ソフトウェア等の脆弱性関連情報の取扱いに関する活動報告レポート

[2015 年第 1 四半期（1 月～3 月）]

ソフトウェア等の脆弱性関連情報の取扱いに関する活動報告レポートについて

日本における公的な脆弱性関連情報の取扱制度である「情報セキュリティ早期警戒パートナーシップ（本報告書では本制度と記します）」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）」に基づき、2004 年 7 月より運用されています。本制度において、独立行政法人情報処理推進機構（以下、IPA）と一般社団法人 JPCERT コーディネーションセンター（以下、JPCERT/CC）は、脆弱性関連情報の届出の受付や脆弱性対策情報の公表に向けた調整などの業務を実施しています。

本レポートでは、2015 年 1 月 1 日から 2015 年 3 月 31 日までの間に実施した、脆弱性関連情報の取扱いに関する活動及び脆弱性の傾向について紹介しています。

独立行政法人情報処理推進機構 技術本部 セキュリティセンター
一般社団法人 JPCERT コーディネーションセンター
2015 年 4 月 23 日

目次

1. 2015 年第 1 四半期　ソフトウェア等の脆弱性関連情報に関する届出受付状況

1-1. 脆弱性関連情報の届出受付状況

～ 脆弱性の届出件数の累計は 10,898 件 ～

表 1-1 は本制度[*1]における届出状況について、2015 年第 1 四半期の脆弱性関連情報（以降「脆弱性」）の届出件数および届出受付開始（2004 年 7 月 8 日）から今四半期までの累計を示しています。今期のソフトウェア製品に関する届出件数は 84 件、ウェブサイト（ウェブアプリケーション）に関する届出は 161 件、合計 245 件でした。届出受付開始からの累計は 10,898 件で、内訳はソフトウェア製品に関するもの 2,034 件、ウェブサイトに関するもの 8,864 件でウェブサイトに関する届出が全体の 81%を占めています。

表 1-1. 届出件数

分類	今期件数	累計
ソフトウェア製品	**84** 件	**2,034** 件
ウェブサイト	**161** 件	**8,864** 件
合計	**245** 件	**10,898** 件

図 1-1 のグラフは過去 3 年間の届出件数の四半期ごとの推移を示したものです。今四半期は、ソフトウェア製品に関する届出が前四半期とほぼ同じ件数、ウェブサイトに関する届出が**前四半期の約 4 割に減少**しました。表 1-2 は過去 3 年間の四半期ごとの届出の累計および 1 就業日あたりの届出件数の推移です。今四半期の 1 就業日あたりの届出件数は 4.17[*2] 件でした。

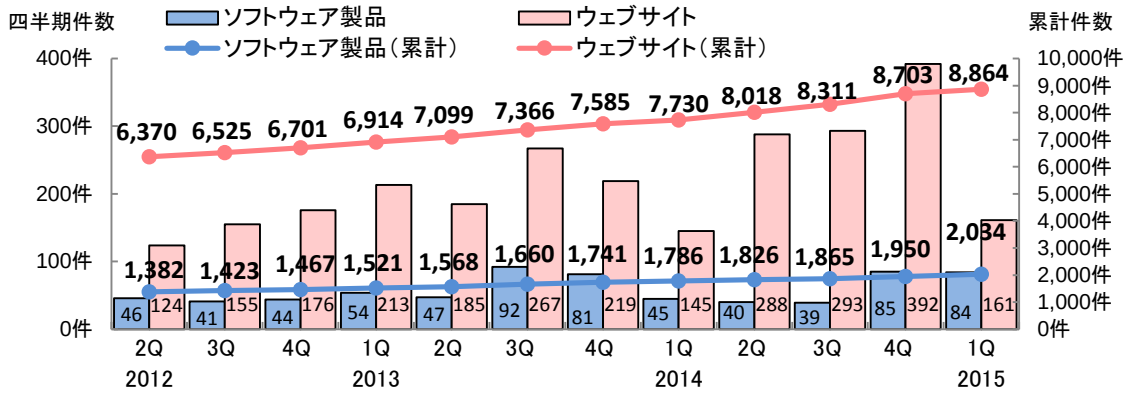


図1−1. 脆弱性の届出件数の四半期ごとの推移

表 1-2. 届出件数（過去 3 年間）

	2012 2Q	3Q	4Q	2013 1Q	2Q	3Q	4Q	2014 1Q	2Q	3Q	4Q	2015 1Q
累計届出件数[件]	7,752	7,948	8,168	8,435	8,667	9,026	9,326	9,516	9,844	10,176	10,653	10,898
1 就業日あたり[件/日]	4.00	3.98	3.78	3.96	3.96	4.00	4.03	4.01	4.04	4.07	4.17	4.17

[*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
https://www.ipa.go.jp/security/ciadr/partnership_guide.html
https://www.jpcert.or.jp/vh/index.html

[*2] 1 就業日あたりの届出件数は、「累計届出件数」/「届出受付開始からの就業日数」にて算出

1-2. 脆弱性の修正完了状況

～ ソフトウェア製品およびウェブサイトの修正件数は累計 7,194 件～

表 1-3 は今四半期と届出受付開始から今四半期までのソフトウェア製品とウェブサイトの修正完了件数を示しています。ソフトウェア製品の場合、修正が完了すると JVN に公表しています（回避策の公表のみでプログラムの修正をしていない場合を含む）。

表 1-3. 修正完了件数

分類	今期件数	累計
ソフトウェア製品	**41** 件	**1,000** 件
ウェブサイト	**253** 件	**6,194** 件
合計	**294** 件	**7,194** 件

今四半期に JVN 公表したソフトウェア製品の件数は 41 件 (*3)（累計 1,000 件）でした。そのうち、4 件が製品開発者による自社製品の脆弱性の届出でした。また、届出を受理してから JVN 公表までの日数が 45 日 (*4) 以内だったのは 9 件（22%）でした。

また、修正完了したウェブサイトの件数は 253 件（累計 6,194 件）でした。これらは届出を受け、IPA がウェブサイト運営者に通知を行い、今四半期に修正を完了したものです。修正を完了した 253 件のうち、ウェブアプリケーションを修正したものは 183 件（72%）、当該ページを削除したものは 70 件（28%）、運用で回避したものは 0 件でした。なお、修正を完了した 253 件のうちウェブサイト運営者へ脆弱関連情報を通知してから 90 日 (*5) 以内に修正が完了したのは 202 件（80%）でした。今四半期は、90 日以内に修正完了した割合が、前四半期（163 件中 110 件（67%））より増加しています。

1-3. 連絡不能案件の取扱状況

本制度では、連絡が取れない製品開発者を「連絡不能開発者」と呼び、連絡の糸口を得るため、当該製品開発者名等を公表して情報提供を求めています (*6)。製品開発者名を公表後、3 ヵ月経過しても製品開発者から応答が得られない場合は、製品情報（対象製品の具体的な名称およびバージョン）を公表します。それでも応答が得られない場合は、情報提供の期限を追記します。情報提供の期限までに製品開発者から応答がない場合は、当該脆弱性情報の公表に向け、「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」に定められた公表条件を満たしているかを公表判定委員会 (*7) で審議します。公表が適当と判定された脆弱性情報は JVN に公表されます。

今四半期に新たに製品開発者名を公表したものはなく、製品開発者と連絡が取れたため調整を再開した 3 件を削除しました。2015 年 3 末時点の連絡不能開発者の累計公表件数は 160 件、その内製品情報を公表しているものは 143 件となりました。

(*3) P.10 表 2-3 参照
(*4) JVN 公表日の目安は、脆弱性の取扱いを開始した日時から起算して 45 日後としています。
(*5) 対処の目安は、ウェブサイト運営者が脆弱性の通知を受けてから、3 ヶ月以内としています。
(*6) 連絡不能開発者一覧：https://jvn.jp/reply/index.html
(*7) 連絡不能案件の脆弱性情報を公表するか否かを判定するために IPA が組織する。法律、情報セキュリティ、当該ソフトウェア製品分野の専門的な知識経験を有する専門家、かつ、当該案件と利害関係のない者で構成される。

1-4. 脆弱性の傾向について

WordPress プラグイン、テーマの脆弱性に注意

～セキュリティパッチの適用は CMS 本体だけではない！～

2015 年第 1 四半期は、41 件の脆弱性対策情報が JVN に公表されました。そのうち 6 件は CMS（Content Management System）の一種である「WordPress」の機能を拡張する部品ともいえる、「プラグイン」や「テーマ」というソフトウェアに作りこまれた脆弱性でした（表 1-4）。この 6 件の中にはウェブ改ざんや情報漏えいにつながる可能性のある SQL インジェクションの脆弱性や、CAPCHA というウェブサイトへのアクセスが人間かを判別する画像認証機能が回避されてしまう脆弱性などがありました。

表 1-4. 2015 年第 1 四半期 JVN 公表一覧

JVN 公表日	JVN 番号	脆弱性	CVSS 基本値
2015/3/31	JVN#75615300	WordPress 用プラグイン「All in One SEO Pack」における情報管理不備の脆弱性	5.0
2015/3/26	JVN#97281747	WordPress 用テーマ「flashy」におけるクロスサイト・スクリプティングの脆弱性	4.3
2015/3/6	JVN#87204433	WordPress 用プラグイン「All In One WP Security & Firewall」におけるクロスサイト・リクエスト・フォージェリの脆弱性	2.6
2015/3/6	JVN#30832515	WordPress 用プラグイン「All In One WP Security & Firewall」における SQL インジェクションの脆弱性	5.1
2015/3/3	JVN#55063777	WordPress 用プラグイン「Google Captcha (reCAPTCHA) by BestWebSoft」における CAPTCHA 保護メカニズムを回避される脆弱性	5.0
2015/3/3	JVN#93727681	WordPress 用プラグイン「Captcha」における CAPTCHA 保護メカニズムを回避される脆弱性	5.0

「WordPress プラグイン」は、「WordPress」で作成したウェブサイトのカスタマイズ・機能強化等を支援するソフトウェアです。また、「WordPress テーマ」は、ウェブサイトの見栄えや構成を容易に変更出来るソフトウェアです。このような 「プラグイン」や「テーマ」などの“拡張機能”を提供するソフトウェアは、不特定の第三者（CMS 製品開発者以外）により自由に開発されて提供されています。そのため、安全性への配慮が十分でない場合“拡張機能”に脆弱性が作りこまれてしまうことがあります。下記は 2014 年 1 月以降 JVN iPedia に登録された、CMS 本体とその“拡張機能”の脆弱性対策情報を四半期毎に集計したものです（図 1-2）。今四半期までの合計は 440 件で、そのうち 90%に相当する 398 件が CMS の“拡張機能”の脆弱性対策情報でした。

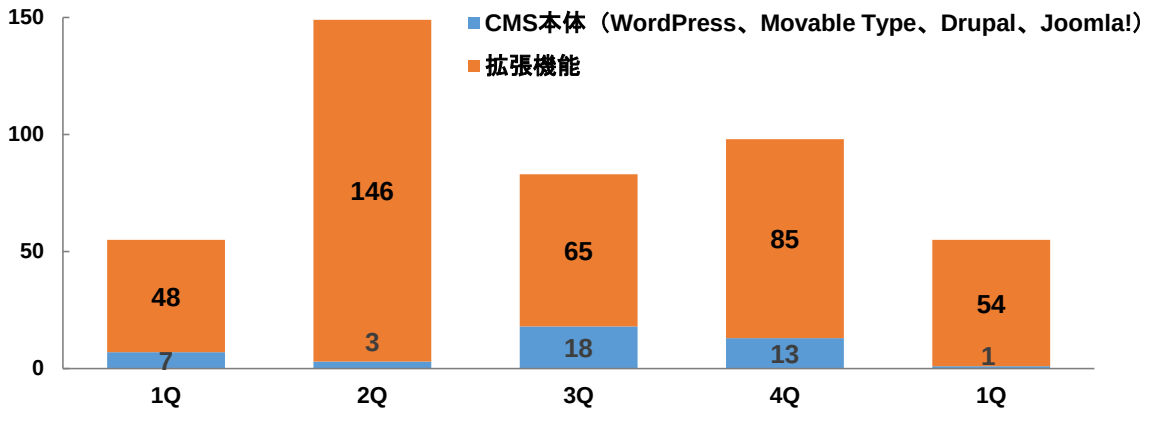


図1-2. JVN iPedia に登録されたCMSに関する脆弱性対策情報（2014年1月～2015年3月）

このように利用者の多い“拡張機能”に脆弱性があった場合、それを使用して作成したウェブサイトには脆弱性が作りこまれてしまい悪意ある第三者によりウェブサイトが改ざんされたり、重要な情報が窃取されたりする可能性があります。一部の報道や警察庁[*8]によると、2015 年 3 月に国内で発生したウェブサイト改ざんの中には「WordPress プラグイン」の脆弱性が悪用された被害がありました。この被害の発生した「プラグイン」 には 2015 年 2 月に最新版が配布されていましたので、このサイトに最新版が適用されていなかった可能性があります。

