-jp/windows/ テクニカル - サポート詐欺から身

を守る -2ebf91bd-f94c-2a8a-e541-f5c800d18435〔2022/4/18 確認〕
※ 129 自動継続課金：ここでは「一定の利用期間ごとに定額を支払う料金方式、かつ、利用契約が自動更新される方式」を指す。なお、「一定の利用期間ごとに定額を支払う料金方式」は、Android では「定期購入」、iPhone では「サブスクリプション」と呼ばれる。
※ 130 IPA：安心相談窓口だより　ブラウザの通知機能から不審サイトに誘導する手口に注意　https://www.ipa.go.jp/security/anshin/mgdayori20210309.html〔2022/4/18 確認〕
※ 131 ブラウザの通知機能：ウェブサイトからブラウザを通じて画面上に配信されるプッシュ型の通知サービス。2021 年 3 月 9 日現在、iOS 端末（iPhone、iPad 等）にはブラウザ通知機能は搭載されていない。
※ 132 reCAPTCHAv2：reCAPTCHA とは、アクセスしているのが機械でなく人間であることの判別をするための認証機能。reCAPTCHA v2 は Google が提供する CAPTCHA（キャプチャ）認証システムの名称。
※ 133 https://www.mcafee.com/ja-jp/consumer-support/help/support/block-fake-alert.html〔2022/4/18 確認〕
※ 134 https://www.mcafee.com/ja-jp/consumer-support/help/common-faq.html?culture=ja-jp&id=commonFAQ〔2022/4/18 確認〕「間違って購入してしまいました。払い戻しの方法を教えてください。」を参照。
※ 135 東京商工リサーチ社：上場企業の個人情報漏えい・紛失事故は、調査開始以来最多の 137 件 574 万人分（2021 年）　https://www.tsr-net.co.jp/news/analysis/20210117_01.html〔2022/4/20 確認〕
※ 136 東京商工リサーチ社：「上場企業の個人情報漏えい・紛失事故」調査（2020 年）　https://www.tsr-net.co.jp/news/analysis/20210115_01.html〔2022/4/20 確認〕
※ 137 株式会社ネットマーケティング：不正アクセスによる会員様情報流出の調査結果と今後の対応について　https://www.net-marketing.co.jp/news/6001/〔2022/4/20 確認〕
※ 138-1 森永製菓株式会社：不正アクセス発生による個人情報流出の可能性のお知らせとお詫び　https://www.morinaga.co.jp/company/newsrelease/detail.php?no=2178〔2022/4/20 確認〕
※ 138-2 弊社公式オンラインショップへの不正アクセスによる個人情報流出に関するお詫びとご報告　https://biz.right-on.co.jp/news/topics/1104-2.php〔2022/5/19 確認〕
※ 139 株式会社リニカル：不正アクセスに伴う原因究明のためのサーバーの一時停止措置に関するお詫びとご報告　https://www.linical.co.jp/news/7ca5d9e93f2674a92830d2dec379d16d1d67f170.pdf〔2022/4/20 確認〕
株式会社リニカル：不正アクセスによる個人情報等流出の可能性に関するお知らせとお詫び　https://www.linical.co.jp/news/17705e29046d75409e91d377bb1410558f8e6e21.pdf〔2022/4/20 確認〕
※ 140 株式会社ユピテル：My Yupiteru 会員様情報の一部流出のお詫びとお知らせ　https://www.yupiteru.co.jp/corp/important/210607.html〔2022/4/20 確認〕
※ 141 株式会社メタップスペイメント：不正アクセスによる情報流出に関するご報告とお詫び　https://www.metaps-payment.com/company/20220228.html〔2022/4/20 確認〕
※ 142 コンディショニングジム GOING：【重要】会費ペイによるクレジット決済停止のお知らせ　https://www.facebook.com/cggoing/posts/3237118433079143〔2022/5/19 確認〕
子どもの発達支援を考える ST の会：「会費徴収システムの情報漏洩に関するご報告」　https://www.kodomost.jp/announce/kaihipay.pdf〔2022/4/20 確認〕
一般社団法人日本機械学会：イベントペイ　クレジットカード不正利用疑いと決済機能の一時停止について　https://www.jsme.or.jp/20211227-2/〔2022/4/20 確認〕
NSフィットネス：【お詫び】WEB 入会時にクレジットカード決済が出来ない件について　https://ns-fit-fukusaki.com/news/【お詫び】WEB 入会時にクレジットカード決済が出 /〔2022/4/20 確認〕
一般社団法人日本集中治療医学会：イベントペイ　クレジットカード不正利用疑いと決済機能の一時停止について　https://www.jsicm.org/news/news211228.html〔2022/4/20 確認〕
有限会社アップリンク：【重要なお知らせ】オンラインチケット一部販売再開のお知らせ　https://joji.uplink.co.jp/news/2022/13116〔2022/4/20 確認〕
※ 143 株式会社日能研：不正アクセスによるメールアドレス流出の可能性に関するお詫びとお知らせ　https://www.nichinoken.co.jp/info/owabi/220129.html〔2022/4/20 確認〕
※ 144 ロゴヴィスタ株式会社：弊社ホームページへの不正アクセスによる被害発生のお詫びとお知らせ　https://www.logovista.co.jp/Iverp/information/information/emergency.html〔2022/4/20 確認〕
※ 145 株式会社石橋楽器店：株式会社石橋楽器店への不正アクセスによる情報流出の可能性に関するお詫びとお知らせ　https://www.ishibashi.co.jp/company/20220111.html〔2022/4/20 確認〕
※ 146 ビーズ株式会社：不正アクセスによるメールアドレス流出の可能性に関するお詫びとお知らせ　https://www.be-s.co.jp/notice/4168〔2022/4/20 確認〕
※ 147 株式会社ヨシハラシステムズ：弊社が運営する「せんたく便」への不正アクセスによる個人情報流出に関するお詫びとお知らせ　https://www.sentakubin.co.jp/news/20210405.html〔2022/4/20 確認〕
※ 148 https://www.ipa.go.jp/security/vuln/documents/2008/200805_SQLinjection.html〔2022/4/20 確認〕
※ 149 IPA：【注意喚起】SQL インジェクションをはじめとしたウェブサイトの脆弱性の再点検と速やかな改修を　https://www.ipa.go.jp/security/announce/website_vuln.html〔2022/4/20 確認〕
※ 150 https://www.ipa.go.jp/files/000017319.pdf〔2022/4/20 確認〕
※ 151 https://www.ipa.go.jp/security/vuln/websecurity.html〔2022/4/20 確認〕
※ 152 日本サブウェイ合同会社：サーバー不正アクセスのご報告（2）https://origin.subway.co.jp/upload/press/f28005a86357b259abfe324a355631e7f8f8f1a2.pdf〔2022/4/20 確認〕
日本サブウェイ合同会社：サーバー不正アクセスのご報告（3）　https://www.subway.co.jp/press/year2021/news2582/〔2022/4/20 確認〕
※ 153 ランドブレイン株式会社：弊社サーバーのウイルス感染及び情報流出に関する調査結果のご報告　https://www.landbrains.co.jp/hp/doc/210519.pdf〔2022/4/20 確認〕
※ 154 Security NEXT：不正アクセス被害のランドブレイン、調査結果を公表 - ランサムウェアは「Cring」　https://www.security-next.com/126310〔2022/4/20 確認〕
※ 155 株式会社オリエンタルコンサルタンツホールディングス：ランサムウェア攻撃に関するご報告　https://www.oriconhd.jp/files/information/news20211008_01.pdf〔2022/4/20 確認〕
※ 156 市原市：委託事業者のサーバーへの不正アクセスについて（調査結果のお知らせ）　https://www.city.ichihara.chiba.jp/article?articleId=6170b83e910de2089661fe84〔2022/4/20 確認〕
市川市：本市の業務委託先の業者のサーバーがサイバー攻撃を受けた件について　https://www.city.ichikawa.lg.jp/sys07/0000373622.html〔2022/4/20 確認〕
東京都総務局：委託業務受託者のサーバーに対するサイバー攻撃について　https://www.metro.tokyo.lg.jp/tosei/hodohappyo/press/2021/09/01/01.html〔2022/4/20 確認〕
東京都港湾局：委託業務受託者へのサイバー攻撃について　https://www.metro.tokyo.lg.jp/tosei/hodohappyo/press/2021/09/01/14.html〔2022/4/20 確認〕
東京都建設局：委託業務受託者へのサーバー攻撃について　https://www.metro.tokyo.lg.jp/tosei/hodohappyo/press/2021/09/01/13.html〔2022/4/20 確認〕
東京都都市整備局：委託業務受託者へのサイバー攻撃について　https://www.metro.tokyo.lg.jp/tosei/hodohappyo/press/2021/09/01/15.html〔2022/4/20 確認〕
東京都下水道局：委託業務受託者へのサイバー攻撃について　https://www.metro.tokyo.lg.jp/tosei/hodohappyo/press/2021/09/03/04.html〔2022/4/20 確認〕
東京都水道局：業務受託者へのサイバー攻撃について　https://www.metro.tokyo.lg.jp/tosei/hodohappyo/press/2021/09/03/01.html〔2022/4/20 確認〕
葛飾区：令和 3 年 8 月に発生した本区業務委託事業者へのサイバー攻撃について（令和 4 年 3 月更新）　https://www.city.katsushika.lg.jp/information/kouho/1005542/1026867.html〔2022/4/20 確認〕
埼玉県：本県業務委託事業者へのサイバー攻撃について　https://www.pref.saitama.lg.jp/a1002/news/page/news20210826.html〔2022/4/20 確認〕
群馬県：【9 月 3 日】本県業務委託事業者へのサイバー攻撃について（建設企画課）　https://www.pref.gunma.jp/houdou/h81g_00043.html〔2022/4/20 確認〕
滋賀県：本県業務委託事業者へのサイバー攻撃について　https://www.pref.shiga.lg.jp/kensei/koho/e-shinbun/oshirase/320910.html〔2022/4/20 確認〕
倉敷市：本市の業務委託（依頼）業者が受けたサイバー攻撃に関する調査状況について　https://www.city.kurashiki.okayama.jp/item/142781.htm#itemid142781〔2022/4/20 確認〕
※ 157 株式会社オリエンタルコンサルタンツホールディングス：特別損失の計上及び業績予想の修正に関するお知らせ　https://www.oriconhd.jp/files/information/news20210917_01.pdf〔2022/4/20 確認〕
※ 158 富士通株式会社：プロジェクト情報共有ツールへの不正アクセスについて（第五報）　https://pr.fujitsu.com/jp/news/2022/03/7-1.html〔2022/4/20 確認〕
富士通株式会社：プロジェクト情報共有ツールへの不正アクセスについて（第四報）　https://pr.fujitsu.com/jp/news/2021/12/9-1.html〔2022/

4/20 確認〕
総務省：富士通株式会社が管理・運営するプロジェクト情報共有ツールへの不正アクセスによる情報の流出　https://www.soumu.go.jp/menu_news/s-news/01kanbo05_02000152.html〔2022/4/20 確認〕
国土交通省：富士通株式会社が管理・運営するプロジェクト情報共有ツールへの不正アクセスによる国土交通省関係情報の流出について　https://www.mlit.go.jp/report/press/joho02_hh_000004.html〔2022/4/20 確認〕
外務省：富士通株式会社が管理・運営するプロジェクト情報共有ツールへの不正アクセスによる情報の流出について　https://www.mofa.go.jp/mofaj/press/release/press4_009061.html〔2022/4/20 確認〕
内閣官房内閣サイバーセキュリティセンター：富士通株式会社が管理・運営するプロジェクト情報共有ツールへの不正アクセスによる情報の流出について　https://www.nisc.go.jp/pdf/press/20210602NISC_press.pdf〔2022/4/20 確認〕
NHK：成田空港 運航管理情報システムへの不正アクセス受け注意喚起　https://www3.nhk.or.jp/news/html/20210526/k10013051551000.html〔2022/4/20 確認〕
※ 159 内閣官房内閣サイバーセキュリティセンター：プロジェクト情報共有ツールに対する不正アクセス対策の確認 に関する政府機関等及び重要インフラ事業者等への注意喚起の発出について　https://www.nisc.go.jp/pdf/press/projectist20210525.pdf〔2022/4/20 確認〕
※ 160 株式会社ジーアール：「オムニECシステム」一部サーバーへの不正アクセスについて　https://www.grinc.co.jp/information202109.pdf〔2022/4/20 確認〕
※ 161 株式会社ベイジア：弊社「ベイシアネットショッピング」委託先への不正アクセスによるお客様情報流出に関するお詫びとお知らせ　https://www.beisia.co.jp/wp-content/uploads/2021/10/c9f3e8b196c27d7f25d6e823c664f247.pdf〔2022/4/20 確認〕
サミット株式会社：弊社「サミット予約ネット」委託先への不正アクセスによるお客様情報流出に関するお詫びとお知らせ　https://www.summitstore.co.jp/20210916net.pdf〔2022/4/20 確認〕
株式会社リウボウストア：オンラインショップへの不正アクセスによる個人情報漏えいについて　https://ryubostore.jp/news_detail.html?code=65〔2022/4/20 確認〕
株式会社天満屋ストア：お客様情報の流出の可能性に関するお知らせとお詫び　http://www.tenmaya-store.co.jp/assets/images/sys/2021/09/20210916_2.pdf〔2022/4/20 確認〕
株式会社丸久：お客様情報の流出の可能性に関するお知らせとお詫び　http://www.mrk09.co.jp/ 重要なお知らせ /〔2022/4/20 確認〕
株式会社マルヨシセンター：弊社が使用する「オンライン予約販売システム」への不正アクセスによるお客様情報の流出に関するお詫びとお知らせ　https://ww2.maruyoshi-center.co.jp/upload/news/202109/ 2021年9月16日発信文書② .pdf〔2022/4/20 確認〕
グラントマト株式会社：不正アクセスによる個人情報流出の可能性に関する調査結果のご報告　https://www.grantomato.jp/topics/topics.php?id=687〔2022/4/20 確認〕
株式会社杏林堂薬局：「杏林堂（公式）オンラインショップおよび「店頭予約者情報」への不正アクセスによる お客様情報漏えいに関するお詫びとお知らせ　https://www.kyorindo.co.jp/news/pdf/kyorindo_online_news.pdf〔2022/4/20 確認〕
株式会社芝寿し：弊社「芝寿しオンラインショップ」委託先への不正アクセスによるお客様情報流出に関するお詫びとお知らせ　https://www.online-shibazushi.com/user_data/20211130_oshirase.pdf〔2022/4/20 確認〕
株式会社アヤハディオ：弊社が運営する「アヤハディオネットショッピング」への不正アクセスによるお客様情報漏洩に関するお詫びとお知らせ　https://www.ayahadio.jp/user_data/20211201.pdf〔2022/4/20 確認〕
沓間水産株式会社：弊社が運営する「魚がし鮨お持ち帰り予約サイト」への不正アクセスによるお客様情報流出に関するお詫びとお知らせ　https://www.uogashizushi.co.jp/wp-content/uploads/2021/12/sps03.pdf〔2022/4/20 確認〕
※ 162 https://privacymark.jp/system/reference/pdf/2020JikoHoukoku_211005.pdf〔2022/4/20 確認〕
※ 163 日本年金機構：年金振込通知書の印刷誤りについて　https://www.nenkin.go.jp/oshirase/taisetu/2021/202110/100602.html〔2022/4/20 確認〕
日本年金機構：年金振込通知書（令和３年 10 月定期支払）の再送付について　https://www.nenkin.go.jp/oshirase/taisetu/2021/202110/1013.html〔2022/4/20 確認〕
※ 164 日本年金機構：「年金振込通知書」（令和3年10月定期支払）の印刷誤り事案に係る検証状況報告について　https://www.nenkin.go.jp/oshirase/taisetu/2021/202112/1203.files/1203.pdf〔2022/4/20 確認〕
※ 165 サンメッセ株式会社：特別損失（製品保証引当金繰入額）の計上及び 2022 年3月期第2四半期連結累計期間の業績予想値と実績値との差異に関するお知らせ　https://www.sunmesse.co.jp/ir/news/file/20211104155237.pdf〔2022/4/20 確認〕
※ 166-1 LINE 株式会社：LINE VOOM の公開範囲の設定における不具合のお知らせとお詫び　https://linecorp.com/ja/security/article/400〔2022/4/20 確認〕
※ 166-2 LINE 株式会社：【LINE Pay】一部ユーザーのキャンペーン参加に関わる情報が閲覧できる状態になっていた件のお知らせとお詫び　https://linecorp.com/ja/pr/news/ja/2021/4032〔2022/4/20 確認〕
※ 167 IPA：「企業における営業秘密管理に関する実態調査 2020」報告書について　https://www.ipa.go.jp/security/fy2020/reports/ts_kanri/index.html〔2022/4/20 確認〕
※ 168 株式会社村田製作所：再委託先社員による不適切なデータの取り扱いについてのお知らせとお詫び　https://corporate.murata.com/ja-jp/newsroom/news/company/general/2021/0805〔2022/4/20 確認〕
※ 169 カッパ・クリエイト株式会社：当社役員に対する競合会社からの告訴について　https://www.kappa-create.co.jp/blog/wp-content/uploads/2021/07/ 当社役員に対する競合会社からの告訴について_20210705.pdf〔2022/4/20 確認〕
※ 170 株式会社 And Do ホールディングス：当社子会社の元従業員の不正行為について　https://www.housedo.co.jp/and-do/news/2022/20220118.html〔2022/4/20 確認〕
※ 171 https://www.ipa.go.jp/security/fy24/reports/insider/〔2022/4/20 確認〕
※ 172 日本郵便株式会社、株式会社ゆうちょ銀行：郵便局におけるお客さま情報の紛失（調査結果）　https://www.post.japanpost.jp/notification/pressrelease/2021/00_honsha/1215_02_01.pdf〔2022/4/20 確認〕
※ 173 金沢信用金庫：お客さま情報の紛失について　http://www.shinkin.co.jp/kanazawa/material/top_news/2022.1.28.pdf〔2022/4/20 確認〕
※ 174 トヨタ自動車株式会社：トヨタ販売店におけるお客様の個人情報の不適切な取扱いについて　https://global.toyota/jp/newsroom/corporate/35909023.html〔2022/4/20 確認〕
トヨタ自動車株式会社：トヨタ販売店におけるお客様の個人情報の不適切な取扱いについて　https://global.toyota/jp/newsroom/corporate/36003832.html〔2022/4/20 確認〕
※ 175 株式会社 SUBARU：SUBARU 販売特約店における、お客様情報の不適切な取り扱いについて　https://www.subaru.co.jp/news/2021_10_27_162724/〔2022/4/20 確認〕
※ 176 株式会社新生銀行、新生フィナンシャル株式会社：業務委託先等への提供データに一部のお客さま情報が含まれていたことに関するお詫び　https://www.shinseibank.com/corporate/news/pdf/pdf2021/210927_personal_info_j.pdf〔2022/4/20 確認〕
株式会社新生銀行、新生フィナンシャル株式会社：業務委託先等への提供データに一部のお客さま情報が含まれていたことに関するお詫び(2)　https://www.shinseibank.com/corporate/news/pdf/pdf2021/220127_personal_info_j.pdf〔2022/4/20 確認〕
※ 177 株式会社新生銀行：お客さま情報を誤って提供したことについてのお詫びとご説明　https://www.shinseibank.com/corporate/news/pdf/pdf2021/220127_personal_info_j.pdf〔2022/4/20 確認〕
※ 178 JPCERT/CC、IPA：Japan Vulnerability Notes　https://jvn.jp/〔2022/4/19 確認〕
※ 179 NIST：National Vulnerability Database　https://nvd.nist.gov/〔2022/4/19 確認〕
※ 180 公表年は、ベンダがアドバイザリを公開した年、他組織やセキュリティポータルサイト等の登録／公開した年、発見者が一般向けに報告した年等、脆弱性対策情報が一般に公表された年を指す。なお、JVN iPedia で脆弱性対策情報を公開した年は「登録年」としている。
※ 181 IPA：共通脆弱性識別子 CVE 概説　https://www.ipa.go.jp/security/vuln/CVE.html〔2022/4/19 確認〕
※ 182 The MITRE Corporation:CVE Numbering Authorities（CNA）　https://www.cve.org/ProgramOrganization/CNAs〔2022/4/19 確認〕
※ 183 The MITRE Corporation：米国政府向けの技術支援や研究開発を行う非営利組織。80 を超える主要な脆弱性情報サイトと連携して、脆弱性情報の収集と、重複のない CVE の採番を行っている。
※ 184 The MITRE Corporation：CVE Adds 7 New CVE Numbering Authorities (CNAs)　https://cve.mitre.org/news/archives/2016/news.html〔2022/4/19 確認〕
※ 185 The MITRE Corporation：VulDB Added as CVE Numbering Authority (CNA)　https://www.cve.org/Media/News/item/news/2021/12/21/VulDB-Added-as-CVE-Numbering〔2022/4/19 確認〕

※ 186 IPA：共通脆弱性タイプ一覧 CWE 概説　https://www.ipa.go.jp/security/vuln/CWE.html〔2022/4/19 確認〕
※ 187 IPA：共通脆弱性評価システム CVSS 概説　https://www.ipa.go.jp/security/vuln/CVSS.html〔2022/4/19 確認〕
※ 188 JPCERT/CC：セキュアコーディング　https://www.jpcert.or.jp/securecoding/〔2022/4/19 確認〕
※ 189 Microsoft 社：Windows 11: ハイブリッド ワークと学習のためのオペレーティング システム　https://blogs.windows.com/japan/2021/06/25/windows-11-the-operating-system-for-hybrid-work-and-learning/〔2022/4/19 確認〕
※ 190 IPA：更新：Apache HTTP Server の脆弱性対策について (CVE-2021-41773, CVE-2021-42013)　https://www.ipa.go.jp/security/ciadr/vul/alert20211006.html〔2022/4/19 確認〕
JPCERT/CC：Apache HTTP Server のパストラバーサルの脆弱性（CVE-2021-41773）に関する注意喚起　https://www.jpcert.or.jp/at/2021/at210043.html〔2022/4/19 確認〕
※ 191 NVD：CVE-2021-41773 Detail　https://nvd.nist.gov/vuln/detail/CVE-2021-41773〔2022/4/19 確認〕
※ 192 NVD：CVE-2021-42013 Detail　https://nvd.nist.gov/vuln/detail/CVE-2021-42013〔2022/4/19 確認〕
※ 193 Security NEXT：わずか 3 日、「Apache HTTPD」が再修正 - 前回修正は不十分、RCE のおそれも　https://www.security-next.com/130520〔2022/4/19 確認〕
※ 194 日本経済新聞：VPN 認証情報また流出　日本は 1000 社、中小企業中心　https://www.nikkei.com/article/DGXZQOUE110A80R10C21A9000000/〔2022/4/19 確認〕
※ 195 経済産業省：「情報処理の促進に関する法律の一部を改正する法律案」が閣議決定されました　https://www.meti.go.jp/press/2019/10/20191015002/20191015002.html〔2022/4/19 確認〕
※ 196 「1.3.2 早期警戒パートナーシップの届出状況から見る脆弱性の動向」では、「ソフトウェア製品」と「Web アプリケーション」は、早期警戒パートナーシップにおける対象の区分を意味するものであり、特に断りのない限り、または文献引用上の正確性を期す必要のない限り、「Web アプリケーション」の省略形として「Web サイト」を使用する。
※ 197 NISC：ApacheLog4j の脆弱性 (CVE-2021-44228) に関する注意喚起　https://www.nisc.go.jp/pdf/press/20211213NISC_press.pdf〔2022/4/18 確認〕
JPCERT/CC：Apache Log4j の任意のコード実行の脆弱性（CVE-2021-44228）に関する注意喚起　https://www.jpcert.or.jp/at/2021/at210050.html〔2022/4/18 確認〕
IPA：更新：Apache Log4j の脆弱性対策について (CVE-2021-44228)　https://www.ipa.go.jp/security/ciadr/vul/alert20211213.html〔2022/4/18 確認〕
※ 198 IPA：情報セキュリティ早期警戒パートナーシップの紹介　https://www.ipa.go.jp/files/000044731.pdf〔2022/4/18 確認〕
※ 199 IPA：脆弱性関連情報の届出受付　https://www.ipa.go.jp/security/vuln/report/index.html〔2022/4/18 確認〕
※ 200 ソフトウェア製品の取り扱い終了は、「不受理」「脆弱性でない」「脆弱性対策情報公表済み」「公表せずに製品開発者が利用者ごとに個別で対策を実施済み」のいずれかであることを指す。Web アプリケーションの取り扱い終了は、「不受理」「脆弱性でない」「連絡不可能」「修正完了」「IPA による注意喚起実施済み」のいずれかであることを指す。
※ 201 IPA：調整不能案件の公表判定業務における取扱いプロセス　https://www.ipa.go.jp/security/vuln/report/unreachable_process.html〔2022/4/18 確認〕
※ 202 「1.3.2 早期警戒パートナーシップの届出状況から見る脆弱性の動向」では、「ウェブアプリケーションソフト」は、Web サイト構築関係のソフトウェアを指す。これは、四半期ごとの脆弱性関連情報の届出状況のレポート（IPA：脆弱性関連情報の届出状況　https://www.ipa.go.jp/security/vuln/report/press.html〔2022/4/18 確認〕）で使用している「製品情報種類」の分野種別と同じである。
※ 203 JVN：JVN#97554111 EC-CUBE におけるクロスサイトスクリプティングの脆弱性　https://jvn.jp/jp/JVN97554111/index.html〔2022/4/18 確認〕
※ 204 株式会社イーシーキューブ：【重要】EC-CUBE 4.0 系における緊急度「高」の脆弱性（JVN#97554111）発覚と対応のお願い（2021/5/24 17:00　更新）（2021/05/24）　https://www.ec-cube.net/news/detail.php?news_id=383〔2022/4/18 確認〕
※ 205 JPCERT/CC：JPCERT/CC　ベストレポーター賞 2021　https://www.jpcert.or.jp/award/best-reporter-award/2021.html〔2022/4/18 確認〕
※ 206 IPA：ソフトウェア等の脆弱性関連情報に関する届出状況［2018 年第 4 四半期（10 月～ 12 月）］　https://www.ipa.go.jp/security/vuln/report/vuln2018q4.html〔2022/4/18 確認〕
※ 207 https://www.ipa.go.jp/security/vuln/websitecheck.html〔2022/4/18 確認〕
※ 208 IPA：セキュアプログラミング講座 Web アプリケーション編 第 5 章 暴露対策 Web サーバからのファイル流出対策　https://www.ipa.go.jp/security/awareness/vendor/programmingv2/contents/401.html〔2022/4/18 確認〕

第2章
情報セキュリティを支える基盤の動向

2021 年度も、新型コロナウイルス感染症の蔓延が続いたが、日本･米国･欧州ではワクチン接種が進み、徐々に経済活動は戻りつつある。一方、2022 年 2 月にはロシアによるウクライナ侵攻が発生し、ウクライナ支援国家に対するサイバー攻撃や安全保障面の懸念が高まっている。

国内ではテレワークやオンライン会議が定着し、業務のデジタル化が進んでいる。政府ではデジタル庁が発足し、政府の IT 基盤整備とセキュリティを統括することとなった。

本章では、情報セキュリティを支える基盤の動向として、国内外の主な政策、人材育成、国際標準化、各種認証制度、組織・個人における情報セキュリティの取り組みの実態等について解説する。

2.1 国内の情報セキュリティ政策の状況

本節では、政府が推進する情報セキュリティ政策の状況を述べる。

2.1.1 政府全体の政策動向

政府全体のサイバーセキュリティに関する政策は、3 年ごとに改訂されている「サイバーセキュリティ戦略」に基づいている。更に、具体的な施策については各年度の年次計画として策定される。本項では、2021 年 9 月に改訂･閣議決定された「サイバーセキュリティ戦略※1」（以下、戦略）で挙げられている四つの施策項目の概要と、各施策項目に基づいて策定された 2021 年度の年次計画「サイバーセキュリティ 2021※2」（以下、年次計画）の主な内容について述べる。

(1) 経済社会の活力の向上及び持続的発展～DX with Cybersecurity の推進～

戦略では、経済社会のデジタル化や DX 推進の動きに併せてサイバーセキュリティ確保に向けた取り組みを同時に推進すること（DX with Cybersecurity）が重要であるとしている。

(a) 経営層の意識改革

企業にとって、DX（デジタルトランスフォーメーション）の必要性が高まり、付加価値の高いデジタルサービスを生み出せることが重要な競争力になり、サイバーセキュリティ対策を前提とした DX の推進が経営者に求められている。

年次計画では、「サイバーセキュリティ経営ガイドライン」「グループ・ガバナンス・システムに関する実務指針」等の普及・啓発、「取締役会の実効性評価」におけるサイバーセキュリティの重要性周知等によるサイバーセキュリティ経営の普及・実践を促進するとしている。

このうちサイバーセキュリティ経営ガイドラインの実践について、経済産業省は IPA を通じ、2021 年 8 月に「サイバーセキュリティ経営可視化ツール」を公開した※3。また、2022 年 3 月に「サイバーセキュリティ 経営ガイドライン Ver2.0 実践のためのプラクティス集 第 3 版※4」を公開した（「2.4.1 (2) セキュリティリスクマネジメント」参照）。

また、IT やセキュリティの専門知識や業務経験を持たない経営層が、セキュリティ専門家と協働するための「プラス・セキュリティ」知識を習得できる環境整備を推進するため、内閣サイバーセキュリティセンター（NISC：National center of Incident readiness and Strategy for Cybersecurity）は、特に経営層や DX を推進する部課長向けのプログラムの普及の参考となるカリキュラムを作成・公開した※5（「2.3.1 (3) 人材育成の取り組み」参照）。

(b) 地域・中小企業における DX with Cybersecurity の推進

地域・中小企業、あるいはこれまで IT 化が進んでいなかった業種・業態の企業でも、デジタル化や DX 推進への対応が求められ、サイバーセキュリティ対策の必

要性も増している。ところが、こうした企業ではサイバーセキュリティの知見や人材等の不足、予算の確保が困難等の課題がある。

これに対する年次計画の取り組みとして、経済産業省はIPAを通じ、中小企業向けにサイバーセキュリティ対策を安価に提供する民間のサービスのうち一定の基準を満たすものに「サイバーセキュリティお助け隊サービス」の商標使用権を付与する制度を構築し（「2.4.2（3）(a) サイバーセキュリティお助け隊サービス制度」参照）、同サービスの普及を推進した。この制度には、2022年4月1日時点で12件のサービスが登録された※6。

(c) 新たな価値創出を支えるサプライチェーン等の信頼性確保に向けた基盤づくり

デジタルサービスの連携が進み、サプライチェーンが複雑化してサイバー攻撃のリスクポイントが増大することから、サプライチェーン全体を見通したリスク管理の重要性が増している。また、サイバーセキュリティ対策の推進のためには、セキュリティ製品・サービスの信頼性確保も課題である。

サイバーフィジカルシステムのサプライチェーンセキュリティ実装を目的に、内閣府は、戦略的イノベーション創造プログラム（SIP）第2期「IoT社会に対応したサイバー・フィジカル・セキュリティ」を実施し、「サイバー・フィジカル・セキュリティ対策基盤」の研究開発を推進している。2021年10月22日、「IoT社会に対応したサイバー・フィジカル・セキュリティONLINEシンポジウム2021※7」を開催し、成果を公開するとともに「Society 5.0におけるサプライチェーンの信頼性を築くデジタルトラスト」等のプレゼンテーションを行った。

セキュリティ製品・サービスの信頼性確保について、経済産業省は、「情報セキュリティサービス審査登録制度」に基づき、同制度のセキュリティサービス基準を満たすサービスリストを、IPAを通じて公開している。2021年度は、サービスリストの利用促進のため、「情報セキュリティサービス普及促進に関する検討会※8」を設置し、3回にわたり検討会を開催した（「2.1.2（4）情報セキュリティサービス審査登録制度」参照）。

(d) 誰も取り残さないデジタル／セキュリティリテラシーの向上と定着

社会のデジタル化に伴って、すべての国民がサイバーセキュリティ上の脅威から自らを守れるようにする必要がある。従って、サイバーセキュリティに関する基本的な知識・能力を習得できる環境の整備が重要となり、官民による普及啓発活動が求められる。

NISCは、サイバーセキュリティの普及啓発や人材育成に関する公的機関等の施策・取り組みを紹介することを目的として、2021年9月に、「みんなで使おうサイバーセキュリティ・ポータルサイト※9」の正式運用を開始した。このサイトは、ニーズ事例から適切な施策を選択できる「目的から選ぶ!施策一覧」と、利用者属性から適切な施策を選択できる「自身の年齢層や所属から選ぶ!施策一覧」とで構成されている。

総務省は文部科学省と協力し、青少年やその保護者のインターネットリテラシー向上を図るため、「e-ネットキャラバン」（「2.1.3（5）(c) 人材育成・普及啓発の推進」参照）等の青少年や保護者等に向けた啓発講座等の実施や、情報教育の中核的な役割を担う教員等を対象とした研修を実施し、サイバーセキュリティを含む情報モラルに関する指導力の向上を図る取り組みを行っている。2021年度は、「インターネットトラブル事例集（2021年度版）※10」を公開し、インターネットトラブルの実例と予防法を紹介した。

なお文部科学省は、学校における「一人一台端末」の実現を目指すGIGAスクール構想を推進している。同構想におけるセキュリティリテラシーの向上については「2.5.1（2）GIGAスクール構想」を参照されたい。

(2) 国民が安全で安心して暮らせるデジタル社会の実現

戦略では、政府は安心して暮らせるデジタル社会を実現するために、自助・共助による自律的なリスクマネジメントの環境づくりに努めるとしている。また公助としては、国民の安全・安心に関わる経済社会基盤について包括的なサイバー防御に取り組み、かつ先進的な取り組みの導入を率先するとしている。

(a) 国民・社会を守るためのサイバーセキュリティ環境の提供

戦略では、サプライチェーンの複雑化を踏まえ、サイバー空間のリスクの可視化、新しい技術・サービスのセキュリティ確保に取り組むとしている。このうち後者について、NISCは2021年11月、クラウドサービスの安全な運用やインシデント発生時の円滑な対応に重点を置いた利用者向けのガイダンスとして「クラウドを利用したシステム運用に関するガイダンス」を公表した※11。

また、内閣官房、デジタル庁、総務省及び経済産業

省は、統一的なセキュリティ要求基準に基づき安全性の評価がされたクラウドサービスの「政府情報システムのためのセキュリティ評価制度（ISMAP）」への追加登録や更新審査を行った。ISMAP クラウドサービスリスト※12 には、2022 年 6 月 1 日現在で 34 件のサービスが登録されている（「2.7.3 政府情報システムのためのセキュリティ評価制度（ISMAP）」参照）。

(b) デジタル庁を司令塔とするデジタル改革と一体となったサイバーセキュリティの確保

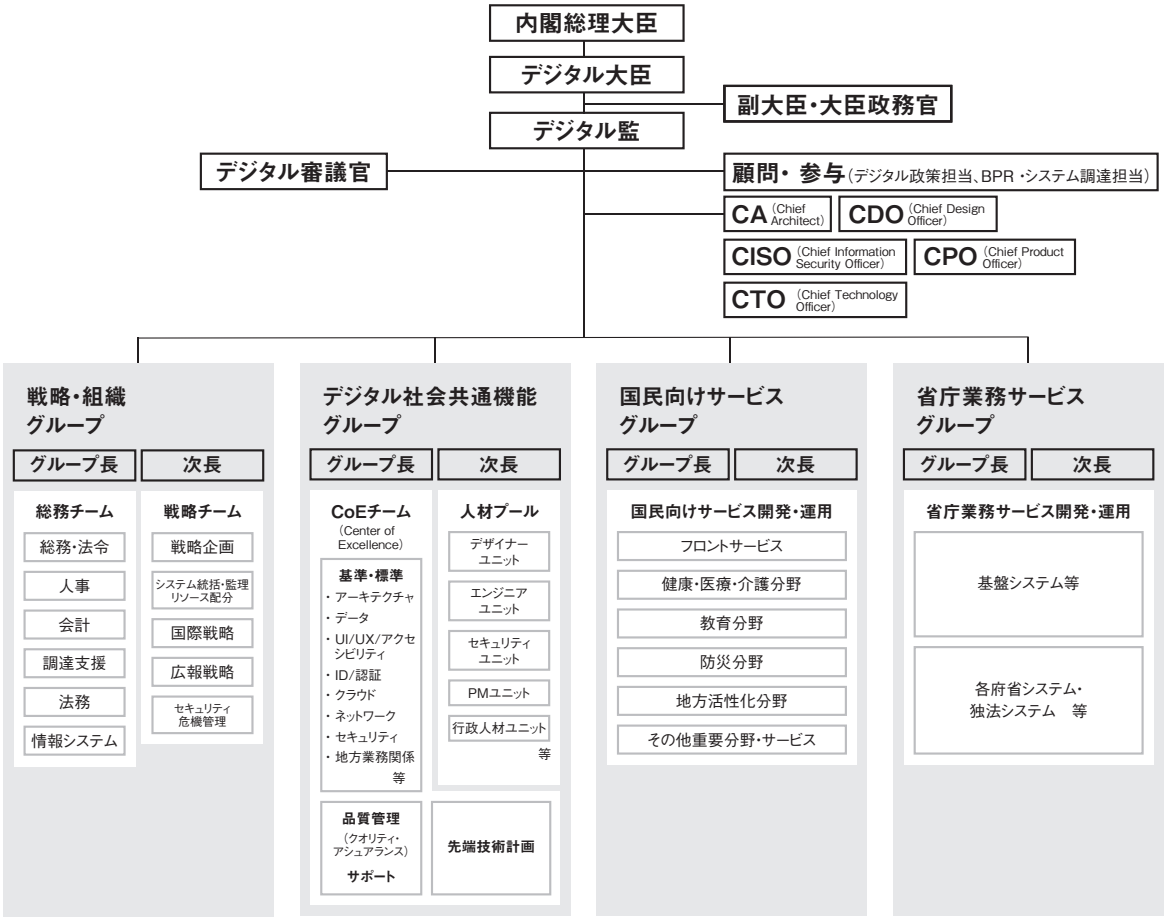
戦略では、国、地方公共団体や公的機関の情報システムの整備・管理の方針をデジタル庁が策定する際に、サイバーセキュリティの基本方針も盛り込み、実装を推進するとしている。デジタル庁において、サイバーセキュリティはデジタル社会共通機能グループの CoE チームが統括する（図 2-1-1）。

また戦略では、マイナンバーカードによる本人確認を前提として、マイナポータルを活用した官民の認証連携やデータ連携を推進する等としている。これを受けてデジタル庁は、「マイナンバー制度及び国と地方のデジタル基盤抜本改善ワーキンググループ」を設置※14して、2021 年度に 3 回開催した。

(c) 経済社会基盤を支える各主体における取り組み

戦略では、各政府機関は、統一的な基準に基づくサイバーセキュリティ対策を施すこととしている。NISC は 2021 年 7 月に、「政府機関等のサイバーセキュリティ対策のための統一基準（令和 3 年度版）※15」及び「政府機関等の対策基準策定のためのガイドライン（令和 3 年度版）※16」を公開した。これらにより、クラウドサービスの利用拡大を見据えた記載や、境界型防御だけでは十分なセキュリティを担保できなくなっている状況を踏まえて、ゼロトラストアーキテクチャの導入を検討すること等が追加された。

また戦略では、政府が共通で利用するシステムはデジタル庁が各府省庁と連携して整備・運用し、サイバーセキュリティも含めて安定的・継続的な稼働を確保するとしており、そのためのクラウドサービス（「ガバメントクラウド」）



■図 2-1-1　デジタル庁の組織体制（2021 年 9 月 1 日現在）
（出典）デジタル庁「組織情報※13」

を2021年度に整備し、翌年度以降は、原則として各府省庁等が活用を検討するとした※17。デジタル庁はこれを受けて、クラウドサービス移行に係る課題の検証を行う先行事業を2021年度から開始するために、協力する自治体を公募した。2021年10月、基幹業務システムは神戸市、倉敷市等8市町村が、セキュリティシステムは青森県、岩手県等7県258市町村が参加するグループ、及び鳥取県、岡山県の46市町村が参加するグループが採択された※18。

このほか、経済・社会を支える重要インフラ等について、政府は各主体の取り組みを促し、支援を行うとしている。これに基づき、NISCは「重要インフラの情報セキュリティ対策に係る第4次行動計画」の改定に先立ってパブリックコメントを募集する目的で、その改訂案※19を2022年1月28日に公開した。

更にNISCは、「多様な主体によるシームレスな情報共有・連携と東京大会に向けた取り組みから得られた知見等の活用」に取り組むとして、2021年12月に「東京オリンピック・パラリンピック競技大会等の大規模国際イベントにおけるサイバーセキュリティの確保に向けた取組の今後の活用方策に関する有識者会議 最終報告※20」をまとめ、公表した。

(3) 国際社会の平和・安定及び我が国の安全保障への寄与

我が国の安全保障環境は厳しさを増し、オープンで自由なサイバー空間を確保するために国際社会との連携を強化する重要性が認識されている。戦略では、サイバー空間の安全・安定の確保のため、法の支配の推進、サイバー攻撃に対する防御力・抑止力・状況把握力の向上、国際協力・連携を一層強化するとしている。

NISCは2021年6月24日、ASEAN（Association of Southeast Asian Nations：東南アジア諸国連合）各国と日本のサイバーセキュリティインシデントへの対応能力向上、国際連携強化を目的に、サイバー情報連絡演習を開催した※21。ASEAN加盟国及び日本の政府機関のサイバー関連業務担当者等308名が参加し、事前に準備したシナリオ（政府に導入されているVPN装置へのサイバー攻撃、医療機関へのランサムウェア攻撃）のもとで、インシデント対応に関する情報共有の演習を実施した。

2021年10月21日には、オンラインにて第14回日本・ASEANサイバーセキュリティ政策会議が開かれた※22。前年の第13回会合で協力が合意された活動（重要インフラ防護、意識啓発、能力構築等）について実施状況を確認し、今後の日・ASEANの連携・協力が検討された。その主な内容は以下のとおりである。

- 情報共有体制及びサイバーインシデント発生時の対処体制の強化
- 重要インフラ防護に関する取り組みの推進、能力構築及び意識啓発における協力の推進
- 産学官連携の推進

なお、日・ASEANの政府間連携については「2.2.1(3) アジア太平洋地域のサイバー連携」を参照されたい。

(4) 横断的施策

戦略では、前述の(1)～(3)に示した施策項目を実行する上で、横断的・中長期的な視点で、研究開発や人材育成等に取り組んでいくことが重要であるとしている。

(a) 研究開発の推進

戦略では、サイバーセキュリティの研究開発においては、脅威情報やユーザニーズを踏まえ、実践的に進めることが重要であるとし、研究開発の国際競争力強化と産学官エコシステムの構築に向けた関係府省庁の振興施策を促進し強化を図るとしている。また、実践的な研究開発の推進においては、サプライチェーンリスクに対応するための技術検証体制の整備、国内産業の育成・発展支援策の推進、攻撃把握・分析・共有基盤の強化、暗号等の研究を推進するとしている。中長期的な対応については、特にAI（Artificial Intelligence：人工知能）技術・量子暗号技術等に関する取り組みを推進するとしている。

サイバーセキュリティ戦略本部は、2021年5月に「サイバーセキュリティ研究開発戦略（改訂）※23」を決定した。これは、2018年7月改訂の「サイバーセキュリティ戦略」を基に、研究開発の進捗と、環境の変化を踏まえた上で、研究・産学官連携の推進方策と産学官エコシステムの構築戦略を示したものである。

2021年度は、国立研究開発法人情報通信研究機構（NICT：National Institute of Information and Communications Technology）等が共同で、AIを用いたプライバシー保護連合学習技術による不正送金検知の実証実験を実施し、その結果を公表した※24。データの機密性を保ったまま機械学習を行う技術等を活用し、金融機関と連携して不正送金等を自動検知するシステムの実現を目指すとしている。

(b) 人材の確保、育成、活躍促進

戦略では、サイバー攻撃が複雑化・巧妙化する環境において新たな価値を創出していくために、サイバーセキュリティ確保に向けた人材の育成・確保が必要であるとしている。

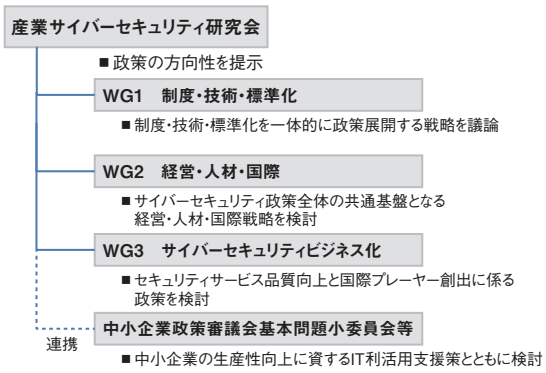
サイバーセキュリティ戦略本部は 2021 年 7 月に、「政府機関におけるデジタル改革に必要な IT・セキュリティ知識を有する人材の確保・育成総合強化方針」を公表した※25。情報システムの開発・運用及びサイバーセキュリティ対策と一体の業務改革に取り組むには、その担い手となる人材の充実が不可欠であるとして、各府省庁の内部人材の育成及び外部登用による確保を図るとしている。

2.1.2 経済産業省の政策

経済産業省は、サイバー空間、フィジカル空間を統合したサプラチェーン全体にわたるセキュリティ対策の実現に向け、制度、標準化、経営、人材、ビジネス等、様々な観点から施策を検討・実施している。

(1) 産業サイバーセキュリティ研究会

2017 年 12 月、経済産業省は我が国の産業界が直面するサイバーセキュリティの課題を洗い出し、関連政策を推進するため、産業界を代表する経営者、インターネット関連の学識経験者等から構成される「産業サイバーセキュリティ研究会」を設置した。図 2-1-2 に同研究会の構成を示す。



■図 2-1-2　産業サイバーセキュリティ研究会の構成
(出典)経済産業省「産業分野におけるサイバーセキュリティ政策※26」

同研究会では 2021 年 4 月に第 6 回会合を開催し、「産業サイバーセキュリティ強化へ向けたアクションプラン※27」(2018 年 5 月発表) で示されたサプライチェーン、経営、人材、ビジネスの 4 パッケージを持続的に発展させるため、以下の三つの課題にチャレンジするとした※28。

- Cyber New Normal における 5 つ※29 の処方箋
  - ①「開発のための投資」から「検証のための投資」へのシフト
  - ②サイバー空間における価値創造を支えるデータマネジメントの枠組みの策定
  - ③セキュリティとセーフティの融合への対応
  - ④サプライチェーンセキュリティ確保のための産業界一丸となった対応
  - ⑤ Like-minded の関係強化
- 国としての対処能力の強化
- For the future infrastructure

以下では、本研究会で合意された取り組み方針に基づいた各 WG の 2021 年度の活動について述べる。

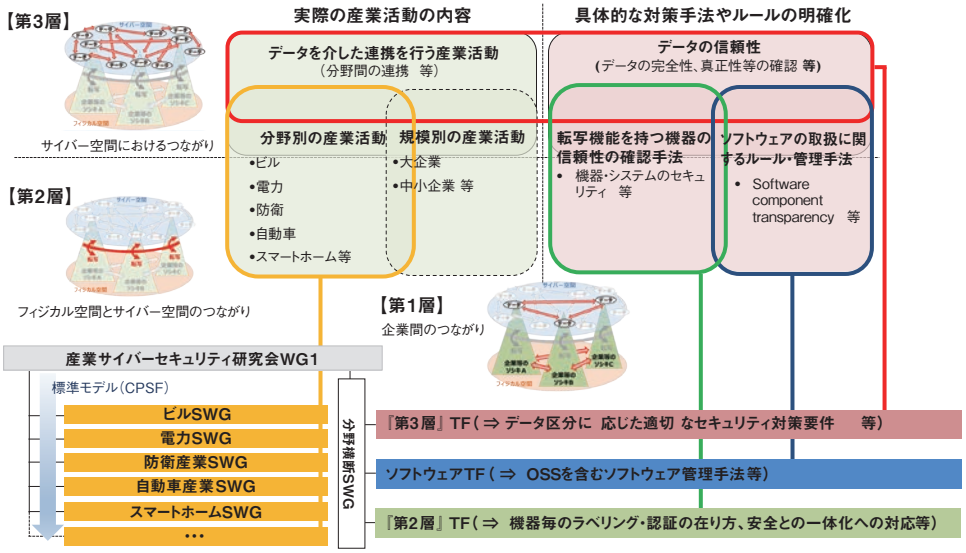
(a) WG1 (制度・技術・標準化)

WG1 では、「サプライチェーンサイバーセキュリティ強化パッケージ」の活動を主に実施しており、産業サイバーセキュリティに関する制度・技術・標準化を一体として政策に展開する戦略を議論している。その前提として、サイバー空間とフィジカル空間の融合により、柔軟かつ動的なサプライチェーンが生まれるとし、これを価値創造過程(バリュークリエイションプロセス)と定義した。また、バリュークリエイションプロセス全体の業界横断的な標準モデルである「サイバー・フィジカル・セキュリティ対策フレームワーク※30 (The Cyber/Physical Security Framework) Version 1.0」(以下、CPSF)を 2019 年 4 月に策定した。

2021 年度は、CPSF をサイバー・フィジカル・システム(CPS)をとらえるモデルの一つとして位置付け、これを日本案として国際規格の策定を推進している。具体的には、ISO/IEC JTC 1/SC 27 WG 4 に Technical Specification (TS)として提案している(「2.6.2 (4) WG 4 (セキュリティコントロールとサービス)」参照)。

CPSF の具体化や実装、分野横断の共通課題を検討するため、WG1 には産業分野別サブワーキンググループ (SWG) と分野横断 SWG が設置されている (次ページ図 2-1-3)。2021 年度の活動の主な成果について述べる。

産業分野別 SWG は、ビル、電力、防衛産業、自動車産業、スマートホーム、宇宙産業、工場の七つの産業分野で活動している。ビル SWG は、ビルシステム全般に共通的な要件をまとめた共通編※31 に続く個別編として「空調システム」を作成中である。防衛産業 SWG は、



■図 2-1-3　タスクフォースの構成
（出典）経済産業省「サプワーキンググループ、タスクフォース等の検討状況※36」

2022 年 4 月に契約企業が保護すべき情報を取り扱う際に適用される情報セキュリティ基準を、米国連邦政府のセキュリティ標準（NIST SP800-171）と同程度まで強化した新情報セキュリティ基準を公開※32した。電力 SWG は、2021 年 2 月に「小売電気事業者のためのサイバーセキュリティ対策ガイドライン Ver1.0※33」を公開した。自動車産業 SWG は、2022 年 4 月に対策項目を拡充した「自工会／部工会・サイバーセキュリティガイドライン 2.0 版※34」を公開した。スマートホーム SWG は、2021 年 4 月に「スマートホームの安心・安全に向けたサイバー・フィジカル・セキュリティ対策ガイドライン Ver1.0※35」を公開した。宇宙産業 SWG は、2022 年 2 月から 3 月に「民間宇宙システムにおけるサイバーセキュリティ対策ガイドラインβ版」に対するパブリックコメントを実施した。工場 SWG は、2022 年 4 ～ 6 月に「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン（案）」に対するパブリックコメントを実施した。

分野横断 SWG は、2020 年度に引き続き CPSF の実装を促進するべく、第 2 層（フィジカル空間とサイバー空間のつながり）及び第 3 層（サイバー空間におけるつながり）に焦点を絞った層別タスクフォース（以下、TF）や、オープンソースソフトウェア（OSS：Open Source Software）等のソフトウェアの活用・脆弱性管理手法を検討するソフトウェア TF で議論を進めた。

第 2 層 TF では、2022 年 4 月に「IoT セキュリティ・セーフティ・フレームワーク（IoT-SSF）」を活用するための「IoT セキュリティ・セーフティ・フレームワーク Version 1.0 実践に向けたユースケース集※37」を公開した。

第 3 層 TF では、2022 年 4 月にデータマネジメントに関する共通の考え方を整理した「協調的なデータ利活用に向けたデータマネジメント・フレームワーク ～データによる価値創造の信頼性確保に向けた新たなアプローチ」を公開した※38。

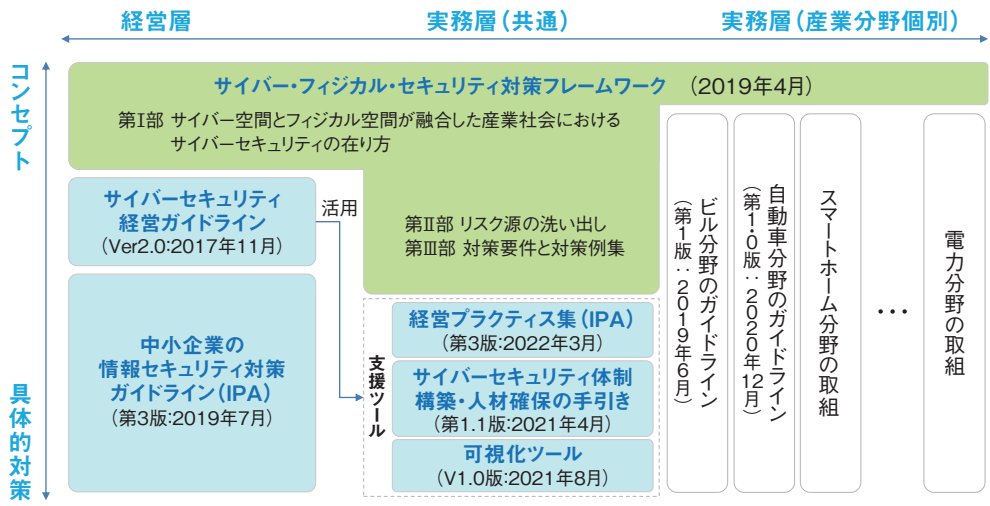
ソフトウェア TF では、2021 年 4 月に「OSS の利活用及びそのセキュリティ確保に向けた管理手法に関する事例集」を公開した※39。またソフトウェア管理手法としての Software Bill of Materials（SBOM：ソフトウェア部品表）の活用促進に向けて、自動運転システム検証基盤ソフトウェア「GARDEN ScenarioPlatform」を対象にした実証事業を実施した※40。

(b) WG2（経営・人材・国際）

「サイバーセキュリティ経営強化パッケージ」と「サイバーセキュリティ人材育成・活躍促進パッケージ」の活動を主に実践する WG2 では、サイバーセキュリティ対策における経営者の参画と人材育成、中小企業の対策、国際連携に関する政策を議論している。各種取り組みは CPSF を軸として整備している（次ページ図 2-1-4）。

経営に関しては、「サイバーセキュリティ経営ガイドライン※42」について、CPSF のコンセプトの反映やサプライチェーンの再整理等の検討を含め、2022 年度中に改訂を実施予定である。

「サイバーセキュリティ経営ガイドライン」の普及・定着については、IPA を通じて 2022 年 3 月に「サイバーセキュリティ経営ガイドライン Ver2.0 実践のためのプラクティス集第 3 版※4」及び経営ガイドラインの「重要 10 項目」の実



■図 2-1-4　CPSF を軸とした各種取り組みの大まかな関係
（出典）経済産業省「事務局説明資料※41」（第 7 回 産業サイバーセキュリティ研究会 ワーキンググループ 2（経営・人材・国際）資料 3）を基に IPA が編集

践をサポートする事例検索ツール「プラクティス・ナビ※43」を公開した。また、2021 年 8 月に「サイバーセキュリティ経営可視化ツール」（Web 版）を公開している（「2.4.1（2）セキュリティリスクマネジメント」参照）。

中小企業のセキュリティ対策の支援に関しては、IPA を通じて、2021 年 2 月には「サイバーセキュリティお助け隊サービス基準（1.0 版）」及び「サイバーセキュリティお助け隊サービス審査登録機関基準（1.0 版）」を、2021 年 7 月には「サイバーセキュリティお助け隊サービス基準」改訂版として 1.1 版を公開した。また、サービス審査登録機関により、サービス基準を満たすことが確認されたサービスに対して「サイバーセキュリティお助け隊マーク」の使用権を付与する事業を開始した。2022 年 4 月 1 日時点で 12 の民間事業者が登録されている※6（「2.4.2（3）（a）サイバーセキュリティお助け隊サービス制度」参照）。

地域に関しては、地域のセキュリティ・コミュニティ（地域 SECUNITY）の取り組みを更に促進するため、2021 年 6 月に「サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3：Supply Chain Cybersecurity Consortium）」において地域 SECUNITY 形成促進 WG を設置した。また各地域における活動にあたって必要となる情報の共有、ベストプラクティスの展開、共通課題に対する解決策の検討等を目的としたワークショップを実施した（「2.4.2（2）（b）地域 SECUNITY 形成促進事業」参照）。

人材に関しては、セキュリティ人材の育成とプラス・セキュリティの普及が取り組みの柱となった。組織における人材確保や体制構築については、2021 年 4 月に「サイバーセキュリティ経営ガイドライン Ver2.0」の付録文書「サイバーセキュリティ体制構築・人材確保の手引き」の改訂第 1.1 版※44 を公開した（「2.3.1（2）セキュリティ業務・役割の広がり」参照）。

更に 2021 年 9 月から、「セキュリティ経営・人材確保の在り方検討 TF」を 9 回開催した（「2.1.2（2）（b）セキュリティ経営・人材確保の在り方検討 TF」参照）。

プラス・セキュリティについては、SC3 の産学官連携 WG において必要なスキルの整理等を行うこととした「2.3.1（3）（b）SC3 産学官連携 WG」参照）。今後、プラス・セキュリティの取り組みを普及させるため、デジタル人材育成プラットフォーム（「2.3.1（3）（a）デジタル人材育成プラットフォーム」参照）、地域 SECUNITY との連携による取り組みの推進等が検討される。

（c）WG3（サイバーセキュリティビジネス化）

「セキュリティビジネスエコシステム創造パッケージ」の活動を主に実践する WG3 では、セキュリティ製品・サービスの品質向上と国際プレイヤー創出に関わる政策として、サイバーセキュリティ製品の有効性を検証する検証基盤の整備を進めている。

セキュリティ製品の有効性検証／実環境における試行検証に関しては、IPA を通じて、製品選定から有効性検証の仕組み（手順・基準等）に基づいた製品検証や実環境での試行を実施し、これを通じ「試行導入・実績公表の手引き※45」の評価を実施した。また、更なるマッチング機会創出に向け、検証結果を活用した表彰制度の立案に向けた検討を行った。

模擬攻撃を含めたハイレベルな検証サービスに関しては、成果として 2021 年 4 月にセキュリティ検証サービス

の高度化を目的に「機器のサイバーセキュリティ確保のためのセキュリティ検証の手引き」の公開等を実施した※46。本手引きは、「機器のセキュリティ検証において検証サービス事業者が実施すべき事項」「より良い検証サービスを受けるために検証依頼者が実施すべき事項及び持つべき知識」「検証サービス事業者・検証依頼者間の適切なコミュニケーションのために二者間で共有すべき情報や留意すべき事項」を整理したものである。本手引きが検証サービス事業者及び依頼者に活用されることで、国内の検証サービスの水準向上や、適切な検証体制の構築が期待される。

中小企業向けセキュリティ製品・サービスの検証事業に関しては、セキュリティ情報提供プラットフォーム仮検証サイトを立ち上げ、有効性検証を実施した。

サイバー・フィジカル・セキュリティに関する情報交流の場であるコラボレーション・プラットフォームに関しては、2021 年度はオンライン開催で計 6 回実施し、計約 800 人が参加した（表 2-1-1）。2021 年度は、新型コロナウイルス感染症（以下、新型コロナウイルス）対策のため聴講主体のオンラインセミナー形式で実施されたが、今後は少人数参加型でのオンラインワーキンググループ形式での開催が検討される。

開催回	テーマ
第 17 回	サイバーセキュリティ検証基盤事業
第 18 回	フェイクデータなど企業価値を毀損する新たな脅威
第 19 回	K 字型（二分化）経済環境下でのセキュリティ投資のあり方
第 20 回	ESG 視点でサイバーリスクマネジメントのあり方を探る
第 21 回	サプライチェーンを標的とするサイバーセキュリティリスクへの課題と対応策
第 22 回	事業変革“DX”の成功を支えるセキュリティ

■表 2-1-1　2021 年度の議論のテーマ

(2) その他の検討会の活動

他の検討会等における活動について述べる。

(a) 企業のプライバシーガバナンスモデル検討会

経済産業省と総務省は、DX における円滑なデータ利活用のためにプライバシーガバナンスの構築を目指している。2021 年度は、IoT 推進コンソーシアムのデータ流通促進 WG のもとに設置された「企業のプライバシーガバナンスモデル検討会」において、2022 年 2 月に「DX 時代における企業のプライバシーガバナンスガイドブック」の改訂版として、実践的な企業の具体例を充実させた ver1.2※47 を公開した。企業が本ガイドブックを参考にすることで、顧客や消費者からの信頼獲得、企業価値向上につながることが期待される。

(b) セキュリティ経営・人材確保の在り方検討 TF

経済産業省は「サイバーセキュリティ経営ガイドラインの見直し」と「セキュリティ人材活躍モデルの構築及び普及啓発」をテーマとして、セキュリティ経営・人材確保の在り方検討 TF を設置、2021 年 9 月から会合を 9 回開催した。「サイバーセキュリティ経営ガイドラインの見直し」については、経営層が自社にどのようなセキュリティ機能が必要かを考える際に、CPSF の枠組みで影響範囲をとらえることが容易となるよう CPSF の内容反映等を議論し、サイバーセキュリティ経営ガイドラインの改訂方針案を策定した。また「セキュリティ人材活躍モデルの構築及び普及啓発」については、2021 年 4 月に公開した「サイバーセキュリティ体制構築・人材確保の手引き 第 1.1 版」について、サプライチェーンや OT（Operational Technology）の観点から体制面での取り組みの強化等を議論した。

(3) 技術等情報管理認証制度

経済産業省は「産業競争力強化法等の一部を改正する法律」に基づき、2018 年 9 月から「技術等情報管理認証制度」を開始した※48。これは、事業者の技術等の情報管理について、国が示す認証基準に適合していることを、事業所管大臣及び経済産業大臣が認定した認証機関が認証を付与する制度である。認証機関に対する支援措置として、独立行政法人中小企業基盤整備機構や IPA からの情報提供支援があり、2022 年 6 月現在 7 事業者が認定を受けている。認証を取得しようとする企業・団体等に対しては、経済産業省が専門家を派遣して認証取得申請の支援を行う事業を行っており、2021 年度は 2021 年 8 月～ 2022 年 3 月の期間に実施した※49。また 2021 年度は、本制度の改善点・普及啓発方策等について検討会を 4 回実施した。機密性の高い技術情報等を保持する中小企業や業界団体等の制度活用が期待される。

(4) 情報セキュリティサービス審査登録制度

情報セキュリティサービスを安心して活用できる環境を醸成するべく、経済産業省は「情報セキュリティサービス基準」（以下、本サービス基準）及び「情報セキュリティサービスに関する審査登録機関基準」を策定し、2018

年2月に公表した※8。2022年1月31日には、両基準に基づく情報セキュリティサービス審査登録制度の一層の普及を図るべく、両基準の第2版を公表し、併せて、初版で「附則」としていた見直し需要の高い項目を「情報セキュリティサービスにおける技術及び品質の確保に資する取組の例示」として新たに公開した※50。

情報セキュリティサービス審査登録制度は、本サービス基準に照らして、情報セキュリティサービスについて一定の品質の維持・向上が図られているか否かを第三者が客観的に判断し、結果を公開することで、利用者が必要なセキュリティサービスを容易に選定できるようにする枠組みである。

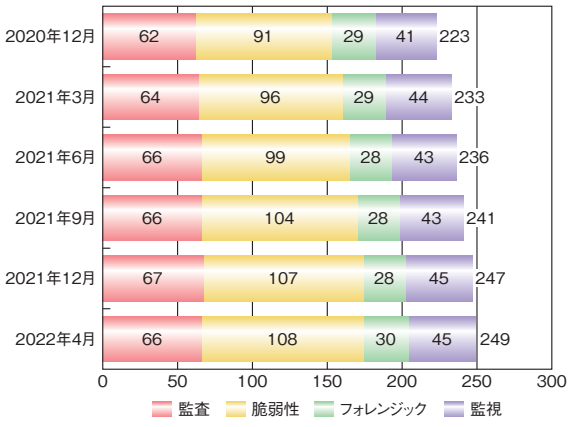
IPAはこの枠組みに基づき、2018年7月から、審査登録機関※51による審査の結果、本サービス基準に適合すると認められ、当該機関の登録台帳に登録され、かつIPAに誓約書を提出した事業者の情報セキュリティサービスを「情報セキュリティサービス基準適合サービスリスト」（以下、本リスト）として公開している※52。また、2021年2月からは、本リスト利用者がサービスを選定する際の参考となるよう、サービスのホームページへのリンク、サービスの概要、主たる対象顧客の分野・業種、対象とする地域の情報を本リストに追加し、提供している。

本サービス基準では、情報セキュリティサービスを以下の四つに分類しており、これらのサービス登録数の合計は2022年4月に249件に達した。登録数の推移としては、ゆるやかな上昇傾向にある（図2-1-5）。

- 情報セキュリティ監査サービス
- 脆弱性診断サービス
- デジタル・フォレンジックサービス
- セキュリティ監視・運用サービス

なお、本リストは、NISCの「政府機関等の対策基準策定のためのガイドライン（令和3年度版）※16」において、以下のケースにおける外部委託先選定の際に活用できるように参照されている。

- 監査業務の外部委託先選定
- 脆弱性診断の外部委託先選定
- インシデントレスポンス業務の外部委託先選定
- セキュリティ監視業務の外部委託先選定



■図2-1-5　情報セキュリティサービス登録数の推移

また、本リストの「情報セキュリティ監査サービス」に掲載されているサービスを提供する監査機関であることは、「政府情報システムのためのセキュリティ評価制度（ISMAP）」において、評価を実施する監査機関の登録申請における要求事項の一つとなっている（「2.7.3 政府情報システムのためのセキュリティ評価制度（ISMAP）」参照）。

今後、本サービスリストの活用が進むことで、情報セキュリティサービスの品質の維持・向上に加え、情報セキュリティサービス市場の活性化にもつながることが期待される。

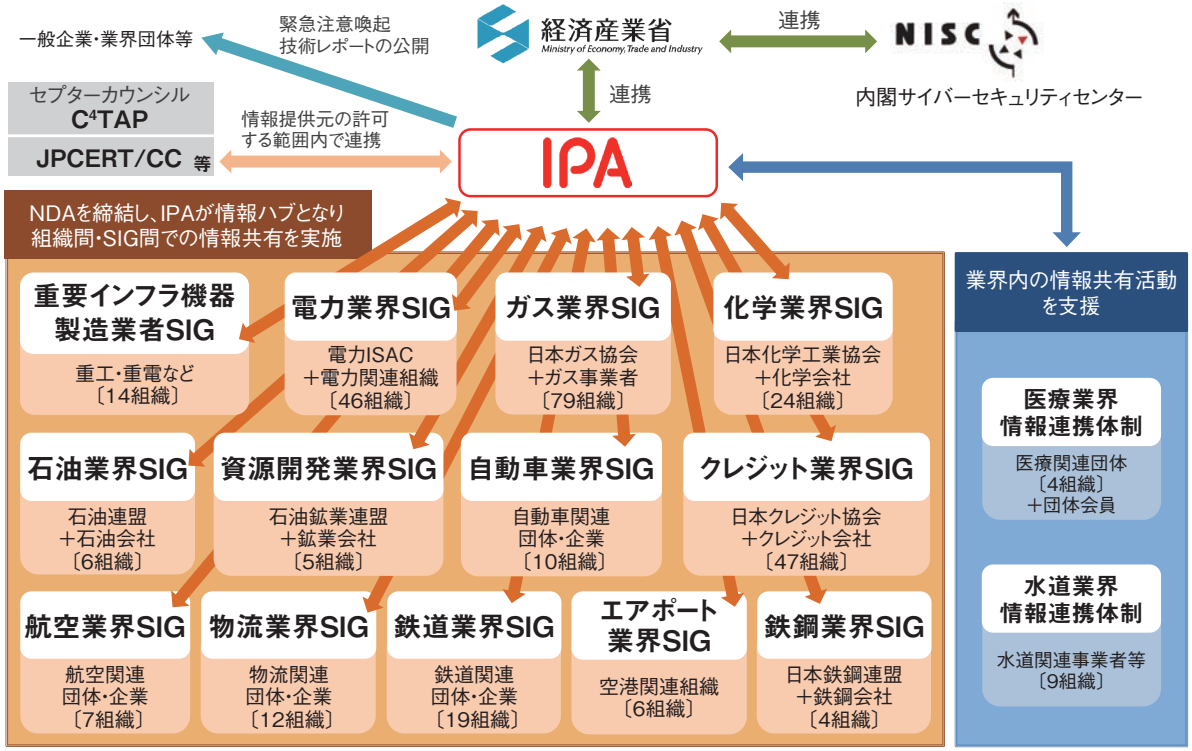
(5) J-CSIP（サイバー情報共有イニシアティブ）

経済産業省の協力のもと、IPAでは2011年10月から、官民連携による標的型攻撃への対策を目的として、J-CSIP（Initiative for Cyber Security Information Sharing Partnership of Japan：サイバー情報共有イニシアティブ）を運用している。

J-CSIPは、日本の基幹産業を担う企業を中心に、サイバー攻撃等に関する情報を相互に共有し、サイバー攻撃の防御とその被害の低減を目指している。2022年3月末日現在、IPAを情報の中継・集約点（情報ハブ）として15の業界から292の企業や業界団体（以下、組織）がJ-CSIPに参加している。参加の形態としては、IPAと各組織との間で個別にNDA（Non-Disclosure Agreement：秘密保持契約）を締結して情報共有を行う業界単位のグループ（SIG※53）と、規約を基に業界の情報共有活動を支援するための枠組みである「情報連携体制」が存在する（次ページ図2-1-6）。

また、J-CSIPはIPAを通じて、経済産業省やセプターカウンシル※54のC⁴TAP、一般社団法人JPCERTコーディネーションセンター（JPCERT/CC：Japan Computer Emergency Response Team Coordination Center）等とも連携している。

J-CSIPでは、IPAと参加組織との間でサイバー攻撃に関する手口や被害の情報、標的型攻撃メール等に関する情報共有を行っている。なお、J-CSIPの中で共有



■図 2-1-6　J-CSIP の体制全体図
（出典）IPA「サイバー情報共有イニシアティブ（J-CSIP）運用状況［2022 年 1 月～ 3 月］※55」

される情報は、提供元が明らかにならないよう、情報提供者の固有の情報を除去するルールがある。

参加組織から提供された、不審なメール、ウイルス※56、攻撃の痕跡等の件数（情報提供件数）、提供を受けた情報のうち標的型攻撃メール等と見なした件数（標的型攻撃件数）、及びそれらを基に J-CSIP 内で情報共有を行った件数（情報共有件数）を表 2-1-2 に示す。年度により件数の増減はあるものの、継続して情報提供や共有が行われていることが分かる。

	2018 年度	2019 年度	2020 年度	2021 年度
参加組織からの情報提供件数	2,020	2,303	6,202	843
標的型攻撃件数（メール、検体等）	213	401	125	35
情報共有件数	195	225	147	118

■表 2-1-2　J-CSIP の運用実績

2021 年度は直近の 3 年間と比較して件数が減っている。これは「Ursnif」やその亜種である「Dreambot」、また「Emotet」と呼ばれるウイルスへの感染を狙う日本語の攻撃メールが大量にばらまかれ続けていたが、2021 年度はそれらの攻撃が減少あるいは停止していた時期が長かったことが影響している。

J-CSIP では、無作為に送信される不審メールやウイルスメール（ばらまき型メール）については、一般的に脅威の度合いが低いと考えられることから、原則として情報の提供依頼や共有の対象とはしていない。しかし、Emotet については、無作為に近い攻撃でありながらも、窃取した正規メールの文面の流用、パスワード付き ZIP ファイルの悪用といった手口が駆使され、多数の企業・組織にとって深刻な脅威であると見なせる状況であった（「1.2.6 ばらまき型メールによる攻撃」参照）。このことから、特に攻撃手口等に大きな変化が確認できた際は、情報共有の対象とし、各組織に対応を促してきた※57。なお、2017 年頃には Ursnif や Dreambot が巧妙な日本語の件名のメールで観測されたことから、同様に一部情報共有を行ってきた。ばらまき型メールと見なせる攻撃であっても、かつて標的型攻撃で使われていたような巧妙な手口が取り入れられている傾向があり、状況に応じ、今後も情報共有を図っていく必要があると思われる。

ビジネスメール詐欺に関しては、2020 年度までと同様、複数の情報提供を受けた。実被害に至る前に偽のメールであることに気付けた事例もあれば、攻撃者の口座へ送金してしまった事例もあった。企業間の取り引きのメールに介入したり、CEO（Chief Executive Officer：最高経営責任者）になりすましたりする等、基本的な騙しの

手口は変わらない（「1.2.3 ビジネスメール詐欺（BEC）」参照）。ただし細かい点では、送金先の変更を依頼する際、新型コロナウイルスの影響であるという嘘をつく等、時流に沿った騙しの手口の変化が見られた。これらの詳しい情報を J-CSIP 内で共有するとともに、情報提供元の許可が得られた範囲で、事例の一般公開も行った。

このほか、ウイルスに感染させる仕掛けが施された PowerPoint や Excel のアドインファイルが添付された攻撃メール、自衛隊の大規模接種センターをかたったフィッシングメール等の情報提供があり、それぞれ共有を行った。

全体的には、2016 年度まで観測されてきた、諜報活動が目的と思われる、日本国内の特定の業界や組織に向けて多数のメールが送信されるような標的型攻撃は減少傾向にある。これは、攻撃者がより慎重に、目立たないように攻撃を行うようになったためであると考えられる。また、発端が標的型攻撃メールであるのか、別の方法であるのか特定できないが、長期に渡って組織内ネットワークへ侵入されていたという情報提供もあった。ひそかに攻撃を行う攻撃者に一層の注意が必要と思われる。

情報共有活動は、攻撃の痕跡や手口の情報を基に、防御側で連携して対抗するための重要な施策の一つであり、IPA は引き続き J-CSIP の運用を継続していく。

(6) J-CRAT（サイバーレスキュー隊）

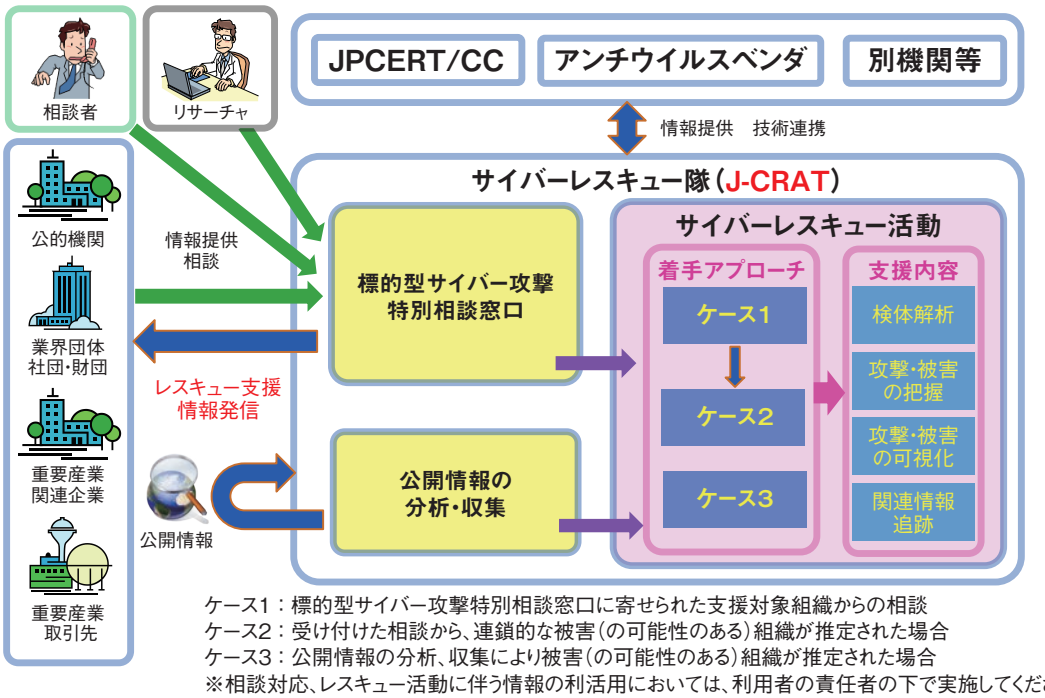
経済産業省の協力のもと、IPA は 2014 年 7 月に J-CRAT（Cyber Rescue and Advice Team against targeted attack of Japan：サイバーレスキュー隊）を発足させた。J-CRAT の目的を以下に示す。

- 攻撃に気付いた組織に対する被害拡大と再発の抑止・低減
- 標的型攻撃による諜報活動等の連鎖の遮断

J-CRAT では、常時「標的型サイバー攻撃特別相談窓口」（以下、窓口）の運営と「公開情報の分析・収集」の二つの活動を実施している。

窓口では、主に公的機関等の組織から、標的型攻撃メールに関する情報提供や相談を受け付けている。「公開情報の分析・収集」では、日々公開されるインターネット上の情報等から、各種ウイルス情報等を収集している。これまでの活動実績から、地政学や国際政治、国際経済や科学技術等に関する動向との関連が明らかになったため、それらの情報収集を幅広く行っている。

標的型サイバー攻撃の被害に遭っている、または遭っている可能性が高い組織のうち、特に公的機関や業界団体、重要インフラ関連企業や取引先等サプライチェーンを構成する組織に対して、被害実態の確認と認知の支援、被害緩和の暫定対応に関する助言を「サイバーレスキュー活動」として実施している[※58]。また、窓口における対応の結果、必要があると判断した組織に対して、攻撃の期間・内容、感染範囲、想定被害等をヒアリン



ケース1：標的型サイバー攻撃特別相談窓口に寄せられた支援対象組織からの相談
ケース2：受け付けた相談から、連鎖的な被害（の可能性のある）組織が推定された場合
ケース3：公開情報の分析、収集により被害（の可能性のある）組織が推定された場合
※相談対応、レスキュー活動に伴う情報の利活用においては、利用者の責任者の下で実施してください。

■図 2-1-7　J-CRAT の活動の全体像とスキーム
（出典）IPA「サイバーレスキュー隊 J-CRAT（ジェイ・クラート）[※59]」

グし、早急な対策着手が行えるよう、民間セキュリティ事業者への移行を前提とした助言を行っている（前ページ図 2-1-7）。

相談を受けた案件のうち、緊急を要する事案に対しては、「レスキュー支援」を行い、更に当該組織での対応が必要な場合は、隊員を派遣する「オンサイト支援」を行っている。それぞれの支援件数を表 2-1-3 に示す。2021 年度の活動実績を 2020 年度と比較すると、「相談件数」は 7.6% 減少しており、内訳を見ると「レスキュー支援件数」が 7.8% 減少、「オンサイト支援件数」も 47.1% 減少している。

	2018 年度	2019 年度	2020 年度	2021 年度
相談件数	413 件	392 件	406 件	375 件
レスキュー支援件数	127 件	139 件	102 件	94 件
オンサイト支援件数	31 件	20 件	17 件	9 件

※一つの事案に対しての複数回のオンサイト対応を要した場合も、1 件として集計

■表 2-1-3　J-CRAT の活動実績

J-CRAT では、定期的に活動状況を公開するほか、情報収集活動や支援活動から得られた結果を技術レポートとして随時公開している。これらの取り組み等を通じ、被害組織のセキュリティインシデントに対する速やかな対応力向上や、平時における標的型攻撃への対策力向上に資する活動を行っている。また、活動を通じて組織のセキュリティ人材の育成、標的型サイバー攻撃の連鎖の解明、及び攻撃の連鎖を遮断することによる被害の低減を推進していく。

2.1.3 総務省の政策

総務省は、IoT・5G 機器に対するサイバー脅威が深刻化している状況を踏まえて 2020 年 7 月に取りまとめた提言「IoT・5G セキュリティ総合対策 2020[※60]」の改訂版として、2021 年 7 月に「ICT サイバーセキュリティ総合対策 2021[※61]」（以下、総合対策 2021）を策定・公表した。総合対策 2021 には、デジタル庁の発足、DX の進展等の環境変化も踏まえ、IoT・5G にとどまらない ICT インフラサービスに対するセキュリティ対策が広く盛り込まれている。

本項では、総合対策 2021 の流れに沿った総務省のセキュリティへの取り組み状況、及び地方自治体のセキュリティへの取り組み状況を述べる。

(1)「ICT サイバーセキュリティ総合対策 2021」の概要

2021 年 7 月、総務省は ICT サービス・インフラにおけるサイバーセキュリティを確保するための具体的な施策について、総合対策 2021 に取りまとめた。以下の方針や考え方に準拠している。

- 2020 年 12 月に閣議決定した「デジタル社会の実現に向けた改革の基本方針[※62]」に基づく社会全体のデジタル改革・DX の推進
- 2021 年 5 月にサイバーセキュリティ戦略本部が発表した「次期サイバーセキュリティ戦略（骨子）[※63]」に基づく「自由、公正、かつ安全なサイバー空間」の確保
- IoT、5G を含む ICT サービス・インフラは、デジタル改革・DX 推進の基盤であり、国民一人ひとりが安心して ICT を活用できるようなサイバーセキュリティの確保が不可欠であるという考え方

総合対策 2021 では、具体的施策として、「電気通信事業者における安全かつ信頼性の高いネットワークの確保」「COVID-19 への対応を受けたセキュリティ対策の推進」「デジタル改革・DX 推進の基盤となるサービス等のセキュリティ対策」「サイバーセキュリティ情報に関する産学官での連携・共有等の促進」を挙げている。また、横断的施策として、「サイバーセキュリティ情報に関する産学官での連携・共有等の促進」「ICT サイバーセキュリティに係る横断的施策」を挙げている。以下では、2021 年度の各施策の実施状況について述べる。

(2) 電気通信事業者における安全でかつ高信頼なネットワーク確保のための対策推進

総合対策 2021 では、5G インフラ構築の進展や IoT 機器の普及、社会のデジタル化進展等によって高まるサイバーリスクに対し、電気通信事業者がセキュリティ対策を講じ、安全で高信頼なネットワークを確保することが重要であるとし、以下の三つの重点施策を挙げている。

(a) 安全かつ信頼性の高いネットワーク確保

総合対策 2021 では、安全かつ信頼性の高いネットワーク確保のため、ガバナンスの確保、及び通信事故の報告・検証に注目している。

- ガバナンスの確保

  総務省は 2021 年 4 月に通信事業者にサイバーセキュリティの実態に関しヒアリングを行うとともに、同年 5 月に「電気通信事業ガバナンス検討会」を立ち上げ、セ

キュリティ対策とデータの取り扱いに対する事業者のガバナンスの在り方を協議した。

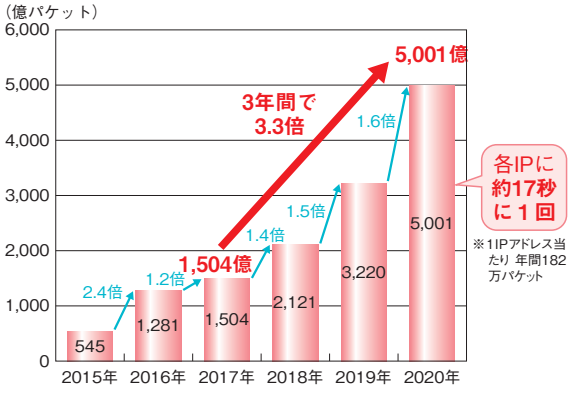
上記検討会では、ネットワークサービス利用者情報の保護の強化が焦点となっていた。具体的には、ネットワークサービス事業者が収集するクッキー・タグ等の取り扱いに関して国内外の施策を調査し、これらの情報を保護するべきとし、事業法である電気通信事業法を改正する方向で議論が進められた。一方で、討議終盤に経済団体から、議論のプロセスが不透明である、電気通信事業法改正による方式は慎重に検討すべき、等の意見が提示された※64。これらの経済団体の意見、及び意見募集を調整した結果は2022年2月18日に公開された※65。利用者情報の保護強化は盛り込まれたが、当初想定されたクッキー利用に関するオプトアウト義務化等は見送られ、事業者の更なるガバナンス強化は今後の検討を待つこととなった。

- 通信事故の報告・検証

総務省は2020年以来、情報通信審議会情報通信技術分科会 IPネットワーク設備委員会にて、IoT導入、マルチステークホルダー等で複雑化する通信事故の報告・原因検証を通じたリスクマネジメントに関するガバナンスを検討している※66。2021年度は、同委員会に事故報告・検証制度等タスクフォースを設置して事業者ヒアリングを実施した。また、事故対応で事業者・官庁・自治体が即応連携する際に課題となるマルチステークホルダーの拡散（増大）について、リスクマネジメント（PDCA、OODA※67ループ等）の強化が重要であるとし、この視点から、サイバー攻撃を原因とする通信事故報告制度や検証制度の在り方、個人情報保護法への対応、事故検証に基づくリスクアセスメント機能の強化等を検討した。これらの検討結果は報告にまとめられ※68、同報告に対する意見募集の結果が2021年9月22日に公表された※69。

(b) 電気通信事業者の積極的なサイバー攻撃対策

総合対策2021では、IoT機器へのサイバー攻撃が急増している状況（図2-1-8）を鑑み、端末側の脆弱性対策だけでなく、ネットワーク側での機動的な対策が必要、としている。具体的に総務省は、情報フロー分析によるC&C（Command and Control）サーバ検知手法の実証施策を検討し、「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会」にて、通信の秘密に抵触しない範囲で事業者が共有できるサーバ情報について整理した。またこの内容を「第四次とりまとめ案」として意見募集を実施※70し、2021年11月24日に結果を公表した※71。結果は、C&Cサーバである疑いの高い機器の検知行為、及びC&Cサーバ検知に関する情報の共有はいずれも適法、というものであった。



■図2-1-8　IoT機器を狙った攻撃の増加
（出典）総務省「ICTサイバーセキュリティ総合対策2021」を基にIPAが編集

(c) 5Gセキュリティの強化

総務省は、制度、技術、情報共有、市場、振興等の各分野で総合的な5Gセキュリティの施策を推進している。2021年時点で注目されるのは、2020年5月に施行、2021年9月にデジタル庁発足を受けて一部改正された「特定高度情報通信技術活用システムの開発供給及び導入の促進に関する法律※72」の運用である。

同法は、5Gの全国基地局やローカル5Gに関わる高度情報通信システムの開発導入を税制面で優遇するもので、導入においてはサプライチェーンセキュリティを含むセキュリティ対策を求めている。税制優遇措置は当初施行後2年であったが、2021年12月、3年間の延長が閣議決定された※73。

上記のサプライチェーンセキュリティには、5G関連機器調達における海外（特に中国）ベンダへの依存リスク対応が含まれる。海外ベンダ依存リスクを低減するため、総務省は、5G製品の相互接続規格化推進、5G市場のオープン化施策を推進している。ベンダに向けた施策としては、相互接続規格O-RAN（Open Radio Access Network）※74の普及、国内のO-RAN相互接続検証拠点の具体化に取り組んでいる。また5G事業者に対しては、周波数帯域割り当てにおいて、オープン化規格に基づく機器の採用計画を必須とし、これを含む特定基地局向け周波数割り当て指針に関して2021年12月に意見募集を行った※75。

このほか、2020年2月にICT-ISACに設置された「5G

セキュリティ推進グループ」は、ローカル 5G のセキュリティ対策調査活動等を実施※76している。具体的には 5G 関連機器ベンダ、通信事業者、ユーザ企業を対象としたアンケート調査結果を 2021 年 3 月に公開し、参照すべきガイドライン策定の必要性を指摘している。今後のガイドラインの整備が期待される。

(3) 新型コロナウイルスへの対応に関するセキュリティ対策の推進

新型コロナウイルスの感染防止対策のため、2020 年 2 月以降、人の移動を抑制し、患者・感染者との接触機会を減らす観点から、テレワークや時差出勤が推進されている。総合対策 2021 では、新型コロナウイルスへの対応に関するセキュリティ対策として、以下の二つの対策を挙げている。

(a) テレワークセキュリティの確保

総務省では、企業等がテレワークを実施する際のセキュリティ上の不安を払拭し、安心してテレワークを導入・活用するための指針として「テレワークセキュリティガイドライン」の初版を 2004 年 12 月に策定した。その後、状況の変化に対応して改定を行い、2021 年 5 月に第 5 版※77を公表した。また、セキュリティの専任担当がいない中小企業等のシステム管理担当者を対象として、テレワークを実施する際に最低限のセキュリティを確実に確保してもらうため「中小企業等担当者向けテレワークセキュリティの手引き（チェックリスト）」等を 2020 年 9 月に策定し、2021 年 5 月に最新のセキュリティ動向等を踏まえて改定を実施した※78。総務省はまた、テレワークを導入する企業等のセキュリティ対策状況の実態調査を実施した。2022 年 3 月に公表された報告書によると、テレワーク導入の課題として、最も多かったのは「テレワークに必要な端末等の整備」(51.9%)、次いで「セキュリティの確保」(51.6%)、「通信環境の整備」(44.3%)という結果で、セキュリティの確保は大きな課題の一つであることがうかがえる※79。

(b) トラストサービスの制度化と普及促進

新型コロナウイルス感染防止のため、対面を前提としない手続きの整備が進んだが、その際、データの改ざんや送信元のなりすまし等を防止する仕組みとしてトラストサービスの必要性が高まった。

総務省では、「プラットフォームサービスに関する研究会」のもとに「トラストサービス検討ワーキンググループ」を立ち上げ、我が国のトラストサービスの在り方に関する検討を行い、2020 年 2 月にトラストサービスの取り組みの方向性について提言した※80。この提言を踏まえ、タイムスタンプ認定制度の適切な運用、電子文書の発行元の真正性を証明する e シール等トラストサービスの普及方策の検討を行った。

タイムスタンプについては、2020 年に「タイムスタンプ認定制度に関する検討会」を立ち上げ、現行の民間の認定制度である「タイムビジネス信頼・安心認定制度」の課題や EU（European Union：欧州連合）等の国際的な制度との整合性等の観点から議論を行い、2021 年 4 月に「時刻認証業務の認定に関する規程（令和 3 年総務省告示第 146 号）」を公布し、国によるタイムスタンプの認定制度を整備した※81。

e シールについては、2020 年 4 月に「組織が発行するデータの信頼性を確保する制度に関する検討会」を立ち上げ、e シールの利用が有効なユースケースや、我が国の e シールの在り方等について検討を行い、2021 年 6 月に「e シールに係る指針」を公表※82し、今後、我が国の e シールの信頼性を担保するために利用者、認証局、e シールサービスの提供事業者、e シールを活用するアプリケーションの提供事業者等に求められる技術上・運用上の基準等について整理した。

電子署名については、2020 年 7 月に「電子署名法 2 条 1 項に関する Q&A※83」を、9 月には「電子署名法 3 条に関する Q&A※84」を公表する等、電子署名法上の電子署名の利便性を改善した。

(4) デジタル改革・DX 推進の基盤となるサービス等のセキュリティ対策の推進

総合対策 2021 では、デジタル改革や DX 推進の基盤として IoT やクラウドサービス、そしてそれらのサービスを組み合わせたユースケースであるスマートシティ等を安全に安心して利用できる環境を整備していくことが重要であるとし、セキュリティ対策として以下の三つの重点施策を挙げている。

(a) IoT のセキュリティ対策

総合対策 2021 では、IoT 機器の設計・製造・販売段階と運用段階のセキュリティ対策強化を並行して行うとしている。

- 設計・製造・販売段階の対策
  製造事業者に対して IoT 機器のセキュリティ・バイ・デザインの考え方を十分に浸透させるとともに、対策

がとられた機器の市場への展開を促進させるために、総務省は「電気通信事業法に基づく端末機器の基準認証に関するガイドライン」（以下、技術基準）を策定し、2020年9月に第2版※85を公表した。一般社団法人重要生活機器連携セキュリティ協議会（CCDS：Connected Consumer Device Security Council）は、この技術基準に加え、製品分野ごとのセキュリティ要件のガイドライン※86を策定し、当該要件に適合したIoT機器に対して適合していることを示すマークを付す認証の仕組み（CCDSサーティフィケーションプログラム）を構築し、運用している※87。2021年10月には、現金自動預け払い機（ATM）関連システムの物理・サイバー攻撃対策に関するCCDSサーティフィケーションプログラムの運用を開始した※88。

- 運用段階の対策

既に運用されているIoT機器のセキュリティを高める対策が必要であるとして、2019年2月よりNICTが脆弱性等のあるIoT機器を調査し、電気通信事業者（ISP: Internet Service Provider）を通じて利用者へ注意喚起を行う取り組み「NOTICE」を実施している※89。2021年度は、総務省のロゴ入り封筒による郵送の注意喚起の実施、注意喚起への対応ができていない利用者（法人）に対する電話ヒアリング等を実施した※90。更に、これまではTelnet及びSSH（パスワード認証）のみを調査対象としてきたが、対象をhttp/httpsプロトコルに広げ、2022年3月から予備調査を開始した※91。

また、2019年6月からは既にウイルスに感染しているIoT機器をNICTの「NICTER」プロジェクトで得られた情報を基に特定し、IPAを通じて利用者へ注意喚起を行う取り組みも実施している。2021年は1IPアドレスあたりで約175万パケットが観測され、2012年以降続いていた増加傾向が減少（約6%減）に転じたが、2019年と比較すると約1.4倍の値であり、依然多くのサイバー攻撃関連パケットが観測されている状況が続いているとのことである※92（2021年度の注意喚起数については「3.2.3(1)国内における実態」参照）。

(b) クラウドサービスの利用の進展を踏まえた対応

総合対策2021では、クラウドサービス利用時の設定ミスを防止・軽減するため、発生している設定ミスやそれに起因する事故、クラウドサービス事業者における取り組み状況等を把握し、当該事業者のセキュリティ対策を促す方策を検討することが適当であるとしている。総務省は、2014年に策定したクラウドサービス事業者向けの「クラウドサービス提供における情報セキュリティ対策ガイドライン」について、全体の構成や責任共有モデルの考え方・管理策の見直し等を行い、2021年10月に改定した※93。改定内容については「3.3.4 クラウドの情報セキュリティに対する政府の取り組み」を参照されたい。

(c) スマートシティのセキュリティ対策

総務省は2021年6月に、安全・安心なスマートシティの実現に資するため、「スマートシティセキュリティガイドライン（第2.0版）※94」を公表した。2020年10月に公表した第1.0版を、よりスマートシティの運用の実態に沿った、スマートシティ構築・運営主体が利用しやすいガイドラインとする改定である。本ガイドラインでは、スマートシティの構成要素を「ガバナンス」「サービス」「都市OS」「アセット」の四つのカテゴリに分け、各カテゴリにおけるセキュリティと、スマートシティ全体としてのセキュリティそれぞれの観点から考慮すべきリスクや対策について整理している。添付のセキュリティ対策一覧表やチェックシートは、スマートシティの分野や特性を踏まえたセキュリティ対策の検討に活用されることが期待される。

また、2021年6月に、上記ガイドラインを活用しようとするスマートシティ推進主体やサービス提供者等に向けた導入ガイドブックとして、「スマートシティセキュリティガイドブック※95」を公表した。上記ガイドラインと同様に活用が期待される。

(5) ICTサイバーセキュリティに係る横断的施策

総合対策2021では、ICTサイバーセキュリティに係る横断的施策として、国際連携の推進、研究開発の推進、人材育成・普及啓発の推進が掲げられている。以下にそれぞれの概要を述べる。

(a) 国際連携の推進

サイバー空間は国境を越えて利用される領域であることから、情報共有、国際的なルール作り、研究開発、人材育成等の多様な取り組みが必要である。アジア地域においてはASEAN各国との関係強化のため、日ASEANサイバーセキュリティ能力構築センター（AJCCBC：ASEAN-Japan Cybersecurity Capacity Building Centre）において、CYDER等を通じて、ASEANのセキュリティ人材の育成支援を実施し、4年間で734名が参加している（2021年12月現在）。また、オンライン環境で受講可能なプログラムの拡充、有志国

との第三者連携、国内企業により開発された演習の提供等を実施している。なお、ASEAN 諸国との包括的な連携については「2.2.1（3）アジア太平洋地域のサイバー連携」を参照されたい。

更に 5G・ポスト 5G 推進とセキュリティ確保、知財権・プライバシー保護を含む安全なデジタルデータ流通について、欧州諸国・EU とも定期的に協議やワークショップを実施している。2021 年度は以下の通り行われた。

- 2021 年 6 月 17 日：日仏 ICT 政策協議（第 21 回）※96
- 2022 年 2 月 3 日：日 EU･ICT 政策対話（第 27 回）※97
- 2022 年 3 月 23 日～ 24 日：日独 ICT 政策対話（第 6 回）※98

(b) 研究開発の推進

NICT は中長期計画に基づき、サイバーセキュリティ分野の基礎的、基盤的な研究開発等を実施している。具体的には、2022 年度までの 3 年間は「電波の有効利用のための IoT マルウェアの無害化、無機能化技術等に関する研究開発」等に取り組んでいる。本研究では、AI 技術を駆使した IoT マルウェアの挙動検知及び駆除、感染した IoT 機器の無害化、無機能化の技術開発に取り組むとしている。

(c) 人材育成・普及啓発の推進

2021 年 4 月に発足したサイバーセキュリティ統合知的・人材育成基盤「CYNEX（Cybersecurity Nexus：サイネックス）」は、我が国のサイバーセキュリティの対応力向上を目指すための共通基盤である※99。CYNEX では、NICT がこれまで取り組んできた、「STARDUST」「NICTER」「CYDER」「ナショナルサイバートレーニングセンター」等の知見、成果を産学官に開放する。更に配下に四つのサブプロジェクト「Co-Nexus」を設け、サイバーセキュリティに関する攻撃分析、データ収集・蓄積、製品検証、人材育成等の活動を行う。2022 年 2 月にはサブプロジェクトの一つであり、演習教材と実機の演習環境からなる「CYROP（サイロップ）※100」のトライアル利用を期間限定で実施した（「2.3.4(7)CYNEX」参照）。

他方、インターネットの安心･安全な利用のため、児童・生徒とその保護者等を対象にした啓発事業「e-ネットキャラバン」を官民連携で実施している。2021 年度の実施件数は 2,559 件、開催場所は 47 都道府県で、全国まんべんなく開催されている。

(6) 地方自治体の情報セキュリティ

本項では、自治体等の情報セキュリティ対策の見直しについて、総務省が 2021 年 9 月より開始した「地方公共団体における情報セキュリティポリシーに関するガイドラインの改定等に係る検討会」からの公表情報等を参照して述べる。

(a) 2021 年度の動向

2021 年 7 月、NISC の「政府機関等のサイバーセキュリティ対策のための統一基準群※15」が改定された。これを踏まえ、総務省は「地方公共団体における情報セキュリティポリシーに関するガイドライン」について、2020 年 12 月に改定した内容を維持しつつ、2021 年 9 月から 12 月にかけて 3 回の検討会を実施※101、2022 年 3 月 25 日に改定版を公開した※102。

主な改定内容は次の 4 点となる※103。

①業務委託・外部サービス利用時の情報資産の取り扱いについて

- 外部サービスを「業務委託」と「外部サービス」に再定義した上で、「機密性 2 以上の情報を取り扱う場合」と「機密性 2 以上の情報を取り扱わない場合」に区分し、取り扱う情報に応じたセキュリティ対策を追記
- 機密性 2 以上の情報を取り扱う外部サービスの利用ライフサイクルに渡るセキュリティ要件の追加、及びシャドー IT 対策となる組織内のサービス利用規定整備の要請を追記
- クラウドサービス選定の指標・基準等として ISMAP や ISO/IEC 27017 等の第三者認証の活用を推奨

②未知の不正プログラム対策製品やソフトウェア等の導入に加え、監視体制や CSIRT との連携を留意点として追記

③多様な働き方を前提としたセキュリティ対策として

- テレワークで職員が確認すべきチェック項目やショルダーハッキング防止等のテレワークの運用面に関するセキュリティ対策を追記
- BYOD（Bring Your Own Device）利用時のセキュリティ対策として IP アドレス、MAC アドレス等による端末認証や端末利用申請手続きの遵守、端末に情報を保存できないようにする機能を設ける等の対策を追記
- Web 会議サービス利用時のセキュリティ対策として Web 会議に無関係な者が参加できないようにする対策等を追記

④マイナンバー利用事務系から外部接続先（eLTAX、ぴったりサービス）へのデータのアップロードについて、地方公共団体に対してリスク分析と情報セキュリティ対策の徹底を条件に認めることを追記

(b) 今後の予定

地方自治体の基幹業務システムの統一・標準化に関しては、「デジタル社会の実現に向けた重点計画」（2021年6月及び12月に閣議決定[※104]。以下、重点計画）において、基幹業務システムを利用する原則すべての地方公共団体が、目標時期である2025年度までに、ガバメントクラウド上に構築された標準準拠システムへ移行できるよう、環境を国が整備する、としている[※105]。また、地方自治体が活用するクラウド環境のセキュリティ対策については「適切に講じる予定[※104]」としており、セキュリティについては、各自治体が個別にセキュリティ対策や運用監視を行う必要がなく、また個別の対応が難しかった最新のセキュリティ対策も導入可能になる、としている[※104]。重点計画は、「自治体の三層の対策」の抜本的見直しを含め、2022年の夏を目途に地方公共団体のガバメントクラウド活用に関するセキュリティ対策の方針を決定していくとし、また先の総務省検討会では「ガバメントクラウド活用に関する新たなセキュリティ対策の在り方については、デジタル庁における検討と連携し、随時検討を行う[※103]」としている。

2021年6月、ガバメントクラウドの先行事業の公募が開始された[※106]。次期自治体情報セキュリティクラウドの一部として活用を希望する都道府県を対象に、ガバメントクラウド等を通じてセキュリティ機能を国が提供する先行事業となる。検証予定とするセキュリティシステムをCDN（Content Delivery Network）及びWAF（Web Application Firewall）とし、サイバー攻撃やシステム障害時の国・地方の役割・連携方法を含め、効果的なセキュリティ対策の実施手法や運用に係る経費の削減等導入効果を検証する予定となっている[※107]（図2-1-9）。

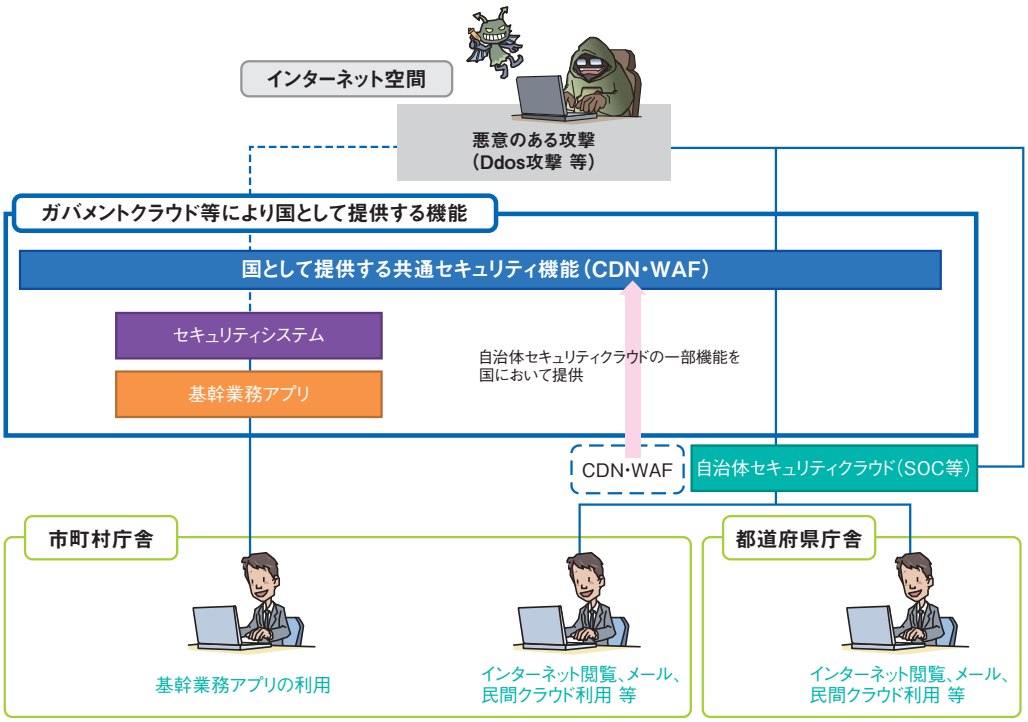
2021年10月、ガバメントクラウド先行事業のうちセキュリティシステムを対象とする自治体について、2グループが採択された[※108]（「2.1.1 (2) (c) 経済社会基盤を支える各主体における取り組み」参照）。

