情報システム等の脆弱性情報の取扱いに関する研究会

- 2019 年度 報告書 -

2020 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 2019 年 9 月末までにソフトウエア製品及びウェブアプリケーションの脆弱性に関する届出は累計で 15,050 件に達している。パートナーシップの拠り所となる経済産業省告示は、制度発足時は「ソフトウエア等脆弱性関連情報取扱基準（2004 年経済産業省告示第 235 号改め、2014 年経済産業省告示第 110 号）」に基づいていたが、2017 年 2 月に「ソフトウエア製品等の脆弱性関連情報に関する取扱規程」（以下、「告示」という）に廃止制定された。

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

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

2020 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 及び 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 2019 年 9 月末までの IPA への脆弱性関連情報の届出件数は、ソフトウエア製品の脆弱性に関するもの 4,390 件、ウェブサイトの脆弱性に関するもの 10,660 件の計 15,050 件であった。四半期毎の届出状況を図 1-1 に示す。

	2016 4Q	2017 1Q	2Q	3Q	4Q	2018 1Q	2Q	3Q	4Q	2019 1Q	2Q	3Q
累計届出件数[件]	12,922	13,064	13,335	13,456	13,526	13,664	13,822	13,999	14,090	14,213	14,710	15,050
1就業日あたり[件/日]	4.25	4.21	4.21	4.17	4.11	4.08	4.06	4.03	3.99	3.96	4.03	4.06

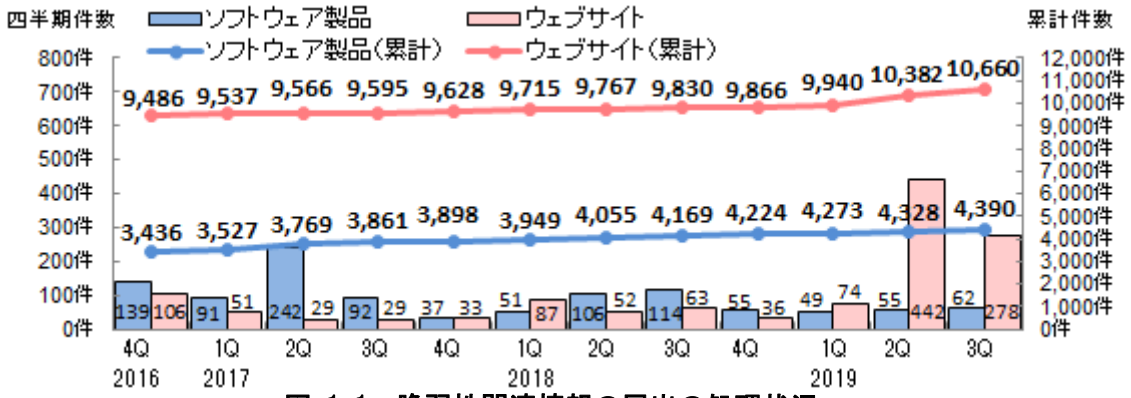
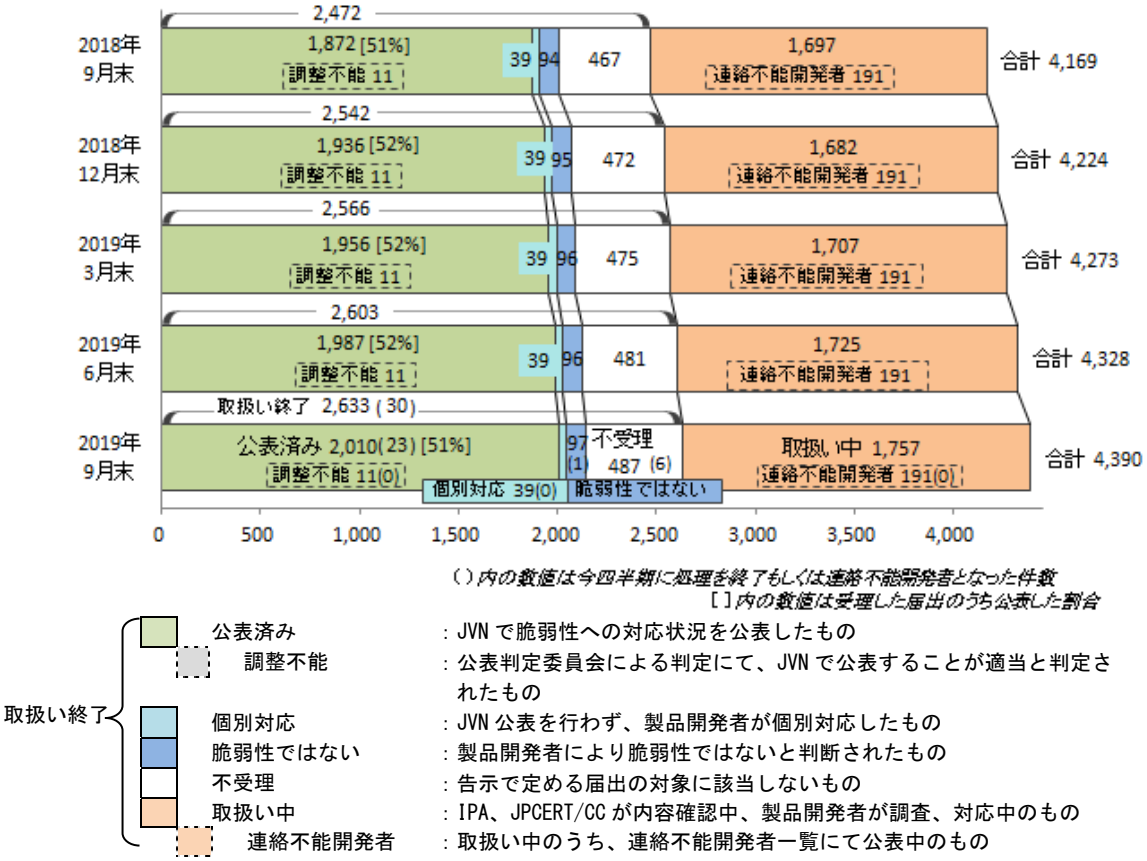


図 1-1　脆弱性関連情報の届出の処理状況

（活動報告レポート[2019 年第 3 四半期（7 月～9 月）]より抜粋）

(1) ソフトウエア製品の脆弱性

ソフトウエア製品の脆弱性関連情報届出に関する処理状況を図 1-2 に示す。



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

取扱い終了
- 公表済み：JVN で脆弱性への対応状況を公表したもの
  - 調整不能：公表判定委員会による判定にて、JVN で公表することが適当と判定されたもの
- 個別対応：JVN 公表を行わず、製品開発者が個別対応したもの
- 脆弱性ではない：製品開発者により脆弱性ではないと判断されたもの
- 不受理：告示で定める届出の対象に該当しないもの
- 取扱い中：IPA、JPCERT/CC が内容確認中、製品開発者が調査、対応中のもの
  - 連絡不能開発者：取扱い中のうち、連絡不能開発者一覧にて公表中のもの

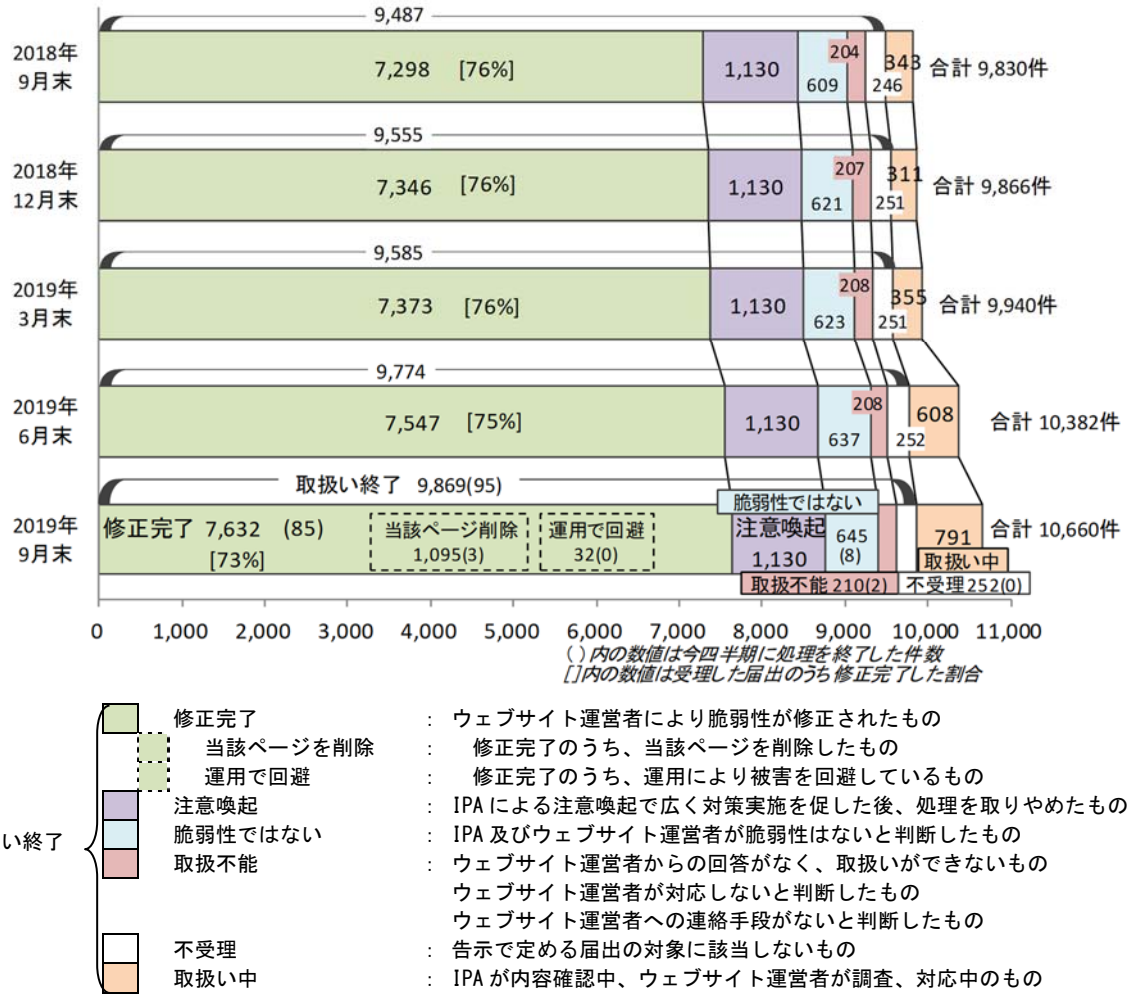
図 1-2　ソフトウエア製品の脆弱性関連情報の届出の処理状況

（活動報告レポート[2019 年第 3 四半期（7 月～9 月）]より抜粋）

ソフトウエア製品の脆弱性関連情報の届出 4,390 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 2,010 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 97 件、取扱い中のものが 1,757 件（うち連絡不能開発者として公表したものが 191 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 487 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。



