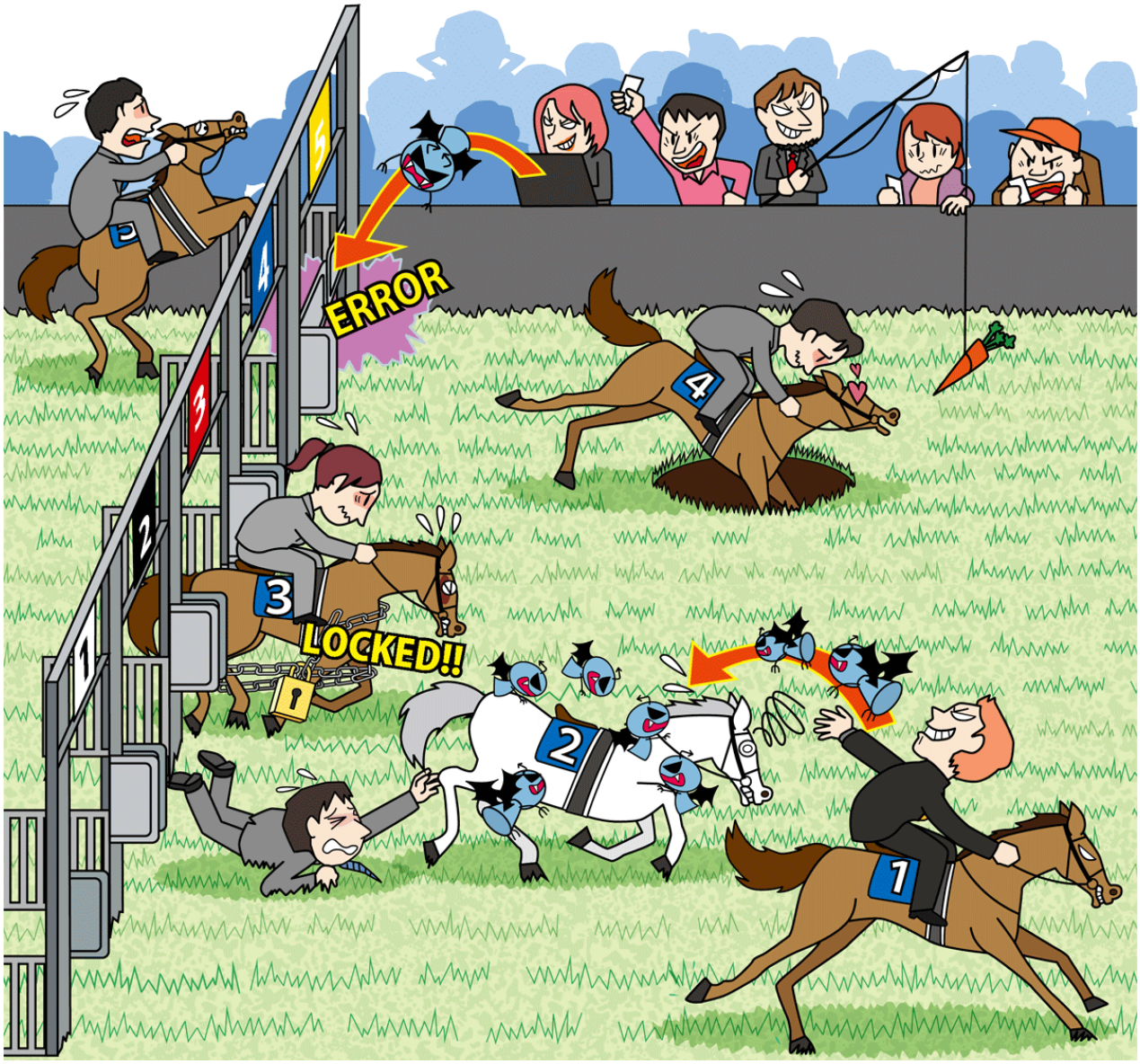
情報セキュリティ

10 大脅威 2022

～誰かが対策をしてくれている。そんなウマい話は、ありません！！～



IPA 独立行政法人情報処理推進機構
セキュリティセンター

2022 年 3 月

本書は、以下の URL からダウンロードできます。

「情報セキュリティ 10 大脅威 2022」
https://www.ipa.go.jp/security/vuln/10threats2022.html

目次

はじめに

本書「情報セキュリティ 10 大脅威 2022」は、情報セキュリティ専門家を中心に構成する「10 大脅威選考会」の協力により、2021 年に発生したセキュリティ事故や攻撃の状況等から脅威を選出し、投票により順位付けして解説した資料である。「個人」と「組織」という異なる立場で、それぞれの脅威を順位付けし、立場毎に 10 大脅威を決定した。

各脅威が自分自身や自組織にどう影響するか確認しながら本書を読み進めることで、様々な脅威と対策を網羅的に把握できる。

本書が、読者自身のセキュリティ対策への取り組みと、各組織の研修やセキュリティ教育等に活用されることによるセキュリティ対策の普及の一助となることを期待する。

【本書の概要】

- 情報セキュリティ 10 大脅威 2022

個人の 10 大脅威では昨年に引き続き順位の変動はあるが同じ 10 個の脅威がランクインした。また、1 位となった「フィッシングによる個人情報等の窃取」は、「10 大脅威 2019」以降続いていた 2 位からランクアップし、初めて 1 位となった。

一方、組織の 10 大脅威では、7 位に初めて「修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）」がランクインした。ゼロデイ攻撃は事前の対策ができないため、組織としては攻撃検知後の対応方針を決め、関係者に徹底しておくことが重要である。

本書では、2021 年の脅威の動向を 10 大脅威として解説する。

情報セキュリティ10 大脅威 2022

情報セキュリティ 10 大脅威 2022

■「情報セキュリティ 10 大脅威 2022」

2021 年において社会的に影響が大きかったセキュリティ上の脅威について「10 大脅威選考会」の投票結果に基づき、「情報セキュリティ 10 大脅威 2022」では、「個人」と「組織」向け脅威として、それぞれ表 1.1 の通り順位付けした。

表 1.1 情報セキュリティ 10 大脅威 2022 「個人」および「組織」向けの脅威の順位

「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

本章で共通的に使われる用語について**表 1.2** に定義を記載する。

表 1.2 情報セキュリティ 10 大脅威 2022 用語定義

用語	意味
個人	家庭等でスマートフォンや PC を利用する人
セクストーション	被害者のプライベートな写真や動画を入手したとして、それをばらまく等と脅迫する行為
組織	企業、政府機関、公共団体等の組織およびその組織に所属している人
組織的犯行グループ	金銭を目的とした攻撃（犯罪）者集団
諜報員、産業スパイ	機密情報窃取を目的とした攻撃（犯罪）集団 国家組織の支援を受けた攻撃（犯罪）集団
犯罪者	金銭や情報窃取（ストーカー行為を含む）を目的とした攻撃（犯罪）者
マイニング	PC 等を使って仮想通貨の取引に関連する情報を計算し、取引を承認する行為。計算の報酬として仮想通貨を得られる。
CSIRT	セキュリティインシデント等の問題が発生した際に原因究明や影響範囲の調査等を行う組織。自組織に関する問題に対応する場合は、自組織 CSIRT と呼ぶ。
IoT	モノのインターネット（Internet of Things）。ネットワークカメラや情報家電、医療機器といった様々な機器がインターネットにつながり、通信を行う仕組み。機器自体を指す場合は、IoT 機器と呼ぶ。

■「情報セキュリティ 10 大脅威 2022」をお読みになる上での留意事項

① 順位に捉われず、立場や環境を考慮する

「情報セキュリティ10 大脅威 2022」は、「10 大脅威選考会」の投票結果に基づき順位付けして「個人」「組織」それぞれ 10 個の脅威を選定している。投票結果により決定した順位ではあるが、上位の脅威だけ、または上位の脅威から優先して対策を行えばよいということではない。

例えば、個人の立場では、フィーチャーフォン（ガラケー）を利用している方であれば、スマートフォン利用者を狙った脅威である「スマホ決済の不正利用」（本書、個人 5 位）や「不正アプリによるスマートフォン利用者への被害」（本書、個人 7 位）への対策の必要性は低くなる。

また、組織の立場では、オンラインショッピング等で個人情報を取り扱う組織であれば、その情報を狙った脅威である「インターネット上のサービスへの不正ログイン」（本書、組織ランク外、昨年の組織 8 位）を優先的に対策しなければならないだろう。

順位が高いか低いかに関わらず、自身または組織が置かれている立場や環境を考慮して優先度を付け、適切な対応を取る必要がある。

② ランクインした脅威が全てではない

「情報セキュリティ 10 大脅威 2022」で新しくランクインした脅威もあるが、それに伴いランク外となった脅威もある。しかし、ランク外になったとしてもその脅威が無くなったわけではない。かつてランクインしていた、「ワンクリック請求等の不当請求」、「ウェブサイトの改ざん」や「サービス妨害攻撃によるサービスの停止」等は、依然として攻撃が行われている状況である。

ランク外の脅威だから対策を行わなくて良いということではなく、継続しての対策が必要となる。

尚、ランク外となった脅威の詳細や対策方法等については、過去の「情報セキュリティ 10 大脅威」を参考にしてほしい。

③ 「情報セキュリティ対策の基本」が重要

世の中には「情報セキュリティ 10 大脅威」へランクインした脅威以外にも多数の脅威が存在する。とは言え、これらが利用する「攻撃の糸口」は似通っており、脆弱性を突く、ウイルスを使う、ソーシャルエンジニアリングを使う等の古くから知られている手口が使われている。

詳しくは「情報セキュリティ 10 大脅威 2015」の1章で解説しているが、表 1.3 に示すように「攻撃の糸口」を 5 つに分類し、それぞれに該当する対策を「情報セキュリティ対策の基本」としている。「攻撃の糸口」に変化がない限り、「情報セキュリティ対策の基本」による効果が期待できるので、これを意識して継続的に対策を行うことで、被害に遭う可能性を低減できると考える。

表 1.3 情報セキュリティ対策の基本

攻撃の糸口	情報セキュリティ対策の基本	目的
ソフトウェアの脆弱性	ソフトウェアの更新	脆弱性を解消し攻撃によるリスクを低減する
ウイルス感染	セキュリティソフトの利用	攻撃をブロックする
パスワード窃取	パスワードの管理・認証の強化	パスワード窃取によるリスクを低減する
設定不備	設定の見直し	誤った設定を攻撃に利用されないようにする
誘導（罠にはめる）	脅威・手口を知る	手口から重要視するべき対策を理解する

また、昨今はクラウドサービスの利用も一般的になってきている。クラウドサービスを利用する場合は、表 1.4 の対策を「情報セキュリティ対策の基本」+ α として行うことで、被害に遭う可能性を低減できると考えるので参考にしてほしい。

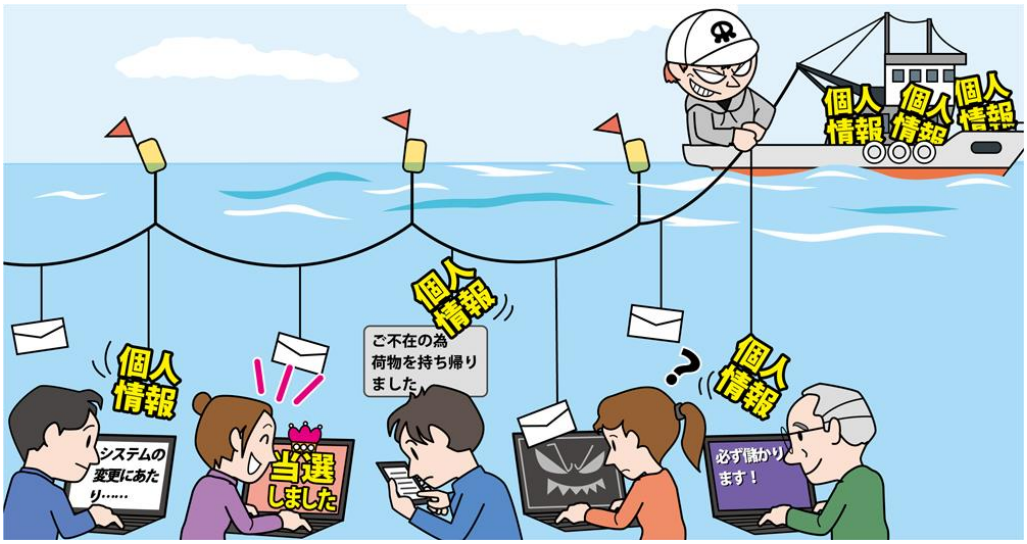
表 1.4 情報セキュリティ対策の基本+ α

備える対象	情報セキュリティ対策の基本＋ α	目的
インシデント全般	責任範囲の明確化（理解）	インシデント発生時に誰（どの組織）が対応する責任があるのかを明確化（理解）する
クラウドの停止	代替案の準備	業務が停止しないように代替策を準備する
クラウドの仕様変更	設定の見直し	仕様変更により意図せず変更された設定を適切な設定に直す（設定不備による情報漏えいや攻撃への悪用を防止する。）

1. 情報セキュリティ 10 大脅威（個人）

1位 フィッシングによる個人情報等の詐取

～宅配の不在通知を装うフィッシング詐欺に要注意！！～



フィッシング詐欺は、公的機関や金融機関、ショッピングサイト、宅配業者等の有名企業を騙るメールやSMS（ショートメッセージサービス）を送信し、正規のウェブサイトを模倣したフィッシングサイト（偽のウェブサイト）へ誘導することで、認証情報やクレジットカード情報、個人情報を入力させ詐取する手口である。攻撃者に詐取された情報を悪用されると金銭的な被害等が発生する。

＜攻撃者＞

- 組織的犯罪グループ
- 犯罪者

＜被害者＞

- 個人（インターネット利用者）
- 組織（インターネット利用者）

＜脅威と影響＞

有名企業を騙ったメールや SMS を送り付け、本文に記載したフィッシングサイトの URL にアクセスさせる。フィッシングサイトで認証情報やクレジットカード情報、個人情報を入力してしまうと、攻撃者に情報を詐取され、詐取された情報は悪用され、最終的に金銭的な被害が発生する。

近年では、メールや SMS 以外に SNS（ソーシャル・ネットワーキング・サービス）を悪用したフィッシング詐欺が発生している。

＜攻撃手口＞

◆ フィッシングサイトへ誘導するメール等を不特定多数に送信

攻撃者が、有名企業のウェブサイトを模倣したフィッシングサイトを作成する。攻撃者は、被害者をそのフィッシングサイトに誘導するために、宛先や本文を本物の有名企業と信じさせる内容のメッセージを SMS、メールや SNS で不特定多数に送信する。それに騙された被害者はフィッシングサイトに誘導され、個人情報やクレジットカード番号等の重要な情報を入力してしまい、情報を詐取される。テキスト表記上の（見た目の）URL と実際のジャンプ先 URL が異なるものもある。

別の手口では、宅配便業者の不在通知を装った SMS を送信し、フィッシングサイトに誘導する（スミッシング）ケースがある。誘導された被害者は、個人情報を入力してしまうと、その情報を攻撃者に詐取される。

◆ 検索サイトの検索結果に偽の広告を表示

検索エンジンの検索結果に表示される広告の仕組みを悪用し、人気商品の大幅な値引き等で目を引く、虚偽の不正な広告を表示する。不正な広告のリンクにアクセスすると、フィッシングサイトへ誘導され、個人情報の入力を促される。

【詐取した情報の悪用例】

- 詐取した個人情報を違法取引のウェブサイトで販売し、攻撃者が金銭を得る。
- 詐取した認証情報でインターネットサービスに不正ログインし、不正送金したり、物品を購入しそれを転売したりすることで金銭を得る。

＜事例または傾向＞

◆ 「水道局」を騙った不審メール

2021 年 12 月、「水道局」を騙った不審メールが確認されているとして、東京都水道局が注意喚起を行った。メールにはフィッシングサイトへ誘導することを目的として「水道料金を支払わなければ断水する」、「リンクをクリックしてお支払いください」といった内容が記載されており、メール内のリンクをクリックすると東京都水道局のサイトを模倣した別サイトに移動する。移動先のサイトでは、フィッシング詐欺やウイルス感染のおそれがあるとしている。[1]

◆ 宅配便の再配達受付を装ったスミッシング

2021 年 8 月、佐川急便は自社を装ったスミッシングの事例を公開した。宅配便の再配達受付サービスを装う SMS が届き、SMS 内のリンクから偽サイトに誘導される。偽サイトは、URL が異なるが佐川急便のページを模倣して作成されており、電話番号やマイナンバーカード等の本人確認書類、Apple ID やパスワードの入力を求めてくる。[2]

◆ フィッシング報告件数は依然として増加傾向

2021 年は 2020 年の報告件数を大幅に上回り、Amazon、三井住友カードを騙るフィッシングが継続して報告されている。[3,4] また、スミッシングについては、宅配業者の不在通知を装った SMS を悪用する事例が依然として確認されている。2021 年 10 月～12 月にかけては、Amazon、au、ドコモを騙るものも確認されている。[4]

＜対策/対応＞[5]

個人（インターネット利用者）

- 被害の予防（被害に備えた対策含む）
  - ・表 1.3「情報セキュリティ対策の基本」を実施
  - ・SMS やメールで受信した URL や、SNS の投稿内の URL を安易にクリックしない

    自身の資産や重要情報を扱うウェブサイトは、ウェブブラウザのブックマーク（お気に入り）にあらかじめ登録した URL やサービス運営者が配布している公式アプリを利用してアクセスする。
  - ・多要素認証の設定を有効にする

    詐取後の不正ログインを防ぐ。
  - ・迷惑メールフィルターを利用
  - ・いつもと異なるログインがあった場合に通知する設定を有効にする

    通知があった際は自身のログインによるものか確認する。
- 被害の早期検知
  - ・利用しているサービスのログイン履歴の確認

    自身のものではないログイン履歴、不正利用がないかを確認する。
  - ・クレジットカードやインターネットバンキングの利用明細を確認
- 被害を受けた後の対応
  - ・パスワードを変更する（他のサービスで同じパスワードを使っていた場合は同様に対応）
  - ・サービス運営者（コールセンター等）へ連絡
  - ・信頼できる機関に相談

    警察、国民生活センター、地域の消費生活センターに相談する。

参考資料

1. 料金請求に関する不審メールについて（東京都水道局）
https://www.waterworks.metro.tokyo.lg.jp/press/r03/press211201-01.html
2. 佐川急便を装った迷惑メールにご注意ください（佐川急便株式会社）
https://www2.sagawa-exp.co.jp/whatsnew/detail/721/
3. 2020/12 フィッシング報告状況（フィッシング対策協議会）
https://www.antiphishing.jp/report/monthly/202012.html
4. 2021/12 フィッシング報告状況（フィッシング対策協議会）
https://www.antiphishing.jp/report/monthly/202112.html
5. フィッシング対策ガイドライン（2021年度版）（フィッシング対策協議会）
https://www.antiphishing.jp/report/antiphishing_guideline_2021.pdf

2位 ネット上の誹謗・中傷・デマ

～1 つの発言が人生を脅かす可能性も～

SNS（ソーシャル・ネットワーキング・サービス）等の匿名で利用できるサービスで特定の個人あるいは企業への誹謗・中傷の行為が行われることが問題となっている。この行為により被害者は精神的苦痛を受ける、風評被害を受けて信頼や信用を損なうことや、経済的な損失を被ることもある。2021 年に東京で開催された、オリンピック・パラリンピックの出場選手をターゲットとした事例もあった。

＜攻撃者＞

- 情報モラル、情報リテラシーが低い人
- 悪意を持っている人

＜被害者＞

- 個人
- 組織（教育機関、公共機関、企業）

＜脅威と影響＞

SNS のサービスの普及に伴い、匿名での広範囲な情報発信が容易に行えるようになっている。一方、そのサービスを利用し、意図的に他人への誹謗・中傷や、脅迫・犯罪予告・デマを書き込む事件が確認されている。さらに、その情報が多くの人に拡散され、大きな問題となる場合がある。

攻撃の対象が個人であれば、精神的苦痛を受けたり、組織であれば、風評被害による経済的な損失を受けたりといった、様々な影響が出る。また、非常時に偽の情報が拡散された場合、社会的な混乱を引き起こすおそれがある。一方、誹謗・中傷やデマの発信は犯罪になりうる事ことや、情報の真偽を確認せず、安易に拡散した人も、その行為を特定され、社会的責任を問われる場合がある。

＜要因＞

◆　匿名性を利用した影響ある情報発信

特定の個人、企業に対する意見や感情を発言する際に、その内容についての影響を考慮せずに発信してしまう。オープンなサービスの場合、1 つの発言が内容によっては大きな規模の影響をもたらすことがある。匿名での発信であることでその内容が過激になりやすい環境であることも要因の 1 つである。なお、匿名であっても警察が調査すれば身元を特定できる場合が多い。

◆　第三者による情報の拡散・改変

SNS 等のサービスで誰かが発信した特定の個人や企業を貶める誹謗中傷や真偽不明のデマについて、それを見た第三者が、悪意の有り無し関係なく真偽を確認せずに拡散する。そして、伝言ゲームのように別の第三者がさらに拡散することで、誹謗中傷やデマが広範囲に周知されてしまう。

また、受け取った内容をさらに別の第三者の真偽不明な情報と紐づけて拡散することで、その第三者にも誹謗中傷が広がる場合もある。

＜事例または傾向＞

◆　オリンピック選手に向けての誹謗・中傷

2021 年 7 月、オリンピックに出場した選手が自身の SNS に対して誹謗・中傷のメッセージが大量に送られてきていることを告白した。選手は、送られてきた悪質なメッセージについては、スクリーンショットで記録を残し、関係各所へ連絡、然るべき措置を取ると意思を示した。[1]

◆　デマ画像によるデマの拡散

2021 年 11 月、SNS 上に、通天閣のネオン表示が新型コロナウイルスのワクチン接種を批判する旨の内容に編集されたデマ画像が出回った。投稿はネット上で拡散され、通天閣の運営会社には事実確認や苦情の連絡が約 30 件寄せられる事態になった。同社は再度デマ画像が拡散された場合、法的措置を検討するとしている。[2]

＜対策/対応＞

個人（発信者）

- 情報モラルや情報リテラシーの向上、法令遵守の意識の向上

  ・誹謗、中傷や公序良俗に反する投稿をしない

  ・投稿前に内容を確認する

  SNS やブログ等のソーシャルメディアに投稿する内容は不特定多数の人に見られることを想定し、投稿して問題ない内容かどうかを投稿前にしっかりと確認する。

  ・匿名性がある場合でも発言には責任を持つ

  匿名で投稿していても、権利侵害があった場合は被害者がプロバイダー等に発信者情報の開示を請求できる。発信者の特定は可能であり、発信者は犯罪になりうるという認識を持ち、発言内容には十分に留意する。

個人（家庭）、組織（教育機関）

- 情報モラル、情報リテラシーの教育

  ・子供たちへの教育の実施

  自宅や学校で子供たちに情報モラルや情報リテラシーの教育を行う。さらに、トラブルの事例を伝え、悪質な行為は犯罪になりうることを理解させる。[3]

個人（閲覧者）

- 情報モラルや情報リテラシーの向上、法令遵守の意識の向上

  ・情報の信頼性の確認

  インターネット上に流通している情報が必ずしも正しいとは限らないことを認識し、その情報を安易に拡散せず、一次情報やその他複数の情報元を確認し、信頼できる情報かどうかを総合的に判断する。[4] また、デマの拡散は、犯罪になりうることを理解する。

