ソフトウェア等の脆弱性関連情報に関する活動報告レポート

[2013 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に関する活動報告レポートについて

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、ソフトウェア等脆弱性関連情報取扱基準（経済産業省告示 第 235 号）に基づき、2004 年 7 月より脆弱性関連情報の届出業務を実施しています。

本レポートでは、2013 年 7 月 1 日から 2013 年 9 月 30 日までの間に受け付けた脆弱性関連情報の統計及び事例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
2013 年 10 月 22 日

目次

1. 2013 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状況

1-1. 脆弱性関連情報の届出状況

～ 脆弱性の届出件数の累計が 8,985 件になりました ～

「情報セキュリティ早期警戒パートナーシップ [(*1)]」（以降、本制度）における届出状況について、表 1-1 は 2013 年第 3 四半期の脆弱性関連情報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件数を示しています。今期のソフトウェア製品に関する届出件数は 51 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 266 件、合計 317 件でした。届出受付開始からの累計件数は 8,985 件で、内訳はソフトウェア製品に関するもの 1,620 件、ウェブサイトに関するもの 7,365 件でウェブサイトに関する届出が全体の 82%を占めています。

表 1-1.　届出件数

分類	今期件数	累計件数
ソフトウェア製品	**51** 件	**1,620** 件
ウェブサイト	**266** 件	**7,365** 件
合計	**317** 件	**8,985** 件

図 1-1 のグラフは過去 3 年間の届出件数の四半期別推移を示したものです。今四半期のソフトウェア製品、ウェブサイトに関する届出はともに前四半期よりも増加しています。表 1-2 は過去 3 年間の四半期別の累計届出件数および 1 就業日あたりの届出件数の推移です。1 就業日あたりの届出件数は今四半期末で 3.97 [(*2)] 件となっています。

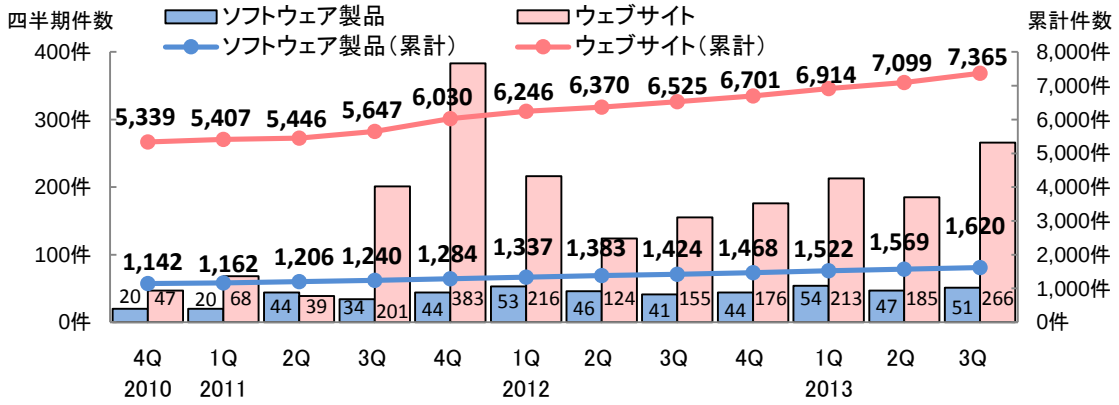


図1−1.脆弱性関連情報の届出件数の四半期別推移

表 1−2. 届出件数（過去 3 年間）

	2010 4Q	2011 1Q	2Q	3Q	4Q	2012 1Q	2Q	3Q	4Q	2013 1Q	2Q	3Q
累計届出件数[件]	6,481	6,569	6,652	6,887	7,314	7,583	7,753	7,949	8,169	8,436	8,668	8,985
1就業日あたり[件/日]	4.10	4.01	3.92	3.91	4.01	4.03	3.99	3.96	3.95	3.97	3.94	3.97

(*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
http://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が 5,900 件を超過しました ～

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。

表 1-3.　修正完了件数

分類	今期件数	累計件数
ソフトウェア製品	**26** 件	**785** 件
ウェブサイト	**204** 件	**5,119** 件
合計	**230** 件	**5,904** 件

ソフトウェア製品の脆弱性の届出のうち、製品開発者が修正を完了し、今四半期に JVN で対策情報を公表したものは 26 件[(*3)]（累計 785 件）でした。2010 年第 4 四半期以降は修正完了件数は 30 件前後で推移しています。今四半期に対策情報を公表した 26 件のうち、届出を受理してから公表までに 46 日[(*4)]以上経過したものは 16 件（62%）でした。

ウェブサイトの脆弱性関連情報の届出のうち、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は 204 件（累計 5,119 件）でした。修正を完了した 204 件のうち、ウェブアプリケーションを修正したものが 180 件（88%）、当該ページを削除したもの 22 件（11%）、運用で回避したもの 2 件（1%）でした。なお、修正を完了した 204 件のうち 48 件（24%）は、運営者へ脆弱関連情報を通知してから修正完了までに 91 日[(*5)]以上を要した届出です。今四半期は、修正完了までに 91 日以上を要した届出の割合が、前四半期（170 件中 73 件（43%））より減少しています。

1-3. 調整不能案件の取扱い状況

本制度において届出を受け付けたソフトウェア製品の開発者に対して、一定期間にわたり連絡を試みても連絡が取れない製品開発者を「連絡不能開発者」と位置づけています。製品開発者と連絡をとる糸口を得るために、「連絡不能開発者一覧[(*6)]」において段階的に製品開発者名と製品情報を公表することで、製品開発者からの連絡および関係者からの情報提供を求めています。

（1）　連絡不能開発者一覧の公表状況

今四半期は新たに「製品開発者名」を 4 件公表し、今四半期末時点の「連絡不能開発者一覧」の公表件数は、110 件となりました。また、今四半期は「製品開発者名」に加えて「製品情報（対象製品の具体的な名称およびバージョン）」を新たに公表したものはありませんでした。

（2）　連絡不能開発者一覧の公表後の取扱状況

今四半期には、製品開発者からの応答はありませんでした。これまでに応答があった 18 件のうち、8 件が本制度における取扱いを終了しました。

(*3)　表 2-3 参照
(*4)　公表日の目安は、脆弱性関連情報の取扱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、脆弱性関連情報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：http://jvn.jp/reply/index.html

1-4. 注目すべき脆弱性

1-4-1. 古いバージョンの CMS を利用しているウェブサイトの届出が増加

～ CMS 本体だけでなく、CMS のプラグインのバージョンも要チェック ～

2013 年の第 2 四半期に引き続き、ウェブサイト改ざんの被害が増加しています。9 月には、IPA や JPCERT/CC をはじめ、複数の組織から注意が呼びかけられました[*7][*8]。ウェブサイト改ざんでは、CMS（ウェブサイトを簡易に構築・管理するためのソフトウェアの総称：Contents Management System）の古いバージョンに存在する脆弱性が悪用された事例が確認されています。

「情報セキュリティ早期警戒パートナーシップ」においても、脆弱性が存在する古いバージョンの CMS を利用している旨の届出が届出開始から今四半期までの累計で 118 件ありました。そのうち、41 件が今四半期(7～9 月)に届出られたものあり、依然として脆弱性が存在する古いバージョンの CMS を利用していることがうかがえます。

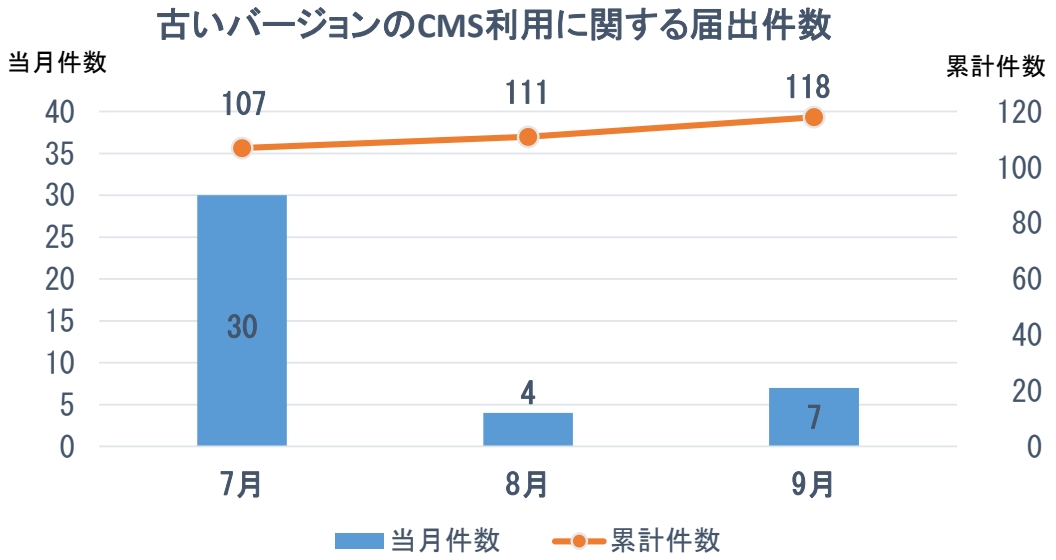


図 1-2　古いバージョンの CMS 利用に関する届出件数

届出の中には、データベースが不正に操作される SQL インジェクションの脆弱性や、第三者にウェブページの編集を可能にしてしまうアクセス制限回避の脆弱性が含まれているバージョンがありました。これらの脆弱性を放置すると、重要な情報の漏えいや、ウェブページが改ざんされる可能があり危険です。

