情報システム等の脆弱性情報の取扱いに関する研究会

- 2021 年度 報告書 -

2022 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 2021 年 12 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 17,139 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、関係団体を通じ既存の普及啓発資料を幅広く認知してもらうために、関係団体に協力してもらう条件等を調査し、普及啓発への協力の依頼を実施した。また、ウェブサイト運営者がパートナーシップ等外部から脆弱性情報の報告を受け付ける連絡先となる窓口設置について、課題を調査するとともに課題解消のための指針をまとめた。あわせて、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。

2022 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 2021 年 12 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 5,009 件、ウェブサイトの脆弱性に関するもの 12,130 件の計 17,139 件であった。四半期毎の届出状況を図 1-1に示す。

	2019 1Q	2Q	3Q	4Q	2020 1Q	2Q	3Q	4Q	2021 1Q	2Q	3Q	4Q
累計届出件数[件]	14,213	14,710	15,055	15,227	15,488	15,676	15,922	16,225	16,476	16,779	16,986	17,139
1 就業日あたり[件/日]	3.96	4.03	4.06	4.04	4.04	4.03	4.03	4.04	4.05	4.06	4.05	4.03

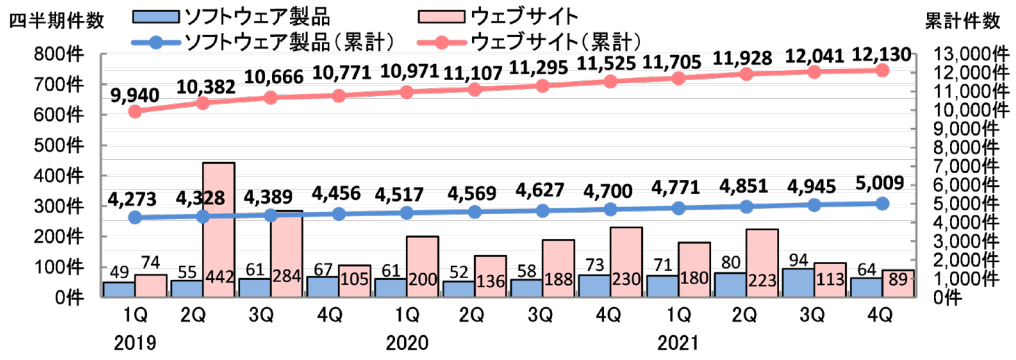


図1-1. 脆弱性の届出件数の四半期ごとの推移

図 1-1　四半期ごとの届出状況

（活動報告レポート[2021 年第 4 四半期（10 月～12 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の届出に関する処理状況を図 1-2 に示す。

