情報システム等の脆弱性情報の取扱いに関する研究会

- 2023 年度 報告書 -

2024 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2023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18,663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、優先情報提供の拡充など、より迅速かつ着実な脆弱性対応の実現に向けた検討を実施し、あるべきパートナーシップの形成をめざした。また、調整機関と製品開発者との間の調整過程における課題や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。

2024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

1.1. 背景 1
1.2. 運用の状況 1
1.3. 本年度研究会における検討 12

2. 製品開発者と調整する過程における３つの課題に関する調査 13

2.1. 調査の概要 13
2.2. 脆弱性の悪用を示す情報に関する情報の取扱い等に関する課題 14
2.3. 製品開発者の脆弱性への対応目途（45 日）に関する課題 16
2.4. 「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 20

3. 優先情報提供の内容拡充等に関する調査 23

3.1. 調査の概要 23
3.2. ISAC 等組織に関する文献調査 23
3.3. ISAC 等組織に関するヒアリング調査 26
3.4. 情報共有体制に関する文献調査 28
3.5. 脆弱性情報の取扱いにおけるより早い段階での情報の提供に向けた調査 29
3.6. 優先情報提供する情報の内容の拡大に向けた調査 30
3.7. その他の検討事項・意見 33

4. パートナーシップの運用改善事項等の調査及び P ガイドラインへの反映 . 35

4.1. 調査の概要 35
4.2. 調整不能案件の改善に関する調査及び P ガイドラインへの反映 36
4.3. その他軽微な修正 38

5. P ガイドラインの改訂等 39

5.1. P ガイドライン改訂案作成 39
5.2. 公表マニュアルの改訂 47

6. 今後の課題 49

参考１　情報システム等の脆弱性情報の取扱いに関する研究会名簿..... 51

参考２　検討経緯 53

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 2023 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 5,670 件、ウェブサイトの脆弱性に関するもの 12,993 件の計 18,663 件であった。四半期毎の届出状況を図 1-1 に示す。

	2021 1Q	2Q	3Q	4Q	2022 1Q	2Q	3Q	4Q	2023 1Q	2Q	3Q	4Q
累計届出件数[件]	16,475	16,778	16,982	17,130	17,302	17,468	17,683	17,842	18,025	18,195	18,353	18,663
1就業日あたり[件/日]	4.04	4.06	4.05	4.02	4.01	3.99	3.98	3.97	3.95	3.94	3.92	3.93

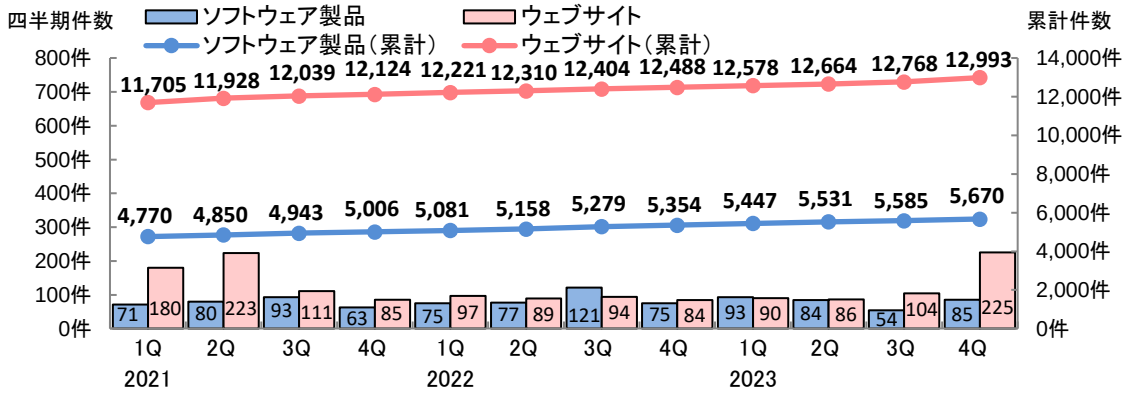


図 1-1　四半期ごとの届出状況

（活動報告レポート[2023 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。

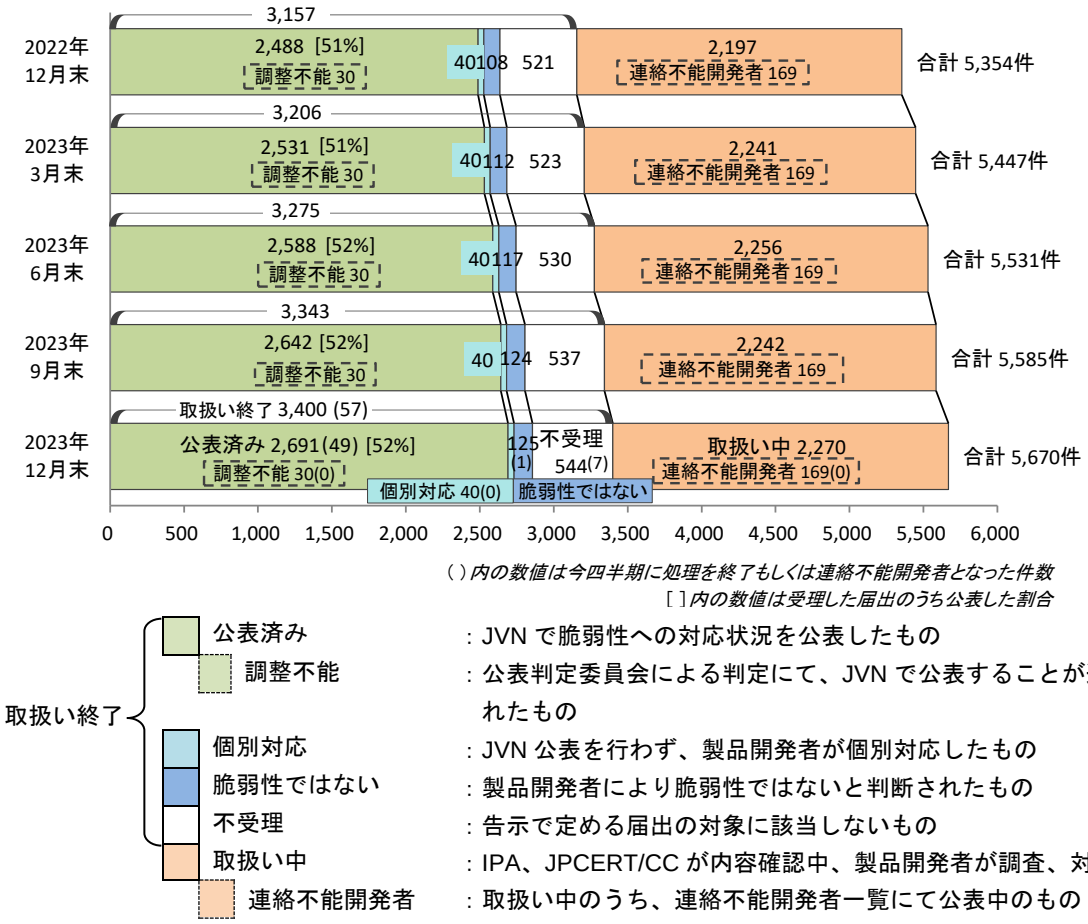


図 1-2　ソフトウエア製品の脆弱性関連情報の届出の処理状況

（活動報告レポート[2023 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 5,670 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 2,691 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 125 件、取扱い中のものが 2,270 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 544 件ある。

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

(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。

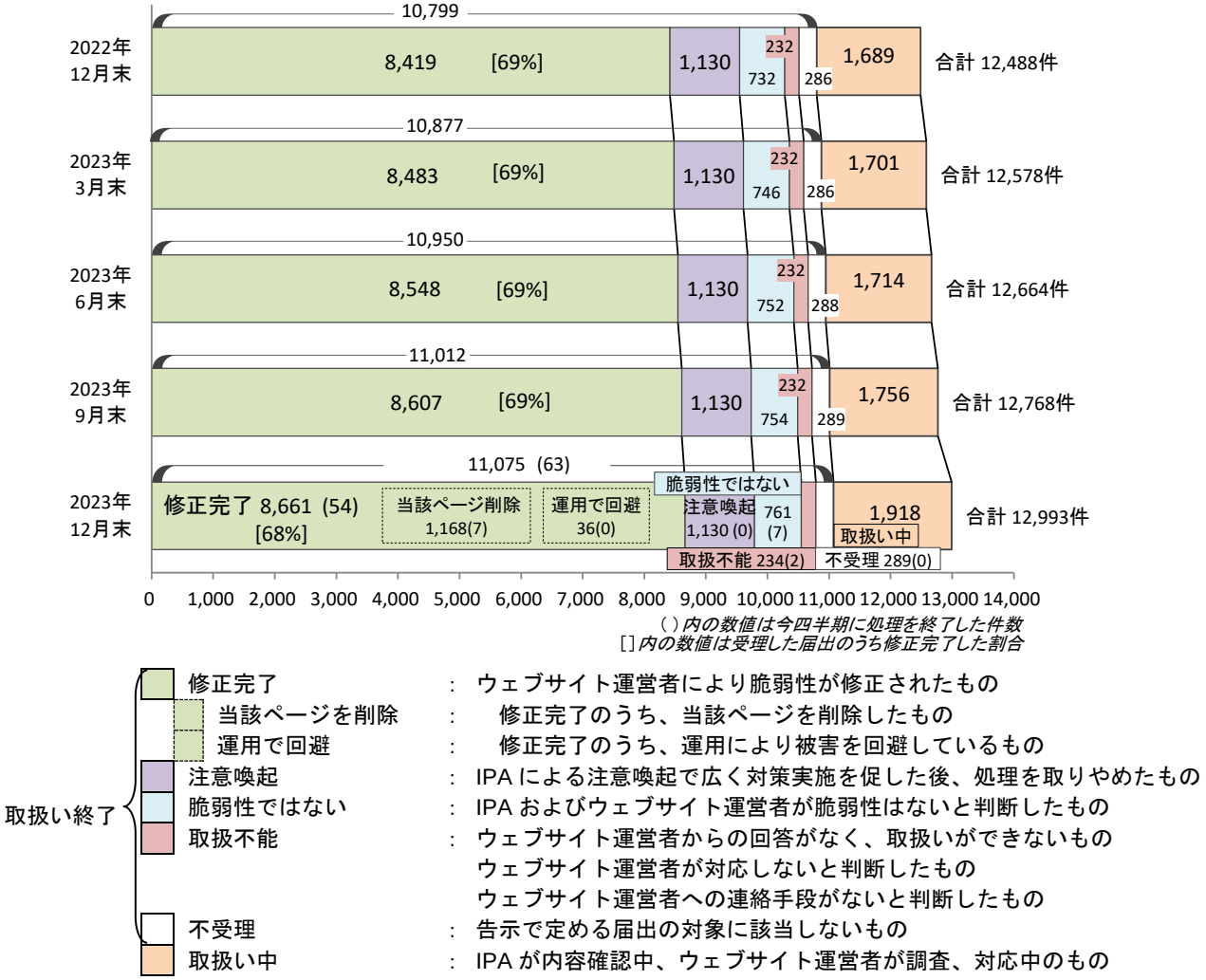


図 1-3 ウェブサイトの脆弱性関連情報の届出の処理状況

（活動報告レポート[2023 年第 4 四半期（10 月～12 月）]より抜粋）

ウェブサイトの脆弱性関連情報の届出 12,993 件のうち、修正が完了したものが 11,075 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 1,168 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 761 件、取扱い中のものが 1,918 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 234 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 289 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 2023 年 12 月末までに 5,164 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

2023 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 2,691 件である。届出受付開始から 2023 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。

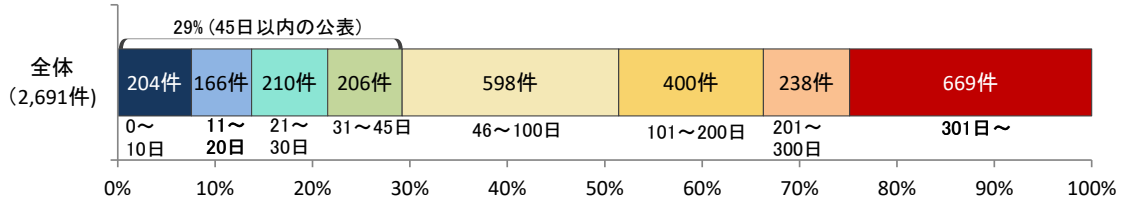


図 1-4 ソフトウエア製品の脆弱性公表までに要した日数

（活動報告レポート[2023 年第 4 四半期（10 月～12 月）]より抜粋）

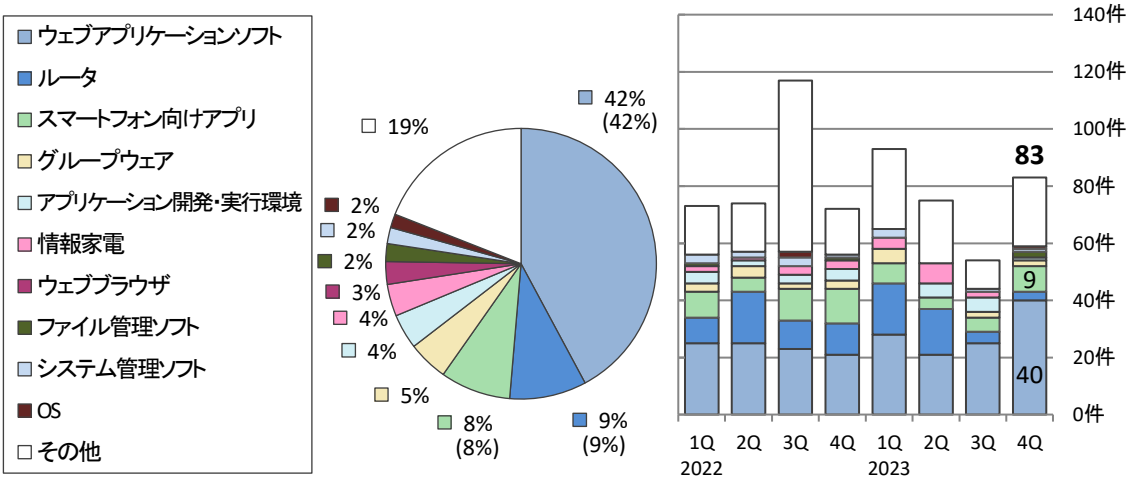
(2) 海外 CSIRT から連絡を受け公表した脆弱性

2023 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 2,984 件である。このうち、2023 年度第 4 四半期（2023 年 10 月から 2023 年 12 月末まで）に JVN で公表した脆弱性関連情報は 85 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 2023 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 5,670 件のうち、不受理分を除いた 5,126 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 42%を占めている。