脆弱性は、CMS 本体だけでなく CMS の機能を拡張する「プラグイン」にも存在する場合があります。プラグインの脆弱性についても攻撃が観測されています[*9]が、対策は見落とされがちです。

ウェブサイト運営者は、利用している CMS やプラグインのバージョンを確認し、古い場合は速やかに最新バージョンへのアップデート等の脆弱性対策を実施してください。アップデートが困難な場合は、開発元が公開している情報を基に、回避策の適用を実施してください。

[*7] https://www.ipa.go.jp/security/topics/alert20130906.html
[*8] https://www.ipa.go.jp/security/topics/alert20130913.html
[*9] http://www-935.ibm.com/services/jp/its/pdf/tokyo_soc_report2013_h1.pdf#page=8

1-4-2. ウェブアプリケーションフレームワークの脆弱性を狙った攻撃の広がりについて
～ Apache Struts の脆弱性を狙った攻撃が国内でも観測される ～

9 月 6 日に公開した JVN#33504150「『Apache Struts』において任意のコマンドを実行される脆弱性」[*10] には、その脆弱性を狙った攻撃が国内でも観測されていました[*11]。攻撃が成功した場合、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す。これは、ウェブサイトが改ざんされたり、サーバが乗っ取られて踏み台にされたりするなどの被害に繋がるものです。

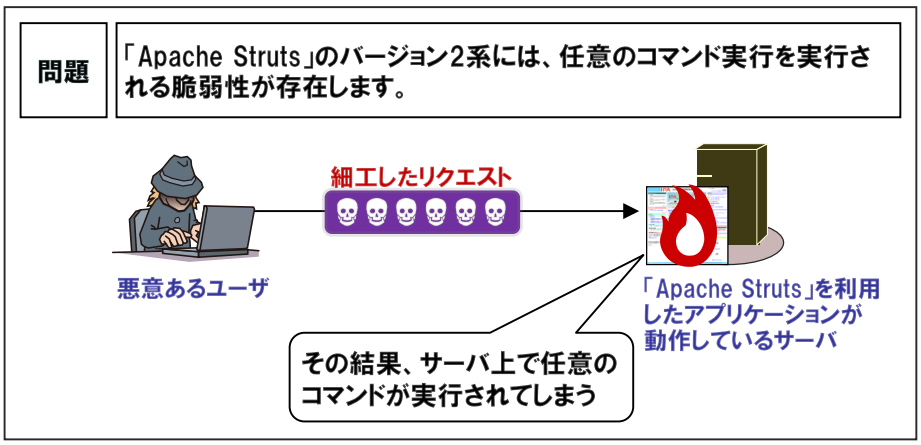


図 1-3　Apache Struts の脆弱性を悪用した攻撃の概要

この Apache Struts に限らず、ウェブアプリケーションフレームワーク（ウェブアプリケーションの基盤となる機能を提供し、開発を助けてくれる仕組み）[*12] の脆弱性を狙った攻撃はここ数年継続しており、ウェブサイト改ざんなどの被害にも繋がっています。今後も同様の攻撃は続くことが予想されるため、継続的な対策が欠かせません。

ウェブアプリケーションフレームワークは、その上で稼動するウェブアプリケーションと密に連携していることが多く、ウェブアプリケーションフレームワークをバージョンアップするためにはウェブアプリケーションの部分的な改修を要する場合があります。しかしウェブアプリケーションが改修できない場合には、ウェブアプリケーションフレームワークもバージョンアップできないことがあり、ウェブサイトの安全な運用に支障をきたします。

ウェブサイト運営者は具体的な対応策として、ウェブアプリケーションを開発した際の設計資料やソースコード等の管理、ウェブアプリケーションに関係するプログラミング言語やフレームワークに明るい技術者の確保、などが求められます。また、こうした運用ができるだけ速やかにできるよう、自組織の運用体制で適切に管理できるウェブアプリケーションフレームワークの選定も重要です。

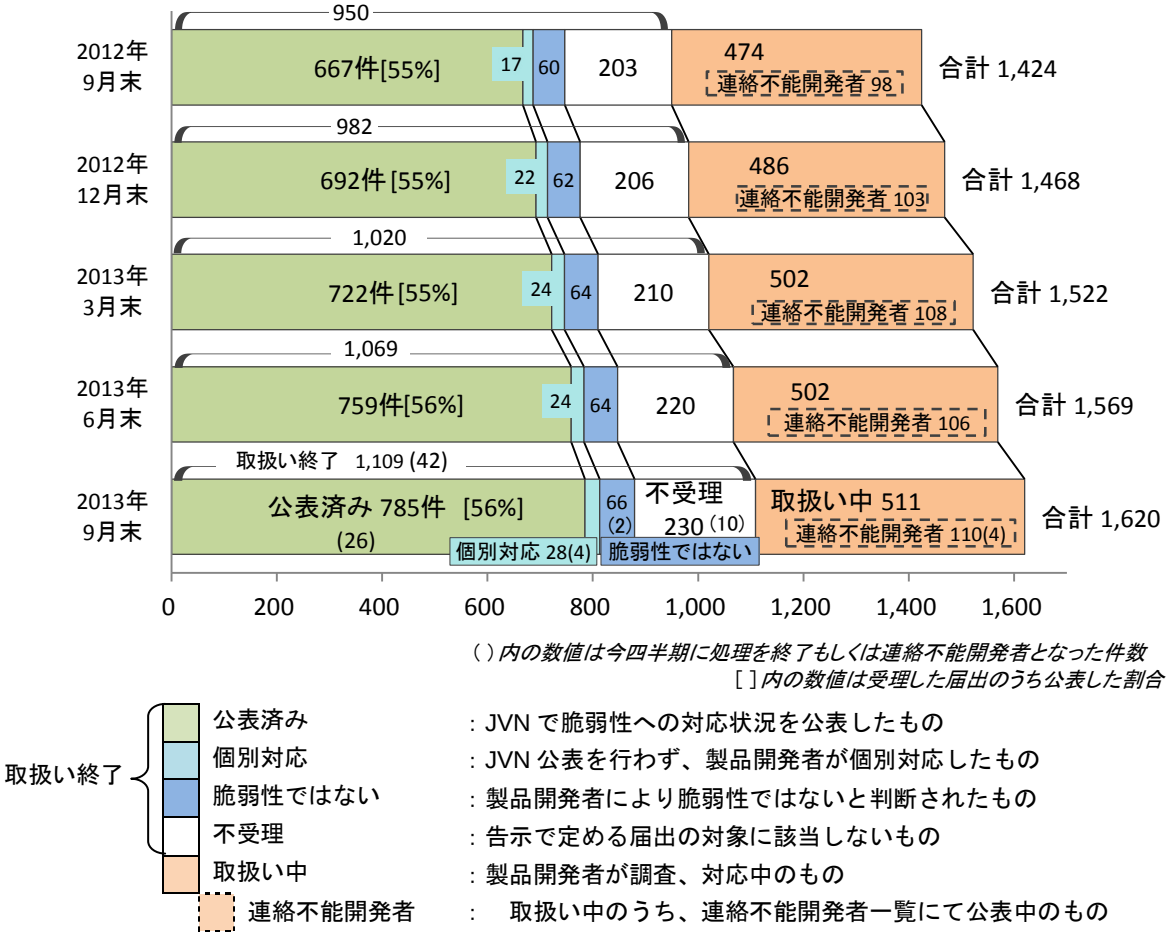
[*10] https://jvn.jp/jp/JVN33504150/
[*11] https://www.jpcert.or.jp/at/2013/at130033.html
[*12] https://www.ipa.go.jp/security/awareness/vendor/programmingv2/contents/004.html

2. ソフトウェア等の脆弱性に関する届出の処理状況（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関連情報の届出における、処理状況の推移を示したものです。2013 年第 3 四半期に公表した脆弱性は 26 件（累計 785 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 4 件（累計 28 件）、製品開発者が「脆弱性ではない」と判断したものは 2 件（累計 66 件）、「不受理」としたものは 10 件 (*13)（累計 230 件）、取扱い中は 511 件でした。今四半期に、取扱中の届出について連絡不能開発者一覧に公表した連絡不能開発者 (*14) は 4 件です。2013 年 9 末時点の連絡不能開発者公表数は 110 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
[ ] 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
- 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 各四半期時点での脆弱性関連情報の届出の処理状況

(*13) 今四半期の届出の中で不受理とした 5 件、前四半期までの届出の中で今四半期に不受理とした 5 件です。
(*14) 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ている製品開発者については、公表回数の累計を計上しています。

