情報システム等の脆弱性情報の取扱いに関する研究会

－ 2018 年度　報告書 －

2019 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 2018 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 14,092 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）が新たに制定された。

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

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

2019 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期待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。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 2018 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 4,226 件、ウェブサイトの脆弱性に関するもの 9,866 件の計 14,092 件であった。四半期毎の届出状況を図 1-1 に示す。

	2016 1Q	2Q	3Q	4Q	2017 1Q	2Q	3Q	4Q	2018 1Q	2Q	3Q	4Q
累計届出件数[件]	11,692	12,444	12,677	12,922	13,064	13,335	13,456	13,526	13,664	13,822	13,999	14,092
1就業日あたり[件/日]	4.09	4.26	4.25	4.25	4.21	4.21	4.17	4.11	4.08	4.06	4.03	3.99

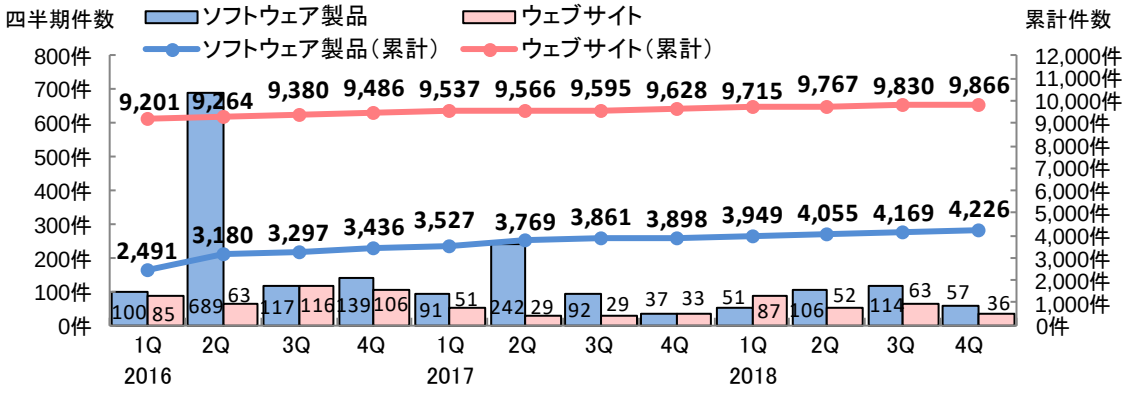


図 1-1　脆弱性関連情報の届出の処理状況

（活動報告レポート[2018 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。

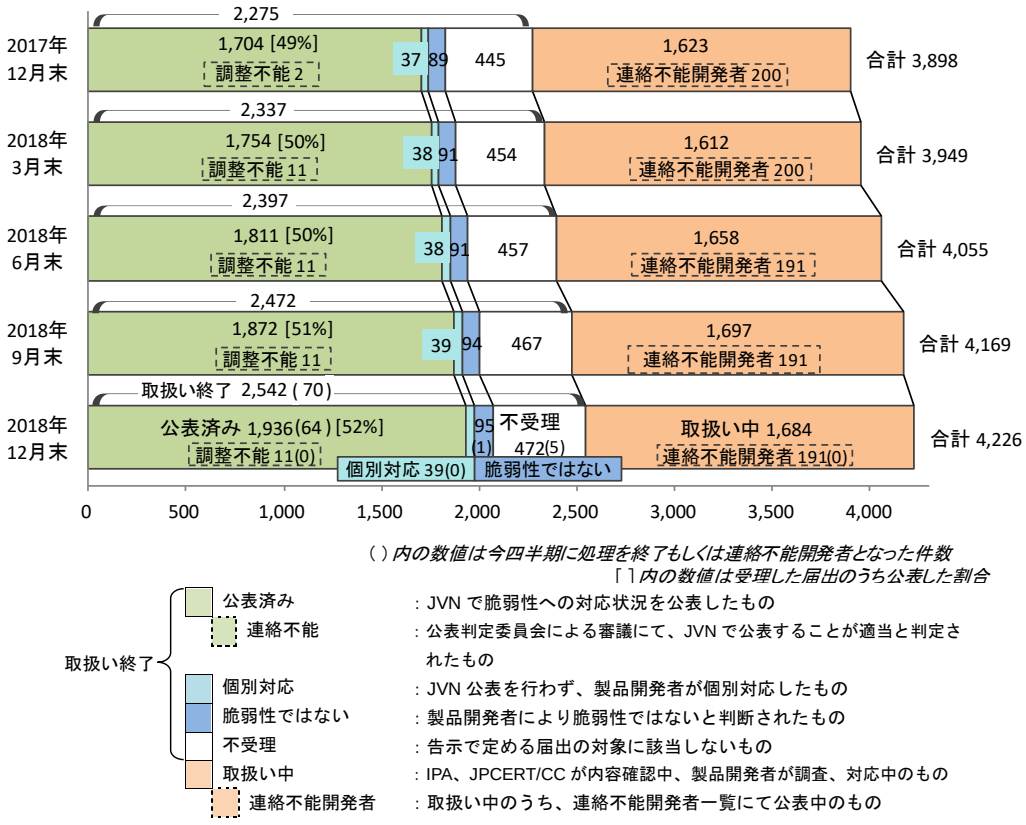


図 1-2　ソフトウエア製品の脆弱性関連情報の届出の処理状況

（活動報告レポート[2018 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 4,226 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 1,936 件（うち公表判定委員会による審議の結果公表されたものが 11 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 95 件、取扱い中のものが 1,684 件（うち連絡不能開発者として公表したものが 202 件）となっている。また、告示で定める要件に合致しないため届出の対象外としたものが 472 件、JVN 公表を行わず製品開発者が個別対応したものが 39 件ある。

(2) ウェブサイトの脆弱性

ウェブサイトの脆弱性関連情報の届出に関する処理状況を図 1-3 に示す。

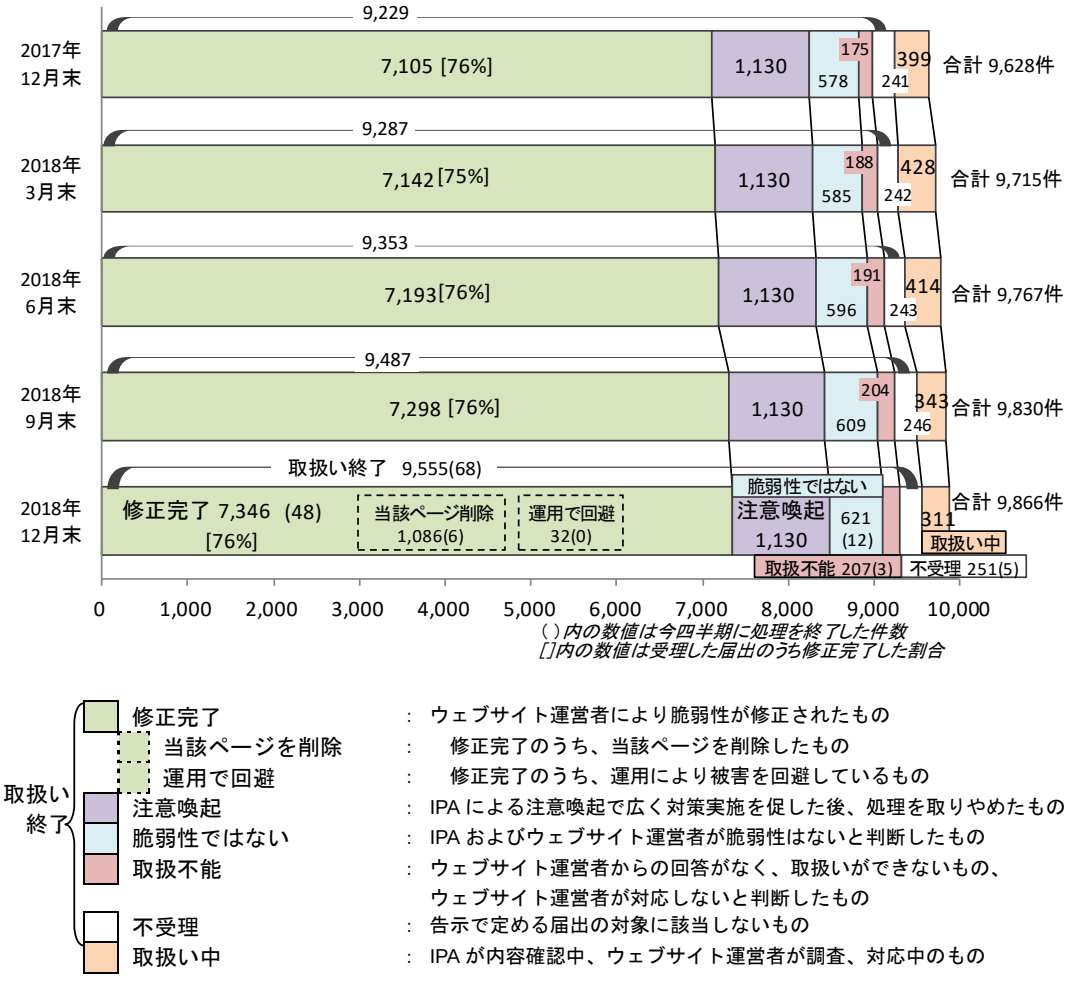


図 1-3　ウェブサイトの脆弱性関連情報の届出の処理状況

（活動報告レポート[2018 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 9,866 件のうち、修正が完了したものが 7,346 件（うち運用で回避されたもの 32 件、当該ページを削除して対応したもの 1,086 件）、IPA による注意喚起で広く対策を促すことにより取扱いを終了したもの 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 621 件、取扱い中のものが 311 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など調整が滞ったものが 207 件、告示で定める要件に合致しないため届出の対象外としたものが 251 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 2018 年 12 月末までに 3,323 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

2018 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 1,936 件である。届出受付開始から 2018 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%(552 件)であり、301 日以上要しているものは 26%(497 件)を占める。

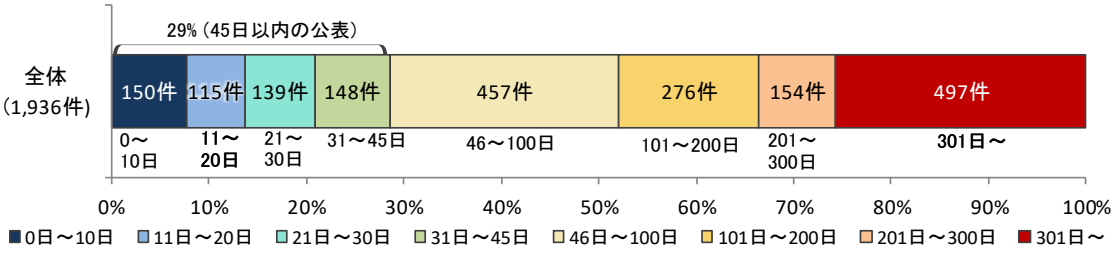


図 1-4 ソフトウエア製品の脆弱性公表までに要した日数

（活動報告レポート[2018 年第 4 四半期（10 月～12 月）]より抜粋）

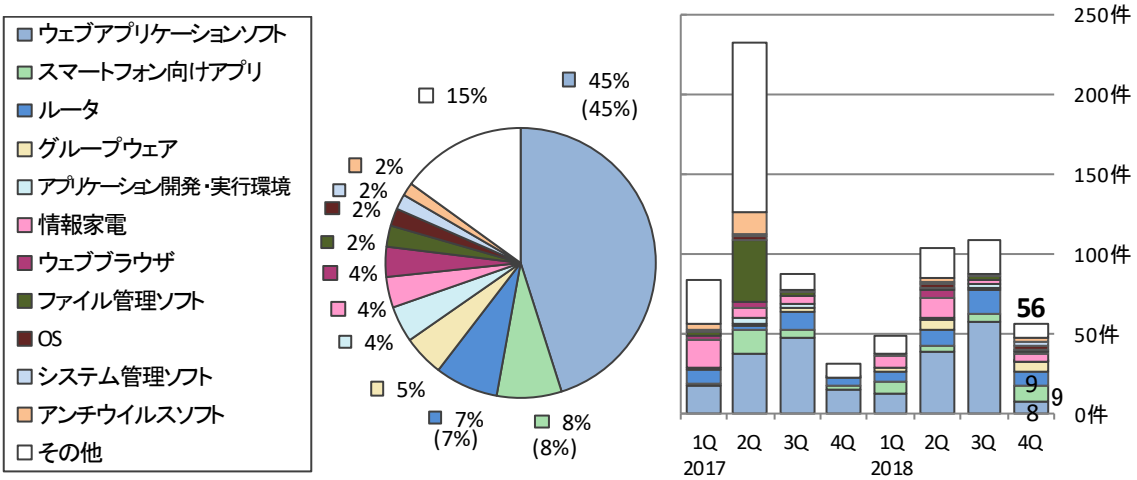
(2) 海外 CSIRT 等から連絡を受け公表した脆弱性

2018 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 1,649 件である。このうち、2018 年第 1 四半期～2018 年第 4 四半期（2018 年 1 月から 2018 年 12 月末まで）に JVN で公表した脆弱性関連情報は 71 件あった。

[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 2018 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 4,226 件のうち、不受理分を除いた 3,754 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 45%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。
（3,754件の内訳、グラフの括弧内は前四半期までの数字）

（過去2年間の届出内訳）

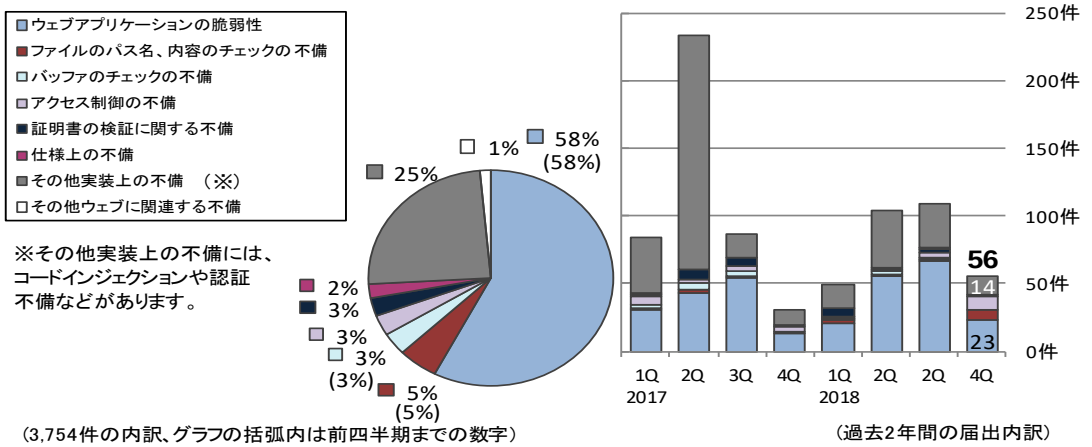
届出累計の製品種類別割合　　**四半期ごとの製品種類別届出件数**

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～2018 年 12 月末）

（活動報告レポート[2018 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 2018 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 4,226 件のうち、不受理分を除いた 3,754 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 58%を占める。



（3,754件の内訳、グラフの括弧内は前四半期までの数字）

（過去2年間の届出内訳）

届出累計の脆弱性の原因別割合　　**．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～2018 年 12 月末）

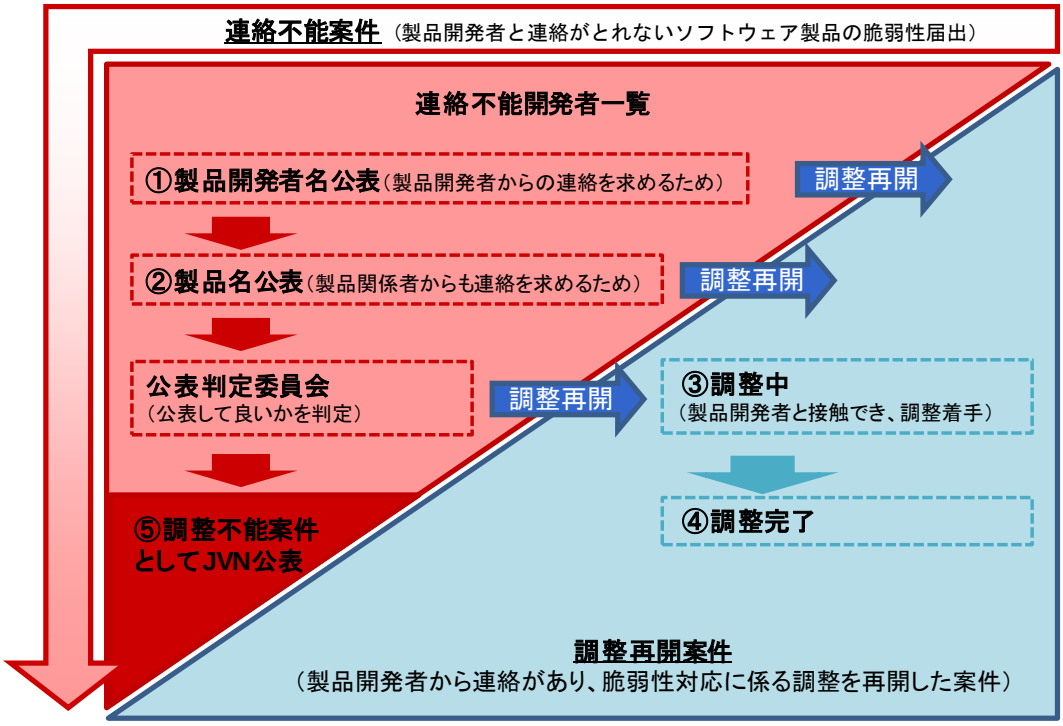
（活動報告レポート[2018 年第 4 四半期（10 月～12 月）]より抜粋）