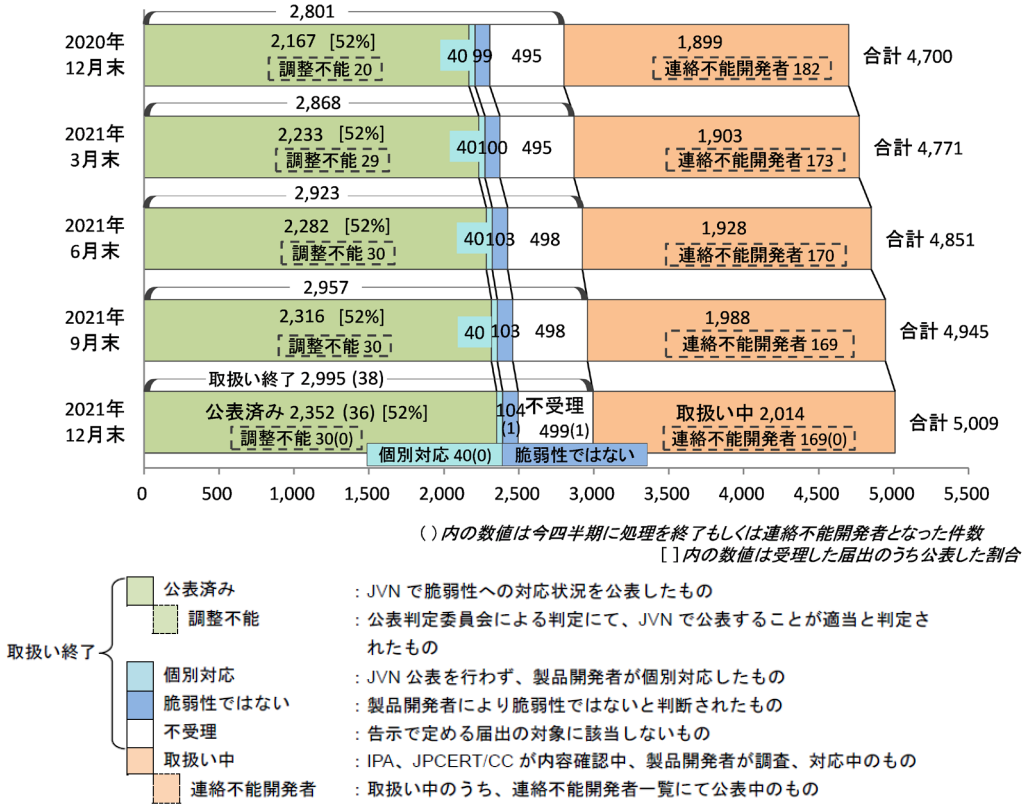


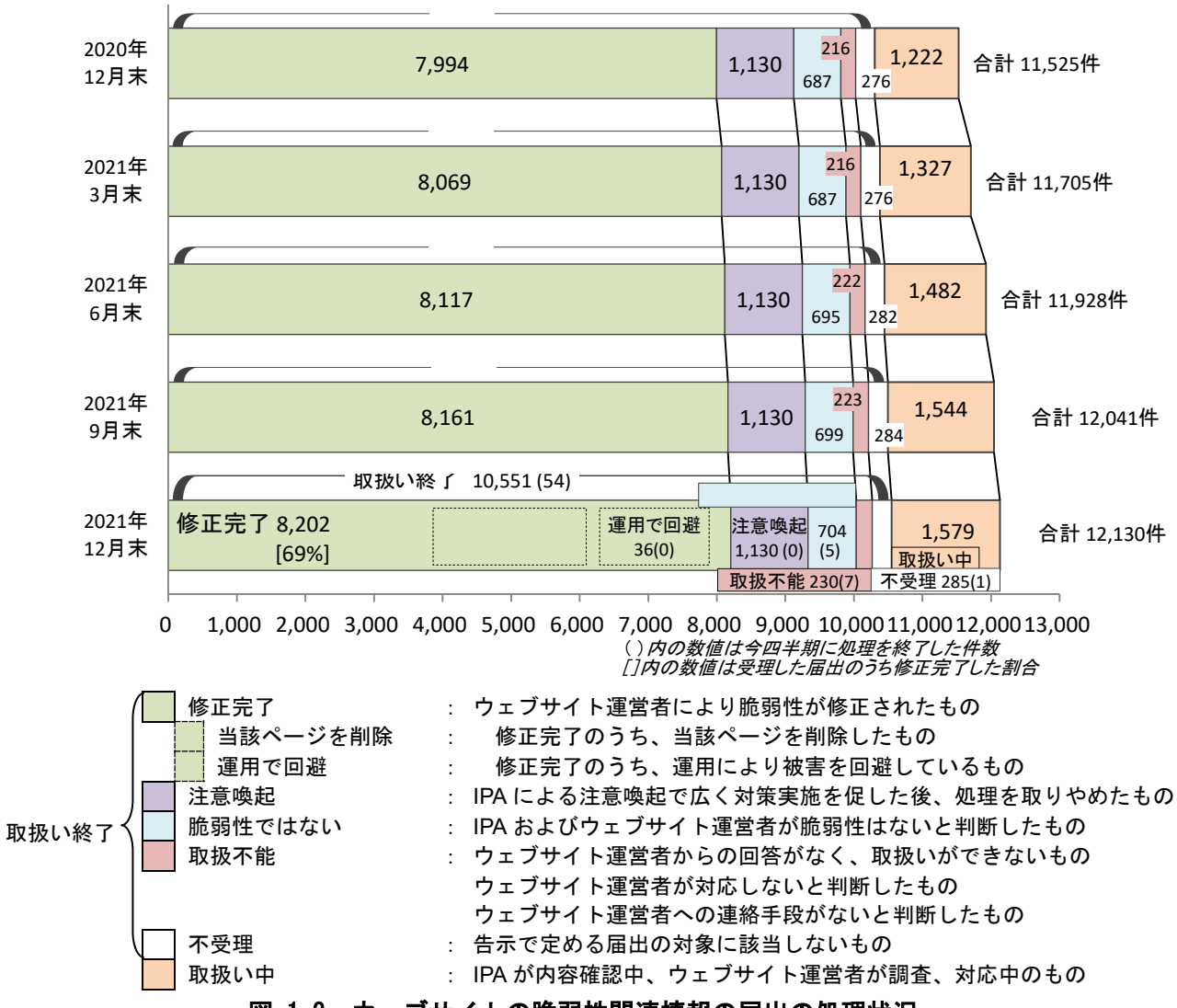
図 1-2　ソフトウエア製品の脆弱性関連情報の届出の処理状況

（活動報告レポート[2021 年第 4 四半期（10 月～12 月）]より抜粋）

ソフトウエア製品の脆弱性関連情報の届出 5,009 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 2,352 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 104 件、取扱い中のものが 2,014 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 499 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。



取扱い終了	修正完了	：	ウェブサイト運営者により脆弱性が修正されたもの
	当該ページを削除	：	修正完了のうち、当該ページを削除したもの
	運用で回避	：	修正完了のうち、運用により被害を回避しているもの
	注意喚起	：	IPA による注意喚起で広く対策実施を促した後、処理を取りやめたもの
	脆弱性ではない	：	IPA およびウェブサイト運営者が脆弱性はないと判断したもの
	取扱不能	：	ウェブサイト運営者からの回答がなく、取扱いができないもの ウェブサイト運営者が対応しないと判断したもの ウェブサイト運営者への連絡手段がないと判断したもの
	不受理	：	告示で定める届出の対象に該当しないもの
	取扱い中	：	IPA が内容確認中、ウェブサイト運営者が調査、対応中のもの

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[2021 年第 4 四半期（10 月～12 月）]より抜粋）

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

ウェブサイトの脆弱性関連情報の届出 12,130 件のうち、修正が完了したものが 8,202 件（うち運用で回避されたもの 36 件、当該ページを削除して対応したもの 1,116 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 704 件、取扱い中のものが 1,579 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 230 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 285 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 2021 年 12 月末までに 4,269 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 12 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 2,352 件である。届出受付開始から 2021 年 12 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。

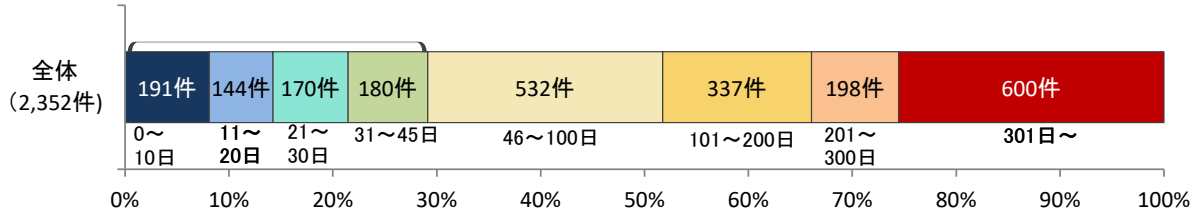


図 1-4　ソフトウエア製品の脆弱性公表までに要した日数

（活動報告レポート[2021 年第 4 四半期（10 月～12 月）]より抜粋）

(2) 海外 CSIRT から連絡を受け公表した脆弱性

2021 年 12 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 2,313 件である。このうち、2021 年度第 4 四半期（2021 年 10 月から 2021 年 12 月末まで）に JVN で公表した脆弱性関連情報は 92 件であった。

[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。

(3) 製品種類別の内訳

届出受付開始から 2021 年 12 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 5,009 件のうち、不受理分を除いた 4,510 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。

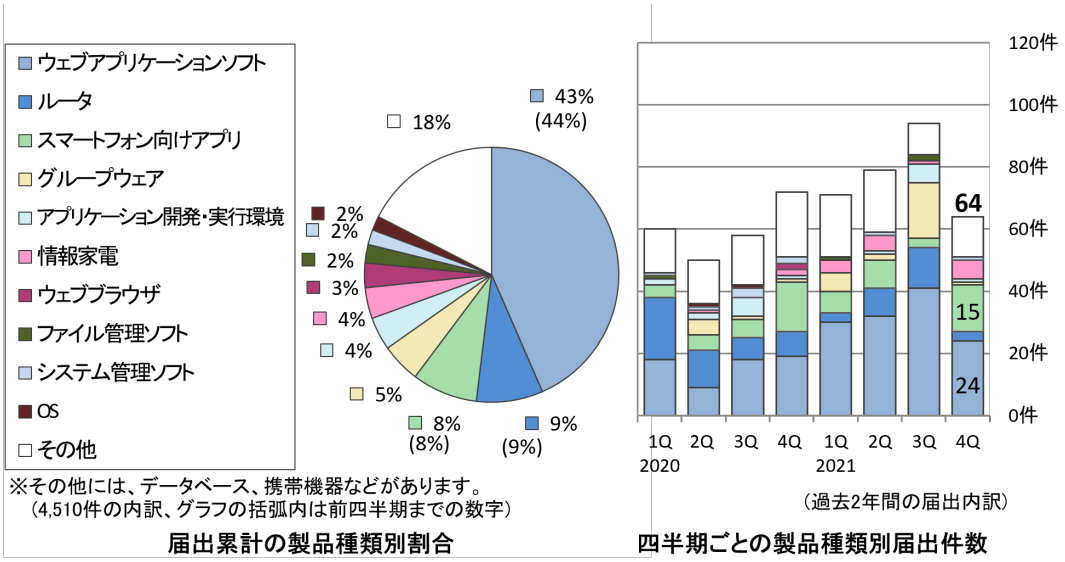


図 1-5　ソフトウエア製品種類別の届出内訳（届出受付開始～2021 年 12 月末）

（活動報告レポート[2021 年第 4 四半期（10 月～12 月）]より抜粋）

(4) 脆弱性の原因別の内訳

届出受付開始から 2021 年 12 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 5,009 件のうち、不受理のものを除いた 4,510 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。

