# 情報システム等の脆弱性情報の取扱いに関する研究会

## - 2020 年度　報告書 -

2021 年 3 月

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

# はじめに

政府や IT 業界、セキュリティ機関等が我が国の情報セキュリティ確保のために協力する形で実現した情報セキュリティ早期警戒パートナーシップ（以下、「パートナーシップ」という）は、ソフトウエアの脆弱性という問題に対処する官民連携の枠組みとして機能してきた。2004 年 7 月の運用開始から 2020 年 9 月末までにソフトウエア製品及びウェブアプリケーションの脆弱性に関する届出は累計で 15,923 件に達している。パートナーシップの拠り所となる経済産業省告示は、制度発足時は「ソフトウエア等脆弱性関連情報取扱基準(2004 年経済産業省告示第 235 号改め、2014 年経済産業省告示第 110 号)」に基づいていたが、2017 年 2 月に「ソフトウエア製品等の脆弱性関連情報に関する取扱規程」（以下、「告示」という）に廃止制定された。

本年度の「情報システム等の脆弱性情報の取扱いに関する研究会」（以下、「脆弱性研究会」という）では、2015 年度に検討された基本構想であるパートナーシップ将来像の実現に向けたロードマップに則り、より迅速な脆弱性対応の実現に向けた検討などを実施し、あるべきパートナーシップの形成をめざした。また、パートナーシップに沿った取扱いの課題や現行の情報セキュリティ早期警戒パートナーシップガイドライン（以下、「P ガイドライン」という）の問題点についても、実効的に改善することをめざした。

本報告書はこれらの検討を集約した成果である。本検討にご尽力いただいた関係各位にあらためて深く御礼申し上げる。

2021 年 3 月
情報システム等の脆弱性情報の取扱いに関する研究会
座長 土居 範久

# 目　次

# 1.情報セキュリティ早期警戒パートナーシップの現状と課題

## 1.1.背景

情報セキュリティ早期警戒パートナーシップ（以下、「パートナーシップ」とする）は、独立行政法人 情報処理推進機構（Information-technology Promotion Agency, Japan；以下、IPA とする）、有限責任中間法人 JPCERT コーディネーションセンター（現在の一般社団法人 JPCERT コーディネーションセンター；以下、JPCERT/CC とする）などが中心となって、2004 年 7 月に運用を開始した。パートナーシップは、情報システム等の脆弱性について、その発見から対策の策定・公表に至るまでの過程に関与する関係者に推奨する行動基準を示すことにより、脆弱性関連情報を適切に流通させ、より迅速な対策方法の提供・適用を促す産官連携の取組みである。2004 年に制定された経済産業省告示「ソフトウエア等脆弱性情報取扱基準」が 2014 年の改正を経て、2017 年に新たに経済産業省告示「ソフトウエア製品等の脆弱性関連情報に関する取扱規程」（以下「告示」という）となったが、この告示に基づく公的な制度として運用されているという点で、国際的にも例を見ない独自の制度といえるが、その一方、脆弱性情報の取扱いは国際的な連携により実施することが必要となることから、運用面では国際的な実務とも整合する形を採用している。

## 1.2.運用の状況

パートナーシップの運用状況については、届出受付機関である IPA および JPCERT/CC から四半期毎に公表されている。以下にその詳細について示す。

### 1.2.1.届出件数

2004 年 7 月 8 日の受付開始から 2020 年 9 月末までの IPA への脆弱性関連情報の届出件数は、ソフトウエア製品の脆弱性に関するもの 4,627 件、ウェブサイトの脆弱性に関するもの 11,296 件の計 15,923 件であった。四半期毎の届出状況を図 1-1に示す。

| | 2017 4Q | 2018 1Q | 2Q | 3Q | 4Q | 2019 1Q | 2Q | 3Q | 4Q | 2020 1Q | 2Q | 3Q |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 累計届出件数[件] | 13,526 | 13,664 | 13,822 | 13,999 | 14,090 | 14,213 | 14,710 | 15,055 | 15,227 | 15,488 | 15,676 | 15,923 |
| 1就業日あたり[件/日] | 4.11 | 4.08 | 4.06 | 4.03 | 3.99 | 3.96 | 4.03 | 4.06 | 4.04 | 4.04 | 4.03 | 4.03 |

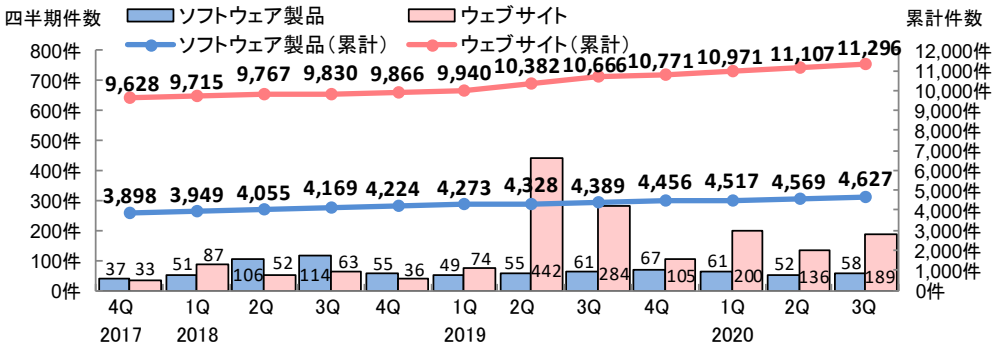
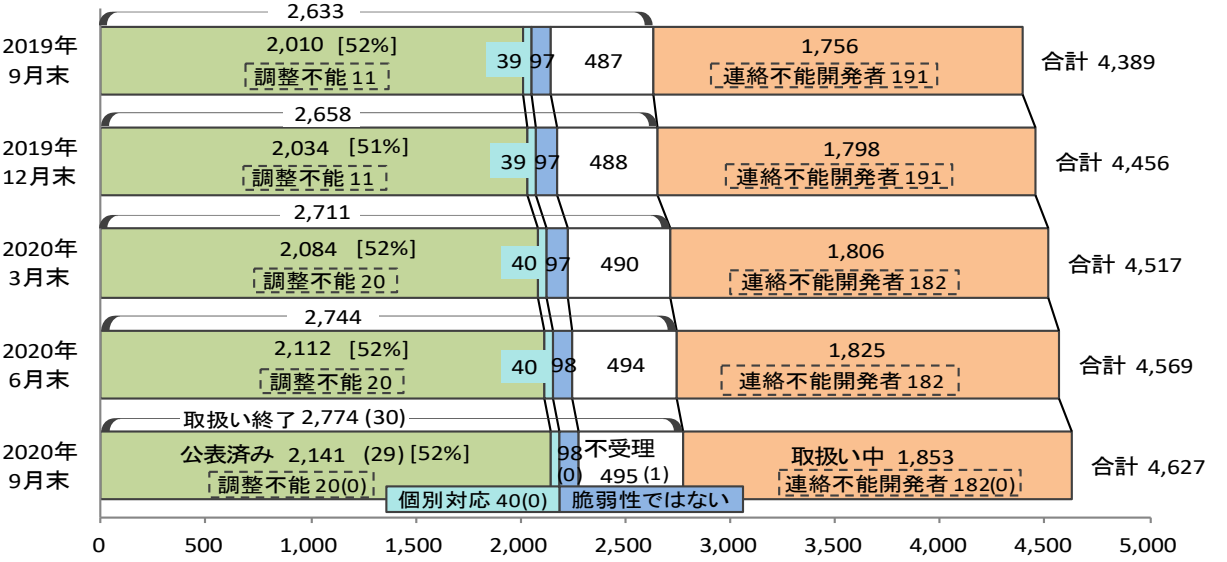



**図 1-1　四半期ごとの届出状況**

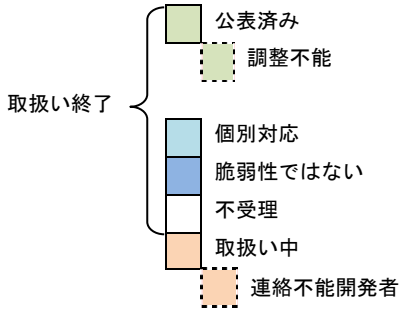
（活動報告レポート[2020 年第 3 四半期（7 月～9 月）]より抜粋）

### (1) ソフトウエア製品の脆弱性

ソフトウエア製品の脆弱性関連情報届出に関する処理状況を図 1-2 に示す。




*( )内の数値は今四半期に処理を終了もしくは連絡不能開発者となった件数*
*[ ]内の数値は受理した届出のうち公表した割合*




：JVN で脆弱性への対応状況を公表したもの

：公表判定委員会による判定にて、JVN で公表することが適当と判定されたもの

：JVN 公表を行わず、製品開発者が個別対応したもの

：製品開発者により脆弱性ではないと判断されたもの

：告示で定める届出の対象に該当しないもの

：IPA、JPCERT/CC が内容確認中、製品開発者が調査、対応中のもの

：取扱い中のうち、連絡不能開発者一覧にて公表中のもの

**図 1-2　ソフトウエア製品の脆弱性関連情報の届出の処理状況**

（活動報告レポート[2020 年第 3 四半期（7 月～9 月）]より抜粋）

ソフトウエア製品の脆弱性関連情報の届出 4,627 件のうち、IPA と JPCERT/CC が共同運営する脆弱性対策情報ポータルサイト JVN[1]において脆弱性が公表されているもの（公表済み）が 2,141 件、製品開発者からの届出のうち製品開発者が個別対応したものが 40 件、製品開発者により脆弱性ではないと判断されたものが 98 件、取扱い中のものが 1,853 件となっている。また、告示で定める脆弱性に該当しないため、届出の対象外（不受理）としたものが 495 件ある。