取扱い終了

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

図 1-3　ウェブサイトの脆弱性関連情報の届出の処理状況

（活動報告レポート[2019 年第 3 四半期（7 月～9 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 10,660 件のうち、修正が完了したものが 7,632 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 1,095 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 及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 645 件、取扱い中のものが 791 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 210 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 252 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 2019 年 9 月末までに 3,443 件になる。

(1) 国内の発見者及び製品開発者から届出があり公表した脆弱性

2019 年 9 月末までに、国内の発見者から IPA に届出があったもの及び製品開発者自身から自社製品の脆弱性・対策方法について連絡を受けたもので、JVN において公表された脆弱性は 2,010 件である。

届出受付開始から 2019 年 9 月末までの届出について、脆弱性関連情報の届出を受理してから製品開発者が対応状況を公表するまでに要した日数を図 1-4 に示す。45 日以内に公表されている件数は全体の 29%(590 件)であり、301 日以上要しているものは 26%(513 件)を占める。

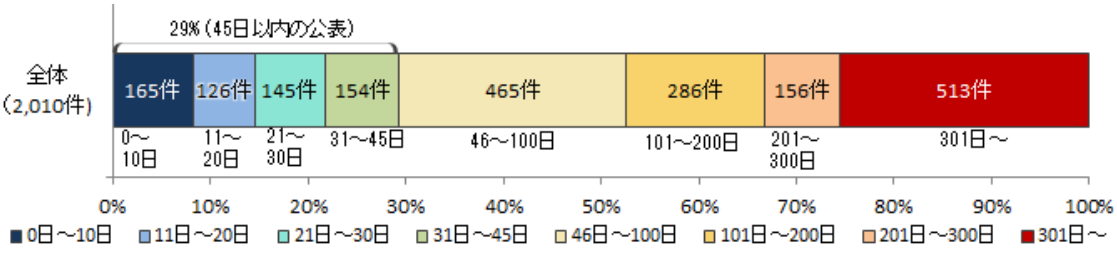


図 1-4　ソフトウエア製品の脆弱性公表までに要した日数

（活動報告レポート[2019 年第 3 四半期（7 月～9 月）]より抜粋）

(2) 海外 CSIRT 等から連絡を受け公表した脆弱性

2019 年 9 月末までに JPCERT/CC が海外 CSIRT 等と連携して JVN で公表した脆弱性情報は 1,711 件である。このうち、2019 年第 1 四半期～2019 年第 3 四半期（2019 年 1 月から 2019 年 9 月末まで）に JVN で公表した脆弱性関連情報は 62 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 2019 年 9 月末までのソフトウエア製品に関する脆弱性関連情報の届出 4,390 件のうち、不受理分を除いた 3,903 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。

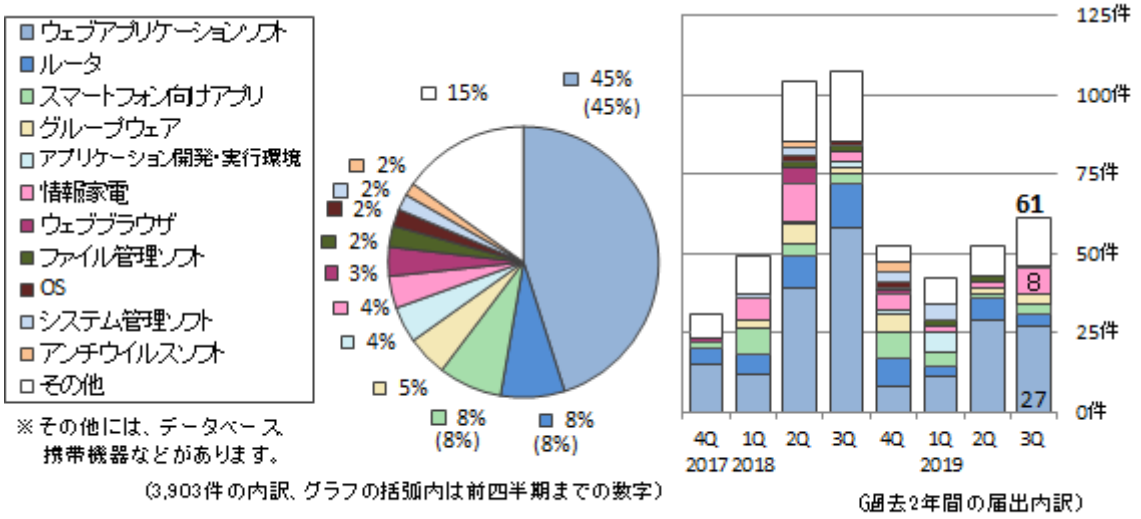


図 1-5　ソフトウエア製品種類別の届出内訳（届出受付開始～2019 年 9 月末）

（活動報告レポート[2019 年第 3 四半期（7 月～9 月）]より抜粋）

(4) 脆弱性の原因別の内訳

届出受付開始から 2019 年 9 月末までのソフトウエア製品に関する脆弱性関連情報の届出 4,390 件のうち、不受理分を除いた 3,903 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 57%を占める。

