情報システム等の脆弱性情報の取扱いに関する研究会

- 2026 年度 報告書 -

2026 年 3 月

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 2025 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 19,859 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、脆弱性対処について製品開発者と製品利用者が抱える課題を把握し、その課題への対処につながる対処策を特定・整理して、「製品開発者向けガイド」と「製品利用者向けガイド」に取りまとめることを通じて、製品開発者と製品利用者の双方が、それぞれ個別に、また、必要があれば協働して、脆弱性の対処を実現できるように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。

2026 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 2025 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 6,392 件、ウェブサイトの脆弱性に関するもの 13,467 件の計 19,859 件であった。四半期毎の届出状況を表 1-1 に示す。

表 1-1　四半期ごとの届出状況

（ソフトウェア等の脆弱性関連情報に関する届出状況[2025 年第 4 四半期（10 月～12 月）]より抜粋）

	2023 1Q	2Q	3Q	4Q	2024 1Q	2Q	3Q	4Q	2025 1Q	2Q	3Q	4Q
累計届出件数[件]	18,026	18,191	18,346	18,651	18,858	18,970	19,086	19,249	19,348	19,448	19,609	19,859
1 就業日あたり[件/日]	3.95	3.94	3.92	3.93	3.93	3.90	3.88	3.86	3.84	3.81	3.79	3.80

(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 1-1 に示す。

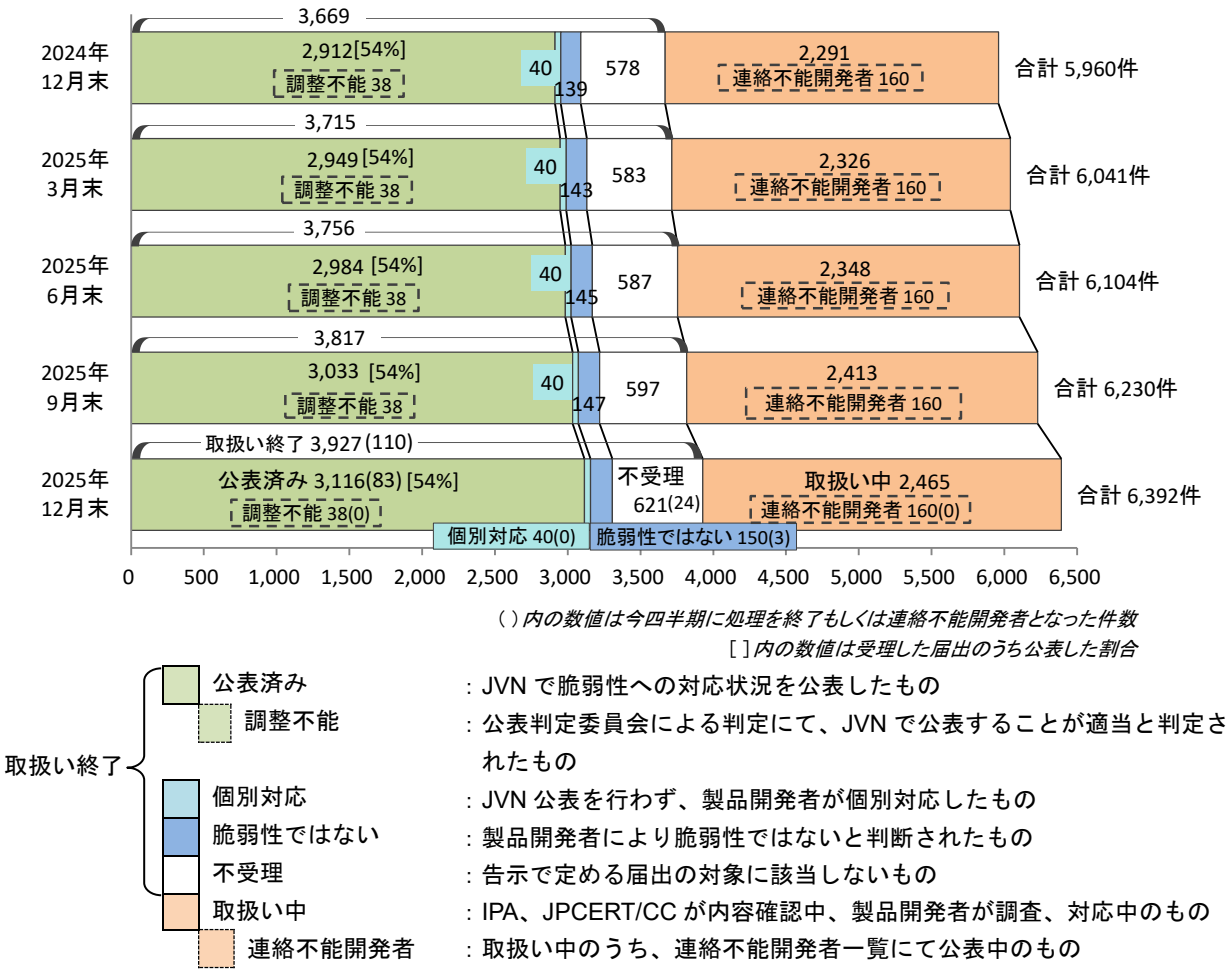


図 1-1　ソフトウエア製品の脆弱性関連情報の届出の処理状況

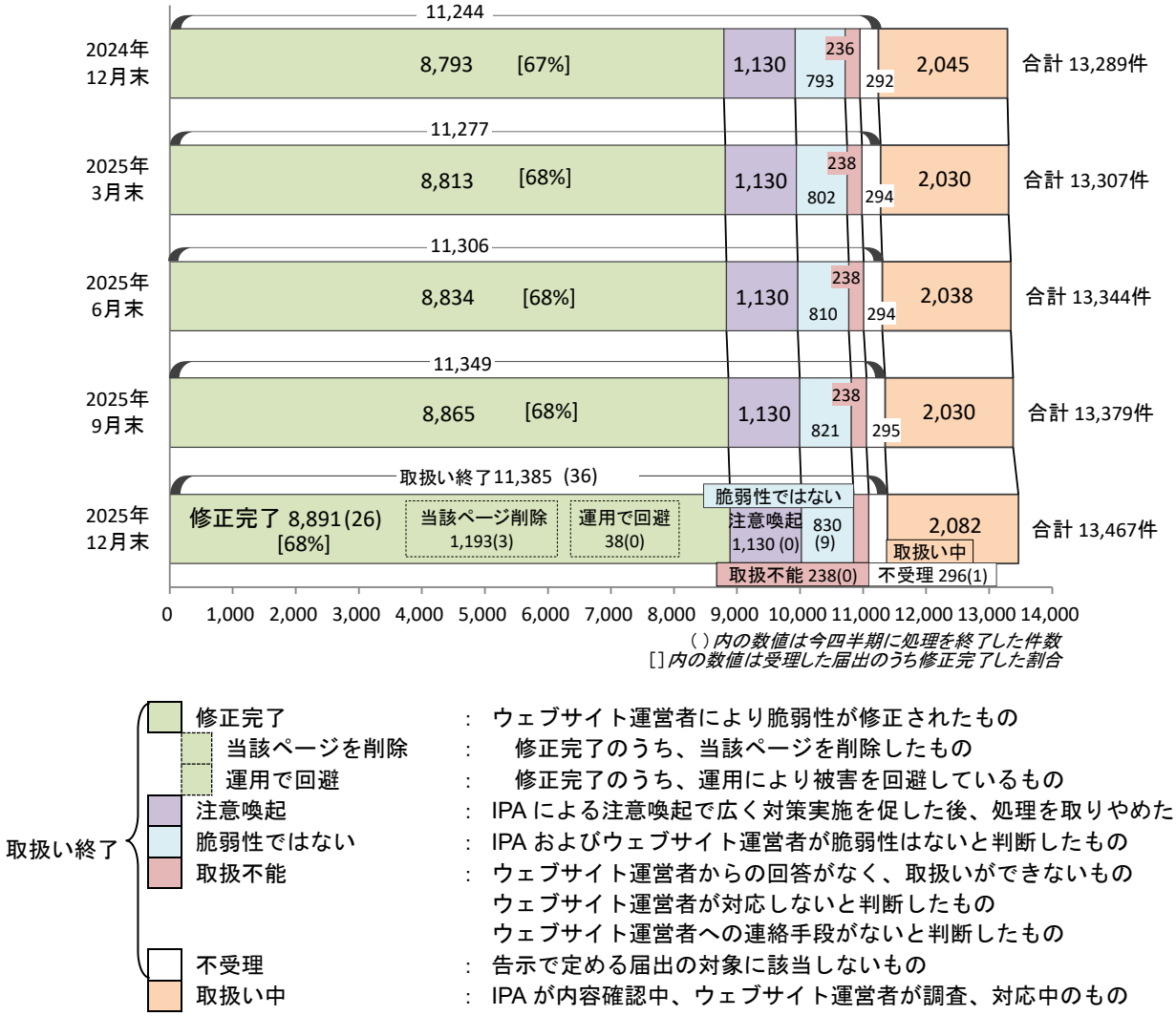
（ソフトウェア等の脆弱性関連情報に関する届出状況[2025 年第 4 四半期（10 月～12 月）]より抜粋）

ソフトウエア製品の脆弱性関連情報の届出 6,392 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 3,116 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 150 件、取扱い中のものが 2,465 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 621 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 1-2 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 1-2　ウェブサイトの脆弱性関連情報の届出の処理状況