### (2) ウェブサイトの脆弱性

ウェブサイトの脆弱性関連情報の届出に関する処理状況を図 1-3 に示す。

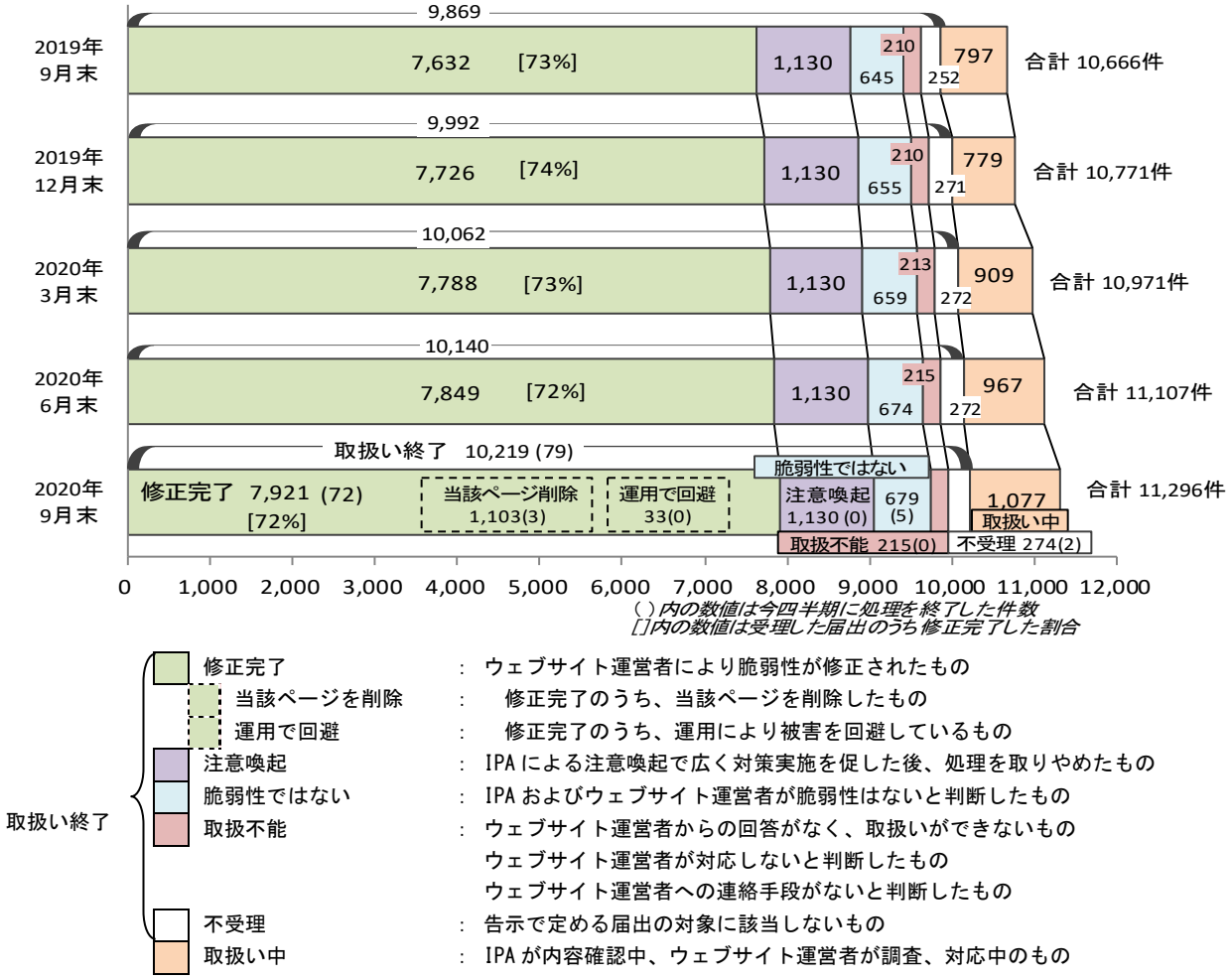



**図 1-3　ウェブサイトの脆弱性関連情報の届出の処理状況**

（活動報告レポート[2020 年第 3 四半期（7 月～9 月）]より抜粋）

ウェブサイトの脆弱性関連情報の届出 11,296 件のうち、修正が完了したものが 7,921 件（うち運用で回避されたもの 33 件、当該ページを削除して対応したもの 1,103 件）、IPA による注意喚起で広く対策を促した後、処理をとりやめた

[1] Japan Vulnerability Notes (https://jvn.jp/)

もの 1,130 件、IPA およびウェブサイト運営者が脆弱性ではないと判断したものが 679 件、取扱い中のものが 1,077 件となっている。この他、ウェブサイト運営者と連絡が取れないもの（取扱不可能）が 215 件、告示で定める脆弱性に該当しないため、届出の対象外（不受理）としたものが 274 件ある。

## 1.2.2. ソフトウエア製品の脆弱性関連情報の届出の内容

JPCERT/CC が国内の製品開発者との調整や海外 CSIRT（Computer Security Incident Response Team）[2]との協力に基づき JVN において公表した脆弱性は 2020 年 9 月末までに 3,739 件になる。

### (1) 国内の発見者および製品開発者から届出があり公表した脆弱性

2020 年 9 月末までに、国内の発見者から IPA に届出があったもの及び製品開発者自身から自社製品の脆弱性・対策方法について連絡を受けたもので、JVN において公表された脆弱性は 2,141 件である。届出受付開始から 2020 年 9 月末までの届出について、脆弱性関連情報の届出を受理してから製品開発者が対応状況を公表するまでに要した日数を図 1-4 に示す。45 日以内に公表されている件数は全体の 29%であり、公表までに時間を要している割合が大きい。

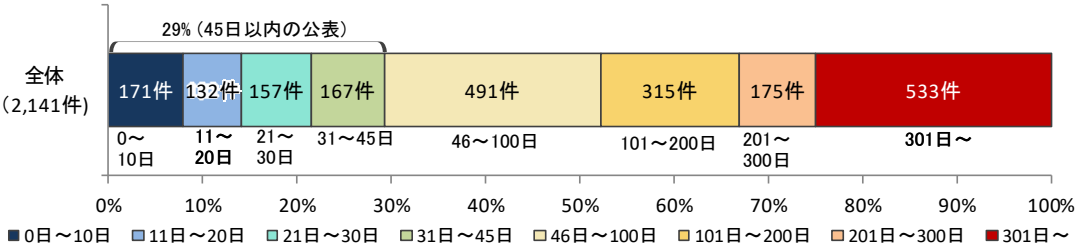



**図 1-4　ソフトウエア製品の脆弱性公表までに要した日数**

（活動報告レポート[2020 年第 3 四半期（7 月～9 月）]より抜粋）

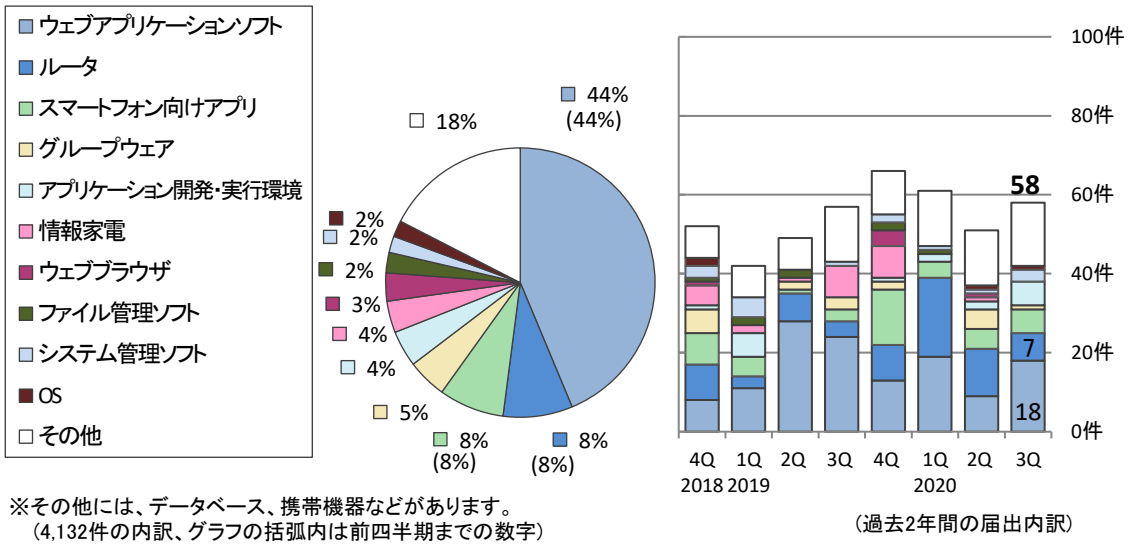
### (2) 海外 CSIRT から連絡を受け公表した脆弱性

2020 年 9 月末までに JPCERT/CC が海外 CSIRT 等と連携して JVN で公表した脆弱性情報は 1,919 件である。このうち、2020 年度第 3 四半期（2020 年 7 月から 2020 年 9 月末まで）に JVN で公表した脆弱性関連情報は 75 件であった。

### (3) 製品種類別の内訳

届出受付開始から 2020 年 9 月末までのソフトウエア製品に関する脆弱性関連情報の届出 4,627 件のうち、不受理分を除いた 4,132 件の製品種類別内訳を図 1-5 に示す。「ウェブアプリケーションソフト」が 44%を占めている。