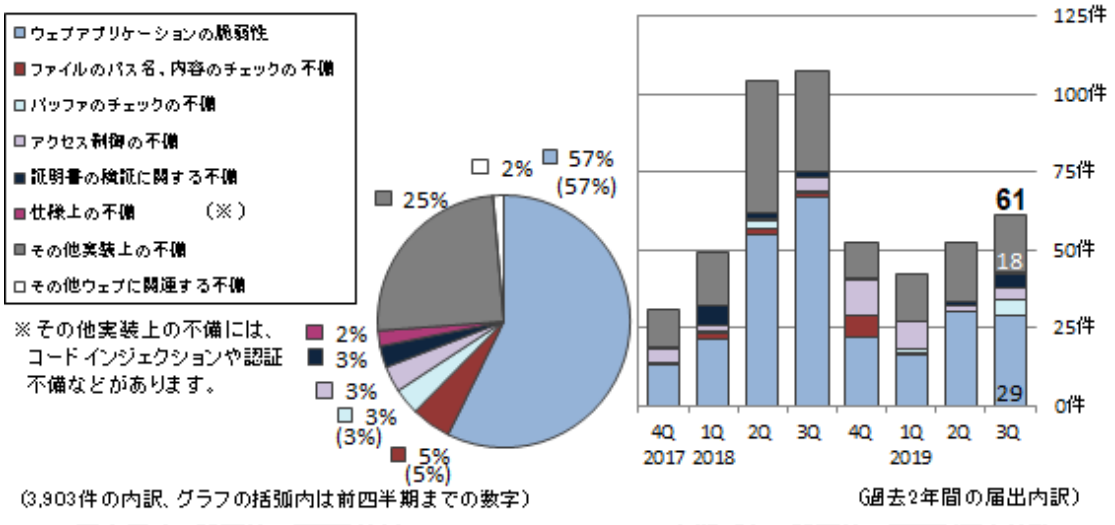


図 1-6　ソフトウエア製品の脆弱性原因別の届出内訳（届出受付開始～2018 年 12 月末）

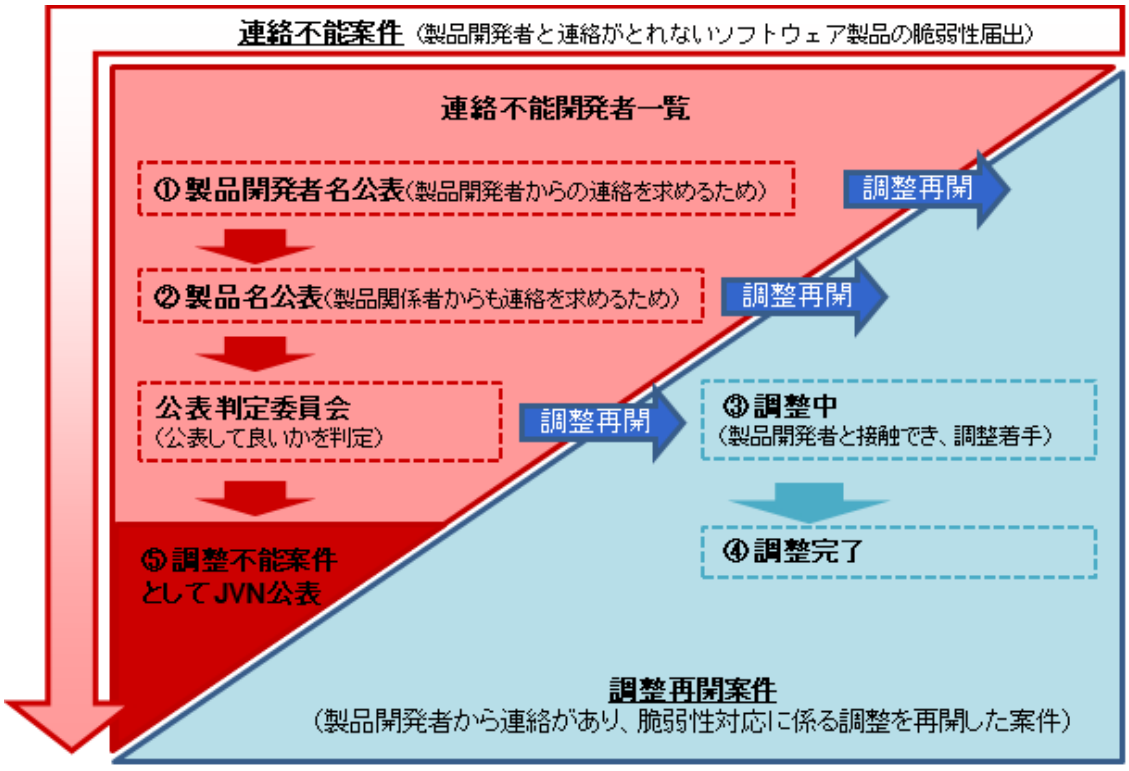
（活動報告レポート[2019 年第 3 四半期（7 月～9 月）]より抜粋）

(5) 優先情報提供の実施状況

2018 年 4 月から、脆弱性による国民の日常生活に必要不可欠なサービスへの被害を低減するために、これらのサービスを提供する重要インフラ事業者 に対して脆弱性対策情報を JVN 公表前に優先的に提供している。2019 年第 1 四半期から第 3 四半期に優先情報提供したものは電力分野 1 件で、累計では 3 件（電力分野 2 件、政府機関 1 件）でした。

(6) 連絡不能案件の処理状況

連絡不能開発者一覧の公表開始（2011 年 9 月 29 日）から 2019 年 9 月末までに公表した連絡不能開発者の件数は累計 251 件、うち 49 件が調整を再開（その中の 26 件が調整完了）したが、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）。



2019年 第2四半期	191件 （①1件 ②190件）	49件 （③23件 ④26件）	⑤11件	合計 251件
2019年 第3四半期	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～2019 年 9 月末）

（活動報告レポート[2019 年第 3 四半期（7 月～9 月）]より抜粋）

1.2.3. ウェブサイトの脆弱性関連情報の届出の内容

(1) 修正された脆弱性の内容

2019 年 9 月末までに届出されたウェブサイトの脆弱性のうち修正の完了した 7,632 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 48%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。

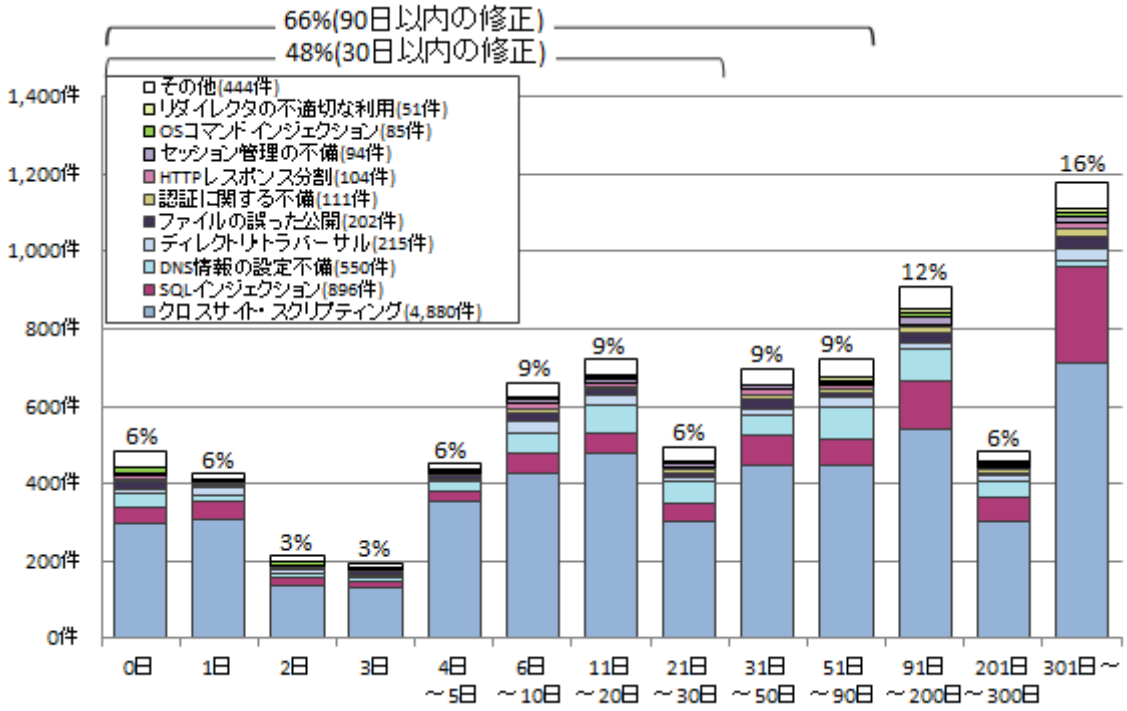


図 1-8　ウェブサイトの脆弱性修正に要した日数（届出受付開始～2019 年 9 月末）

（活動報告レポート[2019 年第 3 四半期（7 月～9 月）]より抜粋）

(2) 届出の脆弱性種類別内訳

2019 年 9 月末までに IPA に届出のあったウェブサイトに関する脆弱性関連情報の届出 10,660 件のうち、不受理のものを除いた 10,408 件の種類別内訳を図 1-9 に示す。脆弱性の種類は依然として「クロスサイト・スクリプティング」(58%)、「DNS 情報の設定不備」(13%)、「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 82%を占める。

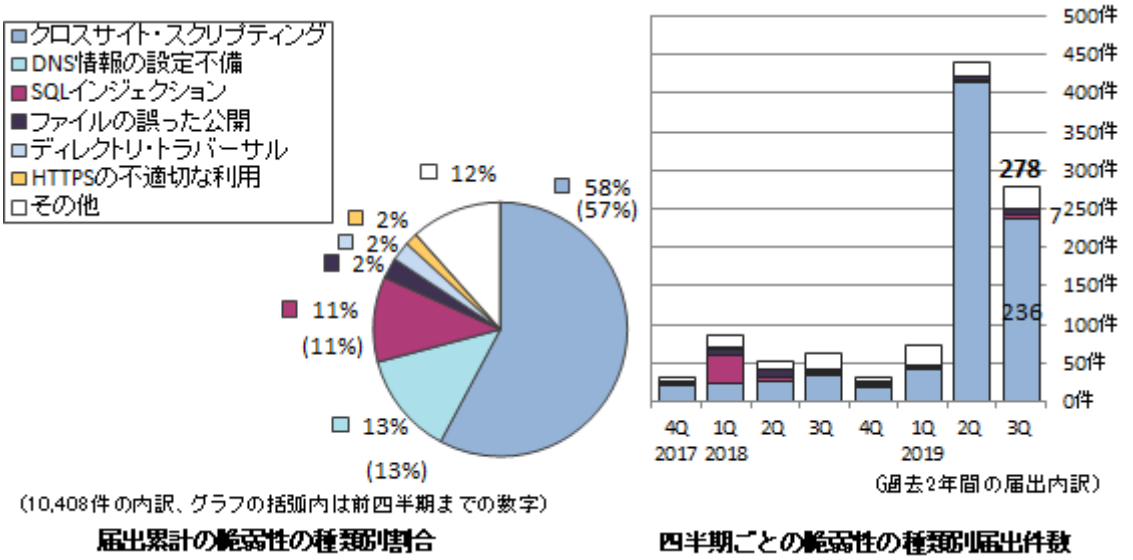


図 1-9　ウェブサイトの脆弱性種類別内訳（届出受付開始～2019 年 9 月末）

（活動報告レポート[2019 年第 3 四半期（7 月～9 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」(56%)、「ドメイン情報の挿入」(13%)、「データの改ざん、消去」(11%) の割合が高い。

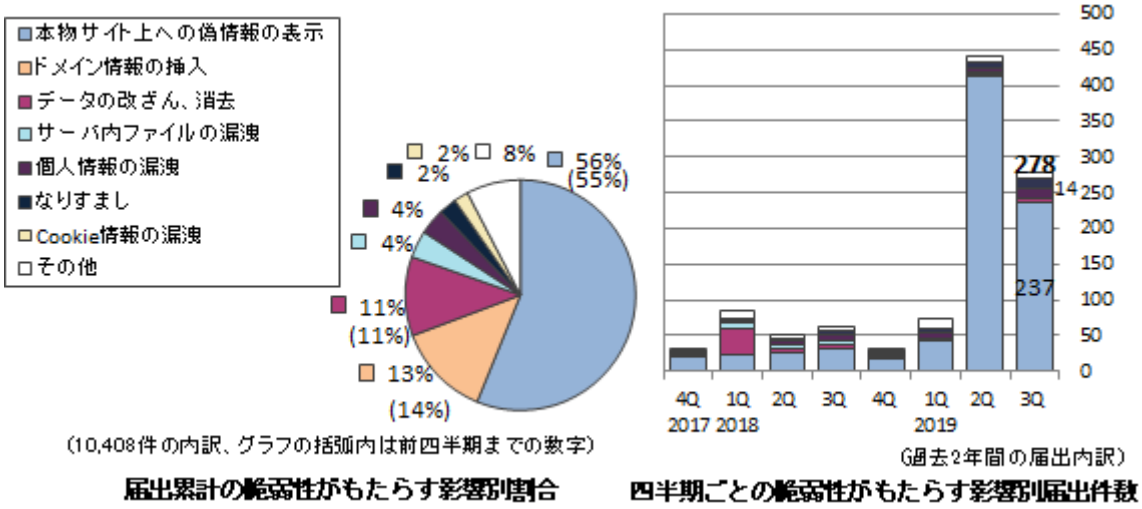


図 1-10　ウェブサイトの脆弱性影響別内訳（届出受付開始～2019 年 9 月末）

（活動報告レポート[2019 年第 3 四半期（7 月～9 月）]より抜粋）

(4) 取扱の状況

ウェブサイトの脆弱性関連情報のうち、取扱いが長期化（IPA からウェブサイト運営者へ脆弱性関連情報を通知してから、90 日以上脆弱性を修正した旨の報告が無い）しているものに関する経過日数別の件数を図 1-11 に示す。経過日数が 90 日以上である件数は 297 件で、前年同期（279 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 21%を占めており、対策の実施が望まれる。

