情報システム等の脆弱性情報の取扱いに関する研究会

－ 2012 年度　報告書 －

2013 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 2012 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 7,950 件に達している。

2012 年度には、一般市民に対する脅威がこれまで以上に注目された。遠隔操作ウイルスによって、市民が誤認逮捕される事態が複数件発生した。また、スマートフォンが急速に普及する中、スマートフォンの内部情報や電話帳、位置情報等を勝手に送信する不正アプリケーションの問題も懸念されている。その一方、stuxnet や Flame 等のマルウェアの登場により、重要インフラや生産拠点を支える制御システムのリスクも高まっていることを受けて、技術研究組合制御システムセキュリティセンターが設立された。こうした脅威の多様化は、我々が対処しなければならない脆弱性問題の拡大と解釈することもできる。

今年度の「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、ウェブサイトの脆弱性届出の大きな割合を占める小企業の脆弱性対策の実態を把握するとともに、そうした取り組みを促すための資料作りに取り組んだ。また、制度運用上の問題解決や改善に関しては、調整不能案件の公表を制度化するにあたり、経済産業省では告示の改正が必要と判断したため、脆弱性研究会では告示改正案へのコメントとその変更を踏まえた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、「ガイドライン」という）の改訂について検討した。

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。

2013 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。経済産業省告示「情報システム等脆弱性情報取扱基準」（2004 年 7 月 7 日公示、以下「告示」とする）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している。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 2012 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 1,424 件、ウェブサイトの脆弱性に関するもの 6,526 件の計 7,950 件であった。四半期毎の届出状況をに図 1-1に示す。

	2009 4Q	2010 1Q	2Q	3Q	4Q	2011 1Q	2Q	3Q	4Q	2012 1Q	2Q	3Q
累計届出件数[件]	5,975	6,146	6,300	6,414	6,481	6,569	6,652	6,887	7,314	7,583	7,752	7,950
1就業日あたり[件/日]	4.47	4.40	4.32	4.22	4.10	4.01	3.92	3.91	4.02	4.03	3.99	3.96

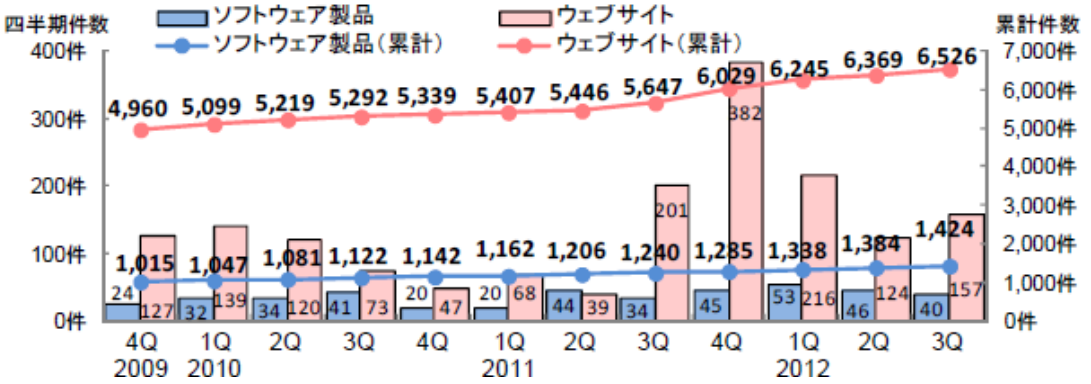
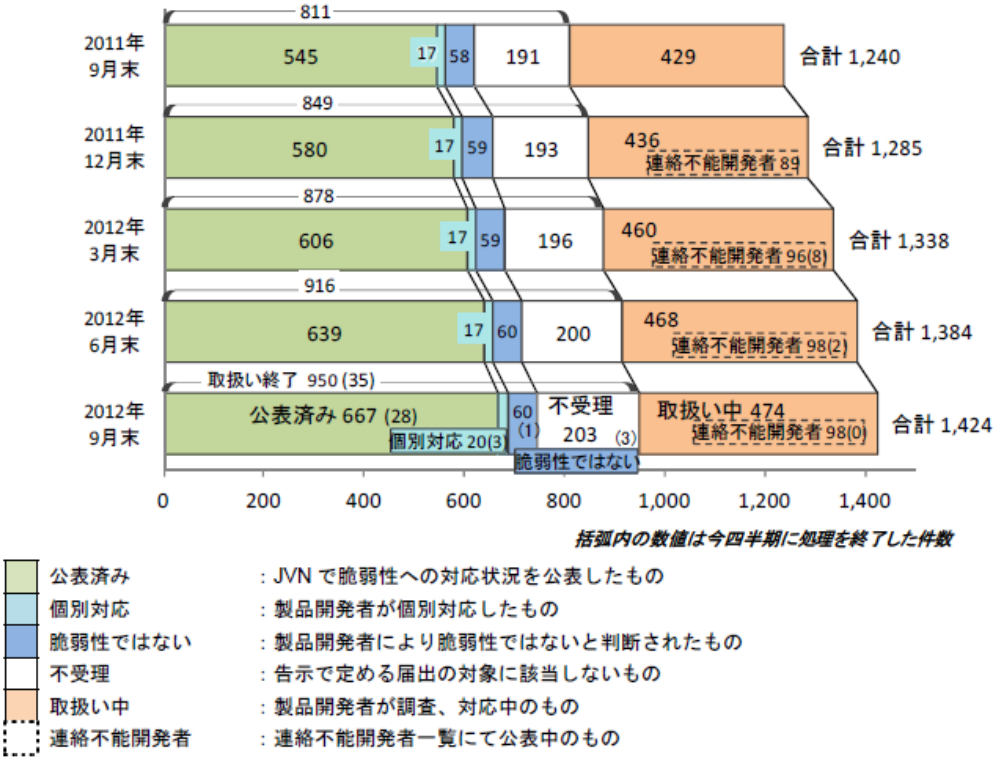


図 1-1　四半期ごとの届出状況

（http://www.ipa.go.jp/about/press/pdf/121022press2.pdf 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。



公表済み	：JVN で脆弱性への対応状況を公表したもの
個別対応	：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	：製品開発者が調査、対応中のもの
連絡不能開発者	：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

（http://www.ipa.go.jp/about/press/pdf/121022press3.pdf より抜粋）

ソフトウエア製品の脆弱性関連情報の届出 1,424 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 667 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 20 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 60 件、取扱い中のものが 474 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 203 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。