※その他には、データベース、携帯機器などがあります。
(5,126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)

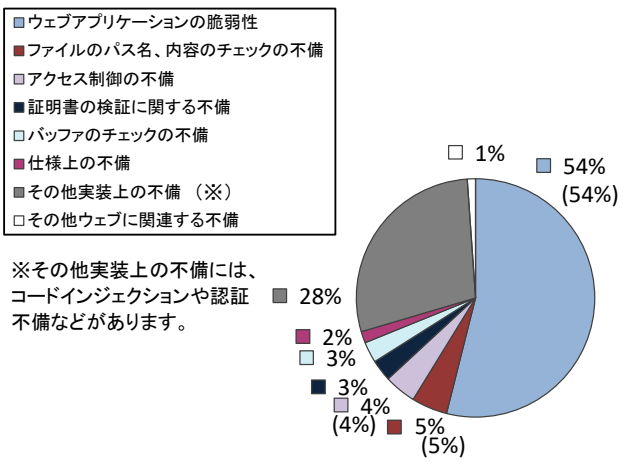
四半期ごとの製品種類別届出件数

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～2023 年 12 月末）

（活動報告レポート[2023 年第 4 四半期（10 月～12 月）]より抜粋）

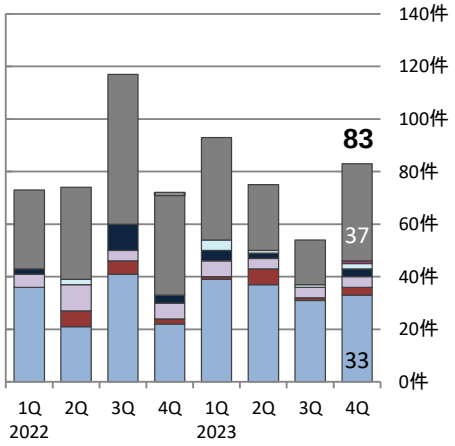
(4) 脆弱性の原因別の内訳

届出受付開始から 2023 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 5,670 件のうち、不受理のものを除いた 5,126 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 54%を占める。



（5,126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～2023 年 12 月末）

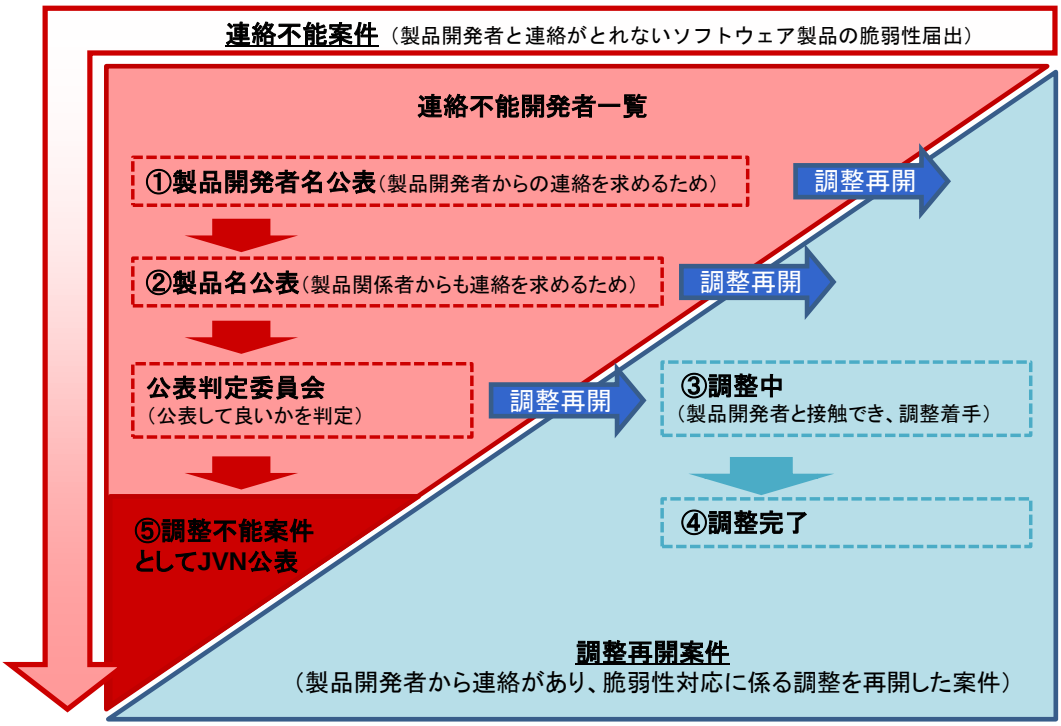
（活動報告レポート[2023 年第 4 四半期（10 月～12 月）]より抜粋）

(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。2023 年第 4 四半期に優先情報提供したものは電力分野 0 件、政府機関 0 件で、累計では 69 件（電力分野 40 件、政府機関 29 件）であった。

(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 2023 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）。



2023年 第3四半期	169件 （①1件 ②168件）	52件 （③20件 ④32件）	⑤30 件	合計 251件
2023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～2023 年 12 月末）

（活動報告レポート[2023 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

2023 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 8,661 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 51%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。

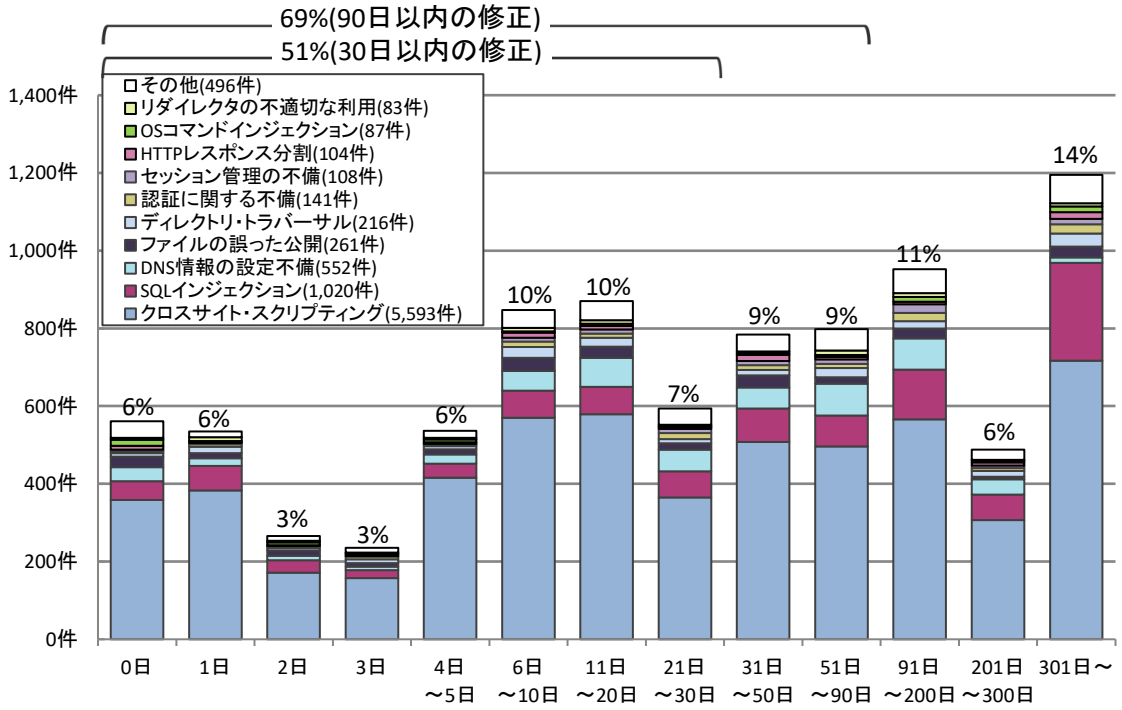
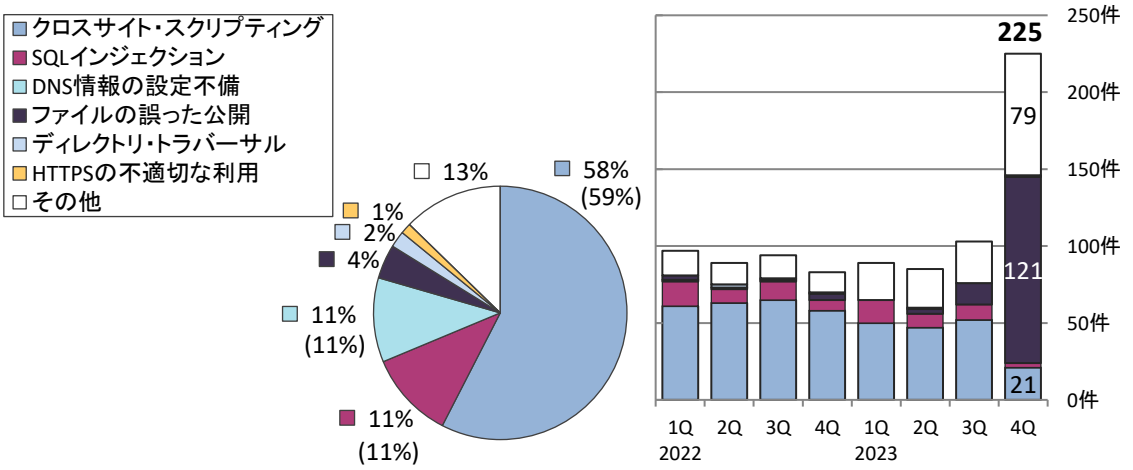


図 1-8 ウェブサイトの脆弱性修正に要した日数（届出受付開始～2023 年 12 月末）

（活動報告レポート[2023 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

2023 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 12,993 件のうち、不受理のものを除いた 12,704 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%)、「SQL インジェクション」(11%)、「DNS 情報の設定不備」(11%)の割合が高く、この３つだけで全体の 80%を占める。



(12,704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)

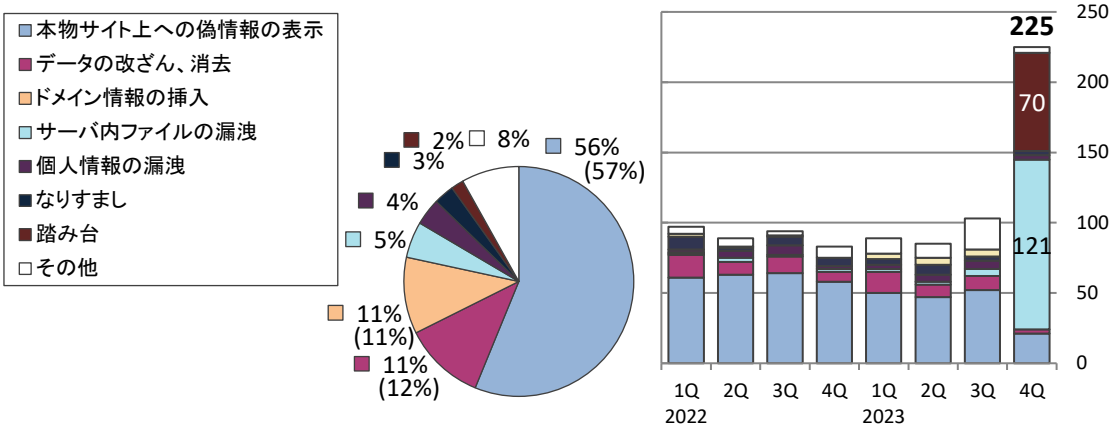
四半期ごとの脆弱性の種類別届出件数

図 1-9　ウェブサイトの脆弱性種類別内訳（届出受付開始～2023 年 12 月末）

（活動報告レポート[2023 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」(56%)、「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。



(12,704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～2023 年 12 月末）

（活動報告レポート[2023 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 846 件で、前年同期（813 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 18%を占めており、対策の実施が望まれる。