(7) その他の取り組み

総務省のその他の取り組みについて述べる。

(a) 無線LANセキュリティ

総務省では、無線LANの利用者・提供者のそれぞれに向けたセキュリティ確保に関するガイドラインとして「Wi-Fi利用者向け簡易マニュアル」及び「Wi-Fi提供者向けセキュリティ対策の手引き」を作成し[※109]、2020年



■図2-1-9　先行事業（セキュリティシステム）について
（出典）内閣官房「地方自治体によるガバメントクラウドの活用（先行事業）について[※107]」を基にIPAが編集

■図 2-1-10　無線 LAN 利用者・提供者向けガイドライン
（出典）総務省「無線 LAN（Wi-Fi）の安全な利用（セキュリティ確保）について※109」

5 月にこれらの改訂を行っている（図 2-1-10）。

「Wi-Fi 利用者向け簡易マニュアル」では、以下のセキュリティ対策の三つのポイントを示し、解説している。

- 接続するアクセスポイントの確認
- https 通信の際の URL の確認
- 自宅に設置している機器の設定の確認

「Wi-Fi 提供者向けセキュリティ対策の手引き」では、利用者を守るための対策や、Wi-Fi を安全に提供するための対策等について解説している。

2021 年度の活動として、無線 LAN のセキュリティ対策に関する周知啓発を目的として、オンライン講座を開講した※110。

(b) 不正アクセス対策

総務省は、「不正アクセス行為の禁止等に関する法律※111」に基づく取り締り等から得た不正アクセスの手口に関する最新情報の提供や、「不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況」を公表すること等を通じ※112、不正アクセスの防御に関する啓発及び知識の普及を図る等により、官民で連携した不正アクセス防止対策を推進している。なお、上記の「不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況」は 2022 年 4 月 7 日に更新された。2021 年 1 月 1 日～ 12 月 31 日の不正アクセス行為発生状況については「2.1.4 (1) (a) サイバー空間の脅威への対応の強化」を参照されたい。

(c) ログ保存の在り方

安全・安心なサイバー空間を構築するための通信履歴等に関するログの保存の在り方について、「電気通信事業における個人情報保護に関するガイドライン※113」の解説を踏まえ、関係事業者における適切な取り組みを推進する等の対応を行っている。同ガイドラインは 2022 年 3 月 31 日に改訂された。

2.1.4 警察によるサイバー犯罪対策

警察庁では、「警察におけるサイバーセキュリティ戦略※114」及び「サイバーセキュリティ重点施策※115」に従い、サイバー空間の脅威への対処に関する取り組みを推進している。

本項では、2021 年度の警察におけるサイバーセキュリティ重点施策への取り組み状況とサイバー犯罪の情勢等について、警察庁が公開している「令和 3 年上半期におけるサイバー空間をめぐる脅威の情勢等について※116」及び「令和 3 年におけるサイバー空間をめぐる脅威の情勢等について※117」等に基づいて述べる。

(1) 警察における主な取り組み

「サイバーセキュリティ重点施策」は、「サイバー空間の脅威への対応の強化」「警察における組織基盤の更なる強化」及び「国際連携及び産学官連携の推進」を主な柱としている。これらを踏まえ、2021 年度の警察におけるサイバー犯罪対策の主な取り組みについて述べる。

(a) サイバー空間の脅威への対応の強化

サイバー空間が社会活動を営む重要かつ公共性の高い場へと変貌を遂げつつある中で 2021 年のサイバー犯罪の検挙件数は 1 万 2,209 件と過去最多を記録した。ランサムウェアによる被害の拡大、不正アクセスによる情報流出、国家を背景に持つ集団によるサイバー攻撃等、サイバー空間をめぐる脅威は、極めて深刻な情勢が続いているという。

- ランサムウェアの傾向と対応

  2020 年下期の企業・団体等におけるランサムウェア被害の報告件数が 21 件であったものが、2021 年上期は 61 件、同年下期は 85 件と急増した（警察庁によるランサムウェア被害の調査結果については「1.1.2 (4) 国内被害が拡大したランサムウェアについて」参照）。

  ランサムウェアへの対策として、警察庁 Web サイトでの注意喚起（2021 年 9 月）※118、一般社団法人日本損害保険協会等との連携による警察への通報促進に向けた取り組み※119、ダーク Web 上のサイトに掲載された「VPN 製品の認証情報」に関係する企業等への

注意喚起、医療機関を標的としたランサムウェアの被害に関する厚生労働省への情報提供等、関係機関と連携した対策を行った。

- 不正アクセスによる政府機関等からの情報流出
  サイバー攻撃による情報窃取事案については、国内において政府機関や研究機関等が外部からの不正アクセスを受け、個人情報等が流出した可能性がある事案が相次いで確認されている。
  具体的な事例としては、国立研究開発法人海洋研究開発機構からの不正アクセス被害の発表（2021年3月）、内閣府からの内閣府、内閣官房、復興庁及び個人情報保護委員会が使用するファイル共有ストレージへの不正アクセス被害の公表（同年4月）、原子力規制庁からの原子力規制委員会ネットワークシステムへの不正アクセス被害の中間報告（同年5月）等がある。
  また警察庁が実施した企業、行政機関等における不正アクセスの実態調査報告（同年12月公開）によると、回答総数716社・団体のうち、過去1年間に不正アクセス等の攻撃・被害に遭ったと回答したのは95団体（13.3%）であった※120。
- 国家を背景に持つ集団によるサイバー攻撃
  警察の捜査により国家レベルの関与の可能性が明らかになったサイバー攻撃の事案がある。
  具体的には、レンタルサーバ不正契約事件の捜査から国立研究開発法人宇宙航空研究開発機構（JAXA：Japan Aerospace Exploration Agency）を始めとする国内企業等へのサイバー攻撃に中国人民解放軍が関与している可能性が高いとした事案※121や、日本製法人版セキュリティソフトの年間使用権の不正取得に係る捜査から、中国人民解放軍が日本国内の各種情報を収集している可能性が高いとした事案がある。
  また2021年7月、外務省はサイバー攻撃集団「APT40」等について中国政府を背景に持つ可能性が高いとする談話を発表※122した。このとき警察はNISCと連携し、情報収集や対策等を進めていく旨を発表※123、被害企業に対し、不正プログラムへの感染の可能性や有効な対応策等の情報を提供する等、被害防止の取り組みも併せて実施している。
- 東京オリンピック・パラリンピック競技大会
  その他、東京2020オリンピック・パラリンピック競技大会では、大会関係機関と協力し、官民一体の共同対処訓練や、大会関係事業者や重要インフラ事業者等に対する注意喚起等を継続的に実施した。大会期間中、24時間体制で臨んだ結果、大会の運営に影響を及ぼすようなサイバー攻撃は見受けられなかった※124（「2.2.1（1）（c）オリンピック開催と期間中の首脳・外相会談」参照）。

（b）警察における組織基盤の更なる強化

警察のサイバー犯罪対応体制としては、警察庁のサイバー攻撃対策室が、都道府県警察が行う捜査に対する指導・調整、官民連携や外国治安情報機関との情報交換に当たっている。また、サイバー攻撃対策室長を長とする「サイバー攻撃分析センター」でサイバー攻撃に係る情報の集約・分析を実施、14都道府県警察には「サイバー攻撃特別捜査隊」を設置している。更に技術面での支援部隊として警察庁の「サイバーフォースセンター」を司令塔に、全国の地方機関の情報通信部に「サイバーフォース」を設置、24時間体制でのサイバー攻撃の予兆・実態把握、標的型メールに添付された不正プログラムの解析等を行っている※121。

2021年、警察庁の私的懇談会であるサイバーセキュリティ政策会議※125において「サイバー局等新組織において取り組む政策パッケージ」が議論され、サイバー空間を取り巻く情勢とリスク、新組織に求められる役割、その役割を果たす上での政策課題及び解決のための具体策等の提言を含む報告書が取りまとめられ、12月に公開された※126。

並行して、警察法の一部を改正する法律案が2022年1月に国会に提出された※127。国会では、サイバー事案に関する政策を一元的に担うサイバー警察局とともに、重大サイバー事案の捜査、実態解明の責を担う捜査部隊を警察庁に設置すること等が審議された。この結果、2022年4月、警察庁にサイバー局、関東管区警察局にサイバー特別捜査隊が発足した。

（c）国際連携及び産学官連携の推進

国境を越えるサイバー犯罪・サイバー攻撃に対処するためには外国捜査機関との協力が必要になる。警察庁では、国際捜査共助の枠組みの活用や、国際会議、専門家会合、国際刑事警察機構（ICPO：International Criminal Police Organization、INTERPOLとも呼ばれる）等が主催するワークショップへの参加をとおして、外国捜査機関等との情報交換、協力関係の確立に積極的に取り組んでいる。また、情報技術解析に関する事案対処に資する技術情報の収集についても、ICPOデジタル・フォレンジック専門家会合に参加している※121。

国内では、一般財団法人日本サイバー犯罪対策センター（JC3：Japan Cybercrime Control Center）等と連携し、産学官の情報や知見をサイバー犯罪・サイバー攻撃の取り締り等に活用している。

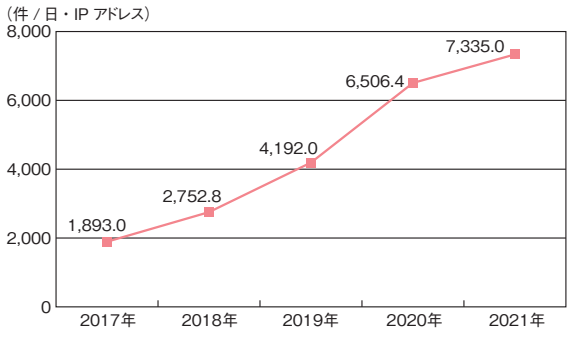
具体的には、2020 年度に引き続き、総務省を装った偽の特別定額給付金申請サイトへの誘導メールに関する注意喚起※128、ワクチン接種予約を装ったフィッシングに関する注意喚起※129、ネット通販サイトの e コマース、通信事業者、クレジット会社等を装ったフィッシングサイトが多数観測されたことへの注意喚起等を JC3 の Web サイト等で実施した※130。

(2) 2021 年のサイバー攻撃の情勢

警察が把握する 2021 年のサイバー攻撃の情勢について述べる。

(a) リアルタイム検知ネットワーク

警察庁では、インターネットとの接続点にセンサーを設置してリアルタイム検知ネットワークシステム※131 を 24 時間体制で運用し、通常のインターネット利用では想定されない接続情報等を検知、集約・分析している。本システムが検知するアクセスの大半は、不特定多数の IP アドレスを対象とするサイバー攻撃やネットワークに接続された機器の脆弱性を探索するサイバー攻撃の準備行為とみられている。2021 年に本システムで検知した不審なアクセス件数は、1 日・1IP アドレス当たり 7,335.0 件（前年比 12.7% 増）で、右肩上がりで増加している（図 2-1-11）。検知したアクセスの送信元は大半が海外であり、海外からのサイバー攻撃等の脅威が高くなっていることが分かる。



■図 2-1-11　サイバー空間における探索行為等とみられるアクセス件数
（出典）警察庁「令和 3 年におけるサイバー空間をめぐる脅威の情勢等について」を基に IPA が編集

また検知したアクセスの宛先ポートも、主として IoT 機器が標準設定で使用するポート番号 1024 以上のポートへのアクセス件数が特に増加しており、2017 年比で 7.1 倍となっている。普及する IoT 機器の脆弱性に対する探索行為であるとみられている※132。

(b) サイバー攻撃への警察の取り組み

サイバー攻撃に対して警察は以下の取り組み等を実施した。

- 海外の捜査当局からの警察庁への情報提供に基づき、総務省と連携し、国内の Emotet に感染している機器の情報をインターネットサービスプロバイダ（ISP：Internet Service Provider）に提供した。また ISP 経由で機器の利用者への注意喚起を実施した。
- サイバー攻撃事案で使用された不正プログラムの解析等を通じて警察が把握した国内 C&C サーバの機能停止（テイクダウン）を、サーバの運営事業者等に働きかけた。運営事業者に対し、不正な蔵置ファイルの削除を依頼する等により無害化措置を実施した結果、27 件の C&C サーバの機能が停止した。
- 電力事業者、自治体、金融機関等重要インフラ事業者等とのサイバー攻撃の発生を想定した共同対処訓練を継続的に実施した。

(3) 2021 年のサイバー犯罪の情勢等

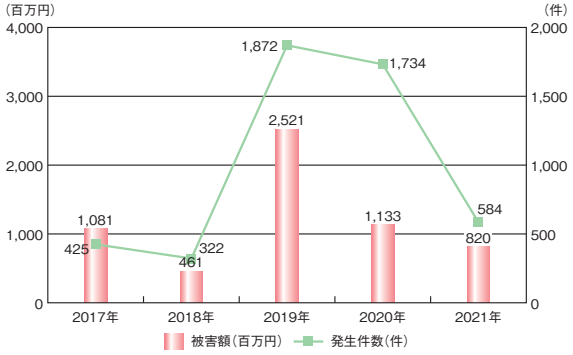
警察が 2021 年に認知したサイバー犯罪の情勢等について述べる。

(a) サイバー犯罪の情勢

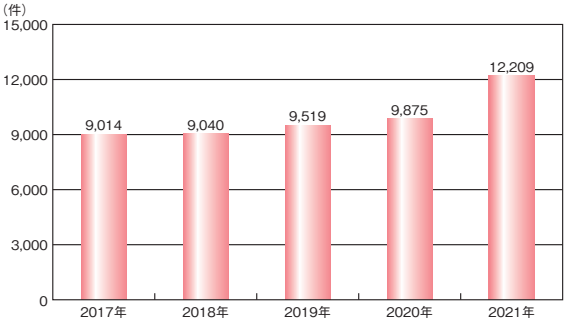
主なサイバー犯罪の情勢について以下に述べる。

- フィッシング等に伴う不正送金・不正利用

「インターネットバンキングに係る不正送金事犯」としては、SMS 等を用いて金融機関等を装ったフィッシングサイトへ誘導する手口のほか、インターネット上のメモアプリ等に保存していたネットバンキングの ID、パスワード等が、同アプリ等への不正アクセスから窃取され不正送金に使用されたと思われるケースが確認されている。インターネットバンキングに係る不正送金事犯による被害が集中している金融機関に対して、警察からはモニタリングの強化、認証手続きに関するセキュリティの強化、利用者への注意喚起の強化等を重点的に実施してきた。2019 年に増加した発生件数、被害額はともに 2 年連続で大きく減少した（次ページ図 2-1-12）。他方、既述の JC3 の注意喚起では、フィッシングのターゲットが従来の銀行等の金融機関から、クレジットカード情報や各種 EC サイトのアカウント情報へと変化して



■図 2-1-12　インターネットバンキングに係る不正送金事犯
(出典)警察庁「令和 3 年におけるサイバー空間をめぐる脅威の情勢等について」を基に IPA が編集



■図 2-1-13　サイバー犯罪の検挙件数
(出典)警察庁「令和 3 年におけるサイバー空間をめぐる脅威の情勢等について」を基に IPA が編集

いる、と分析している。

これらに対し警察は、不正送金組織、口座売買組織の検挙等のほか、金融機関とのサイバー犯罪防犯情報連絡会議等の連携強化、メモアプリ提供事業者に対する被害防止対策の要請や各種注意喚起を実施している。

- 不正商品購入事犯

  2020 年 9 月に確認されたスマートフォン決済サービスを使った不正商品購入の事犯では、2021 年 6 月までに男女 8 人を詐欺等で検挙した。不正に使われたスマートフォン決済サービスに関して、サービス事業者と業務提携する金融機関に開設された口座情報を不正に入手し、振替を行う手口について、金融庁及び関係団体に情報提供するとともに不正防止対策強化の要請を実施した。

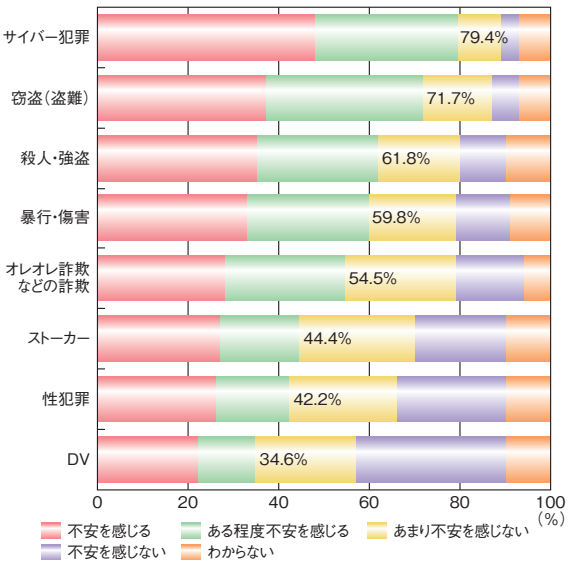
- SMS 認証代行

  二要素認証等において本人確認として使われている SMS 認証を不正に代行する「SMS 認証代行」について、特殊詐欺等に必要な犯行ツールを提供する犯罪インフラにもなりうる懸念から、総務省と連携し、業界団体に対して SMS 機能付きデータ SIM 契約時の本人確認の強化を要請した。併せて都道府県警察に対し、法令に違反する悪質事業者の取り締り強化を図った[※133]。

(b) 検挙件数

警察庁長官官房が公開している「令和 3 年の犯罪情勢[※132]」によると、国内の犯罪情勢を測る指標のうち、刑法犯認知件数の総数は、2003 年以降一貫して減少しており、2021 年は戦後最少を更新している。一方で、サイバー犯罪の検挙件数は 2020 年まで 1 万件弱で推移していたが、2021 年は 1 万 2,209 件に上り、前年から大きく増加した(図 2-1-13)。

2021 年 11 月に警察庁長官官房が実施した犯罪情勢に関するアンケート調査(全国の 15 歳以上の男女 5,000 人を対象)によると、サイバー犯罪に遭うことへの不安感をもっているとの回答が 79.4%(2020 年は 75.3%[※134])となり、その他の犯罪(窃盗、暴行、殺人、詐欺等)を抑え、第一位となっている(図 2-1-14)。同調査で過去 1 年間にサイバー犯罪の被害に遭った、または遭う恐れのある経験をしたとの回答は 35.9% に上る。また、ここ 10 年で日本の治安が悪くなったと思うとした回答が 64.1%、その要因として 57.1% の方がサイバー犯罪を上げている[※132]。国民のサイバー空間に対する不安感は年々高まっている。警察等の公的な機関が必要な役割を果たし、サイバー空間において実空間と同じく安全・安心の確保を図っていくことが求められている。



■図 2-1-14　犯罪に遭うことに関する不安感
(出典)警察庁「令和 3 年の犯罪情勢」を基に IPA が編集

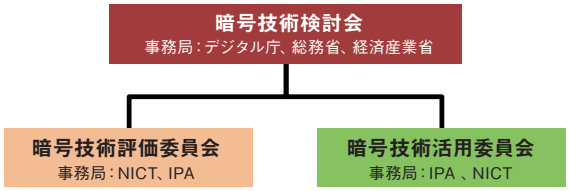
2.1.5 CRYPTRECの動向

電子政府の情報セキュリティを確保するため、デジタル庁、総務省、経済産業省、NICT、及びIPAは安全性と実用性に優れた暗号技術を選び出すことを目的に、CRYPTREC（Cryptography Research and Evaluation Committees）を組織している。CRYPTRECでは、電子政府システムでの利用を推奨する暗号アルゴリズム（CRYPTREC暗号リスト※135）の安全性を評価、監視し、暗号技術の適切な実装法や運用法を調査、検討している。

(1) 2021年度の体制

CRYPTRECは、デジタル庁と総務省、経済産業省が運営し、政策的な判断を含む総合的な観点から電子政府の安全性及び信頼性を確保する活動を推進する「暗号技術検討会」、及びNICTとIPAが運営し、主に技術的な評価を実施する委員会とで構成されている。

委員会には、暗号技術の安全性評価を中心とした技術課題を主に担当する「暗号技術評価委員会」と、セキュリティ対策の推進、暗号技術の利用促進に向けた環境整備を主に担当する「暗号技術活用委員会」が設置されている（図2-1-15）。



■図2-1-15　CRYPTRECの体制

暗号技術検討会と両委員会の主な役割は以下のとおりである。

- 暗号技術検討会
  CRYPTREC活動計画の承認、委員会が作成する各種成果物の承認等、政策的な判断を含む総合的な観点から電子政府の安全性及び信頼性を確保する活動を推進する。
- 暗号技術評価委員会
  暗号技術に対する攻撃技術動向の調査や安全性評価等、暗号技術の技術的信頼に関する検討を担当する。傘下には、量子コンピュータが実用化されても安全性が保てると期待される「耐量子計算機暗号（PQC：Post-Quantum Cryptography）」に関するガイドラインを作成する「暗号技術調査ワーキンググループ（耐量子計算機暗号）」と、従来の暗号技術では実現できないような機能を持つ「高機能暗号」に関するガイドラインを作成する「暗号技術調査ワーキンググループ（高機能暗号）」が設置されている。
- 暗号技術活用委員会
  セキュリティ対策の推進、暗号技術の利用促進等に寄与する運用ガイドラインの整備を中心とした、暗号利用に関する課題の検討を担当する。傘下には、2020年度に公開した「暗号鍵管理システム設計指針（基本編）※136」のガイダンスを作成する「暗号鍵管理ガイダンスワーキンググループ」が設置されている。

(2) 2021年度の主な活動

2021年度の暗号技術検討会及び各委員会の主な活動内容・成果について以下に述べる。

(a) 暗号技術検討会

2021年度には、各委員会の2021年度活動計画、及び活動報告の審議が行われ、承認された。更に、以下の項目についても審議が行われ、承認された。

- 推奨候補暗号リストから電子政府推奨暗号リストへの昇格基準となる「暗号利用実績に関する選定基準」
- 電子政府システムの調達・開発にあたって、調達要件や開発要件として採用すべき「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」
- 鍵長の選択方法や暗号鍵の設定に関する一般的なガイダンスを提供する「暗号鍵設定ガイダンス」
- デジタル署名EdDSA（Edwards-curve Digital Signature Algorithm）※137の推奨候補暗号リストへの追加

(b) 暗号技術評価委員会

CRYPTREC暗号リストに掲載されている暗号技術の安全性と実装性に関わる監視活動のほか、2021年度の主な活動内容・成果は以下のとおりである。

- デジタル署名EdDSAの実装性能調査
  デジタル署名EdDSAについて、2020年度の安全性評価に引き続き、2021年度は実装性能評価を実施した。その結果、EdDSAの実装上の特徴は、いずれも実装性能として有益であると考えられ、楕円曲線DSA（ECDSA：Elliptic Curve Digital Signature Algorithm）と比較しても遜色ない十分な実装性能を有していると判断した。

- 軽量暗号に関する技術動向調査
  2020 年度第 2 回暗号技術検討会での了承に基づき、2021 年度は、2016 年度に作成した「CRYPTREC 暗号技術ガイドライン（軽量暗号）」の更新のため、2017 年度以降の技術動向調査を実施した。特に、2016 年度ガイドラインで紹介された暗号方式を中心とした代表的な軽量暗号に対して、2021 年 9 月時点で脅威につながる脆弱性が指摘されているか否かを 3 段階で分類した。今後は、NIST Lightweight Cryptography コンペティションファイナリスト※138 を対象とした安全性及び実装性能に関わる調査・評価を実施し、新規情報を追加・更新した文書を 2023 年度版ガイドラインとして公開する予定である。
- 暗号技術調査ワーキンググループの活動
  2020 年度第 2 回暗号技術検討会での了承に基づき、2021 年度は、耐量子計算機暗号に関するガイドライン、及び高機能暗号に関するガイドラインを作成するために、耐量子計算機暗号を検討するワーキンググループと高機能暗号を検討するワーキンググループを設置し、それぞれの研究動向を調査している。2022 年秋まで調査を継続し、その結果を踏まえ、2022 年度中にこれらのガイドラインを作成する予定である。この活動に加え、主要な公開鍵暗号（RSA 暗号、楕円曲線暗号）の安全性の根拠となる「素因数分解問題」と「離散対数問題」の困難性に関して、CRYPTREC が公開している「予測図」の改訂も行った※139。

(c) 暗号技術活用委員会

2021 年度の主な活動内容・成果は以下のとおりである。

- 暗号利用実績に関する選定基準の検討
  暗号利用実績に基づく選定基準（選定ルール）は、2012 年度の CRYPTREC 暗号リスト改定の際に初めて導入されたものである。2021 年度の委員会では、2012 年以降の暗号アルゴリズムをめぐる状況変化を踏まえて選定基準の見直しを行った。その結果、電子政府推奨暗号リストへの昇格のための明確な選定基準・閾値は設けず、本基準で示す考慮項目を参考に実際の昇格判断は個々の状況を鑑みて個別に行うものとする基準案を取りまとめた。
- 暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準の検討
  暗号の安全性は暗号アルゴリズムと鍵長の組み合せにより決まるものであるが、今までの CRYPTREC 暗号リストでは鍵長の取り扱いは規定していなかった。そのため、今回、CRYPTREC 暗号リストに掲載されている暗号技術を利用する際に、適切なセキュリティ強度を実現するためのアルゴリズム及び鍵長の選択方法を規定するものとして本基準を作成した。具体的には、電子政府システムを調達または開発する際は、そのシステムの運用寿命全体と、その期間に実現するセキュリティ強度の関係を考慮してセキュリティ強度要件を設定し、その強度要件を満たすアルゴリズムと鍵長の組み合せを調達・開発要件とするように定めている。
- 暗号鍵設定ガイダンスの検討
  暗号技術を利用する際の鍵長の選択方法に関する一般的な考え方のガイダンスとして作成した。具体的には、暗号鍵を安全に設定し、運用していくために考慮すべき項目として、暗号鍵の鍵長についての考え方、暗号鍵のライフサイクル等について解説している。なお、本ガイダンスでは、実際の利用用途や利用期間、環境、コスト、その他様々な制約条件を踏まえて、読者が必要なセキュリティ強度を決めるスタイルを採用している。
- 暗号鍵管理ガイダンスワーキンググループの活動
  情報を安全に取り扱うためには、通信データや保管情報の暗号化に使う暗号アルゴリズムのみに注意を払うだけでは不十分であり、その暗号アルゴリズムに用いられる暗号鍵の管理が適切に行われる必要がある。そこで、2020 年に公開した「暗号鍵管理システム設計指針（基本編）」に引き続き、暗号鍵管理についてのガイダンスを作成するため、暗号鍵管理ガイダンスワーキンググループを設置した。具体的には、情報システム設計者やシステム調達者が暗号鍵管理を適切に扱えることを目的とし、暗号鍵管理で必要となる項目について、シンプルなモデルを例示しつつ、鍵管理における要求や思想が理解できるような記載を目指している。2021 年度は、ガイダンス作成に向けた執筆方針の方向性を取りまとめ、2022 年度中に暗号鍵管理ガイダンスとして完成させる予定である。

COLUMN

デジタル庁が進めるシステム検証とは?

2021年9月1日に、日本のデジタル社会実現の司令塔としてデジタル庁が発足し、注目されています。2021年12月24日には、目指すべきデジタル社会の実現に向けて、政府が重点的に実施すべき施策として、「デジタル社会の実現に向けた重点計画[i]」が閣議決定されました。これは、各府省庁が構造改革や個別の施策に取り組み、それを世界に発信・提言する際の羅針盤となるものです。

この計画では、デジタル社会を形成するための基本原則として、「オープン・透明」「公平・倫理」等10原則を掲げていますが、その中の一つが「安全・安心」です。デジタル改革を進めるに当たって、政府機関・独立行政法人等のサービスにおける国民目線に立った利便性の向上の徹底と、国民への行政サービス等を安定して安全に提供するためのサイバーセキュリティの確保の両立が不可欠であることから、サイバーセキュリティ戦略に基づき、政府全体として同戦略を踏まえた施策を着実に講じていくことにより、サイバーセキュリティの強化に努めることを宣言しています。

その具体的な施策の一つとして、デジタル庁が整備・運用するシステム等の安定的・継続的な稼働の確保等の観点から「システム検証・監査」を実施することとし、その実施体制をデジタル庁とIPAが共同して構築することが記されています。「システム検証」という言葉は、「システム監査」と比べて少し聞きなれないかもしれません。あえて「検証」という言葉を使っているのは、各情報システムがデジタル庁の示す情報システム整備方針に沿った整備・運用を行っているかどうか、という適合性を確認することを主眼としているからです。もちろん確認手段等は「監査」と重なる部分も多いのですが、方針への適合性というより広い視野からの確認を行うことになります。また、この「システム検証」は、NISC・IPAによる府省庁・独立行政法人等へのセキュリティ監査のような第三者による外部監査ではなく、あくまでデジタル庁の内部監査的な位置付けとして実施される予定であることも特徴の一つです。新型コロナウイルス接触確認アプリ「COCOA」における不具合は記憶に新しいところですが、開発チームと独立した検証チームを内部に持つことによって、外部監査よりも迅速かつ柔軟な対応が可能となることが期待されます。

この「システム検証」は、まず2022年度以降、「①デジタル庁システム」(各府省庁が共通で利用する基盤を含む)を中心にスタートし、更に、2023年度以降は、「②デジタル庁・各府省共同プロジェクト型システム」も対象とする予定で、IPAもその一翼を担う組織として取り組みます。

i https://www.digital.go.jp/policies/priority-policy-program/〔2022/5/23確認〕

2.2 国外の情報セキュリティ政策の状況

サイバー脅威は国境を問わず、あらゆる国・地域の脆弱なシステムに対して攻撃が仕掛けられる。また、IT化した社会サービスやそれを支えるサプライチェーンは国境を越えてつながり合い、他国におけるサイバー脅威が自国に深刻な影響を与える可能性がある。更に近年、国家の支援を受けた攻撃者による他国へのサイバー攻撃・虚偽情報流布等の脅威が現実になっている。こうした状況に国や地域が単独で対処することは難しく、国際連携が不可避である。本節では、国際連携に向けた状況理解のために、各国・各地域における情報セキュリティ政策について述べる。なお、米国・欧州については「3.4 米国・欧州の情報セキュリティ政策」を参照されたい。

2.2.1 国際社会と連携した取り組み

2020 年度に引き続き、日本政府は 2021 年度も米国、欧州、インド、ASEAN 諸国等とのサイバーセキュリティに関する連携協議や演習を実施した。それらの活動から主な取り組みを紹介する。2021 年度の傾向として、新型コロナウイルス感染対策に関する国際連携が引き続き重要課題となったが、2022 年 2 月 24 日、ロシアのウクライナ侵攻が勃発、侵攻拡大阻止、ウクライナ政府・避難民の支援、対ロシア経済制裁等に関する国際連携が日本政府にとっても大きな課題となった。サイバーセキュリティの観点では、サイバー戦への対策・ウクライナ支援も国際的な課題となった。

(1) 各国首脳・国際機関との連携

新型コロナウイルスは 2021 年に入っても猛威を振るい、2021 年 6 月以降は感染力の強い変異種デルタ株、同年 11 月以降は更に感染力の強いオミクロン株が世界的に流行した。日本・米国・欧州諸国等は 3 回にわたるワクチン接種や数度のロックダウン等、対応に追われた。

(a) 2021 年 6 月の G7 首脳会合

2020 年度にオンライン形式で開催された G7 首脳会合は 2021 年 6 月 11 ～ 13 日、英国コーンウォール州カービス・ベイにて対面形式で開催された※140。全体テーマはコロナ禍からの「より良い回復」とされ、経済面の回復では、開かれた世界におけるデジタル化、グリーン化、ジェンダー平等、サプライチェーン脆弱性への対処等の方向性が示された。また「より強靭な回復」に向けた議論において、2020 年に引き続き中国に対する懸念が示され、市場の公平性・透明性の担保、人権・自由の尊重、領土問題に関する力による現状変更への反対等も、盛り込まれた。また 2020 年に引き続きワクチン接種等に関する途上国支援が、更に 2021 年の新提案として地球温暖化対策（エネルギーイノベーション）の推進が合意された。

G7 首脳会合で例年議論され、声明が出される「自由でオープンなサイバー空間」の維持に関しては、上記の議論を反映し、2021 年度はより広範な「開かれた社会」を目指す声明が出された※141。同声明には、デジタル、人権、ジェンダー、自由、オープン性・透明性を持つ多国間システム等に加え、ワクチン接種を含む課題への協働、持続可能な開発目標（SDGs：Sustainable Development Goals）の達成支援等が含まれている。

なお、菅義偉首相（当時）は、東京 2020 オリンピック・パラリンピック競技大会の安全・安心な開催の決意を示し、G7 首脳の同意を得た。

(b) 2022 年 3 月の G7 首脳会合・外相会合

2022 年 2 月 24 日、ロシアのウクライナ侵攻が開始された。これに対し G7 首脳は同日に緊急のテレビ会議※142を実施、3 月 12 日に首脳声明を発表し、Vladimir Putin ロシア大統領への非難、侵攻の即時停止と被害者の救済、ロシアへの制裁、ウクライナの支援について団結し合意したことを示した※143。具体的な制裁として、ロシアの最恵国待遇はく奪、多国籍金融機関のロシア融資停止、Putin 政権関係者の資産凍結支援、重要物品・技術の輸出入制限、侵攻関係組織の資金調達制限等が明記された。

更に 2022 年 3 月 24 日、緊急の G7 首脳会合がベルギー・ブリュッセルで開催され、Volodymyr Zelenskyy ウクライナ大統領がオンラインで参加、更なる支援を呼びかけた※144。同会合の首脳声明では、3 月 12 日の首脳声明で明記された金融・経済制裁の強化・ウクライナ支援に加え、原子力施設の安全や核兵器・生物化学兵器使用への懸念、ウクライナのサイバー防御支援・難民支援、ロシア政府の欺瞞的情報統制への非難、エネルギー・食料サプライチェーンの脱ロシアに向けた再

構築、等が盛り込まれた。

侵攻開始1ヵ月のうちに、G7首脳レベルでこのような一枚岩の団結がなされたことは大きなインパクトがあったと思われる。日本政府は、天然ガスや小麦等の供給をロシア・ウクライナに依存しているという課題を抱えながらも、侵攻に対して断固とした態度を取ることを決定している※145。

(c)オリンピック開催と期間中の首脳・外相会談

東京2020オリンピック・パラリンピック競技大会は、デルタ株流行の厳しい状況下となったが、2021年7月23日～9月5日、無観客・感染対策徹底という厳戒態勢のもとに開催された。期間中のセキュリティに関しては、NISCが運用した対処調整センターが観測情報75件、脅威情報32件を関係組織に提供したほか※146、協力通信事業者が4.5億回に上る不審イベントを検知・遮断し、大会運営に影響するインシデントは発生せず、全競技を無事終了した※147。

オリンピック期間中は各国首脳・外相との会談が集中的に行われた。菅首相は11ヵ国（米国・エストニア・フランス・アルメニア・スイス・コソボ・ポーランド・モンテネグロ・トルクメニスタン・モンゴル・南スーダン）の首脳と会談（電話会談を含む）、法の支配に基づく自由で開かれたインド太平洋地域や通商・デジタル化に向けた連携を強化すること等を合意した。また、茂木敏充外相（当時）も6ヵ国（フィンランド・カナダ・アゼルバイジャン・アンティグア-バーブーダ・コソボ・米国）の外相・大統領と会談（電話会談を含む）、上記課題のほかコロナ対策・人権等についても連携を確認した※148。

(d)日米豪印4ヵ国の連携

G7の枠組みとは別に、2019年以降、日米豪印4ヵ国による協議が重ねられている。中国の東シナ海・南シナ海・インド洋への進出政策が各国共通の重要課題となっており、連携を強化する狙いがあると思われる。

2021年9月24日、第2回日米豪印首脳会合がワシントンD.C.で開催され、菅首相、Scott Morrisonオーストラリア連邦首相（Prime Minister of the Commonwealth of Australia）、Narendra Modiインド首相（Prime Minister of India）、Joseph Biden米国大統領が出席した※149。同会談では。2020年の4ヵ国外相会談に引き続き、法の支配に基づく「自由で開かれたインド太平洋」の実現に向けた連携で合意するとともに、ASEAN諸国による取り組みである「インド太平洋に関するASEANアウトルック」を支持し、EUの「インド太平洋における協力のための戦略」も歓迎した。また、ワクチンを含むコロナ対策、気候変動、海洋安全保障、テロ対策、サイバーセキュリティ、人道支援・災害救援等の分野での4ヵ国の協力進展を歓迎し、宇宙、サイバーの分野で作業部会等を立ち上げるとともに、クリーン・エネルギー、人的交流の分野でも協力を強化することで一致した。

(e)国際連合によるサイバー脅威対策推進

2021年5月24～28日、サイバーセキュリティに関する第6会期国連政府専門家会合（GGE：the Group of Governmental Experts）最終会合が開催され、日本から赤堀毅国連・サイバー政策担当大使（総合外交政策局審議官）ほかがオンラインで出席した※150。同会合では、サイバー空間における責任ある国家の行動に関し、2015年のGGE報告書に記載された11個の規範への拘束力のある義務追加の可能性、サイバー空間への国際法、国連憲章の適用、紛争解決のための信頼醸成、能力構築等に関する共通認識を取りまとめた。この結果は報告書として2021年9月の第76回国連総会に提出された。

同報告はサイバー空間の各国の行動に国際法や国連憲章が適用されることとし、違反行為に対する加盟国の責任ある行動を求めた点が特徴である。なお日本政府はサイバー行動に適用される国際法に関する基本的な立場を公表している※151。

続いて2021年11月13～17日、サイバーセキュリティに関する国連オープン・エンド作業部会（OEWG 2021-2025：the Open-Ended Working Group on security of and in the use of information and communications technologies 2021-2025）第1回会合が開催された。OEWGは全加盟国のサイバーセキュリティに関する協議の場として2019年に設置され、2021年3月に報告書を採択していた（「情報セキュリティ白書2021」の「2.2.1(1)(c)国連によるサイバー脅威対策推進」参照）。第75回国連総会決議により、改めて2025年までの活動が決まったものである。同会議では、日本から有馬裕サイバー政策担当大使（総合外交政策局審議官）がビデオメッセージで参加、前述のGGE報告に記載された国際法の適用等の重要性を強調した。

(2)2国間連携の取り組み

「2.2.1(1)(c)オリンピック開催と期間中の首脳・外相会談」で見たとおり、2021年の2国間首脳協議・閣僚

級協議は東京 2020 オリンピック・パラリンピック競技大会期間中に集中的に行われた。以下では、それ以外で行われたサイバーセキュリティ、及びサイバーを含む安全保障に関する 2 国間協議について述べる。

(a)日英サイバー協議

2021 年 6 月 29 日、第 6 回日英サイバー協議がオンライン形式で開催された※ 152。日本からは赤堀審議官、英国からは William Middleton 外務連邦開発省サイバー政策部長（Director Cyber, National Security Directorate, Foreign, Commonwealth and Development Office）を始めとする両国関係省庁の代表者が出席した。

協議においては、2020 年開催の第 5 回に引き続き、サイバー分野における脅威と施策の共有、国際連携、能力構築支援、サイバー強靭性等について議論を行った。

(b)日エストニア・サイバー協議

2021 年 12 月 22 日、第 4 回日エストニア・サイバー協議がオンライン形式で開催された※ 153。日本からは有馬審議官、エストニアからティルマー・クラール外務省サイバー外交担当大使を始めとする両国関係省庁の代表者が出席した。

協議においては、最近のサイバー環境やサイバー分野における両国の施策について意見を交換するとともに、国連の GGE、OEWG の活動等に関する 2 国間連携について討議を行った。

(c)日米安全保障協議委員会

2021 年 3 月 16 日、東京において日米安全保障協議委員会（日米「2 + 2」）が開催され、日本から茂木外務大臣と岸信夫防衛大臣、米国から Antony Blinken 国務長官（Secretary of State of the United States）、Lloyd Austin 国防長官（Secretary of Defense of the United States）が参加した※ 154。同委員会では、中国・北朝鮮情勢に関する地域安全保障及び人権上の懸念と日米豪印 4 ヵ国による連携強化、宇宙・サイバー領域の協力を含む防衛体制強化が議論された。

同委員会は更に 2022 年 1 月 7 日、オンライン形式で開催され、日本からは第 2 次岸田内閣で着任した林芳正外務大臣、岸防衛大臣が出席した※ 155。同会議では、地域安全保障に関しては引き続き中国・北朝鮮対応が最重点となったが、新たにウクライナ情勢の注視が盛り込まれた。また防衛体制については、サイバー領域における自衛隊の体制強化、宇宙における「責任ある行動」の確保に関する両国の連携強化等が議論された。

「責任ある行動」の重視は、国連 GGE や OEWG の活動（サイバー空間における国際法の適用）と連動したものと考えられる。

(d)日米首脳会談

2021 年度は日米首脳会談が 2 回開催された。1 回目は 2021 年 4 月 16 日、ワシントン D.C. にて菅首相と Biden 大統領との会談が行われた※ 156。同会談で、両国は「持続可能な、包摂的で、健康で、グリーンな世界経済の復興」のため、デジタル経済の促進、脱炭素化、健康安全保障等において協力することで合意したほか、「自由で開かれたインド太平洋と包摂的な経済的繁栄の推進」のために同盟を強化するとし、「台湾海峡の平和と安定」を重視することが明記された。

更に 2022 年 1 月 21 日、岸田文雄首相が Biden 大統領とテレビ会談を行った※ 157。同会議では、2021 年 4 月の首脳会談、及び 2022 年 1 月の日米「2+2」会議の合意が再確認されたほか、ウクライナへのロシアの侵攻抑止に関する連携が日米間で初めて言及された。また、経済連携強化のための日米経済政策協議委員会（経済版「2+2」）の設置が合意された。

(e)日 EU 定期首脳協議

2021 年 5 月 27 日、第 27 回日 EU 定期首脳協議がテレビ会議形式で開催された。日本からは菅首相、EU からは Charles Michel 欧州理事会議長（President of the European Council）及び Ursula von der Leyen 欧州委員会委員長（President of the European Commission）が参加した※ 158。

同会議では、新型コロナウイルス終息後の経済復興、高信頼通信インフラの整備、強靭なサプライチェーン構築、安全保障上の観点からの海外投資等、中国の台頭を意識した討議が行われた。

(3)アジア太平洋地域のサイバー連携

アジア太平洋地域における政府レベルの連携施策について述べる。CSIRT に関する連携施策については、「2.2.2 アジア太平洋地域での CSIRT の動向」を参照されたい。

(a)日 ASEAN 首脳会議

2021 年 10 月 27 日、第 24 回日 ASEAN 首脳会議

がオンラインで開催された。Haji Hassanal Bolkiah ブルネイ国王陛下（His Majesty Sultan）が議長を務め、日本からは岸田首相がオンライン形式で参加した※159。岸田首相は「自由で開かれたインド太平洋」の推進を強調し、新型コロナ対策支援、及びASEAN独自の構想「インド太平洋に関するASEANアウトルック」（AOIP：ASEAN Outlook on the Indo-Pacific）の推進等について説明を行った。また、2020年の第23回首脳会議に引き続き、サイバーセキュリティに関する連携強化が議長声明に盛り込まれた。

(b) ASEAN地域フォーラム

ASEAN地域フォーラム（ARF：ASEAN Regional Forum※160）は、ASEAN地域の安全保障環境の向上を目的としたフォーラムで、日本政府は連携を継続している。

サイバーセキュリティに関しては、2021年4月28日、サイバーセキュリティに関する第3回ARF会期間会合がオンライン形式で開催され、日本からは赤堀審議官が参加した※161。同年1月に行われた第6回専門家会合に引き続き、国際的なサイバーセキュリティ環境や各国・地域の取り組み、今後取り組むべき信頼醸成措置について議論が行われた。また、その結果を信頼醸成と予防外交に関する会期間グループ会合（ISG on CBMs and PD）で報告することを確認した。

(c) 日・ASEANサイバーセキュリティ政策会議

2021年10月21日、第14回日・ASEANサイバーセキュリティ政策会議がオンライン形式で開催された※162。議長国は日本、ラオスが務め、日本、ASEANのサイバーセキュリティ・情報通信所管省庁の代表が参加した。同会議では、第13回会議で合意された10項目の協力活動（演習、重要インフラ防護、意識啓発、能力構築、インシデント時情報共有、産学連携等）の状況を確認し、今後の協力を検討した。また、メール等の情報連絡演習や、オンライン会議時のインシデント対応演習等についても活発な意見がかわされた。更に能力構築については、AJCCBCや、次項で述べる「インド太平洋地域向け日米EU産業制御システムサイバーセキュリティウィーク」の研修・演習内容が紹介された。

(d) インド太平洋地域に向けたサイバー演習

日本政府はサイバーセキュリティ能力構築支援の一貫として、インド太平洋地域のサイバー演習を推進している。2021年10月25～29日、経済産業省とIPAは米国政府及び欧州委員会（European Commission）と連携し、インド太平洋地域の重要インフラ事業者、National CSIRT等のIT/OTセキュリティ担当者等を対象に、「インド太平洋地域向け日米EU産業制御システムサイバーセキュリティウィーク」を実施した※163。同演習は、リモートによる模擬プラント操作、日米EUの専門家によるワークショップ・セミナー等により参加者の能力向上を目指す内容である。なお、2021年3月の演習については「3.1.4 (1) 日本政府の取り組み」を参照されたい。

(4) セキュリティ連携に関する国際会議

サイバーセキュリティの国際連携に関する主な会議として、2021年度は、2020年度に引き続き「サイバーセキュリティ国際シンポジウム」「サイバー・イニシアチブ東京」が開催された。

(a) 第11回サイバーセキュリティ国際シンポジウム

本シンポジウムは、サイバー脅威対応に向けた国際間の信頼構築を討議する場として、2016年から日本で開催されている。2021年は慶應義塾大学、大学間の国際連携組織INCS-CoE（InterNational Cyber Security Center of Excellence）、The MITRE Corporation※164の共催の形を取り、10月25～29日にオンラインで開催された※165。米国・英国・オーストラリア・イスラエル大使館及び駐日欧州連合代表部を始め、関係国の省庁が後援し、各国の有識者が参加した。

Global sessionでは、日本政府から平井卓也前デジタル大臣がビデオにより講演し、基調パネルでは、多国間サイバーセキュリティ行動委員会（MCAC：Multilateral Cybersecurity Action Committee）によるナショナルセキュリティにおける国際連携、あるいは相互承認（Mutual Recognition）や信頼性のある自由なデータ流通（DFFT: Data Free Flow with Trust）による社会セキュリティ等がテーマとなり、参加各国の有識者が討議を行った。2020年度に引き続き、産学主導による国際間の信頼構築討議の場となり、政府主導のイベントでありがちな「オープンで自由なサイバー空間」のキャンペーンとは一線を画したものとなった。

(b) サイバー・イニシアチブ東京2021

国内外のセキュリティ・IT専門家を招いたサイバー・イニシアチブ東京2021が、2021年11月29～30日にオンラインで開催された※166。第4回となる同イベントの主

要議題は、社会のデジタル変革におけるセキュリティの実装（デジタル・セキュア社会の実現）とされ、日本政府からは金子恭之総務大臣、萩生田光一経済産業大臣、小田原潔外務副大臣、岸防衛大臣が、台湾政府からはAudrey Tangソーシャルイノベーション担当デジタル大臣（Digital Minister in charge of Social Innovation）が講演したほか、各国の閣僚・有識者が講演・パネル討議に参加した。

また、東京2020オリンピック・パラリンピック競技大会のセキュリティ対策の成果について、坂明デジタル庁CISO（Chief Information Security Officer：最高情報セキュリティ責任者）他の有識者がパネル討議を行ったことも注目された。

2.2.2 アジア太平洋地域でのCSIRTの動向

2021年、ランサムウェアを用いたサイバー攻撃が世界各地で相次ぎ、またEmotetの感染再拡大が確認され、これらの動向はアジア太平洋地域においても深刻な脅威となっている。こうした攻撃による被害拡大を防ぐための対策情報の共有や、被害を受けた後の復旧支援等、インシデント対応連携の窓口となるCSIRTが果たす役割は大きくなっており、各国ではCSIRTの体制や情報連携の強化が進んでいる。本項では、主にアジア太平洋地域におけるCSIRTの設立や機能強化に関する動き、CSIRT間の相互連携の実態について述べる。

(1) CSIRTの設立・機能強化の動き

アジア太平洋地域における各国・地域のCSIRTの機能強化の動きについて述べる。

(a) オーストラリア

2021年4月21日、オーストラリア政府は「国際サイバー・重要技術エンゲージメント戦略（International Cyber and Critical Technology Engagement Strategy）」を発表した※167。本戦略は、オーストラリア、インド太平洋地域及び世界の安全と繁栄を、サイバー空間と重要技術の強化推進によって実現することを目指し策定されたものである。また本戦略は、サイバーと重要技術の諸問題に関して、オーストラリア政府が信頼のおける影響力のあるリーダーとして国際的な評価を得るための戦略的アプローチを示しており、より厳しさを増す国際環境を乗り切るために、サイバー能力の向上及び重要技術の開発や活用を促進するような外交を強化しなければならないと述べている。本戦略における重要技術とは、オーストラリアの繁栄、社会的結束、国家安全保障等の国益を大幅に向上させる、あるいは損なう可能性のある技術と定義されており、人工知能（AI）、5G、IoT、量子コンピューティング、サイバーセキュリティ等が含まれる。サイバーセキュリティに関しては、National CSIRTの機能を担うACSC（Australian Cyber Security Centre）がPaCSON（Pacific Cyber Security Operational Network）やAPCERT（Asia Pacific Computer Emergency Response Team：アジア太平洋コンピュータ緊急対応チーム）等の地域のパートナーと協力し、信頼できるサイバー脅威情報共有ネットワークの構築に取り組んできたことを踏まえて、運用面及び技術面から深刻なサイバーセキュリティの課題に効果的に対処できるよう、ガイダンスや脅威に関するアドバイスを提供していくとしている。また、近隣国であるトンガやバヌアツ、サモア、フィジー、ソロモン諸島のCSIRTやセキュリティ運用センターへのインシデント対応支援を行うことで、地域の集合的なサイバーセキュリティを強化していくとしている。

(b) ニュージーランド

2021年8月16日、ニュージーランド首相内閣府に設置された国家セキュリティグループ（NSG：National Security Group）が「サイバーセキュリティ緊急対応計画（CSERP：Cyber Security Emergency Response Plan）」の第5版を発行した※168。2013年に第1版が発行された後、変化する情勢に応じて、またインシデントからの教訓を反映する形で更新されている。本計画は、サイバーセキュリティに関する緊急事態が起きた際の、政府の対応の枠組みを定めたガイダンスである。緊急を要するインシデントが起きた際は、CERT NZ（Computer Emergency Response Team New Zealand：ニュージーランドコンピュータ緊急対応チーム）及びNCSC（National Cyber Security Centre）がインシデントの重大性を評価し、「深刻」や「重大」等4段階に分類するよう定めている。「深刻」とされたインシデントの場合には、ODESC（Officials Committee for Domestic and External Security Coordination：国内外のセキュリティ調整のための政府委員会）等の設置を含む国家安全保障システムが発動される。「重大」とされたインシデントの場合には、状況に応じてCERT NZ、首相内閣府、NCSC、警察等が、サイバーセキュリティ緊急調整グループを構成して対応にあたることを定めている。

(c)シンガポール

2021年10月5日、National CSIRTであるSingCERT（Singapore Computer Emergency Response Team）を管轄するCSA（Cyber Security Agency：サイバーセキュリティ庁）が「サイバーセキュリティ戦略2021（The Singapore Cybersecurity Strategy 2021）※169」を発表した。同戦略では、「レジリエントなインフラの構築」「より安全なサイバースペースの実現」「国際的なサイバー協力の強化」の三本の戦略的柱を掲げ、それぞれの柱が詳細に述べられている。また、サイバーセキュリティの基礎として「活発なサイバーセキュリティエコシステムの構築」と「強固なサイバー人材供給力の育成」を挙げている。国際的なサイバー協力の強化の項目では、CSIRTネットワークへの積極的な参加と緊密な連携等を通じて、地域及び国際的なパートナーとの多国間協力を強化するとしている。CSAは、毎年ASEANを対象としたサイバーインシデント演習（ACID：ASEAN CERT Incident Drill）を開催し、情報共有メカニズムの強化を行う等、国境を越えたサイバー脅威に立ち向かうために、地域のパートナーとの連携に取り組んでいる。

(d)サモア

2021年5月にSamCERT（Samoa National Computer Emergency Response Team：サモア国家コンピュータ緊急対応チーム）がMCIT（Ministry of Communications and Information Technology：通信情報技術省）の傘下に設立された※170。サイバー攻撃やインシデントに際しては、これまでSMPP（Samoa Ministry of Police and Prisons:サモア警察刑務所省）が報告を受け付け、MCITが支援を行う体制であったが、今後はSamCERTが窓口となってすべてのインシデントに関して報告を受け付け、インシデントが起きた民間企業や非政府組織（NGO：Non-Governmental Organization）、政府機関、及び学術機関と連携して対応するとしている※171。

(e)タイ

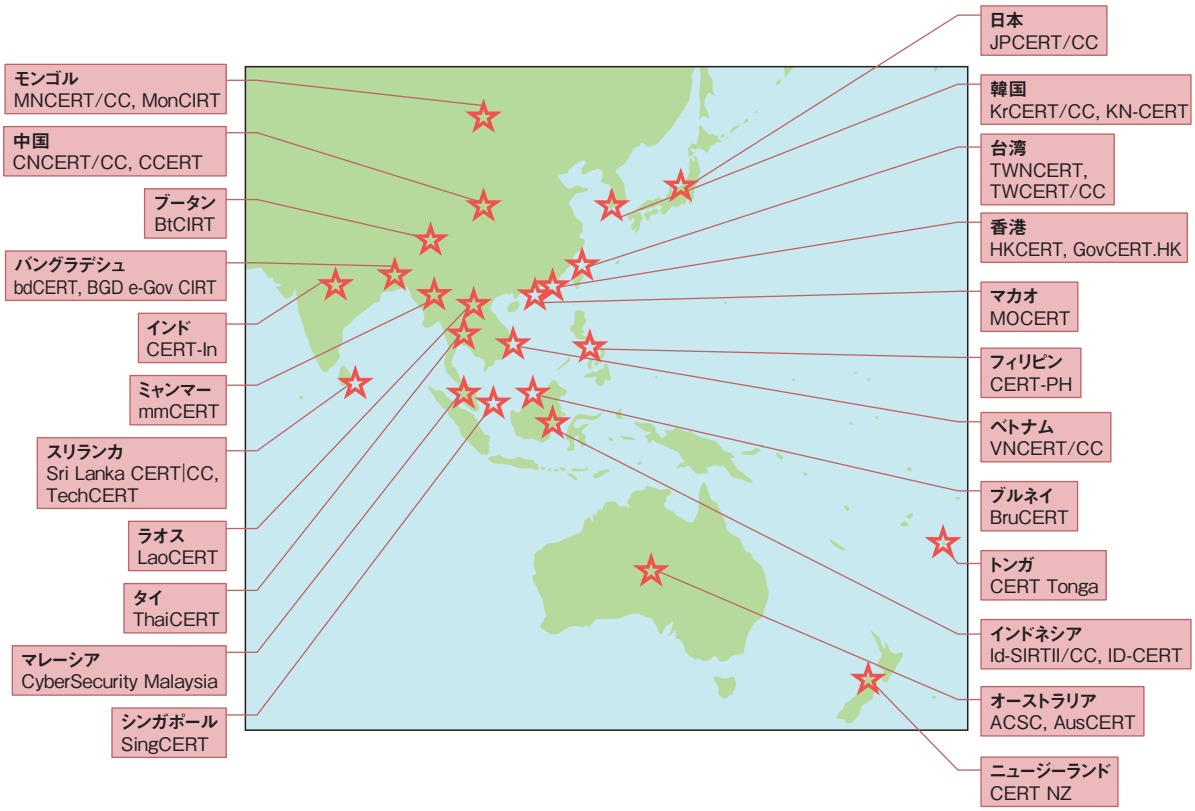
2021年8月18日、タイのMDES（Ministry of Digital Economy and Society:デジタル経済社会省）がNCSA（National Cyber Security Agency：国家サイバーセキュリティ機関）を新設したことを発表した※172。NCSAは、経済及び社会に影響を及ぼす深刻なサイバー脅威に対処する機関として設立され、官民のサイバーセキュリティ関連セクターのセキュリティに関する知識や理解を深め、サイバー脅威の状況認識を高めていくとしている。また、世界中で深刻なサイバー攻撃が増加していることを踏まえ、サイバーセキュリティ能力開発プログラムの提供を通じて、国家安全保障機関、金融、エネルギー、医療分野等を含む七つの主要な重要インフラセクターで働く要員のサイバーセキュリティ能力を高めていく取り組みも行うとしている※173。

(2)アジア太平洋地域のCSIRT間連携

アジア太平洋地域全体のCSIRTからなるコミュニティとして、APCERT（Asia Pacific Computer Emergency Response Team：アジア太平洋コンピュータ緊急対応チーム）※174があり、地域内で発生したインシデント対応における連携の円滑化や、サイバー脅威等に関する情報共有・技術交流の推進を目的に活動している。2003年の設立当初、参加メンバーは12の国・経済地域の15チームだったが、地域内でNational CSIRTの立ち上げが進んだことや、CSIRTコミュニティへの参加を通じた情報共有等の重要性が高まったことから年々メンバーが増え、2022年3月末現在、23の国・経済地域の32チームが、オペレーショナルメンバーとなっている（次ページ図2-2-1）。

JPCERT/CCは、2003年のAPCERT設立当初から事務局を務め、運営委員会の一員として組織運営を支えている。また、JPCERT/CCが主導するネットワーク定点観測共同プロジェクト「TSUBAME」に参加するAPCERTメンバーも多く、APCERT内にワーキンググループを設けて、センサーを用いたサイバー脅威動向の観測や情報共有を推進している。2022年4月末現在、TSUBAMEにはAPCERTメンバーを中心に18の国・経済地域から21チームが参加し、観測結果を共有している※175。

APCERTの主な活動は、年次サイバー演習の実施、及び年次会合の開催であり、年次報告書を公表している。2021年のサイバー演習は、「Supply Chain Attack Through Spear-Phishing - Beware of Working from Home -（スピアフィッシングを発端とするサプライチェーン攻撃）」をテーマに実施された※176。同演習には、APCERTのオペレーショナルメンバーのうち合計19の国・経済地域から25チームが参加した。年次報告書は、APCERT全体の活動に加えて各チームの組織概要や、対応したインシデントの統計等をまとめた文書で、Webサイトで公開されている※177。2021年の年次会合は、新型コロナウイルス感染拡大の影響により、前回に引き



■図 2-2-1　APCERT オペレーショナルメンバー（2022 年 3 月末現在）

続き 9 月にオンライン形式で開催された。マレーシアの CyberSecurity Malaysia[※178] が議長に、中国の CNCERT/CC[※179] が副議長にそれぞれ再選された。また、JPCERT/CC が事務局に再選された。

このほか、APCERT では能力開発の取り組みとして、2014 年以来継続して、電話会議システムを利用して、インシデント対応に関するノウハウを教えるオンライントレーニングを実施している。新型コロナウイルス禍で、対面でのトレーニング開催が困難な中でも、こうしたオンラインで連携する取り組みを継続している。

また、2021 年 10 月には、シンガポールの CSA が立ち上げた ASEAN-Singapore Cybersecurity Centre of Excellence（ASCCE）のキャンパス（活動拠点）が正式にオープンした[※169]。ASCCE は、2019 年に立ち上げられたサイバー能力向上プログラムで、政策及び技術を担当する ASEAN 地域の上級実務者向けにサイバーセキュリティのトレーニング等を提供し、地域のサイバーセキュリティ能力向上の促進や情報連携の強化に取り組んでいる。ASCCE においても、新型コロナウイルス感染拡大の影響により、対面式のキャパシティビルディング（能力向上）等の取り組みが停止したが、状況の変化とニーズに応じてオンライン形式のプログラム提供を行っている。

その他のアジア太平洋地域のサイバーセキュリティ関連イベントの多くが、各国の National CSIRT が主催するカンファレンスを含め、2021 年も前年同様にオンライン形式で実施された。対面の会議や情報交換の機会が制限されている状況下でも、こうした場をとおして CSIRT 間の連携が継続して行われている。

インシデントへの対応を効果的に進めていくためには、諸外国や特に近隣地域との CSIRT 連携が重要となる。CSIRT コミュニティをとおした協力が更に推進されることで、アジア太平洋地域全体のサイバーセキュリティ能力の一層の強化・進展が期待される。

2.3 情報セキュリティ人材の現状と育成

国内のサイバーセキュリティに関わる人材は質的にも量的にも不足しており、人材育成は各界が協力して解決すべき問題である。教育の充実、高度な人材の育成・確保、セキュリティ人材が将来にわたって活躍できる社会環境の整備等、様々な課題が挙げられている。本節では、セキュリティ人材の現状と、産学官における人材育成の取り組みについて述べる。

2.3.1 情報セキュリティ人材の状況

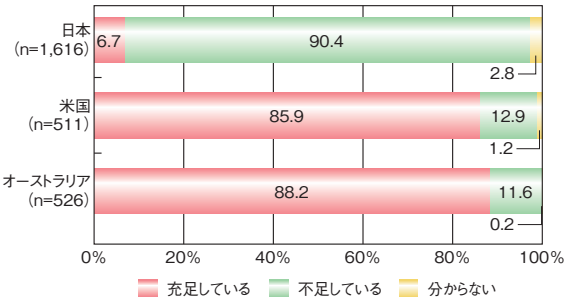
コロナ禍によるテレワークが続き、また、企業におけるDX推進が強く進められるようになってきている。2021年9月に策定された「サイバーセキュリティ戦略」では、セキュリティに関わる人材育成に関して、「DX with Cybersecurityの推進」として「プラス・セキュリティ」知識を補充できる環境整備や「巧妙化・複雑化する脅威への対処」として人材教育プログラムの強化や人材育成共有基盤の構築が盛り込まれた（「2.1.1 (1) 経済社会の活力の向上及び持続的発展～DX with Cybersecurityの推進～」参照）。

情報セキュリティ専門人材への需要は更に伸びるとともに、DX推進によりセキュリティ関連業務を主とする職種以外においてセキュリティ能力を持った人材への需要が高まっている。

(1) セキュリティ人材不足に関する認識

米国（ISC）^{2}（International Information Systems Security Certification Consortium）が発行した「2021 (ISC)^{2} Cybersecurity Workforce Study[※180]」によると、全世界で419万人のセキュリティの専門家がサイバーセキュリティの業務に従事していると推定され、これは前年と比較して70万人以上増加している。また、サイバーセキュリティ人材の不足数は北米、南米、欧州で増加、アジア太平洋地域では減少している。全体としてはサイバーセキュリティ分野の人材不足は2年連続で減少しており、2021年は前年の312万人から272万人に減少しているが、不足数を補うためには世界のサイバーセキュリティ人材を65%増加させる必要があるとし、依然としてセキュリティの人材が不足している状況である。

日米の比較をすると同調査では米国では約38万人、日本では4万人が不足しているとしており、絶対数では日本の方が不足数は低いが、NRIセキュアテクノロジーズ株式会社の「NRI Secure Insight 2021[※181]」では、米国と比較して充足できていない企業が非常に多くなっている（図2-3-1）。その要因として、セキュリティ業務システム化の標準化・自動化が進んでいないことが挙げられる（表2-3-1）。また、DX推進が強く進められている中、



※充足している：「人材が過剰な状態」「充足している（最適な状態）」「どちらかといえば充足している」のいずれかを回答
※不足している：「どちらかといえば不足している」「不足している」のいずれかを回答

■図2-3-1 セキュリティ対策に従事する人材の充足状況
（出典）NRIセキュアテクノロジーズ株式会社「NRI Secure Insight 2021」を基にIPAが編集

	日本 (n=109)	米国 (n=439)	オーストラリア (n=464)
1位	33.9% セキュリティ業務が標準化されており、役割分担が明確化されているため	35.8% セキュリティ業務がシステム等により自動化・省力化されているため	35.3% セキュリティ業務がシステム等により自動化・省力化されているため
2位	32.1% 想定していたほどの有事が少ないため	33.3% セキュリティ業務が標準化されており、役割分担が明確化されているため	32.8% 想定していたほどの有事が少ないため
3位	31.2% セキュリティ業務の量が少ないため	33.0% 想定していたほどの有事が少ないため	31.3% セキュリティ業務は経験豊富な一部のメンバーで対応しているため
4位	19.3% セキュリティ業務は経験豊富な一部のメンバーで対応しているため	31.4% セキュリティ業務の量が少ないため	28.9% セキュリティ業務の量が少ないため
5位	14.7% セキュリティ業務がシステム等により自動化・省力化されているため	29.8% セキュリティ業務は経験豊富な一部のメンバーで対応しているため	21.6% セキュリティ業務を外部委託しているため

■表2-3-1 充足していると考える理由
（出典）NRIセキュアテクノロジーズ株式会社「NRI Secure Insight 2021」を基にIPAが編集

企業で求められるセキュリティに関する業務が変化してきていることも影響している。

(2) セキュリティ業務・役割の広がり

企業でビジネスのIT利用が浸透し、更にDX化が進むにつれて事業部門が自ら様々なITを駆使してビジネス環境を構築することが必要になり、事業部門の中にもITやセキュリティの知識を有する技術者が在籍することが広まりつつある[※182]。

サイバーセキュリティ戦略では、このような状況をとらえて、デジタル化の進展と併せてサイバーセキュリティ確保に向けた取り組みを同時に推進すること（DX with cybersecurity）が盛り込まれた。そして、DXを推進する事業部門の人材を始め、ITやセキュリティの専門知識や業務経験を必ずしも持たない場合にも、セキュリティ専門家と協働できる能力「プラス・セキュリティ」を補充できる環境整備を推進している。

セキュリティに関連する役割・人材を表現する用語について、「サイバーセキュリティ体制構築・人材確保の手引き 第1.1版[※183]」のITSS+（セキュリティ領域）を基に整理すると図2-3-2のようになる。

「戦略マネジメント層」は青枠で示すように、DX推進におけるセキュリティをリードする役割を広く表現しているととらえることができる。「プラス・セキュリティ人材」は緑枠で示すように事業遂行するにあたり、事業部門でセキュリティに関連する業務を担当している役割をセキュリティの観点で表現しているととらえることができる[※184]。「セキュリティ人材」は赤枠で示すように、セキュリティ経営（CISO）、脆弱性診断・ペネトレーション等のセキュリティ対策に関する業務を主とする役割を表現している。特に、その中で中心的な役割を果たすのが「セキュリティ統括」（紫枠）となる。

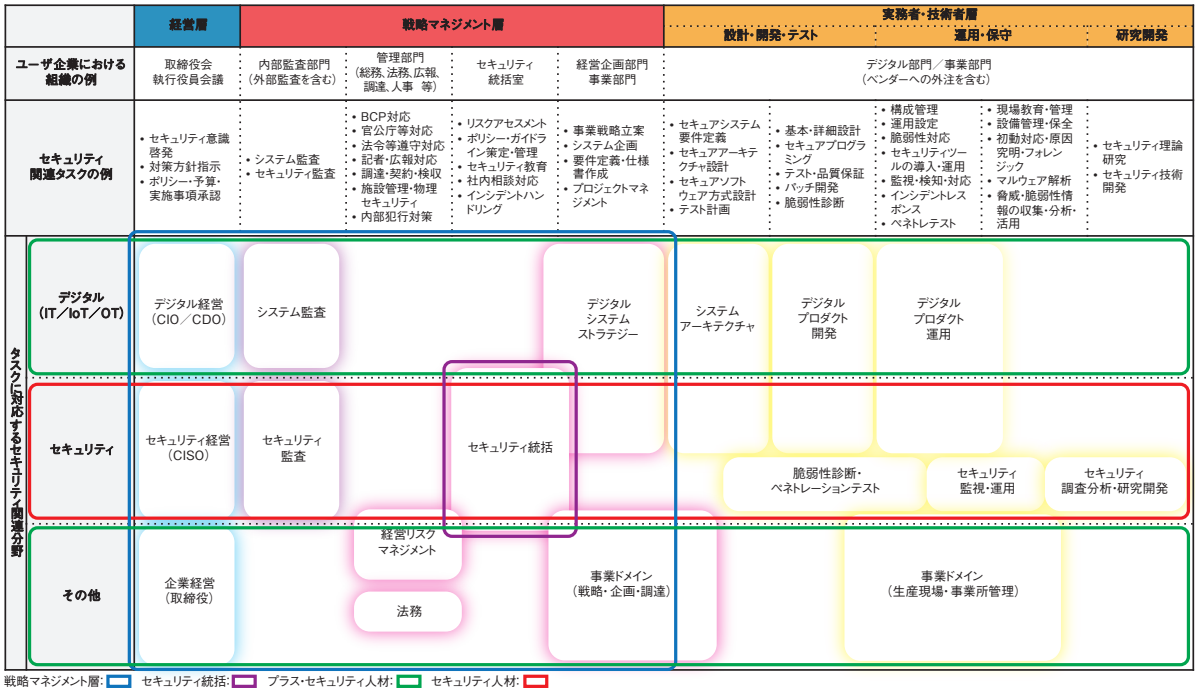
個々の事業責任は推進する事業部門が持っているが、事業で使用するシステム等のセキュリティに関しても、第一義的には事業部門が責任を負う。CISO及び情報システム部門は共通化、標準化すべきインフラ等の整備に加え、事業部門のDX化支援により、企業全体としてのセキュリティ状況を把握し、統括管理する体制に変わりつつある。

企業におけるセキュリティ関連業務が広がっていることを踏まえて、セキュリティ人材育成の取り組みが行われている。

(3) 人材育成の取り組み

経済産業省では人材施策として「サイバーセキュリティ体制構築・人材確保の手引き」（「サイバーセキュリティ経営ガイドライン」付録F）を改訂するとともに、プラス・セキュリティの取り組みを推進するとしている（次ページ図2-3-3）（「2.1.2(1)産業サイバーセキュリティ研究会」参照）。

セキュリティ人材の育成については、中核人材育成プ



■図2-3-2　ITSS+（セキュリティ領域）と人材分類
（出典）経済産業省・IPA「サイバーセキュリティ体制構築・人材確保の手引き 第1.1版」（「サイバーセキュリティ経営ガイドライン」付録F）を基に編集

●昨年度は、「セキュリティ体制構築・人材確保の手引き」の改訂を行うとともに、セキュリティ人材育成の既存施策を進めつつ、特に、セキュリティを本務としない者が自らの業務遂行にあたってセキュリティを意識し、必要かつ十分なセキュリティ対策を実現できる能力を身につける「プラス・セキュリティ」の取組を推進するため、SC3での検討や地域での具体的な取組を推進。

取組の全体像

セキュリティ対策を進めるための体制・人材の考え方

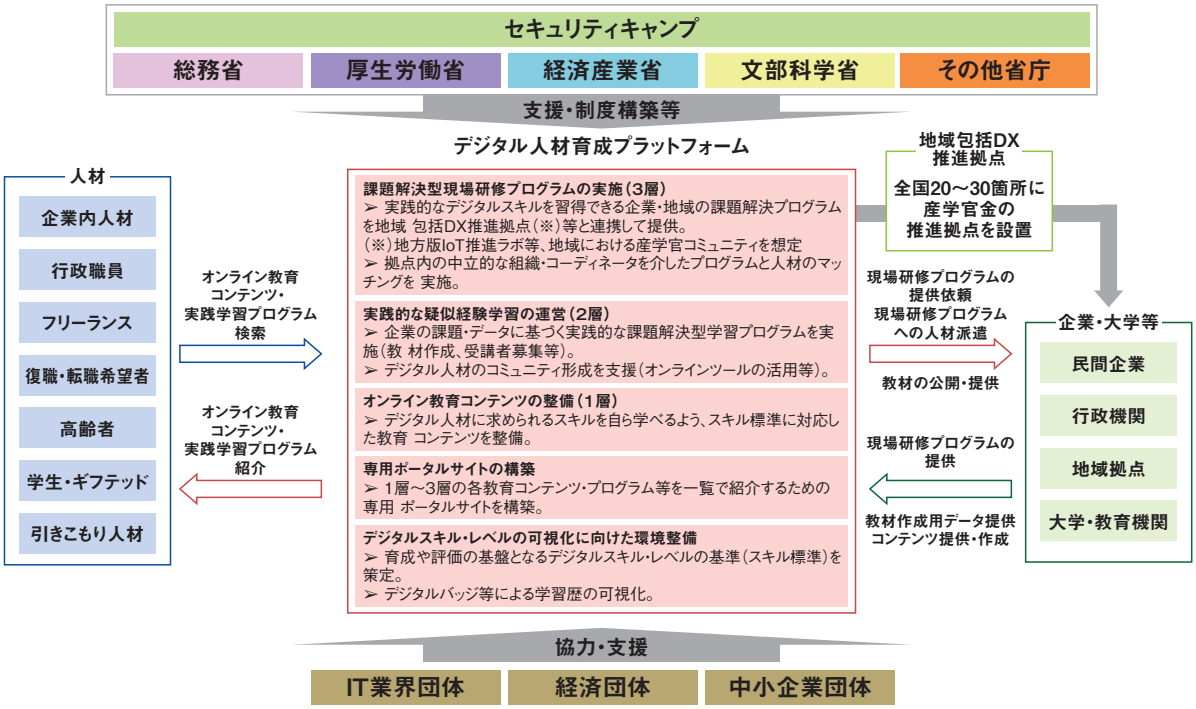
セキュリティ体制構築・人材確保の手引き（「サイバーセキュリティ経営ガイドライン」付録F）

セキュリティ人材の育成	プラス・セキュリティの普及
ICSCoE中核人材育成プログラム	SC3産学官連携WGでのプラス・セキュリティ具体化
情報処理安全確保支援士	NISCにおけるモデルカリキュラム策定
セキュリティキャンプ	地域SECUNITYにおける人材育成
デジタル人材育成プラットフォームにおけるスキル標準の整理・教育コンテンツ・実践型教育	
大学・高専等と産業界の連携	

今後の方向性

●手引きの普及による各企業での体制構築の促進と各種セキュリティ人材育成施策を引き続き実施するとともに、プラス・セキュリティの取組を普及させるため、SC3産学官連携WG、デジタル人材育成プラットフォーム、各地域における産学官連携の取組（地域SECUNITY）との連携による取組の具体化・拡大を進めていく。

■図 2-3-3　サイバーセキュリティ人材施策の全体像
（出典）経済産業省「第７回 産業サイバーセキュリティ研究会 事務局説明資料※185」（資料３）



■図 2-3-4　デジタル人材育成プラットフォーム 概要イメージ
（出典）経済産業省「実践的な学びの場ワーキンググループ活動結果報告※187」（第５回 デジタル時代の人材政策に関する検討会 資料 3-1）を基に IPA が編集

ログラム（「2.3.2（1）中核人材育成プログラム」参照）、セキュリティ・キャンプ（「2.3.4（1）セキュリティ・キャンプ」参照）等の活動が既に実施され継続されている。また、プラス・セキュリティの普及については、NISCにより、経営層・部課長級向けの知識補充のモデルカリキュラム策定等が実施されてきた※186。

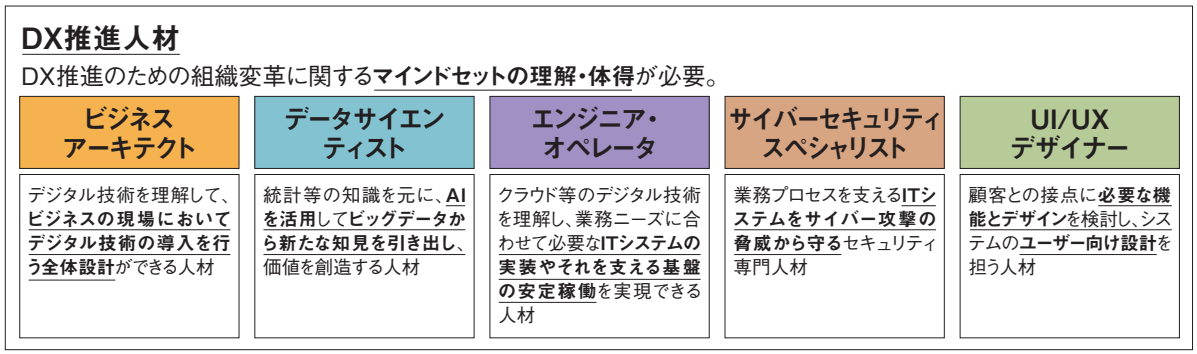
それらに加えて、SC3産学官連携WGにおいて、産学官間でのセキュリティ人材育成をいかに行うべきかの検討が進められている（後述）。また、セキュリティ人材、プラス・セキュリティ人材の基盤として活用可能なプラットフォームとして、「デジタル人材育成プラットフォーム」の構築に向けての検討が進められている。

(a) デジタル人材育成プラットフォーム

本プラットフォームは、ビジネスに求められるデジタルリテラシーとデジタル専門知識の学習機会を提供し、DXを推進できる実践的なDX推進人材の育成手法を確立することを目標としている（前ページ図2-3-4）。

育成するDX推進人材像（仮説）として図2-3-5に示す五つが想定されており、サイバーセキュリティスペシャリストとしてセキュリティ専門人材も含まれている。

プラットフォームで提供される教育コンテンツの整備並

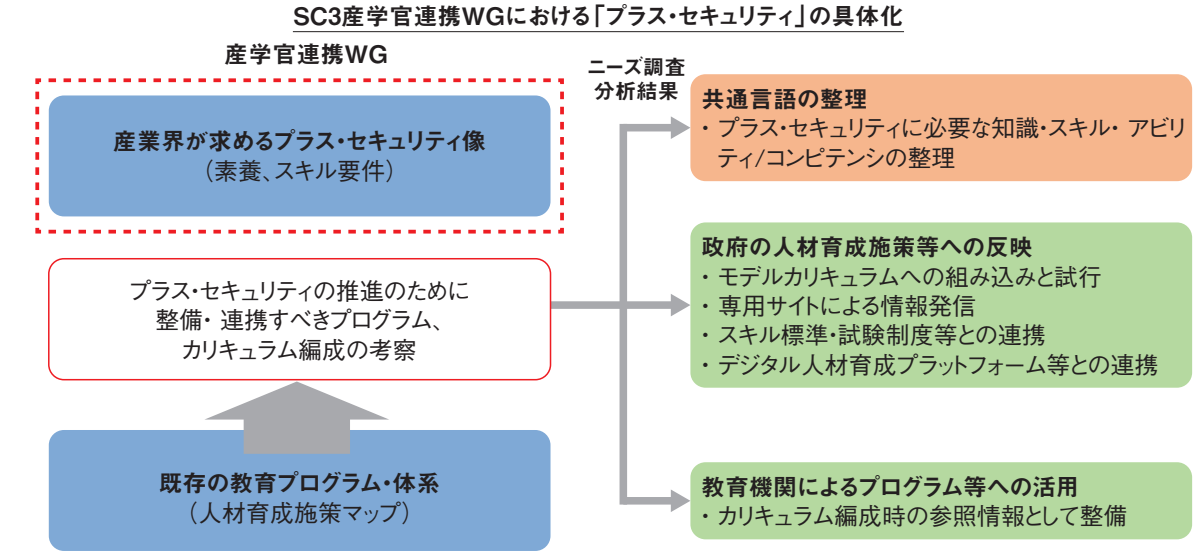


■図2-3-5　DXを進める企業等におけるビジネスパーソンの人材像（仮説）
（出典）経済産業省「実践的な学びの場ワーキンググループ活動結果報告」（第5回 デジタル時代の人材政策に関する検討会 資料3-1）を基にIPAが編集

プラス・セキュリティの普及促進

プラス・セキュリティ

- **プラス・セキュリティ＝（セキュリティが本務ではないが）自らの業務遂行にあたってセキュリティを意識し、必要かつ十分なセキュリティ対策を実現できる能力を身につけること、あるいは身につけている状態のこと。**
- プラス・セキュリティの取組普及のため、SC3産学官連携WGにおいて必要なスキルの整理等が行われているほか、NISCにおいても「プラス・セキュリティ」のモデルカリキュラムの策定や官民のコンテンツのポータルサイトへの掲載などを実施中。デジタル人材育成プラットフォーム事業等の関連施策とも連携し、取組を普及させていく。



■図2-3-6　SC3産学官連携WG「プラス・セキュリティの普及促進」
（出典）経済産業省「事務局説明資料※189」（第8回 産業サイバーセキュリティ研究会 ワーキンググループ2（経営・人材・国際）資料3）

びに教育コンテンツが提供する具体的な学習項目については、DX リテラシー標準として今後検討される。

経済産業省と IPA は、デジタル人材の育成を推進するため、デジタル知識・能力を身に付けるための実践的な学びの場として、デジタル人材育成プラットフォームポータルサイト「マナビ DX（デラックス）」を 2022 年 3 月に開設した※188。ポータルサイトでは、デジタルスキルを学ぶことができる学習コンテンツを紹介するとともに、すべての社会人が身に付けるべきデジタルスキルを示した「DX リテラシー標準」も掲載しており、これまでデジタルスキルを学ぶ機会がなかった人にも新たな学習を始めるきっかけとなることが期待される。

(b) SC3 産学官連携 WG

SC3 産学官連携 WG では、プラス・セキュリティ人材育成の具体化として、産業界が求めるプラス・セキュリティ像と既存の教育プログラム・体系の摺り合わせを行うとしている（前ページ図 2-3-6）。

現時点では、プラス・セキュリティ向けの教育カリキュラムは整備されておらず、SC3 産学官連携 WG ではそれらのセキュリティ教育プログラムで身に付けるべき知識・スキル及びその他の能力を明確にし、共通化する作業も行うとしている。

今後、教育機関、教育ベンダ等がプラス・セキュリティに関する人材育成として具体的な教育プログラムを整備することが期待される。

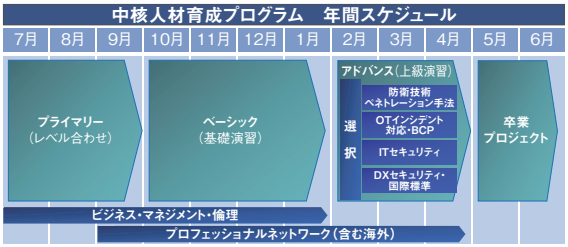
2.3.2 産業サイバーセキュリティセンター

我が国の経済・社会を支える重要インフラ※190 や産業基盤のサイバー攻撃に対する防御力を強化するため、IPA は 2017 年 4 月に産業サイバーセキュリティセンター（ICSCoE：Industrial Cyber Security Center of Excellence）を発足させた。

ICSCoE は、重要インフラや産業基盤のサイバーセキュリティリスクに対応する人材・組織・システム・技術を生み出していくため、「人材育成事業」「制御システムの安全性・信頼性検証事業」「攻撃情報の調査・分析事業」の三つを事業の柱としている。本項では、「人材育成事業」について述べる。

(1) 中核人材育成プログラム

ICSCoE は、2017 年 7 月、制御技術（OT：Operational Technology）と情報技術（IT）、マネジメント、ビジネス分野を総合的に学び、サイバーセキュリティ対策の中核となる人材を育成する「中核人材育成プログラム」を開始した。本プログラムでは、OT 及び IT 知識のレベル合わせからハイレベルな演習までを 1 年間のフルタイムで実施する（図 2-3-7）。第 1 期は 76 名、第 2 期は 83 名、第 3 期は 69 名、第 4 期は 47 名が参加し、2021 年 7 月に開講した第 5 期では、電力・鉄鋼・石油・化学・自動車・鉄道・放送・通信・産業ベンダ等の幅広い業界から 48 名が参加した。



■図 2-3-7　第 5 期中核人材育成プログラムの年間スケジュール

カリキュラムは OT 分野の「防衛技術・ペネトレーション手法」（制御システム固有のセキュリティリスク、攻撃に対する防御技術の理解等）、「OT インシデント対応・BCP」（安全性と事業継続性を両立する OT インシデント対応、制御システム BCP 対応の演習等）、IT 分野の「IT セキュリティ」（制御システムセキュリティ実現のための IT 設計、IT インシデント対応、体制整備等）の 3 領域を基軸として、ビジネスマネジメントに関する実務家による講義や米国・欧州等の先進事例を学ぶ海外派遣演習等を含む構成となっている。

2021 年 10 月には米国政府・EU と連携した制御システムのサイバーセキュリティ対策に関するキャパシティビルディングプログラム「インド太平洋地域向け日米 EU 産業制御システムサイバーセキュリティウィーク※191」を経済産業省と共催した（「2.2.1 (3) (d) インド太平洋地域に向けたサイバー演習」参照）。本演習には第 5 期の受講者及びインド太平洋地域から招聘した外国人受講者 40 名がオンラインで参加し、米国、EU 及び日本の専門家によるエネルギー分野を含むサイバーセキュリティに関するワークショップ、リモートでのハンズオン演習等を実施した。

同年 12 月の海外派遣演習では、英国政府によるサイバーセキュリティ政策の紹介や英国企業によるサプライチェーンサイバーセキュリティについてのケーススタディ等をオンラインで実施した。2022 年 2 月には、2017 年 5 月に合意された「日イスラエル・イノベーション・パートナシップ」等に基づき、イスラエルのテルアビブ大学やイスラエ

ル国家サイバー総局によるサイバーセキュリティ対策に関する講義をオンラインで実施した。

2022 年 5 月の海外派遣演習では、フランスを訪問し、サイバーセキュリティの国際標準や先進的な取り組みの理解、現地トップレベル機関の人材とのネットワーク構築を目的に学術研究機関や産学官連携による研究施設の講義を受講し、自動運転等の模擬システムを見学した。

2018 年 7 月、中核人材育成プログラムの修了者コミュニティとして「叶会※192」が発足し、2019 年夏以降、本プログラムを通じて培った人脈の活用、知見やノウハウの共有を目指し、地域活動や技術をテーマにする複数の部会が設置された。また修了年次をまたがる縦のつながりの形成、最新情報及びノウハウ収集を目的とした叶会総会の第 4 回が 2021 年 11 月に開催された。叶会には第 1 期から第 4 期までの修了者に加え、2022 年 6 月に修了した第 5 期生も参加しており、今後もコミュニティとしての規模を拡大しながら、お互いの顔が見える縦横の人的つながりを形成し、産業サイバーセキュリティに関する適時、適切な情報共有活動を継続することが期待される。

なお、同プログラムの修了者は、「情報処理の促進に関する法律」の規定に基づき、後述する情報処理安全確保支援士試験の全部免除を受けることができる※193。

(2) 短期プログラム

ICSCoE では、セキュリティに関連するスキルの習得機会が充分でない部門責任者や現場責任者、及びセキュリティ実務担当者に向けて、数日間で学ぶ短期演習形式の「サイバー危機対応机上演習（CyberCREST）」「業界別サイバーレジリエンス強化演習（CyberREX）」「戦略マネジメント系セミナー」「制御システム向けサイバーセキュリティ演習」及び「ERAB サイバーセキュリティトレーニング」を提供している。対面形式での実施のほか、新型コロナウイルス対策の一環として、オンライン形式、または対面とオンラインを併用したハイブリッド形式での実施とした。

(a) サイバー危機対応机上演習（CyberCREST）

「サイバー危機対応机上演習（CyberCREST：Cyber Crisis RESponse Table top exercise）※194」は、制御システムを有する企業・団体においてサイバーセキュリティ対策を統括する責任者やセキュリティ・オペレーション・センター（SOC）の責任者、サイバーセキュリティ対策部門の管理職を対象にしたプログラムである。

2021 年 9 月に本演習をオンライン（ライブ配信）で実施した。本演習では、組織を守るために必要なスキルとメソッドを身に付けるため、最新のサイバー脅威の動向や米国の先進的なサイバーセキュリティ戦略である「コレクティブ・ディフェンス」、近年重要性が説かれている「任務保証」等について、米国サイバーコマンド出身の専門家や CISO、セキュリティアーキテクト等が講師となって講演、講義及びロールプレイング演習を行った。受講者からは、多種多様な経験を積んできた講師陣の話をリアルタイムの対話形式で聴くことができたことは有益であった、との反応があった。

(b) 業界別サイバーレジリエンス強化演習（CyberREX）

「業界別サイバーレジリエンス強化演習（CyberREX：Cyber Resilience Enhancement eXercise by industry）※195」は、電力、鉄道、ビル、ガス、金属、石油・化学、自動車（製造）、ファクトリーオートメーション業界において、CISO に相当する役割を担う人材や IT 部門、生産部門等の責任者・マネージャークラスの人材を対象としたプログラムである。

2021 年 10 月にはオンライン（ライブ配信）で、11 月には大阪で本演習を実施した。本演習は、部署・部門のサイバーセキュリティに関するインシデント対応力・回復力を強化するため、仮想企業を想定し、業界の最新動向、業界別に考慮すべきセキュリティ要件、安全性要件を織り込んだシナリオ形式による実践演習を中心に進められた。受講者に加え、サイバーセキュリティの専門家や監督省庁の関係者も参加し、グループ演習を行った。受講者からは、実務で起こりうる事例がシナリオで挙げられており興味深い、外部組織との連携や事業への影響等、高い視座でインシデントを見ることができ有意義であったとの反応があった。

(c) 戦略マネジメント系セミナー

「戦略マネジメント系セミナー※196」は、経営層を補佐し、実務者・技術者を指揮することでセキュリティ対策を進める戦略マネジメント層、及び今後戦略マネジメント層になることが期待される層を対象としたプログラムである。

2022 年 1 月から 2 月にかけて、本セミナーを対面（東京）とオンラインのハイブリッド形式で実施した。本セミナーは、ビジネスのデジタル化・DX 推進に伴うリスクの変化に対応して、セキュリティ対策を組織横断的に統括できる責任者を育成することを目的としている。具体的には、政府の動向やサイバーセキュリティの事故や対策につい

ての先進事例の講演、責任者の役割等を理解するための講義のほか、事例を用いてインシデント発生時に必要な意思決定における課題を発見し、対策ガイドを作成するために、グループワーク（ディスカッション）を行った。受講者からは、どのような視点で経営層と現場をつなげばいいかが理解できた、他社の方と意見交換することで自分の中にはなかった視点を学べたとの反応があった。

(d) 制御システム向けサイバーセキュリティ演習

「制御システム向けサイバーセキュリティ演習[※197]」は、制御システムのサイバーセキュリティを担当する、または今後担当予定の技術者を対象としたプログラムである。

2022 年 2 月に福岡で本演習を実施した。本演習は制御システムのサイバーセキュリティを理解するための導入的な演習に位置付けられ、制御システムの攻撃手法、及び制御システムのサイバーセキュリティ対策の基礎を、簡易模擬システムを用いた実機演習（ハンズオン演習）で体験し、制御システムのセキュリティについて実践的に理解することを目的としている。受講者からは、ハンズオン研修は身に付きやすいと感じた、OT-IT 連携の重要性について腹落ちしたとの反応があった。

(e) ERAB サイバーセキュリティトレーニング

「ERAB サイバーセキュリティトレーニング[※198]」は、電力小売事業に関わる ERAB（Energy Resource Aggregation Business）事業者において、セキュリティ対策を検討し、立案・実施する実務者及び対策の導入・実施を判断する責任者を対象としたプログラムである。

2022 年 2 月にはオンライン（ライブ配信）で、3 月には東京で本トレーニングを実施した。本トレーニングは、経済産業省の「エネルギー・リソース・アグリゲーション・ビジネスに関するサイバーセキュリティガイドライン Ver2.0[※199]」における ERAB 事業者に求められるサイバーセキュリティ対策に関する学習を目的としている。具体的には、本ガイドラインの解説やリスク分析・対策事例の解説やグループワーク、実機を用いた実演（デモ）を中心とした演習を実施した。受講者からは具体的なデモを目の当たりにすることでリスクや事象についてイメージを持つことができた、実機を用いて不正アクセス・制御が実施できることを理解でき対策の必要性を実感できたとの反応があった。

2.3.3 情報セキュリティ人材育成のための国家試験、国家資格制度

本項では、情報セキュリティ人材の育成や確保を目的とした国家試験や国家資格制度に関する動向を紹介する。

(1) 情報セキュリティマネジメント試験

企業・組織においては、組織が定めた情報セキュリティポリシーを部門内に周知して遵守を促し、部門の情報管理を実施する等、情報セキュリティ対策を推進する人材（情報セキュリティマネジメント人材）が必須である。こうした人材を育成するために、2016 年度春期より「情報処理技術者試験」の新たな試験区分として「情報セキュリティマネジメント試験」が実施されている。2019 年度までは、試験を筆記方式で年 2 回実施していたが、2020 年度から CBT（Computer Based Testing）方式[※200]に移行した。CBT 方式への移行により、受験者は、自身で試験日、試験会場を選択することが可能となった。2021 年度は、CBT 方式による試験が年 2 回（上期 7 月 1 ～ 31 日、下期 12 月 1 ～ 26 日）実施され、応募者数 3 万 1,672 人（前年比約 3.3 倍）、合格者数 1 万 5,325 人（前年比約 2.5 倍）であった[※201]。2022 年度も CBT 方式での実施を継続する。

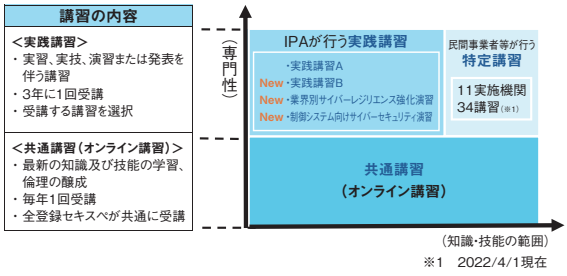
(2) 情報処理安全確保支援士制度

サイバー攻撃の増加・高度化に加え、社会全般に IT が広く普及・活用されていることから、企業・組織におけるサイバーセキュリティ対策の重要性が高まっている。それに伴い、企業・組織での安全なセキュリティ対策を高度なスキルを活かして推進できる人材が求められている。

そこで、最新の知識・技能を備え、サイバーセキュリティ対策を推進する人材の育成と確保を目指し、2016 年 10 月に「情報処理の促進に関する法律」の改正法が施行され、国家資格「情報処理安全確保支援士」制度が創設された。

情報処理安全確保支援士（以下、登録セキスペ）はサイバーセキュリティ分野初の国家資格であり、情報処理安全確保支援士試験合格者等が登録申請後、登録簿に登録されることにより資格を取得できる。試験は年 2 回実施され、2021 年度は応募者数 3 万 2,627 人、合格者数 4,665 人であった[※201]。登録セキスペは 2022 年 4 月 1 日時点で 2 万 253 人[※202]となった。

登録セキスペには、法定講習の受講と、3 年に 1 度



■図 2-3-8 法定講習の全体像
(出典)IPA「情報処理安全確保支援士(登録セキスペ)の受講する講習について※203」

の登録更新が義務付けられている※203。

法定講習の全体像を図 2-3-8 に示す。

「共通講習(オンライン講習)」は、登録セキスペとして期待される情報セキュリティ実践のために必要な知識・技能・倫理について学習することを目的として、すべての登録セキスペが毎年 1 回受講する。

「実践講習」は、実習、実技、演習または発表等を通じて具体的な技術や手法を学ぶことを目的として、3 年に 1 回「IPA が行う実践講習」あるいは「民間事業者等が行う特定講習」から任意の講習を選択して受講する。

「IPA が行う実践講習」のうち「実践講習 A」は主に登録後 3 年目までの登録セキスペを対象とし、情報セキュリティインシデント対応等の演習を通じて情報セキュリティ実践のための具体的な技術や手法を習得することができる。Web 会議ツールを活用したオンライン形式で実施し、2021 年度は全国より 3,016 名が受講した。更に、2022 年 3 月より、主に登録後 4 年目以降の登録セキスペを対象とし、新規事業を立ち上げる際のセキュリティ上の助言を検討する「実践講習 B」を開始した。また専門的な分野の知識・技術修得を望む登録セキスペを対象として、「業界別サイバーレジリエンス強化演習(CyberREX)」と「制御システム向けサイバーセキュリティ演習」が追加され、より選択肢が広がった(演習内容については「2.3.2(2)(b)業界別サイバーレジリエンス強化演習(CyberREX)」「2.3.2 (2)(d) 制御システム向けサイバーセキュリティ演習」参照)。

「民間事業者等が行う特定講習」は、「IPA が行う実践講習」と同等以上の効果を有する講習として経済産業大臣が定める講習※204 であり、2022 年度は、11 実施機関 34 講習が経済産業省より特定講習として定められている。

なお登録セキスペの利便性向上等を目的とし、2021 年度に登録セキスペ専用の「情報処理安全確保支援士ポータルサイト」を開設し、「共通講習(オンライン講習)」受講、資格更新オンライン申請、その他登録セキスペの業務に役立つ情報の掲載等も開始された。

情報処理安全確保支援士制度全体に対して、登録セキスペからは「国家資格保持者である登録セキスペとなることで、単なる情報部門の公務員ではなく、信頼できる情報技術の専門家とみなされるようになった」(地方自治体所属)、「情報処理安全確保支援士の講習で得られる最新の知識・スキルが業務で役立つ重要なツールになっている」(IT ベンダ企業所属)、等の声が聞かれ、今後一層、企業・組織のセキュリティ対策推進に登録セキスペの活躍が期待され、大きな役割を果たしていくと考えられる。

2.3.4 情報セキュリティ人材育成のための活動

情報セキュリティに関する情報共有や情報セキュリティ人材育成の場として、様々なイベントが開催されている。また、複数の大学と産業界がネットワークを形成し、セキュリティ分野の人材を育成する事業が行われている。

(1) セキュリティ・キャンプ

「セキュリティ・キャンプ」は、若年層の情報セキュリティ意識の向上、並びに将来第一線で活躍できる高度な情報セキュリティ人材を発掘・育成する場として、一般社団法人セキュリティ・キャンプ協議会と IPA により運営されている。本項では、一般社団法人セキュリティ・キャンプ協議会と IPA が開催しているプログラム・イベントについて紹介する。

(a) セキュリティ・キャンプ全国大会

年 1 回、主に夏休み期間中に 4 泊 5 日の合宿形式の勉強会としてセキュリティ・キャンプのメインイベントである「セキュリティ・キャンプ全国大会」(以下、全国大会)が実施されてきた。18 回目となる 2021 年度の「全国大会 2021 オンライン」は、2020 年に引き続き新型コロナウイルス感染防止のためオンライン形式による開催となった。過去 3 番目の多さとなる 317 名の応募があり、選考を通過した 81 名が参加した※205。

(b) セキュリティ・ネクストキャンプ

過去の全国大会を修了した、または同等以上のスキルを持つ 25 歳以下の学生等を対象に、さらなる育成の場として「セキュリティ・ネクストキャンプ 2021 オンライン」が全国大会と同時にオンライン形式で開催された。3 回

目の開催となる本プログラムでは選考を通過した 10 名が参加した※206。

(c) セキュリティ・キャンプ地方大会（セキュリティ・ミニキャンプ）

これまで地方において小規模で開催してきた「セキュリティ・ミニキャンプ」も、2020 年に引き続き一部オンライン形式を取り入れて開催された※207。

参加資格を限定しない一般講座は山梨（2021 年 9 月）、広島（2021 年 11 月）、大阪（2022 年 3 月）にて開催し、最新のサイバーセキュリティ脅威の動向や対応策、これからの IT 人材のキャリア等をテーマに、産学官の有識者による講演やディスカッションが行われた※208。

また、2021 年 10 ～ 11 月に行われた「セキュリティ・ミニキャンプ オンライン 2021」は、従来のミニキャンプの特徴を踏襲しつつ、地域ごとのグループによる助け合いと、グループワークによる盛んな交流を取り入れて開催された※207。参加者は、25 歳以下の学生・生徒・児童で、北海道、東北、関東、中部、近畿、中国、四国、九州、沖縄の地域ごとに 4 名程度を選考して実施された。

(d) セキュリティ・キャンプフォーラム 2022

セキュリティ・キャンプ修了生相互の年度を超えた交流と意見交換の場の提供、及び同修了生の認知度向上と現在の活動状況紹介による産業界での活動の機会提供の 2 点を目的として 2022 年 3 月に「セキュリティ・キャンプフォーラム 2022」が開催された。本フォーラムでは講師、チューター、修了生がパネリストとなり、「プログラミングの教育者になるとしたら、何から教えるか」をテーマにパネルディスカッションや修了生による講演が行われた。また、フォーラム終了後には「セキュリティ・キャンプ交流会 2022 春オンライン」が開催され、LT（Lightning Talk）会等、セキュリティ・キャンプ修了生同士の交流が行われた。

(e) Global Cybersecurity Camp

「Global Cybersecurity Camp（GCC）」は「国籍・人種を超えた専門知識のあるグローバル人材の育成」と「国境を超えた友情とゆるやかなコミュニティの形成」を目的として、セキュリティに興味を持つ 25 歳以下の若者がともに学び、友好を深める場として 2018 年度から日本を含むアジア太平洋地域 8 ヵ国の関連団体・大学により開催されている。4 回目となる 2021 年度の「GCC 2022 Taiwan」は台湾で開催され、日本からも選考を通過した数名が参加した※209。

(f) Asian Cyber Security Challenge

「Asian Cyber Security Challenge（ACSC）」はアジアトップの Capture The Flag（CTF）プレイヤーを選出するための CTF 大会である。2021 年 1 月 1 日時点で 25 歳以下のアジア圏在住者を対象とし、成績優秀者はアジア代表チームとして「International Cybersecurity Challenge（ICC）」に参加できる。ファイナリストには 3 名の日本人※210 が選ばれ、2022 年 6 月※211 に開催される ICC にアジア代表のチームメンバーとして参加が予定されている。

(2) enPiT

「enPiT（Education Network for Practical Information Technologies：成長分野を支える情報技術人材の育成拠点の形成）」は、情報技術を高度に活用して社会の具体的な課題を解決できる人材を育成するために、2012 年 4 月から開始された文部科学省の事業である。産学協働の教育ネットワークを形成し、PBL（Problem Based Learning：課題解決型学習）等の実践的な教育を推進・普及することを目的としている。2021 年度 4 月以降は、セキュリティを含む 4 分野において大学により自主展開されている※212。本項では、セキュリティ分野で提供されている三つのプログラムについて紹介する。

(a) SecCap

2012 ～ 2016 年度までは大学院生を対象とした事業「第 1 期 enPiT」が実施された。この活動を継承した教育プログラム「enPiT1」のセキュリティ分野では、五つの大学※213（情報セキュリティ大学院大学、北陸先端科学技術大学院大学、奈良先端科学技術大学院大学、慶應義塾大学、東北大学）が協力して開講する実践セキュリティ人材育成コース「SecCap」が設けられ、産業界が求める「セキュリティ実践力のある IT 人材」を育成するプログラムとなっている。

(b) Basic SecCap

「第 1 期 enPiT」を踏まえて 2016 年度から、学部生を対象とした「第 2 期 enPiT」（以下、enPiT2）が実施されている。enPiT2 は、ビッグデータ・AI、セキュリティ、組み込みシステム、ビジネスシステムデザインの 4 分野を対象として教育プログラムを提供している。enPiT2 のセ

キュリティ分野では、14の大学※214が協力して開講する情報セキュリティ分野の実践的人材育成コース「Basic SecCap」が設けられ、幅広いセキュリティ分野の最新技術や知識を取得可能なプログラムとなっている※215。

(c) enPiT Pro Security

「enPiT Pro Security（情報セキュリティプロ人材育成短期集中プログラム）」は、情報セキュリティ大学院大学、東北大学、大阪大学、和歌山大学、九州大学、慶應義塾大学、長崎県立大学の7大学院※216が連携し、文部科学省「情報セキュリティ人材育成に関する調査研究」で提唱されたモデル・コア・プログラムに基づき、社会人の学び直しを支援する高等教育の体制を整え、様々な分野で活躍する情報セキュリティ分野のリーダー人材を育成する短期集中プログラムである。数学・アルゴリズム・暗号理論等のセキュリティの基盤技術から、サイバーセキュリティ・リスクマネジメント・法制度・暗号技術の応用・ビットコイン・ブロックチェーン・IoT等の最新技術までを幅広くカバーしており、社会システムにセキュリティ技術を安全に適用できる知識の獲得を目的としている※217。