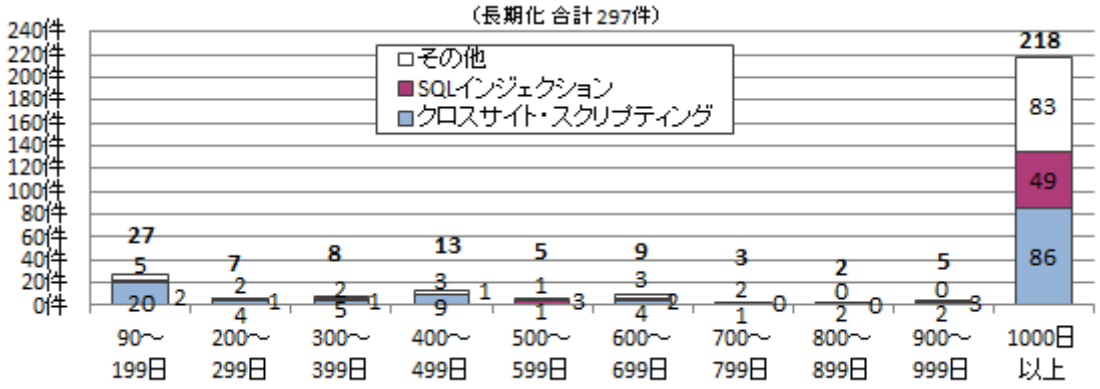


図 1-11 取扱いが長期化(90 日以上経過)しているウェブサイトの経過日数と脆弱性の種類

（活動報告レポート[2019 年第 3 四半期（7 月～9 月）]より抜粋）

1.3. 本年度研究会における検討

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 4 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 ソフトウェア製品の脆弱性対処促進に関する調査
② 一般消費者のリテラシー向上に関する調査
③ サポート終了製品のパートナーシップにおける取扱いに関する調査
④ 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」2018 年度報告書

2. ソフトウェア製品の脆弱性対処促進に関する調査

2.1. 調査の概要

2.1.1. 調査目的

ソフトウェア製品の脆弱性対処について、製品開発者としての責務（望ましい対処）であることを認識させるべく普及啓発を実施しているが、中小企業ではリソース不足等の理由により網羅的に対処することは困難な場合がある。さらに、一般消費者向け製品は価格や機能ばかりが競争要素となっているため、製品開発者が望ましい対処をしても一般消費者によるソフトウェア製品選定の動機づけや競争要素とならないため、脆弱性対処が製品開発者の利益に繋がり辛い。このことから、脆弱性対処への予算が充てられず対処が促進されない状況にあると推測される。

このため、最低限の対処を促進するために望ましい対処の優先度付け及び望ましい対処を実施するための体制や手順、想定されうる課題への対処方法をこれまでの脆弱性研究会での調査結果も踏まえて検討する。さらに、望ましい対処をしているソフトウェア製品が一般消費者から評価されるために対処状況を開示(アピール)する方法を検討する。

調査結果は、「製品開発者における望ましい脆弱性対処・公表に関する調査結果報告書」として取り纏めると共に、「製品開発者向けガイド」を策定する。また、「製品開発者向けガイド」の普及手段及び効果測定方法を取り纏めた資料「普及手段と効果測定方法」の作成、普及啓発に必要な資料「普及促進資料」を作成する。

2.1.2. 調査方法

製品開発者による脆弱性対処に関して、望ましい対処項目及びその開示方法について、文献/事例の調査結果やこれまでの脆弱性研究会報告書を踏まえて、「製品開発者における望ましい脆弱性対処・公表に関する調査結果報告書」として取り纏める。

文献調査結果を踏まえて、後述する「製品開発者向けガイド」の普及手段(普及に協力頂ける他組織、掲載場所、掲載方法、媒体等)及び効果測定方法について検討し、検討結果を資料「普及手段と効果測定方法」として取り纏める。

「製品開発者向けガイド」及び「普及手段と効果測定方法」についてのヒアリング調査を実施する上での具体的な実施時期、対象者、調査項目について「ヒア

リング実施概要」として資料を取り纏める。
　ヒアリング調査を実施するために、「ヒアリング対象者向け主旨説明」資料を作成する。
　文献／事例の調査結果を基にして、「製品開発者向けガイド（骨子）」を作成し、ヒアリング調査の結果を踏まえ、「製品開発者向けガイド（骨子）」を見直し、「製品開発者向けガイド」として取り纏める。

　本調査の調査方法は以下に示す。

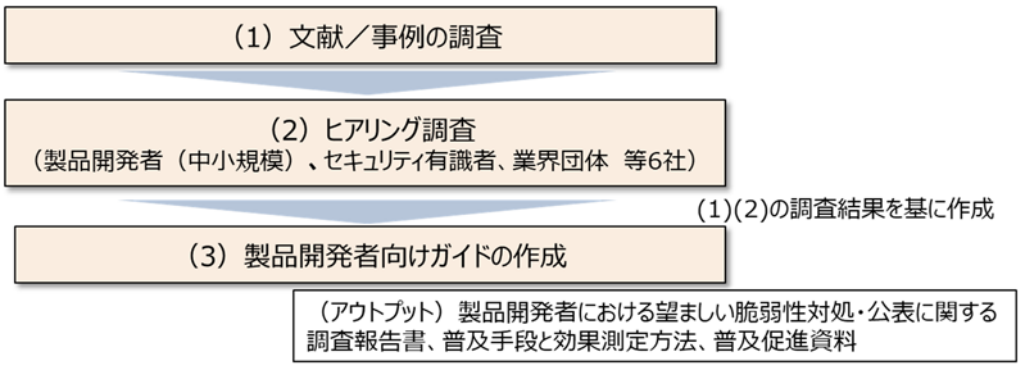


図 2-1　調査方法

2.2. 調査結果

2.2.1. 文献／事例の調査

　文献／事例調査の結果を以下に示す。

(1) 調査概要

　文献／事例調査の概要は以下の通りである。

［調査対象と件数］

　これまでの脆弱性研究会での調査結果を踏まえ、下記のような文献を 10 件以上調査する。

- ISO 等の世界標準規格
- 国内外の政府機関・セキュリティ団体が公開する資料
- 業界団体が公開する資料
- 国内外の製品開発者による望ましい脆弱性対処と開示事例　等

［調査項目］

- 望ましい対処項目を実施する上での阻害要因・課題
- 望ましい対処項目及び優先度

- 望ましい対処項目が実施できない場合の代替策
- 望ましい対処項目の対応状況の開示方法
- 望ましい対処を実施するための体制や手順
- 望ましい対処を阻害する想定課題への対処方法　等

(2) 調査対象

以下の文献について調査を実施した。

表 2-1　文献調査の対象

No.	文献名	記載内容
1	SP 800-40 ver.3, Creating a Patch and Vulnerability Management Program	パッチ及び脆弱性管理プログラムの策定
2	NISTIR 8228, Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks (2019)	IoT 機器により生じるサイバーセキュリティとプライバシーリスクを軽減するための対策例
3	IOTSF (IoT Security Foundation), IoTSF Vulnerability Disclosure Best Practice Guidelines	脆弱性開示のベストプラクティス
4	NIST Small Business Information Security: The Fundamentals	中小企業向けサイバーセキュリティ対策 ※利用者の観点から開発者への要求事項を抽出
5	NISTIR 8259 (DRAFT) Core Cybersecurity Feature Baseline for Securable IoT Devices: A Starting Point for IoT Device Manufacturers	IoT 機器のセキュリティに関するベースライン、考え方、根拠
6	CARNEGIE MELLON UNIVERSITY, The CERT® Guide to Coordinated Vulnerability Disclosure	脆弱性発見時の望ましい報告内容
7	UK DCMS, Code of Practice for consumer IoT security	消費者向け IoT セキュリティに関する 13 項目のベストプラクティス
8	ETSI TS 103 645 CYBER, Cyber Security for Consumer Internet of Things	IoT 機器の最低限のセキュリティ要件

No.	文献名	記載内容
9	経済産業省「サイバーフィジカルセキュリティ対策フレームワーク」	セキュリティの観点から、バリュークリエイションプロセスにおけるリスク源を整理するためのモデル（三層構造と 6 つの構成要素）
10	CSAJ セキュリティ委員会 制度 WG「プロダクト脆弱性対策・対応成熟度シート Version 1.0」	25 のフレームワークを元にした成熟度
11	Draft NISTIR 8267 Security Review of Consumer Home Internet of Things (IoT) Products	家庭用の IoT デバイスのセキュリティ機能の技術的レビュー結果
12	Internet of Things (IoT) Security Policy Platform Statement	各ステークホルダーが構築する IoT セキュリティに関する共通の原則（principles）

なお、ISO/IEC 29147:2018 及び ISO/IEC 30111:2019 の国際標準については、参照は行ったが、ガイド記載事項への反映としては、より具体的な記載のある文献を優先した。