（ソフトウェア等の脆弱性関連情報に関する届出状況[2025 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 13,467 件のうち、修正が完了したものが 8,891 件（うち運用で回避されたもの 38 件、当該ページを削除して対応したもの 1,193 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 830 件、取扱い中のものが 2,082 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 238 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 296 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 2025 年 12 月末までに 6,139 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

2025 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 3,116 件である。届出受付開始から 2025 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 1-3 に示す。45 日以内に公表されている件数は全体の 28%であり、公表までに時間を要している割合が大きい。

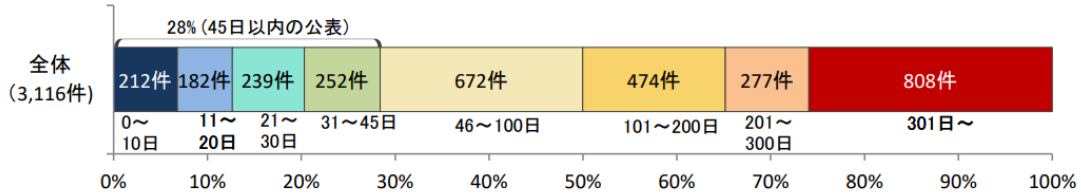


図 1-3　ソフトウエア製品の脆弱性公表までに要した日数

（ソフトウェア等の脆弱性関連情報に関する届出状況[2025 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

2025 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 3,707 件である。このうち、2025 年度第 4 四半期（2025 年 10 月から 2025 年 12 月末まで）に JVN で公表した脆弱性関連情報は 103 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 2025 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 6,392 件のうち、不受理分を除いた 5,771 件の製品種類別内訳を図 1-4 に示す。「ウェブアプリケーションソフト」が 40%を占めている。

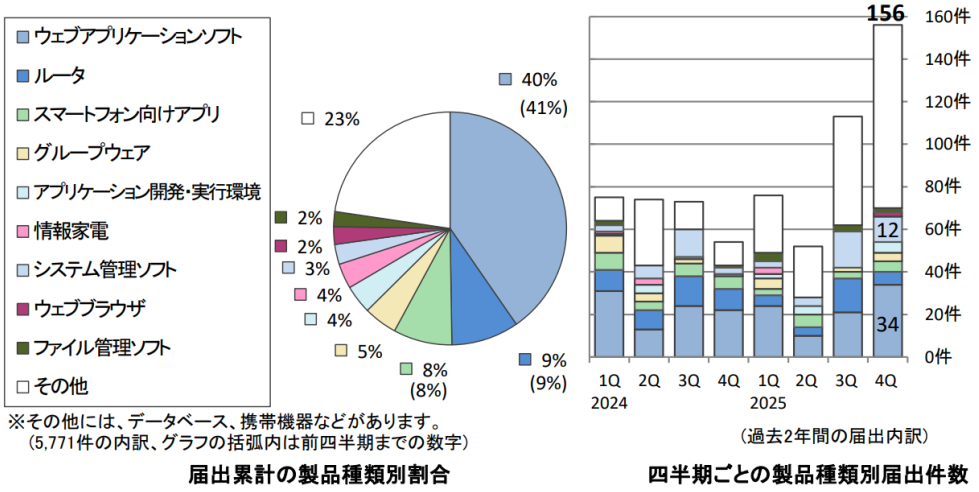


図 1-4　ソフトウエア製品種類別の届出内訳（届出受付開始～2025 年 12 月末）

（ソフトウェア等の脆弱性関連情報に関する届出状況[2025 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 2025 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 6,392 件のうち、不受理のものを除いた 5,771 件の原因別の内訳を図 1-5 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 52%を占める。

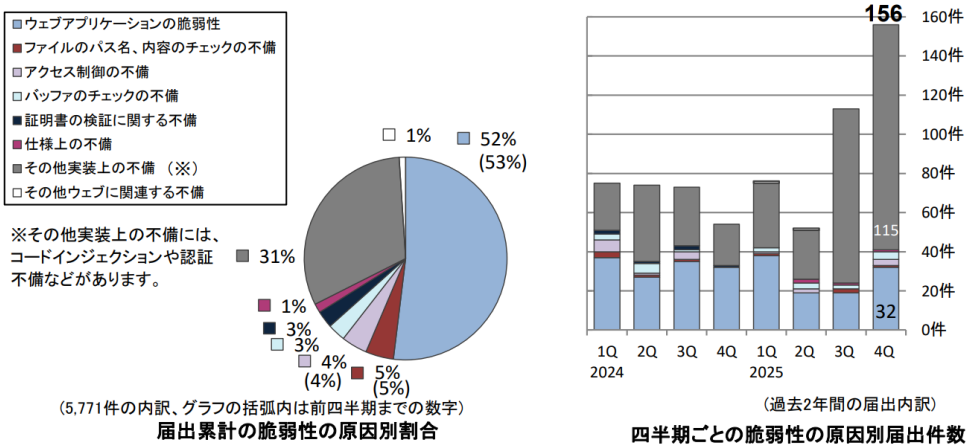


図 1-5　ソフトウエア製品の脆弱性原因別の届出内訳（届出受付開始～2025 年 12 月末）

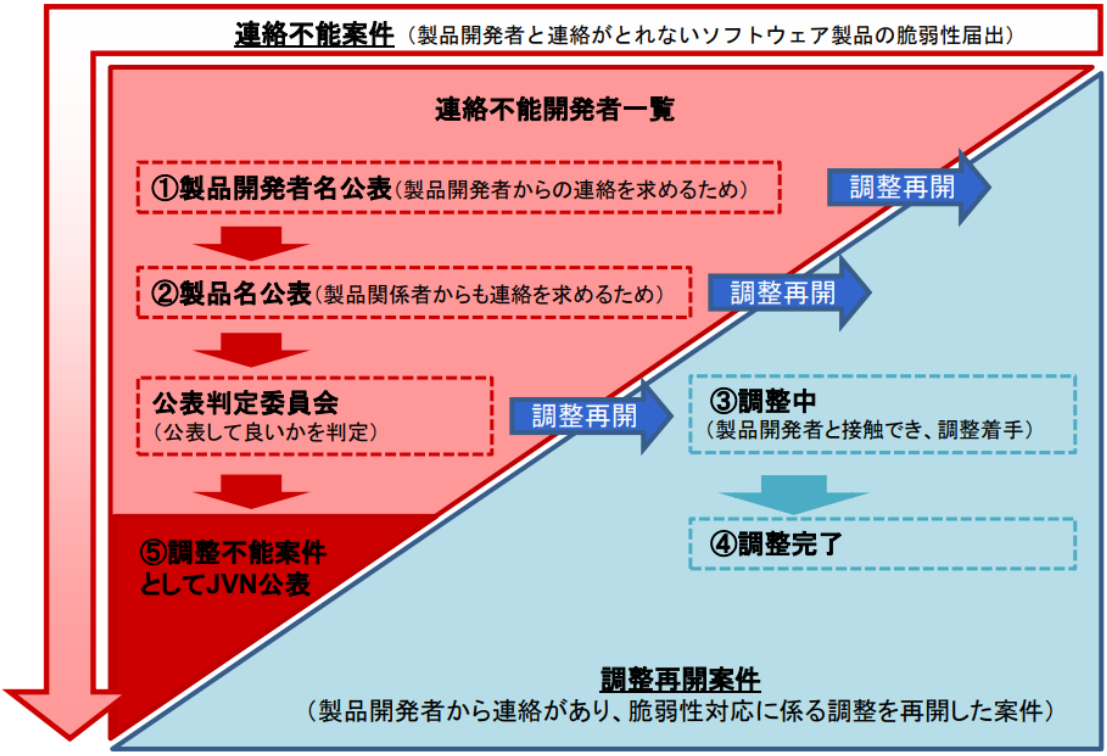
（ソフトウェア等の脆弱性関連情報に関する届出状況[2025 年第 4 四半期（10 月～12 月）]より抜粋）

(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等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。2025 年 12 月までに累計で 87 件（電力分野 49 件、政府機関 38 件）を提供した。

(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 2025 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 53 件が調整を再開（その中の 33 件が調整完了）したが、160 件は製品開発者と連絡がとれない状況にある（図 1-6 参照）。



2025年 第3四半期	160件 （①1件 ②159件）	53件 （③20件 ④33件）	⑤38 件	合計 251件
2025年 第4四半期	160件 （①1件 ②159件）	53件 （③20件 ④33件）	⑤38 件	合計 251件

図 1-6 連絡不能案件の処理状況（連絡不能開発者一覧公表開始～2025 年 12 月末）

（ソフトウェア等の脆弱性関連情報に関する届出状況[2025 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

2025 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 8,891 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 1-7 に示す。全体の 52%の届出が 30 日以内、70%の届出が 90 日以内に修正されている。