(3) SECCON

「SECCON」（SECURITY CONTEST）は、情報セキュリティをテーマに多様な競技を開催する情報セキュリティコンテストイベントとして、特定非営利活動法人日本ネットワークセキュリティ協会（JNSA：Japan Network Security Association）内のSECCON実行委員会により運営されている※218。本イベントは、世界の情報セキュリティ分野で通用する実践的情報セキュリティ人材の発掘・育成を目的とし、日本の情報セキュリティレベルを世界トップレベルに引き上げることを目標としている。競技種目としては、CTFが採用されている※219。本項では、SECCON実行委員会が開催している三つのイベントについて紹介する。

(a) SECCON CTF 2021

世界各国のセキュリティ専門家がCTFの技量を競う「SECCON CTF 2021」は、2021年12月11～12日にオンライン形式で開催され、世界各国から506のチームが参加し、そのうち日本からは312のチームが参加した※220。

その他、コンテストの結果発表やワークショップを行うイベントとして「SECCON 2021 電脳会議」が同年12月18日に開催された※221。

(b) SECCON Beginners CTF

若手のCTFプレイヤーにより運営されている「SECCON Beginners」は、日本国内のCTF参加者を増やし、セキュリティ人材の底上げすることを目的とした勉強会である。CTF初心者・中級者を対象とした「SECCON Beginners CTF」をオンライン形式で2021年5月22～23日に開催した※222。

(c) CTF for GIRLS

「CTF for GIRLS」は、情報セキュリティ技術に興味がある女性（女性と自認されている方を含む）を対象に、気軽に技術的な質問や何気ない悩みを話し合うことができるコミュニティを作ることを目的とした団体である。コミュニティ形成の一環として、2021年6月30日にはExploit※223、2021年9月22日にはフォレンジック※224、2021年12月22日にはWebセキュリティ※225に焦点を当てたワークショップが開催された。

(4) 産学情報セキュリティ人材育成交流会

「産学情報セキュリティ人材育成交流会」は、今後の情報セキュリティ業界を支える人材育成を目的としたJNSAのインターンシップ支援活動である。将来情報セキュリティ業界で活躍したいと考える学生に対し、本交流会を介して2021年度は8社の企業がインターンシップを実施した※226。

(5) サイバーセキュリティ経営戦略コース

東京工業大学社会人アカデミーでは2021年11月11日、MOT（Management of Technology：技術経営）に関する社会人向けプログラムとして「キャリアアップMOT『サイバーセキュリティ経営戦略コース』」を開講した。本コースは2020年に引き続きオンライン講義形式となった。

本コースでは、サイバーセキュリティが企業・組織の経営に及ぼす影響を理解し、サイバーセキュリティ経営及びその戦略立案に求められる知識・能力を備え、企業・組織を先導する人材の育成を目指しており、経営企画、CISO相当業務等の実務者、サイバーセキュリティ経営を学びたい方等、多様な立場の社会人の受講を想定している。本コースは、週1回、産学官の有識者による関連技術・法制・世界情勢等の解説や、事例に基づく演習、討議等を含む全18回の講義で構成される※227。

(6) KOSEN Security Educational Community

「KOSEN Security Educational Community（K-SEC）」は、サイバーセキュリティ専門技術者として必要となる高度な技術を持つ人材だけでなく、工学分野（機械・建築・土木・電気／電子・材料・生命等）の技術者が持つべきセキュリティ技術を身に付けた人材の輩出を目的とした独立行政法人国立高等専門学校機構（以下、国立高専機構）による事業である。セキュリティ知識を身に付けた国立高等専門学校生（以下、高専生）、また高度なセキュリティ技術を身に付けた人材の育成のために、企業、大学、公的機関等の外部組織と連携し、講習会やコンテストの開催、インターンシップの実施等を行っている。

関連するイベントとして、2021 年 12 月 27 ～ 28 日に「K-SEC セキュリティウィンタースクール 2021」がオンライン形式で開催された。本開催で 8 回目となり、全国から 40 名の高専生が参加した。JNSA やトレンドマイクロ株式会社、株式会社日本総合研究所等の様々な講師による講義や演習を通じて、参加者はセキュリティのスキルを学んだ※ 228。

(7) CYNEX

NICT は、保有しているサイバー攻撃に関連した大量のデータや、人材育成の知見を活用し、サイバーセキュリティ分野の産学官の「結節点」となることを目指し、「CYNEX（Cybersecurity Nexus：サイネックス）」を 2021 年 4 月 1 日に設立した※ 99。本組織は、サイバーセキュリティ情報を国内で収集・蓄積・分析・提供するとともに、人材育成の基盤としてサイバーセキュリティ演習に必要となる演習環境や教材を提供することで、日本のサイバーセキュリティの対応能力向上を目的としている（「2.1.3 (5) (c) 人材育成・普及啓発の推進」参照）。

CYNEX の人材育成プロジェクトの一つである「CYDERANGE as an Open Platform（CYROP）」では、国内における民間事業者や教育機関におけるセキュリティ人材育成事業の促進を目的に、NICT の演習プラットフォームをオープン化するための検証を 2022 年度末までの期間限定で実施している。この検証によって演習を実施する組織からフィードバックを得て、演習教材の拡充や演習環境の高度化等を行い、2023 年度には CYROP の本格運用開始が予定されている※ 100。

2.4 組織・個人における情報セキュリティの取り組み

企業・組織、教育機関、政府、地方自治体、一般利用者の情報セキュリティ対策状況及び課題について、政府、IPA 等による取り組み及び公表されている資料を基に述べる。

2.4.1 企業等における対策状況

情報セキュリティに対する企業等の対策状況及びセキュリティリスクマネジメントの取り組みについて述べる。

(1) 情報セキュリティに対する企業等の対策状況

近年、DX の推進に伴うサイバーセキュリティの重要性が注目されている。一方で、海外拠点を含むサプライチェーンのセキュリティ脅威が増しており、ランサムウェア等の攻撃により事業継続に影響する被害も出ている。このような背景を踏まえ、企業のセキュリティ対策・統制状況について、NRI セキュアテクノロジーズ株式会社（以下、NRI セキュア社）の「NRI Secure Insight 2021[※181]」(日本 1,616 社、米国 511 社、オーストラリア 526 社の企業を対象に調査。以下、NRI セキュア社調査）を基に述べる。

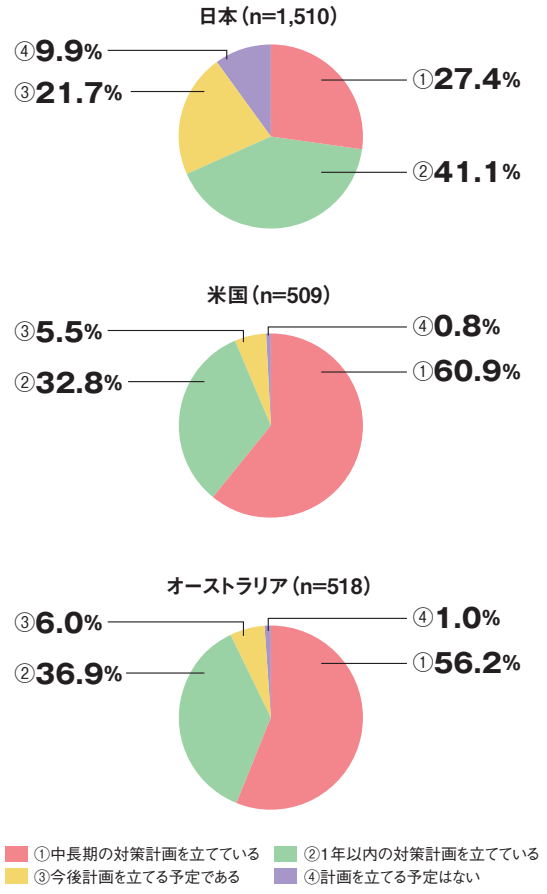
(a) セキュリティ対策計画の策定状況

NRI セキュア社調査（図 2-4-1）によると、 3 年程度の「中長期の対策計画を立てている」企業の割合は日本が 27.4% である一方、米国とオーストラリアは 60% 前後と日本の約 2 倍であった。また、「計画を立てる予定はない」企業の割合は日本が 9.9% である一方、米国とオーストラリアは約 1% であった。

回答企業のうち、1,000 人未満の企業の割合は日本 70.3%、米国 34.3%、オーストラリア 34.8% となっており、日本と米国・オーストラリアの違いは企業規模の構成比が影響している可能性がある。中堅企業、中小企業においても、「サイバーセキュリティ経営ガイドライン[※229]」等を参照して、セキュリティ対策計画を立案し、対策を実施していくことが望まれる。

(b) サプライチェーンのセキュリティ対策状況の把握

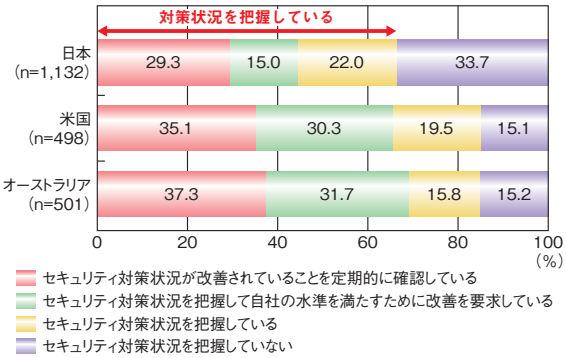
NRI セキュア社調査（図 2-4-2）によると、企業が国内関連子会社のセキュリティ対策状況を把握している割合は、日本では 66.3% で、米国とオーストラリアでは 80%



■図 2-4-1　セキュリティ対策計画の策定状況
(出典)NRI セキュア社「NRI Secure Insight 2021」を基に IPA が作成

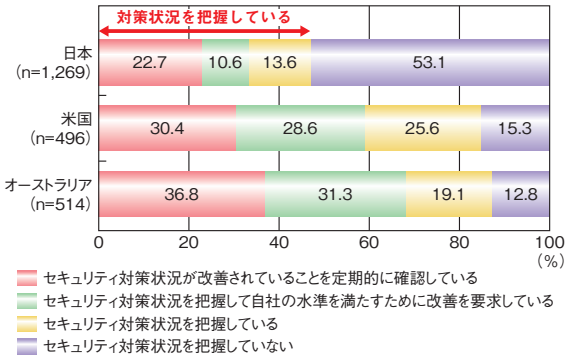
以上であった。また、自社の水準を満たすために関連子会社へ改善要求まで実施している割合は、日本では約 44.3% で、米国とオーストラリアでは 65% 以上であった。

国内パートナー／委託先への統制状況を調査した結果が図 2-4-3 (次ページ) である。国内パートナー／委託先のセキュリティ対策状況を把握している割合は、日本



■図 2-4-2　国内関連子会社に対するセキュリティ統制状況
(出典)NRI セキュア社「NRI Secure Insight 2021」を基に IPA が編集

では 46.9% で、米国とオーストラリアでは 85% 以上であった。また、自社の水準を満たすためにパートナー／委託先へ改善要求まで実施している割合は、日本では 33.3% で、米国とオーストラリアでは 60% 前後であった。



■図 2-4-3　国内パートナー／委託先に対するセキュリティ統制状況
(出典)NRI セキュア社「NRI Secure Insight 2021」を基に IPA が編集

日本でも、サプライチェーン上でのインシデントの増加や政府機関による注意喚起もあったためか、国内関連子会社に対するセキュリティ統制状況（前ページ図 2-4-2）では「セキュリティ状況を把握していない」割合は 33.7% であり、7 割弱の企業が何らかの取り組みを実施していた。しかし、統制対象が国内パートナー／委託先の場合（図 2-4-3）、「セキュリティ状況を把握していない」割合は 53.1% と約半数であった。子会社とは違って統制は容易ではないと推察されるが、米国、オーストラリアでは統制が進んでいることから、国内でも状況の改善が望まれる。2022 年 1 月に IPA が発表した「情報セキュリティ 10 大脅威 2022[※230]」によると、「サプライチェーンの弱点を悪用した攻撃」が 3 位となり、無視できない脅威になっている。業種・業態・事業規模に関係なく、サプライチェーンを構成するすべての事業者が対策を検討し、協力することが重要である。

(c) セキュリティ管理体制の構築状況

NRI セキュア社調査（表 2-4-1）によると、CISO を設置している企業の割合は、米国とオーストラリアが 90% 以上であるのに対し、日本は 46.1% にとどまっている。これは、同社が前年に行った同様の調査[※231]とおおむね同じ結果であり、CISO の設置は進んでいない。

	日本 (n=1,509)	米国 (n=503)	オーストラリア (n=511)
CISO	46.1%	94.8%	91.4%

■表 2-4-1　CISO の設置状況
(出典)NRI セキュア社「NRI Secure Insight 2021」を基に IPA が編集

(d) セキュリティ人材の充足状況

NRI セキュア社調査（表 2-4-2）によると、セキュリティ対策に従事する人材が不足しているとする企業における、不足している人材の種別として、日本では「セキュリティ戦略・企画を策定する人」が 1 位であり、米国とオーストラリアでは「経営層に対して適切な表現で、現状や対策内容等を説明・報告できる人」が 1 位であった。

	日本 (n=1,461)	米国 (n=66)	オーストラリア (n=61)
1 位	54.3% セキュリティ戦略・企画を策定する人	51.5% 経営層に対して適切な表現で、現状や対策内容等を説明・報告できる人	41.0% 経営層に対して適切な表現で、現状や対策内容等を説明・報告できる人
2 位	39.3% セキュリティリスクを評価・監査する人	33.3% セキュリティリスクを評価・監査する人	31.1% 関係部署との調整をしながら、セキュリティ対策を推進・統括できる人
3 位	38.4% ログを監視・分析して、危険な兆候をいち早く察知できる人	28.8% セキュリティ戦略・企画を策定する人	29.5% セキュアなシステム設計ができる人

■表 2-4-2　セキュリティ対策に従事する人材が不足していると考えている企業における、不足している人材種別
(出典)NRI セキュア社「NRI Secure Insight 2021」を基に IPA が編集

「2.4.1 (1) (a) セキュリティ対策計画の策定状況」で述べたとおり、日本では、「中長期の対策計画を立てている」企業の割合が少ない。表 2-4-2 の結果から、その背景として、セキュリティ戦略・企画を策定する人材が不足していることがうかがえる。

一方で、米国及びオーストラリアで「経営層に対して適切な表現で、現状や対策内容を説明・報告できる人」が求められる状況は、CISO 設置率の高さ（表 2-4-1）とも整合し、経営層がセキュリティに関与し、事業継続性やサイバー攻撃に対する防御力向上の観点で適切な経営判断を行うことを重要視していると推察される。

(2) セキュリティリスクマネジメント

国内の企業・組織は、「2.4.1 (1) 情報セキュリティに対する企業等の対策状況」で述べたようなセキュリティリスクに直面している。組織のセキュリティリスクを把握・管理するリスクマネジメントは、企業にとって経営・事業を守るための重要課題の一つである。リスクマネジメントには経営層のリーダーシップが欠かせないため、経済産

業省とIPAは、経営層のセキュリティリスクマネジメント向上を目的として、2017年に「サイバーセキュリティ経営ガイドライン Ver2.0[※232]」（以下、経営ガイドライン）を発行した。またIPAは、経営ガイドラインの実践には、対策状況の可視化や、参考となる実践事例（プラクティス）の提示が重要であることから、それらに関する取り組みを行ってきた。

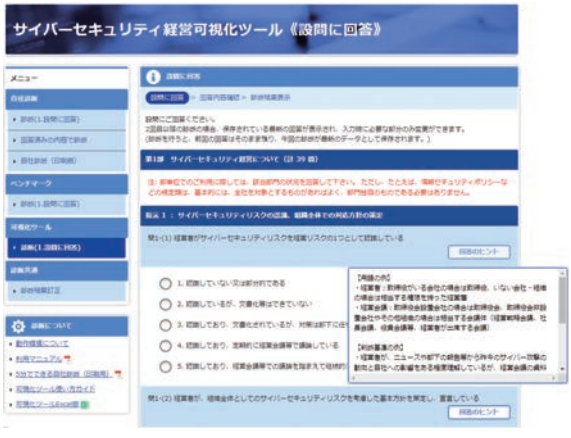
本項では、上記の取り組みを基にしたセキュリティリスクマネジメントについて述べる。

(a) サイバーセキュリティの対策状況

組織のセキュリティリスクマネジメントにおいては、経営層とCISO等のセキュリティマネジメントを統括する部門が情報共有できるように、自組織の対策状況を可視化することが重要である。IPAは、経営ガイドラインに基づく質問に回答することで、サイバーセキュリティ対策状況のレーダーチャート表示や業種平均との比較ができる「サイバーセキュリティ経営可視化ツール[※3]」（以下、可視化ツール）を提供している（図2-4-4）。回答方法は成熟度モデルに基づく5段階（最高5ポイント、最低1ポイント）の選択式（表2-4-3）で、回答者がなるべく客観的に判断できるようなヒントの提示（表2-4-4）により、利用者がより正確に回答できるよう工夫されている。

可視化ツールでは、回答に基づき、対策実施状況を経営ガイドラインで示された「重要10項目」ごとにレーダーチャート表示する。図2-4-5に2021年8～12月に利用者登録された企業全体と業種別（製造業、情報通信業）の回答の平均値を示す。

全回答の総計である「全体」では重要10項目の中で、指示1（サイバーセキュリティリスクの認識、組織全体での対応方針の策定）が3.1ポイントと最も高い。文書化まではできているものの、その見直し体制までは構築できていないことがうかがえる。一方、指示8（インシデントによる被害に備えた復旧体制の整備）、指示9（ビジネスパートナーや委託先を含めたサプライチェーン全体の対策及び状況把握）、指示10（情報共有活動への参加を通じ



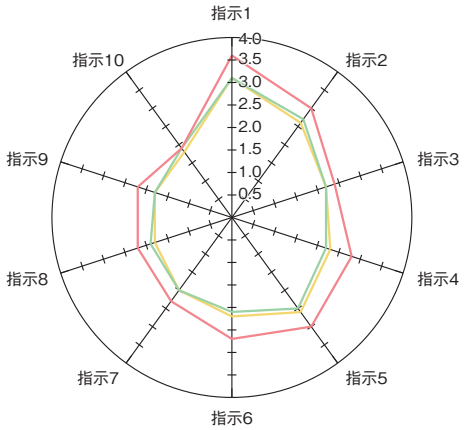
■図2-4-4　サイバーセキュリティ経営可視化ツール画面

問1-(1)	成熟度	企業の対応状況
経営者がサイバーセキュリティリスクを経営リスクの1つとして認識している	レベル1	認識していない又は部分的である
	レベル2	認識しているが、文書化等はできていない
	レベル3	認識しており、文書化されているが、対策は部下に任せている
	レベル4	認識しており、定期的に経営会議等で議論している
	レベル5	認識しており、経営会議等での議論を踏まえて継続的に改善している

■表2-4-3　5段階の成熟度モデルによる回答選択肢の例

問1-(1) の判断基準の例
・経営者が、ニュースや部下の報告等から昨今のサイバー攻撃の動向と自社への影響をある程度理解しているが、経営会議の資料等の形にしていなければレベル2。 ・経営会議の議題に入っているが、資料は付録、情シス責任者の報告を聞き流すだけ等であればレベル3以下。（経営者が自分の言葉で考え、語っているかがポイント。） ・経営会議の議題に入っており、かつ経営者が自分の考え、自分の言葉で議論していればレベル4。 ・経営会議で議論されたことが現場に展開され、その結果がまた経営会議に報告・議論されるというプロセスが回っていればレベル5。

■表2-4-4　問1-(1)の判断のためのヒント



指示1:サイバーセキュリティリスクの認識、組織全体での対応方針の策定
指示2:サイバーセキュリティリスク管理体制の構築
指示3:サイバーセキュリティ対策のための資源（予算、人材等）確保
指示4:サイバーセキュリティリスクの把握とリスク対応に関する計画の策定
指示5:サイバーセキュリティリスクに対応するための仕組みの構築
指示6:サイバーセキュリティ対策におけるPDCAサイクルの実施
指示7:インシデント発生時の緊急対応体制の整備
指示8:インシデントによる被害に備えた復旧体制の整備
指示9:ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策及び状況把握
指示10:情報共有活動への参加を通じた攻撃情報の入手とその有効活用及び提供

■図2-4-5　可視化ツールに利用者登録した企業のサイバーセキュリティ対策状況（2021年8～12月）

た攻撃情報の入手とその有効活用及び提供）は、1.8 ポイントと最も低い。対応方針の策定はできているものの、インシデント復旧体制の整備、サプライチェーンの状況把握、情報共有活動までは十分できていない実態がうかがえる。

個別の業種については、回答数の多かった二つを掲載している。「製造業」は「全体」とほぼ同様の傾向である。一方、「情報通信業」は指示 1 ～ 9 で「全体」を 0.2 ～ 0.5 ポイント上回り、取り組みが進んでいる業種であることがうかがわれる。その「情報通信業」においても指示 10 のポイントは低く、情報共有活動の実践は業種横断的な課題である可能性がある。

(b) セキュリティリスクマネジメントの実践事例

他社のセキュリティリスクマネジメント実践事例は、自社の同様なセキュリティ課題について対策を行う上で、有用な情報である。IPA は、企業へのアンケート及びインタビューを通じて収集した、実際に行われている施策に基づく「サイバーセキュリティ経営ガイドライン Ver 2.0 実践のためのプラクティス集 第 3 版※4」（以下、プラクティス集）を提供している。プラクティス集は、事例ごとに仮想的な企業を想定し、その企業が置かれている事業状況やセキュリティ等の状況、CISO 等及び関係者の役割、対策に関する意思決定、実際の作業について具体的に記載している。

プラクティス集では、二つのタイプ（重要 10 項目の実践に紐づくものと、重要 10 項目を横断する課題の解決に紐づくもの）を掲載している。ここでは、そのうち前者のタイプで重要 10 項目の指示 1 の実践に紐づく事例を紹介する。

従業員数 1 万名規模の精密機器メーカである C 社では、ある拠点で製品サポートを提供した顧客情報の管理不備が見つかった。意図しない漏えいリスクに危機感を抱いた経営層は本社の CISO を中心に対応を指示した。CISO が各拠点の事情を踏まえ実践した手順は次のとおりである。

①専門家の助言を基に、拠点立地国の個人情報やプライバシー情報の保護に関する要求事項（例：EU の GDPR（General Data Protection Regulation：一般データ保護規則））を整理した上、現地に対策を委ねることが困難な拠点を洗い出した。

②当該拠点ごとのチェックリスト（例：個人情報を定められた場所に保存しているか、保管期限を経過した情報を削除しているか等）を作成した。

③各拠点担当者が、本社の支援のもとチェックリストを用いて定期的な自己点検を実施した。

④情報セキュリティ対策に関する内部監査で、上記の自己点検結果を監査することで現地法規制の遵守状況を確認し、必要に応じて是正を指示した。

CISO は①～④のプロセスを統括し、②のチェックリスト作成にあたっては、正確性を担保しつつ現地の商習慣、スタッフの役割等を考慮し各業務内容に沿った記載とすることで、現地スタッフにとって分かりやすい内容となるよう努めた。

なお、上記のような他社のプラクティスを参考にする際は、実践内容をそのまま受け入れるのではなく、自社の問題に置き換えて取り得る対策、重点化する対策等を柔軟に考えることが重要である。

(c) まとめ

セキュリティリスクマネジメントについて、経済産業省はサイバーセキュリティ経営ガイドラインの実践を通じた経営層のコミットメント強化を推進しており、そのための重要な支援ツールとして可視化ツールとプラクティス集が位置付けられている（「2.1.2 (1) (b) WG2（経営・人材・国際）」参照）。企業の経営層や CISO 等を含むリスクマネジメント統括部門はこれらの支援ツールを有効に活用し、セキュリティリスクマネジメントの向上に取り組むことが望まれる。

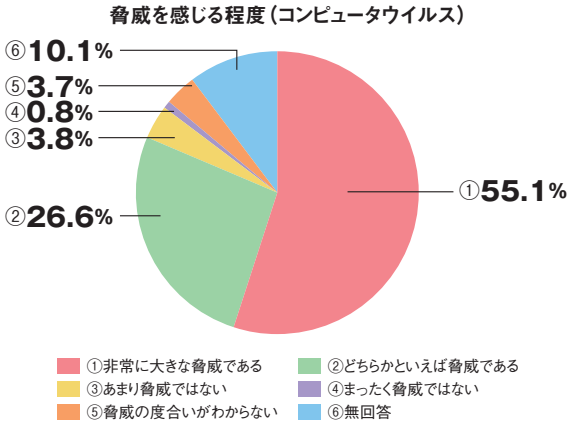
2.4.2 中小企業に向けた情報セキュリティ支援策

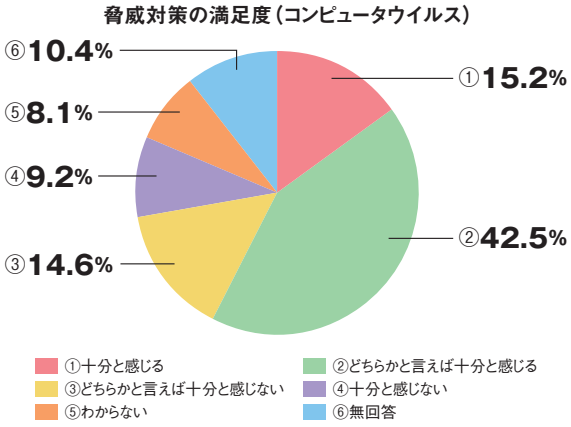
本項では、中小企業における情報セキュリティ、対策支援、及び普及啓発・対策ツールの現状について紹介する。

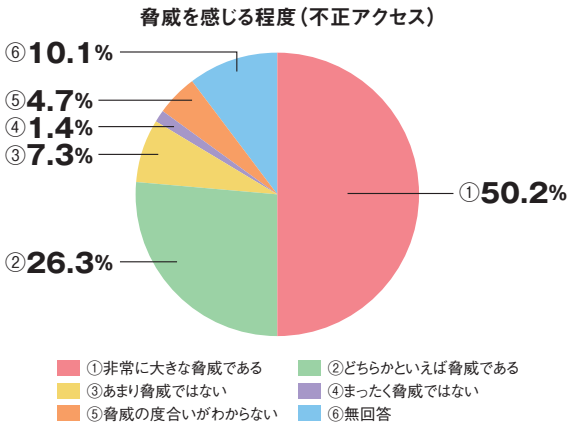
(1) 中小企業の情報セキュリティの現状

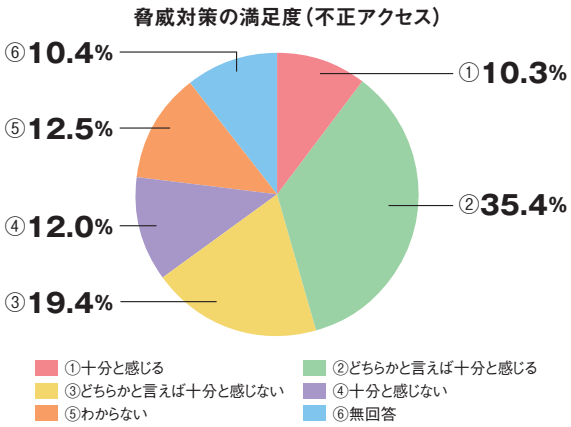
IPA が 2022 年 3 月 31 日に発表した「2021 年度 中小企業における情報セキュリティ対策に関する実態調査報告書※233」によると、情報セキュリティに関する脅威について、コンピュータウイルスを「非常に大きな脅威である」または「どちらかといえば脅威である」と認識している企業の割合は 81.7% であった。また、不正アクセスを「非常に大きな脅威である」または「どちらかといえば脅威である」と認識している企業は 76.5% であった（次ページ図 2-4-6）。

一方で、脅威対策の満足度について、ウイルス対策を









■図 2-4-6　情報セキュリティに関する脅威
（出典）IPA「2021 年度中小企業における情報セキュリティ対策の実態調査報告書」を基に編集

■図 2-4-7　脅威対策の満足度
（出典）IPA「2021 年度中小企業における情報セキュリティ対策の実態調査報告書」を基に編集

「十分と感じる」または「どちらかと言えば十分と感じる」という企業の割合は 57.7% であった。また、不正アクセス対策を「十分と感じる」または「どちらかと言えば十分と感じる」という企業の割合は 45.7% であった（図 2-4-7）。

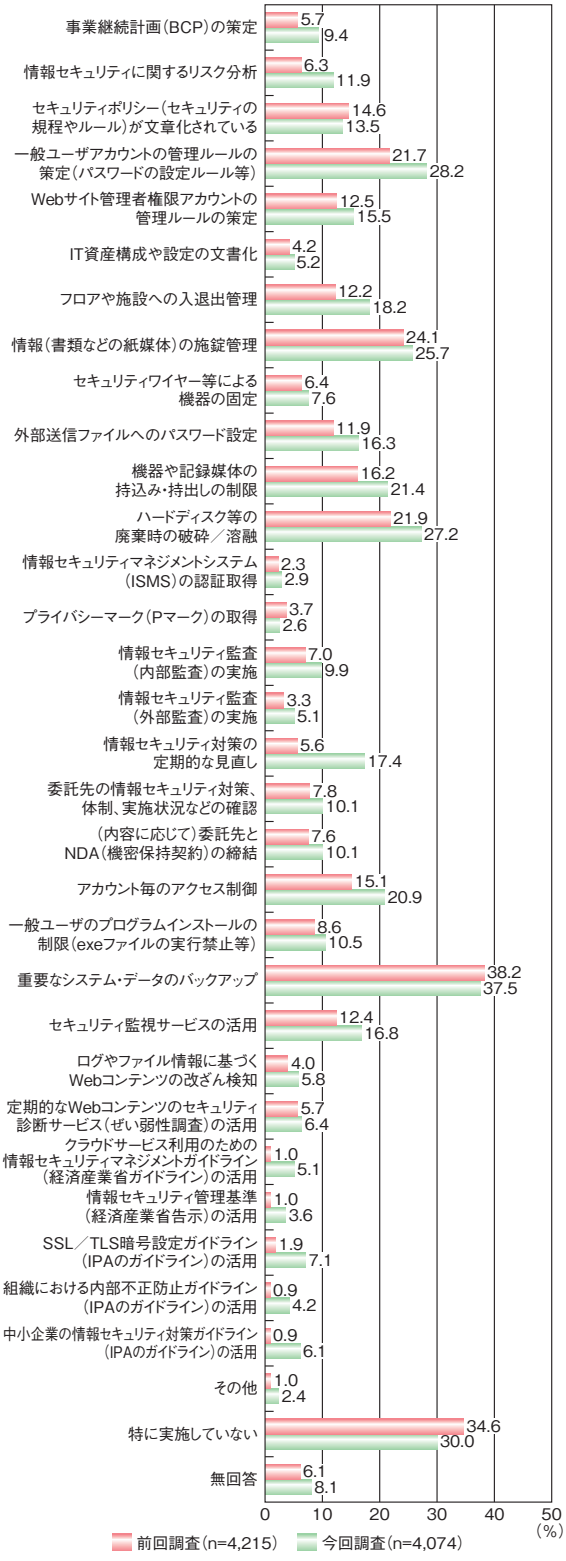
被害防止のための組織面・運用面の対策の実施状況については、「重要なシステム・データのバックアップ」の割合が最も高く 37.5% となっている。次いで、「特に実施していない」（30.0%）、「一般ユーザアカウントの管理ルールの策定（パスワードの設定ルール等）」（28.2%）となっている。2016 年度に実施した同調査の結果と比較すると、「特に実施していない」の割合が 34.6% から 30.0% へ減少し、大半の項目で実施割合がわずかながら増加している（次ページ図 2-4-8）。

情報セキュリティ関連製品やサービスの導入状況については、「ウイルス対策ソフト・サービスの導入」の割合が最も高く 77.2% となっている。次いで、「ファイアウォール」（35.6%）、「VPN」（17.1%）となっている。2016 年度調査の結果と比較すると、「VPN」の導入割合が 11.9% から 17.1% に増加しているものの、その他の選択肢については大きな差はない（次ページ図 2-4-9）。

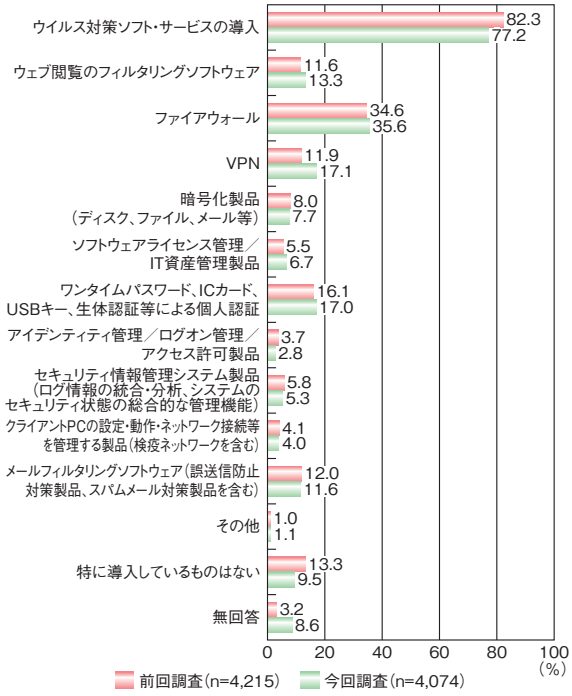
販売先・仕入先との契約締結時における情報セキュリティに関する条項・取引上の義務・要請については、「義務・要請はない」の割合が高く 63.2% となっている。「義務・要請がある」の割合は、26.1% である（次ページ図 2-4-10）。

また、「義務・要請がある」と回答した企業のうち、契約時における情報セキュリティに関する要請について、「秘密保持」の割合が最も高く 93.8% となっている。次いで、「契約終了後の情報資産の扱い（返却、消去、廃棄等）」（36.3%）、「情報セキュリティに関する契約内容に違反した場合の措置」（32.4%）となっている（次ページ図 2-4-11）。

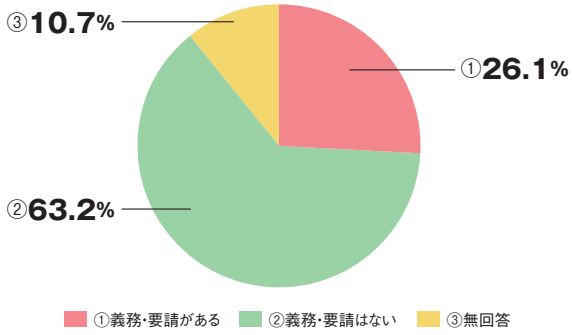
このような調査結果から、中小企業では情報セキュリティに関する脅威を認識しているものの、十分な対策がとられているとは言えない状況にあることが分かった。また、サプライチェーン上の販売先・仕入先等からの情報セキュリティに関する義務・要請も十分に行われていない。しかし、「サイバーセキュリティお助け隊事業（令和 2 年度中小企業向けサイバーセキュリティ対策支援体制構築事業）成果報告書※234」では、業種や事業規模を問わずサイバー攻撃や不審なアクセス等の脅威に晒されて



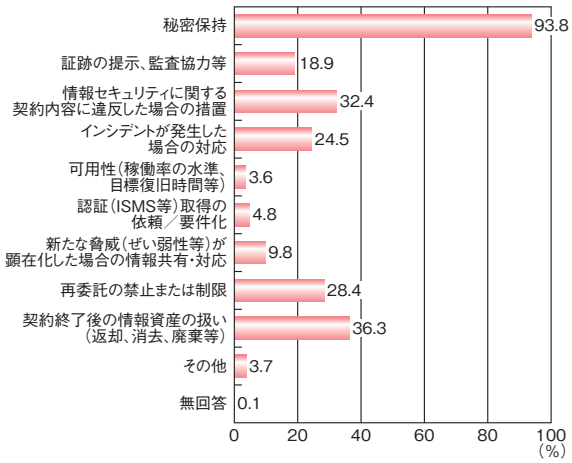
■図 2-4-8　被害防止のための組織面・運用面の対策(複数回答)
(出典)IPA「2021 年度中小企業における情報セキュリティ対策の実態調査報告書」を基に編集



■図 2-4-9　情報セキュリティ関連製品やサービスの導入状況(複数回答)
(出典)IPA「2021 年度中小企業における情報セキュリティ対策の実態調査報告書」を基に編集



■図 2-4-10　販売先・仕入先からの情報セキュリティに関する条項・取引上の義務・要請
(出典)IPA「2021 年度中小企業における情報セキュリティ対策の実態調査報告書」を基に編集



■図 2-4-11　契約時における情報セキュリティに関する要請(販売先(発注元企業)との契約時)(複数回答)
(出典)IPA「2021 年度中小企業における情報セキュリティ対策の実態調査報告書」を基に編集

いる状況が明らかになっている。中小企業を含むサプライチェーン全体でのセキュリティの確保が望まれる。

(2) 中小企業向け情報セキュリティ対策支援施策

政府が 2021 年度に新たに実施した中小企業向け情報セキュリティ対策支援施策を紹介する。

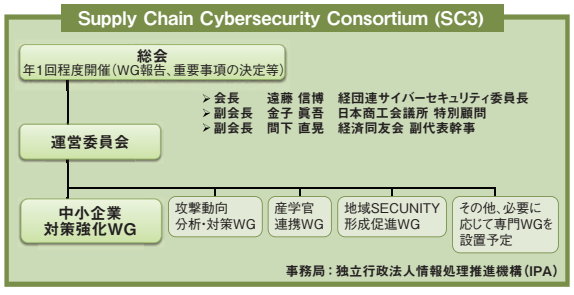
(a) サプライチェーン・サイバーセキュリティ・コンソーシアム(SC3)

経済産業省は 2020 年度に引き続き 2021 年度、IPA を通じて、産業界が一体となって中小企業を含むサプライチェーン全体のサイバーセキュリティ対策を推進する運動「サプライチェーン・サイバーセキュリティ・コンソーシアム(SC3)※235」の支援を行った。

具体的には、中小企業対策強化 WG では、サイバーセキュリティお助け隊サービスの普及に向けた議論や中小企業を対象としたウェビナーの開催等を行った。

また、2021 年 6 月の運営委員会において、攻撃動向分析・対策 WG 及び地域 SECUNITY 形成促進 WG、産学官連携 WG が新たに設置された(図 2-4-12)。このうち地域 SECUNITY 形成促進 WG は、全国各地で活動する地域のセキュリティコミュニティ(通称、地域 SECUNITY)を対象に地域間の情報共有や共通課題の解決に向けた取り組みを検討・推進することを目的としたワークショップを開催した。

今後、各 WG の活動を通じて、地域や業界に閉じない横断的な活動を展開していくことが期待される。



■図 2-4-12　SC3 の組織体制
(出典)IPA「サプライチェーン・サイバーセキュリティ・コンソーシアム(SC3)とは※236」

(b) 地域 SECUNITY 形成促進事業

経済産業省は 2021 年度、地域に根差したセキュリティコミュニティの形成促進のため「地域 SECUNITY 形成促進事業」を実施した。

本事業では、地域のセキュリティ関係者(公的機関、教育機関、地元企業、地元ベンダ等)が集まり、セキュリティについての相談や意見交換を行う地域 SECUNITY の形成を促進するために、地域ごとの形成状況に応じて、調査やセミナー、ワークショップ、専門家派遣、有識者会議等の取り組みを行った。

今後、地域の中でセキュリティに関する情報の収集や相談が行える「共助」の取り組みが、全国各地で展開されることが期待される。

(3) 普及啓発・対策ツール

中小企業に向けた情報セキュリティの普及啓発活動や対策ツールを紹介する。

(a) サイバーセキュリティお助け隊サービス制度

IPA は 2021 年度、中小企業に対するサイバー攻撃への対処として不可欠なサービスの要件をまとめた「サイバーセキュリティお助け隊サービス基準※237」を満たした民間セキュリティ事業者のサービスを「サイバーセキュリティお助け隊サービス※6」として登録・公表した。

サイバーセキュリティお助け隊サービス基準は、相談窓口、異常の監視、緊急時の対応支援、簡易サイバー保険等の各種サービスをワンパッケージで安価に提供することを要件としている(表 2-4-5)。同基準を満たすサービスには、「サイバーセキュリティお助け隊マーク」の利用が許諾される(次ページ図 2-4-13)。

2022 年 3 月末時点で 12 のサービスが登録されている。中小企業が無理なくサイバーセキュリティ対策を導入・運用できる具体的なサービスが明示されることで、サ

主な要件	概要
相談窓口	ユーザからの相談を受け付ける窓口を設置／案内
異常の監視の仕組み	ネットワーク及び／または端末を 24 時間見守る仕組みを提供
緊急時の対応支援	インシデント発生等の緊急時には駆け付け支援
中小企業でも導入・運用できる簡単さ	専門知識がなくても導入・運用できるような工夫
簡易サイバー保険	突発的に発生する駆付け費用等を補償するサイバー保険
中小企業でも導入・維持できる価格	・ネットワーク一括監視型:月額 1 万円以下(税抜き) ・端末監視型:月額 2,000 円以下／台(税抜き) ・併用型:これらの和に相当する価格を超えないこと ※端末 1 台から契約可能であることが条件

■表 2-4-5　サイバーセキュリティお助け隊サービス基準の主な内容
(出典)IPA「サイバーセキュリティお助け隊サービス基準」を基に作成

■図 2-4-13　サイバーセキュリティお助け隊マーク

■図 2-4-14　SECURITY ACTION ロゴマーク

プライチェーン全体のセキュリティの強化が期待される。

(b) SECURITY ACTION

IPA では、中小企業自らが情報セキュリティ対策に取り組むことを自己宣言する制度「SECURITY ACTION※238」を運営し、中小企業と関連の深い中小企業支援機関、士業団体、IT 関連団体と連携して SECURITY ACTION を通じた情報セキュリティの普及啓発を行っている(図 2-4-14)。

SECURITY ACTION に基づく自己宣言は、経済産業省が実施するものづくり・商業・サービス生産性向上促進補助金のデジタル枠の申請要件になっているほか、公的な補助金制度の申請要件としても活用されている。

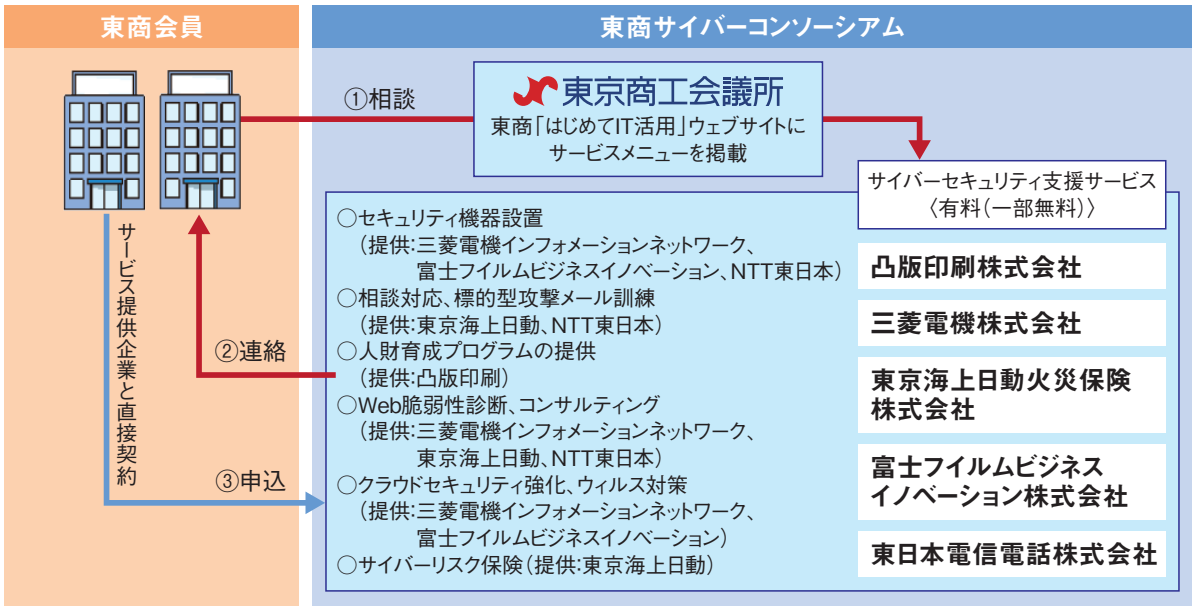
2022 年 1 月末時点の宣言数は 18 万件(個人事業主を含む)を超えている。今後、より多くの中小企業が SECURITY ACTION を宣言し、社内の意識付けや社外への信頼性のアピール等に活用し、対策を推進することが望まれる。

(c) 東商サイバーセキュリティコンソーシアム

東京商工会議所は 2021 年 7 月 30 日、会員企業のサイバーセキュリティ対策支援を目的とした「東商サイバーセキュリティコンソーシアム※239」を設立した(図 2-4-15)。

東京商工会議所では、従前より展開している「『はじめて IT 活用』1 万社プロジェクト」において、中小・小規模事業者の IT 活用を総合的に支援してきた。この枠組みの中でコンソーシアムを設立し、東京商工会議所と参画企業 5 社が連携し、専用 Web サイトを通じて、中小企業向けサイバーセキュリティ支援サービスを提供している。

地域の総合経済団体による中小企業へのサイバーセキュリティ対策支援の取り組みの一つのモデルとして、今後全国へと拡大していくことが期待される。



■図 2-4-15　東商サイバーセキュリティコンソーシアムの連携スキーム図
(出典)東京商工会議所「『東商サイバーセキュリティコンソーシアム』が本日発足　～東商とサイバーセキュリティ対策のノウハウを持つ大手 5 社が業界を横断し、初連携! 増大するサイバーリスクにさらされる中小企業を総合的に支援～※240」を基に編集

2.4.3 教育機関・政府及び地方公共団体等法人における対策状況

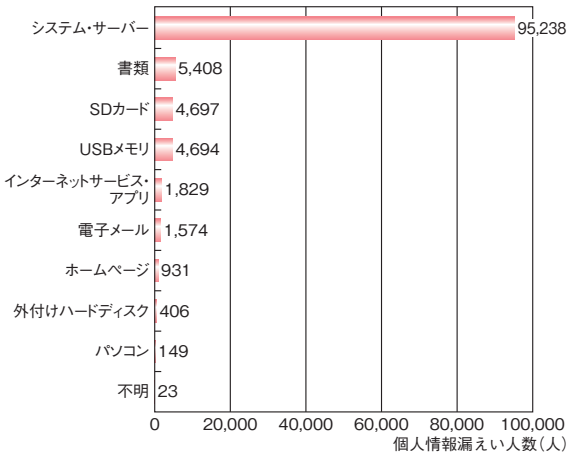
教育機関・政府及び地方公共団体等法人における対策状況について、公表されている資料に基づいて述べる。

(1) 教育機関における個人情報紛失・漏えいの現状

教育ネットワーク情報セキュリティ推進委員会（ISEN：Information Security for Education Network）は、毎年、学校等教育関連機関で発生した個人情報の紛失・漏えい事故について公開情報を調査し、公表している。2021 年 11 月、「令和 2 年度（2020 年度）学校・教育機関における個人情報漏えい事故の発生状況 －調査報告書－ 第 2 版※241」（以下、ISEN 報告書）を公表した。本項では、ISEN 報告書に基づいて、2020 年 4 月 1 日～ 2021 年 3 月 31 日の間の事故の傾向について述べる。

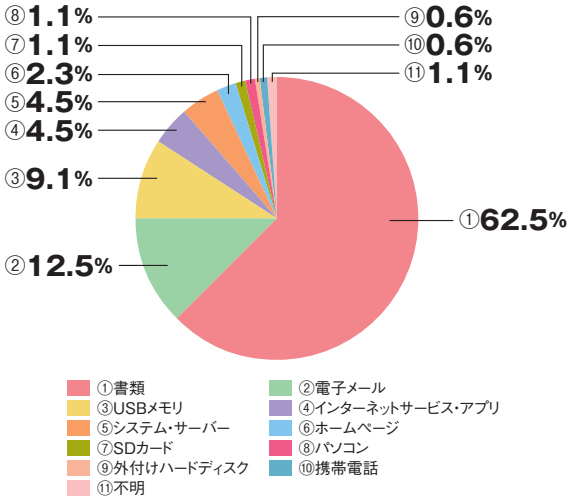
ISEN 報告書によると、2020 年度は 170 件（2019 年度 226 件）の個人情報漏えい事故が発生し、11 万 4,232 人分（2019 年度 23 万 6,185 人分）の個人情報が漏えいした。2019 年度と比較すると、発生件数は約 25% 減少し、漏えい人数は半減した。

漏えいした個人情報の人数を経路・媒体ごとに比較すると、図 2-4-16 に示すように、2020 年度は学校、教育委員会が管理する「システム・サーバー」が 9 万 5,238 人と最も多く、2 位の「書類」以下を大きく引き離している。



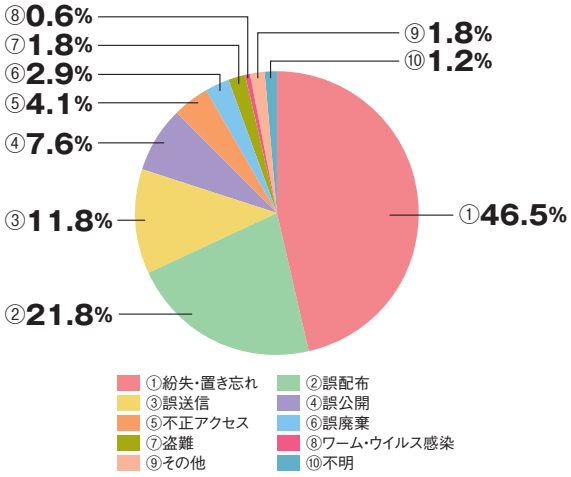
■図 2-4-16　漏えい経路・媒体別個人情報漏えい人数※242
（出典）ISEN 報告書を基に IPA が作成

一方で、漏えいした個人情報の漏えい経路・媒体ごとの事故発生件数は、図 2-4-17 に示すように「書類」の 62.5% が最も多く、次いで「電子メール」の 12.5% となっている。これに対し「システム・サーバー」を起因とする事故発生件数は全体の 4.5% と少なく、1 件あたりの個人情報の漏えい人数が顕著に大きいことが分かる。



■図 2-4-17　漏えい経路・媒体別事故発生件数
（出典）ISEN 報告書を基に IPA が作成

漏えい人数とは別に、事故の種類ごとの発生件数を調べると、「紛失・置き忘れ」「誤配布」「誤送信」「誤公開」「誤廃棄」のように「不注意」による事故が全体の 90.6% に上っている（図 2-4-18）。



■図 2-4-18　漏えい事故種別発生割合
（出典）ISEN 報告書を基に IPA が作成

このように教育機関等においては、個人情報が記録された書類や USB メモリの紛失・置き忘れ、誤配布等の不注意による事故が後を絶たない。学校における安全安心な ICT 活用に向け情報セキュリティ対策を講じることが求められる中、情報管理不備（不注意）対策と「システム・サーバー」等からの情報漏えい対策の徹底が、ますます重要になっている。

(2) 文部科学省における対策

文部科学省における情報セキュリティの取り組みを「『教育情報セキュリティポリシーに関するガイドライン』(令和 4 年 3 月)改定について※243」に基づき述べる。

2017 年 10 月、教育委員会・学校が情報セキュリティポリシーの作成や見直しを行う際の参考となる「教育情報セキュリティポリシーに関するガイドライン」が策定され、その後、順次改定されてきた。

まず 2019 年 12 月、「多様な子供たちを誰一人取り残すことなく、公正に個別最適化され、資質・能力が一層確実に育成できる教育 ICT 環境」の実現を目指す、とする GIGA スクール構想※244 の始動に合わせて 1 回目の改定が実施された。

その後、新型コロナウイルス感染拡大に伴い、学びの環境を保障するために GIGA スクール構想計画は前倒しされた。すなわち、当初「教育の ICT 化に向けた環境整備」については「5 か年計画(2018 ～ 2022 年)※245」とされていたが、1 人 1 台の端末整備や高速大容量の校内通信ネットワークの整備等の GIGA スクール構想計画は、3 度の補正予算によって 2020 年度内に完了した※246。

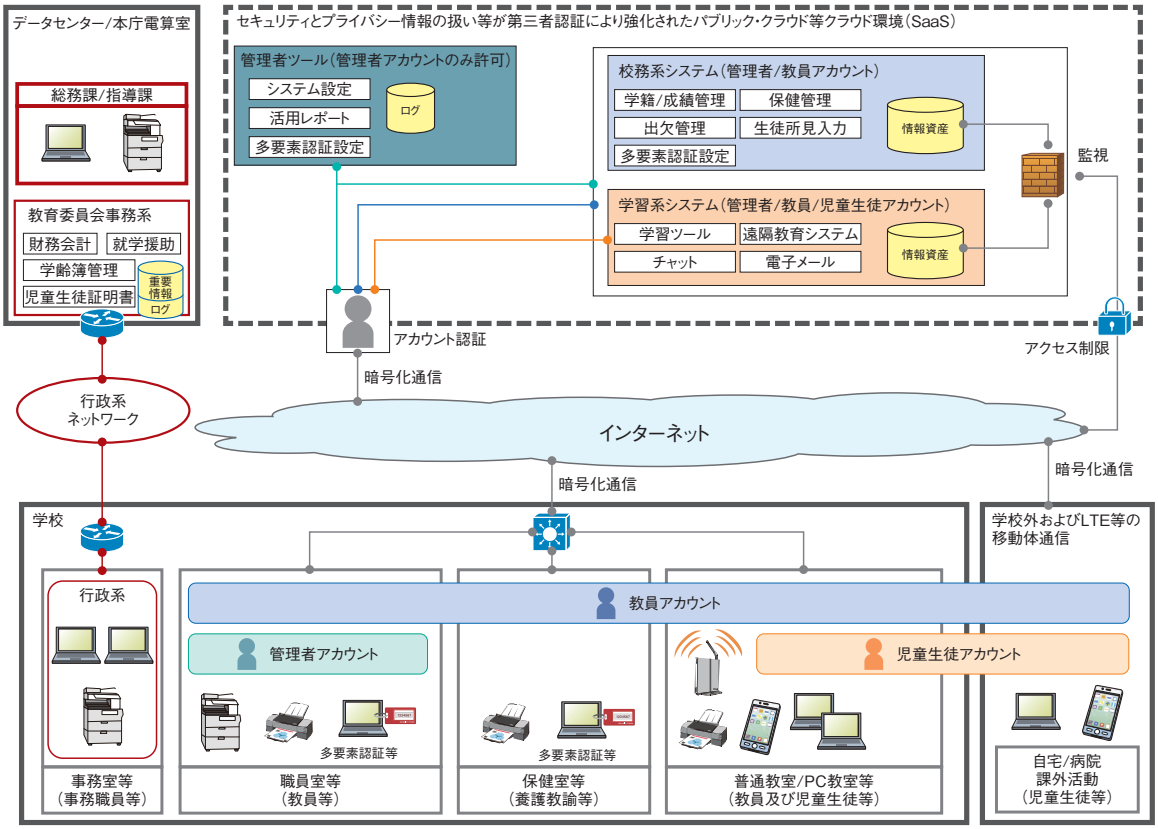
このような環境整備に併せて必要となるセキュリティ対策やクラウドサービスの活用に向けたネットワーク構成等の課題に対応するため、2021 年 5 月に 2 回目の改訂が実施され※247、「『教育情報セキュリティポリシーに関するガイドライン』(令和 3 年 5 月版) ハンドブック※248」も公表された。

2021 年 5 月の改定では、学校内外での学習者用端末の活用や、クラウドサービス活用に向けた ID 管理等に関するセキュリティ対策が多く追記された。また、過渡期としてのローカルブレイクアウト※249 構成や、校務系／学習系のネットワーク分離を必要としない教育情報ネットワークの構成等についても記載された。

更に 2021 年 12 月、「デジタル社会の実現に向けた重点計画」が閣議決定され※250、今後、各地方公共団体においてもクラウドの利用を念頭にセキュリティを検討していくことが方向付けられた。

2022 年 3 月には、その方針を踏まえ、デジタル庁の支援のもと、3 回目となる改定が実施され※251、「『教育情報セキュリティポリシーに関するガイドライン』ハンドブック(令和 4 年 3 月)※252」も公開された。

同ガイドラインで提示された、1 人 1 台端末を活用するために必要なネットワーク構成のイメージ (アクセス制御による対策を講じたシステム構成)を図 2-4-19 に示す。



■図 2-4-19　1 人 1 台端末を活用するために必要なネットワーク構成例
(出典)文部科学省「『教育情報セキュリティポリシーに関するガイドライン』ハンドブック(令和 4 年 3 月)」を基に IPA が編集

2022 年 3 月の改定では、今後の推奨ネットワーク構成となる、校務系／学習系のネットワーク分離を必要としない教育情報ネットワーク構成としての「アクセス制御による対策を講じたシステム構成」と、これまでの「ネットワーク分離による対策を講じたシステム構成」を明確に区分し、その上で「アクセス制御による対策を講じたシステム構成」について、特に校務用端末における「リスクベース認証[※253]」「ふるまい検知[※254]」「マルウェア対策」「暗号化」「SSO（シングルサインオン）の有効性」等の詳細な技術的対策が追記された。

また、上記それぞれの構成における「校務用端末の使い分け」についての記述の適正化や、「校務用端末の持ち出し」に関する記述の適正化が図られた。

今後の GIGA スクール構想の進展において、セキュリティが担保されることで、「これまでの我が国の教育実践と最先端の ICT のベストミックスを図ることにより、教師・児童生徒の力を最大限に引き出す[※244]」環境が整備されることが期待される。

(3) 地方自治体等における対策状況

総務省は、継続的に地方公共団体の情報セキュリティ対策の実施状況を調査している。ここでは総務省が 2021 年 8 月に公表した「地方自治情報管理概要～電子自治体の推進状況（令和 2 年度）～[※255]」に基づき、地方公共団体の情報セキュリティ対策の実施状況の変化について述べる。

表 2-4-6 は、対策項目に関して、都道府県及び市区町村の実施率をまとめたものである。2019 年度[※256]と 2020 年度との実施率の差も併せて記載している。

2019 年度に都道府県では 10 項目、市区町村では全項目について 100%の実施率を達成できていなかったが、2020 年度に都道府県では「重要なデータへのアクセス制限（権限設定、認証）を実施」「情報資産の調達の際、仕様書等に情報セキュリティポリシーに基づいた要件を記載している」の 2 項目について新たに 100% の実施率を達成した。しかしながら、都道府県では全 22 項目中 8 項目が、市区町村では依然として全項目が 100% の

対策実施率（都道府県は 47、市区町村は 1,741）							
	対象項目	都道府県	市区町村		対象項目	都道府県	市区町村
	情報セキュリティの責任者や管理者等の任命の有無	100.0% (0.0ポイント)	99.9% (+0.1ポイント)	(B)	緊急時対応訓練を実施している	87.2% (0.0ポイント)	40.1% (+7.1ポイント)
(A)	緊急時対応計画を整備	100.0% (0.0ポイント)	72.8% (+3.2ポイント)		重要なデータのバックアップを取得	100.0% (0.0ポイント)	99.9% (+0.0ポイント)
	情報資産の重要度に応じて、保管やアクセス、持ち出しについて規定	100.0% (0.0ポイント)	95.5% (+2.6ポイント)		機器や外部記録媒体を廃棄する際、重要なデータを抹消	100.0% (0.0ポイント)	99.7% (0.4ポイント)
	情報資産について、機密性、完全性及び可用性により分類	85.1% (+10.6ポイント)	72.9% (+9.1ポイント)		重要なデータへのアクセス制限（権限設定、認証）を実施	100.0% (+2.1ポイント)	99.8% (+0.1ポイント)
(A)	主要な情報資産について調査及びリスク分析を行っている	80.9% (+6.4ポイント)	55.2% (+7.4ポイント)		許可されていないソフトウェアの導入を禁止	100.0% (0.0ポイント)	98.6% (+0.7ポイント)
	サーバ室等の入退室管理を行っている	100.0% (0.0ポイント)	99.5% (+0.2ポイント)		重要な情報システムのアクセスログを保存し、検査	100.0% (+0.0ポイント)	93.3% (1.6ポイント)
	サーバ等への停電や免振対策を実施している	100.0% (0.0ポイント)	98.1% (+0.7ポイント)		重要なデータを暗号化し保存	89.4% (+2.2ポイント)	56.7% (+6.7ポイント)
	重要情報を含む紙媒体を適切に管理している	100.0% (0.0ポイント)	99.1% (+0.5ポイント)		委託事業者に対し、情報漏えい防止策を契約等により義務付けている	100.0% (+0.0ポイント)	97.8% (+1.5ポイント)
	CD-R、USB メモリ等によるデータの持ち出し、持ち込みを制限している	97.9% (0.0ポイント)	98.9% (+0.6ポイント)		情報資産の調達の際、仕様書等に情報セキュリティポリシーに基づいた要件を記載している	100.0% (+2.1ポイント)	80.0% (+8.9ポイント)
	クラウドサービスやデータセンターを利用している	97.9% (4.3ポイント)	93.7% (+2.5ポイント)	(B)	情報システムの運用等の委託事業者に対する指導・監査を実施している	74.5% (+6.4ポイント)	58.5% (+9.0ポイント)
	情報セキュリティ研修を職員に対して実施している	100.0% (0.0ポイント)	94.1% (+1.2ポイント)	(B)	機密性、完全性及び可用性等についてサービス契約 (SLA) に定め、委託事業者に対し定期的に報告することを定めている	70.2% (+10.6ポイント)	49.1% (+10.4ポイント)

■表 2-4-6　地方公共団体における主な情報セキュリティ対策状況（2020 年度、47 都道府県、1,741 市区町村）
（出典）総務省「地方自治情報管理概要～電子自治体の推進状況（令和２年度）～」「地方自治情報管理概要～電子自治体の推進状況（令和元年度）～[※256]」を基に IPA が作成

実施となっていない。

基本的な個別対策の中で「情報資産について、機密性、完全性及び可用性により分類」については都道府県、市区町村ともに前年度からの改善ポイントは高いものの達成率そのものは都道府県 85.1%、市区町村 72.9% にとどまっている。

また、調査・分析・計画等の項目（表中の（A）の項目）や監査・評価に関する項目（表中の（B）の項目）は、特に市区町村において、今後の改善が求められる。都道府県においても「緊急時対応訓練を実施している」の項目については前年度からの改善が見られていないことから、併せて今後の改善が求められる。

2.4.4 一般利用者における対策状況

IPA では、2005 年から情報セキュリティの脅威に対する意識調査を、2013 年から倫理に対する意識調査を継続して実施しており、標的型攻撃やランサムウェア等の脅威に対する認知度、インターネットを利用する上で利用者に求められる各種対策、SNS 利用における意識、経験等を調査している。2020 年度に調査仕様を見直し、2021 年度調査は仕様変更後 2 回目の調査となった。本項では、同調査※257 のうち、情報セキュリティの脅威に対する意識調査について、主に追加分析を行った結果を紹介する。

(1) 使用機器の違いによる対策状況の差

脅威に対する意識調査はパソコン利用者とスマートフォン利用者※258 を対象に、それぞれの機器の特性や使用環境に応じた質問を設定し、実施している。調査結果では、総じてスマートフォン利用者のセキュリティ対策実施率※259（以下、対策実施率）が低い。具体的には、セキュリティ対策実施の有無を問う全 17 問中、スマートフォン利用者の対策実施率が 50% を超えるのは 3 問のみであった（表 2-4-7 の「A：全体」）。一方、パソコン利用者は全 20 問中、対策実施率が 50% を超える質問は 8 問※260 であった。そこでスマートフォン利用者の対策実施率の低さの要因を探るため、回答者属性等の追加分析を行った。

(2) スマートフォン利用者の対策実施状況

追加分析の結果を以下に示す。

スマートフォン利用者のセキュリティ対策実施状況	A: 全体（n=5,000）	B: スマートフォンのみを利用（n=1,749）	C: スマートフォンでの利用時間が長い（n=3,251）	B-C 差
（可能な機種の場合）OS のアップデート	51.6%	41.3%	57.2%	-15.9%
信頼できる場所（公式サイト、公式ストア等）からアプリをインストールする	56.4%	48.2%	60.8%	-12.6%
アプリをインストールする前または実行時に要求される権限を確認する	46.1%	38.8%	50.0%	-11.2%
端末内のアプリのアップデート	59.2%	53.0%	62.5%	-9.5%
紛失時などに備えたデバイス捜索対策	29.6%	22.4%	33.4%	-11.0%
リモートロックなどの不正利用防止機能	26.1%	20.0%	29.4%	-9.5%
パスワードや PIN、パターンなどによる画面ロック機能	46.4%	39.5%	50.1%	-10.7%
指紋認証・顔認証など、生体認証による画面ロック機能	42.9%	34.4%	47.5%	-13.1%
アプリをインストールする前にレビューやコメントなどを確認する	46.8%	40.3%	50.3%	-10.1%
デバイス内データ（写真、動画、個人情報など）のバックアップ	43.3%	35.8%	47.4%	-11.6%
セキュリティソフト・サービスの導入・活用	38.5%	26.4%	44.9%	-18.5%
重要な情報を扱うアプリの個別ロック機能の活用	24.9%	17.2%	29.1%	-11.9%
パスワード、指紋、ワンタイムパスワード等から 2 種類以上を組合わせる多要素認証の積極的な利用	39.3%	30.8%	43.8%	-13.0%
IoT 機器にアカウント設定があれば、購入後すぐにパスワードの変更等セキュリティ設定を実施	29.1%	22.1%	32.8%	-10.7%
セキュリティのサポートが終了した IoT 機器等の利用を止めている	27.3%	20.6%	30.9%	-10.3%
使わなくなった IoT 機器は、ネットから切り離している	30.1%	22.9%	34.0%	-11.0%
IoT 機器を廃棄する場合には購入時の状態に初期化している	29.6%	22.4%	33.6%	-11.2%

■表 2-4-7　スマートフォン利用者のセキュリティ対策実施状況比較

(a) インターネットを利用する機器の違いによる対策実施率

スマートフォン利用者向け調査は、事前調査の回答から、インターネットの利用をパソコンではなくスマートフォンのみで行う回答者※261と、パソコンも使っているがスマートフォンの方が利用時間が長い※262（以下、スマートフォンでの利用時間が長い）回答者を対象としている。サンプル総数 5,000 人のうち、2021 年度調査では「スマートフォンのみを利用」している人が 1,749 人、「スマートフォンでの利用時間が長い」人が 3,251 人であった。

スマートフォン利用者の対策実施率について、「全体」（以下、A 群）と「スマートフォンのみを利用している人」（以下、B 群）、「スマートフォンでの利用時間が長い人」（以下、C 群）、及び「B 群」「C 群」の実施率の差分を表 2-4-7（前ページ）に示す。

「A 群」の対策実施率が 50% を超えるのは「（可能な機種の場合）OS のアップデート」「信頼できる場所（公式サイト、公式ストア等）からアプリをインストール」「端末内のアプリのアップデート」の 3 問である。そして「B 群」「C 群」と「A 群」を比較すると、「B 群」の対策実施率が全設問で「A 群」より低く、逆に「C 群」は「A 群」より高い。「B 群」と「C 群」では、後者の方がおおむね 10% 程度対策実施率が高かった。表 2-4-7（前ページ）にあるスマートフォン利用者向けの設問の選択肢は、パソコンの使用経験から得られる知見等ではなく、ほとんどがスマートフォンに特化した対策事項である。にもかかわらず、「B 群」の対策実施率が低かった。この要因について以降で考察する。

(b) パスワード設定におけるセキュリティ対策実施率

パスワード設定における対策状況を比較した。パスワードのセキュリティ対策においても「B 群」の実施率が低いことが分かる（表 2-4-8）。「A 群」の母数 4,661 人は、事前質問においてインターネットサービスのアカウントを持っている人（パスワード設定の必要がある人）、また 3,930 人はインターネットのサービスアカウントを 2 個以上保有する人である。

表中の四つの対策のうち、最も実施率が低いのは「使いまわさない」であるが、「B 群」の対策実施率は 41.5%、初期パスワードを変更していない割合も 41.4% と少ない。「A 群」も 36.3% が、例えば Web サービスや IoT 機器等で提供される初期パスワードを変更しないまま、利用していることになる。

表 2-4-7（前ページ）及び表 2-4-8 のとおり、「B 群」は

	A: 全体（n=4,661）	B：スマートフォンのみを利用（n=1,578）	C:スマートフォンでの利用時間が長い（n=3,083）	B-C 差
推測されにくい	70.9%	67.1%	72.8%	-5.7%
出来るだけ長い	59.7%	54.4%	62.4%	-8.0%
初期パスワードを変更	63.7%	58.6%	66.3%	-7.8%
	（n=3,930）	（n=1,264）	（n=2,666）	B-C 差
使いまわさない	45.7%	41.5%	47.7%	-6.2%

■表 2-4-8　パスワード設定におけるセキュリティ対策実施状況

セキュリティ対策全般について、対策実施率が「A 群」より低い。「B 群」は事前アンケートで「現在はパソコンでインターネットを使っていない」を選択しており、調査時点で私物のパソコンを使わない、あるいは所有していない状況だったと考えられる。

このことから、現在、パソコンでインターネットを使っていないことと、セキュリティ対策の学びの少なさに関係があるのではないかとの仮説を立て、セキュリティ教育の受講経験の割合について調べた。

(c) セキュリティ教育の受講経験割合

「スマートフォン利用者」（以下、A 群）及び「パソコン利用者」（以下、D 群）のセキュリティ教育の受講経験割合を確認した（表 2-4-9）。「A 群」と「D 群」で比較すると前者が 1.8% 低いが大きな差ではない。次に「A 群」の中で、前節の「B 群」と「C 群」を比較すると「B 群」の受講経験が 6.6% 低かった。

昨今、パソコンを多用する職場では、社員教育の一環としてセキュリティ教育が進み、教育機会はある程度確保されていると考えられる。上記結果からも、パソコンの利用経験（所有）があることによって、情報セキュリティ教育の受講機会が得られ、セキュリティ対策やリテラシーの向上につながっている可能性がある。その一方で、「B 群」は、受講機会が得られにくく、対策の必要性への理

A 群：スマートフォン利用者（n = 5,000）	15.1%
B 群：スマートフォンのみでインターネットを利用（n = 1,749）	10.8%
C 群：スマートフォンでの利用時間が長い（n = 3,251）	17.4%
D 群：パソコン利用者（n = 5,000）	16.9%
B 群と C 群の差	-6.6%

■表 2-4-9　セキュリティ教育の受講経験割合の比較

解や対策実施率の低さにつながっている可能性が考えられる。セキュリティ教育の受講機会が「D 群」程ないと想定される「B 群」にとって自主的に受講機会を得るのは難しい。「B 群」に対し、どのようなセキュリティの学習（教育）機会をどうやって提供するかが課題と考えられる。

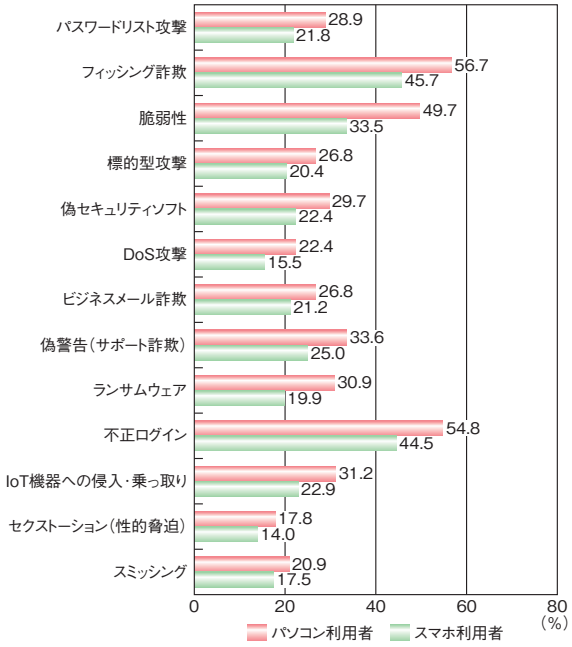
次に、受講経験の割合の低さと、回答者の属性との関係を確認するために「B 群」（1,749 人）のうち、受講経験のない 89.2%（1,560 人）の属性を調べた（表 2-4-10）。属性の分類においては職種によって回答が分かれることを想定し、会社員等職業従事者について、「情報システムや通信関係など IT 関連業務に従事、関与」している人とそうでない人とを分けて集計した。結果は、「パート、アルバイト」（20.8%）、「専業主婦・主夫」（20.0%）、「IT 業務に従事、関与※263していない会社員」（15.9%）、「無職」（14.4%）の順で割合が高かった。

この結果をまとめると B 群の職業に従事していない属性では「専業主婦・主夫」「無職」の割合が高かった。職業に従事する属性では「パート・アルバイト」「IT 業務に従事、関与していない会社員」の割合が高い一方で、「IT 業務に従事、関与している会社員」も一定程度の割合（7.1%）で存在した。こうした属性が混在する職場では、セキュリティ対策が十分にできていない可能性がある。

(3) 脅威名の認知度

各種セキュリティ脅威の認知度についてパソコン利用者とスマートフォン利用者の割合を比較した（図 2-4-20）。

総じて、パソコン利用者における認知度の方がスマートフォン利用者より高いが、認知度が過半数を超えるものは 2021 年度調査では「フィッシング詐欺」（56.7%）、「不正ログイン」（54.8%）の 2 点のみである。その他、社会人には比較的馴染みがあると思われる脅威名であっても、「ビジネスメール詐欺」（26.8%）、「標的型攻撃」（26.8%）、「DoS 攻撃」（22.4%）等の認知度は決して高くない。また、昨今国内でも深刻な被害が発生している「ランサムウェア」も 30.9% である。なお、各種脅威の認知度は過去の調査においても変動があまりなく、おおよそ上記と同様の割合、傾向である。



■図 2-4-20　パソコン及びスマートフォン利用者における各種脅威名の認知度比較

	属性	人数	受講経験割合		属性	人数	受講経験割合
IT 業務に従事・関与している	会社員	111	7.1%	IT 業務に従事・関与していない	会社員	248	15.9%
	公務員・団体職員	21	1.3%		公務員・団体職員	17	1.1%
	教職員	3	0.2%		教職員	2	0.1%
	契約・派遣社員	37	2.4%		契約・派遣社員	52	3.3%
	自営業・自由業・フリーランス	23	1.5%		自営業・自由業・フリーランス	37	2.4%
	経営者・役員	8	0.5%		専業主婦・主夫	312	20.0%
	医者	0	0.0%		無職（定年退職・家事手伝い含）	225	14.4%
	弁護士	0	0.0%		パート・アルバイト	325	20.8%
	医師・弁護士以外の専門職	26	1.7%		短大生・高専生	2	0.1%
	中学生	7	0.4%		大学生	7	0.4%
	高校生	50	3.2%		大学院生	2	0.1%
	専門学校生	4	0.3%		その他	41	2.6%

■表 2-4-10 「B 群：スマートフォンのみを利用」する人で受講経験のない人の属性別割合（n=1,560）

パソコン利用者とスマートフォン利用者とで認知度の差は、「脆弱性」が 16.2 ポイントと最も大きく、「フィッシング詐欺」「ランサムウェア」が 11.0 ポイント、「不正ログイン」が 10.3 ポイントと続いている。スマートフォン利用者がパソコン利用者と比べ、セキュリティ脅威の基本である「脆弱性」の認知度が低いのは、セキュリティ知識の不足の一端を表しているといえる。

(4) まとめ

これらの調査結果全体をとおし、セキュリティの対策実施率、教育の受講経験割合、脅威名の認知度、いずれにおいても、スマートフォン利用者がパソコン利用者に比べ低い傾向にあった。また属性でみると職業に従事していない「専業主婦・主夫」「無職」や、「パート・アルバイト」といった非正規雇用者において低い傾向にあった。こうした属性のスマートフォン利用者に対する教育機会の創出、提供が望まれる。

COLUMN

高齢者層の情報セキュリティ

2021 年 9 月 1 日に日本のデジタル社会実現の司令塔としてデジタル庁が発足しました。デジタルの活用により、一人ひとりのニーズに合ったサービスを選ぶことができ、多様な幸せが実現できる社会を目指し、安全・安心を前提とした「誰一人取り残されない、人に優しいデジタル化」を進めることを目標としています[i]。そのようなデジタル社会において、行政手続きや暮らしに関わるオンラインサービス等の恩恵を社会全体で享受するためには、インターネットやスマートフォンの積極的な活用が広まっていない高齢者層にも、今後はその活用が求められます。

デジタル社会の利便性を向上させていく一方で、情報セキュリティの確保は両立しなくてはならない課題です。特にインターネットやデジタル機器の扱いに慣れていない高齢者層の情報セキュリティの現状には、様々な課題があると考えられます。

具体的には、フィッシングや、偽サイト等のネット詐欺の被害事例が高齢者層で多く確認されています。例えば、独立行政法人国民生活センターが 2022 年 2 月 24 日に発表[ii]した、いわゆる「サポート詐欺」に関する相談における契約当事者の年齢は 60 歳以上が 5 割を超えていて、特に 70 歳以上が被害に遭っているとされています。パソコンやスマートフォン等の端末操作に不慣れで、セキュリティの知識がないことにつけ込まれているとのことです。このような状況からも、高齢者層の情報セキュリティに課題があることが分かります。

IPA は地域での普及啓発活動の一環として、2021 年度は高齢者層向けを意識した「インターネット安全教室[iii]」の開催に力を入れました。この教室では、「パスワードの作り方が分からない」「フィッシングの見分け方を教えて欲しい」「SNS、SMS、二段階認証などの言葉の意味が分からない」といった不安に対して説明を行っています。また、「情報セキュリティ安心相談窓口[iv]」においても、高齢者の方々から数多くの様々なご相談をいただき、それに対してアドバイスを提供しています。

「誰一人取り残されない、人に優しいデジタル社会」を実現するために、社会全体の取り組みとして、高齢者層の情報セキュリティリテラシー向上を目指していく必要があります。

i　デジタル庁：デジタル社会の実現に向けた重点計画　https://www.digital.go.jp/policies/priority-policy-program〔2022/5/23 確認〕
ii　独立行政法人国民生活センター：そのセキュリティ警告画面・警告音は偽物です!「サポート詐欺」にご注意!!　https://www.kokusen.go.jp/pdf/n-20220224_2.pdf〔2022/5/23 確認〕
iii　https://www.ipa.go.jp/security/keihatsu/net-anzen.html〔2022/5/23 確認〕
iv　https://www.ipa.go.jp/security/anshin/〔2022/5/23 確認〕

2.5 情報セキュリティの普及啓発活動

新型コロナウイルスの感染が収まらず、新型コロナウイルスに常に注意を向ける「with コロナ」の生活が続いている。

2020 年から急速な移行を求められたテレワークや、リモート授業・会議は今や日常のものとなり、「オンライン状態」にいる人が多くなっている。

このようにオンライン化が急激に進む中で、必要とされるネットリテラシーと様々な組織による普及啓発活動について述べる。

2.5.1 ネットリテラシーの重要性

新型コロナウイルスの感染拡大に伴い、インターネットを介した非接触のコミュニケーションが推奨され、リモートツール・サービスが我々の生活に浸透してきている。

(1) オンライン取引／契約の注意点

コロナ禍以降は外出の自粛により「おうち時間」が増え、自宅にいながら買い物を楽しんだり、外食の代替として料理の宅配サービスを利用したりと、通信販売の利用が増加した※264。65 歳以上のシニア層世帯でも利用が進んでいる※265 が、通信販売に不慣れだったシニア層がトラブルに巻き込まれるケースも増加している。

独立行政法人国民生活センターは、60 歳代以上から受けた通信販売に関する相談件数が、2020 年度に初めて 10 万件を超え、過去最高となったと発表した※266。60 歳代から 80 歳代以上のいずれの年代も、相談件数の上位は通信販売に関するものとなり、特に 70 歳代及び 80 歳代以上では、過去 5 年間で最も多くなった。

中でも、定額を支払う音楽や動画等の配信サービス利用や、サプリメント等の購入ができる「サブスクリプション」についての相談が多く、そのほとんどがインターネットで契約したものであった※267。具体的には「動画配信サービスの解約を忘れ、利用していないにもかかわらず代金を請求された」等の事例が報告されている。

このサブスクリプション契約に関する対策として、消費者庁は特定商取引に関する法律の通達改正（2022 年 2 月 9 日）において、「通信販売の申込み段階における表示についてのガイドライン※268」を公表した。この中で、「サブスクリプションに見受けられる、無償または割引価格の対象期間後、自動的に価格が変わる契約内容に移行するような場合には、あらかじめ支払い金額を明示する必要がある」としており、表示方法の改善が期待される。

また、政府は消費者契約法改正案を提出するとしており、改正されれば、利用者にとって契約内容や解約方法が分かりやすくなり、トラブルの減少につながることが予想される。

通信販売トラブルはシニア層だけのものではない。若年層の定期購入に関する相談も増加している※269。

1 回だけの「お試し」のつもりで申し込んだが、2 回目の商品が届き定期購入になっていたことに気づいた、等のトラブルが発生しており 10 ～ 20 歳代の若者が巻き込まれるケースも少なくない。このため、独立行政法人国民生活センターは「通信販売にはクーリング・オフ制度がない」「注文する前に販売サイトを隅々まで確認する」等、トラブル防止のポイントをまとめ、公表している※270。また、政府広報オンライン※271 や京都府消費生活安全センター等の公的機関が、定期購入に関する注意喚起動画（図 2-5-1）を公開しており、手軽に学べる機会が提供されている。

■図 2-5-1　定期購入に関する注意喚起動画
（出典）京都府「あなたも気をつけよう!～身近な消費者トラブル～お試し購入編※272」

SNS を介した「個人間融資」にも注意が必要である。コロナ禍による失業や収入の低下によって金銭面で困難な状態にある人が巻き込まれやすいとされる「個人間融資」では、法外な利息を要求されるトラブルが発生している。また、保証金としてお金をとられたり、個人情報が悪用され、さらなる犯罪被害に巻き込まれたりする恐れもある※273。

金融庁は、SNS 等で勧誘し、お金の貸し借りを行う「個人間融資」は、貸金業法の規程に抵触する場合があるとして注意を呼びかけている※274。また、神奈川県もヤミ

金融情報のページを開設[※275]し、成年年齢の引き下げを受け、啓発キャラクタを使用したリーフレットを公開する等して「絶対に借りないこと!」等のアドバイスを行っている。

(2) GIGA スクール構想

文部科学省が推進する GIGA スクール構想は、児童生徒に 1 台ずつ端末を提供し、個別最適化された学びや創造性を育む学びの実現を目指している(「2.4.3(2) 文部科学省における対策」参照)。「端末利活用状況等の実態調査(令和 3 年 7 月末時点)(確定値)[※276]」は、公立の義務教育段階の学校を設置する 1,812 の自治体の 96.2% において、児童生徒がタブレットやノートパソコンを活用できる環境が整ったことを示した。残る自治体でも、その 7 割は 2021 年度内に整備が完了するという。

端末を利用したオンライン授業は、通学の必要がなく、自分のペースで学習できる等のメリットがあるが、教員がそばで操作等について指導ができないため、児童生徒個々のネットリテラシーがより重要になる。

小学 1 年生～中学 3 年生の子どもを持つ保護者と、教員を対象とした「GIGA スクールにおけるセキュリティ実態調査 2021[※277]」を実施したトレンドマイクロ株式会社は、端末を受け取った児童生徒のうち、約 2 割が何かしらのトラブルを経験していると発表した。トラブルのうちセキュリティに関する主な項目は「アカウント(IDとパスワード)情報を盗まれる・悪用される(アカウントのっとり、不正アクセスの被害者となる)」(9.2%)、「不正アプリ(ウイルス)への感染」(7.8%)、「アカウント(ID とパスワード)情報を盗む・悪用する(アカウントのっとり、不正アクセスの加害者となる)」(7.1%)だった。また、「ネットの長時間利用による依存や、学業、健康への悪影響」(9.2%)、「不適切な Web サイトの閲覧」(5.0%)、「ネット上での見知らぬ人との出会い」(5.0%)等、情報モラル・リテラシーに関連する回答も挙がった。

文部科学省は「GIGA スクール構想の下で整備された 1 人 1 台端末の積極的な利活用等について(通知)[※278]」の中で、「情報モラル教育の一層の充実を図ること」を通知しており、「1 人 1 台端末の利用に当たり、保護者等との間で事前に確認・共有しておくことが望ましい主なポイント」として、「端末・アカウント(ID)・パスワードを適切に取り扱う」「就寝 1 時間前からは ICT 機器の利用を控える」「他人を傷つけたり、嫌な思いをさせることをネット上に書き込まない」等の項目を紹介している。また、「はじめてのパスワード指導」や「他人の情報の取り扱い方を考えよう」等、全国の自治体や学校による先進的な実践事例を紹介する Web サイト「StuDX Style[※279]」(図 2-5-2)を公開し、子ども達への指導の際の参考となる情報をまとめている。

■図 2-5-2 「StuDX Style」のホームページ抜粋
(出典)文部科学省「StuDX Style」

心身ともに成長段階にある子ども達は、様々なことを柔軟に吸収する。そして、その柔軟さ故にトラブルの経験は深い傷を残すことがあり、周囲の大人はトラブル回避に奔走する。しかし、当の大人はネット上のトラブルを回避できているだろうか。

IPA が公表した「2020 年度情報セキュリティの倫理と脅威に対する意識調査 -【脅威編】報告書 -[※280]」では、パソコンを利用する回答者のうち「脅威との遭遇経験が過去 1 年間にはなかった」とした人は 28.5% に過ぎず、10 代が最も遭遇経験が少ないとの結果となった。多くのパソコン利用者が何らかのトラブルを経験しており、大人にとっても脅威は身近にあるといえる。

子ども達の端末利用が進む中、大人もネット上の社会倫理や情報セキュリティについてともに学びながら被害を食い止めていかなければならない。

(3) ネット上の誹謗中傷への対策

SNS 等を介したコロナ感染者に対する差別的な発言は後を絶たない。感染者のみならず、医療従事者やその家族までがターゲットとなり、心ない書き込みによって苦しめられている。

法務省人権擁護局は TikTok と連携し、インターネット上の人権侵害防止のキャンペーンを展開した(次ページ図 2-5-3)。TikTok アプリ内に特設ページを開設し、「誹謗中傷」「SNS いじめ」及び「個人情報の取扱い」に関する啓発動画を計 7 本公開している。動画は、人気のクリエイターの協力により制作され、TikTok を利用する若者に向けて人権尊重を訴えた。また、中傷被害を受けている人が相談する窓口の情報も掲載された。

■図 2-5-3 「#誰かのことじゃない～ネットの誹謗中傷・SNS いじめ・個人情報の取扱い～」キャンペーン
（出典）法務省人権擁護局の Tweet※281

コロナ差別への取り組みは、地方自治体でも独自に展開されている。

例えば石川県は「Stop! コロナ差別！」と題した啓発活動を行うとともに、AI を活用して SNS や掲示板を始めとする閲覧可能な Web サービス全般をチェックし、差別的な書き込みを収集している※282。収集した情報は、被害者が訴訟を起こす際の証拠資料として活用できるよう県が保管している。同様の取り組みは、福井県、愛知県、和歌山県、岡山県等でも実施されており、このうち、和歌山県※283 では、条例でプロバイダの責務を規定し、誹謗中傷等の削除や、投稿の抑止のための広報活動等を依頼している。

(4) 新型コロナウイルスに関するフィッシング

2021 年 6 月、「自衛隊大規模接種センター」をかたる新型コロナワクチン接種の予約サイトの案内メールを送信し、フィッシングサイトに誘導する手口が発覚した※284。メールに記載されている URL をクリックするとワクチン接種に関するポータルサイトのようなページに辿りつき、氏名や住所、更にはクレジットカードの情報を入力する画面が表示される。独立行政法人国民生活センターは送信元やメールのタイトルに心当たりがない場合は、クリックやタップをせず、「新型コロナ関連詐欺 消費者ホットライン※285」に相談してほしいと呼びかけている。

また、「新型コロナウイルス特別定額支援金」という偽サイトに誘導する手口も報告されており、厚生労働省は注意を呼びかけている※286。

コロナ禍の不安につけ込んだ同様の手口は、今後も発生する危険がある。受信したメールを鵜呑みにしてメール内のリンクをクリック／タップすることのないよう注意したい（「1.2.7 (3) 世の中の関心に乗じる手口」参照）。

2.5.2 恒常的な啓発活動

ここでは、コロナ禍以前から継続的に実施されている情報セキュリティ・情報リテラシーに関する啓発活動について述べる。

(1) SNS 事業者等による対策

2022 年 1 月、他人の SNS のアカウントに無断でログインした等により不正アクセス禁止法違反容疑で男が逮捕された※287。容疑者は、アカウント名から氏名や生年月日等を割り出し、パスワードを推測していたとされ、ID やパスワードの管理の重要性を改めて知らしめた。

SNS のセキュリティ強化として、Twitter Japan 株式会社は Twitter を安心して使うための「プレイブック日本語版」を 2021 年 12 月に公開した（図 2-5-4）。プレイブックは「安心して使う」「安全を確保する」及び「自分のデジタルフットプリントを管理する」という目的で、該当する機能の紹介を行うものである。シチュエーションごとに有効な機能をフローチャートで紹介し、アカウントの安全を確保するための設定方法等について記載しており、活用が望まれる。

■図 2-5-4 Twitter プレイブック日本語版
（出典）Twitter Japan 株式会社「Twitter の安全機能をまとめた「プレイブック」日本語版を発行※288」

Instagram も、「プロフィール情報の確認」や「ログイン情報を共有しているアカウントの特定」等の「セキュリティに関する確認」4 項目を通知して、アカウントを安全に管理するための設定を促す取り組みを開始している※289。

また、ネット上のハラスメントや権利侵害、若年層保護に対する対策も進んでいる。

Instagram は、急激に注目を集めた利用者を誹謗中傷等から守る機能として「抑制」機能を発表した※290。これは、自身をフォローしていないアカウントや、最近フォローしたばかりのアカウントから届くコメントや DM リクエストを自動的に非表示にするものである。また、若年層保護を

目的として、16 歳未満の全アカウントについて初期設定を「非公開」にすること、若年層のアカウントにブロックされた成人のアカウントは、若年層とやり取りすること等ができなくなる機能を加え、対策を強化した※291。

YouTube は、低評価の数を非表示にすると発表した※292。本来は、動画の内容の良し悪しを判断できるよう設けられた機能だが、動画の内容ではなく動画のクリエイターに対する悪意ある低評価や嫌がらせに使用されるケースが発生しており、このようなハラスメントからクリエイターを守るためとして、2021 年 11 月 10 日から順次展開している。

ヤフー株式会社は、「Yahoo! ニュース」の記事に対し、利用規約等に違反する投稿を繰り返す利用者への対策を始めたと発表した※293。不適切投稿の抑止を目的としたもので、「発信者情報開示請求等を受けた場合、法令上の手続きにのっとり開示を行う場合がある」といった違反投稿を続けた場合に起こり得る法的なリスクを画面に表示する。

このようにサービス事業者の取り組みが進んでおり、利用者側の意識の成熟も望まれる。

(2) 成年年齢引き下げに伴う啓発

2022 年 4 月より成年年齢が 18 歳に引き下げられた。これまで若者は、未成年者取消権によって守られ、親権者の同意を得ずに締結した契約は後から取り消しができた。しかし、成年年齢の引き下げにより、18 歳、19 歳の人はこの保護の対象外となる。

18 ～ 19 歳の新成人となる層から消費者庁、自治体等の消費生活相談に寄せられたトラブルでは、健康食品や化粧品に関するもののほか、デジタルコンテンツや出会い系サイトに関するものが多くみられた※294。これらのトラブルに巻き込まれるきっかけは SNS の広告や書き込み等に誘導されるケースや SNS 上の知り合いから誘われるケース等が挙げられている。

成人と言っても、経験したことのない事柄について判断するのは容易ではない。また、ネット上では、相手の顔が見えない状態で言葉巧みに言いくるめられ騙されることも考えられる。

消費者庁では、「『18 歳から大人』特設ページ※295」を開設して啓発動画を公開したり、Twitter による情報発信を行ったりしている。また、総務省も「インターネットトラブル事例集」の中で「成人年齢の引き下げにあたって学んでおきたいこと※296」をまとめた Web ページを公開している。

法務省も「大人への道しるべ※297」という漫画とクイズで学べるホームページを開設した（図 2-5-5）。「大人って何?」や「契約は人と人との約束」等の項目のほか、「SNS は便利で怖い」や「その動画、アップして大丈夫?」等、ネットにまつわるテーマの漫画とクイズが公開され、ネット上での振る舞いや責任について改めて考えることができる。

■図 2-5-5 「大人への道しるべ」のホームページ抜粋
（出典）法務省「大人への道しるべ」

また、公益社団法人日本消費生活アドバイザー・コンサルタント・相談員協会も「18 歳からのスマート通販学※298」という電子書籍を公開した。「インターネット通販のメリット / デメリット」や「投げ銭型ライブ配信サービス」の注意点等の事例と、トラブルに巻き込まれた際の相談窓口が分かりやすく紹介されている。新たに成人になる 18 ～ 19 歳のみならず、インターネット通販を利用するすべての人に有効な情報であり、活用が推奨される。

(3) オンラインゲームにおけるチート行為対策

2021 年 6 月、日本初のシニアによる e スポーツプロチームが発足した※299。高齢者の健康増進・維持としての活用だけでなく、世代や地域を超えるコミュニケーションを可能にする点でも e スポーツは注目されている。

2021 年 10 月には経済産業省が、社会人 e スポーツリーグ「AFTER 6 LEAGUE」を国の機関としては初めて後援する※300 等、国を挙げた盛り上がりを見せ始めている。

オンラインゲームを活用した e スポーツが競技として楽しまれている一方で、オンラインゲームを悪用した手口による事件も発生している。

京都府警察本部サイバー犯罪対策課はゲームを有利に進めるための「チート行為」を行ったとして 5 人を書類送検した※301。容疑は、ゲーム会社のサーバに不正なデータを送信し、ゲーム内のアイテムを不正に入手する

等した私電磁的記録不正作出・同供用にあたるとしている。過去には、チート行為が「著作者人格権侵害」や「電子計算機損壊等業務妨害罪」となった事例※302もあり、安易にチート行為を行わないよう啓発が必要である。

また、オンラインゲームの開発者にも不正防止の対策が必要である。株式会社ラックは、オンラインゲームのチート対策の知見を集めたホワイトペーパー「オンラインゲーム、スマートフォンゲームのセキュリティ～チートの脅威と対策について～」を開発者向けに公表した※303。

作り手側と使用者側双方の意識向上が望まれる。

(4) 誰も取り残さないセキュリティ・リテラシー

NISCは、セキュリティには「全員参加による共同、普及啓発」が重要だとしており、2022年サイバーセキュリティ月間（2月1日～3月18日）のキャッチフレーズを「#サイバーセキュリティは全員参加」として、国民全体の意識向上を目指す普及啓発活動を行っている。2022年の主なイベントとして「ランサムウェア攻撃対応・東京2020大会の対策から学ぶ※304」と題したセミナーがオンライン配信されたほか、チェコ、フランス、ドイツを始めとする海外のサイバーセキュリティ関係当局及び、日本のサイバーセキュリティ関係省庁が参加した国際サイバーセキュリティワークショップ・演習が開催され※305、インシデント発生時の対処能力の向上、知見の共有が行われた。

また、政府広報オンラインでも、サイバーセキュリティ月間の期間中「家族みんなで考えよう！安全・安心なインターネットの利用※306」という動画を公開し、進級・進学を機にスマートフォンを利用する子どもとその保護者に向けた啓発を行った。

2.5.3 インターネットがもたらす未来

株式会社オリィ研究所が2021年6月に開店した「分身ロボットカフェDAWN ver. β※307」では、筋萎縮性側索硬化症（ALS）等の重度の障害により外出が困難な人が、全国各地から分身ロボットを遠隔操作し接客を行っている（図2-5-6）。これは、健常者が行っているリモートワークの発展形という見方もあり、障害を持つ人の社会参加の場のみならず、コロナ禍において人と人との接触を減らす役割を果たすことも期待できる。

■図2-5-6　分身ロボットカフェ DAWN ver. β
（出典）株式会社オリィ研究所「分身ロボットカフェ DAWN ver. β」

このように、インターネットの技術及び関連するツールは、生活インフラであるという点での重要性のみならず、未来の生活に恩恵をもたらすものである。ただし、インターネットの利用場面が増えると、情報セキュリティ対策が必要な場面も増えていく。また、いかに有用であっても、それを使いこなす側に悪意があれば、一転して我々を脅かす武器になってしまう。悪意がなくても、無知や配慮の欠如によって他者への攻撃になってしまうこともあり得る。

一人ひとりが「有用なツールを正しく使いこなすことができているのか」と自らに問い続け、被害者にも加害者にもならないという意識と行動が一層必要とされている。

COLUMN

インターネット上の戦い

こんにちは！　ぼくは、IPA「ひろげよう情報モラル・セキュリティコンクール」応援隊長のまもるです。ぼくたちは今、新型コロナウイルスに負けないように、マスクを着け、手洗いと換気をして戦っているよ。

そして、地球上ではコロナとは別の戦いが二つ起きています。戦車や爆撃などによる「地上戦」、もうひとつは「サイバー戦争」。ぼくたちが住んでいるところからは遠い国同士の戦いだと思っていたのだけれど、インターネットには国境がないから、「よその国のお話」では済まされないんだと、お父さんが話してくれました。

サイバー戦争で何が起きるのかを調べてみたら、ぼくたちの生活に大きく影響することがわかりました。鉄道や電気、ガス、水道を管理するシステムが攻撃されると、生きるために必要なものを手に入れられなくなるよね。それに、原子力発電所が攻撃されて、制御ができなくなったとしたら……。

ほかにも、もし国に関係するWebサイトが改ざんされてしまうと、自分たちの国がどんな情報を発信しているのか、わからなくなってしまうね。何か嘘の情報を書かれていたとしても、改ざんされていることを知らなかったら、ぼくたちはその情報を信じて間違った行動を起こしてしまうかもしれない。

実際に、ある国の大統領の偽の動画がネットに公開されたことがあったよ。武器を捨てて降伏するよう市民に訴えるディープフェイクだったんだけど、大統領のお話なら信じてしまいそうだよね。

それから、サイバー戦争は、二つの国の間だけで起きているわけではなくて、「攻撃されている国」を助けるという目的で、「攻撃している国」にハッカー集団がサイバー攻撃をしかけているんだって。「攻撃している国」の国営テレビなどをハッキングして戦地の映像を放送した、とSNSに投稿したっていうよ。でも、本当に映像が流れたのかな?