個人（被害者）

- 被害を受けた後の適切な対応

  ・冷静な対応と支援者への相談

  一人で抱え込まず、信頼できる周囲の人や公的相談機関へ相談する。[5] 脅迫や名誉毀損に該当する誹謗・中傷等、犯罪と思われる投稿は警察へ被害届を提出し、必要に応じて弁護士にも相談する。

  ・管理者やプロバイダーへ削除依頼

  問題ある書き込みを削除したいときは本人または関係者がウェブサイトの管理者やプロバイダーに削除を要請する。なお、削除により事態が悪化する可能性もあるため、要請する際は信頼できる周囲の人や弁護士等に相談して慎重に行う。

参考資料

1. 水谷隼「しかるべき措置をとる」 実際の誹謗中傷DMを公開（grape）
https://grapee.jp/991168
2. 通天閣に「射っちゃダメ」 デマ画像拡散に怒り（ITmediaビジネスONLiNE）
https://www.itmedia.co.jp/business/articles/2111/07/news020.html
3. インターネットトラブル事例集 （2021年版）（総務省総合通信基盤局）
https://www.soumu.go.jp/main_content/000707803.pdf
4. ファクトチェックとは（認定NPO法人 ファクトチェック・イニシアティブ）
https://fij.info/introduction
5. #NoHeartNoSNS（ハートがなけりゃSNSじゃない！）（総務省sss総合通信基盤局）
https://www.soumu.go.jp/main_sosiki/joho_tsusin/kyouiku_joho-ka/no-heart-no-sns.html

3位 メールや SMS 等を使った脅迫・詐欺の手口による金銭要求

～公的機関を装ったメール等に注意～

個人の秘密を家族や知人にばらすと脅迫したり、身に覚えのない有料サイトの未納料金を請求したりするメールや SMS（ショートメッセージサービス）、LINE 等を使った詐欺による金銭被害が発生している。公的機関を装った偽の相談窓口に誘導するといった手口もある。

＜攻撃者＞

- 組織的犯行グループ

＜被害者＞

- 個人（インターネット利用者）

＜脅威と影響＞

「アダルトサイトを閲覧している姿を撮影した」等の脅迫メールや有料サイトの未納金があるといった架空請求のメールを送信し、金銭を詐取しようとする攻撃が行われている。また、メールや SMS、LINE 等を使った同様の手口も確認されている。

脅迫・詐欺のメールの内容は虚偽のものであるが、その内容を信じてしまい不安に思ったメール受信者が金銭を支払ってしまう。そして、一度でも攻撃が成功してしまうと、その脅迫は効果が期待できると攻撃者に認識され、同様の手口で多数の宛先へメール送信を行い、さらに被害が拡大するおそれがある。

＜攻撃手口＞

脅迫や架空請求によって金銭を要求する内容のメールや SMS、LINE 等を不特定多数に送り、金銭を詐取しようとする。指定される支払方法には暗号資産（仮想通貨）や電子マネーが多く見られる。また、騙す手口として以下が使われる。

◆ セクストーション（性的脅迫）

「アダルトサイトを閲覧している姿を撮影した」等、周囲に相談しにくい性的な内容で脅す。

◆ ハッキングしたように見せかける

被害者のパスワードや住所等の個人情報をメールに記載し、あたかも被害者の PC をハッキングして情報を得たかのように見せかける。記載している情報はハッキングによるものではなく、外部のサービスから何らかの原因で漏えいした情報を使用している。

◆ 公的機関を装う

公的機関等信頼できる組織の発信を装うことでメール等の信憑性、緊急性を高め、騙そうとする。

◆ メールや電話を併用して信憑性を高める

脅迫・詐欺目的のメールに、偽の問合せ窓口の電話番号を記載して送信し、この電話番号宛に被害者から電話を掛けさせる。電話を掛けてきた被害者に対して、攻撃者は更に脅迫を行ったり、電話口で公的機関を装った偽の相談窓口を紹介し、そ

の窓口に電話を掛けさせて信頼させた上で金銭を支払わせたりする。また、攻撃者から被害者に対して金銭を要求する電話をかけ、その後に弁護士を装った攻撃者から和解を求める旨のメールを送信し、信憑性を高めて騙そうする手口もある。

＜事例または傾向＞

◆ **公的機関を騙り、金銭を要求**

2021 年 10 月、消費者庁は、「消費者庁」、「国民生活センター」等を騙り、架空の「和解金」の交付を持ち掛け、「書類作成費用」等の名目で金銭を支払わせるメールや SMS が確認されたとして注意喚起を行った。支払いは、電子マネーを購入して支払うように誘導し、購入した電子マネーの ID を連絡させることで電子マネーを詐取する。また、受信者がメールを無視すると「罰則を科せられる」等、脅かすようなメッセージが送信される。[1]

◆ **警察の LINE アカウントを装い連絡、架空請求の可能性**

2021 年 9 月、広島県警は、同県警サイバー犯罪対策課を装う LINE アカウントが確認されているとして注意喚起を行った。「あなたの LINE アカウントが通報された」、「自宅または連絡可能な所在地へ郵送にて通達文を送付する」等、不安を煽り、連絡を取るよう求めてくる。同県警は架空請求やフィッシング詐欺の可能性があるとしている。[2]

◆ **暗号資産で金銭を要求するメールの相談件数が昨年より増加**

IPA 情報セキュリティ安心相談窓口によると、暗号資産で金銭を要求する迷惑メールの相談件数が、2020 年の 244 件に対して 2021 年は 513 件となり、大幅に増加している。[3,4] また、2021 年 3 月には、受信者が性的な映像を見ていることを知ったとして、知人にばらされたくなかったらビットコインで送金しろと恐喝するメール（セクストーション）が引き続き確認されている。メール文面の日本語は不自然で、英文を翻訳サイト等の機械翻訳にかけたものと考えられるが、年々、違和感が少なくなってきている。[5]

＜対策/対応＞

個人（インターネット利用者）

- 被害の予防（被害に備えた対策含む）
  - ・表 1.3「情報セキュリティ対策の基本」を実施
  - ・受信した脅迫、詐欺メールは無視する
    受信したメールに、被害者のパスワードが記載されていても、実際にハッキングされていることはほぼない。
  - ・メールに記載されている番号に電話をしない
    受信した脅迫や架空請求のメールについて専門機関に相談したい場合は、そのメールに記載された連絡先ではなく、自身で調べた正規の電話番号やメールアドレスに連絡する。
  - ・メールで要求された支払いには応じない
  - ・多要素認証の設定を有効にする
- 被害を受けた後の対応
  - ・パスワードを変更する（他のサービスで同じパスワードを使っていた場合は同様に対応）
    脅迫・詐欺メールに記載されたパスワードが自身の実際のパスワードと一致しているのであれば、そのパスワードを利用しているサイトからパスワードが漏えいした可能性があるので、早急にパスワードを変更する。また、パスワードは使い回さない。
  - ・警察に相談する

参考資料

1. 消費者庁などの公的機関の名称をかたり、架空の「和解金」などの交付を持ち掛けて金銭を支払わせる事業者に関する注意喚起（消費者庁）
https://www.caa.go.jp/notice/entry/026250/
2. 「あなたのアカウントが通報された」 - 偽警察のLINEアカウントに注意（Security NEXT）
https://www.security-next.com/129668
3. 情報セキュリティ安心相談窓口の相談状況［2020年第4四半期（10月～12月）］（IPA）
https://www.ipa.go.jp/security/txt/2020/q4outline.html
4. 情報セキュリティ安心相談窓口の相談状況［2021年第4四半期（10月～12月）］（IPA）
https://www.ipa.go.jp/security/txt/2021/q4outline.html
5. 性的な映像をばらまくと恐喝し、仮想通貨で金銭を要求する迷惑メールに注意（IPA）
https://www.ipa.go.jp/security/anshin/mgdayori20181010.html

4位 クレジットカード情報の不正利用

～不審な利用記録がないか今一度確認を～

キャッシュレス決済やオンラインショッピングの普及に伴い、クレジットカードを利用する機会が増えている。一方、所有者を狙ったフィッシング詐欺やクレジットカード情報が登録されている各種サービスサイトを狙った不正アクセスによる情報漏えいにより、クレジットカード情報が窃取され、攻撃者にクレジットカードを不正利用される被害が継続して発生している。

＜攻撃者＞

- 組織的犯罪グループ
- 犯罪者

＜被害者＞

- 個人（クレジットカード利用者）
- 組織（サービス事業者、クレジットカード会社）

＜脅威と影響＞

オンラインショッピングの一般化に加え、近年のキャッシュレス決済の普及に伴い、クレジットカードを活用する機会が増えている。そのクレジットカード情報が攻撃者に狙われている。攻撃者は、フィッシング詐欺により詐取したり、クレジットカードで決済を行っている端末にウイルスを感染させることにより窃取したりする。また、オンラインで提供されている各種サービスへ不正アクセスし、そこに保存されているクレジットカード情報を窃取する。

クレジットカード情報が攻撃者に窃取されると、正規の利用者の知らない間に不正利用され金銭的な被害を受けたり、クレジットカード情報を公開されたり、販売されたりするおそれがある。

＜攻撃手口＞

以下の手口でクレジットカード情報を入手し、不正利用を行う。

◆ フィッシング詐欺

メール等を使い、受信者を騙してフィッシングサイトに誘導し、クレジットカード情報等を詐取する。詳細は個人 1 位「フィッシングによる個人情報等の詐取」を参照。

◆ 正規の決済画面を改ざんし入力情報を詐取

ショッピングサイトの脆弱性を悪用し、正規ウェブサイトの決済画面を改ざんする。その後、改ざんした決済画面に被害者を誘導し、クレジットカード情報を入力させることで、クレジットカード情報を詐取する。

◆ 不正アクセス

脆弱性を悪用し、サービス提供者のシステムに不正アクセスを行い、保存されているクレジットカード情報を窃取する。

◆ **ウイルス感染**

ウイルスをメールに添付して開かせたり、悪意あるウェブサイトのリンクを記載したメール等を送信し、リンクをクリックさせたりすることで、端末をウイルスに感染させる。ウイルスに感染した端末で、利用者がクレジットカード情報を入力すると、入力した情報が攻撃者に窃取されたり、利用者の端末内の情報が窃取されたりする。

◆ **漏えいした情報の悪用**

インターネットサービスから漏えいしたクレジットカード情報を悪用する。漏えいしたクレジットカード情報は、一般的な検索エンジンでは検出されない闇サイト（ダークウェブ）等で売買されることもある。

＜事例または傾向＞

◆ **「ブルークレール Web サイト」でクレジットカード情報流出**

2021 年 5 月、ブルークレールは、運営する「ブルークレール Web サイト」が不正アクセスを受け、1,863 件のクレジットカード情報が流出したことを公表した。流出した当該情報の一部は不正利用されたおそれがあった。原因は、システムの一部の脆弱性を悪用した不正アクセスにより、ペイメントアプリケーションの改ざんが行われたためとしている。[1]

◆ **「コスモスオンラインストア」でクレジットカード情報流出**

2021 年 7 月、コスモス薬品は、EC ウェブサイトとして運営している「コスモスオンラインストア」が不正アクセスを受け、2 万 5,484 件のクレジットカード情報が流出したことを公表した。流出した情報の一部は不正利用されたおそれがあることを確認している。[2]

◆ **被害額は増加、9 割以上が番号盗用被害**

日本クレジット協会が公開した「クレジットカード不正利用被害の集計結果」によれば、2021 年 1～9 月における不正利用被害額は約 236 億 9,000 万円となった。前年同期間の被害額は約 180 億 2,000 万円であり、被害額が大幅に増加している。なお、被害額全体に占める番号盗用被害額の割合は年々増加しており、2021 年においては 94.5%を占めている。[3]

＜対策/対応＞

個人（利用者）

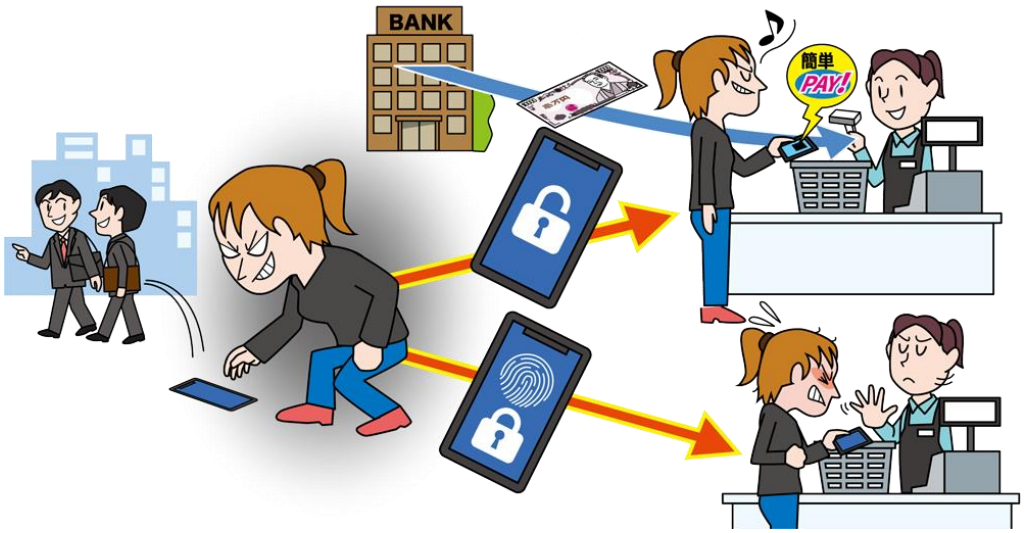
- 被害の予防
  - ・表 1.3「情報セキュリティ対策の基本」を実施
  - ・クレジットカード会社が提供している本人認証サービス（3D セキュア等）の利用
  - ・添付ファイルや URL を安易に開かない
  - ・普段は表示されないような画面やポップアップが表示された場合、情報を入力しない
  - ・プリペイドカードの利用を検討
    不正利用被害額となる利用可能金額の範囲を限定する
- 被害の早期検知
  - ・クレジットカード利用明細の定期的な確認
  - ・サービス利用状況の通知機能の利用
- 被害を受けた後の対応
  - ・サービス運営者（コールセンター等）へ連絡
    クレジットカード会社によっては、全額または一部を補償する場合がある。（補償してくれる期間が短い場合があるので注意）
  - ・クレジットカードの停止
  - ・パスワードを変更する（他のサービスで同じパスワードを使っていた場合は同様に対応）
  - ・ウイルス感染した端末の初期化
  - ・警察への被害届の提出

参考資料

1. 化粧品通販サイトに不正アクセス - クレカ情報流出の可能性（Security NEXT）
https://www.security-next.com/126477
2. 弊社が運営する「コスモスオンラインストア」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（株式会社コスモス薬品）
https://www.cosmospc.co.jp/notice/upload/ed661581b067c469eb29047679fa8a86e6446fe7.pdf
3. クレジットカード不正利用被害の集計結果について（（一社）日本クレジット協会）
https://www.j-credit.or.jp/download/news20211228a1.pdf

5位 スマホ決済の不正利用

～今や「スマートフォン」＝「個人情報、財産」の時代！日頃からリスク管理の徹底を～



近年のスマートフォンの普及に伴い、2018 年頃よりキャッシュレス決済の 1 つであるスマートフォンを利用した決済（スマホ決済）が登場し、その後スマホ決済を使った各社のサービスも登場しその手軽さから普及が進んだ。一方、利便性が高い反面、第三者のなりすましによるサービスの不正利用や、連携する銀行口座からの不正な引き出しも確認されている。

＜攻撃者＞

- 組織的犯行グループ
- 犯罪者

＜被害者＞

- 個人(スマホ決済サービス利用者)
- 個人(スマホ決済サービスと連携可能な銀行口座の所有者)
- 組織（サービス事業者・サービス利用店舗・クレジットカード会社））

＜脅威と影響＞

スマホ決済では、スマートフォンを IC カードリーダーにかざす（非接触型決済）方法や、決済用アプリで生成した QR コードやバーコードを店舗のバーコードリーダーに読み込ませる方法、店舗に置いてある QR コードをスマホアプリで読み込んで決済金額を手動で入力する方法がある。残高をチャージするためには事前にクレジットカード情報や銀行口座番号を登録してそこからチャージできる。これらの情報は決済サービス毎に専用のシステムやアプリで管理されているが、決済サービスや仕組みに不備がある場合、攻撃者に不正利用される。

例えば、決済サービスに不正にログインされると、クレジットカード情報が窃取されたり、意図しない金銭取引をされたり等の被害に遭う。

＜攻撃手口＞

◆　不正アクセスによるアカウントの乗っ取り

被害者が複数のサービスで同一のパスワードを使い回している場合がある。攻撃者は、過去に漏えいした ID とパスワードをリスト化し、それをもとにログインを試みる（パスワードリスト攻撃）。不正ログインに成功すれば、なりすまして不正利用する。また、スマホ決済サービスより提供される多要素認証等のセキュリティ強化機能を利用していない場合、漏えいしたパスワードのみで不正ログインできるため、攻撃者に悪用されやすい。

◆　スマホ決済サービスと連携している銀行口座間における口座振込手続きの不備の悪用

スマホ決済サービスを開発する際に、当該サービスと関連サービスの連携も含めたセキュリティを

十分に考慮していないと、スマホ決済サービスを不正利用できる脆弱性を作り込むおそれがある。

＜事例または傾向＞

◆ **拾ったスマートフォンで PayPay 不正チャージ**

2021 年 10 月、拾ったスマートフォンでスマホ決済サービス「PayPay」に不正チャージした男が「電子計算機使用詐欺」容疑で逮捕された。被害者は携帯電話会社に連絡し、通話や通信機能は使用不能にしていたが、PayPay には届け出ておらず、約 18 万円の不正チャージが行われた。[1]

◆ **PayPay の決済音鳴らし決済完了に見せかけ**

2021 年 8 月、ディスカウントストアでの会計時にスマホ決済サービス「PayPay」の決済音を鳴らすことで会計をしたと見せかけ、食料品等を騙し取った疑いで男が逮捕された。売り上げと PayPay から店への支払い額が合わないケースが複数回あり、発覚した。[2]

◆ **スマホ決済で身に覚えのない不正な支払い**

神奈川県川崎市の経済労働局産業政策部消費者行政センターによると、2021 年 12 月にスマホ決済サービスにおいて、身に覚えのない支払いが行われているとの相談があり、利用限度額いっぱいの 25 万円が使用されていることがわかった。履歴から 15 分間で 10 件の購入を確認されており、事業者に調査依頼をしている。[3]

＜対策/対応＞

個人（スマホ決済サービスの利用者）

- 被害の予防
  - ・表 1.3「情報セキュリティ対策の基本」を実施
  - ・多要素認証の設定を有効にする
  - ・3D セキュアを利用する

  仮にパスワードが攻撃者に漏えいしたとしても、不正ログインや、その後の金銭被害につながる重要な操作を阻止できる確率を高める。
  - ・パスワードは長く、複雑にする [4,5]
  - ・パスワードを使い回さない

  例えばパスワードの基となるコアパスワードを作成し、その前後にサービス毎に異なる識別子を付加することで他と重複しないパスワードを作成することができる。[5]
  - ・パスワード管理ソフトの利用
  - ・フィッシングに注意

  スマホ決済を行っている企業を騙るフィッシングサイトやフィッシングメールに気を付ける。
  - ・利用していないサービスからの退会
  - ・スマートフォンの紛失対策

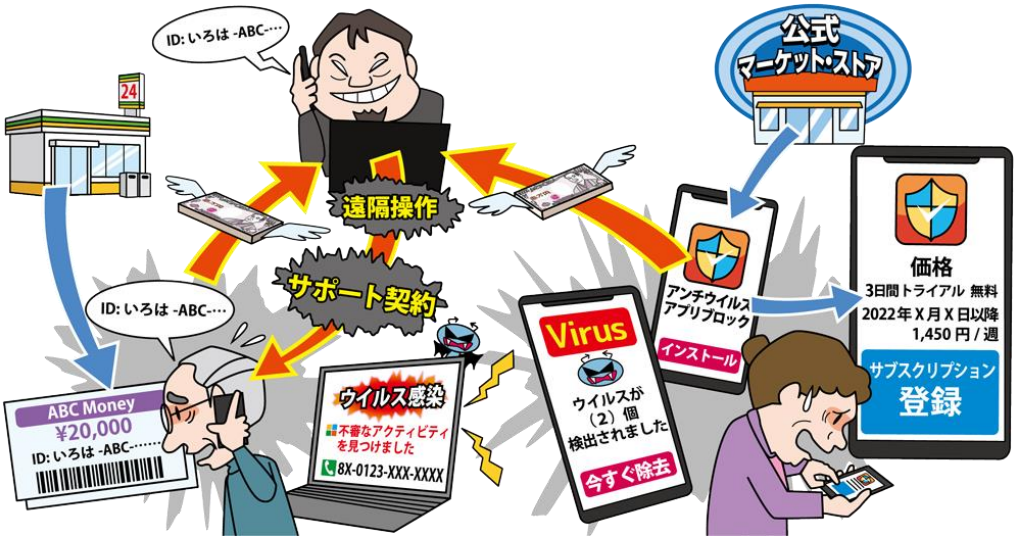
  紛失したスマートフォンを悪用されないために画面ロック等のセキュリティ対策を実施する。
- 被害の早期検知
  - ・スマホ決済サービスの利用状況通知機能の利用および利用履歴の定期的な確認
  - ・連携する銀行口座の出金履歴の確認
- 被害を受けた後の対応
  - ・パスワードを変更する（他のサービスで同じパスワードを使っていた場合は同様に対応）
  - ・サービス運営者（コールセンター等）へ連絡
  - ・連携する金融機関へ連絡
  - ・警察に相談する

参考資料

1. スマホ拾った男、「ペイペイ」で電子マネー詐取…ネット上の撮影写真データで発覚（読売新聞オンライン）
https://www.yomiuri.co.jp/national/20211020-OYT1T50001/
2. 「ペイペイ」決済音鳴らし食品だまし取った疑い、男逮捕（朝日新聞DIGITAL）
https://www.asahi.com/articles/ASP7Y2SXWP7WUTNB011.html
3. キャッシュレス決済の不正利用トラブル（神奈川県川崎市　経済労働局産業政策部消費者行政センター）
https://www.city.kawasaki.jp/280/page/0000135952.html
4. 不正ログイン対策特集ページ（IPA）
https://www.ipa.go.jp/security/anshin/account_security.html
5. 不正ログイン被害の原因となるパスワードの使い回しはNG（IPA）
https://www.ipa.go.jp/security/anshin/mgdayori20160803.html

6位 偽警告によるインターネット詐欺

～それは詐欺です。慌てる、焦るは思うツボ！～



PC やスマートフォンからウェブサイトを閲覧中に、突然「ウイルスに感染しています」等、偽のセキュリティ警告画面を表示して、不審なソフトウェアをインストールさせたり、攻撃者が用意したサポート窓口に電話を掛けさせて PC の遠隔操作や有償サポート契約を結ばされたり、修復費用として金銭を騙し取られたりする被害（サポート詐欺）が発生している。

＜攻撃者＞

- 組織的犯行グループ

＜被害者＞

- 個人（インターネット利用者等）

＜脅威と影響＞

ウェブサイトを閲覧中に、突然「ウイルスが見つかりました」、「Windows のシステムが破損しています」等の偽の警告画面が表示されることがある。表示された警告画面は、実在する企業からの通知のように偽っており、通知される内容を信用させ指示に従うよう促す。