当事者はそれぞれ下記の通り、安全なソフトウェアに求められる作業を実施してください。

■ “拡張機能”等ソフトウェアの製品開発者
- 脆弱性を作りこまないよう、安全性を考慮した開発を行う
- 作成した“拡張機能”が CMS 本体に脆弱性を作りこんでしまわないかを検証する
- 脆弱性が発見された場合は、迅速に修正する
- 修正パッチを利用者に向けて配布、告知し、アップデートを促す

■ CMS および CMS“拡張機能”の利用者
- 使用している CMS および CMS の“拡張機能”等、ソフトウェアの把握する
- 使用しているソフトウェアの脆弱性対策情報の収集する
- 使用していないソフトウェアの削除する
- “拡張機能”を使用し作成したウェブサイトに脆弱性が作りこまれていないかを検証する
- 最新版へのアップデートする

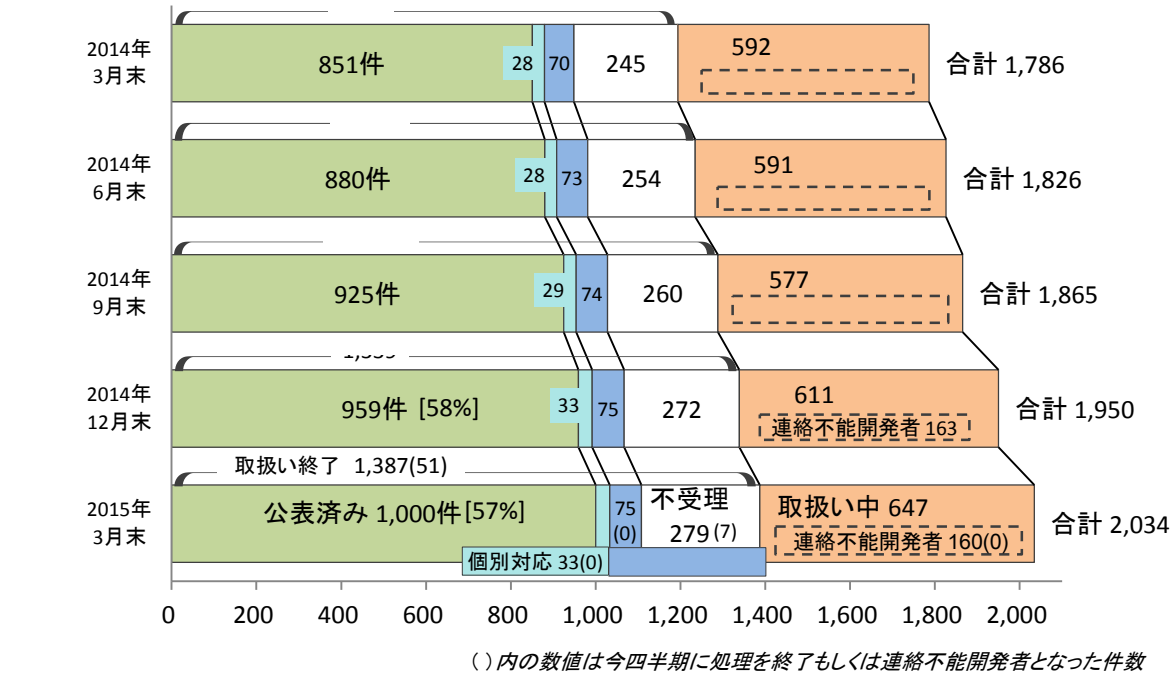
[*8] 「Islamic State（ISIS）」と称する者によるウェブサイト改ざんについて
http://www.npa.go.jp/keibi/biki/201503kaizan.pdf
「Islamic State（ISIS）」と称する者によるウェブサイト改ざんに係る注意喚起について
http://www.npa.go.jp/cyberpolice/detect/pdf/20150312.pdf

2. ソフトウェア等の脆弱性に関する取扱状況（詳細）

2-1. ソフトウェア製品の脆弱性

2-1-1. 処理状況

図 2-1 のグラフはソフトウェア製品の脆弱性届出の処理状況について、四半期ごとの推移を示しています。2015 年 3 月末時点の届出の累計は 2,034 件で、今四半期に脆弱性対策情報を JVN 公表したものは 41 件（累計 1,000 件）でした。また、製品開発者が JVN 公表を行わず「個別対応」したものは 0 件（累計 33 件）、製品開発者が「脆弱性ではない」と判断したものは 0 件（累計 75 件）、「不受理」としたものは 7 件 (*9)（累計 279 件）、取扱い中は 647 件でした。647 件のうち、連絡不能開発者 (*10) 一覧へ新たに公表したものは 0 件で、2015 年 3 月末時点の累計は 160 件になりました。



( ) 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

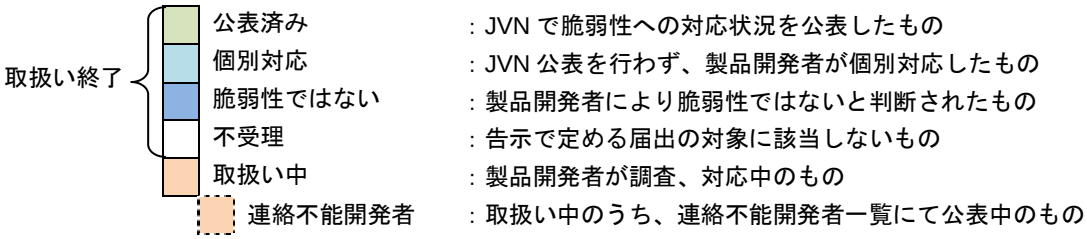


図 2-1. ソフトウェア製品脆弱性の届出処理状況（四半期ごとの推移）

(*9) 内訳は今四半期の届出によるもの 2 件、前四半期までの届出によるもの 5 件。

(*10) 連絡不能開発者一覧への公表および一覧からの削除が複数回行われた製品開発者の公表回数は、その累計を計上しています。

以下に、今までに届出のあったソフトウェア製品の脆弱性 2,034 件のうち、不受理を除いた 1,755 件の届出を分析した結果を記載します。

2-1-2. ソフトウェア製品別届出件数

図 2-2、2-3 のグラフは、届出された製品の分類です。図 2-2 は製品種類別割合を、図 2-3 は過去 2 年間の届出件数の推移を四半期ごとに示したものです。

累計では、「ウェブアプリケーションソフト」が最も多く 39%となっています。今四半期の届出件数で最も多いのも「ウェブアプリケーションソフト」で、次いで「アプリケーション開発・実行環境」となっています。また、スマートフォンやタブレットなどのスマートデバイス向けのアプリの割合が増加したため、**今四半期より「スマートフォン向けアプリ」[*11]という分類を新設し、過去の届出を分類し直しました**。

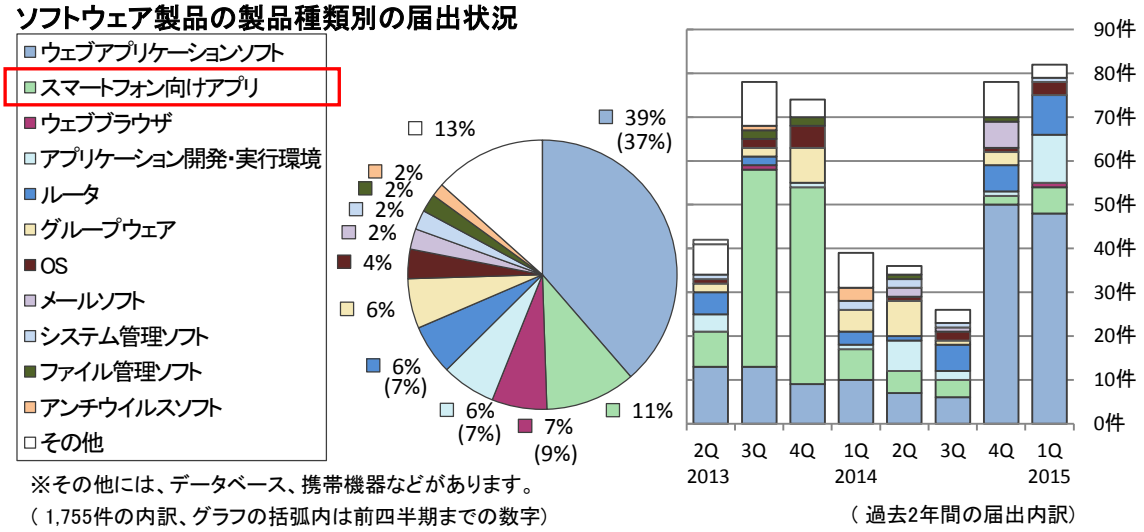


図2-2. 届出累計の製品種類別割合

図2-3. 四半期ごとの製品種類別届出件数

図 2-4、2-5 のグラフは、届出された製品のライセンスを「オープンソースソフトウェア」（OSS）と「それ以外」で分類しています。図 2-4 は届出累計の分類割合を、図 2-5 は過去 2 年間の届出件数の推移を四半期ごとに示したものです。

累計では、オープンソースソフトウェアが 31%を占めています。オープンソースソフトウェアの件数は 10 件前後で推移してきましたが、今四半期は 36 件と急増しました。これは、同一のソフトウェア製品に複数の脆弱性が届出されたためです。

[*11] 「スマートフォン向けアプリ」は、「iOS」、「Android OS」上で動作するアプリを集計しています。

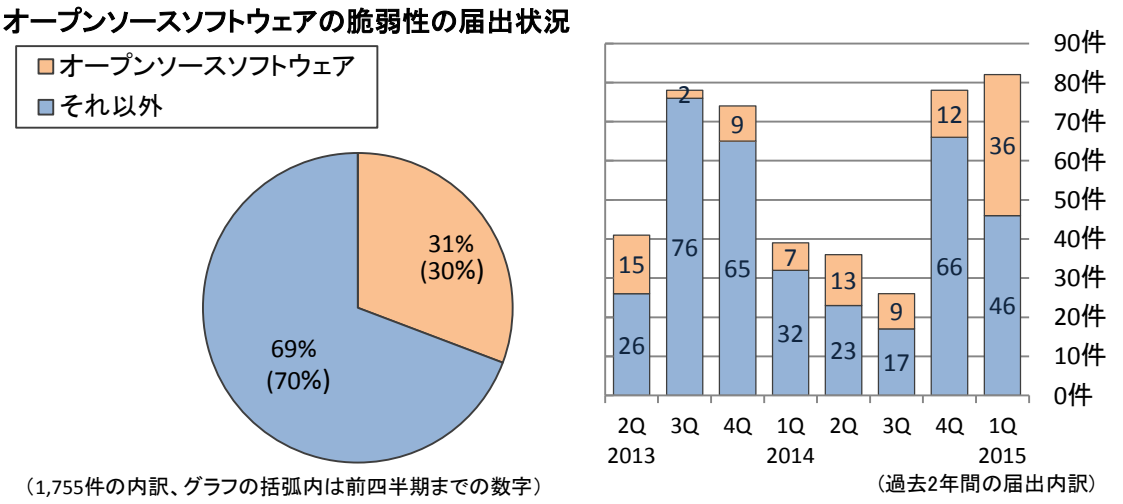


図2-4. 届出累計のオープンソースソフトウェア割合

図2-5. 四半期ごとのオープンソースソフトウェア届出件数

2-1-3. 脆弱性の原因と影響別件数

図 2-6、2-7 のグラフは、届出された脆弱性の原因を示しています。図 2-6 は届出累計の脆弱性の原因別割合を、図 2-7 は過去 2 年間の原因別の届出件数の推移を四半期ごとに示しています。累計では、「ウェブアプリケーションの脆弱性」が過半数を占めています。また、**今四半期の届出件数は「その他実装上の不備」が最多でした**。これは、DLL の読み込みに関する脆弱性 (*12) や署名検証の回避に関する脆弱性が多く届出られたためです。