そのハッカー集団はもともといろんな国の政府や企業にサイバー攻撃を繰り返している人たちで、いつもはみんなが怖がったり非難したりしている存在だから、信じて良いかどうかぼくには判断ができなかったよ。それなのに、世界中の多くの人が「良くやった!」とか「かっこいい!」と称賛する書き込みをしたりして、頭のなかがこんがらがってしまいました。こんなふうに、情報はぼくたちを混乱させ、時には間違った方向に導くこともあるんだね。だから、発信する内容も閲覧する内容もよく確認しなくてはいけないんだ。

それと、ショッキングな情報ほど目について誰かと共有したくなっちゃうんだけど、不確かな情報をむやみに拡散することを止めなくちゃね。安易な拡散によって、いつのまにか自分が誰かを「攻撃する側」に立っていた、なんてことにならないように。

2.6 国際標準化活動

国際標準とは、製品や技術を、国境を越えて利用するために制定される国際的な共通規格であり、国際規格とも呼ばれる。本節では、日本の国際標準化活動への取り組み、及びセキュリティ分野に関わる国際標準化活動の動向を紹介する。

2.6.1 様々な標準化団体の活動

日本の国際標準化活動への取り組みと、作成プロセスや作成組織の違いから見た標準の分類、及び情報セキュリティ分野の主な標準化団体の概要を示す。

(1) 日本の国際標準化活動への取り組み

企業が培ってきた技術や知的財産の秘匿化や、それらを知財として権利化する「クローズ戦略」に対して、標準化は「オープン戦略」に位置付けられている。クローズ戦略により企業のコア領域を守り、他社との差別化を図ることは重要であるが、その技術を利用する市場が広がらなければ、企業としては事業を拡大することが困難である。コア領域を守りつつ、市場を拡大する「オープン&クローズ戦略」が必要である。技術の発展、市場のグローバル化が進み、このオープン&クローズ戦略の考え方は企業にとどまらず、国の政策として位置付けられるようになった。

既に、主要国では、自国に有利な標準化を目指し、官民を挙げて標準化活動に取り組んでおり、例えば、米国の国立標準技術研究所（NIST：National Institute of Standards and Technology）では、政府・国内企業向けの標準策定に関与し、技術的知見や評価結果の提供、民間利害関係者間の調整、政府からの指示を受けた標準化案の検討等を行っている。中国の中国標準化研究院や中国工程院、ドイツのフラウンフォーファー研究機構といった組織でも標準化の取り組みが行われている。日本でも公的機関が民間の標準活用戦略活動を支援することが望ましいとして、国立研究開発法人産業技術総合研究所、IPA、NICT、国立研究開発法人農業・食品産業技術総合研究機構、一般財団法人日本規格協会（JSA：Japanese Standards Association）等の関係機関をネットワーク化し、ワンストップで支援する協働体制「標準活用支援サービスプラットフォーム」を整備した※308。

(2) 標準の分類

国際標準には、公的な標準化団体により所定の手続きを経て行われる「デジュール標準（de jure standard）」、いくつかの団体（企業等）が協力して自主的に作成する「フォーラム標準（forum standard）」、公的な標準化団体を介さず、市場や業界において広く採用された結果として事実上標準化される「デファクト標準（de facto standard）」がある。

デジュール標準では、幅広くステークホルダーを集めて議論をとおして合意形成を行う。次項で紹介するISO、IEC、ITUが作成する国際規格やJIS等の国家規格が該当し、策定プロセスが規定されており、様々な規制等に用いられることも多い。合意形成のために複数の検討段階が設定されており、正式に発行するまでに時間がかかる（ISO/IECは約3年）。

フォーラム標準は業界団体等、共通の関心を持つ企業等が集まって議論し、業界ルール等限定的な範囲で合意される標準である。作成スピードは速く、業界の特性が反映されていることから、該当する業界内では利用が促進されやすい。次項で紹介するIEEE、IETF、TCGが発行する標準が該当する。フォーラム標準はコンソーシアム標準と呼ばれることもある。業界のフォーラム標準が、その後、国際標準化団体に提案され、時間をかけてデジュール標準となる場合もある。

電気製品やIT製品等、開発サイクルの短い分野では、その時点の市場で一般的な規格としてデファクト標準が採用される傾向にある。例えばWindowsのようなOSやGoogleのような検索エンジン等、グローバルなIT企業の製品・サービスが事実上の国際標準となる傾向があり、合意形成プロセスは存在しない。

(3) 情報セキュリティ分野に関する標準化団体

情報セキュリティに関連するデジュール標準やフォーラム標準の策定を行っている主な国際標準化団体を以下に示す。

- ISO（International Organization for Standardization：国際標準化機構）/IEC（International Electrotechnical Commission：国際電気標準会議）JTC 1（Joint Technical Committee 1：第一合同技術委員会）※309：情報セキュリティを含む情報技術の国際規格を策定している。コンピュータや情報分野を扱う国際標準化団

体としてISO、IECはそれぞれ独立に存在しているが、扱う領域の競合を避けるために双方が連携し、JTC1が設立された。日本国内の標準化団体としては、日本産業標準調査会（JISC：Japanese Industrial Standards Committee）がISO、IEC双方のメンバーであり、JTC 1でも活動している※310。

- ITU-T（International Telecommunication Union Telecommunication Standardization Sector：国際電気通信連合 電気通信標準化部門）：電気通信技術に関わる国際規格を策定している。情報セキュリティに関してはSG（Study Group）17が設置され※311、ISOや後述するIETFとともにネットワークやID管理等に関する標準化活動を行っている。策定した標準はITU勧告として定められる。

また、情報セキュリティ分野に関するフォーラム標準を策定する代表的な組織として、以下がある。

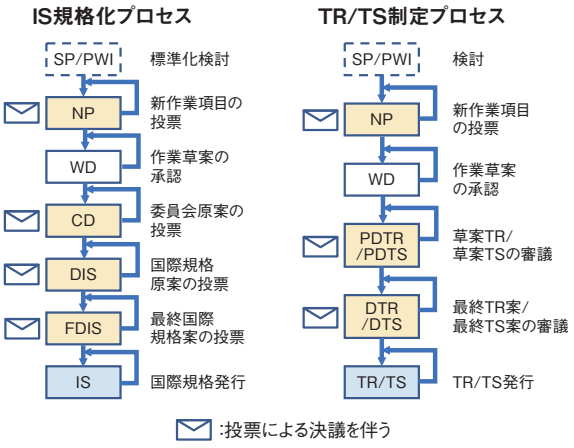
- IEEE（The Institute of Electrical and Electronics Engineers, Inc.）：
  電気工学・電子工学技術に関する国際学会である。標準化活動は内部組織であるIEEE-SA（Standards Association）が行っている。情報セキュリティについては、サイバーセキュリティ、ネットワークセキュリティ、IoTセキュリティ等の広範な領域で標準化を行っている。
- IETF（Internet Engineering Task Force）：
  インターネット技術の国際標準化を行う任意団体である。非常にオープンな組織であり、作業部会のメーリングリストに登録することで誰でも議論に参加できる。情報セキュリティについては、インターネット上のセキュアなプロトコル、暗号、デジタル署名、認証、セキュリティ情報連携（セキュリティオートメーション）等の方式の標準化を行っている※312。標準化した技術文書はRFC（Request For Comments）として参照できる。
- TCG（Trusted Computing Group）：
  信頼できるコンピューティング環境（組み込み機器、パソコン／サーバ、ネットワーク等）に関するセキュリティ技術の標準化を行う業界団体である。ハードウェア、ソフトウェア等のベンダやシステムインテグレータがメンバーとなり、中国、日本にregional forumがある※313。

2.6.2 情報セキュリティ、サイバーセキュリティ、プライバシー保護関係の規格の標準化（ISO/IEC JTC 1/SC 27）

ISO/IEC JTC 1/SC 27（以下、SC 27）は、ISO及びIECの合同専門委員会（ISO/IEC JTC 1）において、情報セキュリティに関する国際標準化を行う分科委員会（SC）である。SC 27は、テーマ別に以下の五つの作業グループ（WG）で構成される。

WG 1：情報セキュリティマネジメントシステム
WG 2：暗号とセキュリティメカニズム
WG 3：セキュリティの評価・試験・仕様
WG 4：セキュリティコントロールとサービス
WG 5：アイデンティティ管理とプライバシー技術

ISO/IECにおける標準化作業は、策定する仕様の完成度によって図2-6-1のような状態があり、それぞれ各国の投票によって次の段階へ進む。なお、ISOにおいて、技術が未成熟である、またはガイダンス等の標準仕様ではないが重要であるとされたものは、技術報告書または技術仕様書として出版する。



■図2-6-1　ISO/IEC JTC 1/SC 27における文書のステータス
（出典）JISC「ISO規格の策定手順※314」を基にIPAが作成

図2-6-1の各文書のステータスと略号は以下のとおりである。

SP：研究期間（Study Period）
PWI：予備業務項目（Preliminary Work Item）
※SPとPWIのどちらを実施するかはWGによって異なる。
NP：新作業項目（New work item Proposal）
WD：作業原案（Working Draft）
CD：委員会原案（Committee Draft）
DIS：国際規格原案（Draft International Standard）
FDIS：最終国際規格案（Final Draft International Standard）
IS：国際規格（International Standard）
PDTR：予備技術報告原案（Preliminary Draft Technical Report）
PDTS：予備技術仕様書原案（Preliminary Draft

Technical Specification）
DTR：技術報告書原案（Draft Technical Report）
DTS：技術仕様書原案（Draft Technical Specification）
TR：技術報告書（Technical Report）
TS：技術仕様書（Technical Specification）

以下に、各 WG の活動概要を述べる。なお本文中では略号を使用する。

（1）WG 1（情報セキュリティマネジメントシステム）

WG 1 では、情報セキュリティマネジメントシステム（ISMS：Information Security Management System）に関する国際規格として、ISO/IEC 27001（ISMS 要求事項を示す規格）及び ISO/IEC 27002（情報セキュリティ管理策及び実施の手引きを示す規格）を中心に、ISO/IEC 27001 が示す ISMS 要求事項に関する手引きや指針を提供する規格、ISO/IEC 27001 及び ISO/IEC 27002 を土台とする分野別規格、及びその他トピックスに関する ISO/IEC 27000 ファミリー規格の国際標準化活動を実施している。

(a) ISO/IEC 27001 及び ISO/IEC 27002 の改訂に関する状況

ISO/IEC 27002:2013 は、1 年間の SP において、次期改訂の設計仕様（Design Specification）を決定後、2018 年 3 月より改訂作業が開始されていたが、2022 年 2 月に改訂版が発行となった。

本改訂では、管理策群の内容としては、基本的に 2013 年版を踏襲しており、それに新しい脅威や技術に合わせて、新規管理策が追加されている。一方で、管理策の構成については、2013 年版から大きく変更されている。ISO/IEC 27002:2022 には、2013 年版管理策との対応表も Annex として掲載されているので、旧管理策との対応や新規管理策を確認することができる。

ISO/IEC 27002:2022 の管理策の構成等が 2013 年版から大きく変わることを受け、ISO/IEC 27001：2013 Annex A との不整合が発生する状況が望ましくないことから、ISO/IEC 27001 を限定的に改訂することが合意された。具体的には、ISO/IEC 27001:2013 Annex A を ISO/IEC 27002:2022 と整合するように変更することに伴う改訂のみを実施する。手続きとしては、まず、Annex A の入れ替えに関連する内容を Amendment（追補）として発行し、先に発行済みの 2 件の Corrigendum（正誤表）の内容も含め、ISO/IEC 27001 の新たな版として 2022 年に発行予定である。

一方、ISO/IEC 27001:2013 の内容を見直す改訂の必要性も認識されており、上記の限定的な改訂を終えた後の次期改訂に向け PWI を設置、検討を開始している。

(b) ISO/IEC 27002:2022 発行の他規格への影響

ISO/IEC 27002:2022 発行に伴い、ISO/IEC 27002:2013 を年号付きで引用、参照している規格は参照元を失ったことになる。また、仮に年号付きで引用、参照していなくとも、今回の改訂で構成が大きく変わったこと等を考慮すると、ISO/IEC 27002 を引用、参照する規格はいずれも何らかの見直しが発生すると想定できる。

最も影響が大きいのは ISO/IEC 27001 であるが、これについては、前述のとおり Annex A を整合するための限定的改訂を現在実施中である。

次に影響が高いものとして、セクター規格がある。ISO/IEC 27011:2016 は、電気通信業界内の組織における、ISO/IEC 27002 に基づいた情報セキュリティマネジメント導入を支援するガイドライン規格であり、ISO/IEC 27002:2013 をベースに追加の管理策やガイダンスが記されている。SC 27 と ITU の共同文書でもある。本規格は、ISO/IEC 27002 改訂版発行を待たずに改訂作業を開始しており、現在 CD ステージである。ISO/IEC 27017:2015 は、クラウドサービスのための情報セキュリティ管理策実践の規範を提供する規格であり、同様に、ISO/IEC 27002:2013 をベースに追加の管理策やガイダンスを提供する。規格の普及状況等を考慮しても、ISO/IEC 27002:2022 発行の影響は大きいため、本規格についても改訂に向けた作業を開始、PWI を設置した。一方、ISO/IEC 27010:2015 は、ISO/IEC 27002 をベースにしたセクター規格でありながらも、改訂による影響は大きくないと判断され、改訂は見送られた。また、エネルギー業界向けセクター規格である ISO/IEC 27019:2017 については、改訂は今後の検討課題となっており、まだ決定していない。

また、ISO/IEC 27001 や ISMS についてのガイダンスを提供する他のガイドライン規格（ISO/IEC 27003:2017、ISO/IEC 27004:2016、ISO/IEC TS 27008:2019 等）についても、ISO/IEC 27002 による影響は想定されるが、セクター規格への対応が優先され、セクター規格に次いだ検討項目となっている。

(c) その他の ISO/IEC 27000 ファミリー規格の国際標準化活動

ISO/IEC 27002:2022 の改訂とは直接関係のない、その他の規格の動向として次がある。

情報セキュリティリスクマネジメントに関するガイドライン規格 ISO/IEC 27005:2018 は、ISO/IEC 27001:2013 への本格的対応を積み残していることから改訂作業中であるが、2022 年 4 月時点で DIS を審議中である。ISO/IEC 20000-1 及び ISO/IEC 27001 の統合実践に関するガイドライン規格である ISO/IEC 27013:2015 は、ISO/IEC 20000-1:2018 の発行を受けて、2021 年 11 月改訂版が発行された。ISMS 専門家の力量に関する要求事項を提供する ISO/IEC 27021:2017 は、2021 年に追補を発行した。

(2) WG 2 (暗号とセキュリティメカニズム)

WG 2 では、暗号プリミティブ (暗号アルゴリズム) や、デジタル署名技術、鍵共有のような汎用的かつ基本的な暗号プロトコル等の標準化を行っている。WG 2 の国際主査、副主査ともに日本人が選出され、WG 2 での活動をリードしている。2021 年度は、新しい規格である「鍵管理　第 7 部 : クロスドメイン・パスワードに基づく認証鍵交換 (ISO/IEC 11770-7)」と「暗号アルゴリズム　第 3 部 : ブロック暗号　追補 1 (ISO/IEC 18033-3/AMD1)」の 2 件、及び既存規格 6 件の改訂版が発行された。このほかの主な活動内容について以下に示す。

(a) PWI

2022 年 5 月時点の主な PWI は、以下のとおりである。個別に議論され、標準化すべきとの判断となった場合、標準化に着手する。なお、最後の項目については、日本から提案された。

- 調整値付き (tweakable) ブロック暗号の利用モード
- 算術演算暗号アルゴリズム (ハッシュ関数を含む)
- 安全なマルチパーティ計算 – 第 3 部 : ガーブル回路※315 を用いたメカニズム
- ID 情報に基づく認証鍵交換の追加メカニズム

(b) 新型コロナウイルス感染拡大の影響によるプロジェクト進捗遅延

WG 2 では、「匿名デジタル署名　第 3 部 : 複数の公開鍵を用いたメカニズム (ISO/IEC 20008-3)」のような、大学関係者がエディタをしているプロジェクトが多くあり、オンライン授業等の対応を優先しなければならなかったため、いくつかの規格作成のスケジュール遅延が目に付くようになっていた。2022 年度に入り、当該大学関係者も標準化作業に時間を割くことができるようになり、これから標準化作業の加速が期待される。

(3) WG 3 (セキュリティの評価・試験・仕様)

WG 3 は 2021 年 10 月、2022 年 4 月にオンライン会議にて定期会合を開催した。それらの会合の議論内容、特に 2021 年度に標準化が承認されたプロジェクトに焦点を当て以下に概説する。

(a) ISO/IEC 5888 "Information security, cybersecurity and privacy protection — Security requirements and evaluation activities for connected vehicle devices"

UNECE (United Nations Economic Commission for Europe : 国際連合欧州経済委員会) の自動車基準調和世界フォーラム WP.29 にて自動車のサイバーセキュリティ基準が採択されたことを受け、自動車業界はその基準への対応を迫られている。自動車の主要なコンポーネントである車載 Engine Control Unit (ECU) に関する技術的詳細を記したサイバーセキュリティ基準は存在していない一方で、多くの脆弱性が検出されている。そのため、WG 3 では 2019 年 4 月テルアビブ会合から車載 ECU のセキュリティ評価基準に関する議論を開始し、2022 年 3 月に ISO/IEC 5888 の開発が承認された。

ISO/IEC 5888 は、車載 ECU に対し具体的にどのようなセキュリティ要件 (例えば、暗号に対する要件や、データ保護に関する要件等) を課すべきか、そのセキュリティ要件を満たしていることを確認するため、どのような脆弱性分析やテストを実施すべきかを定める国際標準である。自動車業界が ISO/IEC 5888 に定義されたテスト等を実施することにより、WP.29 自動車サイバーセキュリティ基準や、その基準において参照されている、自動車のライフサイクル全般にわたるサイバーセキュリティ対策を定めた ISO/SAE 21434 "Road vehicles — Cybersecurity engineering" への適合を主張できることを念頭に置いている。

本国際標準は、情報セキュリティやサイバーセキュリティに関わる国際標準を開発する ISO/IEC JTC 1/SC 27 (Information security, cybersecurity and privacy protection)、及び車載の電気・電子コンポーネントに関わる国際標準を開発する ISO/TC 22/SC 32 (Electrical and electronic components and general

system aspects）の両方に関係するため、双方のSCのJWG（Joint Working Group）6をISO/IEC JTC 1/SC 27配下に設立し、そのJWG 6にて標準開発することで合意されている。共同議長や共同プロジェクトリーダーは双方のSCから既に選出されており、今後メンバー募集終了後、本JWG 6における国際標準活動が開始される予定である。なお、SC 27側の共同プロジェクトリーダーとして日本のエキスパートが指名され、今後ISO/IEC 5888の開発に深く関わることとなる。

(b) ISO/IEC TS※316 9569 “Information security, cybersecurity and privacy protection — Towards Creating an Extension for Patch Management for ISO/IEC 15408 and ISO/IEC 18045”

ISO/IEC 15408に基づくIT製品のセキュリティ評価・認証制度では、IT製品の特定のバージョン・リビジョンに対し評価・認証を実施し、合格したIT製品に認証書が付与される。しかしながら評価・認証が完了したバージョン・リビジョン（例えばIT製品V1R1）に更新プログラムが適用されると、その認証書は更新されたバージョン・リビジョンの製品（IT製品V1R2）に対しては有効ではない。それは、評価・認証を経ていない更新プログラムを適用することにより、新たな脆弱性が混入される可能性があるからである。IT製品に対する軽微な更新の場合は、保証継続と呼ばれる、評価・認証より簡易な仕組みによって、更新されたバージョン・リビジョンの製品に対し認証書を再発行することもできるが、修正量が多い場合は、再度評価・認証を実施し新規の認証書を更新製品に対し発行する必要がある。しかしながら更新が頻繁に発生するIT製品においては、その都度保証継続、あるいは再評価を実施するのは現実的ではない。

本ISO/IEC TS 9569は、上記の問題を解決するため、開発者がセキュアな更新プログラムを開発する際に順守すべき更新プログラムの管理要件や、攻撃者により改変された更新プログラムが適用されることを防ぐためにIT製品が満たすべきセキュリティ機能要件等を定める。現在EUで創設が進められているサイバーセキュリティ認証スキームEUCC※317においては、更新プログラムを適用した際に認証書を更新する仕組みを導入する予定である。EUCCの評価・認証フレームを記した規定文書※318が公開されているが、その認証書更新の際の参照文書としてISO/IEC TS 9569を指定しており、ISO/IEC TS 9569は将来的に欧州における認証書更新の指針となる可能性もある（EUのセキュリティ認証制度については「3.4.2 (3) (b) セキュリティ認証スキームとセキュリティ市場分析」参照）。

(4) WG 4（セキュリティコントロールとサービス）

WG 4では、WG 1が対象とするISMSを実施・運用する際に必要となる具体的なセキュリティ対策、及びセキュリティサービスの標準化を行っている。以下に、WG 4における2021年度の主な成果、活動を紹介する。

(a) IoTのセキュリティとプライバシーのための標準化活動

WG 4では、IoTのセキュリティとプライバシーに関わる標準化として、以下の三つの活動を継続的に進めており、加えて今期は新しい課題の検討がPWI 27404: Cybersecurity Labelling for Consumer IoTとして始まった。これらの規格は、Cybersecurity – IoT security and privacyと名付けられたプロジェクト群（ISO/IEC 27400シリーズ）として規格番号が振られ、規格間でも適切な参照を行うような形で検討が進められている。

- ISO/IEC 27400: Cybersecurity – IoT security and privacy – Guideline
- ISO/IEC 27402: Cybersecurity – IoT security and privacy – Device baseline requirements
- ISO/IEC 27403: Cybersecurity – IoT security and privacy –Guidelines for IoT domotics
- PWI 27404: Cybersecurity Labelling for Consumer IoT

(ア) ISO/IEC 27400: Cybersecurity – IoT security and privacy – Guideline

日本は、IoT関連の製品・システム開発の競争力を強化し、またIoTの国際的なセキュリティレベル向上に寄与するために、IoT推進コンソーシアムが策定した「IoTセキュリティガイドライン※319」の国際標準化を提案した。本ガイドラインに基づき、プライバシー関連の対策を含む形でISO/IEC 27400（IoTのセキュリティとプライバシー）の規格案がSC 27/WG 4で審議されている。以下にISO/IEC 27400の規格について概説する。

ISO/IEC 27400の具体的内容にあたる第5章以降では、第5章で参照モデル、各利害関係者の役割、IoTライフサイクルに言及し、第6章でIoTシステムにおけるリスク源（リスクソース）について言及している。第7章では、セキュリティ対策、及びプライバシー対策が、IoTサービス開発者及びサービスプロバイダ、ユーザのそれぞれの立場での対策内容、目的、導入ガイドといっ

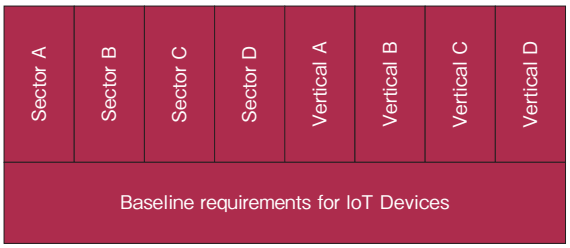
たガイドライン的表現で記載されている。ここで、IoT 機器製造業者は IoT サービス開発者の中に含まれる。現在策定されているドキュメントの枠組みは以下のとおりである。

第 1 章～ 4 章：スコープ、文献、用語定義等
第 5 章：IoT 概念と参照モデル
　5.1 概要
　5.2 IoT システムの特徴
　5.3 IoT システムの利害関係者（利用者、サービス提供者、サービス開発者）
　5.4 IoT エコシステム
　5.5 IoT ライフサイクル
　5.6 ドメインに基づく参照モデル
第 6 章：IoT システムのリスク源（リスクソース）
　6.1 導入
　6.2 リスク源（リスクソース）
第 7 章：セキュリティ／プライバシーのための管理策
　7.1 セキュリティ管理策
　7.2 プライバシー管理策
付録 A（参考情報）：リスクシナリオの事例：IoT モニタリングカメラ

2021 年 10 月にオンラインで開催された SC 27/WG 4 会議において、ISO/IEC 27400 は DIS となっていたが、DIS の投票を通過し、2021 年度末の段階では FDIS となっており、最終発行に近づいている。これまで、本規格に対するコメントは、日本、スイス、フランス、カナダ、ドイツ、インド、中国等の多くの機関から大量に提出されており、審議は極めて活発に行われた。本規格は IoT セキュリティ及びプライバシーの規範となるガイドラインであるため、IoT 利害関係者における認証等への活用が期待されている。

（イ）ISO/IEC 27402: Cybersecurity – IoT security and privacy – Device baseline requirements

本規格は、米国が主導して進めており、IoT 機器が備えるべきセキュリティメカニズムのベースラインとなる要求条件の規定を目指している。ISO/IEC 27400 とは異なるスコープを掲げ、IoT 機器に特化した要件化を視野に入れ、NIST 及び ETSI（European Telecommunications Standards Institute：欧州電気通信標準化機構）の既存のガイドラインを下敷きに標準化を進めている。2020 年 4 月に WD 1 として審議が開始され、一定の完成度と判断され、2020 年 9 月会議では、CD1 に進むことが決定したが、内容の重要性や ISO/IEC 27400 との整合性等が議論され、2021 年 10 月会議で CD2 の状態となっている。本規格の位置付けは、図 2-6-2 にあるように、本規格の基本要求事項が水平方向の基本ベースラインとなり、その上に垂直市場（健康、金融サービス、産業、家電、輸送等）や様々なセクター（民間／工業、公共、防衛、国家安全保障等）のアプリケーションで想定される IoT デバイスの使用とリスクに対する追加要件を構築できるというものになっている。



■図 2-6-2　特定セクターや垂直市場による潜在的な追加要件との関係
（出典）ISO・IEC「ISO/IEC CD 27402.2 - Cybersecurity — IoT security and privacy — Device baseline requirements※320」

また、本規格は IoT 機器の適合性評価スキームの要件を提供することができる。具体的には、まず特定のセクター及び垂直市場の利害関係者が、この水平規格の「上」に構築される、それぞれのコンテキスト固有の要件に関する合意を形成することが期待され、その後、それらの特定のセクター及び垂直市場に関する適合性評価プログラムが開発され、本規格は、共通の基本要件セットを提供しながら、そのようなプログラムに効果的に統合されるといったイメージとなる。

現在策定されているドキュメント（CD2）の枠組みを以下に示す。

第 1 章～ 4 章：スコープ、文献、用語定義、概要
第 5 章 要求事項
　5.1 IoT 機器製造者のための要求事項
　5.1.1 リスクアセスメント
　5.1.2 ユーザへのコミュニケーション
　5.1.3 脆弱性の開示と処理プロセス
　5.2 IoT 機器のための要求事項
　5.2.1 一般事項
　5.2.2 IoT 機器の識別
　5.2.3 構成
　5.2.4 リセット
　5.2.5 ユーザデータの削除
　5.2.6 データの保護
　5.2.7 インタフェースアクセス（Interface access）

5.2.8 ソフトウェアとファームウェアのアップデート

なお、インタフェースアクセスは、IoT デバイスにおいて、秘密鍵やパスワード等の重要なセキュリティパラメータを共有または再利用するためのインタフェースへのアクセスを許可された権限者に限定することに言及している。

上記の要求事項に近い内容は、ハイレベルなセキュリティ対策として ISO/IEC 27400 においても触れられており、ISO/IEC 27400 と ISO/IEC 27402 は、ISO/IEC 27400 シリーズ規格として一貫性を確保する形で規格策定が進められている。

(ウ) ISO/IEC 27403: Cybersecurity – IoT security and privacy –Guidelines for IoT-domotics

本規格は、2019 年 4 月テルアビブ会議において、中国から NP として提案され、同年 10 月のパリ会議では、NP の承認がなされ、2021 年 10 月に CD1 に進んでいる状況にある。「IoT-domotics」とは、娯楽、機器制御、監視等の用途として、居住環境で利用する IoT サービスをいう。本規格は、ISO/IEC 27400 との棲み分けが難しい部分が多いものの、IoT-domotics の特性を抽出し、ISO/IEC 27400 とは異なる視点でセキュリティとプライバシーに関するガイドラインとして整理している。具体的には、IoT-domotics のためのリスクアセスメントの実施を、アプリケーション、ネットワーク、ハードウェアの三点から評価しており、それらの結果を受ける形で、IoT-domotics を構成するサブシステムや IoT ゲートウェイのためのセキュリティ、及びプライバシーのガイドラインを整理する方向としている。

(エ) PWI 27404: Cybersecurity Labelling for Consumer IoT

本 PWI は、2021 年 10 月にシンガポールから提案されたもので、利用者が活用する IoT 機器にセキュリティラベルを付与し、機器にどの程度セキュリティ機能が装備されているかを、IoT 機器の利用者が把握できるようにする目的で検討が開始された。

現在、PWI として審議を継続しているが、ISO/IEC 27402 も IoT 機器に関する基本的な要求事項を規格化しようとしており、そこでも機器認証に関連した議論を行っていることから、簡単に本 PWI は NP とならない可能性が高いと考えられている。

(b) ビッグデータのセキュリティとプライバシーのための標準化活動

ビッグデータとは、主にボリューム、多様性、速度、及び／または変動性の特性を有し、効率的な保管、操作、分析のためにスケーラブルなアーキテクチャを必要とする広範なデータセットのことを指す。ビッグデータを用いた分析により、より優れた意思決定や戦略的なビジネス行動につながる洞察等を導き出すことができるため、近年注目を浴びている。WG 4 では、ビッグデータのセキュリティとプライバシーに関わる標準化として、以下の三つの活動を進めている。

- ISO/IEC 20547-4: Big data reference architecture – Part4: Security and privacy
- PWI 27045: Big data security and privacy — Guidelines for data security management framework
- ISO/IEC 27046: Big data security and privacy — Guidelines for implementation

(ア) ISO/IEC 20547-4: Big data reference architecture – Part4: Security and privacy

ISO/IEC JTC 1/SC 42 で審議されている、ISO/IEC 20547（ビッグデータ参照体系）は四つのパートから成り立っている。そのうちパート 4 は、SC 42 の依頼により SC 27/WG 4 で審議されており、セキュリティ及びプライバシーに関わる参照体系を規定している。本規格は、2019 年パリ会議において DIS に進み、2021 年に発行されている。

(イ) PWI 27045: Big data security and privacy — Guidelines for data security management framework

本規格は、組織のビッグデータのセキュリティとプライバシーを評価及び改善するプロセスの参照モデル、評価・成熟度モデルを規定するものであったが、内容的に規格化の方法が難しいことから、いったん規格化を断念し、PWI のステージに戻った形で議論が再開されている。

タイトルをビッグデータのセキュリティマネジメントのための枠組みを示すガイドラインとしており、多少これまでの検討を修正し、規格として成立しやすい形で審議を開始している。中国が主要なエディタとなり、オランダ、カナダが支援している。

(ウ) ISO/IEC 27046: Big data security and privacy — Guidelines for implementation

本規格は、ビッグデータのセキュリティとプライバシーの主要な課題とリスクを分析し、ビッグデータのリソース、組織化、分散化、計算能力及び破壊等の視点から、ビッグデータのセキュリティとプライバシーの実装のためのガイドラインを記述することを狙っている。2021 年 9 月会議（リモート）においては、WD 5 への移行が決議され、本規格におけるビッグデータのソリューションのためのセキュリティとプライバシーのスコープを図 2-6-3 のように整理している。

(c) サイバーフィジカルシステムのためのセキュリティの枠組み

サプライチェーンに代表される多様な組織が連携するビジネススタイルの急速な進展、サイバー攻撃の出現と巧妙化、更に近年の IoT の利用拡大、IoT システムで収集されるデータの高度利用を考えると、サイバーフィジカルシステム（CPS：Cyber Physical System）という概念を重視し、サイバーフィジカルシステムにおけるセキュリティリスクを特定する必要がある。CPS の導入は、あらゆる社会システムの効率化、新しい産業の創出、知的生産性の向上等の目的に有用である。CPS は、現実世界（物理空間）で発生する膨大な観測データ等の情報を、サイバー空間の強力な計算能力と結びつけて定量化するための方法論を提供するものである。

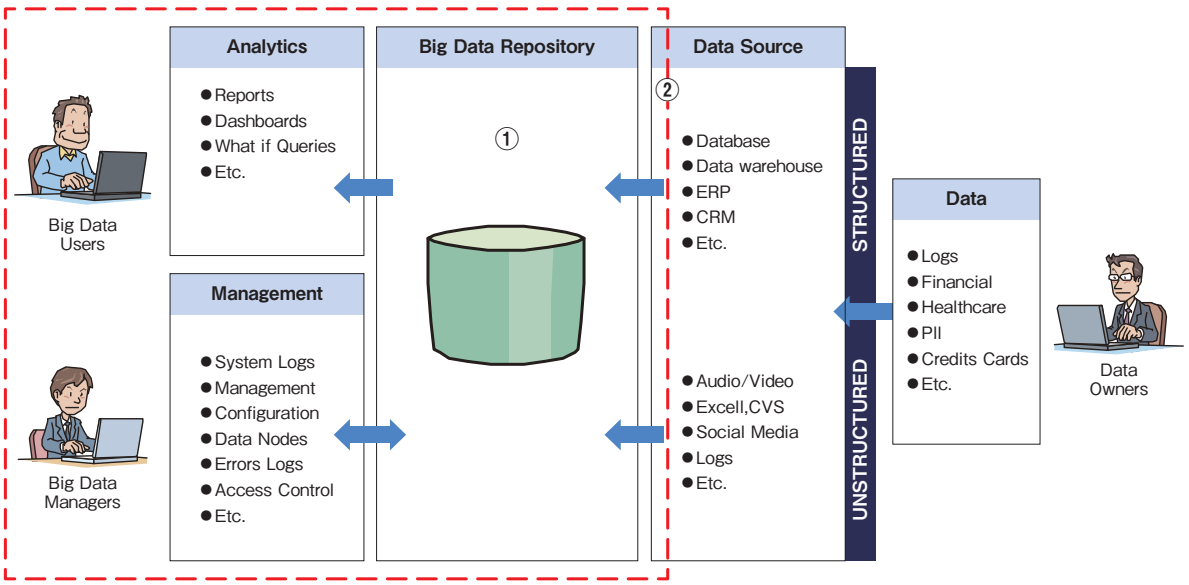
以上の背景から、日本の提案により 2020 年 4 月に PWI 5689 として「CPS のためのセキュリティフレームワーク」の議論が開始された。本フレームワークは経済産業省で構築した「サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）[※322]」に基づいている（「2.1.2 (1) 産業サイバーセキュリティ研究会」参照）。現在のドラフトテキスト（N 5436）では、CPS の概念モデル、CPS 下でのセキュリティ懸念、ISO/IEC TS 27110 や NIST の文書と整合性のあるセキュリティフレームワークの記述がなされている。

規格案が一定のレベルに達したことにより、本 PWI を NP に移行するための投票が 2021 年 12 月 2 日から 2022 年 3 月 5 日まで実施され、規格に賛成した国は多かったものの、規格策定に貢献する国の数が不足していることが理由で投票は否決された。この結果、再審議を実施するため、再度 PWI に戻り、規格スコープを拡張して審議を継続する予定である。

(d) WG 4 に関連するその他の規格群

WG 4 では、上記の IoT 及びビッグデータ以外の課題についても、多数の重要な審議を進めている。以下にその審議課題項目、規格の番号、及び審議状況を示す。

- ビジネス継続のための ICT 準備技術（27031）：PWI、NWI（New Work Item）の審議を経て、現在は WD3 の段階
- インターネットセキュリティガイドライン（27032）：現在は CD3 の段階



■図 2-6-3　ビッグデータソリューションにおけるセキュリティとプライバシーのスコープ
（出典）ISO・IEC「ISO/IEC WD 27046.4 - Information technology — Big data security and privacy — Implementation guidelines [※321]」を基に IPA が編集

- ネットワークセキュリティ（27033-7）：ネットワーク仮想化セキュリティのガイドラインとして NP が成立し、現在は WD4 の段階
- アプリケーションセキュリティ（27034）：パート 4 が FDIS に移行後、認証部分の記述の問題からキャンセルとなり、現在は PWI として審議を継続。他パートは規格化完了
- インシデントマネジメント（27035）：パート 3 は発行。パート 1、及びパート 2 については、見直しのフェーズ。なお、パート 4 が Coordination として提案され、現在 WD4 の段階
- サプライヤー関連セキュリティ（27036）：パート 1 から改版作業を開始
- デジタルエビデンスの識別、収集、確保、保全（27037）：改版作業なし
- リダクション（墨消し技術）（27038）：改版作業なし
- IDPS（不正検知・防止システム）（27039）：改版作業なし
- ストレージセキュリティ（27040）：大規模な改修を視野に入れ改版作業を開始、現在は CD1 の段階
- 仮想化サーバの設計／実装のためのセキュリティガイドライン（21878）：改版作業なし
- 産業用インターネット基盤のためのセキュリティ参照体系（24392）：現在は CD2 の段階
- 仮想化された信頼のルートのためのセキュリティ要件（27070）：現在は FDIS の段階
- 機器とサービス間の信頼接続の構築のためのセキュリティ推奨（27071）：現在は CD2 の段階
- 公開鍵基盤における実践とポリシーの枠組み（27099）：現在は FDIS の段階
- 安全な配備、アップデート、及びアップグレード（4983）：NWI 審議を経て、現在は WD2 の段階
- データの起源―参照モデル（データ追跡のため）（5181）：PWI として審議継続

(5) WG 5（アイデンティティ管理とプライバシー技術）

WG 5 では、アイデンティティ管理、プライバシー、バイオメトリクスの標準化を行っている。2021 年度の主な活動を紹介する。

(a) アイデンティティ管理

2019 年 5 月に発行された ISO/IEC 24760-1（アイデンティティ管理のフレームワーク パート 1：用語と定義）は現在改訂中であり、2022 年 4 月のオンライン会議の結果、DIS に進むことになった。

2015 年 6 月に発行された ISO/IEC 24760-2（アイデンティティ管理のフレームワーク パート 2：リファレンスアーキテクチャと要件）も現在改訂中であり、4 月のオンライン会議の結果、アドホック（特設）グループが設立され、日本からもメンバーが参加し、改訂案を作成中である。

2016 年 8 月に発行された ISO/IEC 24760-3（アイデンティティ管理のフレームワーク パート 3：実践）は追補作成中であり、2022 年 3 月末から 4 月初旬のオンライン会議の結果、DIS に進むことになった。

(b) プライバシー

属性に基づく連結不能なエンティティ認証のためのフレームワークと要求事項を提供する ISO/IEC 27551 は 2021 年 9 月に発行された。

ユーザ主体でプライバシープリファレンス（プライバシー設定）を管理し、PII（Personally Identifiable Information）の提供を制御するフレームワークを規定する規格である ISO/IEC 27556 は、2022 年 5 月 24 日に DIS DoC（Disposition of Comments）オンライン会合を開催し、FDIS に進んだ。

再識別リスク及び非識別データのライフサイクルに関連するリスクを特定し、軽減するための枠組みを提供する ISO/IEC 27559 は、2022 年 5 月 30 日に DIS DoC オンライン会合を開催し、FDIS に進んだ。

中国から新規に提案された、組織とユーザの間で個人データを共有または伝送する際に、共有情報を最小限にしてリスクを低減し、プライバシーを向上させるゼロ知識証明（ZKP：Zero-Knowledge Proof）を利用するためのガイドラインの提供を目的とした ISO/IEC 27565 が、2022 年 2 月の投票の結果、NP から 1st WD へと進んだ。

ISO/IEC 27001 及び 27002 を拡張し、組織による PIMS（Privacy Information Management System：プライバシー情報マネジメントシステム）の構築を支援することを目的とする ISO/IEC 27701 は、発行から 3 年目を迎え pre-review 時期にあたることと、ISO/IEC 27002 の改訂版が 2022 年 2 月に発行されたことを受けて、2022 年 4 月の会合で改訂の必要があることが合意された。改訂範囲等の詳細を議論するアドホックグループが設置され、日本からもメンバーが参加し、議論する予定である。

(c) バイオメトリクス

バイオメトリックデータの保護技術を扱うISO/IEC 24745は、2011年に発行されたが、その後の新技術を反映するための改訂が行われ、2022年2月に第2版が発行された。

モバイル端末におけるバイオメトリック認証のセキュリティとプライバシーの要求事項を扱うISO/IEC 27553は、バイオメトリック処理のすべてをモバイル端末で行うローカルモードと、そうではないリモートモードを別パートで扱うように分割された。ローカルモードを扱うパート1は、2022年5月24～25日にDIS DoCオンライン会合を開催し、FDISに進んだ。リモートモードを扱うパート2は4月のオンライン会議の結果、NPとして登録されることとなった。

2.7 安全な政府調達に向けて

IPA では情報セキュリティ対策の実現に向けて、国民に向けた情報提供や啓発活動、企業・組織に対するセキュリティ施策の促進とともに、政府機関や独立行政法人が安全に IT 製品やクラウドサービス等を調達するために活用できる制度の運営を行っている。

本節では、政府機関等で使用される IT 製品のセキュリティ機能を評価する「IT セキュリティ評価及び認証制度」、政府機関等のシステムに組み込まれる暗号のアルゴリズムを確認する「暗号モジュール試験及び認証制度」、及び政府が求めるセキュリティ要求を満たしているクラウドサービスを評価・登録する「政府情報システムのためのセキュリティ評価制度（ISMAP）」の動向について報告する。

2.7.1 ITセキュリティ評価及び認証制度

サイバーセキュリティ戦略本部は、2021 年 7 月、府省庁及び独立行政法人が遵守すべき情報セキュリティ対策を定めた「政府機関等のサイバーセキュリティ対策のための統一基準（令和 3 年度版）」（以下、政府統一基準）を発行した。この中では、国民の情報等を扱う公的なサービスを提供するシステムを構築する場合、そのシステムを構成する市販の IT 製品についてもセキュリティ要件を策定することを調達者に求めている。

IT 製品の調達において、セキュリティ要件を確認するための仕組みとして、セキュリティ評価制度が先進国を中心に発展し、セキュリティ評価基準が国際規格として策定された。日本でも、このセキュリティ評価基準を用いて IT 製品を評価する「IT セキュリティ評価及び認証制度（JISEC：Japan Information Technology Security Evaluation and Certification Scheme）」を IPA が運営し、政府機関等の IT 製品調達に活用されている。

(1) 政府の IT 製品調達セキュリティ要件

政府統一基準では、調達及び運用において特にセキュリティ要件を策定すべき IT 製品分野として、経済産業省が発行している「IT 製品の調達におけるセキュリティ要件リスト※323」（以下、調達要件リスト）を参照している。調達要件リストには、利用者情報を扱うシステムの基盤となり、攻撃の対象となり得る以下の 11 の製品分野が指定されている。今後も対象製品分野は、拡大される予定である。

- デジタル複合機
- ファイアウォール
- 不正検知・防止システム
- サーバ OS
- データベース管理システム
- スマートカード
- 暗号化 USB メモリ
- ルータ／レイヤ 3 スイッチ
- ドライブ全体暗号化システム
- モバイル端末管理システム
- 仮想プライベートネットワークゲートウェイ

府省庁や独立行政法人の情報システムセキュリティ責任者は、これらの製品分野の IT 製品を調達する場合、想定されるセキュリティ上の脅威にそれらの製品が対抗できていることを確認することが義務付けられている。各組織が調達する IT 製品が、想定するセキュリティ要件を満たしていることを個別に確認する方法に加え、調達要件リストでは、国際標準に基づく第三者認証製品の活用も認めている。

JISEC は、IT 製品のセキュリティ評価の国際標準である ISO/IEC 15408 に基づく第三者認証制度を運営している。組織の調達責任者は、想定する脅威に対抗していることが評価され、JISEC で認証された IT 製品を購入することで、政府統一基準の要求を満たすことができる。

特に、システム構築とは独立して調達されることの多い「デジタル複合機」、国策としてセキュリティ対策が重要となる旅券やマイナンバー等の「スマートカード」の調達で JISEC の認証制度は活用されている。

(2) 認証制度の国際連携

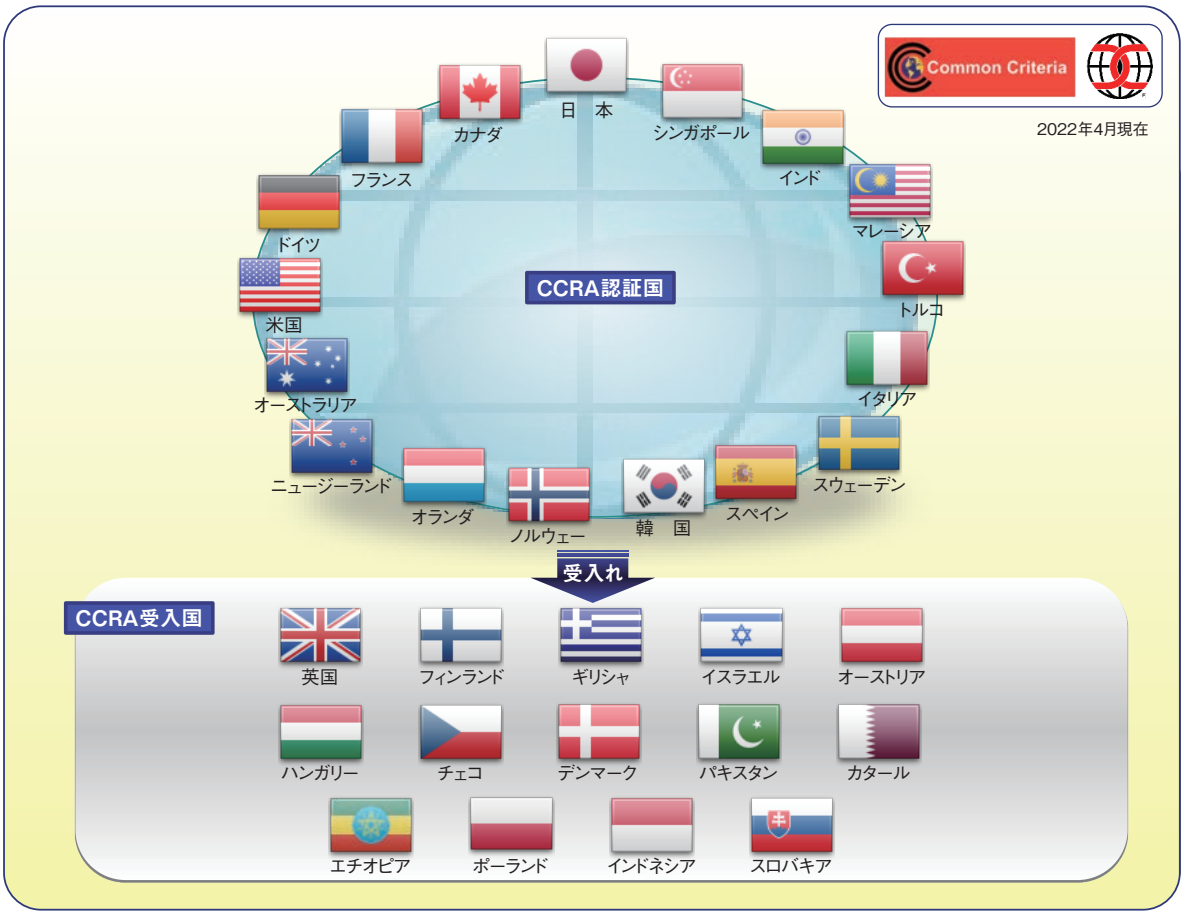
JISEC でも採用しているセキュリティ評価基準である ISO/IEC 15408 は、欧米 6 ヵ国によるコモンクライテリア（共通基準）プロジェクトとして開発された。これらの国々では、同じセキュリティ評価基準であるコモンクライテリアを用いて、その国を代表する公的機関が運営する制度で評価された結果については相互に認め合うことで、調達国ごとに重複する評価を行うコストを低減することを目的とした相互承認協定が締結された。この相互承認の

枠組みは、CCRA（Common Criteria Recognition Arrangement）と呼ばれ、その後多くの国が加盟し、JISEC を運営する日本も 2003 年に加盟している。これにより、日本のベンダは日本語の開発資料をそのまま利用し、JISEC で認証を取得した製品を CCRA 加盟国の政府調達の対象とすることができるようになった。CCRA では、自国で認証制度を運営している「認証国」と、認証制度をまだ有しないが政府調達要件として認証結果を受け入れる「受入国」があり、近年は東ヨーロッパやアフリカの国が受入国として加盟している。2022 年 4 月現在、CCRA 加盟国は認証国 17 ヵ国、受入国 14 ヵ国の計 31 ヵ国に上る（図 2-7-1）。

(3) セキュリティ要件の共通化

コモンクライテリアでは、IT 製品が具備すべきセキュリティ要件を、規定された形式に従って記述する。例えば、アクセス制御機能においては、対象となるオブジェクトやサブジェクトのリスト、セキュリティ属性、それらを用いたアクセス方針をコモンクライテリアで規定された形式で記述する。これにより、調達者が必要としている IT 製品のセキュリティ要件仕様を、あいまいさを排除して製品開発者に伝えることを可能とする。このコモンクライテリア形式で表された調達要件仕様書を「プロテクションプロファイル」と呼び、CCRA 加盟国での IT 製品の政府調達に利用されている。加盟国の調達部門は、調達する IT 製品のセキュリティ要件をプロテクションプロファイルとして作成し、調達要件として公開している。これらのプロテクションプロファイルのうち汎用的なものは、CCRA のポータルサイト※324 にも掲載され、他の機関も同様の分野の製品を調達する際に用いることができる。日本においても、調達要件リストでは製品分野ごとにこれらのプロテクションプロファイルを指定している。また、独自の製品を調達する機関は、プロテクションプロファイルを自ら作成し※325、調達を実施している。

同じ製品分野の IT 製品調達で、似たような調達仕様が調達者ごとに提示されることは、開発者にとっては負荷となる。そこで CCRA では、加盟国の認証機関が中心となり、いくつかの製品分野で共通的に用いるプロテクションプロファイルの策定を行っている。このプロテクションプロファイルは、cPP（collaborative Protection

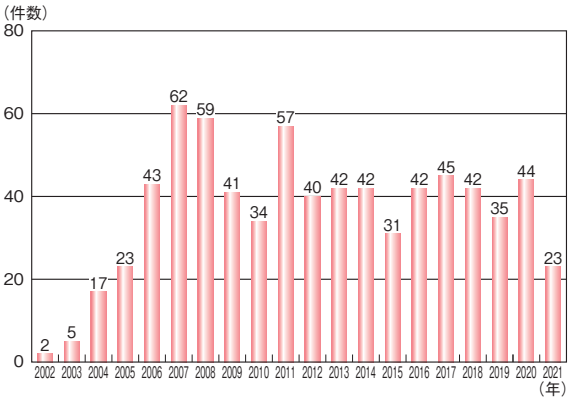


■図 2-7-1　CCRA 加盟国

Profile）と呼ばれ、CCRA 加盟国は、該当する製品分野の調達には、この cPP を用いてセキュリティ要件を指定することとしている。既にファイアウォール、暗号化ディスクドライブ、ネットワークデバイスの製品分野について cPP が策定され、CCRA ポータルサイトで公開されている。現在も、バイオメトリクス認証やデータベースについて cPP の策定が進行中である。日本も、国内に多くの製品ベンダを有するデジタル複合機について、韓国の認証機関とともに発起人となり、各国のベンダや評価機関をメンバーとする技術コミュニティを発足し、cPP の策定を継続して行っている。

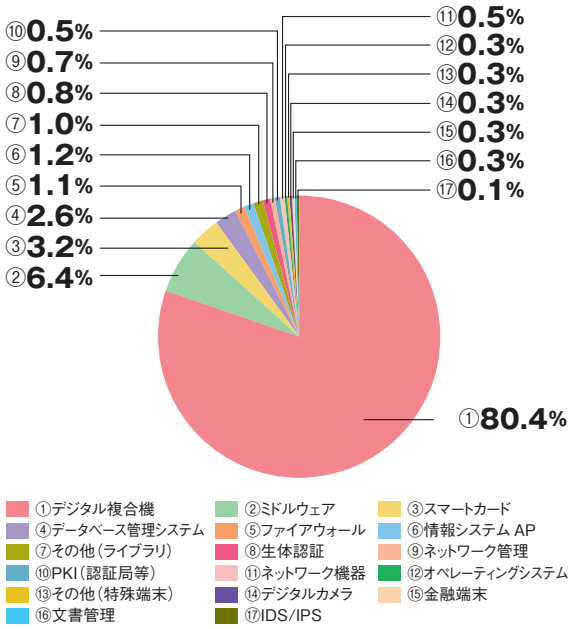
(4) 認証の状況

2021 年度までの JISEC における認証発行件数の推移を図 2-7-2 に示す。リーマンショックの影響による 2009 年の申請数の減少とそのリバウンド（2011 年）以降、毎年 40 件前後の認証発行を行ってきた。しかし、2021 年度の認証発行は前年度比約 48% 減となっている。これはコロナによる要員の配置や半導体調達の影響で、開発の遅延が発生したためである。

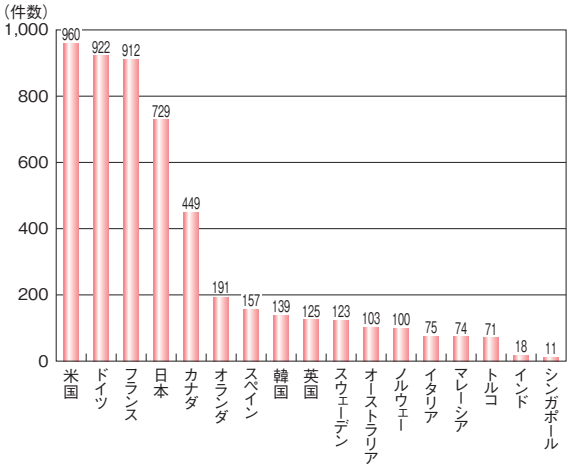


■図 2-7-2　JISEC の認証発行件数の推移

JISEC が認証発行した製品の分野の内訳を図 2-7-3 に示す。認証製品分野としては、デジタル複合機が圧倒的に多い。これは前述のように、日本のベンダが国際的にもシェアを有し、CCRA 加盟国においても政府調達の対象となっているからである。また、その他の製品分野の認証が JISEC で少ないのは、セキュリティ製品全般において日本ベンダの国際的な競争力が弱く、デジタル複合機以外の認証申請取得がなされないこと、ファイアウォールやネットワーク管理製品等はシステム構築の中で組み込まれてテストされ納入されることが多いため、製品単品での調達要件の対象とならないこと等が理由である。JISEC が毎年認証発行している 40 件前後は、ほとんどがデジタル複合機の新機種リリースによるものである。



■図 2-7-3　JISEC の認証発行の製品分野内訳



■図 2-7-4　CCRA 各国の認証件数

CCRA 加盟各国の認証機関が公開している認証発行件数の 2021 年度における累計を図 2-7-4 に示す。日本の認証発行件数は、米国、フランス、ドイツに次いで 4 番目に多い。これらの国は、政府調達に認証製品を活用しているのに加えて、国内に IT 製品の製造業者を多く持つ国々である。英国は、セキュリティ評価の歴史は長いにもかかわらず、国内の製造業者の減少により、2019 年に制度維持コストの削減を理由に認証国から受入国に移行している。韓国では、国際的に大きな市場を持つ製造業者が、製品仕向地に応じてモバイル製品は米国で、スマートカード関連製品はヨーロッパで認証を取得しているため、国内制度の認証発行件数は少ない。

(5) 2021 年度のトピック

JISEC では、IT 製品に対してだけでなく、プロテクションプロファイルに対しての認証[※326]も実施している。2021 年度から 2022 年度にかけて JISEC が認証した 2 件のプロテクションプロファイルを以下に紹介する。

(a) 特定用途機器ー共通セキュリティプロテクションプロファイル

政府統一基準では、調達要件リストとは別に、近年政府において活用されている IoT 製品についてもセキュリティ対策を求めている。更に 2020 年 4 月に施行された「電気通信事業法に基づく端末機器の基準認証」では、IoT 機器の技術基準にセキュリティ対策が追加された。このような背景を踏まえ、IoT 製品分野に係る国内ベンダが多く存在することから、JISEC では、安全な政府調達の推進と国際的な市場競争力の確保を目的に、IoT 製品分野への認証制度活用に向けた取り組みを実施している。

これまでにネットワークカメラシステム及び入退管理システムについて、調達者自身が調達時に必要なセキュリティ要件を確認できるようにチェックリストを公開している。IPA は 2020 年度にネットワークカメラシステムのチェックリストの基本的なセキュリティ要件について、コモンクライテリアの評価手法に従った検証を実施し、コモンクライテリア適用の有効性を確認した。この結果を踏まえ、2021 年度はネットワークカメラシステム等の IoT 機器を含む特定用途機器の基本的セキュリティ要件についてプロテクションプロファイルを策定し、JISEC でのプロテクションプロファイル認証を進めており、2022 年度上期に認証取得できる見込みである。今後、認証を取得したプロテクションプロファイルを用いた特定用途機器分野の政府調達での活用を推進していく。

(b) 電子パスポートプロテクションプロファイル

偽変造防止や安全かつ迅速な空港手続きを目的とした電子パスポートへの移行が、ICAO（International Civil Aviation Organization：国際民間航空機関）での国際標準化策定により各国で進められている。

日本においても、2015 年度に電子パスポート用 IC チップのプロテクションプロファイルの認証を行っている。2021 年度は、ICAO 文書の改訂やコモンクライテリア文書の改訂、パスポート特有のライフサイクル期間（最長 10 年間）を考慮し、ハッシュ関数のハッシュ長拡大、主要暗号アルゴリズムの鍵長拡大、楕円曲線暗号に用いる曲線拡大等、主に暗号面の安全性強化を行った新しいプロテクションプロファイルの認証を行った。今後、本プロテクションプロファイルに基づき製品認証を取得した IC チップが電子パスポートに採用されることにより、更にセキュリティ機能が強化された電子パスポートの推進・普及が期待される。

2.7.2 暗号モジュール試験及び認証制度

暗号モジュール試験及び認証制度（JCMVP：Japan Cryptographic Module Validation Program）とは、利用者が暗号モジュールの信頼性を客観的に把握できるように設けられた第三者適合性評価認証制度である。本制度に基づく認証を取得することにより、暗号アルゴリズムが適切に実装され、暗号鍵等の重要情報を適切に保護している暗号モジュールであることをアピールできる。本制度は、米国の NIST とカナダの CCCS（Canadian Centre for Cyber Security）により運営されている CMVP（Cryptographic Module Validation Program）[※327]と同等の制度であり、IPA が認証機関として運営している。本項では、JCMVP の最新動向、及び関連する CMVP の動向について述べる。

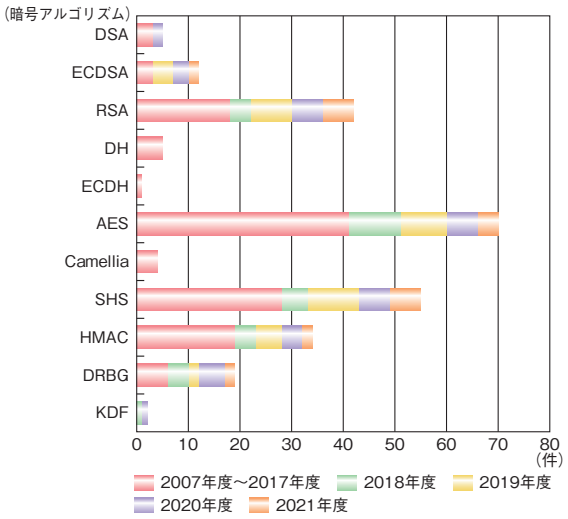
(1) 政府機関等における JCMVP の活用

政府統一基準における暗号・電子署名の遵守事項（6.1.5 節）に対する基本対策事項として、「政府機関等の対策基準策定のためのガイドライン（令和 3 年度版）」では「情報システムセキュリティ責任者は、暗号化又は電子署名を行う情報システムにおいて、以下を例とする措置を講ずること。」として、五つの例が挙げられている。その中の一つに、選択したアルゴリズムがソフトウェア及びハードウェアへ適切に実装されており、かつ、暗号化された情報の復号または電子署名の付与に用いる鍵及びそれに対応する主体認証情報等が安全に保護されることを確実にするため、「暗号モジュール試験及び認証制度」に基づく認証を取得している製品を選択することが挙げられている。また、各府省情報化統括責任者（CIO）連絡会議が決定し、2019 年 2 月に公開された「行政手続におけるオンラインによる本人確認の手法に関するガイドライン[※328]」において、JCMVP により認証されたハードウェアトークンに対して当人認証保証の最高レベル 3 を与えるとされている。

(2) IT セキュリティ評価及び認証制度（JISEC）との連携

IPA が運営する評価認証制度には、JISEC と JCMVP の二つがある。JISEC が 2016 年に発行、2020 年に改定したガイドライン※329 によって、JCMVP の活用方針が示されている（JISEC の活動については「2.7.1 IT セキュリティ評価及び認証制度」参照）。

例えば、この活用方針に関連するデジタル複合機のプロテクションプロファイル「Protection Profile for Hardcopy Devices 1.0 dated September 10, 2015※330」では、信頼できるツールを用いた暗号アルゴリズム実装のテストを求めている。JISEC では、このテストに、JCMVP の暗号アルゴリズム実装試験ツール（JCATT：Japan Cryptographic Algorithm implementation Testing Tool）を活用して認証を行っている。2021 年度は、このプロテクションプロファイルに基づく認証が 8 件完了している※331。このような連携を通じて、図 2-7-5 に示すように、JCATT を使って確認された暗号アルゴリズム実装の実績は、2018 年度から 2020 年度において堅調に増加してきた。2021 年度は 2020 年度よりも増加のペースが鈍ったが、それが新型コロナウイルス感染拡大の影響に起因する一時的なものかどうかは、現時点では不明である。また図 2-7-5 において、楕円曲線暗号の一つである ECDSA（Elliptic Curve Digital Signature Algorithm）は、2019 年度からは毎年実績が増えてきており、鍵長が比較的短くて済む楕円曲線暗号のニーズが反映されていると考えられる。



■図 2-7-5　JCATT により確認された暗号アルゴリズム実装の実績
（出典）IPA の公開情報を基に作成

(3) JIS X 19790 及び X 24759 の改正

JCMVP に関連する JIS 規格として、JIS X 19790（セキュリティ技術－暗号モジュールのセキュリティ要求事項）及び JIS X 24759（セキュリティ技術－暗号モジュールのセキュリティ試験要件）がある※332。JIS X 19790 は、コンピュータシステム及び通信システムの中のセキュリティシステムで使用される暗号モジュールに対するセキュリティ要求事項を規定したものである。JIS X 24759 は、暗号モジュールがその要求事項を満たしていることを試験機関が試験する方法等を規定したものである。これらは、それぞれ国際規格 ISO/IEC 19790 及び ISO/IEC 24759 の対応規格として作られている。

ISO/IEC 19790 は、2015 年 12 月に ISO/IEC 19790:2012/Cor.1:2015 として、暗号モジュールのソフトウェア及びファームウェア構成要素に対する誤り検出符号（EDC：Error-Detecting Code）の適用についての要求事項を追加する等、要求事項をより明確化した訂正版が発行されている。また、ISO/IEC 24759 は、2017 年 3 月に ISO/IEC 24759:2017 として、軽微な誤りの修正、技術的に正確な要件となるような修正を行い、ベンダ情報要件及び試験手順要件の一部を改正し、第 3 版が発行されている※333。

これに対し、JSA 及び IPA は、JIS X 19790 及び JIS X 24759 について、対応国際規格との乖離を解消するとともに技術の実態に即した内容にするための改正を進めることとした。IPA は、民間の有識者、学識経験者及び政府関係者からなる JIS X 19790 及び X 24759 原案作成委員会を組織し、JIS 改正原案を 2022 年 2 月に作成した。原案は JSA による校正を経て、2022 年 6 月に JSA から経済産業省へ提出された。

その後は、60 日間の WTO/TBT 意見受付公告※334 の後、JISC による審議を経て※335、2022 年末ごろに発行される見込みである。

(4) CMVP の動向

NIST と CCCS は、2019 年に CMVP の新しい規格となる FIPS 140-3※336 を発行したことを契機に 2020 年から FIPS 140-2 から FIPS 140-3 への移行を進めている。その移行スケジュールに則り、2021 年 9 月に FIPS 140-2 での新規申請が原則終了した（例外申請が認められた分も 2022 年 3 月で申請終了）。2026 年 9 月に FIPS 140-2 認証製品はすべて Historical List※337 へ移動する予定である。

2.7.3 政府情報システムのための セキュリティ評価制度（ISMAP）

2020 年 6 月 3 日、内閣官房、総務省、経済産業省は政府情報システムのためのセキュリティ評価制度（ISMAP）の開始をアナウンスした※338。本項では、ISMAP の概要について紹介する。

(1) ISMAP の概要

政府情報システムのためのセキュリティ評価制度（Information system Security Management and Assessment Program:通称、ISMAP（イスマップ））は、政府が求めるセキュリティ要件を満たしているクラウドサービスをあらかじめ評価・登録することにより、政府のクラウドサービス調達におけるセキュリティ水準の確保を図り、クラウドサービスの円滑な導入に資することを目的とした制度である。

従来、政府調達にあたっては、個々のクラウドサービスが実施していると表明する情報セキュリティ対策の実施状況を、調達者が直接確認することが必要であったが、本制度により、この確認を省略でき負担を軽減できる。

なお、ISMAP がクラウドサービスの申請受付を開始した 2020 年 10 月 1 日から 1 年間、現状やむを得ず ISMAP に登録されていないクラウドサービスを利用中、または利用予定の各政府機関等に対しては、当該サービスが申請されることを前提として、それらのサービスの利用を可能とする暫定措置期間が設けられていた。その暫定措置期間が 2021 年 9 月 30 日に期限を迎えることから、2021 年 7 月 6 日に開催された「サイバーセキュリティ対策推進会議・各府省情報化統括責任者（CIO）連絡会議」で、真にやむを得ないケースを対象に縮小した新規の暫定措置期間が設定された※339。

(2) ISMAP 制度制定の経緯

2018 年 6 月に公開された「政府情報システムにおけるクラウドサービスの利用に係る基本方針※340」（2021 年 3 月 30 日付けで ISMAP に関する記述が追記されている）では、「クラウド・バイ・デフォルト原則」が掲げられた。これを踏まえ、経済産業省と総務省は、2018 年 8 月から「クラウドサービスの安全性評価に関する検討会※341」を発足させ、適切なセキュリティ要件を満たすクラウドサービスを導入するために必要な評価方法等を検討し、2020 年 1 月に「クラウドサービスの安全性評価に関する検討会とりまとめ※342」が公開された。また、同月のサイバーセキュリティ戦略本部会合において「政府情報システムにおけるクラウドサービスのセキュリティ評価制度の基本的枠組みについて※343」が決定された。

上記検討会において、2019 年 6 月から、政府情報システム調達に応募するクラウド事業者が遵守すべきセキュリティ管理基準（ISMAP 管理基準）の検討が行われた。ISMAP 管理基準は、国際規格をベースに「政府機関等の情報セキュリティ対策のための統一基準群（平成 30 年度版）※344」「NIST SP800-53 rev.4」を参照して作成された。国際規格としては、情報セキュリティに関しては JIS Q 27001（ISO/IEC 27001）、JIS Q 27002（ISO/IEC 27002）とクラウドサービスの情報セキュリティに関する JIS Q 27017（ISO/IEC 27017）が参考にされた。また、これらの国際規格に準拠して編成された「クラウド情報セキュリティ管理基準（平成 28 年度版）」が参考にされ、そこに含まれるガバナンス基準について JIS Q 27014（ISO/IEC 27014）が参考にされた。

(3) ISMAP のフロー

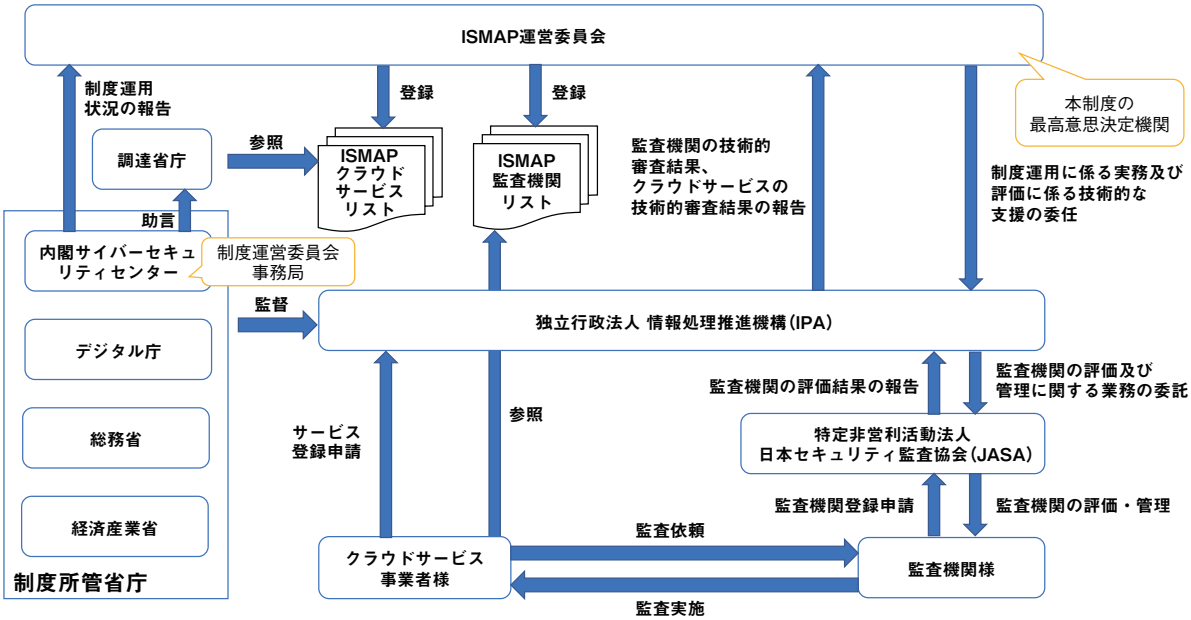
本制度においては、本制度で定められた情報セキュリティ監査の枠組みに基づき、政府機関等が調達するクラウドサービスに要求される基本的な情報セキュリティ管理・運用の基準を満たすセキュリティ対策を実施していることが確認されたクラウドサービスが、ISMAP クラウドサービスリスト（以下、サービスリスト）に登録される。政府機関がクラウドサービスを調達する場合、サービスリストに登録されたサービスを選定候補とする。

また、本制度における監査を実施できる監査機関は、あらかじめ本制度で定める要求事項を満たすことが確認され、本制度が公表する ISMAP 監査機関リスト（以下、監査機関リスト）に登録される。

本制度のフローを図 2-7-6（次ページ）に示す。クラウドサービス提供者は、監査機関リストに登録された機関による監査を受け、ISMAP 運用支援機関である IPA を通じて ISMAP 運営委員会にサービス登録申請を行う。申請を受けた ISMAP 運営委員会は審査を行い、承認されたサービスがサービスリストに掲載される。府省庁の調達者はサービスリストを使って調達先候補を選ぶ。なお、本制度の運用に係る実務及び評価に係る技術的な支援は IPA が行い、そのうち、監査機関の評価及び管理に関する業務については、IPA から特定非営利活動法人日本セキュリティ監査協会（JASA）に委託している。

(4) ISMAP の運用

本制度は、2020 年 6 月に運用が開始された。



(注)制度運用に係る実務及び評価に係る技術的な支援をIPAが行い、うち、監査機関の評価及び管理に関する業務についてJASAに再委託する。

■図 2-7-6　クラウドサービスの安全性評価の制度のフロー
(出典)ISMAP「ISMAP 概要※345」

ISMAP の所管は 2022 年 1 月現在、NISC、デジタル庁、総務省、経済産業省であり、最高意思決定機関として ISMAP 運営委員会を設置し、事務局は NISC に置き、運用実務は IPA が担当している。

制度の概要、基準規程類、監査機関リスト、及びサービスリストは、2021 年 5 月に開設された ISMAP ポータルサイト※346 で公開されており、2022 年 1 月には本制度の登録について、ポータルサイトでの電子申請の受付を開始している。2022 年 6 月 1 日時点で登録されている監査機関は 5 機関、また、クラウドサービスは 34 サービスである。

(5) セキュアなクラウド利用に向けて

IPA は、クラウドサービス事業者がサービスリストへの登録を行うにあたり、セキュリティ対策の進め方及び管理基準の理解の一助となることを目的として、管理基準マニュアルの作成を行っている。

また、ISMAP で公開される情報は、重要インフラ分野等を始めとする民間においても参照されることで、クラウドサービスの適切な活用の推進が期待される。これに関連して、2019 年 5 月 23 日に改定された NISC の「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針(第 5 版)※347」は、「事業環境の変化を捉え、インターネットを介したサービス(クラウドサービス等)を活用するなど新しい技術を利用する際には、国内外の法令や評価制度等の存在について留意する。」としており、国内の評価制度としては ISMAP が該当すると考えられる。

「クラウドサービスの安全性評価に関する検討会とりまとめ」にも記載されたように、情報システムのセキュリティ確保の責任は、一義的に当該システムの利用者である調達省庁が負うものである。本制度に登録されたクラウドサービスを利用したとしても、それだけでは情報システム全体のセキュリティが十分に確保されることにはならない。情報システムの利用者である調達省庁は、利用するクラウドサービスについて適切な設定を行うことに加えて、情報システム全体のセキュリティリスクを分析し、適切な対策を行うことが求められる。

2.8 その他の情報セキュリティ動向

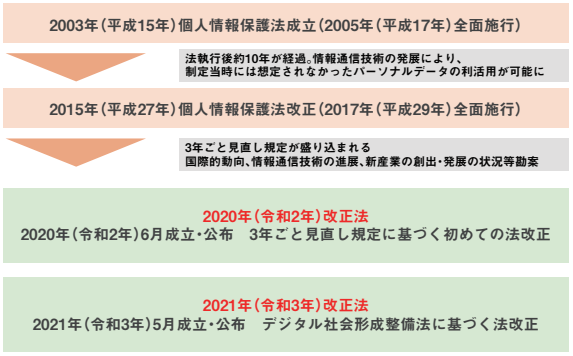
個人情報保護法改正、内部不正防止対策の動向、及び暗号技術の動向について述べる。

2.8.1 個人情報保護法改正

個人情報保護法※348は、情報流通や通信の高度な進展に伴う個人情報利活用の有用性に配慮しながら、個人の権利利益を保護することを目的とした、個人情報の取り扱いに関する法律である。個人情報保護に関する施策推進の基本的方向性や、国、地方公共団体、個人情報取扱事業者等が講ずべき措置の方向性が示されている。

(1) 個人情報保護法改正の経緯

個人情報保護法は2003年に成立、2005年に施行された。その後情報通信技術の進展や個人情報を利活用する要請の高まりに伴い、「個人情報の保護に関する法律及び行政手続における特定の個人を識別するための番号の利用等に関する法律の一部を改正する法律※349」が2015年に成立、2017年に施行され、3年ごとの見直し規定が盛り込まれた。この見直し規定に基づき2020年に法改正され※350（2022年4月全面施行）、個人の権利の保護と活用の強化、越境データの流通増大に伴う新たなリスクへの対応、AI・ビッグデータ時代への対応等が盛り込まれた。更に2021年に「デジタル社会の形成を図るための関係法律の整備に関する法律※351」（デジタル社会形成整備法）に基づく法改正により※352、官民を通じた個人情報保護制度の見直し（官民一元化）が行われた。2021年改正法は2022年4月に政府関係機関・学術研究機関に対する部分が施行された。地方自治体関係機関に対する部分は2023年に施行予定である。



■図2-8-1　個人情報保護法改正の経緯

(2) 個人情報保護法改正の概要

2020年及び2021年の法改正の概要をまとめる。

(a) 2020年の個人情報保護法改正

個人情報に対する意識の高まり、技術革新を踏まえた保護と利活用のバランス、越境データの流通増大に伴う新たなリスクへの対応等の改正が実施された。2020年の改正の主な内容を挙げる。

①個人の権利の在り方

個人情報の利用停止・消去等の個人の請求権、個人データの開示方法、第三者提供記録の本人開示請求等が拡充された。

②事業者の守るべき責務の在り方

個人情報保護委員会への報告や本人への通知が義務化され、不適正な方法での個人情報利用が禁止された。

③事業者による自主的な取り組みを促す仕組みの在り方

認証個人情報保護団体制度で、企業の特定分野（部門）を対象とする団体を認定できるようになった。

④データ利活用の在り方

「仮名加工情報」が創設され、内部分析用途に限定し、開示・利用停止請求への対応義務が緩和された。

⑤ペナルティの在り方

命令違反・虚偽報告等の行為者への罰金が引き上げられ、法人は行為者より罰金刑最高額が引き上げられた（次ページ表2-8-1）。

⑥法の域外適用・越境移転の在り方

日本国内の個人情報等を取り扱う外国事業者を、罰則付きの報告徴収・命令の対象とした。また、外国の第三者への個人データ提供時、移転先での個人情報の取り扱いに関する本人への情報提供の充実が求められた。

なお、2020年の個人情報保護法改正については「情報セキュリティ白書2020※353」の「2.7.4 個人情報保護法の改正」も参照されたい。

		懲役刑		罰金刑	
		改正前	改正後	改正前	改正後
個人情報保護委員会からの命令への違反	行為者	6月以下	1年以下	30万円以下	100万円以下
	法人等	―	―	30万円以下	1億円以下
個人情報データベースなどの不正提供など	行為者	1年以下	1年以下	50万円以下	50万円以下
	法人等	―	―	50万円以下	1億円以下
個人情報保護委員会への虚偽報告等	行為者	―	―	30万円以下	50万円以下
	法人等	―	―	30万円以下	50万円以下

■表 2-8-1　2020 年改正前後の法定刑の比較
（出典）個人情報保護委員会「令和2年 改正個人情報保護法について※350」

(b) 2021 年の個人情報保護法改正

個人情報保護とデータ流通の両立・強化、国際的制度との調和を目的として 2021 年に法改正された。四つのポイントを以下に示す。

①個人情報保護法、行政機関個人情報保護法、独立行政法人等個人情報保護法の 3 本の法律を一つに統合し、地方公共団体の個人情報保護制度についても統合後の法律の中で全国的な共通ルールを規定し、全体の所管を個人情報保護委員会に一元化した（図 2-8-2 の①）。

②医療・学術分野の規律を官民で統一するため、国公立の病院、大学等には原則として民間の病院、大学等と同等の規律を適用した（図 2-8-2 の②）。

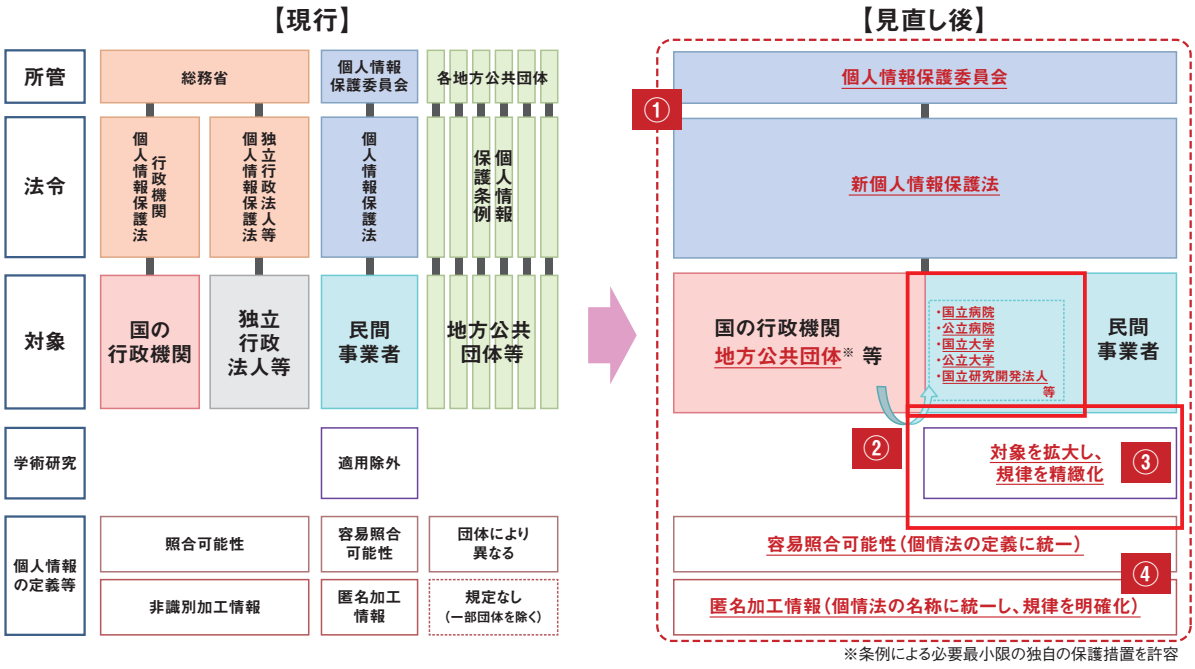
③学術研究分野を含めた GDPR の十分性認定への対応を目指し、学術研究に係る適用除外規定（学術研究目的の利用については本人同意を必須としない等）について、一律の適用除外ではなく、義務ごとの例外規定として精緻化した（図 2-8-2 の③）。

④個人情報の定義等を国・民間・地方で統一するとともに、行政機関等での匿名加工情報の取り扱いに関する規律を明確化した（図 2-8-2 の④）。

2021 年の改正法では、データの保有、利用目的、提供の適不適、例外適用の可否等の法解釈・運用に関する諸権限が、個人情報保護委員会に集約されることとなった。

また、多くのステークホルダーが関与し、全国広範囲で実施されるようなビジネスにおいて、しばしば「個人情報保護法制 2000 個問題※355」と呼ばれていた以下の諸問題について、同法が一律に適用される見込みであり、実効的解決が期待されることとなった。

- 個人情報関連法制が自治体ごとに異なるルール・解釈で運用されていた問題
- 個人情報を含むデータの利用を伴う新規案件の検討・実行の諸手続き解釈等の検討に長時間を要していた問題



■図 2-8-2　2021 年改正の概要
（出典）個人情報保護委員会「個人情報保護制度見直しの全体像※354」

- 効率を高め得る新技術導入が敬遠され、導入時に過度のカスタマイゼーションが求められがちであった問題

各自治体に改正法の統一的な条文が適用される一方、自治体ごとの条例で個別に定めることができるのは、統一的な部分に対するいわゆる上乗せ・横出し部分（条例要配慮個人情報等）になると考えられる。

更に、国公立大学・病院等、日常的活動そのものに官民の差があまりない領域においては、官民で規律を共通化することで連携が容易となり、データが適正に管理されているかの見極めも、個人情報保護委員会が一元的に判断可能となると期待される。

2.8.2 内部不正防止対策の動向

組織が保有する秘密情報の保護は重要な課題であり、内部不正が関係する情報漏えいは、組織において特に注意すべき脅威の一つである。2020 年度に IPA が実施した営業秘密管理に関する実態調査※356 の結果でも、情報漏えいインシデントの多くは内部不正により発生する傾向が高いことが示されている。また同調査によれば、近年のテレワーク等の働き方の変化、クラウド化等の IT プラットフォームの変化は、組織のセキュリティ対策実施のガバナンスを弱め、内部不正のリスクを高めている、との意識も強まっている。

これを受けて IPA は、2013 年に発行した「組織における内部不正防止ガイドライン」（以下、内部不正ガイドライン）を 2022 年 4 月に第 5 版に改訂した※357。本項では改訂にあたり、近年の社会的・技術的環境変化を整理し、インシデントや政策・対策の現状を調査した上で、重要な対策のポイントを整理した結果を紹介する。

(1) 内部不正によるインシデント事例

内部不正ガイドライン改訂に必要な情報収集の一環として、国内外の内部不正によるインシデント事例を報道や公知の文献情報等から調査した。具体的には、悪意による情報の漏えい、退職時の情報持ち出し、不適切に管理された情報の漏えい等に関係した事例を新たに収集した。第 5 版の改訂で内部不正ガイドラインに追記した事例の抜粋を表 2-8-2 に示す。

外部者からの働きかけによる営業秘密情報の漏えい、中途退職者による営業秘密情報の窃取、管理不備による営業秘密情報の外部への持ち出し等、以前から注意喚起され、現在も継続して発生している典型的事例が目を引く。

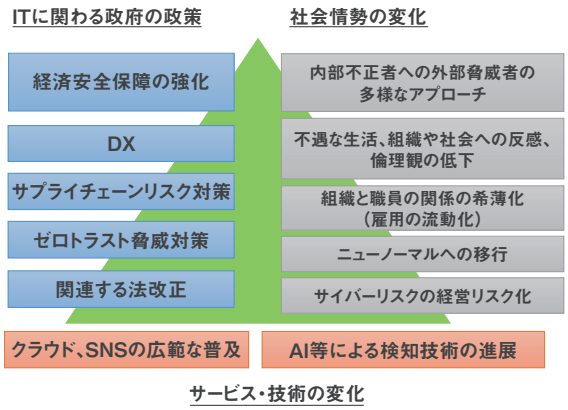
類型	内部不正の内容
技術情報の国外への漏えい	企業の防衛・宇宙部門に在籍していた職員が、防衛・宇宙関連の営業秘密にあたる技術情報を国外に漏えいさせた。 職員の出身国であった外国政府からのアプローチを受けたことによる。
営業秘密情報の漏えい	企業の職員が、退職後に企業のシステム内の機密情報に不正アクセスし営業秘密情報を窃取した。 業績不振を理由に解雇されることに不満があったこと、退職後に共有アカウントのパスワードが変更されていなかったことによる。
顧客情報（営業秘密）・個人情報の不正な持ち出し	企業の共同開発先として委託を受けた海外現地法人の職員が、業務用パソコンへ取引先情報及び個人情報を含むデータを許可なくダウンロードし、海外のクラウドストレージサービスの個人アカウントへアップロードした。 海外現地法人の職員に対する教育や内部不正対策の周知徹底が十分でなかったことによる。
個人情報の暴露	自治体の職員が、貸与パソコンから同自治体職員の個人情報を含むファイルを入手し、新聞社にファイル添付したメールを送信した。 貸与パソコンの中に、個人情報を含むファイルが残されていたこと、同職員には待遇への不満、自治体の情報管理不備をマスコミに告発することによる自己肯定欲求があったことによる。
システム・プログラムの破壊	企業の職員が、退職前に開発中のシステムのソースコードを社内で共有せず自分のパソコンから削除した。 処遇に不満があったこと、プログラム管理システムへのソースコード登録の手続き不備があったことによる。
システム・プログラムの改ざん	企業の職員が貸与されたコンピュータにハッキングツールをインストールし、他の職員の認証情報を盗み、外部の共犯者に渡した。共犯者は同社の Web サイトにその認証情報を用いて不正アクセスし、Web サイトを改ざんした。 支給されたコンピュータにハッキングツールをインストールすることが可能であったことによる。

■表 2-8-2　内部不正ガイドラインに掲載した内部不正事例（抜粋）

(2) 内部不正対策検討のポイント

内部不正のリスクを分析し、対策を検討する前提として、仕事や生活の IT 化・デジタル化に関する環境条件を整理することが有用であると考えられる。本改訂においては、それらの環境条件として IT に関わる政府の政策、社会情勢の変化、サービス・技術の変化の 3 点に注目した（次ページ図 2-8-3）。

IT に関わる政府の政策としては、サイバーセキュリティ戦略本部が公表している「サイバーセキュリティ 2021※2」等の IT セキュリティ戦略の観点から、経済安全保障の



■図 2-8-3　三つの環境条件から見た重要な変化

強化の必要性、DX 推進、サプライチェーンリスク対策、ゼロトラスト脅威対策、関連する法改正等が注目される。社会情勢の変化としては、内部不正者への外部脅威者の多様なアプローチ、不遇な生活・組織や社会への反感、倫理観の低下、組織と職員の関係の希薄化（雇用の流動化）、ニューノーマルへの移行、サイバーリスクの経営リスク化等が注目される。サービス・技術の変化については、クラウド・SNS の広範な普及、AI 等による検知技術の進展等が注目される。

内部不正防止ガイドラインの改訂においては、関連法制調査を含む文献調査の結果と、上記の三つの環境条件に関わる変化点を併せて整理し、新たな内部不正対策を検討するための七つの課題を抽出した。

①営業秘密、とりわけ重要技術情報の漏えいに対する社会的な危機感の拡大
②内部不正が事業経営に及ぼすリスクの増大
③テレワークに代表される働き方の変化、及びその常態化に伴う情報漏えいリスクの増大
④オンラインストレージやクラウド等の外部サービスの利用拡大
⑤セキュリティ技術（特にエンドポイントセキュリティやモニタリング技術）の急速な進展と個人情報に配慮した運用
⑥雇用の流動化による退職者（転職者）の急増
⑦法改正（個人情報保護法、不正競争防止法等）による漏えいの通報義務、重要データ保護等の強化

これらの課題のポイントは、以下として整理できる。

- 経営層のコミットメント
- 法制との整合
- 強化すべき対策

以下では強化すべき対策について、企業・有識者へのインタビュー調査を行い、収集した情報を踏まえた 3 点のポイントを示す。

(a) テレワーク・クラウドの普及に伴う対策

テレワークに代表される働き方の変化や、それに伴うオンラインストレージやクラウド等の外部サービスの利用拡大といった環境変化が顕著である。それらの変化に対応した技術的な対策・証拠保全等の事後対策等が重要であり、特に以下の対策に留意する。

- 個人情報・営業秘密情報等の重要情報が、テレワークやクラウド等の利用により広範囲に分散する傾向が強まるため、重要情報の棚卸しを行い、情報の保存場所・管理責任者等に関する管理ルールを定め、運用する。
- クラウドプロキシや CASB（Cloud Access Security Broker）の導入等により、クラウドの利用状況を把握し、管理されない「野良クラウド」の利用を認めない。
- クラウドサービスのアクセス権限の設定漏れや設定ミス等による意図しない相手への情報の曝露に注意する。
- クラウドサービスへのアクセスの認証ログ・アプリケーションの操作ログを取得し、ログに不正アクセスの痕跡が記録されていないかを定期的に確認する。
- データのダウンロードが制御できるクラウドサービスに限り使用許可を行う。
- テレワーク端末の内蔵記録装置（HDD・SSD 等）の暗号化やデータの遠隔消去等の対策を導入する。

(b) 退職者関連対策

IPA が 2021 年に公開した「企業における営業秘密管理に関する実態調査 2020[※356]」でも、営業秘密の漏えいルートは「中途退職者」による漏えいが 36.3% と最多であった。退職者の内部不正を防止する目的でシステムのモニタリングを行うことは抑止的な対策として有用である。

一方、プライバシーやコンプライアンスの観点からの注意点も存在する。退職予定者を含めた役職員をモニタリングするにあたり、その目的が、正しく業務を行っている役職員を保護するためであることを広く周知するべきである。経営者は、「モニタリングは不正アクセスの検知を目的とし、業績評価を目的としない」「モニタリングは正しい業務を行う職員を守るために行う」等の周知を就業規則等で明確に行い、役職員の理解を得ておくことが望ましい。

なお、退職後の秘密保持契約や誓約書の提出を退

職予定者に拒否されることもありえるため、雇用契約に退職時の禁忌事項を盛り込む等の対策も有効である。また、退職者が組織の外に重要情報を不正に開示するような事態を防ぐために、退職前の事前対策として、重要情報を組織の外に持ち出さないように本人に通知した上で技術的・物理的な情報漏えい対策を講じること等が有効である。

(c) ふるまい検知等の新技術対策

近年、急速に進展してきた新技術に、EDR（Endpoint Detection and Response）等のエンドポイントセキュリティ技術や、パソコン・システム上におけるふるまい検知を含む各種モニタリング技術がある。AI 等によるふるまい検知を行う製品・サービスも内部不正対策として実用レベルになってきている。

こうしたふるまい検知等の新技術を内部不正対策として適用することは効果的である一方、役職員の人権・プライバシーに配慮した運用が求められる。個人情報保護法・欧州の GDPR・米国のプライバシー関連法等のプライバシー保護規制に合わせた個人データの収集・分析や役職員の適切な保護が可能なシステムを選定すること、行動履歴を含む個人データの収集については労働規約等で周知しておくこと、分析を AI まかせにせず、「人間」による判断と「自動化・効率化」を組み合わせた運用を行う等、組織としてモニタリングの説明責任を果たせる運用体制の構築が対策のポイントとなる。

(d) 経営層へのメッセージ

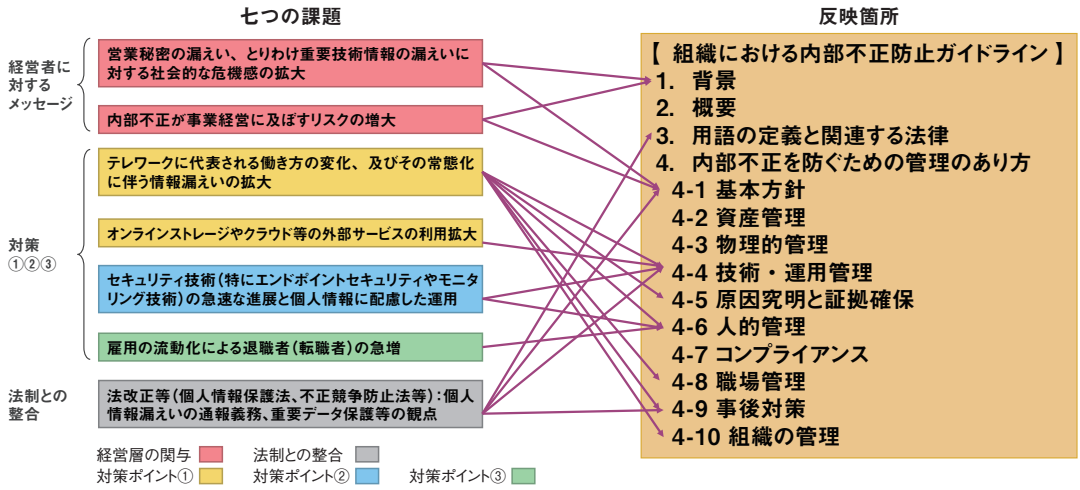
以上 3 点の対策ポイントに加えて、経営層の内部不正リスクに対する問題意識を高める施策はあらゆる対策の根幹として重要である。経営陣が内部不正インシデント発生時のリスクと責任を認識できるよう、インシデントにより引き起こされる事業への影響がどの程度なのか、BIA（Business Impact Analysis）等の分析により評価し、把握することが有用である。併せて、組織のリスクマネジメント体制の中に内部不正リスクを所管する責任者を明示的に置くことも経営リスクと責任の所在の明確化に役立つ。

(3) 内部不正ガイドラインの改訂内容

このように得られた知見に基づき、2022 年 4 月に内部不正ガイドラインを第 5 版に改訂した。検討した内部不正対策の七つの課題に対応する改訂箇所を特定し、前節で述べた対策強化ポイントを反映した（図 2-8-4）。

経営層への内部不正対策の重要性の訴求については、「1. 背景」「4-1 基本方針」部分の加筆を行った。テレワーク・クラウド・AI ／ふるまい検知技術の普及については、「4-4 技術・運用管理」に特に重点を置き加筆した。更に、モニタリング適用時の職員の人権・プライバシー保護等の必要性、雇用の流動化に伴う退職時の対策について「4-6 人的管理」の加筆・修正を行った。

更に、内部不正防止に関連する法制度の変化に対応するため、NISC の「サイバーセキュリティ関係法令 Q & A ハンドブック※359」等を参照し、各施策と個人情報保護法・改正不正競争防止法等の関係法制の対応を明示し、対策実施におけるコンプライアンスも重視した。内部不正ガイドライン第 5 版の今後の活用が望まれる。



■図 2-8-4　内部不正ガイドライン第 5 版の改訂箇所
（出典）株式会社エヌ・ティ・ティ・データ経営研究所「IPA『組織における内部不正防止ガイドライン』の改訂に係る調査等業務 概要説明資料※358」を基に IPA が編集

2.8.3 暗号技術の動向

本項では2021年度における、共通鍵暗号、公開鍵暗号及び実装攻撃に関する研究動向についてそれぞれ解説する。

(1) 共通鍵暗号に関する研究動向

2021年度は、2020年度に引き続き、共通鍵暗号に関する解読について大きな進展はなかったものの、既存の暗号アルゴリズムへの攻撃について、攻撃に必要な計算量の削減等の進展があった。ここでは主な発表を紹介する。

AES※360については、二つの暗号解析論文が注目される。一つ目は、Eurocrypt 2021で、AES鍵スケジュールに対する新しい表現とそれを活用したAES-128に対する不能差分攻撃(impossible-differential attacks)の改善を報告した。INDOCRYPT 2010で報告された攻撃、及びその亜種が今までの最善の攻撃であったが、本提案手法はそれよりも約2.3倍計算量を改善している。この論文はEurocrypt 2021 Best paper awardを受賞した。二つ目は、同じくEurocrypt 2021にて、AES-128ハッシュモードの8段に対する最初の攻撃を報告した。これは、攻撃探索問題を混合整数線形計画法における制約条件のもとでの最適化問題に変換することで、攻撃の探索範囲を拡大し、より攻撃に有効な経路を発見できることを利用している。このように、AESに対する攻撃は2021年度も進展は見られたが、セキュリティマージンはまだ十分にあり、AESの安全性に直ちに影響を与えるものではない。

その他の暗号については、Eurocrypt 2021で、ARX(Addition, Rotation, and XOR)ベースの暗号に対する差分線形解析の改良が発表された。ストリーム暗号の一種であるChaCha※361がこのタイプに属し、研究結果として、時間計算量が2^{51}、データ計算量が2^{51}となるラウンド数6のChaChaに対する攻撃が発表された。この結果は、CRYPTO 2020で発表された今まで最良の攻撃計算量(時間計算量$2^{77.4}$、データ計算量2^{58})よりも大きく削減され、攻撃が進展したことを示している。ただ、ChaCha20のラウンド数20にはまだマージンがあり、早急な対策が必要となるものではない。

(2) 公開鍵暗号に関する研究及び標準化の動向

公開鍵暗号の一種であるRSA※362については、部分的に秘密鍵が分かっている場合の新規の素因数分解アルゴリズム(Partial Key Exposure Attack)がAsiacrypt 2021において提案された。素因数分解する数をNとして、今まではCRT-RSA指数※363のサイズが$N^{0.122}$以下のときの多項式時間攻撃が提案されていたが、本攻撃はCRT-RSA指数の最下位ビット(LSB:Least Significant Bit)の部分的な知識を仮定して、サイズが$N^{0.122}$以上$N^{0.5}$以下の場合の攻撃を実現している。

また、RSAへの攻撃方法を報告するSchnorr氏の査読前論文に関連して、格子理論を用いた素因数分解についての講演が、PKC 2021にて行われた。このSchnorr氏の攻撃方法は直ちにRSAの危殆化につながらないことは、既に専門家の間で暗黙の了解として共有されているものの、格子によるRSAの解析アプローチ自体は重要な研究であるため、今後も動向を注視すべきである。

NISTによる、量子計算機による解読に耐性を持つ暗号「耐量子計算機暗号(PQC:Post-Quantum Cryptography)」の標準化では、NIST PQC 3rd Standardization Conference※364において、NISTは「格子に基づかない汎用的電子署名スキームに関心がある」とした上で、第3ラウンド終了後、新たな提案募集を行う予定を明らかにした。応募期間は6ヵ月から1年の予定であり、特に構造付き格子(structured lattice)以外の汎用的電子署名スキームに興味を示している。第3ラウンドにおけるセレクションは未だ継続中であり、更に続く第4ラウンドもまた12～18ヵ月かけて行われる見通しである。最終的な標準化については、2024年に最終版を提出する予定であるという。

(3) 実装攻撃に関する研究動向

暗号実装に対する攻撃には、消費電力や処理時間等のサイドチャネル情報から暗号鍵等の秘密情報の復元を試みるサイドチャネル攻撃や、ICチップに一時的な誤動作を起こさせることによって暗号鍵等の秘密情報の暴露を試みる故障利用攻撃等が存在する。

CPUの脆弱性を利用した具体的な暗号実装に対する攻撃として、RAS(Return Address Stack)を利用したサイドチャネル攻撃が発表された※365。

CPUには、処理速度を向上させるための様々な機構が実装されているが、その実装の脆弱性を突いた攻撃が近年注目されている。分岐予測※366や投機的実行※367の実装の脆弱性を突いた攻撃として2018年ごろに発見されたSpectre※368が有名である。最近のCPUには、分岐予測・投機的実行による処理速度向上を更に改善

するために、サブルーチンからのリターン命令における戻り先アドレスの予測機構も組み込まれ、そのためにリターンアドレスをCPU内のバッファに保存するRASという仕組みも実装されている。今回発表された攻撃は、このRASに注目し、悪意あるプロセスがRASのバッファを埋め尽くすことによってキャッシュミスを誘発し、タイミング攻撃※369を行うことで秘密鍵の推測につなげるものである。実際にOpenSSLによる楕円曲線P-256を使用したECDSA※370の署名生成に対する攻撃が有効であることも示している。この攻撃はCPUの様々な処理速度高速化手法が攻撃対象となり得ることを示しており、CPUのセキュリティには今後とも注視が必要である。

その他にも、ECDSAに対する攻撃として、テンプレート攻撃※371の一種であるOnline Template Attackに関する論文※372が発表されている。Online Template Attackは、テンプレート生成のための暗号演算の実行回数が少なくても実行できるように改良した攻撃である。以前の研究では理論的な攻撃可能性のみ検討されていたが、今回の発表では具体的な暗号実装であるlibgcrypt、mbedTLS、wolfTLSに対する適用可能性を示している。

※1 https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2021.pdf〔2022/5/12 確認〕
※2 サイバーセキュリティ戦略本部：サイバーセキュリティ 2021（2020 年度年次報告・2021 年度年次計画） https://www.nisc.go.jp/pdf/policy/kihon-s/cs2021.pdf〔2022/5/12 確認〕
※3 IPA：サイバーセキュリティ経営可視化ツール https://www.ipa.go.jp/security/economics/checktool/index.html〔2022/5/12 確認〕
※4 IPA：サイバーセキュリティ経営ガイドライン Ver 2.0 実践のためのプラクティス集 https://www.ipa.go.jp/security/fy30/reports/ciso/index.html〔2022/5/12 確認〕
※5 NISC：プラス・セキュリティ知識補充講座 カリキュラム例 https://security-portal.nisc.go.jp/dx/pdf/plussecurity_curriculum.pdf〔2022/5/12 確認〕
※6 IPA：サイバーセキュリティお助け隊サービス制度 https://www.ipa.go.jp/security/keihatsu/sme/otasuketai/index.html〔2022/5/12 確認〕
※7 NEDO：戦略的イノベーション創造プログラム（SIP）第 2 期／ IoT 社会に対応したサイバー・フィジカル・セキュリティ https://www.nedo.go.jp/activities/ZZJP2_100123.html〔2022/5/12 確認〕
※8 経済産業省：情報セキュリティサービス審査登録制度 https://www.meti.go.jp/policy/netsecurity/shinsatouroku/touroku.html〔2022/5/12 確認〕
※9 https://security-portal.nisc.go.jp/〔2022/5/12 確認〕
※10 総務省：インターネットトラブル事例集 https://www.soumu.go.jp/use_the_internet_wisely/trouble/〔2022/5/12 確認〕
※11 NISC：クラウドを利用したシステム運用に関するガイダンス（詳細版） https://www.nisc.go.jp/pdf/policy/infra/cloud_guidance.pdf〔2022/5/12 確認〕
※12 https://www.ismap.go.jp/csm?id=cloud_service_list〔2022/5/12 確認〕
※13 https://www.digital.go.jp/about/〔2022/5/12 確認〕
※14 デジタル庁：マイナンバー制度及び国と地方のデジタル基盤抜本改善ワーキンググループの開催について https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/658916e5-76ce-4d02-9377-1273577ffc88/20211021_meeting_my_number_wg_01.pdf〔2022/5/12 確認〕
※15 https://www.nisc.go.jp/pdf/policy/general/kijyunr3.pdf〔2022/5/12 確認〕
※16 https://www.nisc.go.jp/pdf/policy/general/guider3.pdf〔2022/5/12 確認〕
※17 政府 CIO ポータル：ガバメント・クラウド先行事業（市町村の基幹業務システム）の公募及びガバメントクラウド先行事業（地方自治体のセキュリティシステム）の公募について【地方自治体職員対象】 https://cio.go.jp/node/2778〔2022/5/12 確認〕
※18 デジタル庁：ガバメントクラウド先行事業（市町村の基幹業務システム等）の採択結果を公表しました https://www.digital.go.jp/news/ZYzU5DYY/〔2022/5/12 確認〕
※19 NISC：重要インフラのサイバーセキュリティに係る行動計画（案） https://www.nisc.go.jp/pdf/policy/infra/pubcom_keikakuan.pdf〔2022/5/12 確認〕
※20 https://www.nisc.go.jp/pdf/council/2020-meeting/2020-meeting-saisyuhoukoku.pdf〔2022/5/12 確認〕
※21 NISC：日・ASEAN 国際サイバー演習の開催 https://www.nisc.go.jp/pdf/press/international_asean_rcx_20210625_jp.pdf〔2022/5/12 確認〕
※22 NISC：第 14 回 日・ASEAN サイバーセキュリティ政策会議の結果 https://www.nisc.go.jp/pdf/press/AMSJ_CPM_20211021_r2.pdf〔2022/5/12 確認〕
※23 サイバーセキュリティ戦略本部：サイバーセキュリティ研究開発戦略（改訂） https://www.nisc.go.jp/pdf/policy/kihon-1/kenkyu2021-kettei.pdf〔2022/5/12 確認〕
※24 NICT：プライバシー保護連合学習技術を活用した不正送金検知の実証実験を実施 https://www.nict.go.jp/press/2022/03/10-1.html〔2022/5/12 確認〕
※25 サイバーセキュリティ対策推進会議等：政府機関におけるデジタル改革に必要なIT・セキュリティ知識を有する人材の確保・育成総合強化方針 https://www.nisc.go.jp/pdf/policy/materials/jinzai_kyoka_hoshin2021.pdf〔2022/5/12 確認〕
※26 https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/pdf/001_05_00.pdf〔2022/5/12 確認〕
※27 https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/pdf/002_03_00.pdf〔2022/5/12 確認〕
※28 経済産業省：第 6 回 産業サイバーセキュリティ研究会 事務局説明資料 https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/pdf/006_03_00.pdf〔2022/5/12 確認〕
※29 2022 年 4 月の「第 7 回 産業サイバーセキュリティ研究会 事務局説明資料」（https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/pdf/007_03_00.pdf〔2022/5/12 確認〕）では「6 つの処方箋」に増えた。
※30 CPSF の詳細については「情報セキュリティ白書 2020」の「2.1.2 (1) (a) WG1（制度・技術・標準化）」(p.69)を参照。
※31 経済産業省：ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン第 1 版 https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_building/20190617_report.html〔2022/5/12 確認〕
※32 防衛省：防衛産業サイバーセキュリティ基準の強化について https://www.mod.go.jp/atla/pinup/pinup040401.pdf〔2022/5/12 確認〕
※33 https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_denryoku/20210222_report.html〔2022/5/12 確認〕
※34 https://www.jama.or.jp/operation/it/cyb_sec/docs/cyb_sec_guideline_V02_00.pdf〔2022/5/12 確認〕
※35 経済産業省：「スマートホームの安心・安全に向けたサイバー・フィジカル・セキュリティ対策ガイドライン」を策定しました https://www.meti.go.jp/press/2021/04/20210401005/20210401005.html〔2022/5/12 確認〕
※36 https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/pdf/006_05_00.pdf〔2022/5/12 確認〕
※37 https://www.meti.go.jp/policy/netsecurity/wg1/IoT-SSF_ver1.0_UseCase.pdf〔2022/5/12 確認〕
※38 経済産業省：協調的なデータ利活用に向けたデータマネジメント・フレームワークを策定しました https://www.meti.go.jp/press/2022/04/20220408005/20220408005.html〔2022/5/12 確認〕
※39 経済産業省：オープンソースソフトウェアの利活用及びそのセキュリティ確保に向けた管理手法に関する事例集を取りまとめました https://www.meti.go.jp/press/2021/04/20210421001/20210421001.html〔2022/5/12 確認〕
※40 経済産業省：サイバー・フィジカル・セキュリティ確保に向けたソフトウェア管理手法等検討タスクフォースの検討の方向性 https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/software/pdf/006_03_00.pdf〔2022/5/12 確認〕
※41 https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_keiei/pdf/007_03_00.pdf〔2022/5/12 確認〕
※42 経済産業省：サイバーセキュリティ経営ガイドラインと支援ツール https://www.meti.go.jp/policy/netsecurity/mng_guide.html〔2022/5/12 確認〕
※43 IPA：プラクティス・ナビ https://www.ipa.go.jp/security/economics/practice/〔2022/5/12 確認〕
※44 経済産業省：サイバーセキュリティ経営ガイドライン Ver2.0 付録 F サイバーセキュリティ体制構築・人材確保の手引き 第 1.1 版 https://www.meti.go.jp/policy/netsecurity/downloadfiles/tekibihontai1.1r.pdf〔2022/5/12 確認〕
※45 IPA：試行導入・導入実績公表の手引き https://www.ipa.go.jp/files/000090566.pdf〔2022/5/12 確認〕
※46 経済産業省：機器のサイバーセキュリティ確保のためのセキュリティ検証の手引きを取りまとめました https://www.meti.go.jp/press/2021/04/20210419003/20210419003.html〔2022/5/12 確認〕
※47 総務省・経済産業省：DX 時代における企業のプライバシーガバナンスガイドブック ver1.2 https://www.meti.go.jp/policy/it_policy/privacy/guidebook12.pdf〔2022/5/12 確認〕
※48 経済産業省：重要技術マネジメント https://www.meti.go.jp/policy/mono_info_service/mono/technology_management/index.html〔2022/5/12 確認〕
※49 株式会社三菱総合研究所：「産業競争力強化法に基づく技術情報管理認証制度の普及促進に向けた調査分析及び専門家派遣等事業」（経済産業省事業）において専門家の派遣を希望する事業者の公募のご案内について https://www.mri.co.jp/news/public_offering/20210805.html〔2022/5/12 確認〕
※50 経済産業省：「情報セキュリティサービス基準第 2 版」及び「情報セキュリティサービスに関する審査登録機関基準第 2 版」を公表しました https://www.meti.go.jp/press/2021/01/20220131003/20220131003.html〔2022/5/17 確認〕
※51 審査登録機関：「情報セキュリティサービスに関する審査登録機関基準」に適合すると IPA が確認した機関。なお、申請事業者が「情報セキュリティサービス基準」に適合するか否かの審査・判定は、各審査登録機関がその責任において実施する。
※52 IPA：情報セキュリティサービス基準適合サービスリストの公開 https://www.ipa.go.jp/security/it-service/service_list.html〔2022/5/17 確認〕