指示に従ってしまうと不審なソフトウェアのインストールや購入をさせられる。また、偽のサポート窓口に連絡をしてしまい、PC の遠隔操作や有償サポート契約を結ばされたり、修復費用を要求されたりする。スマートフォン利用者であれば、不審なアプリをインストールするように誘導される。さらに、ソフトウェアの購入やサポート契約時に入力した氏名、メールアドレス、クレジットカード情報等の個人情報は別の詐欺に悪用され、二次被害につながるおそれもある。

＜攻撃手口＞

◆ 巧妙に細工が施された偽の警告画面

閲覧者を騙すためにウェブサイト等に表示される偽警告は、警告内容を信じさせるために、実在する企業ロゴを使う場合がある。また、警告音を鳴らしたり警告メッセージを音声で流したり、偽警告のポップアップ画面を閉じられないと誤解させたりすることでさらに不安を煽る。

◆ 有償セキュリティソフトの購入へ誘導

閲覧者を偽警告の画面からダウンロードページに誘導し、偽のセキュリティソフトをインストールさせる。最終的に有償ソフトウェアの購入へ誘導する。

◆ サポート詐欺

閲覧者に偽警告の画面に記載されているサポート窓口へ電話をかけさせ、言葉巧みに遠隔操作ツールをインストールさせようとする。その上で、サポート契約や不必要なソフトウェアの購入へ誘導する。サポート契約等の支払い方法はコンビニで

販売されているプリペイド型電子マネーや各種ギフトカードのほか、クレジットカード決済が使われる。

◆　**スマホアプリのインストールへ誘導**

偽警告をスマートフォンの画面に表示し、解決方法として、公式マーケットからスマホアプリをインストールするように誘導する。誘導したことに対して広告主からアフィリエイト収益を得たり、サブスクリプション（自動継続課金）による利用者への料金請求で収益を得たりすることが目的と考えられる。[1]

＜事例または傾向＞

◆　**電話をかけさせて偽のサポートへ誘導**

IPA 安心相談窓口には、「ウイルスに感染している」等、偽のセキュリティ警告の相談が多く寄せられている。2021 年は、偽のセキュリティ警告画面に電話番号を表示して、最初から電話をかけさせて偽のサポートへ誘導する手口が広まった。[2]

電話をかけてしまうと、遠隔操作用ソフトウェアをインストールさせられ、虚偽の説明が行われたり、修理費用として電子マネーの購入を求められたりする。遠隔操作では PC の様々な操作を行うことができ、データの閲覧や消去、PC を起動させなくするといった悪質な操作が行われる危険が伴う。

◆　**PC 修理名目のサポート詐欺事件**

2021 年 11 月、新潟中央警察署はサポート詐欺事案の届出を受理し、特殊詐欺（架空料金請求詐欺）として捜査している。被害者の男性は、自宅で PC を使用していたところ、画面上に「中国にハッキングされている」等のメッセージが表示され、表示されている連絡先に電話したところ、「遠隔操作で PC を修理する。修理費用として電子マネーで支払ってください。」等と言われコンビニエンスストアで電子マネーを購入し、電子マネーの番号を伝え、合計 7 万 5,000 円分騙し取られた。[3]

＜対策/対応＞

個人（インターネット利用者等）

- 被害の予防（被害に備えた対策含む）
  - ・表 1.3「情報セキュリティ対策の基本」を実施
  - ・表示される警告を安易に信用しない
  - ・偽警告が表示されても従わない
    偽警告によって指示されるアプリやソフトウェアはインストールしない。また、電話を掛けない、遠隔操作は許可しない、契約には応じない。
  - ・偽警告が表示されたらブラウザを終了する
  - ・ブラウザの通知機能を不用意に許可しない[4]
    偽警告の中にはブラウザの正規の通知機能を悪用するものもあるので注意する。
  - ・不用意にカレンダーの照会を追加しない[5]
  - ・カレンダー内の不審な予定は削除する
- 被害を受けた後の対応
  - ・端末を初期化する
  - ・虚偽のサポート契約の解消
    近くの消費生活センター[6]に相談する。
  - ・クレジットカード会社へ連絡

参考資料

1. 安心相談窓口だより「スマートフォンで偽のセキュリティ警告からアプリのインストールへ誘導する手口に注意」（IPA）
https://www.ipa.go.jp/security/anshin/mgdayori20190918.html
2. 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！」（IPA）
https://www.ipa.go.jp/security/anshin/mgdayori20211116.html
3. 新潟中央警察署「パソコン修理名目の特殊詐欺被害が発生！！慌てず落ち着いた行動を」（新潟中央警察署）
https://www.pref.niigata.lg.jp/uploaded/attachment/293015.pdf
4. 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」（IPA）
https://www.ipa.go.jp/security/anshin/mgdayori20210309.html
5. 安心相談窓口だより「iPhoneに突然表示される不審なカレンダー通知に注意！」（IPA）
https://www.ipa.go.jp/security/anshin/mgdayori20200330.html
6. 全国の消費生活センター等（（独）国民生活センター）
http://www.kokusen.go.jp/map/index.html

7位 不正アプリによるスマートフォン利用者への被害

～偽装 SMS の URL リンクや不正アプリへの誘導に注意～

スマートフォンの利用者に不正アプリをインストールさせて、スマートフォン内の個人情報を窃取したり、アプリを不正利用して、利用者に不正請求等の損害を与えたりする被害が発生している。昨今は、偽のワクチン接種予約案内や宅配業者になりすました SMS（ショートメッセージサービス）をスマートフォンに送信し、利用者が URL にアクセスすることで不正アプリをインストールさせる他、公式マーケットにウイルスを忍び込ませそのアプリをインストールさせる事例が確認されている。

＜攻撃者＞

- 組織的犯行グループ
- 犯罪者

＜被害者＞

- 個人（スマートフォン利用者）

＜脅威と影響＞

有名な組織を装った SMS がスマートフォンに届き、SMS に記載された URL にアクセスした利用者に対して、不正アプリをインストールするよう誘導してくる。また、公式マーケット上にウイルスを忍ばせた不正アプリを公開し、利用者がそれを知らずにインストールしてしまう場合もある。

不正アプリをスマートフォンにインストールしてしまうと、スマートフォン内に保存されている連絡先や通話記録、位置情報等の情報を窃取される。認証情報を窃取されるとキャリア決済等を不正に使用され、金銭的被害を受けるおそれがある。

また、SMS を送信する踏み台に利用され、意図せず不正な SMS を送信してしまう場合がある。

＜攻撃手口＞

◆ 不正アプリのダウンロードサイトへ誘導する

実在するウェブサイトに似せた不正アプリのダウンロードサイトを用意する。実在の組織やアプリの更新を騙り、SMS や偽警告等からダウンロードサイトに誘導し、直接インストールさせる。

◆ 公式マーケットに不正アプリを紛れ込ませる

不正アプリを正規のアプリと見せかけて公式マーケットに公開する。利用者は正規のアプリだと思い込み、安易にインストールしてしまう。

◆ アプリの更新で不正アプリに変化する

インストール時は悪意ある機能が顕在化していないが、アプリの更新により顕在化し、不正アプリに変化する。

＜不正アプリによるスマートフォンの悪用例＞

- 連絡先等の端末内の重要な情報を窃取
- DDosS 攻撃（ウェブサーバー等に負荷をかける攻撃）や不正な SMS の拡散等の踏み台
- 録画・写真・通話録音機能を不正に利用
- 暗号資産（仮想通貨）のマイニングに利用

＜事例または傾向＞

◆ **通信事業者を騙った SMS から不正アプリのダウンロードサイトに誘導**

日本サイバー犯罪対策センター（JC3）によると、通信事業者になりすました SMS が届き、本文に記載した URL（偽のサイト）にアクセスさせられ、不正アプリをインストールさせられる手口が確認されている。

Android 端末の場合はアクセスした偽のサイトから不正アプリ（*.apk）のインストールへ誘導する手口、iPhone の場合は偽サイトから各種設定を管理する構成プロファイルをダウンロードさせて、不正アプリをインストールさせる手口が確認されている。インストールした不正アプリで認証情報を入力すると、攻撃者にその情報が詐取される。[1]

◆ **偽のワクチン接種予約案内に注意**

2021 年 5 月、トレンドマイクロは、新型コロナウイルスのワクチン接種予約を装う偽の SMS について注意喚起を行った。Android 端末で、SMS に記載された不正な URL にアクセスすると、Chrome のアップデートを装った不正アプリのインストールが促される。インストールしてしまうと、攻撃者が被害者のスマートフォンを介し、不特定多数に対して偽装 SMS を送り付け、不正サイトに誘導する。[2]

◆ **トロイの木馬が仕込まれたゲームアプリからの情報窃取**

セキュリティベンダ Dr.Web によれば Android 端末のゲームアプリ 190 種にトロイの木馬（Cynos プログラムモジュールの亜種）が仕込まれており、930 万以上のスマートフォンにインストールされている可能性が指摘されている。インストールすると携帯電話番号やモバイルネットワークパラメータ等を利用者に無断で収集し、リモートサーバーに送信する。該当するゲームは既にアプリストアから削除されている。[3]

＜対策/対応＞

個人（スマートフォン利用者）

- 被害の予防

・表 1.3「情報セキュリティ対策の基本」を実施

・アプリは公式マーケットから入手

スマートフォンの設定によっては公式マーケット以外からもアプリを入手可能だが、極力公式マーケットから入手する。ただし、公式マーケットにも不正アプリが紛れていることがあるため、レビューの評価に加え、アプリ開発者やアプリのバージョンアップ履歴等の情報を確認し、信頼できるアプリかどうかを判断する。

・アプリインストール時のアクセス権限の確認

アプリのインストール時にアクセス許可が要求された権限について、アプリの機能に対して適切かどうか確認を行う。特にデバイス管理者になる権限を要求している場合は注意が必要である。

・アプリインストールに関する設定に注意

-Android 端末の設定で、提供元不明のアプリのインストールを許可しない。

-iPhone の設定で、「信頼されていないエンタープライズデベロッパ」の表示がされるアプリを信頼しない。

・不要なアプリをインストールしない

不正アプリに限らず、正規のアプリであっても使い方を誤れば意図せず重要な情報を公開してしまうこともある。アプリの機能を理解し不要なアプリをインストールしない等の適切な利用を心がける。

・利用しないアプリはアンインストールする

- 被害を受けた後の対応

・不正アプリのアンインストール

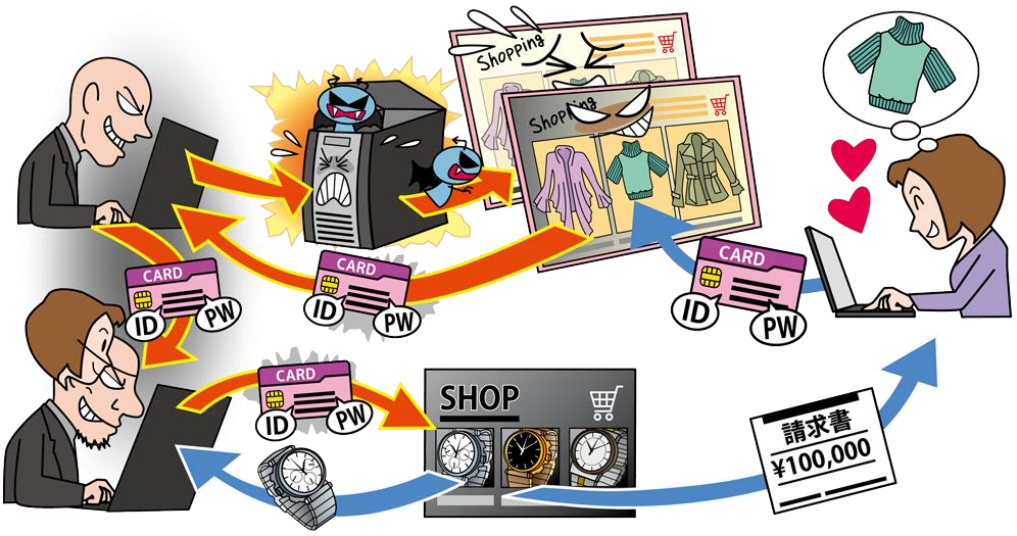
不正アプリをアンインストールする。できない場合は端末を初期化する。

参考資料

1. 通信事業者を装ったフィッシング（（一財）日本サイバー犯罪対策センター）
https://www.jc3.or.jp/threats/examples/article-409.html
2. 【注意喚起】偽のワクチン接種予約案内に注意（トレンドマイクロ株式会社）
https://www.is702.jp/news/3864/
3. トロイの木馬仕込まれたゲームアプリ、Androidユーザー 930万人がダウンロード（株式会社マイナビ）
https://news.mynavi.jp/article/20211125-2198828/

8位 インターネット上のサービスからの個人情報の窃取

～頻発する個人情報の漏えい、利用者もできる限りの対策を～



ショッピングサイト（EC サイト）等、インターネット上のサービスへの不正アクセスや不正ログインが行われ、サービスに登録している個人情報等の重要な情報を窃取される被害が継続して発生している。サービスの利用者は、窃取された情報を悪用されることにより、詐欺メールが送られてきたり、クレジットカードを不正利用されたりといった被害を受けるおそれがある。

＜攻撃者＞

- 組織的犯行グループ

＜被害者＞

- 個人（サービス利用者）
- 組織（サービス利用者）

＜脅威と影響＞

昨今、多くの企業や組織がインターネット上に様々なサービスを提供している。利用者はそのサービスを利用するために会員登録を行い、個人情報等の重要な情報（氏名、性別、生年月日、メールアドレス、クレジットカード情報等）を登録している。一方、サービスを提供している組織が、サービスを構成しているソフトウェアの脆弱性対策や、適切なセキュリティ対策が不十分なままサービスを提供している場合がある。また、利用者においてもログインに利用する ID、パスワード等の認証情報を複数のサービスで使い回している場合がある。攻撃者は、ソフトウェアの脆弱性や他サービスで漏えいした認証情報を悪用して不正アクセスや不正ログインをすることで、サービスに登録されている重要な情報を窃取する。

重要な情報を窃取されると、クレジットカードを不正利用されたり、詐欺メールを送信されたり、窃取された情報を一般的な検索エンジンでは検出されない闇サイト（ダークウェブ）で売買される等、さらなる被害につながるおそれがある。

＜攻撃手口＞

◆ サービスの脆弱性や設定不備を悪用

攻撃者は、適切なセキュリティ対策が行われていないショッピングサイト等に対して、脆弱性や設定不備を悪用して、ウェブサイト内の個人情報等の重要情報を窃取する。

また、攻撃者はウェブサイトの脆弱性を悪用してウェブサイトを改ざんする場合もある。サービスの利用者が改ざんに気づかず情報を入力してしまうと、その情報は攻撃者に窃取される。

◆ 他のサービス等から窃取した認証情報を悪用

他のサービスから窃取した認証情報（ID とパスワード）を悪用してサービスへ不正ログインし、個人情報等の重要な情報を窃取する。詳細は個人

10 位「インターネット上のサービスへの不正ログイン」を参照。

＜事例または傾向＞

◆　クラウドサーバーへの不正アクセス

2021 年 5 月、ネットマーケティングが運営するマッチングアプリ「Omiai」の利用者の年齢確認書類（運転免許証、健康保険証、パスポート、マイナンバーカード等）の画像 171 万 1,756 件が流出したことが公表された。画像が保存されていたクラウドサーバーにアクセスするための情報を不正に取得した第三者によって、正規のアクセスを装って不正アクセスが行われていた。同社が、サービス退会後も 10 年間会員情報を保持する運用としていたことも被害の大きさにつながったとされている。[1,2]

◆　改ざんされた EC サイトからの情報流出

2021 年 7 月、読売情報開発大阪が運営する EC サイト「よみファネット」において不正アクセスがあり、1,301 人分のクレジットカード情報が流出したと公表された。そのうち 58 人分のクレジットカードが不正利用され、被害総額は 767 万 4,605 円となった。不正アクセスによって決済処理プログラムの改ざんが行われており、2020 年 10 月 24 日から 2021 年 3 月 2 日の間に同サイトで入力されたクレジットカード情報が窃取された。[3]

◆　SQL インジェクション攻撃による被害

2021 年 9 月、翻訳ソフト等の開発、販売を行っているロゴヴィスタが、サーバーに不正アクセスを受け、登録ユーザーのメールアドレス約 12 万 8,000 件が流出したことを公表した。利用者から迷惑メールが届くようになったとの連絡を受けて調査をしたところ発覚したもので、サーバーの脆弱性を悪用してデータベースを不正に操作する SQL インジェクション攻撃を受けていたことが判明した。[4]

＜対策/対応＞

個人（インターネット利用者）

- 被害の予防
  - ・サービス利用の必要性を判断する
  - ・不要な情報は安易に登録しない

    情報漏えいに備えて、サービスを利用するための必須項目以外の情報は登録を避ける。
  - ・多要素認証の設定を有効にする
  - ・利用していないサービスからの退会
  - ・不正ログイン対策を実施する [5]
- 被害の早期検知
  - ・クレジットカード利用明細の定期的な確認

    クレジットカード情報が窃取され、不正利用された場合、被害に気づける可能性がある。
- 被害を受けた後の対応
  - ・サービス運営者（コールセンター等）へ連絡
  - ・クレジットカードの停止

    クレジットカード会社へ不正利用の連絡と停止の手続きを行う。
  - ・パスワードを変更する（他のサービスで同じパスワードを使っていた場合は同様に対応）

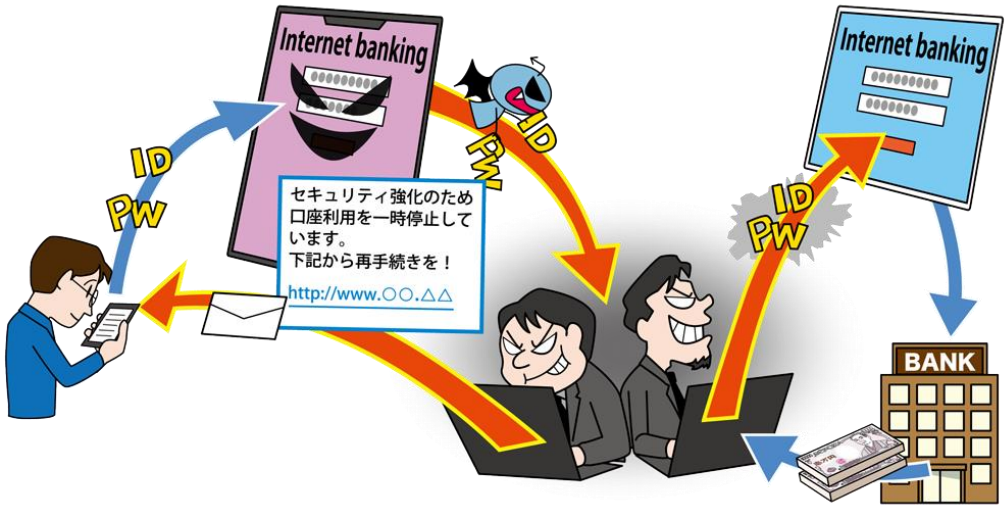
    サービスを継続して利用する場合はパスワードを変更する。
  - ・警察への被害届の提出

参考資料

1. 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（株式会社ネットマーケティング）
https://www.net-marketing.co.jp/news/6001/
2. Omiaiの「個人情報流出」が深刻化した根本原因（東洋経済ONLINE）
https://toyokeizai.net/articles/-/431661
3. 読売新聞子会社でクレカ情報流出　すでに767万円の金銭的被害も確認（ITmedia NEWS）
https://www.itmedia.co.jp/news/articles/2107/14/news116.html
4. 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（ロゴヴィスタ株式会社）
https://www.logovista.co.jp/lverp/information/information/emergency.html
5. 不正ログイン対策特集ページ（IPA）
https://www.ipa.go.jp/security/anshin/account_security.html

9位 インターネットバンキングの不正利用

～金融機関から SMS が送られてきても、ひとまず落ち着こう～



フィッシング詐欺やウイルス感染により、インターネットバンキングの認証情報を窃取されることで、被害者のアカウントから不正な送金が行われたり、不正にサービスを利用されたりする等の被害が確認されている。2021 年もスミッシング（SMS を用いたフィッシング）をきっかけに不正送金される事件が発生している。

＜攻撃者＞

- 組織的犯行グループ
- 犯罪者

＜被害者＞

- 個人（インターネットバンキング利用者）
- 組織（インターネットバンキング利用者）
- 組織（金融機関）

＜脅威と影響＞

実在する金融機関等を装ったメールや SMS からフィッシングサイト（偽のウェブサイト）へと誘導され、偽物であると気付かずに入力してしまい、攻撃者に認証情報を詐取（フィッシング詐欺）される。また、メールに添付された悪意あるファイルを開いて、端末をウイルスに感染させてしまい、攻撃者に認証情報を窃取される等の被害も発生している。

攻撃者に認証情報を窃取された場合、被害者が持つインターネットバンキングアカウントに不正ログインされ、攻撃者が作成した別の口座に不正送金されたり、インターネットバンキング上のサービスを不正利用されたり等の被害に遭うおそれがある。

＜攻撃手口＞

以下の手口でインターネットバンキングの認証情報を入手し、不正送金を行う。

◆ フィッシング詐欺

偽のメールや SMS を被害者に送信し、フィッシングサイトに誘導して、インターネットバンキングの認証情報を入力させ詐取する。また、多要素認証で使う情報（ワンタイムパスワード等）を入力させる場合もある。詳細は、個人 1 位「フィッシングによる個人情報等の詐取」を参照。

◆ ウイルス感染

ウイルスに感染させるように細工したファイルをメールに添付し、巧妙な文面で被害者にファイルを開くよう誘導して、被害者の端末をウイルスに感染させる。また、改ざんされた正規のウェブサイトを被害者に閲覧させることで、ウイルスに感染させる手口も確認されている。ウイルスに感染した端末でインターネットバンキングにログインしようとすると、偽のログインページが表示され、そこに入力した認証情報が攻撃者に送信される。

＜事例または傾向＞

◆　件数は半減、1 件当たりの被害額は増加

警察庁によると、2021 年 1 月から 6 月のインターネットバンキングに関わる不正送金事犯の発生件数は 376 件、被害額は約 4 億 7,900 万円であった。前年同期の 888 件、約 5 億 4,200 万円に比べて、発生件数は半分以下に減少したが、被害額はやや減少に留まり、1 件あたりの被害額は増加している。被害額の約 87%にあたる約 4 億 1,700 万円は個人口座からの不正送金であり、依然として個人の被害が多い状況が続いている。

手口の多くは以前からある SMS やメールを利用したフィッシングと考えられており、メモアプリ等に不正アクセスされ、インターネット上に保存してあった ID やパスワードを用いてインターネットバンキングから不正送金されたと思われるケースも確認されている。[1]

◆　メモアプリ利用時の注意点

警察庁がメモアプリ等に保存したインターネットバンキングの認証情報を悪用した不正アクセスの手口を公表したことから、2021 年 12 月、日本サイバー犯罪対策センター（JC3）はメモアプリ利用に関する注意喚起を行った。この注意喚起の中で JC3 は、メモアプリのフィッシングサイトを確認しており、メールや SMS からメモアプリのインターネットサービス（ログイン画面）へ促されても安易にアクセスしないよう注意を呼び掛けている。[2]

◆　幹部ら 3 人逮捕、被害 130 人 9,300 万円

2021 年 11 月、沖縄県警サイバー犯罪対策課等 9 県警合同捜査本部は、インターネットバンキングに不正アクセスし、17 都府県の約 130 人から総額約 9,300 万円を窃取した事件で、犯行の首謀者ら 3 人を「不正アクセス禁止法違反」、「電子計算機使用詐欺」、「窃盗」の容疑で逮捕した。