(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。2018 年 12 月末までに、優先情報提供したものは電力分野 2 件、政府機関 1 件である。

(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 2018 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 49 件が調整を再開（その中の 26 件が調整完了）したが、191 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）。



2018年 第3四半期	191件 （①1件 ②190件）	49件 （③23件 ④26件）	⑤11件	合計 251件
2018年 第4四半期	191件 （①1件 ②190件）	49件 （③23件 ④26件）	⑤11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～2018 年 12 月末）

（活動報告レポート[2018 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

2018 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 7,346 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 47%の届出が 30 日以内、66%の届出が 90 日以内に修正されている。

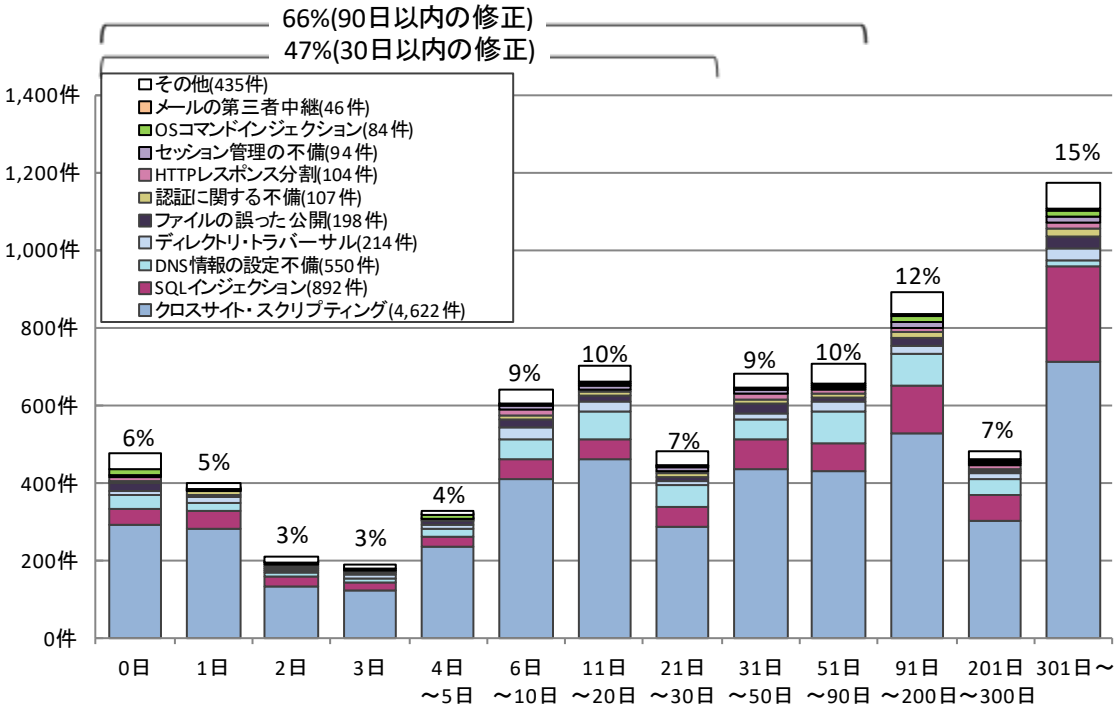


図 1-8　ウェブサイトの脆弱性修正に要した日数（届出受付開始～2018 年 12 月末）

（活動報告レポート[2018 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

2018 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 9,866 件のうち、不受理のものを除いた 9,615 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」(55%)、「DNS 情報の設定不備」(14%)、「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 80%を占める。

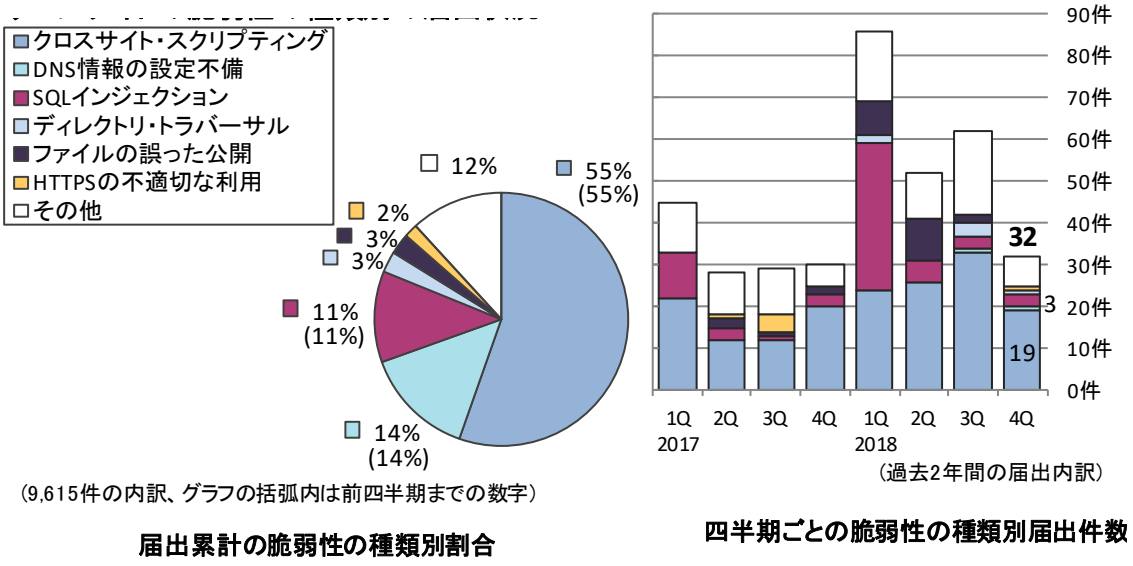


図 1-9　ウェブサイトの脆弱性種類別内訳（届出受付開始～2018 年 12 月末）

（活動報告レポート[2018 年第 4 四半期（10 月～12 月）]より抜粋）

(3) 届出の脆弱性影響別内訳

届出のあった脆弱性から想定される影響別内訳を図 1-10 に示す。脆弱性から想定される影響としては、「本物サイト上への偽情報の表示」(54%)、「ドメイン情報の挿入」（14%)、「データの改ざん、消去」（12%）の割合が高い。

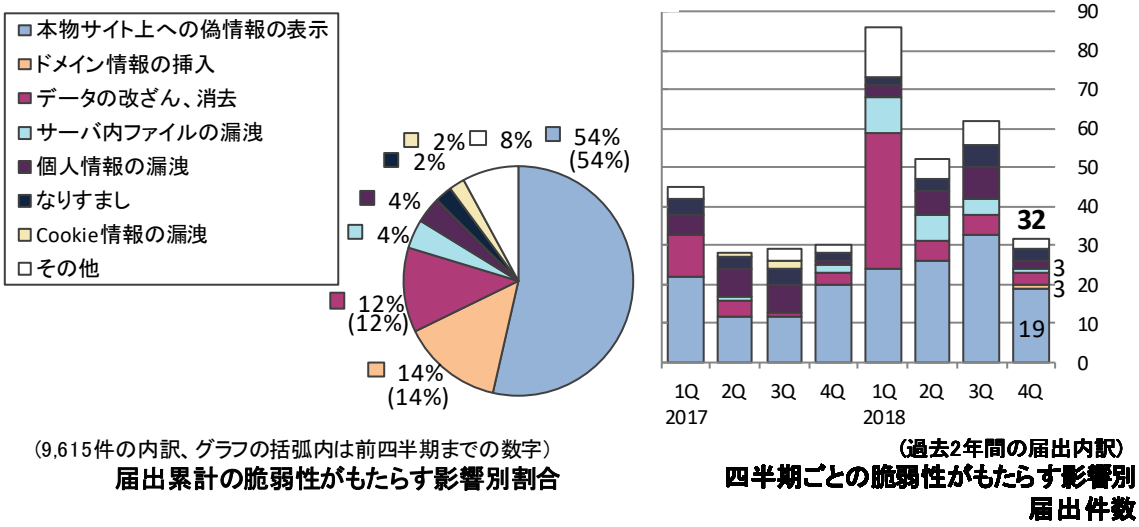


図 1-10　ウェブサイトの脆弱性影響別内訳（届出受付開始～2018 年 12 月末）

（活動報告レポート[2018 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 265 件で、前年同期（259 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 23%を占めており、対策の実施が望まれる。

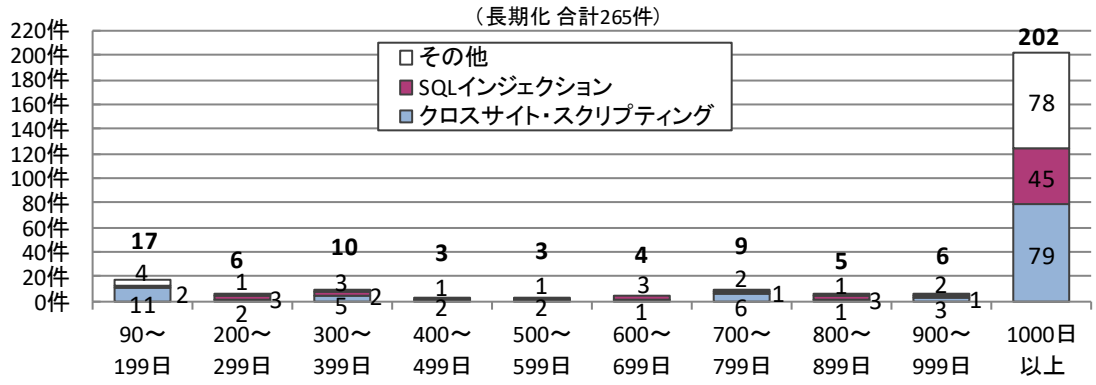


図 1-11　取扱いが長期化（90 日以上経過）しているウェブサイトの経過日数と脆弱性の種類

（活動報告レポート[2018 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

前年度調査結果[3]を踏まえ、本年度の脆弱性研究会は以下の 5 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 ソフトウエア製品の脆弱性対処における実態調査および脆弱性対処の促進に関する調査
② 「優先情報提供」の実績評価、提供先拡大に関する調査
③ 調整不能案件の一覧への掲載、公表手続きの改善に向けた検討
④ 法的課題の整理
⑤ パートナーシップガイドラインの改訂等に関する調査

[3] 「情報システム等の脆弱性情報の取扱いに関する研究会」2017 年度報告書

2. ソフトウエア製品の脆弱性対処における実態調査および脆弱性対処の促進に関する調査

2.1. 調査の概要

2.1.1. 調査目的

ソフトウエア製品の脆弱性への対処・公表について、「製品開発者」としての責務（望むべき対処）であることが十分に認識されていない状況である。

また、脆弱性対処に積極的に取組む「製品開発者」が社会的に評価される位置づけを確立することによって脆弱性対処が促進される可能性がある。

そこで、「製品開発者」における脆弱性対処の実態について文献・ヒアリング調査等を実施し、脆弱性対処の促進に関するパートナーシップでの対応方策について検討する。

さらに、IPA で公表した普及・啓発資料の活用状況の調査および活用促進のための方策等を検討する。

2.1.2. 調査方法

「製品開発者」による脆弱性対処に関する課題(脆弱性対処が進まない、脆弱性情報が公表されない)について、文献(過去の研究会報告書等)調査を実施し、仮説を作成する。また、過去に IPA が公表したソフトウエア製品に対する脆弱性対処に関する普及・啓発資料の活用状況および活用を促進するための方策を検討する。

上記の仮説・施策案に基づき、製品開発者による脆弱性対処に関する実態を把握するため、中小規模のソフトウエア製品開発者（7 社）とシステム構築事業者（3 社）に対するヒアリング調査を実施し、調査結果を基に、対応方法をとりまとめた。本調査の調査方法は以下に示す。

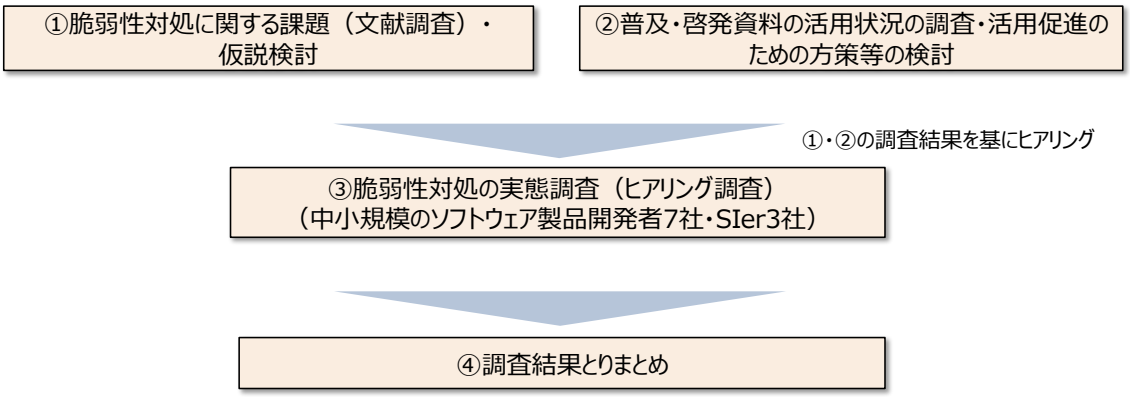


図 2-1　調査方法

2.1.3. 調査仮説

過去の研究会報告書等の文献を調査した結果、ソフトウエア製品開発者の脆弱性への対処・公表状況について、過去の脆弱性研究会でのヒアリング調査等で以下に示す課題点等が明らかになった。

表 2-1　脆弱性対策に関する事業者からの意見

対象者	主な意見
ソフトウエア製品開発者	・ 脆弱性を公表したのはよいが、**公開内容がユーザにきちんと到達し対応していただいているのかわからないことが課題**と考えている。 ・ **脆弱性を公表することにより失注するケース**もある。積極的に脆弱性対応を実施しているという理由で、自社製品の受注につながるという話はこれまでない。 ・ **脆弱性対策の重要性は理解されているが、コストとのバランスが問題**。
システム構築事業者	・ **JVN 上で脆弱性の詳細情報を開示してほしい**。JVN の内容だけでは詳細が把握できず、脆弱性の修正が難しい。 ・ **製品サポートが終了している製品に脆弱性が発見された場合、ソフトウエア製品開発者に対応してもらえない**。 ・ ソフトウエア製品開発者が、**脆弱性の修正をバグの修正として公開**することがあり、**システム構築事業者が修正情報を見落とす**ことがある。

文献調査等の結果から以下の仮説を設定し、整理した。

表 2-2　仮説整理

分類	No.	仮説
脆弱性対処の実態、公表を妨げる要因・課題	1	自社製品の脆弱性に対処する人員・予算・対応方針等社内体制が整備されていないのではないか。
	2	風評被害や売上高への影響、コストをかけて脆弱性対処を実施しても評価されないため、脆弱性を対処・公表していないのではないか。
	3	自社製品の脆弱性を受け付ける窓口が設置されていないのではないか。
	4	サポート終了製品の脆弱性対応方針の検討ができていないのではないか。
	5	他社製品・OSS 等を組込んでおり、脆弱性対処が自社のみで完結せず、対処を妨げているのではないか。
	6	脆弱性が発見された製品について、ソフトウエア製品開発者が提供する情報が不十分なため SIer が十分対処できていないのではないか。
脆弱性対処の必要性の周知・促進策	7	脆弱性対処が製品開発者の責務であることを理解していないのではないか。
	8	製品利用者にパッチ適用等の脆弱性対策の必要性を周知できていないのではないか。
普及・啓発資料	9	IPA の普及・啓発資料を認知していないのではないか。
	10	普及・啓発資料ではまだ取り上げていないテーマや内容（具体的方法論・事例等）等のニーズがあるのではないか。
	11	現在の普及啓発資料で記載されている内容は、リソースが不十分な中小の開発者にとって実施が難しいのではないか。

上記の仮説に基づき、ヒアリング調査では以下の内容等について確認し、ヒアリング結果を基にパートナーシップの対応方策等を検討した。

表 2-3　ヒアリング調査項目

	ソフトウエア製品開発者	システム構築事業者
脆弱性対処の実態、公表を妨げる要因・課題	・脆弱性対処に関する社内組織・方針 ・自社製品の脆弱性公表に対する考え方 ・脆弱性対処経験 ・脆弱性対処に関する具体的取組（例:自動アップデートの導入、ユーザのパッチ適用状況の把握）　等	・脆弱性情報が公開された場合の対処・課題について（対製品開発者・対顧客） ・脆弱性情報が公開されない（脆弱性に対応されない）ソフトウエアへの対応について ・ソフトウエア製品開発者に対する脆弱性情報の公開に関する要望（公表内容、方法、タイミング等）　等
脆弱性対処の必要性の周知・促進策	・特にリリース後の運用段階における脆弱性対処について以下の内容等を確認 ✧ 脆弱性対処の必要性に対する理解 ✧ 利用者に脆弱性対処の必要性理解、パッチ適用等を実施してもらうための周知方法　等	―
普及・啓発資料	・ IPA の脆弱性関連の普及啓発資料の認知・活用状況 ・ 普及・啓発資料をより活用してもらうための周知方法 ・ 普及・啓発資料に求めるテーマ・内容　等	
その他	・ 情報セキュリティ早期警戒パートナーシップに対する要望　等	