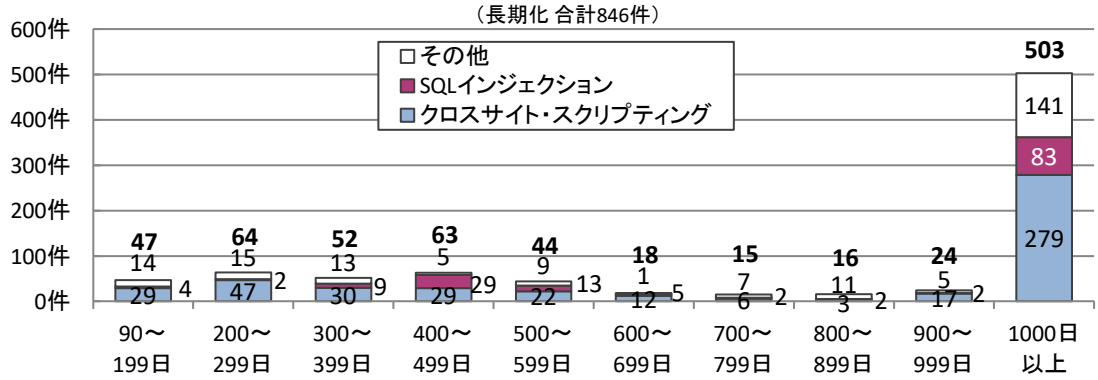


図 1-11 取扱いが長期化（90 日以上経過）しているウェブサイトの経過日数と脆弱性の種類

（活動報告レポート［2023 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製品開発者と調整する過程における３つの課題に関する調査
- 脆弱性の悪用を示す情報に関する情報の取扱い等に関する課題
- 製品開発者の脆弱性への対応目途（45 日）に関する課題
- 「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

②優先情報提供の内容拡充等に関する調査
- ISAC 等組織に関する文献調査
- ISAC 等組織に関するヒアリング調査
- 情報共有体制に関する文献調査
- 情報共有体制に関するヒアリング調査
- 脆弱性情報の取扱いにおけるより早い段階での情報の提供に向けた調査
- 優先情報提供する情報の内容の拡大に向けた調査

③パートナーシップの運用改善事項等の調査及び P ガイドラインへの反映
- 調整不能案件の改善に関する調査及び P ガイドラインへの反映
- その他軽微な修正

2. 製品開発者と調整する過程における３つの課題に関する調査

2.1. 調査の概要

(1) 目的

パートナーシップでは、脆弱性情報を発見した者（以下「発見者」という。）が、受付機関である IPA に対して脆弱性情報の届出を行い、IPA は条件を満たしていると判断した場合、脆弱性情報を受理し、受理した情報を調整機関である JPCERT/CC に通知している。通知を受けた JPCERT/CC は、脆弱性情報を製品開発者へ通知し、脆弱性の検証や検証した結果の報告を求めるといった調整を行っている。そして、製品開発者は、通知された脆弱性情報をもとに脆弱性の検証、対策方法の作成等を行っている。

これらの過程において、以下の３つの課題が生じている。

・脆弱性の悪用を示す情報に関する情報の取扱い等に関する課題
・製品開発者の脆弱性への対応目途（45 日）に関する課題
・「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

これらの３つの課題について、文献調査及びヒアリング調査等を実施し、P ガイドラインの改訂案をとりまとめた。

(2) 手順

(a)脆弱性の悪用を示す情報に関する情報の取扱い等に関する課題

「脆弱性の悪用を示す情報に関する情報の取扱い等に関する課題」については、悪用を示す情報の表示事例等の文献調査等を行い、この調査結果を参考に、悪用を示す情報を JVN に追記したイメージ案や、悪用を示す情報に関して各当事者に推奨される行為を P ガイドラインに追記した修正案、脆弱性対策情報の公表における悪用を示す情報に関する推奨事項を「ソフトウエア製品開発者による脆弱性対策情報の公表マニュアル」に追記した修正案等を作成した。

(b)製品開発者の脆弱性への対応目途（45 日）に関する課題

「製品開発者の脆弱性への対応目途（45 日）に関する課題」については、2021 年度の脆弱性研究会で示された「製品開発者の状況や課題を把握する必要性がある」との意見に基づき、JPCERT/CC が把握する製品開発者の状況等を踏

まえて、JPCERT/CC において作成しているベストプラクティスについて検討した。

(c)「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」については、2021 年度の脆弱性研究会で示された「告示の定義規定における「汎用性を有する製品」の要件との関係から整理が必要であり、その適用する場合についての例示といったわかりやすい説明が必要である」との意見に基づき、パートナーシップの識者や法律専門家、製品開発者へのヒアリングを行い、その意見を踏まえて P ガイドラインの修正案を作成した。

2.2. 脆弱性の悪用を示す情報に関する情報の取扱い等に関する課題

(1) 文献調査

(a)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]

悪用を示す情報の表示事例等の文献調査等を行い、この調査結果を参考に、悪用を示す情報を JVN に追記したイメージ案や、悪用を示す情報に関して各当事者に推奨される行為を P ガイドラインに追記した修正案、脆弱性対策情報の公表における悪用を示す情報に関する推奨事項を「ソフトウエア製品開発者による脆弱性対策情報の公表マニュアル」に追記した修正案等を作成する。

[調査対象]

①国内外の脆弱性情報公表データベースや脆弱性情報公表に関わる公的組織の事例等

②実際に悪用を示す情報を表示している製品開発者の公表ページ事例等

[調査方法]

文献調査（Web 調査）

(b)文献調査結果

文献調査の結果、悪用を示す情報に関して次のような表示のタイプ、事例が存在することが分かった。

①国内外の脆弱性情報公表データベースや脆弱性情報公表に関わる公的組織の事例

- 危険な脆弱性上位〇選という形でレポートされるタイプ
  攻撃コードの詳細を取り扱うものもあるが、年間レポートとして出されており、JVN 公表のような即時性をもつものではないため、公表時点では既に既知の脆弱性となっている。
- 実際に悪用が確認された脆弱性をラインナップしたデータカタログとして公開しているタイプ
  掲載されることで悪用発生の事実は分かるが、攻撃コードまでは掲載されていない。既に CVE ID が割り振られ、対策方法が公開されていることが掲載条件となっている。
- 実際に攻撃コードの詳細を掲載したデータベース
  CVE ID を振られた脆弱性を扱っており、主に研究者や技術者向けのものである。
- 公的機関が公表しているサイバー攻撃被害の共有・公表についてのガイダンス
  被害組織がセキュリティインシデントについて情報提供や公開を行うときを主な対象としたガイダンスであり、脆弱性の悪用を示す情報の扱いについて参考となる記述がある。

②実際に悪用を示す情報を表示している製品開発者の公表ページ事例

- JVN においては、ソフトウェア製品開発者の了解が得られたケースでは、「詳細情報」欄に攻撃確認の事実を記載している。攻撃が確認されていることの記載のみでそれ以上に詳細な情報は示されない。
- ソフトウェア製品開発者が脆弱性対策情報のリリースにおいて攻撃確認の事実を記載しているケースもある。ただし、基本的には攻撃確認の事実の記載のみで、被害組織や攻撃手法等の情報はなく、主に注意喚起の意味で掲載していると思われる。ソフトウェア製品の利用者が、攻撃を受けたかどうかを確認するための情報を掲載しているケースもある。

(2) ガイドライン修正案の作成

文献調査の結果をもとに、以下の方針で P ガイドラインの修正案を作成した。

- 脆弱性の悪用を示す情報は、製品開発者や利用者の当該脆弱性への対応の優先度に影響を与える。その意味で、少なくとも、悪用の事実を表示することにより、必要な効果を与えられると考えられる。現状でもソフトウェ

ア製品開発者の協力や理解を経て悪用確認や対応状況の共有が行われ、それに基づき、JVN の公表日の決定や悪用の事実を表記するケースがある。
- ただし、パートナーシップガイドライン上に具体的な規定があるものではなく、ガイドラインに基づく対応として製品開発者に対応を推奨できないため、ソフトウェア製品開発者の了解が得られないケースもある。
- このため、JVN やソフトウェア製品開発者による現状でのプラクティスを追認的に P ガイドラインに組み込むことが望ましいと思われる。

具体的な修正案については、「5.P ガイドラインの改訂等」を参照のこと。

(3)公表マニュアル修正案の作成

P ガイドラインの修正案と同様に、ソフトウエア製品開発者による脆弱性対策情報の公表マニュアルの修正案を作成した。

具体的な修正案については、「5.P ガイドラインの改訂等」を参照のこと。

2.3.製品開発者の脆弱性への対応目途（45 日）に関する課題

(1)JPCERT/CC における検討状況

(a)製品開発者向けアンケートの実施

JPCERT/CC が把握する製品開発者の状況等を踏まえ、2022 年度に JPCERT/CC において、製品開発者向けの脆弱性対応に関するアンケート調査が実施され、課題と対応策について一定の整理が行われた。

＜アンケート概要＞

[調査主旨]

ソフトウェア製品開発者の脆弱性への対応を迅速化し、対応目途である 45 日に近づけるため、ソフトウェア製品開発者における課題について実態把握し、その改善策を検討するとともに、迅速な脆弱性対応を実現している事例などから対応迅速化のためのヒントを抽出し、ベストプラクティスとして取りまとめる。

［主なアンケート項目］

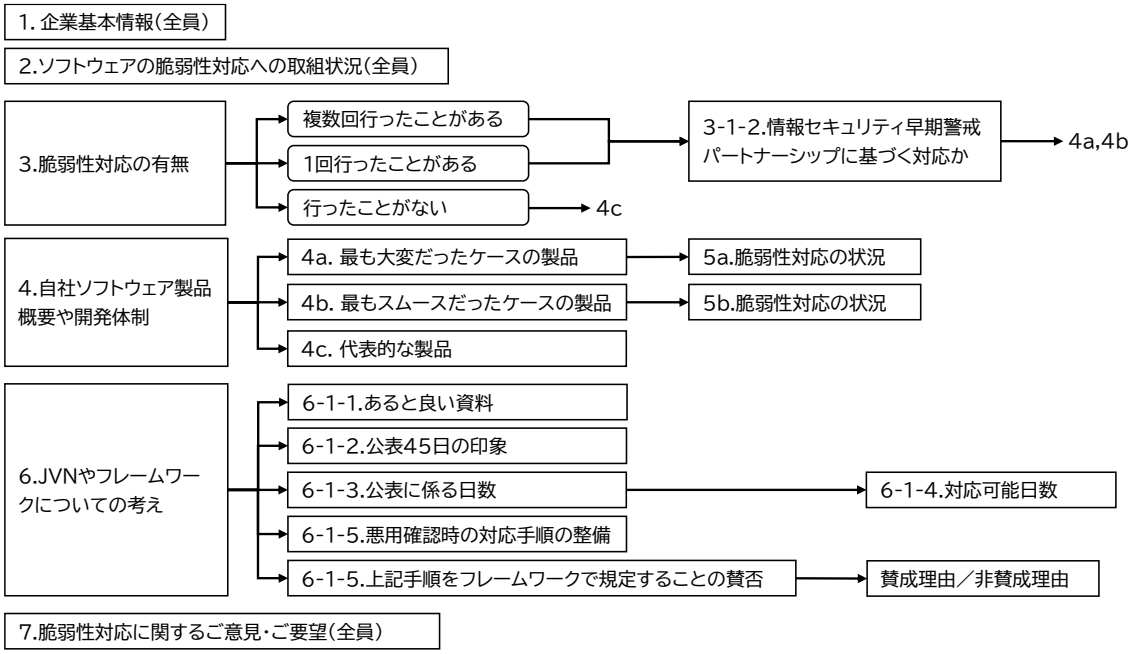


図 2-1 アンケートの構成

（出所：JPCERT コーディネーションセンター）

○脆弱性対応の負荷の原因となると思われる項目（大項目１、２、４）

- 会社の規模
- 海外展開状況
- 開発時のセキュリティへの取組姿勢
- 開発体制や規模

○各作業に対する負荷の大きさから、脆弱性対応における課題点が見えてくると思われる項目（中項目５ａ、５ｂ）

- 脆弱性対応の判断
- 脆弱性の確認
- ソフトウェアの改修作業
- 社内調整
- 社外（OEM/ODM 等）との調整
- 顧客との調整
- 流通経路との調整
- 公表に当たっての調整
- JPCERT/CC との調整

〇脆弱性対応の大変さによって対応に必要な日数への印象も変わると思われる項目（中項目５ａ、５ｂ、大項目６）

- 脆弱性対応の自己評価
- 45 日への評価
- 脆弱性の悪用を示す情報の表示への意見

［アンケート結果によるベストプラクティス案へのヒント］
アンケート結果を分析・整理し、次のようなベストプラクティスへのヒントを得ている。

（1）脆弱性対応窓口について

- 脆弱性対応窓口を設置する
- 脆弱性対応窓口の所属員数を多くし、兼任者には「関係部署」を含める
- 脆弱性対応窓口の引継ぎルールを制定する
- 海外拠点がある場合はそれぞれに窓口を設置する