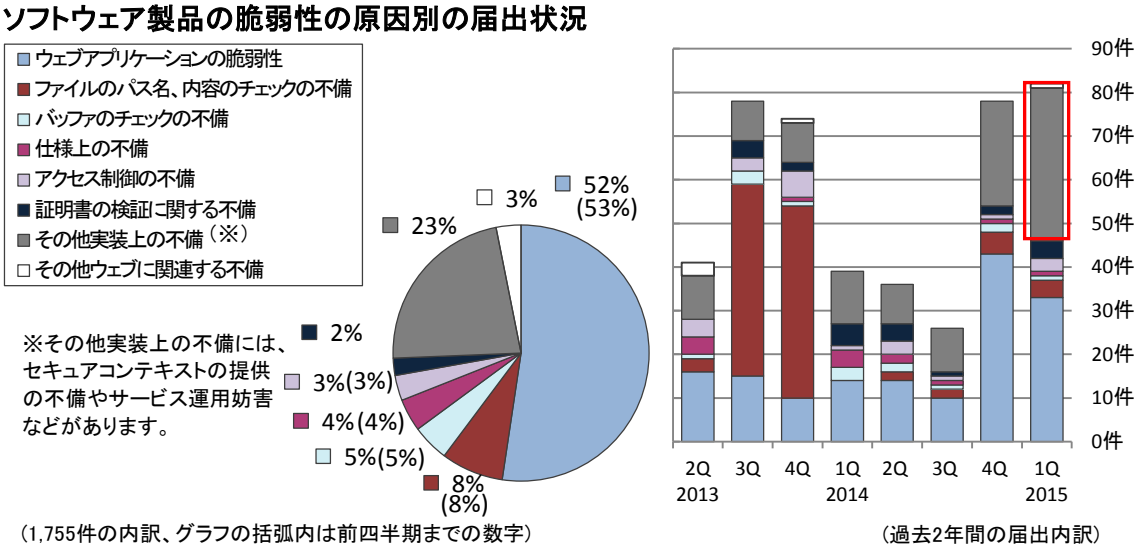


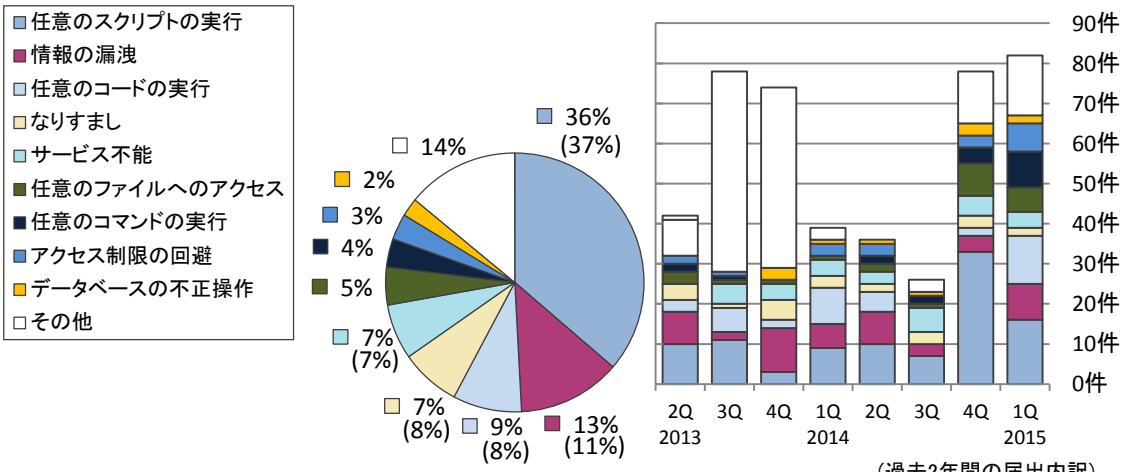
図2-6. 届出累計の脆弱性の原因別割合

図2-7. 四半期ごとの脆弱性の原因別届出件数

図 2-8、2-9 のグラフは、届出された脆弱性がもたらす影響を示しています。図 2-8 は届出累計の影響別割合を、図 2-9 は過去 2 年間の影響別届出件数の推移を四半期ごとに示しています。累計では「任意のスクリプトの実行」が最も多く、次いで「情報の漏洩」となっています。今四半期も、「任意のスクリプト実行」が最も多く、次いで「任意のコードの実行」が多く届出されました。なお、2013 年第 3、第 4 四半期に「その他」が多いのは、「ファイルのパス名、内容のチェックの不備」によりもたらされる影響が「その他」に分類されたためです。

(*12) Windows プログラムの DLL 読み込みに脆弱性：https://jvn.jp/vu/JVNVU707943/

ソフトウェア製品の脆弱性がもたらす影響別の届出状況



（1,755件の内訳、グラフの括弧内は前四半期までの数字）

図2-8. 届出累計の脆弱性がもたらす影響別割合

（過去2年間の届出内訳）

図2-9. 四半期ごとの脆弱性がもたらす影響別届出件数

2-1-4. 調整および公表件数

JPCERT/CC は、本制度に届け出られた脆弱性情報のほか、海外の製品開発者や CSIRT などからも脆弱性情報の提供を受けて、国内外の関係者と脆弱性対策情報の公表に向けた調整を行っています[*13]。これらの脆弱性に対する製品開発者の対応状況は、IPA と JPCERT/CC が共同運営している脆弱性対策情報ポータルサイト JVN（Japan Vulnerability Notes）（URL : https://jvn.jp/ ）に公表しています。表 2-1、図 2-10 のグラフは、公表件数を情報提供元別に集計し、今四半期の公表件数、過去 3 年分の四半期ごとの公表件数の推移等を示したものです。

表 2-1.　脆弱性の提供元別 脆弱性公表件数

	情報提供元	今期件数	累計
①	国内外の発見者からの届出、製品開発者から自社製品の届出を受け JVN で公表した脆弱性	41 件	1,000 件
②	海外 CSIRT 等から脆弱性情報の提供を受け JVN で公表した脆弱性	36 件	1,205 件
	合計	77 件	2,205 件

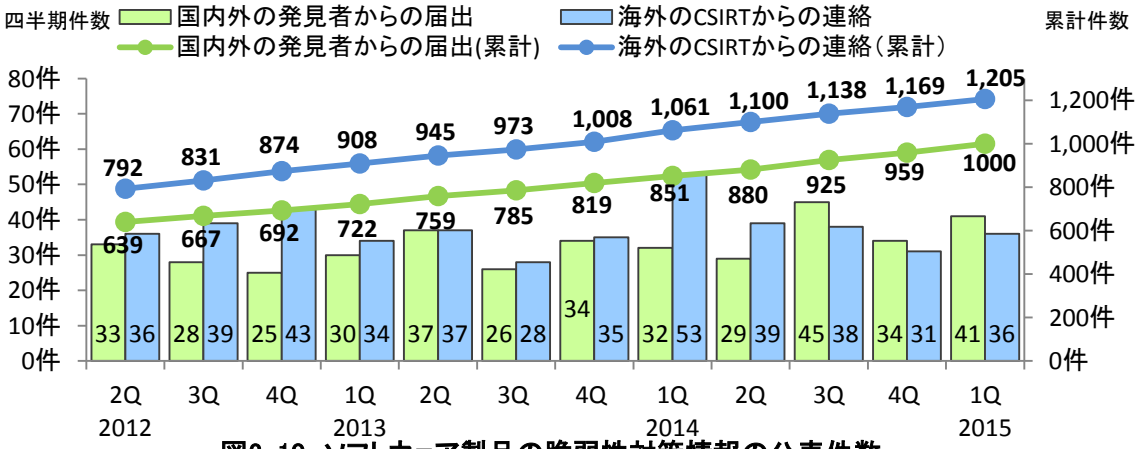


図2−10. ソフトウェア製品の脆弱性対策情報の公表件数

（1）　国内外の発見者および製品開発者から届出を受け JVN で公表した脆弱性

届出受付開始から今四半期までに対策情報を JVN 公表した脆弱性（1,000 件）について、図 2-11 は受理してから JVN 公表するまでに要した日数を示したものです。45 日以内は 32%、45 日を超過した件数は 68%でした。表 2-2 は過去 3 年間において 45 日以内に JVN 公表した件数の割合推移を四半期ごとに示したものです。製品開発者は脆弱性が悪用された場合の影響を認識し、迅速な対策を講じる必要があります。

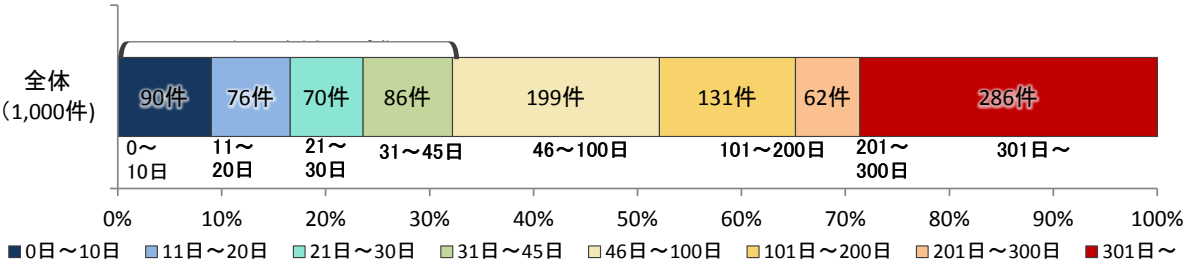


図2−11. ソフトウェア製品の脆弱性公表日数

表 2-2.　45 日以内に JVN 公表した件数の割合推移（四半期ごと）

2012 2Q	3Q	4Q	2013 1Q	2Q	3Q	4Q	2014 1Q	2Q	3Q	4Q	2015 1Q
34%	35%	34%	33%	33%	33%	34%	34%	34%	33%	33%	32%

[*13] JPCERT/CC 活動概要 Page15～21（https://www.jpcert.or.jp/pr/2015/PR20150416.pdf）を参照下さい。

表 2-3 は国内の発見者および製品開発者から受けた届出 41 件について、今四半期に JVN 公表した脆弱性を深刻度別に示しています。オープンソースソフトウェアに関する脆弱性が 12 件（表 2-3 の*1）、製品開発者自身から届けられた自社製品の脆弱性が 3 件（表 2-3 の*2）、複数開発者・製品に影響がある脆弱性が 1 件（表 2-3 の*3）、組込みソフトウェア製品の脆弱性が 4 件（表 2-3 の*4）ありました。