(3) その他、参考文献

IPA が発行する関連文献も参考とした。

表 2-2　IPA が発行する関連文献

No.	文献名	記載内容
13	IPA「つながる世界の開発指針」	IoT 製品の開発者が開発時に考慮すべきリスクや対策
14	IPA「IoT 開発におけるセキュリティ設計の手引き」	IoT 機器及びその使用環境で想定されるセキュリティ脅威と対策
15	IPA「つながる世界のセーフティ＆セキュリティ設計入門」	経営者への啓発、現場の技術者へのセーフティ設計・セキュリティ設計の入門ガイド
16	IoT 推進コンソーシアム・総務省・経済産業省「IoT セキュリティガイドライン ver1.0」	IoT 機器やシステム、サービスについて、セキュリティ確保の観点から求められる基本的な取組

No.	文献名	記載内容
17	IPA「IoT 製品・サービス脆弱性対応ガイド」	経営者・管理者向け、企業が実施すべき IoT 脆弱性対策のポイント

(4) 調査結果

調査結果については、「製品開発者向けガイド」作成の参考とする。

2.2.2. ヒアリング調査

ヒアリング調査の結果を以下に示す。

(1) 調査概要

ヒアリング調査の概要は以下の通りである。

文献／事例調査で取り纏めた調査結果の資料を踏まえて、今回策定する「製品開発者向けガイド」の普及手段(普及に協力頂ける他組織の調査、掲載場所、掲載方法、媒体等)及び効果測定方法について検討し、検討結果を資料「普及手段と効果測定方法」として取り纏める。

このため、今回策定する「製品開発者向けガイド」及び「普及手段と効果測定方法」についてのヒアリング調査を実施し、「ヒアリング調査結果」として取りまとめるとともに、ヒアリング調査結果を踏まえ、「普及手段と効果測定方法」の資料を見直す。さらに、普及啓発に必要な資料「普及促進資料」を作成する。

(2) 調査対象

以下の対象について調査を実施した。

調査対象	＜製品開発者（中小規模）＞ ● 4 社 ＜セキュリティ有識者＞ ● 4 者（うち 1 者は団体からの紹介） ＜業界団体＞ ● 1 団体
実施時期	2019 年 11 月～2020 年 1 月
調査項目	● 総論（「製品開発者向けガイド」の内容の妥当性） ● 望ましい対処ができない理由、課題 ● 課題の解決方法 ● 望ましい対処項目の対応状況の開示方法 ● 効果的な普及手段　等

(3) 調査結果

ヒアリング調査の結果得られた主な意見は以下の通りであった。

表 2-3　ヒアリング調査結果（製品開発者向けガイド）

No	項目	コメント	コメント者	対応内容
1	① ガイドの 妥当性	「最低限実施」、「推奨」などのクラス（レベル）を分けて提示したほうが良い。	開発者	レベル分け可能なものについては下記の難易度を想定し記載した。 レベル 1：最低限実施すべき事項 レベル 2：実施することが望ましい事項 レベル 3　：実施することが理想的な実施事項
2		「6.既知の脆弱性解消」では、どのような情報源があるのかの例を示すべきではないか。	開発者	JVN iPedia の情報を脚注として記載し、既知の脆弱性情報の収集手段、対策方法について記載した。
3		デフォルトパスワードについては、「共通のデフォルトパスワード」が問題であるため、ガイドにはその旨を記載してほしい。	有識者	「4 セキュリティを確保するための設計」の実施内容の補足として、セキュリティ機能を搭載するだけではなく、設定についても、初期状態の時点から安全な設定にすることも考慮する様に記載した。
4		本来やるべきこと、「ここだけは守らないと」という認識を持ってもらうために、重要な項目をピックアップして記載してほしい。	有識者	文献調査等を元に、重要なものとして 12 項目をピックアップした。
5		セキュリティに関する問い合わせがあった場合には、窓口担当者だけで対応すると誤った回答をすることが懸念されるため、開発部門等を含め組織として回答することが重要である。	開発者	「3 製品セキュリティを維持するための体制と管理」において、誤った回答をしないように窓口担当者だけで対応せず、開発部門等に事前に確認・相談のうえ回答する旨を記載した。
6		作成したポリシーが放置されないように、ポリシーが大事である理由を分かってもらえるガイドにする必要がある。	開発者	ポリシーが軽視されないよう実施内容で遵守状況の確認と是正及び法令等や社会要請の変化に応じて見直しを実施することを記載した。

No	項目	コメント	コメント者	対応内容
7	① ガイドの 妥当性	外部から製品を調達する場合にも当ガイドが適切に機能するように、セキュリティを前提とした製品開発というより、製品自体のセキュリティチェックにも配慮したガイドが必要なのではないか。	開発者	「6 既知の脆弱性解消」に調達製品に対しても脆弱性に関して確認・対処を実施する旨を記載した。
8		実施しなかった場合の懸念点は書かないのか。欄外に過去事例などして掲載してもよいのではないか。	開発者	「意義」に実施しなかった場合の懸念点を記載。過去事例については掲載しないと判断をした。
9		開発者が経営者向けに説得する材料として使えるとよい。	有識者	経営者向けに、エグゼクティブサマリを記載した。
10		OSS は普及が進んでいるが、高リスクなので、それを使用して開発している企業に推奨する体制が掲載されているとよい。使用するツール等の情報源も提示されているとよい。	開発者	本指摘については、ガイドへの反映は難しいため、今後の検討課題とする。
11		ガイドとして、一般的な実施推奨テストが示されていると望ましい。ガイドにテスト項目が掲載されていれば、社内で実施して適正判断ができるだろう。	開発者	本指摘については、ガイドへの反映は難しいため、今後の検討課題とする。
12	② 記載されている対処項目ができない理由	リリース後の経過期間に関わらず、利用者からの問合せに対応している現状を考慮すると、サポート期限を企業が言及することも、利用者に理解してもらうこともかなり困難であると考えている。	開発者	文献調査の結果を踏まえ「2 セキュリティサポート方針の明示」に記載はするが、レベル分けをして記載することで可能な範囲から対応できるようにする。また、消費者ガイドにおいては、確認事項として記載し、一般消費者に確認を促す。併せて、サポート終了期限を定めることの意義や必要性について普及啓発を実施することを検討する。
13		利用者の問合せがあれば対応している現状から、新たな脆弱性を作り込まない、脆弱性の継続的な監視等はどこまでできるのか。ずっと監視を続けるのは厳しい。	有識者	レベル分けをして記載することで可能な範囲から対応できるようにする。

No	項目	コメント	コメント者	対応内容
14	② 記載されている対処項目ができない理由	一般的なお客様対応窓口に脆弱性情報が報告されても、窓口担当者が一般的なお問い合わせと誤認してしまい、組織内の脆弱性対応部署まで情報が展開されないことが懸念される。	有識者	「11 脆弱性報告の受付・対策情報の公表」に第三者によって発見された脆弱性の報告受付から情報展開及び脆弱性の対応までの実施手順を記載した。
15		ファームウェアにデジタル署名をデフォルトで一律に入れることは難しい。	業界団体	一律に対応を求めるのではなく、製品の特性等を考慮して判断するよう記載した。
16		委託先の企業が存続できなくなってしまうようなケースもあるため、自社では対応したいと思っていても、対応しきれなくなる可能性がある。	業界団体	セキュリティサポート方針の策定にあたって、サプライチェーンについても考慮要素となることを記載した。
17		ライフサイクルに関して（レベルを分けるとすれば）、サポート期間の明示がレベル3、サポートができない旨を注意喚起やユーザに告知すること（レベル 3 の代替案）がレベル2、誰でもできる案内はレベル1であろう。 レベル１には対応必須としても、全企業が対応できるかは不明。	開発者	レベル分けの際の参考とする。
18	③ ②で挙げられた対処ができない理由に対する解決方法や代替手段	自動アップデートを推奨すべきという方向は共通認識になりつつある。自動アップデートはオン/オフできるが、説明書を読まないとデフォルトはオン。自動アップデートがオフになっている場合にも、大半のケースで通知は存在していることを理解いただいた上で検討してほしい。	開発者	「自動アップデート」を推奨しつつも、製品の性質等を踏まえてアップデート方法を選択するものとして記載した。
19		EOS 以降サポート（保証）を求めないように（規制が）できるなら、メーカーとしてはありがたい。EOS まで十分な保証が行える。	有識者	今後の検討課題とする。
20		情報が一般に伝播する前に対策が取れるよう、危険な情報が日々掲載される（最低限これだけ見ておけばよい）サイトがあるとよい。	有識者	一般公表前の脆弱性情報を含めたポータルサイトの作成については、今後の国の検討課題とする。

No	項目	コメント	コメント者	対応内容
21	④ 対処項目の開示状況や開示方法	量販店の製品はパッケージに商品説明が記載されているものが一般的だが、EC 用は（デザイン重視のため）パッケージに何も書かれていない製品も存在している。	開発者	「2 セキュリティサポート方針の明示」で、記載場所はパッケージに限らず「ウェブサイト等」として記載した。
22		ポリシーには何を書くべきかを説明する必要がある。	業界団体	「1 製品セキュリティポリシーの策定」において例示を記載した。
23		社内でポリシーを持つのは重要。各社それぞれのポリシーがあるので、ライフサイクル何年と決定するのでなく、ライフサイクルに関するポリシーを決め、そのポリシーを守ってサプライチェーンなどを適用していくのがよい。	業界団体	セキュリティサポート方針の策定にあたって、サプライチェーンについても考慮要素となることを記載した。