被害者のスマートフォン等にメガバンクを装った SMS を送り、口座番号やパスワードを入力させるスミッシングが用いられ、メガバンクにある被害者の口座から県内銀行の口座に不正送金され引き出されていた。[3]

＜対策/対応＞

個人（インターネットバンキング利用者）

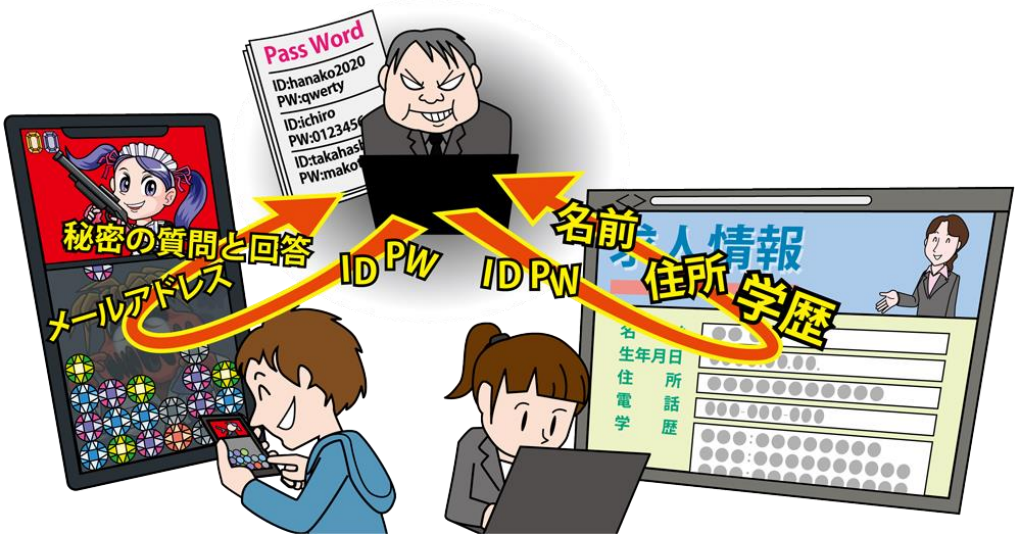
- 被害の予防（被害に備えた対策含む）
  - ・受信メールやウェブサイトの十分な確認
  - ・添付ファイルや URL を安易にクリックしない
    よく利用するウェブサイトは、予めブックマークに登録し、メール等のリンクではなくそこからアクセスする。
  - ・PC 等でファイルの拡張子表示設定をする
    不審なファイルに気づきやすくする。
  - ・普段は表示されないポップアップ画面に個人情報を入力しない
  - ・金融機関や公的機関から公開される注意喚起を確認する
  - ・多要素認証の設定を有効にする
  - ・口座連携済みサービスを確認する
  - ・認証に不備がある銀行口座を利用停止する
    暗証番号のみ等、脆弱（ぜい）な認証で利用可能な銀行口座については、必要がなければインターネット取引の利用を停止しておく。
- 被害の早期検知
  - ・不審なログイン履歴の確認
  - ・口座の利用履歴の確認
  - ・サービス利用状況の通知機能の利用
- 被害を受けた後の対応
  - ・当該サービスのコールセンターへの連絡
    金融機関によっては、全額または一部補償してくれる場合がある。
  - ・警察への被害届の提出
  - ・ウイルス感染した端末の初期化
  - ・パスワードを変更する（他のサービスで同じパスワードを使っていた場合は同様に対応）

参考資料

1. 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（警察庁）
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R03_kami_cyber_jousei.pdf
2. メモアプリ利用時の注意点（（一財）日本サイバー犯罪対策センター）
https://www.jc3.or.jp/threats/topics/article-414.html
3. 旭琉会幹部ら3人逮捕　ネットバンク不正容疑、被害130人9300万円　沖縄県警など（琉球新報）
https://ryukyushimpo.jp/news/entry-1422467.html

10位 インターネット上のサービスへの不正ログイン

～パスワードの使い回しに注意、あなたの個人情報が閲覧されるかも～



インターネット上のサービスへ不正ログインされ、個人情報や金銭等の重要情報が窃取される被害が確認されている。別のサービスと同じ ID やパスワード使い回す利用者を狙ったパスワードリスト攻撃による不正ログインが行われている。また、不正ログインで得た情報を悪用して更に被害を拡大させるおそれがある。

＜攻撃者＞

- 組織的犯行グループ
- 犯罪者（愉快犯、ストーカー等）

＜被害者＞

- 個人（サービス利用者）
- 組織（サービス運営者）

＜脅威と影響＞

不正に入手した ID やパスワードを使い、インターネット上のサービスに対して不正ログインを行う攻撃が行われている。使用される ID やパスワードは、別のサービスから漏えいしたものを使う以外にも、被害者が使いそうなものを類推する手口もある。

不正ログインされると、サービスに応じた被害を受ける。ショッピングサイトであれば、氏名、住所、電話番号やサイトに登録しているクレジットカード情報等を窃取されたり、商品の不正購入やサイト内のポイントを盗用されたりする。また、スマートフォンを利用したキャッシュレスの決済サービスであれば、チャージした残高を不正に利用される。さらに、LINE 等の SNS（ソーシャル・ネットワーキング・サービス）であれば、プライベートな写真やメッセージのやり取り等を覗き見されたり、偽の投稿（フィッシング詐欺等）をされたりする。

＜攻撃手口＞

◆ パスワードリスト攻撃

攻撃者が一般的な検索エンジンでは検出されない闇サイト（ダークウェブ）で購入する等何らかの不正な方法で事前に入手した ID とパスワードのリストを使用し、自動的に入力するプログラム等を用いて、ログイン機能を持つインターネット上のサービスにログインを試みる。複数のサービスで ID とパスワードを使い回していると、それら全てのサービスでログインされるおそれがある。

◆ パスワード類推攻撃

使われやすいパスワードを類推し、そのパスワードでログインを試みる。例えば、芸能人や知人の個人情報（氏名、誕生日等）からパスワードを類推して、ログインを試みる。

◆ ウイルス感染

攻撃者の用意した悪意あるウェブサイトにアクセスさせたり、メールに添付されている悪意あるファイルを開かせたりすることで、利用者の端末をウイ

ルスに感染させる。利用者がその端末でインターネット上のサービスにログインすると、入力した ID やパスワードを攻撃者に窃取され、不正ログインに使われる。

＜事例または傾向＞

◆ **転職情報サイトに不正ログインされ、履歴書を閲覧**

2021 年 2 月、マイナビが運営する転職情報サイト「マイナビ転職」において、外部で不正に取得されたと思われるパスワードを使い、不正ログインされる被害が確認された。同サイトに登録したユーザーのうち 21 万 2,816 人のアカウントが不正ログインされ、ユーザーの Web 履歴書にアクセスされた。被害拡大防止策として全ユーザーのパスワードをリセットし、パスワードの再設定を依頼した。[1]

◆ **パスワードを推測し、SNS に不正グイン**

2020 年から 2021 年にかけて自身のスマートフォンを使い、女子大学生の SNS アカウントへ 4 回の不正アクセスした疑いおよび女性タレントの SNS アカウントのログイン ID やパスワードをインターネット上で保管した疑いで、2022 年 1 月に男が逮捕された。

被害者は、名前や生年月日にちなんだパスワードを設定しており、男はアカウント名やプロフィールの情報を組み合わせてパスワードを類推していた。[2]

◆ **モバイル向けゲームの会員サービスに不正ログイン**

2021 年 10 月、モバイル向けゲームを提供する KLab の会員サービス「KLab ID」において、パスワードリスト型攻撃により、不正ログインされる被害が確認された。不正ログインされたユーザーは 2,846 件で、メールアドレス、ひみつの質問と回答、生年月日等、当該サービスと連携したアプリで閲覧できる全ての情報が閲覧されたおそれがある。同社は、全ユーザーのアカウントに対して二段階認証を必須とする対応を行った。[3]

＜対策/対応＞

個人（ウェブサービス利用者）

- 被害の予防
  - ・表 1.3「情報セキュリティ対策の基本」を実施
  - ・添付ファイルや URL を安易にクリックしない
  - ・パスワードは長く、複雑にする [4,5]

    ID にメールアドレスを用いている場合は、他のサービスでも不正ログインされやすくなるため特に注意する。
  - ・パスワードを使い回さない
  - ・パスワード管理ソフトの利用
  - ・サービスが推奨する認証方式の利用

    多要素認証や多段階認証の設定を有効にする。[4]
  - ・不審なウェブサイトで安易に認証情報を入力しない（フィッシングに注意）
  - ・利用していないサービスからの退会
- 被害の早期検知
  - ・利用しているサービスのログイン履歴の確認
  - ・クレジットカードやポイント等の利用履歴の定期的な確認
- 被害を受けた後の対応
  - ・パスワードを変更する（他のサービスで同じパスワードを使っていた場合は同様に対応）
  - ・クレジットカードの停止
  - ・サービス運営者（コールセンター等）へ連絡
  - ・警察への被害届の提出

参考資料

1. 「マイナビ転職」への不正ログイン発生に関するお詫びとお願い（株式会社マイナビ）
https://www.mynavi.jp/topics/post_29797.html
2. 女子大生・タレントのSNSに不正アクセス…男「プライベートのぞきたくて」（読売新聞オンライン）
https://www.yomiuri.co.jp/national/20220107-OYT1T50005/
3. KLab ID への不正ログインに関するお知らせ（KLab株式会社）
https://www.klab.com/jp/press/info/2021/1027/klab_id_2.html
4. 不正ログイン対策特集ページ（IPA）
https://www.ipa.go.jp/security/anshin/account_security.html
5. 不正ログイン被害の原因となるパスワードの使い回しはNG（IPA）
https://www.ipa.go.jp/security/anshin/mgdayori20160803.html

コラム:あなたが知った情報は真実ですか？ディスインフォメーションに注意を！！

あなたがいつものようにSNSをチェックしていると、支持している政党Aの政治家Bの名前を見つけました。それは「政治家Bが海外視察中に地元民に差別・暴言！」というニュースでした。あなたは、このときどう思い、どう行動しますか？

・ずっと支持していたのに裏切られた！と政治家Bに憤りを感じる？
・そんなことあるのかなぁ？本当かなぁ？と、ひとまず疑ってみる？
・よく分からないから友達にニュースを教えてみる？

でも、そのニュースに類似した記事が他の情報元からも複数発信されていたら・・・。ニュースを疑っていた人でもニュースを信じてしまうかもしれません。そして、政治家Bに対する不信感や嫌悪感が沸き上がり、所属する政党Aに対する不信感にまで膨らんでいったとしても不思議ではありません。

近々、大事な選挙があるとしたら、あなたは誰に投票しますか？
支持政党がなくなったから投票するのをやめますか？でも、せっかくの一票を放棄するのはもったいない話です。どうせ投票するなら、不信感がある政党Aの候補者ではなく、クリーンなイメージの政党Cの候補者にしよう！と言う流れになることも考えられます。

選挙の後、政治家Bの暴言は事実無根だったという新たなニュースが発信され、先日のニュース記事を全面否定したら、あなたはどう感じますか？

ここで少し考えてみましょう。
・ニュースは、一部がウソだったのでしょうか？全部がウソだったのでしょうか？
・ニュースを目にしたあなたの判断や行動は正しかったのでしょうか？
・選挙の結果、政党Cが与党となったら、発信されていたニュースは誰にとってプラスで、誰にとってマイナスだったのでしょうか？

さて、世の中には様々な情報が溢れています。大きく4つに分類されると言われています。[1,2]
(1) 真実の情報(information)
(2) 単純に間違っている偽情報(misinformation)
(3) 誤解させる意図がある偽情報(disinformation)
(4) 誤解させる意図がある真実の情報(ミスリードを促すために真実の一部だけを恣意的に切り取った情報)(malinformation)

特に、(2)、(3)は日本では「フェイクニュース(fake news)」と呼ばれることもあります。(2)、(3)は共に「偽情報」ですが、(3)にはある種の意図が込められており、(2)とは異なる危険性があります。海外では、読み分けて(3)の情報を「ディスインフォメーション(disinformation)」と呼んでいます。

それでは、ディスインフォメーションは何が危険なのでしょうか。その情報には、個人、社会集団、組織、または国を誤解させたり、危害を加えたり、操作したりする意図があることです。例えば、その情報により特定の人を貶めたり、それを見た人の不安を煽ったり、それを見た人を何かに誘導したり等、発信者の様々な目的を達成する意図があります。その情報を見た人の中には信じてしまう人もいるし、信じない人もいるでしょう。しかし、SNS の世界的な普及により、1 回の情報発信で世界中に情報を拡散することができるようになっています。そして、その情報を信じた人が元の情報を引用してさらに発信することで次々と広がっていきます。

また、ディスインフォメーションによる情報操作目的のサイバー攻撃が組織的に行われると、複数の情報元からディスインフォメーションを発信することも不可能ではないため、信憑性が増します。その結果、多くの人がその情報を信じてしまうおそれがあります。なお、2021 年には、外部のプレスリリース配信サイトに他組織を騙って第三者がプレスリリースを掲載されたという事例がありました。[3] あくまで一事例ではありますが、自由に複数の情報元から情報を発信することは容易ではないにしろ可能であるということが見て取れます。

続いて、海外の事例では、以下のディスインフォメーション（一部、malinformation と併用されている可能性あり）によるものとされる国の運営や政治等に対する組織的な情報操作の疑いがありました。

・2016 年アメリカ合衆国大統領選挙

2016 年のアメリカ合衆国大統領選挙では、共和党のドナルド・J・トランプ氏と民主党のヒラリー・クリントン氏が一騎打ちを行い、最終的にトランプ氏が大統領となりました。一方、その選挙の中で、クリントン氏および民主党を標的にした虚偽の情報がSNSを通じてインターネット上に拡散されました。例えば、Facebook上で「クリントン氏が『イスラム国』（ISIS）に武器を販売した」という発信、Twitterに「民主党の上級関係者が人身売買に関わっている」という発信等がされました。発信された偽情報は多くのアメリカ国民に閲覧され、その後の大統領選挙に影響があったとされています。[4,5]

・2016 年イギリスの EU 離脱の是非を問う国民投票

2016 年のイギリスにおいて、EU（欧州連合）離脱の是非を問う国民投票が行われ、最終的にイギリスは EU から離脱することになりました。一方、その投票前に、EU からの離脱を煽るような偽情報が発信されました。離脱派の当時の党首が EU への拠出額が毎週 3 億 5,000 万ポンドかかると主張し、その情報が SNS 上で拡散されました。その情報は偽情報で、実際の拠出額は週 1 億数千万ポンドであり、投票後、当該党首は発言が誤りであったことを認めています。この偽情報が、EU 離脱の国民投票の結果に影響があったとされています。[6,7]

世の中に様々な情報が発信されている中で、読み手はその情報が真実の情報か偽の情報かを見抜く必要があります。例えば、最初の発信元の情報（一次ソース）を確認したり、発信元は信頼できるかを確認したり、別の情報元ではどのような発信をしているかを確認します。そして、聞いたことがない情報元や 1 つの情報元でしか発信されていない、もしくは、別の情報元では内容が異なっている場

合はその情報の取り扱いには注意すると良いでしょう。また、発信された情報はあくまでその時点での情報であり、時間経過に伴い内容が変わる可能性もあるため、最新の情報を確認することも大切です。なお、主義主張、戦争等の対立関係があるデリケートな情報の場合、当事者だけではなく読み手も何らかのバイアス（偏向、先入観、思い込み等）がかかる場合があることを認識し、客観的に情報を取り扱いましょう。

とは言え、情報操作目的で組織的なサイバー攻撃を使って偽情報が発信された場合、それを完全に見抜くことは難しいものです。そのような情報には、真実と偽りが巧妙に織り込まれています。ネットで見つけた興味を引く情報や SNS で受け取った重要そうな情報は、無闇に他人に拡散せず少し立ち止まって考えたり、情報の真偽について家族、友人等の信頼できる人に相談したりすると良いでしょう。また、情報の真偽検証を行うファクトチェックの考え方も参考になると考えます。[8]

一方、ディスインフォメーションに対して、国や組織として取り組みも行われています。例えば、総務省では、「プラットフォームサービスに関する研究会」の中でフェイクニュースや偽情報への対応の在り方について議論され、一般社団法人セーファーインターネット協会では、ディスインフォメーションの流通の実態を正確に把握し、その対応について多面的に検討する「Disinformation 対策フォーラム」が立ち上げられています。[9,10]また、Twitter 社では、誤解を招く情報が含まれていると思われるツイートに対してアクションが取れる機能をテストしています。[11] ディスインフォメーションに対して、個人だけの対応ではなく、国や組織としても取り組み、一丸となって対策を行うことが重要と考えます。

冒頭に仮の選挙のお話をしましたが、あなたの判断が国の運営を変えてしまう可能性もあります。ディスインフォメーションによる情報操作により、あなたや家族・友人、国や組織が振り回されてしまうのは相手の思う壺であり、発信者以外得になりません。身近な人を守るため、情報が溢れる昨今、受け取った情報に対する適切な理解と対応が求められています。

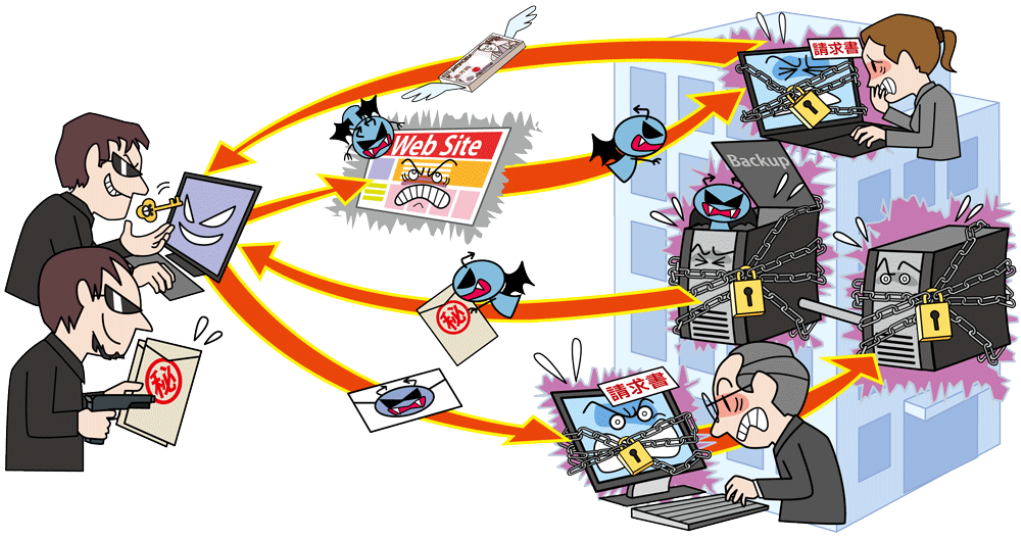
参考資料

1. 判別 AI も出てきた米国・フェイクニュース研究最前線 ── ただ「フェイク」と呼ぶ時代は終わる
https://www.businessinsider.jp/post-183518
2. MIS, DIS, MALINFORMATION
https://www.cisa.gov/mdm
3. 偽プレスリリースに「認知作戦」の影　サイバー情報戦の謎に迫った
https://www.asahi.com/articles/ASQ2P52RJQ2GUTIL035.html
4. This Analysis Shows How Viral Fake Election News Stories Outperformed Real News On Facebook
https://www.buzzfeednews.com/article/craigsilverman/viral-fake-election-news-outperformed-real-news-on-facebook
5. 米民主党の「ピザゲート」？　偽ニュースや陰謀論の生まれ方
https://www.bbc.com/japanese/features-and-analysis-38179131
6. ジョンソン前外相に出廷命令　EU拠出金巡る虚偽発言を受け
https://europe.nna.jp/news/show/1908727
7. 離脱派に広がる「後悔」「Regrexit」の造語も登場　軽い気持ちで投票…やり直したいとも
https://www.sankei.com/article/20160628-S7ABOLPYKFIPXPAX3GVRPBH4JY/
8. ファクトチェックとは - 基本的な考え方
https://fij.info/introduction/basic/
9. プラットフォームサービスに関する研究会における最終報告書（案）に対する意見募集の結果及び最終報告書の公表
https://www.soumu.go.jp/menu_news/s-news/01kiban18_01000075.html
10. Disinformation 対策フォーラム中間とりまとめ
https://www.saferinternet.or.jp/anti-disinformation/disinformation_interim_report/
11. Twitter の Birdwatch について
https://help.twitter.com/ja/using-twitter/birdwatch

2. 情報セキュリティ 10 大脅威（組織）

1位 ランサムウェアによる被害

～社会インフラに大きな影響が出る場合も～



ランサムウェア [1] とはウイルスの一種である。PC やサーバーが感染すると、端末のロックや、データの暗号化が行われ、その復旧と引き換えに金銭を要求される。また、重要な情報が窃取されることもあり、社会的信用を失うおそれがある。さらに、復旧に時間が掛かる場合、更なる経済的損失につながるおそれもある。

＜攻撃者＞

- 組織的犯行グループ
- 犯罪者

＜被害者＞

- 個人
- 組織

＜脅威と影響＞

PC やサーバーのデータを暗号化し、データを復旧することと引き換えに、金銭を要求する等の脅迫文を画面に表示するランサムウェアと呼ばれるウイルスの被害が確認されている。暗号化前に重要情報を窃取し、金銭を支払わなければ窃取した情報を公開すると脅迫する攻撃「二重の脅迫（double extortion）」も近年確認されている。脅迫に従うことによる金銭的被害に加え、窃取された重要情報（組織の機密情報や個人情報等）の漏えいにより信用の失墜にもつながるおそれがある。

なお、金銭を支払ったとしても、データの復旧や漏えいした情報の削除が行われるとは限らない。

＜攻撃手口＞

◆ メールから感染させる

メールの添付ファイルやメール本文中のリンクを開かせることでランサムウェアに感染させる。

◆ ウェブサイトから感染させる

脆弱（ぜい）性等を悪用しランサムウェアをダウンロードさせるよう改ざんしたウェブサイトや攻撃者が用意したウェブサイトを閲覧させることで感染させる。

◆ 脆弱性によりネットワーク経由で感染させる

ソフトウェアの脆弱性を未対策のままインターネットに接続されている機器に対して、その脆弱性を悪用してインターネット経由で感染させる。

◆ 公開サーバーに不正アクセスして感染させる

外部公開しているサーバーにリモートデスクトップ等で不正ログインしランサムウェアに感染させる。

＜事例または傾向＞

◆ バックアップの暗号化による被害の長期化

2021 年 7 月、製粉会社のニップンがサイバー攻撃を受け、大部分のサーバーや一部端末が同時多発的に暗号化される被害を受けた。暗号化されたシステムにはグループ会社も利用している基幹システ

ムも含まれ、システムのオンラインバックアップを管理するサーバーについても暗号化されたことで早期復旧が困難になり、その結果、四半期決算報告書の提出を延期することとなった。[2]

◆ **病院へのランサムウェア攻撃**

2021 年 10 月、徳島県の半田病院がランサムウェアの感染によって、約 8 万 5,000 人分の電子カルテや会計システムにアクセスできなくなる被害を受けた。同病院は身代金を支払わずにシステムの再構築を行い、復旧までの約 2 ヶ月間、一部の診療科で新規患者の受け入れを中止する等の影響があったが、2022 年 1 月、通常診療を再開した。[3]