2.2.　調査結果

2.2.1. ヒアリング調査結果

ヒアリング調査の結果を以下に示す。

(1) ソフトウエア製品開発者へのヒアリング結果

ソフトウエア製品開発者に対するヒアリング結果から、各分類において以下の意見が得られた。得られた意見のうち、課題や施策案について強調している。

	主な意見
脆弱性対処の実態、公表を妨げる要因・課題	・ 脆弱性対処に関する文書化した方針はあまりないが、脆弱性に対して早めに対応しなければならない意識は持っている。 ・ 脆弱性対応は親会社のセキュリティに関する規定に従い、行っている。 ・ 脆弱性に関する一般公表については、 ✧ 脆弱性に関する情報を隠した場合はかえって悪いイメージにつながる可能性がある。 ✧ 脆弱性の情報を公表するという考え方より、脆弱性を修正したパッチを掲載する形となっている。ただし、脆弱性の中に特別な手法やタイミングに合わせて実行しなければ実現できない脆弱性もあるため、**一律に対処・公開することが難しい**。 ✧ **B2B 商品に関する脆弱性情報の公表は顧客企業にも迷惑（例：問い合わせが増える、製品に対する信頼度が下がる）をかける可能性があるため、慎重に考える必要がある**。 ✧ **脆弱性情報の公開は、競合他社に自社製品の評価を下げる情報として使われるおそれ**がある。 ✧ **顧客の多くは IT リテラシーが高くないため**、他の問い合わせにつながる可能性を懸念し、**脆弱性という言葉を使うことには慎重**である。 ・ 脆弱性に対応するために脆弱性検証に苦労した。 ✧ 特に自社製品に組み込まれた**オープンソースに脆弱性が発見されたときの対応が難しい**。 ・ 自動アップデートの導入やユーザ側のアップデート適用状態の把握を実施している。 〈取組例〉 ✧ クラウドサービスを通じて全ての端末まで管理・バージョンアップできる仕組みを提供している。 ✧ システムを運用するための保守契約で顧客の状況を把握でき、脆弱性対応に関する情報は顧客に直接的に連絡している。 ✧ 重大な脆弱性に対し、バージョンアップしないと特定の機能を追加できないという制御をかけたことがある。 ・ 脆弱性の重大性によっては EoL 後であっても対応するパッチ作成等のサポートも検討する。 ✧ 利便性を大きく損なう場合や情報漏えいに関する脆弱性などは対象となりうる。

	主な意見
脆弱性対処の必要性の周知・促進策	・ 脆弱性に対応する必要性については理解している。 〈取組例〉 ✧ 周囲からの理解をえるため、経営層は関連会社や株主等への説明責任を果たした。 ✧ ツールを利用し、JVN 等の情報を週に 1 回ペースで収集している。 ・ 脆弱性に対応した単独のパッチより、バージョンアップ等の大型リリースと一緒に案内する。 〈取組例〉 ✧ Linux をベースにした製品の脆弱性対応は、年に 2 回のジェネラルリリースに乗せるよう努める。 ・ **エンドユーザは脆弱性対応をそこまで重視していないことが課題**だと感じる。 〈具体例〉 ✧ **上位機種は CC 認証を取っているが、日本の消費者に響かない**。米国の消費者なら気にする。 ✧ 10 年、20 年前のソフトウエアでも強制的にバージョンアップできる風土があればよい。 ・ パートナーシップの対応において、各段階の期間および対応内容など**一般的なスケジュールを見える化してほしい**。
普及・啓発資料	・ 社内に対する説明を作成する際に、「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」を参考にした。 ・ 営業や経理の背景しか持ってない人でもわかる**事例ベースの説明等を記載している啓発資料を期待**する。 ・ 消費者に**脆弱性を対応していることを信頼できる企業の条件として認識させるような啓発資料を期待**する。 ・ 脆弱性に関する情報は**重大性や優先度に応じてレベル分けして公表してほしい**。また、**レベル分けの基準等の啓発資料を期待**する。 ・ **窓口の担当者向けのセキュリティ情報提供の講演・セミナー**がほしい。製品開発者との交流の場にもなる。 ・ IT リテラシーの低い使用者を考慮し、**クラウドで運用するほうがセキュリティの向上につながることを理解できるような普及啓発資料を期待**する。

	主な意見
その他	〈脆弱性の公開情報〉 ・ オープンソースに脆弱性が発見される際、**オープンソースの脆弱性により影響を受ける製品の情報もあればよい**のではないか。エンドユーザも使いやすい。 〈製品開発者のモチベーションにつながる提案〉 ・ ビジネスにつながるならば、脆弱性を公開するモチベーションにもなり得る。例えば、**脆弱性公表が認証や資格になり、入札案件の必須条件にすれば、前向きに検討**できる。 〈特定情報の提供〉 ・ **実績のある会社や情報処理安全確保支援士等に限定して脆弱性の調査手法等を提供**できればよいのではないか。脆弱性を見つけるノウハウがわかれば、防ぐことも考えられる。

(2) システム構築事業者へのヒアリング結果

システム構築事業者に対するヒアリング結果から、各分類において以下の意見が得られた。得られた意見のうち、課題や施策案について強調している。

	主な意見
脆弱性対処の実態、公表を妨げる要因・課題	・ 他社製品の脆弱性についてはまず脆弱性の影響度合いを確認する。 〈取組例〉 ✧ 影響度が高い脆弱性である場合は修正される前でも顧客にその情報を伝え、注意喚起を行う。 ✧ 影響度が中あるいは低の場合は、ベンダと対応方法等を確認した上で顧客に伝える。 ✧ 修正した情報は製品サポートサイトでも公開する。 ✧ 脆弱性の影響がない場合でも顧客からの問い合わせに対応するため、サポートサイトで公開し、影響がないことを説明する。 ・ 顧客のほとんどは技術に詳しいわけではないため、脆弱性に関する情報は必要な部分（顧客にとってわかりやすい部分）だけ案内する。 ・ 顧客からの問い合わせに対応するため、**脆弱性情報が一般公開される前に、サービスを提供する側に先に知らせてほしい**。 ・ CSIRT が大手のベンダが発表している情報や IPA の情報等を能動的に収集し、グループ会社全体で情報を共有しているケースもあるが、脆弱性情報を社内で一か所に集約する部署はなく、各部署で管理・対応しているケースもある。 ・ OSS の選定について明確なルールまではないが、メジャーであるかどうかやバージョンの更新頻度などを総合的に判断する。 ・ **脆弱性の対応策がない・わからない段階での脆弱性情報の公表を問題視**している。例えば、直ちにシステムを止めないといけない場合は、対応方法がまだわからなくても危険回避のためにアナウンスしたほうがよいが、そうではない場合との運用を分ける必要がある。

	主な意見
普及・啓発資料	・ JVN や製品開発者から公表される脆弱性情報には、**具体的な脆弱性再現方法が記載されておらず、調べるのに時間がかかる**。 ・ 脆弱性情報に、危険度や攻撃の有無などの情報が含まれていると重要性が判断しやすい。 ・ セキュリティ部門を整備した**中小企業の顧客は少ないので、中小企業または中小企業向けの製品を製造・販売する会社向けの啓発資料**も必要ではないか。 ・ **サイバー情報共有イニシアティブ（J-CSIP）の一般向け版といったイメージの仕組みを期待**する。 ・ 読者のレベル（IT リテラシーの高さ、技術の詳しさなど）に応じて多様な啓発資料を期待する。例：開発者レベルの資料 ・ 脆弱性対策に関して、最終的に**脆弱性による損害が発生した場合を想定した契約事項などのサンプルの提供を期待**する。
その他	・ IPA 等の公的機関から重大な脆弱性についてパッチの適用を求められるのは理解できるが、**脆弱性の影響があまりない場合にも脆弱性に対応するべきであると IPA 等の啓発資料で強調されると困る**。 ・ 保守を顧客が実施している場合、顧客からは脆弱性情報から自社が該当するかどうかを判断しにくいと聞いたことがある。顧客は自社で判断ができないため、脆弱性診断サービスの利用も検討していた。このため、**顧客が自社は該当するかどうかを把握できる方法の提供を期待する。**

(3) ヒアリングの結果に基づく仮説の検証

ソフトウエア製品開発者及びシステム構築事業者へのヒアリング結果に基づき、「2.1.3 調査仮説」を検証した結果は以下となる。

ヒアリング結果の実態（課題）に対する改善策として検討した施策の分類を「施策案[4]」に記載し、詳細は「2.2.2 今後の施策」に示す。

[4] 施策案は（A）奨励制度等の検討、（B）普及啓発の実施、（C）普及啓発資料の周知手段の検討、（D）脆弱性に関する公開情報の内容の検討、（E）パートナーシップ制度の検討と 5 つに分け、詳細は「2.2.2 今後の施策」に記載・検討する。

脆弱性対処の実態、公表を妨げる要因・課題	1	仮説	自社製品の脆弱性に対処する人員・予算・対応方針等社内体制が整備されていないのではないか。
		ヒアリング結果	・ 明確なマニュアル等の体制整備は行われていない。[複数社意見] ・ 体制・予算などを強化するため、**経営層または社内の他部署からの理解も必要**である。
		施策案	（A）奨励制度等の検討 （B）普及啓発の実施
	2	仮説	風評被害や売上高への影響、コストをかけて脆弱性対処を実施しても評価されないため、脆弱性を対処・公表していないのではないか。
		ヒアリング結果	・ **ライバル企業のネガティブキャンペーンを懸念**し、積極的に公開したくない企業もいる。[複数社意見] ・ ただし、**脆弱性を公表することを前向きに捉えている**企業もいる。 ・ **顧客からの問い合わせを懸念**して、脆弱性という表現を使うことに慎重である企業もいる。 ・ 【SIer】脆弱性の影響がない場合でもその情報を公開し、影響がないと説明する企業がいる。
		施策案	（A）奨励制度等の検討 （B）普及啓発の実施
	3	仮説	自社製品の脆弱性を受け付ける窓口が設置されていないのではないか。
		ヒアリング結果	・ 自社製品の**脆弱性を受け付ける窓口が設置されていない**。[複数社意見]
		施策案	（B）普及啓発の実施
	4	仮説	サポート終了製品の脆弱性対応方針の検討ができていないのではないか
		ヒアリング結果	・ 明示されたサポート終了製品の脆弱性対応方針は特になく、**都度経営判断で決める**など、**方針が定まっていない**。
		施策案	（D）脆弱性に関する公開情報の内容の検討

	5	仮説	他社製品・OSS 等を組込んでおり、脆弱性対処が自社のみで完結せず、対処を妨げているのではないか。
		ヒアリング結果	・ **他社製品の脆弱性情報が社内にないため対応に苦労した**。[複数社意見]
		施策案	(D) 脆弱性に関する公開情報の内容の検討 (E) パートナーシップ制度の運用方法の検討
	6	仮説	脆弱性が発見された製品について、ソフトウエア製品開発者が提供する情報が不十分なため SIer が十分対処できていないのではないか。
		ヒアリング結果	・ 対処できていないわけではないが、脆弱性に対応した際、**脆弱性に関する詳細の情報が十分に開示されていないことで苦労した**。[複数社意見] ・ 【SIer】脆弱性の再現方法やその危険度、攻撃の有無などについての情報がほしい。[複数社意見]
		施策案	(D) 脆弱性に関する公開情報の内容の検討 (E) パートナーシップ制度の運用方法の検討
脆弱性対処の必要性の周知・促進策	7	仮説	脆弱性対処が製品開発者の責務であることを理解していないのではないか。
		ヒアリング結果	・ 会社として経営層も含めて概ね必要性を認識されていた。
		施策案	―（仮説は棄却）
	8	仮説	製品利用者にパッチ適用等の脆弱性対策の必要性を周知できていないのではないか。
		ヒアリング結果	・ 企業向けのソフトウエア製品については顧客側の管理者を通じて利用者に周知している。 ・ **エンドユーザは脆弱性対応をそこまで重視していない**。
		施策案	(B) 普及啓発の実施
普及・啓発資料	9	仮説	IPA の普及・啓発資料を認知していないのではないか。
		ヒアリング結果	・ IPA の普及・啓発資料を活用していた企業もいるが、**普及・啓発資料の存在を認知していない企業もいる**。
		施策案	(C) 普及啓発資料の周知手段の検討
	10	仮説	普及・啓発資料ではまだ取り上げていないテーマや内容（具体的方法論・事例等）等のニーズがあるのではないか。

		ヒアリング結果	・ **社内向けの説明資料**（例：脆弱性対応の重要性または脆弱性対応に必要な体制・予算に関する、営業や経理の背景しかもっていない人でもわかりやすい事例ベースの資料）が期待される。 ・ **消費者向けの啓発資料**（例：脆弱性が発見されることを悪いイメージにつなげないような）が期待される。 ・ 【SIer】サイバー情報共有イニシアティブ（J-CSIP）の一般向け版などがあるとよいのではないか。 ・ 【SIer】読者のレベル（IT リテラシーの高さ、技術の詳しさなど）に応じて多様な啓発資料を期待する。 ・ 【SIer】脆弱性対応に関する契約事項などのサンプルの提供を期待する。
		施策案	（B）普及啓発の実施
	11	仮説	現在の普及啓発資料で記載されている内容は、リソースが不十分な中小の製品開発者にとって実施が難しいのではないか。
		ヒアリング結果	・ 普及啓発資料の内容を詳しく把握している企業は少ない。 ・ 組織力の差に応じた啓発資料を期待する。[複数社意見、SIer] ・ **ビジネスモデル（例：B2B やクラウドサービス等）に応じた製品開発者の脆弱性対応方法を考慮した啓発資料**も期待する。
		施策案	（B）普及啓発の実施 （C）普及啓発資料の周知手段の検討 （E）パートナーシップ制度の運用方法の検討

2.2.2. 今後の施策

ソフトウエア製品開発者及びシステム構築事業者へのヒアリング結果から得られた「情報セキュリティ早期警戒パートナーシップ制度」にかかわる改善の施策として盛り込むべき主な意見や要望[5]の内容を抽出し、分類ごとに整理を行い、各施策の有効性評価、IPA での実現可能性については検討した。

（A）奨励制度等の検討

No.	施策例	対象	今後の対応方針
A-1	表彰制度または認証制度により、脆弱性に積極的に対応・公開する企業を評価	製品開発者	表彰／認証は優良ベンダを評価する施策であり、本検討は対策が進まないベンダへの対策のため議論の対象外とするため実施しない
A-2	入札案件の必須条件とし、脆弱性に対応しない／しなかった企業を除外	製品開発者	IPA として実施する施策ではないため実施しない

（B）普及啓発の実施

No.	施策例	対象	今後の対応方針
B-1	専門知識がない部署でも脆弱性対応の重要性等について理解できる説明資料	製品開発者	来年度以降の施策案「（2）製品開発者として必要な対応をまとめた普及啓発資料を作成」に盛り込む
B-2	脆弱性について正しく理解できるような消費者への脆弱性についての解説	製品開発者 SIer	来年度以降の施策案「（3）製品利用者が脆弱性対処を実施している製品／ベンダを評価／選定するためのガイド／チェックシートを作成」に盛り込む
B-3	脆弱性対応に関する契約事項サンプルの提供	SIer	契約項目等については、既存資料があるため、既存資料の普及を検討する
B-4	組織力／技術力等のレベルに応じた啓発資料の作成	製品開発者	新規資料を作成する際に、対象読者として企業規模や技術力等

[5] すでに普及啓発済み／施策実施済みのものを除いて掲載する。

No.	施策例	対象	今後の対応方針
		SIer	についても言及することを検討する
B-5	ビジネスモデル（例：B2B やクラウドサービス等）に応じた、脆弱性対応方法の啓発資料等の作成	製品開発者	来年度以降の施策案「（2）製品開発者として必要な対応をまとめた普及啓発資料を作成」に盛り込む 注）制度としてはすでにルール(全顧客を把握している場合の対応等)がある

（C）普及啓発資料の周知手段の検討

No.	施策例	対象	今後の対応方針
C-1	製品開発者の窓口担当者向けの講演・セミナー講演・セミナー等のイベント開催	製品開発者	SoftwareISAC 等、関連組織イベントでの啓発資料の普及に協力を要請することも検討する
C-2	サイバー情報共有イニシアティブ(J-CSIP)の一般向け版	SIer	一般企業向けのセキュリティ関連情報の発信を強化は、方法含め今後の検討課題とする