※ 53 SIG（Special Interest Group）：「特定の分野（各業界におけるサイバー攻撃に関する情報）について、情報を交換するグループ」という意味で、J-CSIP では各業界の参加組織の集合体を SIG と呼んでいる。
※ 54 セプターカウンシル：各重要インフラ分野で整備されたセプターの代表で構成される協議会で、セプター間の情報共有等を行う、分野横断的な情報共有体制。
※ 55 https://www.ipa.go.jp/files/000098129.pdf〔2022/5/16 確認〕
※ 56 「マルウェア」等の用語を混在して使用すると、読者を混乱させる可能性があるため、本白書では特に断りのない限り、または文献引用上の正確性を期す必要のない限り、総称して「ウイルス」と表現する。
※ 57 IPA：サイバー情報共有イニシアティブ（J-CSIP）運用状況［2021 年 10 月～ 12 月］ https://www.ipa.go.jp/files/000095766.pdf〔2022/5/16 確認〕
※ 58 IPA：サイバーレスキュー隊 J-CRAT（ジェイ・クラート） https://www.ipa.go.jp/security/J-CRAT/index.html〔2022/5/16 確認〕
IPA：J-CRAT ／標的型サイバー攻撃特別相談窓口 https://www.ipa.go.jp/security/tokubetsu/index.html〔2022/5/16 確認〕
※ 59 https://www.ipa.go.jp/security/J-CRAT/index.html〔2022/5/16 確認〕
※ 60 https://www.soumu.go.jp/main_content/000698567.pdf〔2022/5/16 確認〕
※ 61 https://www.soumu.go.jp/main_content/000761893.pdf〔2022/5/16 確認〕
※ 62 https://warp.ndl.go.jp/info:ndljp/pid/11688280/www.kantei.go.jp/jp/singi/it2/dgov/201225/siryou1.pdf〔2022/5/16 確認〕
※ 63 https://www.nisc.go.jp/pdf/council/cs/dai17/17shiryou02.pdf〔2022/5/16 確認〕
※ 64 新経済連盟：電気通信事業法の改正の方向性に対する懸念について https://jane.or.jp/proposal/pressrelease/15987.html〔2022/5/16 確認〕
一般社団法人日本経済団体連合会：総務省『電気通信事業ガバナンス検討会報告書（案）』に対する意見 https://www.keidanren.or.jp/policy/2022/012.html〔2022/5/16 確認〕
※ 65 総務省：「電気通信事業ガバナンス検討会 報告書」及び意見募集の結果の公表 https://www.soumu.go.jp/menu_news/s-news/01kiban05_02000237.html〔2022/5/16 確認〕
※ 66 総務省：IP ネットワーク設備委員会 https://www.soumu.go.jp/main_sosiki/joho_tsusin/policyreports/joho_tsusin/ipnet/ipnet.html〔2022/5/16 確認〕
※ 67 OODA：Observe, Orient, Decide, Act の略。
※ 68 総務省：情報通信審議会 情報通信技術分科会IPネットワーク設備委員会第五次報告（案）～ IoT の普及に対応した電気通信設備に係る技術的条件～ https://www.soumu.go.jp/main_content/000759203.pdf〔2022/5/16 確認〕
※ 69 総務省：情報通信審議会 情報通信技術分科会 IP ネットワーク設備委員会 第五次報告（案）に対する意見募集の結果 https://www.soumu.go.jp/menu_news/s-news/01kiban05_02000228.html〔2022/5/16 確認〕
※ 70 総務省：電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会 第四次とりまとめ（案）についての意見募集 https://www.soumu.go.jp/menu_news/s-news/01kiban18_01000130.html〔2022/5/16 確認〕
※ 71 総務省：「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会 第四次とりまとめ」及び意見募集の結果の公表 https://www.soumu.go.jp/menu_news/s-news/01kiban18_01000134.html〔2022/5/16 確認〕
※ 72 e-GOV 法令検索：特定高度情報通信技術活用システムの開発供給及び導入の促進に関する法律 https://elaws.e-gov.go.jp/document?lawid=502AC0000000037〔2022/5/16 確認〕
※ 73 総務省：令和 4 年度税制改正要望の結果 https://www.soumu.go.jp/menu_news/s-news/01kanbo05_02000157.html〔2022/5/16 確認〕
※ 74 O-RAN：https://www.o-ran.org〔2022/5/16 確認〕
※ 75 総務省：2.3GHz 帯における第 5 世代移動通信システムの普及のための周波数の割当てに関する意見募集 https://www.soumu.go.jp/menu_news/s-news/01kiban14_02000525.html〔2022/5/16 確認〕
※ 76 ICT-ISAC JAPAN:ローカル 5G セキュリティ対策に関するアンケート結果（概要版）の公開について https://www.ict-isac.jp/news/news20210315.html〔2022/5/16 確認〕
※ 77 総務省：テレワークセキュリティガイドライン 第5版 https://www.soumu.go.jp/main_content/000752925.pdf〔2022/5/16 確認〕
※ 78 総務省：中小企業等担当者向けテレワークセキュリティの手引き（チェックリスト）第2版 https://www.soumu.go.jp/main_content/000753141.pdf〔2022/5/16 確認〕
※ 79 株式会社東京商工リサーチ：「テレワークセキュリティに係る実態調査 調査報告書」 https://www.soumu.go.jp/main_content/000811682.pdf〔2022/5/16 確認〕
※ 80 総務省：プラットフォームサービスに関する研究会最終報告書 https://www.soumu.go.jp/main_content/000668595.pdf〔2022/5/16 確認〕
※ 81 総務省：タイムスタンプについて https://www.soumu.go.jp/main_sosiki/joho_tsusin/top/ninshou-law/timestamp.html〔2022/5/16 確認〕
※ 82 総務省：組織が発行するデータの信頼性を確保する制度に関する検討会取りまとめ（案）及び e シールに係る指針（案）に対する意見募集の結果 https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00114.html〔2022/5/16 確認〕
※ 83 総務省・法務省・経済産業省：利用者の指示に基づきサービス提供事業者自身の署名鍵により 暗号化等を行う電子契約サービスに関する Q&A https://www.soumu.go.jp/main_content/000697715.pdf〔2022/5/16 確認〕
※ 84 総務省・法務省・経済産業省：利用者の指示に基づきサービス提供事業者自身の署名鍵により暗号化等を行う電子契約サービスに関する Q&A（電子署名法第3条関係） https://www.soumu.go.jp/main_content/000705576.pdf〔2022/5/16 確認〕
※ 85 総務省：電気通信事業法に基づく端末機器の基準認証に関するガイドライン（第２版） https://www.soumu.go.jp/main_content/000705080.pdf〔2022/5/16 確認〕
※ 86 CCDS：サーティフィケーションプログラムにおけるセキュリティ要件 https://www.ccds.or.jp/certification/requirements.html〔2022/5/16 確認〕
※ 87 CCDS：プログラム概要 https://www.ccds.or.jp/certification/index.html〔2022/5/16 確認〕
※ 88 CCDS：2021.10.15 [CCDS] 現金自動預け払い機 (ATM) 関連システムの物理・サイバー攻撃対策に関する CCDS サーティフィケーションプログラムの運用開始 https://www.ccds.or.jp/event/2021/20211015/20211015.html〔2022/5/16 確認〕
※ 89 総務省・NICT：IoT 機器調査及び利用者への注意喚起の取組「NOTICE」の実施 https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00011.html〔2022/5/16 確認〕
※ 90 総務省：情報通信ネットワークの安全性・信頼性の確保に係るサイバーセキュリティ対策の現状と課題 https://www.soumu.go.jp/main_content/000812244.pdf〔2022/5/16 確認〕
※ 91 NICT：サイバー攻撃に悪用されるおそれのある IoT 機器の調査等（NOTICE）の取組内容の変更について https://notice.go.jp/news/topic/news20220121〔2022/5/16 確認〕
※ 92 NICT：NICTER 観測レポート 2021 https://www.nict.go.jp/cyber/report/NICTER_report_2021.pdf〔2022/5/16 確認〕
※ 93 総務省：「クラウドサービス提供における情報セキュリティ対策ガイドライン（第３版）」（案）に対する意見募集の結果及び「クラウドサービス提供における情報セキュリティ対策ガイドライン（第３版）」の公表 https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00121.html〔2022/5/16 確認〕
※ 94 https://www.soumu.go.jp/main_content/000757799.pdf〔2022/5/16 確認〕
※ 95 https://www.soumu.go.jp/main_content/000757800.pdf〔2022/5/16 確認〕
※ 96 総務省：日仏 ICT 政策協議（第 21 回）の結果 https://www.soumu.go.jp/menu_news/s-news/01tsushin08_02000120.html〔2022/5/16 確認〕
※ 97 総務省：日 EU・ICT 政策対話（第 27 回）の結果 https://www.soumu.go.jp/menu_news/s-news/01tsushin08_02000128.html〔2022/5/16 確認〕
※ 98 総務省：日独 ICT 政策対話（第 6 回）の結果 https://www.soumu.go.jp/menu_news/s-news/01tsushin08_02000130.html〔2022/5/16 確認〕
※ 99 NICT：サイバーセキュリティネクサス https://www.nict.go.jp/cynex/〔2022/5/16 確認〕
※ 100 NICT：サイバーセキュリティ演習基盤 CYROP のオープン化トライアルを開始 https://www.nict.go.jp/press/2022/02/03-1.html〔2022/5/16 確認〕
※ 101 総務省：地方公共団体における情報セキュリティポリシーに関するガイドラインの改定等に係る検討会 https://www.soumu.go.jp/main_sosiki/kenkyu/chiho_security_r03/index.html〔2022/5/16 確認〕
※ 102 総務省：「地方公共団体における情報セキュリティポリシーに関するガイドライン」等の公表及び意見募集の結果 https://www.soumu.go.jp/menu_news/s-news/01gyosei07_02000128.html〔2022/5/16 確認〕
※ 103 総務省：「地方公共団体における情報セキュリティポリシーに関するガイドライン」改定のポイントについて（案）」 https://www.soumu.

go.jp/main_content/000785574.pdf〔2022/5/16 確認〕
※ 104 閣議決定：デジタル社会の形成に関する重点計画・情報システム整備計画・官民データ活用推進基本計画について https://cio.go.jp/sites/default/files/uploads/documents/digital/20211224_policies_priority_package.pdf〔2022/5/16 確認〕
デジタル庁：デジタル社会の実現に向けた重点計画 https://www.digital.go.jp/policies/priority-policy-program〔2022/5/16 確認〕
※ 105 デジタル庁：地方自治体によるガバメントクラウドの活用について（案） https://cio.go.jp/sites/default/files/uploads/documents/digital/20211224_local_governments_02.pdf〔2022/5/16 確認〕
※ 106 内閣官房：ガバメントクラウド先行事業（セキュリティシステム）公募要項 https://cio.go.jp/sites/default/files/uploads/documents/koubosecurity20210604.pdf〔2022/5/16 確認〕
※ 107 内閣官房：地方自治体によるガバメントクラウドの活用（先行事業）について https://cio.go.jp/sites/default/files/uploads/documents/senkoujigyougaiyou20210831.pdf〔2022/5/16 確認〕
※ 108 デジタル庁：ガバメントクラウド先行事業（市町村の基幹業務システム等）の採択結果を公表しました https://www.digital.go.jp/posts/ZYzU5DYY〔2022/5/16 確認〕
※ 109 総務省：無線 LAN（Wi-Fi）の安全な利用（セキュリティ確保）について https://www.soumu.go.jp/main_sosiki/cybersecurity/wi-fi/〔2022/5/16 確認〕
※ 110 総務省：無線 LAN のセキュリティ対策に係るオンライン講座の開講 https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00127.html〔2022/5/16 確認〕
※ 111 e-Gov 法令検索：不正アクセス行為の禁止等に関する法律 https://elaws.e-gov.go.jp/document?lawid=411AC0000000128〔2022/5/16 確認〕
※ 112 総務省：不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況 https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00128.html〔2022/5/16 確認〕
※ 113 https://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/telecom_perinfo_guideline_intro.html〔2022/5/16 確認〕
※ 114 警察庁：サイバーセキュリティ戦略の改定について（依命通達） https://www.npa.go.jp/cybersecurity/pdf/300906_senryaku.pdf〔2022/5/10 確認〕
※ 115 警察庁：サイバーセキュリティ重点施策の改定について（通達） https://www.npa.go.jp/cybersecurity/pdf/300906_juutensesaku.pdf〔2022/5/10 確認〕
※ 116 https://www.npa.go.jp/publications/statistics/cybersecurity/data/R03_kami_cyber_jousei.pdf〔2022/5/10 確認〕
※ 117 https://www.npa.go.jp/publications/statistics/cybersecurity/data/R03_cyber_jousei.pdf〔2022/5/10 確認〕
※ 118 警察庁：企業の皆様へ サイバー犯罪の被害は警察へ通報を! https://www.npa.go.jp/cyber/ransom/pdf/leaflet.pdf〔2022/5/10 確認〕
警察庁：ランサムウェア被害防止対策 https://www.npa.go.jp/cyber/ransom/index.html〔2022/5/10 確認〕
※ 119 一般社団法人日本損害保険協会：多様化するリスクとサイバー保険 https://www.sonpo.or.jp/cyber-hoken/risk/〔2022/5/10 確認〕
※ 120 警察庁：不正アクセス行為対策等の実態調査 アクセス制御機能に関する技術の研究開発の状況等に関する調査 調査報告書 https://www.npa.go.jp/cyber/research/r3/R3countermeasures.pdf〔2022/5/10 確認〕
※ 121 警察庁：令和 3 年版警察白書（特集 2 サイバー空間の安全の確保） https://www.npa.go.jp/hakusyo/r03/pdf/03_tokushu02.pdf〔2022/5/10 確認〕
※ 122 外務省：中国政府を背景に持つ APT40 といわれるサイバー攻撃グループによるサイバー攻撃等について（外務報道官談話） https://www.mofa.go.jp/mofaj/press/danwa/page6_000583.html〔2022/5/10 確認〕
※ 123 NISC・警察庁:中国政府を背景に持つ APT40 といわれるサイバー攻撃グループによるサイバー攻撃等について（注意喚起） https://www.npa.go.jp/cybersecurity/pdf/20210719pr.pdf〔2022/5/10 確認〕
※ 124 警察庁：治安の回顧と展望（令和3年版） https://www.npa.go.jp/bureau/security/publications/kaiko_to_tenbou/R3/kaitenR3.pdf〔2022/5/10 確認〕
※ 125 サイバーセキュリティ政策会議：サイバー空間の脅威への対処について法学・技術系学者、弁護士、ITベンダー、日本サイバー犯罪対策センター等多様な分野の有識者による検討を行うサイバーセキュリティ・情報化審議官主催の私的懇談会。
警察庁：サイバーセキュリティ政策会議 https://www.npa.go.jp/cybersecurity/CS.html〔2022/5/10 確認〕
※ 126 サイバーセキュリティ政策会議：実空間とサイバー空間とが融合したデジタル社会の安全・安心の確保 https://www.npa.go.jp/cybersecurity/pdf/20211217_2.pdf〔2022/5/10 確認〕
※ 127 警察庁：警察法の一部を改正する法律案要綱 https://www.npa.go.jp/laws/kokkai/220128/01_youkou.pdf〔2022/5/10 確認〕
※ 128 JC3：総務省を騙った特別定額給付金に関するフィッシングに注意 https://www.jc3.or.jp/threats/topics/article-42.html〔2022/5/10 確認〕
※ 129 警察庁：警察活動の回顧と展望 https://www.npa.go.jp/bureau/soumu/tenbou/kaikototenbou.pdf〔2022/5/10 確認〕
※ 130 JC3：フィッシングターゲットの変遷 https://www.jc3.or.jp/threats/topics/article-430.html〔2022/5/10 確認〕
※ 131 警察庁：サイバー攻撃に対する技術的対応 https://www.npa.go.jp/joutuu/012.htm〔2022/5/10 確認〕
※ 132 警察庁：令和３年の犯罪情勢 https://www.npa.go.jp/publications/statistics/crime/situation/r3_hanzaijyousei.pdf〔2022/5/10 確認〕
※ 133 警察庁：犯罪インフラ化するSMS認証代行への対策について https://www.npa.go.jp/cyber/policy/pdf/R030422_SMStaisaku.pdf〔2022/5/10 確認〕
※ 134 警察庁：令和２年の犯罪情勢 https://www.npa.go.jp/publications/statistics/crime/situation/r2_report_c.pdf〔2022/5/10 確認〕
※ 135 正式名称は「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC 暗号リスト）」（https://www.cryptrec.go.jp/list/cryptrec-ls-0001-2012r6.pdf〔2022/4/21 確認〕）。現在は、「電子政府推奨暗号リスト」「推奨候補暗号リスト」「運用監視暗号リスト」の三つのリストから構成される。
※ 136 https://www.ipa.go.jp/security/ipg/documents/ipa-cryptrec-gl-3002-1.0.pdf〔2022/4/21 確認〕
※ 137 EdDSA（Edwards-curve Digital Signature Algorithm）：楕円曲線の一種であるエドワーズ曲線を用いたデジタル署名アルゴリズム。
※ 138 NIST Lightweight Cryptography コンペティションファイナリスト：NIST が主催する軽量暗号コンペティション（NIST：Lightweight Cryptography https://csrc.nist.gov/Projects/lightweight-cryptography〔2022/4/21 確認〕）の最終選考に残ったアルゴリズム。
※ 139 CRYPTREC：2021 年度 第1回 暗号技術検討会 https://www.cryptrec.go.jp/report/cryptrec-mt-1011-2021.pdf〔2022/4/21 確認〕
上記に含まれる「配付資料3−4 2021 年度暗号技術調査 WG（耐量子計算機暗号）活動報告」を参照。
※ 140 外務省：G7 コーンウォール・サミット（概要） https://www.mofa.go.jp/mofaj/ecm/ec/page4_005342.html〔2022/5/11 確認〕
※ 141 外務省：2021 年開かれた社会声明 https://www.mofa.go.jp/mofaj/files/100200087.pdf〔2022/5/11 確認〕
※ 142 外務省：G7 首脳テレビ会議 https://www.mofa.go.jp/mofaj/ecm/ec/page6_000665.html〔2022/5/11 確認〕
※ 143 外務省：G7 首脳声明 https://www.mofa.go.jp/mofaj/ecm/ec/page4_005524.html〔2022/5/11 確認〕
※ 144 外務省：G7 首脳会合 https://www.mofa.go.jp/mofaj/ecm/ec/page6_000680.html〔2022/5/11 確認〕
※ 145 首相官邸：ロシアによるウクライナ侵略を踏まえた対応について https://www.kantei.go.jp/jp/headline/ukraine2022/index.html〔2022/5/23 確認〕
※ 146 NISC：東京大会におけるサイバーセキュリティ対策と今後の取組方針 https://www.nisc.go.jp/pdf/policy/2020/Tokyo2020houkoku.pdf〔2022/5/11 確認〕
※ 147 日本電信電話株式会社：東京 2020 オリンピック・パラリンピック競技大会における NTT の貢献 https://group.ntt/jp/newsrelease/2021/10/21/211021a.html〔2022/5/11 確認〕
※ 148 外務省：2020 年東京オリンピック・パラリンピック競技大会に向けた外務省の取り組み https://www.mofa.go.jp/mofaj/p_pd/ep/page24_000800.html#section10〔2022/5/11 確認〕
※ 149 外務省：第２回日米豪印首脳会合 https://www.mofa.go.jp/mofaj/fp/nsp/page4_005424.html〔2022/5/11 確認〕
※ 150 外務省：サイバーセキュリティに関する国連政府専門家会合最終会合における報告書の採択 https://www.mofa.go.jp/mofaj/press/release/press24_000114.html〔2022/5/11 確認〕
※ 151 外務省：サイバー行動に適用される国際法に関する日本政府の基本的な立場について https://www.mofa.go.jp/mofaj/gaiko/page3_003059.html〔2022/5/11 確認〕
※ 152 外務省：第６回日英サイバー協議の開催 https://www.mofa.go.jp/mofaj/press/release/press3_000511.html〔2022/5/11 確認〕
※ 153 外務省：第４回日エストニア・サイバー協議の開催 https://www.mofa.go.jp/mofaj/erp/we/page24_001587.html〔2022/5/11 確認〕
※ 154 外務省：日米安全保障協議委員会（日米「２＋２」）（結果）

https://www.mofa.go.jp/mofaj/na/st/page1_000942.html〔2022/5/11 確認〕
※ 155 外務省：日米安全保障協議委員会（日米「2＋2」）（概要）https://www.mofa.go.jp/mofaj/na/st/page4_005483.html〔2022/5/11 確認〕
※ 156 外務省：日米首脳会談 https://www.mofa.go.jp/mofaj/na/na1/us/page1_000951.html〔2022/5/11 確認〕
※ 157 外務省：日米首脳テレビ会談 https://www.mofa.go.jp/mofaj/na/na1/page1_001086.html〔2022/5/11 確認〕
※ 158 外務省：第 27 回日 EU 定期首脳協議（概要） https://www.mofa.go.jp/mofaj/erp/ep/page6_000563.html〔2022/5/11 確認〕
※ 159 外務省：第 24 回日 ASEAN 首脳会議 https://www.mofa.go.jp/mofaj/area/asean/page3_003142.html〔2022/5/11 確認〕
※ 160 http://aseanregionalforum.asean.org/〔2022/5/11 確認〕
※ 161 外務省：サイバーセキュリティに関する第 3 回 ARF 会期間会合の開催（結果） https://www.mofa.go.jp/mofaj/press/release/press1_000518.html〔2022/5/11 確認〕
※ 162 経済産業省：第 14 回 日・ASEAN サイバーセキュリティ政策会議を開催しました https://www.meti.go.jp/press/2021/10/20211022006/20211022006.html〔2022/5/11 確認〕
※ 163 経産省：「インド太平洋地域向け日米 EU 産業制御システムサイバーセキュリティウィーク」を実施しました https://www.meti.go.jp/press/2021/11/20211101001/20211101001.html〔2022/5/11 確認〕
※ 164 The MITRE Corporation（https://www.mitre.org/〔2022/5/11 確認〕）は 1958 年創立の非営利民間企業で、米国連邦政府機関の出資を受けた研究開発、及び成果の民間移転を推進している。
※ 165 サイバーセキュリティ国際シンポジウム事務局：第 11 回サイバーセキュリティ国際シンポジウム https://symp.cysec-lab.keio.ac.jp/2021oct/index-j.html〔2022/5/11 確認〕
※ 166 株式会社日本経済新聞社・株式会社日経ビーピー：サイバー・イニシアチブ東京 2021 https://project.nikkeibp.co.jp/event/2021z1129cit/〔2022/5/11 確認〕
※ 167 Australian Government：Launch of Australia's International Cyber and Critical Technology Engagement Strategy https://www.internationalcybertech.gov.au/launch-of-australias-international-cyber-critical-tech-strategy〔2022/5/10 確認〕
※ 168 DPMC：New Zealand's Cyber Security Emergency Response Plan https://dpmc.govt.nz/publications/new-zealands-cyber-security-emergency-response-plan〔2022/5/10 確認〕
※ 169 CSA：The Singapore Cybersecurity Strategy 2021 https://www.csa.gov.sg/sgcybersecuritystrategy2021〔2022/5/10 確認〕
※ 170 APNIC：How can organizations support cybersecurity in the Pacific? https://blog.apnic.net/2021/07/29/how-can-organizations-support-cybersecurity-in-the-pacific/〔2022/5/10 確認〕
※ 171 PaCSON：Annual Report 2020 https://pacson.org/sites/default/files/2021-12/PaCSON%202020%20Annual%20report.pdf〔2022/5/10 確認〕
※ 172 Ministry of Digital Economy and Society：https://www.mdes.go.th/news/detail/4583〔2022/5/10 確認〕
上記では、Web ページのタイトルがタイ語のため省略している。
※ 173 National News Bureau of Thailand：Thailand's Cyber Security Agency Will Develop Security Skills in 7 Sectors https://thainews.prd.go.th/en/news/detail/TCATG210917142334222〔2022/5/10 確認〕
※ 174 https://www.apcert.org/〔2022/5/10 確認〕
※ 175 APCERT：TSUBAME Working Group https://www.apcert.org/about/structure/tsubame-wg/index.html〔2022/5/10 確認〕
※ 176 APCERT：APCERT CYBER DRILL 2021 "SUPPLY CHAIN ATTACK THROUGH SPEAR-PHISHING - BEWARE OF WORKING FROM HOME -" https://www.apcert.org/documents/pdf/APCERT_Drill2021_Press%20Release.pdf〔2022/5/10 確認〕
※ 177 APCERT：Documents https://www.apcert.org/documents/index.html〔2022/5/10 確認〕
※ 178 https://www.cybersecurity.my/en/index.html〔2022/5/10 確認〕
※ 179 https://www.cert.org.cn/publish/english/index.html〔2022/5/10 確認〕
※ 180 (ISC)²：(ISC)² Cybersecurity Workforce Study Sheds New Light on Global Talent Demand Amid a Lingering Pandemic https://www.isc2.org/News-and-Events/Press-Room/Posts/2021/10/26/ISC2-Cybersecurity-Workforce-Study-Sheds-New-Light-on-Global-Talent-Demand〔2022/5/12 確認〕
※ 181 https://www.nri-secure.co.jp/download/insight2021-report〔2022/5/12 確認〕
※ 182 Gartner, Inc.：The Rise of Business Technologists https://www.gartner.com/en/articles/the-rise-of-business-technologists〔2022/5/12 確認〕
※ 183 https://www.meti.go.jp/press/2021/04/20210426002/20210426002-1.pdf〔2022/5/12 確認〕
※ 184 業務によりセキュリティ関連のタスクの占める割合は様々と考えられる。
※ 185 https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/pdf/007_03_00.pdf〔2022/5/12 確認〕
※ 186 NISC：プラス・セキュリティ知識 https://security-portal.nisc.go.jp/dx/plussecurity.html〔2022/5/12 確認〕
※ 187 https://www.meti.go.jp/shingikai/mono_info_service/digital_jinzai/pdf/005_03_01.pdf〔2022/5/12 確認〕
※ 188 経済産業省：デジタル人材育成プラットフォーム「マナビ DX」を開設しました! https://www.meti.go.jp/press/2021/03/20220329002/20220329002.html〔2022/5/12 確認〕
※ 189 https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_keiei/pdf/008_03_00.pdf〔2022/5/12 確認〕
※ 190 重要インフラ：他に代替することが著しく困難なサービスを提供する事業が形成する国民生活及び社会経済活動の基盤であり、その機能が停止、低下又は利用不可能な状態に陥った場合に、我が国の国民生活又は社会経済活動に多大なる影響を及ぼすおそれが生じるもので、重要インフラ分野として指定する分野。具体的には、「情報通信」「金融」「航空」「空港」「鉄道」「電力」「ガス」「政府・行政サービス（地方公共団体を含む）」「医療」「水道」「物流」「化学」「クレジット」及び「石油」の 14 分野。
NISC：重要インフラの情報セキュリティ対策に係る第4次行動計画 https://www.nisc.go.jp/pdf/policy/infra/infra_rt4.pdf〔2022/5/10 確認〕
※ 191 IPA：「インド太平洋地域向け日米 EU 産業制御システムサイバーセキュリティウィーク」を実施しました https://www.ipa.go.jp/icscoe/news_all/news20211101.html〔2022/5/10 確認〕
※ 192 IPA：中核人材育成プログラム修了者コミュニティ「叶会（かなえかい）」 https://www.ipa.go.jp/icscoe/program/core_human_resource/icscoe_alumni.html〔2022/5/10 確認〕
※ 193 IPA：情報処理安全確保支援士（登録セキスペ）になるには https://www.ipa.go.jp/siensi/toberiss/index.html〔2022/5/10 確認〕
※ 194 IPA：責任者向けプログラム サイバー危機対応机上演習（CyberCREST） https://www.ipa.go.jp/icscoe/program/short/all_industries/2021.html〔2022/5/10 確認〕
※ 195 IPA：責任者向けプログラム 業界別サイバーレジリエンス強化演習（CyberREX） https://www.ipa.go.jp/icscoe/program/short/specific_industries/2021.html〔2022/5/10 確認〕
※ 196 IPA：戦略マネジメント系セミナー https://www.ipa.go.jp/icscoe/program/middle/strategic_management/2021.html〔2022/5/10 確認〕
※ 197 IPA：実務者向けプログラム 制御システム向けサイバーセキュリティ演習 https://www.ipa.go.jp/icscoe/program/short/icssec/2021.html〔2022/5/10 確認〕
※ 198 IPA：実務者向けプログラム ERAB サイバーセキュリティトレーニング https://www.ipa.go.jp/icscoe/program/short/erab/2021.html〔2022/5/10 確認〕
※ 199 https://www.meti.go.jp/press/2019/12/20191227004/20191227004-1.pdf〔2022/5/10 確認〕
※ 200 CBT（Computer Based Testing）方式：試験会場に設置されたコンピュータを利用して実施する試験方式のこと。受験者はコンピュータに表示された試験問題に対して、マウスやキーボードを用いて解答する。
※ 201 IPA：情報処理技術者試験 情報処理安全確保支援士試験 統計資料 令和 3 年度試験 全試験区分版 https://www.jitec.ipa.go.jp/1_07toukei/toukei_r03.pdf〔2022/5/17 確認〕
※ 202 IPA：国家資格「情報処理安全確保支援士」2022 年 4 月 1 日付登録者 1,016 名の内訳を公開しました https://www.ipa.go.jp/siensi/data/20220401newriss.html〔2022/5/17 確認〕
※ 203 IPA：情報処理安全確保支援士（登録セキスペ）の受講する講習について https://www.ipa.go.jp/siensi/lecture/index.html〔2022/5/17 確認〕
※ 204 経済産業省：情報処理安全確保支援士特定講習 https://www.meti.go.jp/policy/it_policy/jinzai/tokutei.html〔2022/5/17 確認〕
※ 205 IPA:セキュリティ・キャンプ全国大会 2022 オンライン 前回レポート https://www.ipa.go.jp/jinzai/camp/2022/zenkoku2022_report.html〔2022/5/12 確認〕
※ 206 IPA：セキュリティ・ネクストキャンプ 2021 オンライン 応募要項 https://www.ipa.go.jp/jinzai/camp/2021/next2021_vote.html〔2022/5/12 確認〕
※ 207 一般社団法人セキュリティ・キャンプ協議会事務局：セキュリティ・ミニキャンプ オンライン 2021 https://www.security-camp.or.jp/

minicamp/online2021.html〔2022/5/12 確認〕
※ 208 一般社団法人セキュリティ・キャンプ協議会事務局：セキュリティ・ミニキャンプ in 山梨 2021 https://www.security-camp.or.jp/minicamp/yamanashi2021.html〔2022/5/12 確認〕
一般社団法人セキュリティ・キャンプ協議会事務局：セキュリティ・ミニキャンプ in 広島 2021 https://www.security-camp.or.jp/minicamp/hiroshima2021.html〔2022/5/12 確認〕
一般社団法人セキュリティ・キャンプ協議会事務局：セキュリティ・ミニキャンプ in 大阪 2022 https://www.security-camp.or.jp/minicamp/osaka2022.html〔2022/5/12 確認〕
※ 209 一般社団法人セキュリティ・キャンプ協議会事務局（Twitter アカウント）：https://twitter.com/security_camp/status/1483243001359265794?cxt=HHwWhMDTudbpxJUpAAAA〔2022/5/12 確認〕
一般社団法人セキュリティ・キャンプ協議会事務局：GCC 2022 Taiwan - Global Cybersecurity Camp 2022 Taiwan https://www.security-camp.or.jp/event/gcc_online2022.html〔2022/5/12 確認〕
※ 210 Asian Cyber Security Challenge 2021：https://acsc.asia〔2022/5/12 確認〕
一般社団法人セキュリティ・キャンプ協議会事務局：ACSC 2021 - Asian Cyber Security Challenge 2021 https://www.security-camp.or.jp/event/acsc2021.html〔2022/5/12 確認〕
※ 211 International Cybersecurity Challenge：https://ecsc.eu/icc/〔2022/5/12 確認〕
※ 212 大阪大学大学院情報科学研究科 enPiT 事務局：［文部科学省］成長分野を支える情報技術人材の育成拠点の形成（enPiT） https://www.enpit.jp/〔2022/5/12 確認〕
※ 213 SecCap 事務局：SecCap について https://www.seccap.jp/gs/about/〔2022/5/12 確認〕
※ 214 大阪大学大学院情報科学研究科 enPiT 事務局：セキュリティ分野 https://www.enpit.jp/fields/security/index.html〔2022/5/12 確認〕
※ 215 Basic SecCap コンソーシアム：Basic SecCap コース https://www.seccap.jp/basic/pdf/BasicSecCap_pamph.pdf〔2022/5/12 確認〕
※ 216 enPiT Pro Security：https://www.seccap.pro〔2022/5/12 確認〕
※ 217 大阪大学：安全なデータ利活用のためのプロフェッショナル人材育成コース https://cy2sec.comm.eng.osaka-u.ac.jp/miyaji-lab/pro-sec/index-jp.html〔2022/5/12 確認〕
※ 218 SECCON：SECCON 実行委員会／WG メンバー https://www.seccon.jp/2021/seccon/executivecommittee.html〔2022/5/12 確認〕
※ 219 SECCON：SECCON と は https://www.seccon.jp/2021/seccon/about.html〔2022/5/12 確認〕
※ 220 SECCON：SECCON 2021 開催スケジュール https://www.seccon.jp/2021/seccon/schedule.html〔2022/5/12 確認〕
※ 221 SECCON：SECCON 2021 電脳会議 https://www.seccon.jp/2021/ep211218.html〔2022/5/12 確認〕
※ 222 SECCON：第 4 回 SECCON Beginners CTF（5 月 22 日）開催終了しました https://www.seccon.jp/2021/seccon_beginners/_seccon_beginners_ctf_2021.html〔2022/5/12 確認〕
※ 223 CTF for GIRLS：第 16 回 CTF for GIRLS ワークショップ開催レポート http://girls.seccon.jp/news24.html〔2022/5/12 確認〕
※ 224 CTF for GIRLS：第 17 回 CTF for GIRLS ワークショップ開催レポート http://girls.seccon.jp/news25.html〔2022/5/12 確認〕
※ 225 CTF for GIRLS：第 18 回 CTF for GIRLS（ワークショップ）開催のご案内 http://girls.seccon.jp/news0.html〔2022/5/12 確認〕
※ 226 特定非営利活動法人日本ネットワークセキュリティ協会：インターンシップ募集 https://www.jnsa.org/internship/index.html#jnsainternship〔2022/5/12 確認〕
※ 227 東京工業大学：カリキュラム概要 https://www.academy.titech.ac.jp/cumot/cy/schedule.html〔2022/5/12 確認〕
※ 228 独立行政法人国立高等専門学校機構：TOPICS & NEWS https://k-sec.kochi-ct.ac.jp/topics-news/info-1.html〔2022/5/12 確認〕
※ 229 経済産業省：サイバーセキュリティ経営ガイドラインと支援ツール https://www.meti.go.jp/policy/netsecurity/mng_guide.html〔2022/5/12 確認〕
※ 230 https://www.ipa.go.jp/security/vuln/10threats2022.html〔2022/5/19 確認〕
※ 231 NRI セキュア社：NRI Secure Insight 2020 https://www.nri-secure.co.jp/download/insight2020-report〔2022/5/19 確認〕
※ 232 https://www.meti.go.jp/policy/netsecurity/downloadfiles/guide2.0.pdf〔2022/5/17 確認〕
※ 233 IPA：「2021 年度 中小企業における情報セキュリティ対策に関する実態調査」について https://www.ipa.go.jp/security/fy2021/reports/sme/index.html〔2022/5/17 確認〕
※ 234 IPA：サイバーセキュリティお助け隊（令和 2 年度中小企業向けサイバーセキュリティ対策支援体制構築事業）の報告書について https://www.ipa.go.jp/security/fy2020/reports/sme/otasuketai_houkoku.html〔2022/5/17 確認〕
※ 235 https://www.ipa.go.jp/security/sc3/〔2022/5/17 確認〕
※ 236 https://www.ipa.go.jp/security/sc3/about/〔2022/5/17 確認〕
※ 237 https://www.ipa.go.jp/files/000092713.pdf〔2022/5/17 確認〕
※ 238 https://www.ipa.go.jp/security/security-action/〔2022/5/17 確認〕
※ 239 https://www.tokyo-cci.or.jp/hajimete-it/security/〔2022/5/17 確認〕
※ 240 https://www.tokyo-cci.or.jp/page.jsp?id=1025418〔2022/5/17 確認〕
※ 241 https://school-security.jp/pdf/2020.pdf〔2022/5/17 確認〕
※ 242 1 件の事故で複数の経路・媒体から漏えいした場合は、それぞれの経路・媒体に含まれていた個人情報漏えい人数を合算している。
※ 243 https://www.mext.go.jp/content/20220303-mxt_shuukyo01-100003157_005.pdf〔2022/5/17 確認〕
※ 244 文部科学省：GIGA スクール構想の実現へ https://www.mext.go.jp/content/20200625-mxt_syoto01-000003278_1.pdf〔2022/5/17 確認〕
※ 245 内閣府：GIGA スクール構想の実現ロードマップ https://www5.cao.go.jp/keizai-shimon/kaigi/special/reform/committee/20200323/shiryou3_1_1.pdf〔2022/5/17 確認〕
※ 246 文部科学省：GIGA スクール構想の実現 https://www.mext.go.jp/content/20210118-mxt_jogai01-000011648_001.pdf〔2022/5/17 確認〕
文部科学省：令和 2 年度第 3 次補正予算案への対応について https://www.mext.go.jp/content/000091784.pdf〔2022/5/17 確認〕
※ 247 文部科学省：「教育情報セキュリティポリシーガイドライン」の第 2 回改訂に関する説明資料 令和 3 年 5 月改訂 https://www.mext.go.jp/content/20210528-mxt_jogai02-000011648_001.pdf〔2022/5/17 確認〕
※ 248 https://www.mext.go.jp/content/20210630-mxt_jogai02-000011648_052.pdf〔2022/5/17 確認〕
※ 249 ローカルブレイクアウト：WAN のトラフィック負荷軽減のために各拠点のルータなどが特定クラウドサービスについて拠点間の回線網を迂回して直接インターネットへアクセスさせる仕組み。
※ 250 デジタル庁：「デジタル社会の実現に向けた重点計画」が閣議決定されました 公開日：2021 年 12 月 24 日 https://www.digital.go.jp/posts/79b7ZMv1〔2022/5/17 確認〕
※ 251 文部科学省：教育情報セキュリティポリシーに関するガイドライン（令和 4 年 3 月） https://www.mext.go.jp/content/20220304-mxt_shuukyo01-100003157_1.pdf〔2022/5/17 確認〕
※ 252 https://www.mext.go.jp/content/20220303-mxt_shuukyo01-100003157_003.pdf〔2022/5/17 確認〕
※ 253 リスクベース認証：システムへの接続において場所や時間等が通常と異なる場合等に ID・パスワードだけでなく追加の認証を行う方式。
※ 254 ふるまい検知：通信内容等の監視対象の「動き」を分析し、異常、あるいは不審な挙動を検知する仕組み。
※ 255 https://www.soumu.go.jp/main_content/000762715.pdf〔2022/5/17 確認〕
※ 256 総務省：地方自治情報管理概要～電子自治体の推進状況（令和元年度）～ https://www.soumu.go.jp/main_content/000768078.pdf〔2022/5/17 確認〕
※ 257 IPA:「2021 年度情報セキュリティに対する意識調査【倫理編】【脅威編】」報告書 https://www.ipa.go.jp/security/economics/ishikichousa2021.html〔2022/5/17 確認〕
※ 258 2020 年度調査まではスマートデバイス（タブレット及びスマートフォン）利用者を対象としていたが、2021 年度調査からスマートフォン利用者のみを対象にした。
※ 259 対策を「1 年以上前から実施している」「1 年以内に実施し始めた」の総和。
※ 260 IPA：2021 年度 情報セキュリティの倫理と脅威に対する意識調査 -【脅威編】- https://www.ipa.go.jp/files/000096683.pdf〔2022/5/17 確認〕
※ 261 事前調査において、プライベートにおけるパソコン、スマートフォンの利用状況を尋ね、インターネットでパソコンを使用していないと回答した者。
※ 262 事前調査において、プライベートにおいてパソコン、スマートフォンの両方を使用している場合、それぞれの機器の 1 日の利用時間を尋ね、利用時間が長い方の機器で回答者を分類した。
※ 263 「情報セキュリティに対する意識調査」では職業従事者の区分で

ある「会社員」「公務員・団体職員」「教職員」「契約・派遣社員」「自営業・自由業・フリーランス」について、同じ区分であっても職務の分野によって結果に差が出ると想定し、「情報システムや通信関係などIT関連業務に従事、関与」している人としていない人とを分類して集計している。
※264 総務省：オンライン消費の増加　https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r03/html/nd121310.html〔2022/5/17確認〕
※265 総務省統計局：新型コロナウイルス感染症で変わるネットショッピング―家計消費状況調査の結果から―　https://www.stat.go.jp/info/today/162.html〔2022/5/17確認〕
※266 独立行政法人国民生活センター：2020年度にみる60歳以上の消費者トラブル―コロナ禍で、通信販売の相談件数は過去最高に―　https://www.kokusen.go.jp/news/data/n-20210902_1.html〔2022/5/17確認〕
※267 独立行政法人国民生活センター：「解約したはず!」「契約してない!」と思い込んでいませんか?予期せぬ“サブスク”の請求トラブルに注意!　https://www.kokusen.go.jp/pdf/n-20211007_1.pdf〔2022/5/17確認〕
※268 https://www.caa.go.jp/policies/policy/consumer_transaction/specified_commercial_transactions/assets/consumer_transaction_cms202_220209_07.pdf〔2022/5/17確認〕
※269 独立行政法人国民生活センター：【若者向け注意喚起シリーズ<No.3>】健康食品等の「定期購入」のトラブル―「お試し」「1回限り」のつもりが定期購入に!?―　https://www.kokusen.go.jp/news/data/n-20210617_1.html〔2022/5/17確認〕
※270 独立行政法人国民生活センター：【若者向け注意喚起シリーズ<No.3>】健康食品等の「定期購入」のトラブル-「お試し」「1回限り」のつもりが定期購入に!?-　https://www.kokusen.go.jp/pdf/n-20210617_1.pdf〔2022/5/17確認〕
※271 内閣府：ネット通販でトラブル急増!「お試し」のつもりが定期購入に!?　https://www.gov-online.go.jp/useful/article/202012/2.html〔2022/5/17確認〕
※272 https://www.pref.kyoto.jp/net_tv/cm/219.html〔2022/5/17確認〕
※273 内閣府：新たな手口のヤミ金融に注意!「#個人間融資」「給与ファクタリング」　https://www.gov-online.go.jp/useful/article/202103/4.html〔2022/5/17確認〕
※274 金融庁：SNS等を利用した「個人間融資」にご注意ください!　https://www.fsa.go.jp/ordinary/chuui/kinyu_chuui.html〔2022/5/17確認〕
※275 神奈川県：ヤミ金融にご注意を（ヤミ金融情報のページ）　https://www.pref.kanagawa.jp/docs/m6c/cnt/f646/p7876.html〔2022/5/17確認〕
※276 https://www.mext.go.jp/content/20211125-mxt_shuukyo01-000009827_001.pdf〔2022/5/17確認〕
※277 https://www.trendmicro.com/ja_jp/about/press-release/2021/pr-20210729-01.html〔2022/5/17確認〕
※278 https://www.mext.go.jp/content/20210312-mxt_jogai01-000011649_002.pdf〔2022/5/17確認〕
※279 https://www.mext.go.jp/studxstyle/〔2022/5/17確認〕
※280 https://www.ipa.go.jp/files/000088916.pdf〔2022/5/17確認〕
※281 https://twitter.com/moj_jinken/status/1465938718393573378〔2022/5/17確認〕
※282 石川県：「Stop! コロナ差別!」～ネット上の誹謗中傷は許されません～　https://www.pref.ishikawa.lg.jp/soumu/jinken/corona_jinken_monitor.html〔2022/5/17確認〕
※283 和歌山県：新型コロナ誹謗中傷対策条例を施行しました　https://www.pref.wakayama.lg.jp/prefg/021400/d00206062_d/fil/leaflet.pdf〔2022/5/17確認〕
※284 防衛省・自衛隊（Twitterアカウント）：https://twitter.com/modjapan_jp/status/1402589334386008069〔2022/5/17確認〕
※285 独立行政法人国民生活センター：「新型コロナ関連詐欺　消費者ホットライン」をご利用ください　https://www.kokusen.go.jp/info/data/coronavirus_vshotline.html〔2022/5/17確認〕
※286 厚生労働省:新型コロナウイルス感染症に関して厚生労働省を装った詐欺にご注意ください。　https://www.mhlw.go.jp/stf/seisakunitsuite/newpage_00004.html〔2022/5/17確認〕
※287 時事ドットコムニュース：SNS「1500人のぞいた」　不正アクセス容疑で男逮捕―愛知県警　https://www.jiji.com/jc/article?k=2022010601107&g=soc〔2022/5/17確認〕
※288 https://blog.twitter.com/ja_jp/topics/company/2021/playbook-for-safety〔2022/5/17確認〕
※289 Meta Platforms, Inc.：Instagramの安全とセキュリティを確保する　https://about.instagram.com/ja-jp/blog/announcements/keeping-instagram-safe-and-secure〔2022/5/17確認〕
※290 Meta Platforms, Inc.：Instagramコミュニティを不適切なコンテンツから守るための新たな方法　https://about.instagram.com/ja-jp/blog/announcements/introducing-new-ways-to-protect-our-community-from-abuse〔2022/5/17確認〕
※291 Meta Platforms, Inc.:若い利用者のために、安全性とプライバシーを強化したエクスペリエンスを提供　https://about.instagram.com/ja-jp/blog/announcements/giving-young-people-a-safer-more-private-experience〔2022/5/17確認〕
※292 Google LLC：日本版YouTube公式ブログ　https://youtube-jp.googleblog.com/2021/11/youtube.html〔2022/5/17確認〕
※293 ヤフー株式会社：Yahoo! ニュース、コメント欄をより健全化するためユーザーからの違反コメント報告を促進　https://about.yahoo.co.jp/pr/release/2021/12/22b/〔2022/5/17確認〕
※294 独立行政法人国民生活センター：狙われる!? 18歳・19歳「金」と「美」の消費者トラブルに気をつけて!　https://www.kokusen.go.jp/pdf/n-20210408_1.pdf〔2022/5/17確認〕
※295 https://www.caa.go.jp/policies/policy/consumer_education/consumer_education/lower_the_age_of_adulthood/〔2022/5/17確認〕
※296 https://www.soumu.go.jp/use_the_internet_wisely/trouble/reference/reference02.html〔2022/5/17確認〕
※297 https://seinen.go.jp/〔2022/5/17確認〕
※298 https://smart18.info/files/smart18ebook.pdf〔2022/5/17確認〕
※299 MATAGI SNIPERS：https://matagi-snps.com/〔2022/5/17確認〕
※300 funglr Games：社会人eスポーツリーグ「AFTER 6 LEAGUE」を経済産業省が後援決定　https://funglr.games/ja/news/a6l-meti-support/〔2022/5/17確認〕
※301 京都新聞：チート行為で男女5人書類送検　京都府警、ゲーム内のアイテム不正入手疑い　https://www.kyoto-np.co.jp/articles/-/713337〔2022/5/17確認〕
※302 福井県：「チート行為」はやめましょう!～損害賠償請求や違法行為として処罰される可能性も～　http://www.fukui-city.ed.jp/na-fuji-e/moraru/R2%20mararu20.pdf〔2022/5/17確認〕
※303 株式会社ラック：東京ゲームショウ2021 オンラインに出展!チート対策ホワイトペーパーも公開　https://www.lac.co.jp/lacwatch/service/20210910_002704.html〔2022/5/17確認〕
※304 https://www.nisc.go.jp/pdf/policy/kihon-s/set_20220318_cswebinarboshu_r10.pdf〔2022/5/17確認〕
※305 NISC：国際サイバーセキュリティワークショップ・演習の開催　https://www.nisc.go.jp/eng/pdf/international_ws_ttx_2022_jp.pdf〔2022/5/17確認〕
※306 https://www.gov-online.go.jp/pr/media/tv/kasumigaseki/movie/20220218.html〔2022/5/17確認〕
※307 https://dawn2021.orylab.com〔2022/5/17確認〕
※308 知的財産戦略本部：知的財産推進計画2021　https://www.kantei.go.jp/jp/singi/titeki2/kettei/chizaikeikaku20210713.pdf〔2022/5/19確認〕
※309 ISO：ISO/IEC JTC 1　https://www.iso.org/committee/45020.html〔2022/5/19確認〕
※310 JISC：JISCについて　http://www.jisc.go.jp/jisc/index.html〔2022/5/19確認〕
※311 ITU：SG17: Security　https://www.itu.int/en/ITU-T/studygroups/2017-2020/17/Pages/default.aspx〔2022/5/19確認〕
※312 IETF：The IETF Security Area　https://trac.ietf.org/trac/sec/wiki〔2022/5/19確認〕
※313 TCG：Welcome to Trusted Computing Group　https://trustedcomputinggroup.org/work-groups/regional-forums/japan〔2022/5/19確認〕
※314 https://www.jisc.go.jp/international/iso-prcs.html〔2022/5/19確認〕
※315 ガーブル回路：暗号学においてスクランブルされた回路を意味し、2者間の秘密計算を可能とする暗号プロトコル。
※316 TS（Technical Specification：技術仕様書）：現時点では技術的に未成熟等の理由により、国際標準として発行するのは妥当ではない文書。
※317 EUCC（European Union Cybersecurity Certification）：欧州で創立が進められている、ISO/IEC 15408に基づくIT製品のセキュリティ評価・認証制度。
※318 ENISA：CYBERSECURITY CERTIFICATION　https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme-v1-1.1〔2022/5/25確認〕
※319 IoT推進コンソーシアム・総務省・経済産業省：IoTセキュリティ

ガイドライン Ver1.0　http://www.soumu.go.jp/main_content/000428393.pdf〔2022/5/24 確認〕
※ 320 https://www.iso.org/standard/80136.html〔2022/5/24 確認〕
※ 321 https://www.iso.org/standard/78572.html〔2022/5/24 確認〕
※ 322 経済産業省：サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）を策定しました　https://www.meti.go.jp/press/2019/04/20190418002/20190418002.html〔2022/5/24 確認〕
※ 323 https://www.meti.go.jp/policy/netsecurity/cclistmetisec2018.pdf〔2022/5/17 確認〕
※ 324 https://www.commoncriteriaportal.org/〔2022/5/17 確認〕
※ 325 IPA：認証プロテクションプロファイルリスト　https://www.ipa.go.jp/security/jisec/certified_pps/pp_list.html〔2022/5/17 確認〕
※ 326 プロテクションプロファイルに対しての認証：プロテクションプロファイルがコモンクライテリア形式を満たしていることの認証。
※ 327 https://csrc.nist.gov/projects/cryptographic-module-validation-program〔2022/5/30 確認〕
※ 328 https://cio.go.jp/sites/default/files/uploads/documents/hyoujun_guideline_honninkakunin_20190225.pdf〔2022/5/17 確認〕
※ 329 IPA・JISEC：「ハードコピーデバイスのプロテクションプロファイル」適合の申請案件についてのガイドライン 第 1.8 版　https://www.ipa.go.jp/security/jisec/mfp/guidelineforHCD-PP_1.8.pdf〔2022/5/17 確認〕
※ 330 https://www.ipa.go.jp/security/jisec/certified_pps/c0553/c0553_pp.pdf〔2022/5/17 確認〕
※ 331 IPA・JISEC：認証製品リスト　https://www.ipa.go.jp/security/jisec/certified_products/cert_listv31.html〔2022/5/17 確認〕
※ 332 JCMVP の「トピックス」ページ（https://www.ipa.go.jp/security/jcmvp/topics.html〔2022/5/17 確認〕）の「本制度に関連する日本産業規格 (JIS)」参照。
※ 333 JCMVP の「トピックス」ページ（https://www.ipa.go.jp/security/jcmvp/topics.html〔2022/5/17 確認〕）の「本制度に関連する ISO/IEC 規格」参照。
※ 334 JISC：意見受付公告（JIS）　https://www.jisc.go.jp/app/jis/general/GnrOpinionReceptionNoticeList?show〔2022/5/17 確認〕
※ 335 JISC：JIS の制定等のプロセスについて　https://www.jisc.go.jp/jis-act/cap_process.html〔2022/5/17 確認〕
※ 336 「FIPS 140」は暗号モジュールに関するセキュリティ要件を規定する連邦情報処理規格。「-2」は第 2 版、「-3」は第 3 版であることを示す。
※ 337 Historical List：認証の有効期間が満了した製品であることを示すリスト。
※ 338 経済産業省：「政府情報システムのためのセキュリティ評価制度（ISMAP）」の運用を開始しました　https://www.meti.go.jp/press/2020/06/20200603001/20200603001.html〔2022/5/17 確認〕
※ 339 サイバーセキュリティ対策推進会議・各府省情報化統括責任者（CIO）連絡会議：政府情報システムのためのセキュリティ評価制度（ISMAP）の暫定措置の見直しについて　https://www.nisc.go.jp/pdf/policy/general/ismap_minaoshi.pdf〔2022/5/17 確認〕
※ 340 https://cio.go.jp/sites/default/files/uploads/documents/cloud_policy_20210330.pdf〔2022/5/17 確認〕
※ 341 総務省・経済産業省：クラウドサービスの安全性評価に関する検討会について　https://www.meti.go.jp/shingikai/mono_info_service/cloud_services/pdf/001_02_00.pdf〔2022/5/17 確認〕
※ 342 https://www.meti.go.jp/press/2019/01/20200130002/20200130002-1.pdf〔2022/5/17 確認〕
※ 343 https://www.nisc.go.jp/pdf/policy/general/wakugumi2021.pdf〔2022/5/17 確認〕
※ 344 NISC：「政府機関等のサイバーセキュリティ対策のための統一基準群」　https://www.nisc.go.jp/policy/group/general/kijun.html〔2022/5/17 確認〕
※ 345 https://www.ismap.go.jp/csm?id=kb_article_view&sysparm_article=KB0010005〔2022/5/17 確認〕
※ 346 https://www.ismap.go.jp〔2022/5/17 確認〕
※ 347 https://www.nisc.go.jp/pdf/policy/infra/shishin5.pdf〔2022/5/17 確認〕
※ 348 e-Gov 法令検索：個人情報の保護に関する法律　https://elaws.e-gov.go.jp/document?lawid=415AC0000000057〔2022/5/17 確認〕
※ 349 https://www.ppc.go.jp/files/pdf/151112_kaiseian.pdf〔2022/5/17 確認〕
※ 350 個人情報保護委員会：令和2年 改正個人情報保護法について　https://www.ppc.go.jp/personalinfo/legal/kaiseihogohou/〔2022/5/17 確認〕
※ 351 デジタル庁：デジタル社会の形成を図るための関係法律の整備に関する法律　https://cio.go.jp/sites/default/files/uploads/documents/digital/20210901_laws_r3_37_article.pdf〔2022/5/17 確認〕
※ 352 個人情報保護委員会：令和3年 改正個人情報保護法について（官民を通じた個人情報保護制度の見直し）　https://www.ppc.go.jp/personalinfo/minaoshi/〔2022/5/17 確認〕
※ 353 https://www.ipa.go.jp/files/000087025.pdf〔2022/5/17 確認〕
※ 354 https://www.ppc.go.jp/files/pdf/seibihou_gaiyou.pdf〔2022/5/17 確認〕
※ 355 内閣府：個人情報保護法制 2000 個問題について　https://www8.cao.go.jp/kisei-kaikaku/suishin/meeting/wg/toushi/20161115/161115toushi01.pdf〔2022/5/17 確認〕
※ 356 IPA：「企業における営業秘密管理に関する実態調査 2020」報告書について　https://www.ipa.go.jp/security/fy2020/reports/ts_kanri/index.html〔2022/5/17 確認〕
※ 357 IPA：組織における内部不正防止ガイドライン　https://www.ipa.go.jp/security/fy24/reports/insider/〔2022/5/17 確認〕
※ 358 https://www.ipa.go.jp/files/000097371.pdf〔2022/5/17 確認〕
※ 359 https://security-portal.nisc.go.jp/law_handbook/law_handbook.pdf〔2022/5/17 確認〕
※ 360 AES（Advanced Encryption Standard）：米国で NIST により標準化された共通鍵暗号。
※ 361 ChaCha:Daniel J. Bernstein によって開発されたストリーム暗号。Chacha20 は ChaCha を基にした暗号であり、これとメッセージ認証子である Poly1305 とを組み合わせた ChaCha20-Poly1305 は、CRYPTREC の推奨候補暗号リストとなっている。
※ 362 RSA：素因数分解問題が困難であることを安全性の根拠とした公開鍵暗号。
※ 363 CRT-RSA 指数：RSA 暗号の復号時の計算量を下げる際に用いられる、秘密鍵に付随する付加情報。
※ 364 NIST：Third PQC Standardization Conference　https://csrc.nist.gov/Events/2021/third-pqc-standardization-conference〔2022/4/21 確認〕
※ 365 Anirban Chakraborty, Sarani Bhattacharya, Manaar Alam, SikharPatranabis and Debdeep Mukhopadhyay：RASSLE: Return Address Stack based Side-channel LEakage　https://tches.iacr.org/index.php/TCHES/article/view/8795〔2022/4/21 確認〕
※ 366 分岐予測：CPU において、条件分岐命令で分岐するかしないかを予測することによって、パイプライン処理の乱れを極力避けて処理速度の低下を抑えるための機構。
※ 367 投機的実行：CPU において命令を、必要な処理であることが確定する前にパイプラインに投入して実行を始める処理。パイプラインの乱れを極力避けることを目的とする。分岐予測が外れて必要でない処理であることが確定すると、その実行結果は破棄され、正しい分岐先の命令を改めて実行する。
※ 368 Spectre-v1 については、以下を参照。
CVE:CVE-2017-5753 Detail　https://cve.org/CVERecord?id=CVE-2017-5753〔2022/4/21 確認〕
Spectre-v2 については、以下を参照。
CVE:CVE-2017-5715 Detail　https://cve.org/CVERecord?id=CVE-2017-5715〔2022/4/21 確認〕
※ 369 タイミング攻撃：サイドチャネル情報のうち、処理時間の差異を利用する攻撃。
※ 370 ECDSA（Elliptic Curve Digital Signature Algorithm）：楕円曲線暗号を用いたデジタル署名アルゴリズム。
※ 371 テンプレート攻撃：暗号実装に対し、異なる入力値に対するサイドチャネル情報（消費電力、電磁場など）をあらかじめ測定しておき、それをテンプレートとして利用して実際の暗号鍵復元のための攻撃を行う手法。
※ 372 Alejandro Cabrera Aldaya and Billy Bob Brumley：Online Template Attacks: Revisited　https://tches.iacr.org/index.php/TCHES/article/view/8967〔2022/4/21 確認〕

第3章
個別テーマ

本章では個別テーマとして、制御システム、IoT、クラウドのセキュリティについて、報告されたインシデントや攻撃の実態、脆弱性や脅威の動向、国の施策や対策状況等を解説する。2年ぶりに取り挙げるクラウドのセキュリティについては、近年利用が急増しているSaaSに焦点を絞り、解説する。

また、2021年後半以降のウクライナ危機は、武力と情報が組み合わさった新たな脅威を生み出しており、米国や欧州がこの状況にどう対応しているか、関連するセキュリティ政策や政府・民間組織の動向について紹介する。

3.1 制御システムの情報セキュリティ

制御システム（ICS：Industrial Control System）は、電力、ガス、水道、輸送・物流、製造ライン等、我々の生活を支える重要インフラ※1を管理し、制御するシステムである。従来、制御システムの多くは独立したネットワーク、固有のプロトコル、事業者ごとに異なる仕様で構築・運用されており、外部からサイバー攻撃を行うことは困難と考えられていた。しかし、近年、外部ネットワークとの接続、標準プロトコルや汎用製品の利用が進んだこと、10～20年に及ぶライフサイクルの長さ故に、外部との接続やサイバー攻撃を想定していないシステムが今も多数稼働していること、また、攻撃者にとって価値の高い標的であることから、制御システムに対するサイバー脅威が高まっている。実際に、社会経済活動に大規模な被害が出たインシデントも発生している。

本節では、制御システムのセキュリティの動向と主な取り組みについて述べる。

3.1.1 インシデントの発生状況と動向

調査会社による制御システムユーザ等へのアンケート調査において、2020年同様、2021年も制御システムへの侵入や運用障害が発生したという回答が一定数以上あった。

例えば、米国、ドイツ、日本の製造業のIT及び制御・運用技術（OT：Operational Technology）の専門家500名を対象とした調査結果では、61.2%がサイバーセキュリティインシデントを経験した、と回答している。インシデントの74.5%でシステムの停止が発生しており、そのうち43.4%が4日以上の停止の被害に至った、と回答している※2。英国の航空、化学、エネルギー、輸送、水道分野等の重要国家インフラ（CNI：Critical National Infrastructure）組織のIT意思決定者250名を対象とした調査結果では、86%が過去12ヵ月間にOTと制御システムに対するサイバー攻撃を経験しており、そのうち93%が少なくとも1度は攻撃が成功していた、と回答している※3。

2021年に公になったインシデントには、水道やパイプライン等の重要インフラを標的とした攻撃、サイバー攻撃による生産や重要サービスの停止、メディア企業への攻撃による放送や新聞発行の停止、公共交通機関を標的とした攻撃、医療機関への攻撃、USBメモリやパソコンを接続することによるウイルス※4感染、という六つの特徴が見られた。

(1) 水道やパイプライン等の重要インフラが標的となった事例

米国の上下水道施設ではインシデントが相次いだ。2021年1月15日、カリフォルニア州サンフランシスコの浄水場で攻撃者がリモートアクセスソフトウェアTeamViewerのアカウントでログインし、飲料水の処理に使用していたプログラムを削除した。浄水場は翌日ハッキングを発見し、パスワードの変更及びプログラムの再インストールを実施した。飲料水への影響はなかった※5。2021年2月5日には、フロリダ州オールズマーの浄水場が、同じくTeamViewerを介してSCADA（Supervisory Control And Data Acquisition：監視制御及びデータ収集）システムにアクセスされ、水酸化ナトリウムの投入設定値を変更されたが、監視していたオペレータが気付

き、すぐに正常な値に戻した※6。翌3月、ネバダ州の上下水道施設がランサムウェアによる攻撃を受け、SCADAシステム及びバックアップシステムが影響を受けた。また同年7月には、メーン州の上下水道施設の廃水処理のSCADAコンピュータが、リモートアクセス経由でランサムウェアによる攻撃を受けた。復旧するまで、廃水処理システムは手動で実行された。更に8月には、カリフォルニア州にある上下水道施設がランサムウェア「Ghost」の亜種による攻撃を受けた。このランサムウェアは約1ヵ月前からシステムに潜伏していた※7。

2021年5月7日、米国最大手のパイプライン企業Colonial Pipeline Companyがランサムウェアによるサイバー攻撃を受けた。ITシステムのコンピュータのファイルが暗号化され、パイプラインの制御システムは直接の影響を受けなかったが、あらかじめ決められていた全社的なインシデント対応プロセスに則って、予防保全的に停止した。同社のパイプラインは米国東海岸で消費される燃料の約45%を扱っており、6日間続いたパイプラインの停止により、例えば首都ワシントンのガソリンスタンドのうち約81%でガソリンが売り切れ状態となる等、市民生活に大きな影響を与えた※8（「3.4.1（1）（b）Colonial Pipeline事案とその対応」参照）。

(2) サイバー攻撃によって生産や重要サービスが停止した事例

制御システムにおいて最も重要視される「可用性（Availability）」に影響を与えたインシデントも世界中で相次いだ。ITとOTの統合が進んでいることから、メールやWebサイト経由のITシステムのウイルス感染が制御システムまで拡大する例や、ITシステムの感染から間接的に制御システムが影響を受け、生産ラインや重要サービスが停止する事例が増えている。

表3-1-1に、2021年に公にされた、サイバー攻撃によって生産や重要サービスが停止したインシデント事例を示す。

また、2022年2月26日には、自動車大手トヨタ自動車株式会社の取引先部品メーカ小島プレス工業株式会社が、ランサムウェアによる攻撃を受けた。トヨタ自動車への攻撃は確認されていないが、同社は3月1日に国内の14の工場で生産を停止した。約1万3,000台の生産に打撃を与えたが、3月2日に生産を再開した※9。

「制御システムはITシステムの影響を受けない」という認識を持たず、「攻撃や感染がITからOTへ広がることはないか」等、従来の認識によるIT、OT個別の縦割りのリスク管理体制を越えた横断的なリスクの見直しが推奨される。

事例名	発生国	発生年月（報道年月）	影響・被害	内容（原因等）
大手クレーンメーカの工場の稼働停止※10	オーストラリア	2021年1月	ヨーロッパ、北米、南米、アジアにある30以上の工場と組立拠点の稼働停止	ランサムウェアによる攻撃を受け、ITインフラが影響を受けた。
IoT機器メーカの生産停止※11	カナダ	2021年3月	工場での生産停止	ITシステムがランサムウェアによる攻撃を受けた。
食品加工大手の生産停止※12	北米及びオーストラリア	2021年5月	複数の拠点で生産停止	ランサムウェアによる攻撃を受け、北米及びオーストラリアのITシステムを支えるサーバが影響を受け、システムが停止した。
通信事業者のサービス停止及び障害※13	英国	2021年9月	インターネット接続サービスが断続的または完全に停止、音声通話、発着信、SMSサービスに障害が発生	通信事業者2社が、ランサムウェア攻撃グループによる大規模なDDoS攻撃を受けた。
大手インターネットサービスプロバイダのサービス停止※14	ニュージーランド	2021年9月	サービスが30分間停止	DDoS攻撃を受け、DDoS攻撃緩和ルールをアップデートして攻撃をブロックしたが、これが原因でサービスが停止した。
菓子メーカの生産停止※15	米国	2021年10月	工場での生産停止	ランサムウェアによる攻撃を受け、システムが暗号化された。
食品大手の工場及び配送センターの稼働停止※16	米国	2021年10月	工場及び配送センターの稼働停止	ランサムウェアによる攻撃を受け、工場や配送センターの稼働に必要なシステムが使用できなくなった。

■表3-1-1　2021年に公にされた、サイバー攻撃によって生産や重要サービスが停止したインシデント事例

(3) メディア企業への攻撃によって放送や新聞発行が停止した事例

多くの人々に日々多様な情報を伝えるメディアを標的としたサイバー攻撃の事例も多く見られた。

2021 年 3 月 28 日、オーストラリアの放送局 9News がサイバー攻撃を受け、多くの生放送の番組が中断した。同局のニュース制作システムは 24 時間以上にわたってダウンした。同局はインシデントの封じ込め措置として、特定のネットワークをインターネットから切り離したが、一部のネットワークが使えない状況が続いた※17。

2021 年 6 月 3 日、米国のメディア複合企業 Cox Media Group がランサムウェアによる攻撃を受け、テレビとラジオのライブストリーム放送が停止した※18。

2021 年 10 月 16 日、米国のメディア企業 Sinclair Broadcast Group, Inc. がランサムウェアによる攻撃を受け、全米の複数の TV 局が放送を停止した。同社は、セキュリティインシデントを検知した後、調査及び封じ込めの措置を開始したが、翌 10 月 17 日に、一部のサーバ及びワークステーションがランサムウェアによって暗号化され、一部の運用ネットワークが切断され放送が停止していること、及びデータが窃取されたことを確認した※19。

2021 年 12 月、ノルウェーのメディア大手 Amedia AS がサイバー攻撃を受け、コンピュータシステムが停止し、新聞の印刷ができなくなった。また、広告システムや購読システムも影響を受け、広告主の新規広告発注や購読者の登録・解約ができなくなった※20。

(4) 公共交通機関が標的となった事例

日々の移動手段として多くの人々が利用している公共交通機関もサイバー攻撃の標的となった。

2021 年 4 月、米カリフォルニア州サンタクララ郡の公共交通局（VTA：Santa Clara Valley Transportation Authority）が、ランサムウェアによるものと思われる攻撃を受け、コンピュータシステムの多くが数日間オフラインとなった。「Astro」と名乗るハッキンググループが、VTA から 150G バイトのデータを窃取し、身代金の支払い要求に応じなければデータを公開する、と脅迫した後、4 月 22 日に窃取したデータをダーク Web に投稿した。運行情報のリアルタイム提供や職員の電子メール機能等に影響が出たが、VTA が運行しているバス、ライトレール等の交通機関の運行には影響はなかった※21。

2021 年 7 月 9 日、イランの国有鉄道（イラン・イスラム共和国鉄道）においてサイバー攻撃によるものと思われるコンピュータシステム及び列車の電子トラッキングシステムの障害が発生し、数百本の列車が遅延またはキャンセルとなり、前例のない混乱が生じた※22。

2021 年 10 月 28 日、カナダ・オンタリオ州トロントのトロント交通局（TTC：Toronto Transit Commission）がランサムウェアによる攻撃を受けた。駅のスクリーンに表示される車両情報システム、オンライン予約サイト、旅行計画アプリケーション、TTC 内部の電子メールサービス等が停止した。また、車両運転者との通信に使用されるシステムが停止し、無線によるバックアップでコミュニケーションを図った。交通サービスには影響はなかった※23。

(5) 医療機関が標的となった事例

医療機関を標的としたサイバー攻撃も、世界中で相次いだ。米国の 597 の医療機関を対象に実施した調査レポートによると、過去 2 年間で回答者の 43% がランサムウェアによる攻撃を経験しており、そのうち 67% が 1 回、33% が 2 回以上の攻撃を経験した、と回答している。ランサムウェアによる攻撃が患者の治療に大きな影響を与えており、入院期間の長期化（回答者の 71%）、処置や検査の遅延（70%）、患者の転院や施設の転用の増加（65%）、医療処置による合併症の増加（36%）や死亡率の増加（22%）等が報告されている※24。

表 3-1-2（次ページ）に、2021 年に公にされた、医療機関及び医療関連施設を標的としたインシデント事例を示す。

医療機関のコンピュータがランサムウェアに感染すると、保有されている情報資産（データ等）が暗号化され、電子カルテシステムが利用できなくなって診療に支障が生じたり、患者の個人情報が窃取されたりする等の甚大な被害をもたらす可能性がある。国内では、厚生労働省が、医療機関を標的としたランサムウェアによるサイバー攻撃について、2021 年 6 月 28 日に注意喚起を行っている※33（国内病院のランサムウェア被害については「1.2.2 (2) (a) 国内病院の被害事例」参照）。

(6) USB メモリやパソコンを接続することによるウイルス感染

業務用に持ち込んだ USB メモリやパソコンを接続することによるウイルス感染も、継続して発生している。Honeywell International Inc. のレポート「Industrial Cybersecurity USB Threat Report 2021※34」によると、USB メモリを悪用する脅威は、調査した制御システムへのすべての脅威の 37% を占め、2020 年発表のレポートからほぼ倍増している。また、USB メモリやリムーバブ

被害組織	発生国	発生年月（報道年月）	内容・影響・被害
新型コロナウイルスの研究を行っている大学の研究室※25	英国	2021 年 2 月	標的となったシステムに不正アクセスする手段を販売することを目論む攻撃者による攻撃を受け、新型コロナウイルスの研究に使用されている装置が侵害された。
病院※26	フランス	2021 年 3 月	ランサムウェアによる攻撃を受け、デジタルの患者記録や薬の在庫等を管理するシステムが利用できなくなり、スタッフは紙とペンで対応した。
医療、高齢者ケア、障害者支援等のサービスを提供している医療機関※27	オーストラリア	2021 年 4 月	ランサムウェアによる攻撃を受け、社内スタッフの電子メールや患者の予約等、すべての業務システムが停止。スタッフは紙とペンで対応した。
公的医療サービスを提供する保健サービス委員会（HSE：Health Service Executive）※28	アイルランド	2021 年 5 月	ランサムウェア「Conti」による攻撃を受け、IT システムが停止。アイルランド国内の病院サービスや患者のケアに多大な支障をきたした。1990 年代の古いものを含む 8 万台の機器と 2,000 の患者用 IT システムを完全に復旧する必要があり、完全復旧までに 4 ヵ月かかった。
病院、診療所、介護施設を運営している医療機関※29	米国	2021 年 6 月	ランサムウェアによる攻撃を受け、電話システムに障害が発生したほか、オンラインの患者ポータルとアプリ、及びメールシステムが影響を受け、一部の診察予約がキャンセルされた。また、電子カルテが使用できなくなった。
三つの病院と外来サービス拠点等からなる小規模な総合医療機関※30	米国	2021 年 8 月	ランサムウェア攻撃グループ「Hive」による攻撃を受け、コンピュータのファイルが暗号化され、機密情報を含む患者 20 万人分の情報を窃取された。スタッフは紙のカルテで対応した。また、臨床及び財務業務に支障が生じ、緊急手術や放射線検査がキャンセルされた。
病院※31	イスラエル	2021 年 10 月	ランサムウェアによる攻撃を受け、システムに影響が出たため、代替システムを使用し、患者の情報は手書きで書き留めた。また、治療できない患者は、他の病院に移送された。ランサムウェアによってイスラエルの病院のシステムが麻痺した初めての事例となった。
米国の 17 州で 80 以上の外来診療所を運営している外来オピオイド（麻薬性鎮痛薬）治療企業※32	米国	2021 年 12 月	サイバー攻撃を受け、約 1 週間にわたり IT システムと患者の治療に支障をきたした。自宅で使用するための治療薬をオピオイド依存の治療患者に提供している一部の診療所で、コンピュータが使用できず処方箋ラベルが印字できなくなったため、治療薬が提供できなかった。

■表 3-1-2　2021 年に公にされた、医療機関及び医療関連施設が標的となったインシデント事例

ルメディアを起点とするサイバー脅威の 79% が、OT 環境における重要なビジネスの途絶につながる可能性があるとしている。生産施設における USB メモリの使用は 30% 増加しており、リムーバブルメディアへの依存度は高まっている。

2022 年 1 月には、米国連邦捜査局（FBI：Federal Bureau of Investigation）が、2021 年 8 月からサイバー犯罪グループが、システムをマルウェアに感染させた後に攻撃を実行する目的で、輸送、保険、及び防衛産業に関わる米国企業へ悪意のある USB メモリを送付している、と警告した。送付された USB メモリをパソコンに差し込むと、USB メモリがキーボードとして登録され、あらかじめ設定された一連の自動キーストロークを送信するという「BadUSB 攻撃」を実行する。これらのキー操作で PowerShell コマンドを実行し、攻撃者のバックドアとして機能する様々なウイルスを標的とした企業のネットワーク内の端末にダウンロードし、インストールする。FBI が調査したケースでは、このグループは管理者権限を取得した後、他のローカルシステムに横展開していることが確認されている※35。

制御システム運用者は、外部から持ち込まれる情報端末・機器や媒体の管理、及び接続前のウイルスチェックを今一度徹底することが重要である。また、内部関係者の不正やヒューマンエラーによるリスクを軽減するために、セキュリティ教育や意識啓発を通じて、従業員の情報リテラシーや情報モラルを向上させることも重要である。

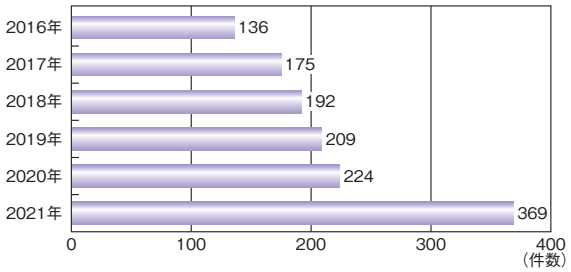
3.1.2 脆弱性及び脅威の動向

本項では、2021 年に見られた、制御システムの脆弱性及び脅威の動向について述べる。

(1) 脆弱性の動向

2021 年も、制御システムの脆弱性が多く公開された。制御システムの脆弱性情報を収集・公開している代表的な組織である米国国土安全保障省（DHS：Department of Homeland Security）の NCCIC（National Cybersecurity and Communications

Integration Center）が、2021 年に公開したアドバイザリは 369 件で、図 3-1-1 に示すように、対前年比 64.7%増と、これまでで最大となった。確認された脆弱性は 1,255 件で、2010 年以降にアドバイザリで確認された共通脆弱性識別子 CVE（Common Vulnerabilities and Exposures）の総数の 28.3% に相当する。アドバイザリで特定された 613 の CVE のうち、重要な製造環境に影響を及ぼす可能性のあるものを分析した結果、その 88.8% は攻撃者が悪用し、直接または間接的に制御システム機器や環境に様々な混乱を引き起こす可能性がある※36。



■図 3-1-1　NCCIC が公開した脆弱性アドバイザリの件数（2016 ～ 2021 年）
（出典）NCCIC の公開情報※37 を基に IPA が作成

非常に影響の大きい脆弱性も複数発見されている。以下では、それらの脆弱性について解説する。

(a) Log4Shell

Apache Software Foundation が開発したオープンソースの Java ベースのロギングライブラリ Apache Log4j に、認証されていないリモートコードの実行（RCE: Remote Code Execution）が可能となる脆弱性（CVE-2021-44228：通称「Log4Shell」※38）が発見された。Log4j は様々なサービス、Web サイト、アプリケーション、OT 製品で、セキュリティやパフォーマンスの情報の記録に広く使用されており、電力、水道、製造、輸送等複数の業界が、この脆弱性を悪用した攻撃に晒される可能性がある※39。更に、サービス拒否（DoS：Denial of Services）攻撃が行われる脆弱性（CVE-2021-45046※40）も発見された※41。DHS のサイバーセキュリティ・インフラストラクチャセキュリティ庁（CISA：Cybersecurity and Infrastructure Security Agency）は、これら 2 件の脆弱性の影響を受ける Web サービスを特定するツールを公開した。また CISA は、連邦政府機関に対し、12 月 23 日までに Log4Shell に対するパッチを適用するよう、12 月 17 日に命じた※42。米連邦取引委員会（FTC：Federal Trade Commission）は、Log4j の脆弱性を是正するための措置を講じない場合、法的な影響を受ける可能性がある、と米国企業に警告した。「脆弱性が悪用された場合、個人情報の喪失や漏えい、金銭的損失、その他取り返しのつかない損害を被る危険性があるため、今すぐ行動することが重要」と警告し、「今後、同様の既知の脆弱性が発生した場合、消費者を保護するために法的権限を適用する予定」としている。CISA は、2022 年 1 月 4 日に「すべての大規模機関から状況報告を受け、パッチを適用したか、リスクに対処するための代替緩和策を展開した」と公表したが、大規模ではない連邦政府機関が期限に間に合ったかどうかについては明らかにしていない※43。

(b) NAME:WRECK

米国のサイバーセキュリティ企業 Forescout Technologies,Inc.（以下、Forescout 社）とイスラエルのセキュリティ企業 JSOF Ltd. は、およそ 1 億台ものサーバや IoT 機器に影響を与える可能性のある九つの脆弱性「NAME:WRECK」を発見した※44。脆弱性は、オープンソースの OS である FreeBSD、Nucleus NET、IPnet、NetX の TCP/IP スタックで発見され、DNS の実装に関連しており、DoS またはリモートコード実行を引き起こす。攻撃者が悪用すると、標的とした機器をオフラインにしたり、コントロールしたりできる。ビルオートメーション、ファイアウォール、ネットワーク機器から、制御システムや超音波診断装置の機器まで、様々な機器が狙われる可能性がある（「1.2.5 (3) (a) 多数の IoT 製品に影響する脆弱性」「3.2.2 (1) (b) NAME：WRECK」参照）。

(c) BadAlloc

Microsoft Corporation（以下、Microsoft 社）は、「BadAlloc」と名付けられたメモリ割り当ての脆弱性 25 件を発見した。詳細は「3.2.2 (1) (d) BadAlloc」を参照されたい。

(d) INFRA:HALT

Forescout 社 と JFrog Ltd. は、InterNiche Technologies, Inc. 製の組み込みシステム用 TCP/IP スタック「NicheStack」（現在は Tuxera Hungary Kft. の一部門 HCC-Embedded が保守担当）に影響を与える 14 件の脆弱性「INFRA:HALT」を発見した※45。「NicheStack」は、製造工場、発電・送電・配電システム、水処理装置等の重要インフラ分野で採用されている。

詳細は「3.2.2(1)(g)INFRA:HALT」を参照されたい。

(e) NUCLEUS:13

Siemens AG は、医療機器、産業用機器、自動車機器、航空宇宙機器等に搭載されている Nucleus リアルタイム OS の 13 件の脆弱性「NUCLEUS:13」を発表した。詳細は「3.2.2(1)(i)NUCLEUS:13」を参照されたい。

(f) スマートメーター製品の脆弱性

産業用サイバーセキュリティ企業 Claroty Ltd. は、Schneider Electric SE のスマートメーター製品 PowerLogic の二つの深刻な脆弱性を発見した。同製品は、電力会社、製造業、医療機関、電力ネットワークを監視するデータセンターで使用されている電子式電力量計である。脆弱性にはそれぞれ異なる CVE が割り当てられた。CVE-2021-22714 は、攻撃者が標的のメーターを再起動させ、場合により任意のコードを実行できる。また、もう一つの CVE-2021-22713 は、デバイスを強制的に再起動する目的でのみ悪用でき、高い深刻度が割り当てられた※46。

(g) ユニバーサルリレー機器の脆弱性

CISA は、General Electric Company のユニバーサルリレー機器の深刻な脆弱性に関するセキュリティアドバイザリを発表した※47。同社のユニバーサルリレー機器のファミリー製品は、エネルギー、製造、医療、輸送等の世界中の重要インフラで、電源管理に使用されている。悪用すると、機密情報へのアクセス、機器の再起動、特権アクセスの取得、またはサービス拒否状態の発生を引き起こす可能性がある※48。

(h) 制御システム専用バックアップソリューションの脆弱性

Claroty Ltd. は、Rockwell Automation, Inc. の制御システム専用バックアップソリューション FactoryTalk AssetCentre の 9 件の脆弱性を発見した。同製品は、産業施設全体のオートメーション関連の資産情報を保護、管理、バージョン管理、トラッキング、レポートするための一元化ツールである。発見された脆弱性は、リモートで任意のコードを実行できる脆弱性、SQL インジェクションの脆弱性、及び OS コマンドインジェクションの脆弱性で、これらの脆弱性を悪用すると、OT ネットワークの PLC 等の自動化機器上でコマンドを実行できる※49。CISA はアドバイザリを発表した※50。

脆弱性が公表された機器の所有者は、脆弱性の影響及び対応の可否を確認し、速やかに必要な対策を実施することが推奨される。

(2) 脅威の動向

2021 年の脅威の動向としては、2020 年に引き続き、ランサムウェアによる攻撃の増加が挙げられる。産業界へのランサムウェア攻撃は、2018 年から 2020 年の間に 6 倍に増加しており、2021 年 1 月から 5 月の間では、更に 2.16 倍に増加している※51。米国、欧州、アジア太平洋地域の IT 及び OT セキュリティの専門家 1,100 人を対象とした調査では、回答者の約 80% が、過去 1 年以内に自分の組織がランサムウェア攻撃を受けたことを認め、そのうち約半数が制御システム／ OT 環境に影響を与えたと回答している。また、7% が 1 週間以上続く完全なオペレーション停止に至ったと回答している※52。

ランサムウェアの脅威への対策として、基本的なウイルス対策、通信制御による対策、重要なデータのバックアップが適切に実施されているかの確認等の感染や脅迫に備えたリスク管理対策を徹底することが推奨される（1.2.2(5)ランサムウェア攻撃への対策」参照）。

3.1.3 海外の制御システムのセキュリティ強化の取り組み

本項では、海外における制御システムのセキュリティ強化の取り組みについて述べる。

(1) 米国 CISA の取り組み

米国の CISA は、2021 年 2 月、国際的なパートナーと協力してサイバーインシデントに対する防御及び重要インフラのセキュリティとレジリエンスを強化し、国家の重要機能に対する重大なリスクを特定して対処し、シームレスでセキュアな緊急時の通信手段を提供するための国際戦略「CISA Global※53」を開始した。この戦略で CISA は、よりオープンで、相互運用性、信頼性が高く、セキュアな相互につながる世界を目指し、政府や業界のセキュリティ専門家やリスク管理者が、利害関係者と連携し、能力強化を行いながら、重要インフラへの脅威を阻止・緩和し、リスクに対処できるグローバルな運用・政策の環境を形成するとしている※54。

また CISA は、2021 年 6 月、ランサムウェア攻撃の増加を受け、重要インフラの所有者や運営者が OT 資産や制御システムを見直すためのガイダンス「Rising Ransomware Threat to Operational Technology Assets※55」を発表した。本ガイダンスは、重要インフラ

が国家安全保障及びその人材やプロセスにとって重要であることを踏まえ、組織がランサムウェア攻撃に対して効果的なレジリエンスを構築できるよう支援することを目的とし、ランサムウェア攻撃を受けた場合に、ビジネスを大きく悪化させるリスクを軽減する方法を解説している※56。

更にCISAは2021年8月5日、重要インフラへのサイバー脅威に対する米国の防衛を支援することを目的とした取り組み「Joint Cyber Defense Collaborative（JCDC）※57」を開始した。JCDCは、ランサムウェアやクラウドサービスへの攻撃に対する取り組みを皮切りに、サイバー情報共有や防衛作戦計画の策定を主導することで、サイバー防衛を一元化することを計画している。大手クラウドサービスプロバイダを始め、連邦政府、州政府、地方自治体のほか、情報共有・分析機関、重要インフラの所有者・運営者、学術機関、その他の民間企業が参加する。

(2) 米国 Biden 政権の取り組み

2021年7月、米国のJoe Biden大統領は、重要インフラ所有者及び運営者にサイバーセキュリティのパフォーマンス目標のベースラインを設定することで、重要インフラのセキュリティを強化することを目的とした国家安全保障に関する覚書を発表した※58。この覚書は、重要インフラのコミュニティと連邦政府が重要インフラの防御に自主的かつ協力的に取り組むために同年4月中旬に設立された「Industrial Control Systems Cybersecurity Initiative（ICS initiative）」を促進し、CISAと商務省（DOC：Department of Commerce）の米国国立標準技術研究所（NIST：National Institute of Standards and Technology）が、他の連邦政府機関と協力して、重要インフラ組織に対するサイバーセキュリティのパフォーマンス目標とガイダンスを策定するよう指示している※59。

2021年5月にColonial Pipeline Companyのインシデントが発生した直後、Biden大統領は5月12日、サイバー攻撃に対する米国の防御力を近代化し、法執行機関の捜査に必要な情報をよりタイムリーに提供するための大統領令EO 14028に署名した※60。また、米国政府は、天然ガスパイプラインとサプライチェーンのサイバーセキュリティを強化するための二つの取り組みを2021年8月に発表した。一つは、NISTが産業界と協力して、セキュアな技術を構築するためのガイドラインを作成する。もう一つは、150の電力会社が導入に合意した制御システムのサイバーセキュリティの取り組みを、天然ガスのパイプラインにも正式に拡大する※61、というものである。なお、Biden政権の政策全般については「3.4.1 (2) Biden 政権の政策」を参照されたい。

(3) エネルギー業界の取り組み

米国エネルギー省（DOE：Department of Energy）は、CISA及び産業界と協力して、電力インフラのサイバーセキュリティ向上のための100日間の取り組みを開始する、と2021年4月に発表した※62。この取り組みは、DOE配下のOffice of Cybersecurity, Energy Security, and Emergency Response（CESER）が制御システムを運用している電力会社のサイバーセキュリティの可視性、検出及び対応能力を向上させる技術やシステムの開発を継続すること、制御システムやOTネットワークにおいて、ほぼリアルタイムの状況認識と対応を可能にするシステムを特定して展開すること、重要インフラのITネットワークのサイバーセキュリティ体制を改善すること等を具体的な目標としている。

2021年3月、北大西洋条約機構（NATO：North Atlantic Treaty Organization）のエネルギー安全保障センター（NATO Energy Security Centre of Excellence（ENSEC COE））と、産業オートメーションと制御システムのセキュリティ標準規格化を行っている国際計測制御学会（ISA：International Society of Automation）のISA99委員会が、エネルギー分野におけるサイバーセキュリティの標準とガイドラインの適用に関連する情報交換と協力のための同意書に署名した※63。

2021年5月、世界経済フォーラム（WEF：World Economic Forum）が、石油・ガス業界全体のサイバーレジリエンスを強化するための計画をまとめたホワイトペーパー※64を発行した。このホワイトペーパーでは、組織がリスクを管理し、推奨される活動によって組織のサイバーセキュリティ体制を強化するための原則を概説している※65。

(4) 米国の非営利団体の取り組み

2021年10月、米国のThe MITRE Corporationが、実際の観測記録に基づいたサイバー攻撃者の戦術と技術に関する、グローバルにアクセス可能なナレッジベース「ATT&CK※66」の第10版を発表※67した。モバイル向け、制御システム向けの各フレームワークの技術、グループ、ソフトウェアを更新し、制御システムに特化した「Stuxnet」や「Industroyer」等のウイルスが、エンタープライズ向けの「ATT&CK for Enterprise」及び制御システム向けの「ATT&CK for ICS」の両方のマトリクス

（戦術と技術をまとめた一覧）で把握できるようにマッピングされている※68。

(5) オーストラリアの取り組み

オーストラリア連邦議会は、「重要インフラ安全保障法（Security of Critical Infrastructure Act 2018）」を改正し、連邦政府が「重要インフラ」資産保護に対する義務を執行する能力を大幅に向上させる「Security Legislation Amendment（Critical Infrastructure）Bill 2021※69」の第1部を可決し、12月2日に発効した。この法律では、「重要インフラ部門」の定義が拡大され、「重要」とされた11分野（通信、データの保存または処理、金融サービス及び市場、上下水道、エネルギー、医療、高等教育・研究、食品・食料品、輸送、宇宙技術、防衛産業分野）が追加されている。また、重要インフラ資産に責任を持つ事業体に、インシデント報告の義務と罰則規定の詳細を定めている※70。

3.1.4 国内の制御システムのセキュリティ強化の取り組み

本項では、制御システムを含む、重要インフラサービスのセキュリティ強化に関する国内の主な取り組みの概要を紹介する。

(1) 日本政府の取り組み

包括的な重要インフラのセキュリティ政策については、「2.1.1 政府全体の政策動向」及び「2.1.2 経済産業省の政策」で取り上げているので、そちらを参照されたい。ここでは特に、制御システムのセキュリティ強化に関連する取り組みについて触れる。

内閣官房内閣サイバーセキュリティセンター（NISC：National center of Incident readiness and Strategy for Cybersecurity）が、2021年度における我が国を取り巻くサイバーセキュリティに関する情勢、及び2018年7月に発表された「サイバーセキュリティ2018」に掲げられた具体的な施策の実施状況等をまとめた「サイバーセキュリティ2021（2020年度年次報告・2021年度年次計画）※71」を2021年9月に発表した。NISCの重要インフラグループは、重要インフラの情報セキュリティ対策を推進するため、2018年策定の「サイバーセキュリティ戦略」及び2017年策定の「重要インフラの情報セキュリティ対策に係る第4次行動計画※72」に基づき、安全基準等の整備及び浸透、情報共有体制の強化、障害対応体制の強化、リスクマネジメント、防護基盤の強化、の五つの施策を進めている。

NISCはまた、ランサムウェアによるサイバー攻撃について、予防・検知・対応・復旧の観点から、具体的な対策を取れるよう、2021年4月30日に、重要インフラ事業者等向けに注意喚起を行った※73。また、ランサムウェアによる攻撃が国内外の様々な組織で確認されていることから、2021年9月1日に運用開始した「サイバーセキュリティ・ポータルサイト※74」内に、「ランサムウェア特設ページ STOP! RANSOMWARE※75」を同年10月13日に開設した。

経済産業省とIPA産業サイバーセキュリティセンター（ICSCoE：Industrial Cyber Security Center of Excellence）は、米国政府（CISA、DOE、国務省（DOS：United States Department of State））と連携し、2021年3月8～12日まで、日米の専門家による制御システムのサイバーセキュリティに関する演習をオンラインで実施した※76。2018年に開始され、3回目となるこの演習は、インド太平洋地域の重要インフラ事業者や国のCSIRT（Computer Security Incident Response Team）におけるOT・ITのサイバーセキュリティ担当者や、関連する政府機関の政策担当者を対象として行われた。更に、2021年10月25～29日まで、EU政府（通信ネットワーク・コンテンツ・技術総局）も加わった4回目の演習を実施した※77（第4回の演習については「2.3.2 (1) 中核人材育成プログラム」参照）。

(2) IPAの取り組み

2021年、IPAでは制御システムのセキュリティに関して、大きく二つの取り組みを行った。

(a) 制御システムのセキュリティリスクアセスメント普及活動

制御システムに対するセキュリティリスクアセスメントの普及を目的として、「制御システムのセキュリティリスク分析ガイド」（以下、リスク分析ガイド）を用いてリスク分析手法を解説するオンラインセミナーを、2021年5～9月と2021年11月～2022年3月の2回開催した。同セミナーでは、約370社・団体の受講者が、リスク分析ガイドを解説した合計約3時間の講義動画の視聴や、電子メールによる質疑応答を行った。

また、「制御システム関連のサイバーインシデント事例」シリーズ（次ページ表3-1-3）を2019年7月以降、順次公開しており、2021年は事例8及び事例9を公開した※78。本シリーズでは、過去のインシデント事例の概要と攻撃

No.	表題	内容	被害
1	2015 年ウクライナ大規模停電	制御端末の外部からの遠隔操作	大規模長時間停電
2	2016 年ウクライナマルウェアによる停電	マルウェアによる遮断器の操作	大規模停電
3	2017 年安全計装システムを標的とするマルウェア	安全計装機器への攻撃スクリプト送信	制御システムの停止
4	Stuxnet：制御システムを標的とする初めてのマルウェア	USB メモリとゼロデイ脆弱性を利用した破壊工作	遠心分離機の破壊
5	2019 年ランサムウェアによる操業停止	情報系を中心としたシステム破壊	生産量の激減
6	2018 年半導体製造企業のランサムウェアによる操業停止	ランサムウェアに感染した新規導入機器からの感染拡大と暗号化	製造システムの操業停止
7	2020 年医療関連企業のランサムウェアによる業務停止	電子カルテサーバからのデータ窃取	患者の個人情報の漏えい
8	2021 年水道局への不正侵入と飲料水汚染未遂	インターネット経由での水処理システムへの侵入及び遠隔操作	薬液投入量の変更
9	2021 年米国最大手のパイプラインのランサムウェア被害	情報系のランサムウェア感染	燃料パイプラインの操業停止

■表 3-1-3 「制御システム関連のサイバーインシデント事例」シリーズ

の流れ（攻撃ツリー）を紹介しており、制御システム保有事業者は、リスク分析ガイドで提唱している「事業被害ベースのリスク分析」を実施する際に、攻撃ツリーの作成、対策の策定に事例を活用できる。

(b) 制御システムのサイバーセキュリティ人材の育成

2017 年 4 月に発足した ICSCoE では、模擬プラントを用いた演習や、攻撃防御の実践経験、最新のサイバー攻撃情報の調査・分析等を通じて、社会インフラ・産業基盤のサイバーセキュリティリスクに対応する人材の育成を支援している（「2.3.2 産業サイバーセキュリティセンター」参照）。2021 年は、リスク分析ガイドの演習付き講義を、中核人材育成プログラムの第 5 期生に対して実施した。

3.2 IoTの情報セキュリティ

IoT（Internet of Things）技術の普及とともに、インターネット接続機能を持つコンピュータ以外の機器（IoT機器）がサイバー攻撃の対象となる脅威が継続している。新型コロナウイルス感染拡大の継続から、新しい生活様式やテレワークに対するサイバー攻撃が注目を集めているが、IoTに対する脅威の認識とセキュリティ対策推進の必要性には変わりがない。

本節では、IoTに対する脅威の動向、IoTセキュリティのサプライチェーンとEOL（End-of-Life）のリスク、脆弱な機器とウイルス感染の実態、セキュリティ対策強化の取り組みについて述べる。

なお、本節中で記載されている脆弱性のうち、脆弱性データベースの登録IDを記載しているものについては、表3-2-1に記載の各データベースで検索することによって、概要、詳細情報、関連情報へのリンク等を確認できる。

登録IDの表記例	登録先データベース
CVE-20xx-xxxxx	NVD※79
JVNDB-20xx-xxxxxx	JVN iPedia※80

■表3-2-1　脆弱性の登録IDの表記例と登録先データベース

3.2.1 残存するIoTのセキュリティ脅威

IoT機器に感染するウイルスは、「機器乗っ取り型ウイルス」「機器保護型ウイルス」「機器破壊型ウイルス」の3種類に分類できる※81。2021年は、前年と同様に、機器保護型ウイルスと機器破壊型ウイルスについて、目立った活動は見られなかった。一方、Mirai※82及びGafgytに代表される機器乗っ取り型ウイルス※83に関しては、感染機器の残存、新たな脆弱性と悪用する亜種の出現、新たな悪用方法の取り込み等が継続している。

本項では、2021年に発生した機器乗っ取り型ウイルスの脅威に関して、種別ごとに時系列（一部例外を除き情報公開順）に沿って紹介する。

(1) VPNFilterの感染機器の残存

「VPNFilter※84」は、2016年から感染活動が確認されていたウイルスで、2018年に世界中で活動が拡大した。2018年5月にはFBIによってC&Cサーバ※85に悪用されるドメインの一部を押収するテイクダウンが実施された※86が、2021年に入っても感染機器が残存していることが報告された※87。VPNFilterは主にルータやNAS（Network-Attached Storage：ネットワーク接続ストレージ）に感染するが、VPNFilterが悪用する脆弱性を有したままネットワークに接続される機器が残存する理由として、以下が指摘されている。

- インターネット接続事業者からレンタルされるルータで、エンドユーザに管理者権限が付与されていないため、ファームウェアが更新できなかった。
- ファームウェアの更新が提供されていたが、機器が自動更新機能を有しておらず、ベンダのサイトにアクセスして手動更新ができないユーザが存在した。

非営利のセキュリティ団体によって、2018年半ばに約1万4,000台観測されていた感染機器は、2020年後半には5,447台にまで減少したが、依然としてかなりの感染が残っていた。現存する感染機器の割合の国・地域別の上位5位は、ウクライナ（18.42%）、米国（14.48%）、イタリア（10.26%）、英国（8.05%）、フランス（7.26%）であった。日本は14位に位置し、1.8%であった。その後、セキュリティベンダと非営利団体の協力により、感染機器のクリーンアップが行われたが、最終的に363台の感染機器の残存が報告されている。

(2) Miraiとその亜種

2016年9月に出現し、同月末にソースコードが公開された「Mirai」は、現在に至っても新たな亜種が発生し、感染活動が継続している。

(a) 各社製ルータの脆弱性を狙うMiraiの亜種

2017年12月、Miraiの亜種「Satori※88」によって、以下に示す脆弱性が初めて感染拡大に悪用された。

- Huawei Technologies Co., Ltd.（华为技术有限公司）製ルータHG532における任意のコード実行の脆弱性（CVE-2017-17215（JVNDB-2017-013014））
- Realtek Semiconductor Corp.（瑞昱半導體股份有限公司。以下、Realtek社）製Realtek SDKを用いたIoT機器におけるUPnP miniigd SOAPサービスの任意のコード実行の脆弱性（CVE-2014-8361（JVNDB-2014-008039））

これらの脆弱性を狙うMiraiの亜種のアクセスが2020年11月以降に再び増加し、2021年1月末まで継続的に観測された※89。

(b) Android機器を狙う「Matryosh」

2021年1月25日、ADB（Android Debug Bridge）インタフェースをとおしてAndroid OSを搭載したIoT機器を狙い、DDoS攻撃の踏み台に悪用しようと試みる攻撃が観測された※90。多重化された暗号化方式とC&Cサーバのアドレス取得方式がマトリョーシカ人形を彷彿させるため、「Matryosh」と名付けられた。独自の暗号化方式や接続経路を匿名化するTor（The Onion Router）ネットワークの利用から、Miraiの亜種「Moobot※91」の更なる亜種「LeetHozer※92」との強い類似性を備える。

(c) 道路状況監視機器の脆弱性を狙う攻撃

2021年2月20日、Iteris, Inc.製の道路状況監視機器Vantage Velocity（道路網に設置して通過車両中のBluetooth対応機器から平均移動時間と速度を計測する監視機器）のリモートコード実行脆弱性（CVE-2020-9020（JVNDB-2020-002044））を狙う攻撃が観測された※93。その挙動からMiraiの亜種「Satori」または「fbot※94」の更なる亜種と考えられており、攻撃対象機器が米国内に187台設置されていることが報告された。

(d) ハニーポット機能を感染拡大に悪用する「ZHtrap」

2021年2月28日、Miraiの新たな亜種の攻撃が観測された※95。このウイルスは以下に示す特徴を有しており、「ZHtrap」と名付けられた。

- 4種類の既知の脆弱性を感染拡大に悪用する。
- 感染機器上でハニーポット機能を実行する。23種類のポートで待ち受けを行い、アクセスしてきたIoT機器を他のウイルスに感染済みの脆弱な機器と見なして、次の攻撃対象に追加する。
- 感染機器のスナップショットを作成し、それに基づき新たなコマンドの実行を禁止することで、他のウイルスの感染を防止して機器を独占する。
- C&CサーバとのTorネットワークを利用しており、Matryosh（「3.2.1（2）（b）Android機器を狙う『Matryosh』」参照）の実装流用が見られる。

(e) 複数のネットワーク機器の脆弱性を狙う亜種

2021年2月16日、複数のネットワーク機器における既知の脆弱性、未知のIoT機器の脆弱性を狙う攻撃が観測された※96。同年の2月23日、3月3日、3月13日には、新たに公開された脆弱性や他の既存の脆弱性を次々と取り込んだMiraiの亜種が検出された。このウイルスが感染拡大において悪用を試みる脆弱性を以下に示す。

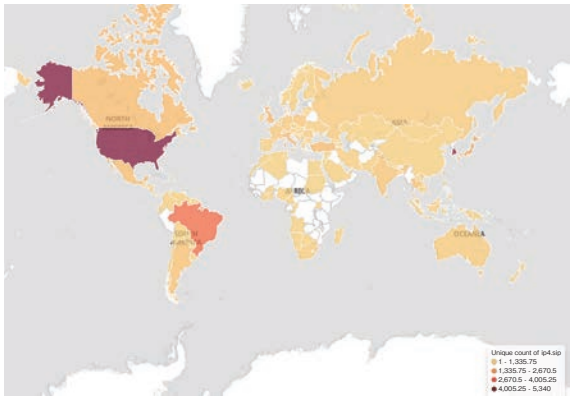
- SonicWALL, Inc.製SSL-VPNアプライアンスにおけるリモートコマンドインジェクションの脆弱性※97
- D-Link Corporation（友讯科技股份有限公司。以下、D-Link社）製NAS DNS-320におけるOSコマンドインジェクションの脆弱性（CVE-2020-25506（JVNDB-2020-015749））
- Yealink Network Technology Co., Ltd.（厦门亿联网络技术股份有限公司）製Device Management Platformにおける非認証ルート権限コマンドインジェクションの脆弱性（CVE-2021-27561）
- Micro Focus International plc製Operations Bridge Reporterにおけるリモートコード実行の脆弱性（CVE-2021-22502（JVNDB-2021-003430））
- Netis Systems Co., Ltd.（深圳市磊科实业有限公司）製無線ルータNetis WF2419におけるリモートコード実行の脆弱性（CVE-2019-19356（JVNDB-2019-014562））
- NETGEAR, Inc.（以下、NETGEAR）製スイッチングハブProSafe Plus JGS516PEの非認証リモートコード実行の脆弱性（CVE-2020-26919（JVNDB-2020-012278））
- 未知のIoT機器のコマンドインジェクション脆弱性（3種類）