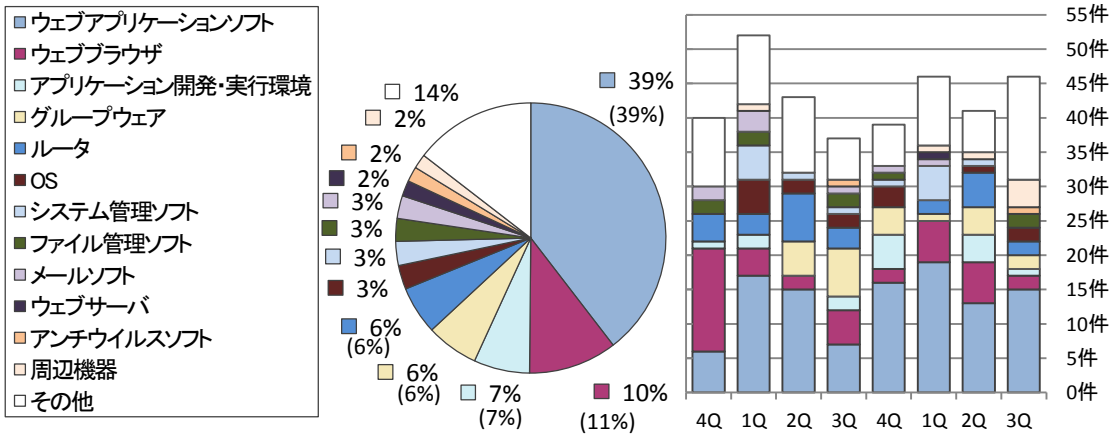
以下に、届出受付開始から今四半期までに届出のあったソフトウェア製品の脆弱性関連情報1,620 件のうち、不受理を除いた 1,390 件の届出を分析した結果を記載します。

2-1-2. ソフトウェア製品の種類

図 2-2 のグラフは製品種類別の届出件数の割合を、図 2-3 は過去 2 年間の製品種類別の届出件数の四半期別推移をそれぞれ示したものです。

今四半期における製品種類別の届出件数は「ウェブアプリケーションソフト」が約 4 割と最も多く、次に「周辺機器」が多く届出されています。

ソフトウェア製品の製品種類別の届出状況



※その他には、データベース、携帯機器などがあります。
（1,390件の内訳、グラフの括弧内は前四半期までの数字）

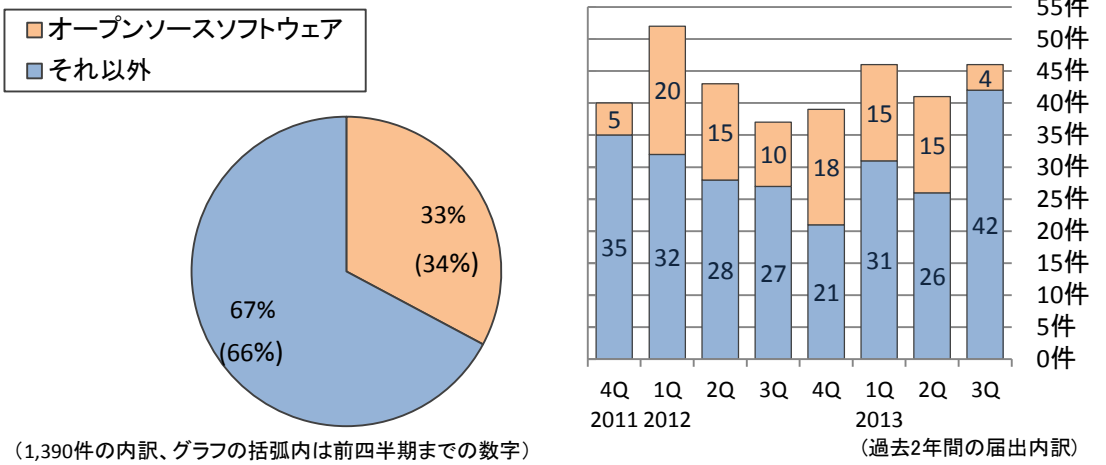
（過去2年間の届出内訳）

図2-2. 製品種類別の届出件数の割合

図2-3. 製品種類別の届出件数(四半期別推移)

図 2-4 のグラフはオープンソースソフトウェアとそれ以外のソフトウェアの脆弱性の届出件数の割合を、図 2-5 は過去 2 年間の「オープンソースソフトウェア」と「それ以外」のソフトウェアの届出件数の四半期別推移をそれぞれ示したものです。届出受付開始から今四半期までの届出のうち、オープンソースソフトウェアの届出が占める割合は、33%となっています。

オープンソースソフトウェアの脆弱性の届出状況



（1,390件の内訳、グラフの括弧内は前四半期までの数字）

（過去2年間の届出内訳）

図2-4. オープンソースソフトウェアの届出件数の割合

図2-5. オープンソースソフトウェアの届出件数（四半期別推移）

図 2-6 のグラフは過去 2 年間の届出件数を「スマートフォン向けアプリ」と「それ以外」のソフトウェアの届出件数の四半期別推移を、図 2-7 のグラフはスマートフォン向けアプリに関する届出の公表までに要した日数を示したものです。「スマートフォン向けアプリ」に関する届出は 2011 年から増加し、2012 年以降は 10 件前後で推移している状況です。また、脆弱性情報を JVN で公表したスマートフォン向けアプリの届出のうち、42%は受理から 45 日以内に対策が行われており、他のソフトウェア製品に比べて早めに対策される傾向にあります。

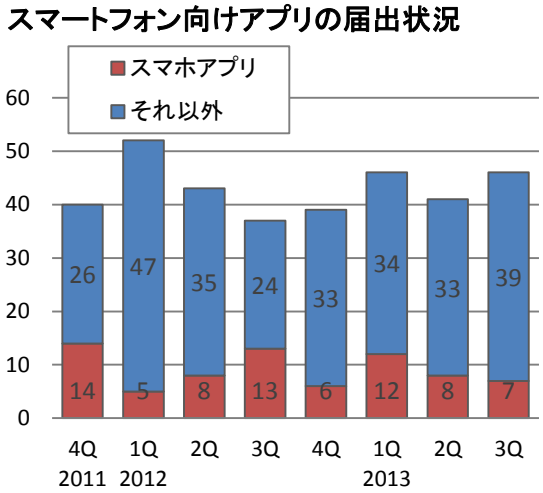


図2-6.スマートフォン向けアプリの届出件数（四半期別推移）

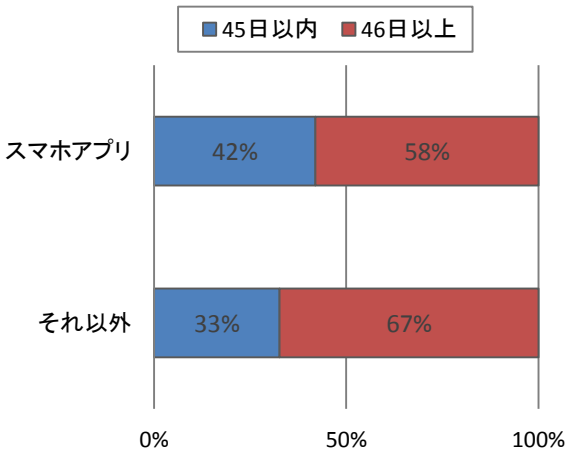
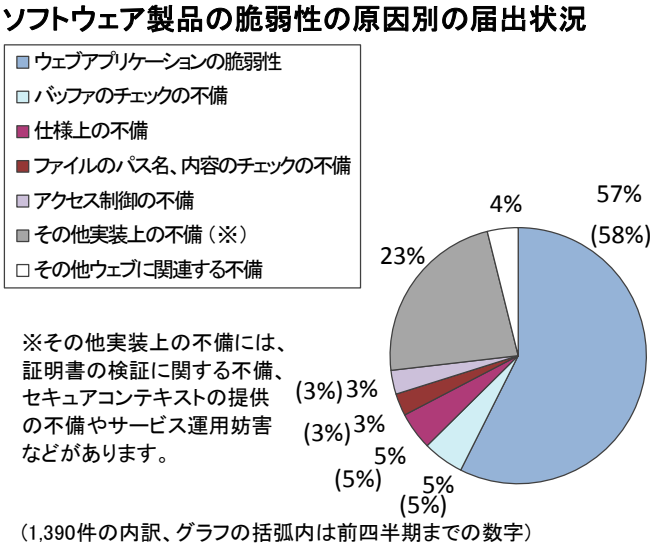


図2-7.スマートフォン向けアプリとそれ以外の公表までの日数

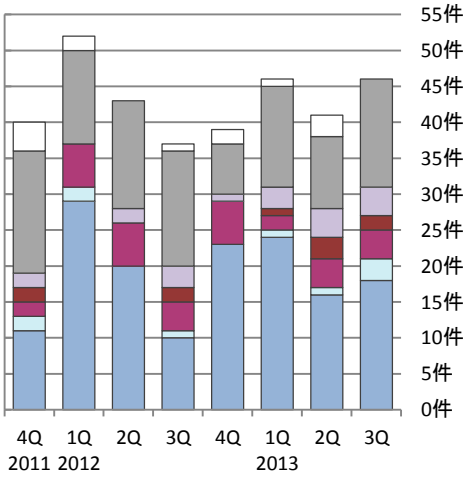
2-1-3. 脆弱性の原因と脅威

図 2-8 のグラフは原因別の届出件数の割合を、図 2-9 のグラフは過去 2 年間の原因別届出件数の四半期別推移をそれぞれ示したものです。今四半期におけるソフトウェア製品の脆弱性の原因別の届出件数は、前四半期と同様に「ウェブアプリケーションの脆弱性」が最多となっています。