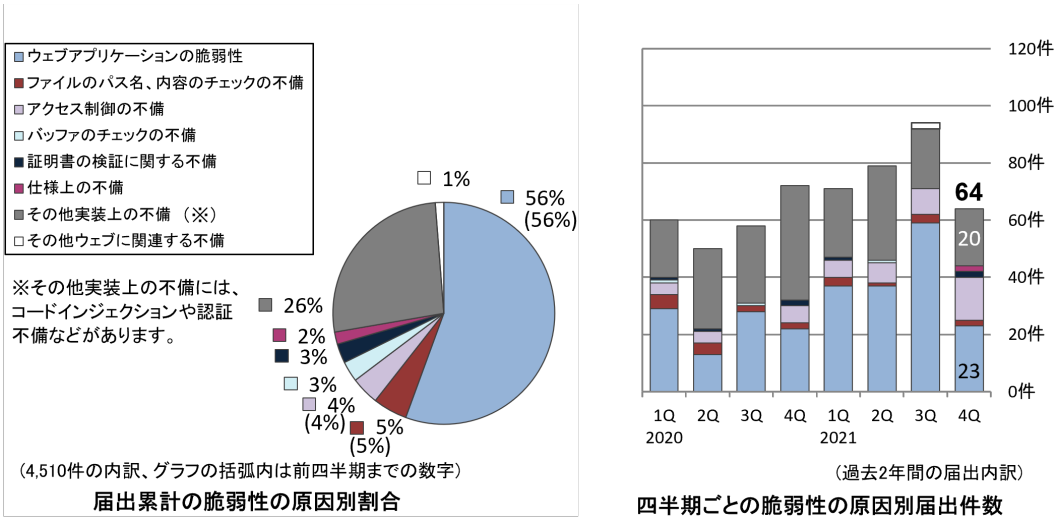


図 1-6　ソフトウエア製品の脆弱性原因別の届出内訳（届出受付開始～2021 年 12 月末）

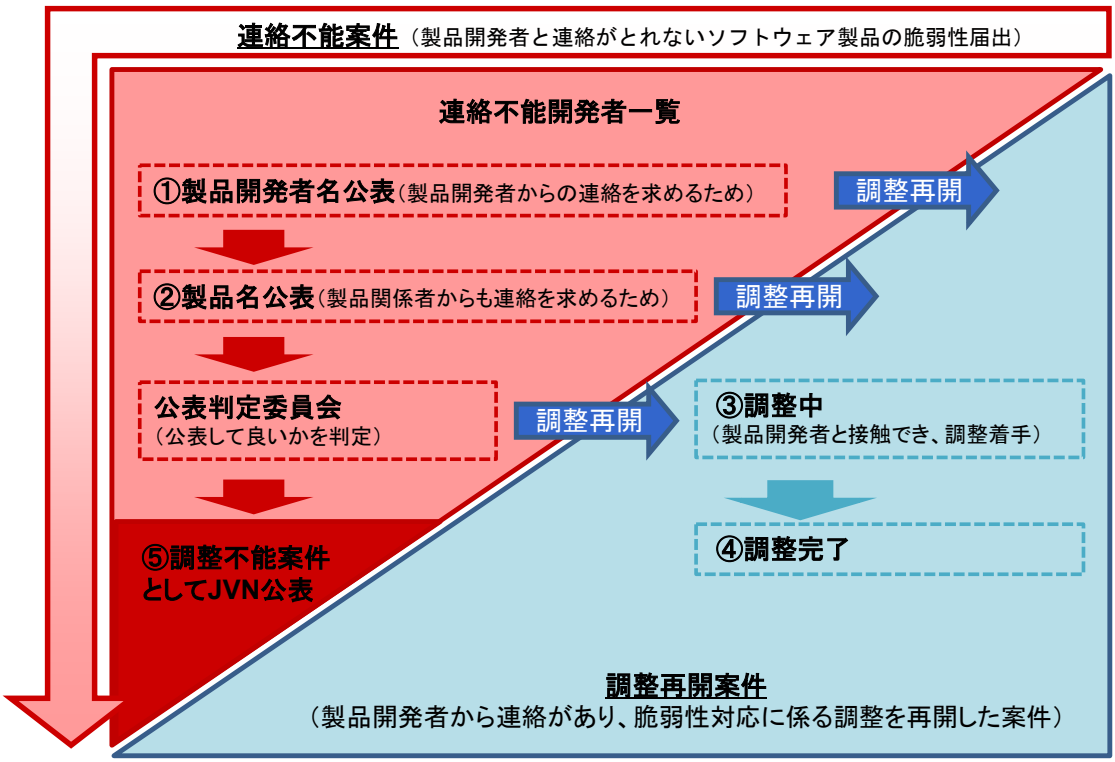
（活動報告レポート[2021 年第 4 四半期（10 月～12 月）]より抜粋）

(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。2021 年度第 4 四半期に優先情報提供したものは電力分野 3 件、政府機関 3 件で、累計では 52 件（電力分野 32 件、政府機関 20 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 2021 年 12 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 52 件が調整を再開（その中の 32 件が調整完了）したが、169 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）。



2021年 第3四半期	169件 （①1件 ②168件）	52件 （③20件 ④32件）	⑤ 30 件	合計 251件
2021年 第4四半期	169件 （①1件 ②168件）	52件 （③20件 ④32件）	⑤30 件	合計 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～2021 年 12 月末）

（活動報告レポート[2021 年第 4 四半期（10 月～12 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

2021 年 12 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 8,202 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、68%の届出が 90 日以内に修正されている。

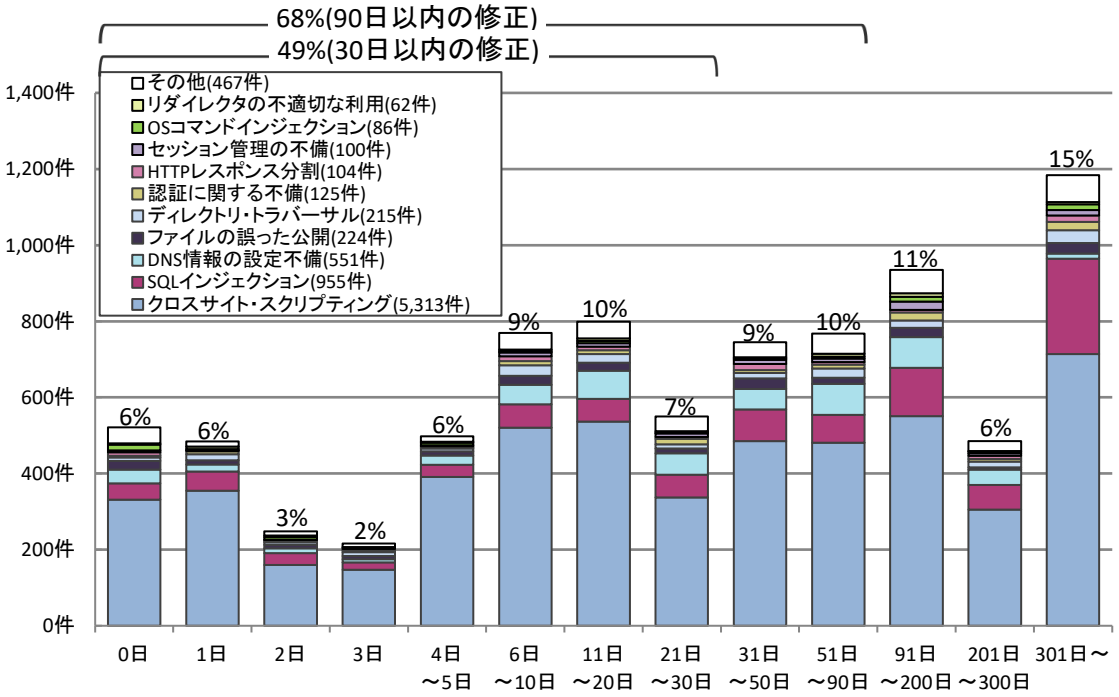
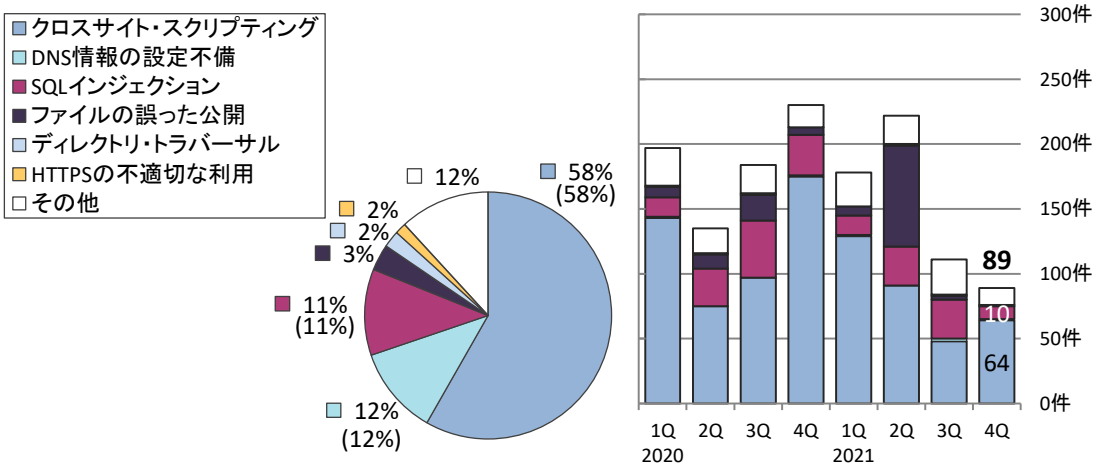


