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 3 四半期（7 月～9 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。

本報告書では、2015 年 7 月 1 日から 2015 年 9 月 30 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に関するトピックについて記載しています。

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 10 月 27 日

目次

1. 2015 年第 3 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 11,272 件 ～

表 1-1 は本制度[*1]における届出状況についてです。2015 年第 3 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 122 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 91 件、合計 213 件でした。届出受付開始からの累計は 11,272 件で、内訳はソフトウェア製品に関するもの 2,242 件、ウェブサイトに関するもの 9,030 件でウェブサイトに関する届出が全体の約 8 割を占めています。

表 1-1.　届出件数

分類	今期件数	累計
ソフトウェア製品	**122** 件	**2,242** 件
ウェブサイト	**91** 件	**9,030** 件
合計	**213** 件	**11,272** 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ウェブサイトに関する届出よりも多く、全体の 57%割合を占めました。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 4.12[*2] 件でした。

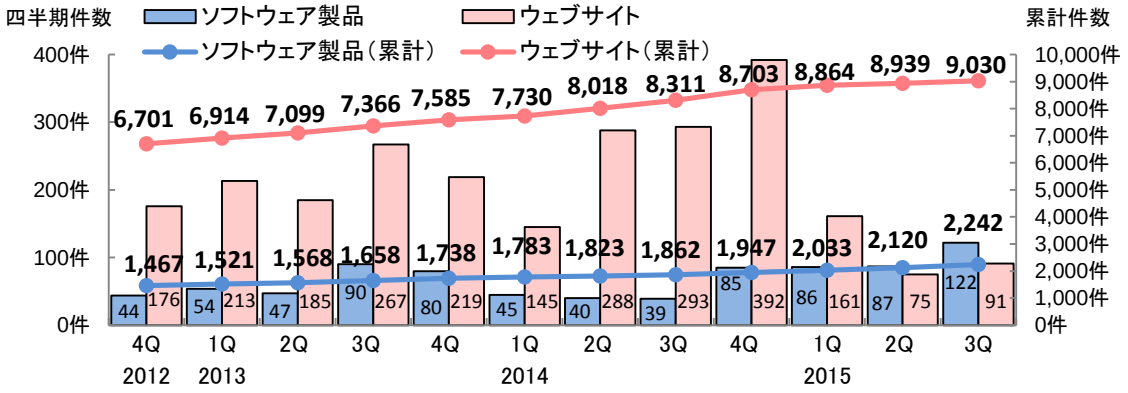


図1-1. 脆弱性の届出件数の四半期ごとの推移

表 1-2.　届出件数（過去 3 年間）

	2012 4Q	2013 1Q	2Q	3Q	4Q	2014 1Q	2Q	3Q	4Q	2015 1Q	2Q	3Q
累計届出件数[件]	9,841	10,17	10,650	10,897	11,059	11,272	9,841	10,173	10,650	10,897	11,059	11,272
1 就業日あたり[件/日]	4.04	4.07	4.17	4.17	4.13	4.11	4.04	4.07	4.17	4.17	4.13	4.12

[*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 7,576 件～

表 1-3 は今四半期、および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（JVN 公表）

分類	今期件数	累計
ソフトウェア製品	**53** 件	**1,095** 件
ウェブサイト	**129** 件	**6,481** 件
合計	**182** 件	**7,576** 件

今四半期に JVN 公表したソフトウェア製品の件数は 53 件 (*3)（累計 1,095 件）でした。そのうち、製品開発者による自社製品の脆弱性の届出は 1 件でした。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 12 件（23%）でした。

また、修正完了したウェブサイトの件数は 129 件（累計 6,481 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 129 件のうち、ウェブアプリケーションを修正したものは 75 件（58%）、当該ページを削除したものは 54 件（42%）、運用で回避したものは 0 件でした。なお、修正を完了した 129 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 43 件（33%）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（158 件中 76 件（48%））より減少しています。

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。

今四半期は、4 件について製品開発者と連絡が取れたため調整を再開し、新たに連絡が取れない製品開発者名を 12 件公表しました。また、公表判定委員会での審議を経て、2 件の脆弱性情報が JVN に公表されました。

2015 年 9 月末時点の連絡不能開発者の累計公表件数は 217 件、その内製品情報を公表しているものは 165 件となりました。

(*3) P.9 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や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. 脆弱性に関するトピック

アプリケーション開発に多用される「アプリケーション開発・実行環境」の脆弱性に注意

～アプリケーション開発者は開発に関連するソフトウェアの脆弱性情報の収集を～

今四半期に JVN 公表した脆弱性対策情報 53 件のうち 6 件は、アプリケーションを効率的に開発するため、汎用的な機能が予め備えられている「アプリケーション開発・実行環境」（以降、「開発・実行環境」）に存在する脆弱性でした（表 1-4）。

表 1-4 今四半期、JVN に公表された「開発・実行環境」に関連するソフトウェアの脆弱性

「スクリプトエンジン」に関連した脆弱性		
JVN公表日	JVN番号	脆弱性名
9月2日	JVN#08494613	「NScripter」におけるバッファオーバーフローの脆弱性

「アプリケーションフレームワーク」に関連した脆弱性		
JVN公表日	JVN番号	脆弱性名
8月20日	JVN#17611367	「Apache Tapestry」における信頼できないデータをデシリアライズする脆弱性
9月4日	JVN#88408929	「Apache Struts」におけるクロスサイト・スクリプティングの脆弱性
9月4日	JVN#95989300	「Apache Struts」におけるクロスサイト・スクリプティングの脆弱性
9月16日	JVN#73346595	「アプリカン」におけるアクセス制限不備の脆弱性
9月29日	JVN#21612597	Apache Cordova プラグイン cordova-plugin-file-transfer における HTTP ヘッダ・インジェクションの脆弱性

アプリケーションには効率的な開発のため、「開発・実行環境」が予め、組み込まれていることが少なくありません。

そのため、アプリケーション開発者は「スクリプトエンジン [*8]」や「アプリケーションフレームワーク [*9]」といった「開発・実行環境」を利用することで、開発コストを削減できます（図 1-2）。

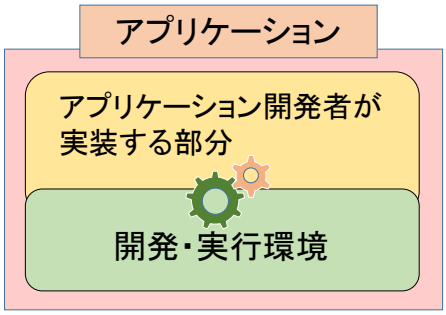


図 1-2 「開発・実行環境」で作成したアプリケーションのイメージ

このため、表 1-4 のような「開発・実行環境」を使用して開発された多くのアプリケーションには、「開発・実行環境」で発見された脆弱性の影響を受け、同じ脆弱性をアプリケーションに内包してしまいます。また、1 つの「開発・実行環境」を用いて複数のアプリケーションが開発され、その結果利用は広範にわたります。そのためアプリケーションそのものに脆弱性が見つかるよりも、「開発・実行環境」に脆弱性が見つかった場合のほうが、その影響は深刻といえます（図 1-3）。