表 2-3. 2015 年第 1 四半期に JVN で公表した脆弱性

項番	脆弱性	セキュリティ上の問題点	JVN 公表日	CVSS 基本値
脆弱性の深刻度=レベル III（危険）、CVSS 基本値=7.0～10.0				
1	「shiromuku(bu2)BBS」における任意のファイルを作成される脆弱性	掲示板ソフト「shiromuku(bu2)BBS」には、任意のファイルを作成される脆弱性が存在しました。このため、サーバ上に任意のファイルを作成され、結果として任意のコードを実行される可能性がありました。	2015 年 1 月 23 日	7.5
2 (*2)	サイボウズ「リモートサービスマネージャー」におけるサービス運用妨害(DoS)の脆弱性	管理ソフト「リモートサービスマネージャー」には、サービス運用妨害(DoS)の脆弱性がありました。このため、第三者により稼働するサーバのリソースが枯渇させられる可能性がありました。	2015 年 1 月 30 日	7.1
3	「C-BOARD Moyuku」における任意のファイルを作成される脆弱性	掲示板ソフト「C-BOARD Moyuku」には、任意のファイルを作成される脆弱性が存在しました。このため、サーバ上に任意のファイルを作成され、結果として任意のコードを実行される可能性がありました。	2015 年 2 月 17 日	7.5
4	「Joyful Note」におけるファイル操作に関する脆弱性	掲示板ソフト「Joyful Note」には、ファイル操作に関する脆弱性が存在しました。このため、第三者によりサーバ上の任意のファイルを作成または削除される可能性がありました。	2015 年 2 月 27 日	7.5
5	「MP Form Mail CGI eCommerce 版」におけるコード・インジェクションの脆弱性	メールフォーム CGI「MP Form Mail CGI eCommerce 版」には、コード・インジェクションの脆弱性が存在しました。このため、サーバ上で、任意の Perl コードを実行される可能性がありました。	2015 年 3 月 20 日	7.5
脆弱性の深刻度=レベル II（警告）、CVSS 基本値=4.0～6.9				
6	シンクグラフィカ製「ダウンロードログ CGI」におけるディレクトリ・トラバーサルの脆弱性	ダウンロード数をカウント・解析する CGI「ダウンロードログ CGI」には、ファイル名の処理に問題があり、ディレクトリ・トラバーサルの脆弱性が存在しました。このため、遠隔の第三者によって、サーバ上の任意のファイルを取得される可能性がありました。	2015 年 1 月 19 日	5.0
7 (*4)	「NP-BBRM」における UPnP に関する脆弱性	有線 LAN ルータ「NP-BBRM」には、UPnP に関する脆弱性がありました。このため、第三者により踏み台として DDoS 攻撃に悪用される可能性がありました。	2015 年 1 月 26 日	5.0
8 (*4)	複数の ASUS 製無線 LAN ルータにおける OS コマンド・インジェクションの脆弱性	ASUS JAPAN が提供する複数の無線 LAN に OS コマンド・インジェクションの脆弱性がありました。このため、第三者により任意のコマンドを実行されたりする可能性がありました。	2015 年 1 月 27 日	5.2

項番	脆弱性	セキュリティ上の問題点	JVN 公表日	CVSS 基本値
9	複数の VMware 製品における任意のファイルが上書きされる脆弱性	複数の VMware 製品には、仮想マシンの設定ファイルを変更可能なユーザによって、ホスト OS 上の任意のファイルが上書きされてしまう脆弱性が存在しました。このため、結果として、ホスト OS 上での権限を昇格されるなどの可能性がありました。	2015 年 1 月 29 日	6.0
10	「Fumy News Clipper」におけるクロスサイト・スクリプティングの脆弱性	ブログツール「Fumy News Clipper」には、ウェブページを出力する際の処理に問題がありました。このため、第三者によりウェブページにスクリプトを埋め込まれる可能性がありました。	2015 年 1 月 30 日	4.3
11	「shiromuku(u1)GUESTBOOK」におけるクロスサイト・スクリプティングの脆弱性	掲示板ソフト「shiromuku(u1)GUESTBOOK」には、ウェブページを出力する際の処理に問題がありました。このため、第三者によりウェブページにスクリプトを埋め込まれる可能性がありました。	2015 年 2 月 5 日	4.3
12	「PerlTreeBBS」におけるクロスサイト・スクリプティングの脆弱性	掲示板ソフト「PerlTreeBBS」には、ウェブページを出力する際の処理に問題がありました。このため、第三者によりウェブページにスクリプトを埋め込まれる可能性がありました。	2015 年 2 月 10 日	5.0
13	「スマホ通帳」における SSL サーバ証明書の検証不備の脆弱性	オンラインバンキングソフト「スマホ通帳」には、SSL サーバ証明書の検証不備の問題がありました。このため、中間者攻撃による暗号通信の盗聴などが行われる可能性がありました。	2015 年 2 月 13 日	4.0
14 (*1)	「Saurus CMS Community Edition」におけるクロスサイト・スクリプティングの脆弱性	コンテンツ管理システム「Saurus CMS Community Edition」には、ウェブページを出力する際の処理に問題がありました。このため、第三者によりウェブページにスクリプトを埋め込まれる可能性がありました。	2015 年 2 月 17 日	4.3
15 (*1)	「Squid」における HTTP ヘッダ・インジェクションの脆弱性	プロキシサーバ「Squid」には、HTTP ヘッダを出力する際の処理に問題がありました。このため、第三者により偽の情報が表示させられる可能性や任意のスクリプトが実行されてしまう可能性がありました。	2015 年 2 月 20 日	4.3
16	「AL-Mail32」におけるディレクトリ・トラバーサルの脆弱性	メールクライアントソフト「AL-Mail32」には、ディレクトリ・トラバーサルの脆弱性がありました。このため、第三者によりファイルを作成されたり既存のファイルを上書きされたりする可能性がありました。	2015 年 2 月 20 日	4.3
17	「AL-Mail32」におけるサービス運用妨害(DoS)の脆弱性	メールクライアントソフト「AL-Mail32」には、添付ファイルの処理に問題がありました。このため、ファイル名を細工された添付ファイルを処理することで、当該製品を応答不能な状態にされる可能性がありました。	2015 年 2 月 20 日	4.3
18	「AL-Mail32」におけるバッファオーバーフローの脆弱性	メールクライアントソフト「AL-Mail32」には、添付ファイルの処理に問題がありました。このため、ファイル名を細工された添付ファイルを処理することで、任意のコードを実行される可能性がありました。	2015 年 2 月 20 日	6.8

項番	脆弱性	セキュリティ上の問題点	JVN 公表日	CVSS 基本値
19	Speed Software 製「Root Explorer」および「Explorer」におけるディレクトリ・トラバーサルの脆弱性	Android 用ファイル管理ソフト「Root Explorer」および「Explorer」には、ディレクトリ・トラバーサルの脆弱性がありました。このため、第三者によりファイルを作成されたり既存のファイルを上書きされたりする可能性がありました。	2015 年 2 月 24 日	4.3
20	シンクグラフィカ製メールフォームプロ CGI において任意のコードを実行される脆弱性	メールフォーム「メールフォームプロ CGI 」はメール送信処理に問題がありました。このため、任意のコードが実行される可能性がありました。	2015 年 2 月 25 日	6.8
21 (*1)	「checkpw」におけるサービス運用妨害(DoS)の脆弱性	パスワード認証プログラム「checkpw」には、サービス運用妨害(DoS)の脆弱性がありました。このため、第三者により稼働するサーバのリソースが枯渇させられる可能性がありました。	2015 年 2 月 27 日	5.0
22	KENT-WEB 製「Clip Board」における任意のファイルを削除される脆弱性	掲示板ソフト「Clip Board」には、任意のファイルを削除される脆弱性がありました。このため、第三者によりサーバ上の任意のファイルを削除される可能性がありました。	2015 年 2 月 27 日	6.4
23 (*2)	「SEIL」シリーズにおけるサービス運用妨害(DoS)の脆弱性	ルータ製品「SEIL」シリーズには、サービス運用妨害(DoS)の脆弱性がありました。このため、第三者により当該製品を応答不能な状態にされる可能性がありました。	2015 年 2 月 27 日	4.3
24	WordPress 用プラグイン「Google Captcha (reCAPTCHA) by BestWebSoft」における CAPTCHA 保護メカニズムを回避される脆弱性	WordPress 用のプラグイン「Google Captcha (reCAPTCHA) by BestWebSoft」には、CAPTCHA 保護メカニズムを回避される脆弱性がありました。このため、ユーザによって、CAPTCHA 保護メカニズムを回避される可能性がありました。	2015 年 2 月 27 日	5.0
25	WordPress 用プラグイン「Captcha」における CAPTCHA 保護メカニズムを回避される脆弱性	WordPress 用プラグイン「Captcha」には、CAPTCHA 保護メカニズムを回避される脆弱性がありました。このため、ユーザによって、CAPTCHA 保護メカニズムを回避される可能性があります。	2015 年 3 月 3 日	5.0
26	「まろやか一言ボード」におけるクロスサイト・スクリプティングの脆弱性	文章を投稿するための CGI「スクリプトまろやか一言ボード」には、ウェブページを出力する際の処理に問題がありました。このため、第三者によりウェブページにスクリプトを埋め込まれる可能性がありました。	2015 年 3 月 4 日	5.0
27	「まろやかイメージアルバム」におけるクロスサイト・スクリプティングの脆弱性	画像を埋め込むための CGI「まろやかイメージアルバム」には、ウェブページを出力する際の処理に問題がありました。このため、第三者によりウェブページにスクリプトを埋め込まれる可能性がありました。	2015 年 3 月 4 日	4.3
28	「まろやかリレー小説」におけるクロスサイト・スクリプティングの脆弱性	文章を投稿するための CGI「まろやかリレー小説」には、ウェブページを出力する際の処理に問題がありました。このため、第三者によりウェブページにスクリプトを埋め込まれる可能性がありました。	2015 年 3 月 4 日	5.0

項番	脆弱性	セキュリティ上の問題点	JVN 公表日	CVSS 基本値
29 (*1)	WordPress 用プラグイン「All In One WP Security & Firewall」における SQL インジェクションの脆弱性	WordPress 用セキュリティプラグイン「All In One WP Security & Firewall」には、SQL 文を組み立てる処理に問題がありました。このため、第三者により任意の SQL 命令を実行される可能性がありました。	2015 年 3 月 6 日	5.1
30 (*1)	「eXtplorer」におけるクロスサイト・スクリプティングの脆弱性	ウェブベースのファイルマネージャ「eXtplorer」には、ウェブページを出力する際の処理に問題がありました。このため、第三者によりウェブページにスクリプトを埋め込まれる可能性がありました。	2015 年 3 月 17 日	4.3
31	「LINE」における意図しないアプリ内関数が呼び出される脆弱性	コミュニケーションアプリ「LINE」には、WebView 上の処理に不備がありました。このため、第三者により不正な JavaScript コードを実行され、意図しないアプリ内関数が呼び出される可能性がありました。	2015 年 3 月 20 日	5.1
32 (*1) (*2)	「TERASOLUNA Server Framework for Java(WEB)」の Validator に入力値検査回避の脆弱性	ウェブアプリケーション開発支援フレームワーク「TERASOLUNA Server Framework for Java(Web)」には、Apache Struts 1.2.9 の脆弱性に起因する、Validator に入力値検査回避の脆弱性が存在していました。このため、想定外のデータがデータベースに登録されるなどの可能性がありました。	2015 年 3 月 24 日	4.3
33	「Fumy Teacher's Schedule Board」におけるクロスサイト・スクリプティングの脆弱性	スケジュール表示用 CGI「Fumy Teacher's Schedule Board」には、ウェブページを出力する際の処理に問題がありました。このため、第三者によりウェブページにスクリプトを埋め込まれる可能性がありました。	2015 年 3 月 26 日	4.3
34 (*1)	WordPress 用テーマ「flashy」におけるクロスサイト・スクリプティングの脆弱性	WordPress 用のテーマ「flashy」には、ウェブページを出力する際の処理に問題がありました。このため、第三者によりウェブページにスクリプトを埋め込まれる可能性がありました。	2015 年 3 月 26 日	4.3
35 (*1)	WordPress 用プラグイン「All in One SEO Pack」における情報管理不備の脆弱性	WordPress 用プラグイン「All in One SEO Pack」における情報管理不備の脆弱性がありました。このため、パスワード保護したページの本文の一部が、パスワードを知らない第三者によって閲覧される可能性がありました。	2015 年 3 月 31 日	5.0
脆弱性の深刻度=レベル I（注意）、CVSS 基本値=0.0～3.9				
36 (*4)	複数の ASUS 製無線 LAN ルータにおけるクロスサイト・リクエスト・フォージェリの脆弱性	ASUS JAPAN が提供する複数の無線 LAN にクロスサイト・リクエスト・フォージェリの脆弱性がありました。このため、第三者により意図しない操作をさせられる可能性がありました。	2015 年 1 月 27 日	2.6
37	Android 版「スマホ通帳」における情報管理不備の脆弱性	オンラインバンキングソフト「スマホ通帳」には、ユーザによって入力された情報をログに出力してしまう情報管理不備の問題がありました。このため、Android 端末のログ情報を閲覧する権限のあるアプリケーションによって、当該製品に入力された情報を取得される可能性がありました。	2015 年 2 月 13 日	2.6