（D）脆弱性に関する公開情報の内容の検討

No.	施策例	対象	今後の対応方針
D-1	脆弱性悪用の回避策、脆弱性によって影響のある関連ソフトウエア等の情報	製品開発者	来年度以降の施策案「（1）脆弱性情報の提供については、「脆弱性対策情報公表マニュアル」を改訂」に盛り込む
D-2	サポート終了製品の脆弱性の公表方法	製品開発者	来年度以降の施策案「（1）脆弱性情報の提供については、「脆弱性対策情報公表マニュアル」を改訂」に盛り込む

（E）パートナーシップ制度の運用方法の検討

No.	施策例	対象	今後の対応方針
E-1	脆弱性公表後にシステム構築事業者に対して迅速に情報提供するための方策（事前登録制度等）の検討	製品開発者 SIer	まずは開発者の脆弱性対処の促進を優先し、SIer への情報提供に関しては、今後の検討課題とする

以上の結果を踏まえて来年度以降検討する施策案は以下に示す。

なお、施策案「(1)「脆弱性対策情報公表マニュアル」の改訂」は来年度中に実施する予定である。

表 2-4　来年度以降検討する施策案

施策案	**(1)「脆弱性対策情報公表マニュアル」の改訂**
内容	公表する情報に以下のような情報を追記する。 ・　SIer が必要としている攻撃シナリオ、深刻度／CVSS ・　システム管理者が必要としている修正した箇所／機能 ・　サポート終了製品の脆弱性の公表
施策案	**(2) 製品開発者として必要な対応をまとめた普及啓発資料の作成**
内容	・　2004 年 JEITA /JISA が公開した「製品開発ベンダーにおける脆弱性関連情報取扱に関する体制と手順整備のためのガイドライン」を基に適宜必要な情報を記載した資料を作成し公開する。 ・　内容としては、あるべき論だけでなく具体的な手法／サンプル／ベストプラクティス等を記載するものと想定する。 ・　成果物としては、既に公表している「ウェブサイト運営者のために脆弱性対応ガイド」や「セキュリティ担当者のための脆弱性対応ガイド」のような資料となることを想定している。 ・　下記（3）に対応して、製品利用者からの評価を受けるために製品開発者による公開が必要な情報等を記載する。 ・　ビジネスモデル（例：B2B やクラウドサービス等）に応じた脆弱性対応方法を記載する。
施策案	**(3) 製品利用者が脆弱性対処を実施している製品開発者を評価・選定するためのチェックシート等の作成**
内容	・　製品利用者だけでなく、製品開発者が組み込む部品／プログラムを選定する際に考慮することも含める。 ・　将来的には、一般消費者へのリーチ手段として量販店や販社等へ協力してもらうことも検討する。
施策案	**(4) システム構築事業者への情報提供の検討**
内容	・　システム構築事業者へ情報提供（脆弱性情報、対策情報等）する仕組みについて検討する。

3. 「優先情報提供」の実績評価、提供先拡大に関する調査

3.1. 調査の概要

3.1.1. 調査目的

パートナーシップが本格稼働してから 10 年以上が経過し、社会環境も変化したことから、2015 年度、パートナーシップに関する様々な問題点とその改善策の検討・提言等を行う脆弱性研究会において、今後求められるパートナーシップのあり方について検討を実施した。そして、その成果を「新たな情報セキュリティ早期警戒パートナーシップの基本構想」として取りまとめた。その基本構想にあるパートナーシップ将来像の実現に向けたロードマップに則り、「優先情報提供」を電力分野以外の他の重要インフラ分野に提供先を拡大するに際し、「優先情報提供」の有効性の評価および現状の課題を整理し、「優先情報提供」の有効性を高めるための方策についての検討を実施した。

また、新たな手続きとして「優先情報提供」を受けたい重要インフラ分野から申請書をもとに拡大する手段について検討を実施した。

3.1.2. 調査方法

本調査では、重要インフラ分野に提供先を拡大するに際し、既存の優先情報提供際である電力事業者及び政府機関を対象にアンケート調査を実施し、電力事業者を対象にヒアリング調査を実施した。その後、アンケート調査並びにヒアリング調査を踏まえて新たな手続き方法に関する検討を行った。

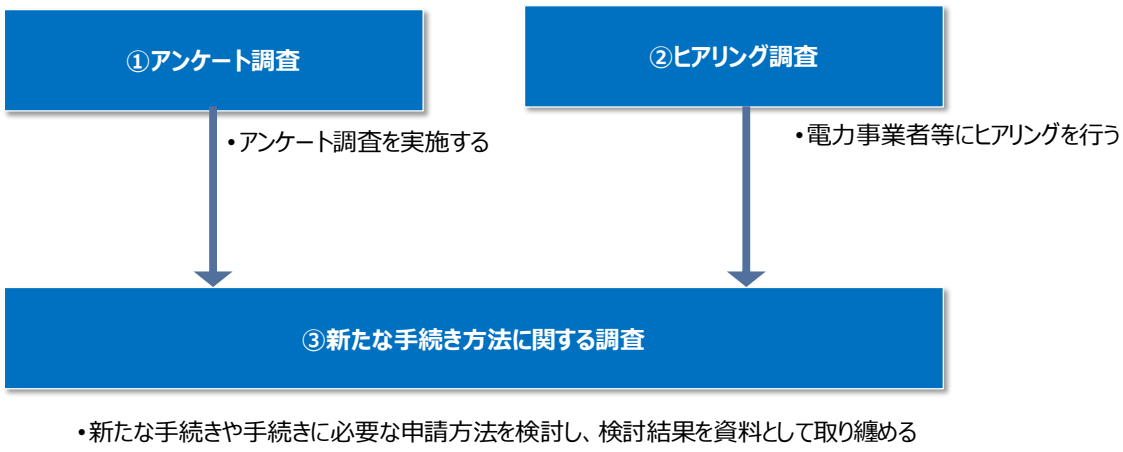


図 3-1　調査方法

3.2.アンケート調査

3.2.1. アンケート調査概要

現在、電力事業者に対して行っている「優先情報提供」の改善、及び「優先情報提供」を電力分野以外の他の重要インフラ分野に提供先を拡大するに際し、「優先情報提供」の有効性の評価および現状の課題を整理し、「優先情報提供」の有効性を高めるための方策について検討を実施した。

上記の検討に資する情報を集めるために、「優先情報提供」を実施した重要インフラ事業者を対象とした、「優先情報提供」の有効性に関するアンケート調査を実施した。

アンケート調査概要を以下の表 3-1 に示す。

表 3-1　アンケート調査概要

調査対象	以下 2 分野へ実施。アンケート回答者は組織窓口を想定。 電力事業者（電力 ISAC 所属企業）：アンケート送付 17 件／受領回答数：14 件 政府機関：アンケート送付 130 件／受領回答数：88 件
調査票の分量	A4 表裏 1 枚程度
調査項目	過去に優先提供を受けた案件について伺う。※回答可能な項目を回答いただく。 • 優先情報提供に向けた事前準備内容 • 自組織内への情報の展開状況 • 優先情報提供への希望
調査手法	電子メールで配布・回収（IPA で実施）
実施期間	2018 年 11 月中旬～2018 年 12 月上旬

アンケート調査では、優先情報提供の制度全般に関わる内容及び実際の優先情報提供を受けて情報の展開状況等を伺った。

実際の優先情報提供を受けて情報の展開状況を伺う場合は、具体的な優先情報提供事例（情報系・制御系問わず）を想定し、ご回答いただいた。

2018 年 12 月までに優先情報提供を行った脆弱性情報等の件数は、施行運用期間中に 2 件、本運用期間中に 2 件の計 4 件である。

3.3.ヒアリング調査

3.3.1. ヒアリング調査概要

アンケート調査を補足するため、重要インフラ事業者（電力事業者）を対象とした「優先情報提供」の有効性に関するヒアリング調査を実施した。
アンケート調査結果およびヒアリング調査結果は、「優先情報提供」における課題整理・改善方策の検討および「優先情報提供」の有効性を高める方策の検討の参考とする。
ヒアリング調査概要を以下に示す。

調査対象	「優先情報提供」を実施した重要インフラ事業者（電力事業者 4 社）
調査項目	＜優先情報提供の実施状況について＞ • ベンダからの一般公開前の脆弱性情報提供の有無、提供形態、その課題 • 脆弱性情報提供を受けた対応内容、パッチ適用の有無、パッチが適用できない場合の脆弱性情報の活用内容 • 重要インフラ事業者としてベンダ・製品開発者へお願いしたいこと ＜改善方策＞ • 「優先情報提供」の改善方策 • 優先情報提供を受ける際の手続き（ISAC-電力事業者間、または電力事業者内、または電力事業者-システム構築事業者の覚書や提供方法）に関するご意見 • 情報の内容に関する問題点 • 公表までの猶予期間に関する問題点 • 優先情報提供で入手したいソフトウエアの種類・分野等 ＜有効性を高めるための方策＞ • 入手した情報の展開状況、問題点 ➢ 自組織内で展開する際に困難だった点 ➢ システム構築事業者への情報展開の有無、展開していない場合の理由

	• 入手した情報の活用状況、問題点 ➢ 活用する上で困難だった点 ➢ 優先情報提供の有無による対応実施時期の違い • 有効性を高める方策 ➢ 優先情報提供の取り組み指針等の必要性 ➢ 今後のパートナーシップへの希望
実施期間	2018 年 12 月～2019 年 1 月

3.4. 優先情報提供制度課題整理、改善策・有効性を高める方策

3.4.1. 優先情報提供制度の有効性評価

アンケート調査では、過去の優先情報提供事例において、組織窓口から組織内に情報展開できたとする組織が電力分野では約 6 割あった。

政府機関では、情報展開できた割合は約 3 割であったが、残りの約 7 割の組織も、そのうち約 7 割超が、該当するソフトウエアを利用していなかったため展開しなかったとしており、全体の約 8 割の組織において、優先提供された情報が自組織に影響するのか判断、活用されている状況が浮かびあがった。

アンケート調査では優先情報提供に関する否定的な意見はほぼなかった。

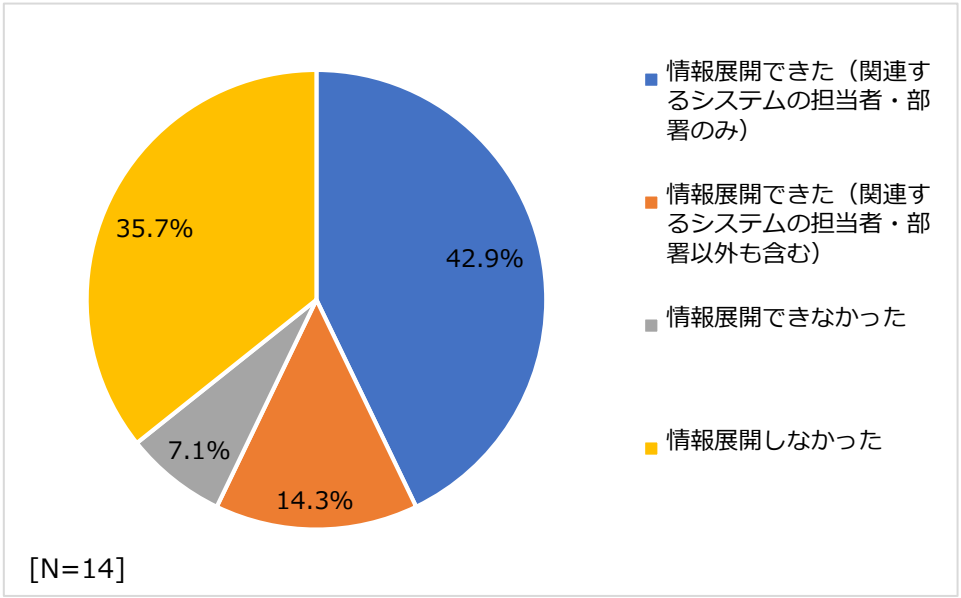


図 3-2 関連するシステムの担当者・部署への情報展開可否【電力分野】

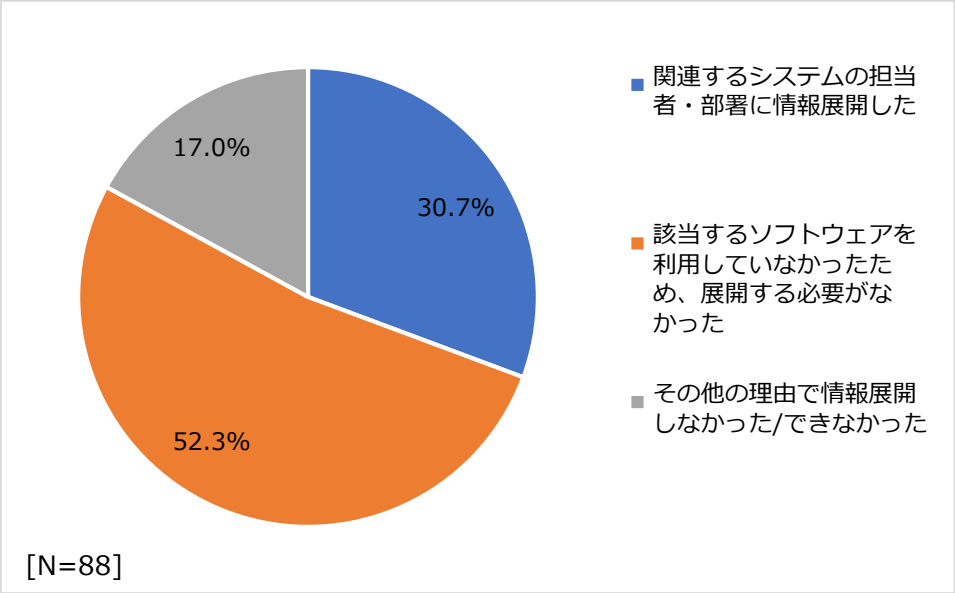


図 3-3 優先提供された情報の判断・活用状況【政府機関】

ヒアリング調査では、優先情報提供を受けた組織の感想として「優先情報提供を受けたことで、脆弱性を放置することなく、情報漏えいを防ぐことができた。」が挙げられたことからも、優先情報提供制度は一定の有効性があると評価できる。

また、優先情報提供の枠組みは、何かあった際に情報が提供できるようにしておくという観点から重要である。尚、本制度は製品開発者の自立的な対応を促進していくものであり、優先情報提供の件数拡大を図るものではない。

3.4.2. 優先情報提供制度の課題抽出

優先情報提供制度自体の課題として、本調査では以下が判明した。

① 様々な機関から類似の情報が提供されることによる情報の取捨選択の負担

重要インフラ事業者にはNISC・警察・保守事業者等様々な機関から類似情報の連絡が入るため、同一性の判断が難しく「情報の交通整理」に時間がかかる場合があった。具体的には、過去の優先情報提供例において、優先情報提供をされるよりも前に、保守事業者から情報提供された場合もあった。

② 優先情報提供の見落とし
組織窓口において、優先情報提供が見落とされていた事例が複数件あった。この理由としてはメールの件名がわかりにくいことが挙げられた。

3.4.3. 優先情報提供制度の改善方策

3.4.2 で示した優先情報提供制度自体の課題を受け、改善方策としては以下が考えられる。

① 様々な機関から類似の情報が提供されることによる情報の取捨選択の負担への改善方策
A) 様々な機関からの情報を一本化する。一本化が難しい場合は、様々な機関から配信される情報が同じ事案に関する情報かどうか判断できるよう、各機関共通の番号を利用する。

② 優先情報提供の見落としへの改善方策
A) 優先情報提供の見落としを防ぐために、優先情報提供のメールの場合は特別な件名をつける。
B) J-CSIP、C4TAP のように、ツール等を用いて、担当者に優先情報が届くような提供方法をとる。

3.4.4. 制度改善以外に有効性を高めるための方策

優先情報提供の有効性を高めるための方策案として以下の要望が挙げられた。要望への対応方針は以下の通り。

No.	概要	要望	今後の対応方針
A	アップデート情報の有無や対応方法等詳細の記載	①より詳細な情報(具体的な攻撃手法、設定で回避する方法、回避できていることの確認方法、シグネチャ等)、②脆弱性に対応したバージョンの更新プログラム、③優先情報提供先の分野で一般的に利用されているシステムに及ぼす影響、④攻撃可能性・頻度、等を優先情報提供時に併せて提供してほしい。	ベンダからの情報提供が必須であり、来年度以降の検討課題とする
B	アップデート情報	ベンダによるアップデートが配信された際に、優先情報提供で通知し	ベンダ自身が実施すべきことであり、IPA

	等の続報の配信	ていた脆弱性等に対するアップデートが行われた旨の続報案内を行ってほしい。	は他に優先すべき対応があるため対象外とする
C	優先情報提供の属人化を防ぐ取り組み	各組織に優先情報を展開する際には、優先情報提供の仕組みの説明や取扱い方法等、優先情報提供制度に関して組織内で周知するために活用できる資料も添付してほしい。	IPA と JPCERT/CC で対応を検討する
D	ツールに取り込むことができるファイル形式での提供	最近は特定のファイル形式であればツールに取り込めるようになっている。情報提供の際のファイル形式が決まるとよい。	IPA と JPCERT/CC で対応を検討する
E	優先情報提供先の拡大	「独立行政法人等における情報セキュリティ対策の推進について」に定めている国と密接な関係のある組織についても優先情報提供の対象とし、一層のサイバーセキュリティ体制の強化を図ってほしい。	実態を改めて確認の上、適宜対応を検討する。