（1,390件の内訳、グラフの括弧内は前四半期までの数字）

図2-8. 脆弱性の原因別の届出件数の割合

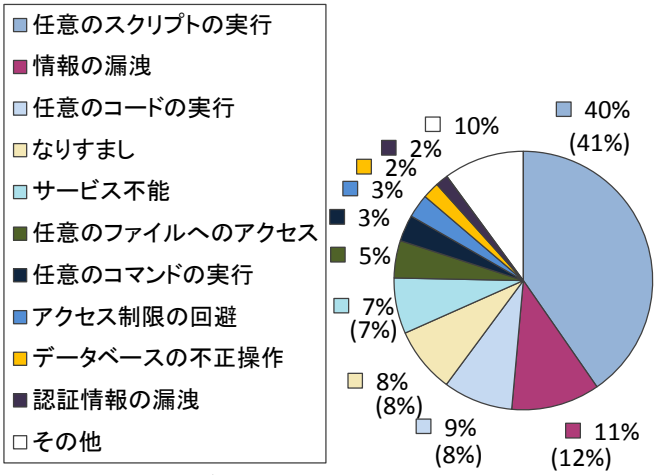


（過去2年間の届出内訳）

図2-9. 脆弱性の原因別の届出件数(四半期別推移)

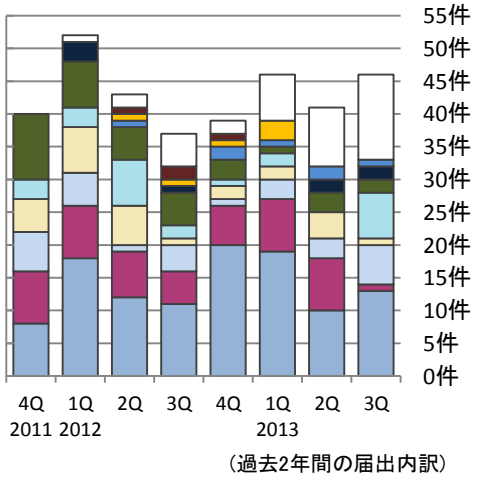
図 2-10 のグラフは脅威別の届出件数の割合を、図 2-11 は過去 2 年間の脅威別の届出件数の四半期別推移をそれぞれ示したものです。届出受付開始から今四半期までの届出のうち、「任意のスクリプトの実行」が約 40%を占めています。また、今四半期は「情報の漏洩」が前四半期が 8 件なのに対して、今四半期 1 件と前期と比べ減少しています。一方「任意のコードの実行」は、前四半期 3 件なのに対して、今四半期 6 件、および「サービス不能」前四半期 0 件、今四半期 7 件と増加しています。

ソフトウェア製品の脆弱性がもたらす脅威別の届出状況



（1,390件の内訳、グラフの括弧内は前四半期までの数字）

図2-10. 脆弱性がもたらす脅威別の届出件数の割合



（過去2年間の届出内訳）

図2-11. 脆弱性がもたらす脅威別の届出件数（四半期別推移）

2-1-4. 調整および公表状況

表 2-1 は今四半期の脆弱性の公表件数および届出受付開始から今四半期までの累計公表件数を示しています。JPCERT/CC は、2 種類の脆弱性関連情報について、日本国内の製品開発者や関係者との調整、および海外 CSIRT の協力のもと海外の製品開発者との調整を行っています[*15]。これらの脆弱性関連情報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： http://jvn.jp/ ）において公表しています。図 2-12 のグラフは、届出受付開始から今四半期までの届出および海外 CSIRT 等との連携の中で、対策情報を公表した 1,757 件について、過去 3 年間の公表件数の四半期別推移を示したものです。

表 2-1. 脆弱性関連情報の提供元別 脆弱性公表件数

	情報提供元	今期件数	累計件数
①	国内外の発見者から届出があったもの、および製品開発者自身から自社製品の脆弱性、対策方法について届出を受けたもの	26 件	785 件
②	海外 CSIRT 等と連携して公表したもの	28 件	972 件
	合計	54 件	1,757 件

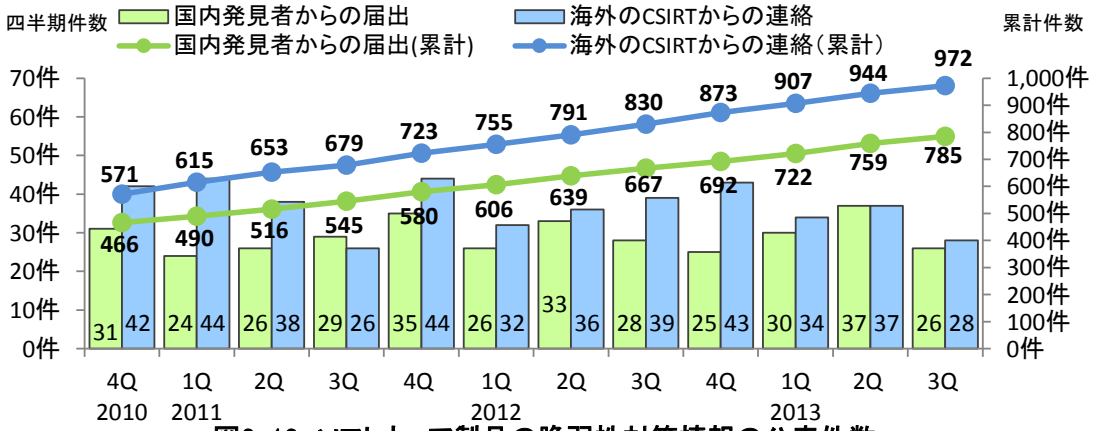


図2-12. ソフトウェア製品の脆弱性対策情報の公表件数

（1） 国内外の発見者および製品開発者から届出があり、公表した脆弱性

届出受付開始から今四半期までに届出のあったソフトウェア製品の脆弱性関連情報（表 2-1 の①）について、図 2-13 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。表 2-2 は過去 3 年間において 45 日以内に公表した件数の割合推移を四半期別に示したものです。45 日以内に公表した件数は今四半期で 33%、45 日を超過した件数は 67%です。製品開発者は脆弱性を攻撃された場合の危険性を認識し、迅速な対策を講じる必要があります。

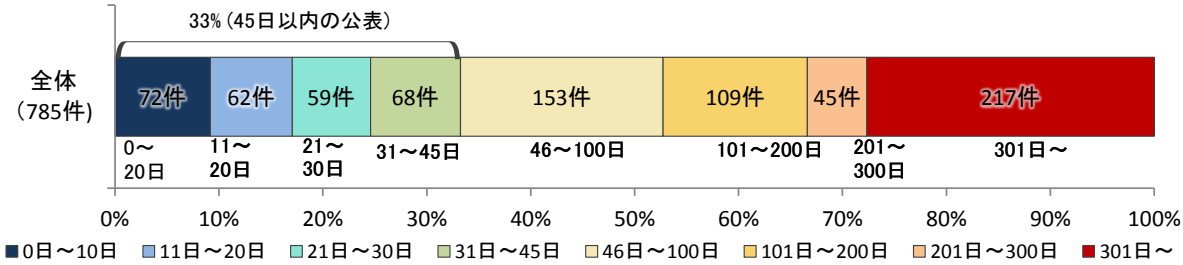


図2-13. ソフトウェア製品の脆弱性公表日数

表 2-2. 45 日以内に公表した件数の割合推移（四半期別）

4Q	2011 1Q	2Q	3Q	4Q	2012 1Q	2Q	3Q	4Q	2013 1Q	2Q	3Q
38%	38%	36%	34%	33%	34%	34%	35%	34%	33%	33%	33%

[*15] JPCERT/CC 活動概要 Page15～21(http://www.jpcert.or.jp/pr/2013/PR20131010.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届出があり、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し公表したものが 7 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 6 件（表 2-3 の*2）、複数開発者・製品に影響がある脆弱性 1 件（表 2-3 の*3）、組込みソフトウェア製品の脆弱性が 8 件（表 2-3 の*4）ありました。