（2）脆弱性対応の判断について

- 脆弱性対応や判断についてのルールを定める
- 脆弱性対応は脆弱性対応窓口の責任者が判断する

（3）日常的なセキュリティへの取組みについて

- セキュリティ・バイ・デザインを推進する
- 脆弱性情報入手の間口を広げておく
- ソフトウェア開発者へのセキュリティ教育を行う

（4）製品について

- 製品をなるべく小さな単位に分割し、コンパクトな体制で開発を行う
- ユーザについて把握するようにする

(b)ヒアリング調査の実施

2022 年度に実施されたアンケート調査を受け、さらに 2023 年度において、脆弱性対応として他の参考となりそうな特徴を持つ製品開発者向けのヒアリング調査が実施され、ベストプラクティスとしての取りまとめがなされた。

＜ヒアリング概要＞
［主なヒアリング項目］

〇共通質問項目

ヒアリング項目	ヒアリング内容
PSIRT の成り立ち	貴社 PSIRT（脆弱性対応窓口）の成り立ちを教えてほしい。 また、現在に至るまでの過程において解決した課題、未だ残っている課題を教えてほしい。
脆弱性の判断、確認	脆弱性の初期判断（再現確認、リスク判断、対応方針の決定等）はどの様に実施しているか？ 規則・ルール、リスク判断は何か参考にしたものがあるか？ それでも対応に困ること（脆弱性）はあるか？
制度やフレームワークと業務のギャップ	実際の脆弱性調整作業と「情報セキュリティ早期警戒パートナーシップ」や「PSIRT フレームワーク」等とのギャップを感じることはあるか？ ある場合、具体的には何か？

(2) ベストプラクティスの取りまとめ

(a)ベストプラクティスの位置づけ

JPCERT/CC において作成されるベストプラクティスに関して、次の方針とすることとした。

- 第 1 版の作成完了は今年度（2023 年度）末を予定
- 当面は JPCERT/CC が調整業務の実務で利用する補足資料とし、製品開発者との間で認識の共有のために利用
- 来年度（2024 年度）はトライアル利用とし、その間に積み上げた知見をもとにブラッシュアップを図り、来年度（2024 年度）の脆弱性研究会にて情報セキュリティ早期警戒パートナーシップに対する位置づけや取扱いを検討することを想定

(b)ベストプラクティス案の整理

以下にベストプラクティス案イメージを示す。

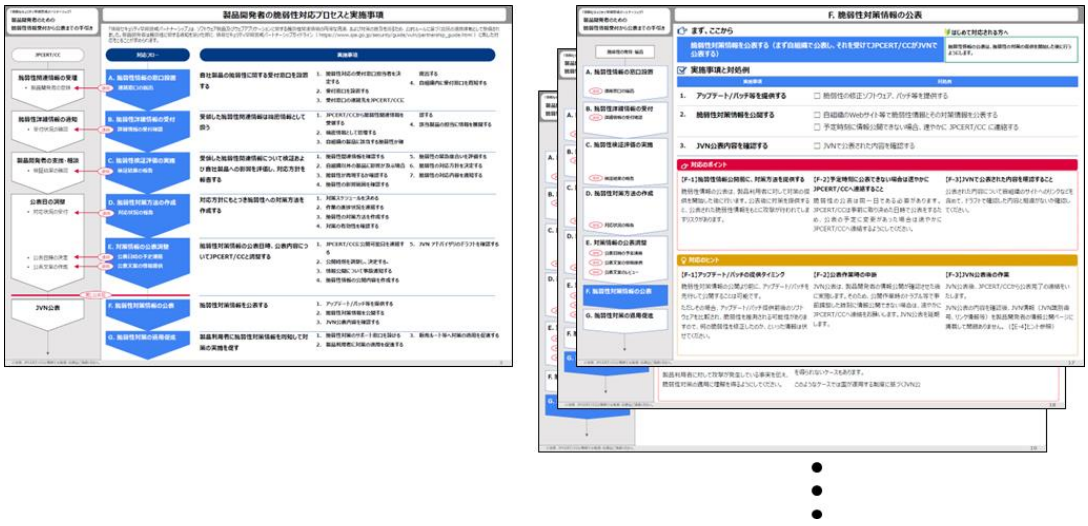


図 2-2 ベストプラクティス案のイメージ

（出所：JPCERT コーディネーションセンター）

2.4. 「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

(1) ヒアリング調査

「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点について、有識者や脆弱性対応の当事者である製品開発者にヒアリングを行い、その意見をもとに、P ガイドラインへの具体的修正点について検討をした。

(a)ヒアリング調査概要

以下に実施したヒアリング調査の概要を示す。

［ヒアリング主旨］

「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して、「汎用性を有する製品」の解釈を整理し、その条件・要件を適用する場合についての有効な例示を確認し、それらをもとに P ガイドラインの修正案を作成する。

［調査対象］

①パートナーシップの識者や法律専門家

②製品開発者

［実施時期］
2023 年 12 月～2024 年 2 月

［調査方法］
オンライン

［調査項目］
(1) 汎用性を有する製品の解釈に関するご意見
数について条件
販売・提供経路についての条件
製品の対象者や目的についての条件
製品の形態や開発経緯についての条件（プラットフォーム製品、受託開発等）
(2) 取扱い終了の具体的事例とその適用を行う際の条件・要件についてのご意見
実際に取扱い終了となったケースにおける状況、条件等
取扱い終了とならなかったケースにおける状況、条件等
(3) 解釈上の誤解を減らす方法について
「製品開発者がすべての製品利用者に通知する場合」における適切な終了条件・要件、例示等
IPA・JPCERT/CC と製品開発者の間で取り交わす覚書に記載すべき事項等

(b)ヒアリング結果
ヒアリングの結果、次のような論点とその対応を整理した。
〇ヒアリング結果を踏まえた対応の論点
１．規定（オ）「製品開発者がすべての製品利用者に通知する場合」を維持すべきか否か
２．「6.その他」（発見者ではなく、製品開発者が自ら発見した脆弱性に関する規定）におけるすべての製品利用者に通知する場合の記述を維持すべきか否か
〇論点 1 について
• ヒアリングにおいて、製品開発者からは、汎用性（利用者が不特定または多数かどうか）ではなく、サポート契約等により利用者を把握できている

かどうかが重要であるとのコメントがあり、現状の規定ぶりに否定的な意見はなかった。

- ヒアリングにおいて、有識者（委員）からは、経緯的・理論的整理から規定（オ）を削除し、規定（イ）「本ガイドラインの適用対象外」に一本化する方向性の示唆を得た。
- ただし、規定（イ）として明示的に整理してしまうと、そのような届出はパートナーシップ対象外＝不受理となると発見者に認識され、届出を提出すること自体を控えられてしまい、脆弱性を製品開発者に通知する機会ごと失ってしまう可能性も考えられる。
- そのため規定（オ）は維持しつつ、付録に例示を補足する案を検討することとした。

〇論点 2 について

- 「6.その他」については、製品開発者からの自発的な届出について、パートナーシップにおいてどのように位置づけるべきか、現行の規定のみで十分とすべきか、といった検討事項があるため、別途機会を改めて、検討することとした。

(2) ガイドライン修正案の作成

論点整理の結果をもとに、P ガイドラインの修正案を作成した。

具体的な修正案については、「5.P ガイドラインの改訂等」を参照のこと。

3.優先情報提供の内容拡充等に関する調査

3.1.調査の概要

(1)目的

パートナーシップでは、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及び政府機関に対して、脆弱性対策情報を JVN で公表する前に優先的に提供している。この優先情報提供について、提供先の拡大、脆弱性情報の取扱いにおけるより早い段階での情報の提供、及び優先情報提供する情報の内容拡大のために文献調査、ヒアリング調査及びその結果とりまとめを実施した。

(2)調査手法

ISAC 等組織に関する文献調査を行い、新たな優先情報提供先となり得る候補を特定した。この候補組織へのヒアリング調査を行い、優先情報提供の実施の可能性、実施に当たっての課題、及び課題解決策についてとりまとめた。同様に情報共有体制に関する調査も行った。

また、現在は公表日の決定後に実施している優先情報提供をより早い段階で実施できるようにするための、提供タイミングが異なる実施案を複数検討し、この実施案について、製品開発者、優先情報の提供先の組織に対してヒアリングを行い、ヒアリングの結果を踏まえて改善に向けた論点の整理を行った。

さらに、現在は JVN で公表している情報と同等の情報である優先情報提供に関して、より効果的な脆弱性対策の実施を目的としてより多くの情報を提供できるようにしたり、優先情報提供の機会を拡大する観点からより少ない情報を提供できるようにしたりするための実施案を複数検討し、この実施案について、製品開発者、優先情報の提供先の組織に対してヒアリングを行い、ヒアリングの結果を踏まえて改善に向けた論点の整理を行った。

3.2.ISAC 等組織に関する文献調査

現在、電力分野及び政府機関に対して実施している優先情報提供について、電力分野以外の他の重要インフラ分野にも情報を提供するために、重要インフラ分野ごとの ISAC、その他の重要インフラ事業者等、及びそれらの委託先（シ

ステム構築事業者、セキュリティベンダ等）から構成される組織（以下「ISAC 等組織」という。）について文献調査を行った。

文献調査の結果をもとに、優先情報提供の新たな提供先となり得る ISAC 等組織（以下「新たな提供先候補」という。）を特定した。

(1)国内のセキュリティ情報共有組織の整理

国内の代表的なセキュリティ情報共有組織としては、各業界団体等が運営する、①ISAC（Information Sharing and Analysis Center)と、内閣サイバーセキュリティセンター（NISC）が事務局支援を行う、②セプター（CEPTOAR：Capability for Engineering of Protection, Technical Operation, Analysis and Response）、さらに、NISC と JPCERT/CC が事務局支援を行う、③サイバーセキュリティ協議会、経済産業省と情報処理推進機構（IPA）が主導する、④サイバー情報共有イニシアティブ（J-CSIP: Initiative for Cyber Security Information sharing Partnership of Japan）、⑤日本シーサート協議会、⑥日本サイバー犯罪対策センター（JC3）等がある。

J-CSIP やセプターは政府機関との情報共有が主となっており、相互に連携している。

(2)国内の各 ISAC 一覧

同じ業界内でのサイバーセキュリティに関する情報を共有する組織として ISAC がある。2023 年 11 月現在の国内の代表的な ISAC は以下のとおり。

表 3-1 国内の代表的な ISAC 一覧

対象分野	金融機関	ISPを含む通信事業者、放送事業者、ソフトウェアベンダー、情報提供サービス事業者、情報関連機器製造事業者等	電気事業者	交通・運輸事業者
ISAC名称	金融ISAC	ICT-ISAC	電力ISAC	交通ISAC
運営主体	一般社団法人 金融ISAC	一般社団法人 ICT-ISAC	電気事業連合会	一般社団法人交通ISAC
構成員	正会員436組織 賛助会員2組織 アフィリエイト会員31組織	46会員 オブザーバー8組織	正会員39組織 特別会員3組織 テクニカル会員12組織	89会員 うち正会員　68会員 賛助会員　11会員 オブザーバー　10会員

対象分野	自動車	ソフトウェア協会会員	商社
ISAC名称	J-Auto-ISAC	Software ISAC	日本貿易会ISAC
運営主体	一般社団法人Japan Automotive ISAC	一般社団法人 ソフトウェア協会	一般社団法人 日本貿易会
構成員	会員数111社	会員数731組織	会員24社 ※2021年3月時点

（出所：各組織の公開資料等より作成）

(3) ISAC の情報共有体制

前項で示した各 ISAC について、ISAC 内の情報共有体制についての文献調査をし、整理を行った。

(4) 重要インフラ事業者からなるセプターの運営組織の概要

重要インフラ事業者からなるセプターの運営組織の概要については以下のとおり。

表 3-2 セプターの概要

分野	情報通信			金融					航空	空港
事業の範囲	電気通信		放送	銀行等	証券	生命保険	損害保険	資金決済	航空	空港
セプター名称	T-CEPTOAR	ケーブルテレビ CEPTOAR	放送 CEPTOAR	金融CEPTOAR連絡協議会				資金決済 CEPTOAR	航空 CEPTOAR	空港 CEPTOAR
				銀行等 CEPTOAR	証券 CEPTOAR	生命保険 CEPTOAR	損害保険 CEPTOAR			
運営主体	ICT-ISAC	日本ケーブルテレビ連盟	日本民間放送連盟、日本放送協会	全国銀行協会 事務・決済システム部	日本証券業協会IT統括部	生命保険協会 総務部	日本損害保険協会IT企画部	日本資金決済業協会 事務局	定期航空協会	空港・空港ビル協議会
構成員	27社 1団体	310社 1団体	194社 2団体	1,276社	281社 7機関	42社	47社	191社	14社 1団体	8社

分野	鉄道	電力	ガス	政府・行政サービス	医療	水道	物流	化学	クレジット	石油
事業の範囲	鉄道	電力	ガス	政府地方公共団体	医療	水道	物流	化学	クレジット	石油
セプター名称	鉄道 CEPTOAR	電力 CEPTOAR	GAS CEPTOAR	自治体 CEPTOAR	医療 CEPTOAR	水道 CEPTOAR	物流 CEPTOAR	化学 CEPTOAR	クレジット CEPTOAR	石油 CEPTOAR
運営主体	日本鉄道電気技術協会	電力 ISAC	日本ガス協会技術部製造グループ	地方公共団体情報システム機構システム統括室リスク管理課	日本医師会情報システム課	日本水道協会総務部総務課	日本物流団体連合会	石油化学工業協会	日本クレジット協会	石油連盟
構成員	22社 1団体	24社	12社 1団体	47 都道府県 1,741 市区町村	1グループ 21機関	8水道 事業体	6団体 17社	13社	51社	11社