このウイルスを構成するバイナリファイルの（亜種命名に用いられることが多い）ファイル名の一つに「dark」という文字列が含まれている。

(f) KGUARD社製DVRの非公開の脆弱性を攻撃する亜種「Mirai_ptea」「Mirai_aurora」

2021年6月22日、KGUARD INFORMATION Co., Ltd.（廣盈資訊股份有限公司。以下、KGUARD社）製DVR（Digital Video Recorder）の非公開の脆弱性を攻撃するMiraiの亜種が観測され、「Mirai_ptea」と名付けられた※98。同月25日には、別の亜種「Mirai_aurora」が同じ脆弱性を感染拡大に悪用する活動が観測されている。2016年以前にリリースされたファームウェアを使用するKGUARD社製DVRには、非認証のリモートコマンド実行の脆弱性があり、少なくと

も約 3,000 台が脆弱性を有したままインターネット上に接続されていることが確認された。6 月 24 日の時点で最大約 1 万 5,000 台の感染機器が観測されたボットネットの分布は、米国・韓国・ブラジルに集中している。感染機器の地理的分布を図 3-2-1 に示す。



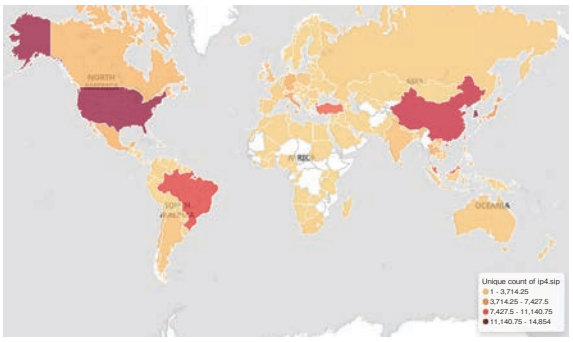
■図 3-2-1　ウイルス感染が疑われる KGUARD 社製 DVR の地理的分布
（出典）Qihoo 360 Technology Co., Ltd.「Mirai_ptea Botnet is Exploiting Undisclosed KGUARD DVR Vulnerability※98」

(g) WebSVN のコマンドインジェクション脆弱性を狙う亜種

2021 年 6 月 26 日、オープンソースの Web アプリケーション WebSVN のコマンドインジェクションの脆弱性（CVE-2021-32305（JVNDB-2021-006964））を狙う Mirai の亜種が観測された※99。この亜種は、12 種類の異なるアーキテクチャ用のバイナリが用意されており、感染機器を DDoS 攻撃の踏み台として悪用する。実行ファイルは、オープンソースのパッカーである UPX を修正したもので圧縮されており、解析者によるリバースエンジニアリングツールを用いた自動解凍を困難にしている。

(h) RUIJIE 社製ルータのゼロデイ脆弱性を狙う「Mirai_ptea_Rimasuta」

2021 年 9 月 5 日、Ruijie Networks Co.,Ltd.（北京星网锐捷网络技术有限公司。以下 RUIJIE 社）製ルータ NBR700 シリーズのゼロデイ脆弱性を狙う Mirai の亜種が観測された。「Mirai_ptea」（「3.2.1 (2) (f) KGUARD 社製 DVR の非公開の脆弱性を攻撃する亜種『Mirai_ptea』『Mirai_aurora』」参照）を基に作成されており、「Mirai_ptea_Rimasuta」と名付けられた※100。RUIJIE 社製の当該ルータには、認証後のコマンドインジェクションの脆弱性が存在しており、脆弱な初期パスワードと組み合わせることで感染可能となっていた。翌 9 月 6 日に脆弱性が RUIJIE 社に報告され、同月 9 日に同社がその存在を確認したが、サポート終了製品であり、初期パスワードを変更することで緩和可能なため、修正ファームウェアは提供されなかった。この脆弱性は、6 月 10 日に別の亜種「Mirai_aurora」（「3.2.1 (2) (f) KGUARD 社製 DVR の非公開の脆弱性を攻撃する亜種『Mirai_ptea』『Mirai_aurora』」参照）による悪用が初観測されている。7 月下旬の時点で最大約 2 万台の感染が観測されたボットネットの分布は、米国・韓国・中国・ブラジル等に渡っている。感染機器の地理的分布を図 3-2-2 に示す。



■図 3-2-2　ウイルス感染が疑われる RUIJIE 社製ルータの地理的分布
（出典）Qihoo 360 Technology Co., Ltd.「Mirai_ptea_Rimasuta variant is exploiting a new RUIJIE router 0 day to spread※100」

(3) Gafgyt とその亜種

2014 年に活動を開始した Gafgyt（別名 Bashlite、QBot 等）は、2015 年のソースコード公開後、様々な亜種が発生し、感染活動が継続している。

(a) Tor を利用する亜種「Gafgyt_tor」

2021 年 2 月 15 日以降、C&C サーバとの通信に Tor ネットワークを初めて利用する Gafgyt の亜種が観測され、「Gafgyt_tor」と名付けられた※101。この亜種は「Necro」（「3.2.1 (4) (a)『Necro』の亜種」参照）と同一の集団によって運用されていると考えられ、脆弱な TELNET パスワード及び以下に示す脆弱性を感染拡大に悪用する。

- D-Link 社製品におけるリモートコード実行の脆弱性（CVE-2019-16920（JVNDB-2019-009977））
- Liferay, Inc. 製 Liferay Portal のリモートコード実行の脆弱性（CVE-2020-7961（JVNDB-2020-003135））
- Citrix Systems, Inc. 製品におけるパストラバーサルの脆弱性（CVE-2019-19781（JVNDB-2019-013490））

(b) Gafgyt の亜種「Mozi」

2021 年 8 月 30 日、Gafgyt の亜種「Mozi※102」の現在の状況が報告された※103。2019 年 9 月から活動を開始した Mozi は、2020 年 4 月の時点で 1 万 5,000 台以

上の感染が確認されていた※104。2020年9月には、16万台／日の勢いで感染拡大を続け、感染機器は150万台（内半数以上の約83万台は中国国内に存在）に達した※105。2021年7月、セキュリティベンダが提供した解析情報を基に、Moziの作者は中国法執行当局によって逮捕された※106。また2021年8月、Microsoft社がMoziの防御方法を公開した※107。Moziの更新は停止されたが、感染機器は残存しており、ボットネットとして長期間存続する可能性が指摘されている。

(4) その他のウイルスとその亜種

MiraiやGafgytとそれらの亜種以外にも、IoT機器を狙ったウイルスは存在しており、新たな脆弱性や悪用の方法を取り込んだ進化が続いている。

(a)「Necro」の亜種

2015年に発見された「Necro」は、プログラミング言語Pythonで記述されたボットネットである。当初はWindowsを感染対象としていたが、2021年1月1日以降、Linuxの動作するIoT機器を攻撃対象とする感染活動が観測された※108。この亜種は、以下に示す特徴を備える。

- 3種類の異なるバージョン、バージョン1（necro.py（作成者による命名。以下同様））、バージョン2（out.py）、バージョン3（benchmark.py）がある。
- 脆弱なTELNETパスワードに加えて、TerraMaster Technology Co., Ltd.（深圳市图美电子技术有限公司）製NAS用TOS（TerraMaster Operating System）におけるOSコマンドインジェクションの脆弱性（CVE-2020-35665（JVNDB-2020-014767））を感染拡大に悪用する。
- バージョン2以降では、Zend Technologies Ltd.（現、Perforce Software, Inc.の一部門）製Webアプリケーションフレームワーク Zend Frameworkにおける信頼できないデータのデシリアライゼーションに関する脆弱性（CVE-2021-3007（JVNDB-2021-002421））を感染拡大に悪用する。
- バージョン3では、解析を困難とするために、ドメイン生成アルゴリズム（DGA：Domain Generation Algorithm）を用いてC&Cサーバのアドレスを動的に生成し、Pythonスクリプトを大幅に難読化している。
- バージョン2及びバージョン3のダウンロードと実行では、Python2プログラムをを PyInstallerで作成されたELF（Executable and Linkable Format）形式の実行ファイルとして配布することで、同言語がインストールされていない機器への感染も試みる。
- ウイルスのダウンロードサーバは、Miraiの亜種の配布も実施しており、他のウイルスを用いたボットネットも同時に運用していると考えられる。

2021年3月2日、Necroの新たな亜種が観測され、以下に示す点が強化されていることが確認された※109。

- Webアプリケーションフレームワーク Laravelにおけるリモートコード実行の脆弱性（CVE-2021-3129（JVNDB-2021-002557））、Oracle Corporation製WebLogic Serverにおけるリモートコード実行の脆弱性（CVE-2020-14882（JVNDB-2020-009778））が感染拡大の悪用手段として追加された。
- 2種類のバージョンがある。一方は、C&Cサーバとの通信にTorネットワークを利用する。他方は、DGAを用いたサブドメイン生成と動的ドメイン名の組み合わせによってC&Cサーバ名を動的に生成する。
- WebLogic Serverが動作するWindowsも攻撃対象とする。
- 特定のLinux機器に対しては、「Gafgyt_tor」（「3.2.1 (3) (a) Torを利用する亜種『Gafgyt_tor』」参照）をダウンロードする。
- 感染機器のWebサービスページを改ざんして、ブラウザマイニング（暗号資産（仮想通貨）の採掘処理）の実行、ユーザデータの窃取、ユーザのブラウザのDDoSボット化、ハッシュクラッキングへの悪用を試みる。

上記の挙動から、NecroとGafgyt_torは同一の集団によって運用されていると考えられる。

(b) QNAP社製NASのマイニング悪用

2021年3月2日、QNAP Systems, Inc.（威聯通科技股份有限公司。以下、QNAP社）製NASを標的として感染し、暗号資産のマイニングに悪用する攻撃が観測された※110。この攻撃は、同社製NAS用ヘルプデスクアプリケーションの不適切な認証の脆弱性（CVE-2020-2506）及びOSコマンドインジェクションの脆弱性（CVE-2020-2507（JVNDB-2020-015853））を悪用して感染し、マイニングプログラムXMRigを不正実行する。2020年8月以前にインストールされたヘルプデスクアプリケーションが影響を受けるとされ、全世界で感染の恐れがある機器が429万7,426台確認されている。インターネット上から観測可能なQNAP社製NASの国別分布を、

表 3-2-2 に示す。同月 11 日、QNAP 社は公開済みアドバイザリを更新した※111。

国名	台数
米国	554,481
中国	550,465
イタリア	371,327
フランス	279,294
ドイツ	270,667
日本	229,005
英国	172,782
オーストラリア	158,073

■表 3-2-2　QNAP 社製 NAS の国別台数（上位 8 ヵ国）
（出典）Qihoo 360 Technology Co., Ltd.「QNAP NAS users, make sure you check your system※110」

(c) NAS を標的とするランサムウェア「eCh0raix」の亜種

ランサムウェア「eCh0raix」は、QNAP 社製 NAS 及び Synology Inc.（群暉科技股份有限公司。以下、Synology）製 NAS を標的としたランサムウェアである。QNAP 社は、2019 年 8 月 12 日※112、2020 年 6 月 8 日※113、2021 年 5 月 14 日※114 等のアドバイザリを公開してきた。2021 年 4 月 22 日、QNAP 社製 NAS 用バックアップソフトウェア HBS 3（Hybrid Backup Sync）における不適切な認証の脆弱性（CVE-2021-28799（JVNDB-2021-007313））に関するアドバイザリ※115 が公開されたが、同年 6 月 21 日に eCh0raix による悪用が確認された※116。

(d) Edgewater Networks アプライアンスを狙う「EwDoor」

2021 年 10 月 27 日、Edgewater Networks, Inc.（現、Ribbon Communications US LLC の一部門）製ネットワーク機器を狙った新しいボットネットによる攻撃が観測され、「EwDoor」と命名された※117。EwDoor は、同社製アプライアンスのコマンドインジェクションの脆弱性（CVE-2017-6079（JVNDB-2017-004169））を介して感染を拡大する。主に EdgeMarc Enterprise Session Border Controller を攻撃対象としており、観測時点では、米国の通信事業者 AT&T Inc. に属する約 5,700 台の感染が確認されている。

3.2.2 サプライチェーンとEOLのリスク

IoT のセキュリティ対策を困難にしている理由の一つに、IoT 機器の開発に用いられる共通コンポーネントや標準プロトコルに起因する脆弱性（IoT 機器のサプライチェーンリスク）がある。また、脆弱性が発見された IoT 製品がサポート終了した EOL（End-of-life）ステータスにある場合、更新ファームウェアが提供されないことが多く、脆弱性を残したままインターネットへの接続が継続される恐れが生じる。本項では、2021 年に発生したサプライチェーンと EOL のリスク事例を紹介する。

(1) 共通コンポーネントの脆弱性

2020 年に引き続いて、IoT 機器の開発においてサードパーティ製ハードウェア部品及びソフトウェア部品として採用される共通コンポーネントにおいて、数多くの脆弱性が発見された。

(a) NUMBER:JACK

2021 年 2 月 10 日、9 種類の TCP/IP スタック（uIP、FNET、picoTCP、Nut/Net、CycloneTCP、uC/TCP-IP、NDKTCPIP、MPLAB Net、NucleusNET※118）において発見された 9 種類の脆弱性（表 3-2-3）が報告され、「NUMBER:JACK」と名付けられた※119。該当する TCP/IP スタックは、TCP コネクションの初期シーケンス番号（ISN：Initial Sequence Number）を適切に生成していないため、攻撃者が特定可能である※120。数百万台の機器で使用されていると考えられ、医療機器、風力タービン監視システム、RTU（Remote Terminal Unit）、IT ストレージシステム等で利用が確認されている。同月 11 日、ICS-CERT はアドバイザリを公開し、随時更新している※121。

(b) NAME：WRECK

2021 年 4 月 12 日、4 種類の著名な TCP/IP スタック

脆弱性 ID	脆弱性の概要	対象スタック
CVE-2020-27213	不十分なランダム値の使用	Nut/Net
CVE-2020-27630		uC/TCP-IP
CVE-2020-27631		CycloneTCP
CVE-2020-27632		NDKTCPIP
CVE-2020-27633		FNET
CVE-2020-27634		uIP
CVE-2020-27635		picoTCP
CVE-2020-27636		MPLAB Net
CVE-2020-28388		NucleusNET

■表 3-2-3　NUMBER:JACK の脆弱性
（出典）Forescout Technologies, Inc.「NUMBER:JACK – Forescout Research Labs Finds Nine ISN Generation Vulnerabilities Affecting TCP/IP Stacks※119」を基に IPA が作成

（FreeBSD、NucleusNET、IPnet、NetX）において発見された 9 種類の脆弱性（表 3-2-4）が報告され、「NAME:WRECK」と名付けられた※122（「1.2.5 (3) (a) 多数の IoT 製品に影響する脆弱性」参照）。該当する TCP/IP スタックは、DNS プロトコルのメッセージ圧縮機能が正しく実装されていないため、リモートコード実行・DoS 攻撃・DNS キャッシュポイズニングの攻撃に晒される恐れが存在する。世界中に 100 億台を超える実装機器が存在しており、少なくともそのうち 1 億台が影響を受けると推定されている。

脆弱性 ID	脆弱性の概要	対象スタック
CVE-2020-7461	境界外書き込み	FreeBSD
CVE-2016-20009	境界外書き込み	IPnet
CVE-2020-15795	境界外書き込み	NucleusNET
CVE-2020-27009	範囲外のポインタオフセットの使用	NucleusNET
CVE-2020-27736	不適切な NULL による終了	NucleusNET
CVE-2020-27737	境界外読み取り	NucleusNET
CVE-2020-27738	バッファエラー	NucleusNET
CVE-2021-25677	不十分なランダム値の使用	NucleusNET
未割り当て	ポインタ値非確認に起因する境界外アクセス	NetX

■表 3-2-4　NAME:WRECK の脆弱性
（出典）Forescout Research Labs & JSOF「NAME:WRECK Breaking and fixing DNS implementations※123」を基に IPA が作成

(c) Arcadyan 社製ルータ用ファームウェアの脆弱性

2021 年 4 月 26 日、Arcadyan Technology Corporation（智易科技股分有限公司。以下、Arcadyan 社）製ルータ及び同社製ファームウェアを用いたルータ等におけるディレクトリトラバーサルの脆弱性（CVE-2021-20090（JVNDB-2021-002008））が報告された※124。Arcadyan 社製ファームウェアは、世界各国の通信事業者やベンダのルータ／モデムで採用されている（表 3-2-5）。

株式会社バッファロー製ルータの一部機種には、同時に機種固有の脆弱性（CVE-2021-20091（JVNDB-2021-005999）、CVE-2021-20092（JVNDB-2021-006000））も発見されており、同月 27 日、ファームウェア更新情報が公開された※125。影響を受ける機器が更に発見されたため、2021 年 7 月 20 日、米国の CERT Coordination Center（以下、CERT/CC）はアドバイザリを公開し、その後も随時更新している※126。

事業者名・ブランド名／製造会社名	国・地域名
ADB（Advanced Digital Broadcast）SA	スイス
Arcadyan Technology Corporation	台湾
ASMAX	ポーランド
ASUSTeK Computer Inc.（華碩電脳股份有限公司）	台湾
Beeline	ロシア
BT Group plc（旧 British Telecom）	英国
Deutsche Telekom AG	ドイツ
Hughes Network Systems, LLC（HughesNet）	米国
Koninklijke KPN N.V.	オランダ
Telefónica, S.A.（O2）	スペイン
Orange S.A.（旧 France Télécom S.A.）	フランス
Spark New Zealand Limited（Skinny/Spark NZ）	ニュージーランド
Telecom Argentina S.A.	アルゼンチン
Teléfonos de México, S.A.B. de C.V.（TelMex）	メキシコ
Telstra Corporation	オーストラリア
Telus Corporation	カナダ
Verizon Communications Inc.	米国
Vodafone Group Plc	英国
株式会社バッファロー	日本

■表 3-2-5　Arcadyan 社製ファームウェアの採用事業者
（出典）Tenable, Inc.「Multiple Vulnerabilities in Buffalo and Arcadyan manufactured routers※124」を基に IPA が作成

(d) BadAlloc

2021 年 4 月 29 日、広く利用されているリアルタイム OS（RTOS：Real-Time Operating System）、ソフトウェア開発キット（SDK：Software Development Kit）、C 言語標準ライブラリ（libc）の実装におけるメモリ割り当て機能の脆弱性が報告され、「BadAlloc」と名付けられた※127。これらのメモリ管理機能は、入力パラメータの適切な検証を実施していないため、攻撃者は脆弱性を悪用してヒープオーバーフローを実行し、悪意のあるリモートコード実行が可能となる。2021 年 11 月 30 日、ICS-CERT はアドバイザリ（次ページ表 3-2-6）を公開し、その後も随時情報を更新している※128。

脆弱性 ID	影響を受けるRTOS／SDK／ライブラリ
CVE-2021-30636	Media Tek LinkIt SDK
CVE-2021-27431	ARM CMSIS-RTOS2
CVE-2021-27433	ARM mbed-ualloc memory library
CVE-2021-27435	ARM mbed OS
CVE-2021-27427	RIOT OS
CVE-2021-22684	Samsung Tizen RT RTOS
CVE-2021-27439	TencentOS-tiny
CVE-2021-27425	Cesanta Software Mongoose OS
CVE-2021-26461	Apache Nuttx OS
CVE-2020-35198	Wind River VxWorks
CVE-2020-28895	
CVE-2021-31571	Amazon FreeRTOS
CVE-2021-31572	
CVE-2021-27417	eCosCentric eCosPro RTOS
CVE-2021-3420	Redhat newlib
CVE-2021-27421	NXP MCUXpresso SDK
CVE-2021-22680	NXP MQX
CVE-2021-27419	uClibc-ng
CVE-2021-27429	Texas Instruments TI-RTOS
CVE-2021-22636	
CVE-2021-27504	FREERTOS を用いた Texas Instruments 製品
CVE-2021-27502	Texas Instruments TI-RTOS
未割り当て	Google Cloud IoT Device SDK
CVE-2021-27411	Micrium OS
CVE-2021-26706	Micrium uC/OS: uC/LIB
CVE-2020-13603	Zephyr Project RTOS
CVE-2021-22156	BlackBerry QNX SDP
	BlackBerry QNX OS

■表 3-2-6　脆弱性 BadAlloc の影響を受ける RTOS／SDK／ライブラリ
（出典）ICS-CERT「ICS Advisory (ICSA-21-119-04)※128」を基に IPA が作成

(e) Qualcomm 製チップセットの脆弱性

2021 年 5 月 6 日、Qualcomm, Inc. 製携帯電話向けチップセット MSM（Mobile Station Modem）のファームウェアにおける、バッファオーバーフローの脆弱性（CVE-2020-11292（JVNDB-2021-007821））が報告された※129。全世界の携帯電話の約 3 割に採用されており、攻撃者が脆弱性を悪用することで、ユーザの通話履歴と SMS へのアクセスや SIM ロックの解除が可能であった。

(f) ThroughTek P2P SDK の脆弱性

2021 年 6 月 15 日、ThroughTek Co., Ltd.（物聯智慧股份有限公司）製 IoT 開発プラットフォーム ThroughTek Kalay P2P SDK の脆弱性（CVE-2021-32934（JVNDB-2021-001889））が報告された※130。この脆弱性は、固定鍵を用いてパケットペイロードが暗号化されているため、容易に解読可能というものであった。このソフトウェア開発キットは、ネットワークカメラの OEM ベンダ向けにインターネット経由のオーディオ／ビデオストリームの Peer-to-Peer 通信機能を提供しており、数百万台の機器に採用されている。

2021 年 8 月 17 日、Kalay P2P SDK の新たな脆弱性（CVE-2021-28372（JVNDB-2021-002281））が報告された※131。不適切なアクセス制御を悪用して、攻撃者の端末を Kalay ネットワークに不正接続することで、ネットワークカメラ内の情報へのアクセスや任意のコードの実行が試みられる恐れがある。

(g) INFRA:HALT

2021 年 8 月 4 日、InterNiche Technologies, Inc. 製の組み込みシステム用 TCP/IP スタック NicheStack（現在は Tuxera Hungary Kft. の一部門 HCC-Embedded が保守担当）の 14 種類の脆弱性（表 3-2-7）が報告され、「INFRA:HALT」と名付けられた※132。約 200 社の産業機器ベンダに採用されており、調査時点で約 6,400

脆弱性 ID	脆弱性の概要	対象プロトコル
CVE-2020-25928	長さパラメータ不整合時の不適切な取り扱い	DNSv4 Client
CVE-2021-31226	ヒープベースのバッファオーバーフロー	HTTP Server
CVE-2020-25767	境界外読み取り	DNSv4 Client
CVE-2020-25927	長さパラメータ不整合時の不適切な取り扱い	DNSv4 Client
CVE-2021-31227	ヒープベースのバッファオーバーフロー	HTTP Server
CVE-2021-31400	例外処理の不備	TCP
CVE-2021-31401	不適切な入力値検証	TCP
CVE-2020-35683	不適切な入力値検証	ICMP
CVE-2020-35684	不適切な入力値検証	TCP
CVE-2020-35685	不十分なランダム値の使用	TCP
CVE-2020-27565	不適切な例外条件の処理	HTTP
CVE-2021-36762	NULL 終端文字の欠落	TFTP
CVE-2020-25926	不十分なランダム値の使用	DNSv4 Client
CVE-2021-31228	不十分なランダム値の使用	DNSv4 Client

■表 3-2-7　INFRA:HALT の脆弱性
（出典）JFrog Ltd「INFRA:HALT 14 New Security Vulnerabilities Found in NicheStack※132」を基に IPA が作成

台の採用機器のインターネット接続が確認されている。

(h) Realtek 社製の無線機器向け SDK の脆弱性

2021 年 8 月 16 日、Realtek 社製の無線機器向け SDK の 4 種類の脆弱性（表 3-2-8）が報告された[※133]。65 社以上のベンダにおける数十万台の IoT 製品で脆弱性が存在すると見られている。同 SDK を採用する事

脆弱性 ID	脆弱性の概要
CVE-2021-35392	スタックバッファオーバーフロー
CVE-2021-35393	ヒープバッファオーバーフロー
CVE-2021-35394	コマンドインジェクション
CVE-2021-35395	コマンドインジェクション、境界外書き込み

■表 3-2-8　Realtek 社製 SDK の脆弱性
（出典）IoT Inspector GmbH（現、ONEKEY GmbH）「Advisory: Multiple issues in Realtek SDK affect hundreds of thousands of devices down the supply chain[※133]」を基に IPA が作成

事業者名・ブランド名／製造会社名	国・地域名
A-Link Europe Ltd	フィンランド
ARRIS Group, Inc.	米国
AirLive Technology Corporation（鑫志股份有限公司）	台湾
Abocom Systems Inc.（兆勁科技股份有限公司）	台湾
Shenzhen Zhuqiao Digital Technology Co., Ltd.（Algital）（深圳市竹桥数码科技有限公司）	中国
Amped Wireless	米国
Askey Computer Corporation（亞旭電腦股份有限公司）	台湾
ASUSTeK Computer Inc.（華碩電腦股份有限公司）	台湾
Shenzhen Best One Technology Co., Ltd.（深圳倍易通科技有限公司）	中国
Beeline	ロシア
Belkin International, Inc.	米国
Calix Inc.	米国
China Mobile Communications Group Co., Ltd.（中国移动通信集团有限公司）	中国
Compal Broadband Networks, Inc.（鎧寶科技股份有限公司）	台湾
D-Link Corporation（友讯科技股份有限公司）	台湾
DASAN Networks, Inc.（다산네트웍스）	韓国
Davolink Inc.（다보링크）	韓国
Edgecore Networks Corporation（鈺登科技股份有限公司）	台湾
Edimax Technology Co., Ltd.（訊舟科技股份有限公司）	台湾
EnGenius Technologies, Inc.	米国
Esson Technology Inc.	中国
EZ-NET Ubiquitous Co., Ltd.	韓国
Fida International (S) Pte Ltd（Prolink）	シンガポール
Hama GmbH & Co KG	ドイツ
Hawking Technologies, Inc.	米国
LG International（現、LX International Corp.）	韓国
LINK-NET TECHNOLOGY CO., LTD.	ベネズエラ（不確定）
MMC Technology, Inc.	韓国
MT-LINK Technologies Co. Ltd.	中国
NetComm Wireless Limited	オーストラリア
Netis Systems Co., Ltd.（深圳市磊科実业有限公司）	中国

事業者名・ブランド名／製造会社名	国・地域名
NETGEAR	米国
Nexxt Solutions	米国
Observa Telecom, Ltd	スペイン
Occtel Communication Co., Ltd.（福億通訊股份有限公司）	台湾
Omega Technology	ポーランド
PATECH（파테크）	韓国（不確定）
PLANET Technology Corporation（普萊德科技股份有限公司）	台湾
Realtek Semiconductor Corp.（瑞昱半導體股份有限公司）	台湾
Revogi Innovation Co., Ltd.（易家智能（深圳）有限公司）	中国
Sitecom Europe BV	オランダ
CFD 販売株式会社（Skystation）	日本
Sercomm Corporation（中磊電子股份有限公司）	台湾
Shaghal Ltd.（Jetstream）	米国
Shenzhen Yichen（JCG）Technology Development Co., Ltd.	中国
Shenzhen Skyworth Digital Technology Co., Ltd（创维数字股份有限公司）	中国
Smartlink	不明
TCL Communication Technology Holdings Limited（TCL 通讯科技控股有限公司）	中国
Technicolor, SA	フランス
Telewell Oy	フィンランド
Shenzhen Tenda Technology Co.,Ltd.（深圳市吉祥腾达科技有限公司）	中国
Zioncom（Hong Kong）Technology Limited（Totolink）（吉翁科技（香港）有限公司）	香港
TRENDnet, Inc.	米国
UPVEL LLC	米国
ZTE Corporation（中兴通讯股份有限公司）	中国
Zyxel Networks Corporation（合勤科技股份有限公司）	台湾
エレコム株式会社	日本
プラネックスコミュニケーションズ株式会社	日本
ロジテック株式会社	日本
株式会社アイ・オー・データ機器	日本
株式会社バッファロー	日本

■表 3-2-9　Realtek 社製 SDK の採用事業者
（出典）IoT Inspector GmbH（現、ONEKEY GmbH）「Advisory: Multiple issues in Realtek SDK affect hundreds of thousands of devices down the supply chain」を基に IPA が作成

業者の一部を表 3-2-9（前ページ）に示す。

(i) NUCLEUS:13

2021 年 11 月 9 日、Accelerated Technology, Inc.（現在は、Mentor Graphics Corporation を経て Siemens AG の一部門）製の組み込み機器向け Nucleus RTOS の TCP/IP スタックに 13 種類の脆弱性（表 3-2-10）が報告され、「NUCLEUS:13」と命名された※134。同日、ICS-CERT はアドバイザリを公開した※135。

脆弱性 ID	脆弱性の概要	対象プロトコル
CVE-2021-31344	型の取り違え	ICMP
CVE-2021-31345	入力で指定された数量の不適切な検証	UDP
CVE-2021-31346	入力で指定された数量の不適切な検証	IP / ICMP
CVE-2021-31881	境界外読み取り	DHCP Client
CVE-2021-31882	バッファエラー	DHCP Client
CVE-2021-31883	バッファエラー	DHCP Client
CVE-2021-31884	境界外読み取り	DHCP Client
CVE-2021-31885	不適切な長さの値によるバッファへのアクセス	TFTP Server
CVE-2021-31886	不適切な NULL 終端	FTP Server
CVE-2021-31887	不適切な NULL 終端	FTP Server
CVE-2021-31888	不適切な NULL 終端	FTP Server
CVE-2021-31889	整数アンダーフロー	TCP Server
CVE-2021-31890	一貫性のない構造要素の不適切な処理	TCP Server

■表 3-2-10　NUCLEUS:13 の脆弱性
（出典）Forescout Technologies, Inc.「New Critical Vulnerabilities Found on Nucleus TCP/IP Stack※134」を基に IPA が作成

(j) MediaTek 製スマートフォン用 SoC の脆弱性

2021 年 11 月 24 日、MediaTek Inc.（聯發科技股份有限公司）製スマートフォン用 SoC（System-on-a-chip）において、4 種類の脆弱性が発見された※136。全世界の 37% のスマートフォンや IoT 機器で採用されており、SoC 内のオーディオ処理用 DSP（Digital Signal Processor）のファームウェア及びオーディオのハードウェア抽象化レイヤに脆弱性（表 3-2-11）が存在し、DSP 上で不正プログラムを実行して盗聴に悪用される恐れがある。

脆弱性 ID	脆弱性の概要
CVE-2021-0661	境界外書き込み
CVE-2021-0662	境界外書き込み
CVE-2021-0663	境界外書き込み
CVE-2021-0673	不適切な入力確認

■表 3-2-11　MediaTek SoC の脆弱性
（出典）Check Point Software Technologies LTD.「Check Point Research discover vulnerabilities in smartphones chips embedded in 37% of smartphones around the world※136」を基に IPA が作成

(2) 標準プロトコルの脆弱性

IoT 機器が通信機能として採用・実装する標準プロトコルにおいて、脆弱性が発見されている。

(a) Wi-Fi の脆弱性「FragAttacks」

2021 年 5 月、無線 LAN 規格 Wi-Fi 仕様の設計上の欠陥及び実装上の誤りに起因する 12 種類の脆弱性（次ページ表 3-2-12）が公開され、「FragAttacks」と名付けられた※137。1997 年に制定された IEEE 802.11 に起因する 3 種類の設計上の欠陥とそれらに対する攻撃を、以下に示す。

設計①：アグリゲーション攻撃（aggregation attack）

Wi-Fi のフレームアグリゲーション機能（小さな複数のフレームを大きな集約フレームに結合することでネットワーク速度とスループットを向上する機能）において、集約されたか否かを示すフラグ「is aggregated」が認証されていないため、攻撃者による改ざんの恐れが存在する。

設計②：混合キー攻撃（mixed key attack）

Wi-Fi のフレームフラグメンテーション機能（大きなフレームを小さなフラグメントに分割することで接続の信頼性を向上する機能）において、受信者が複数のフラグメントからフレームを再構築する際、フラグメントが等しければ同一であるべき暗号鍵の同一性を確認していないため、攻撃者によるデータ窃取の恐れが存在する。

設計③：フラグメントキャッシュ攻撃（fragment cache attack）

Wi-Fi のフレームフラグメンテーション機能において、クライアントのネットワークからの切断時、サーバ（アクセスポイント）が再構築されていないフラグメントの残りをメモリ上から削除しないため、攻撃者によるデータ窃取の恐れが存在する。

2021 年 5 月 11 日、Wi-Fi Alliance※138 及び ICASI（Industry Consortium for Advancement of Security on the Internet、現 FIRST PSIRT SIG の一部）がそれぞれ声明を発表した。Wi-Fi 機能を実装したほぼすべての機器が影響を受け、各ベンダは対応に追われることとなった。

脆弱性 ID	原因	脆弱性の概要
CVE-2020-24588	設計①	アグリゲーション攻撃
CVE-2020-24587	設計②	混合キー攻撃
CVE-2020-24586	設計③	フラグメントキャッシュ攻撃
CVE-2020-26145	実装	不適切な入力確認
CVE-2020-26144		不適切な入力確認
CVE-2020-16140		インジェクション
CVE-2020-26143		不適切な入力確認
CVE-2020-26139		不適切な認証
CVE-2020-26146		不適切な入力確認
CVE-2020-26147		その他の脆弱性
CVE-2020-26142		インジェクション
CVE-2020-26141		完全性チェック値（ICV：Integrity Check Value）の検証不備

■表 3-2-12　Wi-Fi の脆弱性「FragAttacks」
（出典）New York University Abu Dhabi「FragAttacks: Security flaws in all Wi-Fi devices※137」を基に IPA が作成

(b) Bluetooth 仕様の脆弱性

2021 年 5 月 24 日、CERT/CC は、フランスの国防安全保障事務局傘下の ANSSI（Agence Nationale de la Sécurité des Systèmes d'Information）が近距離無線通信規格 Bluetooth の仕様である Core Specification の一部（Bluetooth BR/EDR（Basic Rate/Enhanced Data Rate）、Bluetooth Low Energy（BLE））及び Mesh Profile の脆弱性情報（表 3-2-13）を開示した、と発表した※139。Bluetooth SIG は、各脆弱性に対する緩和策を含む声明を発表した※140。影響を受ける製品は広範囲に渡っており、各ベンダは対応に追われた。

脆弱性 ID	対象	脆弱性の概要
CVE-2020-26558	Core Spec.	パスキーエントリープロトコルを利用したなりすまし
CVE-2020-26555		PIN コードペアリングプロトコルを利用したなりすまし
未割り当て		LE レガシーペアリングを利用したなりすまし
CVE-2020-26560	Mesh Profile	メッシュプロビジョニングを利用したなりすまし
CVE-2020-26557		不適切な値の利用による AuthValue の特定
CVE-2020-26556		ブルートフォース攻撃による AuthValue の特定
CVE-2020-26559		取得可能な値を利用した AuthValue の特定

■表 3-2-13　Bluetooth 仕様の脆弱性
（出典）CERT/CC「Vulnerability Note VU#799380※139」を基に IPA が作成

(3) EOL 機器の脆弱性

2021 年を通じて、各社の Wi-Fi ルータ製品等における脆弱性の発見が相次いだが、その中にはサポートが終了した EOL（End-of-life）製品が多く含まれていた（表 3-2-14）。当該製品に対するファームウェアの更新は提供されないため、緩和策が存在する機器は対策を実施し、そうでない機器は使用を中止せざるを得ない状況が発生した。

報告日	ベンダ名及び EOL 機器
2021 年 1 月 22 日※141	NEC プラットフォームズ株式会社 ・Aterm WF800HP
2021 年 1 月 26 日※142	エレコム株式会社 ・WRC-1467GHBK-A 他
	ロジテック INA ソリューションズ株式会社 ・LAN-WH450N/GR 他
2021 年 4 月 9 日※143	NEC プラットフォームズ株式会社 ・Aterm WG1200HS 他
2021 年 4 月 27 日※144	株式会社バッファロー ・WBR-B11、WBR-G54 他
2021 年 7 月 6 日※145	エレコム株式会社 ・WRC-1167FS-W/B 他 ・WRC-300FEBK 他

■表 3-2-14　脆弱性が発見された EOL 機器
（出典）各社の公開情報及び報道を基に IPA が作成

3.2.3 脆弱な IoT 機器とウイルス感染の実態

IoT 機器に対する脅威が残存し続けている中、脆弱な IoT 機器とウイルス感染の実態はどうなっているのか。

本項では、セキュリティ対策強化の取り組みの公開情報等から、脆弱なまま運用されている IoT 機器とウイルス感染の実態を考察する。

(1) 国内における実態

総務省及び NICT は、2019 年 2 月以降、インターネット接続事業者と連携し、サイバー攻撃に悪用される恐れのある IoT 機器の調査及び当該機器の利用者への注意喚起を行う取り組み「NOTICE（National Operation Towards IoT Clean Environment）※146」を継続している。2021 年 1 月以降の取り組み結果を、表 3-2-15（次ページ）に示す。

- 「NOTICE 注意喚起」（ログイン可能機器利用者への注意喚起）は、1 年間をとおしてほぼ同一の値を示しており、実態として大きな変化はないと考えられる。なお、2021 年 1 月の値のみ一時的に減少した要因は、同時期に外部から攻撃・侵入が行われ、NOTICE の調査が正常に実施できなかったことによると推測さ

れている。
- 「NICTER 注意喚起」（ウイルス感染機器利用者への注意喚起）は、2021 年 2 月末～ 4 月と 9 月下旬～ 11 月にかけて一時的な増加が見られた。これは、海外での Mirai の亜種の活動活発化を受けて、国内の脆弱な機器（脆弱性が存在するが対処方法が存在しない機器）が感染したものと考えられる。

なお、2022 年 3 月の時点で、NOTICE 参加 ISP は 69 社、調査対象 IP アドレスは約 1.12 億アドレスである。

	NOTICE 注意喚起（ログイン可能機器）	NICTER 注意喚起（ウイルス感染機器）
2021 年 1 月	1,581 件	平均 79 件／日
2021 年 2 月	1,948 件	平均 94 件／日
2021 年 3 月	1,883 件	平均 469 件／日
2021 年 4 月	1,857 件	平均 554 件／日
2021 年 5 月	1,817 件	平均 181 件／日
2021 年 6 月	1,823 件	平均 209 件／日
2021 年 7 月	1,770 件	平均 96 件／日
2021 年 8 月	1,790 件	平均 107 件／日
2021 年 9 月	1,774 件	平均 246 件／日
2021 年 10 月	1,769 件	平均 681 件／日
2021 年 11 月	1,739 件	平均 373 件／日
2021 年 12 月	1,670 件	平均 194 件／日
2022 年 1 月	1,665 件	平均 198 件／日
2022 年 2 月	1,686 件	平均 231 件／日
2022 年 3 月	1,664 件	平均 193 件／日

■表 3-2-15　国内における注意喚起の取り組みの実施結果
（出典）NOTICE サポートセンター「実施状況[※147]」を基に IPA が作成

(2) 脆弱な IoT 機器の実態

2021 年 12 月 2 日、IoT Inspector GmbH（現、ONEKEY GmbH）は、大手ベンダ 8 社の Wi-Fi ルータ 9 機種に対して、ドイツの IT 雑誌 CHIP と共同でセキュリティテストを実施した結果、合計 226 種類の脆弱性を発見したと報告した（表 3-2-16）[※148]。当該機種は、全世界で数百万台流通しており、すべてのベンダが抱えている典型的な問題例として以下を挙げている。
- 古いバージョンのオペレーティングシステム（Linux カーネル）やソフトウェアコンポーネント（標準ツールとしての BusyBox 等）を使用している。
- マルチメディア機能や VPN といったルーティング以外の付加サービスの実装も旧式である。
- 初期パスワードとして、脆弱な「admin」等が使用されている。

最も多くの脆弱性が発見されたのは、TP-Link Technologies Co., Ltd.（普联技术有限公司。以下、TP-Link 社）製 Archer AX6000 であり、同月 10 日、TP-Link 社はアドバイザリを公開して、ファームウェア更新を呼びかけた[※149]。

ベンダ名	機種名	脆弱性数
ASUSTeK	ROG Rapture GT-AX11000	25
AVM GmbH	FRITZ!Box 7530 AX	20
	FRITZ!Box 7590 AX	18
D-Link	DIR-X5460	26
Edimax	BR-6473AX	25
Linksys[※150]	MR9600	21
NETGEAR	Nighthawk AX12	29
Synology	RT2600ac	30
TP-Link	Archer AX6000	32

■表 3-2-16　セキュリティテスト実施対象と発見された脆弱性
（出典）IoT Inspector GmbH（現、ONEKEY GmbH）「WLAN-Router im Sicherheits-Check[※151]」を基に IPA が作成

3.2.4 セキュリティ対策強化の取り組み

これまで述べたように、脆弱性を有したままの IoT 機器をインターネットに接続すると、サイバー攻撃を受けてウイルス感染する脅威は残存しており、IoT 機器のセキュリティ対策強化の必要性に変わりはない。本項では、対策を検討・推進する上で参考となるセキュリティガイド等の発行状況や国内外の取り組みについて紹介する。

(1) IoT 関連セキュリティガイド等の改訂・新規発行

これまでに公開された IoT セキュリティに関するガイドラインや手引き等の改訂版、新たなガイドライン等が引き続き公開されている。2021 年以降に国内及び海外で公開された資料を、表 3-2-17（次ページ）と表 3-2-18（次々ページ）に示す。

(2) 米国 IoT 製品のサイバー・セキュリティ・ラベルの検討

2021 年 5 月 12 日、米国政府は大統領令 EO 14028「Improving the Nation's Cybersecurity」を公表した[※152]（「3.4.1 (2) Biden 政権の政策」参照）。本大統領令の Sec.4 でソフトウェアサプライチェーンの強化が挙げられ、項番（s）にて IoT 機器のセキュリティ機能とソフトウェアの開発方法について一般の人々を教育するための

プログラムを開始、項番（t）にて本命令の日付から270日以内に「消費者向けラベリングプログラムのためのIoTサイバーセキュリティ基準」を特定する、とされた。

これを受けて、NISTは、同年8月31日に草案「DRAFT Baseline Security Criteria for Consumer IoT Devices[※153]」を、同年12月3日にディスカッションペーパー「Consumer Cybersecurity Labeling for IoT Products：Discussion Draft on the Path Forward[※154]」を公開した。その後、2022年2月4日、NISTは「Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things（IoT）Products[※155]」を公開した。消費者向けに提供されるIoT製品を対象にしたラベリング制度を確立しようとする制度オーナが実際にプログラムを開発する際に考慮すべき、以下の検討事項と推奨事項を示している。

- 推奨ベースライン製品基準（2章）
- ラベリングに関する考慮事項（3章）
- 適合性評価に関する考慮事項（4章）

（3）共通ガイドラインに基づく国際間の協調

シンガポール首相官邸傘下のCSA（Cyber Security Agency of Singapore）では、IoTのセキュリティを向上する取り組みとして、消費者向けスマートデバイス機器向けのCLS（Cybersecurity Labelling Scheme）[※156]を2020年10月7日から実施してきたが、2021年1月21日、そのスコープをすべての消費者向けIoT機器に拡大した。このスキームは、ETSI（European Telecommunications Standards Institute：欧州電気通信標準化機構）が制定した欧州標準ETSI EN 303 645（CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements）に基づいている。2021年10月6日、異なる国家における重複した試験実施を削減するため、シンガポール政府とフィンランド政府は、両国が発行するセキュリティラベルを相互に承認

公開機関・団体	公開資料名	対象読者	主な内容	公開年月
経済産業省	機器のサイバーセキュリティ確保のためのセキュリティ検証の手引き[※159]	IoT機器のセキュリティ検証サービス事業者、検証依頼者（機器製造者）	検証サービス事業者の実施事項、検証依頼者の準備情報、二者間コミュニケーションにおける留意事項、信頼できる事業者の判断基準	2021年4月
総務省	ICTサイバーセキュリティ総合対策2021[※160]	IoTセキュリティ関係者	ICTインフラ・サービス（IoT・5Gを含む）に関するセキュリティ対策の総合的な推進に向けて取り組むべき課題	2021年7月
IPA	IoT開発におけるセキュリティ設計の手引き（2022年3月版）[※161]	IoT開発におけるセキュリティ設計担当者	具体的な設計手法（脅威分析、対策検討、脆弱性対策）	2022年3月
一般社団法人重要生活機器連携セキュリティ協議会（CCDS：Connected Consumer Device Security Council）	IoT機器セキュリティ要件ガイドライン2021年版：CCDS-GR01-2021 Ver.2.0[※162]	IoT機器及びシステムのサーティフィケーションプログラム[※163]申請者	IoT機器及びシステムの最低限のセキュリティ要件	2021年6月
	IoT機器セキュリティ要件ガイドライン別冊12要件における解説編 ー2021年版ー[※164]	IoT機器のユーザ企業、ベンダ企業	IoT機器のセキュリティ要件の解説（脅威の背景と事例、対応策等）	
	IoT機器セキュリティ要件_2021年版_対策方針チェックリスト_v1.0[※165]	同上	IoT機器のセキュリティ要件の対策方針チェックリスト	
一般社団法人日本クラウドセキュリティアライアンス（CSA-JC：Cloud Security Alliance Japan Chapter）	CSA IoTセキュリティコントロールフレームワーク利用ガイド バージョン2[※166]	IoTシステムの設計者、開発者、評価者	フレームワークスプレッドシートを用いたIoTシステムの評価・実装方法	2021年1月（英語版）2021年5月（日本語版）
	CSA IoT セキュリティコントロールフレームワーク バージョン2[※167]		IoTシステムの評価・実装に利用可能なセキュリティコントロール	
一般社団法人セキュアIoTプラットフォーム協議会（SIOTP：Secure IoT Platform Consortium）	IoTセキュリティ手引書Ver2.0[※168]	IoT機器の製造事業者、IoTシステムの提供に関わる事業者	IoT機器に求められるセキュリティ対策について、製品ライフサイクルの各分類における業界基準の解釈と検証結果	2022年1月

■表3-2-17　2021年以降に国内で新規公開・改訂されたIoT関連のガイドライン等
（出典）各団体の公開情報を基にIPAが作成

公開機関・団体	公開資料名	対象読者	主な内容	公開年月
ISO（International Organization for Standardization：国際標準化機構）／IEC（International Electrotechnical Commission：国際電気標準会議）	ISO/IEC 30147:2021 Internet of Things (IoT) - Integration of IoT trustworthiness activities in ISO/IEC/IEEE 15288 system engineering processes※169	IoT 製品・サービスの開発者や保守者	IoT 製品やサービスにおけるトラストワージネス※170 の実装・保守のためのシステムライフサイクルプロセス	2021 年 5 月
NIST（National Institute of Standards and Technology：米国国立標準技術研究所）	NISTIR 8259B: IoT Non-Technical Supporting Capability Core Baseline※171	IoT 機器の製造者	製造業者が製造する IoT 機器をサポートするために導入を検討すべき四つの非技術的サポート機能	2021 年 8 月
	SP 800-213: IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements※172	米国政府機関職員	IoT 機器を既存システムに統合する際に検討に資する推奨事項	2021 年 11 月
	SP 800-213A: IoT Device Cybersecurity Guidance for the Federal Government: IoT Device Cybersecurity Requirement Catalog※173	同上	詳細化された IoT 機器のサイバーセキュリティ機能と非技術的サポート機能のカタログ	2021 年 11 月
ENISA（European Union Agency for Cybersecurity/ European Network and Information Security Agency：欧州ネットワーク・情報セキュリティ機関）	Cybersecurity Certification – EUCC, a candidate cybersecurity certification scheme to serve as a successor to the existing SOG-IS v1.1.1※174	ICT 製品の製造者や提供者、ICT サービス提供者、規制当局、ICT 製品のエンドユーザ	欧州サイバーセキュリティ認証フレームワークにおける最初の候補スキーム	2021 年 5 月
ETSI（European Telecommunications Standards Institute：欧州電気通信標準化機構）	ETSI TS 103 701 v1.1.1 (2021-08): Conformance Assessment of Baseline Requirements※175	消費者向け IoT 機器の提供者及び実装者、ユーザ企業、試験実施機関等	ETSI TS 103 645 及び ETSI EN 303 645 に対応した消費者向け IoT 機器の適合性評価手法	2021 年 10 月

■表 3-2-18　2021 年以降に海外で新規公開・改訂された IoT 関連のガイドライン等
（出典）各団体の公開情報を基に IPA が作成

する覚書（MoU：Memorandum of Understanding）に署名した※157。フィンランドでは、2019 年 11 月 26 日から Finnish Transport and Communications Agency Traficom が ETSI EN 303 645 に基づくラベリングを実施しており※158、両国の間で合意が成立した。

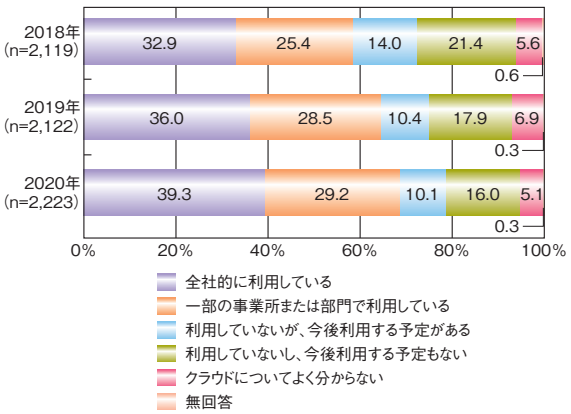
3.3 クラウドの情報セキュリティ

IT システムの利用は、組織の業務に応じたソフトウェアの開発を業務委託して個別に開発する形態から、サービスを選定し、必要な機能を必要なだけ利用するという形態に変わりつつある。その形態の一つとしてクラウドサービス（SaaS/PaaS/IaaS 等）があり、利用する組織が増加している。一般社団法人日本情報システム・ユーザー協会（JUAS：Japan Users Association of Information Systems）の「企業 IT 動向調査報告書 2021[※176]」によれば、1,142 社を対象とする調査において、パブリッククラウド（SaaS）を「導入済み」あるいは「試験導入中・導入準備中」と回答した企業が 67.2%（前年 65.9%）、パブリッククラウド（IaaS、PaaS）を「導入済み」あるいは「試験導入中・導入準備中」と回答した企業が 57.1%（前年 57.5%）となり、多くの企業でクラウドサービスへ移行している傾向が鮮明になっているという。特に SaaS については 2016 年度調査以降 5 年連続で増加傾向が見られた。更に、政府のデジタル化･クラウド化等の政策により、コミュニケーションの活性化や作業の効率化においてクラウドサービスの利用が必須となっている。しかし、クラウドサービスは利便性が高い反面、管理面で利用者・提供者の責任分担があり、提供者側の管理状況を利用者が把握しにくい、クラウド環境に精通しない利用者による設定ミスがおこる等、課題も存在する。

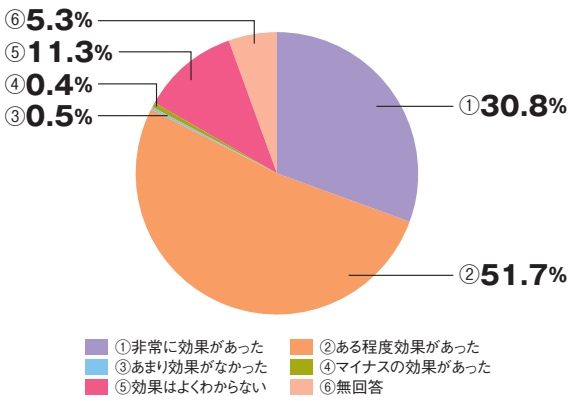
「情報セキュリティ白書 2020[※177]」の「3.4 クラウドの情報セキュリティ」では、クラウドサービス全般の情報セキュリティについて取り上げ、インシデントや対策について述べた。本節では、近年利用が急増している SaaS に焦点を絞り、SaaS 利用の現状、インシデント被害、セキュリティの課題と対策、セキュリティの政策について述べる。

3.3.1 クラウドサービスの利用状況

総務省の「令和 2 年通信利用動向調査報告書（企業編）[※178]」（以下、総務省調査）によれば、従業員 100 人以上の企業 2,223 社について、クラウドサービスを利用していると回答した割合は 68.5% で、2019 年（令和元年）の 64.5% より 4 ポイント増加した（図 3-3-1）。サービス利用の効果について「非常に効果があった」または「ある程度効果があった」と回答した企業が 8 割を超えた（図 3-3-2）。今後も企業・組織でのデジタル化の進展とともにクラウドサービスの利用は更に増加していくと考えら



■図 3-3-1　クラウドサービスの利用状況の推移
（出典）総務省「通信利用動向調査報告書（企業編）」を基に IPA が編集



■図 3-3-2　クラウドサービスの効果（n=1,595）
（出典）総務省「通信利用動向調査報告書（企業編）」を基に IPA が編集

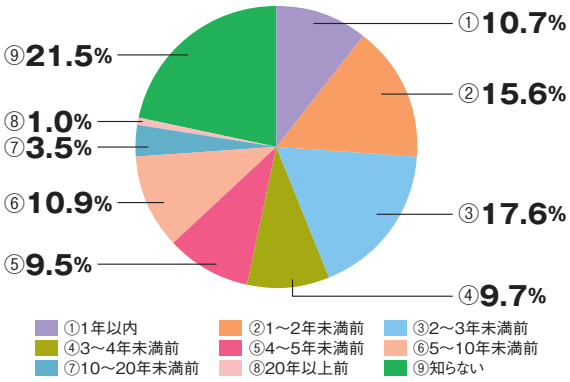
れる。

パロアルトネットワークス株式会社の「クラウドネイティブセキュリティジャパンサーベイ 2021 年版[※179]」（以下、パロアルト調査）では、国内企業のワークロード（業務量）全体の 43% がパブリッククラウド上で稼働しており、今後 2 年間で 60%に達すると予測している。この値は海外企業の回答と比べて数ポイント低いものの大きな差はなく、国内企業でのクラウド活用は一層進むと考えられている。

Gartner, Inc. の調査では、パブリッククラウドサービスへの全世界のエンドユーザの支出は、2021 年に 3,961 億ドルに達し、2022 年には更に 21.7%増加して 4,821 億ドルに達すると予測している。中でも SaaS サービスの支出は最も多く 2021 年に 1,719 億ドルと予測している[※180]。

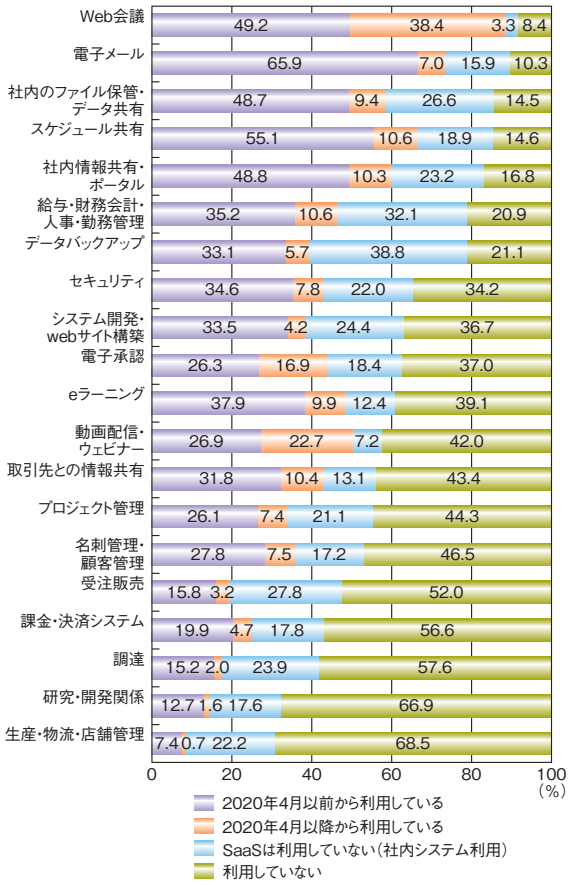
株式会社 LegalForce の国内調査「SaaS の導入実態調査（2021 年 12 月実施）[※181]」では、自部署で SaaS

を導入して 3 年未満という回答者が 43.9%（図 3-3-3）であり、新型コロナウイルス感染拡大防止や DX 推進により、SaaS の利用者が短期間に増えている様子がうかがえる。



■図 3-3-3　SaaS の導入時期（n=1,000）
（出典）株式会社 LegalForce「SaaS の導入実態調査（2021 年 12 月実施）」を基に IPA が編集

IPA が 2022 年 2 ～ 3 月に実施した「企業・組織におけるテレワークのセキュリティ実態調査※182」から、組織での SaaS の利用状況の調査結果を図 3-3-4 に示す。



■図 3-3-4　SaaS の利用状況（n=809）
（出典）IPA「企業・組織におけるテレワークのセキュリティ実態調査」を基に編集

「新型インフルエンザ等対策特別措置法に基づく緊急事態宣言」（以下、緊急事態宣言）が発出された 2020 年 4 月以前から組織が利用している SaaS サービスの割合は、「電子メール」が最も高く（65.9%）、「スケジュール共有」（55.1%）、「Web 会議」（49.2%）と続く。また、緊急事態宣言以降に利用を開始した SaaS サービスとしては「Web 会議」（38.4%）、「動画配信・ウェビナー」（22.7%）、「電子承認」（16.9%）の順であり、従来対面あるいは書面で実施されていた業務がデジタル化され、SaaS サービスの導入が進んだことが分かる。

3.3.2 クラウドサービスのインシデント被害

2021 年はクラウドサービスの利用者の設定ミスに起因するセキュリティインシデント（以下、インシデント）が多く見られた。更に、不正アクセスやクラウドの開発環境のスクリプトが改ざんされるといったインシデントも報告された。主な SaaS のインシデントの事例について以下に述べる。

(1) 設定ミスに起因するインシデント

2021 年 1 月 4 日、株式会社コナミデジタルエンタテインメント及び株式会社コナミアミューズメントにおいて、外部からの指摘によりクラウド型顧客管理システムの設定不備が発覚した※183。当該システムへのアクセスについて調査を実施したところ、個人情報データの一部に対して第三者のアクセスがあったという。

第三者のアクセスが確認された個人情報データはログイン ID、メールアドレス、電話番号であり、ログイン ID に紐づけられた個人を識別できる複合情報（氏名・住所・電話番号・メールアドレス・生年月日等）については別のシステムで管理していたため、流出の可能性はないとしている。株式会社コナミデジタルエンタテインメント及び株式会社コナミアミューズメントは 2021 年 3 月 1 日の時点で当該システムの設定変更を完了し、監督官庁へ報告を実施するとともに、個人情報データへの第三者アクセスが確認された顧客に対して順次個別に経緯・状況を説明した。更に、システムの設定変更、詳細な調査、及び監督官庁への報告を実施し、システムの設定変更後は第三者からのアクセスは確認されていないという。現状の点検と再発防止に取り組み、管理体制の強化に努めるとしている。

2021 年 2 月 9 日、神戸市が運営する情報共有アプリ「KOBE ぽすと」が保管している情報に対する外部の第三者からのアクセスが発覚した。神戸市の調査によると、

「KOBE ぽすと」が活用するクラウド型情報管理アプリケーション「Salesforce※184」の外部からの参照設定の不備と、その影響に対する認識誤りが原因であったという。第三者によるアクセスは、ログの解析結果から、5回のアクセスで延べ103件のユーザ情報にアクセスがあり、そのうち1件に個人情報（メールアドレスと生年月日）が含まれていた。神戸市は個人情報が参照された可能性がある1名にお詫びの連絡を行うとともに、二次被害等が生じていないことを確認した。また同システムの設定変更を2021年2月1日に完了し、同年2月9日の時点で問題のある状態は解消したと報告している。更に、再発防止策として委託事業者における情報収集経路、管理、共有体制の見直しの実施及びインシデント情報の収集に努める等、委託事業者と一体となってセキュリティ対策の強化を図るとしている※185。

このほか、2020年12月から2021年1月にかけては、Salesforceを利用する多くの企業、自治体等において、設定不備による意図しない情報の公開や、実際に情報が外部から参照される等のインシデントが発生した（2020年度に発生した事例については「情報セキュリティ白書2021※186」の「1.2.8 (3) 過失やシステム不具合による情報漏えい・情報紛失」参照）。

このような状況を重く見て、NISCは、2021年1月29日に重要インフラ事業者等に向けて、Salesforceの設定不備による情報流出の可能性について、サービスの利用状況や各種設定の見直し等のセキュリティ対策が必要である旨、注意喚起を行った※187。

(2) 不正アクセスに起因するインシデント

株式会社ネットマーケティング（以下、ネットマーケティング社）は2021年5月21日、同社が運営するマッチングアプリサービス「Omiai」への第三者からの不正アクセスによって、会員情報の一部である年齢確認書類画像データ（運転免許証、健康保険証、パスポート、マイナンバーカード（表面）等）171万1,756件分が流出したことを公表した※188。

不正アクセスは、2021年4月20日から4月26日の間、複数回にわたり行われ、ネットマーケティング社のAPIサーバを介し、同社が契約するクラウドサーバより年齢確認書類画像データが不正取得されていた。

調査により、第三者が年齢確認書類画像データにアクセスするための情報を不正取得し、それを利用して当該画像データへのリクエストを大量生成することで、不正アクセスに成功したものと判明した。不正アクセスの方法が正規のデータリクエストを装ったものであったため、正常なアクセスログから不正アクセスを特定する必要があり、調査に時間を要したという。

ネットマーケティング社は、不正アクセス発見後、アクセスを遮断して保有するすべての年齢確認書類画像データの安全確保措置を実施した。その後は新たな不正アクセスの痕跡は確認されていないとしている。更にシステムセキュリティ全般に対して、以下を含む再発防止対策を実施している。

- 外部ネットワークからのアクセスやリクエスト制限の厳格化
- アプリケーションの認証設定の見直し
- 保有する年齢確認書類画像データの保管場所の移動と暗号化
- アクセス制御と権限の厳格化及びパスワードポリシーの強化
- ログイン認証の厳格化と監査証跡の強化
- 社内エンドポイントへの定常的な動態調査基盤の導入
- 社内ネットワーク及びサービスやコーポレートサイト等外部公開サービスに関する脆弱性診断の実施
- 診断に基づくネットワーク構成及びアプリケーションの実装の見直しとセキュリティ強化
- 年齢確認審査業務の厳格化及び安全性向上を目的とする、オンライン本人認証サービスの導入

なお、本インシデントをきっかけとして、特定非営利活動法人結婚相手紹介サービス業認証機構では2022年3月17日にインターネット型結婚相手紹介サービス業認証制度の認証基準を一部改訂し、個人情報保護に関する認証基準の要求事項を強化したことを公開している※189。

(3) スクリプトの改ざんに起因するインシデント

2021年1月31日、Codecov LLC（以下、Codecov社）は、同社が提供するテストのコード網羅率（プログラムのソースコードが自動テストされた割合）を計測するツール「Codecov」が利用するコンテナ環境が不正アクセスされ、同ツールの利用時に実行される「Bash Uploader」スクリプトが改ざんされ、ツール利用者の情報が流出した可能性があることを公開した※190。不正アクセスされた原因は、コンテナを用いたアプリケーション作成・配布・実行のプラットフォームである「Docker」のイメージ作成時のエラーにより、スクリプトを変更するための認証情報を攻撃者に窃取されたためとしている。

本ツールを利用していた株式会社メルカリ（以下、メル

カリ社）は、2021 年 5 月 21 日に、メルカリ社が運営するフリマアプリ「メルカリ」のソースコードの一部及び一部の顧客情報等、累計 2 万 7,972 件が外部に流出したことを公開した※191。改ざんされたスクリプトを実行した際に、メルカリ社の認証情報が不正に取得、流用され、GitHub 上に格納されていた同社の情報に不正アクセスされたという。メルカリ社では不正アクセスされた全認証情報の調査及び初期化、被害状況の特定とセキュリティ強化、個人情報保護委員会等への報告を行い、流出した情報の対象者への個別案内を実施、問い合わせ専用窓口を設置したとしている。更に外部の専門企業の協力のもと、本事案の影響範囲に関する調査を実施し、2021 年 8 月 6 日に、調査の完了及び流出した情報の悪用による被害は確認されていないと報告している。

Codecov 社は、影響を受けたスクリプトを改修し、Bash Uploader に関するキーを含むインシデントに関連する既存の重要なアクセスキーを無効化し、その後も継続的な監視を行うとした。また、Codecov のバージョンの確認方法とバージョン更新方法を公開した。

(4) 複数の組織に波及したインシデント

2022 年 3 月 21 日、SB テクノロジー株式会社は、同社が構築と管理を行う「自治体情報セキュリティクラウド」のメールシステムが踏み台とされ、91 万 2,299 件の迷惑メールが発信されたと発表した※192。

同社のメール中継システムにおいて送信障害が発生し、緊急メンテナンスを行った際に設定不備があり、本来は不可能な外部から外部へのメール送信が、不正中継（オープンリレー）可能な状態になってしまった。悪意の第三者がこの不備を利用し、インターネット上で入手したと思われるメールアドレス宛に迷惑メールを送信した。大量のメールが送信されたことにより、送信元アドレスが送信先の受信拒否リストに登録され、自治体の一部のメールが送信できなくなった。

同社の運用規定では、設定を変更し有効化する際は、作業者とは別の者が問題ないことを二重チェックするルールだったが、送信障害の緊急メンテナンスにおいてはチェック体制が不十分な状態で、しかも、設定変更後の不正中継テストを実施せず、早期発見ができなかったという。不正メールの発信元に詐称されたのは、青森県八戸市、秋田県秋田市、横手市、福島県郡山市、栃木県宇都宮市、矢板市、新潟県糸魚川市、長岡市の 5 県 8 市で、同社は不正中継により送信された 15 種類のメールの件名を公開し、不審なメールを受信した人は本文中のリンクをクリックしたり、添付ファイルを開封したりせずにメールを削除するよう呼びかけた。

3.3.3 クラウドサービスのセキュリティの課題と対策

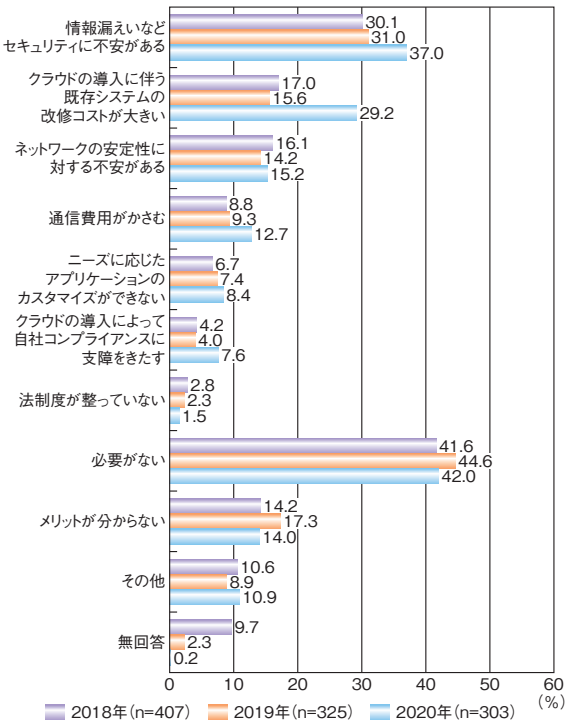
クラウドサービスの利用状況とインシデントの被害事例を基に、クラウドのセキュリティ課題と対策について述べる。

(1) クラウドサービスのセキュリティ課題

「3.3.1 クラウドサービスの利用状況」に述べたように、クラウドサービスの利用範囲や利用者数は拡大し、企業活動におけるクラウドの重要性はますます高まることが予想される。これに伴い脅威や脆弱性も増えており、セキュリティリスクの高まりが懸念される。

総務省調査では、クラウドサービスを利用しない理由として、最も多かったのは「必要がない」（42.0%）であったが、次いで多かったのは「情報漏えい等セキュリティに不安がある」（37.0%）で、この値は、年々高くなっている（図 3-3-5）。導入が更に進むと考えられるクラウドサービスを安全・安心に利用するためにセキュリティ対策の実施が求められる。

企業・組織において、許可されていない端末やクラウドサービス利用（シャドー IT）は大きなリスク要因となり得る。キヤノンマーケティングジャパン株式会社が 2021 年



■図 3-3-5　クラウドサービスを利用しない理由（複数回答）
（出典）総務省「通信利用動向調査報告書（企業編）」を基に IPA が編集

4 月に実施した「情報セキュリティ意識に関する実態調査レポート※193」によれば、勤務先で許可が得られていないクラウドサービス・アプリを業務で利用することについて「許可がないものは利用しない」とする回答が 47.7%（2019 年調査 47.0%）、「許可がなくても問題ない」が 11.7%（2019 年調査 13.1%）、「勤務先が用意していないためやむを得ない」が 12.2%（2019 年調査 13.6%）であった。また、個人的に登録あるいは契約（有償・無償問わず）して業務で利用しているシャドー IT が「ある」が 27.3%（2019 年調査 25.3%）、「ない」は 55.3%（2019 年調査 61.0%）であった。

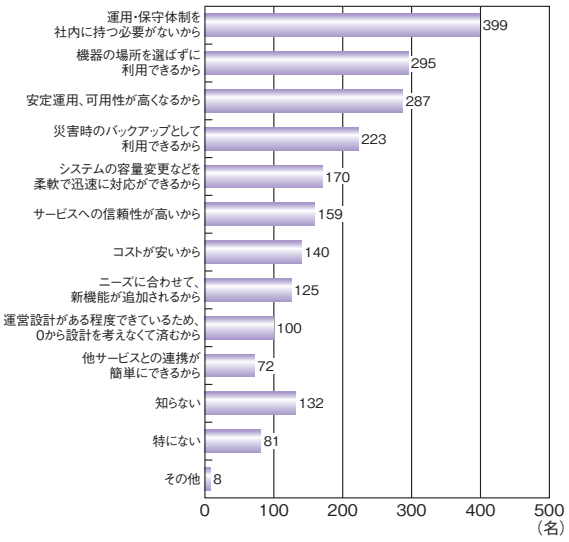
2019 年調査と比較して、シャドー IT の利用は問題であるという認識は高まっているが、「シャドー IT を利用している」とする回答も 2 ポイント増えている。2021 年調査はコロナ禍の最中に行われており、テレワークやオンライン会議等の急激な ICT 環境の変化にルール見直しや従業員への研修等組織的な対策の準備が間に合わず、シャドー IT が利用されてしまっている可能性がある。

また 2021 年調査では回答者の 41.7% はコロナ禍によって情報セキュリティの意識が高まったとしている。一方で、過去 1 年間の情報セキュリティ研修や勉強会の「実施（参加）」は 22.7%（2019 年調査　29.4%）、「実施なし」は 54.7%（2019 年調査 45.3%）であった。セキュリティ知識やスキルを学ぶ機会が減り、適切な行動がとれないことによるリスクの高まりを示唆していると考えられる（シャドー IT の対策については「情報セキュリティ白書 2020」の「3.4 クラウドの情報セキュリティ」参照）。

(a) サービス利用者の責任分担

パロアルト調査によれば、自社のクラウド環境におけるセキュリティの脅威・懸念で最も多いのは「情報流出」（45%）、次いで「マルウェア」（12%）、「アプリケーションの脆弱性」（10%）という結果であった。情報流出は社会的信用の失墜等、企業価値に大きく影響することから、特に、懸念が大きいと思われる。これらの懸念は、クラウドサービスだけでなく、自社に設置し運用するオンプレミスシステム（以下、オンプレミス）でも懸念されることである。しかし、クラウドサービスの場合は、サービス利用者が管理する範囲が限られ、どのようなセキュリティ対策がされているのか詳細に把握することが難しい、自社のセキュリティポリシーに従った対策（例えば、サービス事業者への監査や検査報告のチェック等）がとりにくいといった課題がある。また、サービス利用者とサービス事業者の責任範囲（責任分界点）について双方の認識に差が生じ、必要な対策が取られないことがある、という課題もある。特に SaaS の場合は、施設やハードウェアからアプリケーションに至る全般的なセキュリティ対策をサービス事業者に任せるため、サービス利用者にもデータやアカウント管理、更には環境の設定に責任があるという意識が希薄になりがちであり、サービス利用者側の体制も十分でない可能性がある。

株式会社 LegalForce の「SaaS の導入実態調査（2021 年 12 月実施）」では、最初に導入した SaaS の導入理由として回答者の約 4 割が「運用・保守体制を社内に持つ必要がないから」と回答した（図 3-3-6）。



■図 3-3-6　最初に導入した SaaS の導入理由（n=1,000、複数回答）
（出典）株式会社 LegalForce「SaaS の導入実態調査（2021 年 12 月実施）」を基に IPA が編集

しかし、システムやソフトウェアの運用・保守の必要がなくても、サービス利用者はデータやアカウント管理、環境設定、シャドー IT 対策を含む利用ルール作り、教育等を行う必要がある。シャドー IT は、組織的な管理対象に含まれないため、監視やアカウント管理ができず、インシデントの発生に気が付くのが遅れたり、原因が追跡できなかったりする等により、影響が大きくなる可能性がある。

「3.3.2（1）設定ミスに起因するインシデント」の Salesforce の事例では、サービス利用者が実施するべき設定の変更がなされなかったことが情報流出の原因であった。サービス事業者はサービス利用者向けに設定の変更方法について公開をしていたが、複数のサービス利用者が対応の必要性を認識していなかった。この事例により、サービス利用者とサービス事業者のセキュリティに関する責任分担が SaaS においても重要であるこ

とが再確認された。

(b) サービス事業者のサプライチェーンセキュリティ

サービス事業者は、セキュリティ対策についてアプリケーション種別ごとの多様なセキュリティ要件や攻撃を想定する必要があり、高度な対策が求められる。SaaS 市場は拡大しつつあり、短期間に多様なサービスを構築し、提供するため、オープンソースソフトウェア（OSS：Open Source Software）の利用や他社サービスとの連携、製品の調達等が不可欠となっている。この点ではサービス事業者は、サービス利用者の側面を持ち合わせており、SaaS の開発・運用におけるサプライチェーンが形成されている。一つのサービスにおいても複数の OSS やサービスが利用・連携されうることから、サプライチェーン全体は複雑なものとなる。一般に、システム開発において再委託先以降の状況把握は困難であるが、SaaS においては OSS 利用やサービス連携も自社の管理下にはないため、更に状況把握が必要である。また、OSS や他社サービスは機能改修や脆弱性対応等で日々アップデートされることから、サプライチェーン上の関係する組織間での情報共有、正確でタイムリーな情報管理等の活動が重要となる。

このようなサプライチェーン上のインシデントは原因の把握、影響範囲の特定等が困難であり、大きな被害につながる恐れがある。被害範囲の最小化、迅速な復旧のための対策も課題である。

(2) クラウドセキュリティの対策

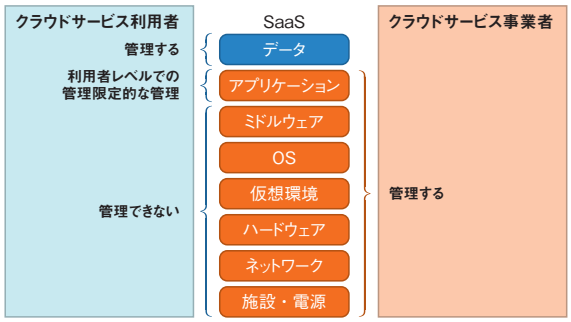
サービス利用者、サービス事業者が各々実践すべき、あるいは協力して取り組むべきクラウドサービスのセキュリティ対策について述べる。

(a) 責任共有モデルの実践

「3.3.3 (1) (a) サービス利用者の責任分担」でも記載したようにクラウドサービスを利用することにより、サービス利用者の責任範囲は狭くなるが、サービス事業者との間で責任を分担し、ともにその責任を果たすことが求められている。

総務省の「クラウドサービス提供における情報セキュリティ対策ガイドライン（第 3 版）※194」では、SaaS における管理と責任共有について説明している（図 3-3-7）。

図 3-3-7 によれば、サービス事業者は、契約（約款）や SLA ※195 等に基づくサービスを提供するために、施設・電源からアプリケーションまでの実装、設定、更新、



■図 3-3-7　SaaS における管理と責任共有
（出典）総務省「クラウドサービス提供における情報セキュリティ対策ガイドライン（第 3 版）」

及び運用の管理責任を有する。

これに対して、サービス利用者はアプリケーションを利用するためのデータやアプリケーション上で生成されたデータの管理（データに対する編集・削除等の行為）をする権限と責任を有する。

また、アプリケーションについてはサービス利用者がアカウント権限の設定をする場合がある。サービスの利用にあたっては、誰が、どのサービスで、何をすることができるかといった利用者権限の決定とサービス上の設定、そして、その内容が適切に維持されているかの見直しをすることが大切である。

Salesforce の事例では、サービス事業者からサービス利用者が実施するべき設定確認と変更方法について情報提供がされていた。しかし、サービス利用者には他社の情報も含めて日々多くの情報提供がされており、情報流出等のインシデントを防ぐための対応についての情報であることを認識することは困難であった可能性がある。

サービス利用者は SaaS 導入時にはサービス事業者と契約（約款）を取り交わすが、利用経験の浅い利用者には内容が難解で十分理解できない、あるいは、契約時点で情報システムや法務の担当者が確認しただけで、利用する従業員に周知されないといったこともありうる。サービス利用者は、クラウドサービス利用上の注意を周知するとともに、サービス事業者もサービス利用者の責任分担について契約等で明確にする、脆弱性情報のリスクを分かりやすく説明する、等の配慮が必要である。

サービス利用者は、サービス事業者から提供される情報に適切に対応するよう注意を払うことが必要である。例えば、SaaS サービスを基幹業務で利用し、顧客情報や営業秘密等重要な情報を取り扱う等の場合には特に注意を払い、望ましい設定やリスクの大きさが分からな

ければサービス事業者に確認する等、リスクに関する理解度を高めることも必要である。

サービス事業者は、アプリケーションのバージョンアップや機能追加の情報セキュリティへの影響や対策をサービス利用者が理解できるように、サービス利用者に適切な情報提供を行う必要がある。また見落としを防ぐために、提供する情報の重要度の表示の仕方を工夫したり、適切な設定がされない場合のリスクを説明したりといった情報提供の工夫が求められる。

(b) 利用者のアカウント管理

IBM Corporation が 2020 年 7 月から 2021 年 7 月にかけて複数のダーク Web 市場を調査した結果、約 3 万件のクラウドサービスのアカウントが、1 件あたり数ドルから、1 万 5,000 ドル以上の売値で取り引きされていたという※196。株式会社東京商工リサーチの集計によると、国内では、2012 年から 2021 年までに上場企業とその子会社が公表した漏えい・紛失の可能性がある個人情報は、累計 1 億 1,979 万人分に達したとされる※197。これらの個人情報にはメールアドレス、ログイン ID 等が含まれており、アカウントの悪用に使われた恐れがある。

正規のアカウントが悪用された場合、システム側が攻撃者と利用者を判別することは困難である。そのため、不正入手したアカウントを利用してクラウドに侵入しシステム内の重要な情報を窃取し、更に大量の情報漏えいやウイルス感染、踏み台による大量のメール送信等のインシデントを引き起こす可能性がある。SaaS サービスの場合、アカウント情報を窃取されるとインターネット上のどこからでもサービスにアクセスされる恐れがあり、注意が必要である。

アカウント情報は必要な人に必要な範囲で付与し、使いまわしをせず、十分に長いパスワードで利用する等のアカウント管理の基本的な対策を徹底することが必要である。またアカウントの管理方法については社内ルールを定め、守られていることを定期的に確認することが望ましい。特に、機密性の高い情報へのアクセスや操作が可能なアカウントについては、利用方法や利用手順等独自のルールを定め、不正な利用であるか否かを判別できるようにする工夫も考えられる。

(c) クラウドサービスのセキュリティ認証※198

クラウドサービスの導入を検討する際、サービス事業者の Web サイトやカタログだけではどのようなセキュリティ対策が取られているのかが読み取れないことも多い。

セキュリティ対策の内容についてサービス事業者に照会することも可能であるが、多くの利用者の問い合わせにサービス事業者が迅速に対応することは困難である。このような場合、サービス事業者がセキュリティ認証を取得していればこれを参考にできる。

サービス事業者はセキュリティ認証を取得することにより、ある基準に適合していることを客観的に示すことができ、そのサービスの利用を検討する組織に求めるセキュリティ基準を満たしているかの判断材料を提供できる。

サービス利用者はセキュリティ認証を参考にすることで、顧客情報を預けるような SaaS サービスについて、セキュリティ面で事業者は十分な準備をしているか等の判断が容易になる。

セキュリティ認証としては ISMS（Information Security Management System）が国内では知られているが、クラウドサービスに特化した認証制度もある。「情報セキュリティ白書 2020」の「3.4 クラウドの情報セキュリティ」では JASA - クラウドセキュリティ推進協議会（JCISPA：JASA -Cloud Information Security Promotion Alliance）が認証する CS マーク※199 と ISO/IEC 27017 のクラウドセキュリティ認証※200 を紹介している。「政府情報システムのためのセキュリティ評価制度（ISMAP）」も新しい制度として今後参考となる（「2.7.3 政府情報システムのためのセキュリティ評価制度（ISMAP）」参照）。

また、一般社団法人日本クラウド産業協会※201 では、サービス事業者が安全・信頼性に係る情報を適切に開示していることを認定する制度を運用している。この制度では総務省等が定めた各種ガイドライン、「クラウドサービスの安全・信頼性に係る情報開示指針※202」（以下、情報開示指針）を基に認定を行っている。

なお、情報開示指針は、利用者によるクラウドサービスの比較・評価・選択等を容易にすることを目的として総務省が発行しており、2022 年 2 月に追加された「AI を用いたクラウドサービスの安全・信頼性に係る情報開示指針（ASP・SaaS 編）」を合わせ、八つの分野の情報開示指針からなる※203。サービス事業者は情報開示指針を基に開示項目を整理し、公表することにより、クラウドサービスの安全・信頼性を示すことができる。サービス利用者は、セキュリティ認証による確認ができなかったサービスの対策について、サービス事業者に問い合わせ等を行う際に同指針を参考にできる。

(d) クラウドサプライチェーン上の情報共有

2021 年の IBM Corporation の調査※196 によれば、

クラウドに展開されているアプリケーションの脆弱性は、直近の 5 年で 150% 増加し、2,500 を超えているという。サービス事業者は、開発段階で既知の脆弱性について対策を行うが、日々報告される新たな脆弱性に対応しなければならない。同様にサプライチェーン上で連携している他のサービスや利用している OSS・パッケージ等にも脆弱性が発見される可能性がある。クラウドサービスは SLA に基づき可用性が重要視されることから、発見された場合は限られた時間内での確実な対応が要求される。SaaS サービスにおいては、システムがどのようなソフトウェアやサービスで構成されているか、調達したソフトウェアがどのような出自であるかを把握し、それらに関する脆弱性情報を速やかに入手し、対応の検討ができる体制をサプライチェーン上の開発企業やコミュニティ等と協力して整えることが必要である。

OSS の管理については、経済産業省が 2021 年 4 月に公開した「OSS の利活用及びそのセキュリティ確保に向けた管理手法に関する事例集※204」が参考になる。当事例は自動車、製造、保険、情報サービス等 15 社のヒアリングと 3 件の文献調査が詳細されており、Software Bill of Materials（SBOM：ソフトウェア部品表）※205 の利用等、今後利用が広がると思われる活動についても触れられている。

3.3.4 クラウドの情報セキュリティに対する政府の取り組み

クラウドサービスのセキュリティ対策を促進するために、政府機関は「3.3.3 (2) (c) クラウドサービスのセキュリティ認証」で挙げた「クラウドサービスの安全・信頼性に係る情報開示指針」を始めとして、多くのガイドラインや基準を発行している。ここでは、2021 年度に発行や改版が実施されたガイドライン及びガイダンスについて述べる。

総務省では安全・安心なクラウドサービスの利活用推進のため、クラウド事業者が実施すべき情報セキュリティ対策やサプライチェーンにおける実施ポイントをまとめた「クラウドサービス提供における情報セキュリティ対策ガイドライン」を 2014 年に策定した。本ガイドラインは、クラウドサービスにおける責任分界の在り方や国際規格等との整合性の観点から見直され、2021 年 9 月に 3 版に改定されている※206。改定のポイントは以下の 3 点である。

① SaaS/PaaS/IaaS の特性や、クラウドサービス提供におけるクラウドサービス同士の相関性を踏まえた責任分界の在り方を追記

②ガイドラインの章構成を以下の三つのパターンに整理する形で見直し

- 共通編：SaaS/PaaS/IaaS を提供するクラウドサービス事業者で共通的に実施が求められる情報セキュリティ対策
- SaaS 編：SaaS を提供するクラウドサービス事業者に実施が求められる情報セキュリティ対策
- PaaS/IaaS 編：PaaS/IaaS を提供するクラウドサービス事業者に実施が求められる情報セキュリティ対策

③国際規格（ISO/IEC 27017:2016）や NIST SP800-53 rev.5 のセキュリティ対策と整合

NISC は、クラウドサービス利用者のインシデント抑制やインシデント対応等を取りまとめた「クラウドを利用したシステム運用に関するガイダンス※207」を 2021 年 11 月に公開した。本ガイダンスは、「サイバーセキュリティ戦略」（2021 年 9 月 28 日閣議決定）の方針を受けて、クラウドサービスの選定や利用、サービス環境の構築や運用等にあたり、インシデントの抑制、インシデント対応及びステークホルダーとの連携の重要性等、クラウドサービスの安全な運用に重点を置いた利用者向けのガイダンスである。

今後も利用の増加が想定されるクラウドサービスを安全に利用するためには、サービス利用者は契約や運用にあたり、セキュリティ要求を満たしていることが確認できる制度やガイドライン等を活用し、組織がクラウドを利用する目的に見合ったセキュリティ対策を実施していくことが重要である。また、サービス事業者は、サービス利用者に向けた適切な情報開示を行い責任範囲の理解と対応を促すとともに、サプライチェーン全体でのセキュリティレベルの向上を目指した連携や情報共有を進めていくことが期待される。

COLUMN

DXとセキュリティの相性は悪いのか

DX（デジタルトランスフォーメーション）のセキュリティとはなんでしょうか。何をしなければいけないのでしょうか。業務デジタル化のセキュリティ、つまりセキュアなデジタルプラットフォームの構築が大事なのでしょうか。いやいや、トランスフォーメーション、すなわち変革による価値創造がDXのコアであり、そこで重要なのはデータ分析であるから、データセキュリティこそが大事なのでしょうか。

どちらも重要そうに見えます。IPAの発行した「DX実践手引書ITシステム構築編[i]」では、企業・組織が構築するDXシステムのセキュリティに関して、以下の4点が強調されています。

①対策は多層的に行うことを認識し、クラウド等外部サービスとの責任分担を明確化する。
②守るべき資産（データとシステム）を明確化し、資産の重要度に基づいた対策・データ共有を実施する。
③開発では設計時からセキュリティ機能の作りこみを行い、開発環境もセキュアに保つ。
④データはセキュリティに加え、プライバシー・コンプライアンスルールに基づいた管理を行う。

この4点はDXシステムの基盤構築、及びそこで扱うデータの管理についてセキュリティの大原則として挙げられていますが、DXだから特別に対応が必要というものではありません。むしろ、これまで言われてきた対策をDX化において再確認する、ということかもしれません。

しかし、この原則に基づいて対策を実践するのは容易なことではないでしょう。もしDXが「新たな価値を創出するビジネス形態への変革」を目指すものであるなら、そこでは「現行ルールとの不整合」や「試行錯誤」が多く発生する可能性があります。例えば、事業部門を横断したデータの統合分析を行おうとしたが守秘義務規定でできない、あるいは秘密管理規定が事業部で異なり共有できない等の問題は、いろいろな組織でありそうです。あるいは新たにデータを収集して分析を行う場合、どんなデータが付加価値を生むのか、何が重要で何が不要か、最初は分類できないかもしれません。このことは更に、組織外とのデータ授受や統合においてデータの信頼度が分からない、というサプライチェーン問題に発展し、DXで意図した外部連携ができない可能性も出てきます。

現行規則を杓子定規に適用するとDX化をなかなか進めることができない、一方で、セキュアなDXプラットフォームを作らなければいけない、というジレンマは、今後（あるいは現在）多くの組織が直面する問題かもしれません。しかし、DXで業務革新を狙うとすれば、セキュリティに限らずこうした摩擦はあるでしょう。まずセキュリティ上問題の少ないデータでトライアルを行い、どのような価値創造が見込めるかに加え、セキュリティやコンプライアンス上でどんなルールがあるべきかを具体化することが必要かもしれません。セキュリティ責任者は、求めるベネフィットに対してセキュリティリスクをどこまで統制するか、DX化に関わる他部門の責任者とともに知恵を出し合うことが重要であると思われます。

i　https://www.ipa.go.jp/files/000094497.pdf〔2022/6/8確認〕

3.4 米国・欧州の情報セキュリティ政策

2021 年度は、新型コロナウイルス感染によるパンデミックや情報の混乱（インフォデミック）が徐々に収束に向かう一方で、ロシアのウクライナ侵攻による新たな緊張が生まれ、国際社会は武力と情報が組み合わされたハイブリッドな紛争、冷戦時代を想起させる国家間の分断に直面した。分断や対立における虚偽情報拡散のリスクも顕在化した。

このような状況下で、米国と欧州のサイバーセキュリティ、データ保護や安全保障に関する政策がどのようなものであったかについて紹介する。

3.4.1 米国の政策

2020 年後半から 2021 年前半にかけ、米国は SolarWinds Worldwide, LLC のネットワーク管理システムの脆弱性を突いたサプライチェーン攻撃、Colonial Pipeline Company（以下、Colonial 社）のパイプラインシステムを狙ったランサムウェア攻撃等が相次ぎ、Biden 政権は 2021 年早々から政府機関・重要インフラへのサイバー攻撃対策に取り組み、国立標準技術研究所（NIST：National Institute of Standards and Technology）によるソフトウェア調達セキュリティガイドライン策定、サイバーセキュリティ・インフラセキュリティ庁（CISA：Cybersecurity and Infrastructure Security Agency）を始めとする連邦政府機関のランサムウェア対策強化等を指示した。

サプライチェーンリスクについては、2021 年度に引き続き中国対策が懸案となり、環太平洋・インド洋を包括する安全保障の枠組みをインド・オーストラリア・日本・英国等と構築する等、中国への対抗姿勢を鮮明にした。また人権問題への抗議から北京 2022 オリンピック・パラリンピック冬季競技大会に対して外交的ボイコットを行った※208。しかし、2021 年秋以降のウクライナ危機により、中国への対応は抑制的になっている。

対中国戦略重点化のために修復が望まれたロシアとの関係は、上記のウクライナ危機で急速に悪化し、2022 年 2 月 24 日にウクライナ侵攻が開始されると、1962 年のキューバ危機以来といえる状況にまで険悪化、核兵器の使用さえ想定される事態となった。サイバーセキュリティの視点では、侵攻以前に米国が描いていた「安全でオープンなサイバー空間の構築」という構想が崩れ、ロシア対ウクライナとそれを支援する北大西洋条約機構（NATO：North Atlantic Treaty Organization）諸国及び民間組織、という構図でサイバー空間上の情報戦が一気に拡大するという未曽有の事態となった。

本項では、このような状況下で推進された米国政府のサイバーセキュリティ政策について述べる。

(1) 米国重要インフラに対する脅威の動向

以下では 2021 年に入って発覚した Microsoft Exchange Server 事案、Colonial Pipeline 事案について述べる。この 2 事案いずれも、米国の敵対的勢力とみなされる中国・ロシアが支援したとされている。

(a) Microsoft Exchange Server 事案とその対応

2021 年 3 月 2 日、Microsoft Corporation（以下、Microsoft 社）は、中国に支援された攻撃者グループ Hafnium がオンプレミス用メールサーバソフトウェア Exchange Server の脆弱性を突いた標的型攻撃を行っているとし、緊急セキュリティ更新プログラムをリリースした。米国政府も 3 月 3 日、CISA が政府機関に対して緊急指令を発してパッチ適用を指示する※209 とともに、17 日に国家安全保障局（NSA：National Security Agency）主導のサイバー統合調整グループ UCG（Cyber Unified Coordination Group）を招集、中小企業の対策・調査にあたり、サイバー防御において民間との連携を強化する、とした※210。この攻撃は「ProxyLogon」と呼ばれる脆弱性を突いたもので、米国のみで数万企業にメール窃取等の影響が及ぶと懸念された。

2021 年 7 月 19 日、Antony Blinken 国務長官は、上記の攻撃は中華人民共和国国家安全部（MSS：The Ministry of State Security）によるものと断定、MSS は「ハッカーのエコシステムを結集して攻撃を実施、知的財産の窃取やランサムウェア身代金等による多大な金銭被害が出ている」と中国を非難した※211。また、同年 8 月に Exchange server の他の脆弱性が Microsoft 社から公開された（「1.2.5 (2) Microsoft 製品の脆弱性を対象とした攻撃」参照）が、大規模な攻撃被害は報告されていない。

(b) Colonial Pipeline 事案とその対応

2021 年 5 月 7 日、米国の石油パイプライン事業最大

手であるColonial社は、サイバー攻撃による操業の停止を発表※212、翌8日にはランサムウェア攻撃を受けたことを認めた。米国東部地域に深刻な石油不足の懸念が生じ、Joseph Biden大統領は10日、「影響を緩和する措置をとり、攻撃を阻止し、攻撃者を訴追する」と言明した。またFBI（Federal Bureau of Investigation：連邦捜査局）はRaaS（Ransomware as a Service）をビジネスとする東欧系ハッカー集団DarkSideによる攻撃であることを確認した※213。更にBiden大統領はロシアが一定の責任を負うとコメントしたが、名指しされたDarkSideは、攻撃の目的は金銭であり、政治的意図はないと発表した※214。11日、FBIとCISAは更なるランサムウェア攻撃への対処について注意喚起を行った※215。Colonial社はパイプラインの再稼働を12日から始めるとし※216、燃料不足の懸念は沈静化した。身代金については500万ドル相当の支払いがあったと報じられ※217、Colonial社のCEOも「早期復旧のために支払った」ことを認めた※218。

身代金は暗号資産で支払われたため、FBIは送金記録の残るブロックチェーン上で追跡を試みた。6月7日、司法省（Department of Justice）は「FBIが身代金を受け取るビットコインウォレットのロックを解除する鍵を入手し、200万ドル以上を回収した、と発表した※219。どのように鍵を入手したかは不明だが、ロシアが支援したとされるランサムウェア攻撃で、半額に近い身代金を短期に回収したことは、FBIの追跡能力を示すこととなった。

またこの経験から暗号資産追跡の重要性が認識され、2021年10月、州を越えてビジネスを行う事業者が身代金を支払った場合、48時間以内に国土安全保障省（DHS: Department of Homeland Security）に届け出ることを義務化する法案（Ransom Disclosure Act）が米国議会に提出された※220。セキュリティ関係者は同法案について、政府のランサムウェア対策のために重要だとする一方、被害企業にとっては情報開示に対する抵抗感が大きいとの懸念も示している※221。

（2）Biden政権の政策

前節のとおり、米国の重要インフラへのサプライチェーン攻撃・ランサムウェア攻撃は現行の対策の大幅な強化を迫っている。Biden政権は2021年当初より矢継ぎ早にセキュリティ関連の大統領令を発し、対策の強化を図った。以下では主要なセキュリティ施策について述べる。

（a）大統領令と覚書

2021年4月15日、Biden大統領はSolarWinds事案の調査結果を受け、攻撃を支援したとされるロシアに対する制裁措置に関する大統領令に署名した※222。同大統領令では、SolarWinds事案や米国に対する選挙妨害活動が、ロシア対外情報庁（SVR：Sluzhba vneshney razvedki Rossiyskoy Federatsii）によるものとし、協力したロシア企業6社を特定、またロシア政府と米国金融機関の取り引きを一部停止するとした。Donald Trump前大統領はロシアの関与を認めていなかったが、明確な方針転換となった。一方ロシア政府は同事案への関与を否定、報復措置を取るとした※223。

2021年5月12日、Biden政権はSolarWinds事案に対応してサプライチェーンセキュリティ強化を目指した大統領令（以下、EO 14028※224）を発表した。内容は「情報セキュリティ白書2021」の「2.2.2（7）Biden政権の政策」で詳述したが、重要な点を再掲する。

- 官民の脅威情報共有の障壁除去
  政府システムにおける民間プラットフォーム調達が拡大する中で、調達契約においてセキュリティ情報を共有する方策を明確にする。既存の枠組みである業界単位のISACs（Information Sharing and Analysis Centers）、コミュニティ単位のISAOs（Information Sharing and Analysis Organizations）による情報共有体制が十分でないとの認識があると思われる。
- 連邦政府セキュリティの現代化（Modernization）
  Trump政権時代からの懸案である政府システムのセキュリティ対策刷新のため、ゼロトラストアーキテクチャの実装、政府共通のクラウドセキュリティ戦略等を新たに求める。政府調達クラウド認証制度FedRAMP（Federal Risk and Authorization Management Program）の現代化も行う。
- ソフトウェアサプライチェーンセキュリティの強化
  重要（Critical）なソフトウェアのセキュア開発・調達に関して、NISTを中心とした新たなガイドラインの1年以内の策定を求める。ガイドラインにはチェック自動化、SBOM等の項目も含まれる。このほか、消費者向けIoT機器のセキュリティ対策情報を利用者に提供する消費者向けラベリングプログラムの実施を求める。

ランサムウェア対策について、Biden政権は2021年5月以降、犯罪者ネットワーク・資金源の遮断・国際連携に関する下記の四つの重点施策を打ち出し、関係政府機関に実践させた※225。また、監視等のセキュリティ

対策はCISAに委ねた。CISAの活動については「3.4.1(2)(c)CISAの施策」で述べる。

- 攻撃者・支援者ネットワーク、資金源の分断
  財務省と司法省は、違法な取り引きに関与した暗号資産交換事業者(SUEX OTC, S.R.O.)を特定し、関係する資産移動を遮断する措置を発動した※226。
- 重要インフラ事業者等のセキュリティ強化
  Biden大統領は2021年7月、重要インフラ事業者と政府の連携を推進する「産業制御システムサイバーセキュリティイニシアティブ(ICS Initiative)」を正式に立ち上げた※227(同年4月からの試行については「3.1.3(2)米国Biden政権の取り組み」参照)。DHSの米国連邦航空省運輸保安局(TSA:The Transportation Security Administration)は、重要なパイプライン所有者・運用者にセキュリティ対策強化を指示した。またNSA、国防総省(DoD:Department of Defense)のサイバー軍(CYBERCOM:US Cyber Command)はランサムウェアのインテリジェンス情報を民間に提供した。
- 資金洗浄・テロ支援への対応
  財務省は前掲の暗号資産交換の監視とともに、同省の金融犯罪取締ネットワーク(FinCEN:Financial Crime Enforcement Network)により、金融不正に関するインジケータ・類型に関する情報共有を主導した。
- 国際連携による犯罪エコシステム分断とセーフハーバーの解消
  Biden政権はG7、NATO諸国やFATF(Financial Action Task Force)※228と協調して政府の能力向上とセーフハーバー排除を進め、またロシア政府とランサムウェア対策専門家討議を実施することで合意した(2021年10月時点)。

更に2022年1月19日、Biden大統領は国家機密・軍事情報を扱うセキュリティシステム(NSS:National Security System)へのEO 14028実装に関する覚書に署名した※229。同覚書により、Paul Nakasoneサイバー軍司令官がナショナルマネージャーとしてNSS所管組織の統括権限を持つこととなり、政府機関の統制が強化された※230。

(b)NISTの施策

NISTはDHS配下で計測に関する技術研究、標準規格策定を担う機関である(「情報セキュリティ白書2021」の「3.4 NISTのセキュリティ関連活動」参照)が、前掲のEO 14028の要請を始め、政府のサイバーセキュリティ対策の具現化に重要な役割を果たしている。主な活動を以下に示す。

(ア)セキュアなソフトウェア調達のための施策

EO 14028により、NISTは①重要インフラ事業者等が用いる重要ソフトウェア(Critical software)の評価、②ソフトウェアサプライチェーンのセキュリティ評価、③消費者向けラベリングプログラムのためのIoTサイバーセキュリティ基準、等の方式策定を求められた。

①について、NISTは2021年6月24日に重要ソフトウェアの定義を※231、7月8日に重要ソフトウェアのセキュリティ評価手法※232を公開した。また②について、2021年6月2～3日にワークショップを開催、ソフトウェア開発ライフサイクル全般にわたるセキュリティを検討し、2022年2月4日に利用者向けの「ソフトウェアサプライチェーンセキュリティガイダンス※233」、開発者向けの「セキュアソフトウェア開発フレームワークVer.1.1(NIST SP800-218)※234」を公開した。このフレームワークでは、ソフトウェア開発で必要性が論じられてきたSBOMの利用が例示されている。連邦政府の重要ソフトウェア調達者、開発ベンダは上記フレームワークをツールとしてセキュリティを確保することが求められる。

また③について、NISTは2021年12月3日、セキュリティラベリングの討議ドラフトを公開した※235。消費者の知識不足、IoT機器の多様性等の課題が論じられたが、2022年2月4日にラベルの設計、消費者教育等に関する推奨事項を公開した※236。同年5月10日、NISTはラベリングプログラムの概要を国家安全保障担当大統領補佐官(APNSA: Assistant to the President for National Security Affairs)に提出した※237。

(イ)サプライチェーンセキュリティ関係活動の強化

他のサプライチェーンセキュリティ関連活動も強化されている。2021年8月25日、NISTは「サプライチェーンセキュリティに関する官民を推進する国家イニシアティブ(NIICS:National Initiative for Improving Cybersecurity in Supply Chains)」を設置した。Biden政権の官民連携強化の姿勢に応えたものといえる。続いて10月28日、サプライチェーンリスクマネジメントの標準ガイドであるNIST SP800-161の改訂ドラフトが公開され※238、更に2022年2月18日、サプライチェーンセキュリティ、及びサイバーセキュリティフレームワークに関する意見募集が公表された※239。この意見募集は、

NIICSの官民連携の方策、及びNISTサイバーセキュリティフレームワーク1.1版の強化や他のリスクマネジメントガイドとの整合に関する意見を求めるものである。サイバーセキュリティフレームワークへの意見募集では、特にサプライチェーンセキュリティ対応でどのような改訂がなされるか、注目される。

(c)CISAの施策

CISAはEO 14028を含むBiden政権のサイバーセキュリティ政策の実装、普及を主導している。

(ア)EO 14028の実装

EO 14028の要請については、CISAは以下のような活動を行っている※240。

- 連邦政府セキュリティの現代化に関するクラウドセキュリティの強化支援
- ソフトウェアサプライチェーンセキュリティガイド策定に関するNISTの支援
- 政府機関を監督するサイバー安全レビューボードの設置
- 政府機関向け脆弱性・インシデント対応手順書の策定

(イ)ランサムウェア対策

CISAはFBI等と連携し、国内組織へのサイバー攻撃監視・犯罪者集団の動向追跡、及びアラート・注意喚起・対策指示を行っている。2021年4月以降のランサムウェア関連のアラート・注意喚起には、同年5月のColonial社を攻撃したDarkSideの脅威※215、同年6月のOTシステム資産防御のためのファクトシート※55、同年9月と2022年3月のロシア系ハッカー集団Contiの脅威※241、2021年10月の上下水道システムへの脅威※7(「3.1.1 (1) 水道やパイプライン等の重要インフラが標的となった事例」参照)、同月のBlackMatterの脅威※242等が含まれる。