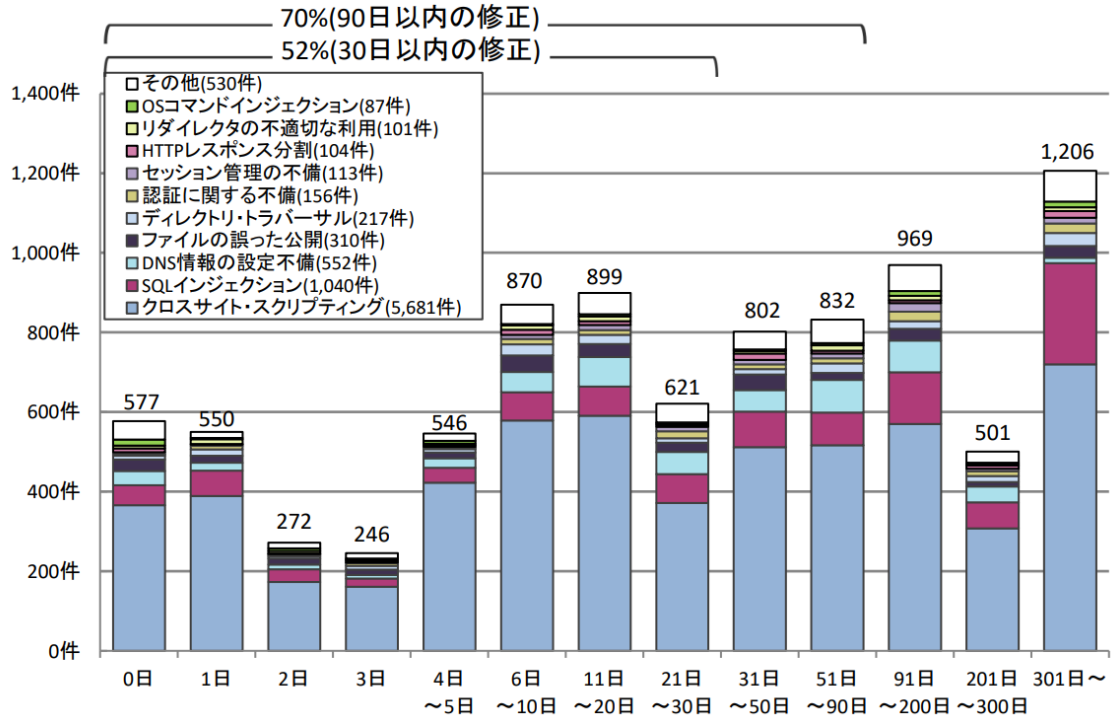
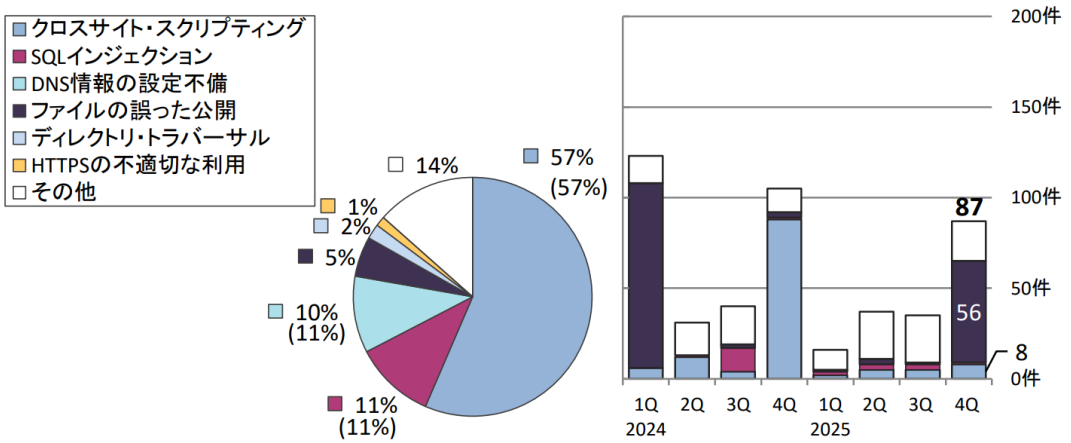


図 1-7　ウェブサイトの脆弱性修正に要した日数（届出受付開始～2025 年 12 月末）

（ソフトウェア等の脆弱性関連情報に関する届出状況[2025 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

2025 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 13,467 件のうち、不受理のものを除いた 13,171 件の種類別内訳を図 1-8 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」(57%)、「SQL インジェクション」(11%)、「DNS 情報の設定不備」(10%)の割合が高く、この３つだけで全体の 78%を占める。



(13,171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)

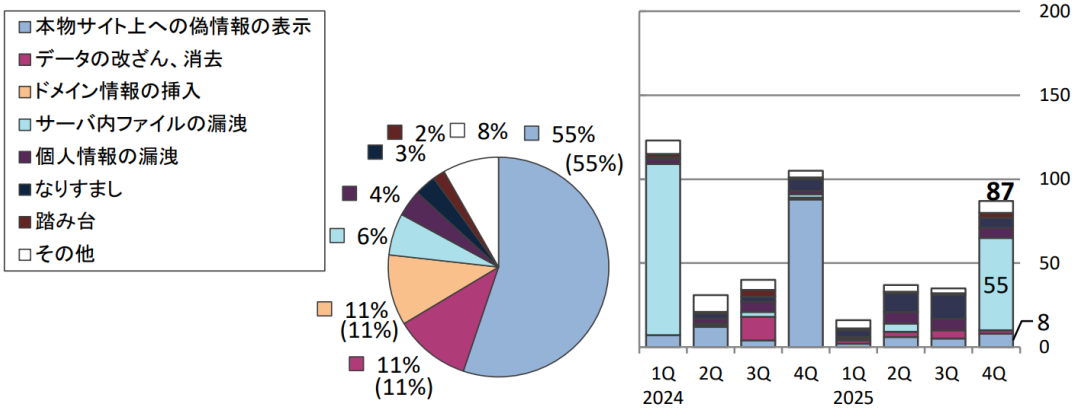
四半期ごとの脆弱性の種類別届出件数

図 1-8　ウェブサイトの脆弱性種類別内訳（届出受付開始～2025 年 12 月末）

（ソフトウェア等の脆弱性関連情報に関する届出状況[2025 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 1-9 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」(55%)、「データの改ざん、消去」(11%)、「ドメイン情報の挿入」(11%)の割合が高い。



(13,171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 1-9　ウェブサイトの脆弱性脅威別内訳（届出受付開始～2025 年 12 月末）

（ソフトウェア等の脆弱性関連情報に関する届出状況[2025 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 1-10 に示す。経過日数が 90 日以上である件数は 1,050 件で、前年同期（1,045 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。

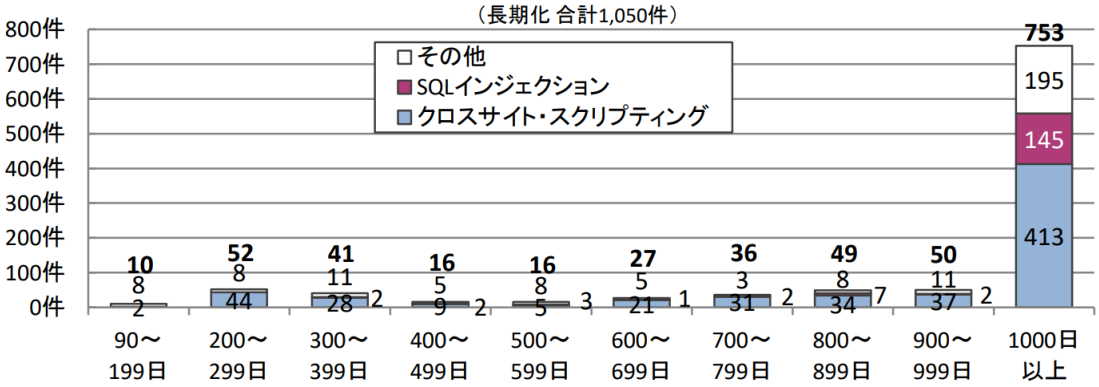


図 1-10　取扱いが長期化（90 日以上経過）しているウェブサイトの経過日数と脆弱性の種類

（ソフトウェア等の脆弱性関連情報に関する届出状況[2025 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、製品開発者（PSIRT 組織）における脆弱性対応、製品利用者（CSIRT 組織）における脆弱性対応を支援するため、製品開発者、製品利用者のそれぞれに向けてガイドを作成した。以降の章では、これらに関する検討成果を示す。

①製品開発者の脆弱性対策に関する調査及び製品開発者向けガイドの作成
・製品開発者の抱える課題に関する文献調査
・製品開発者に対するアンケート調査
・製品開発者に対するヒアリング調査
・製品開発者向けガイドの作成

②製品利用者の脆弱性対策に関する調査及び製品利用者向けガイドの作成
・製品利用者の抱える課題に関する文献調査
・製品利用者に対するアンケート調査
・製品利用者に対するヒアリング調査
・製品利用者向けガイドの作成

また、研究会の各会合においては、上記のガイドの作成に関連する検討に加え、サイバー対処能力強化法の施行に伴う告示の改正についても審議・検討を実施した。

2. 製品開発者の抱える課題に関する調査及び製品開発者向けガイドの作成

2.1. 調査の概要

(1) 目的

近年においては、製品開発者に対してソフトウェア開発ライフサイクル全体にわたって脆弱性管理を行うことが求められており、特に計画・要件定義段階や設計・開発段階といった上流工程でセキュリティ対策を組み込むという「セキュア・バイ・デザイン」や「シフトレフト」の考え方の重要性が再認識されている。

そうした中、欧州市場に上市するデジタル製品に対して、サイバーセキュリティ要件や脆弱性ハンドリング要件の遵守を求めるEUサイバーレジリンス法や、IoT 機器に対する脆弱性管理等を求めるセキュリティ要件適合評価及びラベリング制度（JC-STAR）などを契機として、製品開発者においては、PSIRT（Product Security Incident Response Team）体制の構築が進んできている。

さらに、PSIRT体制では、これまでソフトウェア製品やソフトウェアを組み込んだハードウェア製品に関して、外部から脆弱性報告を受領した場合や未修正の脆弱性が開示され悪用された場合などの緊急時の対応を主な役割とし、その部分に重点が置かれてきたが、このような状況を踏まえ、脆弱性の作り込みを回避するために、安全なソフトウェア開発を実践する場合や設計・開発するソフトウェアにセキュリティ機能を組み込む場合などの平常時の対応を役割として明確に位置付けることが必要になっている。