項番	脆弱性	セキュリティ上の問題点	JVN 公表日	CVSS 基本値
38 (*1)	日本語版「Zen Cart」におけるクロスサイトスクリプティングの脆弱性	ショッピングサイト構築システム「Zen Cart」には、ウェブページを出力する際の処理に問題がありました。このため、第三者によりウェブページにスクリプトを埋め込まれる可能性がありました。	2015 年 2 月 25 日	2.6
39 (*1)	「jBCrypt」におけるストレッチング処理に関する脆弱性	パスワードのハッシュ値を計算する Java 実装である「jBCrypt」には、ストレッチング処理が正しく行われなくなる問題がありました。このため、第三者によってパスワードのハッシュ値を取得された場合に、総当たり攻撃によって容易にパスワードを解読される可能性がありました。	2015 年 2 月 25 日	2.6
40 (*1)	WordPress 用プラグイン「All In One WP Security & Firewall」におけるクロスサイト・リクエスト・フォージェリの脆弱性	WordPress 用セキュリティプラグイン「All In One WP Security & Firewall」には、クロスサイト・リクエスト・フォージェリの脆弱性が存在しました。このため、第三者により本プラグインが管理するアクセスログを削除される可能性がありました。	2015 年 3 月 6 日	2.6
41 (*1) (*3) (*4)	「Android OS」がオープンリゾルバとして機能してしまう問題	「Android OS」には、を搭載しているデバイスには、オープンリゾルバとして機能してしまう問題が存在します。このため、第三者により対象機器が DDoS 攻撃に悪用される可能性がありました。	2015 年 3 月 27 日	2.6

(*1)：オープンソースソフトウェア製品の脆弱性
(*2)：製品開発者自身から届けられた自社製品の脆弱性
(*3)：複数開発者・製品に影響がある脆弱性
(*4)：組込みソフトウェアの脆弱性

(2) 海外 CSIRT 等から脆弱性情報の提供を受け JVN で公表した脆弱性

表 2-4、2-5 は JPCERT/CC が海外 CSIRT 等と連携し、今四半期に公表した脆弱性および対応状況を示しています。今四半期に公表した脆弱性は 36 件あり、表 2-4 は通常の脆弱性情報 35 件、表 2-5 には対応に緊急を要する Technical Cyber Security Alert の 1 件を示しています。

近年、Android 関連製品や OSS 製品の脆弱性の対策情報公表に向けた調整活動では、製品開発者が所在するアジア圏の調整機関、特に韓国の KrCERT/CC や中国の CNCERT/CC、台湾の TWNCERT との連携が増えています。これらの情報は、JPCERT/CC 製品開発者リスト (*14) に登録された製品開発者へ通知したうえ、JVN に掲載しています。

表 2-4. 海外 CSIRT 等と連携した脆弱性および対応状況

項番	脆弱性	対応状況
1	UEFI EDK1 にバッファオーバーフローの脆弱性	注意喚起として掲載 複数製品開発者へ通知
2	Intel BIOS ロッキングメカニズムに競合状態の脆弱性	注意喚起として掲載 複数製品開発者へ通知
3	複数の UEFI システムにおいて EFI S3 Resume Boot Path で使われる boot script が適切に保護されていない問題	注意喚起として掲載 複数製品開発者へ通知

(*14) JPCERT/CC 製品開発者リスト：https://jvn.jp/nav/index.html。

項番	脆弱性	対応状況
4	OpenSSL に複数の脆弱性	注意喚起として掲載 複数製品開発者へ通知
5	Panasonic Arbitrator Back-End Server (BES) に平文通信の脆弱性	注意喚起として掲載 特定製品開発者へ通知
6	Ceragon FibeAir IP-10 に root パスワードがハードコードされている問題	注意喚起として掲載
7	Windows 向け iPass Open Mobile クライアントに任意のコード実行の脆弱性	注意喚起として掲載
8	LabTech に権限昇格の脆弱性	注意喚起として掲載
9	QPR Portal に複数の脆弱性	注意喚起として掲載
10	glibc ライブラリにバッファオーバーフローの脆弱性	注意喚起として掲載 複数製品開発者へ通知
11	複数の Apple 製品の脆弱性に対するアップデート	注意喚起として掲載
12	SerVision HVG Video Gateway のウェブインターフェースに複数の脆弱性	注意喚起として掲載
13	Topline Systems Opportunity Form に情報漏えいの脆弱性	注意喚起として掲載
14	Ektron CMS に複数の脆弱性	注意喚起として掲載
15	横河製品の HART Device DTM にバッファオーバーフローの脆弱性	注意喚起として掲載 特定製品開発者へ通知
16	Microsoft Windows グループ ポリシーに脆弱性	注意喚起として掲載 特定製品開発者へ通知
17	Henry Spencer の正規表現 (regex) ライブラリにバッファオーバーフローの脆弱性	注意喚起として掲載 複数製品開発者へ通知
18	ISC BIND 9 にサービス運用妨害 (DoS) の脆弱性	注意喚起として掲載 複数製品開発者へ通知
19	Komodia Redirector がルート CA 証明書と秘密鍵をインストールする問題	注意喚起として掲載
20	Adtrustmedia PrivDog に SSL サーバ証明書の検証不備の脆弱性	注意喚起として掲載
21	Bluetooth Stack for Windows by Toshiba および TOSHIBA Service Station に権限昇格の脆弱性	注意喚起として掲載 特定製品開発者へ通知
22	ShareLaTeX に複数の脆弱性	注意喚起として掲載
23	SSL/TLS の実装が輸出グレードの RSA 鍵を受け入れる問題 (FREAK 攻撃)	注意喚起として掲載 複数製品開発者へ通知
24	複数の Apple 製品の脆弱性に対するアップデート	注意喚起として掲載
25	Telerik Analytics Monitor ライブラリに DLL ハイジャックが可能な脆弱性	注意喚起として掲載
26	D-Link DCS-93xL シリーズにファイルアップロードの脆弱性	注意喚起として掲載
27	D-Link DAP-1320 Rev Ax に OS コマンドインジェクションの脆弱性	注意喚起として掲載
28	HP ArcSight アプライアンス製品に複数の脆弱性	注意喚起として掲載
29	Apple Safari における複数の脆弱性に対するアップデート	注意喚起として掲載
30	OpenSSL に複数の脆弱性	注意喚起として掲載 複数製品開発者へ通知
31	Apple OS X における複数の脆弱性に対するアップデート	注意喚起として掲載
32	NSIS Inetc プラグインに SSL サーバ証明書の検証不備の脆弱性	注意喚起として掲載
33	複数の BIOS 実装において SMRAM の領域外を参照する SMM 関数呼び出しが可能な問題	注意喚起として掲載
34	ANTlabs 製 InnGate の複数のモデルにおいて認証なしでファイルシステムへの読書きが可能な脆弱性	注意喚起として掲載
35	複数の認証局においてメールアドレスのみに基づいて証明書を発行している問題	注意喚起として掲載 複数製品開発者へ通知

表 2-5.米国 US-CERT [*15] と連携した脆弱性関連情報および対応状況

項番	脆弱性
1	Superfish がインストールされた Lenovo 製 PC に HTTPS スプーフィングの脆弱性

2-1-5. 連絡不能案件の処理状況

図 2-12 は、2011 年 9 月末から 2015 年 3 月末までに、「連絡不能開発者」と位置づけて取扱った 185 件の処理状況の推移を示したものです。

2015 年 3 月末時点での処理状況は、185 件のうち、製品開発者との脆弱性対策情報の公表に向けた調整が再開したため連絡不能開発者一覧から削除したものは 25 件で、製品開発者と連絡が取れないため公表を継続しているものは 160 件（前四半期は 163 件）となりました。