図 1-8　ウェブサイトの脆弱性修正に要した日数（届出受付開始～2021 年 12 月末）

（活動報告レポート[2021 年第 4 四半期（10 月～12 月）]より抜粋）

(2)届出の脆弱性種類別内訳

2021 年 12 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 12,130 件のうち、不受理のものを除いた 11,845 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。



（11,845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

（過去2年間の届出内訳）

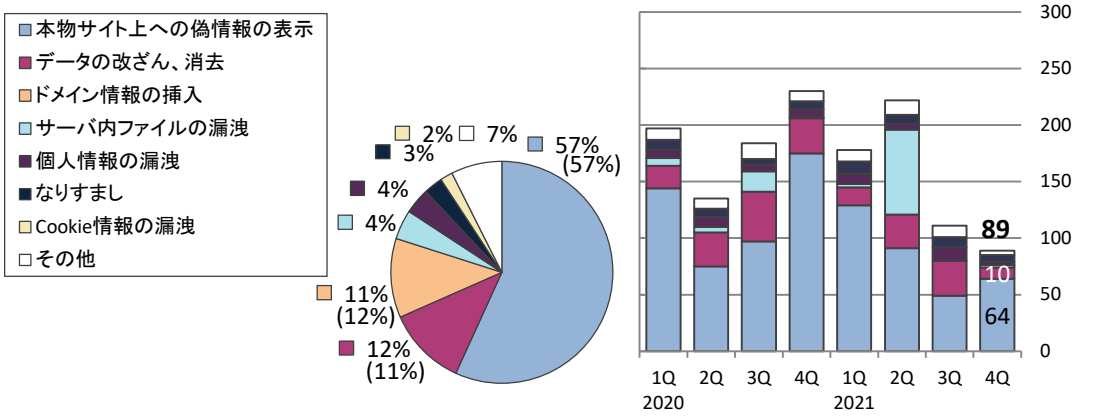
四半期ごとの脆弱性の種類別届出件数

図 1-9　ウェブサイトの脆弱性種類別内訳（届出受付開始～2021 年 12 月末）

（活動報告レポート[2021 年第 4 四半期（10 月～12 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」(57%)、「データの改ざん、消去」(12%)、「ドメイン情報の挿入」(11%)の割合が高い。



（11,845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

（過去2年間の届出内訳）

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～2021 年 12 月末）

（活動報告レポート[2021 年第 4 四半期（10 月～12 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 551 件で、前年同期（444 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 16%を占めており、対策の実施が望まれる。

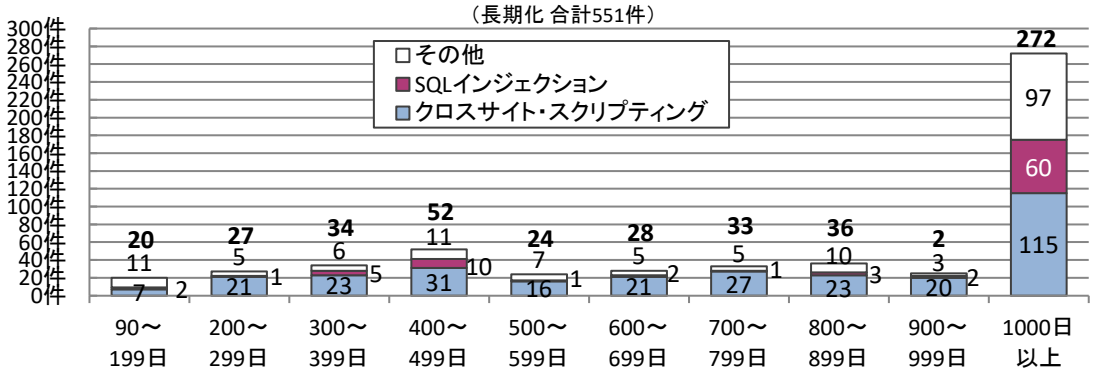


図 1-11　取扱いが長期化（90 日以上経過）しているウェブサイトの経過日数と脆弱性の種類

（活動報告レポート[2021 年第 4 四半期（10 月～12 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 3 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普及啓発の促進に関する調査
・普及啓発資料の内容や情報展開にあたっての協力の条件等に関する関係団体に対する調査
（ヒアリング調査）
・普及啓発に関する施策の検討
・「普及啓発の促進に関する調査報告書」の取りまとめ

②ウェブサイト運営者の窓口設置に関する調査
・窓口設置済および窓口未設置のウェブサイト運営者に対する調査
（ヒアリング調査）
・窓口設置推奨資料の作成

③パートナーシップガイドラインの取扱いに関する検討
・パートナーシップガイドラインの取扱い

2. 普及啓発の促進に関する調査

2.1. 調査の概要

(1) 目的

製品開発者、ウェブサイト運営者、製品利用者等の様々な主体に対して、脆弱性対策を普及啓発するための資料を作成、公表しており、ウェブサイトやセミナー開催等を通じて普及啓発を図ってきた。しかしながら、昨年度のアンケート調査結果によると、これらの普及啓発資料を認知していない層が存在し、その層には資料が活用されていないことが判明していることから、脆弱性対策が進展していないという状況があると推察される。

このため、脆弱性対策の進展を目的として、普及啓発資料の認知状況の改善を図るべく、製品開発者、ウェブサイト運営者、製品利用者について、それらの当事者への情報展開のルートをもつ関係団体に対し、当該関係団体を通じた普及啓発の協力を依頼するため、協力にあたっての前提条件等に関するヒアリング調査を行った。ヒアリング調査は、昨年までの調査において普及啓発資料の作成にあたってヒアリング先となった組織を優先して対象とするものとし、普及啓発資料の内容や、情報展開にあたっての協力の条件等を確認した。その結果を踏まえ、条件を満たす対応を行ったうえで、実際に協力を依頼した。

また、上記のヒアリングにおいて、今後実施すべき普及啓発活動の内容や課題についても調査し、その結果を基に、今後実施すべき普及啓発活動の内容や課題について検討を行った。

(2) 手順

製品開発者、ウェブサイト運営者、製品利用者について、それらの当事者への情報展開のルートをもつ関係団体を対象にヒアリング調査行った。

［調査対象］

①製品開発者関係団体

- 製品開発者を 100 社以上会員としている団体を対象とすること。
- パッケージソフトウェアの企画・開発・販売または情報家電等の組み込み機器の企画・開発・販売を実施する企業が主に含まれる業界団体を 2 件以上含むこと。

②ウェブサイト運営者関係団体

- ウェブサイトを運営する者を含む、組織の規模として、組織的にセキュリティ対策が実施可能である程度の規模（50 名から 300 名程度）を有する中小企業の商工業者によって組織される団体、またはそれらの団体を会員に持つ団体を 2 件以上含むこと。

③製品利用者関係団体

- 情報家電の販売を行う家電量販店を 1 件以上含むこと。
- 消費生活の相談に関する活動を実施する組織を 1 件以上含むこと。

[調査件数]

①製品開発者関係団体：5 件

②ウェブサイト運営者関係団体：4 件

③製品利用者関係団体：2 件

合計 10 件以上

[調査項目]