（出所：各組織の公開資料等より作成）

(5) セプターの情報共有体制について

前項で示した各セプターについて、各セプター内の情報共有体制についての文献調査をし、整理を行った。

(6) 新たな提供先候補の抽出

各組織の情報共有体制についての調査の結果、複数の組織を新たな提供先候補として抽出した。

3.3. ISAC 等組織に関するヒアリング調査

(1) ヒアリングの実施概要

前節で抽出した新たな提供先候補に関して、以下要領でヒアリング調査を実施した。

表 3-3 ヒアリング概要

項目	内容
調査方法	対面ヒアリング
調査対象	ISAC 及びセプター7 組織 ※ただし、内 1 組織は先方辞退により実施せず。また、1 組織は書面により実施。
調査実施期間	2024 年 1 月～2 月

(2)調査項目

ヒアリングの主な調査項目は以下の通りである。

＜ヒアリング項目と主な想定質問＞

(1) 情報共有組織の構造について

・組織のメンバー体制、会員の種別、会員の種別ごとの規模、会員の種別ごとの会費、会員の種別ごとに受けられるサービスや義務の違い、会員になるための条件、会員期間について

(2) サイバーセキュリティに関する情報共有の状況

・情報共有の対象者、共有する情報の種別や詳細内容、情報共有の実施頻度、対象者の種類に応じた情報共有の差別化等

・特に、共有する情報として脆弱性情報と攻撃情報の扱いの違い（共有相手、共有する情報のレベル／丸め方等）

・特に、外部から提供された情報を会員内で共有した実績について

(3) 情報共有における条件及び規律

・情報共有を受ける前提としての NDA 等の契約の必要有無、相手別／種類別のルール設定（TLP 設定等）、その他情報提共有に求める条件等

・共有した情報の目的外利用や制限を越えた流出を防ぐ方法、共有情報のトレーサビリティ確保についての方策

(4) 優先情報提供に対する認識および評価

・優先情報提供に対応する組織づくりの実現可能性について

(5) 情報共有以外の活動

・情報共有以外のセキュリティに関する相談・指導・支援、攻撃等の分析、周知活動、教育活動、他の組織との連携等

(6) その他

(3)ヒアリング結果の整理と今後の対応方針検討

ヒアリング結果についてヒアリング相手毎にヒアリング項目の各観点で整理した。その結果を総合し、今後の対応方針を整理した。そのうち、候補となり得る可能性が高いと考えられるものについては、以下の通りである。

表 3-4 提供先候補となり得る ISAC 等組織に関する方針整理

方針	対象団体	理由
優先候補	A 組織	事務局、会員共にセキュリティへの意識が高く、自ら監視システムをもつケースも多いので、これらの脆弱性情報を合わせることで、より効果的な状況確認と迅速対応が期待できる。
次点候補	B 組織	情報管理がしっかりできており、会員同士の情報共有も盛んである。事務局も前向きで、現行の規定等で十分か確認する意思も示している。
可能性を検討	C 組織	情報共有はあまり盛んではないが、分野の情報に絞ればニーズは見込める。まず会員の意向確認をしてみたいというスタンスである。

3.4. 情報共有体制に関する文献調査

優先情報提供について、新たに情報提供先を拡大することを目的として、サイバーセキュリティ協議会、サイバー情報共有イニシアティブ、その他サイバーセキュリティに関する情報を共有することを目的とする主要な情報共有体制について、文献調査を行い、結果をとりまとめた。

(1)各組織の情報共有体制の整理

情報共有体制として、サイバーセキュリティ協議会、サイバー情報共有イニシアティブ、その他サイバーセキュリティに関する情報を共有することを目的とする各組織における情報共有体制を文献調査し、整理した。

各組織の概要は下表のとおりである。

表 3-5 各組織の情報共有体制

対象分野	国の行政機関、重要社会基盤事業者、サイバー関連事業者等、官民の多様な主体	重要インフラ 13 業界（重要インフラ機器製造業者、電力、ガス、化学、石油、資源開発、自動車業界、クレジット、航空、物流、鉄道、エアポート、鉄鋼）	全分野（CSIRT を有する組織全般）	産業界、学術機関、法執行機関等
組織名称	サイバーセキュリティ協議会	J-CSIP	日本シーサート協議会	日本サイバー犯罪対策センター（JC3）
運営主体	NISC、JPCERT/CC	IPA、各参加組織	一般社団法人 日本コンピュータセキュリティインシデント対応チーム協議会	一般財団法人 日本サイバー犯罪対策センター（JC3）
構成員	全 315 者	279 組織 ＋2 情報連携体制	517 チーム ※2023 年 11 月 24 日時点	正会員 35 社 特定会員 8 社 賛助会員 38 社 賛同会員 4 組織

（出所：各組織の公開資料等より作成）

(2) 新たな提供先候補の抽出

情報共有体制については、重要インフラ以外の組織も含むことや、政府におけるセキュリティ情報の共有に関する検討の進展状況などを考慮し、現段階では、候補の抽出やその後のヒアリング調査は保留することとした。

3.5. 脆弱性情報の取扱いにおけるより早い段階での情報の提供に向けた調査

現在の優先情報提供は、P ガイドラインにおいて「IPA および製品開発者と協議の上、対策方法が作成されてから一般公表日までの間に、脆弱性情報と対策方法を、政府機関や当該基盤保有事業者等に対して優先的に提供することができます。」とされているとおり、対策方法が策定された後に実施することが想定されている。実施時期については、より早い段階とすることで、より効果的な脆弱性対策につなげられることが考えられる。そのため、パートナーシップの全体フローのより早い段階で優先情報提供を実施することを検討した。

より早い段階で実施できるようにするための、提供タイミングが異なる実施案を複数検討し、この実施案について、製品開発者及び優先情報の提供先の組織に対してヒアリングを行い、結果をとりまとめた。

なお、この調査は次節とヒアリング対象者が重複するため、次節と合わせて実施した。具体的な調査内容及び調査結果の報告は次節において行う。

3.6.優先情報提供する情報の内容の拡大に向けた調査

現在の優先情報提供で提供している内容として、告示において「当該脆弱性情報等をあらかじめ通知することができる。」と規定されている。「当該脆弱性情報等」は JVN で公表する情報と同等の情報としているが、より効果的な脆弱性対策の実施を目的として、より多くの情報を提供できるようにし、また、優先情報提供の機会を拡大する観点から、より少ない情報を提供できるようにすることで、優先情報提供を更に充実したものとできると考えられる。

このため、現状について整理し、より多くの情報及びより少ない情報を提供できるようにするための実施案を複数検討し、この実施案について、製品開発者、及び優先情報の提供先の組織に対してヒアリングを行い、結果をとりまとめた。

なお、この調査は前節と対象者が重複するため、前節と合わせて実施した。具体的な調査内容及び調査結果の報告を以下に示す。

(1)ヒアリング実施概要

表 3-6 ヒアリング概要

項目	内容
調査方法	リモート
調査対象	優先情報提供先組織として３組織を設定 ※ただし、うち１組織は先方辞退により実施せず
	製品開発者として４社を設定 ・A 社（優先情報提供の実施経験と、候補となったが実際には実施しなかった経験のある製品開発者） ・B 社（優先情報提供の候補となったが、実際には実施しなかった経験のある製品開発者） ・C 社（優先情報提供の実施経験のある製品開発者） ・D 社（優先情報提供の実施経験のある製品開発者）

(2) ヒアリング項目

ヒアリングにあたり、「より早い段階での情報の提供」と「優先情報提供する情報の内容拡大・減少」の実施案を検討した。その内容は以下の通りである。

(a) より早い段階での情報の提供

より早い段階での情報の提供については、以下の段階を想定した。より早い段階ほど、情報が不正確であったり、情報量が少ないなどにより、情報提供先組織において可能な対応が限られることが考えられる。

- 脆弱性情報の届出があった段階
- 製品開発者が脆弱性を確認した段階
- 製品開発者が脆弱性の確認方法をまとめた段階
- 製品開発者が脆弱性の回避方法をまとめた段階
- 製品開発者が脆弱性対策をまとめた段階

(b) 優先情報提供する情報の内容拡大・減少

優先情報提供する情報の内容拡大については、従来の JVN 公表相当の情報に、以下の情報を加えることを想定した。

- 攻撃の再現手法に関する情報
- 実際の攻撃の発生に関する情報（IoC 情報等）

また、情報を減らした状態での提供情報としては、以下の内容を想定した。

- 製品名のみ
- JVN 公表予定のタイトル（製品名、製品開発者名、脆弱性種類等を含む）と公表時期のみ

上記の実施案を踏まえた、ヒアリングの主な調査項目は以下の通りである。

＜ヒアリング項目と主な想定質問＞

(1) より早い段階での情報の提供について

- 優先情報提供先組織に対するヒアリング項目
  - 優先情報提供をより早い段階で実施した場合に期待される効果、どのくらい早い段階で情報を欲しいか
  - 優先情報提供をより早い段階で実施した場合のハードル、課題、条件
- ソフトウェア製品開発者に対するヒアリング項目

- 優先情報提供をより早い段階で行うためのハードル、課題、条件、どの程度ならば早くできるか

(2)優先情報提供する情報の内容拡大・減少について

- 優先情報提供先組織に対するヒアリング項目
  - 優先情報提供する情報内容を増やすことで期待される効果、その場合に欲しい情報
  - 優先情報提供する情報内容を増やした場合の情報管理・情報展開上のハードル、課題、条件
  - 優先情報提供する情報内容を減らして機会拡大を行うことで期待される効果、その場合に減らしても良い情報、望まれる情報提供の頻度についての要望
  - 優先情報提供する情報内容を減らして機会拡大を行うためのハードル、課題、条件
- ソフトウェア製品開発者に対するヒアリング項目
  - 優先情報提供の情報を増やすにあたってのハードル、課題、条件、どのような情報なら追加提供できるか
  - 優先情報提供の情報を減らして機会拡大を行うためのハードル、課題、条件、どの程度なら頻度拡大できるか

(3)その他・現状の優先情報提供について

- 優先情報提供先組織・ソフトウェア製品開発者共通のヒアリング項目
  - 現状の優先情報提供の場合に生じる通常の公表と異なる部分、負荷となる部分
  - その他、優先情報提供に関するご意見等
- ソフトウェア製品開発者に対するヒアリング項目
  - 過去に優先情報提供を実施できなかった場合に課題となった点（該当する場合）

(3)ヒアリング結果の整理・主要な意見

ヒアリング結果について検討テーマ別に、ヒアリングから得られた主要な意見を下記の表で整理した。

表 3-7 より早い段階での提供／提供する情報の内容の拡大に関する主要な意見

検討テーマ	主要な意見
より早い段階での情報の提供	・ 最低限、脆弱性の回避策が判明した後での情報提供をしてほしい ・ パッチができてからの情報提供がより望ましい

優先情報提供する情報の内容拡大	・ 追加で欲しい情報はない（攻撃手法等の情報は情報管理上のリスクが大きい） ・ 追加情報については不必要な情報管理の負担増を無くすため、対象製品を使っているユーザに絞って提供できるように、二段階で出す等の工夫ができると良い
優先情報提供する情報の内容減少による機会拡大	・ 脆弱性情報と深刻度は無くても良いが、JVN で提供されるそれ以外の情報である製品名、製品開発者名、バージョン、想定される影響、対策・回避策はすべて必要である
その他の意見・要望	・ 海外製品についての情報提供を増やしてほしい

3.7.その他の検討事項・意見

経済産業省からの要請に基づいて、優先情報提供の提供先について、告示を改めることを前提に、基幹インフラ事業者等を追加することの方向性について議論がなされた。なお、研究会の最終会合までに告示を改めることに向けた対応には至らなかった。

また、JPCERT/CC からは、優先情報提供の拡充等について以下の意見が示された。

- 優先情報提供した情報が、提供先組織やその関係先で不適切に取り扱われることについて、優先情報提供に協力いただいた製品開発者側に懸念が生じている。
- 優先情報提供の拡充等を検討するにあたり、不適切な取扱いを防止する方策や優先情報提供の効果の検討が十分に行われるべきである。
- 第１回、第２回会合で意見を述べた通り、2023 年度の調査結果を踏まえて、拡充等の判断を行うべきであり、その判断においては、特に、トレーサビリティの確保や不適切な取扱いの防止策等の「安全装置」が十分であるかどうかが重要な要素となる。
- 優先情報提供の枠組みの検討を行った過去の研究会での議論の観点を踏まえた調査検討がなされることとともに、製品開発者側からの理解や協力を得られる環境が整うことも拡充等にあたって必要となる。
- 以下の点について改めて確認する。今後の実務対応にあたって参考とされたい。
  - ✓ 優先情報提供の分野の拡大は、2023 年度に実施した調査結果を踏まえるものとすべきであり、2024 年度の検討対象とすべきである。また、情報