◆ **社会インフラ関連企業における被害**

2021 年 5 月、アメリカ最大の石油パイプラインであるコロニアル・パイプラインが、ランサムウェアの被害を受けて 5 日間の操業停止に追い込まれ、ガソリン不足を心配した市民がガソリンを買いだめし、売り切れや価格高騰といった大きな影響が出た。DarkSide という犯罪グループによる犯行で、脆弱な設定の VPN 経由での不正アクセスによってランサムウェアに感染させていた。データの暗号化の他にデータの窃取もされており、二重の脅迫を受けた同社は身代金 440 万ドルを暗号資産（ビットコイン）で支払い、システムを復旧させた。なお、6 月に FBI は身代金の大部分を回収したと報じた。[4]

＜対策/対応＞

組織（経営者層）

- 組織としてのランサムウェア対応体制の確立
  - ・対策の予算の確保と継続的な対策の実施
  - ・CIO など専門知識を持つ責任者を配置

組織（システム管理者、従業員）

- 被害の予防
  - ・迅速、継続的に対応できる体制（CSIRT 等）の構築
  - ・表 1.3「情報セキュリティ対策の基本」を実施
  - ・多要素認証の設定を有効にする
  - ・添付ファイルやリンクを安易にクリックしない
  - ・提供元が不明なソフトウェアを実行しない
  - ・機器の脆弱性対策を迅速に行う
    パッチ適用を迅速に行い、サポート切れの OS は利用停止し、リスクを最小化する。
  - ・セキュリティ対策ツールの利用や設定見直し
    アプリケーション実行制限や、メールおよびウェブのフィルタリングを行う。ポリシー設定を見直し、遮断設定を極力有効にする。
  - ・ネットワーク分離
  - ・共有サーバー等へのアクセス権の最小化と管理の強化
  - ・公開サーバーへの不正アクセス対策
  - ・バックアップの取得 [5]
    取得だけでなくバックアップから復旧できることを定期的に確認する。
- 被害を受けた後の対応
  - ・組織の方針に従い各所へ報告、相談する
    上司、CSIRT、関係組織、公的機関等
  - ・バックアップからの復旧
  - ・復号ツールの活用 [6]
  - ・影響調査および原因の追究、対策の強化
  - ・迅速な隔離を行い、関連組織、取引先への被害拡大の防止

＜例外ケース＞

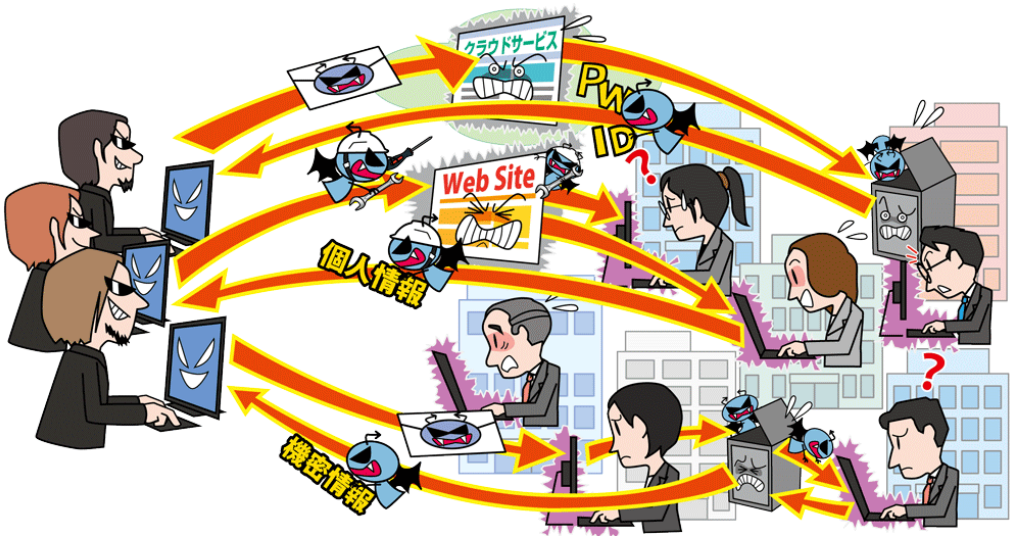
過去には、組織の事情により、金銭を支払ったケースもあった。

参考資料

1. ストップ！ ランサムウェア ランサムウェア特設ページ（内閣サイバーセキュリティセンター）
https://security-portal.nisc.go.jp/stopransomware/
2. 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（株式会社ニップン）
https://www.nippn.co.jp/topics/detail/__icsFiles/afieldfile/2021/08/16/20210816-1.pdf
3. サイバー攻撃受けた徳島・半田病院 約2カ月ぶりに通常診療全面再開（朝日新聞DIGITAL）
https://www.asahi.com/articles/ASQ145J9MQ13PTLC00P.html
4. ランサムウエア攻撃で石油パイプラインが停止、犯罪組織DarkSideの手口を検証（日経クロステック）
https://active.nikkeibp.co.jp/atcl/act/19/00324/100800001/
5. ランサムウエア対策に不可欠、バックアップの「3-2-1ルール」とは？（日経クロステック）
https://active.nikkeibp.co.jp/atcl/act/19/00282/041900001/
6. The No More Ransom Project（No More Ransomプロジェクト）
https://www.nomoreransom.org/

2位 標的型攻撃による機密情報の窃取

～組織化しているサイバー攻撃～



標的型攻撃とは、特定の組織（官公庁、民間団体、企業等）を狙う攻撃のことであり、機密情報等を窃取することや業務妨害を目的としている。攻撃者は社会の変化や、働き方の変化に便乗し、状況に応じた巧みな攻撃手法で機密情報等を窃取しようとする。

＜攻撃者＞

- 諜報員、産業スパイ
- 組織的犯行グループ
- 犯罪者

＜被害者＞

- 組織（官公庁、民間団体、企業、研究機関、教育機関等）

＜脅威と影響＞

特定の企業や民間団体、官公庁に狙いを定め、機密情報等の窃取を目的としたウイルスを PC に感染させることで、組織内部へ潜入する標的型攻撃が確認されている。攻撃者はウイルス感染させた PC を悪用し組織内部の侵害範囲を拡大しながら機密情報等の窃取を行う。

窃取された機密情報が悪用された場合、企業の事業継続や国家の安全保障等に重大な影響を及ぼすおそれがある。また、データ削除やシステム破壊により企業等の活動が妨害されたり、その企業のサプライチェーンに属する関連組織への攻撃の踏み台にされたりすることもあり、業種や組織の規模に関わらず狙われるおそれがある。

＜攻撃手口＞

◆ メールへのファイル添付やリンクの記載

メールの添付ファイルやリンク先にウイルスを仕込み、ファイルを開封させたり、リンクにアクセスさせたりすることで PC をウイルスに感染させる。メール本文や件名、添付ファイル名は業務や取引に関連するような内容に偽装され、実在する組織の差出人名が使われる場合もある。またメールのやり取りを複数回行い油断させる、不審を抱かれにくいようにする手口が使われる。（やり取り型攻撃）

◆ ウェブサイトの改ざん

標的となった組織が頻繁に利用するウェブサイトを調査し、そのウェブサイトを改ざんする。従業員が改ざんされたウェブサイトにアクセスするよう誘導され、そのウェブサイトにアクセスすることで PC がウイルスに感染する。（水飲み場型攻撃）

◆ 不正アクセス

標的の組織が利用するクラウドサービスやウェブサーバー、VPN などの脆弱性を悪用し、不正アクセスを行い、認証情報等を窃取する。その認証情報等を悪用し、正規の経路で組織のシステムへ侵入して、PC やサーバーをウイルスに感染させる。

＜事例または傾向＞

◆　**サイバー攻撃で企業情報と個人情報漏えい**

2021 年 12 月、「業務スーパー」を展開する神戸物産は、同社サーバーがサイバー攻撃を受け、個人情報や一部企業情報が外部に流出したことを明らかにした。発覚の経緯は、本社で利用するサーバーで共有ファイルが開けなくなり、メールが届かない不具合が発生したためとしている。その後、外部との通信を遮断し、システムの復旧を行った。[1]

◆　**情報共有ツールから受託情報が外部に流出**

2021 年 5 月、富士通が提供するプロジェクト情報共有ツール「ProjectWEB」が第三者から不正アクセスを受け、顧客から預かった情報の一部が窃取されたことが公表された。本ツールは、同社やグループ会社、外部の協力企業、顧客間のシステム開発等のプロジェクト管理（開発工程やソース、タスクの管理等）に用いられていた。[2]

◆　**サイバー攻撃に関する情報共有**

サイバー情報共有イニシアティブ（J-CSIP）によると 2021 年に受け付けた標的型攻撃メールとみなした情報提供は 36 件であった。また、7 月から 9 月の期間には、標的型攻撃かは判断できないが、情報提供元組織で繰り返し利用しているインターネット上の無償イラスト素材提供サイトからダウンロードした画像ファイルに URL リンクが関連付けられており、最終的に不正ファイルとしてセキュリティソフトが検知したという情報提供があった。[3]

＜対策/対応＞

組織（経営者層）

- 組織としての体制の確立
  - ・CSIRT の構築
  - ・対策予算の確保と継続的な対策の実施
  - ・セキュリティポリシーの策定

組織（セキュリティ担当者、システム管理者）

- 被害の予防／対応力の向上
  - ・情報の管理と運用ルール策定
    情報は暗号化する等、管理や運用のルールを定めて運用する。
  - ・サイバー攻撃に関する継続的な情報収集
  - ・従業員に対するセキュリティ教育の実施
  - ・インシデント対応の定期的な訓練を実施
    関係者やセキュリティ業者、専門家と迅速に連携できる対応方法や連絡方法を整備する。
  - ・管理端末への継続的セキュリティパッチ適用
  - ・統合運用管理ツール等によるセキュリティ対策状況の把握
    従業員や職員が利用する PC のソフトウェア更新状況を管理し、リスクの可視化を行う。
  - ・アプリケーション許可リストの整備
  - ・アクセス権の最小化と管理の強化
  - ・ネットワーク分離
  - ・重要サーバーの要塞化（アクセス制御、暗号化等）
  - ・取引先のセキュリティ対策実施状況の確認
  - ・海外拠点等も含めたセキュリティ対策の向上
- 攻撃の予兆／被害の早期検知
  - ・UTM、IDS/IPS、WAF、仮想パッチ等の導入
    導入後も対策情報（設定等）を定期的に更新する作業を想定し、予算や体制を確保する。
  - ・EDR 等を用いたエンドポイントの監視、防御
- 被害を受けた後の対応
  - ・CSIRT の運用によるインシデント対応
  - ・影響調査および原因の追究、対策の強化

組織（従業員、職員）

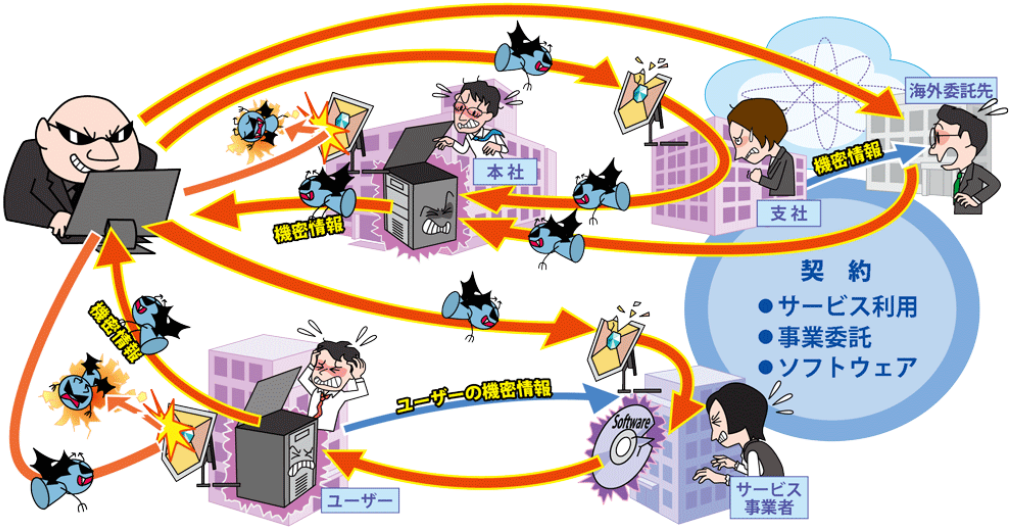
- 被害の予防（通常、組織全体で実施）
  - ・表 1.3「情報セキュリティ対策の基本」を実施
  - ・添付ファイルやリンクを安易にクリックしない
- 被害を受けた後の対応
  - ・組織の方針に従い各所へ報告、相談する
    上司、CSIRT、関係組織、公的機関等

参考資料

1. 神戸物産にサイバー攻撃、詳細を調査 - システムは2日後に復旧（Security NEXT）
https://www.security-next.com/132686/
2. 社内外で利用する「プロジェクト情報共有ツール」に不正アクセス - 富士通（Security NEXT）
https://www.security-next.com/126507
3. 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,2021年4月～6月,2021年7月～9月,2021年10月～12月]（IPA）
https://www.ipa.go.jp/security/J-CSIP/index.html

3位 サプライチェーンの弱点を悪用した攻撃

～サプライチェーン攻撃の世界的な被害増加に伴い、今一度リスクの見直しを～



商品の企画・開発から、調達、製造、在庫管理、物流、販売までの一連のプロセス、およびこの商流に関わる組織群をサプライチェーンと呼ぶ。このサプライチェーンの関係性を悪用し、セキュリティ対策の強固な企業を直接攻撃せずに、その企業が構成するサプライチェーンの中でセキュリティ対策が手薄な関連組織や利用サービスの脆弱性等を最初の標的とし、そこを踏み台として本命の標的である組織を攻撃する手口がある。関連組織に預けた情報が漏えいしたり、本来の標的である企業が攻撃を受けたりすることで被害が発生する。

＜攻撃者＞

- 組織的犯行グループ
- 犯罪者

＜被害者＞

- 組織（自組織、自組織の商流に関わる組織）

＜脅威と影響＞

組織には、必ず何らかの形でサプライチェーンとの関係性が存在する。例えば、取引先や委託先、導入しているソフトウェアまでと多岐にわたる。直接攻撃が困難な組織に対し、そのサプライチェーンの脆弱な部分を攻撃し、そこを経由して間接的または段階的に標的の組織を狙う。外部に対しては強固なセキュリティ対策を行っている組織でも取引先等のサプライチェーンを足掛かりとされることで、攻撃者の侵入を許してしまうおそれがある。

攻撃を受けた場合、機密情報の漏えいや信用の失墜等、様々な被害が発生する。また、取引先の組織においても、自組織が被害を受けるだけでなく、取引相手にも損害を与えてしまうことで、取引相手を失ったり、場合によっては、損害賠償を求められたりするおそれがある。

＜攻撃手口＞

◆ **取引先や委託先が保有する機密情報を狙う**

標的の組織よりもセキュリティが脆弱な取引先や委託先等を攻撃し、その組織が委託業務において保有していた標的組織の機密情報等を窃取する。

◆ **ソフトウェア開発元や MSP 等を攻撃し、標的を攻撃するための足掛かりとする**

ソフトウェアの開発元やサービス提供元、企業システムの運用・監視等を請け負う事業者（MSP）が利用するオープンソースや提供されているソフトウェアアップデートに攻撃者がウイルスを仕込んだりする。その後、開発元等から公開されたアップデートを適用した利用者がウイルスに感染し、そのウイルスを介して標的組織に侵入する。

＜事例または傾向＞

◆ **サプライチェーン攻撃の世界的な増加**

米 Sonatype 社の調査結果によれば、OSS（オープンソースソフトウェア）をターゲットとしたサプライチェーン攻撃が、2021 年は 1 万 2,000 件を超え、前年比 650%増となったとしており、世界的に攻撃が急増している。[1]また、クラウドの運用を含む技術者 300 人の内 36%が情報漏えいや侵害等の問題を経験しており、83%が企業においてクラウドの設定ミスに関連する重大なデータ侵害に対して脆弱であることを懸念している。[2]

◆ 子会社や海外拠点を狙った攻撃

2021 年 4 月、国内の光学機器メーカーHOYA の米子会社がランサムウェア攻撃を受け、約 300 ギガバイトの財務や顧客情報等が窃取され、ダークウェブ上のウェブサイトに公開されていることが明らかになった。「アストロチーム」と名乗るサイバー犯罪グループが本件の犯行声明を出している。[3]

◆ 業務委託先から貸与データが外部に流出

2021 年 9 月、建設コンサルティングのオリエンタルコンサルタンツは 8 月に受けたランサムウェア攻撃により連結業績で約 7 億 5000 万円の特別損失を計上すると発表した。同社に業務を委託していた東京都や千葉県市川市が、貸与していたデータも被害を受けた可能性があると発表している。[4]

＜対策/対応＞

組織（自組織）

- 被害の予防
  - ・業務委託や情報管理における規則の徹底
    製造においては原材料や部品の調達経路、物流経路等も考慮する。
  - ・報告体制等の問題発生時の運用規則整備
    攻撃を受けた場合を想定し、インシデント対応計画を整備し、定期的な訓練により見直す。
  - ・信頼できる委託先、取引先組織の選定
    商流に関わる組織の信頼性評価や品質基準を導入し、定期的に監査を行う。
  - ・複数の取引先候補の検討
  - ・納品物の検証
  - ・契約内容の確認
    組織間の取引や委託契約における情報セキュリティ上の責任範囲を明確化し、合意を得る。また、賠償に関する契約条項を盛り込む。
  - ・委託先組織の管理
    委託元組織が委託先組織のセキュリティ対策状況と情報資産の管理の実態を定期的に確認できる契約とすることが重要である。
- 被害を受けた後の対応
  - ・影響調査および原因の追究、対策の強化
  - ・被害への補償

組織（自組織/自組織の商流に関わる組織共通）

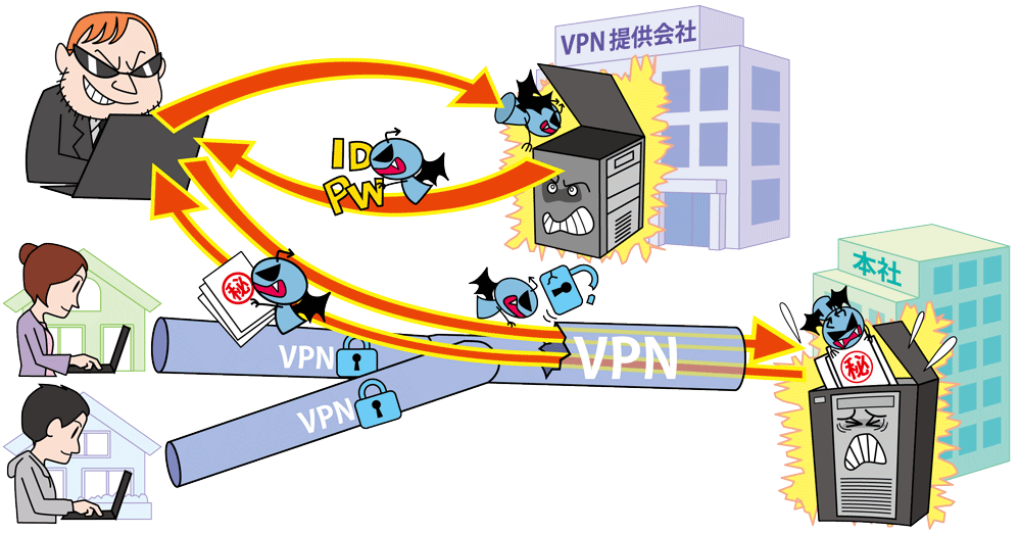
- 被害の予防
  - ・取引先や委託先の情報セキュリティ対応の確認、監査
  - ・情報セキュリティの認証取得
    ISMS、P マーク、SOC2、ISMAP 等を取得し、必要な運用を維持するよう定期的に見直す。
  - ・公的機関が公開している資料の活用 [5,6,7]
- 被害を受けた後の対応
  - ・組織の方針に従い各所へ報告、相談する
    上司、CSIRT、関係組織、公的機関等

参考資料

1. 2021 State of the Software Supply Chain Report（sonatype）
https://www.sonatype.com/resources/state-of-the-software-supply-chain-2021
2. The State of Cloud Security 2021（sonatype）
https://www.sonatype.com/hubfs/State_of_Cloud_Security_2021.pdf
3. HOYA米子会社にサイバー攻撃 機密情報が闇サイトで公開か（日本放送協会）
https://www3.nhk.or.jp/news/html/20210424/k10012994941000.html
4. ランサムウェア攻撃で7億円超の特別損失、建設コンサル大手のオリエンタルコンサルタンツが発表（ITmedia NEWS）
https://www.itmedia.co.jp/news/articles/2109/17/news149.html
5. サプライチェーンのセキュリティ脅威に備える（IPA）
https://www.ipa.go.jp/files/000073868.pdf
6. サイバーセキュリティ経営ガイドライン（経済産業省）
https://www.meti.go.jp/policy/netsecurity/mng_guide.html
7. 外部委託等における情報セキュリティ上のサプライチェーン・リスク対応のための仕様書策定手引書（内閣サイバーセキュリティセンター）
https://www.nisc.go.jp/pdf/policy/general/risktaiou28.pdf

4位 テレワーク等のニューノーマルな働き方を狙った攻撃

～テレワークのセキュリティは企業と従業員の結束が不可欠～



2020 年から続く新型コロナウイルス感染症（COVID-19）の世界的な蔓延（まん）に伴い、感染症対策の一環として政府機関がニューノーマルな働き方の１つであるテレワークを推奨している。勤労形態としてテレワークが活用され、ウェブ会議サービスや VPN 等の本格的な活用がされる中、それらを狙った攻撃が行われている。

＜攻撃者＞

- 組織的犯行グループ
- 犯罪者

＜被害者＞

- 組織
- 組織（テレワーカー）

＜脅威と影響＞

2020 年以降、組織の積極的なテレワークへの移行に伴い、自宅等から VPN 経由で社内システムにアクセスしたり、ウェブ会議サービスを利用して自組織または他組織と会議を行ったりする機会が増えた。また、テレワークのために私有端末（PC やスマートフォン等）や自宅のネットワークを利用し、初めて使うソフトウェアを導入する等、新たな業務環境が追加された。このような業務環境の急激な変化を狙った攻撃が行われている。

業務環境に脆弱性があると、ウェブ会議をのぞき見されたり、テレワーク用の端末にウイルスを感染させられたり、感染した端末から社内システムに不正アクセスされたりするおそれがある。

＜攻撃手口/発生要因＞

◆ テレワーク用ソフトウェアの脆弱性の悪用

VPN 等のテレワーク用に導入している製品の脆弱性や設定ミス等を悪用し、社内システムに不正アクセスしたり、PC 内の業務情報等を窃取したりする。また、ウェブ会議サービスの脆弱な設定を悪用し、ウェブ会議をのぞき見する。

◆ 急なテレワーク移行による管理体制の不備

テレワークへの急な移行によりルール整備やセキュリティ対策のノウハウが不十分なまま業務利用を開始してしまっている。

◆ 私有端末や自宅のネットワークを利用

私有端末では、ウェブサイトや SNS へのアクセスや、様々なソフトウェアをインストールすることがある。端末のウイルス感染や、ソフトウェアの脆弱性を攻撃者に悪用され、業務上の情報やテレワーク用の認証情報等を窃取されるおそれがある。また、組織支給の端末を利用している場合でも、自宅やシェアオフィスのネットワーク環境に適切なセキュリティ対策が行われていないと組織のセキュリティ対策が適用されず、端末がウイルスに感染する等のおそれがある。