表 2-3. 2013 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 (*4)	「Oracle Outside In」におけるバッファオーバーフローの脆弱性	ファイル形式デコードライブラリ「Oracle Outside In」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。	2013 年 7 月 17 日	7.5
2 (*1)	「Apache Struts」において任意のコマンドを実行される脆弱性	ウェブアプリケーション開発支援フレームワーク「Apache Struts」には、HTTP リクエストの処理に不備がありました。 このため、第三者により 任意のコマンドを実行される可能性がありました。	2013 年 9 月 6 日	7.5
3 (*1)	「VMware ESX および ESXi」におけるバッファオーバーフローの脆弱性	仮想化ソフトウェア（ハイパーバイザー）「VMware ESX および ESXi」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、第三者によりサービス運用妨害 (DoS) 攻撃を受けたり、任意のコードを実行されたりする可能性がありました。	2013 年 9 月 6 日	7.5
4 (*2) (*4)	「SEIL」シリーズにおけるバッファオーバーフローに関する脆弱性	ルータ製品「SEIL」シリーズには、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を実行される可能性がありました。	2013 年 9 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				
5 (*4)	「AQUOS フォトプレーヤー HN-PP150」におけるサービス運用妨害 (DoS) の脆弱性	フォトプレーヤー「AQUOS フォトプレーヤー HN-PP150」には、通信におけるパケットの処理に不備がありました。このため、第三者によりネットワーク関係の機能を停止される可能性がありました。	2013 年 7 月 11 日	5.0
6	「サイボウズ Office」におけるセッション管理不備の脆弱性	グループウェア「サイボウズ Office」には、セッション管理不備の脆弱性がありました。このため、第三者がユーザになりすまして当該製品にアクセスする可能性がありました。	2013 年 7 月 16 日	4.0
7 (*4)	「Oracle Outside In」におけるサービス運用妨害 (DoS) の脆弱性	ファイル形式デコードライブラリ「Oracle Outside In」には、Hangul Word Processor ファイルの処理に不備がありました。このため、第三者により Oracle Outside In のプロセスをハングされる可能性がありました。	2013 年 7 月 17 日	5.0
8 (*1)	「JBoss RichFaces」において任意のコードが実行される脆弱性	ウェブアプリケーション開発支援フレームワーク「JBoss RichFaces」には、deserialize の処理に不備がありました。 このため、第三者によりサーバ上に任意のファイルが書き込まれたり、任意のコードを実行されたりするなどの可能性がありました。	2013 年 7 月 19 日	6.8
9	「Oracle Enterprise Manager」におけるクロスサイト・スクリプティングの脆弱性	Oracle データベース管理ソフト「Oracle Enterprise Manager」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。	2013 年 7 月 22 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
10 (*1)	「WordPress」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「WordPress」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。	2013 年 7 月 26 日	4.3
11	「JP1/IT Desktop Management - Manager」および「Hitachi IT Operations Director」における権限昇格の脆弱性	PC 管理ソフト「JP1/IT Desktop Management - Manager」および「Hitachi IT Operations Director」には、権限昇格の脆弱性がありました。こ のため、第三者により管理者権限を取得される可能性がありました。	2013 年 7 月 29 日	5.5
12 (*1)	「PHP OpenID Library」における XML 外部実体参照に関する脆弱性	OpenID 用ライブラリ「PHP OpenID Library」には、XML 外部実体参照に関す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情報が漏えいする、またはサーバのリソースが過度に消費されるなどの可能性がありました。	2013 年 8 月 21 日	6.4
13 (*1)	「EC-CUBE」における Windows 環境でのディレクトリ・トラバーサルの脆弱性	ショッピングサイト構築システム「EC-CUBE」は、Windows 環境で使用している場合に、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任意のファイルにアクセスされる可能性がありました。	2013 年 8 月 30 日	5.0
14 (*1)	「VMware ESX および ESXi」におけるディレクトリ・トラバーサルの脆弱性	仮想化ソフトウェア (ハイパーバイザー)「VMware ESX および ESXi」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、第三者によりホスト OS 上の任意のファイルを削除される可能性がありました。	2013 年 9 月 6 日	6.4
15	「ChamaCargo」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「ChamaCargo」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。	2013 年 9 月 13 日	4.3
16 (*3) (*4)	複数のブロードバンドルータがオープンリゾルバとして機能してしまう問題	複数のブロードバンドルータには、オープンリゾルバとして機能してしまう問題がありました。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。	2013 年 9 月 19 日	5.0
17 (*2)	「Internet Explorer」において任意のコードが実行される脆弱性	ウェブブラウザ「Internet Explorer」には、任意のコードが実行される脆弱性がありました。このため、細工されたウェブページを閲覧することで、任意のコードが実行される可能性がありました。	2013 年 9 月 19 日	6.8
18 (*4)	D-Link「DWL-2100AP」におけるサービス運用妨害 (DoS) の脆弱性	ルータ製品「DWL-2100AP」シリーズには、SSH の実装に不備がありました。このため、第三者により当該製品を再起動させられる可能性がありました。	2013 年 9 月 20 日	6.8
19 (*4)	D-Link「DES-3810」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「DES-3810」シリーズには、SSH の実装に不備がありました。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。	2013 年 9 月 20 日	6.8
20 (*2) (*4)	「SEIL」シリーズにおける RADIUS 認証に関する脆弱性	ルータ製品「SEIL」シリーズには、RADIUS 認証に関す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サービスに不正にアクセスされる可能性がありました。	2013 年 9 月 20 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
脆弱性の深刻度=レベル I（注意）、CVSS 基本値=0.0～3.9				
21	「ドコモ海外利用アプリ」における接続処理に関する脆弱性	アクセスポイント接続ソフト「ドコモ海外利用アプリ」には、Wi-Fi アクセスポイントへの接続処理に問題がありました。このため、第三者によりユーザの情報が取得される可能性がありました。	2013 年 8 月 7 日	3.3
22（*2）	「サイボウズ メールワイズ」における情報漏えいの脆弱性	メール管理ソフト「サイボウズ メールワイズ」には、件名に別のメールの内容が表示される問題がありました。このため、第三者により閲覧権限のないメールの内容を取得される可能性がありました。	2013 年 8 月 13 日	3.5
23	「ヤフオク!」における SSL サーバ証明書の検証不備の脆弱性	ネットオークションアプリ「ヤフオク!」には、SSL サーバ証明書の検証不備の脆弱性がありました。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。	2013 年 8 月 19 日	2.6
24（*2）	Android 版「Yahoo!ショッピング」における SSL サーバ証明書の検証不備の脆弱性	Android 版ネットショッピングアプリ「Yahoo!ショッピング」には、SSL サーバ証明書に検証不備の脆弱性がありました。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。	2013 年 8 月 19 日	2.6
25（*2）	「サイボウズ Office」におけるクロスサイト・スクリプティングの脆弱性	グループウェア「サイボウズ Office」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。	2013 年 9 月 9 日	2.6
26	「Opera」におけるクロスサイト・スクリプティングの脆弱性	ウェブブラウザ「Opera」には、ページのエンコード設定が UTF-8 になっている場合に、クロスサイト・スクリプティング の脆弱性がありました。このため、ウェブブラウザ上で任意のスクリプトが実行される可能性がありました。	2013 年 9 月 12 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 等と連携して公表した脆弱性

表 2-4、表 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 28 件あり、うち表 2-4 には通常の脆弱性情報 25 件、表 2-5 には対応に緊急を要する Technical Cyber Security Alert の 3 件を示しています。これらの情報は、通常関連する登録済み製品開発者へ通知したうえ、JVN に掲載しています。

表 2-4.米国 CERT/CC [*16] 等と連携した脆弱性関連情報および対応状況

項番	脆弱性	対応状況
1	HP System Management Homepage にスタックバッファオーバーフローの脆弱性	注意喚起として掲載
2	KnowledgeView 製品にクロスサイトスクリプティングの脆弱性	注意喚起として掲載
3	iDRAC にクロスサイトスクリプティングの脆弱性	注意喚起として掲載
4	Apple iTunes におけるメモリ破損の脆弱性に対するアップデート	注意喚起として掲載
5	Apple iOS 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
6	Apple Safari 5 におけるメモリ破損の脆弱性に対するアップデート	注意喚起として掲載
7	Dahua Technology 製 DVR に複数の脆弱性	注意喚起として掲載
8	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
9	Oracle E-Business Suite にパスワード漏えいの脆弱性	注意喚起として掲載
10	AdvancePro に情報漏えいの脆弱性	注意喚起として掲載
11	Cisco Prime NCS および Cisco WCS にクロスサイトスクリプティングの脆弱性	注意喚起として掲載
12	Supermicro 製の IPMI に複数の脆弱性	注意喚起として掲載
13	CourseMill LMS に複数の脆弱性	注意喚起として掲載
14	Corporater EPM Suite に複数の脆弱性	注意喚起として掲載
15	RealPlayer のファイル名の処理にスタックバッファオーバーフローの脆弱性	注意喚起として掲載
16	SearchBlox に複数の脆弱性	注意喚起として掲載
17	Web Viewer for Samsung DVR に複数の脆弱性	注意喚起として掲載
18	Dell の BIOS 更新処理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
19	HP/H3C 製および Huawei 製ネットワーク機器がパスワードの暗号化に DES を使用している問題	注意喚起として掲載
20	HTTPS レスポンスから暗号化されたデータの一部が推測可能な脆弱性 (BREACH)	注意喚起として掲載
21	Open Shortest Path First (OSPF) プロトコルの Link State Advertisement (LSA) に関する問題	複数製品開発者へ通知
22	TrustGo Antivirus & Mobile Security にサービス運用妨害 (DoS) の脆弱性	注意喚起として掲載
23	Verizon Wireless Network Extender に複数の脆弱性	複数製品開発者へ通知
24	EMBASSY Remote Administration Server に SQL インジェクションの脆弱性	注意喚起として掲載
25	Choice Wireless Green Packet 4G WiMax modem WIXFMR-111 に脆弱性	注意喚起として掲載