の不適切な取扱いの防止策についても、2023 年度の調査結果を踏まえ、改めて研究会等において検討すべきである。

- ✓ 優先情報提供の拡充・拡大に伴い不適切な取扱いが生じる可能性も高くなるため、製品開発者側の懸念を払しょくすべく、製品開発者側に適切な説明がなされるべきであり、また、優先情報提供という取組みについて協力依頼がなされるべきである。
- ✓ 不適切な取扱いの防止や製品開発者からの理解を得る観点から、専門的な知見のある事務局が存在し、明確な情報管理の規律、罰則等のある情報共有活動の枠組みを活用することも検討すべきである。
- ✓ 優先情報提供の提供先組織でシステム運用を担う IT ベンダが優先情報提供の提供内容の情報に触れる可能性があるが、その IT ベンダが製品開発者の競合企業であることもあり得る。競合他社間で未公開の機微な脆弱性対策情報のやり取りが生じることについても、検討する必要がある。
- ✓ 国や重要インフラ等の重要性の高いシステムが影響を受ける脆弱性、とりわけゼロデイの脆弱性や悪用が観測されている脆弱性については、JPCERT/CC において、注意喚起や対象ホスト利用組織への直接通知等の活動を実施している。そのような他の活動もあるなか、優先情報提供が効果的な取組みとして機能することの不断の検証が必要である。
- ✓ 昨今、運用保守ベンダが管理・提供するアプライアンス経由での侵入や、運用保守ベンダがサプライチェーン攻撃の踏み台になる事案が多発している。このような事案は、製品の利用組織ではなく、IT サプライチェーン上に存在する事業者が対処する必要がある。そのような脅威動向やインシデント対応の現場の実情を踏まえて、優先情報提供の提供先拡大について議論する必要がある。
- ✓ 国家安全保障戦略で示されるサイバー安全保障分野での新体制・制度検討が進むなか、脅威情報の提供・情報共有という大きな枠組みのなかで、優先情報提供を総合的に検討すべきであると考えられる。

4. パートナーシップの運用改善事項等の調査及びPガイドラインへの反映

4.1. 調査の概要

(1)目的

パートナーシップでは、ソフトウェア製品の脆弱性情報について、製品開発者への連絡及び公表に係る調整が不可能であると判断した届出（以下「調整不能案件」という。）に対して、製品利用者が脆弱性による被害を受ける可能性を低減することを目的として公表判定委員会を開催し、調整不能案件の脆弱性情報を公表するか否かを調整不能案件に利害関係のない委員にて判定の上、その判定結果により脆弱性情報を公表している。

2018年度の脆弱性研究会において、調整不能案件に関する運用改善の検討を行った。この検討結果を踏まえ、パートナーシップの運用の改善に必要となるパートナーシップガイドライン（Pガイドライン）の改訂に向けた検討を行い、修正案を作成した。

(2)手順

(a)調整不能案件の改善に関する調査及びPガイドラインへの反映

2018年度の脆弱性研究会において、脆弱性検証の可否や脆弱性の影響度に応じた調整不能案件の取扱方針について検討を行った。当時の検討結果を踏まえた方針について、Pガイドラインには明示的に規定されていないことから、Pガイドラインの改訂のために以下の作業を実施した。

- 2018年度報告書の48頁の(3)「連絡不能案件の取扱方針の見直し」に関する改善方針の検討結果にもとづき、修正が必要となるガイドラインの規定を特定し、修正案を作成した。
- 修正に当たっては、既存の条項の修正だけではなく、ガイドラインの付録を新設して必要な規定をまとめて記載することを検討した。

(b)その他軽微な修正

IPAウェブサイトのリニューアルに伴うURLの変更や、引用している資料名の変更に対応した。

4.2. 調整不能案件の改善に関する調査及びPガイドラインへの反映

(1)2018 年度研究会における見直し方針の確認

2018 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報告書において、「連絡不能案件の取扱方針の見直し」の方針が示されている。

表 4-1 2018 年度報告書における見直し方針の記述

項目	現在の運用	改善方針
公表判定委員会の判定対象案件	■ Pガイドライン上判定対象の案件に制限はないが、重要度の高い案件から判定いただくため、内規を設けて運用。	■ 内規での制限を廃止。 ■ 判定4条件に合致する「優先対応」「通常対応」案件のみとする。 ■ 「簡易対応」案件は、判定対象としない。 ■ 脆弱性検証不可のうち「優先対応」案件は検証にかかるコストを踏まえて購入等を判断する。
判定対象外の案件の取扱い	■ 公表判定委員会に諮ることができないため滞留 ■ 影響度評価で簡易対応の案件は、詳細情報を通知していれば(脆3)取扱終了できるが、詳細情報未通知のもの(脆1、脆2)は連絡不能になると通知できず滞留	■ Pガイドラインの、受領後の対応の条件(ア)を告示の記載(脆弱性関連情報に該当しないこと)に修正し、本制度で取扱価値があるか否かが条件に含まれると解釈を拡大する。 ■ 価値(価値の条件例:費用対効果等)が低い度判断した案件は取扱終了とし、連絡不能開発者一覧への掲載を取り止める。 ■ 取扱価値のある案件か否かの判断基準作成及び判断は IPA が実施する。

また、2018 年度研究会においては、この見直し方針に基づき、連絡不能案件について、影響度と脆弱性検証可否の組み合わせにより、取扱終了とするものと、公表判定委員会で判定するものとが整理された。整理された結果は下記の表の通りである。

表 4-2 影響度と脆弱性検証可否の組み合わせによる取扱方針の整理

影響度の考え方	脆弱性検証	取扱方針
優先対応	検証可	公表判定委員会で判定
	検証不可	検証に掛かるコストを考慮し適宜公表判定委員会で判定
通常の対応	検証可	公表判定委員会で判定
	検証不可	取扱終了(連絡不能開発者一覧から削除)
簡易な対応	検証可	取扱終了(連絡不能開発者一覧から削除)
	検証不可	取扱終了(連絡不能開発者一覧から削除)

2018 年度の脆弱性研究会で検討した方針については、その検討結果を、IPA（事務局）から、公表判定委員会の委員に説明することとなっていた。2021 年度及び 2022 年度の公表判定委員会において、委員に説明を行い、方針については了承を得た。また、下記 2 点について対応するよう意見があった。

- 連絡不能案件については、取扱いを終了する前に、審議対象とはしないものの、公表判定委員会に報告すること。
- 優先対応（脆弱性の影響度が高い）かつ検証不可（検証用の製品が有償である等）の案件について、検証のために製品を購入すべきかどうかについて、公表判定委員会で検討できるようにすること。

(2)修正案の検討

(a)修正方針の整理

P ガイドラインにおいて、調整不能案件や連絡不能に係る記述は、

> Ⅳ. ソフトウェア製品に係る脆弱性関連情報取扱
> 3. IPA(受付機関)の対応
> (2)調整不能案件の公表判定について
> 4. JPCERT/CC(調整機関)の対応
> 2) 製品開発者への連絡
> 付録2 脆弱性情報取扱いのフロー
> 付録5 ソフトウェア製品における連絡不能案件の取扱いについて

等を中心に記述がみられる。これらの条項との整合性を維持しつつ、分かりやすい記述とする観点から、具体的には付録において一か所にまとめる形で必要な記述を行う方向で検討を実施した。

(b)修正案の作成

P ガイドラインの修正案としては、「付録５ソフトウエア製品における連絡不能案件の取扱いについて」に新たに項目３を設定し、まとめて記述する案を作成した。

具体的な修正案については、「5.P ガイドラインの改訂等」を参照のこと。

4.3.その他軽微な修正

P ガイドラインでは、IPA ウェブサイトに掲載されている普及啓発資料等への URL が記載されている。これらの URL について、2023 年の IPA のウェブサイトのリニューアルに伴い変更が生じている。また、引用している資料名についても変更しているものもあった。これらについて、最新の情報に改める対応を実施した。

5.P ガイドラインの改訂等

「2. 製品開発者と調整する過程における３つの課題に関する調査」及び「4. パートナーシップの運用改善事項等の調査及びP ガイドラインへの反映」において検討した個別の条項の修正案をもとに、P ガイドライン、及びソフトウエア製品開発者による脆弱性対策情報の公表マニュアルの冊子としての改訂案を作成した。

5.1.P ガイドライン改訂案作成

本年度の調査結果をもとに、以下の方針に従ってP ガイドライン改訂案をとりまとめた。

表 5-1 P ガイドライン改訂案の作成方針

方針	概要
「製品開発者と調整する過程における３つの課題に関する調査」の結果の反映	・脆弱性の悪用を示す情報に関する情報の取扱い等に関する検討結果を反映する。 ・「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検討結果を反映する。
「パートナーシップの運用改善事項等の調査」の結果の反映	・製品開発者への連絡及び公表に係る調整が不可能であると判断した届出(調整不能案件)における取扱い終了に関する検討結果を反映する。
その他、参照先情報の変更等の反映	・本文において参照している各種コンテンツの URL や名称等の変更結果を反映する。

(1)脆弱性の悪用を示す情報に関する情報の取扱い等に関する検討結果の反映

(a)発見者向けの規定

現行規定	改定案
2.発見者の対応 5) 届け出る情報の内容 発見者は、届け出る情報の中で以下の点を明示してください（詳細は、https://www.ipa.go.jp/security/vuln/ を参照）。 (ア) 氏名等の発見者を識別するための情報	2.発見者の対応 5) 届け出る情報の内容 発見者は、届け出る情報の中で以下の点を明示してください（詳細は、https://www.ipa.go.jp/security/vuln/ を参照）。 (ア) 氏名等の発見者を識別するための情報

(イ) 電子メールアドレス等の発見者の連絡先 (ウ) (ア)および(イ)の製品開発者への通知の可否 (エ) 製品開発者から直接連絡を受けることの可否 (オ) (ア)の公表の可否 (カ) 脆弱性関連情報に係るソフトウエア製品の名称 (キ) 脆弱性関連情報の内容(脆弱性関連情報を確認する環境、手順および結果) 可能であれば、脆弱性が存在する証拠 5 を一緒に提出してください。ただし、証拠の取得に際しては、関連法令に触れることがないように留意してください(付録3を参照)。 (ク) 個人情報の取扱方法(製品開発者への通知および直接の情報交換の可否、一般への公表の可否) ・発見者が望まない場合、IPA は、JPCERT/CC および製品開発者に対して、発見者を特定しうる情報を通知することはありません。 ・発見者が望む場合、IPA および JPCERT/CC は、脆弱性情報と製品開発者ごとの脆弱性検証の結果、対策方法および対応状況を公表する際に発見者名を付記するとともに、製品開発者に対しても、対策方法の公表時に発見者名を付記することを推奨します。 (ケ) 他組織(製品開発者、他のセキュリティ関係機関等)への届出の状況等	(イ) 電子メールアドレス等の発見者の連絡先 (ウ) (ア)および(イ)の製品開発者への通知の可否 (エ) 製品開発者から直接連絡を受けることの可否 (オ) (ア)の公表の可否 (カ) 脆弱性関連情報に係るソフトウエア製品の名称 (キ) 脆弱性関連情報の内容(脆弱性関連情報を確認する環境、手順および結果) 可能であれば、脆弱性が存在する証拠 5 を一緒に提出してください。ただし、証拠の取得に際しては、関連法令に触れることがないように留意してください(付録3を参照)。 (ク) 個人情報の取扱方法(製品開発者への通知および直接の情報交換の可否、一般への公表の可否) ・発見者が望まない場合、IPA は、JPCERT/CC および製品開発者に対して、発見者を特定しうる情報を通知することはありません。 ・発見者が望む場合、IPA および JPCERT/CC は、脆弱性情報と製品開発者ごとの脆弱性検証の結果、対策方法および対応状況を公表する際に発見者名を付記するとともに、製品開発者に対しても、対策方法の公表時に発見者名を付記することを推奨します。 (ケ) 他組織(製品開発者、他のセキュリティ関係機関等)への届出の状況等 (コ) その他、当該脆弱性情報に関する参考情報 ・当該脆弱性情報を取り扱う上で参考となる情報(製品の利用者数や利用者の特性(重要インフラ事業者等の利用がある等)、当該脆弱性への攻撃の観測情報等)があれば、併せて提出してください。

(b) IPA 向けの規定

現行規定	改定案
3.IPA(受付機関)の対応 (1) 脆弱性関連情報の届出受付と取扱いについて 13) 一般への情報の公表 IPA および JPCERT/CC は、JVN を通じて、一般に対し、脆弱性情報と JPCERT/CC から連絡したすべての製品開発者の脆弱性検証の結果、対策方法および対応状況を公表します。	3.IPA(受付機関)の対応 (1) 脆弱性関連情報の届出受付と取扱いについて 13) 一般への情報の公表 IPA および JPCERT/CC は、JVN を通じて、一般に対し、脆弱性情報と JPCERT/CC から連絡したすべての製品開発者の脆弱性検証の結果、対策方法および対応状況を公表します。