(4) 普及手段と効果測定方法

ヒアリング調査の結果等を踏まえ、「製品開発者向けガイド」の普及手段及び効果測定方法について検討を行った。

「製品開発者向けガイド」の普及手段及びガイドの内容がどれだけ認知（理解）されたか、適用されたかについての効果測定方法を検討する。

「製品開発者向けガイド」の普及手段は以下の通り。

普及に協力いただける他組織	業界団体	SIer・製品ベンダ	セミナー・研修事業者	セキュリティベンダ	ITメディア系Webサイト	IPAが参加するイベント・セミナー
普及対象	• 製品開発者（会員）	• 製品開発者（取引先）	• 製品開発者（受講者）	• 製品開発者（サービス提供者）	• 製品開発者	• 製品開発者
場所	• Webサイト（電子ファイル掲載） • イベント等	• 取引、契約等の連絡時	• セミナー・研修	• セキュリティサービス提供時	• Webサイト	• イベント会場
方法	• パンフの配布 • ガイドの掲載 • ガイドの配布・紹介	• パンフの配布 • ガイドの配布	• パンフの配布 • ガイドの配布	• パンフの配布 • ガイドの配布	• 寄稿 • ガイドの掲載	• パンフの配布 • ガイドの配布
媒体	• 電子ファイル • 紙媒体	• 電子ファイル • 紙媒体	• 紙媒体	• 紙媒体	• 電子ファイル	• 紙媒体

図 2-2「製品開発者向けガイド」の普及手段

これらの普及手段を活用した、「製品開発者向けガイド」の効果測定方法については以下の通り。

① ヒアリング調査：協力組織に対して、「利用目的」や「利用後の評価」についてヒアリング調査を行う。
② 専用のアンケート調査：業界団体会員、セミナー・研修等受講者、ベンダ等に対して、 「利用目的」や「利用の可能性」及び「利用されない理由（不足している内容等）」についてアンケート調査を行う。
③ チェックリストダウンロード者への簡易アンケート調査：チェックリストファイルをダウンロードする際に、簡易的なアンケートを行い、「利用目的」などを確認する。さらに、連絡用のメールアドレスを登録し（ダウンロードしたチェックリストがバージョンアップした際の案内等も実施）、更新時に 「利用後の評価」、「次回バーションアップに期待すること」などのアンケート調査を行う。

普及に協力いただける他組織		業界団体	SIer・製品ベンダ	セミナー・研修事業者	セキュリティベンダ	ITメディア系Webサイト	IPAが参加するイベント・セミナー
方法		• パンフの配布 • ガイドの掲載 • ガイドの配布・紹介	• パンフの配布 • ガイドの配布	• パンフの配布 • ガイドの配布	• パンフの配布 • ガイドの配布	• 寄稿 • ガイドの掲載	• パンフの配布 • ガイドの配布
媒体		• 電子ファイル • 紙媒体	• 電子ファイル • 紙媒体	• 紙媒体	• 紙媒体	• 電子ファイル	• 紙媒体
効果測定手法	①ヒアリング調査（サンプリング）	–	○	○	○	–	–
	②専用のアンケート調査	○ 会員向け	–	○ 事業者向け/受講者向け	○ 事業者向け	–	–
	③チェックリストダウンロード者への簡易アンケート調査	○	○	○	○	○	○

図 2-3「製品開発者向けガイド」の効果測定方法

ヒアリングの結果得られた「製品開発者向けガイド」の普及啓発に関する意見と対応方針は以下の通り。

コメント者	得られた意見	対応方針
有識者	個別項目を開示されても利用者からしても厳しい。開示すべき項目については、認証プログラム（認証マーク等）のようにわかりやすい仕組みが必要ではないか。	認証は何に対する保証なのか明確にすべきとの研究会での意見があり、今後の社会動向や関係者のニーズ等、状況を見極めていく。
有識者	IPA の SECURITY ACTION セキュリティ対策自己宣言のような形式も考えられるのではないか。	
開発者	第三者の基準（お墨付き）があると助かる。	
業界団体	EoL/EoS について記載するのはよいが、業界としてそれを参考に EoL 等を設定する動きになっていくかどうかはわからない。	関連団体と意見交換をしながら、より適切な普及啓発に努める。

コメント者	得られた意見	対応方針
開発者	「家庭のネットは自分で守る」というような啓発も必要ではないか。	次年度以降、家電量販店等にも協力を依頼し、普及啓発資料を用いて啓発を行う。
開発者	普及のアプローチ先はプレスがあり、全国に広める場合は自治体なども考えられる。	次年度の普及啓発の状況を踏まえ、対象範囲を拡大していく。
開発者	大学生がベンチャーを起業することも考えると、大学に配布することも考えられるだろう。	次年度の普及啓発の状況を踏まえ、対象範囲を拡大していく。

普及啓発に必要な資料として、ガイドの特徴や概要、活用方法等をとりまとめた。

2.2.3. 製品開発者向けガイドの作成

「製品開発者向けガイド」において採り上げる項目（骨子）は、文献／事例調査結果を基にして作成した。骨子は、ヒアリング結果や脆弱性研究会での意見を踏まえ見直し、「製品開発者向けガイド」として取り纏めた。

「製品開発者向けガイド」の作成にあたり、以下の事項について考慮した。

- 製品開発者にとって分かり易い内容で作成する
- 表紙等についてはデザイナーに依頼をして作成する
- ウェブページでの公表及び冊子化しての配布等をすることを前提として資料を作成する

(1) 記載事項の検討

「製品開発者向けガイド」において採り上げる項目は、文献調査において選定した文献に記載があり、ガイドの対象とする中小規模の製品開発者にとって有用な項目とする。

具体的な項目は以下の通りとする。

エグゼクティブサマリ
概要
　背景
　本ガイドについて
　対象製品
　想定読者
　本ガイドの構成
　活用方法

Ⅰ. 方針・組織
　1. 製品セキュリティポリシーの策定
　2. セキュリティサポート方針の明示
　3. 製品セキュリティを維持するための体制と管理

Ⅱ. 設計・開発
　4. セキュリティを確保するための設計
　5. アップデートを考慮した設計
　6. 既知の脆弱性解消
　7. セキュアコーディング

8. 開発環境のセキュリティ確保
9. 開発時の脆弱性検査

Ⅲ. 出荷後の対応
10. 製品と構成要素の脆弱性監視
11. 脆弱性報告の受付・対策情報の公表
12. 一般消費者の製品利用時における実施事項の明示

Ⅳ. 一般消費者に向けて実施すべきこと
一般消費者へ開示すべきこと

用語集

附属：主要な関係者・役割表
別紙：製品開発者向けガイド　チェックリスト

(2) 製品開発者向けガイド

以上の検討に基づき、別紙の通り「製品開発者向けガイド」を作成した。

3. 一般消費者のリテラシー向上に関する調査

3.1. 調査の概要

3.1.1. 調査目的

ソフトウェア製品の脆弱性対処に関して製品開発者が望ましい対処と開示等を行った場合でも、一般消費者のセキュリティに関するリテラシーが低い場合は、脆弱性対処がなされている製品が選定されない。また、安全な製品利用(適切な設定やパッチ適用など)がされていない状況にある。これにより、脆弱性が放置された状態で利用されているソフトウェア製品が多数存在すると推察される。

本調査では、一般消費者が安全なソフトウェア製品等を選定するための確認事項及びソフトウェア製品等を購入後に安全に利用するために必要な対応事項を検討する。

検討結果から、「一般消費者向けガイド」として「一般消費者向けガイド(ネット接続製品の安全な選定)」と「一般消費者向けガイド(ネット接続製品の安全な利用)」の 2 つを策定する。また、「一般消費者向けガイド」の普及手段及び効果測定方法を取り纏めた資料「普及手段と効果測定方法」の作成、普及啓発に必要な資料「普及促進資料」を作成する。

3.1.2. 調査方法

「ソフトウェア製品の脆弱性対処促進に関する調査」を基に、一般消費者が安全なソフトウェア製品を選定するための確認事項について「一般消費者向けガイド（ネット接続製品の安全な選定)」として取り纏める。

ソフトウェア製品購入後に安全に利用するために必要な対応事項についての調査結果を踏まえ、「一般消費者向けガイド（ネット接続製品の安全な利用)」として取り纏める。

「一般消費者向けガイド」の作成にあたり、以下の事項について考慮する。

- 一般消費者にとって分かり易い内容で作成する
- 一般消費者に手に取って頂ける様に、全体構成やイラスト等についてはデザインに配慮して作成する
- ウェブページでの公表及び冊子化しての配布等をすることを前提として資料を作成する

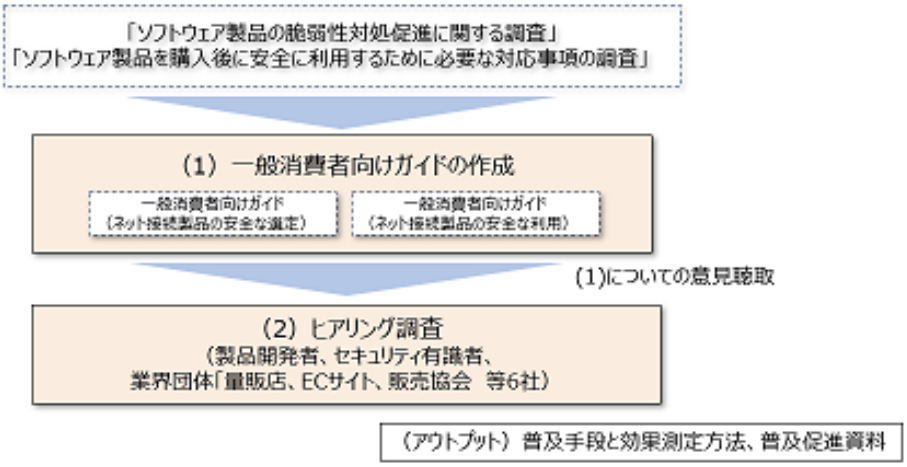


図 3-1　調査方法

3.2. 調査結果

3.2.1. 一般消費者向けガイドの作成

調査の結果を以下に示す。

(1) 一般消費者向けガイド（ネット接続製品の安全な選定）

「一般消費者向けガイド（ネット接続製品の安全な選定）」において採り上げる項目は、以下の通り。選定時に確認可能な内容とし、一般消費者による安全な製品選定を可能とする。