[*16] CERT/Coordination Center：1988 年のウイルス感染事件を契機に米国カーネギーメロン大学に設置された CSIRT。

表 2-5.米国 US-CERT [*17] 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	Microsoft 製品の複数の脆弱性に対するアップデート
2	Microsoft 製品の複数の脆弱性に対するアップデート
3	Microsoft 製品の複数の脆弱性に対するアップデート

2-1-5. 調整不能案件の処理状況

（1） 連絡不能開発者一覧（製品開発者名および製品情報）の公表状況

図 2-14 は今四半期の連絡不能開発者一覧(製品開発者名および製品情報)の公表件数と今四半期までの累計件数を示しています。「連絡不能開発者一覧」にある「製品開発者名」の公表件数の累計は 128 件で、このうち 18 件が調整を再開しています。また、今四半期は、新たに「製品開発者名」を 4 件公表し、合計 110 件を公表しています。

（2） 製品開発者情報の公開調査結果

図 2-15 は今四半期までに公表した連絡不能開発者の公開調査の結果を示しています。今四半期末時点の公開中の連絡不能開発者件数は、110 件です。また、「連絡不能開発者一覧」の公開開始（2011 年 9 月 29 日）から今四半期末時点までに 18 件が調整を再開し、2013 年 2Q 以前に製品開発者と調整を再開した 1 件の調整が今四半期に完了し、累計 8 件が本制度における取扱いを終了しました。「連絡不能開発者一覧」の公開開始から 2 年が経過しましたが、今四半期末時点で 110 件は依然として、製品開発者からの連絡が無い状況です。

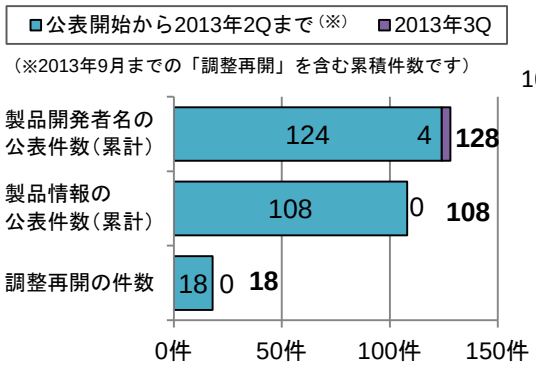


図2-14. 2013年3Qの公表および調整再開の状況

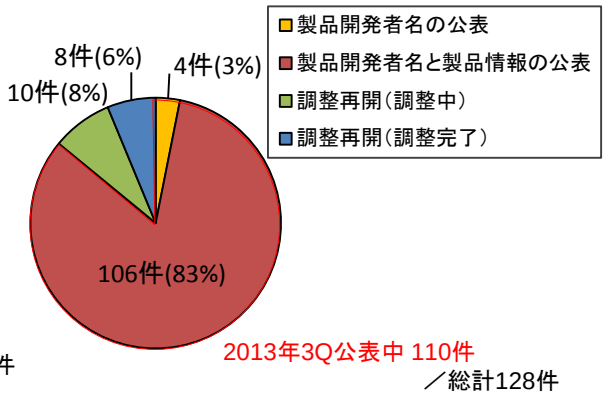


図2-15. 公開調査後の対応状況

[*17] 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

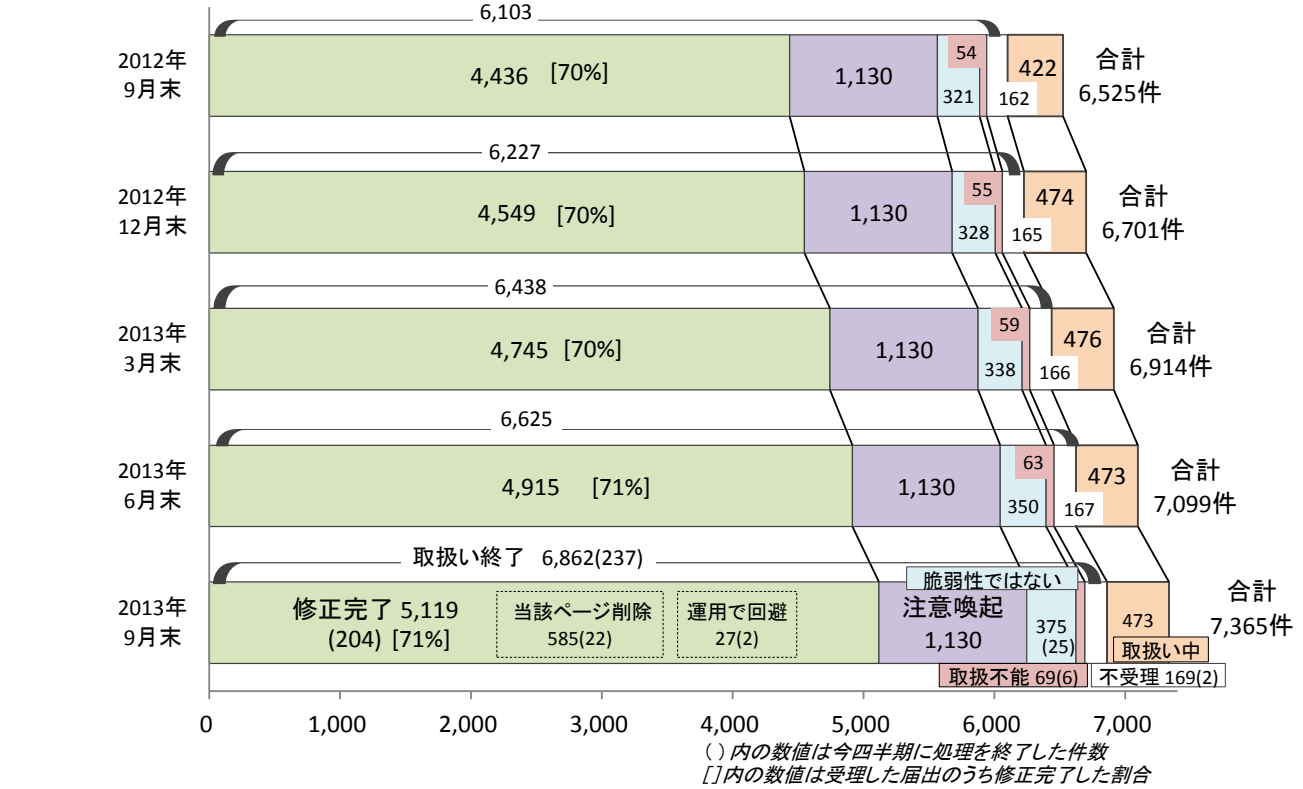
2-2-1. 処理状況

図 2-16 はウェブサイトの脆弱性関連情報の届出における、処理状況の推移を示したものです。ウェブサイトの脆弱性について、今四半期中に取扱いを終了したもの 237 件（累計 6,862 件）でした。このうち「修正完了」したものは 204 件（累計 5,119 件）、注意喚起を行い処理を取りやめたものは 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 25 件（累計 375 件）でした。処理の取りやめとは、例えば 1 つの脆弱性が多数のウェブサイトに存在するという届出があった場合「注意喚起」を行った上、処理を取りやめという本制度に則ったものです

。なお、メールでウェブサイト運営者と連絡が取れない場合は電話や郵送で連絡を試みるなどの対応をしていますが、それでもウェブサイト運営者と連絡が取れずに「取扱不能」となったものは 6 件（累計 69 件）でした。「不受理」としたものは 2 件（累計 169 件）でした。

取扱いを終了した累計 6,862 件のうち「注意喚起」「取扱不能」「不受理」を除く累計 5,494 件（80%）は、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ました。

「修正完了」したもののうち、ウェブサイト運営者が当該ページを削除することにより対応したものは 22 件（累計 585 件）、ウェブサイト運営者が運用により被害を回避しているものは 2 件（累計 27 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
  - 該当ページを削除 ： 修正完了のうち、当該ページを削除して対応したもの
  - 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 2-16. ウェブサイト 各四半期時点での脆弱性関連情報の届出の処理状況

以下に、届出受付開始から今四半期までに届出のあったウェブサイトの脆弱性関連情報 7,365 件のうち、不受理を除いた 7,196 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

図 2-17 のグラフは過去 2 年間に届出のあっ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示しています。今四半期も企業が運営するウェブサイトに関する届出が多数を占めています。