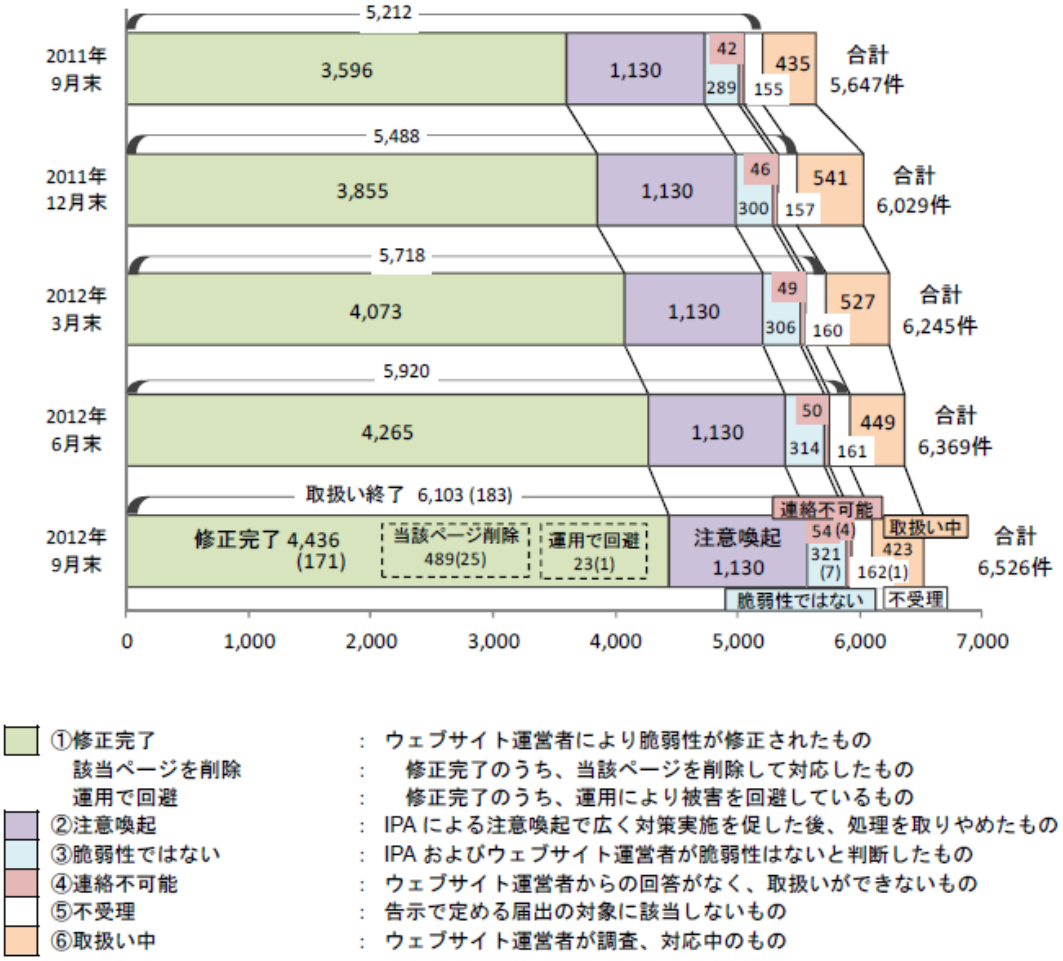


図 1-3　ウェブサイトの脆弱性関連情報の届出の処理状況

（http://www.ipa.go.jp/about/press/pdf/121022press3.pdf より抜粋）

ウェブサイトの脆弱性関連情報の届出 6,526 件のうち、修正が完了したものが 4,436 件（うち運用で回避されたもの 23 件、当該ページを削除して対応

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

したもの 489 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 321 件、取扱い中のものが 423 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（連絡不可能）が 54 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 162 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 2012 年 9 月末までに 1,497 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

2012 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 667 件である。届出受付開始から 2012 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 35%であり、公表までに時間を要している割合が大きい。

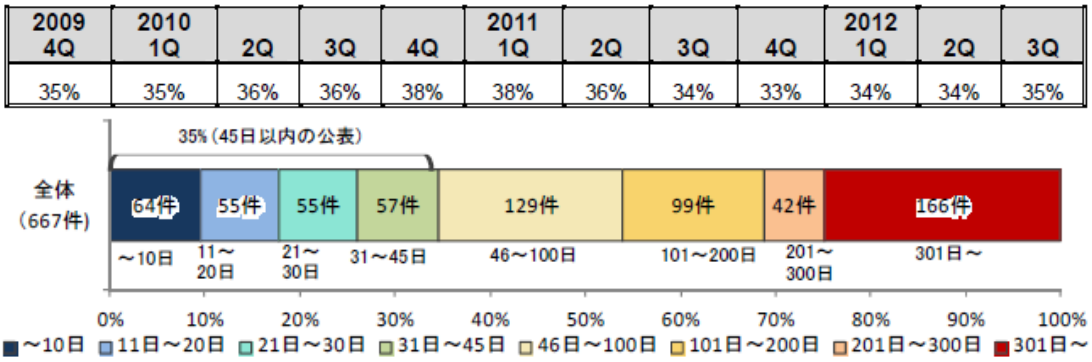


図 1-4　ソフトウエア製品の脆弱性公表までに要した日数

（http://www.ipa.go.jp/about/press/pdf/121022press3.pdf より抜粋）

(2)公表された脆弱性の内容

2011 年度第 4 四半期～2012 年第 3 四半期（2011 年 10 月から 2012 年 9 月末まで）に IPA が国内の発見者及び製品開発者自身から届出・連絡を受け、JVN で公表された脆弱性は 122 件である。このうち、複数の製品開発者のソフトウエア製品に影響のあるものは 2 件であった。また、オープンソースソ

[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。

フトウエア（OSS）製品の脆弱性は 42 件、製品開発者自身から届け出られた自社製品の脆弱性は 12 件、組込みソフトウエア製品の脆弱性は 8 件、制御システムの脆弱性は 3 件であった。

(3)海外 CSIRT から連絡を受け公表した脆弱性

2012 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 830 件である。このうち、2011 年度第 4 四半期～2012 年第 3 四半期（2011 年 10 月から 2012 年 9 月末まで）に JVN で公表した脆弱性関連情報は 151 件、うち通常の脆弱性情報が 130 件、対応に緊急を要する米国 US-CERT[3]等の Technical Cyber Security Alert が 21 件であった。

(4)製品種類別の内訳

届出受付開始から 2012 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 1,424 件のうち、不受理分を除いた 1,221 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 40%を占めている。

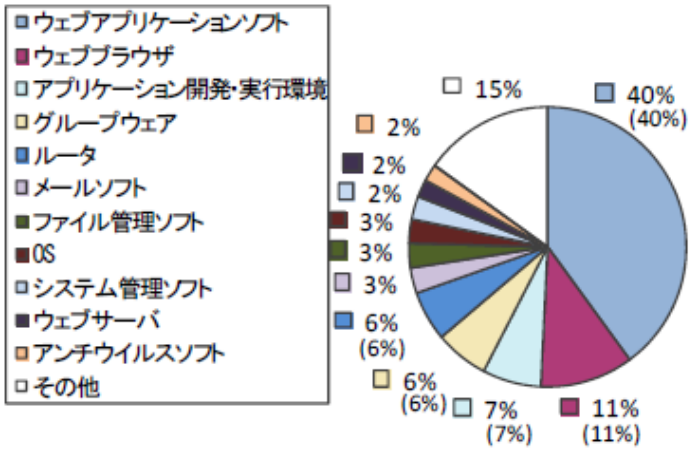


図 1-5　ソフトウエア製品種類別の届出内訳（届出受付開始～2012 年 9 月末）

（http://www.ipa.go.jp/about/press/pdf/121022press3.pdf より抜粋）

(5)脆弱性の原因別の内訳

届出受付開始から 2012 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 1,424 件のうち、不受理のものを除いた 1,221 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 60%を占める。