このような背景のもと、製品開発者の抱える課題や脆弱性対策について、文献調査、アンケート調査及びヒアリング調査を実施し、製品開発者向けガイドをとりまとめた。

(2) 手順

最初に、2019年度に開催された脆弱性研究会で作成した、「脆弱性対処に向けた製品開発者向けガイド」をもとに必要となる加除修正を施しつつ、製品開発者の抱える課題に関する国内外の文献調査を実施し、その結果を反映して、製品開発者向けガイドの骨子案を作成した。

次に、製品開発者に対するアンケート調査を実施するにあたり、製品開発者

の抱える課題や脆弱性対策について仮説を構築して、アンケート調査票を作成するとともに、アンケート調査を実施した。

さらに、アンケート調査の内容を深堀りして、製品開発者が実際に取り組んでいる脆弱性対策や、業務上抱える課題を把握するにあたり、ヒアリング調査項目を作成するとともに、ヒアリング調査を実施した。

その上で、製品開発者向けガイドの骨子案に対して、アンケート調査やヒアリング調査の結果を反映して、加除修正を施しつつ、製品開発者向けガイドをとりまとめた。

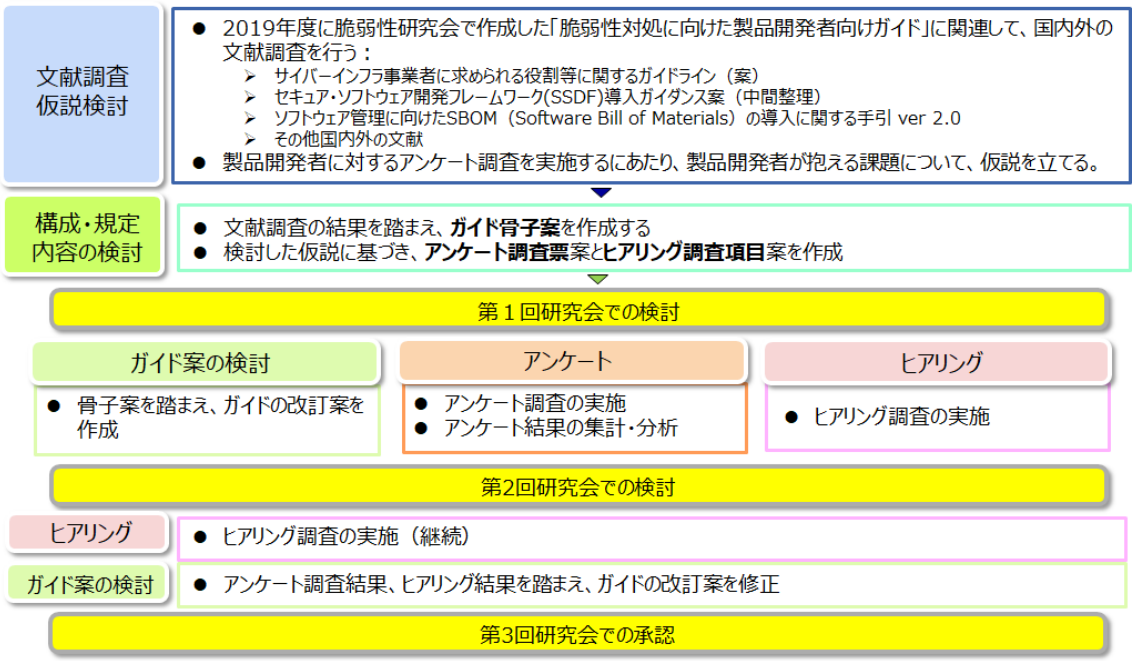


図 2-1 「製品開発者向けガイドの策定」の実施内容全体

2.2. 製品開発者の抱える課題に関する文献調査

(1) 文献調査概要

以下に実施した文献調査の概要を示す。

［文献調査主旨］

サイバーインフラ事業者が認識すべき責務や、セキュア・ソフトウェア開発フレームワーク（SSDF：Secure Software Development Framework）導入の基本方針、導入プロセス、ソフトウェア部品表（SBOM：Software Bill of Materials）を活用した脆弱性管理プロセスについて考慮しつつ、これらに関連して、製品開発者の抱える課題を把握する。

［調査対象］

「サイバーインフラ事業者に求められる役割等に関するガイドライン（案）」や「セキュア・ソフトウェア開発フレームワーク（SSDF）導入ガイダンス」を含め、以下の国内外の文献を対象に文献調査を行った。

①CISA「サイバーセキュリティリスクのバランスを変える：セキュアバイデザイン、セキュアバイデフォルトの原則とアプローチ」
②NIST SP 800-218 Secure Software Development Framework (SSDF) Version 1.1
③セキュア・ソフトウェア開発フレームワーク(SSDF)導入ガイダンス案（中間整理）
④ソフトウェア管理に向けた SBOM（Software Bill of Materials）の導入に関する手引 ver 2.0
⑤サイバーインフラ事業者に求められる役割等に関するガイドライン（案）
⑥FIRST PSIRT Services Framework Version 1.1
⑦ASD ACSC Choosing secure and verifiable technologies
⑧CISA Software Acquisition Guide for Government Enterprise Consumers
⑨CISA Information Technology (IT) Sector-Specific Goals (SSGs)
⑩BSA | The Software Alliance The BSA Framework for Secure Software : A NEW APPROACH TO SECURING THE SOFTWARE LIFECYCLE
⑪NSA ESF Securing the Software Supply Chain : RECOMMENDED PRACTICES GUIDE FOR DEVELOPERS

［調査方法］

文献調査、Web 調査

(2)文献調査を踏まえて想定する仮説・問題

文献調査の結果から得られた脆弱性対処における課題を踏まえ、製品開発者が抱える構造的課題として、以下に示すものを仮説として想定することとした。

- 組織として情報受付窓口の未整備や部門間での情報共有・管理をする仕組みがない

  情報が共有されないことにより、脆弱性対処が放置されたり、情報がたらい回しになって、脆弱性対処が遅れたりしている。
- 組織内で脆弱性対処について、責任を担い、部門間で調整し対処を促進する仕組みがない

脆弱性対処が遅れることにより、組織の信用が失墜したり、適切な対処（情報公開等）が行われないことにより、利用者が不利益を被ったりしている。

- セキュア・バイ・デザインやセキュア・バイ・デフォルトへの対応が求められているが、組織全体として対応を担当する部門がない
  要求事項への対応が遅れ、製品が調達要件等を満たすことができなくなる。
- ソフトウェアサプライチェーンリスクへの取り組みに対応する部門がない
  一貫したサプライチェーン管理ができず、サプライチェーンリスクの影響を低減することができなくなる。
- 海外の法制（EU サイバーレジリエンス法等）へ対応する組織（部門）や仕組みが整備されていない
  要求事項への対応が遅れ、製品が調達要件等を満たすことができなくなる。
- 経営部門が脆弱性対処の必要性の認識、取り組む動機が乏しい
  組織として、脆弱性対処のリソースが配分されず、組織としての脆弱性対処の体制構築、対処が行われない。
- 自組織以外から調達した部品（ソフトウェア等）の脆弱性対処に関する対応方針や仕組みが整備されていない
  脆弱性対処が遅れることにより、組織の信用が失墜したり、適切な対処（情報公開等）が行われないことにより、利用者が不利益を被ったりしている。

2.3. 製品開発者に対するアンケート調査

(1) アンケート調査概要

以下に実施した製品開発者に対するアンケート調査の概要を示す。

［調査主旨］

製品開発者の抱える課題や脆弱性対策のうち、ソフトウェア開発ライフサイクルを考慮しつつ、以下に示す内容についてより詳細かつ適切に把握する。

①PSIRT 体制に関する課題への対応策
②国内外の法令・規制への対応のための体制に関する課題への対応策
③ソフトウェアを構成するコンポーネントにおける課題への対応策

④セキュア・バイ・デザインやセキュア・バイ・デフォルトに対応した製品の開発に関する課題への対応策
⑤脆弱性情報の外部からの連絡の受付や対策情報の公表対応に関する課題への対応策
⑥脆弱性パッチの提供等のサポート体制の維持及びその終了に関する課題への対応策
⑦経営層・管理層のコミットメントに関する課題への対応策

［調査対象］

不特定または多数の顧客に提供するソフトウェアの開発を行っている事業者（なお、特定の顧客に提供するソフトウェアの開発を行っている事業者はこれに含まれない。）かつ、以下のいずれかの条件を満たす事業者を対象にアンケート調査を行った。

①自組織において、上記で開発したソフトウェア自体を製品として提供している事業者（いわゆるソフトウェアの場合）
②自組織において、上記で開発したソフトウェアを組み込んだ製品を提供している事業者（いわゆるハードウェアの場合）

また、アンケートの想定回答者は、ソフトウェアの開発を担う開発部門、ソフトウェアのセキュリティ維持を担うセキュリティ部門又は品質管理部門とし、いずれでも回答可能とした。ただし、自部門のみでの回答が難しい場合には、他部門とも調整して回答してもらうこととした。