なお、制御システムのセキュリティ対策については「3.1.3 (1)米国CISAの取り組み」を参照されたい。

(ウ)政府システムの脆弱性可視化

2021年11月3日、CISAは既知の脆弱性悪用に関する重大リスクの削減に関する運用指令(Binding Operational Directive)を発表した※243。同指令は、CISAが作成・更新する「悪用された既知の脆弱性カタログ※244」に基づき、各政府機関が管理または運用委託しているシステムの脆弱性管理手順の60日以内の見直し・修正を求めるものである。また、各機関は同指令の実施状況について、政府システムの資産状況可視化基盤(CDM Agency and Federal Dashboard)※245を介して報告することが期待されている。上記ダッシュボードは、巨大な連邦政府システムの資産データを自動収集・可視化する野心的な試みであり、効果が注目される。

(エ)Disinformation対策

2020年は新型コロナウイルス対策関連の詐欺情報によるフィッシング、及び大統領選挙における投票操作不正等の悪意の虚偽情報(Disinformation)による混乱が国家的な課題であった。2021年は、SNS事業者によるチェック強化等で混乱はいったん沈静化したように見えるが、CISAは、選挙セキュリティ(election security)の一貫としてDisinformation対策を進め、2022年3月30日に情報操作に関する注意、続いて4月1日にSNSボットによる意見誘導への注意、更に同月12日にDisinformationに対処する手順に関する注意喚起を行った※246。なお表面には現れないが、Disinformation拡散活動を封じるハッカー対策も関連組織と連携して取られていると思われる。

(オ)ロシアが支援するサイバー攻撃への対応

ロシアに支援されたサイバー活動組織(以下、ロシア系ハッカー)に対し、CISAはFBI、NSA等と連携して監視を続けている。2022年2月15日の時点で、CISAはすべての米国の組織に対してロシア系ハッカーの攻撃に備えるよう要請していた※247。また2月16日、ロシア系ハッカーが少なくとも2020年から2022年2月まで、DoDの防衛契約事業者とそのサブコントラクターのコミュニティ(CDCs:Cleared Defense Contractors)を狙い、様々な手法で機密情報の窃取を行っているとし、CDCsに対策を求めた※248。

ロシアのウクライナ侵攻開始直後の2月26日、CISAはFBIと共同で、ウクライナで使用された破壊的なウイルスWhisperGateとHermeticWiper、及びその防止策に関するアドバイザリを公開した※249。更に3月2日、CISAは想定されるサイバー攻撃対策に関する専用サイト「SHIELDS UP※250」を公開した。SHIELDS UPでは、基本的なセキュリティ対策に関するガイドに加え、ランサムウェア対策、前述のCISA脆弱性カタログ、ロシア系ハッカーによる個別攻撃の注意喚起等を掲載、逐次更新している。

3月21日、Biden大統領は国家のサイバーセキュリティ

に関する声明を発表し、すべての企業・組織がロシアのサイバー攻撃に備えるよう呼びかけた※251。CISA は SHIELDS UP における逐次情報更新や、前記（ア）～（エ）についての改めての注意喚起により、対策司令塔の役割を果たしている。

2022 年 5 月末の時点で、米国の政府システム、重要インフラシステムへの深刻な攻撃被害、あるいはロシア系ハッカーによる深刻な Disinformation の混乱はなく、CISA・FBI・NSA 等の連携による対策が奏功していると思われる。

(3) 情報配信の規制と課題

クラウド、EC、SNS 等のサービス基盤を提供するグローバルプラットフォーム事業者（いわゆる GAFA）の巨大な影響力に対する懸念が増加し、規制の議論が欧州、米国、日本等で進んでいる。EU では、2018 年に発覚した大量の Facebook 個人情報の政治広告不正流用※252 や Brexit 関連のフェイクニュースの混乱を契機として、GDPR（General Data Protection Regulation）施行を始め、GAFA の情報収集・配信活動を規制する法案の整備を進めている（「3.4.2 (4) (a) インフォデミックに関するガバナンス」参照）。米国政府は、GAFA の規制について不干渉方針を取ってきたが、2016 年の大統領選挙におけるフェイクニュースや選挙干渉の混乱以降は規制に舵を切り、2019 年、連邦取引委員会（FTC：Federal Trade Commission）と司法省が反トラスト法違反の疑いで GAFA の調査を開始した※253。米国下院司法委員会も同法に基づく調査を実施し、2020 年 10 月、GAFA は「独占企業で力を持ちすぎており、分割が必要」と提言した※254。Biden 政権発足後は上下両院で GAFA 規制に関する複数の反トラスト法改正案が議論されている。2021 年 6 月 11 日には下院にて※255、また同年 10 月 18 日には上院にて※256、GAFA の自社製品優遇を規制する法案が別個に提出され、2022 年 1 月 20 日、上院司法委員会は上院への提出法案を承認した※257。一方 GAFA は、自社製品の採用は市場の選択の結果であり、このような規制は技術革新を抑制し、国家のセキュリティにとって有害である、と一斉に反論している。法案成立の可能性は流動的だが、GAFA に対する規制圧力は高まっている。

一方で、フェイクニュース等の Disinformation 配信規制に米国議会は慎重である。具体的には、AI による映像生成技術 Deepfake の状況について、選挙干渉の懸念から DHS に定期報告を求めた Deepfake Report Act※258 を 2019 年に成立させたのみで、情報配信の統制を重視する EU とは対照的である。

ところがこの状況の中で、Facebook の不適切な情報配信を Meta Platforms, Inc.（以下、Meta 社）は放置している、との内部告発がなされた。Meta 社の元プロダクトマネージャー（在職当時は Facebook, Inc.）Frances Haugen 氏は、同社の内部文書を報道機関にリークし、Meta 社は人権抑圧・暴力・性等の有害情報（Harmful information）配信に関して以下のような不適切な対応をした、と報道された※259。

- 著名人の言説に対する人権・暴力等のルール適用免除
- 10 代女性に対する有害情報配信の放置
- アルゴリズム変更による有害情報のランク上昇放置（類似の興味を持つ人の投稿、内容が過激な投稿が重視され、有害情報共有が増幅するエコーチェンバー現象※260）
- 発展途上国における有害情報配信による人権抑圧・闘争誘発放置

2021 年 10 月 5 日、Haugen 氏は上院公聴会で Meta 社幹部は「利用者の安全より利益を優先した」と証言した※261。これに対し Meta 社の Mark Zuckerberg CEO は、アルゴリズム変更は善意に基づくもので、必要な対応を取る等と釈明、悪意の「いいね」操作等につけ込まれやすいアルゴリズムを修正したという。しかし、Disinformation や有害情報の蔓延抑制には、アルゴリズムの評価に加え、虚偽情報生成の低コスト化と真贋判定の困難、表現に関する私権の制限、広告配信モデルへの過度の依存等、根本的な解決が難しい課題があり、状況は簡単に改善しないと思われる。政府、事業者がどのように対応するか、注目される。

(4) 米ロ関係の悪化とウクライナ侵攻

SolarWinds 事案で悪化した米ロ関係は、ウクライナ情勢を巡り更に混迷した。2022 年 2 月 24 日のウクライナ侵攻により、ロシア・ベラルーシと米国等 NATO 諸国との対立は決定的となった。2022 年 4 月末時点までの経緯を述べる。

(a) 米ロ首脳会談から侵攻までの経緯

米国がロシアに SolarWinds 事案の制裁を課した直後の 2021 年 6 月 16 日、Biden 大統領は Vladimir Putin ロシア大統領とスイス・ジュネーブにて初の会談を

行った※262。同会談についてBiden、Putin両大統領はともに「冷戦以降最も冷えきった関係の中で対面した」ことを強調し、新たな軍備管理に関する協議開始等で合意する等、関係改善への模索が見られた※263。サイバーセキュリティについては、「破壊的なサイバー攻撃を行わない重要セクター」に関する討議で合意したが、Putin大統領は、ロシアは選挙妨害に無関係、との態度を変えなかった。Putin政権を批判する政治活動家Alexey Navalny氏等への人権問題、ウクライナ問題についても意見は合わず平行線をたどった。

2021年6月以降も、ウクライナのNATO加盟を脅威とみなすロシアの軍備強化は続き、同年12月3日にはウクライナ国境付近に17万5,000人が集結したと報道された※264。12月6日、Biden大統領はNATO諸国と対応を協議、翌7日のPutin大統領とのオンライン協議※265で、ロシアがウクライナに侵攻した場合「重大かつ深刻な経済的損害を与える」と警告した。Putin大統領側は軍備強化を否定し、東方へ拡大を続けるNATOこそ脅威であり※266、ウクライナのNATO加盟を禁止せよ、と反論したと見られる。

緊張が高まる中、2021年12月30日、2022年2月12日と電話による首脳会談が行われた。2021年12月30日の会談では、Biden大統領は「ウクライナ侵攻があれば、経済制裁・NATOの強化・ウクライナ軍事支援を行う」とし、一方Putin大統領は「制裁発動はロシアと米欧諸国の関係に壊滅的な打撃となる」として警告の応酬となった※267。2022年2月12日の会談では、Biden大統領から欧州の安全保障に関する説明があったが、ロシアが求めるNATOの東方拡大阻止の明文化等は含まれず、状況打開はできなかった※268。Biden政権は同12日、在ウクライナ米国大使館職員の国外退避を命じた。

2022年1月以降、Biden政権はロシア軍の動向等に関するインテリジェンス情報を開示し、ロシアの動きをけん制するアプローチを取った。2月18日、Biden大統領は「Putin大統領はウクライナ侵攻を決定し、首都キーウ（キエフ）を狙うことを確信できる情報を得た。これを発表するのは衝突を望むからでなく、ロシアの侵攻を正当化する事態を招かないためである」と述べ、ウクライナの親ロシア派が攻撃されている、等を偽装する偽旗作戦（False flag operation）にも言及した※269。ロシア政府は侵攻準備について、「米国のヒステリー」として終始否定を続けたが、2月24日に侵攻は始まった。その後の戦闘経緯は、米国のインテリジェンス情報がかなりの精度であったことを示している。

このような、インテリジェンス情報の開示や偽装に関する警告が先行して行われたことは過去に例がない。また侵攻開始後、Volodymyr Zelenskyyウクライナ大統領やウクライナ軍がSNS等で積極的に情報や戦闘の映像を開示し、国際的な支持において優位に立ったこと、更にITベンダやハッカー集団等の民間組織・個人が紛争当事国のサイバー防御・攻撃に関わったことも過去に例がない（後述）。現代の紛争が武力と情報の組み合わせによるハイブリッドな戦い（ハイブリッド戦）であることを示すものとなった。

(b) 国防授権法と軍産連携によるサイバー防御

2021年12月27日、2022会計年度（2021年10月～2022年9月）の米国国防関連予算と活動を定める国防授権法（National Defense Authorization Act）※270にBiden大統領が署名した。同法は予算総額7,700億ドルを計上し、米軍の活動基金「太平洋抑止イニシアティブ（PDI：Pacific Deterrence Initiative）」を2021年度の22億ドルから71億ドルに増額し、中国の台湾に対する活動の既成事実化に対抗することを米国の政策とする等、アジア太平洋地域への継続的コミットメントを強化している※271。欧州については、NATOへの支持、ウクライナ安全支援イニシアティブ（Ukraine Security Assistance Initiative）への5,000万ドルの増額等が盛り込まれたが、ロシアのウクライナ侵攻で、NATO諸国との連携は大幅に強化されることとなった。

サイバーセキュリティに関しては、DoD自身のセキュリティ基盤強化にゼロトラストモデルやセキュリティ検証自動化が、またCYBERCOM強化に関し、民間IT事業者との連携による防御が盛り込まれた。このような事業者との連携は過去数年のDoDの方針を踏襲したものである。

2022年1月15日、Microsoft社はウクライナの政府機関・関連組織がランサムウェアに偽装した破壊的ウイルスにより攻撃されていると発表した※272。更に同社は2月24日、ロシアの侵攻開始直前、ウクライナ政府・金融機関への大規模サイバー攻撃を観測、FoxBladeと呼ばれるウイルス群についてウクライナのサイバー防衛当局に情報を提供した。Brad Smith会長は28日、自身のブログで「我々は国家ではないが、連邦政府・NATO・EUとともにウクライナ政府と継続的に連携する」と述べ、「数年前なら数週間・数ヵ月かかっていた情報提供が数時間で見事にできた」とした。Microsoft社はウクライナへのサイバー防御支援を継続しており、ロシア

からのサイバー攻撃に対処できていると思われる。

また CISA、FBI、NSA 等も前節（「3.4.1 (2) (c) (オ) ロシアが支援するサイバー攻撃への対応」）で述べたとおり、ロシア系ハッカーの監視と対応、民間への情報発信で貢献している。一方、CYBERCOM の活動に関する情報は開示されないが、前述の高い精度のインテリジェンス情報でウクライナや米国政府・民間組織のサイバー防御・攻撃、あるいは Disinformation の流通抑制を支援していると思われ、軍産官の連携は機能していると推定される。

(c) 民間組織・個人のサイバー戦対応

このほか、米国のグローバル企業はウクライナ支援に積極的に活動した。Space Exploration Technologies Corp. の Elon Musk CEO は 2 月 26 日、Mykhailo Fedorov ウクライナ副首相兼デジタル転換相の求めに応じて衛星インターネットサービス Starlink の機器を提供、ウクライナのインターネットを支えた※273。Apple Inc.（以下、Apple 社）、IBM Corporation、Microsoft 社、Oracle Corporation を含む多くのグローバル IT 企業がロシア政府・企業との取り引きを停止した※274。Google LLC（以下、Google 社）は侵攻に関するフェイクニュースを絶つとして、RT（Russia Today）、SPUTNIK 等の親ロシアメディアのコンテンツ配信を遮断、ロシア政府の支援を受けるメディアの広告配信等も無期限に停止した※275。一方、Meta 社はウクライナ侵攻に関わる政治的・暴力的投稿について、同社のポリシーを臨時に緩和、許容した※276 が、ロシア政府の抗議を受けてこれを撤回した。

IT 企業とは別に、ハッカー集団の一員としての個人もロシアとのサイバー攻撃・防御に参画した。その代表格である集団 Anonymous は 2 月 25 日、ロシア政府にサイバー戦を宣言し、政府関係サイトへの DDoS 攻撃、同サイト乗っ取りによるウクライナ支援メッセージ表示、金融機関システムへの侵入によるデータ窃取、軍関係の個人情報窃取・暴露等を継続的に行っている、としている※277。こうした紛争当事国と紐づかない個人の参画は、これまでは専門の傭兵・義勇兵しか考えられなかったが、ウクライナ侵攻は、通常の業務を行っている民間人が同時にサイバー戦に参加できる、という事態を招いた。

更に、ドローン等による戦闘映像がリアルタイムに近い状況で世界に配信されることがウクライナ支援の大きな力になっていることは疑いないが、配信する映像・情報によって国際世論が形成される、ということは、仮にこれらの情報が偏っていた場合、あるいは偽装された場合に大きなリスクをはらむ。

このように、ウクライナ侵攻における「情報の戦い」は、配信される情報の信頼度の見極め、第三者である民間人のサイバー戦への参画、という難しい問題を世界に突きつけることとなった。

(d) ロシアへの対抗策

Biden 政権は武力によるウクライナ介入は避け、ロシアへの経済制裁を発動している。2022 年 3 月 8 日、同政権はロシアの石油・天然ガス・石炭の禁輸措置を発表※278、EU 諸国もドイツがロシアの天然ガスパイプラインの認可手続きを停止する※279 等で同調し、ロシアとの協調姿勢を転換した（「3.4.2 (6) (b) ロシアへの対応」参照）。更に 4 月 6 日、Biden 政権は G7、EU 諸国と連携してロシアへの新規投資凍結、主要銀行・政府系企業・政権に近い個人との取引停止、海外資産凍結等を発表した※280。銀行制裁対象の主要銀行が国際決済ネットワーク SWIFT（Society for Worldwide Interbank Financial Telecommunication）からの排除対象に含まれない、エネルギーをロシアに依存する欧州はエネルギー禁輸が難しい、中立を保つとする中国、インド等による支援の可能性がある等により、効果を疑問視する声もある※281。2022 年 3 月 18 日、Biden 大統領は中国の習近平主席とテレビ会議を行い、ロシアを支援しないように警告した※282。

一方で禁輸、欧米系企業との取引停止によりロシアの工業・IT 系サプライチェーンには大きな支障が出ると思われる。同年 4 月 20 日、20 ヵ国・地域（G20）財務大臣・中央銀行総裁会議がワシントン D.C. で開催され、ロシア代表がリモートで発言したが、米国・カナダ・英国等の米欧の参加者が退席、ロシアの参加を認め、議論を行うとする新興国との意見の対立が鮮明になった※283。ロシアとウクライナの戦いは 4 月に入り長期化の様相を呈し、制裁による経済の分断に加え、ロシア排除を是とするか否かの意見の分断に世界は揺さぶられている。日本は、米国・EU 諸国と歩調を合わせることが大前提となるが、この分断にどう対応するか、難しい判断を迫られることとなる。

3.4.2 欧州の政策

2021 年 5 月 1 日、「EU・英国の通商と協力に関する協定（TCA：EU-UK Trade and Cooperation Agreement）」が正式に発効、新たな枠組みのもとでの

EU・英国の通商が本格化した※284。その一方で、2021年度も新型コロナウイルスの蔓延とその対策は欧州全域で継続し、経済や流通の回復に影を落とし続けた。

更に2021年10月以降、ウクライナに対するロシアの侵攻準備に対し、NATO加盟国を中心とする欧州でも危機感が高まった。2022年2月24日、ウクライナ侵攻が開始されると欧州各国は一斉にロシアを非難、直ちに米国と連携して経済制裁で対抗した。

以下ではこのような状況下における、英国及びEU諸国のセキュリティ・データ保護に関する政策動向について述べる。

(1) Brexitの英国における評価

2021年5月1日に発効したTCAには、アイルランド（EU加盟国）と北アイルランド（英国）の間の国境管理を避けるため、実質的に北アイルランドをEU圏内に留める、とした北アイルランド議定書が含まれ、発効直後からこれが問題化した。英国本土と北アイルランドとの間に通関障壁が発生、議定書に対する英国の不満が高まったためである。2021年10月13日、欧州委員会（European Commission）が議定書の調停案を示したが、両者の意見は平行線のままで、解決の糸口は見えていない※285。

2021年12月の時点で、経済専門家はBrexitにより英国経済は停滞している、とした※286。停滞の要因は通関手続きの煩雑化による取引減少、英国への人的移動の減少等が考えられるが、パンデミックの影響もあり、Brexit自体の影響はまだ不確定とされる。英国民にも、Brexitは負の影響が大きい、との不満が強まり、「EU再加盟」の声も上がり始めている※287。しかし、英国政府はEU復帰で再度国論を二分するような争いを避けたいこと、2国間のFTA（Free Trade Agreement：自由貿易協定）締結や日本が主導するTPP（Trans-Pacific Partnership：環太平洋パートナーシップ）協定加盟等の動きが始まっていること等から、当面現行の通商の枠組みを維持するとみられる。

(2) 新型コロナウイルスへの対応

2021年の欧州は、新型コロナウイルスの新しい株（デルタ株、オミクロン株）の流行に見舞われたが、3回目のワクチン接種の進展や厳しい対策への根強い反発等から、徐々に対策が緩和された。

(a) 感染状況

欧州は2020年3～4月に新型コロナウイルス流行の第1波、10～12月に第2波に襲われ、ロックダウン等を余儀なくされたが、2021年初頭からワクチン接種効果もあって感染者は急減した。英国では2021年1月初旬に6万人超であった7日間平均の感染者数が4月末時点で2,000人弱に減少※288、通常の生活が戻ることを期待させた。しかし、6月に感染者が急増、その9割以上がデルタ株であり、インドからの渡航者の多さが主な原因と推定された※289。デルタ株は急速に欧州に広まったものの、ドイツ・フランス・イタリア等では感染者爆発は免れ※290、2021年夏以降、コロナ対策の制限緩和を求める世論が各国で高まった。感染者数が急増した英国・スペインも死者数は限定的であり、教育や一部職域等での制限、入国制限を除き、規制緩和が維持された。

2021年12月には感染力の強い新たな変異種（オミクロン株）が世界的に蔓延、2022年2月1日には欧州全体の感染者数が177万人を越える大規模な流行（第5波）となった※291。各国政府は3回目のワクチン接種を急ぐ一方、これだけの蔓延には隔離や渡航制限等は効果がなく、ワクチンと投薬で対応するとの方針をとった。例えば英国政府は2022年1月5日、入国者への検査体制を緩和すると発表※292、同年2月21日には、Boris Johnson首相がイングランドにおける新型コロナウイルス感染者隔離の法的義務を撤廃し、4月1日から無料のPCR検査を「最も影響を受けやすい人」に限定する、というliving with Covid計画を発表した※293。2022年4月の時点で第5波は収束しつつある。

(b) ワクチンパスポート

「情報セキュリティ白書2021」の「2.2.3 欧州の政策」で詳述したとおり、欧州は世界保健機関（WHO：World Health Organization）の慎重姿勢とは裏腹に、公的なワクチン接種証明を早期に導入し、欧州域内の人の移動制限を緩和しようという動きが急である。2021年3月17日、欧州委員会はEU域内の自由で安全な移動を保証するワクチン接種証明書に関する法案を発表した※294。同年4月14日、欧州理事会（European Council）は、加盟国政府の接種証明導入における人権保護ガイダンスを公開した※295。これらの法案・ガイドは、接種証明をワクチン非接種者への差別要因とさせないこと、記録する個人情報は最小限にすること等を明示している。

2021年7月1日、欧州委員会は接種証明書（Digital

COVID Certificate：通称グリーンパス）の発行・運用を開始した。グリーンパスは、「ワクチン接種」「検査陰性」「感染からの回復」のいずれかの証明を加盟国が発行するもので、保持者は検疫等を受けることなくEU域内を移動できる※296。接種・検査を行った医療機関等の署名も含む、個人情報はパスの署名チェック時には参照されない、等のセキュリティが担保されるという。越境時の運用については煩雑さが指摘されたが、2021年の夏は、2年ぶりに南欧等の観光地が賑わうこととなった。また2022年4月時点で、個人情報漏えい、あるいはGDPR違反等の大きな事案は起きていない。

EU以外の国のワクチン接種証明書も、EUと同等の条件であればEU域内移動制限が緩和される。EUを離脱した英国も、同国の発行する証明書があればEU域内への移動に制限はなく、またグリーンパスにより英国への移動も自由である。アジアではタイ・マレーシア・シンガポール・台湾等も同様である。これに対し、米国や日本が求める接種証明や規制緩和の要件はグリーンパスと適合せず、普及の懸案事項となっている。例えばどのワクチンの接種を有効と認めるか、で証明書の互換性に問題が生じる懸念は導入以前からあったが、米国とEUのケースではそれが顕在化している※297。

(c) ワクチン接種義務化

欧州各国はワクチン接種率向上の手段として義務化政策を試みているが、接種の可否判断は個人の権利と考える市民の反対は根強く、対応に苦慮している。

フランス政府は2021年7月、ワクチン接種済み、またはPCR検査陰性を証明する衛生パス（passe sanitaire）を導入、公共空間にアクセスする18歳以上の人に提示を求めた。実際に衛生パスはワクチン接種率向上に効果があったとされる※298。フランス政府は更に2022年1月24日、ワクチン接種を実質的に義務化するワクチンパス（passe vaccinal）を導入※299、16歳以上で飲食・文化・娯楽施設、地域間交通サービス等を利用する場合に提示必須とした。一方で、マスク着用、イベント・飲食等に関する制限を順次緩和し、2月28日にはワクチンパス適用施設内のマスク着用義務を解除した※300。また2月以降第5波が収束に向かったこと等から、Jean Castex首相は3月3日、ワクチンパスの適用を3月14日から一時停止すると発表した※301。ワクチン義務化への根強い不満に対して、大統選選挙直前に配慮がなされたという見方もある。

ドイツは、2021年9月の総選挙で与党キリスト教民主・社会同盟（CDU-CSU）が敗北、中道左派の社会民主党（SPD）が第一党となり※302、首相はAngela Merkel氏からOlaf Scholtz氏に交代した。Scholtz首相はワクチン接種義務化と規制緩和の方針を継続、2022年3月15日から発効予定の医療・高齢者介護従事者等への接種義務化法案を、一般市民に拡大することを目指した。2021年12月22日にドイツ倫理委員会はこれを「一定の条件のもとで推奨」するとし、経済界も同調した※303。しかし、オミクロン株にワクチンが有効でないとの疑義が出たことから野党が反発、連立与党（SPD、緑の党、自由民主党）も合意できず、審議は紛糾した。与党賛同者が「60歳以上への義務化」という妥協的な法案を提出したが、2022年4月7日、ドイツ連邦議会で否決された※304。Scholtz首相のコロナ対策は冒頭でつまずいた形である。

イタリアでは2021年8月6日以降、国内の飲食やイベント施設へのアクセスで接種証明の提示を義務付け※305、国内向けの詳細な適用規格を整備した※306。一方英国の対応は二転三転した。英国は当初イングランドにて、イタリアと同様にイベント等で接種証明提示を求める計画であったが、反対意見が強く、2021年9月12日、Sajid Javid保健相が導入見送りを発表した※307。経済界はこれに反発、同年12月14日、英国下院は、議員の賛否が割れる中で、接種証明提示義務化案を承認した※308。ところが2022年1月31日、Javid保健相はヘルスケア従事者に対するワクチン接種義務化の決定を撤回する、と発表した※309。ワクチン接種を忌避したいヘルスケア従事者の雇用に配慮したと思われるが、政府の対応は義務化をめぐる混乱を示すものとなった。

(3) サイバーセキュリティ政策

欧州のサイバーセキュリティ政策は、欧州ネットワーク・情報セキュリティ機関（ENISA：The European Union Agency for Cybersecurity）が主導し、重要インフラに関するNIS指令（NIS Directive）の実装、あるいは域内の製品・サービスのセキュリティを担保するサイバーセキュリティ認証スキームの構築等を中心として進められている。以下では、これらの施策の最新動向について述べる。

(a) 重要インフラのセキュリティ

2016年8月8日に発効したNIS指令は、EU域内の重要インフラ・サービスのセキュリティについて、加盟国の対策能力向上、加盟国間の連携と情報共有、重

要事業者のCSIRTのリスクマネジメントとインシデント報告の監督、の3点について義務を規定し、加盟国の国内準拠法・規格の状況を公開している。ENISAはまた、加盟国によるNIS調整グループ（NIS Coordination Group）を組織し、加盟国間の情報共有とEU CSIRTの方針調整、各種ガイドラインの策定を行っている[※310]。2021年11月に公開されたNIS Investments Reportによれば、調査対象の重要インフラ・サービス事業者の48.9%が「NIS指令により自社のセキュリティ対策に重要なインパクトがあった」とし、50%が「検知能力が向上した」、また26%が「復旧能力が向上した」と回答した[※311]。

この間ENISAは2021年6月3日にエネルギー業界、ヘルスケア業界のPSIRTの実態調査報告[※312]を、また同年11月11日に医療・保健業界のCSIRTの実態調査報告を公開した[※313]。コロナ対策という背景もあり、ENISAの医療・保健業界の能力向上重視がうかがわれる。

一方、NIS指令の実装が本格化するとともに、対象とする業種拡大の必要性が課題として表面化した。欧州委員会はこれを検討し、重大エンティティ（essential entity）と呼ぶカテゴリに、基幹サービス7分野に加えて行政、下水道、宇宙の3分野を追加、また重要エンティティ（important entity）と呼ぶカテゴリに、デジタルサービス提供者に加えて郵便、廃棄物処理、化学、食品、製造等を追加すること、またサプライチェーンセキュリティ、効率的なインシデント報告、EU内の統合的な罰則等のセキュリティ強化が必要であるとするNIS指令の改正案NIS2 directiveを作成した。次いで欧州議会（European Parliament）内の産業研究エネルギー委員会（Industry, Research and Energy Committee）がこれを審議、2021年10月28日に承認した[※314]。今後改訂に向けた手続きが進むこととなる。

(b) セキュリティ認証スキームとセキュリティ市場分析

EUのサイバーセキュリティ認証制度（Cybersecurity Certification Framework）は、EU域内で提供されるICT製品・サービスのセキュリティ認証を各国任せにせず、EUの統一規格（スキーム）による認証で置きかえ、欧州デジタル単一市場（EU Digital Single Market）を実現しようとするもの[※315]で、ENISAが提出、2019年6月27日に発効したEUサイバーセキュリティ法（Regulation（EU）2019/881）[※316]に準拠している。このスキームには、法案提出当初から「製品カテゴリで要件が違いすぎる」「民間に任せるべき」等の反対意見が出されていたが、ENISAは2020年7月2日、コモンクライテリア認証をベースとする候補認証スキーム（EUCC scheme：Common Criteria based European candidate cybersecurity certification scheme）[※317]を、2021年5月25日に同スキームの改版V1.1.1[※174]を公開した。V1.1.1によれば、本スキームは、欧州がこれまでスマートカード認証等で運用して実績のあるコモンクライテリアスキームの後継で、ISO/IEC 15408、ISO/IEC 18045に準拠するとし、更にEUサイバーセキュリティ法のセキュリティ要件を満たし、より広いICT製品・サービスのセキュリティ向上に貢献する、としている。本スキームは法制化が想定され、法制化された場合のICTセキュリティベンダへの影響は大きい。

続いてENISAは2020年12月22日、クラウドの認証スキームドラフトを公開した[※318]。本スキームは、EUサイバーセキュリティ法に基づいてCSPCERT（Cloud Service Provider Certification）Working Groupが2019年に作成した推奨事項[※319]を引き継ぎ、保証レベルをbasic、substantial、highの3段階とし、ISO 27000シリーズのクラウド認証標準と監査に関する規格のいずれにも配慮した、としている。本スキームの利用は任意であり、法制化はない、とされる。

更に2021年2月3日、ENISAは欧州委員会の要請により、5Gネットワークの認証スキーム策定に着手すると発表[※320]、アドホックワーキンググループを2021年夏に設置した[※321]。ドラフト作成作業はやや遅れ、2023年の公開が想定されている。

一方で、これらの認証スキームにも提案当時から「製品カテゴリで要件が違いすぎる」「民間に任せるべき」等の異論があり、実施にスキームが利用され、市場に受け入れられるかは未知数である。ENISAはこれに対し、認証スキームの市場へのインパクト計測について検討を行い、2021年4月9日、特定のセキュリティ市場（TOA: Target of Analysis）における認証スキーム導入の有効性評価を行う手法を公開した[※322]。

このほかENISAは、「EU域内市場活性化の要件」及び「欧州のサイバーセキュリティ産業・市場の育成」を主眼とするサイバーセキュリティ市場ワーキンググループを設置し、2022年4月8日にサイバーセキュリティ市場分析の枠組み、及びIoTセキュリティ市場に関する分析報告を公開した[※323]。このような、EU共通の規格策定と並行してEU統合セキュリティ市場の分析を行う活動は注目に値する。

(4) セキュリティガバナンスに関する政策

セキュリティガバナンスに関して、EU は IT サービス利用者である EU 域内市民の権利・プライバシー・資産保護の立場から施策を策定している。以下では、インフォデミック、AIに関するガバナンス施策について述べる。なお、GDPR の運用状況については「3.4.2 (5) GDPR の運用状況」で紹介する。

(a) インフォデミックに関するガバナンス

新型コロナウイルスの感染対策やワクチン接種、大統領選挙等に関するフェイクニュース等の Disinformation による混乱（インフォデミック）に対し、欧州は厳しい態度をとり続けている。

2020 年 12 月 3 日、欧州委員会は Disinformation による政治活動過激化への対策として「欧州民主主義行動計画（European Democracy Action Plan）」（以下、行動計画）を発表した※324。行動計画は、「デジタル空間において、虚偽や悪意を排した事実に基づき、自由でオープンな意見表明と討議を可能にし、欧州の民主主義を強化する」として、以下の 3 点について施策を講ずるとしている。

①自由で公正な選挙の推進
②メディアの自由と多元主義の強化
③虚偽・有害情報対策

①については、選挙コンサルティング会社 Cambridge Analytica Ltd が Facebook の大量個人情報を選挙活動に悪用した等の苦い経験から、政治広告への規制を主眼としている。

②については、ジャーナリスト（特に女性）の安全を確保し、メディアの多元性の強化を加盟国と推進する、としている。ここでは言及されないが、中国・ロシアへの警戒があり、中国・ロシア資本によるメディアの所有や政治広告等に対する監視を強めると考えられる。

③について欧州は、米国とは対照的に、一貫してプラットフォーム事業者規制の立場をとっている。行動計画では、欧州委員会が策定した SNS、ネット広告等における「虚偽・有害情報に関する行動規範（Code of Practice on Disinformation）※325」（以下、行動規範）の内容を準規則化（co-regulatory framework）し、プラットフォーム事業者の監視を強めるとしている。また、2020 年 12 月に欧州委員会が提出した包括的なデジタルプラットフォーム規制法案「デジタルサービス法（DSA：Digital Services Act）※326」と整合させる、としている。DSA によれば、例えば「超大規模オンラインプラットフォーム」（GAFA 等が想定される）に対して、違法コンテンツ配信・人権侵害等のリスク評価、リコメンデーションシステムに関する情報開示とカスタム化機能、オンライン広告の情報開示、EU 加盟国の調整担当官による監督、等の義務が課される※327。2022 年 4 月 23 日、欧州委員会は欧州議会と EU 加盟国が DSA について合意した、と発表した※328。

同年 3 月 25 日、欧州委員会は、デジタルプラットフォーム事業者による不公正・独占的なビジネス慣行の是正、透明性の確保を義務化する「デジタル市場法（DMA：Digital Markets Act）※329」についても、欧州議会と EU 加盟国が合意した、と発表した※330。DMA は、欧州委員会により「ゲートキーパー（デジタルサービスや顧客への玄関口）」と認定された事業者に対し、アプリのプリインストール等の禁止やメッセージサービスの相互互換性等を求めており、違反には高額の制裁金が科される。欧州委員会の Margrethe Vestager 副執行委員長は、DMA は 2022 年 10 月に発効する、とした※331。これに対してゲートキーパーとされる Google 社、Apple 社等は「利用者の不便」「知的財産権への配慮」「技術革新への影響」等の不満・懸念を表明している。

以上のように、欧州の公平・公正なデジタルマーケットの統制は DMA、DSA が柱となっており、インフォデミック対策も、その中で実装されていくと考えられる。Disinformation・有害情報の蔓延については、DSA のリスク評価に基づき、事業者が主導的に対処すると思われるが、行動計画の施策①、②に含まれる政治広告の規制・関連組織の監視については、EU 加盟国政府との連携も必要であり、今後の検討が待たれる。

(b) AI に関するガバナンス

AI は、IT 技術革新の重要な要素であり、欧州委員会も AI 利用は EU の国際競争力の源泉と考えている。同時に欧州委員会は、AI が EU 市民の権利を保護し、安心して利用できるという信頼（trustworthy AI）も必須であるとしている※332。

欧州委員会において、信頼できる AI に関する検討は 2018 年に開始されたが、2021 年 4 月 21 日、同委員会は、AI 利用に伴うリスク及びその対処に関する法案「Artificial Intelligence Act」（以下、AI 法）を提出した※333。AI の利用リスクについては、特に人権・プライバシー侵害や軍事利用に関する倫理面の議論が企業・研究機関・国際標準化機関等で検討され、多くの

ガイドランが提示されている。米国 DoD も、2020 年 2 月に国防の AI 利用について倫理原則の受け入れを発表している（「情報セキュリティ白書 2020」の「2.2.2 (5) (d) AI 倫理原則の採用」参照）。しかし、罰則を含む法制化は AI 法が初めてであり、世界各国から注目されている。

AI 法では、AI 利用時のリスクの大きさにより利用類型を分類し、段階的な規制を設けている。最も厳しいカテゴリは利用の「禁止」で、類型には「サブリミナル技術の悪用」「子どもや精神障害等の脆弱性の悪用」「個人の信用評価等の悪用※334」「法執行におけるリアルタイム生体識別」が含まれる。

禁止に次いで厳しいカテゴリが「ハイリスク AI」で、類型には「個人の生体識別」「重要インフラ管理･安全確保」「学生の成績評価」「被雇用者の管理・業績評価」「受給資格審査・与信評価」 等が含まれる。「ハイリスク AI」の提供者・利用者には、それぞれ公平・公正な利用のための義務規定が記載されるが、提供者側の責任が大きい。

次に、利用者の不利益を回避するために説明責任を求めるカテゴリ「透明性義務を伴う AI」がある。類型には、利用において AI と利用者のやり取りが必要だが自明でない場合にそれを開示する、ディープフェイク等による本人と類似した合成画像の利用において、合成であることを開示する、等がある。

リスクカテゴリごとの規定に違反した場合、制裁金が科される。リスクカテゴリ、提供者と利用者の義務、制裁金等の設計においては、GDPR や司法捜査からの個人情報保護規定である Law Enforcement Directive※335 を始めとする EU の既存法制との整合が重視されている。EU としては、AI 法を GDPR にならい、世界標準規格にしたい意図があるともいわれる。

しかし提出法案に対しては、産業界やプラットフォーム事業者から多くの懸念・異論が出ている※336。主要なものとしては以下がある。

- AI の定義が広すぎる。ハイリスク AI の定義もあいまいである。
- 複雑な AI エコシステムが考慮されず、AI 提供者の義務が大きすぎる。
- 義務規定で実施困難なものがある。
- ハイリスク AI の類型については既存法制と重なり、過剰規制の懸念がある。
- AI 技術の進展による柔軟な改変が必要である。

AI 法案審議では、上記の懸念について検討が進められ、最終確定までにはまだ時間を要すると思われる。

(5) GDPR の運用状況

GDPR の実際の運用は 2018 年 5 月の発効から 3 年半以上を経過し、厳格さを増している。

(a) EU・米国間の個人データ移転の新たな枠組み

2020 年 7 月 16 日、欧州司法裁判所は、米国の個人データ保護は GDPR と同等のレベルになく、米国と EU の間の包括的データ移転の枠組みであった「プライバシーシールド」は無効である、との判断を示した※337。その後、EU・米国間の個人データ移転は個々の契約に基づいていたが、2022 年 3 月 25 日、個人データ移転の新しい枠組みについて EU と米国が合意に達した※338。これは欧州司法裁判所にデータ移転停止を求められ、抗議している Meta 社には朗報であり、Google 社も合意を歓迎したが、あくまで政治合意であり、「内容はプライバシーシールドと同じではないか」との懸念も残っている。今後の司法専門家の精査が待たれる。

(b) GDPR 違反の状況

国際法律事務所 DLA Piper の調査によれば、2021 年 1 月 28 日から 2022 年 1 月 18 日までの GDPR 違反の制裁金総額は約 11 億ユーロとなり、2020 年 1 月から 2021 年 1 月の間の制裁金総額（1 億 5,850 万ユーロ）の約 7 倍に上った※339。違反届け出件数ではドイツ、オランダが突出した。制裁金額ではルクセンブルグが 7 億 4,600 万ユーロで突出し、アイルランドが 2 億 2,500 万ユーロで続いた。ルクセンブルグの制裁金は Amazon.com, Inc.（以下、Amazon 社）に科されたもので、2019 年に Google 社に科された 5,000 万ユーロを超え、過去最大である。

Amazon 社の欧州拠点はルクセンブルグにあるため、フランスのプライバシー保護団体は 2018 年、同社が「広告と情報提供において、欧州市民の意図に反して個人情報を使っている」との申し立てをルクセンブルグの国家データ保護委員会（CNPD：Commission Nationale pour la Protection des Données）に提出していた。CNPD は 2021 年 7 月 16 日、同社の行為を GDPR 違反であるとし、ビジネス慣行の改善を求め、制裁金を科した。ただし、違反行為の詳細は明らかにしていない※340。Amazon 社は裁定に強く反発し、米国証券取引員会（SEC：U.S. Securities and Exchange Commission）

への四半期報告において「顧客情報は守られており、広告の選択は欧州のプライバシー保護法に基づいている」と述べた※341。

なお制裁金の高額化について、DLA Piper は「欧州司法裁判所のプライバシーシールド無効判決の影響が大きい。高額な制裁金はビジネスの活性化にはつながらない」としている。

Amazon 社の事案のほか、制裁金額の大きな事案には以下がある。

- 2021 年 12 月 31 日、フランスデータ保護機関（CNIL: Commission Nationale de l'Informatique et des Libertés）は、Google 社に、利用者のクッキー拒否を阻害するようなユーザインタフェースが GDPR 違反であるとし、9,000 万ユーロの制裁金を科した※342。また Google Ireland Ltd. に対しても、同様な GDPR 違反があるとして 6,000 万ユーロの制裁金を科した※343。制裁金の算定には、利用者数の多さ、2 回目の違反裁定であること、等が考慮された。更に CNIL は、上記 2 社に対し、3 ヵ月以内にフランスの利用者にクッキー拒否が容易にできる機能を提供するよう命じた。
- 同じく 2021 年 12 月 31 日、CNIL は、Facebook Ireland Ltd. に対しても、Google 社の場合と同様な GDPR 違反があるとし、6,000 万ユーロの制裁金を科した。制裁金の算定には、利用者数の多さ、2 回目の違反であること等が考慮された※344。
- 2021 年 12 月 16 日、イタリアデータ保護機関（Garante）は、エネルギー供給事業者 Enel Energia S.p.A. に対し、同社が数百万に及ぶ顧客情報をテレマーケティングに不正に流用したこと、顧客がテレマーケティングを断るための情報を提示しなかったこと、データ保護機関の査察に協力しなかったこと等が GDPR 違反であるとし、2,650 万ユーロの制裁金を科した※345。
- 2022 年 2 月 10 日、イタリアデータ保護機関（Garante）は、米国系の顔認識ソフトウェアベンダ Clearview AI に対し、同社のイタリア国内での監視サービスに用いる顔画像データが不正に処理されており、また利用者への情報開示の不備や利用目的の逸脱が GDPR 違反であるとし、2,000 万ユーロの制裁金を科した※346。
- 2022 年 3 月 15 日、アイルランドデータ保護機関（Data Protection Authority of Ireland）は Meta 社に対し、2018 年 6 月、12 月時点の技術的・組織的な情報セキュリティ対策が不十分であったとし、1,700 万ユーロの制裁金を科した※347。

(6) 中国・ロシアへの対応

欧州は、2000 年代以降中国、ロシアと緊密な連携を構築してきたが、2021 年に入り、激変している。以下では中国、ロシアそれぞれとの関係、及び NATO としての対応について述べる。

(a) 中国への対応

2020 年以降、中国と欧州の関係は新型コロナウイルス対策をめぐって急速に冷却した。更にサプライチェーンの中国依存リスクや、香港・新疆ウイグル自治区における人権問題が加わり、英国・EU 諸国は中国と距離を置く政策に舵を切った。5G・重要インフラ関連調達についてもこの政策が引き継がれている。5G における中国ベンダ排除に積極的な英国では、2021 年 11 月 17 日、通信事業者の機器調達におけるセキュリティ要件を厳格化し、「ハイリスクベンダ」依存等のサプライチェーンリスクを削減する通信セキュリティ法「Telecommunications（Security）ACT 2021」が成立した※348。また 2022 年 3 月 1 日、同法に基づく通信セキュリティ規則案が英国政府から公開された※349。

5G における名指しの中国ベンダ排除が難しいドイツでは、重要インフラ事業者のセキュリティを強化する IT セキュリティ法改正法「IT Security ACT 2.0」が 2021 年 5 月 28 日に施行された※350。同法は、「3.4.2 (3) (a) 重要インフラのセキュリティ」で述べた NIS2 directive に歩調を合わせ、重要インフラ業種の追加と対策義務強化を規定している。また重要部品の調達について、ベンダからの信頼証明（guarantee declaration）取得、連邦内務省（BMI：Bundesministerium des Innern und für Heimat）への事前申告を義務付けている※351。申告や政府の監督により中国依存リスクに対処する、というアプローチだが、5G ネットワーク普及の妨げになる、という民間の懸念の声もある。

以上のように、欧州の 5G・重要インフラ機器調達において中国の参画は困難になりつつある。また「3.4.2 (4) (a) インフォデミックに関するガバナンス」で述べた行動計画や DSA 等により、EU は「自由な情報の発信」について、中国に毅然とした態度を取ろうとしている。

2022 年 4 月 1 日、EU 首脳と中国首脳は 2020 年 12 月以来となるテレビ会議を行った※352。EU は中国に対し、制裁の抜け道を使ってロシアのウクライナ侵攻を支援しないよう警告し、中国は欧州のロシア制裁をけん制するとともに、「中国・欧州の情勢を安定化するべく、自主的な政策をとる」ことを要請した。中国・EU ともに関係を修

復したいとする思惑はあるが、人権問題やロシア制裁に対する意見の隔たりは大きく、関係修復は見通せない状況である。

(b)ロシアへの対応

ロシアへの対応について、欧州は難しい選択を迫られた。「3.4.1 (4) 米ロ関係の悪化とウクライナ侵攻」で述べたとおり、2021 年秋以降、ロシアのウクライナ侵攻準備が進み、ロシアとの関係は悪化の一途をたどった。2021 年 12 月 10 日、Ursula von der Leyen 欧州委員会委員長は、ロシアに対して「ウクライナ軍事侵攻は代償を伴う※353」と警告し、2022 年 2 月 16 日の欧州議会では「クレムリンが侵攻を選択すれば、制裁は素早く広範なものになる」と発言した。EU の制裁は侵攻直前の 2 月 23 日、ウクライナ東部の一部の国家承認に関わった個人や団体に対して開始され、2 月 25 日以降、英国も含め、5 回にわたり制裁措置を発動した※354。主な措置としては以下がある※355。

- ロシア・ベラルーシ政府関係者・資産家 1,091 人、金融機関・政府系企業等 80 組織の資産凍結
- ロシア中央銀行を含む金融機関、政府系企業の欧州市場取引停止。主要銀行の国際決済ネットワーク SWIFT からの排除。ロシア企業の信用格付け停止
- 石油精製技術の禁輸。エネルギー分野の新規投資制限
- 航空・宇宙関係部品の禁輸。ロシア航空便の欧州運航禁止。ロシア貨物船の欧州入港制限
- ドローン・暗号化ソフトウェア・半導体を含む軍事転用可能製品(dual-use goods)の禁輸
- G7 諸国と連携した最恵国待遇の停止、鉄鋼・ハイテク製品等の禁輸(「3.4.1 (4) (d) ロシアへの対抗策」参照)
- Disinformation 配信・情報操作の主体とされる政府系メディア(RT, SPUTNIK)の免許・認可取り消し※356

侵攻当初、エネルギー供給をロシアに依存する欧州が一枚岩で制裁を発動できるか、という懐疑が存在したが、短期間に広範な措置が EU 全体で合意されたことは注目される。しかし、これには代償も伴う。例えばドイツは、ロシアと推進してきた天然ガスパイプライン計画 (Nord Stream 2) を凍結する、という重い決断をした※357。更に 2022 年 4 月 26 日、ロシアからの石油禁輸に対応できる、とした※358。これにより、ドイツのエネルギー政策は見直しを迫られる。

石油禁輸は実効的な制裁手段として EU が提案しているが、実施を求めるポーランド・エストニア・ラトビア・リトアニアと原油の 65% をロシアに依存するハンガリー等との調整が難しくなっている。ドイツの決断は制裁の実現を一歩進めるものだが、急激なエネルギーのロシア依存脱却は欧州全域のインフレ加速、景気後退を招く恐れがあり、制裁を科す欧州も困難な時期を迎えると思われる。

(c)NATO の対応

ウクライナ侵攻においては、NATO の対応も注目された。NATO はソ連崩壊後の 1997 年に NATO- ウクライナ委員会(NUC:NATO-Ukraine Commission)を設置、2014 年のロシアのクリミア侵攻以降はウクライナの防衛体制の再編強化を支援してきた。2020 年 9 月、Zelenskyy 大統領は NATO とのパートナーシップを柱とする国家セキュリティ戦略を承認した※359。この間、NATO とロシアの対話は膠着した。ソ連崩壊後、NATO はロシアとも「平和のためのパートナーシップ」の枠組みのもとで対話を行っていたが、前述のクリミア侵攻でこの取り組みは挫折した※360。

ウクライナ侵攻直後、NATO はロシアを「最も強い言葉で非難」したが、ウクライナへの直接介入はできず、加盟国の自発的な武器供与等に任せた。こうした NATO の限界がロシアに侵攻を決断させた、という見方がある※361 一方、クリミア侵攻の教訓を生かした NATO の支援が、武力と情報のハイブリッド戦においてウクライナの善戦を引き出した、とする見方もある。

ウクライナ民間人の被害と、中立国が侵攻されかねないという懸念は、Trump 前政権の NATO 軽視戦略で米国との関係に摩擦が生じていた NATO を再結束させ、更なる拡大を促す結果となった※362。地政学的な状況から NATO 非加盟であったフィンランドとスウェーデンでは世論が劇的に変わり、両国は NATO 加盟を検討した※363。一方 NATO は両国の判断としながらこれを歓迎し、加盟手続き中の両国の安全保障に言及した※364。2022 年 5 月 17 日、フィンランド・スウェーデン両国首脳は同時に NATO 加盟を申請する、と正式に発表した※365。

しかし、フィンランド・スウェーデンの NATO 加盟が実現すればロシアにとって大きな誤算であり、NATO 諸国とロシアの更なる緊張は避けられない。5 月 14 日、Putin 大統領はフィンランドの Sauli Niinistö 大統領との電話会談で「NATO 加盟は過ち」であると述べ※366、報復を示唆した。欧州の状況は予断を許さないものとなっている。

COLUMN

Disinformationの脅威とは

「3.4 米国・欧州の情報セキュリティ政策」には Disinformation という耳慣れない言葉が出てきました。定まった日本語訳はなく、しいて言えば「虚偽情報」でしょうか。Misinformation という言葉もありますが、これは「誤報・デマ」に近く、Disinformation はもっとたちが悪い。米国、欧州では、人を騙す・誘導する等の悪意を持って虚偽の情報を作成・配信する場合、その情報を Disinformation と呼ぶことがあります。「フェイクニュース」に近い語感ですが、国家や政治勢力等が自らの利益のために情報を操作する、という文脈でよく用いられるようです。

「3.4 米国・欧州の情報セキュリティ政策」には有害情報（Harmful information）という言葉も出てきました。これは虚偽か否かを問わず、誹謗中傷、人権侵害、暴力扇動等の倫理的に許されない目的で用いられる情報をさしますが、一部 Disinformation にかぶると思われます。

Disinformation は、事実の隠蔽・ねつ造、特定意見への誘導、争議過熱による市民の分断等に加え、ネットニュースや SNS で配信される情報の信頼性の棄損、という IT 社会の根幹を揺るがす問題になる危険性をはらんでいます。その脅威は 2016 年の米国大統領選挙にロシアが介入したとされる事案で顕在化し、それ以来、英国の EU 離脱における混乱、新型コロナウイルス感染拡大における非難合戦、対策における市民の混乱（インフォデミック）、2020 年の米国大統領選挙における「不正選挙」キャンペーンと世論の分断、そしてウクライナ危機における虚実を含む情報戦、と枚挙にいとまがない状態です。

もっとも、情報操作による誘導や混乱は古くからある手口で、IT 固有の問題ではありません。しかし現在の IT プラットフォームは、虚偽情報の生成・配信をかつてない程高精度・低コスト・ピンポイントで行える場となってしまいました。各国政府や IT プラットフォーム事業者、民間の監視機関等も、怪しい情報の検知やコントロールについて政策・技術等あの手この手で対策を取り始めています。しかしまだまだ十分ではなく、当面 Disinformation や有害情報の氾濫は続くのでしょう。

Disinformation に惑わされないためには、政府等の対策に頼るだけでなく、私達一人ひとりの意識も重要だと思います。「人は自分の見たいものしか見ない」は、ユリウス・カエサルの名言ですが、自分の気に入ったソースのコンテンツしか見ない、気の合う人としか話さない環境が、今は実に簡単に作れます。そして、それを狙っているのはネットビジネスだけではありません。人を騙そう、混乱を起こそうとしている勢力の狙う脆弱点でもあるのです。同じ意見を何度も目にする、違う意見は見ない、が続けば、それが当たりだと思うようになっても不思議はありません。

何か大事なことを考えたり決定したりする場合には、いつものソースの情報を見るだけでなく、違うソースの情報を見る、違う人の意見を参考にする等で、少しでも広い視野を持つことはとても大切だと思います。そして、これが Disinformation 対策の第一歩になるのではないかと思います。

※ 1　NISC が重要インフラの運営を担う事業者と、そこで行われるセキュリティ対策を支援する所管省庁が参照すべき指針として公表している「重要インフラの情報セキュリティ対策に係る行動計画」では、「重要インフラ」として 14 分野が定義されている。
NISC：重要インフラグループ　https://www.nisc.go.jp/policy/group/infra/index.html〔2022/4/21 確認〕
※ 2　トレンドマイクロ株式会社：日米独 3 か国のスマートファクトリーにおけるセキュリティ実態調査を発表　https://www.trendmicro.com/ja_jp/about/press-release/2021/pr-20210422-01.html〔2022/4/21 確認〕
トレンドマイクロ株式会社：Whitepaper:The State of Industrial Cybersecurity　https://resources.trendmicro.com/Industrial-Cybersecurity-WP.html〔2022/4/21 確認〕
※ 3　Bridewell Consulting Limited：CNI cyber risks: looking forward to 2025　https://www.bridewellconsulting.com/cni-cyber-risks-looking-forward-to-2025〔2022/4/21 確認〕
※ 4　「マルウェア」等の用語を混在して使用すると、読者を混乱させる可能性があるため、本白書では特に断りのない限り、または文献引用上の正確性を期す必要のない限り、総称して「ウイルス」と表現する。
※ 5　NBC News Digital：50,000 security disasters waiting to happen: The problem of America's water supplies　https://www.nbcnews.com/tech/security/hacker-tried-poison-calif-water-supply-was-easy-entering-password-rcna1206〔2022/4/21 確認〕
※ 6　IPA：制御システム関連のサイバーインシデント事例 8 ～ 2021 年水道局への不正侵入と飲料水汚染未遂～　https://www.ipa.go.jp/files/000093824.pdf〔2022/4/21 確認〕
※ 7　CISA：Alert (AA21-287A) Ongoing Cyber Threats to U.S. Water and Wastewater Systems　https://www.cisa.gov/uscert/ncas/alerts/aa21-287a〔2022/4/21 確認〕
※ 8　IPA：制御システム関連のサイバーインシデント事例 9 ～ 2021 年米国最大手のパイプラインのランサムウェア被害～　https://www.ipa.go.jp/files/000093825.pdf〔2022/4/21 確認〕
※ 9　トヨタ自動車株式会社：2022 年 3 月 国内工場の稼働について（2/28 時点）　https://global.toyota/jp/newsroom/corporate/36960974.html〔2022/4/21 確認〕
トヨタ自動車株式会社：3/2（水）以降の国内工場における稼働再開について　https://global.toyota/jp/newsroom/corporate/36964714.html〔2022/4/21 確認〕
トヨタ自動車株式会社：ウィルス感染被害によるシステム停止事案発生のお知らせ（第２報）　https://www.kojima-tns.co.jp/news/news0003235/〔2022/4/21 確認〕
※ 10 Bleeping Computer：Leading crane maker Palfinger hit in global cyberattack　https://www.bleepingcomputer.com/news/security/leading-crane-maker-palfinger-hit-in-global-cyberattack/〔2022/4/21 確認〕
International Cranes and Specialized Transport：Palfinger attack highlights escalation in cyber crimes　https://www.internationalcranes.media/news/palfinger-attack-highlights-escalation-in-cyber-crimes/8013885.article〔2022/4/21 確認〕
※ 11 ZDNet：Ransomware attack halts production at IoT maker Sierra Wireless　https://www.zdnet.com/article/ransomware-attack-halts-production-at-iot-maker-sierra-wireless/〔2022/4/21 確認〕
※ 12 Bleeping Computer：Food giant JBS Foods shuts down production after cyberattack　https://www.bleepingcomputer.com/news/security/food-giant-jbs-foods-shuts-down-production-after-cyberattack/〔2022/4/21 確認〕
GlobeNewswire, Inc：Media Statement: JBS USA Cybersecurity Attack　https://www.globenewswire.com/news-release/2021/05/31/2239049/0/en/Media-Statement-JBS-USA-Cybersecurity-Attack.html〔2022/4/21 確認〕
※ 13 The Register：UK VoIP telco receives 'colossal ransom demand', reveals REvil cybercrooks suspected of 'organised' DDoS attacks on UK VoIP companies　https://www.theregister.com/2021/09/02/uk_voip_telcos_revil_ransom/〔2022/4/21 確認〕
※ 14 The Register：New Zealand internet outage blamed on DDoS attack on nation's third largest internet provider　https://www.theregister.com/2021/09/03/nz_outage/〔2022/4/21 確認〕
※ 15 THE HILL：Major US candymaker targeted in ransomware attack　https://thehill.com/business-a-lobbying/business-a-lobbying/577576-major-us-candymaker-targeted-in-ransomware-attack〔2022/4/21 確認〕
※ 16 ZDNet：Schreiber Foods back to normal after ransomware attack shuts down milk plants　https://www.zdnet.com/article/schreiber-foods-back-to-normal-after-ransomware-attack-shut-down-milk-plants/〔2022/4/21 確認〕
※ 17 ABC 17：Cyberattack forces Australian TV channel off air　https://abc17news.com/money/2021/03/29/cyberattack-forces-australian-tv-channel-off-air/〔2022/4/21 確認〕
※ 18 BleepingComputer：Cox Media Group confirms ransomware attack that took down broadcasts　https://www.bleepingcomputer.com/news/security/cox-media-group-confirms-ransomware-attack-that-took-down-broadcasts/〔2022/4/21 確認〕
※ 19 BleepingComputer：Sinclair TV stations crippled by weekend ransomware attack　https://www.bleepingcomputer.com/news/security/sinclair-tv-stations-crippled-by-weekend-ransomware-attack/〔2022/4/21 確認〕
※ 20 CPO MAGAZINE：Norwegian Media Company Amedia Suffered a Serious Cyber Attack That Left Newspapers Unprinted　https://www.cpomagazine.com/cyber-security/norwegian-media-company-amedia-suffered-a-serious-cyber-attack-that-left-newspapers-unprinted/〔2022/4/21 確認〕
※ 21 The MediaNews：VTA targeted in apparent ransomware attack, hackers threaten to release trove of data　https://www.mercurynews.com/2021/04/22/cyberattack-targets-vta-unclear-if-personal-information-breached/〔2022/4/21 確認〕
※ 22 Jewish Press：Cyberattacks Cripple Iranian Transportation Infrastructure Twice in Two Days　https://www.jewishpress.com/news/middle-east/iran-news/cyberattacks-cripple-iranian-transportation-infrastructure-twice-in-two-days/2021/07/11/〔2022/4/21 確認〕
※ 23 MobileSyrup：Several TTC services are still down following ransomware attack　https://mobilesyrup.com/2021/11/01/several-ttc-services-are-still-down-following-ransomware-attack/〔2022/4/21 確認〕
※ 24 Industrial Cyber：Ransomware attacks on healthcare networks lead to impact on patient care, delays in procedures　https://industrialcyber.co/article/ransomware-attacks-on-healthcare-networks-lead-to-impact-on-patient-care-delays-in-procedures/〔2022/4/21 確認〕
※ 25 ZDNet：Oxford University lab with COVID-19 research links targeted by hackers　https://www.zdnet.com/article/oxford-university-biochemical-lab-involved-in-covid-19-research-targeted-by-hackers/〔2022/4/21 確認〕
Forbes：Exclusive: Hackers Break Into 'Biochemical Systems' At Oxford University Lab Studying Covid-19　https://www.forbes.com/sites/thomasbrewster/2021/02/25/exclusive-hackers-break-into-biochemical-systems-at-oxford-uni-lab-studying-covid-19/?sh=1af4f092a391〔2022/4/21 確認〕
※ 26 Security Affairs：Another French hospital hit by a ransomware attack　https://securityaffairs.co/wordpress/115434/cyber-crime/french-hospital-ransomware-attack.html〔2022/4/21 確認〕
※ 27 iTWire：Healthcare provider UnitingCare Queensland hit by ransomware　https://itwire.com/security/healthcare-provider-unitingcare-queensland-hit-by-ransomware.html〔2022/4/21 確認〕
※ 28 ComputerWeekly.com：Reports of stolen Irish health service data being leaked online　https://www.computerweekly.com/news/252501064/Reports-of-stolen-Irish-health-service-data-being-leaked-online〔2022/4/21 確認〕
HSE：HSE publishes independent report on Conti cyber attack　https://www.hse.ie/eng/services/news/media/pressrel/hse-publishes-independent-report-on-conti-cyber-attack.html〔2022/4/21 確認〕
U.S. Department of Health & Human Services：Lessons Learned from the HSE Cyber Attack　https://www.hhs.gov/sites/default/files/lessons-learned-hse-attack.pdf〔2022/4/21 確認〕
※ 29 SC MEDIA：Health care ransomware attacks: Oklahoma health system driven to EHR downtime　https://www.scmagazine.com/news/health-care/health-care-ransomware-attacks-oklahoma-health-system-driven-to-ehr-downtime〔2022/4/21 確認〕
※ 30 BleepingComputer：Hive ransomware attacks Memorial Health System, steals patient data　https://www.bleepingcomputer.com/news/security/hive-ransomware-attacks-memorial-health-system-steals-patient-data/〔2022/4/21 確認〕
※ 31 Security Affairs：For the first time, an Israeli hospital was hit by a major ransomware attack　https://securityaffairs.co/wordpress/123350/hacking/israeli-hospital-ransomware-attack.html〔2022/4/21 確認〕
※ 32 BleepingComputer：Cyberattack on BHG opioid treatment network disrupts patient care　https://www.bleepingcomputer.com/news/security/cyberattack-on-bhg-opioid-treatment-network-

disrupts-patient-care/〔2022/4/21 確認〕
※ 33 厚生労働省：医療機関を標的としたランサムウェアによるサイバー攻撃について（注意喚起） https://www.mhlw.go.jp/hourei/doc/tsuchi/T210630U0010.pdf〔2022/4/21 確認〕
※ 34 https://www.honeywell.com/us/en/honeywell-forge/cybersecurity/cybersecurity-threat-report-2021〔2022/4/21 確認〕
※ 35 The Record BY RECORDED FUTURE：FBI: FIN7 hackers target US companies with BadUSB devices to install ransomware https://therecord.media/fbi-fin7-hackers-target-us-companies-with-badusb-devices-to-install-ransomware/〔2022/4/21 確認〕
※ 36 Industrial Cyber：ICS-CERT advisories affecting ICS environments show significant increase in 2021 https://industrialcyber.co/threats-attacks/ics-cert-advisories-affecting-ics-environments-show-significant-increase-in-2021/〔2022/4/21 確認〕
※ 37 ICS-CERT の Web サイトで暦年（1/1 ～ 12/31）ごとに公開された ICSA Advisories の件数をカウントした。ただし、ICSMA（医療機器の脆弱性）は除く。カウントは公表日ベースとした（公表日が 2021 年なら、採番年度が 2020（ICSA-2020-xxx-x）でも 2021 年でカウント）。
CISA：ICS-CERT Advisories https://www.cisa.gov/uscert/ics/advisories〔2022/4/21 確認〕
※ 38 NIST：CVE-2021-44228 Detail https://nvd.nist.gov/vuln/detail/CVE-2021-44228〔2022/4/21 確認〕
※ 39 Industrial Cyber：Log4j vulnerability now hits industrial sector, as CISA calls upon users to identify, mitigate, patch affected products https://industrialcyber.co/news/log4j-vulnerability-now-hits-industrial-sector-as-cisa-calls-upon-users-to-%e2%80%8b%e2%80%8bidentify-mitigate-patch-affected-products/〔2022/4/21 確認〕
※ 40 NIST：CVE-2021-45046 Detail https://nvd.nist.gov/vuln/detail/CVE-2021-45046〔2022/4/21 確認〕
※ 41 The Apache Software Foundation：Apache Log4j Security Vulnerabilities https://logging.apache.org/log4j/2.x/security.html〔2022/4/21 確認〕
CISA：Apache Log4j Vulnerability Guidance https://www.cisa.gov/uscert/apache-log4j-vulnerability-guidance〔2022/4/21 確認〕
JPCERT/CC：Apache Log4j の任意のコード実行の脆弱性（CVE-2021-44228）に関する注意喚起 https://www.jpcert.or.jp/at/2021/at210050.html〔2022/4/21 確認〕
GIGAZINE：Java の Log4j ライブラリで「Log4Shell」に加えて新たな脆弱性「CVE-2021-45046」が発覚、アップデートで対応可能 https://gigazine.net/news/20211216-log4j-log4shell-cve-2021-45046/〔2022/4/21 確認〕
※ 42 BleepingComputer：CISA releases Apache Log4j scanner to find vulnerable apps https://www.bleepingcomputer.com/news/security/cisa-releases-apache-log4j-scanner-to-find-vulnerable-apps/〔2022/4/21 確認〕
CISA：Log4j Scanner https://github.com/cisagov/log4j-scanner〔2022/4/21 確認〕
CISA：EMERGENCY DIRECTIVE 22-02 MITIGATE APACHE LOG4J VULNERABILITY https://www.cisa.gov/emergency-directive-22-02〔2022/4/21 確認〕
※ 43 CyberScoop：FTC warns of potential penalties for firms that fail to fix Log4j software flaws https://www.cyberscoop.com/ftc-warns-of-action-against-firms-that-fail-to-fix-log4j-software-flaws/〔2022/4/21 確認〕
※ 44 iTnews：NAME:WRECK vulnerabilities could impact 100 million servers, IoT devices https://www.itnews.com.au/news/namewreck-vulnerabilities-could-impact-100-million-servers-iot-devices-563286?〔2022/4/21 確認〕
Forescout 社：Forescout and JSOF Disclose New DNS Vulnerabilities, Impacting Millions of Enterprise and Consumer Devices https://www.forescout.com/company/blog/forescout-and-jsof-disclose-new-dns-vulnerabilities-impacting-millions-of-enterprise-and-consumer-devices/〔2022/4/21 確認〕
※ 45 Industrial Cyber：INFRA:HALT vulnerabilities target OT, IoT devices, exploit weakness in NicheStack TCP/IP stack https://industrialcyber.co/article/infrahalt-vulnerabilities-target-ot-iot-devices-exploit-weakness-in-nichestack-tcp-ip-stack-2/〔2022/4/21 確認〕
Forescout 社：INFRA:HALT https://www.forescout.com/research-labs/infra-halt/〔2022/4/21 確認〕
※ 46 SecurityWeek：Serious Vulnerabilities Found in Schneider Electric Power Meters https://www.securityweek.com/serious-vulnerabilities-found-schneider-electric-power-meters〔2022/4/21 確認〕
※ 47 CISA：ICS Advisory (ICSA-21-075-02) GE UR family https://us-cert.cisa.gov/ics/advisories/icsa-21-075-02〔2022/4/21 確認〕
※ 48 The Daily Swig：GE patches serious vulnerabilities in UR power management devices https://portswigger.net/daily-swig/ge-patches-serious-vulnerabilities-in-ur-power-management-devices〔2022/4/21 確認〕
※ 49 Help Net Security：Vulnerabilities in ICS-specific backup solution open industrial facilities to attack https://www.helpnetsecurity.com/2021/04/07/vulnerabilities-ics-specific-backup/〔2022/4/21 確認〕
※ 50 CISA：ICS Advisory (ICSA-21-091-01) https://us-cert.cisa.gov/ics/advisories/icsa-21-091-01〔2022/4/21 確認〕
※ 51 Nozomi Networks, Inc.：OT/IT Security Report：What You Need to Know to Fight Ransomware and IoT Vulnerabilities https://www.nozominetworks.com/downloads/Nozomi-Networks-OT-IoT-Security-Report-2021-07.pdf〔2022/4/21 確認〕
※ 52 SecurityWeek：Ransomware Often Hits Industrial Systems, With Significant Impact: Survey https://www.securityweek.com/ransomware-often-hits-industrial-systems-significant-impact-survey〔2022/4/21 確認〕
Claroty Ltd.：The Global State of Industrial Cybersecurity 2021: Resilience Amid Disruption https://claroty.com/wp-content/uploads/2022/02/Claroty_Report_State_of_Industrial_Cybersecurity_2021.pdf〔2022/4/21 確認〕
※ 53 https://www.cisa.gov/global〔2022/4/21 確認〕
※ 54 Industrial Cyber：CISA Global aims at international alliance to combat cyber threats https://industrialcyber.co/news/cisa/cisa-global-aims-at-international-alliance-to-combat-cyber-threats/〔2022/4/21 確認〕
※ 55 CISA：Rising Ransomware Threat to Operational Technology Assets https://www.cisa.gov/sites/default/files/publications/CISA_Fact_Sheet-Rising_Ransomware_Threat_to_OT_Assets_508C.pdf〔2022/4/21 確認〕
※ 56 Industrial Cyber：CISA releases guidelines to critical infrastructure owners, operators in light of rising ransomware attacks https://industrialcyber.co/article/cisa-releases-guidelines-to-critical-infrastructure-owners-operators-in-light-of-rising-ransomware-attacks/〔2022/4/21 確認〕
※ 57 https://www.cisa.gov/jcdc〔2022/4/21 確認〕
※ 58 The White House：National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-security-memorandum-on-improving-cybersecurity-for-critical-infrastructure-control-systems/〔2022/4/21 確認〕
※ 59 BleepingComputer：New US security memorandum bolsters critical infrastructure cybersecurity https://www.bleepingcomputer.com/news/security/new-us-security-memorandum-bolsters-critical-infrastructure-cybersecurity/〔2022/4/21 確認〕
※ 60 BleepingComputer：Biden issues executive order to increase U.S. cybersecurity defenses https://www.bleepingcomputer.com/news/security/biden-issues-executive-order-to-increase-us-cybersecurity-defenses/〔2022/4/21 確認〕
The White House：Executive Order on Improving the Nation's Cybersecurity https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/〔2022/4/21 確認〕
※ 61 CyberScoop：White House rolls out pipeline, supply chain security initiatives as companies pledge billions in cyber spending https://www.cyberscoop.com/biden-cybersecurity-summit-nist-ics/〔2022/4/21 確認〕
※ 62 DOE：Biden Administration Takes Bold Action to Protect Electricity Operations from Increasing Cyber Threats https://www.energy.gov/articles/biden-administration-takes-bold-action-protect-electricity-operations-increasing-cyber-0〔2022/4/21 確認〕
The White House：Statement by NSC Spokesperson Emily Horne on the Biden Administration's Efforts to Protect U.S. Critical Infrastructure https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/20/statement-by-nsc-spokesperson-emily-horne-on-the-biden-administrations-efforts-to-protect-u-s-critical-infrastructure/〔2022/4/21 確認〕
The Office of the Federal Register：Notice of Request for Information (RFI) on Ensuring the Continued Security of the United States Critical Electric Infrastructure https://www.federalregister.

gov/documents/2021/04/22/2021-08482/notice-of-request-for-information-rfi-on-ensuring-the-continued-security-of-the-united-states〔2022/4/21 確認〕

※ 63 CISON PRWeb：NATO Energy Security Center for Excellence and ISA Establish Cooperative Agreement on Cybersecurity Standards https://www.prweb.com/releases/nato_energy_security_center_for_excellence_and_isa_establish_cooperative_agreement_on_cybersecurity_standards/prweb17783764.htm〔2022/4/21 確認〕

※ 64 World Economic Forum：Cyber Resilience in the Oil and Gas Industry：Playbook for Boards and Corporate Officers https://www.weforum.org/whitepapers/cyber-resilience-in-the-oil-and-gas-industry-playbook-for-boards-and-corporate-officers〔2022/4/21 確認〕

※ 65 Help Net Security：Enhancing cyber resilience in the oil and gas industry https://www.helpnetsecurity.com/2021/05/26/cyber-resilience-oil-gas/〔2022/4/21 確認〕

※ 66 https://attack.mitre.org/〔2022/4/21 確認〕

※ 67 The MITRE Corporation：Updates - October 2021 https://attack.mitre.org/resources/updates/updates-october-2021/〔2022/4/21 確認〕

※ 68 Industrial Cyber：MITRE ATT&CK v10 comes with new techniques, groups, software for enterprises, ICS frameworks https://industrialcyber.co/article/mitre-attck-v10-comes-with-new-techniques-groups-software-for-enterprises-ics-frameworks/〔2022/4/21 確認〕

※ 69 Parliament of Australia：Security Legislation Amendment (Critical Infrastructure) Bill 2021 https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bld=r6657〔2022/4/21 確認〕

※ 70 Clayton Utz：Significant reform to Australia's cyber security laws with passage of critical infrastructure reforms https://www.claytonutz.com/knowledge/2021/december/significant-reform-to-australias-cyber-security-laws-with-passage-of-critical-infrastructure-reforms〔2022/4/21 確認〕

※ 71 https://www.nisc.go.jp/pdf/policy/kihon-s/cs2021.pdf〔2022/4/21 確認〕

※ 72 https://www.nisc.go.jp/pdf/policy/infra/infra_rt4_r2.pdf〔2022/4/21 確認〕

※ 73 NISC：ランサムウェアによるサイバー攻撃に関する注意喚起について https://www.nisc.go.jp/pdf/policy/infra/ransomware20210430.pdf〔2022/4/21 確認〕

※ 74 https://security-portal.nisc.go.jp/〔2022/4/21 確認〕

※ 75 https://security-portal.nisc.go.jp/stopransomware/〔2022/4/21 確認〕

※ 76 経済産業省:「インド太平洋地域向け日米産業制御システムサイバーセキュリティウィーク」を実施しました https://www.meti.go.jp/press/2020/03/20210315001/20210315001.html〔2022/4/21 確認〕

※ 77 経済産業省：「インド太平洋地域向け日米 EU 産業制御システムサイバーセキュリティウィーク」を実施しました https://www.meti.go.jp/press/2021/11/20211101001/20211101001.html〔2022/4/21 確認〕

※ 78 IPA：制御システムのセキュリティリスク分析ガイド補足資料：「制御システム関連のサイバーインシデント事例」シリーズ https://www.ipa.go.jp/security/controlsystem/incident.html〔2022/4/21 確認〕

※ 79 NIST：National Vulnerability Database（NVD） https://nvd.nist.gov/〔2022/4/26 確認〕

※ 80 IPA：JVN iPedia 脆弱性対策情報データベース https://jvndb.jvn.jp/〔2022/4/26 確認〕

※ 81 「情報セキュリティ白書 2020」の「表 3-2-1 IoT 機器に感染するウイルスの分類」(p.166)を参照。

※ 82 Mirai の詳細に関しては、IPA の「情報セキュリティ 10 大脅威 2017」（https://www.ipa.go.jp/security/vuln/10threats2017.html〔2022/4/26 確認〕）の「3.1.IoT におけるセキュリティ脅威の顕在化」(p.71-74)を参照。

※ 83 感染した IoT 機器上で不正なプログラムを実行し、ボットネットを構成するとともに、DDoS 攻撃の踏み台等のサイバー攻撃への悪用を試みるウイルス。典型例である「Mirai」や「Gafgyt（別名、Bashlite、QBot 等）」は、それぞれソースコードが公開されており、様々な亜種が出現している。

※ 84 VPNFilter の詳細に関しては、「情報セキュリティ白書 2019」の「3.2.1 (3) VPNFilter」(p.168)を参照。

※ 85 C&C サーバ：Command and Control サーバの略。ウイルス等により乗っ取ったコンピュータ等（ここでは IoT 機器）に対し、遠隔から命令を送り制御するサーバ。

※ 86 The United States Department of Justice：Justice Department Announces Actions to Disrupt Advanced Persistent Threat 28 Botnet of Infected Routers and Network Storage Devices https://www.justice.gov/opa/pr/justice-department-announces-actions-disrupt-advanced-persistent-threat-28-botnet-infected〔2022/4/26 確認〕

※ 87 Trend Micro Incorporated：VPNFilter Two Years Later: Routers Still Compromised https://www.trendmicro.com/en_us/research/21/a/vpnfilter-two-years-later-routers-still-compromised-.html〔2022/4/26 確認〕
トレンドマイクロ株式会社:ルータや NAS に感染する IoT ボット「VPNFilter」の流行から 2 年、その現状と課題を解説 https://blog.trendmicro.co.jp/archives/27775〔2022/4/26 確認〕

※ 88 Satori の詳細に関しては、「情報セキュリティ白書 2018」の「3.1.1 (3) (d) Satori/Okiru」(p.164)を参照。

※ 89 警察庁：脆弱性が存在する複数の IoT 機器を標的としたアクセスの増加等について https://www.npa.go.jp/cyberpolice/detect/pdf/20210305.pdf〔2022/4/26 確認〕

※ 90 Qihoo 360 Technology Co., Ltd.：New Threat: Matryosh Botnet Is Spreading https://blog.netlab.360.com/matryosh-botnet-is-spreading-en/〔2022/4/26 確認〕

※ 91 Moobot の詳細に関しては、「情報セキュリティ白書 2020」の「3.2.1 (1) (h) Moobot」(p.172)を参照。

※ 92 LeetHozer の詳細に関しては、「情報セキュリティ白書 2021」の「3.2.1 (9) Moobot の亜種『LeetHozer』」(p.200)を参照。

※ 93 Qihoo 360 Technology Co., Ltd.：Fbot is now riding the traffic and transportation smart devices https://blog.netlab.360.com/fbot-is-now-riding-the-traffic-and-transportation-smart-devices-en/〔2022/4/26 確認〕
Palo Alto Networks, Inc.：Satori: Mirai Botnet Variant Targeting Vantage Velocity Field Unit RCE Vulnerability https://unit42.paloaltonetworks.com/satori-mirai-botnet-variant-targeting-vantage-velocity-field-unit-rce-vulnerability/〔2022/4/26 確認〕
パロアルトネットワークス株式会社：Mirai ボットネット亜種 Satori が Vantage Velocity フィールドユニットのリモートコード実行 (RCE) 脆弱性を標的に https://unit42.paloaltonetworks.jp/satori-mirai-botnet-variant-targeting-vantage-velocity-field-unit-rce-vulnerability/〔2022/4/26 確認〕

※ 94 fbot：Satori と同一の作成者 Nexus-Zeta による Mirai の亜種の一つ。fbot の詳細に関しては、「情報セキュリティ白書 2020」の「3.2.1 (1) (b) fbot」(p.167)を参照。

※ 95 Qihoo 360 Technology Co., Ltd.:New Threat: ZHtrap botnet implements honeypot to facilitate finding more victims https://blog.netlab.360.com/new_threat_zhtrap_botnet_en/〔2022/4/26 確認〕

※ 96 Palo Alto Networks, Inc.：New Mirai Variant Targeting Network Security Devices https://unit42.paloaltonetworks.com/mirai-variant-iot-vulnerabilities/〔2022/4/26 確認〕
パロアルトネットワークス株式会社：ネットワークセキュリティ機器を標的にする新しい Mirai 亜種 https://unit42.paloaltonetworks.jp/mirai-variant-iot-vulnerabilities/〔2022/4/26 確認〕

※ 97 Darren Martyn：VisualDoor: SonicWall SSL-VPN Exploit https://darrenmartyn.ie/2021/01/24/visualdoor-sonicwall-ssl-vpn-exploit/〔2022/4/26 確認〕

※ 98 Qihoo 360 Technology Co., Ltd.:Mirai_ptea Botnet is Exploiting Undisclosed KGUARD DVR Vulnerability https://blog.netlab.360.com/mirai_ptea-botnet-is-exploiting-undisclosed-kguard-dvr-vulnerability-en/〔2022/4/26 確認〕

※ 99 Palo Alto Networks, Inc.：New Mirai Variant Targets WebSVN Command Injection Vulnerability (CVE-2021-32305) https://unit42.paloaltonetworks.com/cve-2021-32305-websvn/〔2022/4/26 確認〕
パロアルトネットワークス株式会社：新たな Mirai 亜種 WebSVN のコマンドインジェクション脆弱性（CVE-2021-32305）を標的に https://unit42.paloaltonetworks.jp/cve-2021-32305-websvn/〔2022/4/26 確認〕

※ 100 Qihoo 360 Technology Co., Ltd.：Mirai_ptea_Rimasuta variant is exploiting a new RUIJIE router 0 day to spread https://blog.netlab.360.com/rimasuta-spread-with-ruijie-0day-en/〔2022/4/26 確認〕

※ 101 Qihoo 360 Technology Co., Ltd.：Gafgtyt_tor and Necro are on the move again https://blog.netlab.360.com/gafgtyt_tor-and-necro-are-on-the-move-again/〔2022/4/26 確認〕

※ 102 Mozi の詳細に関しては、「情報セキュリティ白書 2020」の「3.2.1 (1) (n) Mozi」(p.175)を参照。

※ 103 Qihoo 360 Technology Co., Ltd.：The Mostly Dead Mozi and Its' Lingering Bots https://blog.netlab.360.com/the-mostly-dead-mozi-and-its-lingering-bots/〔2022/4/26 確認〕

※ 104 Lumen Technologies, Inc.：New Mozi Malware Family Quietly Amasses IoT Bots https://blog.lumen.com/new-mozi-malware-family-quietly-amasses-iot-bots/〔2022/4/26 確認〕
※ 105 Tencent Holdings Limited：深度追踪 Mozi 僵尸网络：360 安全大脑精准溯源，揪出幕后黑手 https://mp.weixin.qq.com/s/Su0-uU5JaUrAh8ptTzTCsA〔2022/4/26 確認〕
※ 106 Qihoo 360 Technology Co., Ltd.（Twitter アカウント）：https://twitter.com/360Netlab/status/1420390398825058313〔2022/4/26 確認〕
※ 107 Microsoft 社：How to proactively defend against Mozi IoT botnet https://www.microsoft.com/security/blog/2021/08/19/how-to-proactively-defend-against-mozi-iot-botnet/〔2022/4/26 確認〕
※ 108 Qihoo 360 Technology Co., Ltd.：Necro is going to version 3 and using PyInstaller and DGA https://blog.netlab.360.com/necro/〔2022/4/26 確認〕
※ 109 Qihoo 360 Technology Co., Ltd.：Necro upgrades again, using Tor + dynamic domain DGA and aiming at both Windows & Linux https://blog.netlab.360.com/necro-upgrades-again-using-tor-dynamic-domain-dga-and-aiming-at-both-windows-linux/〔2022/4/26 確認〕
※ 110 Qihoo 360 Technology Co., Ltd.：QNAP NAS users, make sure you check your system https://blog.netlab.360.com/qnap-nas-users-make-sure-you-check-your-system/〔2022/4/26 確認〕
※ 111 QNAP Systems, Inc.：Multiple Vulnerabilities in Helpdesk https://www.qnap.com/en/security-advisory/QSA-20-08〔2022/4/26 確認〕
※ 112 QNAP Systems, Inc.：Security Advisory for eCh0raix Ransomware https://www.qnap.com/en/security-advisory/nas-201907-11〔2022/4/26 確認〕
※ 113 QNAP Systems, Inc.：eCh0raix Ransomware https://www.qnap.com/en/security-advisory/QSA-20-02〔2022/4/26 確認〕
※ 114 QNAP Systems, Inc.：eCh0raix Ransomware https://www.qnap.com/en/security-advisory/QSA-21-18〔2022/4/26 確認〕
※ 115 QNAP Systems, Inc.：Improper Authorization Vulnerability in HBS 3 (Hybrid Backup Sync) https://www.qnap.com/en/security-advisory/QSA-21-13〔2022/4/26 確認〕
QNAP Systems, Inc.:Qlockerによるランサムウェア攻撃に対するご案内: QNAP NAS を安全にお使いいただくために https://www.qnap.com/ja-jp/security-news/2021/qlocker- によるランサムウェア攻撃に対するご案内 qnap-nas- を安全にお使いいただくために〔2022/4/26 確認〕
※ 116 Palo Alto Networks, Inc.：New eCh0raix Ransomware Variant Targets QNAP and Synology Network-Attached Storage Devices https://unit42.paloaltonetworks.com/ech0raix-ransomware-soho/〔2022/4/26 確認〕
パロアルトネットワークス株式会社：QNAP/Synology の両 NAS デバイスを標的とする新たな eCh0raix ランサムウェア亜種 https://unit42.paloaltonetworks.jp/ech0raix-ransomware-soho/〔2022/4/26 確認〕
※ 117 Qihoo 360 Technology Co., Ltd.：EwDoor Botnet Is Attacking AT&T Customers https://blog.netlab.360.com/warning-ewdoor-botnet-is-attacking-att-customers/〔2022/4/26 確認〕
※ 118 NucleusNET：Mentor Graphics Corporation 製組み込み用リアルタイムオペレーティングシステム Nucleus RTOS の TCP/IP スタック
※ 119 Forescout Technologies, Inc.：NUMBER:JACK – Forescout Research Labs Finds Nine ISN Generation Vulnerabilities Affecting TCP/IP Stacks https://www.forescout.com/blog/numberjack-forescout-research-labs-finds-nine-isn-generation-vulnerabilities-affecting-tcpip-stacks/〔2022/4/26 確認〕
※ 120 JVN：JVNVU#90767599 複数の TCP/IP スタック製品における初期シーケンス番号の脆弱性 https://jvn.jp/vu/JVNVU90767599/〔2022/4/26 確認〕
※ 121 ICS-CERT：ICS Advisory (ICSA-21-042-01) Multiple Embedded TCP/IP Stacks (Update B) https://www.cisa.gov/uscert/ics/advisories/icsa-21-042-01〔2022/4/26 確認〕
※ 122 Forescout Technologies, Inc.：Forescout and JSOF Disclose New DNS Vulnerabilities, Impacting Millions of Enterprise and Consumer Devices https://www.forescout.com/blog/forescout-and-jsof-disclose-new-dns-vulnerabilities-impacting-millions-of-enterprise-and-consumer-devices/〔2022/4/26 確認〕
※ 123 https://www.forescout.com/resources/namewreck-breaking-and-fixing-dns-implementations/〔2022/4/26 確認〕
※ 124 Tenable, Inc.：Multiple Vulnerabilities in Buffalo and Arcadyan manufactured routers https://www.tenable.com/security/research/tra-2021-13〔2022/4/26 確認〕
※ 125 株式会社バッファロー：【更新】一部ルーター商品における複数の脆弱性とその対策方法 https://www.buffalo.jp/news/detail/20220207-02.html〔2022/4/26 確認〕
※ 126 CERT/CC：Arcadyan-based routers and modems vulnerable to authentication bypass, Vulnerability Note VU#914124 https://kb.cert.org/vuls/id/914124〔2022/4/26 確認〕
※ 127 Microsoft 社：“BadAlloc” – Memory allocation vulnerabilities could affect wide range of IoT and OT devices in industrial, medical, and enterprise networks https://msrc-blog.microsoft.com/2021/04/29/badalloc-memory-allocation-vulnerabilities-could-affect-wide-range-of-iot-and-ot-devices-in-industrial-medical-and-enterprise-networks/〔2022/4/26 確認〕
※ 128 ICS-CERT：ICS Advisory (ICSA-21-119-04) Multiple RTOS (Update E) https://www.cisa.gov/uscert/ics/advisories/icsa-21-119-04〔2022/4/26 確認〕
※ 129 Check Point Software Technologies LTD.：Security probe of Qualcomm MSM data services https://research.checkpoint.com/2021/security-probe-of-qualcomm-msm/〔2022/4/26 確認〕
※ 130 Nozomi Networks Inc.：New IoT Security Risk: ThroughTek P2P Supply Chain Vulnerability https://www.nozominetworks.com/blog/new-iot-security-risk-throughtek-p2p-supply-chain-vulnerability/〔2022/4/26 確認〕
※ 131 Mandiant, Inc.：Mandiant Discloses Critical Vulnerability Affecting Millions of IoT Devices https://www.mandiant.com/resources/mandiant-discloses-critical-vulnerability-affecting-iot-devices〔2022/4/26 確認〕
※ 132 JFrog Ltd：INFRA:HALT 14 New Security Vulnerabilities Found in NicheStack https://jfrog.com/blog/infrahalt-14-new-security-vulnerabilities-found-in-nichestack/〔2022/4/26 確認〕
JFrog Ltd：INFRA:HALT NicheStack に新たな 14 件のセキュリティ脆弱性が発見される https://jfrog.com/ja/blog/infrahalt-14-new-security-vulnerabilities-found-in-nichestack/〔2022/4/26 確認〕
※ 133 IoT Inspector GmbH（現、ONEKEY GmbH）：Advisory: Multiple issues in Realtek SDK affect hundreds of thousands of devices down the supply chain https://onekey.com/blog/advisory-multiple-issues-realtek-sdk-iot-supply-chain/〔2022/6/6 確認〕
※ 134 Forescout Technologies, Inc.：New Critical Vulnerabilities Found on Nucleus TCP/IP Stack https://www.forescout.com/blog/new-critical-vulnerabilities-found-on-nucleus-tcp-ip-stack/〔2022/4/26 確認〕
※ 135 ICS-CERT：ICS Advisory (ICSA-21-313-03) Siemens Nucleus RTOS TCP/IP Stack https://www.cisa.gov/uscert/ics/advisories/icsa-21-313-03〔2022/4/26 確認〕
※ 136 Check Point Software Technologies LTD.：Check Point Research discover vulnerabilities in smartphones chips embedded in 37% of smartphones around the world https://blog.checkpoint.com/2021/11/24/check-point-research-discover-vulnerabilities-in-smartphones-chips-embedded-in-37-of-smartphones-around-the-world/〔2022/4/26 確認〕
※ 137 New York University Abu Dhabi：FragAttacks: Security flaws in all Wi-Fi devices https://www.fragattacks.com/〔2022/4/26 確認〕
※ 138 Wi-Fi Alliance：Wi-Fi Protected Access Security Considerations, May 2021 https://www.wi-fi.org/download.php?file=/sites/default/files/private/Security_Considerations_20210511.pdf〔2022/4/26 確認〕
※ 139 CERT/CC：Devices supporting Bluetooth Core and Mesh Specifications are vulnerable to impersonation attacks and AuthValue disclosure, Vulnerability Note VU#799380 https://kb.cert.org/vuls/id/799380〔2022/4/26 確認〕
※ 140 Bluetooth SIG, Inc.：Reporting Security Vulnerabilities https://www.bluetooth.com/learn-about-bluetooth/key-attributes/bluetooth-security/reporting-security/〔2022/4/26 確認〕
Bluetooth SIG, Inc.：Bluetooth SIG Statement Regarding the ‘Malleable Commitment’ Vulnerability https://www.bluetooth.com/learn-about-bluetooth/key-attributes/bluetooth-security/malleable/〔2022/4/26 確認〕
※ 141 日本電気株式会社：Aterm シリーズにおける複数の脆弱性 https://jpn.nec.com/security-info/secinfo/nv21-005.html〔2022/4/26 確認〕
株式会社インプレス：NEC 製無線 LAN ルーター 3 機種に脆弱性。2 機種はファームウェアアップデートで対策可能 https://pc.watch.impress.co.jp/docs/news/1302295.html〔2022/4/26 確認〕
※ 142 エレコム株式会社：無線 LAN ルーターなどネットワーク製品の一部における脆弱性に関して https://www.elecom.co.jp/news/security/20210126-01/〔2022/4/26 確認〕

株式会社インプレス：エレコムのルーターなどで脆弱性。サポート終了のため使用中止を勧告　https://pc.watch.impress.co.jp/docs/news/1302714.html〔2022/4/26 確認〕
※ 143 日本電気株式会社：複数の Aterm 製品における脆弱性　https://jpn.nec.com/security-info/secinfo/nv21-008.html〔2022/4/26 確認〕
株式会社インプレス：NEC 製 Wi-Fi ルーター「Aterm」シリーズに複数の脆弱性報告　https://k-tai.watch.impress.co.jp/docs/news/1317677.html〔2022/4/26 確認〕
※ 144 株式会社バッファロー：【更新】ルーター等の一部商品におけるデバッグオプションの脆弱性とその対処方法　https://www.buffalo.jp/news/detail/20210506-01.html〔2022/4/26 確認〕
株式会社インプレス:バッファローの一部 Wi-Fi ルーターなどに脆弱性、「製品の使用停止」を推奨　https://k-tai.watch.impress.co.jp/docs/news/1322908.html〔2022/4/26 確認〕
※ 145 エレコム株式会社：無線 LAN ルーターなどネットワーク製品の一部における脆弱性に関して　https://www.elecom.co.jp/news/security/20210706-01/〔2022/4/26 確認〕
株式会社インプレス：エレコム製ルーターに脆弱性。修正はなく使用中止を勧告　https://pc.watch.impress.co.jp/docs/news/1336252.html〔2022/4/26 確認〕
※ 146 https://notice.go.jp/〔2022/4/26 確認〕
※ 147 https://notice.go.jp/status〔2022/4/26 確認〕
※ 148 IoT Inspector GmbH（ 現、ONEKEY GmbH）：Hackers welcome: Major security test uncovers vulnerabilities in all common Wi-Fi routers　https://onekey.com/blog/router-security-check-2021/〔2022/6/6 確認〕
※ 149 ティーピーリンクジャパン株式会社：IoT Inspector から報告された ArcherAX6000 の脆弱性に関して　https://www.tp-link.com/jp/support/faq/3252/〔2022/4/26 確認〕
※ 150 Linksys：現在は、台湾 Foxconn Technology Group（鴻海科技集団／富士康科技集団）に買収され、同社ネットワーク製品のブランド名となっている。
※ 151 https://www.iot-inspector.com/wp-content/uploads/2021/11/Chip-IoT-Inspector-Router-Sicherheit-Test.pdf〔2022/4/26 確認〕
※ 152 Federal Register：Improving the Nation's Cybersecurity　https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity〔2022/4/26 確認〕
※ 153 https://www.nist.gov/system/files/documents/2021/08/31/IoT%20White%20Paper%20-%20Final%202021-08-31.pdf〔2022/4/26 確認〕
※ 154 https://www.nist.gov/system/files/documents/2021/12/03/FINAL_Consumer_IoT_Label_Discussion_Paper_20211202.pdf〔2022/4/26 確認〕
※ 155 https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.02042022-2.pdf〔2022/4/26 確認〕
※ 156 Cyber Security Agency of Singapore：Cybersecurity Labelling Scheme (CLS)　https://www.csa.gov.sg/Programmes/certification-and-labelling-schemes/cybersecurity-labelling-scheme/about-cls〔2022/4/26 確認〕
※ 157 Cyber Security Agency of Singapore：CSA Pushes Ahead with Efforts to Improve IOT Security　https://www.csa.gov.sg/News/Press-Releases/csa-pushes-ahead-with-efforts-to-improve-iot-security〔2022/4/26 確認〕
※ 158 Finnish Transport and Communications Agency（Traficom）：Finland becomes the first European country to certify safe smart devices – new Cybersecurity label helps consumers buy safer products　https://www.traficom.fi/en/news/finland-becomes-first-european-country-certify-safe-smart-devices-new-cybersecurity-label〔2022/4/26 確認〕
※ 159 経済産業省：機器のサイバーセキュリティ確保のためのセキュリティ検証の手引きを取りまとめました　https://www.meti.go.jp/press/2021/04/20210419003/20210419003.html〔2022/4/26 確認〕
※ 160 総務省：「ICT サイバーセキュリティ総合対策 2021」（案）に対する意見募集の結果及び「ICT サイバーセキュリティ総合対策 2021」の公表　https://www.soumu.go.jp/menu_news/s-news/02cyber01_04000001_00192.html〔2022/4/26 確認〕
※ 161 IPA：「IoT 開発におけるセキュリティ設計の手引き」を公開　https://www.ipa.go.jp/security/iot/iotguide.html〔2022/4/26 確認〕
※ 162 https://www.ccds.or.jp/public/document/other/CCDS_SecGuide-IoTReq_2021_v2.0_jpn.pdf〔2022/4/26 確認〕
※ 163 「情報セキュリティ白書 2021」の「3.2.4（4）民間における取り組み」（p.209）を参照。
※ 164 https://www.ccds.or.jp/public/document/other/CCDS_SecGuide-IoTReq_2021-extra_v2.0_jpn.pdf〔2022/4/26 確認〕
※ 165 https://www.ccds.or.jp/public/document/other/CCDS_IoTReq_2021-checklist_v1.0_jpn.xlsx〔2022/4/26 確認〕
※ 166 https://cloudsecurityalliance.jp/site/WG_PUB/IoT_WG/CSA-Guide-to-the-IoT-Security-Controls-Framework-Version-2_J.pdf〔2022/4/26 確認〕
※ 167 https://cloudsecurityalliance.jp/site/WG_PUB/IoT_WG/CSA%20IoT%20Security%20Controls%20Framework%20Version%202_J.xlsx〔2022/4/26 確認〕
※ 168 一般社団法人セキュア IoT プラットフォーム協議会：「IoT セキュリティ手引書 Ver2.0」をリリース ～ IoT ビジネスに関わる事業者向けにセキュリティの課題と対応策のガイドラインを提示～　https://www.secureiotplatform.org/release/2022-01-31〔2022/4/26 確認〕
※ 169 ISO：ISO/IEC 30147:2021 Information technology - Internet of things - Methodology for trustworthiness of IoT system/service　https://www.iso.org/standard/53267.html〔2022/4/26 確認〕
IEC：ISO/IEC 30147:2021 Internet of Things (IoT) - Integration of IoT trustworthiness activities in ISO/IEC/IEEE 15288 system engineering processes　https://webstore.iec.ch/publication/62644〔2022/4/26 確認〕
※ 170 トラストワージネス：セキュリティ、プライバシー、セーフティ、リライアビリティ、レジリエンス等によって、システムがその関係者の期待に応える能力。
※ 171 https://csrc.nist.gov/publications/detail/nistir/8259b/final〔2022/4/26 確認〕
※ 172 https://csrc.nist.gov/publications/detail/sp/800-213/final〔2022/4/26 確認〕
※ 173 https://csrc.nist.gov/publications/detail/sp/800-213a/final〔2022/4/26 確認〕
※ 174 ENISA：Cybersecurity Certification: Candidate EUCC Scheme V1.1.1　https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme-v1-1.1〔2022/4/26 確認〕
※ 175 ETSI：ETSI releases test specification to comply with world-leading Consumer IoT Security standard　https://www.etsi.org/newsroom/press-releases/1983-2021-10-etsi-releases-test-specification-to-comply-with-world-leading-consumer-iot-security-standard〔2022/4/26 確認〕
ETSI：ETSI TS 103 701 V1.1.1 (2021-08)　https://www.etsi.org/deliver/etsi_ts/103700_103799/103701/01.01.01_60/ts_103701v010101p.pdf〔2022/4/26 確認〕
※ 176 https://juas.or.jp/cms/media/2021/04/JUAS_IT2021.pdf〔2022/5/23 確認〕
※ 177 https://www.ipa.go.jp/files/000087025.pdf〔2022/5/23 確認〕
※ 178 https://www.soumu.go.jp/johotsusintokei/statistics/pdf/HR202000_002.pdf〔2022/5/23 確認〕
※ 179 パロアルトネットワークス株式会社：クラウドネイティブセキュリティジャパンサーベイ 2021 年版　https://start.paloaltonetworks.jp/2021-state-of-cloud-native-security-japan-survey.html〔2022/5/23 確認〕
※ 180 Gartner, Inc.：Gartner Says Four Trends Are Shaping the Future of Public Cloud https://www.gartner.com/en/newsroom/press-releases/2021-08-02-gartner-says-four-trends-are-shaping-the-future-of-public-cloud〔2022/5/23 確認〕
※ 181 株式会社 LegalForce：【LegalForce 調査レポート】SaaS 活用者の約 7 割が「SaaS の活用により、DX が進んだ」と回答～ SaaS の活用に関する実態調査を公表～　https://legalforce-corp.com/3381/〔2022/5/23 確認〕
※ 182 IPA：企業・組織におけるテレワークのセキュリティ実態調査　https://www.ipa.go.jp/security/fy2021/reports/scrm/index-telework.html〔2022/6/30 確認〕
※ 183 株式会社コナミデジタルエンタテインメント、株式会社コナミアミューズメント：第三者のアクセスによる情報流出について　https://www.konami.com/games/corporate/ja/news/topics/20210301a/〔2022/4/11 確認〕
※ 184 Salesforce は株式会社セールスフォース・ドットコム（現在の社名は株式会社セールスフォース・ジャパン）が提供するアプリケーションである。
※ 185 神戸市：情報共有アプリ「KOBE ぽすと」システムへの第三者によるアクセスについて　https://www.city.kobe.lg.jp/a57337/shise/press/908644162304.html〔2022/5/23 確認〕
※ 186 https://www.ipa.go.jp/files/000094186.pdf〔2022/5/23 確認〕
※ 187 NISC：Salesforce の製品の設定不備による意図しない情報が外部から参照される可能性について　https://www.nisc.go.jp/pdf/policy/infra/salesforce20210129.pdf〔2022/5/23 確認〕