各ヒアリング対象者とも同様に以下の項目、質問でヒアリングを実施。

(1) 普及啓発資料の内容に関するご意見

- 会員企業等の現状と照らして、有用と思う点
- わかりにくい点、補足等が必要な点、追記が望ましい点、等

(2) 普及啓発の効果的な実施方法に関するご意見

- 宣伝や周知の方法（利用可能な既存のチャンネルの存在等）
- 普及啓発が効果的と想定される対象（製品や業種の種別、企業規模、消費者の行動特性等）
- 問い合わせ対応の支援への要求や内容、等

(3) 普及啓発の実施に対する阻害要因

- 取組を躊躇させる何らかの阻害要因
- 会員企業における阻害要因（情報セキュリティへの取組レベルの現状、経営的要因、制度的要因、技術的要因等）
- 利用者／消費者における阻害要因（コスト意識、そもそも情報セキュリティへの意識が低い等）、等

(4) 普及啓発にあたり今後 IPA が実施すべき方策

- セミナーや説明会等による周知、利用者／消費者向けチャンネルにおける直接的な情報周知
- 現状資料への補足情報の展開、等

(5) 普及啓発へのご協力可否、条件（啓発対象者の範囲、数、配布媒体等）

- 会員企業、消費者等への普及啓発の協力の可否
- 協力いただける場合の範囲や規模、方法

・ 協力いただける場合に IPA にしてほしいこと（問い合わせ対応の支援など）、等

2.2. ヒアリング調査

以下に、ヒアリング調査から得られた知見を取りまとめる。

(1) 製品開発者関係団体

(a)普及啓発への協力提案

・ 会員向け発信による協力
  - 周知文面をもらえれば会員向けにメールを投げることは可能。
  - メールでガイドラインを会員に配布、告知することが可能。
  - Web ニュースに掲載して周知することが可能。
  - 他団体の参考情報を掲載する Web ページに掲載可能。

・ 組織内の会合やイベントでの協力
  - 不定期に年間 3、4 回の実施する会合があり、ライトニングトークを実施するケースもあるので、IPA から 10 分くらい話してもらうことも可能。
  - 組織内の WG で招待講演を行っており、IPA に開発者向けガイドラインを使用した講演をお願いしたい。
  - IPA が作成した IoT 向けセキュリティ教材を活用したエンジニア向けセミナーを 2022 年から開始する予定。その他に各種ワークショップやウェビナーを開催し、年 3 回大規模な組込み向け展示会を実施しており、それらの場で協力することが可能。
  - 一般向け大型家電展示会のオンライン展示会に参加してもらうなどが検討可能。

・ 組織間の連携による協力
  - 当方のガイドを IPA ルートで紹介いただく、IPA のイベントを当方で協力する等が可能。
  - 組込み機器に関わる他組織と活動協力を進めている。IPA とも協力できると良い。

(b)ガイドの内容に関する意見

・ ガイド内に具体例、サンプルを記載すべき
  - 1 つの機器を設計することを想定した具体的なユースケースをもとに対策のサンプルを示すと、エンジニアにとって非常に有用である。

- 企業はどのような業種、立場の企業に向けて発信しているガイドなのかを重視する。実際のケーススタディを掲載し、ターゲットを明確化し、同業種の対策例など、実務に応用できるような情報を掲載すると有用である。
- ガイドの内容として、実装レベルでどうするべきかの記載も欲しい。実装レベルの内容を学べると良い。
- 詳細に関して外部資料を参考として挙げている項目が多いが、資料内で具体例を提示することでより使いやすいガイドになる。
- チェックリストで規約や機能の有無を問う設問があるが、内容面の十分さにも触れてチェックできるようにした方が良い。

・ ガイドへ項目を追加すべき
- 製品開発者にとって「消費者がどのような不安を抱いているのか」という情報が手に入りづらい。消費者の不安の事例について、解決策とともにガイドに掲載するとよい。

・ 業界・市場種別や読者属性別に内容を整理すべき
- 「製品のセキュリティ対策はどこまでやったら良いのか」を経営層に理解してもらうことが大事である。見せ方を変えて、経営層に刺さるようにできると良い。
- IoT 機器で要求されるセキュリティ対策レベルは業界・製品市場によって異なるため、製品毎のセキュリティレベルを理解して記載する必要がある。
- サプライチェーンの末端の中小企業にとっては、ガイドを見ても具体的に何をしたら良いのか判断が難しい。参考として挙げられている資料も分量が多く読み込むのは難しい。
- 経営企画部門や情報システム部門を対象に書かれているため、製造部門のエンジニアには自分事として理解され難い。部門ごとに整理し、各部門が果たす役割について伝える必要がある。

(c)IPA の今後の活動に関する意見

・ コンシューマ機器の分野では様々な規格が乱立している（JEITA、CCDS、IoT 推進コンソーシアム等）。IPA が中心的な役割となって、とりまとめをするべき。

・ 民間事業者による IoT ビジネスの発展を阻害しない形で、セキュリティ安全性の高い製品を買ってもらうための啓発活動を行ってほしい。

・ セキュリティ対策には費用がかかるということを発注者に認識してもらう必要がある。発注者の意識改革を進めてほしい。

・ セキュリティスキルのあるエンジニアの市場価値の向上に努めてもらいた

い。
・ 既存の関連団体を束ねて、セキュリティに関する最新情報のすべてを集約・発信できるような団体を組織して欲しい。
・ 脆弱性対策に関するロゴや認定制度があると、消費者の製品選考基準に情報セキュリティが含まれるようになってくると思われる。

(2)ウェブサイト運営者関係団体

(a)普及啓発への協力提案

・ 会員向け発信による協力
  - 全国各地にある下部組織に情報発信を依頼する。実際の発信は各下部組織の判断によるが、メルマガや Web サイトに普及開発資料のリンクを掲載することが可能。
  - 会員企業に対して、ガイド類を紹介するメールを送付することは可能。その際に新たな内容やホットトピックや事例などがあると関心が強まる。
  - 中小企業経営者向けのポータルサイトで紹介可能である。最も簡単なのは中小企業向け News 欄。また経営協会・企業関連のコンテンツで紹介することも可能。
  - 会報誌を毎月発行しており、その記事の中で本件の記事やガイド類のリンクを掲載する方法もある。
・ 組織内の会合やイベントでの協力
  - 中小企業向けのWebセミナーを開催しており、テーマが合えばセキュリティ対策の講義を行うことも調整可能である。
  - 部会活動においてWebセキュリティの意見交換を行う際にIPAに参加してもらうことも可能。各企業の法務担当者が所属する部会があり、IPAのガイドを説明してもらうと良い。
・ 組織間の連携による協力
  - IPA 主催のウェビナーを開催する際に、全国下部組織への通知などの協力が可能。
  - EC モールへの出店検討企業への相談窓口を設置している。年間 300 件程度の問い合わせがあり、これらのうちアドバイスを求める企業に IPA のガイドを送付することは可能。

(b)ガイドの内容に関する意見

・ コンテンツの導線が分かりづらい
  - （Web サイトを含め普及啓発資料内で）情報が整理されておらず、複数のページにリンクする構造で、全体が分かり難い。

・IPA トップページから、目的とするコンテンツに辿り着きづらい。
  - 情報発信の内容・方法を検討すべき
  - 情報セキュリテイの知識がない者には抵抗感がある。「イラストや漫画を活用して内容を簡素化する」、「業種毎の具体的な事例を記載する」、「必要なセキュリティレベルや対策に必要なコストについて記載する」等の改善がなされるとよい。
  - 動画による情報発信が効果的。ストーリー性のあるドラマ仕立ての動画として発信することで、敬遠されがちな IT やセキュリティに関心を持ってもらうきっかけとなる。テーマごとに 5～10 分程度の短い動画でまとめると理解しやすい。
  - 全 26 ページの資料を一度に理解させることは難しい。別途、一枚物の要約資料を作成して誘導する方法も考えられる。
  - 自社 EC サイト運営企業向けに、「自社で Web サイトを制作する際にチェックすべき項目」と、「Web 制作会社を起用する際のチェックすべき項目」の両方が記載されたチェックシートなどがあれば有用。