---

[3] United States - Computer Emergency Readiness Team（米）：DHS(Department of Homeland Security)と CERT/CC の共同事業として 2003 年 9 月に開始。脆弱性データベース（US-CERT Technical Alert）や国民向けのセキュリティ情報サービス（National Cyber Alert System）の管理運用等を行っている。http://www.uscert.gov/

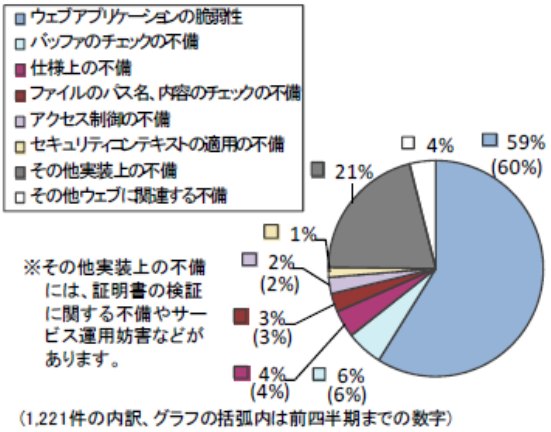


図 1-6　ソフトウエア製品の脆弱性原因別の届出内訳（届出受付開始～2012 年 9 月末）

（http://www.ipa.go.jp/about/press/pdf/121022press3.pdf 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

2012 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 4,436 件について、IPA からウェブサイト運営者に脆弱性関連情報の詳細を通知してから、修正されるまでに要した日数を、脆弱性の種類別にまとめたものを図 1-7 に示す。全体の 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。

	2009 4Q	2010 1Q	2Q	3Q	4Q	2011 1Q	2Q	3Q	4Q	2012 1Q	2Q	3Q
修正完了件数	2,655	2,886	3,052	3,209	3,342	3,448	3,510	3,596	3,855	4,073	4,265	4,436
90 日以内の件数	1,905	2,028	2,082	2,163	2,216	2,247	2,280	2,311	2,528	2,700	2,825	2,924
90 日以内の割合	72%	70%	68%	67%	66%	65%	65%	64%	66%	66%	66%	66%

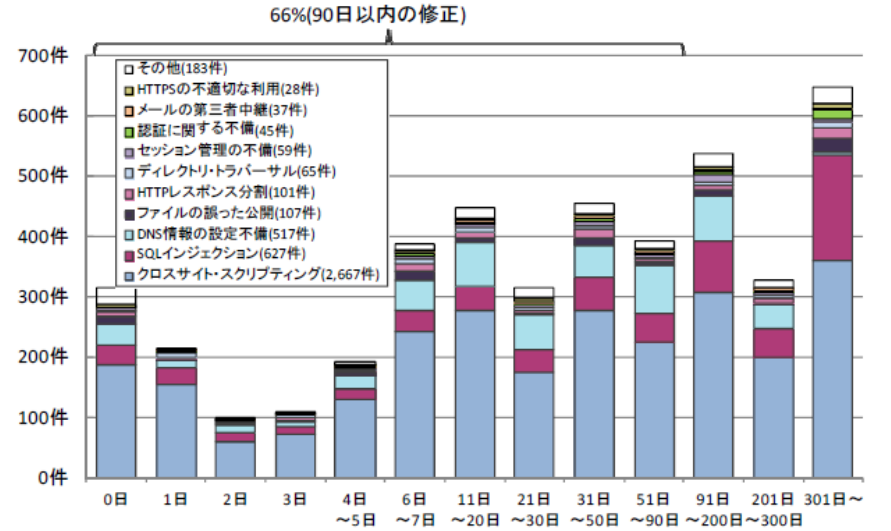


図 1-7　ウェブサイトの脆弱性修正に要した日数（届出受付開始～2012 年 9 月末）

（http://www.ipa.go.jp/about/press/pdf/121022press3.pdf より抜粋）

(2)届出の脆弱性種類別内訳

2012 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 6,526 件のうち、不受理のものを除いた 6,364 件の種類別内訳を図 1-8 に示す。脆弱性の種類は依然として「クロスサイト・スクリプティング」(52%)、「DNS 情報の設定不備」(21%)、「SQL インジェクション」(13%)の割合が高く、この３つだけで全体の 86%を占める。

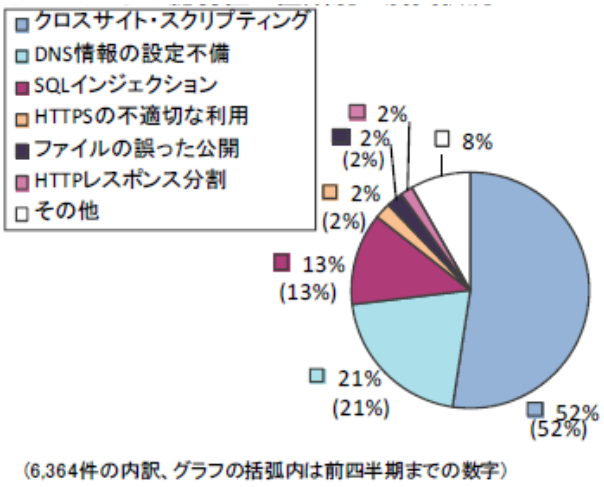


図 1-8　ウェブサイトの脆弱性種類別内訳（届出受付開始～2012 年 9 月末）

(http://www.ipa.go.jp/about/press/pdf/121022press3.pdf より抜粋)

(3)届出の脆弱性脅威別内訳

届出のあった脆弱性から想定される脅威別内訳を図 1-9 に示す。脆弱性から想定される脅威としては、「本物サイト上への偽情報の表示」(50%)、「ドメイン情報の挿入」(21%)、「データの改ざん、消去」(12%)の割合が高い。

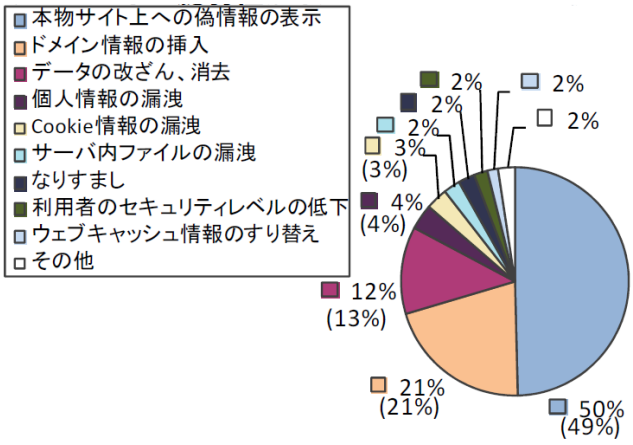


図 1-9　ウェブサイトの脆弱性脅威別内訳（届出受付開始～2012 年 9 月末）

(http://www.ipa.go.jp/about/press/pdf/121022press3.pdf より抜粋)

(4)届出の脆弱性脅威別内訳

過去 2 年間に IPA に届出のあったウェブサイトの脆弱性関連情報のうち、不受理を除いたウェブサイトの運営主体の種類別届出件数の四半期別推移をに図 1-9 に示す。2012 年第三半期に届出されたウェブサイトの届出 157 件のうち、不受理を除いた 156 件のウェブサイト運営主体は、株式企業（上場）が 8%、株式企業（非上場）が 56%、その他企業が 7%であり、これら「企業」が全体の 74%を占めている。