［アンケート項目］

回答組織の属性・体制（７問）
問１　回答者の所属部門
問２　回答組織の従業員数
問３　採用しているソフトウェア開発手法とその開発実績
問４　PSIRTの構築の有無・構築形態
問５　PSIRTの配置要員数
問６　PSIRTが担当している対応業務
問７　セキュアなソフトウェア開発の実践等に関する担当部門
計画フェーズ（３問）
問８　内部関係者・外部関係者との連携体制の構築
問９　リスクベースの分析・評価の実施内容
問10　ソフトウェアのセキュリティ確保に向けた取組方針
要件定義フェーズ（３問）
問11　セキュリティ要件の特定・文書化
問12　内部関係者・外部関係者との間での問題発生状況
問13　問題の再発防止のための改善策
設計フェーズ（８問）
問14　ソフトウェアコンポーネントのセキュリティ確保対策
問15　セキュリティ要件への準拠状況の確認の有無・方法
問16　対処できないリスク等への対応方法
問17　ソフトウェアにデフォルトで実装しているセキュリティ機能
問18　提供するソフトウェアでの問題発生状況とその原因
問19　問題の再発防止のための改善策
問20　脆弱性の作り込み回避のためのプロセスの定義・実装
問21　特定されなかった脆弱性を発見するためのテストの実施
供給フェーズ（１問）
問22　ソフトウェアを配信する際のセキュリティ確保対策

運用・保守フェーズ（13問）
問23　残存する脆弱性を発見するための対策
問24　脆弱性発見後の対処すべき問題の分析・特定
問25　ソフトウェア部品表(SBOM)の具体的な活用方法
問26　脆弱性に対処した際の問題発生状況とその原因
問27　問題の再発防止のための改善策
問28　利用顧客等向けに必要となる情報提供
問29　残存する脆弱性が発見されたときに直面した事態
問30　インシデントが発生した場合の対策
問31　利用顧客等におけるインシデントの発生有無
問32　ソフトウェアの脆弱性が作り込まれた原因
問33　インシデントの発生に備えた利用顧客等との契約対応
問34　インシデントが発生した場合の利用顧客等への対応
問35　ソフトウェアのセキュリティ維持に関わる対応責任の要求
廃棄フェーズ（１問）
問36　顧客のシステム等の停止・廃棄時における対策
ソフトウェア開発ライフサイクル全体（６問）
問37　セキュリティ維持の必要性に対する経営層の認識
問38　ポリシーや計画等のセキュリティ文書の策定状況
問39　特定したリスクを軽減するためのツールの利用状況
問40　外部委託の活用状況
問41　ソフトウェア開発や脆弱性対処での生成AI活用の取組
問42　生成AIの活用における課題
ヒアリングへの協力（１問）
問43　ヒアリングへの協力可否

図 2-2 アンケートの構成

○回答組織の属性・体制に関するアンケート項目（問１～問７）
○計画フェーズにおける課題と対応策に関するアンケート項目（問８～問 10）
○要件定義フェーズにおける課題と対応策に関するアンケート項目（問 11～問 13）

〇設計フェーズにおける課題と対応策に関するアンケート項目（問 14～問 21）
〇供給フェーズにおける課題と対応策に関するアンケート項目（問 22）
〇運用・保守フェーズにおける課題と対応策に関するアンケート項目（問 23～問 35）
〇廃棄フェーズにおける課題と対応策に関するアンケート項目（問 36）
〇ソフトウェア開発ライフサイクル全体における課題と対応策に関するアンケート項目（問 37～問 42）
〇その他（ヒアリングへの協力可否）（問 43）

(2)アンケート調査結果から得られた知見

アンケート調査結果から得られた主な知見を以下に示す。

- 製品開発者のほとんどが、PSIRT を構築済み。PSIRT の組織形態としては、IT・セキュリティ部門の配下が最も多く、次いで多いのは、開発部門の配下、品質管理部門の配下、経営層直轄の順である。
- PSIRT の要員数としては、10 名未満が中心。担当している対応業務としては、サプライチェーン強化や、ソフトウェア開発ライフサイクル全体のリスク管理に関わる業務などが十分にカバーされていない。
- ソフトウェアの脆弱性対処や、ソフトウェア開発ライフサイクル全体におけるセキュリティ維持のために必要な関係者との連携体制については、自組織内の関連する関係部門との間で事前に業務・役割分担の明確化や具体的な手順の策定等を行っている場合が多い。一方、ソフトウェアの開発や運用・保守の委託先やソフトウェアコンポーネントの調達先などの外部との連携体制については十分とは言えない。
- ソフトウェアのセキュリティ要件を定義する際に、製品開発者のほとんどがリスクベースの分析・評価を実施している。但し、攻撃シナリオ・攻撃ツリーの作成や、脅威の発生可能性や事業被害等への影響度の分析といったより高いセキュリティレベルでのリスク分析・評価の実施については、十分に浸透していない。
- サポート期間の設定や、セキュアな調達については、取組方針を定めていない製品開発者が比較的多い。
- ソフトウェアの開発環境、ビルド環境、テスト環境、配布環境及びそれらのツールについては、満たすべきセキュリティ要件を特定していない製品開発者が多い。
- ソフトウェアコンポーネントのセキュリティ確保のための対策については、多くの製品開発者で対策が講じられているものの、実施している対策の内容

はさまざまであり、全体としてみると、ソフトウェアサプライチェーンリスク管理計画の策定や、調達先に対する自組織で定めたセキュリティ要件の説明、セキュリティを考慮した調達仕様の策定といった対策はいずれも実施率が低調であった。

- 脆弱性の作り込みを回避するためのセキュアソフトウェア開発プロセスについては、セキュアコーディングの実践に関するプロセスが主流。一方で、セキュアなビルドの実践に関するプロセスやデフォルトでの安全な設定・構成に関するプロセスは十分に実装されていない。
- 特定されたリスクへの対処状況の確認や、定義されたセキュリティ要件への準拠状況の確認については、設計・開発フェーズでは実施できていても、運用・保守フェーズでは実施できていない製品開発者が一定数存在する。
- レビューや分析・評価を行った結果、対処できないリスクや準拠できないセキュリティ要件が出てきたときの例外措置の実施可否は、設計・開発の現場において判断する場合が多い。
- セキュアバイデフォルトとして、ソフトウェアに実装しているセキュリティ機能については、通信データの傍受や改ざんを防ぐための暗号化通信機能や、不正アクセスを防ぐためのインシデント検知機能、ログ出力機能が主流である。それらに比べて、運用フェーズで検出された脆弱性に対処するためのアップデート機能や、廃棄フェーズにおいてデータや設定情報の漏えいを防ぐための初期化機能の実装については十分とは言えない。
- すべての製品開発者が、ソースコード等のレビュー・分析を通じて特定されなかった脆弱性を発見するために、脆弱性診断テストを実施している。一方で、ファジングや侵入テストについては、実施率が低い。
- ソフトウェアやコンポーネントの脆弱性が発見された後に対処すべき問題であるかを分析・特定するために、SBOM を活用している製品開発者は全体の半数を下回る。SBOM は、脆弱性の箇所の特定や影響範囲の分析、リスクの受容可能性の確認、脆弱性対応の優先順位付けに活用しているケースが多い。その他にも、脆弱性リストの取得やソフトウェアライセンスの管理等において活用されている。
- ソフトウェアの開発や、ソフトウェア開発ライフサイクル全体における脆弱性対処において、生成 AI の活用に関する取組を実施している製品開発者が多い。生成 AI を活用して自動化・効率化している領域については、プログラムのコーディングや、テストケース・テストコードの生成、コードレビュー・品質レビューなど、多岐にわたる。
- 生成 AI の活用においては、品質面の課題（生成されたコードへの予期せぬ不具合の混入や保守性の考慮不足、アウトプットの信頼性に関する判断基

準・手法の未整備など）や、ガバナンス面の課題（生成 AI の進化に追いつけない社内体制や、ルールの適応による利用制限、社内標準の未整備など）、教育面の課題（生成されたコードや出力された情報を精査する人間の能力不足など）、運用面の課題（リスク判定が難しいなど）が見られた。

- リリースしたソフトウェアの脆弱性を起因としたインシデントが発生した場合の対策においては、インシデント対応計画の策定や、緊急対策会議の設置に必要な社内規程の作成、手順どおりに業務を行えることを検証するための訓練・演習それぞれの実施率が比較的低い。
- ソフトウェアのセキュアな利用を促進するために、利用顧客等に対して、ソフトウェアの適切な導入・設定・操作に関する情報や、ソフトウェアの保守・サポート終了（EOL：End of Life）に関する情報、ソフトウェアの販売終了（EOS：End of Sales）に関する情報を継続的に提供している製品開発者は比較的多いが、他方、ソフトウェアの適切な廃棄に関する情報を継続的に提供している企業は少ない。

2.4. 製品開発者に対するヒアリング調査

(1) ヒアリング調査概要

以下に実施した製品開発者に対するヒアリング

［調査主旨］

アンケート調査の回答内容をさらに深堀りして、製品開発者が実際に取り組んでいる脆弱性対策や、業務上抱える課題を把握する。

［調査対象］

PSIRT 組織を有する事業者、PSIRT 組織を有さない事業者の双方を対象にヒアリング調査を行った。

［主なヒアリング項目］

ヒアリング項目	ヒアリング内容
製品開発者が実際に取り組んでいる対策、業務上抱える課題	以下に示す観点に基づき、アンケート調査の回答内容を深堀りして、どのような背景や事情があるか。また、何か課題になるような事象が起きていないか。課題がある場合に、どのような解決策を講じているか。 ①PSIRT 体制に関する課題への対応策 ②国内外の法令・規制への対応のための体制に関する課