(c)IPA の今後の活動に関する意見

・中小企業へのサポートを実施すべき
  - 地方は情報も少なく、頼れるベンダーも少ないため、地方の中小企業が利用できるサポートの仕組みを展開してもらいたい。
  - Web セキュリティに関する注意喚起だけでなく、自社サイトの立ち上げ支援などを行うことも、IPA の普及啓発活動において効果的。
  - 身近な場面でサイバー攻撃などの脅威にさらされていることがわかるような普及活動が必要。IPA の「サイバーセキュリティお助け隊サービス」は非常にわかりやすい。
・IPA の知名度向上をすべき
  - IPA の知名度は高いとは言えず、IT 関連を装った詐欺集団も多いため、経営幹部から警戒される恐れもある。まずはマスコミ等を活用して IPA 自身の普及・PR 活動が必要。
・中小企業に関係する他の機関と協力をすべき
  - 中小規模の小売店では、IT 関連業務は内製せずに外部の IT コンサルタントを活用している。したがって小売店を直接のターゲットとするのではなく、IT コンサルタントのような専門家を介した普及活動が効果的。
  - 中小企業庁と中小企業支援機関が運営するネットマガジンがあり、現在使っていないのであれば、活用することを進める。
  - 通販業界や EC サイト運営では、サブスクリプション振興会やリピート通販協会など様々な団体ができている。IPA が主導する形で WEB セキュリテ

ィに関して各団体が協力できる形が作れると良い。

・ 消費者に向けた普及啓発・認証制度を実施すべき
  - 法規制などにより悪質な事業者を完全に排除することは難しいので、消費者教育を進めることも大事である。その時に、安全性を伝えられるわかりやすいマークを作ることは有効である。

(3)製品利用者関係団体

(a)普及啓発への協力提案

・ 会員向け発信による協力
  - メールで紹介するなども可能。
  - ホームページで紹介するなども可能。

・ 組織内の会合やイベントでの協力
  - セミナーで紹介するなども可能。
  - IT サポートをしている人や IT エンジニアを目指す人など普及啓発をしていく立場の人たちを対象に年に 3、4 回の勉強会を実施しているのでそこで紹介することは可能。

・ 組織間の連携による協力
  - 若年層への安全教育のために教育関係者と連携をしている。主婦連合会、消費生活センターへの資料提供などを行っており、Web サイトの安全性に関するセミナーへの要望もあるため、機会があれば IPA に協力をお願いしたい。

(b)ガイドの内容に関する意見

・ 資料の内容は適切だと思う。ただし、興味のある人は知っていて当然の内容であり、興味のない人は、内容が充実していても能動的に情報を得ることはない。興味のない人にどのように届けるかが課題。

・ 知識や関心がない人にとっては理解が難しい。解決策として実際の事件や事例を題材として扱うことが効果的であると考える。① 事件に巻き込まれるリスクとチェックリストの相関を示す、② 実際の事件と照合してポイントをまとめることで、より効果的に理解が深まると考えている。

(c)IPA の今後の活動に関する意見

・ 他組織の活動との差別化を図るべき
  - 総務省や、多数の啓発団体から類似の資料が発信されている。どれも充実した内容であるが、それぞれに目的やターゲットが異なる。これらの資料内容を把握し、目的やターゲットを理解した上で IPA が発信する当該資料との差別化を図る。そのためには先ず、IPA が最も強調して発信したい要点とターゲットを明確にすることが必要である。

・普及啓発を実施する団体との協力を深めるべき
  - IPA 単独で PR するのは難しいと思う。啓発団体に PR を手伝ってもらうだけでなく、IoT や機器を買う場所に置いてもらうなどもできると良い。コンピュータ販売協会等の団体を巻き込めると良い。
  - IPA の情報発信に関する課題として、他の啓発団体に対する能動的なアプローチが少ない。本件のようなヒアリングを行っているにもかかわらず、その後に具体的なアクションが一切なく完結している。他団体が実施する活動を把握し、それらの機会で当該資料の紹介・説明および活用を提案する必要がある。

2.3.普及啓発に関する施策の検討

ヒアリング調査の結果を基に普及啓発に関する施策を検討した結果を報告する。

(1)３つの協力形態について

いずれのヒアリング先も前向きに協力いただける方向で回答、提案をいただいた。協力方式としては、メール配信、ウェブサイト掲載、SNS 発信、会報掲載等の会員向け発信による協力、ワーキンググループや勉強会等の組織内会合や外部向けセミナー等のイベントでの協力、組織間で互いに連携した協力の大きく 3 種類に分かれた。このうち、会員向け発信による協力は直ぐにでも取り組める方法であり、依頼にあたっての周知文を用意し、一部では実際に会員向け周知等を実施していただいた。それ以外は、今後、組織間の情報交換を盛んにし、機会に応じて連携することとした。

(2)中長期の検討課題について

ヒアリングの結果いただいたガイドの内容に関する意見は、いずれもしっかりした検討が必要な内容であり、ガイドの次期改定に向けて対応を検討することとした。

また、IPA の今後の活動等への意見については、中長期的な検討・調整を必要とするものが多いため、引き続き検討課題としていくこととした。

(3)組織間の連携協力について

今回のヒアリングを通して、実際にヒアリングに対応いただけた組織はいず

れも協力に前向きな姿勢を示してくれた。それだけでなく、連携した活動を提案してくれた組織も非常に多く、今回の機会を生かして継続的に連絡を保ち、イベント等のタイミングに合わせて協力関係を深めていくことが重要と考えられる。

特に各組織は、それぞれの対象となる会員を抱え、会員への様々なサービスや啓発活動に従事しているが、情報セキュリティを専門で実施しているものではない。一方、IPA では情報セキュリティに専門に取り組む組織があり、その普及啓発に取り組んでいるが、実際に普及のターゲットとなる企業やユーザへの直接の連絡方法をほとんど持ち合わせていない。つまり、両組織が連携することで、各組織が抱える会員に対して情報セキュリティの向上に向けた知見やサービスを届けていくことが可能になる。

今回試みた各組織の会員向け周知協力を足掛かりに、さらに広範な活動に継続的に結びつつけていくことが重要である。

3.ウェブサイト運営者の窓口設置に関する調査

3.1.調査の概要

(1)目的

ウェブサイトの脆弱性対策の一つとして、運営しているウェブサイトについてのセキュリティ上の問題に関する情報を受け付けるための連絡先となる窓口の設置が挙げられるが、窓口の設置の必要性が理解されにくい状況にある。また、窓口の設置・運営にあたっての課題やその対処方法も広く知られてはいない。

このため、脆弱性情報の迅速な流通による脆弱性による被害の減少を目的に、ウェブサイト運営者による窓口設置・運営体制の強化を実現するため、ウェブサイト運営者による窓口設置について、窓口設置済みのウェブサイト運営者および窓口未設置のウェブサイト運営者の双方に課題等についてヒアリングを実施し、その結果を踏まえ、窓口未設置のウェブサイト運営者に向けた「窓口設置推奨資料」を取りまとめた。

(2)手順

窓口設置済みのウェブサイト運営者および窓口未設置のウェブサイト運営者を対象にヒアリング調査行った。

［調査対象］

①窓口設置済みのウェブサイト運営者

－自組織内に CSIRT を設置している企業等、脆弱性を含めたセキュリティ上の問題に関する連絡先窓口の情報をウェブサイト上に開示している企業であること

②窓口未設置のウェブサイト運営者

［調査件数］

①窓口設置済みのウェブサイト運営者：6 件

②窓口未設置のウェブサイト運営者：5 件

［調査項目］

① 窓口設置済みウェブサイト運営者

・窓口の設置を実施した理由・きっかけ
・窓口の設置・運営にあたり苦労した点、苦労している点
・窓口の設置・運営における課題とその課題解決の方法
・窓口の設置・運営におけるノウハウ
・窓口の設置・運営に関する対応についての疑問点 等