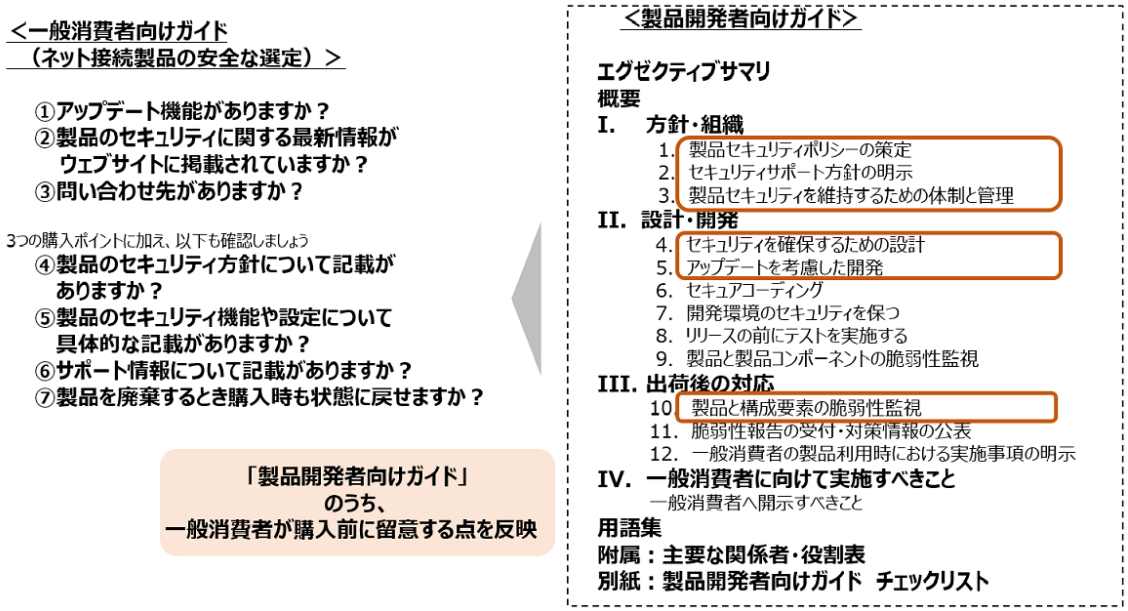


図 3-2「一般消費者向けガイド（ネット接続製品の安全な選定）」の項目

以上の検討に基づき、別紙の通り「一般消費者向けガイド（ネット接続製品の安全な選定）」を作成した。

(2) 一般消費者向けガイド（ネット接続製品の安全な利用）

「一般消費者向けガイド（ネット接続製品の安全な利用）」において採り上げる項目は、以下の通り。利用時に認識・実施可能な内容とし、一般消費者による製品の安全な利用を可能とする。

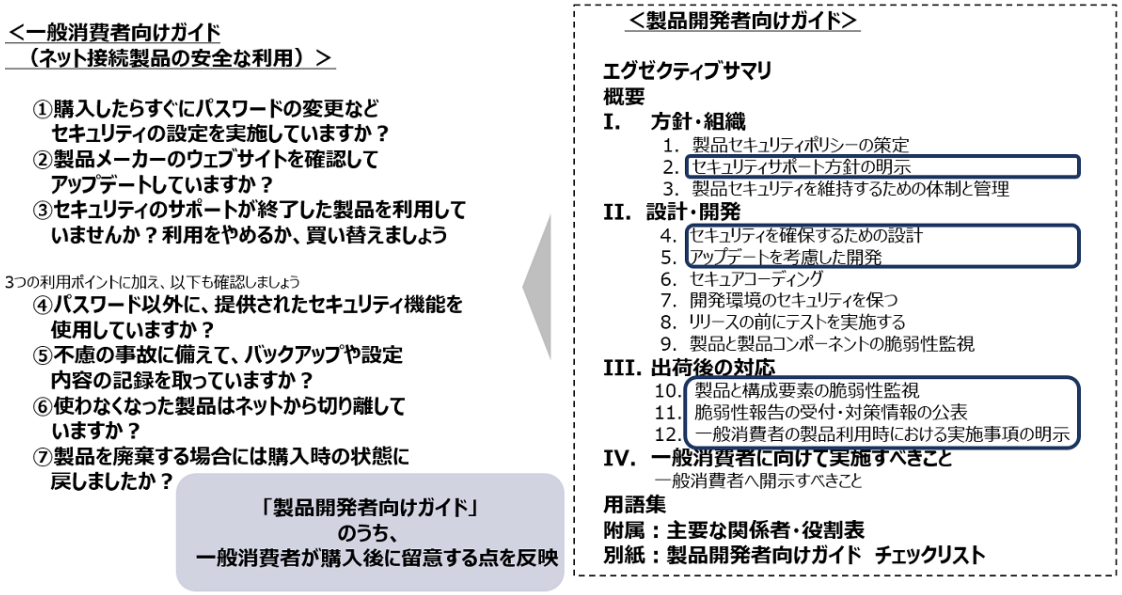


図 3-3「一般消費者向けガイド（ネット接続製品の安全な利用）」の項目

以上の検討に基づき、別紙の通り「一般消費者向けガイド（ネット接続製品の安全な利用）」を作成した。

3.2.2. ヒアリング調査

ヒアリング調査の結果を以下に示す。

(1) 調査概要

「一般消費者向けガイド（ネット接続製品の安全な選定）」、「一般消費者向けガイド（ネット接続製品の安全な利用）」及び「普及手段と効果測定方法」についてのヒアリング調査を実施し、ヒアリング調査結果を取り纏めた資料「ヒアリング調査結果」を作成した。

(2) 調査対象

以下の対象について調査を実施した。

調査対象	＜製品開発者＞ ● 1社 ＜セキュリティ有識者＞ ● 1者 ＜業界団体（量販店、ECサイト、販売協会）＞ ● 4社/団体
実施時期	2019年11月～2020年1月
調査項目	● 一般消費者向けガイドの内容の妥当性 ● 効果的な普及手段 ● 業界団体による活用方法案 ● 業界団体による普及・活用における課題とその解決方法　等

(3) 調査結果

ヒアリング調査の結果得られた主な意見と対応方針は以下の通り。

表 3-1　ヒアリング調査結果（一般消費者向けガイド）

No	項目	コメント	コメント者	対応内容
1	① 内容の妥当性	高年齢層は、低年齢層と比較し、内容をよく読む傾向にあり、絵（図解）と文字は大きいほうが望ましい。	開発者	イラストを活用するとともに、伝えたいメッセージに関してはフォントサイズが小さくならないよう留意する。
2		全ての製品にアカウント機能が存在しているわけではない。また、アカウント機能がある場合でも、初期設定の状態からセキュアにしておくことが近年のトレンドである。これらのような、アカウントの初期設定が不要な製品については、取扱説明書等で、初期設定の説明書きがなされないこととなるが、記載がないからといって、セキュリティが確保できていないわけではない。説明書に記載がないことで、否定的評価になるようなガイドにするべきではない。	開発者	アカウント設定がある製品については、パスワード変更等のセキュリティ設定を実施する旨を記載する
3		認識してもらうために、繰り返し情報提供することが重要だと考えられる。	有識者	普及啓発は、継続的に実施していく。

No	項目	コメント	コメント者	対応内容
4	② 効果的な普及手段	小学校のICT教育の一環の消費者教育のように、教材として使えるパワーポイントなどを公開する方法は教育者に喜ばれるかもしれないため、検討してほしい。	業界団体	次年度の普及啓発の状況を踏まえ、普及のためのコンテンツを拡大していく。
5		実現できるかわからないが、「安全な利用」の方であれば、パソコンのスクリーンセーバーを作り、展示しているパソコンで、そのスクリーンセーバー見せておくことはできるかもしれない。	量販店	次年度の普及啓発の状況を踏まえ、普及のためのコンテンツを拡大していく。
6	③ 活用方法案	消費生活相談員等向けの研修において、ガイドの説明を実施検討してほしい。	有識者	次年度の普及啓発の状況を踏まえ、ガイドの配布先等を検討していく。
7		JNSAの全国セミナー（5ヶ所）は経産省が後援しているが、次年度は、NISCと総務省を入れて協賛でやらないかとの話もある。IPAが講演できるとよいのではないか。	業界団体	
8	④ 普及・活用における課題とその解決方法	IPA（第三者機関）によるチェック機関を設け、認定マークを発行してもらえると利用者にも理解しやすいのではないか。	業界団体 有識者	ガイドの内容及びマークについて下記が懸念されるため、今回の検討からは見送りとする。 ・クリア前提の内容となっている。 ・マークに対する利用者の理解が浸透しない可能性がある。

(4) 普及手段と効果測定方法

ヒアリング調査の結果等を踏まえ、「一般消費者向けガイド」の普及手段及び効果測定方法について検討を行った。

「一般消費者向けガイド」の普及手段及びガイドの内容がどれだけ認知（理解）されたか、適用されたかについての効果測定方法を検討する。

「一般消費者向けガイド」の効果測定方法については以下の通り。

① ヒアリング調査：協力組織に対して、「利用目的」や「利用後の評価」についてヒアリング調査を行う。

② 専用のアンケート調査：家電量販店、EC サイト、消費者関連団体、教育機関等に対して、「利用目的」や「利用の可能性」及び「利用されない理由（不足している内容等）」についてアンケート調査を行う。

③ QR コードから詳細情報を確認する際の簡易アンケート調査：詳細情報を確認する際に、簡易的なアンケートを行う。（スマホアプリの評価を参考に★1 つ～★5 までの評価）また、連絡用のメールアドレスを登録し、バージョンアップや更新した際の案内等も実施。