[*8] ゲームソフトの開発に利用されます。
[*9] ウェブアプリケーションやスマートフォンアプリなどの開発に利用されます。

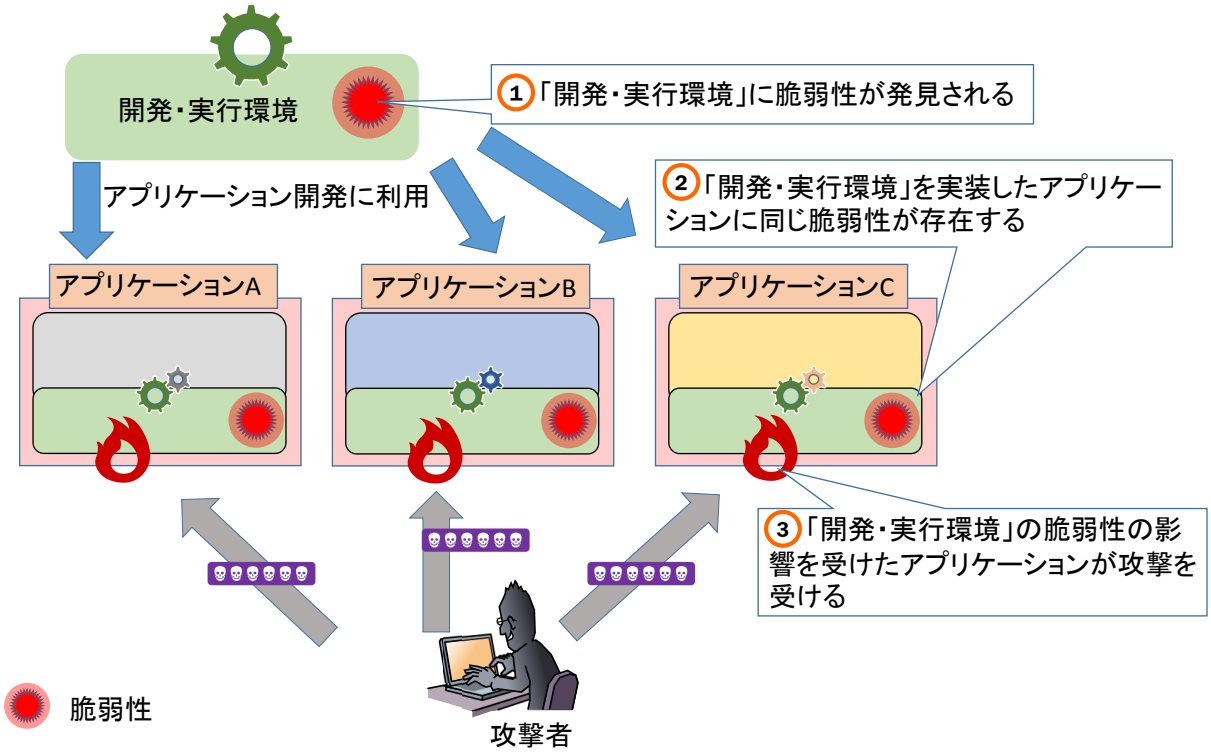


図 1-3 「開発・実行環境」に見つかった脆弱性の影響範囲

また、そのような脆弱性の影響を受けたアプリケーションが標的となる事実も確認しています。そのため、アプリケーション開発者およびウェブサイト管理者は日頃から開発に利用した「開発・実行環境」などソフトウェアの把握及び脆弱性対策情報の収集に努めるようにしてください。役割、立場に応じてそれぞれの対応は以下のように異なります。

・アプリケーション開発者

脆弱性対策情報が公表された場合は速やかに、アプリケーションの再構築等を行う必要があります。その後、修正した脆弱性情報とともに、修正したアプリケーションもしくは修正パッチを公開し、アプリケーション利用者へアップデートもしくは修正パッチを適用するように通知してください。

・ウェブサイト管理者

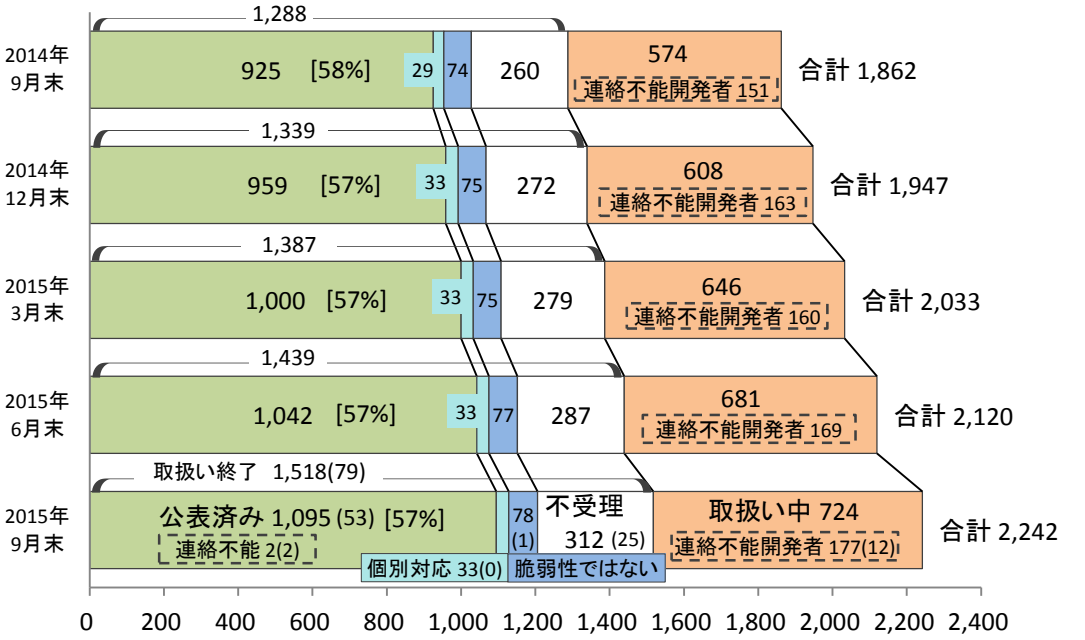
「開発・実行環境」を使用して構築したウェブアプリケーションは、の脆弱性対策（保守・メンテナンス）は、ウェブサイト管理者が行う必要があります。その場合、「開発・実行環境」の修正パッチ適用を検討のうえ、適用してください。修正パッチを適用しない場合は、脆弱性による影響を受けないための回避策を検討し、対策を実施してください。

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 9 月末時点の届出の累計は 2,242 件で、今四半期に脆弱性対策情報を JVN 公表したものは 53 件（累計 1,095 件）でした。このうち 2 件は、公表判定委員会による審議にて JVN 公表することが適当と判定された連絡不能案件です。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 1 件（累計 78 件）、「不受理」としたものは 25 件 (*10)（累計 312 件）、取扱い中は 724 件でした。724 件のうち、連絡不能開発者 (*11) 一覧へ新規に公表したものは 12 件で、2015 年 9 月末時点で 177 件が公表中です。



( ) 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
	連絡不能	：公表判定委員会による審議にて、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	：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 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）

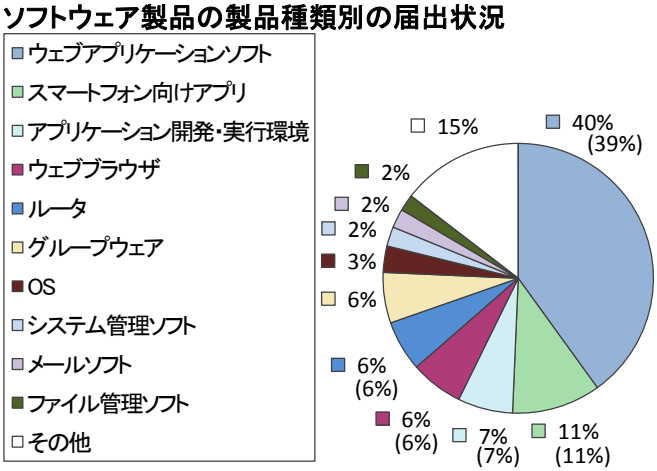
(*10) 内訳は今四半期の届出によるもの 9 件、前四半期までの届出によるもの 16 件。
(*11) 連絡不能開発者一覧への公表および一覧からの削除が複数回行われた製品開発者の公表回数は、その累計を計上しています。

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 2,242 件のうち、不受理を除いた 1,930 件の届出を分析した結果を記載します。

2-1-2. ソフトウェア製品種類別届出件数

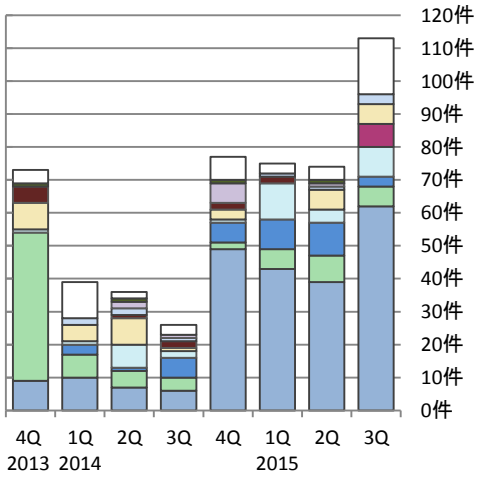
図 2-2、2-3 のグラフは、届出された脆弱性の製品種類別の分類です。図 2-2 は製品種類別割合を、図 2-3 は過去 2 年間の届出件数の推移を四半期ごとに示したものです。

累計では、「ウェブアプリケーションソフト」が最も多く 40%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、次いで届出件数が多いのは、「アプリケーション開発・実行環境」となっています。



※その他には、データベース、携帯機器などがあります。
（ 1,930件の内訳、グラフの括弧内は前四半期までの数字）

図2-2. 届出累計の製品種類別割合

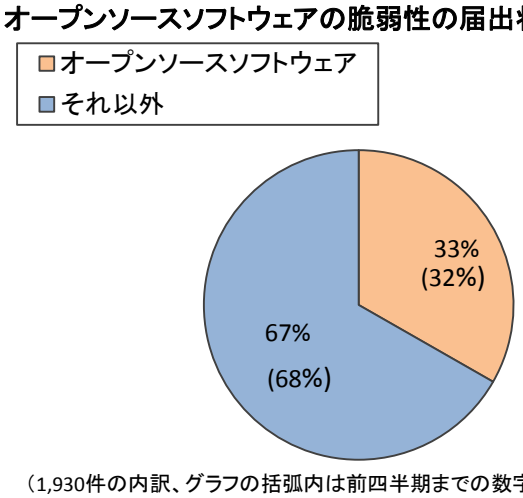


（ 過去2年間の届出内訳）

図2-3. 四半期ごとの製品種類別届出件数

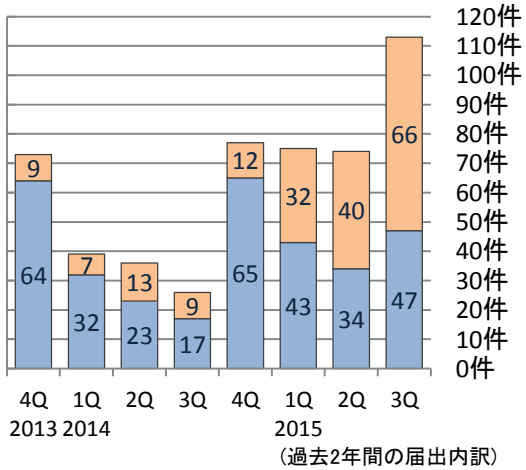
図 2-4、2-5 のグラフは、届出された製品のライセンスを「オープンソースソフトウェア」（OSS）と「それ以外」で分類しています。図 2-4 は届出累計の分類割合を、図 2-5 は過去 2 年間の届出件数の推移を四半期ごとに示したものです。