＜事例または傾向＞

◆ **VPN 機器の認証情報、数万社分流出**

2021 年 9 月、フォーティネット製の VPN 機器の認証情報が数万社分流出した。2019 年に修正済みの脆弱性が悪用されており、機器への脆弱性対策を講じていない組織が攻撃を受ける可能性がある。流出した認証情報には日本企業も約 1,000 社含まれ、その多くは中小企業とみられている。[1]

◆ **リモートデスクトップへの総当たり攻撃急増**

カスペルスキーの公式ブログによると、WHO（世界保健機関）のパンデミック宣言前後で、RDP（リモートデスクトッププロトコル）への総当たり攻撃の件数が、9,310 万件（2020 年 2 月）から 2 億 7,740 万件（2020 年 3 月）へと約 3 倍に増加している。その後は月に 3 億件を超える状態が続いている。[2]

◆ **約 14%の業務利用端末が会社未認知**

キヤノンマーケティングジャパンの情報セキュリティ意識に関する実態調査結果によると、37.6%が個人所有の端末を業務に利用し、13.8%が勤務先からの許可が不要、または許可を得ずに個人所有の端末で業務を行っている実態が判明した。従業員が勤務先の許可を得ない問題だけでなく、企業としての体制やルールが定められていない実態が明らかになっている。[3]

＜対策/対応＞[4]

個人（テレワーカー）

- 被害の予防（被害に備えた対策含む）
  - ・表 1.3「情報セキュリティ対策の基本」を実施
  - ・組織のテレワークのルールを遵守（使用する端末、ネットワーク環境、作業場所等）
- 被害を受けた後の対応
  - ・組織の方針に従い各所へ報告、相談する
    上司、CSIRT、関係組織、公的機関等

組織（経営者層）

- 組織としての体制の確立
  - ・CSIRT の構築
  - ・対策予算の確保と継続的な対策の実施
  - ・テレワークのセキュリティポリシーの策定
  - ・有事の際の連絡窓口やフローの確立
    確立後は定期的な訓練により運用を見直す。

組織（セキュリティ担当者、システム管理者）

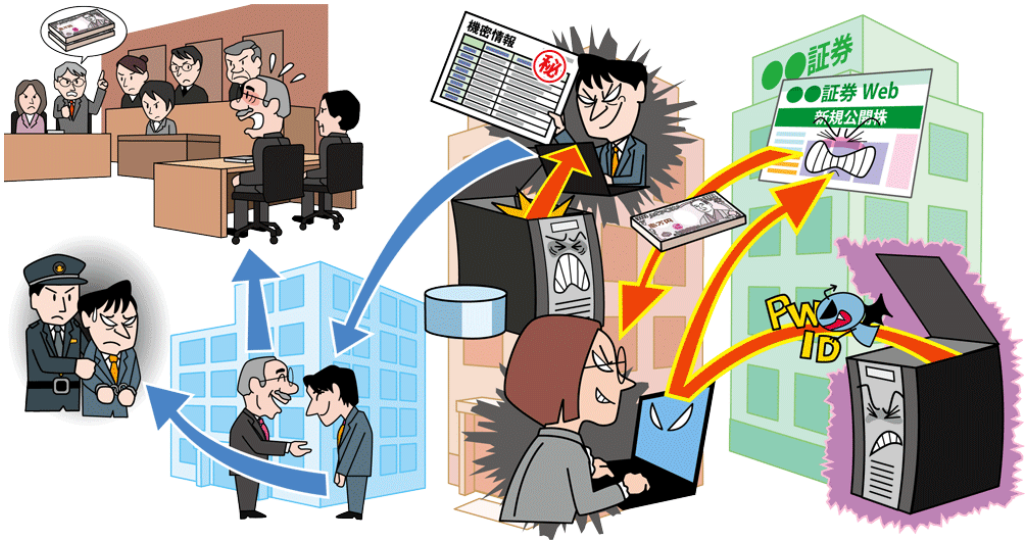
- 被害の予防（被害に備えた対策含む）
  - ・シンクライアント、VDI、VPN、ZTNA/SDP 等のセキュリティに強いテレワーク環境の採用
  - ・テレワークの規程や運用ルールの整備
    組織支給端末と私有端末の違いを考慮する。また、テレワーク開始時の暫定的なセキュリティ対策や例外措置とした運用を見直す。
  - ・従業員に対するセキュリティ教育の実施
  - ・利用するソフトウェアの脆弱性情報の収集と周知、対策状況の管理
  - ・セキュリティパッチの適用（VPN 装置、ネットワーク機器、PC、スマートフォン等）
    使用中の機器だけでなく予備機等は使用する前に最新のパッチを適用する。
  - ・ネットワークレベル認証（NLA）を行う
  - ・多要素認証の設定を有効にする
- 攻撃の予兆／被害の早期検知
  - ・適切なログの取得と継続的な監視
  - ・ネットワーク監視、防御
  - ・UTM、IDS/IPS、WAF、仮想パッチ等の導入
    導入後も対策情報（設定等）を定期的に更新する作業を想定し、予算や体制を確保する。
- 被害を受けた後の対応
  - ・CSIRT の運用によるインシデント対応
    テレワーク環境をリモートから調査する。
  - ・影響調査および原因の追究、対策の強化

参考資料

1. VPN認証情報また流出　日本は1000社、中小企業中心（日経電子版）
https://www.nikkei.com/article/DGXZQOUE110A80R10C21A9000000/
2. カスペルスキー、リモートデスクトップへの総当たり攻撃急増を報告（マイナビニュース）
https://news.mynavi.jp/article/20210406-1865958/
3. 情報セキュリティ意識に関する実態調査レポート2021（キヤノンマーケティングジャパン株式会社）
https://eset-info.canon-its.jp/malware_info/special/detail/210708.html
4. テレワークにおけるセキュリティ確保（総務省）
https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/

5位 内部不正による情報漏えい

～組織は内部不正をさせない、内部不正で取得された情報を利用しない～



組織に勤務する従業員や元従業員等の組織関係者による機密情報の持ち出しや悪用等の不正行為が発生している。また、組織内における情報管理のルールを守らずに情報を持ち出し、紛失や情報漏えいにつながるケースも散見される。組織関係者による不正行為は、組織の社会的信用の失墜、損害賠償による経済的損失により、組織に多大な損害を与える。また、不正に取得した情報を他組織に持ち込んだ場合、その組織も損害賠償等の対象になるおそれがある。

＜攻撃者＞

- 組織の従業員（在職者、離職者）

＜被害者＞

- 組織
- 個人（顧客、サービス利用者）

＜脅威と影響＞

悪意を持った組織関係者が、組織が保管する技術情報や顧客情報等の重要情報を閲覧し、不正に持ち出し、外部へ公開、有利に転職するための情報提供または競合他社等に売却、漏えいする事で組織に損害を与えることがある。これらは金銭目的や組織への私怨や私欲等で行われる。また、自宅で作業するために、組織の情報管理のルールを守らずに情報を外部に持ち出し、その情報を紛失してしまい、情報漏えいにつながるケースもある。

漏えいした情報の重要性や機密性、漏えいの規模によっては、組織の社会的信用の失墜や、顧客等に対する損害賠償や補填による経済的損失が発生し、組織の経済的競争力の大幅な低下に繋がる。その結果、組織の経営の根幹を揺るがすインシデントに発展するおそれがある。また、組織に持ち込まれた情報が不正に取得されたものであることを知りつつ使用した場合、刑事罰の対象になることもある。

＜攻撃手口＞

◆ アクセス権限の悪用

付与された権限を悪用し、組織の重要情報を窃取する。必要以上に高いアクセス権限が付与されている場合、より重要度の高い情報が窃取され、被害が大きくなるおそれがある。

◆ 在職中に割り当てられたアカウントの悪用

組織の離職者が、在職中に使用していたアカウントを悪用し、組織内部の情報を窃取する。

◆ 内部情報の不正な持ち出し

組織内部の情報を、USB メモリーや HDD 等の外部記憶媒体、メール、クラウドストレージ、スマホカメラ、紙媒体等を利用し、外部に不正に持ち出す。

＜事例または傾向＞

◆ **営業秘密を持ち出した元従業員の転職先に対して損害賠償請求**

2021 年 1 月、ソフトバンクの元従業員が営業秘密に該当するネットワーク技術に関わる情報を不正に持ち出していたとして逮捕された。また、同社は、同従業員の転職先の会社に対して業務上利用するサーバー内に持ち出した情報が保存され、従業員に開示された事実を確認したとして、その情報の利用停止、廃棄、約 1,000 億円の損害賠償請求権の一部として 10 億円の支払い等を求める民事訴訟を東京地方裁判所へ提起した。[1,2,3]

◆ **取引先の顧客情報を不正利用**

2021 年 3 月、SCSK の元従業員がシステムの保守・運用等を受託していた取引先にて、取引先の顧客 15 名の ID、パスワード、暗証番号等を不正に取得し、顧客になりすまして有価証券の売却や現金の不正出金を行ったとして逮捕された。顧客 15 名の被害総額は約 2 億円となった。[4]

＜対策/対応＞[5]

組織（システム管理者）

- 被害の予防
  - ・基本方針の策定

    組織内での効率的な対策推進は、経営層の積極的な関与が重要である。内部不正対策の責任は経営者にあり、最高責任者である経営者が総括責任者の任命並びに管理体制及び実施策の承認を行い、組織横断的な管理体制を構築する必要がある。
  - ・資産の把握、対応体制の整備

    重要資産を把握し、その重要度をランク付けした上で重要情報の管理者を定める。
  - ・重要情報の管理、保護

    重要情報の利用者 ID およびアクセス権の登録・変更・削除に関する手順を定めて運用する。従業員の異動や離職に伴い不要となった利用者 ID 等は直ちに削除する。また、それらの適切な管理、定期的な監査を実施する。さらに、利用者 ID の共用禁止等の処置を検討する。DLP 等のツールの導入を検討する。
  - ・物理的管理の実施

    重要情報の格納場所や重要情報を扱う執務室への入退室を管理する。USB メモリーやスマートフォン等の記録媒体は利用制限を行い、持ち出し/持ち込みの管理をする。また、記録媒体の廃棄を行う際には、適切なデータ消去の運用を実施する。
- 情報リテラシーや情報モラルの向上
  - ・人的管理及びコンプライアンス教育の徹底

    情報取扱ポリシーの作成、内部不正者に対する懲戒処分等を規定した就業規則等の整備を行い、従業員に対する教育を定期的に実施する。その際、従業員に秘密保持義務を課す誓約書を作成させることも重要である。
- 攻撃の予兆／被害の早期検知
  - ・システム操作履歴の監視

    重要情報へのアクセス履歴や利用者の操作履歴等のログ、証跡を記録し、監視する事で早期検知に努める。また、監視していることを従業員に周知することで不正を予防する。
- 被害を受けた後の対応
  - ・組織の方針に従い各所へ報告、相談する

    上司、CSIRT、関係組織、公的機関等
  - ・影響調査および原因の追究、対策の強化
  - ・内部不正者に対する適切な処罰の実施

参考資料

1. 楽天モバイルへ転職した元社員の逮捕について（ソフトバンク株式会社）
https://www.softbank.jp/corp/news/press/sbkk/2021/20210112_01/
2. 楽天モバイルと楽天モバイル元社員に対する訴訟を提起 1,000億円規模の損害賠償請求権を主張（ソフトバンク株式会社）
https://www.softbank.jp/corp/news/press/sbkk/2021/20210506_01/
3. 当社に対する訴訟の提起について（楽天モバイル株式会社）
https://corp.rakuten.co.jp/news/update/2021/0506_01.htmll
4. 当社元社員による不正行為について（SCSK株式会社）
https://www.scsk.jp/news/2021/pdf/20210324.pdf
5. 組織における不正防止ガイドライン（IPA）
https://www.ipa.go.jp/security/fy24/reports/insider/

6位 脆弱性対策情報の公開に伴う悪用増加

～その脆弱性は実は関係してるかも？情報収集と適切な対応を！～

ソフトウェアや機器類の脆弱性対策情報の公開は、脆弱性の脅威や対策情報を製品の利用者に広く呼び掛けられるメリットがある。一方で、その情報を攻撃者に悪用され、当該製品に対する脆弱性対策を講じていないシステムを狙う攻撃が行われている。近年では脆弱性関連情報の公開後に攻撃コードが流通し、攻撃が本格化するまでの時間もますます短くなっている。

＜攻撃者＞

- 組織的犯罪グループ

＜被害者＞

- 組織（開発ベンダー）
- 組織、個人（ソフトウェア利用者）

＜脅威と影響＞

一般的に、ソフトウェアに脆弱性が発見された場合、当該ソフトウェアの開発ベンダー等が脆弱性の修正プログラム（パッチ）を作成する。その後、ベンダーはセキュリティ対応機関等と連携するか、または自身で脆弱性対策情報として脆弱性の内容とパッチまたは対策方法を公開し、当該ソフトウェアの利用者へ対策を促す。

一方、公開された脆弱性対策情報を基に攻撃者が攻撃コード等を作成し、パッチ適用等の対策を実施していないソフトウェアに対して脆弱性を悪用した攻撃を行うことで、情報漏えいや改ざん、ウイルス感染等の被害の発生が確認されている。特に、Apache Struts2 や WordPress（プラグイン含む）といった広く利用されているソフトウェアの脆弱性の場合、攻撃コード等が公開されると被害が広範囲に拡散するおそれがある。

昨今、脆弱性が発見されてからそれを悪用した攻撃が発生するまでの期間が短くなっており、より迅速な対応が求められる。

＜攻撃手口＞

◆ 対策前の脆弱性（N デイ脆弱性）を悪用

ソフトウェアに脆弱性が発見され、パッチや回避策が公開されたものの、そのパッチを適用するか回避策を講じるまでにはいくらかの時間が掛かる。この未対応の時間に存在する脆弱性をＮデイ脆弱性と呼ぶ。また、POC コードを公開され、攻撃に悪用されることもある。

ソフトウェアの管理が不適切な企業は、未対応の時間が長くなるため、被害に遭うリスクが大きくなる。

◆ 公開されている攻撃ツールを使用

公開された脆弱性に対する攻撃ツールは短期間で作成され、ダークウェブ上のウェブサイト等で販売されたり、攻撃サービスとして提供されたりすることがある。また、オープンソースのツールに脆

弱性を利用する機能が実装され、それを悪用されることもある。

＜事例または傾向＞

◆ **Java のログ出力ライブラリ「Apache Log4j」の脆弱性**

2021 年 12 月 9 日（米国時間）、Apache Software Foundation はログ出力ライブラリ「Apache Log4j」の脆弱性（CVE-2021-44228）を公表した。この脆弱性は「Log4Shell」と呼ばれ、リモートから任意のコードが実行可能なものであった。

脆弱性公表の翌日には POC（実証コード）が公開され、POC を悪用した攻撃が多数確認された。「Apache Log4j」を利用している「Apache Struts2」、「Apache Solr」など Java で実装されている製品のほか、クラウドサービス等にも影響がある。[1,2,3]

◆ **「Movable Type」の脆弱性を狙う攻撃**

2021 年 10 月 20 日に公表された「Movable Type」の脆弱性は、公表から 6 日後の 10 月 26 日に POC が公開されていることが確認された。セキュリティ企業は、10 月 27 日から脆弱性を探索する通信が観測され、11 月 1 日頃から攻撃も確認されているとの報告があった。[4,5] また、11 月 7 日には、この脆弱性を悪用して、企業のホームページへの不正アクセスと改ざんの被害もあった。[6]

＜対策/対応＞

個人、組織（システム管理者／ソフトウェア利用者）

- 被害の予防
  - ・表 1.3「情報セキュリティ対策の基本」を実施
  - ・資産の把握、対応体制の整備
    パッチまたは回避策を適用する場合、サービスが正常に動作することを事前に検証する必要がある。そのため、検証するための体制や環境も事前に準備する必要がある。
  - ・脆弱性関連情報の収集と対応
  - ・ネットワークの監視および攻撃通信の遮断
    ネットワーク経由で脆弱性を悪用する攻撃を監視する。攻撃の疑いがある場合は、ファイアウォール等により通信を遮断する。
  - ・セキュリティのサポートが充実しているソフトウェアやバージョンを使う
    パッチや回避策の提供が迅速である等。
  - ・一時的なサーバー停止等
    パッチや回避策をすぐに適用できない場合、一時的にサーバー停止等を実施して、攻撃を回避する対策を取ることも検討する。
- 攻撃の予兆／被害の早期検知
  - ・UTM、IDS/IPS、WAF、仮想パッチ等の導入
    導入後も対策情報（設定等）を定期的に更新する作業を想定し、予算や体制を確保する。
- 被害を受けた後の対応
  - ・組織の方針に従い各所へ報告、相談する
    上司、CSIRT、関係組織、公的機関等
  - ・影響調査および原因の追究、対策の強化

組織（開発ベンダー）

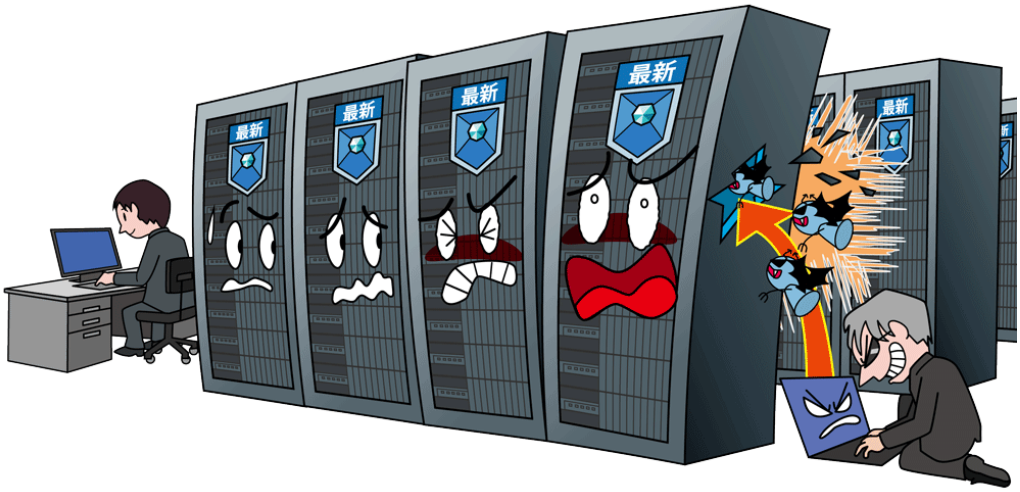
- 製品セキュリティの管理、対応体制の整備
  - ・製品に組み込まれているソフトウェアの把握、管理の徹底（SBOM を活用する）
  - ・脆弱性関連情報の収集と対応
  - ・脆弱性発見時の対応手順の作成
  - ・情報を迅速に発信できる仕組みの整備

参考資料

1. 【注意喚起】Log4jの脆弱性を狙う攻撃を多数検知、至急対策を！（株式会社ラック）
https://www.lac.co.jp/lacwatch/alert/20211213_002820.html
2. Javaライブラリ「Apache Log4j」の脆弱性（CVE-2021-44228）を標的とした攻撃の観測について（警察庁）
https://www.npa.go.jp/cyberpolice/important/2021/202112141.html
3. 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（（一社）JPCERTコーディネーションセンター）
https://www.jpcert.or.jp/at/2021/at210050.html
4. Movable TypeのXMLRPC APIにおける脆弱性（CVE-2021-20837）に関する注意喚起（（一社）JPCERTコーディネーションセンター）
https://www.jpcert.or.jp/at/2021/at210047.html
5. Movable Type及びPowerCMSのXMLRPC APIにおける脆弱性（CVE-2021-20837及びCVE-2021-20850）を標的とした攻撃の観測について（警察庁）
https://www.npa.go.jp/cyberpolice/important/2021/202111261.html
6. 弊社ホームページへの不正アクセスと改ざんの経緯と原因、今後の対策について（株式会社サンメディア）
https://www.sunmedia.co.jp/news20211110/

7位 修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）

～ゼロデイの脆弱性はセキュリティ担当者泣かせ～



ソフトウェアの脆弱性が発見され、脆弱性の修正プログラム（パッチ）や回避策が公開される前に脆弱性を悪用したサイバー攻撃が行われることがある。これをゼロデイ攻撃と呼ぶ。多くのシステムで利用されているソフトウェアに対してゼロデイ攻撃が行われると、社会が混乱に陥るおそれがある。

＜攻撃者＞

- 組織的犯行グループ

＜被害者＞

- 組織（開発ベンダー）
- 組織、個人（ソフトウェア利用者）

＜脅威と影響＞

ソフトウェアの開発ベンダー等が脆弱性を発見した場合、脆弱性の修正プログラム（パッチ）や回避策が公開されるが、それより先に攻撃者が脆弱性を発見した場合、攻撃コード等を作成し、当該ソフトウェアの脆弱性を悪用した攻撃（ゼロデイ攻撃）が行われる。この場合に組織で事前にできる対策は限られており、確実に防ぐことは難しい。

攻撃が成功すると、情報漏えいや改ざん、ウイルス感染等の被害が発生する。開発ベンダー等から脆弱性対策情報が公開されていない場合、被害に早期に気付いても原因の特定やその対策が難しく、適切な対応が取れないため、組織は対応に悩まされる。また、広く利用されているソフトウェアの脆弱性がゼロデイ攻撃に悪用された場合、被害が広範囲で発生するおそれがある。

＜攻撃手口＞

◆ ソフトウェアの脆弱性を悪用

開発ベンダー等が修正プログラムを公開する前に、攻撃者がソフトウェアの脆弱性を悪用して攻撃する。脆弱性の内容により、攻撃方法は様々であり、その被害も情報漏えいや改ざん、ウイルス感染等、様々である。

＜事例または傾向＞

◆ VPN 製品へのゼロデイ攻撃

2021 年 4 月 20 日（米国時間）、Pulse Secure 社の VPN 製品「Pulse Connect Secure」に遠隔の第三者が認証を回避し、任意のコードを実行されるおそれがある脆弱性が確認された。国内での攻撃は確認されていないが、米国では既に脆弱性を悪用した攻撃が行われていた。5 月 6 日に修正プログラムがリリースされるまでは、同社が公開している暫定的な回避策を実施するか、当該製品を一時的に使用停止する必要があった。[1,2]

◆ 印刷スプーラーへのゼロデイ攻撃

2021 年 7 月 1 日（米国時間）、Microsoft より Windows の印刷スプーラー「Windows Print

Spooler」の脆弱性に関する情報が公開された。この脆弱性は「PrintNightmare」と呼ばれ、攻撃者によって任意のコードを実行される等の被害が発生するおそれがあった。脆弱性の公開時点では修正プログラムのリリースはなく、同社が提供した回避策や緩和策を適用する必要があった。修正プログラムは 7 月 7 日から段階的に公開された。[3,4]