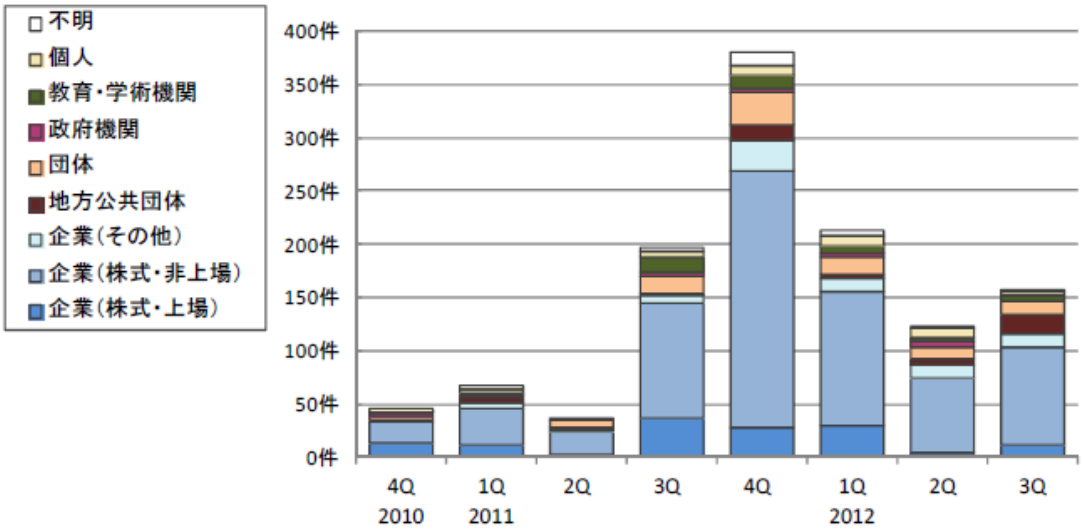


図 1-10　ウェブサイトの運営主体の種類別の届出件数(四半期別推移)

(http://www.ipa.go.jp/about/press/pdf/121022press3.pdf より抜粋)

1.3. 本年度研究会における検討

前年度調査結果を踏まえ、本年度の脆弱性研究会は以下の 2 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小企業のウェブサイト運営者向け脆弱性対策支援
- 小企業のウェブサイト運営に関するアンケート調査
- 小企業ウェブサイトの運営者及び関係者に対するヒアリング調査
- 小企業のための脆弱性対応ガイド（仮称）作成

②ガイドラインの見直しに関する調査
- 告示改正に関する意見の集約と、それに伴うガイドラインの改訂に関する検討
- 現場での制度運用上の問題解決のための改訂調査
- ①の調査結果に基づく効果的な運用に向けた改善のための改訂調査

2. 小企業のウェブサイト運営者向け脆弱性対策支援

2.1. 調査の概要

(1) 目的

現在、IPA において受け付けているウェブサイトの脆弱性届出では、小企業のウェブサイトが約 7 割を占めている。したがって、小企業のウェブサイトの脆弱性対策は喫緊の課題であり、効果的な促進策を適用することが求められる。

しかし、小企業においては、一般的に、予算や人手が十分でなく、ウェブサイトにおける適切な脆弱性対策の実施は容易でないと考えられる。また、情報セキュリティに関する知見に乏しく、サイバー攻撃が自社にもたらす影響を十分に理解していない可能性もある。

そこで、このような背景のもと、小企業のウェブサイト運営における脆弱性対策の課題を明らかにして、望ましい脆弱性対策を促すため、以下の調査を行った。

a) 小企業のウェブサイト運営に関するアンケート調査
b) 小企業ウェブサイトの運営者及び関係者に対するヒアリング調査
c) 小企業のための脆弱性対応ガイド（仮称）の作成

(2) 手順

a) 小企業のウェブサイト運営に関するアンケート調査

企業モニターを対象としたウェブアンケート調査を行った。調査精度を向上させるため、調査モニターの IT 担当者等に対してプレ調査を行い、回答者の中からウェブサイト運営に関与する者を抽出した上で本調査を実施した。

［調査方法］ウェブアンケート調査（企業モニター）

［調査対象］国内の小企業等のウェブサイト担当者や情報システム担当者（本調査は 310 件が対象）
小企業（従業員数 30 人未満、卸売業・小売業（飲食店を含む）・サービス業で従業員 10 人未満の企業）に所属し、「自組織のシステムの企画・構築・運用・保守」および「情報セキュリティに関わる業務」に関与している者とする。

［有効回収数］243 件（本調査）

[調査項目] 調査の主な設問項目は以下の通りである。

・回答者および所属する企業等の基本属性
・ウェブサイトに係る業務への関与
・ウェブサイトの特徴
・ウェブサイトの構築・運用の実態
・ウェブサイトの脆弱性対策に関する理解
・ウェブサイトのセキュリティ対策／脆弱性対策の現状
・脆弱性対策に関する課題
・脆弱性およびセキュリティ対策関連事業等に関する認知度

b) 小企業ウェブサイトの運営者及び関係者に対するヒアリング調査

小企業のウェブサイト運営者に対するヒアリング調査の概要を以下に示す。

[調査対象] 小企業のウェブサイト運営者

（首都圏：5 件、地方中枢都市：3 件、地方中核都市：2 件）

アンケート調査回答者のうち、所在地とウェブサイトの形態から以下の対象者を抽出した。

表 2-1　ヒアリング調査対象者の属性

ウェブサイトの形態	首都圏	地方中枢都市*1	地方中核都市*2
オーサリングツール利用	3	1	2
独自開発	1		
外部事業者に委託		1	
ISP 提供サービス利用	1		
ショッピングモール利用		1*3	
合　計	5	3	2

*1) 地方中枢都市：大阪圏、名古屋圏、及び札幌市、仙台市、広島市、福岡市・北九州市

*2) 地方中核都市：地方圏（三大都市圏以外の地域）における地方中枢都市以外の県庁所在地及び人口が概ね 30 万人以上の都市。

*3) 本回答者は、現状はショッピングモールを活用しているが、元々は独自開発をしていたことから、「独自開発」の意見や移行の意図等について確認するため、調査対象者に設定した。

[調査方法] ヒアリング調査

・首都圏（5 件）：グループインタビュー方式
・地　方（5 件）：訪問方式

[調査実施期間] 2013 年 1 月

[調査項目] 調査では、a)の回答を元に以下の内容について質問した。

・ウェブサイトの構築・運用の形態
・ウェブサイトの構築・運用のリソース

・脆弱性対策への課題
・脆弱性対策を促すための方策やその普及方策

また、これらの運営者ヒアリングの結果について確認するため、小企業のウェブサイト構築・運用を支援する事業者等の業界団体に対するヒアリング調査の概要を以下に示す。

［調査対象］以下の 3 機関；
一般社団法人 日本コンピュータシステム販売店協会
一般社団法人 日本 Web ソリューションデザイン協会
特定非営利活動法人 IT コーディネータ協会

［調査方法］ヒアリング調査（訪問方式）

［調査実施期間］2013 年 1 月

［調査項目］調査項目は小企業ウェブサイトの運営者と同様に設定した。

c) 小企業のための脆弱性対応ガイド（仮称）の作成

小企業における脆弱性対策の適切な理解と実施を促すための資料を作成した。資料作成にあたっては、調査項目 a)、b)の結果を考慮した。併せて、その効果的な周知の方法についても検討した。