累計の割合は、オープンソースソフトウェアが 33%に過ぎませんが、四半期別でみると、過去 1 年は四半期ごとに増加傾向にあり、今四半期は 66 件と過半数を占めました。



（1,930件の内訳、グラフの括弧内は前四半期までの数字）

図2-4. 届出累計のオープンソースソフトウェア割合



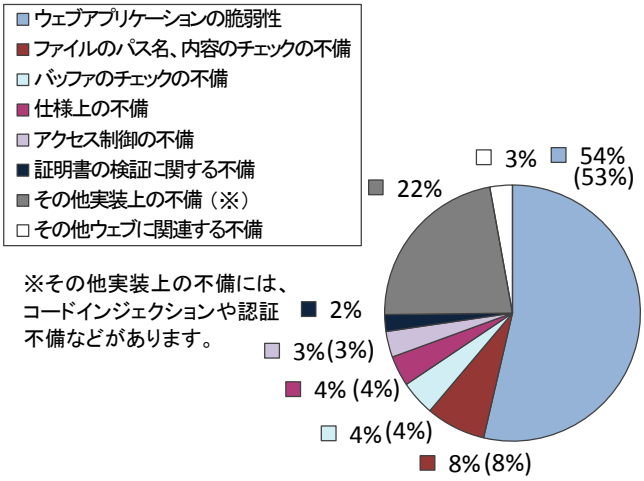
（過去2年間の届出内訳）

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

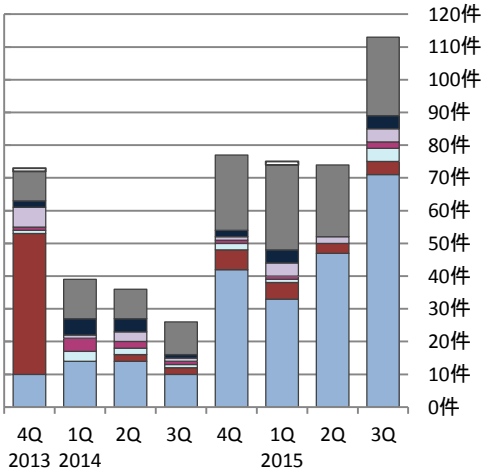
図 2-6、2-7 のグラフは、届出された脆弱性の原因を示しています。図 2-6 は届出累計の脆弱性の原因別割合を、図 2-7 は過去 2 年間の原因別の届出件数の推移を四半期ごとに示しています。累計では、「ウェブアプリケーションの脆弱性」が過半数を占めています。

ソフトウェア製品の脆弱性の原因別の届出状況



（1,930件の内訳、グラフの括弧内は前四半期までの数字）

図2-6. 届出累計の脆弱性の原因別割合

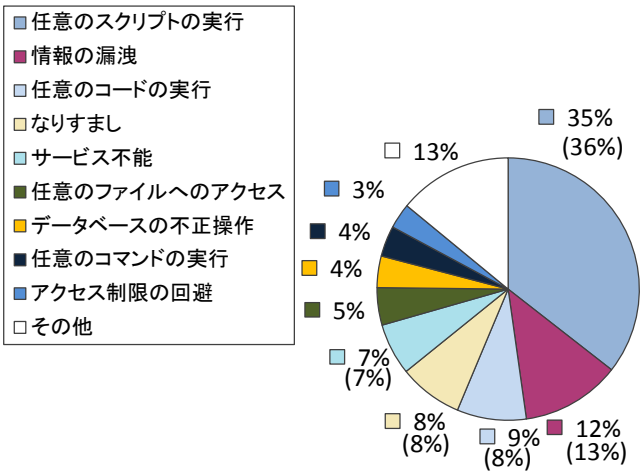


（過去2年間の届出内訳）

図2-7. 四半期ごとの脆弱性の原因別届出件数

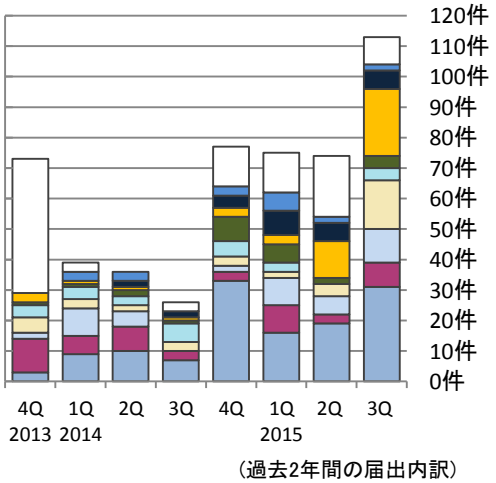
図 2-8、2-9 のグラフは、届出された脆弱性がもたらす影響を示しています。図 2-8 は届出累計の影響別割合を、図 2-9 は過去 2 年間の影響別届出件数の推移を四半期ごとに示しています。累計では「任意のスクリプトの実行」が最も多く、35%となっています。今四半期は、「任意のスクリプトの実行」が最も多く、次いで多かったのは「データベースの不正操作」でした。

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



（1,930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[*12]。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	53 件	1,095 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	39 件	1,277 件
	合計	92 件	2,372 件

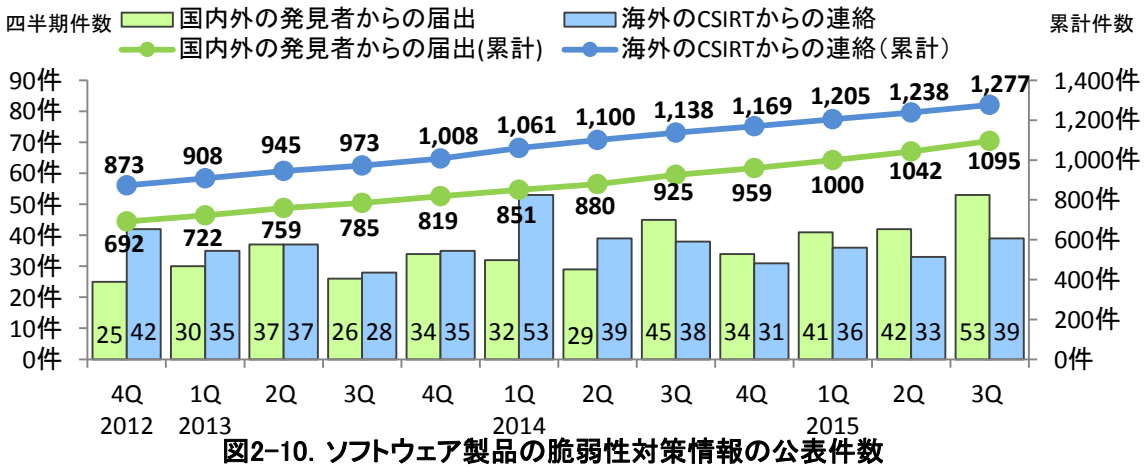


図2−10. ソフトウェア製品の脆弱性対策情報の公表件数

（1） JVN で公表するまでに要した日数で分類した“国内外の発見者および製品開発者から届出を受けた”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（1,095 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 31%、45 日を超過した件数は 69%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。

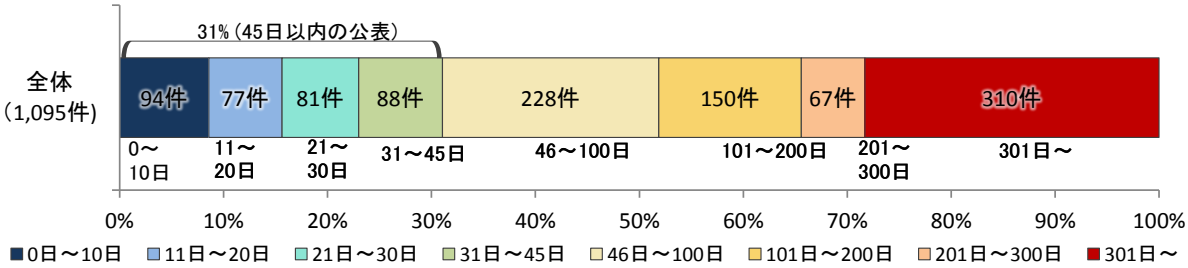


図2−11. ソフトウェア製品の脆弱性公表日数

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 4Q	2013 1Q	2Q	3Q	4Q	2014 1Q	2Q	3Q	4Q	2015 1Q	2Q	3Q
34%	33%	33%	33%	34%	34%	34%	33%	33%	32%	31%	31%