普及に協力いただける他組織		家電量販店	ECサイト	業界団体	消費者関連団体	教育機関
方法		• 設置 • 配布 • パンフ配布	• 掲載	• 配布（カタログ送付時同封） • 掲載	• 設置 • 配布 • 掲示	• 掲示板での掲載 • 配布 • 講義等での解説
媒体		• 紙媒体	• 電子ファイル	• 紙媒体 • 電子ファイル	• 紙媒体	• 電子ファイル • 紙媒体
効果測定手法	①ヒアリング調査（サンプリング）	○	–	○	○	–
	②専用のアンケート調査	○	○	–	○	○
	③QRコードから詳細情報（ウェブサイト）を確認する際の簡易アンケート調査	○	○	○	○	○

図 3-4「一般消費者向けガイド」の普及手段及び効果測定方法（1/2）

その他のメディア等		ITメディア系 Webサイト	IPAが参加するイベント・セミナー	IPA インターネット安全教室	IPA セキュリティプレゼンター	SNS (Facebook, Twitter) メール配信	IPA 意識調査
方法		• 寄稿 • ガイドの掲載	• ガイドの配布	• 教材への取り込み • ガイドの配布	• ガイドの配布	• 告知文とリンク掲載	• アンケート調査の設問に組み入れ
媒体		• 電子ファイル	• 紙媒体	• 紙媒体 • 電子ファイル	• 紙媒体	• SNS • メール	• 電子ファイル
効果測定手法	①ヒアリング調査（サンプリング）	○	–	–	–	–	–
	②専用のアンケート調査	–	○	○	○	–	○
	③QRコードから詳細情報（ウェブサイト）を確認する際の簡易アンケート調査	○	○	○	○	○	○

図 3-5「一般消費者向けガイド」の普及手段及び効果測定方法（2/2）

(5) 普及促進資料

「一般消費者向けガイド」の普及に必要な資料「普及促進資料」を作成した。

普及促進資料としては、家電量販店に消費者向けガイドを置いて頒布していただくためには、店員等に対してガイドの内容を理解していただく必要がある。そのため、家電量販店の店員など、消費者向けガイドの頒布者に向けたガイドのパンフレットを作成した。

＜記載項目＞

・製品選定時の“確認項目” 、何を見ればよいのかの説明
・製品利用時の“設定項目” 、何を設定すればよいのかの説明
・上記を行わない場合の危険性（リスク）等

また、ガイドに記載したQRコードから誘導したウェブサイトの詳細情報には、消費者向けガイドの内容をより深く理解していただくために、以下を記述することとした。

＜記載項目＞

・購入前確認項目・利用時設定項目
・確認方法（製品、マニュアル類、メーカーWebページなど）
・対策されていない場合の脅威
・（対策されていない場合の）消費者が実施することが望ましい代替策等

4. サポート終了製品のパートナーシップにおける取扱いに関する調査

4.1. 調査の概要

4.1.1. 調査目的

パートナーシップの運用において、サポート終了製品の取扱いが明確となっていない部分及び取扱いをする上での課題があるため、取扱いが停滞する場合がある。このため、明確となっていない部分と課題となっている部分についての運用及び改善方法について検討する。

具体的に停滞する事例としては以下のような状況が発生する場合がある。
現行で取扱いを実施している案件のなかに下記の状況を全て満たすものがある。

- 製品開発者のウェブサイトにおいて、EoL 宣言が公表されている。
- EoL 宣言で規定されるサポート終了期限を既に経過している。
- EoL となっているが、現時点においても重要インフラ事業者等で利用されている可能性がある（優先情報提供の候補案件）。
- 当該 EoL 製品を組み込んだ製品が、当の EoL の製品開発者とは異なる者によって開発されており、この異なる製品開発者の製品も重要インフラ事業者等で利用されている可能性がある。

EoL であることを理由に、製品開発者との調整が難航する可能性があったため、現場担当者間で取扱方針の検討を進めていた。

その検討のなかで、取扱い（とりわけ優先情報提供）について、明確ではない点があることが判明したため、それらの整理・方針検討を実施する必要がある。

4.1.2. 調査方法

調査方法は図 4-1 に示す通りである。

パートナーシップにおいてサポート終了製品の取扱いが明確となっていない部分及び取扱いをする上での課題について、IPA 及び JPCERT/CC へヒアリングを行い、その結果を基にして、IPA 及び JPCERT/CC と協議し、課題の改善策、新たな運用ルールを資料として取り纏めた。

図 4-1　調査方法概要

4.2. 調査結果

4.2.1.　課題の整理

サポート終了におけるリスクと製品開発者の望むべき対応は以下の通り。

- 製品開発者にとって永遠にサポートすることは大きな負担
- 一般的にサポート終了製品は、脆弱性対策や公表は行われず、製品利用者が脆弱性のリスクを知らぬまま製品を使い続ける
- 製品開発者の望むべき対応は、「製品の利用中止」の公表

また、パートナーシップにおける問題と対処は以下の通り。

- パートナーシップでは、製品開発者がサポート終了であることを理由に対応を拒否すると調整が難航し、調整不能案件・連絡不能案件となる
- 調整不能案件・連絡不能案件は公表判定委員会にて審議
- JVN にて「製品の利用中止」を公表

そこで、2016 年度脆弱性研究会における検討結果をもとに、想定される取扱いケースごとにパートナーシップでの取扱いについて、下記の通り整理した。

	取扱いケース	パートナーシップでの取扱い
A	サポート終了しており、製品開発者に脆弱性情報を通知。但し、**脆弱性による影響度が小さい**	取扱い終了（通常取扱い）
B	サポート終了しており、製品開発者に脆弱性情報を通知後、製品開発者が対策を**策定し、JVN公表に同意する**	JVN公表（通常取扱い） 優先情報提供可能
C	サポート終了しており、製品開発者に脆弱性情報を通知後、製品開発者は対策を**新規に策定せずに、「利用中止」のJVN公表に同意する**	JVN公表（通常取扱い） 優先情報提供可能
D	サポート終了しており、製品開発者に脆弱性情報を通知後、製品開発者が対策を**策定せず、「利用中止」のJVN公表にも同意しない**	**「調整不能」案件**として**公表判定委員会**での判定 その後、「利用中止」のJVN公表
E	サポート終了しており、製品開発者に脆弱性情報を**通知できない、または、製品開発者に通知したが、その後製品開発者から応答が無い**	**「連絡不能」案件**として**公表判定委員会**での判定 その後、「利用中止」のJVN公表

4.2.2. サポート終了した製品の優先情報提供の実施方法

取扱いケース別に整理した結果を踏まえ、さらなる検討を実施したところ、取扱いケース「D・E」の調整不能・連絡不能案件となった場合について、以下の様な課題がある。これは、サポート終了であるかどうかによらない問題であるため、来年度以降に改めて課題の調査・整理することを検討したい。

課題１：公表判定委員会を経ない限りは、利用者が脆弱性情報を知る事が出来ない。
→利用者に迅速に周知する必要がある脆弱性情報については、判定対象が１件でも公表判定委員会を開催できる運用を検討する。

課題２：公表判定委員会後に、「利用中止」の JVN 公表について、優先情報提供をする必要性の有無。
重要インフラ事業者は、重要なシステムで利用している製品の脆弱性情報を、一般への公表（JVN 公表）より数日程度、利用中止を知る事の有効性について検討が必要。
→現行の告示及びガイドラインでは本ケースでの優先情報提供は検討できていないため、提供の必要性を検討し、必要な場合は、告示及びガイドラインの改正も踏まえて検討する。

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

5.1. 調査結果

2 章～4 章の検討結果や IPA・JPCERT/CC のパートナーシップの運用関係者からの意見を踏まえ、報告書執筆時点でのパートナーシップガイドラインの改訂は実施しないが、今後の検討を踏まえ対応を行うものとする。4.2.2 で挙げたように、今後、サポート終了製品に限らず、調整不能案件・連絡不能案件の取り扱い及びガイドラインの改訂等について、検討を行うことが望ましい。

参考１

2019 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 12 月 25 日時点

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

（五十音順、敬称略）

オブザーバ

奥家 敏和	経済産業省 サイバーセキュリティ課長
尾崎 洸	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
宮下 清	一般社団法人日本情報システム・ユーザー協会（JUAS）
笹岡 賢二郎	一般社団法人コンピュータソフトウェア協会（CSAJ）
戸島 拓生	一般社団法人コンピュータソフトウェア協会（CSAJ）
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)
椎木 孝斉	一般社団法人 JPCERT コーディネーションセンター(JPCERT/CC)
洞田 慎一	一般社団法人 JPCERT コーディネーションセンター(JPCERT/CC)
高橋 紀子	一般社団法人 JPCERT コーディネーションセンター(JPCERT/CC)
石川 貴博	一般社団法人 JPCERT コーディネーションセンター(JPCERT/CC)
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
土屋 昭治	独立行政法人情報処理推進機構
板橋 博之	独立行政法人情報処理推進機構
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
村野 正泰	株式会社三菱総合研究所
江連 三香	株式会社三菱総合研究所
小川 博久	株式会社三菱総合研究所
朱 ユーティン	株式会社三菱総合研究所
平林 徹	株式会社三菱総合研究所

（順不同、敬称略）

参考２

脆弱性研究会の検討経緯

■研究会第 1 回会合（2019 年 10 月 30 日）
- 今年度の検討方針について
- ソフトウェア製品の脆弱性対処促進に関する調査について
- 一般消費者のリテラシー向上に関する調査について
- スケジュールについて

■研究会第 2 回会合（2019 年 11 月 22 日）
- 前回会合の確認
- ソフトウェア製品の脆弱性対処促進に関する調査について
- 一般消費者のリテラシー向上に関する調査について
- サポート終了製品のパートナーシップにおける取扱いに関する調査について
- スケジュールについて

■研究会第 3 回会合（2019 年 12 月 25 日）
- 前回会合の確認
- ソフトウェア製品の脆弱性対処促進に関する調査について
- 一般消費者のリテラシー向上に関する調査について
- サポート終了製品のパートナーシップにおける取扱いに関する調査について
- 情報システム等の脆弱性情報の取扱いに関する調査実施報告書（案）について