3.5.新たな手続き方法に関する調査

3.5.1. 現行制度の整理

(1) 検討背景

過去の研究会において、優先情報提供に関して表 3-2 の通り過去 4 年にわたり検討されてきた。

表 3-2 過去の検討経緯

年度	検討内容
2015 年度	• 重要インフラ分野への優先情報提供の提言 「パートナーシップは、我が国の安全に重大な影響を及ぼすおそれがあるものに対して、これまで以上に強い姿勢で協力を促すモデルへとシフトし、社会的リスクを低減すべき」

	• 優先情報提供のロードマップの作成（図 3-4）
2016 年度	• 電力事業者を対象として優先情報提供を行うことで合意 • 優先提供すべき情報の判断基準・範囲・内容、タイミング、通知方法、通知先、情報管理体制に関する検討
2017 年度	• 電力 ISAC を窓口として電力事業者に対する優先情報提供の試験運用開始（4 月） • 政府機関(省庁と独法)に対する情報提供体制について検討
2018 年度	• NISC を窓口として政府機関に対する優先情報提供の試験運用開始（4 月）

優先情報提供を受ける組織のメリットとしては以下が挙げられる。

- 事業者：一般公表前の深刻度の高い脆弱性対策情報について提供を受けることで、世間で話題となる前あるいは攻撃が発生する前に対策に関する判断を早期にできるため、脆弱性対応前の攻撃リスクを低減することが可能。
- 優先情報展開組織（ISAC 等）：事業者が ISAC 等に加盟するインセンティブとして上記のメリットを提供することができる。

2015 年度研究会で作成されたロードマップでは、2017 年度以降の研究会において優先情報提供を電力分野以外の他の重要インフラ分野に提供先を拡大することについて検討することになっていた。しかしながら、重要インフラ分野の事業者に対する優先情報提供をより迅速に行うために、脆弱性研究会において分野ごとに個別に優先情報提供可否を審議せず、優先情報提供を受けたい重要インフラ分野からの申請書をもとに提供する手段について検討することとした。

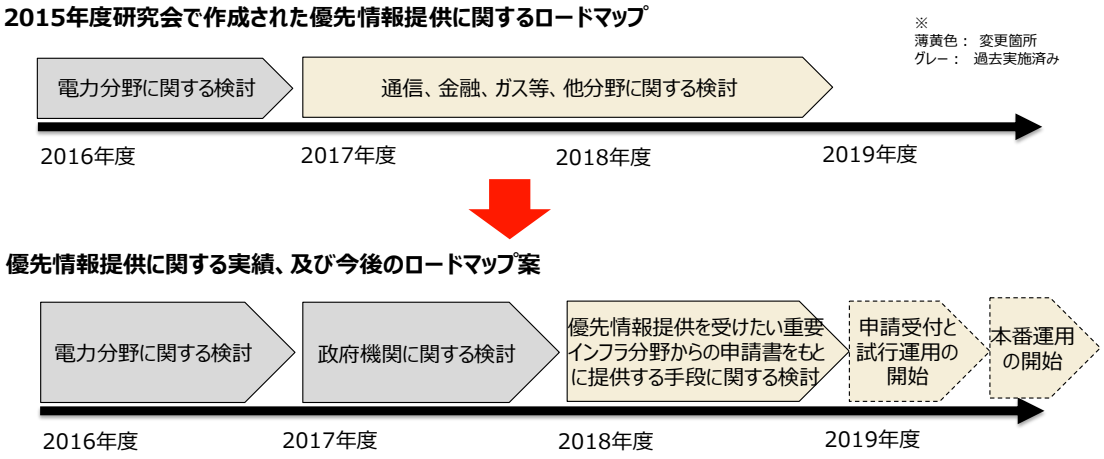


図 3-4　ロードマップの修正

(2) 告示上の対象事業者に関する記載

「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」（平成 29 年経済産業省告示第 19 号）の告示において、優先情報提供の対象となる事業者が特定されている。

優先情報提供の対象となる事業者

調整機関は、対策方法が作成された日から脆弱性情報公表日までの間であって、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脆弱性に起因する重大な影響が及ぶおそれがあると認められるときは、受付機関及び製品開発者と協議をした上で、政府機関や当該設備を用いる事業者等（脆弱性情報等を適切に管理できる者に限る。）に当該脆弱性情報等をあらかじめ通知することができる。

（「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」（平成 29 年経済産業省告示第 19 号）より抜粋）

優先情報提供を電力分野以外の他の重要インフラ分野に提供先を拡大する場合は、対象となる事業者は告示で規定されている以下の要件を満たす必要がある。

（１）対象となりうる事業者の種別

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を有する事業者。

（２）対象とする事業者の要件

脆弱性情報等の適切な管理ができる者に限る。

(3) P ガイドライン上の対象事業者に関する記載

P ガイドライン（平成 29 年 5 月改正）では、重要インフラ等に対し特に影響が大きいと推察される場合を想定し、「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る」と明記している。

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 12)優先的な情報提供実施時の発見者への通知 IPA は、届出がなされた脆弱性関連情報に関して、JPCERT/CC から政府機関や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を保有する事業者等に対して優先的に提供された場合、発見者に対して、その旨を通知します。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。

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とします。

（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（平成 29 年 5 月改正）より抜粋）

(4) 2016 年度研究会電力分野選定理由

2016 年度脆弱性研究会では告示の要件を以下のように解釈し、対象事業分野の選定を行った。

表 3-3　2016 年度脆弱性研究会における告示の解釈の検討

告示上の対象事業者に関する要件	要件の解釈
（１）対象となりうる事業者の種別 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を有する事業者	内閣サイバーセキュリティセンター（NISC）は、第３次行動計画 において、重要インフラを、『他に代替することが著しく困難なサービスを提供する事業が形成する国民生活及び社会経済活動の基盤であり、その機能が停止、低下又は利用不可能な状態に陥った場合に、わが国の国民生活又は社会経済活動に多大なる影響を及ぼすおそれが生じるもの』 と定義し、「重

	要インフラ分野」として 13 分野　を特定し、「重要インフラ事業者」を重要インフラ分野に属する事業者等及び当該事業者等から構成される団体としている。 NISC の定義するこの重要インフラ事業者と、告示の特定する 2(1)の事業者はほぼ同義であるとみなすことができる。従って、まずこの 13 分野から選定することが妥当であると考えられる。
（２）対象とする事業者の要件 脆弱性情報等の適切な管理ができる者に限る。	脆弱性情報等の適切な管理ができるためには、告示における優先提供の趣旨も鑑み、以下の要件を満たす必要があると考えられる。 ①秘密情報の管理 情報提供された当該事業者の中での秘密情報管理が徹底されること。 ②秘密情報の展開先の管理 当該事業者の基盤への活用を検討するにあたり、第三者（基盤システム構築事業者、製品開発事業者、セキュリティサービス事業者等）の協力や支援が不可欠であることが想定されるため、そのようなケースでは、該当する第三者内でも秘密情報管理が徹底されること。 ③秘密情報の利用目的の制約 優先提供される目的は、告示の趣旨から、当該事業者の基盤を防護する目的に対してのみ情報を利用することが徹底されること。

上記で示した事業者の選定基準に従い、下記に示す理由から、優先情報提供先として電力事業者が選定された

① 電力事業者は(1)で示した重要インフラ事業者に属している。また、他の

全ての重要インフラ事業との相互依存性が NISC の調査で報告されている。

② 電気事業連合会は、2015 年度から電力業界としての脆弱性の取扱いの検討を他業界に先行して着手している 。また、電力 ISAC の設立を来年度に計画しており、その対象情報に脆弱性情報も含まれている。 従って、(2)で示した脆弱性情報等の適切な管理を課すことが業界として期待できる。

3.5.2. 申請手続きの検討

(1) 検討概要

電力分野への優先情報提供は、検討開始から試行運用開始まで 1 年要したが、他重要インフラ分野における優先情報提供先を迅速にかつ効率的に拡大することを目指し、電力分野や政府機関への優先情報提供で得た知見を基に、要望がある重要インフラ分野からの申請を元に審査を行い、申請内容に問題がない分野について優先提供を実施する手続きを検討した。申請手続きに必要な情報を検討する上で、事業者の選定基準や審査の方法・体制についても併せて検討を行った。

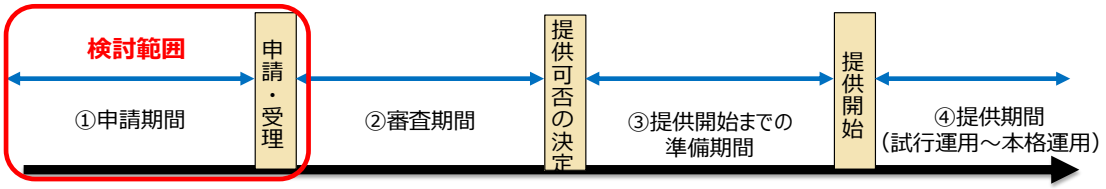


図 3-5 申請から優先情報提供開始までの流れ[6]

表 3-4 検討項目一覧

[6] なお、申請承認後は 1 年程度試行運用を実施し、本運用に向けて発生した課題を解決し、優先提供の対象となる分野に特化した製品を取りまとめることを想定している。試行運用中は、優先提供を行いながら、その結果をフィードバック頂き（アンケートも実施）、1 年程度試行運用を実施したのち、本格運用を実施するかについて関係者間で協議の上判断する。

No.	対象期間	論点	概要
1	ー	申請制可否	申請に基づき優先情報提供を行うことの検討
2	②	申請組織・事業者の選定基準	対象事業分野、申請組織・事業者の要件（情報管理体制等）の検討
3	②	機関の役割	申請受理機関役割分担
4	①	申請手続きに必要な情報	申請手続き書類の記載項目の検討
5	ー	P ガイドラインの改正必要性	申請手続きに関する記載必要性の検討

(2) 申請制の可否

脆弱性研究会での検討を経て優先情報提供を開始するスキームを今後も行う場合、提供先拡大のスピードが緩やかなものとなることが想定される。一方で重要インフラ分野への脅威は拡大しており、迅速にリスク低減することが望まれる。重要インフラ分野の事業者に対する優先情報提供をより迅速かつ効率的に行うために、優先情報提供を受けたい重要インフラ分野からの申請書をもとに提供する。

申請制の長所としては、脆弱性研究会において分野ごとに個別に審議しないことにより、提供先の拡大を迅速に行うことが可能となる。また、電力分野への優先情報提供を通じて、優先情報提供を受ける者においても一定程度の負荷が発生することが判明していることから、優先情報提供への積極的な意志を持つことが望ましい。申請制を採用することで、優先情報提供を受ける準備の整った分野から提供をすることができるため、提供開始後の優先情報提供内容の調整が迅速に進むと想定される。

申請制の短所としては、2015 年脆弱性研究会で審議されたロードマップでは、通信、金融、ガス等、他分野に対して優先情報提供を行うことが提言されていたが、それらの分野から申請がなされないおそれがある。

対応案としては、提供先を拡大する際は、原則として申請制をとるが、優先情報提供の必要性が生じた場合、申請の有無に寄らず対象分野と協議の上、優先情報の提供に向けた調整を行う。また、申請制の導入時には IPA より主要な業界団体等に対し周知を行う。

(3) 申請組織・事業者の選定基準

申請組織の事業分野としては、現行の P ガイドラインに則り、13 分野（情報通信・金融・航空・空港・鉄道・電力（すでに開始済み）・ガス・医療・水道・物流・化学・クレジット・石油）及び政府（すでに開始済み）・行政サービスを対象とする。なお、これ以外の分野を対象とする場合は P ガイドラインの改定が必要である。

また、申請組織は以下の条件を満たす団体とする。

- 上記の対象事業分野に含まれる複数事業者から構成される団体。（迅速かつ効率的に優先情報の提供を行うため）
- 以下の情報管理体制 3 要件をすべて満たす団体。（現行の P ガイドラインに従うため）
  - （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

申請組織としては、原則 ISAC を想定するが、上記の条件をすべて満たす組織であれば審査の上認める場合がある。尚、申請の審査時には情報共有する能力を持つ組織か否かの判断は行わない。

電力 ISAC への優先情報提供を踏まえ、IPA・JPCERT/CC から情報を提供する際は、申請組織の窓口に提供し、申請組織窓口から加盟組織に展開するスキームとする。

申請組織が優先情報を提供できる事業者の要件として、現行の P ガイドラインに則り、優先情報の受け取りは上記の情報管理体制 3 要件をすべて満たす重要インフラ事業者に限る。申請組織の連絡窓口が重要インフラ事業者でない場合は、上記の条件を満たす重要インフラ事業者に優先情報を展開することを目的とする場合のみ、優先情報を取扱うことができる。

(4) 機関の役割

優先情報提供を希望する団体からの申請を以下の手順で受け付ける。

図 3-6 申請手順

(5) 申請手続きに必要な情報

優先情報提供を希望する申請組織は、下記の情報等を申請書に記入し、申請する。なお、申請手続きに必要な情報は今後検討する。

- 申請組織概要（所在地、代表者等）
- 優先情報を受ける対象事業分野（13 分野から選択）
- 申請組織の連絡窓口
- 申請組織としての情報管理体制のチェック（別途、IPA・JPCERT/CC と結ぶ情報管理体制と同等のレベルの情報管理体制を加盟組織に対し求める覚書を締結する。）
- 添付資料：定款（規約）、申請組織概要、申請組織図、申請組織に加盟する全事業者/重要インフラ事業者該当有無一覧、申請組織の情報管理体制（３要件）が確認できる資料

(6) P ガイドライン改訂の必要性

No.1～4 の論点への対応案は現行の P ガイドラインに反するものではないため、本年度の P ガイドライン改訂は不要と結論付けた。

4. 調整不能案件の一覧への掲載、公表手続きの改善に向けた検討

4.1. 調査の概要

4.1.1. 調査目的

ソフトウエア製品の届出において、長期にわたり脆弱性対策が行われず、連絡不能開発者一覧(以下「一覧」という。）にも公表されないまま滞留している案件や、一覧公表後に公表判定委員会で判定できないまま長期滞留してる案件がある。一覧への公表や公表判定委員会での公表判定という手続き（以下「本手続き」という。）は、製品利用者が脆弱性対策が行われていないソフトウエア製品を利用し続けることによる被害を低減するための手続きであるが、現時点では以下に示す認識の通り、有効活用できていない。

- 調整不能（連絡不能）案件が公表できずに滞留している
- 手続きが迅速に進まないことによる関係者（発見者）の不満
- 世の中の利用者が少ないものについて膨大なコストをかける必要性があるか疑問視されている

上記の現状認識を踏まえ、本年度の調査目的を以下の通りとした。

- スムーズな調整ができるよう運用を改善し滞留を解消する
- 関係者（発見者）の不満を解消する
- 案件の影響度を鑑みてより重要な案件へ注力できる体制・運用を検討する

4.1.2. 調査方法

調査方法は図 4-1 に示す通りである。

調査では、過去の研究会の報告書等の文献調査や IPA・JPCERT/CC での検討結果を基に改善案を検討した。検討した改善案については有識者（脆弱性研究会委員及び公表判定委員会委員 5 名、経済産業省）にヒアリングを実施し、ヒアリングの意見をもとに改善案の見直しを実施した。

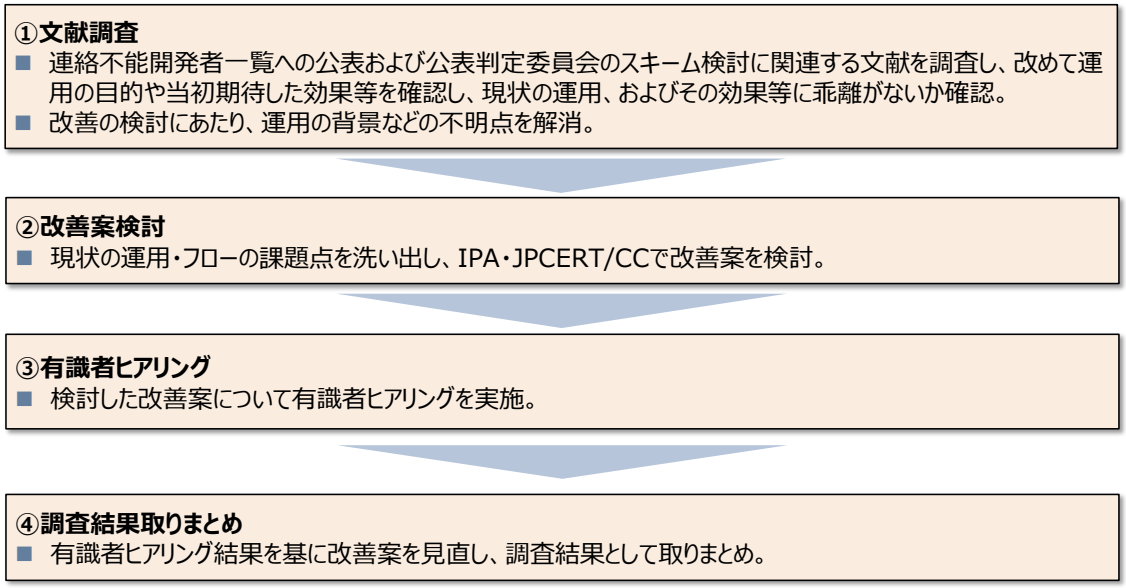


図 4-1　調査方法概要

4.2. 調査結果

4.2.1. 調整不能（連絡不能）案件の取扱いプロセスと課題

調整不能（連絡不能）案件の取扱いプロセスと課題は以下に示す通りである。

連絡不能開発者一覧へは、JPCERT/CC から製品開発者に連絡・督促を実施し、コンタクト開始から一定期間製品開発者からの回答がない場合、連絡不能開発者一覧に掲載されるプロセスとなっている。しかし、現時点では表 4-1 に示す要因により、連絡不能開発者一覧へ公表されないまま滞留している案件が在している。