「連絡不能」は、前四半期から 3 件減りました。また、今四半期は、新たに公表したものはなく、「開発者名公表」の 12 件は前四半期に公表したものです。

また、「調整再開」は、製品開発者との JVN 公表内容の調整を経て脆弱性対策情報の公表が完了したため、「調整再開（調整完了）」が 3 件増加しました。

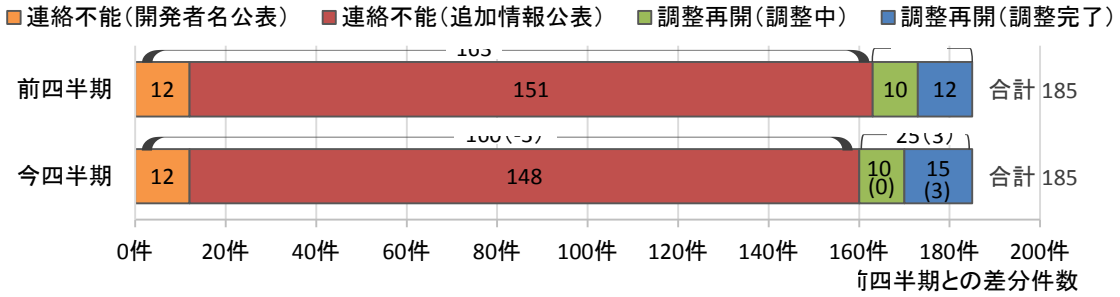


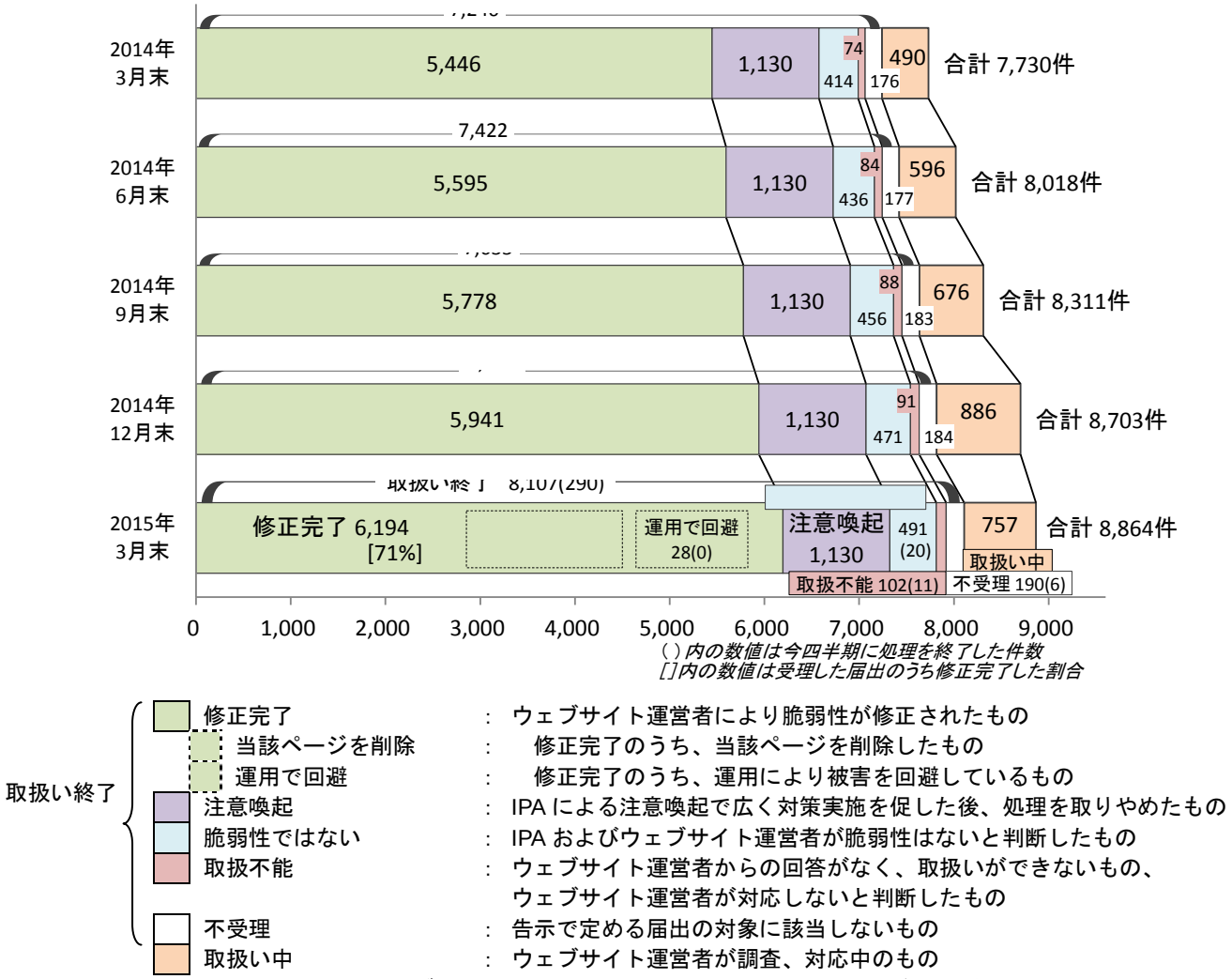
図2-12連絡不能開発者一覧の処理状況

[*15] United States Computer Emergency Readiness Team：米国の政府系 CSIRT。

2-2. ウェブサイトの脆弱性

2-2-1. 処理状況

図 2-13 のグラフは、ウェブサイトの脆弱性届出の処理状況について、四半期ごとの推移を示したものです。2015 年 3 月末時点の届出の累計は 8,864 件で、今四半期中に取扱いを終了したものは 290 件（累計 8,107 件）でした。このうち「修正完了」したものは 253 件（累計 6,194 件）、「注意喚起」により処理を取りやめたもの[*16]は 0 件（累計 1,130 件）、IPA およびウェブサイト運営者が「脆弱性ではない」と判断したものは 20 件（累計 491 件）でした。なお、ウェブサイト運営者への連絡は通常メールで行い、連絡が取れない場合に電話や郵送での連絡も行っています。しかしウェブサイト運営者への連絡手段がない場合などは「取扱不能」案件となります。今期その件数は 11 件（累計 102 件）でした。また「不受理」としたものは 6 件[*17]（累計 190 件）でした。取扱いを終了した累計 8,107 件のうち「修正完了」「脆弱性ではない」の合計 6,685 件は全て、ウェブサイト運営者からの報告もしくは IPA の判断により指摘した点が解消されていることが確認されています。なお「修正完了」のうち、ウェブサイト運営者が当該ページを削除したものは 70 件（累計 768 件）、ウェブサイト運営者が運用により被害を回避したものは 0 件（累計 28 件）でした。



取扱い終了
- 修正完了 : ウェブサイト運営者により脆弱性が修正されたもの
  - 当該ページを削除 : 修正完了のうち、当該ページを削除したもの
  - 運用で回避 : 修正完了のうち、運用により被害を回避しているもの
- 注意喚起 : IPA による注意喚起で広く対策実施を促した後、処理を取りやめたもの
- 脆弱性ではない : IPA およびウェブサイト運営者が脆弱性はないと判断したもの
- 取扱不能 : ウェブサイト運営者からの回答がなく、取扱いができないもの、ウェブサイト運営者が対応しないと判断したもの
- 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 : ウェブサイト運営者が調査、対応中のもの

図 2-13.ウェブサイト脆弱性の届出処理状況（四半期ごとの推移）

[*16] 「多数のウェブサイトにおいて利用されているソフトウェア製品に修正プログラムが適用されていない」といった届出があった場合、効果的に周知徹底するため「注意喚起」を公表することがあります。そうした場合、「注意喚起」をもって届出の処理を取りやめます。

[*17] 内訳は今四半期の届出によるもの 3 件、前四半期までの届出によるもの 3 件。

以下に、今までに届出のあったウェブサイトの脆弱性 8,864 件のうち、不受理を除いた 8,674 件の届出を分析した結果を記載します。

2-2-2. 運営主体の種類別の届出件数

図 2-14 のグラフは、届出された脆弱性のウェブサイト運営主体の種類について、過去 2 年間の届出件数の推移を四半期ごとに示しています。今四半期は全体の 5 割を企業が占めています。

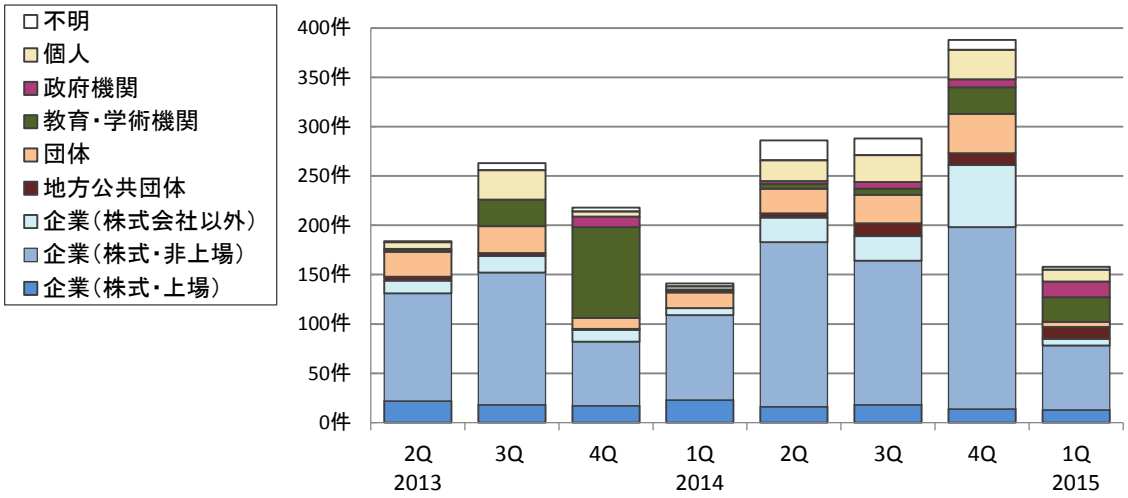


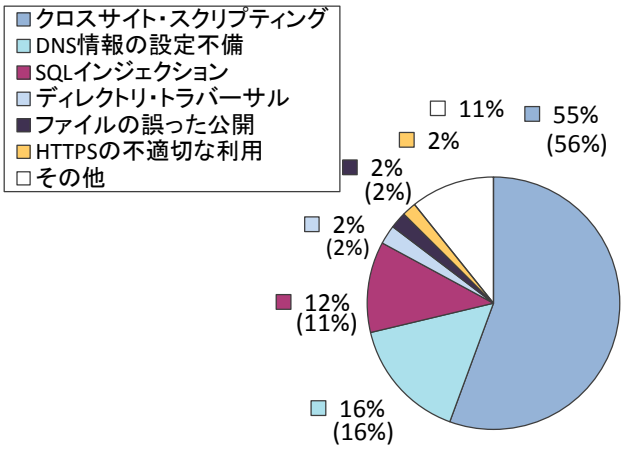
図2-14. 四半期ごとの運営主体の種類別届出件数

2-2-3. 脆弱性の種類・影響別届出

図 2-15、2-16 のグラフは、届出された脆弱性の種類を示しています。図 2-15 は今までの届出累計の割合を、図 2-16 は過去 2 年間の届出件数の推移を四半期ごとに示しています[*18]。

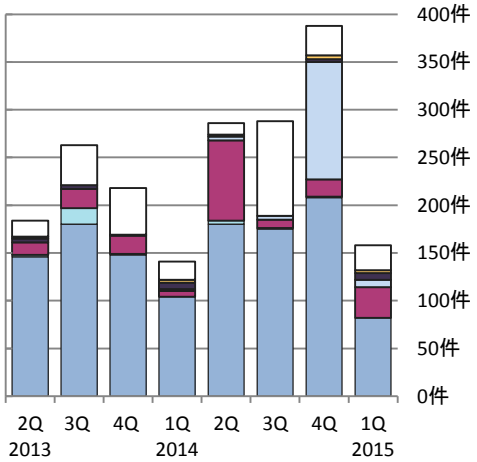
累計では、「クロスサイト・スクリプティング」だけで 55%を占めており、次いで「DNS 情報の設定不備」「SQL インジェクション」となっています。「DNS 情報の設定不備」は 16%ありますが、2008 年から 2009 年にかけて多く届出されたのが反映されたものです。今四半期は「クロスサイト・スクリプティング」が約 5 割を占めています。なお、この統計は本制度における届出の傾向であり、世の中に存在する脆弱性の傾向と必ずしも一致するものではありません。

ウェブサイトの脆弱性の種類別の届出状況



(8,674件の内訳、グラフの括弧内は前四半期までの数字)

図2-15. 届出累計の脆弱性の種類別割合



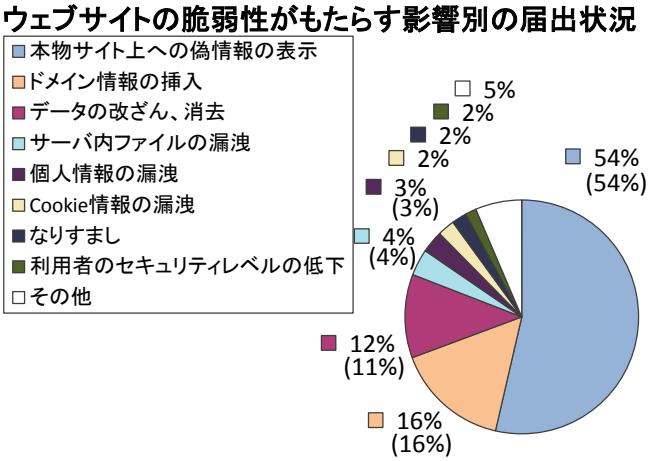
(過去2年間の届出内訳)

図2-16. 四半期ごとの脆弱性の種類別届出件数

[*18] それぞれの脆弱性の詳しい説明については付表 2 を参照してください。

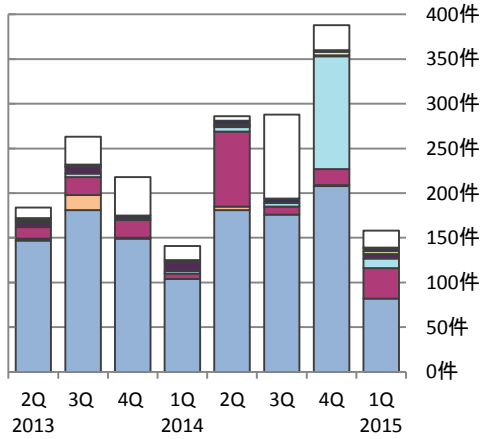
図 2-17、2-18 のグラフは、届出された脆弱性がもたらす影響別の分類です。図 2-17 は届出の影響別割合を、図 2-18 は過去 2 年間の届出件数の推移を四半期ごとに示しています。

累計では、「クロスサイト・スクリプティング」「DNS 情報の設定不備」「SQL インジェクション」などにより発生する、「本物サイト上での偽情報の表示」「ドメイン情報の挿入」「データの改ざん、消去」が全体の 8 割を占めています。前四半期は、「ディレクトリ・トラバーサル」の脆弱性が多く届出されたため「サーバ内ファイルの漏洩」が急増しましたが、今四半期は減少しています。



(8,674件の内訳、グラフの括弧内は前四半期までの数字)

図2-17. 届出累計の脆弱性がもたらす影響別割合



(過去2年間の届出内訳)