[2] コンピュータセキュリティに関するインシデント（事故）への対応や調整、サポートをするチーム。




※その他には、データベース、携帯機器などがあります。
（4,132件の内訳、グラフの括弧内は前四半期までの数字）

**届出累計の製品種類別割合**

（過去2年間の届出内訳）

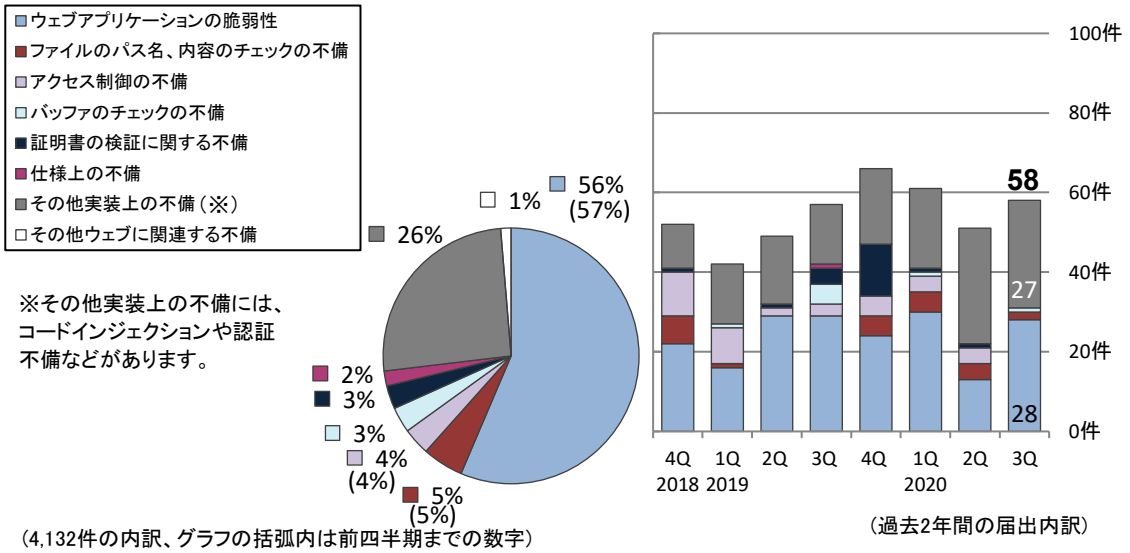
**四半期ごとの製品種類別届出件数**

**図 1-5　ソフトウエア製品種類別の届出内訳（届出受付開始～2020 年 9 月末）**

（活動報告レポート[2020 年第 3 四半期（7 月～9 月）]より抜粋）

## (4) 脆弱性の原因別の内訳

届出受付開始から 2020 年 9 月末までのソフトウエア製品に関する脆弱性関連情報の届出 4,627 件のうち、不受理のものを除いた 4,132 件の原因別の内訳を図 1-6 に示す。脆弱性の原因は「ウェブアプリケーションの脆弱性」が 56%を占める。




（4,132件の内訳、グラフの括弧内は前四半期までの数字）

**届出累計の脆弱性の原因別割合**

（過去2年間の届出内訳）

**四半期ごとの脆弱性の原因別届出件数**

**図 1-6　ソフトウエア製品の脆弱性原因別の届出内訳（届出受付開始～2020 年 9 月末）**

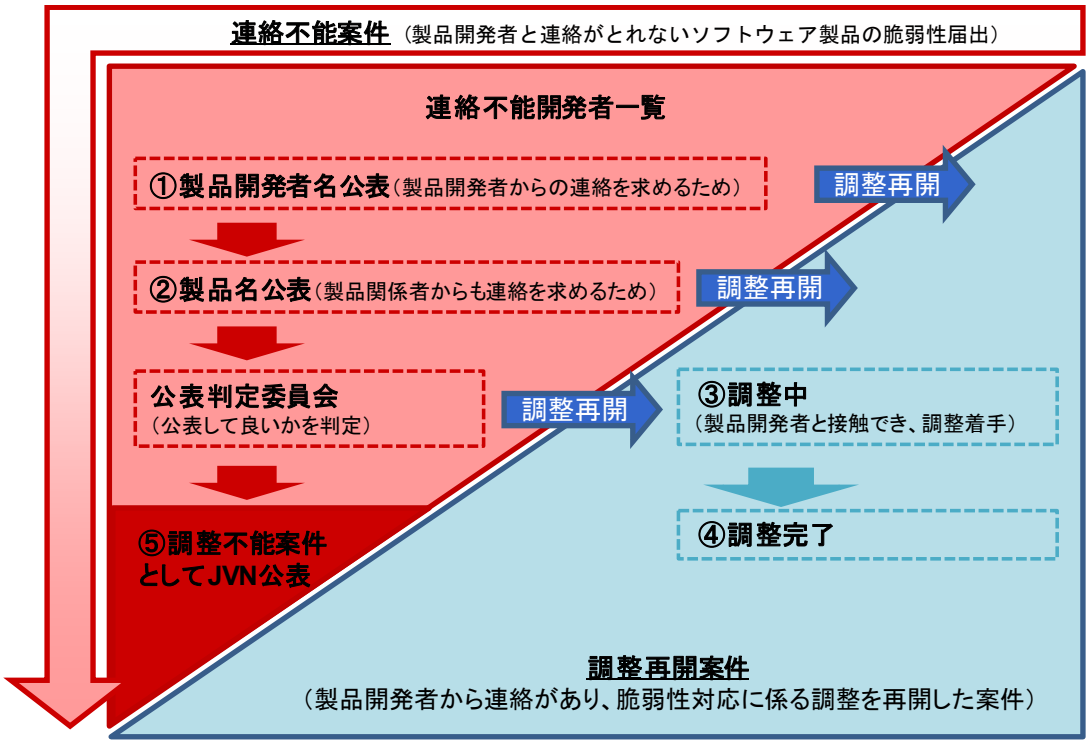
（活動報告レポート[2020 年第 3 四半期（7 月～9 月）]より抜粋）

### (5) 優先情報提供の実施状況

2018 年 4 月から、脆弱性による国民の日常生活に必要不可欠なサービスへの被害を低減するために、これらのサービスを提供する重要インフラ事業者 に対して脆弱性対策情報を JVN 公表前に優先的に提供している。2020 年度第 1 四半期から第 3 四半期に優先情報提供したものは電力分野 7 件、政府機関 5 件で、累計では 18 件（電力分野 10 件、政府機関 8 件）でした。

### (6) 連絡不能案件の処理状況

連絡不能開発者一覧の公表開始（2011 年 9 月 29 日）から 2020 年 9 月末までに公表した連絡不能開発者の件数は累計 251 件、うち 49 件が調整を再開（その中の 26 件が調整完了）したが、182 件は製品開発者と連絡がとれない状況にある（図 1-7参照）。




| | | | | |
|---|---|---|---|---|
| 2020年<br>第2四半期 | 182件<br>（①1件 ②181件） | 49件<br>（③23件 ④26件） | ⑤ 20 件 | 合計<br>251件 |
| 2020年<br>第3四半期 | 182件<br>（①1件 ②181件） | 49件<br>（③23件 ④26件） | ⑤20 件 | 合計<br>251件 |

**図 1-7 連絡不能案件の処理状況（連絡不能開発者一覧公表開始～2020 年 9 月末）**

（活動報告レポート[2020 年第 3 四半期（7 月～9 月）]より抜粋）

## 1.2.3. ウェブサイトの脆弱性関連情報の届出の内容

### (1)修正された脆弱性の内容

2020 年 9 月末までに届出されたウェブサイトの脆弱性のうち修正の完了した 7,921 件について、IPA からウェブサイト運営者に脆弱性関連情報の詳細を通知してから、修正されるまでに要した日数を、脆弱性の種類別にまとめたものを図 1-8 に示す。全体の 49%の届出が 30 日以内、67%の届出が 90 日以内に修正されている。

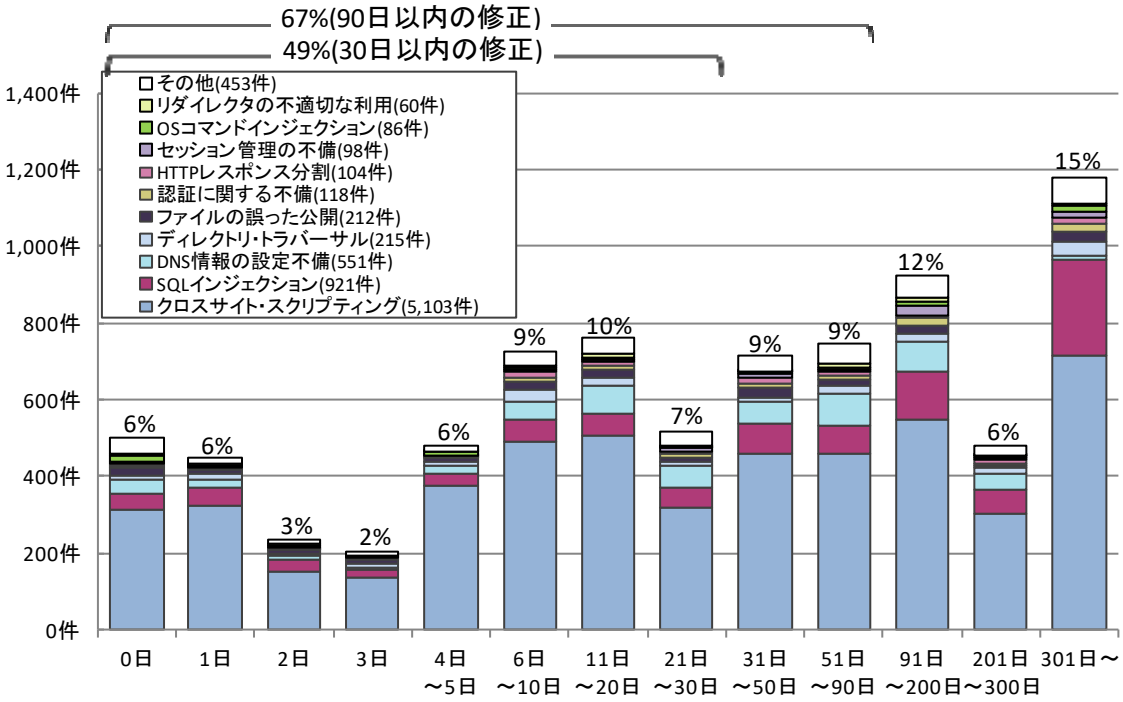
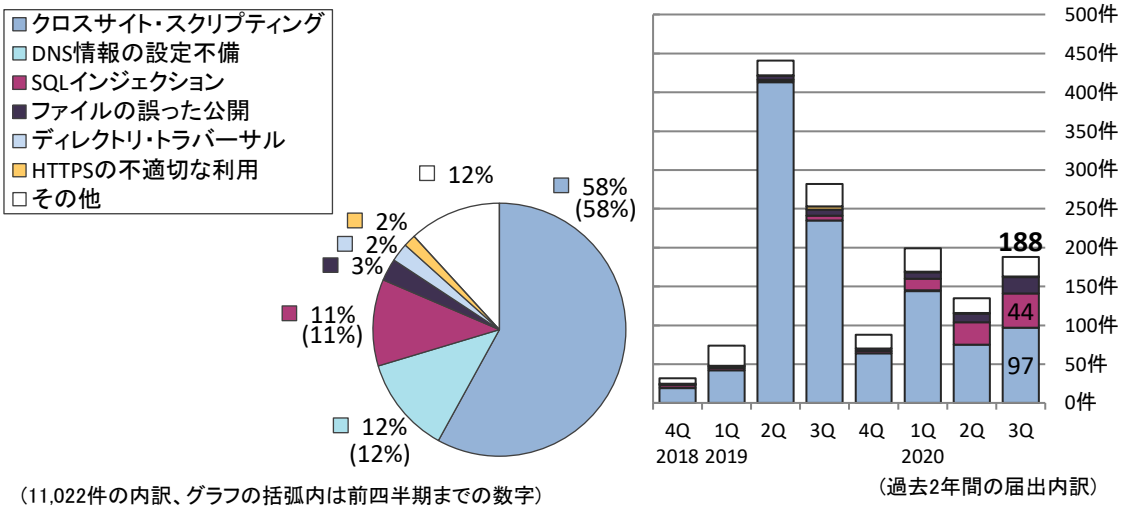