[*12] JPCERT/CC 活動概要 Page15〜21（https://www.jpcert.or.jp/pr/2015/PR20151008.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 53 件について、今四半期に JVN 公表した脆弱性を深刻度が高いものから順に示しています。オープンソースソフトウェアに関する脆弱性が 17 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 1 件（表 2-3 の*2）、組込みソフトウェア製品の脆弱性が 2 件（表 2-3 の*3）、開発者に連絡がとれない脆弱性が 2 件（表 2-3 の*4）ありました。

表 2-3. 2015 年第 3 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（*1）	「Thetis」における SQL インジェクションの脆弱性	グループウェア「Thetis」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 7 月 15 日	7.5
2	「yoyaku_v41」における任意のファイルを作成される脆弱性	施設の予約管理ソフト「yoyaku_v41」には、任意のファイルを作成される脆弱性がありました。このため、第三者によって、サーバ上に任意のファイルを作成される可能性があり、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 7 月 29 日	7.5
3	「yoyaku_v41」における OS コマンド・インジェクションの脆弱性	施設の予約管理ソフト「yoyaku_v41」には、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、第三者によりサーバ上で任意のコマンドを実行される可能性がありました。	2015 年 7 月 29 日	7.5
脆弱性の深刻度=レベル II（警告）、CVSS 基本値=4.0～6.9				
4	「Cacti」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	ネットワーク管理ソフト「Cacti」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、第三者により意図しない操作をさせられる可能性がありました。	2015 年 7 月 9 日	4.0
5	「シンプルお絵描き掲示板」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「シンプルお絵描き掲示板」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 7 月 10 日	5.0
6	「シンプルお絵描き掲示板」における任意のファイル削除の脆弱性	掲示板ソフト「シンプルお絵描き掲示板」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 7 月 10 日	6.4
7	「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 7 月 10 日	5.1
8	「acmailer」におけるディレクトリ・トラバーサルの脆弱性	メール配信 CGI「acmailer」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削除される可能性がありました。	2015 年 7 月 15 日	4.0

項番	脆弱性	セキュリティ上の問題点	JVN 公表日	CVSS 基本値
9 (*1)	Windows 版「PHP」における OS コマンド・インジェクションの脆弱性	プログラミング言語「Windows 版『PHP』」には、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 OS コマンドを実行させられる可能性がありました。	2015 年 7 月 17 日	6.8
10	「Research Artisan Lite」におけるクロスサイト・スクリプティングの脆弱性	アクセス解析ソフト「Research Artisan Lite」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 7 月 24 日	4.3
11	「Research Artisan Lite」における認証不備の脆弱性	アクセス解析ソフト「Research Artisan Lite」には、認証不備の脆弱性がありました。このため、第三者により認証を回避して当該製品の機能が実行される可能性がありました。	2015 年 7 月 24 日	5.0
12 (*1)	「Welcart」における SQL インジェクションの脆弱性	WordPress プラグイン「Welcart」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、ログインできるユーザにより任意の SQL 命令を実行される可能性がありました。	2015 年 7 月 24 日	6.5
13	「画像掲示板 plus」のファイルアップロード処理における脆弱性	画像掲示板ソフト「画像掲示板 plus」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 7 月 28 日	5.0
14	「yoyaku_v41」における認証回避の脆弱性	施設の予約管理ソフト「yoyaku_v41」には、認証回避の脆弱性がありました。このため、第三者によって認証を回避され、不正に予約操作を実施される可能性がありました。	2015 年 7 月 29 日	5.0
15	Android 版「ヨドバシ」において任意の Java のメソッドが実行される脆弱性	Android 版アプリ「ヨドバシ」には、任意の Java のメソッドが実行される脆弱性がありました。このため、第三者により当該製品の権限で実行可能な任意の Java メソッドを実行される可能性がありました。	2015 年 8 月 7 日	5.8
16	Android 版「ヨドバシ」における SSL サーバ証明書の検証不備の脆弱性	Android 版アプリ「ヨドバシ」には、SSL サーバ証明書の検証不備の脆弱性が存在しました。このため、中間者攻撃による暗号通信の盗聴などが行なわれる可能性がありました。	2015 年 8 月 7 日	4.0
17	「Microsoft Office」における情報漏えいの問題	文書作成ソフト等が含まれている「Microsoft Office」には、情報漏えいの問題が存在しました。このため、当該製品で作成されたファイルを取得した第三者によって、ファイルシステムやユーザ名に関する情報を取得される可能性がありました。	2015 年 8 月 12 日	4.3
18	「【Gallery01】PC、スマホ、ガラケー3 デバイス対応写真ギャラリーCMS フリー（無料）版」におけるクロスサイト・スクリプティングの脆弱性	画像公開ソフト「【Gallery01】PC、スマホ、ガラケー3 デバイス対応写真ギャラリーCMS フリー（無料）版」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 8 月 12 日	4.0

項番	脆弱性	セキュリティ上の問題点	JVN 公表日	CVSS 基本値
19 (*2) (*3)	複数のアイ・オー・データ製ルータにおける UPnP に関する脆弱性	有線 LAN ルータ「NP-BBRS」および無線 LAN ルータ「WN-G54/R2」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 8 月 18 日	5.0
20 (*1)	「Apache Tapestry」における信頼できないデータをデシリアライズする脆弱性	ウェブアプリケーションフレームワーク「Apache Tapestry」には、データをデシリアライズす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コードが実行される可能性がありました。	2015 年 8 月 20 日	6.8
21	「Twit 掲示板」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「Twit 掲示板」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 9 月 1 日	5.0
22	「desknet's NEO」におけるディレクトリ・トラバーサルの脆弱性	グループウェア「desknet's NEO」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、当該製品にログイン可能なユーザによって、サーバ上のファイルを意図せず閲覧される可能性がありました。	2015 年 9 月 1 日	4.0
23	iOS 版アプリ「楽天カード」における SSL サーバ証明書の検証不備の脆弱性	iOS 版アプリ「楽天カード」には、SSL サーバ証明書の検証不備の脆弱性が存在しました。このため、中間者攻撃による暗号通信の盗聴などが行なわれる可能性がありました。	2015 年 9 月 1 日	4.0
24	「NScripter」におけるバッファオーバーフローの脆弱性	ゲームスクリプトエンジン「NScripter」には、バッファオーバーフローの脆弱性がありました。このため、第三者により任意のコードが実行される可能性がありました。	2015 年 9 月 2 日	6.8
25 (*1) (*4)	「hitSuji (rktSNS2)」におけるクロスサイト・スクリプティングの脆弱性	SNS 構築ソフト「hitSuji (rktSNS2)」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 9 月 3 日	4.3
26 (*4)	「BBS X102」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「BBS X102」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 9 月 3 日	5.0
27 (*1)	「Apache Struts」におけるクロスサイト・スクリプティングの脆弱性	ウェブアプリケーションフレームワーク「Apache Struts」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 9 月 4 日	4.3
28 (*1)	「OpenDocMan」におけるクロスサイト・スクリプティングの脆弱性	ドキュメント管理システム「OpenDocMan」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 9 月 4 日	4.3
29	ActiveX コントロール「ELPhoneBtnV6」におけるバッファオーバーフローの脆弱性	ActiveX コントロール「ELPhoneBtnV6」には、バッファオーバーフローの脆弱性がありました。このため、第三者により任意のコードが実行される可能性がありました。	2015 年 9 月 7 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
30	「Japan Connected-free Wi-Fi」におけるアクセス制限不備の脆弱性	Wi-Fi検索アプリ「Japan Connected-free Wi-Fi」には、アクセス制限不備の脆弱性がありました。このため、任意のページを表示させられ、結果として任意の API が実行される可能性がありました。	2015 年 9 月 11 日	6.8
31	「Japan Connected-free Wi-Fi」におけるスクリプト・インジェクションの脆弱性	Wi-Fi検索アプリ「Japan Connected-free Wi-Fi」には、SSID の表示に起因する脆弱性がありました。このため、任意のスクリプトが実行される可能性がありました。	2015 年 9 月 11 日	5.4
32 (*3)	「PIXUS MG7530」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	インクジェットプリンター「PIXUS MG7530」には、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 9 月 11 日	4.0
33	「アプリカン」におけるアクセス制限不備の脆弱性	Android および iOS 向けアプリケーションの開発環境「アプリカン」には、アクセス制限不備の脆弱性がありました。このため、任意の URL に誘導され、結果として任意の API が実行される可能性がありました。	2015 年 9 月 16 日	6.8
34	「Auction Camera」におけるアクセス制限不備の脆弱性	スマホアプリ「Auction Camera」には、アクセス制限不備の脆弱性がありました。このため、任意の URL に誘導され、結果として任意の API が実行される可能性がありました。	2015 年 9 月 16 日	6.8
35	「MEGAPHONE MUSIC」におけるアクセス制限不備の脆弱性	スマホアプリ「MEGAPHONE MUSIC」には、アクセス制限不備の脆弱性がありました。このため、任意の URL に誘導され、結果として任意の API が実行される可能性がありました。	2015 年 9 月 16 日	6.8
36	「こりトレ」におけるアクセス制限不備の脆弱性	スマホアプリ「こりトレ」には、アクセス制限不備の脆弱性がありました。このため、任意の URL に誘導され、結果として任意の API が実行される可能性がありました。	2015 年 9 月 16 日	6.8
37	「AI 黒白棋」におけるアクセス制限不備の脆弱性	スマホアプリ「AI 黒白棋」には、アクセス制限不備の脆弱性がありました。このため、任意の URL に誘導され、結果として任意の API が実行される可能性がありました。	2015 年 9 月 16 日	6.8
38	「Photon」におけるアクセス制限不備の脆弱性	スマホアプリ「Photon」には、アクセス制限不備の脆弱性がありました。このため、任意の URL に誘導され、結果として任意の API が実行される可能性がありました。	2015 年 9 月 16 日	6.8
39 (*1)	「H2O」におけるディレクトリ・トラバーサルの脆弱性	ウェブサーバソフト「H2O」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、第三者によりサーバ上のファイルを意図せず閲覧される可能性がありました。	2015 年 9 月 17 日	5.0
40 (*1)	Apache Cordova プラグイン「cordova-plugin-file-transfer」における HTTP ヘッダ・インジェクションの脆弱性	Apache Cordova プラグイン「cordova-plugin-file-transfer」には、HTTP ヘッダ・インジェクションの脆弱性がありました。このため、任意のスクリプトが実行される可能性や、Cookie に任意の値が設定される可能性がありました。	2015 年 9 月 29 日	4.3