＜対策/対応＞

個人、組織（システム管理者）

- 被害の予防
  - ・表 1.3「情報セキュリティ対策の基本」を実施
  - ・資産の把握、対応体制の整備
  - ・ネットワークの監視および攻撃通信の遮断
    ネットワーク経由で脆弱性を悪用する攻撃を監視する。攻撃の疑いがある場合は、ファイアウォール等により通信を遮断する。
  - ・EDR 等を用いたエンドポイントの監視、防御
  - ・セキュリティのサポートが充実しているソフトウェアやバージョンを使う
    パッチや回避策の提供が迅速である等。
  - ・利用するソフトウェアの脆弱性情報の収集と周知、対策状況の管理
- 攻撃の予兆／被害の早期検知
  - ・UTM、IDS/IPS、WAF、仮想パッチ等の導入
    導入後も対策情報（設定等）を定期的に更新する作業を想定し、予算や体制を確保する。
- 修正プログラムリリース前の対応
  - ・回避策や緩和策の適用
  - ・当該ソフトウェアの一時的な使用停止
- 修正プログラムリリース後の対応
  - ・修正プログラムの適用
    必要に応じて回避策、緩和策を無効化する。
- 被害を受けた後の対応
  - ・組織の方針に従い各所へ報告、相談する
    上司、CSIRT、関係組織、公的機関等
  - ・影響調査および原因の追究、対策の強化

「Apache Log4j」の脆弱性への攻撃について

2021 年 12 月 9 日（米国時間）、Apache Software Foundation はログ出力ライブラリ「Apache Log4j」の脆弱性（CVE-2021-44228）を公開した。

この脆弱性に関しては、米 Cloudflare 社の CEO であるマシュー・プリンス（Matthew Prince）氏が「12 月 1 日に CVE-2021-44228 の Exploit を初めて確認した」と Twitter に投稿している。[5] また、Cisco Talos のブログでは「12 月 2 日に悪用を観測した」と報告している。[6]

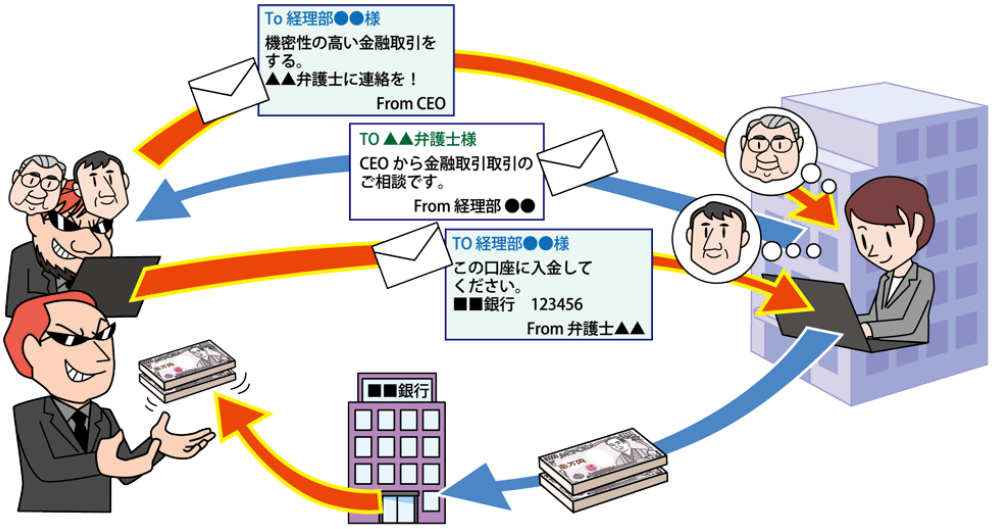
これらの報告を見ると、ゼロデイ攻撃の事例と言えなくもないが、脆弱性公開の直後から攻撃が増加している [7,8] ことに注目して、本書では組織 6 位「脆弱性対策情報の公開に伴う悪用増加」の事例の１つとして取り扱うこととした。

参考資料

1. Pulse Connect Secureの脆弱性（CVE-2021-22893）に関する注意喚起（（一社）JPCERTコーディネーションセンター）
https://www.jpcert.or.jp/at/2021/at210019.html
2. Pulse Connect Secure の脆弱性対策について（CVE-2021-22893）（IPA）
https://www.ipa.go.jp/security/ciadr/vul/alert20210421.html
3. Windowsの印刷スプーラーの脆弱性（CVE-2021-34527）に関する注意喚起（（一社）JPCERTコーディネーションセンター）
https://www.jpcert.or.jp/at/2021/at210029.html
4. Microsoft Windows 製品の Windows Print Spooler の脆弱性対策について(CVE-2021-34527)（IPA）
https://www.ipa.go.jp/security/ciadr/vul/20210705-ms.html
5. マシュー・プリンス氏のTwitter
https://twitter.com/eastdakota/status/1469800951351427073
6. Cisco Talosのブログ
http://blog.talosintelligence.com/2021/12/apache-log4j-rce-vulnerability.html
7. Javaライブラリ「Apache Log4j」の脆弱性（CVE-2021-44228）を標的とした攻撃の観測について（警察庁）
https://www.npa.go.jp/cyberpolice/important/2021/202112141.html
8. Apache Log4j2のRCE脆弱性（CVE-2021-44228）を狙う攻撃観測（（一社）JPCERTコーディネーションセンター）
https://blogs.jpcert.or.jp/ja/2021/12/log4j-cve-2021-44228.html

8位 ビジネスメール詐欺による金銭被害

～経営者からの秘密の依頼、取引先からの口座変更依頼、電話で確認しよう～



ビジネスメール詐欺（Business E-mail Compromise：BEC）は、巧妙な騙しの手口を駆使した偽のメールを組織・企業に送り付け、従業員を騙して送金取引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。2021 年も経営者になりすました手口が引き続き確認されている。

＜攻撃者＞

- 組織的犯行グループ

＜被害者＞

- 組織（企業、金銭の決裁権限を持つ責任者、金銭を取り扱う担当者）

＜脅威と影響＞

取引先や自社の経営者等を装い、偽のメールを組織の従業員へ送りつけ、攻撃者が用意した口座へ送金させる金銭的な被害をもたらすビジネスメール詐欺が行われている。差出人（送信元）のメールアドレスは取引先を模したメールアドレスや本物のメールアドレスを使ったり、不自然な日本語が少ないメール本文だったり等、本物のメールと見分けづらいようになっている。

受信者が偽のメールを本物のメールとして取り扱ってしまうと攻撃者が用意した口座に送金してしまうおそれがある。ビジネスメール詐欺は組織内外における金銭の授受を装うため金銭の被害は高額になる傾向があり、組織が被害に遭った際の影響が大きい。

＜攻撃手口＞

◆　取引先との請求書の偽装

取引先と請求に係るやり取りをメールで行っている際に、攻撃者が取引先になりすまし、攻撃者の用意した口座に差し替えた偽の請求書等を送りつけ、振り込ませる。なお、攻撃者は取引のやり取りや関係している従業員の情報を何らかの方法により入手した上で攻撃している。

◆　経営者等へのなりすまし

組織の経営者等になりすまし、同組織の従業員に攻撃者の用意した口座へ振り込ませる。この時、攻撃者は事前に入手した経営者や関係している従業員の情報を利用し、通常の社内メールであるかのように偽装する。

◆　窃取メールアカウントの悪用

従業員のメールアカウントを乗っ取り、その従業員の取引実績のある組織の担当者へ偽の請求書等を送り付け、攻撃者の用意した口座に振り込ませる。メール本文は巧妙に偽装され、送信元が本物のアカウントであるため、受信したメールが攻撃であることに気づきにくい。

◆　**社外の権威ある第三者へのなりすまし**

弁護士等の社外の権威ある第三者になりすまし、組織の財務担当者等に対して攻撃者の用意した口座へ振り込ませる。

◆　**詐欺の準備行為と思われる情報の窃取**

詐欺を実行する前の準備行為として、標的組織の情報を窃取する場合がある。例えば、攻撃者が詐欺の標的とする組織の経営者や経営幹部、または人事担当等の特定任務を担う従業員になりすまし、組織内の他の従業員の個人情報等を窃取する。

＜事例または傾向＞

◆　**会社役員を騙り海外関連企業を狙った攻撃**

サイバー情報共有イニシアティブ（J-CSIP）が公表したレポートによると、2021 年 8 月、J-CSIP 参加組織の海外関連企業の担当者が同社役員を騙ったビジネス詐欺メールを受信した。

メールは「機密性の高い金融取引を個人的に依頼したい」という簡素な内容で、実在する弁護士事務所の弁護士へ連絡を取ってほしいというものであった。差出人（From）の表示名には会社役員の名前とメールアドレスが設定されていたが、実際にはフリーメールアドレスから送られていた。また、同報先（CC）には、弁護士のメールアドレスを騙った偽のメールアドレスが設定されており、弁護士が同報されているように見せかけていた。[1]

◆　**一般社員になりすました詐欺メールを確認**

トレンドマイクロによると、継続的に実施しているビジネスメール詐欺（BEC）の脅威動向監視において、2021 年 1～9 月にかけて検出数が増加しており、8 月に大幅な増加が見られたとしている。過去数年のビジネスメール詐欺の手口は、攻撃者が経営幹部等になりすました詐欺メールであったが、2021 年は、一般社員になりすました詐欺メールを確認している。[2]

＜対策/対応＞

組織

- 被害の予防（被害に備えた対策含む）
  - ・表 1.3「情報セキュリティ対策の基本」を実施
  - ・ガバナンスが機能する業務フローの構築

    金銭が絡むものは特に上長や複数名の確認、取引相手（請求元）へのメール以外での事実確認を必要とするなど、個人の判断や命令で取引や金銭の移動がされないルールやシステムの構築。
  - ・メールに依存しない業務フローの構築
  - ・メールに電子署名を付与（S/MIME や PGP）

  ＜メールの真正性の確認＞
  - ・メールだけでなく複数の手段で事実確認

    振込先の口座変更等がある場合、電話等、メール以外の方法で取引先に確認する。また、口座の名義等を金融機関に確認する。[3]
  - ・普段とは異なるメールに注意

    普段とは異なる言い回しや、表現の誤り、送信元のメールドメインに注意する。
  - ・判断を急がせるメールに注意

    至急の対応を要求する等、担当者に真偽の判断時間を与えないようにする手口も考えられる。真偽を確認するフローを策定しておく。

  ＜メールアカウントの適切な管理＞
  - ・パスワードの適切な管理やログイン通知機能、多要素認証等の利用
- 被害を受けた後の対応
  - ・組織の方針に従い各所へ報告、相談する

    上司、CSIRT、関係組織、公的機関等
  - ・影響調査および原因の追究、対策の強化

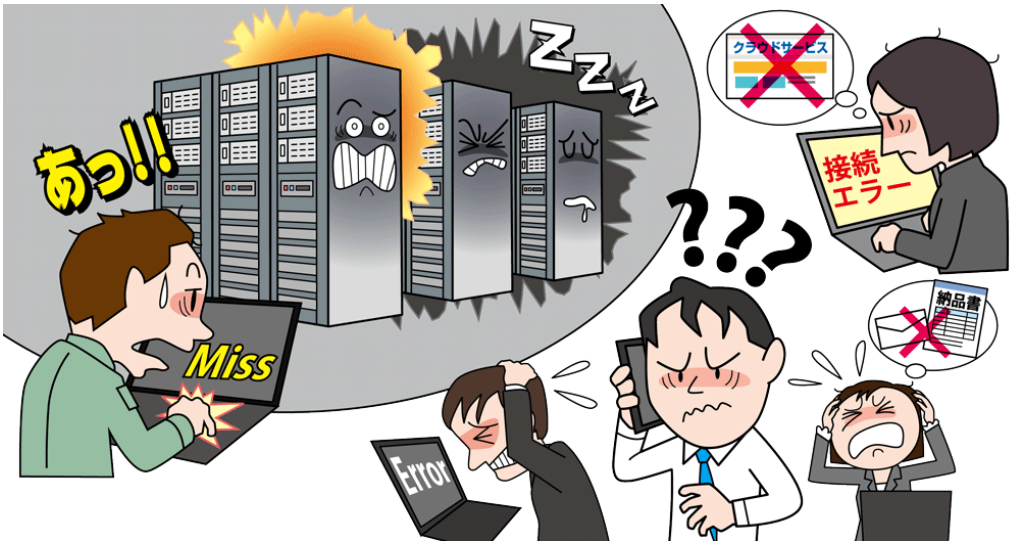
    メールアカウントに意図しない転送設定やフォルダー振り分け設定等がないかを確認
  - ・被害（侵害）を受けたメールサーバー上の全メールアカウントのパスワード変更

参考資料

1. 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]（IPA）
https://www.ipa.go.jp/files/000094117.pdf
2. 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（トレンドマイクロ株式会社）
https://blog.trendmicro.co.jp/archives/29272
3. 海外取引先を装うBEC（ビジネスメール詐欺）に注意！（警視庁Twitter）
https://twitter.com/MPD_cybersec/status/1400256494134693895

9位 予期せぬ IT 基盤の障害に伴う業務停止

～平常時から代替手段の検討を～



組織が利用するサーバーやインターネット上のサービス、業務システム等で使用しているネットワークやクラウドサービス等の IT 基盤に予期せぬ障害が発生し、長時間にわたり利用者や従業員に対するサービスを提供できなくなるケースがある。こうした IT 基盤の停止はシステムの可用性を侵害する情報セキュリティリスクであり、IT 基盤を利用している組織の事業に大きな影響を与えるおそれがある。

＜加害者＞

- 企業（IT 基盤提供事業者）
- 組織(組織内 IT 基盤設備)

＜被害者＞

- 個人（IT システム利用者）
- 組織（IT システム利用者、IT 基盤利用者）

＜脅威と影響＞

企業や民間団体、官公庁等多くの組織は自社の機器をデータセンターに設置する場合や、クラウドの IT 基盤を利用するケースがある。利用している IT 基盤で、自然災害、人為的な作業事故、データセンターの設備障害、利用しているシステムの障害等により、予期せぬ障害が発生すると、IT 基盤を利用して外部に提供しているサービスや社内の業務システムが突然停止する。

それにより、組織が提供しているサービスの利用者がそのサービスを利用できなくなったり、組織の業務が停止したりする。長時間停止した場合、組織の利益減少や競争力の弱体化等、経済的損失につながる。また、人々の日常生活にも支障をきたすおそれがある。

＜発生要因＞

◆ 自然災害

地震や台風、洪水等の自然災害により、IT 基盤の設備や施設が被害を受け、IT 基盤に障害が発生する。

◆ 作業事故

インフラ設備のメンテナンス作業における人為的ミスにより通信回線断や電力供給断等の事故が発生したり、システムの設定変更作業における作業ミス等によりシステムの正常動作に影響を及ぼしたりすることで、IT 基盤に障害が発生する。

◆ 設備障害

データセンター等、様々なサービスが稼働している施設において、空調設備等の制御システムの障害により、施設内にある機器の稼働環境（温度や湿度等の条件）を維持できなくなり機器が停止する等、IT 基盤に障害が発生する。

◆ **システム障害**

IT 基盤を構成する機器のハードウェアやソフトウェアに不具合が発生したり、ネットワークの輻輳や不具合が発生したりすることで、IT 基盤に障害が発生する。

＜事例または傾向＞

◆ **Amazon Web Services で障害発生**

2021 年 9 月、Amazon Web Services が提供する専用ネットワーク接続である「AWS Direct Connect クラウドサービス」で障害が発生した。ネットワークの反応時間を最適化するために導入していた新しいプロトコルにより、東京リージョンのデータセンターのネットワーク機器に障害が発生したことが原因であった。同社はこのプロトコルを無効化することで障害を解消した。[1]

この障害により、三菱 UFJ 銀行やみずほ銀行のアプリ、SBI 証券などネット証券の Web サイト、KDDI の au Pay の入金等に影響が出ている。[2]

◆ **NTT ドコモで通信障害発生**

2021 年 10 月、NTT ドコモが提供する音声通話・データ通信サービスで障害が発生した。原因はネットワーク工事の切り戻しに伴う信号量増大によるネットワーク輻輳としている。障害発生の同日に回復が発表されたものの、利用者が利用しづらい状態は翌日まで続いた。影響は延べ 1,290 万人に及んだ。[3,4]

◆ **大雨災害発生時に気象庁HPが閲覧障害**

2021 年 8 月、九州や広島県に大雨特別警報が発表[5,6]された日に、気象庁ホームページが閲覧しにくい状況となった。気象庁のシステムは過去の災害時の最大規模のアクセスに耐えられるようにしていたが、当日はそれ以上のアクセスがあり、システムの処理能力が追いつかなくなった。[7]

＜対策/対応＞

組織（システム管理者）

- 被害の予防（被害に備えた対策を含む）

  ・事業継続マネジメント（BCM）の実践（BCP 策定と運用）[8]

  IT 基盤の様々なトラブルを事前に想定し、対応策を準備する。また、事業の継続や早期復旧をするため、行動計画や復旧目標を定め、事業継続計画（BCP）を策定し、運用する。

  ・可用性の確保と維持（システム設計や監視）

  システムの冗長化や過負荷対策についても検討する。

  ・データバックアップ（復旧対策）

  ・契約や SLA 等を確認

  IT 基盤側との契約や SLA 等を確認する。IT 基盤を利用して顧客にサービスを提供する場合は、顧客との契約や SLA 等も確認する。

  ・障害時の IT 基盤側との連携を確認

  対応マニュアルを作成し、定期的な訓練により見直す。

- 被害を受けた後の対応

  ・BCP に従った対応

  影響調査、対策強化等

  ・組織の方針に従い各所へ報告、相談する

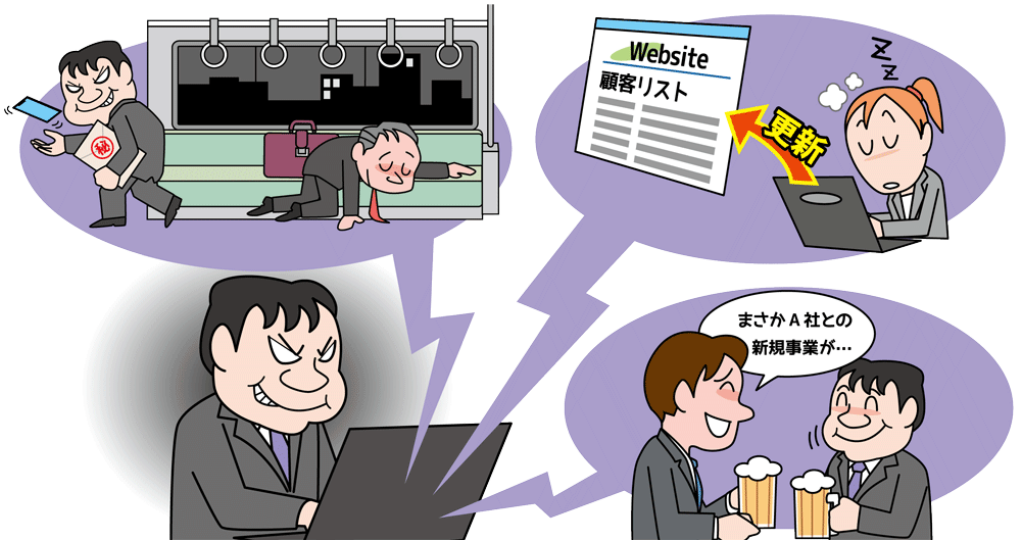
  上司、CSIRT、関係組織、公的機関等

参考資料

1. 東京リージョン(AP-NORTHEAST-1)で発生したAWS Direct Connectの事象についてのサマリー（Amazon Web Services）
https://aws.amazon.com/jp/message/17908/
2. アマゾン子会社AWSで障害 データ管理サービス 広範囲に影響（日本放送協会）
https://www3.nhk.or.jp/news/html/20210902/k10013238691000.html
3. 音声通話・データ通信サービスがご利用しづらい事象について（株式会社NTTドコモ）
https://www.nttdocomo.co.jp/info/network/kanto/pages/211014_00_m.html
4. ドコモの10月通信障害、延べ1290万人に影響（（日経電子版）
https://www.nikkei.com/article/DGXZQOUC080YW0Y1A101C2000000/
5. 福岡県に大雨特別警報発表（気象庁）
https://www.jma.go.jp/jma/press/2108/14b/20210814_2.html
6. 広島県に大雨特別警報発表（気象庁）
https://www.jma.go.jp/jma/press/2108/14c/20210814_3.html
7. 気象庁ホームページが閲覧しにくい状況となったことについて（気象庁）
https://www.jma.go.jp/jma/press/2108/15b/hp.pdf
8. 事業継続計画策定ガイドライン（経済産業省）
https://www.meti.go.jp/policy/netsecurity/downloadfiles/6_bcpguide.pdf

10位 不注意による情報漏えい等の被害

～そのメールの宛先、本当にあっていますか？～



組織で取り扱う重要情報について、組織の規程の不備や情報を扱う従業員に対する情報リテラシー教育の不足、不注意・ミスによって引き起こされる情報漏えいが後を絶たない。漏えいした情報が悪用され、他の脅威を誘発してしまうおそれがある。また、組織の社会的信用の失墜や、経済的な損失にもつながる可能性がある。

＜加害者（情報を漏えいさせた側）＞

- 組織（従業員）

＜被害者（情報を漏えいされた側）＞

- 個人（当事者のサービス利用者等）
- 組織（当事者の取引先企業等）
- 組織（当事者自身）

＜脅威と影響＞

組織において、サービス内容や業務内容によっては個人情報や機密情報を取り扱うことがある。しかし、組織の情報管理に関する規程の不備や、従業員のセキュリティ意識の低さ、不注意によるミス等によってこれらの重要情報を漏えいさせてしまう事件が発生している。

漏えいした情報が悪用されると詐欺被害等の二次被害に繋がるおそれがある。また、社会的信用の失墜やそれに伴う経済的損失が発生する可能性がある。

＜要因＞

◆　取り扱い者の情報リテラシーの低さ

自身の扱う情報の機密性や重要性等を理解していないために、不用意に外部へ漏えいしてしまう。例えば、重要情報の記載されたメールの宛先間違いや重要情報が入った端末の紛失等が挙げられる。また、重要情報を私的に利用して外部のサイト等に公開してしまい情報漏えいにつながるケースもある。

◆　情報を取り扱う際の本人の状況

体調不良や多忙等、情報を取り扱う従業員が置かれた状況から注意力散漫になり、メールの誤送信等のミスによる情報漏えい事故を起こしてしまう。

◆　組織規程および取り扱いプロセスの不備

組織で制定している情報の取り扱いプロセスに不備があると情報漏えいが起きやすい。例えば、外部に情報を持ち出す際の確認手順や作業時の確認手順等に関するプロセスの不備が挙げられる。

＜不注意による情報漏えい例＞

- メールの誤送信（宛先間違い、TO/CC/BCC の設定間違い、添付ファイル間違い等）
- 不適切なウェブ公開（重要情報のマスク不備、公開ファイルや参照権限設定誤り等）
- 重要情報を保存した情報端末（PC やスマートフォン等）・記録媒体（USB メモリー等）の紛失

- 重要書類（紙媒体）の紛失
- 私的利用による外部流出

＜事例または傾向＞

◆ 委託先のソースコードを私的利用で情報漏えい

2021 年 1 月、三井住友銀行は同行のシステムで使用しているソースコードが外部サイトにて公開されていることを明らかにした。原因は、同行より委託されていた企業の社員が、自身の書いたソースコードをアップロードすることで年収を診断できるサービスを利用するために外部サイトにソースコードをアップロードしたことである。同行は顧客情報の流出はなくセキュリティには問題ないとしている。[1]

◆ 送付データに不備があり情報漏えい

2021 年 9 月、クレジットカード等の信販事業を手掛けるアプラスはカード会員向けサービスで使用する 47 万 5,813 人分の ID とパスワードが、本来は渡す必要のない委託先 2 社に渡っていたことを明らかにした。提供したデータが委託先以外に渡った形跡はなく、不正利用は確認されていない。原因は、委託先に送付する際の、確認手法に不備があったためとしている。同社はデータを渡す際の仕組みを見直すほか、社員の意識改善を進めるとしている。[2]