**図 1-8　ウェブサイトの脆弱性修正に要した日数（届出受付開始～2020 年 9 月末）**

（活動報告レポート[2020 年第 3 四半期（7 月～9 月）]より抜粋）

### (2)届出の脆弱性種類別内訳

2020 年 9 月末までに IPA に届出のあったウェブサイトに関する脆弱性関連情報の届出 11,296 件のうち、不受理のものを除いた 11,022 件の種類別内訳を 図 1-9 に示す。脆弱性の種類は依然として「クロスサイト・スクリプティング」(58%)、「DNS 情報の設定不備」(12%)、「SQL インジェクション」(11%)の割合が高く、この３つだけで全体の 81%を占める。




(11,022件の内訳、グラフの括弧内は前四半期までの数字)

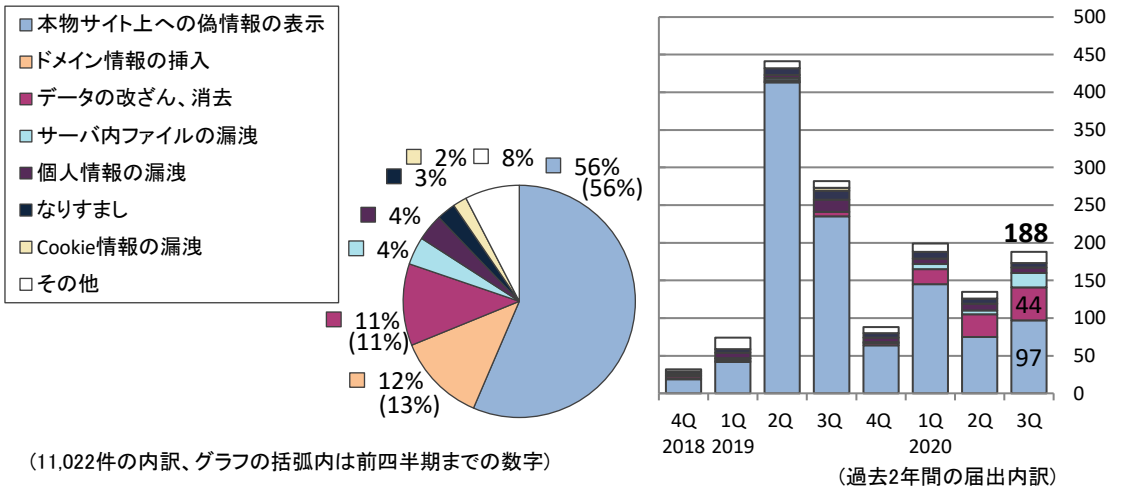
**届出累計の脆弱性の種類別割合**　　**四半期ごとの脆弱性の種類別届出件数**

**図 1-9　ウェブサイトの脆弱性種類別内訳（届出受付開始～2020 年 9 月末）**

（活動報告レポート[2020 年第 3 四半期（7 月～9 月）]より抜粋）

### (3) 届出の脆弱性脅威別内訳

届出のあった脆弱性から想定される脅威別内訳を図 1-10 に示す。脆弱性から想定される脅威としては、「本物サイト上への偽情報の表示」(56%)、「ドメイン情報の挿入」(12%)、「データの改ざん、消去」(11%) の割合が高い。




(11,022件の内訳、グラフの括弧内は前四半期までの数字)

**届出累計の脆弱性がもたらす影響別割合**　　**四半期ごとの脆弱性がもたらす影響別届出件数**

**図 1-10　ウェブサイトの脆弱性脅威別内訳（届出受付開始～2020 年 9 月末）**

（活動報告レポート[2020 年第 3 四半期（7 月～9 月）]より抜粋）

### (4)取扱の状況

ウェブサイトの脆弱性関連情報のうち、取扱いが長期化（IPA からウェブサイト運営者へ脆弱性関連情報を通知してから、90 日以上脆弱性を修正した旨の報告が無い）しているものに関する経過日数別の件数を図 1-11 に示す。経過日数が 90 日以上である件数は 409 件で、前年同期（391 件）に比べ増加している。深刻度の高い SQL インジェクションが全体の約 17%を占めており、対策の実施が望まれる。

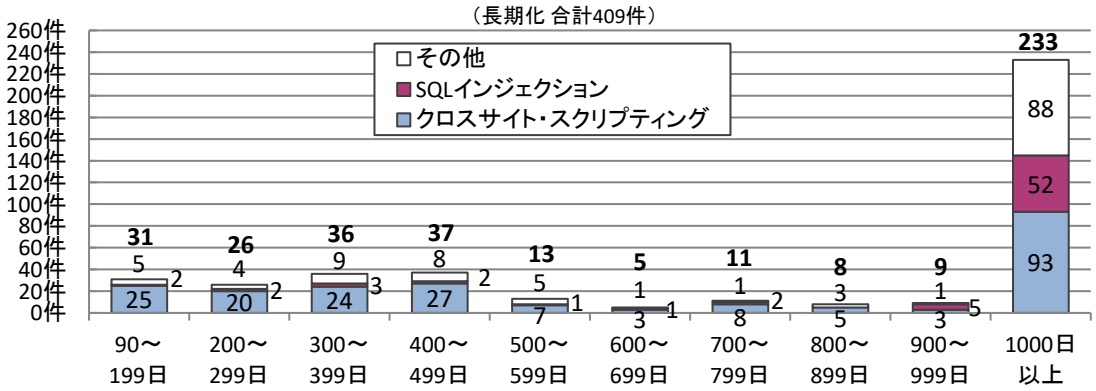



**図1-11. 取扱いが長期化(90日以上経過)している届出の取扱経過日数と脆弱性の種類**

（活動報告レポート[2020 年第 3 四半期（7 月～9 月）]より抜粋）

## 1.3. 本年度研究会における検討

本年度の脆弱性研究会は以下の 2 項目に整理して検討を進めた。以降の章では、これらに関する検討成果を示す。

①小規模のウェブサイト運営者向け脆弱性対策支援
・小規模ウェブサイト運営者の脆弱性対策に関する調査
（アンケート調査）
・ウェブサイトの最近の被害事例に関する調査
（文献調査、ヒアリング調査）
・企業ウェブサイトのための脆弱性対応ガイドの改訂要否の検討

②パートナーシップの運用改善の対応方針検討
・海外の政府機関等における脆弱性対策の取組みに関する調査
・パートナーシップの運用改善の対応方針

# 2. 小規模ウェブサイト運営者の脆弱性対策に関する調査

## 2.1. 調査の概要

### (1) 目的

ウェブサイトの脆弱性対処について、ウェブサイト運営者としての責務（望ましい対処）であることが認識されるよう普及啓発を実施してきている。しかし、パートナーシップでのウェブサイトに関する届出や修正対応の状況を踏まえると、特に小規模ウェブサイト運営者において脆弱性対策を進めるうえで課題があると推測される。

このため、ウェブサイトでの適切な脆弱性対処の実現をめざすため、小規模ウェブサイト運営者における脆弱性対処の現状に関するアンケート調査を行った。その結果から導き出されるウェブサイト運営者としての課題を抽出するとともに、課題への対処方法をこれまでの脆弱性研究会での調査結果も踏まえて検討した。

調査結果及び検討結果は、「小規模ウェブサイト運営者の脆弱性対策に関する調査報告書」として取り纏めた。また、これらの結果は、ウェブサイトの最近の被害事例に関する調査の調査結果と合わせて「企業ウェブサイトのための脆弱性対応ガイド」の改訂の要否及び改訂の内容を検討するにあたって参考とし、その改訂する内容が本調査で抽出できた課題の解消に資するものとなるようにした。

### (2) 手順

企業モニターを対象としたウェブアンケート調査を行った。調査精度を向上させるため、調査モニターの IT 担当者等に対してプレ調査を行い、回答者の中からウェブサイト運営に関与する者を抽出した上で本調査を実施した。

［調査方法］ウェブアンケート調査（企業モニター）

［調査対象］国内の小規模ウェブサイト担当者や情報システム担当者
小規模とは、中小企業基本法において定義された「小規模企業者」（おおむね常時使用する従業員が 20 人以下、商業・サービス業で従業員 5 人以下の事業者）を含むよう、従業員が 50 名以下の企業を対象とした。