② 窓口未設置ウェブサイト運営者
・窓口の設置・運営ができない理由
・窓口の設置・運営に関する対応についての疑問点 等

3.2. ヒアリング調査

ヒアリング調査結果の概要を以下に報告する。

(1)窓口設置済みウェブサイト運営者のヒアリング結果

(a)窓口の設置を実施した理由・きっかけ

・ 顧客からの要求をきっかけに自社のセキュリティチェックを受けたり、体制を整えたりした。

(b)窓口の設置・運営にあたり苦労した点、苦労している点

・ セキュリテイにお金も掛けられず、十分なリソースも確保できないため、一人 CSIRT 状態である。CSIRT 運営をセキュリティベンダに支援してもらって対応している。

(c)窓口の設置・運営における課題とその課題解決の方法

・ 経営からの指示で CSIRT 設置を検討しても、はじめは何をどうしたら良いのか分からない。セキュリティベンダに支援してもらって対応している。

(d)窓口の設置・運営におけるノウハウ

・ 専門知識を持つプロの支援をもらう。

(e)窓口の設置・運営に関する対応についての疑問

・ 会社としての活動の 99%は実業に傾けられ、滅多に発生しない事象に傾けられるリソースは限られる。一回の健康診断的なセキュリティチェックで終わるところも多い。
・ セキュリティの格付け制度など、ブランディングに役立つような、コストからプロフィットに転換するような状態にならないと、窓口設置は進まない。

(2)窓口未設置ウェブサイト運営者のヒアリング結果

(a)窓口の設置・運営ができない理由

・プライバシーマークのように定まったフォーマットがあれば実施しやすいが、まだ実例が少ないため、周囲への説明や調整に手間がかかる。
・プライバシーマークではサイト運営者は個人情報を預かる立場であるため非常に高い関心と責任意識を持って取組むが、ウェブサイトのセキュリティ対策はサイト制作や運用をする外注任せの風潮がある。運営者自身は問い合わせが来ても困るというスタンスが多い。
・多くの中小企業ではウェブサイト制作、運用を外部委託しており、自社内に対応ノウハウがない。
・中小企業ではそもそもセキュリティ対策への関心が薄いため、経営者に理解してもらうことが難しい。

(b)窓口の設置・運営に関する対応についての疑問点

・インフラとしてAWSを利用するケースが多く、最低限の脆弱性対応はAWS側で対応してくれ、インフラ側で一斉にアップデートしてもらえる。通常気にするのは、AWSの設定漏れくらいであり、窓口設置の必要性を感じていない。
・セキュリティ対策は成果を視認できない上に、いくらコストを掛けようが100%防げるものではないとの認識が多い。どちらかというと、周期的なバックアップや冗長化によって可用性を高める対策の方が現実的であり、窓口設置をして脆弱性の連絡に対応することによって得られるセキュリティ対策としての効果に疑問がある。
・多くのウェブサイト運用を手伝っているが、脆弱性に関する問い合わせも、外部から脆弱性に関する指摘を受けることも殆どなく、窓口を設置する意義が見出せない。
・自社でスクラッチでウェブサイトを制作している会社は少ない。多くはホスティングを利用しており、基本的な対策はホスティング事業者が実施するため、自ら窓口を持つ意識は薄い。
・WordPressを利用しているため、その部分では脆弱性は随時チェックしている。その他、IPAやJPCERT/CCの発信やホスティングサービスの情報提供も気にしており、十分な対応ができているので、さらに窓口設置をする必要性は分からない。
・個人情報は重要な情報資産として社内的に管理体制も整え、問い合わせ窓口も用意しているが、そもそも脆弱性についての窓口設置が必要であるとの認識がなかった。
・ほとんどのサービスはAWSで作っており、アップデートやセキュリティ関連の情報はAmazonから通知が来るので、都度判断している。それ以外のセキュリ

ティ情報も時々チェックしており、それ以上の対応が必要という認識がなかった。

(c)窓口の設置・運営を進めるために必要な条件・施策

・ セキュリティ対策についてレイヤー毎にチェックできるようなチェックリストがあり、簡単にチェックできると良い。ウェブサイトの制作、運営は、フロントエンド、インフラ、バックエンドと担当が分かれており、それぞれ分断されていることが多いので、これらの関係を整理し、エスカレーションの手順やルールを整理してからでないと、窓口の話にならないだろう。
・ 情報セキュリティ対策に限定したガイドやチェックリストでは､中小企業の経営者は興味を持たない。プライバシーマークや DX 推進などと絡めて実施する方が、認識を広められるだろう。
・ 窓口設置・運営に関して、何らかのインセンティブ設計が必要だと思う。IT 企業や事業会社ならウェブサイトは重要だと思っているかもしれないが、業界によって温度差があるため、必要性についてのそもそもの啓発活動が必要だと思う。まずは繰り返し言い続けて、空気感を醸成していくことが必要である。
・ お金に換算しないと動けない経営者もいる｡サイバー攻撃の可能性を伝えても響かないが、過去の事例の賠償額を伝えると重要性を認識してくれる。対策実施にあたっては、セキュリティだけを言ってもダメで、ビジネスとセットにして、事業投資の中にセキュリティ予算を組み込むようにできれば、進みやすくなると思う。
・ 通知する情報はなるべく噛み砕いて伝えるようにして欲しい。(実際に通知を受けたわけではないので分からないが) CVE レベルの情報では、エンジニアならわかるかもしれないが、そうでない人たちが受け付けても、受け止めきれないと思う。

3.3.窓口設置推奨資料の作成

(1)作成方針

窓口設置推奨資料については、次のような方針に基づいて作成を行った。

・ ヒアリング調査結果を基にして、窓口設置推奨資料を作成する。
・ 「窓口設置推奨資料」の作成にあたり、以下の事項について考慮する。
  - ウェブサイト運営者にとって分かり易い内容・構成となるよう工夫する
  - ウェブページでの公表を前提とする

- 50 名から 300 名規模の企業のウェブサイト運営者を対象とする
- Microsoft Word 形式とし、A4 サイズで 4 ページ程度の量とする

・ 内容等については以下を想定する。

(1) 窓口の設置・運営が必要な背景/理由
(2) 実施に際して必要な体制や手順
(3) 実施を阻害する要因/課題
(4) 課題への対処方法

この方針に基づき、窓口設置推奨資料を作成した。詳細は別紙資料を参照のこと。

4. パートナーシップガイドラインの取扱いに関する検討

4.1. 調査の概要

(1) 目的

製品開発者との調整機関である JPCERT/CC からの問題提起を踏まえ、パートナーシップガイドラインの改善方針、改訂案を検討する。

(2) 手順

以下の手順によって、検討を行った。

・第 1 回脆弱性研究会
  - JPCERT/CC からの問題提起
  - 寄せられた意見に基づいて課題の検討

・第 2 回脆弱性研究会
  - 課題の再確認
  - 意見招請の実施

・第 3 回脆弱性研究会
  - 意見の確認

4.2. 検討結果

パートナーシップガイドラインの改善、改訂案作成に向けて 3 つの課題を設定して検討を行った。検討結果の概要を以下に報告する。

(1) 課題設定

・ 課題１：インシデントの分析過程で新たな脆弱性が確認され、パートナーシップへの届出に至ったケースでの情報流通に関する課題
  - 脆弱性の悪用（いわゆる「in the wild」）に関する情報の取扱いや保護についての課題