さらに、一旦公表した後、製品開発者から新たな対策方法と対応状況のいずれかまたは両方を受け取った場合、その都度更新します。 また、IPA および JPCERT/CC は、JVN に関する問い合わせ先を明示し、主として OSS 等に関して、システム構築事業者や製品利用者の脆弱性対応を促すことを目的として、問い合わせ対応を実施します。なお、問い合わせに関する内容については、必要に応じて JVN の公表情報に反映します。 一般への情報の公表に際しては、IPA は、発見者にその旨を通知します。	さらに、一旦公表した後、製品開発者から新たな対策方法と対応状況のいずれかまたは両方を受け取った場合、その都度更新します。また、当該脆弱性に関する悪用の事実を把握した場合には、製品開発者と協議のうえ、JVN において悪用に関する記載を行います。当該悪用に関する情報が公開の情報でない場合、IPA および JPCERT/CC は、JVN において記載を行うまでの間、当該悪用に関する情報を第三者に漏えいしないよう適切に管理します。 また、IPA および JPCERT/CC は、JVN に関する問い合わせ先を明示し、主として OSS 等に関して、システム構築事業者や製品利用者の脆弱性対応を促すことを目的として、問い合わせ対応を実施します。なお、問い合わせに関する内容については、必要に応じて JVN の公表情報に反映します。 一般への情報の公表に際しては、IPA は、発見者にその旨を通知します。

(c)JPCERT/CC 向けの規定

現行規定	改定案
4.JPCERT/CC(調整機関)の対応 3) 公表日の決定 JPCERT/CC は、製品開発者から脆弱性検証の結果を受け取り、製品開発者と相談した上で、脆弱性情報と製品開発者の対策方法および対応状況の公表日を決定し、IPA および関係する製品開発者に通知します。公表日は、JPCERT/CC が「製品開発者への連絡」(4. 2)を参照)にて規定された連絡を最初に試みた日(起算日、2. 注釈 4 を参照)から 45 日後を目安とします。ただし、公表日の決定に際しては、以下の点も考慮します。 ① 対策方法の作成に要する期間 ② 海外の調整機関との調整に要する期間 ③ 脆弱性情報流出に係るリスク また、通知した製品開発者が複数いて、その一部の製品開発者しか脆弱性検証の結果報告をしない場合、JPCERT/CC は、得られた結果報告を踏まえつつ、過去の類似事例や②③を参考にして公表日を決定し、IPA および関係する製品開発者に通知します。	4.JPCERT/CC(調整機関)の対応 3) 公表日の決定 JPCERT/CC は、製品開発者から脆弱性検証の結果を受け取り、製品開発者と相談した上で、脆弱性情報と製品開発者の対策方法および対応状況の公表日を決定し、IPA および関係する製品開発者に通知します。公表日は、JPCERT/CC が「製品開発者への連絡」(4. 2)を参照)にて規定された連絡を最初に試みた日(起算日、2. 注釈 4 を参照)から 45 日後を目安とします。ただし、公表日の決定に際しては、以下の点も考慮します。 ① 対策方法の作成に要する期間 ② 海外の調整機関との調整に要する期間 ③ 脆弱性情報流出に係るリスク ④ 当該脆弱性の悪用に関するリスク また、通知した製品開発者が複数いて、その一部の製品開発者しか脆弱性検証の結果報告をしない場合、JPCERT/CC は、得られた結果報告を踏まえつつ、過去の類似事例や②③を参考にして公表日を決定し、IPA および関係する製品開発者に通知します。

現行規定	改定案
4.JPCERT/CC（調整機関）の対応 8） 優先的な情報提供 JPCERT/CC は、届出がなされた脆弱性関連情報に関して、国民の日常生活に必要不可欠なサービスを提供するための基盤となる設備に対し特に影響が大きいと推察される場合、IPA および製品開発者と協議の上、対策方法が作成されてから一般公表日までの間に、脆弱性情報と対策方法を、政府機関や当該基盤保有事業者等に対して優先的に提供することができます。 なお、優先的な情報提供を受ける基盤保有事業者は、以下の条件をすべて満たす必要があります。 (ア)情報を提供された当該事業者の中で秘密情報管理を徹底すること (イ)当該事業者自身の委託先（システム構築事業者、セキュリティベンダ等）各社において、秘密情報管理を徹底すること (ウ)JPCERT/CC から優先的に提供される情報は当該基盤を防護する目的に対してのみ利用することを徹底すること ただし、優先提供の趣旨を鑑み、運用方法および提供対象事業者を継続的に見直していくものとします。 当該基盤保有事業者は、内閣サイバーセキュリティセンター（NISC）の最新の「重要インフラの情報セキュリティ対策に係る行動計画」で定める重要インフラ事業者等とします。	4.JPCERT/CC（調整機関）の対応 8） 優先的な情報提供 JPCERT/CC は、届出がなされた脆弱性関連情報に関して、国民の日常生活に必要不可欠なサービスを提供するための基盤となる設備に対し特に影響が大きいと推察される場合、IPA および製品開発者と協議の上、対策方法が作成されてから一般公表日までの間に、脆弱性情報と対策方法を、政府機関や当該基盤保有事業者等に対して優先的に提供することができます。また、提供が可能である場合には、悪用に関する記載を含みます。 なお、優先的な情報提供を受ける基盤保有事業者は、以下の条件をすべて満たす必要があります。 (ア)情報を提供された当該事業者の中で秘密情報管理を徹底すること (イ)当該事業者自身の委託先（システム構築事業者、セキュリティベンダ等）各社において、秘密情報管理を徹底すること (ウ)JPCERT/CC から優先的に提供される情報は当該基盤を防護する目的に対してのみ利用することを徹底すること ただし、優先提供の趣旨を鑑み、運用方法および提供対象事業者を継続的に見直していくものとします。 当該基盤保有事業者は、内閣サイバーセキュリティセンター（NISC）の最新の「重要インフラの情報セキュリティ対策に係る行動計画」で定める重要インフラ事業者等とします。

現行規定	改定案
4.JPCERT/CC（調整機関）の対応 9） 一般への情報の公表 JPCERT/CC および IPA は、JVN を通じて、一般に対し、脆弱性情報と JPCERT/CC から連絡したすべての製品開発者の脆弱性検証の結果、対策方法および対応状況を公表します。 さらに、一旦公表した後、製品開発者から新たな対策方法と対応状況のいずれか一つ以上を受け取った場合、その都度更新します。 また、製品開発者が製品利用者に生じるリスクを低減できると判断した場合、JPCERT/CC は製品開発者と調整した上で、製品開発者が製品利用者に脆弱性検証の結果、対策方法およ	4.JPCERT/CC（調整機関）の対応 9） 一般への情報の公表 JPCERT/CC および IPA は、JVN を通じて、一般に対し、脆弱性情報と JPCERT/CC から連絡したすべての製品開発者の脆弱性検証の結果、対策方法および対応状況を公表します。 さらに、一旦公表した後、製品開発者から新たな対策方法と対応状況のいずれか一つ以上を受け取った場合、その都度更新します。また、当該脆弱性に関する悪用の事実を把握した場合には、製品開発者と協議のうえ、JVN において悪用に関する記載を行います。当該悪用に関する情報が公開の情報でない場合、JPCERT/CC および IPA は、JVN において記

び対応状況を公表前に通知することを認めることができます。 さらに、JPCERT/CC および IPA は、JVN に関する問い合わせ先を明示し、主として OSS 等に関して、システム構築事業者や製品利用者の脆弱性対応を促すことを目的として、問い合わせ対応を実施します。なお、問い合わせに関する内容については、必要に応じて JVN の公表情報に反映します。	載を行うまでの間、当該悪用に関する情報を第三者に漏えいしないよう適切に管理します。 また、製品開発者が製品利用者に生じるリスクを低減できると判断した場合、JPCERT/CC は製品開発者と調整した上で、製品開発者が製品利用者に脆弱性検証の結果、対策方法および対応状況を公表前に通知することを認めることができます。 さらに、JPCERT/CC および IPA は、JVN に関する問い合わせ先を明示し、主として OSS 等に関して、システム構築事業者や製品利用者の脆弱性対応を促すことを目的として、問い合わせ対応を実施します。なお、問い合わせに関する内容については、必要に応じて JVN の公表情報に反映します。

(d)製品開発者向けの規定

現行規定	改定案
5. 製品開発者の対応 3) 脆弱性情報の公表日の調整 製品開発者は、検証の結果、脆弱性が存在することを確認した場合、対策方法の作成や外部機関との調整に要する期間、当該脆弱性情報流出に係るリスクを考慮しつつ、脆弱性情報の公表に関するスケジュールについて JPCERT/CC と相談してください。なお、公表日は、JPCERT/CC が「製品開発者への連絡」(4. 2)を参照)にて規定された連絡を最初に試みた日(起算日、2. 注釈 4 を参照)から 45 日後を目安とします。公表に更なる時間を要する場合は、JPCERT/CC と相談してください。	5. 製品開発者の対応 3) 脆弱性情報の公表日の調整 製品開発者は、検証の結果、脆弱性が存在することを確認した場合、対策方法の作成や外部機関との調整に要する期間、当該脆弱性情報流出に係るリスクおよび脆弱性の悪用に関するリスクを考慮しつつ、脆弱性情報の公表に関するスケジュールについて JPCERT/CC と相談してください。なお、公表日は、JPCERT/CC が「製品開発者への連絡」(4. 2)を参照)にて規定された連絡を最初に試みた日(起算日、2. 注釈 4 を参照)から 45 日後を目安とします。公表に更なる時間を要する場合は、JPCERT/CC と相談してください。また、公表日の調整に際して考慮するため、脆弱性情報の公表までの過程において、当該脆弱性が悪用されていることを把握した場合には、JPCERT/CC にその旨を連絡してください。

現行規定	改定案
5. 製品開発者の対応 7) 対策方法および対応状況の連絡 製品開発者は、脆弱性情報の一般への公表日までに脆弱性関連情報に係る対策方法を作成するように努めて、対策方法および対応状況を JPCERT/CC に連絡してください。 JPCERT/CC に対する対策方法および対応状況の報告をもって、IPA にも報告したこととみな	5. 製品開発者の対応 7) 対策方法および対応状況の連絡 製品開発者は、脆弱性情報の一般への公表日までに脆弱性関連情報に係る対策方法を作成するように努めて、対策方法および対応状況を JPCERT/CC に連絡してください。 JPCERT/CC に対する対策方法および対応状況の報告をもって、IPA にも報告したこととみな

されます。また、新たな対策方法を作成した場合や対応状況が変わった場合、その都度、JPCERT/CC に最新の情報を連絡してください。	されます。また、新たな対策方法を作成した場合や対応状況が変わった場合、その都度、JPCERT/CC に最新の情報を連絡してください。また、脆弱性情報の公表までの過程において、当該脆弱性が悪用されていることを把握した場合には、JPCERT/CC にその旨を連絡し、JVN での記載について協議してください。

(2)「製品開発者が全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検討結果の反映

(a)IPA 向けの規定

現行規定	改定案
3.IPA(受付機関)の対応 (1) 脆弱性関連情報の届出受付と取扱いについて 7) 脆弱性関連情報の受理後の対応 IPA は、JPCERT/CC に通知した脆弱性関連情報に関して、以下のいずれかに該当する場合、発見者に連絡するとともに、処理を取りやめることがあります。 (ア) 脆弱性関連情報に該当しない場合 (イ) 本ガイドラインの適用範囲外である場合 (ウ) 脆弱性による影響が小さい場合(付録4を参照) (エ) 脆弱性関連情報が既知であり、かつ公表されている場合 (オ) 製品開発者がすべての製品利用者に通知する場合(システム構築事業者を介して通知するケースを含む)	3.IPA(受付機関)の対応 (1) 脆弱性関連情報の届出受付と取扱いについて 7) 脆弱性関連情報の受理後の対応 IPA は、JPCERT/CC に通知した脆弱性関連情報に関して、以下のいずれかに該当する場合、発見者に連絡するとともに、処理を取りやめることがあります。 (ア) 脆弱性関連情報に該当しない場合 (イ) 本ガイドラインの適用範囲外である場合 (ウ) 脆弱性による影響が小さい場合(付録4を参照) (エ) 脆弱性関連情報が既知であり、かつ公表されている場合 (オ) 製品開発者がすべての製品利用者に通知する場合(システム構築事業者を介して通知するケースを含む)(付録1を参照)

(b)JPCERT/CC 向けの規定

現行規定	改定案
4.JPCERT/CC(調整機関)の対応 4) 公表日決定後の対応 JPCERT/CC は、製品開発者から、一般への公表日の変更の要請を受けた場合、公表日を変更することがあります。その場合、変更した公表日を IPA および脆弱性関連情報に関して連絡を行ったすべての製品開発者に連絡します。 さらに、以下の場合、一般への公表を取りやめることがあります。その場合、その旨を製品開発者および IPA に連絡します。	4.JPCERT/CC(調整機関)の対応 4) 公表日決定後の対応 JPCERT/CC は、製品開発者から、一般への公表日の変更の要請を受けた場合、公表日を変更することがあります。その場合、変更した公表日を IPA および脆弱性関連情報に関して連絡を行ったすべての製品開発者に連絡します。 さらに、以下の場合、一般への公表を取りやめることがあります。その場合、その旨を製品開発者および IPA に連絡します。

(ア)通知を行った製品開発者から脆弱性情報に該当しないとの連絡を受けた場合 (イ)通知を行った製品開発者から脆弱性による影響がないとの連絡を受けた場合 (ウ)通知を行った製品開発者から脆弱性による影響が小さいとの連絡を受けた場合(付録4を参照) (エ)脆弱性関連情報が既知であり、脆弱性情報等が公表されている場合 (オ)製品開発者がすべての製品利用者に通知する場合(システム構築事業者を介して通知するケースを含む)	(ア)通知を行った製品開発者から脆弱性情報に該当しないとの連絡を受けた場合 (イ)通知を行った製品開発者から脆弱性による影響がないとの連絡を受けた場合 (ウ)通知を行った製品開発者から脆弱性による影響が小さいとの連絡を受けた場合(付録4を参照) (エ)脆弱性関連情報が既知であり、脆弱性情報等が公表されている場合 (オ)製品開発者がすべての製品利用者に通知する場合(システム構築事業者を介して通知するケースを含む)(付録1を参照)