項番	脆弱性	セキュリティ上の問題点	JVN 公表日	CVSS 基本値
41	iOS アプリ「niconico」における SSL サーバ証明書の検証不備の脆弱性	iOS アプリ「niconico」には、SSL サーバ証明書の検証不備の脆弱性が存在しました。このため、中間者攻撃による暗号通信の盗聴などが行なわれる可能性がありました。	2015 年 9 月 29 日	4.0
42 (*1)	「抹茶請求書」における SQL インジェクションの脆弱性	請求書作成ソフト「抹茶請求書」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、ログインできるユーザにより任意の SQL 命令を実行される可能性がありました。	2015 年 9 月 30 日	6.5
43 (*1)	「抹茶請求書」におけるコード・インジェクションの脆弱性	請求書作成ソフト「抹茶請求書」には、インストール時のデータベース設定処理に問題がありました。このため、任意の PHP コードを実行される可能性がありました。	2015 年 9 月 30 日	5.1
44 (*1)	「抹茶 SNS」におけるコード・インジェクションの脆弱性	SNS 構築ソフト「抹茶 SNS」には、インストール時のデータベース設定処理に問題がありました。このため、任意の PHP コードを実行される可能性がありました。	2015 年 9 月 30 日	5.1
45 (*1)	「抹茶 SNS」におけるアクセス制限不備の脆弱性	SNS 構築ソフト「抹茶 SNS」には、アクセス制限不備の脆弱性がありました。このため、管理者権限を持たないユーザによって、管理者権限を取得される可能性がありました。	2015 年 9 月 30 日	5.1
46 (*1)	「baserCMS」におけるアクセス制限不備の脆弱性	コンテンツ管理システム「baserCMS」には、アクセス制限不備の脆弱性が存在しました。このため、システムにログインしたユーザが、細工したリクエストを送信することで、他のユーザの設定を変更できる可能性がありました。	2015 年 9 月 30 日	5.5
47 (*1)	「抹茶 SNS」における SQL インジェクションの脆弱性	コンテンツ管理システム「baserCMS」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 9 月 30 日	6.5
脆弱性の深刻度=レベル I（注意）、CVSS 基本値=0.0～3.9				
48	「Cacti」におけるクロスサイト・スクリプティングの脆弱性	ネットワーク管理ソフト「Cacti」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。項番 49 とは異なる問題です。	2015 年 7 月 9 日	2.6
49	「Cacti」におけるクロスサイト・スクリプティングの脆弱性	ネットワーク管理ソフト「Cacti」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。項番 48 とは異なる問題です。	2015 年 7 月 9 日	2.6
50 (*1)	「Welcart」におけるクロスサイト・スクリプティングの脆弱性	WordPress プラグイン「Welcart」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 7 月 24 日	3.5

項番	脆弱性	セキュリティ上の問題点	JVN 公表日	CVSS 基本値
51	「【Gallery01】PC、スマホ、ガラケー3 デバイス対応写真ギャラリーCMS フリー（無料）版」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	画像公開ソフト「【Gallery01】PC、スマホ、ガラケー3 デバイス対応写真ギャラリーCMS フリー（無料）版」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、第三者により意図しない操作をさせられる可能性がありました。	2015 年 8 月 12 日	2.6
52	ファイル暗号化ソフト「ED」に小さいファイルを暗号化した場合において暗号化データの解読が比較的容易になる問題	ファイル暗号化ソフト「ED」には、サイズの小さいファイルを暗号化した際に解読が比較的容易になる問題がありました。このため、16 バイト未満のファイルを暗号化した場合、ファイルが復号される可能性がありました。	2015 年 8 月 27 日	2.6
53 (*1)	「Apache Struts」におけるクロスサイト・スクリプティングの脆弱性	ウェブアプリケーションフレームワーク「Apache Struts」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 9 月 4 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）：組込みソフトウェアの脆弱性
（*4）：開発者に連絡がとれない脆弱性

（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 39 件あり、表 2-4 には脆弱性情報 38 件、表 2-5 には Alert [(*13)]（注意喚起情報）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	ANTLabs InnGate に複数の脆弱性	注意喚起として掲載
2	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
3	Adobe Flash Player (ByteArray) に解放済みメモリ使用 (use-after-free) の脆弱性	緊急案件として掲載
4	Grandstream GXV3611_HD カメラに SQL インジェクションの脆弱性	注意喚起として掲載 複数製品開発者へ通知
5	Windows の Adobe Type Manager モジュールに特権昇格の脆弱性	緊急案件として掲載
6	OpenSSL に証明書チェーンの検証不備の脆弱性	注意喚起として掲載 複数製品開発者へ通知
7	Adobe Flash Player (opaqueBackground) に解放済みメモリ使用 (use-after-free) の脆弱性	緊急案件として掲載

(*13) US-CERT が公表した注意喚起情報
(*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
8	Adobe Flash Player (BitmapData) に解放済みメモリ使用 (use-after-free) の脆弱性	緊急案件として掲載
9	Kaseya VSA に複数の脆弱性	注意喚起として掲載
10	Total Commander 用プラグイン FileInfo にサービス運用妨害 (DoS) の脆弱性	注意喚起として掲載
11	SolarWinds N-able N-central にドメイン管理パスワードを復号するためのパラメータがハードコードされている問題	注意喚起として掲載
12	Honeywell Tuxedo Touch Controller に複数の脆弱性	注意喚起として掲載
13	Fiat Chrysler Automobiles (FCA) UConnect に車両の遠隔操作の脆弱性	注意喚起として掲載
14	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
15	Android Stagefright に複数の脆弱性	緊急案件として掲載 複数製品開発者へ通知
16	複数の BIOS 実装において、スリープモードからの復帰後に UEFI の書き込み保護が適切に設定されない問題	複数製品開発者と調整
17	Chiyu Technology の指紋認証入退室管理システムに複数の脆弱性	注意喚起として掲載
18	ALEOS を使用する Sierra Wireless の複数のデバイスがハードコードされたパスワードを使用する問題	注意喚起として掲載
19	Mobile Devices 製 C4 OBD2 ドングルに複数の脆弱性	注意喚起として掲載
20	Actiontec GT784WN Wireless N DSL モデムルータに複数の脆弱性	注意喚起として掲載
21	Cisco Prime Infrastructure に SUID root された実行ファイルが存在する問題	注意喚起として掲載
22	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 特定製品開発者へ通知
23	Trend Micro Deep Discovery Inspector に複数の脆弱性	注意喚起として掲載
24	Dedicated Micros のデジタルビデオレコーダが、平文で通信し、パスワード認証をしていない問題	注意喚起として掲載
25	複数の DSL ルータ製品がハードコードされたパスワードを使用する問題	注意喚起として掲載
26	UPnP を実装した複数のルータ製品にセキュリティ機能の実装が不十分な問題	注意喚起として掲載
27	Philippine Long Distance Telephone SpeedSurf 504AN および Kasda KW58293 に複数の脆弱性	注意喚起として掲載
28	Belkin N600 DB Wireless Dual-Band N+ Router に複数の脆弱性	複数製品開発者と調整
29	Seagate および LaCie ワイヤレスストレージ製品に複数の脆弱性	注意喚起として掲載
30	ISC BIND 9 に複数の脆弱性	緊急案件として掲載 複数製品開発者へ通知
31	OrientDB および OrientDB Studio に複数の脆弱性	注意喚起として掲載
32	Mediabridge Medialink Wireless-N Broadband Router に複数の脆弱性	注意喚起として掲載
33	CENTUM を含む複数の YOKOGAWA 製品の通信機能に複数の脆弱性	注意喚起として掲載
34	Impero Education Pro に複数の脆弱性	特定製品開発者と調整
35	Securifi Almond ルータ製品に複数の脆弱性	注意喚起として掲載
36	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
37	refbase (Web Reference Database) に複数の脆弱性	注意喚起として掲載
38	HTTP リクエスト経由で設定された Cookie によって HTTPS 接続がバイパスされたり情報漏えいが発生する問題	注意喚起として掲載