［有効回収数］301 件（本調査）

［調査項目］調査の主な設問項目は以下の通りである。

・ウェブサイトの構築・運用の形態や内容
・脆弱性対策への理解
・脆弱性対策の現状と課題
・IPA の普及啓発資料に関する認知度（活用度）

## 2.2.小規模のウェブサイト運営に関するアンケート調査

アンケート調査の詳細は「小規模ウェブサイト運営者の脆弱性対策に関する調査報告書」に示す。以下に、アンケート調査から得られた知見を取りまとめる。

### (1)調査仮説の検証

a）ウェブサイトの構築・運用の実態

（仮説 1）自社社員が少人数（ほぼ 1 名）で運用者が不明確

ウェブサイトにトラブルが生じたときに「自身がトラブルに対処する」と答えた回答者は全体の 44.5%であった。（予備調査 問 9）

また、ウェブサイトのセキュリティ管理を「組織的には行っていない」小企業は 39.1%であった。他方で「担当者がいる」小企業は 32.7%、「主担当業務以外にウェブサイトのセキュリティ管理を兼任する担当者がいる」小企業は 15.7%となり、担当者がいると答えた回答を合計すると 48.4% となった。（本調査 問 9）

これらの結果から、半数程度で担当者が定まっており、仮説は必ずしも正しいとは言えないが、少人数でウェブサイトの運用をしている様子が伺われる。

なお、ウェブサイトの脆弱性対策・セキュリティ対策に必要な費用や人員については、充分に確保できているが 6.0%、おおむね確保できているが 34.9%と確保できている率は合計 40.9%、やや不足しているが 24.3%、全く足りてないが 13.3%と確保できていない率は合計 37.6%という結果であった。（本調査 問 25）

（仮説 2）構築および運用の方針は経営者が決定

ウェブサイトの運用・構築についてのトップ（社長や経営陣）の関与の状況は、「トップ自らが運用・構築にあたっている」小企業が 35.5%であった。この割合は従業員数 5 人以下の企業では 56.8%であったが、6 人～30 人の企業では、8.7%だった。また、「積極的に担当者に指示を出す」小企業は、全体で 20.3%であり、5 人以下の企業では 14.2%、6 人～30 人の企

業では、29.8%であった。(本調査 問 5)

脆弱性対策等のセキュリティ対策の適用について「組織のトップ」が判断する小企業は 37.2%であった。(本調査 問 22)

これらの結果から、仮説は必ずしも正しいとは言えないが、より小規模な組織ほど、経営層が関わっている様子が伺える。

(仮説 3) セキュリティ対策は運用段階の対策を実施している

脆弱性対策の実施状況については、「構築時も運用時も脆弱性対策をしている」小企業が全体の 48.8%と最も多く、次いで「運用時にのみ対策をしている」小企業が 22.9%であった。「構築時にのみ対策をしている」小企業は皆無に近い状態 (2.0%) であった。(本調査 問 17 および本調査 問 19)

これらの結果から、運用時に対策が行われている様子が伺えた。また、「一切対策をしていない」小企業も 16.6%と多くあった。

b) 脆弱性対策への理解

(仮説 4) 脅威を認識しておらず危機感がない (主に大企業が狙われており小企業は攻撃されないという考え)

(仮説 5) 脆弱性対策が脅威への根本的解決策となることを理解していない

ウェブサイトの機能・画面について、脆弱性対策が必要となる例を挙げて質問したところ、半数以上の小企業のウェブサイトには脆弱性対策が必要と考えられる機能・画面が備えられていた。(予備調査 問 10)

ウェブサイトの脆弱性について知っているか尋ねたところ、約 25～30%は詳しく知っており、約 40%は聞いたことがあるという結果を得た。(本調査 問 11)

脆弱性対策を行わないと答えた者にその理由を尋ねたところ、「個人情報を扱っていない」(51.8%)「クレジットカード等の決済を行っていない」(38.6%) という理由が挙げられていた。「サイトが著名でないので、被害に遭うとは考えにくいから」も理由として挙げられているが 27.7%であり、「小企業は攻撃されない」という考え以外の理由もあることが伺われる。(本調査 問 20)

さらに、国内のウェブサイトへの脆弱性を悪用した攻撃などによって企業や組織が被害を受けていることを知った時の行動としては、「被害事例を参考に対策を実施したいが十分にできていない」が 46.2%、「被害事例は気になるが何もしない」が 24.9%で、合計 71.1%という結果であった。(本調査 問 12)

これらから、脆弱性については一定の脅威として認識している場合もあ

るが、ウェブサイトに積極的に対策を行う強い必要性が認められないため対策を行わないという状況が伺える。

c) 脆弱性対策の現状と課題

(仮説 6) ウェブサイトを一時停止し修正作業が必要な脆弱性対策を行うことに消極的

ウェブサイトに脆弱性対策などのセキュリティ対策を進める上での課題について尋ねたところ、「脆弱性を修正すると、ウェブ上のアプリケーションが動かなくなる可能性がある」、「脆弱性の問題でサービスを止めると、顧客を失ってしまう」のいずれの項目についても、「特に課題ではない」とする回答が 46.2%、52.8%と約半数となった。これらよりも「脆弱性やセキュリティに関する技術の習得が難しい」(74.4%)や「脆弱性やセキュリティに関する情報が多すぎて選別が難しい」(64.1%)の方が課題と認識されていることが伺われる。(本調査 問 26(6)(8))

このことから、仮説は必ずしも正しいとは言えず、脆弱性の修正に消極的な理由としては、ウェブ上のアプリケーションが動かなくなるやサービスを止めると顧客を失ってしまうことではなく、予算、人材不足、技術習得の難しさが理由として大きい様子が伺える。

(仮説 7) ウェブサイトのセキュリティ対策へ費やす予算や人手が十分ではない

費用と人員の確保状況について、「十分に確保できている」(6.0%)、「おおむね確保できている」(34.9%)とする回答を合わせると約 40%であった。一方、「やや不足している」(24.3%)、「まったく足りていない」(13.3%)とする回答も合わせて 40%近くであった。「わからない」とする回答が 21.6%と多く、適正なコストを見積もれない状況が伺える。(本調査 問 25)

予算と人員の確保について課題とみなす回答は全体の約 60%であった。(本調査 問 26(1)(3))

(仮説 8) セキュリティ技術が担当者には難しく理解し難い

ウェブサイト担当者の選定理由をたずねたところ、「パソコンに詳しい／慣れているから」とする回答が最も多く (52.5%)、ついで「デザインができるから」「運営や管理ができるから」といった理由が挙げられた。(本調査 問 8)

「脆弱性やセキュリティに関する技術の習得が難しい」ことを課題として挙げる回答は全体の約 70%であった。(本調査 問 26(2))

これらから、小企業のウェブサイトの運営に関与する経営者や担当者にとって、脆弱性やセキュリティに関する技術が難しく、理解が及んでいない様子が伺えた。

(仮説 9) トラブルが生じても脆弱性対策による根本的な解決は行われない

脆弱性に起因する被害経験について尋ねたところ、「業務に影響が生じる被害が発生した」という回答が全体の 5.0%、「実害が発生したことはないが被害に遭ったことはある」という回答が 15.3%あった。これらを合わせ約 20%の回答者が被害に遭ったと答えている。(本調査 問 23)

運用中のウェブサイトに脆弱性が発見された場合に「特に脆弱性対策は取らない」とする回答は全体の 13.6%であった。(本調査 問 24)

運用中のウェブサイトの脆弱性対策については、運用における脆弱性対策はしていないとする回答は全体の 13.3%であった。(本調査 問 19)

また、脆弱性に起因する被害経験「業務に影響が生じる被害が発生した」、「実害が発生したことはないが被害に遭ったことはある」という回答者について、脆弱性の発見時の対応に関してクロス集計した結果、「可能な限り速やかに修正を行っている」が全体で 47.5%、「脆弱性が発見されたら、その深刻さについて調べ、対処方法を検討する」が全体で 29.5%であった。(本調査 問 19 と問 23)

これらから、仮説は必ずしも正しいとはいえず、脆弱性発見等のトラブルが生じた場合に一定数は修正対応をするといえるが、そうでない場合も一定数あることが伺われる。

d) IPA の普及啓発資料に関する認知度

(仮説 10) 無償で利用可能な良いコンテンツがあるならば利用したい

情報セキュリティ早期警戒パートナーシップの取組みについて尋ねたところ、聞いたことがあるとした回答は約 50%であった。(本調査 問 27)

IPA による脆弱性関連の情報等の認知状況については、約 20～40%ほどが聞いたことがあるとしている。(本調査 問 28)

ウェブサイトのセキュリティ対策の運用・管理、セキュアなウェブサイトの構築、最近のウェブサイトに関するセキュリティ脅威の動向などの情報セキュリティに関する普及啓発コンテンツを利用してみたいかを尋ねたところ、何らかのコンテンツを利用してみたいと答えた回答が約 70%であった。

e) ウェブサイトの対策・重要性の変化

（仮説 11）基本的なセキュリティ対策は、10 年前と比較しても変化せず、実施している中小企業は少ない

ウェブサイトでの基本的な脆弱性対策の実施について尋ねたところ、「ソフトウェアの定期的な更新」は 30.2%が実施したことはないという結果であったが､「定期的な設定の見直し」を実施したことがないが 46.2%、「脆弱性（脅威、手口など）の最新情報取得」は 50.2%が実施したことがないという回答となり、半数程度の実施率であった。（本調査 問 13）

なお、構築年数による脆弱性対策の大きな変化はなかった。（問 7 と問 15）

これらから、実施も不実施も半数程度であり、仮説は必ずしも正しいとはいえない状況であることが伺われる。

（仮説 12）ウェブサイトの役割や重要性が高まっているが、脆弱性対策やセキュリティ対策にかけるコストは変わらない

ウェブサイトの重要性・事業影響度の変化について尋ねたところ、「変わらない」という回答が 46.2%、「大幅に高まった」、「高まった」という回答の合計は 42.5%であり、「重要性が低下した」という回答は少なく、変わらないまたは重要性が高まったという回答が多い傾向にある。（本調査 問 6）

また、この 10 年程度のウェブサイトのセキュリティ対策コストの増減については、「変わらない」が 63.8%であり、この 10 年程度のウェブサイトの構築コストの増減についても「変わらない」が 58.8%、この 10 年程度のウェブサイトの運用コストの増減についても「変わらない」が 61.8%であった。（本調査 問 14、16、18）