◆ メールの返信ミスによる情報漏えい

2021 年 1 月、FX 等を取り扱うゴールデンウェイ・ジャパンは顧客への問い合わせ対応のメールに顧客の個人情報 2,873 件を誤添付し、流出させたと明かした。同社は送付した顧客にデータの削除を依頼し、ファイルは破棄されたとしている。同社はこの問題を受け、個人情報の管理体制を強化、社員への教育や業務フローをルール化し、再発防止に取り組むとのこと。[3]

＜対策/対応＞

組織（当事者）

- 情報リテラシーや情報モラルの向上
  - ・従業員のセキュリティ意識教育
  - ・組織規程および確認プロセスの確立
    特定の担当者への業務集中が発生しないような体制の構築も重要である。
  - ・組織規程および確認プロセスの見直し
    確立した規程やプロセスが適切に運用できているか定期的に見直す。
- 被害の予防（被害に備えた対策含む）
  - ・確認プロセスに基づく運用
  - ・情報の保護（暗号化、認証）、機密情報の格納場所の掌握、可視化
  - ・DLP（情報漏えい対策）製品の導入
  - ・外部に持ち出す情報や端末の制限
    外部との適切なファイル送受信の運用を検討する（クラウドストレージ利用、暗号化等）
  - ・メールの誤送信対策等の導入
  - ・業務用携帯端末の紛失対策機能の有効化
- 攻撃の予兆／被害の早期検知
  - ・問題発生時の内部報告体制の整備
  - ・外部からの連絡窓口の設置
- 被害を受けた後の対応
  - ・組織の方針に従い各所へ報告、相談する
    上司、CSIRT、関係組織、公的機関等
  - ・影響調査および原因の追究、対策の強化
  - ・被害拡大や二次被害要因の排除
  - ・漏えいした内容や発生原因等の公表

個人/組織（被害者）

- 被害を受けた後の対応
  - ・クレジットカードの停止
    クレジットカード会社へ不正利用の連絡と停止の手続きを行う。

参考資料

1. 三井住友銀行などのソースコードが流出 “年収診断”したさにGitHubに公開か【追記あり】（ITmedia NEWS）
https://www.itmedia.co.jp/news/articles/2101/29/news107.html
2. 親会社の委託先にID・パスワード47万人分を誤提供、新生銀行傘下のアプラスがクレカ会員向けサービスで（ITmedia NEWS）
https://www.itmedia.co.jp/news/articles/2109/17/news126.html
3. 問い合わせメールの返信ミスで顧客情報2,873件が流出
https://cybersecurity-jp.com/news/47890（サイバーセキュリティ.com）

コラム：被害事例から学ぶクラウドサービス利用時の注意点

昨今、企業ではメールや Microsoft Office 等でクラウド上のサービス（以降、クラウドサービス）を利用したり、クラウド上に自社のサービスを構築して、顧客に提供したりする機会が多くなっています。また、家庭でも特に意識することなくクラウドサービスを利用し、写真や連絡先等、個人に関わる情報をクラウドに保存しています。クラウドサービスの利用は、私たちの日常生活で欠かせないものになっています。

本コラムでは以下のように定義します。
・クラウド事業者：クラウド基盤（Amazon Web Services、Microsoft Azure 等）を提供する組織
・クラウドサービス事業者：クラウド基盤上でクラウドサービスを提供する組織
・クラウドサービス利用者（以降、利用者）：クラウドサービスを利用する人および組織

その一方で、近年はクラウドサービスから情報漏えいしたり、クラウド基盤自体が停止し、クラウドサービスにアクセスできなくなったりする被害事例がたびたび発生しています。

例えば、以下のような事例があります。

①2020 年末及び 2021 年、セールスフォース・ドットコムが提供するクラウド型顧客関係管理ソリューション Salesforce を利用する複数の企業から、不正アクセスにより、情報漏えいが発生したことが公表されました。例えば、PayPay では、加盟店の店名、住所等、最大 2,007 万 6,016 件[1]、SMBC 信託銀行では、口座開設に関わる氏名、生年月日等、最大 3 万 7,176 件に不正アクセスされ得る状態になっていました。[2]

原因は、Salesforce の脆（ぜい）弱性に起因するものではなく、ゲストユーザーへのアクセス制御の権限設定の問題とされ、利用組織で適切な設定を行っていない場合に影響を受けました。[3] なお、設定が必要となったきっかけは、2016 年に追加された Lightning Experience という新しいインタフェースで Web ページを作成した際に生成される Salesforce の ID やパスワードがなくてもアクセスできるゲストユーザーの権限がデフォルトで「有効」となったこととされています。[4]

②2021 年 4 月、Atlassian が提供するプロジェクト管理ツール Trello 上で個人情報が部外者から閲覧可能になっていることが話題になりました。具体的には、顧客や採用活動等の情報を Trello 上で管理していた一部組織で、住所、氏名、運転免許証、パスポートの画像等が公開状態でアップロードされていました。原因は、Trello 側の問題ではなく、その利用者が設定ミスで閲覧範囲を「公開」状態にしていたためとされています。[5]

③2021 年 9 月、クラウド基盤として利用される Amazon が提供する Amazon Web Services（以降、AWS）の東京リージョンで障害が発生し、Direct Connect サービスが約 6 時間アクセスしづらい状況となり、AWS でサービスを提供する企業やその利用者が影響を受けました。NTT ドコモでは、d メニュー、d マーケット等一部のサービスが利用しづらい状況になりました。[6]また、全日本空輸では、羽田空港で一時的にチェックインができなくなり、国内線 17 便に最大 13 分の遅延が発生しました。[7]
Amazon は、AWS が数ヶ月前に導入した新しいプロトコルが障害に関係していると考え、これを無効化することでネットワークが安定し、サービスが復旧しました。[8]

これらの事例からクラウドサービス利用上の注意点が見えてきます。

まず、①②③を通じて分かることはクラウドサービスを利用する際、「責任共有モデル（Shared Responsibility Model）」の考え方が大前提であり、**必ず運用責任がクラウド事業者、クラウドサービス事業者、利用者に発生します。**そのため、クラウドサービス事業者や利用者はクラウド基盤やクラウドサービスを利用した際にどのような責任を負うのかを理解する必要があり、その責任に応じた対処策を考慮した設計や運用をすることが必要になります。また、契約書や SLA でしっかりと確認して、責任共有モデルを理解しておく必要があります。

続いて、①と②の事例からは、**利用者はクラウドサービスを利用する際は、適切な設定（データへのアクセス権限の設定、不要アカウントの削除等）を付与する責任がある**ことが分かります。適切な設定を行わないと、本来公開してはいけない情報がインターネット上に公開され、情報漏えいにつながる恐れがあります。

さらに、①の事例からは、クラウドサービスの仕様変更や機能追加は基本的にクラウドサービスの提供元から一方的に行われるため、**利用者はクラウドサービスの仕様変更や機能追加に随時対応する責任がある**ということが分かります。つまり、クラウドサービスの利用開始時には問題とならなかった設定が、クラウドサービスの仕様変更や機能追加をきっかけに、不適切な設定に変わったり、隠れていた設定上の問題が顕在化したりする恐れがあります。**最初に問題なく設定したからと安心せず、定期的に設定の見直しを行うことが重要です。**さらに、クラウドサービス事業者が発表するリリース情報を把握し、仕様変更や機能追加を発表した（適用した）場合には、その都度、設定の見直しを行う必要があります。また、適切な設定を行うためには、クラウドサービスの仕様を理解しておく必要があります。つまり、利用するクラウドサービスの選定を適切に行い、マニュアル等から少なくともセキュリティに関する設定の初期値を確認し、変更方法等を事前に調べておくことが重要です。

次に、③の事例からは、**クラウドサービスは突然止まる恐れがある**ということが分かります。また、そのことから、**クラウドサービス事業者は大規模障害に備えた設計を行い、単一拠点での運用ではリスクがあることを考慮する責任がある**ということも分かります。障害の要因は、クラウドサービス自体の問題やクラウドサービスを動作させているクラウド基盤の問題など様々です。特に後者は複数のクラウドサービスに影響を与える恐れがあるため、**クラウドサービス事業者および利用者は、クラウドサービスが突然停止することを想定して、代替手段を準備することが重要です。**例えば、クラウドサービス事業者は、各国の法律（GDPR 等）や社内規程で許される範囲内において複数のリージョンでクラウドサービスを提供できるように冗長化を図ったり、クラウドサービスが停止していることを利用者に伝えるための手段を整えたりします。また、利用者（特に組織の利用者）は、長期間のサービス停止も想定して、BCP（Business Continuity Plan：事業継続計画）を策定しておくことが重要です。

クラウドサービスは、今や私たちの仕事や生活と密接な関係があります。そのため、適切な対策や準備を怠ると様々な被害に遭う恐れがあります。クラウドサービス事業者やクラウド事業者は、公的機関等から公開されているガイドラインや注意点等を参考にして、適切なセキュリティ対策を行い、安全にクラウドサービスの提供をお願いします。また、利用者は、クラウドサービスを安全に利用するために適切な管理を行いましょう。[9,10,11]

参考資料

1. 当社管理サーバーのアクセス履歴について（PayPay 株式会社）
https://paypay.ne.jp/notice/20201207/02/
2. クラウド型口座開設システムへの第三者のアクセスについて（株式会社 SMBC 信託銀行）
https://www.smbctb.co.jp/news/2021/pdf/news_030821_01.pdf
3. Salesforce サイトおよびコミュニティにおけるゲストユーザのアクセス制御の権限設定について
https://www.salesforce.com/jp/company/news-press/stories/salesforce-update/
4. Salesforce 利用者なら知っておきたい、セキュリティリスクとその対策を解説（株式会社 SHIFT）
https://service.shiftinc.jp/column/4995/
5. Trello の設定ミス、「公開」の誤解が原因？　分かりやすい表現とローカライズを考える（ITmedia NEWS）
https://www.itmedia.co.jp/news/articles/2104/07/news129.html
6. 【お詫び/回復】一部サービスがご利用しづらい事象について（株式会社 NTT ドコモ）
https://www.nttdocomo.co.jp/info/notice/page/210902_00_m.html
7. アマゾンクラウドで一時障害　航空やネット証券に影響（JIJI.COM）
https://www.jiji.com/jc/article?k=2021090200676&g=eco
8. 東京リージョン(AP-NORTHEAST-1)で発生した AWS Direct Connect の事象についてのサマリー（Amazon.com）
https://aws.amazon.com/jp/message/17908/
9. 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）（内閣サイバーセキュリティセンター）
https://www.nisc.go.jp/pdf/policy/infra/cloud_guidance.pdf
10. 中小企業の情報セキュリティ対策ガイドライン - 付録 6：クラウドサービス安全利用の手引き（IPA）
https://www.ipa.go.jp/files/000072150.pdf
11. クラウドサービス利用上の注意点（総務省）
https://www.soumu.go.jp/main_sosiki/joho_tsusin/security/enduser/security02/06.html

10 大脅威選考会

氏名	所属	氏名	所属
石田 淳一	(株)アールジェイ	佐藤 宏昭	京セラコミュニケーションシステム(株)
中嶋 美貴	アクセンチュア(株)	山田 淳二	京セラコミュニケーションシステム(株)
石井 彰	旭化成(株)	増田 博史	キンドリル(株)
岡田 良太郎	(株)アスタリスク・リサーチ	宮内 雄太	(一社)金融 ISAC
徳丸 浩	EG セキュアソリューションズ(株)	清水 将人	(一社)草の根サイバーセキュリティ運動全国連絡会
一條 敦	ヴイエムウェア(株)	印藤 晃	(株)グラビティ
井部 俊生	ヴイエムウェア(株)	高崎 庸一	グローバルセキュリティエキスパート(株)
橋本 賢一郎	ヴイエムウェア(株)	久津 英雄	グローバルセキュリティエキスパート(株)
安西 真人	(株)エーアイセキュリティラボ	三木 剛	グローバルセキュリティエキスパート(株)
関根 鉄平	(株)エーアイセキュリティラボ	小熊 慶一郎	(株)KBIZ / (ISC)2
溝口 英利	(株)SRA	保村 啓太	KPMG コンサルティング(株)
佐藤 直之	SCSK(株)	北田 高之	(株)神戸デジタル・ラボ
鈴木 寛明	SCSK(株)	バロウズ ダニエル	(株)神戸デジタル・ラボ
辻 伸弘	SB テクノロジー(株)	久柴 克宏	(株)神戸デジタル・ラボ
大塚 淳平	NRI セキュアテクノロジーズ(株)	宮﨑 清隆	国際マネジメントシステム認証機構(株)
田中 悠一郎	NRI セキュアテクノロジーズ(株)	中山 貴禎	(株)サイバーセキュリティクラウド
芳賀 夢久	NRI セキュアテクノロジーズ(株)	渡辺 洋司	(株)サイバーセキュリティクラウド
中西 克彦	NEC ネクサソリューションズ(株)	福森 大喜	(株)サイバーディフェンス研究所
杉井 俊也	NEC フィールディング(株)	荒川 大	(一社)サイバーリスク情報センター(CRIC)
大湊 健一郎	(株)NTT-ME	宮内 伸崇	(株)サイント
高橋 昌士	(株)NTT-ME	佐藤 裕二	(一社)JPCERT コーディネーションセンター
北河 拓士	NTT コミュニケーションズ(株)	持永 大	(一社)JPCERT コーディネーションセンター
斯波 彰	NTT コミュニケーションズ(株)	唐沢 勇輔	Japan Digital Design(株)
真鍋 太郎	NTT コミュニケーションズ(株)	大久保 隆夫	情報セキュリティ大学院大学
大石 眞央	(株)NTT データ	岡 邦彦	(株)スクウェア・エニックス
宮本 久仁男	(株)NTT データ	山田 宜史	(株)スクウェア・エニックス
矢竹 清一郎	(株)NTT データ	正木 義和	スワットブレインズ(株)
池田 和生	NTTデータ先端技術(株)	原子 拓	合同会社西友
植草 祐則	NTTデータ先端技術(株)	東 恵寿	NPO セカンドワーク協会
前田 典彦	(株)FFRI セキュリティ	金城 夏樹	(株)セキュアイノベーション
結城 亮史	(株)FFRI セキュリティ	栗田 智明	(株)セキュアイノベーション
岡田 祐太朗	エムオーテックス(株)	鉢嶺 光	(株)セキュアイノベーション
徳毛 博幸	エムオーテックス(株)	阿部 実洋	(株)セキュアベース
間嶋 英之	エムオーテックス(株)	林 達也	(一社)セキュリティ対策推進協議会 (SPREAD)
池田 耕作	(株)オージス総研	持田 啓司	(一社)セキュリティ対策推進協議会 (SPREAD)
大月 一孝	(株)オージス総研	上村 理	ゼットスケーラー(株)
姫野 猛	(株)オージス総研	勝海 直人	(株)ソニー・インタラクティブエンタテインメント
松本 純	サイボウズ株式会社	坂本 高史	(株)ソニー・インタラクティブエンタテインメント
岡村 耕二	九州大学	阿部 巧	ソフトバンク(株)
岡部 卓真	京セラコミュニケーションシステム(株)	中西 基裕	ソフトバンク(株)

氏名	所属	氏名	所属
楢原 盛史	タニウム合同会社	田中 秀和	(株)日立ソリューションズ
小島 博行	地方公共団体情報システム機構(J-LIS)	古賀 洋一郎	ビッグローブ(株)
八島 一司	地方公共団体情報システム機構(J-LIS)	山口 裕也	(株)ファイブドライブ
田中 卓朗	TIS(株)	大高 利夫	藤沢市役所
三木 基司	TIS(株)	中村 洋介	富士通(株)
尾﨑 尚子	DXC テクノロジー・ジャパン(株)	原 和宏	富士通(株)
前田 隆行	DXC テクノロジー・ジャパン(株)	綿口 吉郎	富士通(株)
松本 隆	(株)ディー・エヌ・エー	荒井 大輔	(株)Bridge
坂 明	デジタル庁	海老原 俊一	(株)Bridge
内山 巧	(株)電算	柳川 俊一	(株)Bridge
駒澤 悠二	(株)電算	近藤 隆雄	(株)ベリサーブ
中西 祐介	東京海上日動システムズ(株)	中根 啓佑	(株)ベリサーブ
石川 朝久	東京海上ホールディングス(株)	樅山 清	(株)ベリサーブ
小島 健司	(株)東芝	太田 良典	弁護士ドットコム(株)
田岡 聡	(株)東芝	垣内 由梨香	マイクロソフトコーポレーション
大浪 大介	東芝インフォメーションシステムズ(株)	花村 実	マイクロソフトコーポレーション
原田 博久	(株)Doctor Web Pacific	山室 太平	マカフィー(株)
大山 水帆	戸田市役所	高江洲 勲	三井物産セキュアディレクション(株)
今 佑輔	トレンドマイクロ(株)	東内 裕二	三井物産セキュアディレクション(株)
岡本 勝之	トレンドマイクロ(株)	山谷 晶英	三井物産セキュアディレクション(株)
加藤 雅彦	長崎県立大学	篠原 巧	(株)三菱総合研究所
須川 賢洋	新潟大学	平田 真由美	みゅーらぼ
柳 優	日本アイ・ビー・エム(株)	江面 祥行	(株)ユビテック
山下 慶子	日本アイ・ビー・エム(株)	島田 理枝	(株)ユビテック
高倉 万記子	(一財)日本情報経済社会推進協会(JIPDEC)	高岡 隆守	横浜市役所
初見 卓也	(一財)日本情報経済社会推進協会(JIPDEC)	牧野 尚彦	横浜市役所
淵上 真一	日本電気(株)	三国 貴正	(株)YONA
住本 順一	日本電信電話(株)	橘 喜胤	楽天ウォレット(株)
常川 直樹	パナソニック(株)	福本 佳成	楽天グループ(株)
渡辺 久晃	パナソニック(株)	伊藤 彰嗣	楽天モバイル(株)
林 薫	パロアルトネットワークス(株)	山崎 圭吾	(株)ラック
浜田 譲治	PwC コンサルティング合同会社	若居 和直	(株)ラック
古澤 一憲	PwC コンサルティング合同会社	六宮 智悟	(株)リクルート
岩佐 功	東日本電信電話(株)	木下 諒	(株)両備システムズ
小林 淳史	東日本電信電話(株)	鈴木 堅太	(株)両備システムズ
水越 一郎	東日本電信電話(株)	矢儀 真也	(株)両備システムズ
折田 彰	(株)日立システムズ	清水 秀一郎	
樋田 拓也	(株)日立システムズ	piyokango	
寺田 真敏	(株)日立製作所		
沼田 亜希子	(株)日立製作所		

著作・制作　独立行政法人情報処理推進機構（IPA）

編集責任　土屋 正

イラスト製作　株式会社 創樹

執筆協力者　10 大脅威選考会

10 大脅威執筆者　土屋 正　内海 百葉　亀山 友彦
大友 更紗　吉本 賢樹　丹野 菜美
佐々木 敬幸　佐藤 輝夫　湯澤 凱貴

IPA 執筆協力者　瓜生 和久　桑名 利幸　渡辺 貴仁
松坂 志　加賀谷 伸一郎

情報セキュリティ 10 大脅威 2022

2022 年 3 月 10 日　初 版

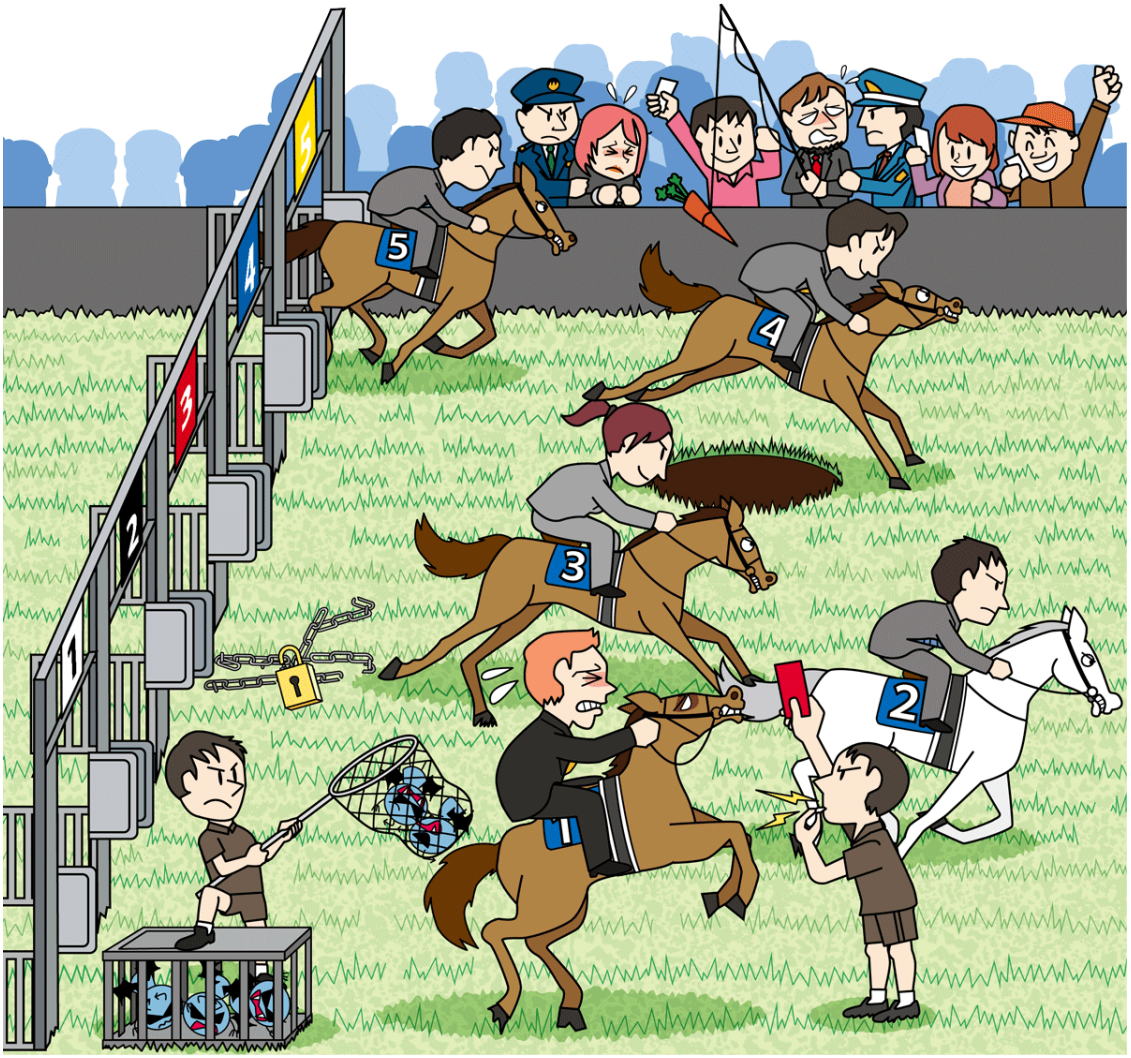
［事務局・発行］　独立行政法人情報処理推進機構

〒113-6591

東京都文京区本駒込二丁目 28 番 8 号

文京グリーンコートセンターオフィス

https://www.ipa.go.jp/



IPA 独立行政法人 **情報処理推進機構**
セキュリティセンター
〒113-6591
東京都文京区本駒込二丁目 28 番 8 号
文京グリーンコートセンターオフィス
TEL:03-5978-7527
https://www.ipa.go.jp/security/