また、連絡不能開発者一覧に掲載された調整不能案件については、公表判定委員会で判定されるが、公表判定委員会で判定されないまま滞留している案件も存在している。

上記背景から、現行の取扱いプロセスを継続した場合、滞留の解消が期待できないばかりだけではなく、滞留案件が今後増加する見込みである。

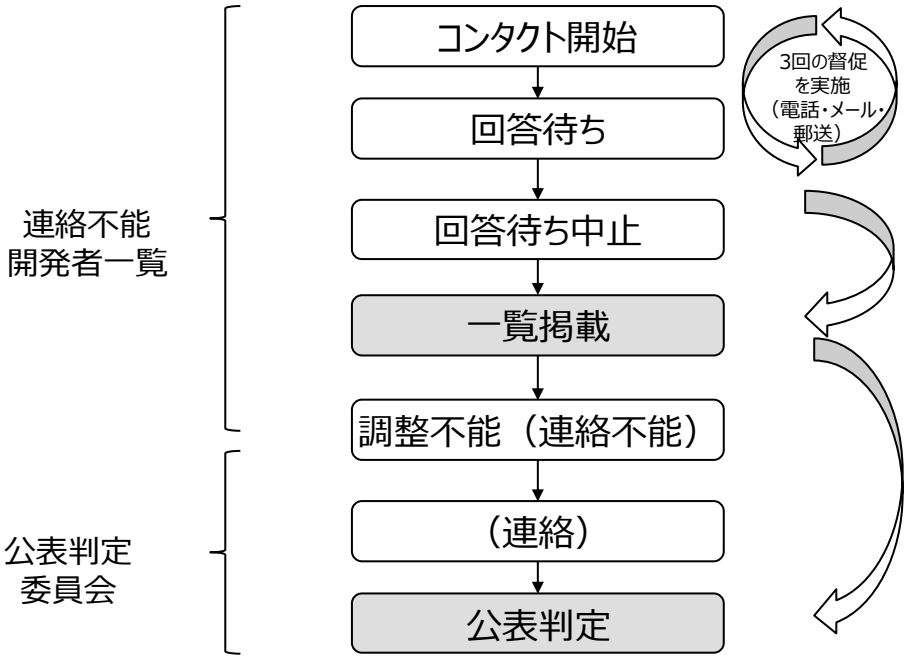


図 4-2　調整不能（連絡不能）案件の取扱いプロセス

表 4-1　調整不能（連絡不能）案件の取扱い上の課題

要因	説明	発生箇所
1. 連絡不能の判断の難しさ	・連絡不能案件について、十分に連絡を行ったのかどうかの判断と、いつまで待てばよいのか判断が難しい ⇒一覧への掲載が行われない案件が滞留する	連絡不能開発者一覧
2. 連絡に係る作業負荷	・連絡不能開発者に対して複数手段で連絡を取る必要があるが、作業負荷が高い（郵送等） ⇒一覧への掲載が行われない案件が滞留する	連絡不能開発者一覧
3. 手続きが最適化されていない	・連絡不能案件の公表判定に係る手続きにおいても、製品開発者への通知等を除き、他の調整不能案件と同等の厳格な手続きを実施している ⇒公表判定の手続きが進まずに、案件が処理できない	公表判定委員会
4. 選定条件の未設定	・連絡不能案件について、すべての案件が対象となっているが、公表判定の 4 条件を満たさない案件や、委員から指摘を受けた公表する意義が低そうな案件がある ⇒これらを処理できず滞留したままとなる	連絡不能開発者一覧・公表判定委員会

4.2.2. 改善方針

(1) 改善方針概要

調査結果を基に改善箇所を以下の 3 点に整理し、改善方針を検討した。

- 連絡不能開発者一覧掲載までの製品開発者への連絡の改善
- 連絡不能案件の取扱方針の見直し
- 公表判定委員会の運用改善

改善箇所ごとの改善方針の概要と、解消される要因は表 4-2 に示す通りである（各改善方針の詳細は後述）。これら、改善方針の実施により、滞留している調整不能案件の解消、関係者（発見者）の不満解消、重要な案件に注力できる運用・体制を実現する。

表 4-2 改善方針概要

改善箇所	改善方針	解消される要因
(1)連絡不能開発者一覧掲載までの製品開発者への連絡の改善	■ 連絡先の**調査対象と調査方法をチェックリスト化し、必要最低限の連絡先へ 3 回連絡することで連絡業務を効率化**する。 ■ 製品開発者の住所が判明している場合、**2 回目のコンタクトで郵送を実施し、製品開発者の対応を促す**。	1.連絡不能の判断の難しさ 2.連絡に係る作業負荷
(2)連絡不能案件の取扱方針の見直し	■ 公表判定委員会の**判定対象を、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。 ■ **脆弱性検証不可と「簡易対応」案件は、判定対象としない**。 ■ 検証不可能な優先対応案件は、本制度で取扱価値のある案件(「通常対応」案件以上のコストを掛ける案件)か否かの条件を追加。**価値が低いと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**。	3.手続きが最適化されていない 4.選定条件の未設定
(3)公表判定委員会の運用改善	■ IPA・JPCERT/CC で判定 4 条件のチェックリストを作成。 ■ **チェックリストを基にした事務局案を**	3.手続きが最適化されていない 4.選定条件の未

	公表判定委員会に諮り、判定を依頼。 ■ 滞留している調整不能案件の処理を進める。	設定

(2)「連絡不能開発者一覧掲載までの製品開発者への連絡の改善」に関する改善方針

連絡先の調査方法は、どこまで調査すればよいのか担当者の調査スキルに依存しないようにチェックリストを設ける。また、OSS 等では連絡先を公開していないケースもあり、調整機関が連絡先を探すのに時間を要している。過去の案件で、発見者が製品開発者の連絡先を把握しているケースがあったため、発見者への確認を追加する。

郵送は製品開発者の対応を促す上で高い効果があることから、郵送でのコンタクトを早期に実施する運用に変更する。

新たな連絡先を発見する度に 3 回連絡するのは際限がないため、最低限チェックリストの宛先へ 3 回連絡すればよい運用とする。

現在の運用と改善方針を比較したものを表 4-3 に示す。

表 4-3　現在の運用と改善方針

項目	現在の運用	改善方針
連絡先の調査方法	■ 届出情報や製品に添えられた宛先情報、インターネット等から製品開発者を調査	■ 調査対象と調査方法をチェックリスト化する。 ■ 適宜、発見者に製品開発者の連絡先を把握していないか、確認するプロセスを追加する。
連絡方法	■ メール、郵送、SNS 等の複数の連絡方法で実施	変更なし
連絡回数	■ 3 回実施（途中で新たな連絡先を発見した場合は、その連絡先へも3回連絡を実施する）その後督促状を送付(住所を把握している場合は郵送)	製品開発者の住所の把握状況により運用を変更する。 ■ 製品開発者の**住所を把握している場合** ➢ 2 回目のコンタクトを郵送で実施。 ■ 製品開発者の**住所を把握していない場合** ➢ 郵送以外の方法で 3 回実施(最低限チェック

		リストの宛先にのみ)。

上記改善方針について、有識者ヒアリングでは以下のような意見をいただいた。ヒアリングでは有識者から、上記の改善方針で問題ない旨のご意見をいただいた。

主なご意見
・ 郵送は最後の切り札であり、2 回目のコンタクトで郵送とすることも問題ないのではないか。 ・ 宛先が見つかった時ごとに 3 回コンタクトを実施することは不必要であり、チェックリストで連絡する方針でよい。方針を変更しても、通知義務を果たしたと認められると考えてよいのではないか。 ・ パートナーシップ制度が誰（個人または組織）に対して実施することを想定しているか整理したほうがよい。対組織であれば最初から郵送で問題ない。 ・ 連絡がつかないのは時間の問題ではなく手段の問題である。連絡が来ないなら連絡不能に掲載すればよく、6 か月待っても状況は変わらない。製品開発者へ連絡を開始してから 1 か月以内には連絡不能の判断をして連絡不能開発者一覧へ公表するべきではないか。 ・ 有償製品は開発者として責任があるため、厳しく対応してもよい。 ・ 住所がわからない場合、1 か月に 3 回メールを出して反応がなければ連絡不能と判断してもよいのではないか。スパムで届いていない可能性もあるため、連絡不能開発者一覧に掲載するときに、スパム判定で届いていない可能性がある等の説明を追加すればよい。 ・ 連絡先の調査方法のチェックリストは、どのようなプロセスで実施しているか公表したほうがよい。ブラックボックスで実施していると発見者の不満につながる可能性がある。取扱いプロセスはわかりやすい形で透明化したほうがよい。内部の運用手順の一部を公表できる形にすればよい。 ・ 連絡先は漏れや見落としがないようにしたほうがよい。容易に連絡が取れるのに、連絡できておらず公表した場合問題になる可能性がある。チェックリスト等については公表判定委員会委員が確認してもよいのではないか。 ・ 担当者が行政手続きにまだ習熟していないこと、連絡先の調査ノウハウ等が担当者間で共有されておらず何を実施すべきかが十分理解できていないこと等が、通知方法がうまくいかない背景にあるのではないか。

(3)「連絡不能案件の取扱方針の見直し」に関する改善方針

連絡不能案件のうち、公表判定委員会に諮ることができない案件が滞留しており、現在の制度では取扱終了とする出口がない。

そこで、公表判定委員会で判定する対象を整理し、判定対象外の案件については、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。

また、脆弱性の検証不可案件については製品の調達にかかるコストをかけてまで実施する必要はないと判断することとする（「優先対応」案件で脆弱性の検証不可となる案件は現時点では存在しない）。連絡不能案件のうち「簡易対応」の案件について JVN 公表は不要と判断（連絡不能案件ではない「簡易対応」の案件（脆 3）は、製品開発者への通知をもって JVN 公表せずに終了していることから、同様の取扱いとする）。

なお、特段の事情がある案件は個別配慮することとする。

表 4-4　現在の運用と改善方針

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、受理後の対応の条件（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）が低いと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。

改善案導入後の、連絡不能案件の取扱は下表の通りとなる。

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）

上記改善方針について、有識者ヒアリングでは以下のような意見をいただいた。ヒアリングでは有識者から、上記の改善方針で問題ない旨のご意見をいただいた。

主なご意見
・ 影響度の考え方にパートナーシップ制度で取扱う価値がない（コストをかける意義がない、連絡が取れないため取扱いを継続する意義がない）を追加してはどうか。脆弱性の有無を IPA が確認できない状況であれば、発見者に戻すのが大原則ではないか。 ・ 簡易対応は公表判定委員会にかけず通知して終了でよい。連絡不能の場合は取扱終了でよい。 ・ OSS は個人かチームにより取扱いが難しい。例えば、GitHub 上のすべての OSS を制度で扱うのは現実的には無理であり、影響度やダウンロード数等で判断する必要があるのではないか。ダウンロード数が少ない案件は簡易対応とすればよい。客観的な指標があるとよい。 ・ EoL の考え方がまだ浸透しておらず、明確にしているところはまだ少ない。しかし、EoL 製品であれば制度で取扱わない、公表判定委員会にかけない等も検討する必要があるのではないか。

・　基準/ルールに該当しない特殊な案件を想定し、その様な案件にも個別配慮し対処できるよう内部の運用ルールを検討したほうがよい。機械的な運用とした場合、基準に該当しない案件が排除される可能性がある。 ・　リソースの制約があるのであれば、本当に重要な案件を取扱えるような運用を考えたほうがよい。

(4)「公表判定委員会の運用改善」に関する改善方針

これまでの公表判定委員会の運用経験・議論の結果等を基に、判定 4 条件に関するチェックリストを作成し、IPA・JPCERT/CC が機械的／客観的に判定 4 条件を判断できるようにする。

チェックリストを基に IPA・JPCERT/CC が作成した事務局案を公表判定委員会に諮り、判定を依頼する。公表判定委員会では、IPA・JPCERT/CC が機械的/客観的に判断できない条件や、委員が事務局案に関して議論が必要と判断したものを中心に、審議し判定を依頼する運用とする。

委員会資料の作成負担を減らし、効率化をすることで限られた時間での処理件数を増やす。

表 4-5　現在の運用と改善方針

項目	現在の運用	改善方針
公表判定委員会の判定方法	■　判定 4 条件について、すべて同様に判定。（内容によって簡略化や重みづけは実施していない）	■　**IPA・JPCERT/CC で判定 4 条件について、これまでの運用を基にしたチェックリスト等を作成（内容は公表判定委員会委員が確認）し機械的／客観的に条件を満たすか確認**。 ■　IPA・JPCERT/CC の判断結果を基に作成した**事務局案を公表判定委員会に諮り、委員会で判定し承認を実施** ➢　IPA・JPCERT/CC で機械的/客観的に判断できない条件は委員に当該条件を満たすか否か判定を依頼する ➢　事務局案で委員が議論

		の必要があると判断したものは、審議し判定を依頼する ■ 公表が不適当と判定された案件について、その後の取扱いについても、公表判定委員会に判断を委ねる。 ■ IPA で事前に判定条件（エ）を満たさないと判断（例：身体生命に影響を及ぼすため公表すべきではないと思われる）した場合は、公表判定委員会に取扱方針を仰ぐため、判定を依頼する
公表判定委員会の資料等	■ 公表判定委員会の資料は製本（紙）で配布し、成果物レビュー等を実施 ■ 委員会議事録を作成	■ 資料は必要最低限とし、製本（紙）は行わずデータでの取扱いとする。 ■ **議事概要を作成**する（録音データ等はIPAの文書管理規程等に基づき管理する）。

上記改善方針について、有識者ヒアリングでは以下のような意見をいただいた。ヒアリングでは有識者から、上記の改善方針で問題ない旨のご意見をいただいた。

主なご意見
・ 定型的に処理できる案件と、そうでないものを分けたほうが、処理が進むのではないか。重要な案件を公表判定委員会で審議したほうがよく、重要な案件が公表判定委員会にかけられていないのであれば、その課題を整理することも必要ではないか。 ・ 公表判定委員会の委員数を増やし、各分野の専門家が少なくとも一人出席すればよいのではないか。参加できる人のみで調整し、一定の質が保てればよい。 ・ 公表判定委員会の審議内容にメリハリつけることはよい。審議が必要なものだけ議論してもらえばよい。機械的に決まったものを議論するのは意味がない。 ・ 疑義があるものだけ、資料を作成して議論すればよい。 ・ 公表判定委員会を四半期に１回程度実施しなければ滞留する状況は改善しないのではないか。 ・ 公表判定委員会の開催回数を増やしたほうがよい。年に１回では緊急性のある案件に対応できない。また、開催回数を増やすことにより事務局にノウハウが蓄積され、運用の効率化も進むのではないか。 ・ 公表判定委員会に諮る案件について、事務局案を作成し、委員が疑問がある箇所についてのみ審議する運用にすればよいのではないか。 ・ 議事録は議事概要のみ作成すればよいのではないか。 ・ 委員会の運用状況を確認し見直すことも、公表判定委員会の審議事項として、審議してもよいのではないか。

(5) その他、調整不能案件に関わる改善事項

有識者ヒアリングによるコメントを受け、次年度以降、以下の点について IPA・JPCERT/CC で改善案を検討する。

表 4-6　有識者ヒアリング結果を基にした次年度検討内容

改善箇所	次年度検討内容
連絡不能開発者一覧	■ 調整プロセスの見える化のため、連絡先の調査方法(チェックリスト等)についてウェブサイト等で公開を行う。 ■ 「連絡不能開発者一覧」に掲載する際に、以下に例示するような情報も発信し、製品開発者・発見者等の協力が得やすい環境を構築する。 例) ・ スパムフィルタで受信できていない可能性があること ・ 修正方法が分からない開発者に対して IPA・JPCERT/CC から技術資料を提供すること ・ メンテナンス／サポート終了の場合、修正せずに、対策として利用停止を促す JVN 公表が可能であること
公表判定委員会	■ 各分野の委員の増員を検討する ■ 委員会開催回数について、来年度に新たな運用手順で運用を開始後検討する。