これらから、ウェブサイトの役割や重要性が高まっているが、脆弱性対策やセキュリティ対策にかけるコストは変わらない結果であった。

f) クラウド利用対策及び複数・複合的な対策

（仮説 13）クラウド等のサービス利用時に、セキュリティ対策は、サービス提供事業者が対応しているので、自組織の対応が不要と思っている

開発・構築及び運用・管理で利用しているサービスのセキュリティ対策について自社の責任範囲とサービス提供者の責任範囲が明確になっているかについて尋ねた。全体としては、「明確になっている」が 49.7%と最も多いが、次いで「明確になっていない」が 36.9%との回答であり、委託先やサービス提供者との責任範囲は約 40%が明確になっていない状況

であった。また、従業員数別でも同様の傾向であった。(本調査 問 4)

この結果から、仮説は必ずしも正しいとは言えないが、責任範囲が不明であり、自組織と委託先やサービス提供者のどちらで対応すべきか明確になっていない状況が伺える。

(仮説 14) 運用時の脆弱性対策として何らかの対応が実施されてはいるが、複数の対策による複合的な対応まではなされていない

ウェブサイトの運用時に実施しているセキュリティ対策や脆弱性対策について尋ねたところ、問 15 で確認した 7 項目について、全項目で対策をしていない者は 24.9%、一つの対策を実施しているのは 4.3%、二つは 5.3%、三つは 7.0%、四つは 7.3%、五つは 6.6%、六つは 5.6%で、全項目七つを実施しているのは 38.9%であった。(問 15・複数対策)

この結果から、仮説は誤りであり、二つ以上の複数の対策が実施されていることが伺われる。

## 2.3.企業ウェブサイトのための脆弱性対応ガイドの改訂

小規模ウェブサイト運営に関するアンケート調査の結果を基に企業ウェブサイトのための脆弱性対応ガイドの改訂に盛り込むべき情報を検討した結果を報告する。

### (1)小規模ウェブサイト運営者の意識について

ウェブサイトに脆弱性対策などのセキュリティ対策を進める上での課題として、「脆弱性やセキュリティに関する技術の習得が難しい」を課題として認識している運営者は(重要な課題、課題のひとつのとの回答を合わせ)約 70%、同様に「脆弱性やセキュリティに関する情報がどこにあるかわからない」は約 60%等と高い(問 26)。そのため、「企業ウェブサイトのための脆弱性対応ガイド」に小規模ウェブサイトの運営者向けに、脆弱性や脆弱性対策に必要となる情報を集約し、基礎的な情報から技術習得が可能な情報を提供する必要がある。

### (2)啓発について

脆弱性対策・セキュリティ対策に関する IPA の提供情報は約 60%から 80%が認知していない状況(問 28)であるが、今回のアンケート調査結果で求められる情報を提供し、啓発を促進することが考えられる。ウェブサイトの脆弱性を悪用した攻撃によって組織が被害を受けている情報を「参考にしたい」が約 70%と高い(問 12)ため、「企業ウェブサイトのための脆弱性対応ガイド」に具体的な被害情報を提供する必要がある。

### (3)社会環境について

従業員 5 人以下の組織、従業員 6 人～30 人以下の組織ともに「自社で運用・管理」「ホスティング利用」が減少し、「クラウド利用」が増加している（問 3）。これらのことから、自組織のみで運用や対策を行うのではなく、外部サービスも利用することが多くなってきているため、「企業ウェブサイトのための脆弱性対応ガイド」にクラウドサービスの利用や外部委託先に依頼する際に検討すべき点を提供する必要がある。

### (4)制度運用について

「情報セキュリティ早期警戒パートナーシップ」の取組みを「聞いたことがない」は 2012 年度調査と今回調査で約 50%と高い（問 27）状態で変化がなく、脆弱性情報の届出を受け付け、コーディネーションしていることが広く認識されていない。パートナーシップの認知度を向上させ、望ましい脆弱性対処の方法についてウェブサイト運営者に認識させることで、パートナーシップでの対応がより早期に、より適切に実施できるようにすることが望ましい。

# 3. ウェブサイトの最近の被害事例に関する調査

## 3.1. 調査の概要

### (1) 目的

ウェブサイトの脆弱性対策については、ウェブサイト運営者に対して、脆弱性対策の必要性について普及・促進を実施しているが、ウェブサイトの脆弱対策の必要性が理解されにくい状況である。そこで、脆弱性対策の必要性を理解して頂くためには、脆弱性を放置していると被害が発生することを示すことが効果的と考え、実際に発生したウェブサイトの被害事例を調査して資料として取り纏め、「企業ウェブサイトのための脆弱性対応ガイド」の改訂に利用する。

### (2) 手順

a) 文献調査

これまでの脆弱性研究会での調査結果を踏まえ、脆弱性に起因すると思われる主に下記のような被害を受けた国内組織の被害事例を文献等により調査した。

［調査対象］以下の被害を受けた者を対象とする。

- ・ウェブサイトの改ざん被害
- ・ウェブサイトのサービス停止被害
- ・ウェブサイトからの情報漏えい被害
- ・上記の一次被害による風評被害や金銭被害等の二次被害　等

［調査件数］国内組織の被害事例 10 件以上

［調査項目］調査の主な項目は以下の通りである。

- ・発生した被害の内容と影響範囲
- ・発生した被害の直接原因、根本原因
- ・発生した被害の技術的な原因、人員的な原因
- ・被害発生後に実施した対策
- ・今後被害を発生させないために実施した脆弱性対策を含む対策　等

b) ヒアリング調査

文献調査した被害事例等も参考に、被害対象者に対して、文献調査では調査しきれない事項について、ヒアリング調査を実施した。

［調査対象］調査対象の被害は以下の通りである。

・ウェブサイトの改ざん被害
・ウェブサイトのサービス停止被害
・ウェブサイトからの情報漏えい被害
・上記の一次被害による風評被害や金銭被害等の二次被害　等

［調査件数］国内組織の被害事例 5 件以上

［調査項目］調査の主な設問項目は以下の通りである。

・発生した被害の内容と影響範囲
・発生した被害の直接原因、根本原因
・発生した被害の技術的な原因、人員的な原因
・被害発生後に実施した対策
・今後被害を発生させないために実施した脆弱性対策を含む対策　等

## 3.2. 文献調査結果

文献調査結果の概要を以下に報告する。

**表 3-1　文献調査結果**

| No | 公表日・属性等 | | | | 調査対象被害 | | | | 調査項目 | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 公表日 | 企業・団体名 | 企業規模 | Cloud 利用 | 1.改ざん | 2.サービス停止 | 3.情報漏えい | 4.風評被害/二次被害 | 1.内容と影響範囲 | 2.直接・根本原因 | 3.技術的・人員的原因 | 4.発生後の対応策 | 5.再発防止策 |
| 1 | 2020 年 1 月 15 日 | 企業 A | 小 | × | ○ | × | ○ | ○ | ○ | ○ | × | ○ | ○ |
| 2 | 2019 年 9 月 12 日 | 企業 B | 中 | × | ○ | × | ○ | ○ | ○ | ○ | × | ○ | ○ |
| 3 | 2020 年 6 月 11 日 | 企業 C | 中 | × | ○ | △ | × | × | ○ | ○ | × | ○ | ○ |
| 4 | 2020 年 6 月 23 日 | 企業 D | 小 | × | ○ | ▲ | ○ | ○ | ○ | ○ | × | ○ | ○ |
| 5 | 2019 年 12 月 5 日 | 企業 E | 大 | × | × | × | ○ | ○ | ○ | ○ | × | ○ | ○ |
| 6 | 2020 年 10 月 23 日 | 企業 F | 中 | × | ○ | ▲ | ○ | × | ○ | ○ | × | ○ | ○ |
| 7 | 2018 年 5 月 17 日 | 企業 G | 大 | × | × | ▲ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| 8 | 2019 年 1 月 25 日 | 企業 H | 大 | × | × | ▲ | ○ | ○ | ○ | ○ | × | ○ | ○ |
| 9 | 2019 年 1 月 25 日 | 企業 I | 中 | × | × | × | ○ | × | ○ | ○ | ○ | ○ | ○ |
| 10 | 2020 年 11 月 17 日 | 企業 J | 大 | × | ○ | × | ○ | × | ○ | ○ | × | ○ | ○ |

○：確認できた項目、X：記載及び事実がなかった項目、△：被害が発覚した時点でサービスを停止し、その後再開、
▲：被害が発覚した時点でサービスを停止

- 事例 1 は、決済モジュールの脆弱性を悪用したウェブサイト機能の改ざんであり、決済モジュールの改ざん・偽の決済フォームの設置により、特定の期間に決済に利用したクレジットカード情報が抜き出されていた。
- 事例 2 は、不正アクセスによる被害事例であり、決済アプリケーションの改ざんにより、決済情報入力画面が書き換えられ、顧客が当該画面で入力したクレジットカード情報が盗取された。
- 事例 3 は、ウェブサイトの改ざんによる被害事例であり、不正アクセスされウェブサイトの設定を書き換えられたことによって、該当ウェブサイトから第三者のウェブサイトに転送される状態となっていた。
- 事例 4 は、不正アクセスによる被害事例である。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設置された偽のクレジットカード情報入力画面に入力したクレジットカード情報が流出した。
- 事例 5 は、不正アクセスによる被害事例である。システムの一部の脆弱性を突いた攻撃により不正アクセスされ、個人情報の流出につながった。また、不正アクセスにより流出したメールアドレス宛に偽装メールが送信された。
- 事例 6 は、ウェブサイトの改ざんによる被害事例である。運営しているウェブサイトに不正な記事の書き込みが行なわれた。また情報流出については管理者情報が流出した恐れがあるが、利用者の個人情報は流出していない。
- 事例 7 は、不正アクセスによる被害事例である。公開されている脆弱性情報に対応しなかったことで攻撃を受け、不正アクセスおよび個人情報の流出につながった。
- 事例 8 は、不正アクセスによる被害事例である。展開しているウェブサービスで使用中の一部のサーバが不正アクセスされ、個人情報の流出につながった。
- 事例 9 は、不正アクセスによる情報漏えい被害事例である。SQL インジェクション攻撃が行われ、DB サーバ内に格納されている個人情報が盗取された。
- 事例 10 は、不正アクセスによる被害事例である。グループ会社のサイトから侵入され、グループで保管していた個人情報が流出した。