図2-18. 四半期ごとの脆弱性がもたらす影響別届出件数

2-2-4. 修正完了状況

図 2-19 のグラフは、過去 3 年間のウェブサイトの脆弱性の修正完了件数を四半期ごとに示しています。2015 年第 1 四半期に修正を完了した 253 件のうち 202 件（80%）は、運営者へ脆弱関連情報を通知してから修正完了までの日数が 90 日以内の届出でした。今四半期は、90 日以内に修正完了した届出の割合が、前四半期（163 件中 110 件（67%））より増加しています。

表 2-5 は、過去 3 年間に修正が完了した全届出のうち、ウェブサイト運営者に脆弱性を通知してから、90 日以内に修正が完了した累計およびその割合を四半期ごとに示しています。今期の割合は 68%でした。

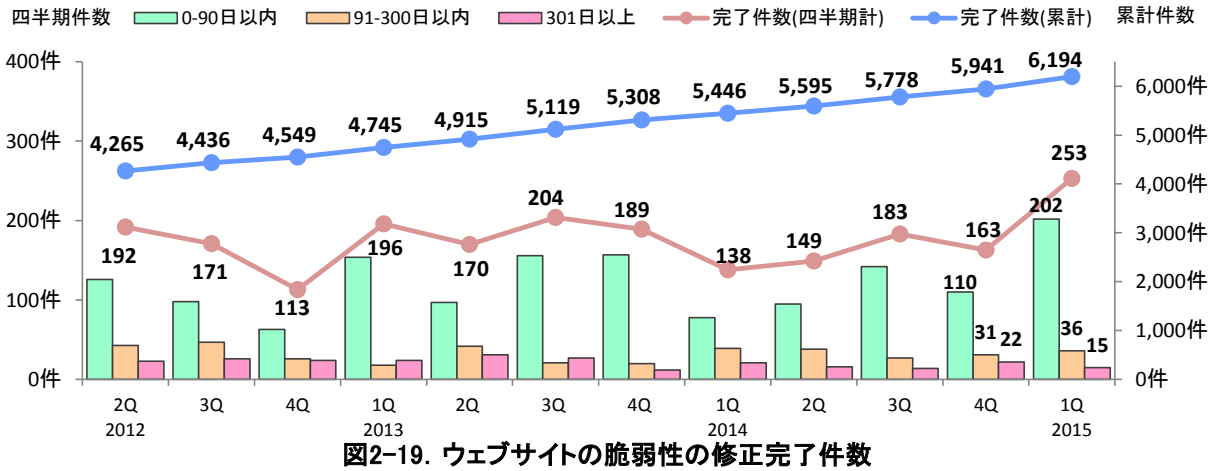


図2-19. ウェブサイトの脆弱性の修正完了件数

表 2-5. 90 日以内に修正完了した累計およびその割合の推移

	2012 2Q	3Q	4Q	2013 1Q	2Q	3Q	4Q	2014 1Q	2Q	3Q	4Q	2015 1Q
修正完了件数	4,265	4,436	4,549	4,745	4,915	5,119	5,308	5,446	5,595	5,778	5,941	6,194
90 日以内の件数	2,832	2,930	2,993	3,147	3,244	3,400	3,557	3,635	3,730	3,872	3,982	4,184
90 日以内の割合	66%	66%	66%	66%	66%	66%	67%	67%	67%	67%	67%	68%

図 2-20、2-21 は、ウェブサイト運営者に脆弱性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分類し、その傾向を示しています [(*19)]。全体の 49%の届出が 30 日以内、全体の 68%の届出が 90 日以内に修正されています。

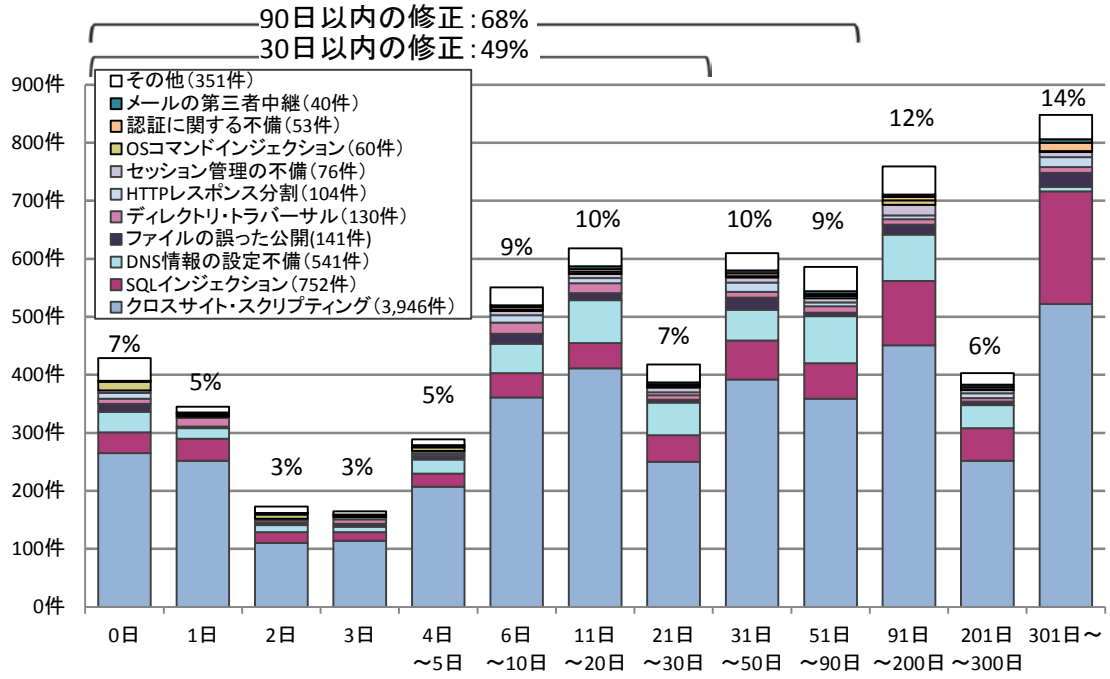


図2-20. ウェブサイトの修正に要した日数

(*19) 運営者から修正完了の報告があったもの、および、脆弱性が修正されたと IPA で判断したものも含めて示しています。なお、0 日は詳細情報を通知した当日に修正されたもの、または運営者へ詳細情報を通知する前に修正されたものです。

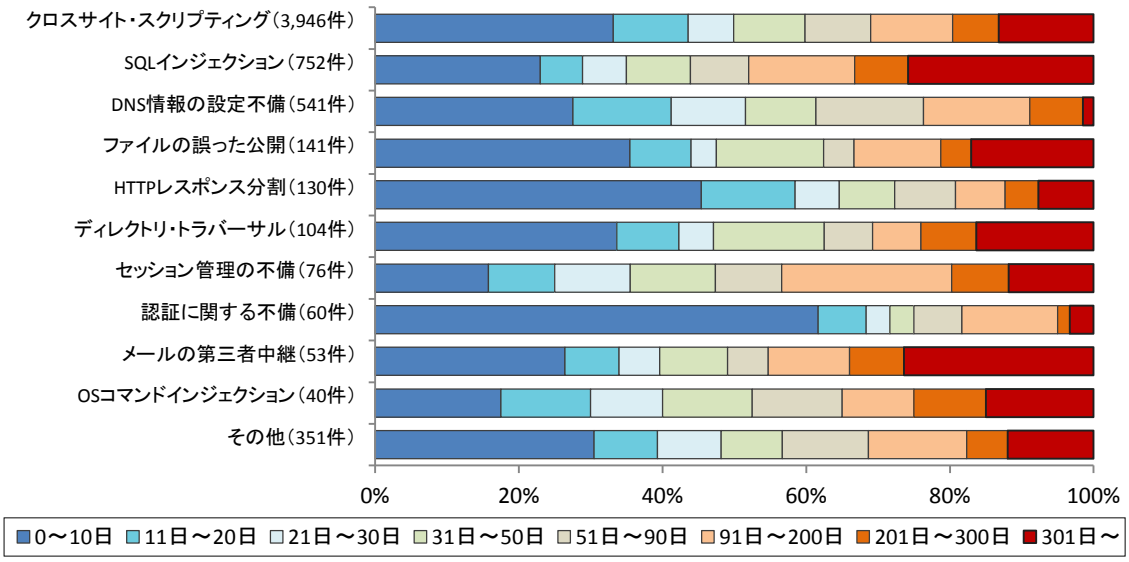


図2-21. ウェブサイトの修正に要した脆弱性種類別の日数の傾向

2-2-5. 取扱中の状況

ウェブサイト運営者から脆弱性を修正した旨の報告が無い場合、IPA はウェブサイト運営者に 1～2 ヶ月毎に電子メールや電話、郵送などの手段でウェブサイト運営者に連絡を試み、脆弱性が悪用されて攻撃を受けた場合の危険性を分かりやすく解説し、脆弱性対策の実施を促しています。

図 2-22 は、ウェブサイトの脆弱性のうち、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）しているものについて、経過日数別の件数を示したものです。これらの合計は 415 件（前四半期は 448 件）です。

取扱いが長期化しているものの中には、ウェブサイトの情報が窃取されてしまうなどの危険性がある、SQL インジェクションという深刻度の高い脆弱性も含まれています。

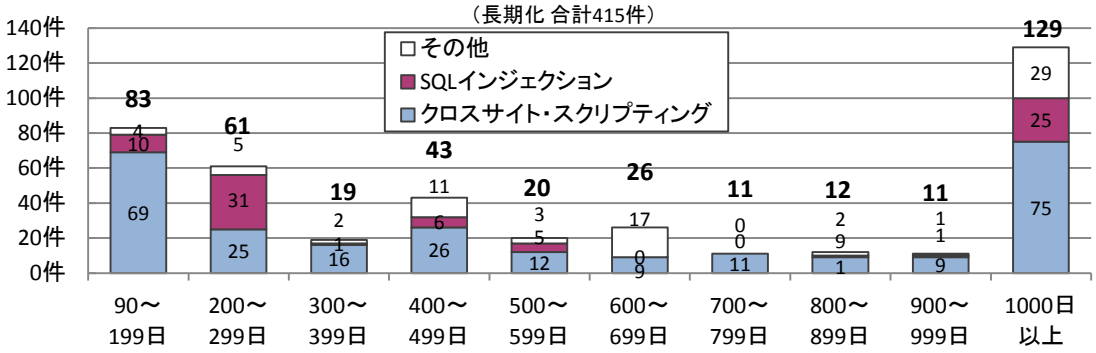


図2−22. 取扱いが長期化(90日以上経過)しているウェブサイトの経過日数と脆弱性の種類

表 2-6 は、過去 2 年間の四半期末時点で取扱い中の届出と、取扱いが長期化している届出の件数および、その割合を示しています。その推移をみると、取扱いが長期化している割合は減少傾向にあるといえます。

表 2-6. 取扱いが長期化している届出件数および割合の四半期ごとの推移

	2013 2Q	3Q	4Q	2014 1Q	2Q	3Q	4Q	2015 1Q
取扱い中の件数	473	504	505	490	596	676	886	757
長期化している件数	307	302	358	357	353	402	448	415
長期化している割合	65%	60%	71%	73%	59%	59%	51%	55%

3. 関係者への要望

脆弱性の修正促進のための、各関係者への要望は以下のとおりです。

3-1. ウェブサイト運営者

多くのウェブサイトで利用しているソフトウェア製品に脆弱性が発見されています。自身のウェブサイトでどのようなソフトウェア製品を利用しているかを把握し、脆弱性対策を実施することが必要です。

なお、脆弱性の理解にあたっては、以下の IPA が提供するコンテンツが利用できます。

⇒「知っていますか？脆弱性（ぜいじゃくせい）」： https://www.ipa.go.jp/security/vuln/vuln_contents/

⇒「安全なウェブサイト運営入門」： https://www.ipa.go.jp/security/vuln/7incidents/

また、対策実施にあたっては、以下のコンテンツが利用できます。

⇒「安全なウェブサイトの作り方」: https://www.ipa.go.jp/security/vuln/websecurity.html

⇒「安全な SQL の呼び出し方」: https://www.ipa.go.jp/security/vuln/websecurity.html

⇒「Web Application Firewall 読本」: https://www.ipa.go.jp/security/vuln/waf.html

また、ウェブサイトの脆弱性診断実施にあたっては、以下のコンテンツが利用できます。

⇒「ウェブ健康診断仕様」: https://www.ipa.go.jp/security/vuln/websecurity.html

⇒「動画で知ろう！クロスサイト・スクリプティングの被害！」（約 7 分）:
https://www.ipa.go.jp/security/keihatsu/videos/index.html#eng