2.2.小企業のウェブサイト運営に関するアンケート調査

アンケート調査の詳細は「小企業における脆弱性対応の実態に関する調査結果」に示す。以下に、アンケート調査から得られた知見を取りまとめる。

(1)調査仮説の検証

a) ウェブサイトの構築・運用の実態

（仮説 1）自社社員が少人数（ほぼ 1 名）で運用者が不明確

ウェブサイトにトラブルが生じたときに「自身がトラブルに対処する」と答えた回答者は全体の 49.5%であった。また、ウェブサイトのセキュリティ管理を「組織的には行っていない」小企業は 52.7%と多く、「担当者がいる」小企業は 21.6%、「主担当業務以外にウェブサイトのセキュリティ管理を兼任する担当者がいる」小企業は 16.5%にとどまった。

これらの結果から、少人数でウェブサイトの運用をしている様子が裏付けられる。

（仮説 2）構築および運用の方針は経営者が決定

ウェブサイトの運用・構築についてのトップ（社長や経営陣）のは関与の状況は、「トップ自らが運用・構築にあたっている」小企業が 35.4%と多かった。この割合は従業員数 5 人以下の企業では 58.3%であった。脆弱性対策等のセキュリティ対策の適用について「組織のトップ」が判断する小企業は 37.8%であった。

これらの結果から、経営者がウェブサイトの構築および運用の方針に強く関わっている様子がうかがえる。

（仮説 3）セキュリティ対策は構築段階の対策が全てでその後は検討や改善は殆ど行っていない

脆弱性対策の実施状況については、「構築時も運用時も脆弱性対策をしている」小企業が全体の 45.4%と最も多く、次いで「運用時にのみ対策をしている」小企業が 19.0%であった。「構築時にのみ対策をしている」小企業は皆無（0.4%）であった。

これらから仮説は誤りであり、構築時の計画的な対策よりも運用時に必要に応じて対策が行われている様子が伺えた。また、「一切対策をしていない」小企業も 16.8%と多くあった。

b) 脆弱性対策への理解

(仮説 4) 脅威を認識しておらず危機感がない（主に大企業が狙われており小企業は攻撃されないという考え）

(仮説 5) 脆弱性対策が脅威への根本的解決策となることを理解していない

ウェブサイトの機能・画面について、脆弱性対策が必要となる例を挙げて質問したところ、半数以上の小企業のウェブサイトには脆弱性対策が必要と考えられる機能・画面が備えられていた。ウェブサイトの脆弱性について知っているか尋ねたところ、約 6 割は詳しく知っており、9 割は聞いたことがあるという結果を得た。一方で、脆弱性対策を行わないと答えた者にその理由を尋ねたところ、「クレジットカード等の決済を行っていない」(59.8%)、「個人情報を扱っていない」(58.8%)、「サイトが著名でないので、被害に遭うとは考えにくい」(33.3%) という理由を挙げる者が多かった。

これらから、脆弱性については一定の脅威として認識している場合もあるが、ウェブサイトに積極的に対策を行う強い必要性が認められないため対策を行わない、という状況が伺える。

c) 脆弱性対策の現状と課題

(仮説 6) ウェブサイトを一時停止し修正作業が必要な脆弱性対策を行うことに消極的

ウェブサイトに脆弱性対策などのセキュリティ対策を進める上での課題について尋ねたところ、「脆弱性を修正すると、ウェブ上のアプリケーションが動かなくなる可能性がある」、「脆弱性の問題でサービスを止めると、顧客を失ってしまう」のいずれの項目についても、「特に課題ではない」とする回答が半数を超えた。

このことより、脆弱性の修正時に伴う問題についてまで深く考えて課題とする意識は必ずしも高くはない様子が伺える。

(仮説 7) ウェブサイトのセキュリティ対策へ費やす予算や人手が十分ではない

費用と人員の確保状況について、「十分に確保できている」(8.4%)、「おおむね確保できている」(35.6%) とする回答を合わせると約 4 割であった。一方、「やや不足している」(20.1%)、「まったく足りていない」(16.5%) とする回答も合わせて 4 割近くであった。「わからない」とす

る回答が 19.4%と多く、適正なコストを見積もれない状況が伺える。予算と人員の確保について課題とみなす回答は全体の約 6 割であった。従業員数が 6～30 人の企業においては、費用・人員が不足であるとする回答がより多かった。

（仮説 8）セキュリティ技術が担当者には難しく理解し難い

ウェブサイト担当者の選定理由をたずねたところ、「パソコンに詳しい／慣れているから」とする回答が最も多く（60.8%）、ついで「デザインができるから」「運営や管理ができるから」といった理由が挙げられた。

「脆弱性やセキュリティに関する技術の習得が難しい」ことを課題として挙げる回答は全体の約 7 割であった。

これらから、ウェブサイトの運営に関与する経営者や担当者にとって、脆弱性やセキュリティに関する技術が難しく、理解が及んでいない様子が伺えた。

（仮説 9）トラブルが生じても脆弱性対策による根本的な解決は行われない

脆弱性に起因する被害経験について尋ねたところ、「業務に影響が生じる被害が発生した」という回答が全体の 4.8%、実害が発生したことはないが被害に遭ったことはあるという回答が 10.3%あった。これらを合わせ 15%の回答者が被害に遭ったと答えている。

運用中のウェブサイトに脆弱性が発見された場合に「特に脆弱性対策は取らない」とする回答は全体の 9.9%であった。

d) IPA の普及啓発資料に関する認知度

（仮説 10）無償で利用可能な良いコンテンツがあるならば利用したい

情報セキュリティ早期警戒パートナーシップの取組みについて尋ねたところ、聞いたことがあるとした回答は約 4 割であった。IPA による脆弱性関連の情報等の認知状況については、約 20～30%ほどが聞いたことがあるとしている。

ウェブサイトのセキュリティ対策の運用・管理、セキュアなウェブサイトの構築、最新のウェブサイトに関するセキュリティ脅威の動向などの情報セキュリティに関する普及啓発コンテンツを利用してみたいかを尋ねたところ、何らかのコンテンツを利用してみたいと答えた回答が約 7 割であった。

(2)企業規模による相違点

従業員数 5 人以下の企業と 6～30 人の企業とでは、表 2-2 のような違いが見られる。

表 2-2　企業規模（従業員数）による相違点

	従業員数 5 人以下	従業員数 6～30 人
ウェブサイト構築・運用について	・ホスティングを利用しコンテンツを自前で構築している。 ・経営トップ自らが中心的役割を果たしている。	・外部委託による構築がより多い。 ・ウェブサイト担当者（責任者）を設けて経営者から指示。
ウェブサイトのセキュリティ対策（脆弱性対策）について	・経営トップが判断。 ・組織的にはあまり行っていない。	・ウェブサイト担当者（責任者）が判断。
セキュリティ対策の委託について	・委託の実施率に差異はあまりない（わずかに低い）。 ・委託ルールが未整備（セキュリティ要件の指定、セキュリティ報告書の取得の割合は低い）。	・委託の実施率に差異はあまりない（わずかに高い）。 ・委託ルールがしっかりしている（セキュリティ要件を指定しセキュリティ報告書を取得している割合がより高い）。