## 3.3.ヒアリング調査結果

ヒアリング調査結果の概要を以下に報告する。

**表 3-2　ヒアリング調査結果**

| No | 発生日・属性等 | | | | | 調査対象被害 | | | | 調査項目 | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 発生・発覚日 | 脆弱性の概要 | ウェブサイトの形態 | 企業規模 | Cloud 利用 | 1.改ざん | 2.サービス停止 | 3.情報漏えい | 4.風評被害/二次被害 | 1.内容と影響範囲 | 2.直接原因、根本原因 | 3.技術的・人員的原因 | 4.発生後の対策 | 5.再発防止策 |
| 1 | 2018 年 6 月 | CMS の脆弱性を悪用したウェブサイトの改ざん | 自社構築・運営 | 小 | × | ○ | × | × | × | ○ | ○ | ○ | ○ | ○ |
| 2-1 | 2020 年 1 月 | CMS の脆弱性を悪用した EC サイトの改ざん | 自社構築・運営 | 小 | ○ | ○ | ▲ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| 2-2 | 2018 年 12 月 | 管理者の個人 PC がマルウェアに感染、管理者アカウントを悪用した EC サイトの情報漏えい | 自社構築・運営 | 大 | × | × | △ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| 3 | 2019 年 11 月 | ウェブサイトの改ざん事例（原因は不明） | 自社構築・運営 | 大 | × | ○ | △ | × | × | ○ | × | × | × | ■ |
| 4 | 2018 年 | ウェブサイトの改ざん事例（原因は不明） | 外部サービス利用 | 小 | × | ○ | △ | × | × | ○ | ○ | ○ | ○ | ○ |
| 5 | 2016 年 | ウェブサイトの改ざん事例（原因は不明） | 自社構築・運営 | 大 | × | ○ | △ | × | × | ○ | ■ | ■ | ○ | ○ |
| 6 | 2020 年 | ウェブサイトダウン（原因は不明） | 自社構築・運営 | 中 | × | × | ○ | × | × | ○ | × | ■ | ○ | ○ |

○：確認できた項目、×：確認できなかった、または未使用の項目、■：担当部分で確認できた項目

△：被害が発覚した時点でサービスを停止し、その後再開、▲：被害が発覚した時点でサービスを停止

- 事例 1 は、使用していた CMS 及び CMS のプラグインの脆弱性を悪用された結果、自社ウェブサイトを改ざんされ、意図しない外部に誘導するリンクが混入していた事例である。
- 事例 2-1 は、CMS の脆弱性を悪用された結果、自グループ会社の EC サイトが改ざんされ、20 件程度のクレジットカード情報が流出した事例である。
- 事例 2-2 は、管理者の私用 PC がマルウェア感染し、自グループ会社の EC サイトの管理者アカウントを第三者に悪用され、クレジットカード情報が 100 件流出した事例である。
- 事例 3 は、自社ウェブサイトへの不正アクセスによって自社ウェブサイトが改ざんされた事例である。なお、本ヒアリング対象者は、コンテンツ作成担当であり、調査・対策担当でないため、原因は不明であった。

- 事例 4 は、自社ウェブサイトへの不正アクセスによる改ざんが 2 回あった事例である。なお、本ヒアリング対象者は、相談先や相談方法がわからなかったため原因は不明であり、自組織で出来る範囲の対応を行った事例である。
- 事例 5 は、自社ウェブサイトへの不正アクセスによる改ざん事例である。なお、本ヒアリング対象者は、調査担当者でないため、原因は不明であった。
- 事例 6 は、自社のウェブサイトがダウンした結果、サービス停止に繋がった事例である。なお、本ヒアリング対象者は、ウェブサイトの UI/UX 系の担当であり、対策担当者でないため、原因は不明であった。

## 3.4. 企業ウェブサイトのための脆弱性対応ガイドの改訂

### (1) 文献調査結果からの考察

被害を受けた原因を考慮した結果、「構成管理」「脆弱性情報の収集」「ハードウェア、ソフトウェアの定期的な更新」「必要に応じて外部サービスを利用したセキュリティ確保」が対策として求められていることが分かった。これらの対策を踏まえ、「企業ウェブサイトのための脆弱性対応ガイド」を改訂する。

なお、事故が発生した際に企業規模問わず、大部分の企業が第三者機関を利用した原因解明もしくは再発防止に取り組んでおり、利用者に対して調査結果や再発防止策等の報告を実施していた。

### (2) ヒアリング調査結果からの考察

「CMS も含めた構成管理」「脆弱性情報の収集」「管理アカウントや管理アカウントを利用する環境の適切な管理」「ウェブサイトの改ざんなどの監視」「被害が発生した場合の相談先や相談方法に関する情報収集」が対策として求められていることが分かった。これらの対策を踏まえ、「企業ウェブサイトのための脆弱性対応ガイド」を改訂する。

# 4. 海外の政府機関等における脆弱性対策の取組みに関する調査

## 4.1. 調査の概要

### (1) 目的

国内においては、「パートナーシップ」という脆弱性届出制度があるが、海外の政府機関、公的な機関等においても、法律などに基づいて脆弱性対策に関する取組みが実施されている。それらの取組みについて、どの様な対象に、どの様な対応を実施しているかについて文献等により調査を実施した。また、本調査・検討で得られた「パートナーシップ」の運用改善の対応方針を検討した。

### (2) 手順

海外の政府機関、公的な機関等が、法律等に基づき実施している脆弱性対策に関して、文献等を調査した。

［調査件数］海外の政府機関、公的な機関 6 件以上

［調査項目］調査の主な項目は以下の通りである。

- 脆弱性受付の有無
- 法律等に基づいて実施している脆弱性対策の取組み内容、実施方法
- 法律の適用（強制）範囲
- 脆弱性対策を実施することによる期待する効果、実績
- 脆弱性対策を実施する上での課題や、阻害要因
- 今後実施する取組み、実施スケジュール
- 調整有無
- 報告対象の限定（政府システムの脆弱性のみ、IoT の脆弱性のみ等）

調査対象の政府機関、公的な機関は以下の通りである。

**表 4-1　調査対象の海外政府機関・公的な機関**

| 国/地域 | 名称 |
|---|---|
| 欧州 | 1. Computer Emergency Response Team for the EU institutions, agencies and bodies (CERT-EU) |
| | 2. The European Union Agency for Cybersecurity (ENISA) |
| 英国 | 3. Centre for the Protection of National Infrastructure (CPNI) |
| | 4. National Cyber Security Centre (NCSC-UK) |

| 国/地域 | 名称 |
|---|---|
| 英国 | 5. Oxford Information Labs |
| | 6. Department for Digital, Culture, Media & Sport (DCMS) |
| 米国 | 7. CERT Coordination Center (CERT/CC) |
| | 8. Cybersecurity & Infrastructure Security Agency (CISA) |
| | 9. National Institute of Standards and Technology (NIST)及び Office of Management and Budget(OMB) |
| カナダ | 10. Canadian Centre for Cyber Security (CCCS)及び Government of Canada |
| 韓国 | 11. Korea Internet & Security Agency (KISA)及び KrCERT/CC |
| シンガポール | 12. Singapore Computer Emergency Response Team (SingCERT) |
| | 13. Infocomm Media Development Authority (IMDA) |
| | 14. Government Technology Agency (GovTech) |
| フィンランド | 15. National Cyber Security Centre Finland (NCSC-FI) |
| オランダ | 16. National Cyber Security Centre Netherlands (NCSC-NL) |

## 4.2. 文献調査結果

文献調査結果の概要を以下に報告する。

**表 4-2　海外政府機関・公的な機関の調査結果概要**

| No | 国/地域 | 名称/取組 | 調査項目 | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | 1 脆弱性の受付有無 | 2 法律に基づく取組み | 3 法律適用 | 4 効果・実績 | 5 課題・阻害要因 | 6 今後の取組み | 7 調整有無 | 8 報告対象の限定 |
| 1 | 欧州 | CERT-EU | ○ | × | × | × | × | × | ○ | × |
| 2 | | ENISA | × | × | × | × | × | × | × | × |
| 3 | 英国 | CPNI | × | × | × | × | × | × | × | × |
| 4 | | NCSC-UK | ○ | × | × | × | × | × | ○ | ○2 |
| 5 | | Oxford Information Labs | ○ | × | × | × | × | × | ○ | ○1 |
| 6 | | DCMS | × | ○6 | ○ | × | × | × | × | ○1 |
| 7 | 米国 | CERT/CC | ○ | × | × | × | × | × | ○ | × |
| 8 | | CISA (BOD 20-01) | ○ | ○7 | × | × | × | × | ○ | ○2 |
| | | CISA (ICS, IoT, 医療機器) | ○ | × | × | × | × | × | ○ | ○ 1･4 |
| 9 | | NIST 及び OMB | × | ○7 | × | × | × | × | × | × |
| 10 | カナダ | CCCS | × | × | × | × | × | × | × | × |

| No | 国/地域 | 名称/取組 | 調査項目 | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | 1 脆弱性の受付有無 | 2 法律に基づく取組み | 3 法律適用 | 4 効果・実績 | 5 課題・阻害要因 | 6 今後の取組み | 7 調整有無 | 8 報告対象の限定 |
| 11 | 韓国 | KISA 及び KrCERT/CC | ○ | × | × | × | × | × | ○ | × |
| 12 | シンガポール | SingCERT | × | × | × | × | × | × | × | × |
| 13 | | IMDA | ○ | × | × | × | × | × | × | ○3 |
| 14 | | GovTech | ○ | × | × | × | × | × | × | ○2 |
| 15 | フィンランド | NCSC-FI | ○ | × | × | × | × | × | ○ | × |
| 16 | オランダ | NCSC-NL | ○ | × | × | × | × | × | ○ | ○ 2･5 |