3-2. 製品開発者

JPCERT/CC は、ソフトウェア製品の脆弱性関連情報を、「製品開発者リスト」に基づき、一般公表日の調整等を行います。迅速な調整が進められるよう、「製品開発者リスト」に登録してください（URL：https://www.jpcert.or.jp/vh/regist.html）。また、製品開発者自身が自社製品の脆弱性関連情報を発見した場合も、対策情報を利用者へ周知するために JVN を活用することができます。JPCERT/CC もしくは IPA へ連絡してください。

なお、製品開発にあたっては、以下のコンテンツが利用できます。

⇒「組込みシステムのセキュリティへの取組みガイド（2010 年度改訂版）」:
https://www.ipa.go.jp/security/fy22/reports/emb_app2010/

⇒「ファジング：製品出荷前に機械的に脆弱性をみつけよう」:
https://www.ipa.go.jp/security/vuln/fuzzing.html

⇒「Android アプリの脆弱性の学習・点検ツール AnCoLe」:
https://www.ipa.go.jp/security/vuln/ancole/index.html

3-3. 一般のインターネットユーザー

JVN や IPA、JPCERT/CC など、脆弱性情報や対策情報を公表しているウェブサイトを参照し、パッチの適用など、自発的なセキュリティ対策を日ごろから心がける必要があります。ソフトウェアを利用する場合は、脆弱性対策を実施してから利用してください。

なお、一般インターネットユーザー向けには、以下のツールを提供しています。

⇒「MyJVN 情報収集ツール」: http://jvndb.jvn.jp/apis/myjvn/mjcheck.html
脆弱性対策情報を効率的に収集するためのツール。

⇒「MyJVN バージョンチェッカ」: http://jvndb.jvn.jp/apis/myjvn/vccheck.html
利用者の PC、サーバ上にインストールされたソフトウェア製品のバージョンを容易にチェックする等の機能。

3-4. 発見者

脆弱性関連情報の適切な流通のため、届出した脆弱性関連情報については、脆弱性が修正されるまでは、第三者に漏れないよう、適切に管理してください。

付表 1. ソフトウェア製品の脆弱性の原因分類

	脆弱性の原因	説明	届出において 想定された脅威
1	アクセス制御の不備	アクセス制御を行うべき個所において、アクセス制御が欠如している。	設定情報の漏洩 通信の不正中継 なりすまし 任意のスクリプトの実行 認証情報の漏洩
2	ウェブアプリケーションの脆弱性	ウェブアプリケーションに対し、入力された情報の内容の解釈や認証情報の取扱い、出力時の処理に問題がある。「クロスサイト・スクリプティング」攻撃や「SQL インジェクション」攻撃などに利用されてしまう。	アクセス制限の回避 価格等の改ざん サービス不能 資源の枯渇 重要情報の漏洩 情報の漏洩 セッション・ハイジャック 通信の不正中継 なりすまし 任意のコマンドの実行 任意のスクリプトの実行 任意のファイルへのアクセス 認証情報の漏洩
3	仕様上の不備	RFC 等の公開された規格に準拠して、設計、実装した結果、問題が生じるもの。	サービス不能 資源の枯渇
4	証明書の検証に関する不備	ウェブブラウザやメールクライアントソフトに証明書を検証する機能が実装されていない、または、検証が正しく行われずに、偽の証明書を受けいれてしまう。	証明書の確認不能 なりすまし
5	セキュリティコンテキストの適用の不備	本来、厳しい制限のあるセキュリティコンテキストで取り扱うべき処理を、緩い制限のセキュリティコンテキストで処理してしまう。	アプリケーションの異常終了 情報の漏洩 任意のコードの実行 任意のスクリプトの実行
6	バッファのチェックの不備	想定外の長さの入力が行われた場合に、長さをチェックせずバッファに入力してしまう。「バッファオーバーフロー」攻撃に利用されてしまう。	サービス不能 任意のコードの実行 任意のコマンドの実行
7	ファイルのパス名、内容のチェックの不備	処理の際のパラメータとして指定されているディレクトリ名やファイル名、ファイルの内容をチェックしていない。任意のディレクトリのファイルを指定できてしまい、「ディレクトリ・トラバーサル」攻撃に利用されてしまう。また、破損したファイルや不正に書き換えられたファイルを処理した際に不具合が生じる。	アプリケーションの異常終了 サービス不能 資源の枯渇 任意のファイルへのアクセス 認証情報の漏洩

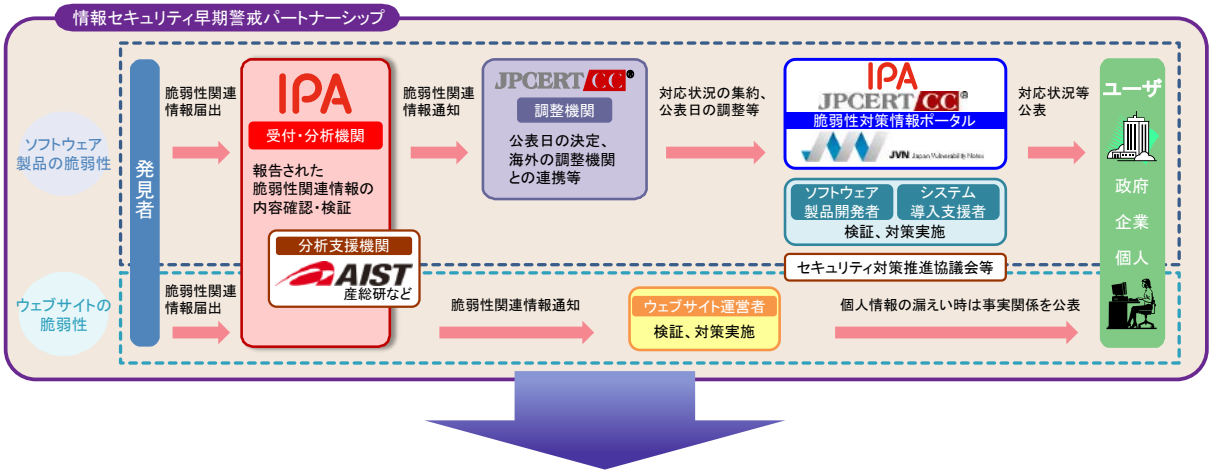
付表 2. ウェブサイトの脆弱性の分類

	脆弱性の種類	深刻度	説明	届出において想定された脅威
1	ファイルの誤った公開	高	一般に公開すべきでないファイルが公開されており、自由に閲覧できる状態になっている	個人情報の漏洩 サーバ内ファイルの漏洩 データの改ざん、消去 なりすまし
2	パス名パラメータの未チェック	高	ユーザからの入力を処理する際のパラメータとして指定されているファイル名を、ユーザが変更し、ウェブサーバ上の任意のディレクトリのファイルを指定できてしまう	サーバ内ファイルの漏洩
3	ディレクトリ･トラバーサル	高	ウェブサーバ上のディレクトリのアクセス権を超えて、本来許可されている範囲外のディレクトリにアクセスできる	個人情報の漏洩 サーバ内ファイルの漏洩
4	セッション管理の不備	高	セッション管理に、推測可能な情報を使用しているため、他のユーザの情報が容易に推測でき、他のユーザになりすまして、サービスを利用することができる	Cookie 情報の漏洩 個人情報の漏洩 なりすまし
5	SQL インジェクション	高	入力フォームなどへ SQL コマンド（データベースへの命令）を入力し、データベース内の情報の閲覧、更新、削除などができる	個人情報の漏洩 サーバ内ファイルの漏洩 データの改ざん、消去
6	DNS 情報の設定不備	高	DNS サーバに不適切な情報が登録されているため、第三者がそのドメイン名の持ち主であるかのようにふるまえてしまう	ドメイン情報の挿入
7	オープンプロキシ	中	外部の第三者により、他のサーバへのアクセスを中継するサーバとして利用され、不正アクセスなどの際にアクセス元を隠すための踏み台にされてしまう	踏み台
8	クロスサイト･スクリプティング	中	ユーザの Cookie 情報を知らないうちに転送させたり、偽の情報を表示させたりするような罠のリンクをユーザにクリックさせ、個人情報等を盗むことができる	Cookie 情報の漏洩 サーバ内ファイルの漏洩 個人情報の漏洩 データの改ざん、消去 なりすまし 本物サイト上への偽情報の表示
9	クロスサイト・リクエスト・フォージェリ	中	ユーザを罠のページに誘導することで、そのユーザが登録済みのサイトにひそかにアクセスさせ、登録情報の変更や商品の購入をさせることができる	データの改ざん、消去
10	HTTP レスポンス分割	中	攻撃者がユーザに対し、悪意のある要求をウェブサーバに送信するように仕向けることで、ウェブサーバからの応答を分割させて応答内容をすり替え、ユーザに対して偽のページを表示させることができる	ウェブキャッシュ情報のすり替え
11	セキュリティ設定の不適切な変更	中	ユーザに対し、ソフトウェアをインストールさせたり、ブラウザのセキュリティレベルを下げるよう指示することでクライアント PC のセキュリティ設定を低下させる	利用者のセキュリティレベルの低下
12	リダイレクタの不適切な利用	中	ウェブサーバに設置したリダイレクタが悪意あるリンクへの踏み台にされたり、そのウェブサイト上で別のサイト上のページを表示させられてしまう	踏み台 本物サイト上への偽情報の表示

	脆弱性の種類	深刻度	説明	届出において想定された脅威
13	フィルタリングの回避	中	ウェブサイトのサービスやブラウザの機能として提供されているフィルタリング機能が回避される問題。これにより、本来制限されるはずのウェブページを閲覧してしまう	利用者のセキュリティレベルの低下 なりすまし
14	OS コマンド・インジェクション	中	攻撃者がウェブアプリケーションを介してウェブサーバの OS コマンドを実行できてしまい、サーバ内ファイルの閲覧やシステム操作、不正なプログラムの実行などを行われてしまう	任意のコマンドの実行
15	メールの第三者中継	低	利用者が入力した内容を管理者が指定したメールアドレスに送信する機能で、外部の利用者が宛先メールアドレスを自由に指定できてしまい、迷惑メール送信の踏み台に悪用される	メールシステムの不正利用
16	HTTPS の不適切な利用	低	HTTPS による暗号化をしているが、暗号の選択や設定が十分でなかったり、ウェブサイトでのユーザへの説明に間違いがある、または、ウェブサイトの設計上、ユーザから証明書が確認できない	なりすまし
17	価格等の改ざん	低	ショッピングサイトにおいて、価格情報等が利用者側で書き換えられる。書き換えによる被害は、ウェブサイト側に限定される	データの改ざん

- API : Application Program Interface
- CGI : Common Gateway Interface
- DNS : Domain Name System
- HTTP : Hypertext Transfer Protocol
- HTTPS : Hypertext Transfer Protocol Security
- ISAKMP : Internet Security Association Key Management Protocol
- MIME : Multipurpose Internet Mail Extension
- RFC : Request For Comments
- SQL : Structured Query Language
- SSI : Server Side Include
- SSL : Secure Socket Layer
- TCP : Transmission Control Protocol
- URI : Uniform Resource Identifier
- URL : Uniform Resource Locator

付図１．「情報セキュリティ早期警戒パートナーシップ」（脆弱性関連情報の取扱制度）



【期待効果】

①製品開発者及びウェブサイト運営者による脆弱性対策を促進
②不用意な脆弱性関連情報の公表や脆弱性の放置を抑制
③個人情報等重要情報の流出や重要システムの停止を予防

※IPA:独立行政法人情報処理推進機構，JPCERT/CC:一般社団法人 JPCERT コーディネーションセンター、産総研：国立研究開発法人産業技術総合研究所