2.3.小企業ウェブサイトの運営者及び関係者に対するヒアリング調査

ヒアリング調査の詳細は「小企業における脆弱性対応の実態に関する調査結果」に示す。以下に、ヒアリング調査から得られた知見を取りまとめる。

(1) ウェブサイトの構築・運用の形態

ウェブサイトの構築形態については、オーサリングツールを利用するケースが主流であった。使用するツールとしては、大半が「Dreamweaver」を挙げている。同製品を含め、オーサリングツールには、製品のコマンドを利用して生成したコードに脆弱性が含まれるケースやサンプルフォームに脆弱性が内包されているケースが指摘されている。したがって、使用するオーサリングツールのバージョンを最新に保つとともに、関連の脆弱性情報に留意することが望まれる。

また、ウェブサイトの運用形態については、多くがホスティングサービスを利用している。ホスティングサービスは、一般にはOSやミドルウェアの脆弱性が発覚した際は、ホスティング事業者側がパッチ適用等の対策を実施する。そうした脆弱性対策の責任分担が明記されていることを確認すべきである。

(2) ウェブサイトの構築・運用のリソース

ヒアリング先の大半が、2 章の仮説検証で採り上げたとおり、構築・運用の担当を一人で任されている。任命は、スキルが評価されたわけではなく、「PC に慣れているから」「担当部門のメンバーだから」など、必然性の乏しい理由によるケースが多い。また、前任者の退職により、他に選択肢がなく、後を引き継ぐケースもある。これらの担当者にとって、サーバ等の IT 管理業務は既存の業務との兼務であり、負担となっている。担当者には問題意識や意欲もあり、可能であればセキュリティについて学びたいと考えているケースもあるが、学ぶ時間がないという指摘もあった。

ウェブサイトの構築は経営者が判断することが多いが、すべてに口を挟むわけではなく、詳細は担当者に任せている。一方で、ウェブサイトの運営に対する経営者の関心はあまり高くなく、たとえばトラブル対応に費用がかかることがわかると、「サイトそのものをやめてしまう」という可能性も指摘されている。

(3) 脆弱性対策への課題

小企業において脆弱性対策が進まない理由の一つに、「自社のサイトは重要な情報がなく、著名でもないので狙われない」という思い込みが指摘されている。したがって、たとえ重要情報がなくても、脆弱性があるだけで狙われて踏み台にされてしまい、時に取引先にまで迷惑をかけるリスクがあることについて、理解していただく必要がある。

また、担当者にとっては、その脆弱性が自社に影響するのか、どのように対応すべきか判断できない状況があり、理解しやすい情報提供や専門家の助言が必要であるとの指摘もあった。

(4) 脆弱性対策を促すための方策やその普及方策

脆弱性対策を促す方策として、脆弱性の有無を検証するツールの提供が挙げられた。ただし、そうしたツールは攻撃を誘発する可能性もあり、提供方法に工夫が必要となる。

脆弱性対策を促す啓発資料を小企業に届ける手段として、商工会議所や関連業界団体との共同セミナーの開催、ウェブサイト構築やマーケティング等のイベントでのプレゼンテーション、関連業界団体の会員企業（システム販売店、ウェブ制作会社、IT コーディネータ）のコンサルタント、営業、SE、ディレクター等を介した情報提供等を展開することが提案された。

なお、首都圏と地方で、専門セミナーの開催頻度等、情報量の差は指摘されなかったが、首都圏では「システム構築事業者経由の提供」が有効との回答を得た一方、地方では「商工会議所のセミナー開催」が有効との回答が複数見られた。

2.4.小企業のための脆弱性対応ガイド（仮称）の作成

2.2,2.3 節の調査結果を踏まえ、小企業のウェブサイト運営における脆弱性対策を促進するための啓発資料を作成した。

ウェブサイトの運営については関わるが情報セキュリティや脆弱性に関して知識が少ない読者を想定し、まずは手に取っていただくことを狙い、タイトルは、「安全なウェブサイト運用に向けて ～ 企業ウェブサイトのための脆弱性対応ガイド ～」（以下、「対応ガイド」という。）とした。

対応ガイド作成に際しては、以下の観点や指摘に基づき内容を精査した。

●アンケート調査で得た小企業の現状および必要なメッセージ

- ・小企業においては少人数でウェブサイトの運用やセキュリティ対策をしている。担当者が明確になっていない場合も多い。
- ・ウェブサイトの構築・運用には経営者（組織のトップ）自身が深く関与し決定権を持っている。
- ・ウェブサイト構築時の計画的対策が行われている場合は少なく、運用時に必要に応じて対策が行われる傾向がある。
- ・脆弱性については一定の脅威と認識している場合もあるが、自社のウェブサイトが狙われると考えていない場合が多く、積極的に脆弱性対策／セキュリティ対策を行おうとする意識には乏しい。
- ・ウェブサイトのセキュリティ対策について予算や人手は十分ではなく、課題として認識されている。
- ・ウェブサイトの運営に関わる経営者や担当者にとって、脆弱性やセキュリティに関する技術は難解であり、知識の理解は進んでいない。

●脆弱性研究会からの指摘

- ・委託時のセキュリティ対策／脆弱性対策について言及すべきである。
- ・本格的な脆弱性検査を最初から推奨することは小企業にはハードルが高い。「ウェブ健康診断」のような手段で、まず自社のウェブサイトの実態を把握することを勧めるべきである。
- ・ウェブサイトを乗っ取られて踏み台とされ、サイバー攻撃に悪用される事例も近年増加しているため、これに言及すべきである。

●ヒアリング調査での指摘

- ・使用するオーサリングツールを最新版とし、関連の脆弱性情報に留意すべき。

・ホスティング事業者との脆弱性対策に関する責任分担を確認すべき。
・担当者にはセキュリティについて学ぼうという意欲はあるが時間が無い。
・経営者はウェブサイト構築について判断はするが、詳細は担当者に任せている。運営への関心はそれほど高くなく、セキュリティ対策に費用がかかる場合には、ウェブサイト運用そのものをやめてしまうこともある。
・「自社のウェブサイトは狙われない」という思い込みが強い。踏み台として悪用される場合などリスクについて理解を促す必要がある。
・担当者が理解しやすい情報の提供や専門家からの助言が必要である。

これらの観点や指摘を踏まえて、対応ガイドを検討し、その案を作成した。対応ガイドの目次構成を 表 2-3 に示す。

表 2-3 「企業ウェブサイトのための脆弱性対応ガイド」の目次構成

うちの会社にはサイバー攻撃は関係ない？

1. ウェブサイトを安全に運用するために
 1.1. ウェブサイトと脆弱性
 1.2. 脆弱性が元で起きる問題の例

2. 脆弱性対策を必ず行うべきウェブサイトとは
(1) 個人情報、顧客情報等の重要な情報を預かっている
(2) ウェブサイトに脆弱性となりやすい機能がある
(3) ウェブサイトの構築後にメンテナンスをしていない

3. ウェブサイトの脆弱性対策のポイント
(1) まず脆弱性を知る
(2) 脆弱性への対処をより詳しく検討する
(3) ウェブサイトの構築時にセキュリティに配慮する
(4) セキュリティ対策を外部に任せる
(5) セキュリティの担当者と作業を決めておく
(6) 脆弱性の報告やトラブルには適切に対処する
(7) 難しければ専門家に支援を頼む