×：掲載無、○：掲載有、○1： IoT の脆弱性報告に限定、○2：政府システムの脆弱性報告に限定、○3：情報通信分野事業者の脆弱性に限定、○4：制御系製品、医療機器等の脆弱性報告に限定、○5：身体生命に関するシステムに限定、○6：脆弱性開示ポリシーの公開を製品開発者に義務化、○7：脆弱性への対応を政府機関に義務化

## 4.3. パートナーシップの運用改善の対応方針

パートナーシップと諸外国の取組みを参考として比較分析を行った。参考とする対象は、パートナーシップと同様に脆弱性の届出の受け付けを行っている取組みとした。また、届出を受け付ける対象の限定については、政府システム等の脆弱性の届出を行っている事例が多いことから、政府システム等に限定している取組みに加えた。

上記観点に見合い、パートナーシップの運用改善の参考となる取組みは、CERT-EU、CERT/CC、CISA（連邦政府機関に対する脆弱性開示ポリシー指令 BOD 20-01）、KISA と KrCERT/CC、NCSC-NL とした。

参考となる取組みをパートナーシップに導入した場合の効果、導入にあたっての検討事項・課題を検討した結果を以下に報告する。CERT-EU は謝辞公表の追加、CERT/CC は一定期間経過による脆弱性情報の公開、CISA は法的な担保の追加、KISA と KrCERT/CC 及び NCSC-NL は報奨金の追加について導入にあたっての検討事項・課題を検討した。

**表 4-3　海外政府機関・公的な機関の調査結果概要**

| 機関 | 導入した場合の効果 | 導入にあたっての検討事項･課題 |
|---|---|---|
| CERT-EU | ・発見者に対する謝辞を公表することが発見者へのインセンティブとなり、届出件数が増える可能性がある | ・稼働中のウェブサイトの脆弱性については検査方法等によってはウェブサイト運営者とのトラブルを誘発する可能性があり、インセンティブを設けることの適切性を検討する必要がある |
| CERT/CC | ・受付けた脆弱性が調整不能案件になった場合も脆弱性情報を 45 日後に公表することで脆弱性の影響を低減できる場合もある | ・「公表判定委員会」等による中立的な透明性･妥当性のある手続きを経ない場合、訴訟リスクが生じる可能性がある |
| CISA | ・法的な担保があるため脆弱性への対処を強制できる | ・立法等に向け、法的な課題整理が必要 |
| KISA と KrCERT/CC | ・脆弱性報告の届出に報奨金を出すことが発見者のインセンティブとなり、届出件数が増える可能性がある | ・報奨金を出すための制度の改訂、財源の確保等が必要 |
| NCSC-NL | ・脆弱性報告の届出に報奨金を出すことが発見者のインセンティブとなり、届出件数が増える可能性がある | ・報奨金を出すための制度の改訂、財源の確保等が必要 |

上記に示したパートナーシップに導入した場合の効果/検討事項･課題において検討した結果、これらの参考となる取組みについては、パートナーシップに導入する場合、告示・ガイドライン等を含むパートナーシップ制度全体に影響する内容を含むものであるため、今後の検討の参考にする余地はあるが、現時点でパートナーシップの運用の変更を行うまでに至らないと判断した。

# 5. 今後の課題

今後取り組むべき検討課題について以下に示す。

### (1) 小規模のウェブサイト運営者向け脆弱性対策支援

2 章に示した通り、脆弱性対策の支援についてはパートナーシップの認知度は一定程度向上しているが、脆弱性対策の理解及び定期的な見直し等の基本な脆弱性対策が実施されていない状況である。また、3.2 節の被害事例の文献調査においても以前から知られている脆弱性を悪用した被害が現在でも発生している。また、被害が発生した場合の相談先や相談方法がわからず、抜本的な対策を実施出来ていないことも考えられる。小規模ウェブサイトの運営者においては、ウェブサイトの脆弱性対策を実施するが難しいことも考えられ、外部リソースの利用（クラウドサービスや運用の外部委託等）を含めて検討する必要がある。これらを含めて、「企業ウェブサイトのための脆弱性対応ガイド」を改訂した。

今後、改訂した「企業ウェブサイトのための脆弱性対応ガイド」など、小規模ウェブサイトの構築・運営に関する情報の周知を行うことが望ましい。

しかしながら、アンケートの調査結果に示されているように、IPA が公開している脆弱性に関する普及啓発資料の認知度は必ずしも高いものとはいえない。今回、改訂対象となった「企業ウェブサイトのための脆弱性対応ガイド」も同様の認知度になる可能性があるといえる。

今まで、IPA において、他の部署とも連携をして、小規模のウェブサイトの運営者、管理者に対して脆弱性対策についての普及啓発活動を実施してきているが、今後も、他の部署や他団体、関係機関とも引き続き対策を検討、連携をして実施していくことが重要である。

### (2) パートナーシップの運用改善の対応方針検討

4 章に示した通り、ソフトウエア製品およびウェブアプリケーションの脆弱性に関する届出の受付け及び関係者との調整については、諸外国の政府機関等において様々な取組みが実施されている。しかしながら、各組織における取組みの手順・手続きの詳細や判断の指標、取組みの法的根拠といった事情については、公開情報には記載されていないこともあり、調査が困難であった。今後、各組織の取組についてより深い調査を実施する場合には、公開情報からの情報収集だけでなく、ヒアリングや現地調査等の他の手法を組み合せて実施することを検討することが望ましい。

参考１

# 2020 年度 情報システム等の脆弱性情報の取扱いに関する研究会
# 参加者名簿

2021 年 2 月 3 日時点

| | | |
|---|---|---|
| 座長 | 土居 範久 | 慶應義塾大学 |
| 委員 | 秋山 卓司 | 一般社団法人日本インターネットプロバイダー協会（JAIPA） |
| | 歌代 和正 | 一般社団法人 JPCERT コーディネーションセンター（JPCERT/CC） |
| | 垣内 由梨香 | マイクロソフトコーポレーション |
| | 北澤 繁樹 | 三菱電機株式会社 |
| | 栗田 博司 | 株式会社日立製作所 |
| | 小島 健司 | 東芝デジタルソリューションズ株式会社 |
| | 柴﨑 正道 | 株式会社網屋 |
| | 下村 正洋 | NPO 日本ネットワークセキュリティ協会（JNSA） |
| | 新　誠一 | 電気通信大学 |
| | 鈴木 裕信 | NPO フリーソフトウェアイニシアティブ |
| | 高木 浩光 | 国立研究開発法人産業技術総合研究所 |
| | 高橋 郁夫 | 株式会社 IT リサーチ・アート |
| | 谷川 哲司 | 日本電気株式会社 |
| | 中尾 康二 | 国立研究開発法人情報通信研究機構 |
| | 中野 学 | パナソニック株式会社 |
| | 西嶋 勉 | 富士通株式会社 |
| | 山崎 圭吾 | 株式会社ラック |
| | 渡辺 研司 | 名古屋工業大学 |

（五十音順、敬称略）

オブザーバ

| | |
|---|---|
| 奥家 敏和 | 経済産業省 サイバーセキュリティ課長 |
| 鴨田 浩明 | 経済産業省 サイバーセキュリティ課 企画官 |
| 手塚 久美子 | 経済産業省 サイバーセキュリティ課 課長補佐 |
| 宮下 清 | 一般社団法人日本情報システム・ユーザー協会（JUAS） |
| 笹岡 賢二郎 | 一般社団法人コンピュータソフトウェア協会（CSAJ） |
| 戸島 拓生 | 一般社団法人コンピュータソフトウェア協会（CSAJ） |
| 椎木 孝斉 | 一般社団法人 JPCERT コーディネーションセンター（JPCERT/CC） |
| 洞田 慎一 | 一般社団法人 JPCERT コーディネーションセンター（JPCERT/CC） |
| 高橋 紀子 | 一般社団法人 JPCERT コーディネーションセンター（JPCERT/CC） |
| 石川 貴博 | 一般社団法人 JPCERT コーディネーションセンター（JPCERT/CC） |
| 阿部 力也 | 一般社団法人 JPCERT コーディネーションセンター（JPCERT/CC） |
| 村瀬 一郎 | 技術研究組合制御システムセキュリティセンター（CSSC） |

（順不同、敬称略）

事務局

| | |
|---|---|
| 富田 達夫 | 独立行政法人情報処理推進機構 理事長 |
| 戸髙 秀史 | 独立行政法人情報処理推進機構 理事 |
| 瓜生 和久 | 独立行政法人情報処理推進機構 |
| 桑名 利幸 | 独立行政法人情報処理推進機構 |
| 寺田 真敏 | 独立行政法人情報処理推進機構 |
| 渡辺 貴仁 | 独立行政法人情報処理推進機構 |
| 土屋 昭治 | 独立行政法人情報処理推進機構 |
| 板橋 博之 | 独立行政法人情報処理推進機構 |
| 井上 真弓 | 独立行政法人情報処理推進機構 |
| 唐亀 侑久 | 独立行政法人情報処理推進機構 |
| 村野 正泰 | 株式会社三菱総合研究所 |
| 江連 三香 | 株式会社三菱総合研究所 |
| 小川 博久 | 株式会社三菱総合研究所 |
| 朱 ユーティン | 株式会社三菱総合研究所 |
| 平林 徹 | 株式会社三菱総合研究所 |

（順不同、敬称略）

参考２

検討経緯

■研究会第 1 回会合（2020 年 11 月 11 日）
・昨年度の研究会における検討について
・今年度の検討方針について
・小規模ウェブサイト運営者の脆弱性対策に関する調査について
・最新のウェブサイトの被害事例に関する調査について
・海外の政府機関等における脆弱性対策の取組みに関する調査
・スケジュールについて

■研究会第 2 回会合（2021 年 2 月 3 日）
・前回会合の確認
・小規模ウェブサイト運営者の脆弱性対策に関する調査について
・最新のウェブサイトの被害事例に関する調査について
・企業ウェブサイトのための脆弱性対応ガイドの改訂(案)について
・海外の政府機関等における脆弱性対策の取組みに関する調査について
・情報システム等の脆弱性情報の取扱いに関する調査実施報告書(案)について