	題への対応策 ③ソフトウェアを構成するコンポーネントにおける課題への対応策 ④セキュア・バイ・デザインやセキュア・バイ・デフォルトに対応した製品の開発に関する課題への対応策 ⑤脆弱性情報の外部からの連絡の受付や対策情報の公表対応に関する課題への対応策 ⑥脆弱性パッチの提供等のサポート体制の維持及びその終了に関する課題への対応策 ⑦経営層・管理層のコミットメントに関する課題への対応策
経営層の関与・関心の状況	脆弱性対処やソフトウェア開発ライフサイクル全体でのセキュリティ維持に対する経営層の関心事項は何か。
過去に生じた脆弱性対応に関するトラブルやその対応	脆弱性対応に関するトラブルは、どのような問題であったか。問題の再発防止のため、どのような対策を講じたか。
脆弱性の対処に関するベストプラクティス	脆弱性の対処に関する取組で特に力を入れているものは何か。
課題に対する対応にあたって実施した事例や対応が成功した事例	業務上抱える課題に対して、対応上何か工夫を行っている事例はあるか。
ヒアリング実施時点の製品開発者向けガイド案に関する意見	アンケート調査により把握した課題に対して検討した解決策（ガイド案に記載した解決策）が有効であるかどうかの意見や、検討した解決策以外の解決策（ガイド案に記載していない解決策）として考えられる案についての意見があるか。

(2) ヒアリング調査結果から得られた知見

ヒアリング調査結果から得られた主な知見を以下に示す。

- PSIRT 組織には、IT・セキュリティ部門や品質管理部門等の関連部門から人材を出してもらい、アサインすることで、それぞれの部門との連携を取りやすくしている。また、開発部門や開発機能を持つグループ会社等の現場側においても、PSIRT 組織で定めた全社方針や規程を、現場のルールに組み込んで統制を進めてくれる人材をアサインしてもらっている。これらの人材を含めた、バーチャルな組織として PSIRT 体制を構築している。

- 調達先に求めるセキュリティ対策については、現状では、脆弱性が発見されたときにその情報を連携してほしい、外部から脆弱性情報を受ける対応窓口を設置してほしい、ということについて調達先に依頼することを考えている。一方で、追加で要求したところで、対応してくれる調達先がどれだけあるのかという課題がある。また、追加の要求に対応できないと言われた場合に、取引先を切れるかどうかの判断は、事業部においても難しいはずである。
- エンドユーザーを把握しきれないという課題がある。誰が製品を使っているかが分からないため、ユーザーマニュアルの周知が重要になると考えている。
- 自社開発した IoT 製品における JC-STAR の★1(レベル 1)の取得を契機として、製品セキュリティの必要性が社内で認識され、さらに脆弱性管理手順を定めることを求められたことから、脆弱性管理に関わる社内規程の整備や、脆弱性情報の報告や、報告受領後の対応、情報公開、継続的な改善に関わる取組からなる脆弱性開示ポリシーの策定・公開につながった。
- 脆弱性について社外から指摘され、取組を始めてから数年たって、経営トップに脆弱性対応の仕組みが必要であることを認識してもらい、各事業部における製品セキュリティ担当者の人員配置が決定された。こうした各事業部側の推進体制を構築するうえで経営トップが果たす役割は大きい。
- 社内に製品セキュリティ資格制度を設けており、各レベルの認定を受けるためには、脅威分析で何を実施し、何を得られるかなどを知らなくてはならない。脅威分析を実施する人と脅威分析した結果を監査する人で必要な知識・スキルが違うのでその点も分けて研修を実施している。
- 開発工程が自動化される中で、CI/CD パイプラインを作り、日々ビルド、テスト、デプロイが自動で行われているが、その部分におけるセキュリティ対策は非常に重要と考えている。
- ソフトウェアのリリース前には脆弱性診断により、日々使用するライブラリ、OSS などの脆弱性を検出する取組などを実施している。リリース後にはライブラリが定期的にアップデートされる中で脆弱性が新たに出てくる可能性もあるため、ソフトウェア構成解析（SCA：Software Composition Analysis）を定期的に実施し、ライブラリの脆弱性管理を進めている。
- 組織内に AI について詳しく勉強している社員がいて、より良い回答品質を得るための AI への質問の投げ方、チューニングの仕方、判断の仕方などをノウハウとして蓄積していき、そのようなノウハウをチーム内で共有することにより、開発業務の効率化につながっている。

2.5. 製品開発者向けガイドの作成

(1) 製品開発者向けガイドの作成

前述した文献調査をもとに作成した製品開発者向けガイドの骨子案に対して、アンケート調査やヒアリング調査の結果を反映して、加除修正を施しつつ、製品開発者向けガイドを取りまとめた。

製品開発者向けガイドの各章は、前述した「脆弱性対処に向けた製品開発者向けガイド」の構成を踏襲し、意義、実施内容、実施手順、開示方法の 4 つにより構成した。

2019 年度の「脆弱性対処に向けた製品開発者向けガイド」の目次と今回作成した「製品開発者向けガイド」の目次の比較を以下に示す。

脆弱性対処に向けた製品開発者向けガイド	本ガイド（製品開発者向けガイド）
エグゼクティブサマリ 概要	はじめに　エグゼクティブサマリ 本ガイドの概要 脆弱性管理の全体像とその基本的な考え方
Ⅰ．方針・組織 1 製品セキュリティポリシーの策定 2 セキュリティサポート方針の明示 3 製品セキュリティを維持するための体制と管理	Ⅰ．計画 1 ソフトウェア開発ライフサイクル全体を通じた人材・プロセス・技術の整備 2 セキュアなソフトウェア開発を実践するための方針・体制 3 脆弱性の対処やインシデント対応を円滑に実施するための方針・体制
Ⅱ．設計・開発 4 セキュリティを確保するための設計 5 アップデートを考慮した設計 6 既知の脆弱性解消 7 セキュアコーディング 8 開発環境のセキュリティ確保 9 開発時の脆弱性検査	Ⅱ．要件定義・設計・開発 4 セキュリティを確保するための設計 5 既知の脆弱性解消 6 セキュアコーディング・セキュアビルド 7 開発時の脆弱性検査 8 開発に使用する環境及びツールのセキュリティ確保
Ⅲ．出荷後の対応 10 製品と構成要素の脆弱性監視 11 脆弱性報告の受付・対策情報の公表 12 一般消費者の製品利用時における実施事項の明示	Ⅲ．供給・配布 9 ソフトウェア製品のセキュアな配布
	Ⅳ．運用 10 脆弱性の発見 11 脆弱性の検証（脆弱性情報のトリアージと分析） 12 脆弱性の修正対策と対策情報の公表 13 ソフトウェアの脆弱性に起因したインシデントが発生した場合の対応 14 製品利用者における製品利用時の実施事項の明示
	Ⅴ．廃棄 15 ソフトウェアのサポート終了と廃棄対応

図 2-3 脆弱性対処に向けた製品開発者向けガイドの目次と
製品開発者向けガイドの目次の比較

なお、製品開発者向けガイドの詳細については、別冊を参照のこと。

3. 製品利用者の抱える課題に関する調査及び製品利用者向けガイドの作成

3.1. 調査の概要

(1) 目的

近年においては、製品利用者における自組織で利用するシステム・サービスの開発形態や、当該システム・サービスに含まれるソフトウェアやソフトウェアを組み込んだ機器の調達形態は複雑になっており、それに伴って、製品利用者において構築される CSIRT（Computer Security Incident Response Team）体制において必要となる脆弱性の対処やインシデント対応に係る取組も多様化している。

また、近年においては、製品開発者に対してソフトウェア開発ライフサイクル全体にわたって脆弱性管理を行うことが求められる中で、製品開発者、製品利用者のぞれぞれの脆弱性の対処における役割分担についても見直すことが必要となるとともに、双方が両輪となって脆弱性の対処に取り組むことにより、ソフトウェアの脆弱性を悪用する攻撃への対応能力を高めることが重要となっている。

このような背景のもと、製品利用者の抱える課題や脆弱性対策について、文献調査、アンケート調査及びヒアリング調査を実施し、製品開発者向けガイドと対となるガイドとして、製品利用者向けガイドをとりまとめた。

(2) 手順

最初に、製品利用者の抱える課題に関する国内外の文献調査を実施し、その結果を反映して、製品利用者向けガイドの骨子案を作成した。

次に、製品利用者に対するアンケート調査を実施するにあたり、製品利用者の抱える課題や脆弱性対策について仮説を構築して、アンケート調査票を作成するとともに、アンケート調査を実施した。

さらに、アンケート調査の内容を深堀りして、製品利用者が実際に取り組んでいる脆弱性対策や、業務上抱える課題を把握するにあたり、ヒアリング調査項目を作成するとともに、ヒアリング調査を実施した。