参考資料
参考 1. 脆弱性（ぜいじゃくせい）とは？
参考 2. ウェブサイトの脆弱性対策の要否に関するチェックリスト
参考 3. 脆弱性の指摘への対処
参考 4. 情報セキュリティ早期警戒パートナーシップ
参考 5. 参考 URL

3. ガイドラインの見直しに関する調査

経済産業省による告示の改正や、パートナーシップの業務プロセス上の問題解決等に伴い、ガイドライン改訂が必要となる。本年度研究会ではこの改訂に向けた検討を実施した。これらの検討結果のうち、3.1.節については、研究会委員の意見を集約した。また、3.2.節～3.4.節については、本年度の検討内容を踏まえ、次年度以降引き続き脆弱性研究会等にて検討する。

3.1. 告示の改正への対応に向けた検討

脆弱性研究会のオブザーバである経済産業省では、これまでのパートナーシップの活動を踏まえ、調整不能案件[4]の公表を実施できるようにすべく、告示の改正を検討している（調整不能案件およびその公表の考え方については2011 年度の検討結果[5, 6]を参照されたい）。そこで、本年度の研究会では、これまでの検討、および経済産業省における検討内容を踏まえ、告示改正に関する意見を集約するとともに、必要となるガイドラインの改訂について検討を行った。

(1) 告示改正に関する意見

告示の改正に関して研究会委員より得た主な意見を以下に示す。

① 「調整不能」の示し方について

・告示とガイドラインで、「調整不能」に該当する案件の定義について整合させるべき。

② 公表判定委員会について

・公表判定委員会が公表すべきと判断したが、実際には公表しないケースがあるのは適切でない。公表判定委員会の判断は参考意見か、決定か明確にすべきである。

③公表に関する裏付けについて

・そもそも告示は合意なしに公表できる内容であったと思う。

・告示では、調整機関が定めた公表日までに調整ができなければ公表できる内容であったと思われる。このままだと、公表判定委員会によらず調

[4] JPCERT/CC が製品開発者と連絡がとれない、または調整が難航して事実上調整が困難な案件。

[5] IPA「脆弱性情報に係る調整不能案件の公表に関する基礎調査報告書」, 2011/09 http://www.ipa.go.jp/security/fy23/reports/vuln_handling/chouseifunou_basicrep.pdf

[6] IPA「脆弱性情報に係る調整不能案件の公表のあり方に関する調査報告書」, 2011/09 http://www.ipa.go.jp/security/fy23/reports/vuln_handling/chouseifunou_report.pdf

整機関が独自に公表できることになるので、整理が必要ではないか。
・連絡がとれているが脆弱性や評価について意見が合わなかった場合、調整不能とはせず、調整した結果として、公表する場合の手続きで残すという考え方もある。
・元来、告示・ガイドラインでは、製品開発者の合意を得るべく努力することが前提。
・調整不能案件の公表判定のプロセスに進んだ後に、改めて調整が進む場合について配慮すべきである。

⑵ ガイドライン改訂について

ガイドラインの改訂について、研究会委員より得た主な意見を以下に示す。

①公表判定委員会について

・公表判定委員会の委員の利害関係の有無は重要。選任する方法を工夫してほしい。
・他の例だと、委員を多めにプールして、案件毎に利害関係のない適任者を選出する方法がある。

②その他

・脆弱性情報の流通に関してはボリューム、スピード、カバレージの率が性能指標であり、組織として業務効率を示すことが重要。今回の改正で新たな機能が追加されるので、それらについても明示していくべきである。

なお、本年度の検討では、告示改正の検討状況を踏まえ、その時点でのガイドラインの改訂案を策定したが、まだ告示の改正内容が確定していないため、ガイドライン改訂案も暫定的な内容にとどまる。したがって、ガイドライン改訂案の公表は、告示改正の内容が確定した段階で、その変更を反映した版で実施するものとする。

3.2.制度運用上の問題解決に関する改訂に向けた検討

情報セキュリティ早期警戒パートナーシップの制度運用上の問題として以下の項目を採り上げ、これらを解決するためのガイドライン改訂の要否について、脆弱性研究会に提起した。これらの問題解決については、次年度以降、引き続き検討するものとする。

(1) 匿名の届出の取扱い

a)概要

製品の脆弱性届出では、発見者に氏名・連絡先の記載を求めており、IPA の受理判断の基準に「匿名の届出でないこと（発見者への連絡が可能であることを確認できること)」という条件が明記されている。

したがって、匿名であることが明らかであれば不受理となるが、それが本当に脆弱性であった場合、それを見逃すことになりかねない。

なお、ウェブサイトの脆弱性でも発見者に氏名・連絡先の記載を求めているが、IPA の受理判断の基準には匿名か否かに係る条件はない。

b)検討内容

脆弱性研究会や関係者の検討において、以下の指摘が得られた。

- 原則として、脆弱性を見逃すことがない方向に動くべきである。結果的に届出があったにもかかわらず、対応しなかったという事態がないように対応すべき。
- 制度立ち上げ時の議論では、犯罪に当たる方法で脆弱性を確認することを抑制するという目的で、氏名を記載することとした。実際には、それで犯人を追及できる訳でもなく予防策としては不十分だが、氏名を記載することで、ある種の責任を認識していただく意図であった。責任ある届出を求める意味はあるのではないか。
- 実際の作業上は、匿名であることより発見者と連絡が取れることのほうが重要である。匿名か否かと、発見者への連絡が可能か否かという点は別の条件であり、分けて扱うべき。連絡が取れて、届け出いただいた情報が脆弱性である場合には、受け付けるべきではないか。
- 現実の問題として、匿名か否かの事実関係について確認する妥当な手段はない。

(2) ソフトウエア製品とウェブサイトの境界領域

a)概要

情報セキュリティ早期警戒パートナーシップの制度では、ソフトウエア製品の脆弱性かウェブサイトの脆弱性かによって処理の流れが異なる。しかし、ソフトウエア製品とウェブサイトの境界領域に係る脆弱性の場合、それがどちらの問題であるか分析しなければ判別できないケースがあり、それによりしばしば制度上取扱いが難しい状況に陥る。

たとえば、ウェブサイトの脆弱性として届け出られた案件が、検証の結果、ソフトウエア製品の脆弱性であることが判明し、製品開発者に連絡したところ、既知の脆弱性とわかるケースが年に数件程度発生している。「既知の脆弱性」であるため取扱いルール上は JVN 公表をしていないが、未対応のサイトが残っていることから、製品利用者への周知が十分でないケースもあると考えられる。

b)検討内容

脆弱性研究会や関係者の検討において、以下の指摘が得られた。

- 検証結果に応じて、ケースバイケースの柔軟な対応が必要となる。
- 製品開発者から、一般に公表された内容が脆弱性と認識できる内容でない場合には、製品利用者が対応の必要性を理解できないことから、JVN 公表などの対処が必要ではないか。