「対応状況」について

・複数製品開発者へ通知

JVN 公表と同時もしくは公表後に複数製品開発者にその旨通知したもの

・特定製品開発者へ通知
JVN 公表と同時もしくは公表後に該当製品開発者にその旨通知したもの
・緊急案件として掲載
緊急度の高い脆弱性情報に「緊急」マークを付け注意喚起として公表したもの
・注意喚起として掲載
CERT/CC が独自に（事前の国際連携や調整等なく）公表した脆弱性情報を、JPCERT/CC が翻訳して注意喚起として公表したもの（公表後の通知なし）
・複数製品開発者と調整
CERT/CC や ICS-CERT 等海外の関連組織から国際調整依頼をうけて、JPCERT/CC が日本国内の複数の製品開発者との調整を行ったもの
・特定製品開発者と調整
CERT/CC や ICS-CERT 等海外の関連組織から国際調整依頼を受けて、もしくは製品開発者自身から自社製品の脆弱性としての届出があり、それに併せて CERT/CC や ICS-CERT 等との国際連携と調整の依頼も受け、JPCERT/CC が国際調整を実施後 JVN にて公表したもの

表 2-5.米国 US-CERT (*15) と連携した注意喚起情報

項番	脆弱性
1	Adobe Flash Player および Microsoft Windows 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 9 月末までに、「連絡不能開発者」と位置づけて取扱った 217 件の処理状況の推移を示したものです。

2015 年 9 月末時点での処理状況は 217 件のうち、製品開発者と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 40 件（前四半期は 36 件）、連絡不能件数は 177 件（前四半期は 169 件）となりました。この 177 件は新規に製品開発者名を公表した 12 件と届出のあった製品名および対象となるバージョンを追加情報として(*16)公表した 165 件とで構成されています。また今期は、4 件の「連絡不能開発者」と連絡がとれたため「連絡不能開発者」一覧から削除しました。その結果、新規に公表された 12 件と差引き、8 件の純増となりました。

また、今期「調整再開（調整完了）」した 3 件は JVN の公表に向け製品開発者と調整を行った結果、脆弱性対策情報の公表に至ったものです。「連絡不能（JVN 公表）」の 2 件は、公表判定委員会の審議にて JVN 公表が適当であると判定され JVN 公表に至ったものです。

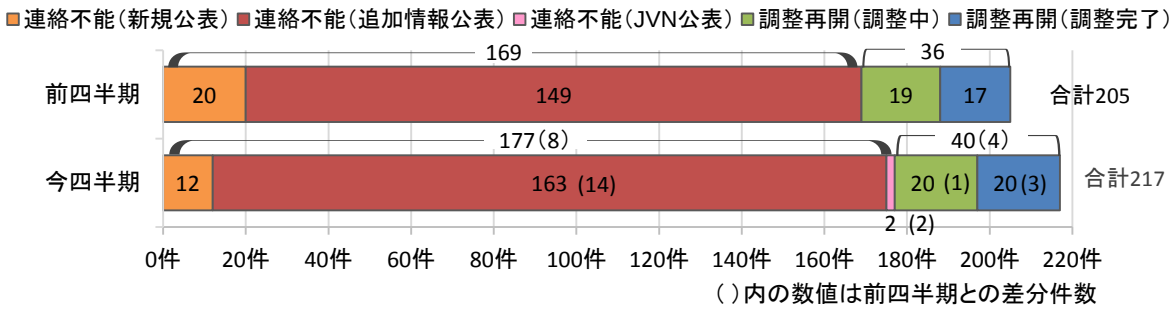


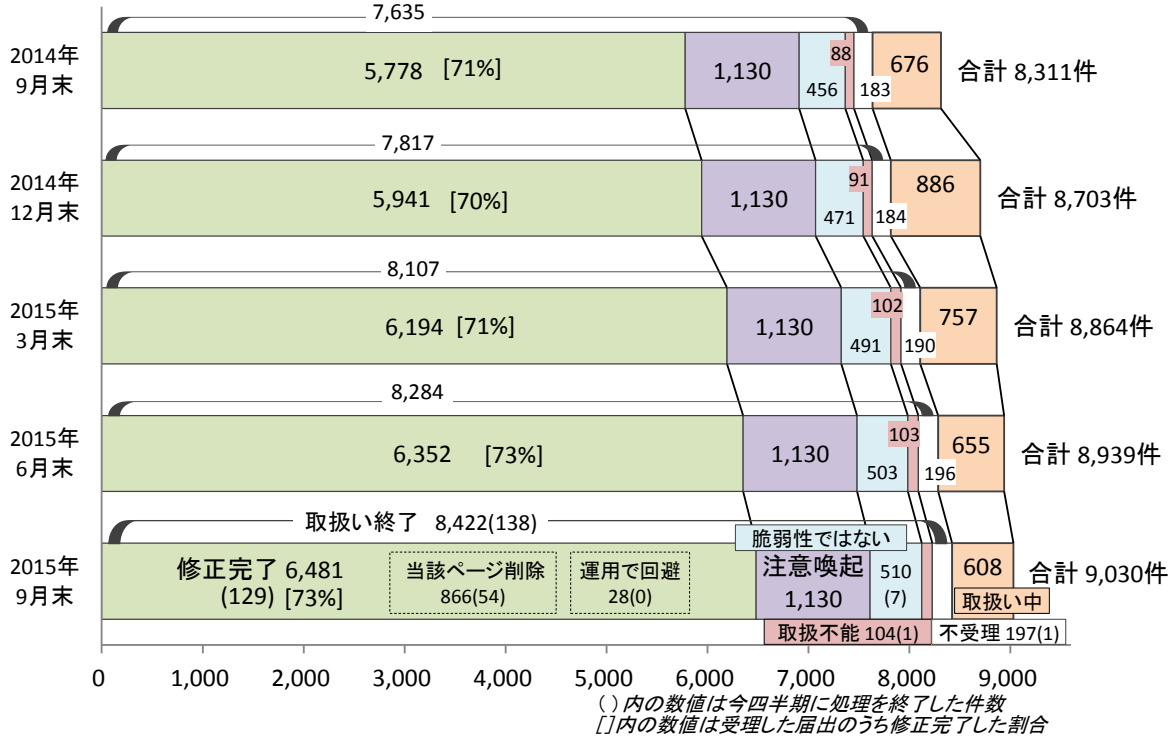
図2-12. 連絡不能開発者一覧の処理状況

(*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 9 月末時点の届出の累計は 9,030 件で、今四半期中に取扱いを終了したものは 138 件（累計 8,422 件）でした。このうち「修正完了」したものは 129 件（累計 6,481 件）、「注意喚起」により処理を取りやめたもの[*17] 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 7 件（累計 510 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 1 件（累計 104 件）でした。また「不受理」としたものは 1 件（累計 197 件）でした。取扱いを終了した累計 8,422 件のうち「修正完了」「脆弱性ではない」の合計 6,991 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を確認しています。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 54 件（累計 866 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の四半期別推移

[*17] 「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。

以下に、今までに届出のあったウェブサイトの脆弱性 9,030 件のうち、不受理を除いた 8,833 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 7 割を企業が占めています。