その上で、製品利用者向けガイドの骨子案に対して、アンケート調査やヒアリング調査の結果を反映して、加除修正を施しつつ、製品利用者向けガイドを

とりまとめた。

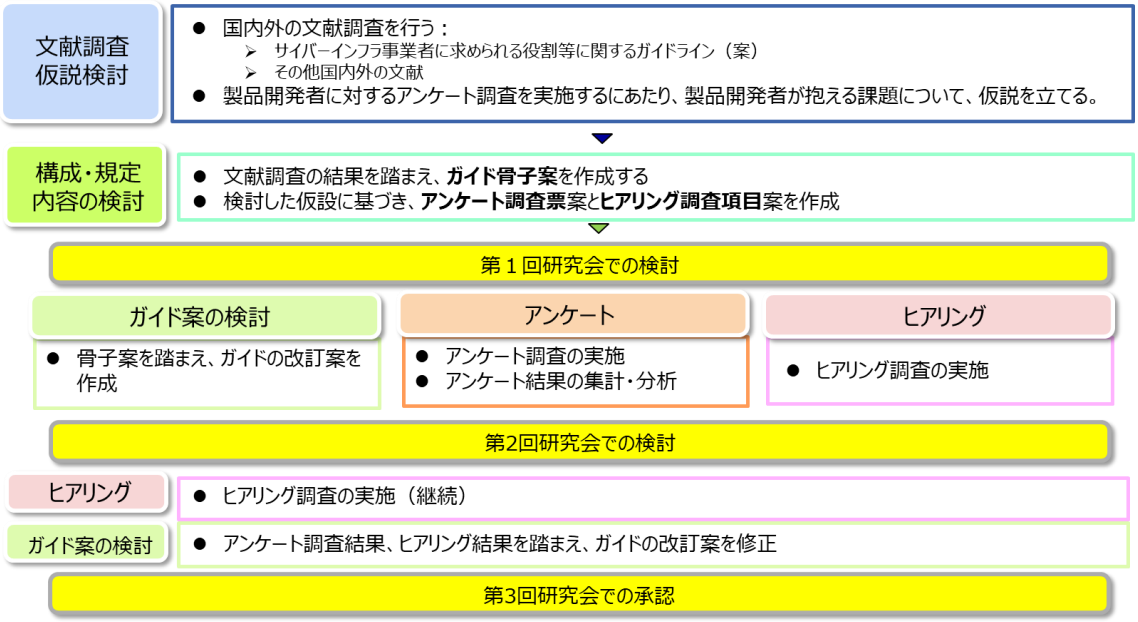


図 3-1 「製品利用者向けガイドの策定」の実施内容全体

3.2. 製品利用者の抱える課題に関する文献調査

(1) 文献調査概要

以下に実施した文献調査の概要を示す。

［文献調査主旨］

顧客が認識すべき責務について考慮しつつ、製品利用者における方針・組織体制に加え、脆弱性対処の観点から調達先に要求すべき事項や、システム・サービスの計画・要件定義から、システム・サービスの運用中のセキュリティパッチの適用等、各フェーズにおける脆弱性対処に関連して、製品利用者の抱える課題を把握する。

［調査対象］

「サイバーインフラ事業者に求められる役割等に関するガイドライン（案）」を含め、以下の国内外の文献を対象に文献調査を行った。

①日本セキュリティオペレーション事業者協議会「脆弱性トリアージガイドライン作成の手引き」

②日本セキュリティオペレーション事業者協議会「ASM 導入検討を進めるためのガイダンス（基礎編）」

③日本セキュリティオペレーション事業者協議会「セキュリティ対応組織（SOC/CSIRT）の教科書 ～X.1060 フレームワークの活用～ 第 3.2 版」
④日本シーサート協議会「脆弱性管理の手引書 システム管理者編 1.1 版」
⑤日本ネットワークセキュリティ協会の「CISO 支援ワーキンググループ」の各種成果物
⑥サイバーインフラ事業者に求められる役割等に関するガイドライン（案）
⑦NIST SP 80040 Rev.4 Guide to Enterprise Patch Management Planning Preventive Maintenance for Technology
⑧NIST SP 1800 31 Improving Enterprise Patching for General IT Systems Utilizing Existing Tools and Performing Processes in Better Ways
⑨NSA ESF Securing the Software Supply Chain：RECOMMENDED PRACTICES GUIDE FOR CUSTOMERS

[調査方法]
文献調査、Web 調査

(2)文献調査を踏まえて想定する仮説・問題

文献調査の結果から得られた脆弱性対処における課題を踏まえ、製品利用者が抱える構造的課題として、以下に示すものを仮説として想定することとした。

- 組織として、脆弱性情報の収集や対処を行うための方針・ポリシー・規程が整備されていない
  実施すべき内容やプロセスが示されず、脆弱性対処が放置されている。
- 脆弱性対処について、責任を担い、社内外の連携の旗振り役となって調整する部門・人材が十分ではない
  脆弱性対処が遅れることにより、組織の信頼が失墜したり、社内外の連携が疎かになり、脆弱性対処が非効率になったりしている。
- 経営層が脆弱性対処の必要性を理解しておらず、十分なリソースを投資することができない
  組織として、脆弱性対処のリソースが配分されず、組織としての脆弱性対処の体制構築、対処が行われない。
- 調達先・委託先に対し、セキュアコーディングや脆弱性診断等を求めていない

開発段階から脆弱性が放置されることにより、サプライチェーンにおける脆弱性リスクが増大している。

- 調達先・委託先に対し、脆弱性を検知し、報告するための体制や役割を十分に求めていない

  脆弱性の検知が遅れることにより、脆弱性を狙った攻撃を受けるリスクが増大している。
- 脆弱性対処やインシデント対応に要する社内外の連携について、役割や責任分担が十分ではない

  適切な役割や分担による円滑な脆弱性対処を行うことができず、脆弱性対処に要する時間・コストが増大している。
- 脆弱性対処の対象となる IT 資産の洗い出し・変更管理、リスク評価が十分ではない

  脆弱性対処を行うべき範囲や、対応すべきリスクが明確化されないことにより、脆弱性対処が進まない。
- 膨大な脆弱性情報について、対応の要否や優先順位を検討し、適切に対処することができない

  自社が優先的に対処すべき脆弱性が明確化されないことにより、脆弱性対処が非効率になっている。
- システムの可用性の観点から、セキュリティパッチを適用することができない

  脆弱性が放置されることにより、攻撃を受けるリスクやインシデント発生・被害拡大のリスクが増大している。

3.3. 製品利用者に対するアンケート調査

(1) アンケート調査概要

以下に実施した製品利用者に対するアンケート調査の概要を示す。

［調査主旨］

製品利用者の抱える課題や脆弱性対策のうち、システム開発ライフサイクルを考慮しつつ、以下に示す内容についてより詳細かつ適切に把握する。

①CSIRT 体制に関する課題への対応策

②製品開発者のサポート・保守契約及び SI 事業者との間の保守運用契約に関する課題への対応策

③脆弱性パッチの適用に関する課題への対応策

④経営層の予算確保や対策投資に関する課題への対応策

［調査対象］

ソフトウェア製品やサービス（貴社が利用する基幹系システムや情報系システム、IT サービスなど）を利用している事業者を対象にアンケート調査を行った。

また、アンケートの想定回答者は、セキュリティ担当、システム管理担当、又は運用担当とし、いずれでも回答可能とし、いずれでも回答可能とした。ただし、自部門のみでの回答が難しい場合には、他部門とも調整して回答してもらうこととした。

［アンケート項目］

図 3-2 アンケートの構成

〇回答組織の属性・体制に関するアンケート項目（問１～問７）
〇計画・要件定義フェーズにおける課題と対応策に関するアンケート項目（問８～問 18）
〇導入フェーズにおける課題と対応策に関するアンケート項目（問 19～問 21）
〇運用フェーズにおける課題と対応策に関するアンケート項目（問 22～問 28）
〇廃棄フェーズにおける課題と対応策に関するアンケート項目（問 29）
〇その他（ヒアリングへの協力可否）（問 30）

(2)アンケート調査結果から得られた知見

アンケート調査結果から得られた主な知見を以下に示す。

- 製品利用者のほとんどが CSIRT を構築済み。CSIRT の組織形態としては、IT・セキュリティ部門の配下が最も多く、次いで多いのは、各部門横断のバーチャル組織として構築、経営層直轄、情報システム部門の配下の順である。
- CSIRT の要員数としては、10 名未満が中心。担当している対応業務としては、ログやアラート等の監視およびインシデント検知が十分にカバーされていない。
- 製品利用者のほとんどで脆弱性対処やセキュリティに関連するポリシー・方針・規定が設けられているが、人材教育・訓練を示す人的なポリシーやソフトウェア製品の管理手順・脆弱性スキャンに関するポリシーの策定については十分とは言えない。
- 製品利用者は、システム・サービスの開発委託契約において、委託先の事業者に対して脆弱性対処の観点から必要となる要求を行っているが、その一方で、セキュリティテストの実施や結果の報告、第三者による脆弱性診断の実施等については要求が十分とは言えない。
- 製品利用者の半数以上が、サービスレベル契約（SLA）において、脆弱性対処の観点からの要求をできていない。脆弱性を利用した攻撃等の傾向を把握できるログの保存や提出の要求などを行っている製品利用者は、限定的である。
- 製品利用者の多くがシステム・サービスの運用・保守契約において、脆弱性対処の観点から必要となる要求を行っているが、その一方で、インシデントの検知、封じ込め・駆除などの対応、インシデントからの復旧や再発防止策などの事後対応等については、要求が十分とは言えない。
- システム・サービスの構築を計画する際に、より詳細な資産管理のために、SBOM を活用している製品利用者はかなり少ない。

- セキュリティパッチを適用しなかった際にサイバー攻撃等の被害を受けたことがある製品利用者は一定数存在する。被害を契機として、パッチ適用の定常業務化や EDR の導入、パッチが適用できない場合のアクセス制御の強化、運用ベンダに対する適用の徹底の指示、他の機器のチェックや攻撃を受けた機器の廃棄など、さまざまな対策が実施されている。
- セキュリティパッチの副作用によるシステム・サービス停止を経験したことがある製品利用者は比較的多い。その後、検証環境を用意し、事前の検証を行う改善が行われている。
- 製品利用者のほとんどが廃棄時の脆弱性対策として、不要なデータの消去を実施している。