4.2.3. 来年度以降の対応方針

本年度の検討結果を基に、以下の通り来年度以降対応を進める。なお、来年度実施内容に関しては、公表判定委員会委員へ事前に説明し了承を得る。

表 4-7　来年度以降の対応方針

改善箇所	P ガイドライン改訂	来年度以降実施・検討内容
(1) 連絡不能開発者一覧掲載までの製品開発者への連絡の改善	不要	■ 連絡先の調査対象と調査方法についてチェックリストを作成。 ■ 今年度検討した改善方針に基づき運用を実施。
(2) 連絡不能案件の取扱方針の見直し	要	■ 「簡易対応」と判断できる案件については、次年度以降、取扱いを終了する運用を開始。 ■ 「通常対応」で、検証不可の案件については、ガイドラインの改訂後に運用を開

		始。 ■ 告示改正の必要性については経済産業省で検討する。
(3)公表判定委員会の運用改善	不要	■ IPA・JPCERT/CC で判定 4 条件のチェックリストを作成。 ■ チェックリスト作成後、今年度検討の改善方針に基づき、公表判定委員会の運用を開始。 ■ 新たな運用開始後に、運用結果について公表判定委員会で評価することを検討する。
(4)その他、調整不能案件に係る改善事項	不要	■ IPA・JPCERT/CC で改善案を検討し、実施。

5. 法的課題の整理

5.1. 調査の概要

5.1.1. 調査目的

近年の法整備・改正を踏まえ、法的な観点からパートナーシップの法的解釈について再度整理を行う。

5.1.2. 調査方法

本調査は、パートナーシップに詳しい法務専門家が主導する形で、検討が必要な項目を整理し、調査を実施した。

調査結果に関して、P ガイドライン上の法律に関係する解説については、2004 年に公表した「情報システム等の脆弱性情報の取扱いにおける法律面の調査報告書」の内容を改定する形で、「法律面の調査報告書改定版」として取りまとめた。また、P ガイドラインの修正が必要な項目については、具体的な P ガイドラインの修正案を作成し、「別紙 1_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改訂案」、P ガイドライン改訂方針については、「別紙 2_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説明資料」に反映した。

5.2. 調査結果

5.2.1. 検討項目

近年の法整備・改正を踏まえ、パートナーシップに詳しい法務専門家が主導する形で、本年度の調査検討項目を以下の通り整理した。

検討項目は、P ガイドライン改訂に関する項目と法律面の調査報告書の改定に関する項目に分けて整理した。

表 5-1　検討項目一覧

検討箇所		概要
P ガイドラインの改訂		P ガイドラインの適用範囲の明確化
		ソフトウエアの脆弱性情報に関する調整機能の実現
		脆弱性の定義の「不適切な運用」について
		「受理」の概念と脆弱性の特定の関係
		法改正などを加味した付録の記載の見直し・修正
		提供情報と漏えい概念の整理
法律面の調査報告書の改定	第 1 章　脆弱性情報と取扱いルールと法律とのかかわり	違法な手段で入手された脆弱性関連情報
		公表判定委員会の概要・趣旨について
		脆弱性調査としてのリバースエンジニアリングについての問題点
		IoT 機器の脆弱性調査に関する事項
		IoT をめぐる P ガイドラインと安全規制の関係
		脆弱性調査をめぐる法的事件
	第　2　章「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」における法的関連記述の逐条解説	P ガイドラインの改訂検討結果に基づく P ガイドラインの適用範囲の明確化
		自社製品届出の開発者の位置づけ
		「不特定または多数の人々に影響する」の意味
		P ガイドラインの改訂検討結果に基づく「受理」の概念と脆弱性の特定の関係
		ソフトウエア製品の定義について

5.2.2.　P ガイドライン改訂に関する項目の検討結果

検討結果は、「別紙 1_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改訂案」として取りまとめた。

5.2.3. 法律面の調査報告書の改定に関する項目の検討結果

検討結果は、「法律面の調査報告書改定版」として取りまとめた。

2004 年に公表した「情報システム等の脆弱性情報の取扱いにおける法律面の調査報告書」を改定するにあたり、報告書の構成を以下の通り見直した。また、報告書の改定にあたっては、2004 年当時は制度運用前の報告書モデル案に対する法的解説であった点を、P ガイドラインに対する法的解説へと記載を見直すとともに、諸外国の動向に関する記載（第 2 章及び付録 1・2）は調査時点から時間が経過し情報が古いことから削除した。

法律面の調査報告書の現在の構成

第1章	脆弱性情報と取扱いルールと法律とのかかわり
第2章	米国における脆弱性情報と法的論点
第3章	報告書モデル案における法的関連記述の解説
付録1	米国における脆弱性の取扱いに関する法律面の動向
付録2	韓国における脆弱性の取扱いに関する法律面の動向

法律面の調査報告書改定版の構成

第1章	脆弱性情報と取扱いルールと法律とのかかわり
第2章	「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」における法的関連記述の逐条解説

6. パートナーシップガイドラインの改訂等に関する調査

6.1. 調査結果

本年度の調査結果を基に、P ガイドラインを改訂する。本年度は以下に示す 3 つの方針を基に改訂した。

表 6-1　P ガイドライン改訂方針

方針	改訂概要
調整不能案件の一覧への掲載、公表手続きの改善に向けた検討結果の反映	● P ガイドラインの受理後の対応のうち、処理を取り止めることができる条件を告示の表現に合わせる。 ● 条件の解釈を拡大し、本制度で取扱価値があるか否かの条件を追加する。
法的課題の整理結果の反映	● 法務専門家の検討結果を基に修正をおこなう。 ● 具体的には以下の通り。 ➢ 用語の定義や P ガイドラインの適用範囲等の修正 ➢ 受理要件に関する表現の修正 ➢ 法律の改正や最新の判例に合わせた修正
表現等の軽微な修正	● 誤字脱字や表現の揺れ、参照文献の URL の更新等の軽微な修正をおこなう。

本年度の検討結果を基にした P ガイドラインの改訂案については、「別紙 1_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改訂案」を参照のこと。

6.1.1.　調整不能案件の一覧への掲載、公表手続きの改善に向けた検討結果の反映

調整不能案件の検討結果を基に、本制度で取扱価値のある案件か否かを取扱終了の条件として追加し、価値が低いと判断した案件は取扱終了できるようにした。

P ガイドラインの受理後の対応の表現を告示に合わせる形で改訂し、「脆弱性関連情報に該当しない場合」に本制度で取扱価値があるか否かが含まれるという解釈を「法律面の調査報告書改定版」に追記した（告示改正の必要性については来年度以降検討する）。

【改訂箇所】

ⅠⅤ．ソフトウエア製品に係る脆弱性関連情報取扱

３．IPA（受付機関）の対応

現在のＰガイドライン	Ｐガイドライン改訂案
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） 脆弱性ではない場合 （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）	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）

【改訂箇所】

Ⅴ．ウェブアプリケーションに係る脆弱性関連情報取扱

３．IPA（受付機関）の対応

現在のＰガイドライン	Ｐガイドライン改訂案
4）脆弱性関連情報への対応続行の判断 IPA は、以下の条件のいずれかと合致した場合、処理を取りやめるとともにウェブサイト運営者および発見者に連絡します。なお、取扱いを終了する場合、IPA の発見者に対する情報非開示依頼は効力を失います。 （ア） 脆弱性でない場合 （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）	4）脆弱性関連情報への対応続行の判断 IPA は、以下の条件のいずれかと合致した場合、処理を取りやめるとともにウェブサイト運営者および発見者に連絡します。なお、取扱いを終了する場合、IPA の発見者に対する情報非開示依頼は効力を失います。 （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） ウェブサイト運営者から脆弱性関連情報が既知であり、その脆弱性が修正されていると連絡があった場合	（エ） ウェブサイト運営者から脆弱性関連情報が既知であり、その脆弱性が修正されていると連絡があった場合

6.1.2. 法的課題の整理結果の反映

(1) P ガイドラインの適用範囲の明確化

ウェブアプリケーションの作成に関して、豊富なプラグイン等が提供されるようになったことから、日本語への機械翻訳サービスを利用した上で、ウェブサイトを日本語で表示するページが増えてきている。

アクセスが実質的にわが国の利用者にとって、重要であるか否かが P ガイドラインが適用されるために重要な指標になっていることから、「実質的に」アクセスがなされることを適用の要件として追加した。

【改訂箇所】

Ⅲ. 本ガイドラインの適用の範囲

現在の P ガイドライン	P ガイドライン改訂案
○主に日本国内からのアクセスが想定されているウェブサイトで稼働するウェブアプリケーション	○~~主に~~日本国内からのアクセスが実質的になされているウェブサイトで稼働するウェブアプリケーション

(2) ソフトウエアの脆弱性情報に関する調整機能の実現

未修正の製品の脆弱性情報について、その製品を組み込んでいる製品/ウェブサイトについて届出があった場合、組み込んでいる製品開発者/ウェブサイト運営者にも通知できるのが、調整機能の実現において望ましいと考えられる。また、脆弱性を含むソフトウエア製品を組み込んで一体のソフトウエア製品として提供しているものも製品開発者とみなすことができることから、このようなケースにおいても調整機能が実現できるよう改訂した。

【改訂箇所】

Ⅳ. ソフトウエア製品に係る脆弱性関連情報取扱

3. IPA（受付機関）の対応

現在の P ガイドライン	P ガイドライン改訂案
5) 脆弱性関連情報の取扱い IPA は、脆弱性関連情報に関して、それに関	5) 脆弱性関連情報の取扱い IPA は、脆弱性関連情報に関して、正当な理

する脆弱性情報が一般に公表されるまでの間は、発見者・JPCERT/CC・当該製品開発者以外の第三者に提供しないように適切に管理します。ただし、脆弱性が再現する状況を特定できない等正当な理由がある場合、IPA は、秘密保持契約を結んだ上で、独立行政法人産業技術総合研究所や技術研究組合制御システムセキュリティセンター等の外部機関に脆弱性関連情報に関する技術的分析を依頼することや、関係者の許諾を得た上で、JPCERT/CC と連携し、脆弱性の再現に必要な情報を製品開発者に提供することがあります。	由がない限り発見者・JPCERT/CC・当該製品開発者以外の第三者に開示しません。ただし、以下のような正当な理由がある場合、IPA は第三者に情報を開示することがあります。なお、技術的分析を依頼する場合、IPA は秘密保持契約を結びます。 （ア） 脆弱性を有するソフトウエア製品が、他のソフトウエアやウェブサイトで利用されている場合に、それらの製品開発者やウェブサイト運営者に連絡する場合 （イ） 脆弱性が再現する状況を特定できない等の場合に、国立研究開発法人産業技術総合研究所や技術研究組合制御システムセキュリティセンター等の外部機関に脆弱性関連情報に関する技術的分析を依頼する場合 この場合、関係者の許諾を得た上で、JPCERT/CC と連携し、脆弱性の再現に必要な情報を製品開発者に開示することがあります。 また、IPA は、脆弱性関連情報に関して、それに関する脆弱性情報が一般に公表されるまでの間は、発見者・JPCERT/CC・当該製品開発者以外の第三者に漏えいしないように適切に管理します。

【改訂箇所】

Ⅳ．ソフトウエア製品に係る脆弱性関連情報取扱

４．JPCERT/CC（調整機関）の対応

現在の P ガイドライン	P ガイドライン改訂案
2）製品開発者への連絡 JPCERT/CC は、届け出られた脆弱性関連情報の IPA からの通知を受け、製品開発者リストの活用や脆弱性関連情報を分析することに	2）製品開発者への連絡 JPCERT/CC は、届け出られた脆弱性関連情報の IPA からの通知を受け、製品開発者リストの活用や脆弱性関連情報を分析することに

より、速やかに製品開発者を特定し、必要に応じて製品開発者リストに当該製品開発者を追加した上で、その製品開発者に連絡を行います。その際に、各製品開発者に対して、脆弱性検証を行い、その結果を報告することを求めます。 　また、JPCERT/CC は、OSS に関する事前通知を、製品開発者または開発コミュニティに加えて、必要に応じて以下へ通知します。 ・OSS を導入した製品の開発者 ・ディストリビュータ ・製品の仕様を決定するサービス提供者（例：携帯電話会社）	より、速やかに製品開発者を特定し、必要に応じて製品開発者リストに当該製品開発者を追加した上で、その製品開発者に連絡を行います。その際に、各製品開発者に対して、脆弱性検証を行い、その結果を報告することを求めます。 　JPCERT/CC は、届け出られた製品と実質的な相互関係にある製品を特定した場合には、その製品開発者に連絡を行い、調整することができます。 　また、JPCERT/CC は、OSS に関する事前通知を、製品開発者または開発コミュニティに加えて、必要に応じて OSS を導入した製品の開発者・ディストリビュータ・製品の仕様を決定するサービス提供者（例：携帯電話会社）へ通知します。

(3) 脆弱性の定義の「不適切な運用」について

ソフトウエア製品において、製品リリース前の確認不備により製品開発者の機微情報が製品にハードコードされたまま頒布される等の可能性があるが、製品開発者の機微情報が利用者に影響を与えるか否かが不明な場合がある。

そのような場合でも、ウェブアプリケーションと根本的に取り扱いを変える合理性はないために、双方において、不適切な実装・運用により、当事者の意図に反しセキュリティが維持できなくなっている場合について、パートナーシップ制度の適用対象とするため改訂した。

【改訂箇所】

Ⅱ．用語の定義と前提

1．脆弱性

現在のＰガイドライン	Ｐガイドライン改訂案
なお、ウェブアプリケーションにおいて、ウェブサイト運営者の不適切な運用によって、個人情報等が適切なアクセス制御の下に管理されておらずセキュリティが維持できなくなっている状態も含みます。（ウェブサイトの	なお、製品開発者の不適切な実装やウェブサイト運営者の不適切な運用によって、個人情報等が適切なアクセス制御の下に管理されておらずセキュリティが維持できなくなっている状態も含みます。（ウェブサイトの不適切

不適切な運用に関しては付録１に例を示します。）	な運用に関しては付録１に例を示します。）

(4)「受理」の概念と脆弱性の特定の関係

「IPA が精査した結果、脆弱性が存在する可能性があると判断できる」という表現は、届け出られた報告を実際に再現して、IPA が脆弱性の存否を確認しなければならないと解釈される可能性がある。しかし、IPA が届出に際して審査する事項は、その形式的な事項のみで、実質的な脆弱性の有無は審査しない。

そこで、脆弱性が存在する可能性があると判断できるという表現を避け、届出した事実が、存在すれば、脆弱性であることを受理の実際的な要件となるよう改訂した。

【改訂箇所】

Ⅳ．ソフトウエア製品に係る脆弱性関連情報取扱

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

現在の P ガイドライン	P ガイドライン改訂案
2）届出の受理 IPA は、以下の条件がすべて満たされていると判断した時、その時点で届出を受理し、発見者に連絡します。 （ア）上記２．5)の項目がすべて記載されていること （イ）届出内容に矛盾等が無いこと （ウ）届出の対象が本ガイドラインの適用範囲に該当すること（Ⅱ章参照） （エ）記載されている内容が脆弱性であること IPA は、以下のいずれかに該当することを確認します。 ・IPA が精査した結果、脆弱性が存在する可能性があると判断できる ・届出に脆弱性が存在する事実を示す証拠が添付されている	2）届出の受理 IPA は、届出の記載が以下の条件をすべて満たしていると判断した時、その時点で届出を受理し、発見者に連絡します。 （ア）上記２．5)の項目がすべて記載されていること （イ）届出内容に矛盾等が無いこと （ウ）届出の対象が本ガイドラインの適用範囲に該当すること（Ⅲ章を参照） （エ）記載されている内容が脆弱性であること ~~IPA は、以下のいずれかに該当することを確認します。~~ ~~・IPA が精査した結果、脆弱性が存在する可能性があると判断できる~~ ~~・届出に脆弱性が存在する事実を示す証拠が~~

	~~添付されている~~

【改訂箇所】

Ⅴ．ウェブアプリケーションに係る脆弱性関連情報取扱

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

現在のPガイドライン	Pガイドライン改訂案
2）届出の受理 IPA は、以下の条件がすべて満たされていると判断した時、その時点で届出を受理し、発見者に連絡します。 （ア）上記２．4)の項目がすべて記載されていること （イ）届出内容に矛盾等が無いこと （ウ）届出の対象が本ガイドラインの適用範囲に該当すること（Ⅱ章参照） （エ）記載されている内容が脆弱性であること IPA は、以下のいずれかに該当することを確認します。 ・IPA が精査した結果、脆弱性が存在する可能性があると判断できる ・届出に脆弱性が存在する事実を示す証拠が添付されている	2）届出の受理 IPA は、届出の記載が以下の条件をすべて満たしていると判断した時、その時点で届出を受理し、発見者に連絡します。 （ア）上記２．4)の項目がすべて記載されていること （イ）届出内容に矛盾等が無いこと （ウ）届出の対象が本ガイドラインの適用範囲に該当すること（Ⅲ章を参照） （エ）記載されている内容が脆弱性であること ~~IPA は、以下のいずれかに該当することを確認します。~~ ~~・IPA が精査した結果、脆弱性が存在する可能性があると判断できる~~ ~~・届出に脆弱性が存在する事実を示す証拠が添付されている~~