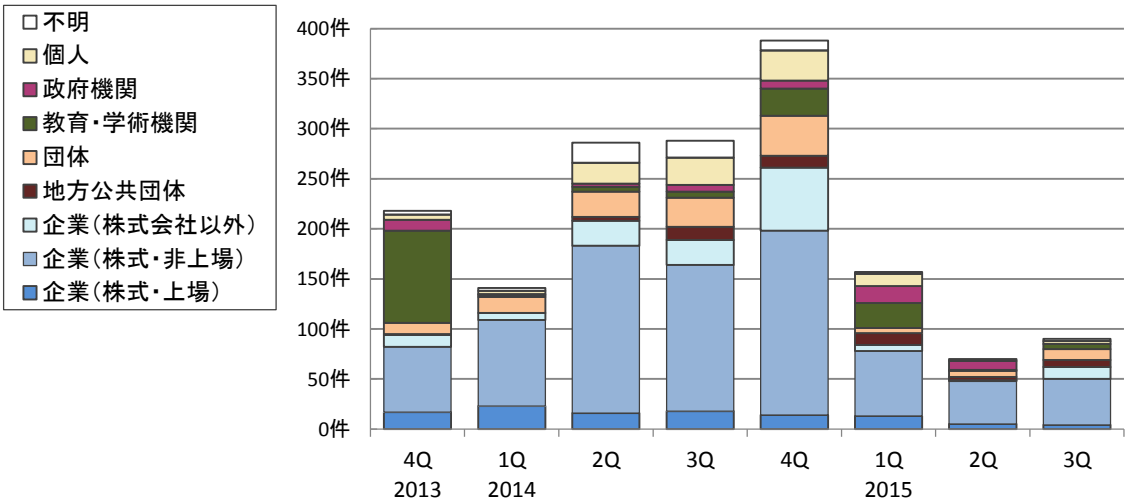


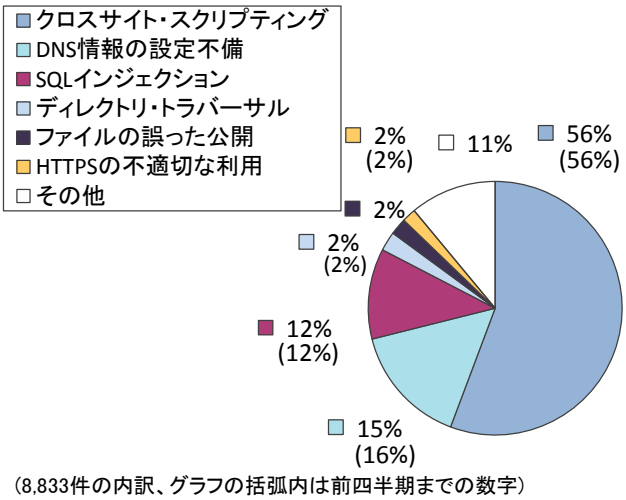
図2-14. 四半期ごとの運営主体の種類別届出件数

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]。

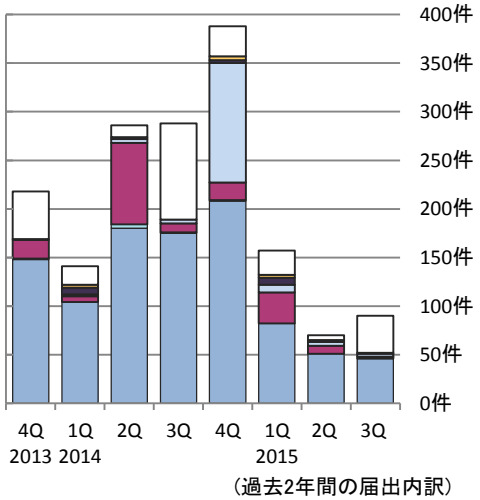
累計では、「クロスサイト・スクリプティング」だけで 56%を占めており、次いで「DNS 情報の設定不備」「SQL インジェクション」となっています。「DNS 情報の設定不備」は 15%ありますが、2008 年から 2009 年にかけて多く届出されたのが反映されています。今四半期は「クロスサイト・スクリプティング」が約半数を占めています。今期は「OS コマンドインジェクション」が多く届出されたため「その他」が多くなっています。なお、この統計は本制度における届出の傾向であり、世の中に存在する脆弱性の傾向と必ずしも一致するものではありません。

ウェブサイトの脆弱性の種類別の届出状況



(8,833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



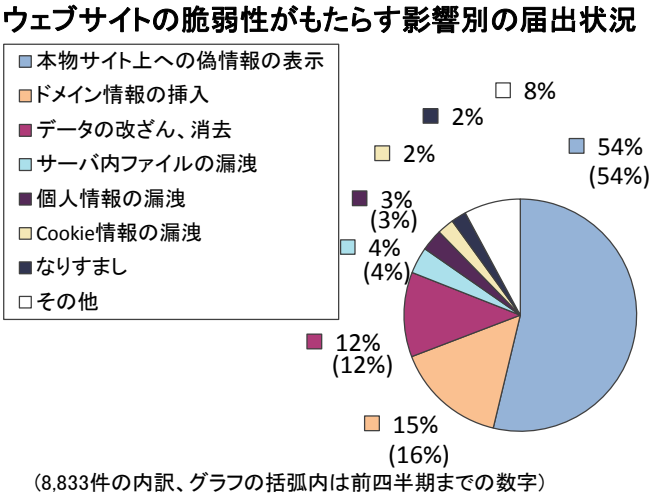
(過去2年間の届出内訳)

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。

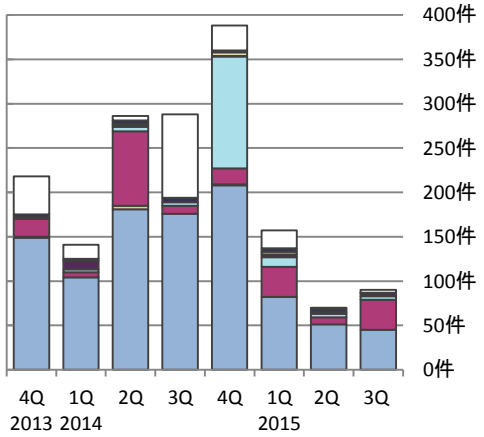
図 2-17、2-18 のグラフは、届出された脆弱性がもたらす影響別の分類です。図 2-17 は届出の影響別割合を、図 2-18 は過去 2 年間の届出件数の推移を四半期ごとに示しています。

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 割超を占めています。



(8,833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 3 四半期に修正を完了した 129 件のうち 43 件（33%）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（158 件中 76 件（48%））より減少しています。

表 2-6 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通知してから、90 日以内に修正が完了した脆弱性の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 67%でした。

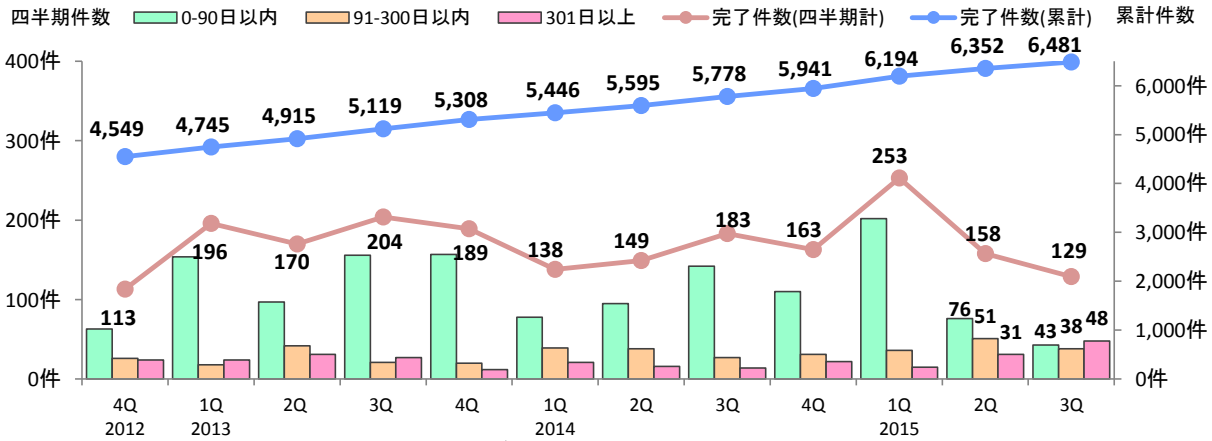


図2-19. ウェブサイトの脆弱性の修正完了件数

表 2-6. 90 日以内に修正完了した累計およびその割合の推移

	2012 4Q	2013 1Q	2Q	3Q	4Q	2014 1Q	2Q	3Q	4Q	2015 1Q	2Q	3Q
修正完了件数	4,549	4,745	4,915	5,119	5,308	5,446	5,595	5,778	5,941	6,194	6,352	6,481
90 日以内の件数	2,993	3,147	3,244	3,400	3,557	3,635	3,730	3,872	3,982	4,184	4,260	4,303
90 日以内の割合	66%	66%	66%	66%	67%	67%	67%	67%	67%	68%	67%	67%

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 47%の届出が 30 日以内、全体の 66%の届出が 90 日以内に修正されています。