・ 課題２：脆弱性情報の公表日（45 日目安）に関する課題
  - 実態と目標の乖離、国内の製品開発者・PSIRT のエンカレッジや活動の推進、その他速やかな対応に向けた課題

・ 課題３ :「製品開発者がすべての製品利用者に通知する場合」における取扱い終了に関する課題
  ➢製品開発者と利用者にとってより良い制度とする上での課題

(2)各課題の概要と検討内容

(a)課題１

・ 課題の概要・背景
  ➢サイバーセキュリティ攻撃があり、その被害を分析したところ未知の製品の脆弱性が悪用されていることがわかり、その脆弱性情報がパートナーシップに届出されることがある。
  ➢JVN アドバイザリにおいて、攻撃の発生を示す情報（いわゆる「in the wild」表示）をするにあたり、当該情報の取扱い・保護について、ガイドラインに明示的な記載がない。
  ➢JVN アドバイザリにおける「in the wild」表示は製品利用者が脆弱性対策を進める上で有益な指標となり得るが、ガイドライン上「in the wild」表示するための根拠となる記載が無いため、製品開発者との公表内容の調整に苦慮することがある。

・ 研究会での検討

  研究会において、委員から下記の意見が示された。
  ➢製品利用者に早期の対応を促すためにも、脆弱性の悪用を示す情報はアドバイザリに記載するべきである。また、アドバイザリにおいて悪用を示す場合の文例を示すべきである。
  ➢悪用を示す情報の記載は必須とはせず、製品開発者との調整の上で記載するものとすべきである。
  ➢製品開発者が自社製品に関するサイバーセキュリティ攻撃・インシデントを分析し、その分析により発見された届出をする場合、PSIRT と開発現場が協働する必要がある。PSIRT 活動や製品開発プロセスについて推奨モデルを策定すべきである。
  ➢自社製品の届出を推奨するための仕組みを検討すべきである。

・ 検討を踏まえた今後の対応
  ➢IPA、JPCERT/CC および経済産業省において引き続き検討を実施する。パートナーシップの運用改善により対応できる点については、IPA、JPCERT/CC で確認・調整し対応を検討する。

(b)課題２

・ 課題の概要・背景

- 公表日は起算日から 45 日を目安としているが、現実的には達成が 30%程度に留まっている。
- 45 日以内での公表をより多くするために改善点を検討すべきではないか。
- 制御システム等製品種別やその他の事情により、45 日の達成が難しい製品について、別途適切な公表日の目安を定めることも検討すべきではないか。

・ 研究会での検討

研究会において、委員から下記の意見が示された。

- 45 日という目安は、パートナーシップが目指す究極的な目標でもあり日数自体の変更は不要である。国際的にも、製品開発者の対応目途の日数を変更する議論はなされていないのではないか。
- 45 日を超えたからといって、製品開発者の脆弱性対応が「悪」と捉えられないようにすべきである。
- 無理に 45 日を超えないように対応すれば、修正不備が生じる要因となりかねない。
- 製品開発者の脆弱性対応の期間をより短くするために、製品開発者の実態調査を進めるべき。
- 中小企業や OSS コミュニティを含め、サプライチェーンにおける各当事者の課題を踏まえて検討すべきである。

・ 検討を踏まえた今後の対応

2021 年度に JPCERT/CC において実施した製品開発者向けアンケートの結果を踏まえ、JPCERT/CC において次年度以降に製品開発者、PSIRT の対応状況や課題の調査の実施を検討する。

(c)課題３

・ 課題の概要・背景

- ガイドラインにおいて、JVN 公表をせず取扱いを終了する場合として「製品開発者がすべての製品利用者に通知する場合」と規定している。
- JVN 公表対応を回避するためか、「すべての製品利用者に通知する場合」と判断される要件について製品開発者から問い合わせが JPCERT/CC になされることがあるが、説明をしても必ずしも理解されないこともある。
- 「すべての製品利用者に通知する場合」の条件・要件を、よりわかりやすいものとすべきではないか。

・研究会での検討

研究会において、委員から下記の意見が示された。

- すべての製品利用者に通知するかどうかが基準となるのではなく、ソフトウエア製品の定義における「汎用性を有する製品」かどうか、多数または不特定の利用者がいるかどうかが基準となるのではないか。
- 「汎用性」という用語は、製品が一般的な目的のものであるのか、特殊な目的のためのものであるのかを指し示すためにも使われる用語であり、分かりやすい用語とはいえないのではないか。
- 「汎用性」の有無により判断するとして、JVN 公表の直前のタイミングではなく、より前の時点で判断するべきではないか。
- 製品利用者が限定される場合、JVN 公表をすることで製品利用者の不利益につながることもあるのではないか。
- 取扱い終了できる場合をガイドライン上で例示する等して、わかりやすい内容とすべきである。

・検討を踏まえた今後の対応

- IPA、JPCERT/CC および経済産業省において引き続き検討を実施する。パートナーシップの運用改善により対応できる点については、IPA、JPCERT/CC で確認・調整し対応を検討する。

4.3.パートナーシップガイドラインの取扱い

JPCERT/CC から提起された課題をもとに、パートナーシップガイドラインの改訂について検討を行った。

現時点では、パートナーシップガイドラインの改訂を行う上ではさらなる調査、検討が必要と判断した。引き続きの課題として、検討を継続する。

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) 普及啓発に関する調査

2 章に示した通り、多くの組織が普及啓発への協力の意思を示してくれた。まず直ぐに取り組めることとして、各組織の会員向け周知に取り組むとともに、今回のヒアリングを機に組織間の関係を構築して、今後は継続的な協力関係を維持していくことが重要である。普及啓発活動は一時的なものでは効果が限られるとともに、内容面でも随時改訂が必要であり、タイミングに応じて改訂内容等を展開していくことが重要である。相互の連携の重要性を認識するとともに、相手先組織ごとに普及啓発の対象となる会員等の属性やサイバーセキュリティへの認識状況や取り組み状況の違いなども意識して、相手に応じた多角的な資料作成・資料展開を検討するなどして取り組むことが大事である。

(2) ウェブサイト運営者の窓口設置に関する調査

3 章に示した通り、ウェブサイト運営者向け窓口設置推奨資料を作成した。しかしヒアリングでも明らかなように、多くの中小企業はまだその必要性を認識しておらず、たとえ必要性を認識しても様々な課題の存在から窓口設置に手を付けられないところが多い。今後はさらにほかの方策も含めて多面的な解決策を検討していくことが重要である。

(3) パートナーシップガイドラインの取扱いに関する検討

4 章に示した通り、3 つの課題はそれぞれに難しい問題を含んでいる。改めてソフトウェア開発者が抱える課題の実情を明らかにし、実情を踏まえた対策を検討していくことが大事となる。それらの調査も試みながら、今後のさらなる検討を継続していくことが求められる。

参考１

2021 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

2022 年 2 月 14 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	株式会社東芝
	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

奥田 修司	経済産業省 サイバーセキュリティ課長
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	一般社団法人ソフトウェア協会（SAJ）
戸島 拓生	一般社団法人ソフトウェア協会（SAJ）
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
関澤 弘子	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
津國 剛	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
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（2021 年 12 月 6 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
・普及啓発の促進に関する調査について
・ウェブサイト運営者の窓口設置に関する調査について
・パートナーシップガイドラインの取扱いに関する検討について

■研究会第 2 回会合（2022 年 1 月 17 日）
・前回会合の確認
・普及啓発の促進に関する調査について
・ウェブサイト運営者の窓口設置に関する調査について
・パートナーシップガイドラインの取扱いに関する検討について

■研究会第 3 回会合（2022 年 2 月 14 日）
・前回会合の確認
・普及啓発の促進に関する調査について
・ウェブサイト運営者の窓口設置に関する調査について
・パートナーシップガイドラインの取扱いに関する検討について
・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