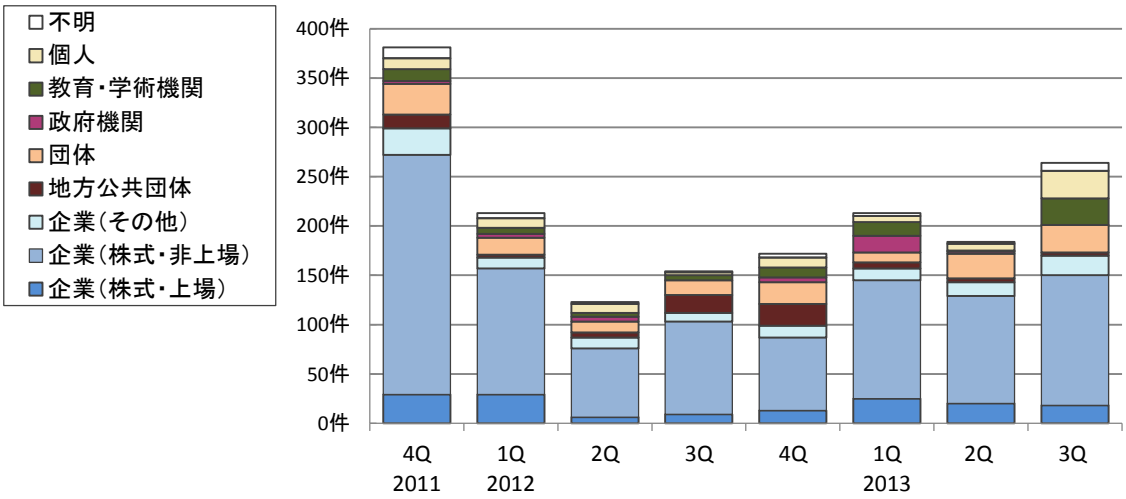
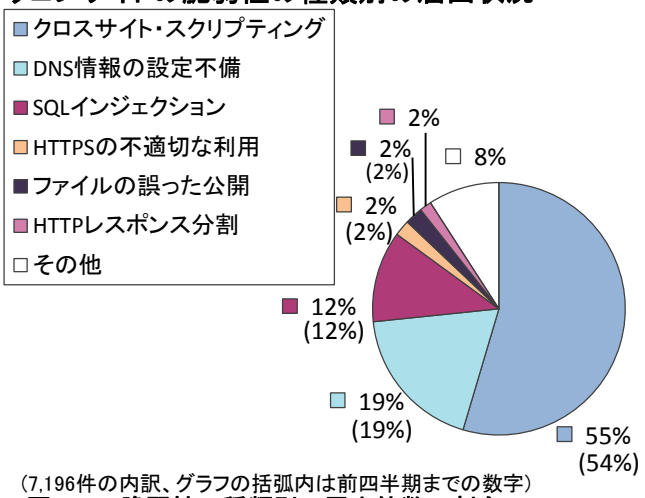


図2-17. ウェブサイトの運営主体の種類別の届出件数(四半期別推移)

2-2-3. 脆弱性の種類と脅威

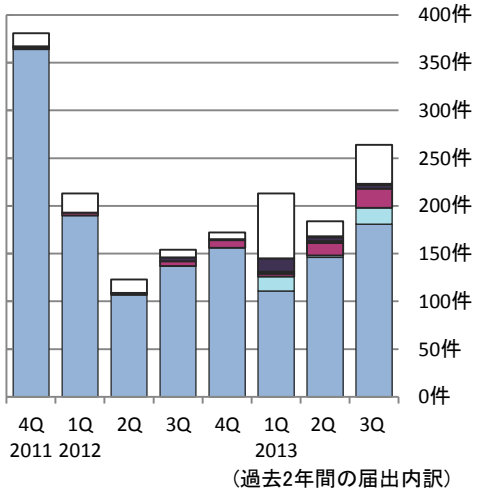
図 2-18 のグラフは脆弱性の種類別の届出件数の割合を、図 2-19 は過去 2 年間の脆弱性の種類別届出件数の四半期別推移をそれぞれ示したものです[*18]。脆弱性の種類は届出の多い「クロスサイト・スクリプティング」「DNS 情報の設定不備」「SQL インジェクション」の 3 種類の脆弱性が全体の 86%を占めています。2008 年第 3 四半期から 2009 年第 3 四半期にかけて多く届出のあった「DNS 情報の設定不備」の届出は、2009 年第 4 四半期以降はありませんでしたが、2013 年の第 1 四半期および第 3 四半期に届出が 34 件ありました。過去 2 年間は「クロスサイト・スクリプティング」が届出全体の約 7 割以上を占めています。

ウェブサイトの脆弱性の種類別の届出状況



(7,196件の内訳、グラフの括弧内は前四半期までの数字)

図2-18. 脆弱性の種類別の届出件数の割合

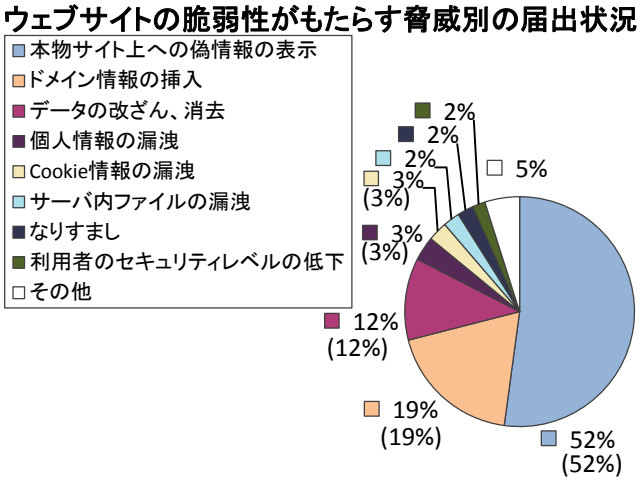


(過去2年間の届出内訳)

図2-19. 脆弱性の種類別の届出件数 (四半期別推移)

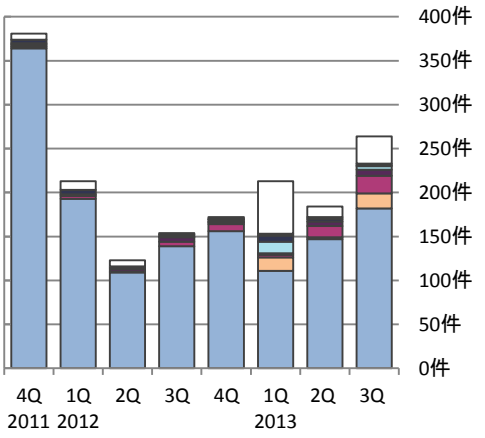
[*18] それぞれの脆弱性の詳しい説明については付表 2 を参照してください。

図 2-20 のグラフは脅威別の届出件数の割合を、図 2-21 は過去 2 年間の脅威別届出件数の四半期別推移をそれぞれ示したものです。「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、「本物サイト上への偽情報の表示」「ドメイン情報の挿入」「データの改ざん、消去」が全体の 83%を占めています。



(7,196件の内訳、グラフの括弧内は前四半期までの数字)

図2-20. 脆弱性がもたらす脅威別の届出件数の割合



(過去2年間の届出内訳)

図2-21. 脆弱性がもたらす脅威別の届出件数 (四半期別推移)

2-2-4. 修正完了状況

図 2-22 のグラフは、ウェブサイトの脆弱性について過去 3 年間の四半期別の修正完了件数を示しています。修正を完了した 204 件のうち 48 件（24%）は、運営者へ脆弱関連情報を通知してから修正完了までに 91 日以上を要した届出です。今四半期は、修正完了までに 91 日以上を要した届出の割合が、前四半期（170 件中 73 件（43%））より大幅に減少しています。表 2-6 は、過去 3 年間の四半期末の時点で、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関連情報を通知してから、90 日以内に修正が完了した件数の割合を示したものです。2010 年 3Q 以降に「90 日以内」に修正が完了した割合は約 65%で、その傾向に大きな変動はありません。

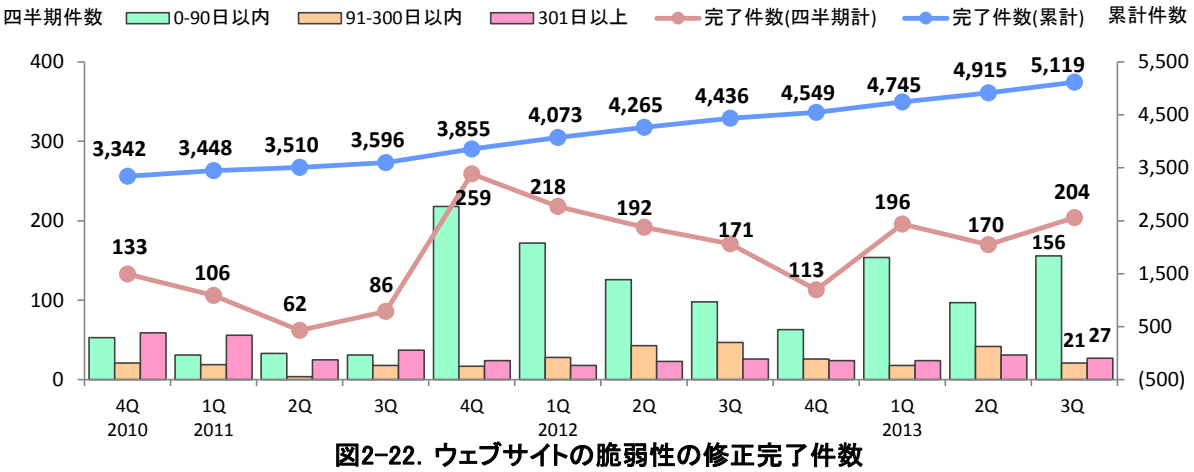


図2-22. ウェブサイトの脆弱性の修正完了件数

表 2-6. 90 日以内に修正完了した件数および割合の推移

	2010 4Q	2011 1Q	2Q	3Q	4Q	2012 1Q	2Q	3Q	4Q	2013 1Q	2Q	3Q
修正完了件数	3,342	3,448	3,510	3,596	3,855	4,073	4,265	4,436	4,549	4,745	4,915	5,119
90 日以内の件数	2,221	2,252	2,285	2,316	2,534	2,706	2,832	2,930	2,993	3,147	3,244	3,400
90 日以内の割合	66%	65%	65%	64%	66%	66%	66%	66%	66%	66%	66%	66%