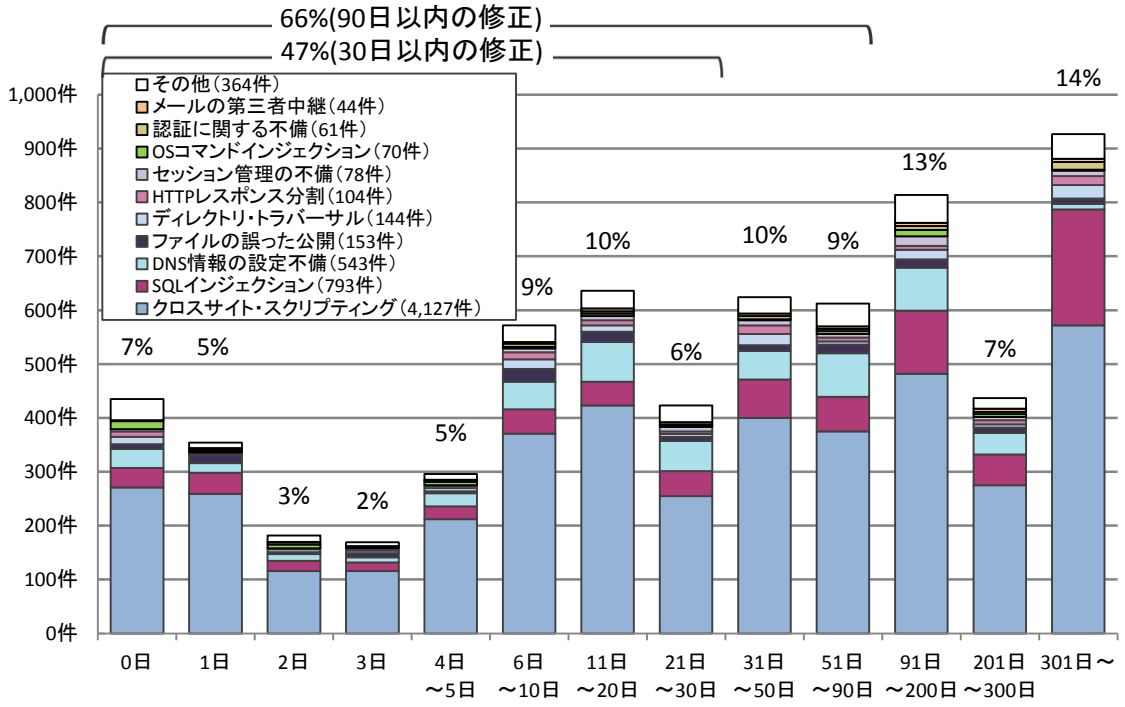


図2-20. ウェブサイトの修正に要した日数

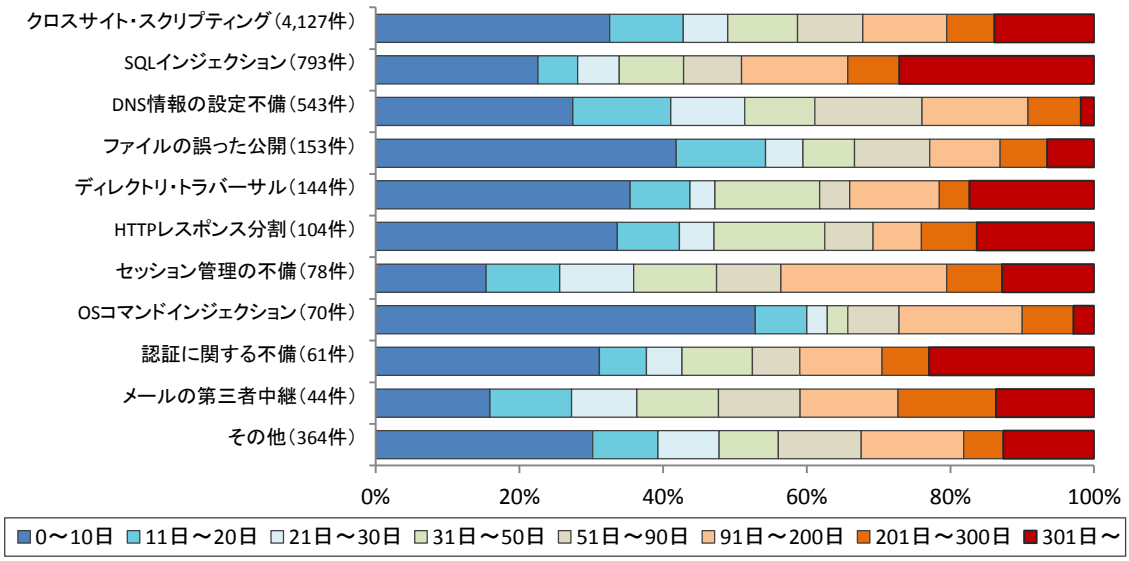


図2-21. ウェブサイトの修正に要した脆弱性種類別の日数の傾向

[*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。

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 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繰り返し連絡を試み、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後、90 日以上経っても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 504 件（前四半期は 562 件）と前期からは減少しています。

なお、既にウェブサイトが閉鎖されている、もしくは問題のあるページが削除されていることが確認できたものは取扱い終了としています。また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が含まれる割合は全体の約 15%を占めています。

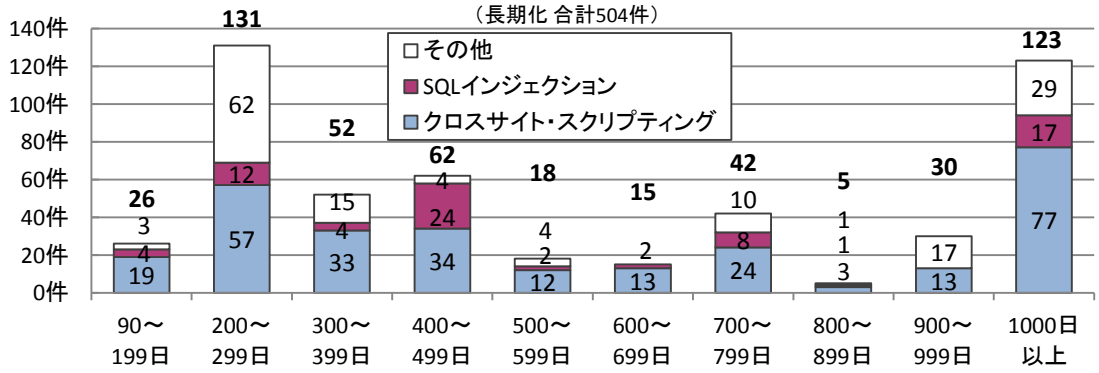


図2-22. 取扱いが長期化(90日以上経過)しているウェブサイトの経過日数と脆弱性の種類

表 2-7 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。今期は 504 件と前四半期の 562 件から数パーセントの微減ですが、前年度比では大幅に増化しています

表 2-7. 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 4Q	2014 1Q	2Q	3Q	4Q	2015 1Q	2Q	3Q
取扱い中の件数	505	490	596	676	886	757	655	608
長期化している件数	358	357	353	402	446	415	562	504
長期化している割合	71%	73%	59%	59%	50%	55%	86%	83%

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把握し、脆弱性対策を実施する事が必要です。脆弱性の理解・対策にあたっては、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/

⇒「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

⇒「安全なウェブサイトの構築と運用管理に向けての 16 ヶ条 ～セキュリティ対策のチェックポイント～」
https://www.ipa.go.jp/security/vuln/websitecheck.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

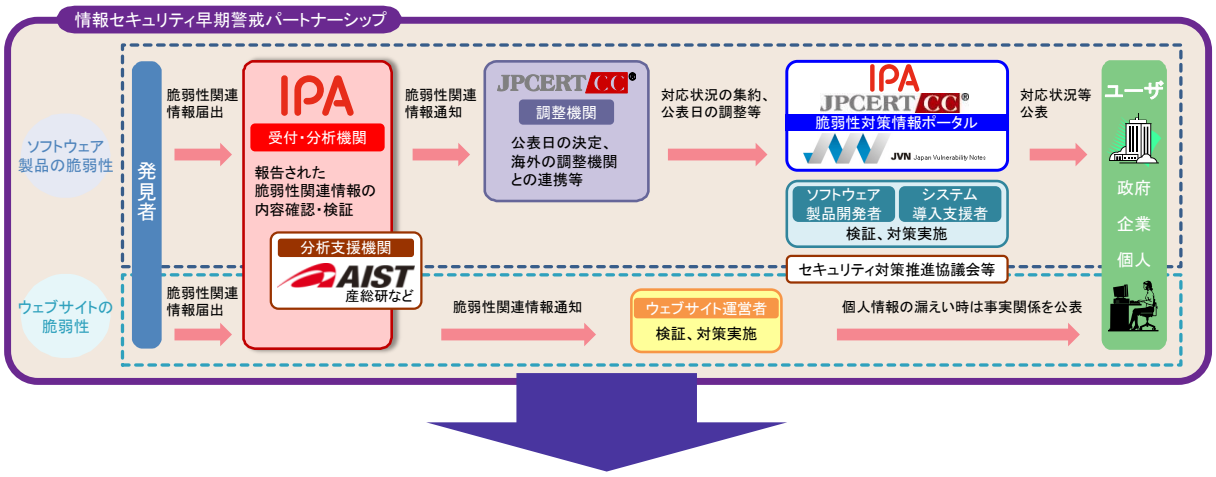
付表 2. ウェブサイトの脆弱性の分類

	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