3.4. 製品利用者に対するヒアリング調査

(1) ヒアリング調査概要

以下に実施した製品利用者に対するヒアリング

［調査主旨］

アンケート調査の回答内容をさらに深堀りして、製品利用者が実際に取り組んでいる脆弱性対策や、業務上抱える課題を把握する。

［調査対象］

CSIRT 組織を有する事業者、CSIRT 組織を有さない事業者、重要インフラ事業者、SI 事業者、ウェブサイト運営者、クラウドサービス事業者、製品利用者やセキュリティに関する業界団体のそれぞれを対象にヒアリング調査を行った。

［主なヒアリング項目］

ヒアリング項目	ヒアリング内容
製品利用者が実際に取り組んでいる対策、業務上抱える課題	以下に示す観点に基づき、アンケート調査の回答内容を深堀りして、どのような背景や事情があるか。また、何か課題になるような事象が起きていないか。課題がある場合に、どのような解決策を講じているか。 ①CSIRT 体制に関する課題への対応策 ②製品開発者のサポート・保守契約及び SI 事業者との間の保守運用契約に関する課題への対応策 ③脆弱性パッチの適用に関する課題への対応策

	④経営層の予算確保や対策投資に関する課題への対応策
経営層の関与・関心の状況	脆弱性対処やインシデント対応に対する経営層の関心事項は何か。
過去に生じた脆弱性対応に関するトラブルやその対応	脆弱性対応に関するトラブルは、どのような問題であったか。問題の再発防止のため、どのような対策を講じたか。
脆弱性の対処に関するベストプラクティス	脆弱性の対処に関する取組で特に力を入れているものは何か。
課題に対する対応にあたって実施した事例や対応が成功した事例	業務上抱える課題に対して、対応上何か工夫を行っている事例はあるか。
ヒアリング実施時点の製品利用者向けガイド案に関する意見	アンケート調査により把握した課題に対して検討した解決策（ガイド案に記載した解決策）が有効であるかどうかの意見や、検討した解決策以外の解決策（ガイド案に記載していない解決策）として考えられる案についての意見があるか。

(2) ヒアリング調査結果から得られた知見

ヒアリング調査結果から得られた主な知見を以下に示す。

- CSIRT 組織はインシデントが発生した際、他の実務要員や組織内外と連携する際の旗振り役を務めている。自組織内の連携には役割分担の明確化や、定期的な情報交換が必須である。また、CSIRT に属する人員には、セキュリティに関する知見だけではなく、情報収集能力や解析能力が備わっていることが望ましい。
- 外部事業者から製品を調達、もしくは外部事業者に開発・構築、運用を委託する場合は、それぞれに対し、セキュリティ要件やチェック項目を設け、その内容の定期的な確認を求めている。また廃棄の際には、安全な廃棄を自社で実施する、もしくは委託した上で廃棄証明書を取得している。
- セキュリティ修正プログラムを適用するためには、事前に適用の影響を検証するための検証環境の構築が必要である。また適用に関して、対処すべき脆弱性の優先順位や、セキュリティ修正プログラムの適用範囲の考え方を定めたうえで、セキュリティ修正プログラムの適用の定常業務化を図ることが必要である。

- 昨今のサイバー攻撃の事例や他社の被害状況を受け、セキュリティに対する経営層の感度が高まっており、対策への投資や、自組織内の運用の再点検、従業員に対するセキュリティ教育に関与する機会が増えている。
- ハイエンドなセキュリティ技術が求められるなど、自組織のリソースだけでは対応が難しい範囲については外部委託で補いつつ、一方、解釈や判断が求められる対応については自組織が主導することにより、対応の効率化を実現している。
- 安全な調達を実現するための方針やポリシーを整備しており、調達・委託先においてサポートが充実しているかどうか、経営面から事業継続性があるか等を確認した上で、セキュリティの観点からも審査を行っている。
- 自組織内にセキュリティ意識やセキュリティ確保の取組を浸透させるため、経営層からのメッセージの発信、関連部門長を対象とした副 CISO 制の導入、e-ラーニング・対面形式でのセキュリティ教育機会の提供、外部のセキュリティ専門家との情報交換等を実施している。

3.5.製品利用者向けガイドの作成

(1)製品利用者向けガイドの作成

前述した文献調査をもとに作成した製品利用者向けガイドの骨子案に対して、アンケート調査やヒアリング調査の結果を反映して、加除修正を施しつつ、製品利用者向けガイドを取りまとめた。

製品利用者向けガイドの各章は、製品開発者向けガイドの構成に合わせつつ、構築・調達形態に応じた利用方法を新たに追加し、構築・調達形態に応じた利用方法、意義、実施内容、実施手順の 4 つにより構成した。

今回作成した「製品利用者向けガイド」の目次を以下に示す。

本ガイド（製品利用者向けガイド）
はじめに エグゼクティブサマリ 本ガイドの概要
脆弱性管理の全体像と基本的な考え方
Ⅰ．計画・要件定義 1 脆弱性リスクを適切に管理するための人材・プロセス・技術の整備 2 安全なシステム・サービスを構築するための方針・体制 3 脆弱性対処やインシデント対応を円滑に実施するための方針・体制
Ⅱ．設計・開発 4 セキュリティを確保するための設計
Ⅲ．導入 5 ソフトウェアを導入するためのIT資産管理 6 ソフトウェアを導入する際における脆弱性対処
Ⅲ．運用 7 ソフトウェアの運用時における脆弱性対処 8 ソフトウェアの運用時にインシデントが発生した場合の対応
Ⅳ．廃棄 9 ソフトウェアの廃棄時における脆弱性対処

図 3-3 製品利用者向けガイドの目次

なお、製品利用者向けガイドの詳細については、別冊を参照のこと。

4. 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)サイバー対処能力強化法の施行に伴う告示の改正等を踏まえた必要となる対応事項のガイドラインへの追加

2025 年 5 月 23 日に公布されたサイバー対処能力強化法及び同整備法においては、基幹インフラ事業者に対して、インシデント報告や、使用される電子計算機やプログラムへの脆弱性対応の強化等が求められている。

これに伴って、パートナーシップが果たすべき役割も見直され、活動の根拠となる告示の改正に向けた検討が進められている状況である。

このような新法及び告示改正の具体的内容を踏まえ、2026 年度中を目途として、「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」の改訂が検討されなければならない。

(2)製品開発者向けガイド及び製品利用者向けガイドの改訂に関する検討

(1)に記載する新法等の影響を含め、製品開発者や製品利用者に求められる対応や責務は、今後も変化・拡大していくことが考えられる。

そのような求められる対応等に大きな変化があるかどうかについては、中長期的に評価を継続し、変化があった場合には、今回取りまとめた製品開発者向けガイドや製品利用者向けガイドをその時代に合うよう改訂することを検討すべきである。

またその際には、脆弱性対処に関連する規定を持つ他のセキュリティ基準や規格、業界ルールとの整合・相違についても確認することが望まれる。

参考１

2025 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

2026 年 2 月 16 日時点

座長	土居 範久	慶應義塾大学
委員	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	日本マイクロソフト株式会社
	北泉 公之	富士通株式会社
	北澤 繁樹	三菱電機株式会社
	木谷 浩	一般社団法人情報サービス産業協会サイバーセキュリティ部会（キヤノンＩＴソリューションズ）
	小島 健司	株式会社東芝
	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 ホールディングス株式会社
	森田 光	株式会社日立製作所
	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

田中 貴大	総務省　サイバーセキュリティ統括官室
入谷 忠久	総務省　サイバーセキュリティ統括官室
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）
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)
佐々木 勇人	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)
桑原 俊	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

積田 北辰	内閣官房 国家サイバー統括室　参事官
伊藤 建	内閣官房 国家サイバー統括室　企画官
澤村 新之介	内閣官房 国家サイバー統括室
吉井 護	内閣官房 国家サイバー統括室
武尾 伸隆	経済産業省 サイバーセキュリティ課　課長
薄羽 利光	経済産業省 サイバーセキュリティ課
関戸 多聞	経済産業省 サイバーセキュリティ課
清水 幹治	独立行政法人情報処理推進機構 理事
高柳 大輔	独立行政法人情報処理推進機構
酒井 崇行	独立行政法人情報処理推進機構
神田 雅透	独立行政法人情報処理推進機構
川口 修司	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
板橋 博之	独立行政法人情報処理推進機構
北爪 亮太郎	独立行政法人情報処理推進機構
夏目 典大	独立行政法人情報処理推進機構
大久保 直人	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
山本 以誠	株式会社野村総合研究所
平岩 杏奈	株式会社野村総合研究所
山口 啓太	株式会社野村総合研究所

（順不同、敬称略）

参考２

検討経緯

■研究会第 1 回会合（2025 年 9 月 10 日）
・本研究会の運営について
・サイバー対処能力強化法及び同整備法について
・2023 年度調査の報告について
・今年度の脆弱性調査の方針について
・個別調査の概要について
・スケジュールについて

■研究会第 2 回会合（2025 年 12 月 9 日）
・第 1 回会合の振り返りについて
・ サイバー対処能力強化法の施行に伴う告示・ガイドライン見直しの方向性（案）について
・脆弱性悪用情報に係る課題と優先情報提供スキームの改善について
・脆弱性調査の進捗報告と製品開発者向けガイドの記載事項の検討について
・スケジュールについて

■研究会第 3 回会合（2026 年 2 月 16 日）
・第 2 回会合の振り返りについて
・サイバー対処能力強化法の施行に伴う告示改正状況の説明について
・製品開発者向けガイド（案）について
・製品利用者向けガイド（案）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