3.3.研究会における運用上の問題点指摘による改訂に向けた検討

脆弱性研究会では、以下の事項に関するガイドライン改訂等の検討の状況について報告された。

(1) 制御システム用製品の脆弱性情報の取扱い

近年、マルウェアによる攻撃等を契機として、制御システムセキュリティのリスクが注目されている。特に、米国では、ICS-CERT が制御システムの脆弱性に関する新しい公表ルールを発表、また官民連携による制御システムセキュリティ合同 WG（ICSJWG）が一般的な制御システムの脆弱性公表フレームワークを策定するなど、脆弱性情報の公表を巡る動きが活発化している。さらに、米セキュリティ企業が日本の制御システム用製品の脆弱性を突く攻撃手法を公表するなど、制御システム用製品ベンダを取り巻く状況は急速に変わりつつある。

我が国の制御システム用製品ベンダが脆弱性情報の公表に向けた対応を迫られる可能性を考慮すれば、当該ベンダやセキュリティ関連組織等の間で、制御システム用製品の脆弱性情報に関する取扱のルールを明確化することにより、国際的な協力関係を形成できる立ち位置を築くことが望まれる。

そこで、JPCERT コーディネーションセンターでは、2012 年 9 月、「制御システム用製品の脆弱性情報の取扱に関する研究会」を発足し、以下の検討に着手した。

- ・制御システム用製品ベンダにおける脆弱性対応のあり方
- ・情報セキュリティ早期警戒パートナーシップの関連制度（告示、ガイドライン）との整合

なお、上記研究会の検討は 2013 年 3 月の取りまとめを予定しているが、その後、脆弱性研究会においてその成果を踏まえたガイドラインの見直しについて引き続き検討する見込みである。

3.4. 小企業のウェブサイト脆弱性対応に係る効果的な運用改善のための改訂に向けた検討

a)概要

小企業のウェブサイト運営者における脆弱性対策を促進する効果的な運用改善の方向について検討した。

b)検討結果

脆弱性研究会や関係者の検討において、以下の指摘が得られた。

・小企業では、ウェブサイトの構築・運用は外注先に任せきりで、ほとんど状況を把握していないケースが少なくない。

・IPA からの通知メールを受けた人がそのままブログに掲載したケースがある。高圧的な印象があるなら改善し、送付先によって通知文を使い分けることも検討してはどうか。

・IPA から小企業のウェブサイトの脆弱性について通知した際、必要に応じて、地域の IT コーディネータ等、専門家を紹介することを検討してはどうか。

4. 今後の課題

今後取り組むべき検討課題について以下に示す。

(1) 制御システム用製品の脆弱性情報の取扱に関する検討への対応

3.3.節に示したとおり、「制御システム用製品の脆弱性情報の取扱に関する研究会」からの提言を踏まえ、制御システム分野への対応と整合に必要なガイドライン等の改訂を検討する。具体的には、上記研究会の提言に沿った告示改正に伴うガイドラインへの反映を検討する。また、上記研究会の提言に基づくガイドライン案について、現行のガイドラインと一本化する場合には、運用上の整合性を含め、必要な改訂を検討する。

(2) 制度運用上の問題解決に応じたガイドラインの見直し

関係者から提言される制度運用上の問題解決に柔軟に対応し、適切にガイドラインを改訂する。具体的には、3.2.節、3.4.節において提示した問題に加え、以下の項目も挙げられている。

- サポートが終了した製品の脆弱性届出に関する取扱い
- 製品開発者が脆弱性対策についてすべての製品利用者に通知可能な場合の取扱い
- ガイドラインの記載内容と運用上の対応とのずれ

(3) 国際化に伴う情報セキュリティ早期警戒パートナーシップの展開

現在、社外関係者に対する製品開発者の脆弱性開示に係る対応を規定したガイドライン[7]や製品開発者の組織内における脆弱性情報取扱いの手順を規定したガイドライン[8]が、それぞれ国際標準化作業の最終段階（DIS：Draft International Standard）を迎えている。今後は、国際標準と対比する形で、パートナーシップの位置づけが問われることになる。

また、パートナーシップは、現在は国内のユーザのための仕組みとして機能しているが、今後は、国際展開を図る我が国企業を支援する役割を担うことを検討すべきとの指摘もある。

こうした意見を踏まえ、パートナーシップの今後の在り方について検討する。

---

[7] ISO/IEC 29147（Vulnerabilty Disclosure：脆弱性開示）

[8] ISO/IEC 30111（Vulnerability Handling Process：脆弱性ハンドリングプロセス）

参考１

2012 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

2013 年 1 月 31 日時点

座長	土居 範久	中央大学
委員	秋山 卓司	社団法人日本インターネットプロバイダー協会（JAIPA）
	今井 秀樹	中央大学
	北澤 繁樹	三菱電機株式会社
	楠堂 忠夫	パナソニック株式会社
	小島 健司	東芝ソリューション株式会社
	下村 正洋	NPO 日本ネットワークセキュリティ協会（JNSA）
	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	独立行政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
	高橋 正和	日本マイクロソフト株式会社
	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	KDDI 株式会社
	西尾 秀一	株式会社 NTT データ
	野山 英郎	株式会社日立製作所
	早貸 淳子	一般社団法人 JPCERT コーディネーションセンター（JPCERT/CC）
	山口 英	奈良先端科学技術大学院大学
	山崎 圭吾	株式会社ラック

（五十音順、敬称略）

オブザーバ

上村 昌博	経済産業省 情報セキュリティ政策室長
守谷 学	経済産業省 情報セキュリティ政策室 課長補佐
安藤 成純	経済産業省 情報セキュリティ政策室 係長
坂本 寛	経済産業省 情報セキュリティ政策室 係長
小島 智行	経済産業省 情報セキュリティ政策室 係長
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）
渕 眞澄	社団法人日本情報システム・ユーザー協会（JUAS）
安田 直義	NPO 日本ネットワークセキュリティ協会（JNSA）
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）
古田 洋久	一般社団法人 JPCERT コーディネーションセンター（JPCERT/CC）
佐藤 祐輔	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）

（順不同、敬称略）

独立行政法人 情報処理推進機構

藤江 一正	理事長
仲田 雄作	理事

事務局

笹岡 賢二郎	独立行政法人 情報処理推進機構
湯原 孝志	独立行政法人 情報処理推進機構（2012 年 12 月迄）
堀田 博幸	独立行政法人 情報処理推進機構（2012 年 11 月から）
小林 偉昭	独立行政法人 情報処理推進機構
金野 千里	独立行政法人 情報処理推進機構
中 野　学	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
相馬 基邦	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
大森 雅司	独立行政法人 情報処理推進機構
村瀬 一郎	株式会社三菱総合研究所
川口 修司	株式会社三菱総合研究所
井上 信吾	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（2012 年 11 月 9 日）
・昨年度の研究会における検討について
・2011 年度～2012 年度のパートナーシップの活動状況について
・制御システム用製品の脆弱性情報の取扱いに関する研究会について
・今年度の研究会活動について
・小企業のウェブサイト運営に関する実態調査について

■研究会第 2 回会合（2013 年 1 月 8 日）
・前回の開催結果概要について
・調整不能案件の公表に係る告示・ガイドラインの改訂について
・小企業のウェブサイト運営に関する実態調査 アンケート調査について
・制御システム用製品の脆弱性情報の取扱に関する研究会の検討状況について

■研究会第 3 回会合（2013 年 1 月 21 日）
・前回の開催結果概要について
・告示・ガイドラインの改訂について
・制御システム用製品の脆弱性情報の取扱に関する研究会からの提案について
・企業ウェブサイトのための脆弱性対策ガイド（案）について