(c)付録の規定

現行規定	改定案
付録1 用語の解説 [新設]	付録1 用語の解説 8.製品開発者がすべての製品利用者に通知する場合 ソフトウエア製品の脆弱性の取扱いにおける「製品開発者がすべての製品利用者に通知する場合」とは、すべての製品利用者に製品開発者から脆弱性情報および対策方法を適時かつ確実に通知できる場合(システム構築事業者を介して通知するケースを含む) が該当します。特に、オーダーメイドで作成された特定個社向けの情報システムに関する脆弱性や、製品開発者が、製品利用者との間で有償の保守運用契約を締結しており、支払いの手続きの過程によるものを含め、すべての製品利用者の連絡先を製品開発者が把握しており、脆弱性情報および対策方法を通知できる場合が考えられます。

(3)「調整不能案件」における取扱い終了に関する検討結果の反映

(a)IPA 向けの規定

現行規定	改定案
3.IPA(受付機関)の対応 (2)調整不能案件の公表判定について 1) 公表判定委員会の組織 IPA は、JPCERT/CC からⅣ.4. 10)の通知を受けて、JPCERT/CC と製品開発者との間で脆弱性情報の公表に係る調整が不可能であると判断した場合(以下「調整不能」という)、その案件が脆弱性情報を公表する条件を満たしている	3.IPA(受付機関)の対応 (2)調整不能案件の公表判定について 1) 公表判定委員会の組織 IPA は、JPCERT/CC からⅣ.4. 10)の通知を受けて、JPCERT/CC と製品開発者との間で脆弱性情報の公表に係る調整が不可能であると判断した場合(以下「調整不能」という)、その案件が脆弱性情報を公表する条件を満たしている

かを判定する「公表判定委員会」を組織します。 調整不能とは、具体的には以下のいずれかのケースに該当します。 (ア)Ⅳ．4．2)に示した連絡方法をすべて試みても製品開発者と 6 ヶ月以上連絡が取れない場合（以下、「連絡不能」という） (イ)製品開発者と JVN 公表に関する調整を行ったが合意に至ることが社会通念上困難になったと判断される場合 IPA は、公表判定委員会において、脆弱性情報を公表しない場合に製品利用者等が受けうる被害と、公表した場合に製品開発者、製品利用者等が被りうる不利益とのバランスに配慮するとともに、社会的影響も考慮し、不利益を被りうる関係者が意見を表明することも可能な、透明性・妥当性のある判定プロセスを整備します。 IPA は、中立性を考慮し、当該調整不能案件に利害関係がない有識者、法律やサイバーセキュリティの専門家、当該ソフトウエア製品分野の専門家を公表判定委員会の委員に指名します。公表判定委員会は、関係者に意見表明の機会を提供し、その意見を踏まえ、公表が適当か否かを判定します。	かを判定する「公表判定委員会」を組織します。 調整不能とは、具体的には以下のいずれかのケースに該当します。 (ア)Ⅳ．4．2)に示した連絡方法をすべて試みても製品開発者と 6 ヶ月以上連絡が取れない場合（以下、「連絡不能」という） (イ)製品開発者と JVN 公表に関する調整を行ったが合意に至ることが社会通念上困難になったと判断される場合 IPA は、公表判定委員会において、脆弱性情報を公表しない場合に製品利用者等が受けうる被害と、公表した場合に製品開発者、製品利用者等が被りうる不利益とのバランスに配慮するとともに、社会的影響も考慮し、不利益を被りうる関係者が意見を表明することも可能な、透明性・妥当性のある判定プロセスを整備します。 IPA は、中立性を考慮し、当該調整不能案件に利害関係がない有識者、法律やサイバーセキュリティの専門家、当該ソフトウエア製品分野の専門家を公表判定委員会の委員に指名します。公表判定委員会は、関係者に意見表明の機会を提供し、その意見を踏まえ、公表が適当か否かを判定します。 また、IPA は、影響度が小さい等の理由により、判定を実施せず取扱いを終了する調整不能案件について、付録5に従い、公表判定委員会への報告等の対応を行います。

(b)付録の規定

現行規定	改定案
付録5 ソフトウエア製品における連絡不能案件の取扱いについて [新設]	付録5 ソフトウエア製品における連絡不能案件の取扱いについて 3 判定対象としない連絡不能案件の取扱いについて 影響度が小さい等の理由から、公表判定委員会での判定を経ずに取扱いを終了する連絡不能案件（連絡不能案件であって、製品開発者に脆弱性情報を通知できていないものを含む）について、IPA は公表判定委員会に対し、その案件の概要と取扱方針を報告します。 公表判定委員会での判定を経ずに取扱いを終了する連絡不能案件は以下の表に従い IPA が判断します。公表判定委員会への報告後、IPA は JPCERT/CC および発見者に、取扱いを終了する旨を連絡し、その取扱いを終了します。 また、優先対応かつ検証不可の案件については、公表判定委員会に対し、検証コストを踏まえた判定要否について検討を依頼します。公表判定委員会は、判定対象とするかどうかについ

<table>
<tr>
<td></td>
<td>て検討を行い、その結果を IPA に連絡します。IPA はその結果に従い、対応を行います。

<table>
<tr><th>影響度の考え方*1</th><th>脆弱性検証*2</th><th>取扱方針</th></tr>
<tr><td rowspan="2">優先対応</td><td>検証可</td><td>公表判定委員会で判定</td></tr>
<tr><td>検証不可</td><td>検証に掛かるコストを考慮し適宜公表判定委員会で判定</td></tr>
<tr><td rowspan="2">通常の対応</td><td>検証可</td><td>公表判定委員会で判定</td></tr>
<tr><td>検証不可</td><td>取扱終了（連絡不能開発者一覧から削除）</td></tr>
<tr><td rowspan="2">簡易な対応</td><td>検証可</td><td>取扱終了（連絡不能開発者一覧から削除）</td></tr>
<tr><td>検証不可</td><td>取扱終了（連絡不能開発者一覧から削除）</td></tr>
</table>

*1 影響度の考え方は付録4に従って判断します。
*2 通常対応および簡易対応の案件に関する脆弱性検証の可否は、対象となるソフトウエア製品の入手への費用の要否、IPA における検証環境の用意の可否、届出における検証コードの記載の有無といった、当該案件について脆弱性の再現性を明らかにできる状況にあるか否かで判断します。</td>
</tr>
</table>

(4) その他、参照先情報の変更等の反映

(a)その他の修正事項

- IPA ウェブサイトリニューアルに伴う、各種コンテンツの URL の変更
- P ガイドラインで引用する内閣サイバーセキュリティセンターの資料「重要インフラのサイバーセキュリティに係る行動計画」（旧：重要インフラの情報セキュリティ対策に係る第4次行動計画）の名称変更の反映

5.2. 公表マニュアルの改訂

(1) 脆弱性の悪用を示す情報に関する情報の取扱い等に関する検討結果の反映

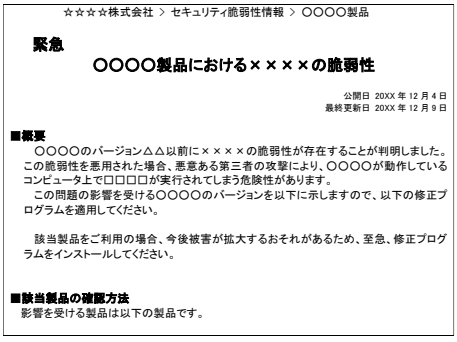
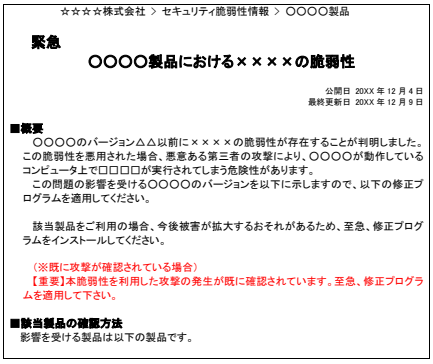
(a)「脆弱性対策について利用者が必要としている情報」の規定

現行規定	改定案
2. 脆弱性対策について利用者が必要としている情報	2. 脆弱性対策について利用者が必要としている情報

(5) 他に公表されている脆弱性関連情報 開発者が公表する脆弱性対策情報以外にも、深刻さや緊急性を測るための参考情報があるならば、利用者はそれもあわせて確認するものです。したがって、それらの情報を参考情報として示すことが求められます。	(5) 他に公表されている脆弱性に関する参考情報 開発者が公表する脆弱性対策情報以外にも、深刻さや緊急性を測るための参考情報があるならば、利用者はそれもあわせて確認するものです。したがって、それらの情報を参考情報として示すことが求められます。深刻さや緊急性を測るための情報としては、既にその脆弱性が悪用されている可能性があることを示す情報などが含まれます。

(b)「脆弱性対策情報の公表項目と公表例」の規定

現行規定	改定案
3. 脆弱性対策情報の公表項目と公表例 3.1. 脆弱性対策情報の公表項目 3.1.2. 概要 利用者が脆弱性の要点を迅速に把握できるように、内容を簡潔にまとめた概要を冒頭に示します。 特に、緊急の対応が必要な場合には、その旨を記載することを推奨します。 （例）「本脆弱性については、今後被害が拡大する可能性があるため、至急、修正プログラムを適用して下さい。」	3. 脆弱性対策情報の公表項目と公表例 3.1. 脆弱性対策情報の公表項目 3.1.2. 概要 利用者が脆弱性の要点を迅速に把握できるように、内容を簡潔にまとめた概要を冒頭に示します。 特に、緊急の対応が必要な場合や、攻撃の発生が確認されている場合には、その旨を記載することを推奨します。 （例）「本脆弱性については、今後被害が拡大する可能性があるため、至急、修正プログラムを適用して下さい。」 （例）「本脆弱性を利用した攻撃の発生が既に確認されています。至急、修正プログラムを適用して下さい。」

現行規定	改定案
3. 脆弱性対策情報の公表項目と公表例 3.2. 脆弱性対策情報の公表例 ・望ましい公表の例 	3. 脆弱性対策情報の公表項目と公表例 3.2. 脆弱性対策情報の公表例 ・望ましい公表の例 

6.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)製品開発者と調整する過程における３つの課題に関する調査

「脆弱性の悪用を示す情報に関する情報の取扱い等に関する課題」と「「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」については、改訂後のＰガイドラインに従った運用がなされることが重要である。その運用のなかで新たな課題が確認された際には改めて検討することが求められる。

一方、「製品開発者の脆弱性への対応目途（45 日）に関する課題」については、JPCERT/CC においてベストプラクティスの作成が行われたが、来年度（2024 年度）はトライアルとブラッシュアップ、そしてパートナーシップへの位置づけの検討を行うこととなる。今後、この取組みと検討を更に進める必要がある。

(2)優先情報提供の内容拡充等に関する調査

ISAC 等組織については、新たな提供先候補を優先順位を付けて整理をしたので、今後は具体的な調整が望まれる。

一方、より早い段階での情報の提供や優先情報提供する情報の内容の拡大については、現在の優先情報提供の改善という観点でより総合的に検討していく必要があると思われる。

(3)パートナーシップの運用改善事項等の調査及びＰガイドラインへの反映

改訂後のＰガイドラインに従い、連絡不能案件の公表判定委員会への報告等の対応がなされることで、公表判定委員会のより有効な運用につながることが期待される。

参考１

2023 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

2024 年 2 月 9 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
	佳山 こうせつ	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（キヤノンＩＴソリューションズ）
	栗田 博司	株式会社日立製作所
	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

武尾 伸隆	経済産業省 サイバーセキュリティ課長
吉川 弘晃	経済産業省 サイバーセキュリティ課 課長補佐
梶本 裕城	経済産業省 サイバーセキュリティ課
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）
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）
木村 浩樹	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

齊藤 裕	独立行政法人情報処理推進機構 理事長
小見山 康二	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
菅野 和弥	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
大久保 直人	独立行政法人情報処理推進機構
山下 恵一	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
津國 剛	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
田中 則通	株式会社三菱総合研究所
須賀 隆裕	株式会社三菱総合研究所
山中 翔太	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（2023 年 12 月 4 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
・製品開発者と調整する過程における３つの課題に関する調査について
・優先情報提供の内容拡充等に関する調査について
・パートナーシップの運用改善事項等の調査及び P ガイドラインへの反映について

■研究会第 2 回会合（2024 年 1 月 12 日）
・前回会合の確認
・製品開発者と調整する過程における３つの課題に関する調査について
・優先情報提供の内容拡充等に関する調査について
・パートナーシップの運用改善事項等の調査及び P ガイドラインへの反映について

■研究会第 3 回会合（2024 年 2 月 9 日）
・前回会合の確認
・製品開発者と調整する過程における３つの課題に関する調査について
・優先情報提供の内容拡充等に関する調査について
・パートナーシップの運用改善事項等の調査及び P ガイドラインへの反映について
・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