※ 188 ネットマーケティング社：不正アクセスによる会員様情報流出に関するお詫びとお知らせ https://www.net-marketing.co.jp/news/5873/〔2022/5/23 確認〕
ネットマーケティング社：不正アクセスによる会員様情報流出の調査結果と今後の対応について https://www.net-marketing.co.jp/news/6001/〔2022/5/23 確認〕
※ 189 特定非営利活動法人結婚相手紹介サービス業認証機構：インターネット型結婚相手紹介サービス業認証制度の認証基準を一部改訂しました。 https://www.ims-npo.org/pdf/220317_info.pdf〔2022/5/23 確認〕
※ 190 Codecov 社：Bash Uploader Security Update https://about.codecov.io/security-update/〔2022/5/23 確認〕
※ 191 メルカリ社：「Codecov」への第三者からの不正アクセスによる当社への影響および一部顧客情報等の流出について https://about.mercari.com/press/news/articles/20210521_incident_report/〔2022/5/23 確認〕
メルカリ社：【調査結果のご報告】「Codecov」への第三者からの不正アクセスによる当社への影響および一部顧客情報等の流出について https://about.mercari.com/security/news/articles/20210806_incident_report/〔2022/5/23 確認〕
※ 192 SB テクノロジー株式会社：当社が管理するメール中継システムによる外部メール不正中継について https://www.softbanktech.co.jp/news/topics/info/2022/006/〔2022/5/23 確認〕
SB テクノロジー株式会社：当社が管理するメール中継システムによる外部メール不正中継について（第二報） https://www.softbanktech.co.jp/news/topics/info/2022/007/〔2022/5/23 確認〕
※ 193 キヤノンマーケティングジャパン株式会社：情報セキュリティ意識に関する実態調査レポート 2021 ～コロナ禍で高まる「シャドー IT」の情報セキュリティリスク～ https://eset-info.canon-its.jp/malware_info/special/detail/210708.html〔2022/5/23 確認〕
キヤノンマーケティングジャパン株式会社：情報セキュリティ意識に関する実態調査レポート～把握しておくべき『シャドー IT』の実態について～ https://eset-info.canon-its.jp/malware_info/trend/detail/200313.html〔2022/5/23 確認〕
※ 194 https://www.soumu.go.jp/main_content/000771515.pdf〔2022/5/23 確認〕
※ 195 SLA（Service Level Agreement）：サービス事業者と利用者の間で結ばれるサービスのレベル（定義、範囲、内容、達成目標等）に関する合意サービス水準、サービス品質保証のこと。
※ 196 IBM Corporation：2021 IBM Security X-Force Cloud Threat Landscape Report https://www.ibm.com/downloads/cas/WMDZOWK6〔2022/5/23 確認〕
※ 197 株式会社東京商工リサーチ：上場企業の個人情報漏えい・紛失事故は、調査開始以来最多の 137 件 574 万人分（2021 年） https://www.tsr-net.co.jp/news/analysis/20210117_01.html〔2022/5/23 確認〕
※ 198 認証と認定は制度によってどちらも使われることがある。それらを総称してセキュリティ認証と表記している。
※ 199 JCISPA：JASA - クラウドセキュリティ推進協議会 https://jcispa.jasa.jp/〔2022/5/23 確認〕
※ 200 一般社団法人情報マネジメントシステム認定センター：ISMS 適合性評価制度 https://isms.jp/isms.html〔2022/5/23 確認〕
※ 201 一般社団法人 ASP・SaaS・AI・IoT クラウド産業協会（ASPIC）は 2022 年 4 月 1 日より一般社団法人日本クラウド産業協会に名称変更された。
※ 202 https://www.soumu.go.jp/main_content/000477838.pdf〔2022/5/23 確認〕
※ 203 総務省：「クラウドサービスの安全・信頼性に係る情報開示指針」における「AI を用いたクラウドサービスの安全・信頼性に係る情報開示指針（ASP・SaaS 編）」の追加 https://www.soumu.go.jp/menu_news/s-news/01ryutsu06_02000306.html〔2022/5/23 確認〕
※ 204 経済産業省：オープンソースソフトウェアの利活用及びそのセキュリティ確保に向けた管理手法に関する事例集を取りまとめました https://www.meti.go.jp/press/2021/04/20210421001/20210421001.html〔2022/5/23 確認〕
※ 205 Software Bill of Materials（SBOM：ソフトウェア部品表）：「ソフトウェア部品構成表」等とも呼ばれる、様々なソフトウェア部品の名称とそのライセンス等で構成される一覧表。米国商務省電気通信情報局（NTIA：National Telecommunications and Information Administration）が設立した「Software Component Transparency」において 2018 年から議論されている。
※ 206 総務省：「クラウドサービス提供における情報セキュリティ対策ガイドライン（第 3 版）」（案）に対する意見募集の結果及び「クラウドサービス提供における情報セキュリティ対策ガイドライン（第 3 版）」の公表 https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00121.html〔2022/5/23 確認〕
※ 207 NISC：クラウドを利用したシステム運用に関するガイダンス（詳細版） https://www.nisc.go.jp/pdf/policy/infra/cloud_guidance.pdf〔2022/5/23 確認〕
※ 208 The New York Times：U.S. Will Not Send Government Officials to Beijing Olympics https://www.nytimes.com/2021/12/06/us/politics/olympics-boycott-us.html〔2022/5/11 確認〕
※ 209 CISA：CISA Issues Emergency Directive and Alert on Microsoft Exchange Vulnerabilities https://us-cert.cisa.gov/ncas/current-activity/2021/03/03/cisa-issues-emergency-directive-and-alert-microsoft-exchange〔2022/5/11 確認〕
※ 210 The White House：Statements by Press Secretary Jen Psaki & Deputy National Security Advisor for Cyber Anne Neuberger on Microsoft Exchange Vulnerabilities UCG https://www.whitehouse.gov/briefing-room/statements-releases/2021/03/17/statements-by-press-secretary-jen-psaki-deputy-national-security-advisor-for-cyber-anne-neuberger-on-microsoft-exchange-vulnerabilities-ucg/〔2022/5/11 確認〕
※ 211 CNET：Biden administration blames China for Microsoft Exchange email hack https://www.cnet.com/news/privacy/biden-administration-blames-china-for-microsoft-server-hack/〔2022/5/11 確認〕
※ 212 The New York Times：Cyberattack Forces a Shutdown of a Top U.S. Pipeline https://www.nytimes.com/2021/05/08/us/politics/cyberattack-colonial-pipeline.html〔2022/5/11 確認〕
※ 213 The New York Times：The F.B.I. confirms that DarkSide, a ransomware group, was behind the hack of a major U.S. pipeline. https://www.nytimes.com/2021/05/10/us/politics/dark-side-hack.html〔2022/5/11 確認〕
※ 214 WIRED：DarkSide Ransomware Hit Colonial Pipeline—and Created an Unholy Mess https://www.wired.com/story/darkside-ransomware-colonial-pipeline-response/〔2022/5/11 確認〕
※ 215 CISA：Alert (AA21-131A) DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks https://us-cert.cisa.gov/ncas/alerts/aa21-131a〔2022/5/11 確認〕
※ 216 Forbes：Colonial Pipeline Restarts Operations As Biden Seeks To Protect Government From Cyber Attacks https://www.forbes.com/sites/edwardsegal/2021/05/12/colonial-pipeline-restarts-operations-as-biden-seeks-to-protect-government-from-cyber-attacks/?sh=17093d217814〔2022/5/11 確認〕
※ 217 The New York Times：Colonial Pipeline Paid Roughly $5 Million in Ransom to Hackers https://www.nytimes.com/2021/05/13/us/politics/biden-colonial-pipeline-ransomware.html〔2022/5/11 確認〕
※ 218 The Wall Street Journal：Colonial Pipeline CEO Tells Why He Paid Hackers a $4.4 Million Ransom https://www.wsj.com/articles/colonial-pipeline-ceo-tells-why-he-paid-hackers-a-4-4-million-ransom-11621435636〔2022/5/11 確認〕
※ 219 The Washington Post：Feds recover more than $2 million in ransomware payments from Colonial Pipeline hackers https://www.washingtonpost.com/business/2021/06/07/colonial-pipeline-ransomware-payment-recovered/〔2022/5/11 確認〕
※ 220 CONGRESS.GOV：H.R.550 - Immunization Infrastructure Modernization Act of 2021 https://www.congress.gov/bill/117th-congress/house-bill/550〔2022/5/11 確認〕
※ 221 SECURITY：Ransom Disclosure Act would require victims to disclose ransom payments within 48 hours https://www.securitymagazine.com/articles/96254-ransom-disclosure-act-would-require-victims-to-disclose-ransom-payments-within-48-hours〔2022/5/11 確認〕
※ 222 The White House：FACT SHEET: Imposing Costs for Harmful Foreign Activities by the Russian Government https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/〔2022/5/11 確認〕
※ 223 FCW：White House sanctions Russia over SolarWinds campaign, election interference https://fcw.com/articles/2021/04/15/katz-russia-cyber-sanctions.aspx〔2022/5/11 確認〕
※ 224 The White House：Executive Order on Improving the Nation's Cybersecurity https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/〔2022/5/11 確認〕
※ 225 The White House：FACT SHEET: Ongoing Public U.S. Efforts to Counter Ransomware https://www.whitehouse.gov/

briefing-room/statements-releases/2021/10/13/fact-sheet-ongoing-public-u-s-efforts-to-counter-ransomware/〔2022/5/11 確認〕
※ 226 U.S. Department of the Treasury：Treasury Takes Robust Actions to Counter Ransomware https://home.treasury.gov/news/press-releases/jy0364〔2022/5/11 確認〕
※ 227 The White House: FACT SHEET: Biden Administration Announces Further Actions to Protect U.S. Critical Infrastructure https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/fact-sheet-biden-administration-announces-further-actions-to-protect-u-s-critical-infrastructure/
※ 228 FATF（金融活動作業部会）：マネーロンダリング、テロ資金供与対策に関する国際協調を推進する政府間会合。 https://www.fatf-gafi.org/〔2022/5/11 確認〕
※ 229 The White House：Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems/〔2022/5/11 確認〕
※ 230 National Security Agency/Central Security Service：President Biden Signs Cybersecurity National Security Memorandum https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/2904637/president-biden-signs-cybersecurity-national-security-memorandum/〔2022/5/11 確認〕
※ 231 NIST：Critical Software Definition https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/critical-software-definition〔2022/5/11 確認〕
※ 232 NIST：Security Measures for “EO-Critical Software” Use https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/security-measures-eo-critical-software-use-2〔2022/5/11 確認〕
※ 233 NIST：Software Supply Chain Security Guidance Under Executive Order (EO) 14028 Section 4e https://www.nist.gov/system/files/documents/2022/02/04/software-supply-chain-security-guidance-under-EO-14028-section-4e.pdf〔2022/5/11 確認〕
※ 234 NIST：SP 800-218 Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities https://csrc.nist.gov/publications/detail/sp/800-218/final〔2022/5/11 確認〕
※ 235 NIST：Consumer Cybersecurity Labeling for IoT Products: Discussion Draft on the Path Forward https://www.nist.gov/system/files/documents/2021/12/03/FINAL_Consumer_IoT_Label_Discussion_Paper_20211202.pdf〔2022/5/11 確認〕
※ 236 NIST：White Paper NIST CSWP 24 Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products https://csrc.nist.gov/publications/detail/white-paper/2022/02/04/criteria-for-cybersecurity-labeling-for-consumer-iot-products/final〔2022/5/11 確認〕
※ 237 NIST：Report for the Assistant to the President for National Security Affairs (APNSA) on Cybersecurity Labeling for Consumers: Internet of Things (IoT) Devices and Software https://www.nist.gov/system/files/documents/2022/05/24/Cybersecurity Labeling for Consumers under Executive Order 14028 on Improving the Nation's Cybersecurity Report (FINAL).pdf〔2022/6/6 確認〕
※ 238 NIST：SP 800-161 Rev. 1 (Draft) PRE-DRAFT Call for Comments: Supply Chain Risk Management Practices for Federal Information Systems and Organizations https://csrc.nist.gov/publications/detail/sp/800-161/rev-1/draft〔2022/5/11 確認〕
※ 239 NIST：Request for Information about Evaluating and Improving Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management https://www.nist.gov/cyberframework/request-information-about-evaluating-and-improving-cybersecurity-resources〔2022/5/11 確認〕
※ 240 CISA：EXECUTIVE ORDER ON IMPROVING THE NATION’S CYBERSECURITY https://www.cisa.gov/executive-order-improving-nations-cybersecurity〔2022/5/11 確認〕
※ 241 CISA：Alert (AA21-265A) Conti Ransomware https://www.cisa.gov/uscert/ncas/alerts/aa21-265a〔2022/5/11 確認〕
※ 242 CISA：Alert (AA21-291A) BlackMatter Ransomware https://www.cisa.gov/uscert/ncas/alerts/aa21-291a〔2022/5/11 確認〕
※ 243 CISA：BINDING OPERATIONAL DIRECTIVE 22-01-REDUCING THE SIGNIFICANT RISK OF KNOWN EXPLOITED VULNERABILITIES https://www.cisa.gov/binding-operational-directive-22-01〔2022/5/11 確認〕
※ 244 CISA：KNOWN EXPLOITED VULNERABILITIES CATALOG https://www.cisa.gov/known-exploited-vulnerabilities-catalog〔2022/5/11 確認〕
※ 245 CISA:CONTINUOUS DIAGNOSTICS AND MITIGATION (CDM) https://www.cisa.gov/cdm〔2022/5/11 確認〕
※ 246 CISA：ELECTION INFRASTRUCTURE SECURITY https://www.cisa.gov/election-security〔2022/5/11 確認〕
※ 247 HOMELAND SECURITY TODAY.US：Shields Up: CISA Recommends All Organizations Adopt Heightened Cybersecurity Posture https://www.hstoday.us/federal-pages/dhs/shields-up-cisa-recommends-all-organizations-adopt-heightened-cybersecurity-posture/〔2022/5/11 確認〕
※ 248 CISA：Alert (AA22-047A) Russian State-Sponsored Cyber Actors Target Cleared Defense Contractor Networks to Obtain Sensitive U.S. Defense Information and Technology https://www.cisa.gov/uscert/ncas/alerts/aa22-047a〔2022/5/11 確認〕
※ 249 CISA：CISA AND FBI PUBLISH ADVISORY TO PROTECT ORGANIZATIONS FROM DESTRUCTIVE MALWARE USED IN UKRAINE https://www.cisa.gov/news/2022/02/26/cisa-and-fbi-publish-advisory-protect-organizations-destructive-malware-used〔2022/5/11 確認〕
※ 250 CISA：SHIELDS UP https://www.cisa.gov/shields-up〔2022/5/11 確認〕
※ 251 The White House：Statement by President Biden on our Nation’s Cybersecurity https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/21/statement-by-president-biden-on-our-nations-cybersecurity/〔2022/5/11 確認〕
※ 252 The Guardian：The Cambridge Analytica Files https://www.theguardian.com/news/series/cambridge-analytica-files〔2022/5/11 確認〕
※ 253 ITmedia：米司法省、IT 大手を独禁法違反の疑いで調査すると発表 https://www.itmedia.co.jp/news/articles/1907/24/news053.html〔2022/5/11 確認〕
※ 254 The New York Times：House Lawmakers Condemn Big Tech’s ‘Monopoly Power’ and Urge Their Breakups https://www.nytimes.com/2020/10/06/technology/congress-big-tech-monopoly-power.html〔2022/5/11 確認〕
※ 255 CONGRESS.GOV：H.R.3825 - Ending Platform Monopolies Act https://www.congress.gov/bill/117th-congress/house-bill/3825〔2022/5/11 確認〕
※ 256 日本経済新聞：米議会、独禁法改正で IT 追及 上院も「自社優遇禁止」案 https://www.nikkei.com/article/DGXZQOGN14F5Y0U1A011C2000000/〔2022/5/11 確認〕
※ 257 POLITICO：Gaming out tech antitrust’s next obstacles https://www.politico.com/newsletters/morning-tech/2022/01/21/gaming-out-tech-antitrusts-next-obstacles-799994〔2022/5/11 確認〕
※ 258 CONGRESS.GOV：S.2065 - Deepfake Report Act of 2019 https://www.congress.gov/bill/116th-congress/senate-bill/2065〔2022/5/11 確認〕
※ 259 The Wall Street Journal：The Facebook Files A Wall Street Journal investigation https://www.wsj.com/articles/the-facebook-files-11631713039〔2022/5/11 確認〕
※ 260 朝日新聞：フェイスブック、拡散されやすくなった有害投稿 アルゴリズム変更で https://digital.asahi.com/articles/ASPDV4F5XPDNUHBI008.html〔2022/5/11 確認〕
※ 261 The Washington Post：Facebook whistleblower Frances Haugen tells lawmakers that meaningful reform is necessary ‘for our common good’ https://www.washingtonpost.com/technology/2021/10/05/facebook-senate-hearing-frances-haugen/〔2022/5/11 確認〕
※ 262 The Washington Post:Biden, Putin aired differences at a high-stakes summit but agree on little https://www.washingtonpost.com/politics/biden-putin/2021/06/16/cdd677dc-ce0a-11eb-8014-2f3926ca24d9_story.html〔2022/5/11 確認〕
The Washington Post：Biden, Putin hold 'positive' summit but divisions remain over human rights, cyberattacks, Ukraine https://www.washingtonpost.com/politics/2021/06/16/biden-putin-live-updates/〔2022/5/11 確認〕
※ 263 朝日新聞：米ロ首脳、軍備管理へ新協議 融和ムード演出、人権では平行線 https://digital.asahi.com/articles/DA3S14942861.html?iref=pc_ss_date_article〔2022/5/11 確認〕
※ 264 The Washington Post：Russia planning massive military offensive against Ukraine involving 175,000 troops, U.S. intelligence warns https://www.washingtonpost.com/

national-security/russia-ukraine-invasion/2021/12/03/98a3760e-546b-11ec-8769-2f4ecdf7a2ad_story.html〔2022/5/11 確認〕
※ 265 The New York Times：'Greetings, Mr. President': Biden and Putin Hold 2-Hour Virtual Summit https://www.nytimes.com/2021/12/07/us/politics/biden-putin-ukraine-summit.html〔2022/5/11 確認〕
※ 266 JIJI.COM：米ロ首脳がオンライン会談　バイデン氏、制裁警告―ウクライナ情勢で対立 https://www.jiji.com/jc/article?k=2021120800014&g=int〔2022/5/11 確認〕
※ 267 The Guardian：Biden and Putin exchange warnings during phone call amid rising Ukraine tensions https://www.theguardian.com/us-news/2021/dec/30/biden-putin-call-russia-us-ukraine-tensions〔2022/5/11 確認〕
※ 268 NHK：米ロ首脳 電話会談 バイデン大統領 "侵攻の場合 厳しい制裁" https://www3.nhk.or.jp/news/html/20220213/k10013481281000.html〔2022/5/11 確認〕
※ 269 The Washington Post：Biden says U.S. believes Putin has decided to invade Ukraine https://www.washingtonpost.com/world/2022/02/18/russia-ukraine-updates/〔2022/5/11 確認〕
※ 270 CONGRESS.GOV：S.1605 - National Defense Authorization Act for Fiscal Year 2022 https://www.congress.gov/bill/117th-congress/senate-bill/1605/text〔2022/5/11 確認〕
※ 271 Summary of the Fiscal Year 2022 National Defense Authorization Act https://www.armed-services.senate.gov/imo/media/doc/FY22%20NDAA%20Agreement%20Summary.pdf〔2022/5/11 確認〕
※ 272 ZDNet Japan：ウクライナ政府狙った破壊的なマルウェア攻撃、マイクロソフトが報告 https://japan.zdnet.com/article/35182150/〔2022/5/11 確認〕
※ 273 CNET：Elon Musk Warns of Russian Attacks on Donated Starlink Internet Hubs in Ukraine https://www.cnet.com/science/space/elon-musk-activates-starlink-in-ukraine-amid-internet-disruption/〔2022/5/11 確認〕
※ 274 ZDNET Japan：ウクライナ侵攻で IT 企業がロシア事業から撤退、戦争と IT の関係 https://japan.zdnet.com/article/35185629/〔2022/5/11 確認〕
※ 275 Google: GLOBAL Ukraine：How Google is helping https://www.thinkwithgoogle.com/collections/how-google-is-supporting-ukraine/〔2022/5/11 確認〕
※ 276 REUTERS：Facebook allows war posts urging violence against Russian invaders https://www.reuters.com/world/europe/exclusive-facebook-instagram-temporarily-allow-calls-violence-against-russians-2022-03-10/〔2022/5/11 確認〕
※ 277 The Guardian：Anonymous: the hacker collective that has declared cyberwar on Russia https://www.theguardian.com/world/2022/feb/27/anonymous-the-hacker-collective-that-has-declared-cyberwar-on-russia〔2022/5/11 確認〕
※ 278 The White House：FACT SHEET: United States Bans Imports of Russian Oil, Liquefied Natural Gas, and Coal https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/08/fact-sheet-united-states-bans-imports-of-russian-oil-liquefied-natural-gas-and-coal/〔2022/5/11 確認〕
※ 279 日本経済新聞：ドイツ、ロシアとのガス管計画を凍結 「弱腰」から転換 https://www.nikkei.com/article/DGXZQOGR22E700S2A220C2000000/〔2022/5/11 確認〕
※ 280 The White House：FACT SHEET: United States, G7 and EU Impose Severe and Immediate Costs on Russia https://www.whitehouse.gov/briefing-room/statements-releases/2022/04/06/fact-sheet-united-states-g7-and-eu-impose-severe-and-immediate-costs-on-russia/〔2022/5/11 確認〕
※ 281 JIJI.COM：対ロ制裁、効果に限界　ウクライナ大統領、強化訴え―エネルギー禁輸が焦点 https://www.jiji.com/jc/article?k=2022040700980&g=int〔2022/5/11 確認〕
※ 282 The Washington Post：Biden warns China's Xi not to help Russia on Ukraine https://www.washingtonpost.com/world/2022/03/18/biden-xi-china-call-ukraine-russia-war/〔2022/5/11 確認〕
※ 283 JIJI.COM：ロシア排除で分断露呈　米など途中退席、共同声明見送り―G20財務相・中銀総裁会議 https://www.jiji.com/jc/article?k=2022042100152&g=pol〔2022/5/11 確認〕
※ 284 POLITICO：European Parliament ratifies post-Brexit trade deal https://www.politico.eu/article/european-parliament-post-brexit-trade-deal-ratification/〔2022/5/11 確認〕
※ 285 JETRO：欧州委、北アイルランド議定書の調整を提案 https://www.jetro.go.jp/biznews/2021/10/99615fe86d21a386.html〔2022/5/11 確認〕
※ 286 Financial Times：Brexit one year on: the impact on the UK economy https://www.ft.com/content/c6ee4ce2-95b3-4d92-858f-c50566529b5e〔2022/5/11 確認〕
※ 287 日本経済新聞：EU 離脱 2 年の英　強まる不満背に「再加盟派」そろり始動 https://www.nikkei.com/article/DGXZQOGR17ETG0X10C22A3000000/〔2022/5/11 確認〕
※ 288 GOV.UK：Coronavirus（Covid-19）in the UK https://coronavirus.data.gov.uk/〔2022/5/11 確認〕
※ 289 BBC: Covid：Why has the Delta variant spread so quickly in UK? https://www.bbc.com/news/health-57489740〔2022/5/11 確認〕
※ 290 WHO：WHO Coronavirus (COVID-19) Dashboard https://covid19.who.int/〔2022/5/11 確認〕
※ 291 REUTERS：COVID-19 Tracker 欧州 https://graphics.reuters.com/world-coronavirus-tracker-and-maps/ja/regions/europe/〔2022/5/11 確認〕
※ 292 BBC：Covid: Pre-departure travel tests to be scrapped https://www.bbc.com/news/business-59876063〔2022/5/11 確認〕
※ 293 BBC：Covid: England ending isolation laws and mass free testing https://www.bbc.com/news/uk-60467183〔2022/5/11 確認〕
※ 294 European Commission：Coronavirus: Commission proposes a Digital Green Certificate https://ec.europa.eu/commission/presscorner/detail/en/ip_21_1181〔2022/5/11 確認〕
※ 295 Council of Europe：Vaccine passports: Council of Europe issues guidance to governments to safeguard human rights https://www.coe.int/en/web/portal/-/vaccine-passports-council-of-europe-issues-guidance-to-governments-to-safeguard-human-rights〔2022/5/11 確認〕
※ 296 European Commission：EU Digital COVID Certificate https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/safe-covid-19-vaccines-europeans/eu-digital-covid-certificate_en#what-is-the-eu-digital-covid-certificate〔2022/5/11 確認〕
※ 297 在ボストン日本国総領事館：米国の新たな水際措置（ワクチン接種証明提示義務化ほか）について https://www.boston.us.emb-japan.go.jp/itpr_ja/11_000001_00269.html〔2022/5/11 確認〕
※ 298 Naturemedicine：The French health pass holds lessons for mandatory COVID-19 vaccination https://www.nature.com/articles/s41591-021-01661-7〔2022/5/11 確認〕
※ 299 JETRO：新型コロナワクチンパスを 1 月 24 日から施行、2 月から規制緩和へ https://www.jetro.go.jp/biznews/2022/01/df11a188e5336fd4.html〔2022/5/11 確認〕
※ 300 JETRO：フランス、新型コロナ規制緩和の第 2 段階へ、入国規制も 2 月 12 日に緩和 https://www.jetro.go.jp/biznews/2022/02/62f2642befab0ac8.html〔2022/5/11 確認〕
※ 301 GOVERNMENT：Pass vaccinal https://www.gouvernement.fr/info-coronavirus/pass-vaccinal〔2022/5/11 確認〕
※ 302 BBC：Germany elections: Centre-left claim narrow win over Merkel's party https://www.bbc.com/news/world-europe-58698806〔2022/5/11 確認〕
※ 303 JETRO：オミクロン株対策で追加接種加速、接種義務も拡大へ https://www.jetro.go.jp/biznews/2021/12/e6fa3459d9db02ab.html〔2022/5/11 確認〕
※ 304 POLITICO：German parliament rejects mandatory coronavirus vaccination https://www.politico.eu/article/german-parliament-rejects-mandatory-coronavirus-vaccination/〔2022/5/11 確認〕
※ 305 France 24：Italy makes Covid-19 'Green Pass' mandatory for restaurants, public transport https://www.france24.com/en/europe/20210805-italy-makes-covid-19-health-pass-mandatory-for-teachers〔2022/5/11 確認〕
※ 306 ItaliaPass, LLC：ITALY GREEN PASS https://italygreenpass.com/guide-to-green-pass-restrictions-starting-april-1/〔2022/5/11 確認〕
※ 307 BBC：England vaccine passport plans ditched, Sajid Javid says https://www.bbc.com/news/uk-58535258〔2022/5/11 確認〕
※ 308 読売新聞：ワクチン接種証明提示、イングランド全域で義務化…ナイトクラブや劇場など https://www.yomiuri.co.jp/world/20211215-OYT1T50134/〔2022/5/11 確認〕
※ 309 Nursing Notes：Government makes spectacular U-turn on mandatory vaccinations for health and social care workers https://nursingnotes.co.uk/news/workforce/government-makes-spectacular-u-turn-on-mandatory-vaccinations-for-health-and-social-care-workers/〔2022/5/11 確認〕

※ 310 ENISA：NIS Directive https://www.enisa.europa.eu/topics/nis-directive〔2022/5/11 確認〕
※ 311 ENISA：NIS Investments Report 2021 https://www.enisa.europa.eu/publications/nis-investments-2021〔2022/5/11 確認〕
※ 312 ENISA：PSIRT Expertise and Capabilities Development https://www.enisa.europa.eu/publications/csirt-expertise-and-capabilities-development〔2022/5/11 確認〕
※ 313 ENISA：On the Watch for Incident Response Capabilities in the Health Sector https://www.enisa.europa.eu/news/enisa-news/on-the-watch-for-incident-response-capabilities-in-the-health-sector〔2022/5/11 確認〕
※ 314 European Parliament：The NIS2 Directive A high common level of cybersecurity in the EU https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf〔2022/5/11 確認〕
※ 315 European Commission：The EU cybersecurity certification framework https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-certification-framework〔2022/5/11 確認〕
※ 316 EUR-Lex：Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance) https://eur-lex.europa.eu/eli/reg/2019/881/oj〔2022/5/11 確認〕
※ 317 ENISA：Cybersecurity Certification: Candidate EUCC Scheme https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme〔2022/5/11 確認〕
※ 318 ENISA：EUCS – Cloud Services Scheme https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme〔2022/5/11 確認〕
※ 319 CSPCERT WG：Recommendations for the implementation of the CSP Certification scheme https://ecp.nl/wp-content/uploads/2020/01/PT-2019-CSP-CERT-WG-Recommendations-for-the-implementation-of-the-CSP-Certification-scheme-20190607-Final-version.pdf〔2022/5/11 確認〕
※ 320 ENISA：Securing EU's Vision on 5G: Cybersecurity Certification https://www.enisa.europa.eu/news/enisa-news/securing_eu_vision_on_5g_cybersecurity_certification〔2022/5/11 確認〕
※ 321 ENISA：Ad-Hoc Working Group 03 - on 5G Cybersecurity Certification https://www.enisa.europa.eu/topics/standards/adhoc_wg_calls/ad-hoc-working-group-on-5g-cybersecurity-certification〔2022/5/11 確認〕
※ 322 ENISA：Cybersecurity Certification Market Study https://www.enisa.europa.eu/publications/cybersecurity-certification-market-study〔2022/5/11 確認〕
※ 323 ENISA：ENISA Cybersecurity Market Analysis Framework (ECSMAF) https://www.enisa.europa.eu/publications/enisa-cybersecurity-market-analysis-framework-ecsmaf〔2022/5/11 確認〕
ENISA：EU Cybersecurity Market Analysis - IoT in Distribution Grid https://www.enisa.europa.eu/publications/eu-cybersecurity-market-analysis-iot-in-distribution-grid〔2022/5/11 確認〕
※ 324 European Commission：European Democracy Action Plan: making EU democracies stronger https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2250〔2022/5/11 確認〕
※ 325 European Commission：Code of Practice on Disinformation https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation〔2022/5/11 確認〕
※ 326 EUR-Lex：Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A825%3AFIN〔2022/5/11 確認〕
※ 327 総務省：インターネット上の違法・有害情報を巡るEUの動向 ー Digital Services Act について ー https://www.soumu.go.jp/main_content/000738571.pdf〔2022/5/11 確認〕
※ 328 European Commission：Digital Services Act: Commission welcomes political agreement on rules ensuring a safe and accountable online environment https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2545〔2022/5/11 確認〕
※ 329 European Commission：The Digital Markets Act: ensuring fair and open digital markets https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en〔2022/5/11 確認〕
※ 330 European Commission：Digital Markets Act: Commission welcomes political agreement on rules to ensure fair and open digital markets https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1978〔2022/5/11 確認〕
※ 331 Reuter：New rules for U.S tech giants to come into force in October, EU's Vestager says https://www.reuters.com/technology/rules-against-us-tech-giants-come-into-force-october-eus-vestager-says-2022-03-25/〔2022/5/11 確認〕
※ 332 European Commission：A European approach to artificial intelligence https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence〔2022/5/11 確認〕
※ 333 European Commission：Proposal for a Regulation laying down harmonised rules on artificial intelligence https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence〔2022/5/11 確認〕
※ 334 中国が試行している行動履歴情報等による個人格付けは民主主義にとって脅威である、との判断によると思われる。
※ 335 EUR-Lex：DIRECTIVE (EU) 2016/680 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016L0680〔2022/5/11 確認〕
※ 336 DIGITALEUROPE：DIGITALEUROPE's initial findings on the proposed AI Act https://www.digitaleurope.org/resources/digitaleuropes-initial-findings-on-the-proposed-ai-act/〔2022/5/11 確認〕
European Commission：Feedback from: Google https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12527-Artificial-intelligence-ethical-and-legal-requirements/F2662492_en〔2022/5/11 確認〕
European Tech Alliance：EUTA Reaction to Commission's Artificial Intelligence Act proposal https://eutechalliance.eu/ai-euta-reaction-to-commissions-artificial-intelligence-act-proposal/〔2022/5/11 確認〕
日本経済団体連合会：欧州 AI 規制法案に対する意見 https://www.keidanren.or.jp/policy/2021/069.html?v=p〔2022/5/11 確認〕
※ 337 The New York Times：E.U. Court Strikes Down Trans-Atlantic Data Transfer Pact https://www.nytimes.com/2020/07/16/business/eu-data-transfer-pact-rejected.html〔2022/5/11 確認〕
※ 338 TechCrunch：EU, US agree on data transfer deal to replace defunct Privacy Shield https://techcrunch.com/2022/03/25/eu-and-us-agree-data-transfer-deal-to-replace-defunct-privacy-shield/〔2022/5/11 確認〕
※ 339 DLA Piper：DLA Piper GDPR fines and data breach survey: January 2022 https://www.dlapiper.com/ja/japan/insights/publications/2022/1/dla-piper-gdpr-fines-and-data-breach-survey-2022/〔2022/5/11 確認〕
※ 340 TechCrunch：EU hits Amazon with record-breaking $887M GDPR fine over data misuse https://techcrunch.com/2021/07/30/eu-hits-amazon-with-record-breaking-887m-gdpr-fine-over-data-misuse/〔2022/5/11 確認〕
※ 341 U.S. Securities and Exchange Commission：AMAZON.COM, INC. FORM 10-Q For the Quarterly Period Ended June 30, 2021 PART II. OTHER INFORMATION https://www.sec.gov/ix?doc=/Archives/edgar/data/0001018724/000101872421000020/amzn-20210630.htm#i5986f88ea1e04d5c91ff09fed8d716f0_103〔2022/5/11 確認〕
※ 342 CMS：GDPR Enforcement Tracker https://www.enforcementtracker.com/ETid-978〔2022/5/11 確認〕
※ 343 CMS：GDPR Enforcement Tracker https://www.enforcementtracker.com/ETid-979〔2022/5/11 確認〕
※ 344 CMS：GDPR Enforcement Tracker https://www.enforcementtracker.com/ETid-980〔2022/5/11 確認〕
※ 345 CMS：GDPR Enforcement Tracker https://www.enforcementtracker.com/ETid-1005〔2022/5/11 確認〕
※ 346 CMS：GDPR Enforcement Tracker https://www.enforcementtracker.com/ETid-1098〔2022/5/11 確認〕
※ 347 TechCrunch：Facebook fined $18.6M over string of 2018 breaches of EU's GDPR https://techcrunch.com/2022/03/15/facebook-2018-breaches-dpc-decision/〔2022/5/11 確認〕
※ 348 legislation.gov.uk：Telecommunications (Security) Act 2021 https://www.legislation.gov.uk/ukpga/2021/31/contents/enacted〔2022/5/11 確認〕
※ 349 GOV.UK：Closed consultation Proposal for new telecoms security regulations and code of practice https://www.gov.uk/government/consultations/proposal-for-new-telecoms-security-

regulations-and-code-of-practice〔2022/5/11 確認〕
※ 350 JETRO：IT セキュリティー法 2.0 施行、5G 機器など重要部品の審査厳格化 https://www.jetro.go.jp/biznews/2021/06/2b71160a630f99aa.html〔2022/5/11 確認〕
※ 351 SCC Online：Germany ¦ IT Security Act 2.0 passed by Government https://www.scconline.com/blog/post/2021/06/03/germany-it-security-act-2-0-passed-by-government/〔2022/5/11 確認〕
※ 352 日本経済新聞：EU・中国が首脳協議、習氏「自主的な対中政策」要求 https://www.nikkei.com/article/DGXZQOGR30CQO0Q2A330C2000000/?unlock=1〔2022/5/11 確認〕
※ 353 Reuters：EU warns Russia: 'Aggression comes with a price tag' https://www.reuters.com/world/europe/eu-warns-russia-aggression-comes-with-price-tag-2021-12-10/〔2022/5/11 確認〕
※ 354 European Commission：EU Solidarity with Ukraine https://ec.europa.eu/info/strategy/priorities-2019-2024/stronger-europe-world/eu-solidarity-ukraine_en〔2022/5/11 確認〕
※ 355 European Commission：EU sanctions against Russia following the invasion of Ukraine https://ec.europa.eu/info/strategy/priorities-2019-2024/stronger-europe-world/eu-solidarity-ukraine/eu-sanctions-against-russia-following-invasion-ukraine_en〔2022/5/11 確認〕
※ 356 European Commission：Ukraine: Sanctions on Kremlin-backed outlets Russia Today and Sputnik https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1490〔2022/5/11 確認〕
※ 357 The New York Times：Germany puts a stop to Nord Stream 2, a key Russian natural gas pipeline. https://www.nytimes.com/2022/02/22/business/nord-stream-pipeline-germany-russia.html〔2022/5/11 確認〕
※ 358 Politico：Germany says Russia oil embargo would be 'manageable' https://www.politico.eu/article/germany-says-russia-oil-embargo-would-be-manageable/〔2022/5/11 確認〕
※ 359 NATO：Relations with Ukraine https://www.nato.int/cps/en/natohq/topics_37750.htm〔2022/5/11 確認〕
※ 360 NATO：Relations with Russia https://www.nato.int/cps/en/natohq/topics_50090.htm〔2022/5/11 確認〕
※ 361 朝日新聞：プーチン氏がよく知る、NATO の「弱点」 ウクライナ危機の深層 https://digital.asahi.com/articles/ASQ2T72SLQ2TUHBI02K.html?_requesturl=articles%2FASQ2T72SLQ2TUHBI02K.html&pn=13〔2022/5/11 確認〕
※ 362 Reuters：焦点：ウクライナ侵攻受けNATO拡大機運、「露の脅威」現実に https://jp.reuters.com/article/nato-putin-idJPKCN2LX0DJ〔2022/5/11 確認〕
※ 363 BBC：Nato expansion: No set date for Finland application – minister https://www.bbc.com/news/world-us-canada-61226640〔2022/5/11 確認〕
※ 364 AFP：NATO、フィンランドの加盟手続き中に防衛支援表明 https://www.afpbb.com/articles/-/3402755〔2022/5/11 確認〕
※ 365 The New York Times: The leaders of Finland and Sweden say they will jointly submit their NATO applications. https://www.nytimes.com/2022/05/17/world/europe/sweden-finland-nato.html〔2022/5/11 確認〕
※ 366 BBC：Ukraine war: Putin warns Finland joining Nato would be 'mistake' https://www.bbc.com/news/world-europe-61450694〔2022/5/11 確認〕

付録

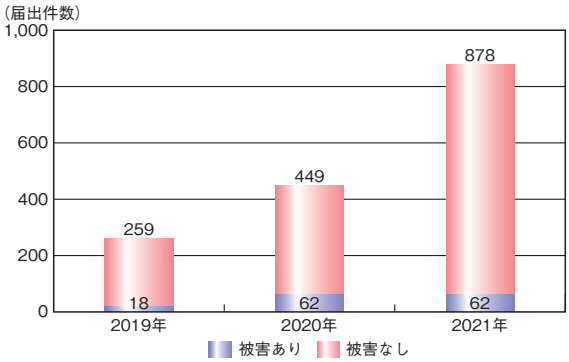
資料･ツール

資料A　2021年のコンピュータウイルス届出状況

IPA が 2021 年 1 月から 12 月の期間に受け付けたコンピュータウイルス（以下、ウイルス）届出の集計結果について述べる。

A.1　届出件数

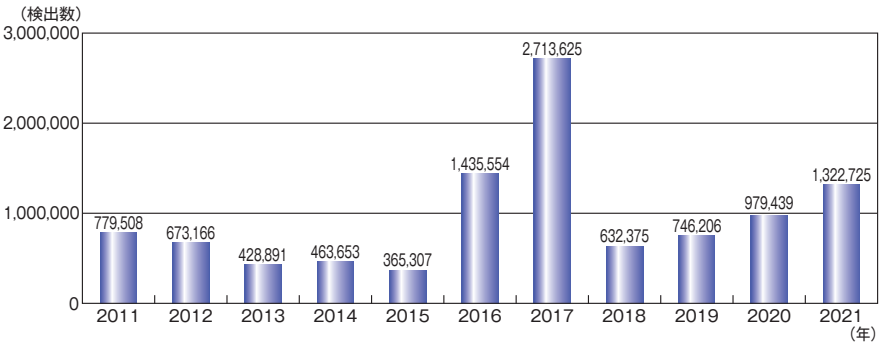
2021 年の年間届出件数は、前年の 449 件より 429 件（95.5%）多い 878 件であった（図 A-1）。そのうち、ウイルス感染の実被害があった届出は 62 件であった。



■図 A-1　ウイルス届出件数推移（2019～2021 年）

A.2　届出のあったウイルス等検出数

2021 年に寄せられたウイルス等の検出数は、前年の 97 万 9,439 個より 34 万 3,286 個（35.0%）多い 132 万 2,725 個であった（図 A-2）。



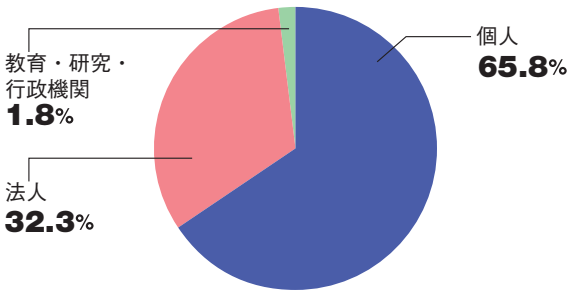
■図 A-2　ウイルス等検出数推移（2011～2021 年）

A.3　届出者の主体別届出件数

2021 年は前年と比較すると、全体の届出件数は増加した一方で、「教育・研究・行政機関」からの届出は減少した。届出者の主体別の比率では「個人」からの届出が 65.8%（578 件）と最も多かった（表 A-1、図 A-3）。

届出者の主体	2019 年	2020 年	2021 年
個人	28	188	578
法人	195	232	284
教育・研究・行政機関	36	29	16
合計（件）	259	449	878

■表 A-1　ウイルス届出者の主体別届出件数（2019～2021 年）



■図 A-3　ウイルス届出者の主体別届出件数の比率（2021 年）

A.4　傾向

2021 年でウイルス感染の実被害に遭った届出 62 件のうち、39 件がランサムウェアに感染した被害であり、半数以上を占めた。本白書では「1.2.2 ランサムウェア攻撃」にて攻撃手口や対策について詳しく述べているので、ぜひ一読していただきたい。

参照

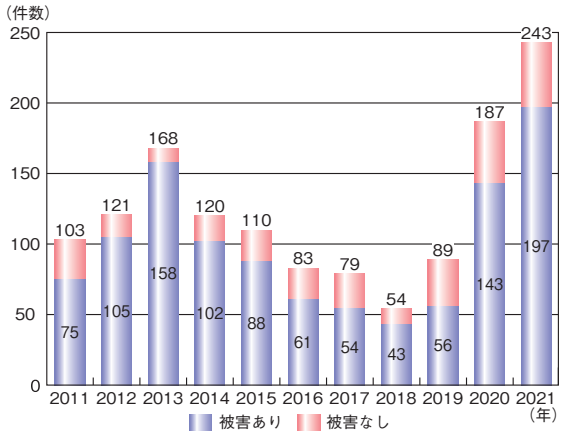
■コンピュータウイルス・不正アクセスの届出状況［2021年（1月～12月）］
https://www.ipa.go.jp/security/outline/todokede-j.html

資料B　2021年のコンピュータ不正アクセス届出状況

IPA が 2021 年 1 月から 12 月の期間に受け付けたコンピュータ不正アクセス（以下、不正アクセス）届出の集計結果について述べる。

B.1　届出件数

2021 年の年間届出件数は、前年の 187 件より 56 件（29.9%）多い 243 件であった（図 B-1）。そのうち、実被害があった届出は 197 件であった。



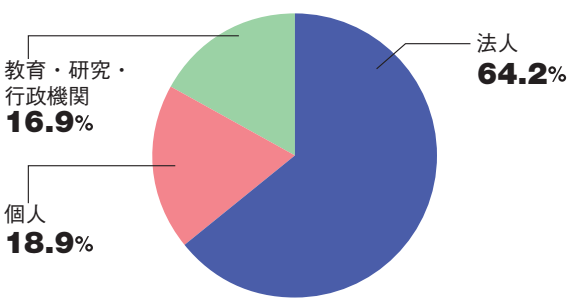
■図 B-1　不正アクセス届出件数推移（2011～2021 年）

B.2　届出者の主体別届出件数

2021 年は前年と比較すると、「教育･研究･行政機関」からの届出件数が倍以上に増加した。届出者の主体別の比率では「法人」からの届出が 64.2%（156 件）と最も多かった（表 B-1、図 B-2）。

届出者の主体	2019 年	2020 年	2021 年
法人	49	114	156
個人	30	57	46
教育・研究・行政機関	10	16	41
合計（件）	89	187	243

■表 B-1　不正アクセス届出者の主体別届出件数（2019～2021 年）

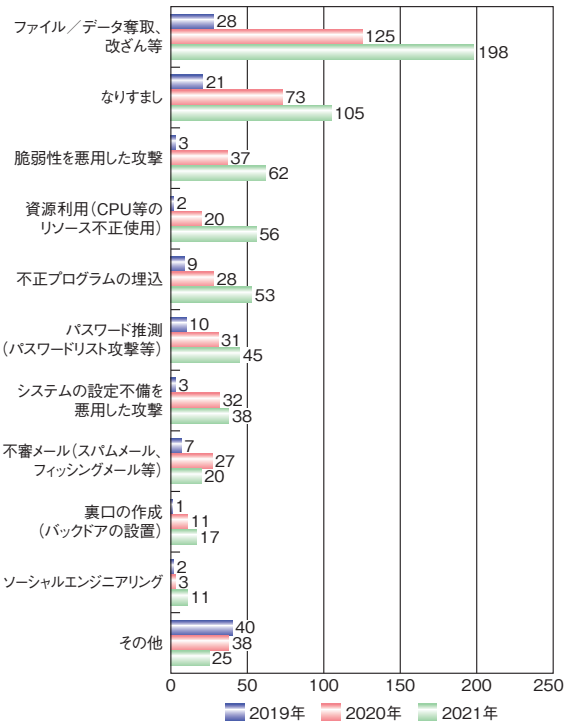


■図 B-2　不正アクセス届出者の主体別届出件数の比率（2021 年）

B.3　手口別件数

届出を攻撃行為（手口）により分類した件数を図 B-3 に示す。なお、以降の分類も含め、届出 1 件につき、複数の分類項目が該当する場合がある。その場合は該当する項目のそれぞれにカウントした。

2021 年の届出において最も多く見られた手口は、前年と同様に「ファイル／データ窃取、改ざん等」の 198 件であり、次いで「なりすまし」が 105 件、「脆弱性を悪用した攻撃」が 62 件であった。



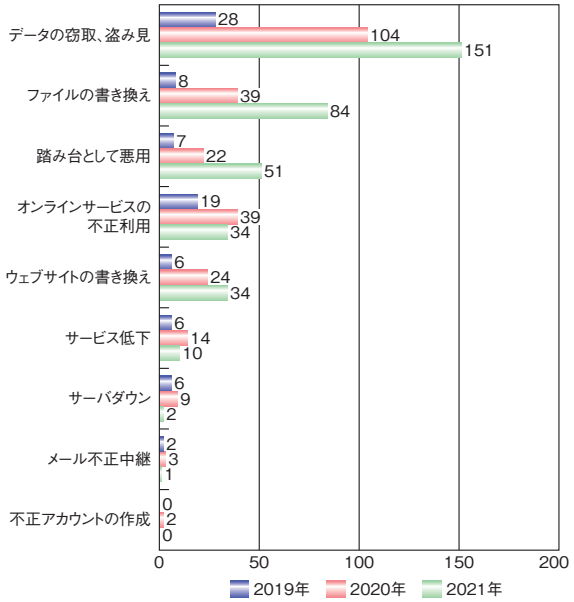
■図 B-3　不正アクセス手口別件数の推移（2019～2021 年）

B.4　被害内容別件数

届出のうち、実際に被害に遭った届出について、被害内容により分類した件数を図 B-4（次ページ）に示す。2021 年の届出において最も多く見られた被害は、前年と同様に「データの窃取、盗み見」（151 件）であった。次いで「ファイルの書き換え」が 84 件、「踏み台として悪用」が 51 件であり、ともに前年から倍以上に増加した。

なお、具体的な被害事例については、「コンピュータウイルス・不正アクセスの届出事例［2021 年上半期（1 月～ 6 月）］」及び「コンピュータウイルス・不正アクセスの届

出事例[2021 年下半期(7 月～ 12 月)]」(https://www.ipa.go.jp/security/outline/todokede-j.html) において紹介している。そちらも、ぜひ参考にしていただきたい。



■図 B-4　不正アクセス被害内容別件数の推移（2019～2021 年）

B.5 原因別件数

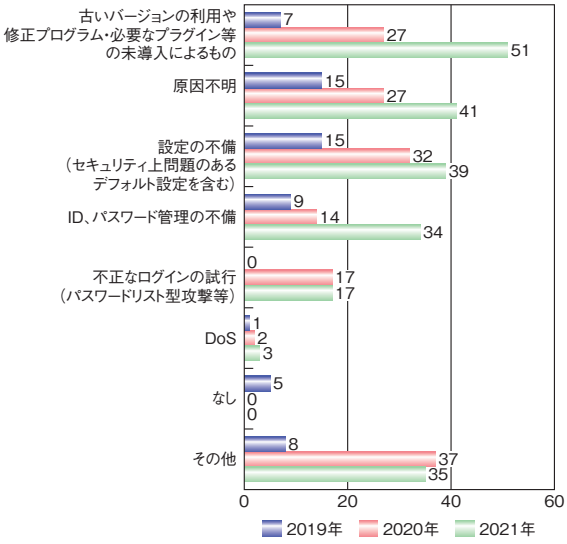
実際に被害に遭った届出について、不正アクセスの原因となった問題点／弱点で分類した件数を図 B-5 に示す。2021 年の届出において最も多く見られた原因は、「古いバージョンの利用や修正プログラム・必要なプラグイン等の未導入によるもの」であり 51 件であった。次いで「設定不備（セキュリティ上問題のあるデフォルト設定を含む）」が 39 件であり、「ID、パスワード管理の不備」については 34 件と前年から倍以上に増加した。

B.6 傾向と対策

不正アクセス被害の傾向と対策について述べる。

(1) 企業・組織の被害の傾向と対策

2021 年は VPN 装置の脆弱性を悪用して窃取した認証情報を使用した不正侵入の被害が多く見られた（「1.2.5 (1) VPN 製品の脆弱性を対象とした攻撃」参照）。



■図 B-5　不正アクセス原因別件数の推移（2019～2021 年）

また、EC サイトの脆弱性を悪用した改ざん等によるクレジットカード情報や個人情報の窃取の被害も依然として多く見られた（「1.3.2 (1) (b) 2021 年の JVN 公表の動向」参照）。

システム管理者が行うべき重要な対策の一つは、VPN 装置や EC サイト等に限らず、脆弱性の解消である。ネットワーク機器やサーバ、各種ソフトウェアに関する脆弱性情報の収集と修正プログラムの適用、Web アプリケーションの脆弱性診断の実施等により、着実に脆弱性を解消していく必要がある。

(2) システム利用者の被害の傾向と対策

2021 年はメールアカウントへの不正なログインにより、迷惑メールやフィッシングメール等を不正に送信されたという被害が多く見られた。

不正なログインの主な原因として、パスワードリスト攻撃や総当たり攻撃により認証が突破されたことが挙げられている。システム利用者が行うべき対策としては、他者に推測されにくい複雑なパスワードを設定する、パスワードの使いまわしをしない、多要素認証等のセキュリティオプションを積極的に採用する等がある。各利用者において、適切なアカウント管理を実施していただきたい。

参照

■コンピュータウイルス・不正アクセスの届出状況[2021年(1月～12月)]
https://www.ipa.go.jp/security/outline/todokede-j.html

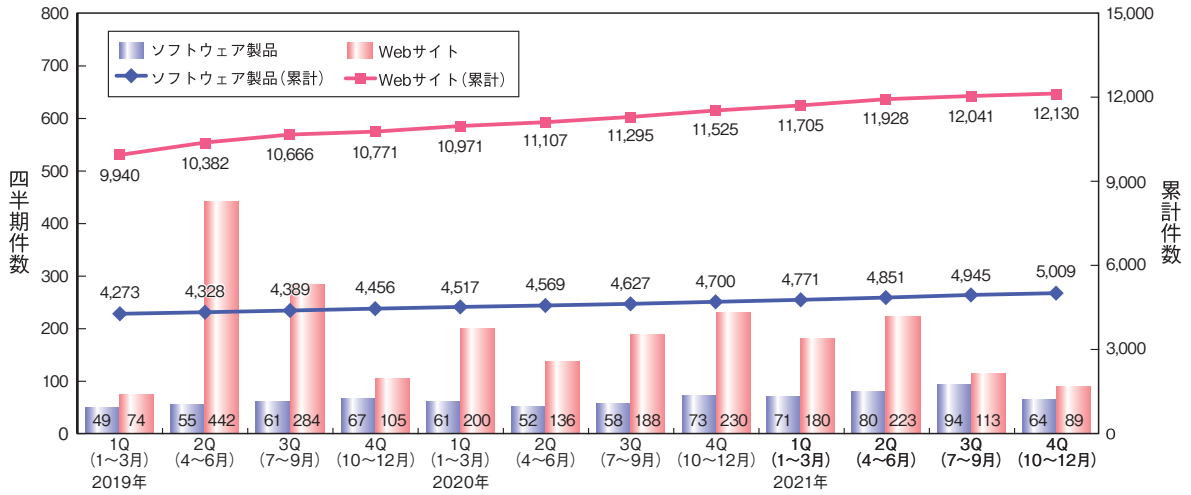
資料C　ソフトウェア等の脆弱性関連情報に関する届出状況

IPA が受け付けた脆弱性関連情報に関する届け出は、2021 年末までに 1 万 7,139 件に達した。

C.1　脆弱性の届出概況

2021 年末時点で、届出受付開始（2004 年 7 月 8 日）からの累計は、ソフトウェア製品に関するもの 5,009 件、Web サイトに関するもの 1 万 2,130 件、合計 1 万 7,139 件で、Web サイトに関する届出が全体の 70.8% を占めている（図 C-1）。

表 C-1 に示すように、届出受付開始から各四半期末時点までの就業日 1 日あたりの届出件数は、2021 年第 4 四半期末時点で 4.03 件となっている。届けられた脆弱性の種類はソフトウェア製品、Web サイトともにクロスサイト・スクリプティングの脆弱性が一番多くなっている。



■図 C-1　脆弱性関連情報の届出件数の四半期別推移

2020年1Q（1～3月）	2020年2Q（4～6月）	2020年3Q（7～9月）	2020年4Q（10～12月）	2021年1Q（1～3月）	2021年2Q（4～6月）	2021年3Q（7～9月）	2021年4Q（10～12月）
4.04	4.03	4.03	4.04	4.05	4.06	4.05	4.03

■表 C-1　就業日 1 日あたりの届出件数（届出受付開始から各四半期末時点）

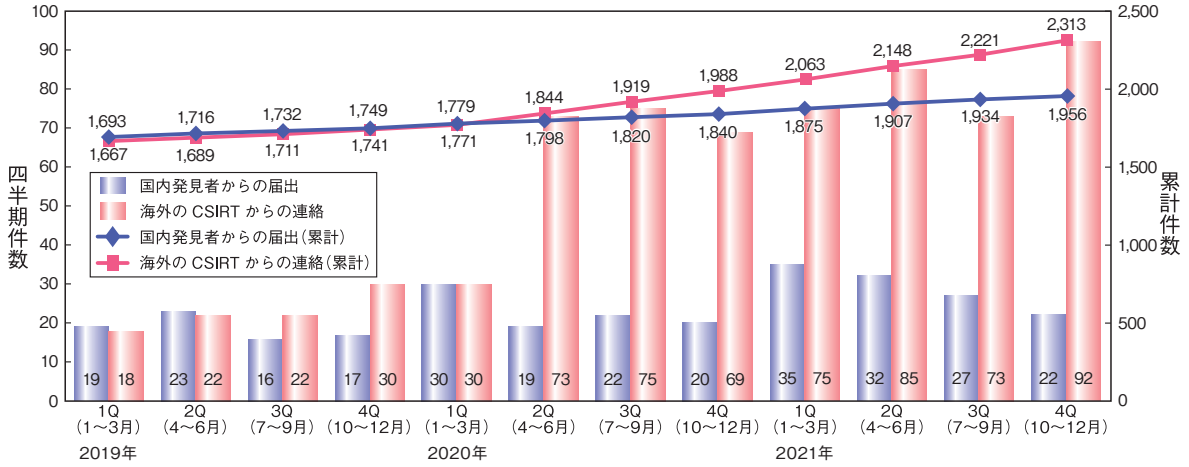
C.2　ソフトウェア製品の脆弱性の処理状況届出種別

2021 年末時点のソフトウェア製品に関する脆弱性の処理状況は、JPCERT/CC が調整を行い、製品開発者が脆弱性の修正を完了し、JVN で対策情報を公表したものは 2,352 件、製品開発者からの届出のうち JVN で公表せず製品開発者が個別対応を行ったものは 40 件、製品開発者が脆弱性ではないと判断したものは 104 件、告示で定める届出の対象に該当せず不受理としたものは 499 件で、これらの取り扱いを終了したものの合計は 2,995 件に達した（表 C-2）。

このほか、海外の CSIRT から JPCERT/CC が連絡を受けた 2,313 件を JVN で公表した。これらの公表済み件数の期別推移を図 C-2（次ページ）に示す。

分類		累計件数
修正完了	公表済み	2,352件
	個別対応	40件
脆弱性ではない		104件
不受理		499件
合計		2,995件

■表 C-2　ソフトウェア製品の脆弱性の終了件数



■図 C-2　ソフトウェア製品の脆弱性対策情報の公表件数

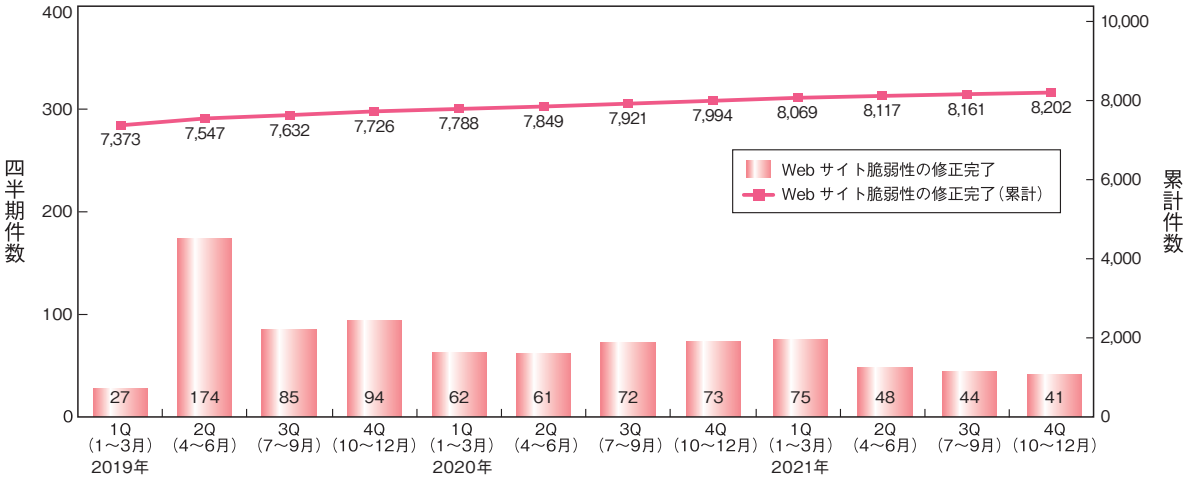
C.3 Webサイトの脆弱性の処理状況

2021 年末時点の Web サイトに関する脆弱性の処理状況は、IPA が通知を行い Web サイト運営者が修正を完了したものは 8,202 件、IPA が注意喚起等を行った後に処理を終了させたものは 1,130 件、IPA 及び Web サイト運営者が脆弱性ではないと判断したものは 704 件、Web サイト運営者と連絡が不可能なもの、または Web サイト運営者の対応により取り扱いが不能なものが 230 件、告示で定める届出の対象に該当せず不受理としたものは 285 件で、これらの取り扱いを終了したものの合計は 1 万 551 件に達した（表 C-3）。

これらのうち、修正完了件数の期別推移を図 C-3 に示す。

分類	累計件数
修正完了	8,202件
注意喚起	1,130件
脆弱性ではない	704件
取扱不能	230件
不受理	285件
合計	10,551件

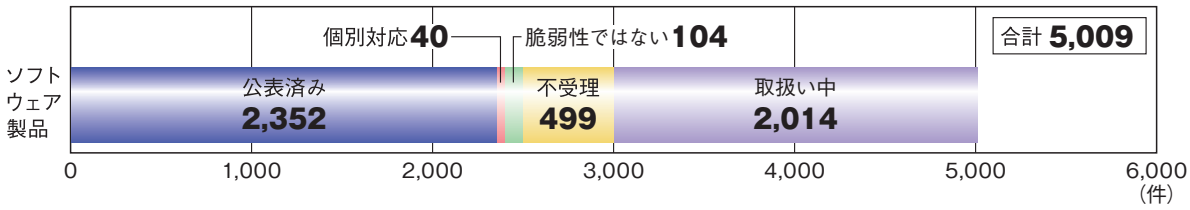
■表 C-3　Web サイトの脆弱性の終了件数



■図 C-3　Web サイトの脆弱性の修正完了件数

C.4 ソフトウェア製品の脆弱性の届出の処理状況

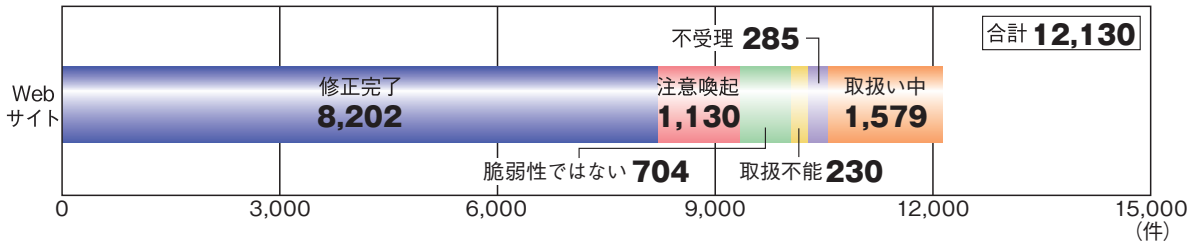
ソフトウェア製品の脆弱性関連情報の届出について処理状況を図 C-4 に示す。



■図 C-4　ソフトウェア製品の脆弱性関連情報の届出の処理状況

C.5 Webサイトの脆弱性の届出の処理状況

Web サイトの脆弱性関連情報の届出について処理状況を図 C-5 に示す。



■図 C-5　Web サイトの脆弱性関連情報の届出の処理状況

参照

■ソフトウェア等の脆弱性関連情報に関する届出状況［2021年第4四半期（10月～12月）］
https://www.ipa.go.jp/security/vuln/report/vuln2021q4.html

資料D　2021年の情報セキュリティ安心相談窓口の相談状況

2021 年 1 月から 12 月の期間に IPA が対応した、相談対応状況の集計結果について述べる。

なお、IPA 情報セキュリティ安心相談窓口では、新型コロナウイルス感染症の拡大防止と職員の安全確保を図るために、下記の期間において相談電話対応業務を停止した。そのため当該期間中は電子メール、FAX、郵送のみで相談を受け付けていた。

相談電話対応業務停止期間：

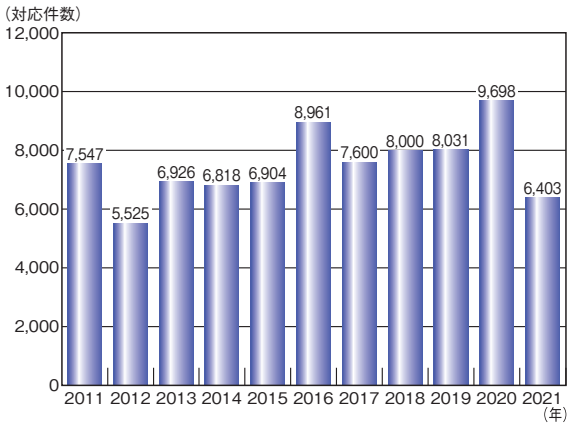
2021 年 1 月 12 日～ 2021 年 3 月 22 日

2021 年 4 月 27 日～ 2021 年 6 月 20 日

2021 年 7 月 12 日～ 2021 年 9 月 30 日

D.1　相談員対応件数

2021 年の年間相談員対応件数は 6,403 件となり、2020 年の相談員対応件数 9,698 件より 3,295 件（34.0%）の減少となった（図 D-1）。



■図 D-1　相談員対応件数推移（2011～2021 年）

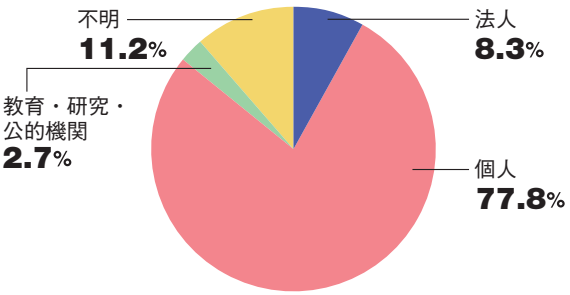
D.2　相談者の主体別相談対応件数

2021 年は個人からの相談が 4,984 件（77.8%）と最も多かった。

2020 年と比較すると、「法人」「個人」「教育・研究・行政機関」いずれにおいても、前年より減少した（表 D-1、図 D-2）。

相談者の主体	2019 年	2020 年	2021 年
法人	422	782	530
個人	7,046	8,110	4,984
教育・研究・公的機関	394	359	170
不明	169	447	719
合計（件）	8,031	9,698	6,403

■表 D-1　情報セキュリティ安心相談窓口の主体別相談対応件数（2019～2021 年）



■図 D-2　情報セキュリティ安心相談窓口の主体別相談件数の比率（2021 年）

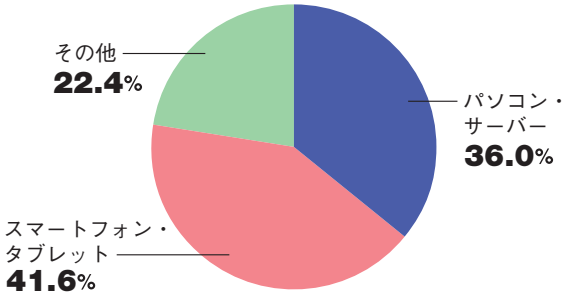
D.3　相談者の機種別相談件数

2021 年は「スマートフォン・タブレット」に関する相談が 2,666 件（41.6%）と最も多かった。

「スマートフォン・タブレット」に関する相談は 2020 年より 2 年連続で、「パソコン・サーバー」に関する相談件数を上回った（表 D-2、次ページ図 D-3）。

相談者の主体	2019 年	2020 年	2021 年
パソコン・サーバー	4,007	4,163	2,304
スマートフォン・タブレット	3,272	4,411	2,666
その他	752	1,124	1,433
合計（件）	8,031	9,698	6,403

■表 D-2　情報セキュリティ安心相談窓口の機種別相談件数（2021 年）

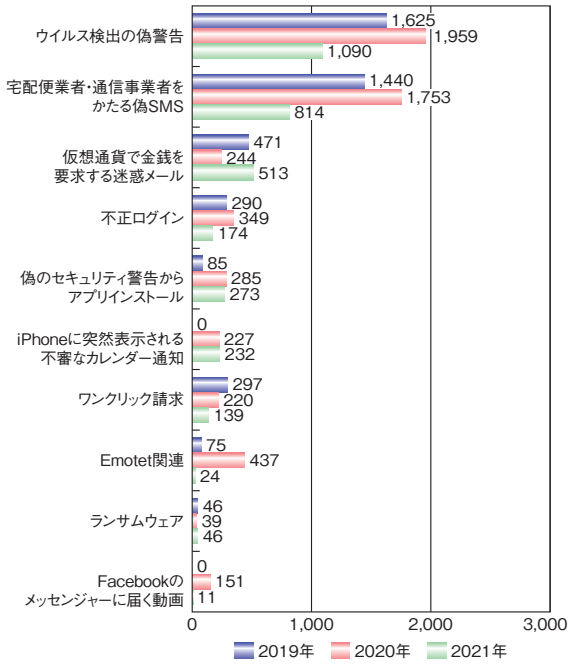


■図 D-3　情報セキュリティ安心相談窓口の機種別相談件数の比率（2021 年）

D.4　相談種別件数

主な相談種別ごとの件数を（図 D-4）に示す。2021 年の相談で最も多く寄せられたのは、「ウイルス検出の偽警告」に関する相談で1,090 件（17.0%）であった。次いで、「宅配便業者・通信事業者をかたる偽 SMS」に関して 814 件（12.7%）、「仮想通貨で金銭を要求する迷惑メール」に関して 513 件（8.0%）であった。上位三つの種別による相談件数は 2,417 件で、全相談件数（6,403 件）の 37.7% であった。

問い合わせの多い相談種別については、情報セキュリティ安心相談窓口の発行する「安心相談窓口だより」や、「手口検証動画」で注意喚起を行っている。ぜひ参考にしてほしい。



■図 D-4　主な相談種別件数の推移（2019～2021 年）

参照

■安心相談窓口だより
https://www.ipa.go.jp/security/anshin/mgdayoriindex.html
■手口検証動画シリーズ
https://www.ipa.go.jp/security/anshin/verificationmov.html

IPAの便利なセキュリティツール

情報セキュリティ対策ベンチマーク
https://security-shien.ipa.go.jp/diagnosis/

診断

用途・目的	自組織のセキュリティレベルを診断
利用対象者	情報セキュリティ担当者
特 長	• 他組織と比較した自組織のセキュリティレベルが判る • 自組織に不足しているセキュリティ対策が判る

概要

「セキュリティ対策の取り組み状況に関する評価項目」27 問と「企業プロフィールに関する評価項目」19 問、計 46 問に回答すると以下の診断結果を表示します。

■提供される診断結果
- セキュリティレベルを示したスコア(最高点 135 点、最低点 27 点)と度数分布状況と偏差値
- 情報セキュリティリスクの指標の分布と企業規模、業種、情報資産数等が自組織と近い他組織と比較し、自組織の位置が示された散布図
- 自組織の過去診断結果との比較や従業員数別での比較を含む 4 種類のレーダーチャート
- 結果に応じた推奨される取り組み

○ベンチマークに使用する診断データは 2022 年 3 月に Ver.5.1 にアップデート

脆弱性体験学習ツール「AppGoat」
https://www.ipa.go.jp/security/vuln/appgoat/

学習

用途・目的	脆弱性の基礎的な知識の学習
利用対象者	• アプリケーション開発者 • Web サイト管理者
特 長	脆弱性の概要や対策方法等、脆弱性に関する基礎的な知識を実習形式で体系的に学べる 3 種のツール

概要

■ AppGoat の種類
- Web アプリケーション用学習ツール(個人学習モード)、(集合学習モード)
  SQL インジェクション、クロスサイト・スクリプティング等 12 種の脆弱性を学習
- サーバ・デスクトップアプリケーション用学習ツール
  バッファオーバーフロー、ディレクトリ・トラバーサル等 7 種の脆弱性を学習

■活用方法例

○Web アプリケーション用学習ツール(個人学習モード)やサーバ・デスクトップアプリケーション用学習ツールを利用した、自宅等での個人学習

○Web アプリケーション用学習ツール(集合学習モード)を利用した、学校の講義や組織内のセミナー等における複数人での学習

脆弱性対策情報データベース「JVN iPedia」
https://jvndb.jvn.jp/

対策

用途・目的	自組織で使用しているソフトウェア製品の脆弱性の確認と対策
利用対象者	• システム管理者 • 製品・サービスの保守を担う担当者
特 長	14 万件超の国内外のソフトウェア製品の公開された脆弱性の対策情報が掲載されたキーワードで検索が可能なデータベース

概要

■掲載情報例
- 脆弱性の概要
- 脆弱性がある製品名とそのベンダ名
- 共通脆弱性識別子 CVE
- 脆弱性の深刻度 CVSS 基本値
- 本脆弱性に関わる製品ベンダ等のリンク

■活用方法例

○ネット記事等に記載された CVE 番号を JVN iPedia で検索し、脆弱性の詳細を確認

○自組織で使用している製品名で検索し、脆弱性の詳細を確認

MyJVN バージョンチェッカ for .NET
https://jvndb.jvn.jp/apis/myjvn/vccheckdotnet.html

対策

用途・目的	PC にインストールされたソフトウェア製品が最新バージョンかどうかを確認
利用対象者	PC 利用者全般
特 長	対象製品を使用している場合、最新バージョンかを一括確認でき、判定結果とインストールされているソフトウェアのバージョン等を表示

概要

■判定対象ソフトウェア製品

- Adobe Reader
- Mozilla Firefox
- Lunascape
- VMware Player
- JRE
- Mozilla Thunderbird
- Becky! Internet Mail
- Google Chrome
- Lhaplus
- iTunes
- OpenOffice.org
- LibreOffice

■活用方法例

毎朝 MyJVN バージョンチェッカを実行して、使用しているソフトウェアが最新かどうかをチェックし、最新でなければそのソフトウェアを更新

■動作環境・必須ソフトウェア

- Windows 8、10
- .NET Framework

サイバーセキュリティ注意喚起サービス「icat for JSON」
https://www.ipa.go.jp/security/vuln/icat.html

対策

用途・目的	IPA が発信する「重要なセキュリティ情報」のリアルタイム取得
利用対象者	• システム管理者 • サービスの保守を担う担当者 • 個人利用者
特 長	Web ページに HTML タグを埋め込むと、IPA が発信する「重要なセキュリティ情報」とリアルタイムに同期した情報を表示させる

概要

■「重要なセキュリティ情報」発信例

- 利用者への影響が大きい製品の脆弱性情報
- 広く使われる製品のサポート終了情報
- サイバー攻撃への注意喚起

■活用方法例

icat を自組織の従業員がよくアクセスする Web ページ（イントラページ等）に表示させ、ソフトウェアの更新等の対策の啓発を促す

注意警戒情報サービス
https://jvndb.jvn.jp/alert/

対策

用途・目的	脆弱性対策に必要な最新情報の収集
利用対象者	• システム管理者 • 製品・サービスの保守を担う担当者
特 長	日本で広く利用され、脆弱性が悪用されると影響の大きいサーバ用オープンソースソフトウェアのリリース情報と IPA が発信する「重要なセキュリティ情報」を提供

概要

■掲載情報例

- Apache HTTP Server
- Bind
- WordPress
- Apache Struts
- Joomla!
- 重要なセキュリティ情報
- Apache Tomcat
- OpenSSL

■活用方法例

定期的に自組織で使用しているオープンソースソフトウェアのリリース情報や IPA が発信する「重要なセキュリティ」が公表されているかどうかを確認し、公表されていれば内容の確認、必要に応じ対応を行う

Web サイトの攻撃兆候検出ツール「iLogScanner」
https://www.ipa.go.jp/security/vuln/iLogScanner/index.html

診断

用途・目的	Web サイトに対する攻撃の痕跡、攻撃の可能性を検出
利用対象者	Web サイト運営者
特 長	Web サイトのアクセスログ、エラーログ、認証ログを解析し、攻撃の痕跡や攻撃に成功した可能性があるログを解析結果レポートに表示

概要

■アクセスログ、エラーログから検出可能な項目例
- SQL インジェクション
- OS コマンド・インジェクション
- ディレクトリ・トラバーサル
- クロスサイト・スクリプティング

■認証ログ（Secure Shell、FTP）から検出可能な項目例
- 大量のログイン失敗
- 短時間の集中ログイン
- 同一ファイルへの大量アクセス
- 認証試行回数

■活用方法例
定期的に iLogScanner を実行し、自組織の Web サイトを狙った攻撃が行われているか確認

知っていますか？脆弱性
https://www.ipa.go.jp/security/vuln/vuln_contents/

学習

用途・目的	Web サイトの脆弱性の理解
利用対象者	• Web サイト制作者・運営者 • 一般利用者
特 長	Web サイトにおける、よくありがちな運営上の不備と脆弱性の特徴、攻撃例、及び対策を説明

概要

ありがちなシチュエーションで発生した問題を「博士」役が対話形式で、分かりやすく解説します。

■対象の脆弱性
- SQL インジェクション
- クロスサイト・スクリプティング
- クロスサイト・リクエスト・フォージェリ
- パス名パラメータの未チェック／ディレクトリ・トラバーサル
- OS コマンド・インジェクション
- セッション管理の不備
- HTTP ヘッダ・インジェクション
- HTTPS の不適切な利用
- サービス運用妨害（DoS）
- メール不正中継

情報セキュリティ対策支援サイト
https://security-shien.ipa.go.jp/

対策

用途・目的	立場、役割に応じた情報セキュリティ対策に関する情報の収集
利用対象者	経営者、対策実践者、従業員、啓発者、教職員、学生等
特 長	情報セキュリティ対策について「知りたい」「学びたい」「続けたい」当事者に対して、IPA が提供するサービスを一元的にまとめたポータルサイト

概要

「経営者」「対策実践者」「啓発者／教職員」「一般／学生」といった立場、役割別に、情報セキュリティ対策に必要な情報（実践すべきこと、資料、ツール、動画等）を分類し、一元化しています。
特に経営者に対しては情報セキュリティ対策の重要性を理解できるよう「対策を怠ることで組織が被る不利益」「経営者が追う法的・社会的責任」といった問題を具体的に提示し、対策の実践に必要な材料を提供しています。
また、セキュリティ対策を普及啓発するセキュリティプレゼンターの登録、利用方法についても紹介しています。

情報セキュリティ・ポータルサイト「ここからセキュリティ！」
学習 診断 対策
https://www.ipa.go.jp/security/kokokara/

用途・目的	• 情報セキュリティや情報リテラシーに関する情報収集 • 国内の主なレポート、ガイドライン、学習・診断等のツール等の利用
利用対象者	• インターネットの一般利用者（小学生～大人） • 企業の管理者／一般利用者
特 長	情報セキュリティ関連の民間及び公的な団体が公開する無償の資料、情報、ツールを網羅的に掲載。目的別、用途別、役割別に情報を選択し利用が可能

概要

• セキュリティベンダ、公的機関、政府等から発信される注意喚起や、資料・動画・ツール等のコンテンツを網羅的に掲載したポータルサイト
• コンテンツを「被害に遭ったら」「対策する」「教育・学習」「セキュリティチェック」「データ＆レポート」に分類。必要な情報が見つけやすい
• セキュリティレベルを診断するクイズを「小学生」「中高生・ホームユーザ」「社会人」というカテゴリー別に紹介。楽しみながら学べる

サイバーセキュリティ経営ガイドライン実施状況の可視化ツール
診断
https://www.ipa.go.jp/security/economics/checktool/index.html

用途・目的	セキュリティ対策の実施状況のセルフチェック
利用対象者	主に従業員 300 名以上の企業の CISO 等、サイバーセキュリティ対策の責任者
特 長	サイバーセキュリティ経営ガイドラインに準拠したセキュリティ対策の実施状況を成熟度モデルで自己診断し、レーダーチャートで可視化

概要

経営者がサイバーセキュリティ対策を実施する上で責任者となる担当幹部（CISO 等）に指示すべき“重要 10 項目”が、適切に実施されているかどうかを 5 段階の成熟度モデルで自己診断し、その結果をレーダーチャートで可視化するツール。

診断結果は、経営者への自社のセキュリティ対策の実施状況の説明資料として利用でき、経営者が対策状況を定量的に把握することで、サイバーセキュリティに関する方針の策定や適切なセキュリティ投資の検討、投資家等ステークホルダとのコミュニケーション等に役立てることができます。

■提供される主な機能
・重要 10 項目の実施状況の可視化
・同業種及び全業種平均との診断結果の比較
・低い点数の項目に対する参考事例
・グループ企業同士の診断結果を比較できる比較シート

手口検証動画シリーズ
学習 対策
https://www.ipa.go.jp/security/anshin/verificationmov.html

用途・目的	動画で「だましの手口」を知り被害防止につなげる
利用対象者	スマートフォン、パソコンの一般利用者
特 長	ネット上に実際にある「だましの手口」に引っかかる様子を動画で見て知り、被害にあった場合の対処や、被害にあわないための対策を学べる

概要

IPA 情報セキュリティ安心相談窓口に寄せられる相談の手口を実際に検証した際の様子を「手口検証動画シリーズ」として 8 本公開しています。最近の「だましの手口」は巧妙で、スマートフォンの機能や様々なネット上のサービスを悪用した手口が増加。動画は 1 本あたり 3 分前後で、手口を知り、被害にあった場合の対処や、被害にあわないための対策を判りやすく学ぶことができます。

IPAコンクール応援隊長「まもるくん」

第17回 IPA「ひろげよう情報モラル・セキュリティコンクール」2021 受賞作品

IPAは、子どもたちがインターネットにまつわる課題に自ら向き合い、解決策を見出すきっかけとして、全国の小学生・中学生・高校生・高専生を対象とするコンクールを開催しています。

ここでは、全64,959点の応募作品の中から、受賞した作品の一部をご紹介いたします。なお、すべての受賞作品は下記のWebサイトで公開しています。

[https://www.ipa.go.jp/security/event/hyogo/]

最優秀賞

〈独立行政法人情報処理推進機構〉

〈標語部門〉

ぼくだけの
ひみつができたよ
パスワード

鹿児島県 鹿児島大学教育学部附属小学校 1年 **松田 貫義**さん

〈ポスター部門〉

愛知県 椙山女学園高等学校 1年 **前田 綾音**さん

〈4コマ漫画部門〉

東京都 福生市立福生第一中学校 3年
髙橋 音羽さん

優秀賞

〈独立行政法人情報処理推進機構〉

〈標語部門〉

使いすぎ　スマホと取ろう　ディスタンス

北海道　函館市立北昭和小学校　6年
土谷 萌々子さん

公開が　あなたにとっては　後悔へ

京都府　洛南高等学校附属中学校　1年
塩田 陽稀さん

映えてるね　その一方で　バレてるね

広島県　尾道高等学校　3年
栗巣 吉平さん

〈ポスター部門〉

兵庫県 雲雀丘学園小学校 4年
森下 陽也さん

愛知県 刈谷市立依佐美中学校 1年
横川 成介さん

岐阜県 岐阜県立岐阜各務野高等学校 1年
田川 琴絵さん

〈4コマ漫画部門〉

東京都 世田谷区立希望丘小学校 6年
村上 咲希さん

鹿児島県 志布志市立有明中学校 1年
菅田 拓海さん

佐賀県 佐賀県立白石高等学校（普通科キャンパス） 1年
小池 颯人さん

標語部門　優秀賞

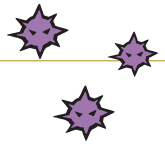
〈警察庁〉
消しゴムで　消せない言葉　SNS
京都府　京都府立乙訓高等学校　1年
松井 七星さん

〈特定非営利活動法人ITコーディネータ協会〉
指一本　ネットで他人に　とげ一本
北海道　北斗市立久根別小学校　6年
松田 晴さん

〈一般社団法人情報サービス産業協会〉
今の時代　ピースの写真で　指紋ばれ
千葉県　千葉県立八千代東高等学校　2年
伊藤　樂さん

〈一般社団法人組込みシステム技術協会〉
考えず　情報公開　後後悔
新潟県　長岡工業高等専門学校　3年
近 歩久登さん

〈一般社団法人日本情報システム・ユーザー協会〉
匿名の　安心感が　闇となる
京都府　舞鶴市立若浦中学校　1年
濱田 凪斗さん



〈一般社団法人ソフトウェア協会〉
やってみよう　私を守る　二段階認証
山梨県　山梨学院小学校　5年
伊東 ねいろさん

〈一般社団法人JPCERTコーディネーションセンター〉
セキュリティ　守るあなたが　守られる
宮城県　宮城県松島高等学校　1年
安倍 晴陽さん

〈一般社団法人全国地域情報産業団体連合会〉
許可取った?　みんなが持ってる　肖像権
神奈川県　川崎市立川崎高等学校附属中学校　3年
松本 彩那さん

〈株式会社カスペルスキー〉
タンチョウ(単調)に　クリックしたら　サギ(詐欺)だった
大阪府　大阪府立狭山高等学校　1年
吉田 咲恵さん

〈ソースネクスト株式会社〉
パスワード　絶対言わず　守り抜く
鹿児島県　鹿児島大学教育学部附属小学校　6年
叢 睿初さん

〈株式会社ディー・エヌ・エー〉
送信前　思いやりボタン　押したかな
鹿児島県　鹿児島市立広木小学校　6年
本藏 雅也さん

〈株式会社ラック〉
パスワード　見せず・言わずが　キーワード
埼玉県　立教新座高等学校　2年
小林 慶人さん

〈北海道警察〉
手の用心　書き込み一言　炎上(かじ)の元
北海道　北海道帯広柏葉高等学校　2年
菅原 悠大さん

〈一般社団法人宮城県情報サービス産業協会〉
見られてる　その一枚が　命撮り
宮城県　宮城県涌谷高等学校　1年
馬籠 優人さん

〈福島県警察本部〉
どこだろう　瞳に映る　君の場所
福島県　いわき市立小名浜第二中学校　1年
若松 亜湖さん

〈茨城県教育庁学校教育部高校教育課〉
スマホにも　マスク着用　フィルタリング
茨城県　茨城県立下妻第二高等学校　2年
寺﨑　旭さん

〈茨城県教育庁学校教育部義務教育課〉
SNS　絶対載せるな　パスワード
茨城県　北茨城市立中郷中学校　3年
豊田 怜大さん

〈茨城県メディア教育指導員連絡会〉
見ざる　聞かざる　言わざる　個人情報・パスワード
茨城県　北茨城市立中郷中学校　3年
鳥居塚 日稀さん

〈茨城県情報通信ネットワークセキュリティ協議会〉
向き合おう　自分の心　相手の心
茨城県　北茨城市立中郷中学校　3年
上遠野 ひなさん

〈公益社団法人埼玉県情報サービス産業協会〉
パスワード　手間が自分を　守り抜く
埼玉県　埼玉県立志木高等学校　1年
飯島 優真さん

〈千葉県警察本部〉
SNS　全ての言葉に　責任を
千葉県　日出学園小学校　5年
一條 裕仁さん

〈警視庁生活安全部サイバー犯罪対策課〉
盛れたけど　漏れてもいるよ　その写真
東京都　東京都立清瀬高等学校　3年
山口 花央さん

〈長野県青少年インターネット適正利用推進協議会〉
スマホ一つで　簡単に　人の心を　変えられる
長野県　南木曽町立南木曽中学校　1年
松原 陽さん

〈長野県インターネットプロバイダ防犯連絡協議会〉
善と悪　表裏一体　ネット社会
長野県　南木曽町立南木曽中学校　1年
樋口 煌さん

〈ネット安全・安心ぎふコンソーシアム〉
その言葉　匿名じゃなきゃ　言えないの?
岐阜県　城南高等学校　2年
熊崎 志恵利さん

〈静岡県警察本部〉
(S)知らぬ間に　(N)覗く人あり　(S)慎重に


静岡県　日本大学三島高等学校　2年
水谷　日菜乃さん

〈京都府教育委員会〉
やめようよ　歩きスマホと　言い訳は
京都府　京都精華学園中学校　2年
垣内 陽翔さん

〈一般社団法人京都府情報産業協会〉
SNS　便利と危険が　同居する
京都府　京都産業大学附属高等学校　1年
植松 小遥さん

〈京都情報大学院大学〉
顔見えない　仲は良くても　要注意
京都府　洛南高等学校附属中学校　2年
杉原 旬生さん

〈大阪私学教育情報化研究会〉
パスワード　文字と数字の　二刀流

大阪府　大阪市立東高等学校　2年
瀬 功太郎さん

〈特定非営利活動法人奈良地域の学び推進機構〉
まわりの人に　目配り　気配り　心配り

奈良県　奈良文化高等学校　1年
谷川 綾音さん

〈鳥取県警察本部〉
その一言　面と向かって　言えますか?
鳥取県　鳥取県立鳥取西高等学校　1年
向山 健さん

〈島根県警察本部〉
セキュリティ　ネット社会の　命綱
島根県　島根県立松江商業高等学校　1年
勝部　悠香さん

〈島根県教育委員会〉
向き合おう　スマホじゃなくて　人と人
島根県　島根県立松江商業高等学校　1年
江藤 莉吏花さん

〈岡山県警察本部〉
S 知らぬ間に　N 泣かせているかも　S その投稿
岡山県　岡山大学教育学部附属中学校　3年
山﨑 巨泉さん

〈岡山県情報セキュリティ協議会〉
言の葉が　知らぬ間に　言の刃に
岡山県　岡山大学教育学部附属中学校　3年
宮原 健太郎さん

〈広島県警察本部〉
SNS　後悔のない　公開を
広島県　廿日市市立七尾中学校　1年
大野 楓さん

〈一般社団法人広島県情報産業協会〉
ネットこそ　人の気持ちを　第一に。

広島県　広島県立三原東高等学校　2年
門松 桃花さん

〈徳島県警察本部〉
会いたいな　ネットの友だち　それ安心?
徳島県　徳島市八万中学校　3年
山上 瑠偉さん

〈徳島県教育委員会〉
送る前に　その言葉で　本当にいいの?　再確認
徳島県　阿波市立阿波中学校　1年
尾﨑 由梨さん

〈公益財団法人e-とくしま推進財団〉
消せたらな　あの日送った　メッセージ
徳島県　徳島県立城ノ内中等教育学校　4年
西出 璃子さん

〈香川県教育委員会〉
とく名だ　だからいいの?　その言葉
香川県　高松市立香東中学校　1年
寺沢 凰雅さん

〈情報通信交流館(e-とぴあ・かがわ)〉
死ぬまで一緒　ささった傷は　言葉のトゲ
香川県　高松市立香東中学校　2年
和田 響太さん

〈香川県プロバイダ等防犯連絡協議会〉
守ろうよ　心も　体も　情報も
香川県　高松市立香東中学校　2年
東藤 拓也さん

〈愛媛県情報サービス産業協議会〉
その投稿　本名出して　言えるかな
愛媛県　愛媛県立松山南高等学校　1年
二宮 駿介さん

〈高知県教育委員会〉
寝るまえに　スマホいじらず　夢みよう
高知県　明徳義塾中学校　1年
小坂 遼さん

〈一般社団法人高知県情報産業協会〉
ネットには　たくさん気持ち　こもってる
高知県　明徳義塾高等学校　1年
山中 孝太さん

〈福岡県教育委員会〉
パスワード　やってはいけない　リサイクル
福岡県　福岡市立那珂中学校　1年
福嶋 悠人さん

〈特定非営利活動法人ITサポートさが〉
SNS　消えない投稿　消える友
佐賀県　佐賀県立唐津東高等学校　1年
徳田 葵さん

〈長崎県警察本部〉
スマホ時間　増えれば減る　家族の時間
長崎県　長崎県立長崎北陽台高等学校　1年
本村 成陽さん

〈一般社団法人長崎県情報産業協会〉
その言葉　自分の心を　見直して
長崎県　長崎精道小学校　5年
鴨田 和奏さん

〈大分県情報サービス産業協会〉
消えないよ　キオクとキロクに　残る書き込み
大分県　臼杵市立北中学校　2年
青木 そらさん

〈一般社団法人宮崎県情報産業協会〉
その油断　スマホも感染　陽性反応
宮崎県　宮崎県立佐土原高等学校　3年
清田 舜斗さん

〈鹿児島県警察本部〉
「よし盛れた!」　載せれば情報　「あ、漏れた」
鹿児島県　日置市立吹上中学校　3年
栗島 愛華さん

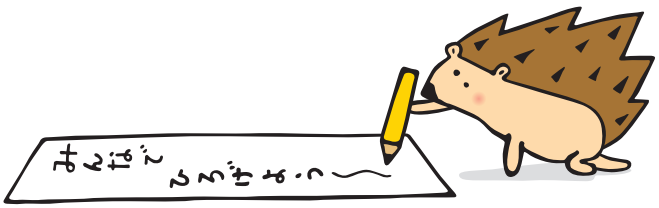
〈鹿児島市教育委員会〉
匿名は　批判のための　仮面じゃない
鹿児島県　鹿児島市立鹿児島玉龍中学校　3年
大脇 美桜さん

〈一般社団法人鹿児島県情報サービス産業協会〉
じょうほうも　かぞくと同じで　たいせつに
鹿児島県　鹿児島市立草牟田小学校　2年
井口 翔理さん

〈特定非営利活動法人鹿児島インファーメーション〉
親も子も　ゆだんをするな　ネットさぎ
鹿児島県　鹿児島市立広木小学校　6年
宮副 響太郎さん

〈沖縄県警察本部〉
その言葉　ほんとに言える?　目の前で
沖縄県　沖縄県立糸満高等学校　1年
新垣 龍季さん

〈沖縄県情報通信関連産業団体連合会〉
WiFiゲット　あなたの情報　誰かがGET
沖縄県　沖縄県立那覇西高等学校　1年
山内 はなさん



ポスター部門　優秀賞

〈公益社団法人著作権情報センター〉

東京都 工学院大学附属高等学校 2年

立本 千乃さん

〈一般社団法人日本教育情報化振興会〉

広島県 安田女子高等学校 1年

佐伯 文音さん

〈フィッシング対策協議会
「STOP. THINK. CONNECT.」〉

大阪府 大阪府立寝屋川高等学校（全日制課程） 2年

橋口 太一さん

〈実教出版株式会社〉

兵庫県 兵庫県立東播磨高等学校 1年

佐伯 和香さん

〈株式会社ノートンライフロック〉

鹿児島県 鹿児島県立川内商工高等学校 3年

石井 玲奈さん

〈株式会社ネットワールド〉

神奈川県 川崎市立川崎総合科学高等学校 3年

松﨑 蒼生さん

〈札幌市教育委員会〉

北海道 市立札幌開成中等教育学校 1年

鈴木 可脩さん

〈岩手県警察本部〉

岩手県 北上市立上野中学校 2年

久松 実玖さん

〈秋田県警察本部〉

秋田県 秋田県立矢島高等学校 1年

佐藤 真緒さん

〈茨城県〉

茨城県 牛久市立ひたち野うしく小学校 4年

井上 羽南さん

〈栃木県警察本部〉

栃木県 宇都宮文星女子高等学校 2年

黒子 彩音さん

〈群馬県警察本部〉

群馬県 伊勢崎市立境北中学校 2年

松本 妃花子さん

〈神奈川県警察
サイバーセキュリティ対策本部〉

神奈川県 神奈川県立神奈川工業高等学校 3年

内海 菜乃香さん

〈新潟県警察本部〉

新潟県 新潟県立五泉高等学校 1年

木了 ひかるさん

〈富山県警察本部〉

富山県 富山県立砺波高等学校 2年

中橋 和奏さん

〈山梨県警察本部〉

山梨県 山梨学院高等学校 2年

山田 彩愛さん

〈長野県警察本部〉

長野県 長野県駒ケ根工業高等学校 3年

中村 岳寛さん

〈愛知県警察本部〉

愛知県 桜花学園高等学校 1年

渥美 日香梨さん

〈三重県警察本部〉

三重県 いなべ市立大安中学校 3年

原田 百絵さん

〈京都府警察本部〉

京都府 京都産業大学附属高等学校 1年

子池 橙香さん

〈公益社団法人京都府防犯協会連合会〉

京都府 京都翔英高等学校 1年

山中 美空さん

〈奈良県警察本部〉

奈良県 奈良県立香芝高等学校 1年

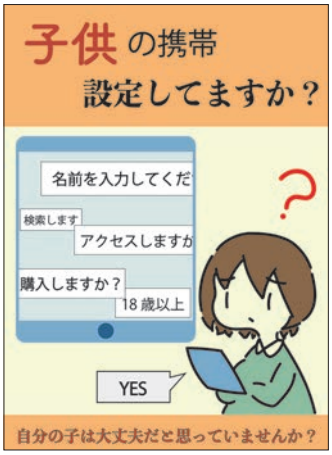
吉岡 穂の香さん

〈和歌山県警察本部〉

和歌山県 有田川町立吉備中学校 3年

今井 寧々さん

〈鳥取県サイバーセキュリティ対策ネットワーク〉



鳥取県 鳥取県立鳥取湖陵高等学校 3年

太田 弓葉さん

〈一般社団法人島根県情報産業協会〉

島根県 島根県立松江北高等学校 1年

原田 莉子さん

〈山口県警察本部〉

山口県 宇部フロンティア大学付属香川高等学校 1年

成松 さくらさん

〈一般社団法人徳島県情報産業協会〉

徳島県 阿波市立市場中学校 2年

武田 未羽さん

〈かがわ情報化推進協議会〉

香川県 香川県立高松工芸高等学校 3年

中平 琴葉さん

〈愛媛県警察本部〉

愛媛県 愛光中学校 2年

川村 美葵さん

〈高知県警察本部〉

高知県 高知市立高知商業高等学校 2年

刈谷 彩花さん

〈佐賀県警察本部〉

佐賀県 佐賀県立白石高等学校(商業科キャンパス) 2年

土井 誠也さん

〈熊本県警察本部〉

熊本県 熊本学園大学付属高等学校 1年

竹原 瑚陽さん

〈大分県警察本部〉

大分県 豊後大野市立三重中学校 2年

波津久 想さん

〈宮崎県警察本部〉

宮崎県 宮崎県立五ヶ瀬中等教育学校 6年

黒木 未麗さん

〈鹿児島県教育委員会〉

鹿児島県 鹿児島県立鹿児島工業高等学校 3年

新井 智之さん

〈沖縄県〉

沖縄県 南城市立佐敷中学校 3年

棚原 美南海さん

４コマ漫画部門　優秀賞

〈特定非営利活動法人日本ネットワークセキュリティ協会〉

隠れた個人情報

熊本県 熊本県立御船高等学校 1年

伊藤 萌衣さん

〈一般社団法人北海道情報システム産業協会〉

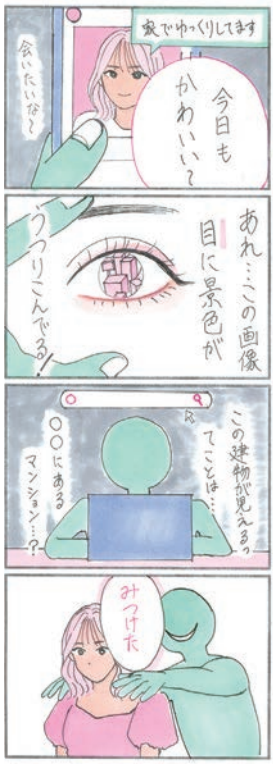
みんなどうして？

北海道 札幌市立西野中学校 3年

秋場 美南さん

〈青森県警察本部〉

目は口ほどに…



青森県 三沢市立第一中学校 3年

砂倉 彩花さん

〈宮城県警察本部〉

なりすましに注意!!

宮城県 聖ウルスラ学院英智高等学校 1年

奥西 南凪さん

〈山形県警察本部〉

気軽に会って大丈夫…？

山形県 山形県立酒田光陵高等学校 3年

髙橋 亜捺惟さん

〈茨城県警察本部〉

一瞬の過ちは一生の後悔

茨城県 水戸女子高等学校 3年

岡﨑 紘佳さん

〈埼玉県警察本部〉

直接話そう

埼玉県 埼玉県立新座総合技術高等学校 1年

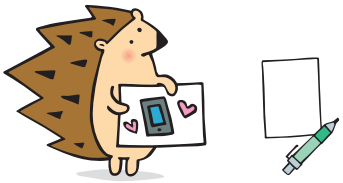
犬竹 夢花さん

〈東京情報大学〉

甘い罠

千葉県 市川高等学校 1年

植田 夏帆さん



もし言葉の暴力が具現化されたら？

〈一般社団法人東京都情報産業協会〉

東京都 東京都立葛飾総合高等学校 3年

伊藤 柚衣さん

スマホで友達ができました

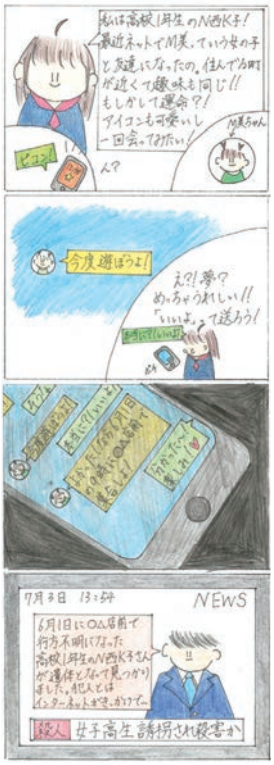
〈石川県警察本部〉

石川県 野々市市立野々市中学校 2年

酒谷 奏海さん

相手は誰…

〈一般社団法人石川県情報システム工業会〉



石川県 石川県立小松明峰高等学校 1年

井上 聖徠さん

アカウントを乗っ取られたら…？

〈福井県警察本部〉

福井県 福井県立美方高等学校 1年

岩本 結愛さん

無題

〈一般社団法人長野県情報サービス振興協会〉

長野県 上田市立第五中学校 2年

小澤 奈都美さん

その人本当に信頼できますか？

〈岐阜県警察本部〉

岐阜県 岐阜県立岐阜総合学園高等学校 1年

田中 清羽さん

フリー WiFi

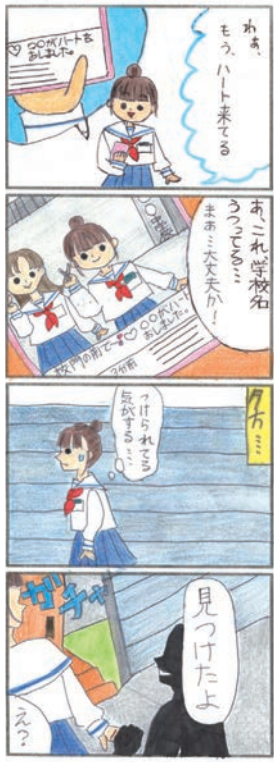
〈特定非営利活動法人ふじのくに情報ネットワーク機構〉

静岡県 静岡県立浜名高等学校 1年

大石 好美さん

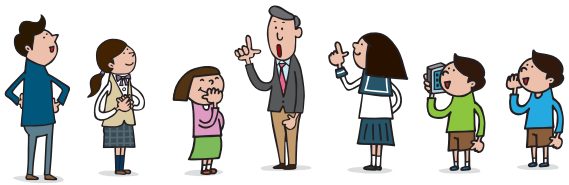
脅威はすぐそばに

〈滋賀県警察本部〉



滋賀県 愛荘町立秦荘中学校 2年

青木 杏佳さん



ちょっと待って！

〈京都府私立中学高等学校情報科研究会〉

京都府 京都聖母学院高等学校 1年

長谷 唯杏さん

ウイルス対策

〈京都コンピュータ学院〉

京都府 京都府立綾部高等学校東分校 1年

沖 泉希さん

デマ情報に気をつけろ！

〈大阪府警察本部〉

大阪府 帝塚山学院高等学校 1年

山田 小夕姫さん

電車の風景

〈兵庫県警察本部〉

兵庫県 兵庫県立大学附属高等学校 1年

中村 有希さん

自ら考える

〈一般社団法人システムエンジニアリング岡山〉

岡山県 岡山県立倉敷南高等学校 1年

髙倉 優依さん

そのパスワードで大丈夫？

〈広島県インターネット・セキュリティ対策推進協議会〉

広島県 広島県立福山葦陽高等学校 1年

谷廣 陽子さん

恐怖の連鎖

〈福岡県警察本部〉

福岡県 福岡県立小倉東高等学校 2年

東 奈月さん

その一言が・・・

〈長崎県ネットワーク・セキュリティ連絡協議会〉

長崎県 諫早市立西諫早中学校 2年

赤石 心奈さん

索引

I

J

K

L

M

N

O

P

R

さ

た

な

は

ま

ら

MEMO

MEMO

おわりに

2021年度もコロナ禍が継続し、厳しい制限はありましたが、東京と北京のオリンピック・パラリンピック競技大会は無事開催され、大規模なサイバー攻撃被害もありませんでした。その一方で、ランサムウェア、フィッシング等の攻撃はより巧妙になりました。 テレワークや生活のデジタル化の進展により、攻撃被害はより深刻になることが懸念されます。

更に2022年にはいり、ウクライナ危機という新しい脅威が出現し、武力だけでなく情報の戦いが前面に出て、紛争当事者ではない組織や個人がサイバー攻撃や情報の混乱に巻き込まれる、というリスクが顕在化しました。このリスクには虚偽の情報による混乱が含まれますが、3章の個別テーマ「3.4 米国・欧州の情報セキュリティ政策」で丁寧に解説しました。

本白書のサブタイトルは「ゆらぐ常識、強まる脅威：想定外にたちむかえ」としました。これまで想定できなかった大きな環境変化においてもリスク管理の基本を見失わず、連携して対処していこうという思いを込めています。

本白書は多岐にわたるサイバーセキュリティに関する国内外の事象や動向を調査・分析し、分かりやすい解説を心掛け、IPA職員だけでなく外部有識者の協力を得て作成しています。また、IPAのWebサイトからPDF版が無料でダウンロードいただけます。 冊子、PDF版ともに、皆さまのサイバーセキュリティ対策の検討・実践の一助となれば幸いです。

編集子

著作・製作　独立行政法人情報処理推進機構（IPA）

編集責任　瓜生 和久　小川 隆一　小山 明美　白石 歩　佐川 陽一
涌田 明夫

執筆者　IPA
伊藤 吉史　小川 隆一　神田 雅透　小山 明美　島田 毅
白石 歩　西尾 秀一　松坂 志　山里 拓己　赤木 伸悟
荒牧 慧　板垣 寛二　伊藤 彰朗　江島 将和　大島 尚
大友 更紗　奥田 美幸　小幡 宗宏　甲斐 成樹　亀田 恭史
亀山 友彦　河合 真吾　木村 泰介　栗原 史泰　黒岩 俊二
佐伯 稔　佐川 陽一　佐藤 栄城　柴本 憲一　竹内 俊輝
武智 洋　田島 威史　田村 智和　丹野 菜美　近澤 武
辻 宏郷　中島 尚樹　野村 春佳　橋本 徹　長谷川 智香
平尾 謙次　福岡 尊　福原 聡　冨士 愛恵里　松島 伸彰
松田 琳花　宮本 一弘　宮本 冬美　森 淳子　安田 進
横山 美晴　吉野 和博　與那嶺 崇　渡邉 祥樹　藁科 綾子
株式会社日立製作所　相羽 律子
国立研究開発法人情報通信研究機構　中尾 康二
一般社団法人 JPCERT コーディネーションセンター　米澤 詩歩乃
情報規格調査会 JTC 1 ／ SC 27 ／ WG 5 小委員会

協力者　IPA
加賀谷 伸一郎　桑名 利幸　田口 聡　日向 英俊　前田 祐子
松井 洋二　松田 修平　渡辺 貴仁　石田 淳一　板橋 博之
伊藤 博康　内海 百葉　川﨑 宏　塩田 英二　土屋 正
遠山 真　西原 栄太郎
一般社団法人 JPCERT コーディネーションセンター　江田 佳領子
長崎県立大学　島 成佳
三井物産セキュアディレクション株式会社　増田 聖一
経済産業省商務情報政策局サイバーセキュリティ課
経済産業省貿易経済協力局安全保障貿易管理課

情報セキュリティ白書 2022

ゆらぐ常識、強まる脅威：想定外にたちむかえ

2022 年 7 月 15 日　第 1 版発行

企画・著作・制作・発行　**独立行政法人情報処理推進機構（IPA）**
〒 113-6591
東京都文京区本駒込2丁目 28 番8号
文京グリーンコートセンターオフィス 16 階
URL　https://www.ipa.go.jp/
電話　03-5978-7503
E-Mail spd-book@ipa.go.jp

表紙デザイン／本文 DTP・編集　**伊藤 千絵、久磨 公治、涌田 明夫、北林 俊平**