(5) 法改正などを加味した記載の見直し・修正

個人情報保護法の改正に合わせ改訂した。

【改訂箇所】

Ⅴ　ウェブアプリケーションに係る脆弱性関連情報取扱

３IPA（受付機関）の対応

現在のPガイドライン	Pガイドライン改訂案
7）脆弱性関連情報の管理および開示 IPA は、脆弱性関連情報に関して、発見者・ウ	7）脆弱性関連情報の取扱い IPA は、脆弱性関連情報に関して、発見者・ウ

ェブサイト運営者以外の第三者に提供しないように適切に管理します。ただし、下記のような正当な理由がある場合は、外部機関と脆弱性関連情報を開示することがあります （略） （エ）個人情報漏えいしている恐れがあり、ウェブサイト運営者による対応がされない場合、IPA は所轄官庁に脆弱性関連情報を連絡し、個人情報保護法（平成 15 年法律第 57 号）第 34 条に基づく措置を依頼する	ェブサイト運営者以外の第三者に開示しないように適切に管理します。ただし、下記のような正当な理由がある場合は、外部機関と脆弱性関連情報を開示することがあります （略） （エ）個人情報が漏えいしている恐れがあり、ウェブサイト運営者による対応がされない場合、IPA は個人情報保護委員会に脆弱性関連情報を連絡し、個人情報保護法（平成 15 年法律第 57 号）第 42 条に基づく措置を依頼する

ガイドラインの「付録３ 法的な論点について」において、電波法 109 条の 2 に触れる可能性があるとしていた行為について従来の「無線 LAN の WEP キーの解読等」という例示は、平成 29 年 4 月 27 日　東京地裁（裁判所ウェブサイト）において「WEP 鍵は，それ自体無線通信の内容として送受信されるものではなく，あくまで暗号文を解いて平文を知るための情報であり，その利用は平文を知るための手段・方法に過ぎない。」という判決の判断中の表現をもとにすれば、その解読のみでは、電波法違反が成立しないことになるため、改訂した。

【改訂箇所】
付録 3. 法的な論点について
1. 発見者が心得ておくべき法的な論点
1－1. 脆弱性関連情報の発見に際しての法的な問題
（1）関連する行為と法令の関係

現在の P ガイドライン	P ガイドライン改訂案
b）暗号化されている無線通信の復号化 ・暗号化されている無線通信を傍受し復号する行為（無線 LAN の WEP キーの解読等）は、電波法 109 条の 2 に触れる可能性があります。	b）暗号化されている無線通信の復号化 ・暗号化されている無線通信を傍受し復号する行為（無線 LAN の WEP キーを解読して通信内容を復号すること）は、電波法 109 条の 2 に触れる可能性があります。

民事債権法（2020 年 4 月 1 日施行）改正により、瑕疵担保責任は、債務不履行のひとつの例として位置づけられて、条文自体が削除されたため、法的見解からも瑕疵担保責任の規定を削除した。

【改訂箇所】
付録 3. 法的な論点について
2　製品開発者が心得ておくべき法的な論点

現在のＰガイドライン	Ｐガイドライン改訂案
製品開発者が心得ておくべき法的な問題に関する法律専門家の見解を述べます。 (1)ソフトウエアの提供行為についていえば、セキュリティに問題が生じず、日頃の運用で安心して使えるというレベルのソフトウエアを提供することが、法律上、債務の本旨に従った履行（民法４１５条）として求められています。 （略） (a) 上記の対策方法の選択について、状況に応じて債務不履行責任（民法４１５条）、不法行為責任（民法７０９条）、瑕疵担保責任（同法５７０条、５６６条、商法５２６条１項等）の対象となる可能性があります。	製品開発者が心得ておくべき法的な問題に関する法律専門家の見解を述べます。 (1)ソフトウエアの提供行為についていえば、セキュリティに問題が生じず、日頃の運用で安心して使えるというレベルのソフトウエアを提供することが、法律上、債務の本旨に従った履行（民法４１５条）として求められています。 （略） (a) 上記の対策方法の選択について、状況に応じて債務不履行責任（民法４１５条）、不法行為責任（民法７０９条）、~~瑕疵担保責任（同法５７０条、５６６条、商法５２６条１項等）~~の対象となる可能性があります。

(6) 提供情報と漏えい概念の整理

告示では、脆弱性関連情報については、第三者が了知しうる状況について、意図した場合と意図しない場合で、「開示」と「漏えい」と用語が使い分けられている。

しかし、現在のＰガイドラインでは、用語の使い分けがなされていないため、第三者が了知しうる状況に意図的にすることを開示といい、意図しない場合を漏えいとし、用語を告示にそろえる形で改訂した。

【改訂箇所】
Ⅳ. ソフトウエア製品に係る脆弱性関連情報取扱
２．発見者の対応

現在のＰガイドライン	Ｐガイドライン改訂案
4) 脆弱性関連情報の管理および開示 発見者は、IPA および JPCERT/CC が脆弱性情報を公表するまでの間は、脆弱性関連情報が第三者に漏れないように適切に管理してく	4) 脆弱性関連情報の管理および開示 発見者は、~~IPA および JPCERT/CC が脆弱性情報を公表するまでの間は、~~脆弱性関連情報を正当な理由がない限り第三者に開示しない

ださい（発見者に対する情報非開示依頼、以下「情報非開示依頼」という）。ただし、正当な理由があって脆弱性関連情報を開示する必要がある場合には、事前に IPA に相談してください。脆弱性関連情報の管理および開示に係わる法的問題に関しては、付録３に示します。 　なお、起算日から 1 年間以上経過した届出については、発見者は IPA に対し、情報非開示依頼の取り下げを求めることができます。	でください（発見者に対する情報非開示依頼、以下「情報非開示依頼」という）。ただし、正当な理由があって脆弱性関連情報を開示する必要がある場合には、事前に IPA に相談してください。脆弱性関連情報の管理および開示に係る法的な問題に関しては、付録３を参照してください。 　なお、起算日から 1 年以上経過した届出については、発見者は IPA に対し、情報非開示依頼の取り下げを求めることができます。 　また、情報非開示依頼の効力のある間は、脆弱性関連情報が第三者に漏えいしないように適切に管理してください。

【改訂箇所】

Ⅳ. ソフトウエア製品に係る脆弱性関連情報取扱

3. IPA（受付機関）の対応

現在の P ガイドライン	P ガイドライン改訂案
5）脆弱性関連情報の取扱い 　IPA は、脆弱性関連情報に関して、それに関する脆弱性情報が一般に公表されるまでの間は、発見者・JPCERT/CC・当該製品開発者以外の第三者に提供しないように適切に管理します。ただし、脆弱性が再現する状況を特定できない等正当な理由がある場合、IPA は、秘密保持契約を結んだ上で、独立行政法人産業技術総合研究所や技術研究組合制御システムセキュリティセンター等の外部機関に脆弱性関連情報に関する技術的分析を依頼することや、関係者の許諾を得た上で、JPCERT/CC と連携し、脆弱性の再現に必要な情報を製品開発者に提供することがあります。	5）脆弱性関連情報の取扱い 　IPA は、脆弱性関連情報に関して、正当な理由がない限り発見者・JPCERT/CC・当該製品開発者以外の第三者に開示しません。ただし、以下のような正当な理由がある場合、IPA は第三者に情報を開示することがあります。なお、技術的分析を依頼する場合、IPA は秘密保持契約を結びます。 （ア）脆弱性を有するソフトウエア製品が、他のソフトウエアやウェブサイトで利用されている場合に、それらの製品開発者やウェブサイト運営者に連絡する場合 （イ）脆弱性が再現する状況を特定できない等の場合に、国立研究開発法人産業技術総合研究所や技術研究組合制御システムセキュリティセンター等の外部機関に脆弱性関連情

	報に関する技術的分析を依頼する場合 　この場合、関係者の許諾を得た上で、JPCERT/CC と連携し、脆弱性の再現に必要な情報を製品開発者に開示することがあります。 　また、IPA は、脆弱性関連情報に関して、それに関する脆弱性情報が一般に公表されるまでの間は、発見者・JPCERT/CC・当該製品開発者以外の第三者に漏えいしないように適切に管理します。

【改訂箇所】

Ⅳ. ソフトウエア製品に係る脆弱性関連情報取扱

4. JPCERT/CC（調整機関）の対応

現在の P ガイドライン	P ガイドライン改訂案
5) JPCERT/CC における脆弱性関連情報の取扱い 　JPCERT/CC は、脆弱性情報を一般に公表するまでは、第三者に漏洩しないように管理します。ただし、以下のような正当な理由がある場合、JPCERT/CC は第三者に情報を提供することがあります。 （ア）海外製品であり外国企業の日本法人や総代理店が無い場合 （イ）海外に大きな影響を与える脆弱性関連情報の場合 （ウ）脆弱性関連情報の詳細な分析が必要な場合 等 　具体的には、秘密保持契約を締結した上で、海外の調整機関または IPA を含む外部機関に連絡や分析を依頼するケースがあります。	5)脆弱性関連情報の取扱い 　JPCERT/CC は、脆弱性関連情報を~~一般に公表するまでは、~~第三者に開示しません。ただし、以下のような正当な理由がある場合、JPCERT/CC は第三者に情報を開示することがあります。 （ア）海外製品であり外国企業の日本法人や総代理店が無い場合 （イ）海外に大きな影響を与える脆弱性関連情報の場合 （ウ）脆弱性関連情報の詳細な分析が必要な場合　等 　具体的には、秘密保持契約を締結した上で、海外の調整機関または IPA を含む外部機関に連絡や分析を依頼するケースがあります。 　また、JPCERT/CC は、脆弱性情報を一般に公表するまでは、第三者に漏えいしないように管理します。

【改訂箇所】

Ⅳ. ソフトウエア製品に係る脆弱性関連情報取扱

5. 製品開発者の対応

現在のPガイドライン	Pガイドライン改訂案
9) 製品開発者内の情報の管理と開示 製品開発者は、上記 3)で作成した脆弱性情報の一般公表スケジュールおよび脆弱性関連情報を、脆弱性情報を一般に公表する日まで第三者に漏洩しないように管理してください。また、製品開発者は、正当な理由がない限り、第三者に脆弱性関連情報を開示しないでください。 ただし、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、製品開発者は、JPCERT/CC と調整した上で、直接あるいはシステム構築事業者を介して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ができます。その際、製品開発者は、通知先に対し、脆弱性情報を一般に公表するまでの間、脆弱性情報と対策方法について、第三者に漏洩しないように適切に管理することを要請してください。	9) 製品開発者内の情報の管理と開示 製品開発者は、正当な理由がない限り、第三者に脆弱性関連情報を開示しないでください。また、製品開発者は、上記 3)で作成した脆弱性情報の一般公表スケジュールおよび脆弱性関連情報を、脆弱性情報を一般に公表する日まで第三者に漏えいしないように管理してください。~~また、製品開発者は、正当な理由がない限り、第三者に脆弱性関連情報を開示しないでください。~~ ただし、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、製品開発者は、JPCERT/CC と調整した上で、直接あるいはシステム構築事業者を介して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ができます。その際、製品開発者は、通知先に対し、脆弱性関連情報を第三者に開示しないこと、および脆弱性情報を一般に公表するまでの間、脆弱性情報と対策方法について、第三者に漏えいしないように適切に管理することを要請してください。

【改訂箇所】

Ⅴ. ウェブアプリケーションに係る脆弱性関連情報取扱

2. 発見者の対応

現在のPガイドライン	Pガイドライン改訂案
3)脆弱性関連情報の管理および開示 発見者は、脆弱性が修正されるまでの間は、脆弱性関連情報が第三者に漏れないように適切に管理してください（発見者に対する情報	3)脆弱性関連情報の管理および開示 発見者は、脆弱性関連情報を正当な理由がない限り第三者に開示しないでください。ただし、正当な理由があって脆弱性関連情報を

非開示依頼、以下「情報非開示依頼」という）。ただし、正当な理由があって脆弱性関連情報を開示する場合には、事前に IPA に相談してください。脆弱性関連情報の管理および開示に係わる法的な論点に関しては、付録３に示します。	開示する場合には、事前に IPA に相談してください。発見者は、脆弱性が修正されるまでの間は、脆弱性関連情報が第三者に漏えいしないように適切に管理してください（発見者に対する情報非開示依頼、以下「情報非開示依頼」という）。~~ただし、正当な理由があって脆弱性関連情報を開示する場合には、事前に IPA に相談してください。~~脆弱性関連情報の管理および開示に係る法的な問題に関しては、付録３を参照してください。

【改訂箇所】

Ⅴ．ウェブアプリケーションに係る脆弱性関連情報取扱

4．ウェブサイト運営者の対応

現在の P ガイドライン	P ガイドライン改訂案
4） ウェブサイト運営者内での情報の管理と開示 ウェブサイト運営者は、脆弱性が修正されるまでの間は、脆弱性関連情報を第三者に漏洩しないように管理してください。また、ウェブサイト運営者は、正当な理由がない限り、第三者に脆弱性関連情報を開示しないようにしてください。ただし、ウェブサイト運営者が脆弱性修正を依頼した外部機関、およびウェブサイトの管理を委託している外部機関には、秘密保持契約を締結した上で脆弱性関連情報を連絡することを推奨します。 なお、ウェブサイト運営者は、脆弱性の修正の過程でソフトウエア製品の脆弱性であることを認識した場合、当該脆弱性情報等が公表されるまで情報を適切に管理してください。	4） ウェブサイト運営者内の情報の管理と開示 ウェブサイト運営者は、脆弱性関連情報を正当な理由がない限り第三者に開示しないでください。ただし、ウェブサイト運営者が脆弱性修正を依頼した外部機関、およびウェブサイトの管理を委託している外部機関には、秘密保持契約を締結した上で脆弱性関連情報を連絡することを推奨します。 また、ウェブサイト運営者は、脆弱性が修正されるまでの間は、脆弱性関連情報を第三者に漏えいしないように管理してください。なお、ウェブサイト運営者は、脆弱性の修正の過程でソフトウエア製品の脆弱性であることを認識した場合、脆弱性関連情報を第三者に正当な理由がない限り開示しないでください。また、当該脆弱性情報等が公表されるまで情報を第三者に漏えいしないように管理してください。

参考１

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
参加者名簿

2019 年 1 月 28 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)
	河野 省二	日本マイクロソフト株式会社
	北澤 繁樹	三菱電機株式会社
	栗田 博司	株式会社日立製作所
	小島 健司	東芝デジタルソリューションズ株式会社
	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
	土屋 昭治	富士通株式会社
	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
	油井 秀人	富士通エフ・アイ・ピー株式会社
	渡辺 研司	名古屋工業大学

（五十音順、敬称略）

オブザーバ

奥家 敏和	経済産業省 サイバーセキュリティ課長
加畑 晶規	経済産業省 サイバーセキュリティ課 課長補佐
河本 哲志	経済産業省 サイバーセキュリティ課 課長補佐
曽我部 雄太	経済産業省 サイバーセキュリティ課 総括係長
宮下 清	一般社団法人日本情報システム・ユーザー協会（JUAS）
笹岡 賢二郎	一般社団法人コンピュータソフトウェア協会（CSAJ）
鈴木 啓紹	一般社団法人コンピュータソフトウェア協会（CSAJ）
宮地 利雄	一般社団法人 JPCERT コーディネーションセンター(JPCERT/CC)
久保 啓司	一般社団法人 JPCERT コーディネーションセンター(JPCERT/CC)
中谷 昌幸	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)
伊藤 智貴	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
江口 純一	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
板橋 博之	独立行政法人情報処理推進機構
木曽田 優	独立行政法人情報処理推進機構
田中 里実	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
小林 桂	独立行政法人情報処理推進機構
天野 農	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
綿谷 謙吾	株式会社三菱総合研究所
磯江 麻里	株式会社三菱総合研究所
朱 ユーティン	株式会社三菱総合研究所

（順不同、敬称略）

参考２

脆弱性研究会の検討経緯

■研究会第 1 回会合（2018 年 10 月 18 日）
- 今年度の検討方針について
- ソフトウエア製品の脆弱性対処における実態調査および脆弱性対処の促進に関する検討について
- 調整不能案件の一覧への掲載、公表手続きの改善に向けた検討について
- 法的課題の整理について
- スケジュールについて

■研究会第 2 回会合（2018 年 12 月 17 日）
- 前回会合の確認
- ソフトウエア製品の脆弱性対処における実態調査および脆弱性対処の促進に関する検討について
- 「優先情報提供」の実績評価、提供先拡大に関する検討について
- 調整不能案件の一覧への掲載、公表手続きの改善に向けた検討について
- 法的課題の整理について
- スケジュールについて

■研究会第 3 回会合（2019 年 1 月 28 日）
- 前回会合の確認
- ソフトウエア製品の脆弱性対処における実態調査および脆弱性対処の促進に関する検討について
- 「優先情報提供」の実績評価、提供先拡大に関する検討について
- 調整不能案件の一覧への掲載、公表手続きの改善に向けた検討について
- 法的課題の整理について
- 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改訂（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