図 2-23 および図 2-24 は、ウェブサイト運営者に脆弱性関連情報を通知してから修正されるまでに要した日数およびその傾向を脆弱性の種類別に示したものです[*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。

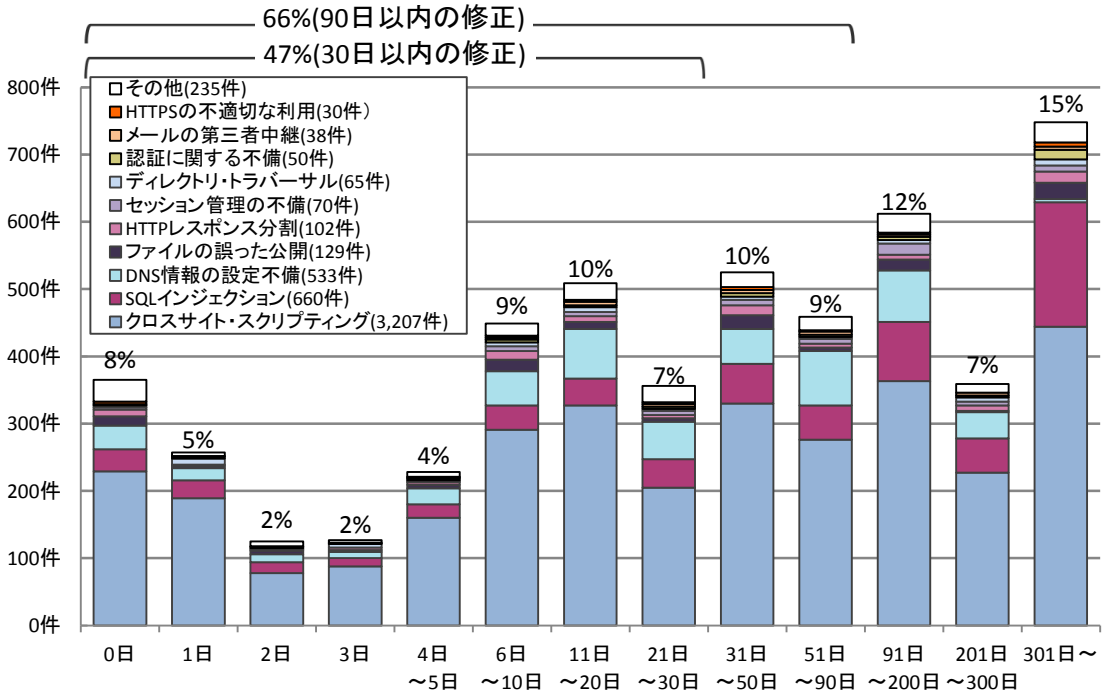


図2-23.ウェブサイトの修正に要した日数

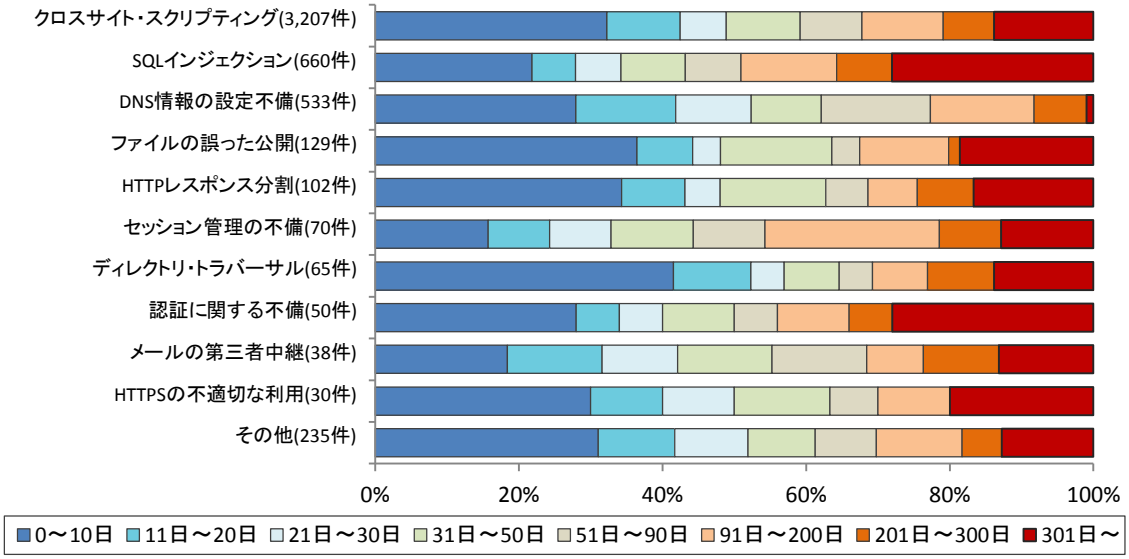


図2-24.ウェブサイトの修正に要した脆弱性種類別の日数の傾向

[*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通知が無い場合、IPA は運営者に脆弱性が悪用されて攻撃された場合の危険性を分かりやすく解説し、1～2 ヶ月毎に電子メールや電話、郵送などの手段で運営者に連絡を試み、脆弱性対策の実施を促しています。

図 2-25 は、ウェブサイトの脆弱性関連情報のうち、取扱いが長期化（IPA からウェブサイト運営者へ脆弱性関連情報を通知してから、90 日以上脆弱性を修正した旨の報告が無い）しているものについて、経過日数別の件数を示したものです。経過日数が 90 日から 199 日に達したものは 41 件、200 日から 299 日のものは 53 件など、これらの合計は 302 件（前四半期は 307 件）です。また、1000 日以上経過している届出脆弱性には、SQL インジェクションなどの比較的危険度の高い脆弱性が含まれており、速やかな対策が望まれます。

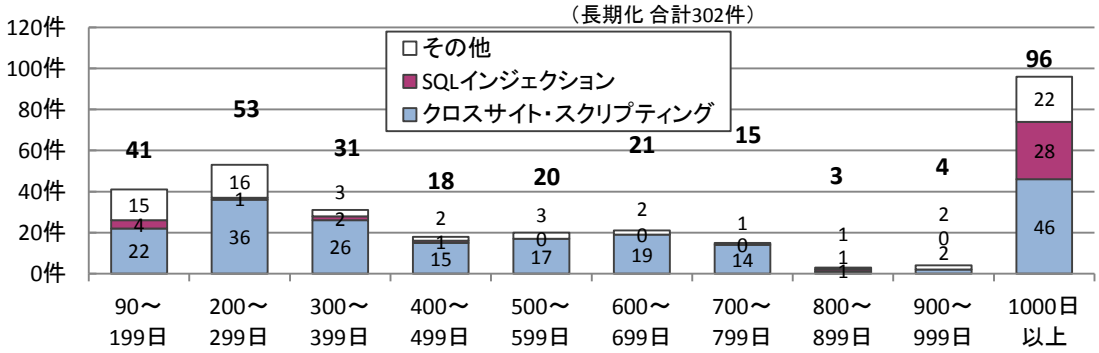


図2-25.取扱いが長期化(90日以上経過)しているウェブサイトの経過日数と脆弱性の種類

表 2-7 は、過去 2 年間の四半期末時点で取扱い中の届出について、取扱いが長期化している届出件数および、長期化している割合の四半期別推移を示しています。

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別推移

	2011 4Q	2012 1Q	2Q	3Q	4Q	2013 1Q	2Q	3Q
取扱い中件数	541 件	527 件	449 件	423 件	473 件	474 件	473 件	503 件
長期化している件数	237 件	298 件	318 件	302 件	296 件	301 件	307 件	302 件
長期化している割合	44%	57%	71%	71%	63%	60%	65%	60%

ウェブサイトの情報が盗まれてしまう可能性のある SQL インジェクションのように、取扱いが長期化しているものの中には深刻度の高い脆弱性もあります。ウェブサイト運営者は脆弱性を攻撃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。

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）」： http://www.ipa.go.jp/security/vuln/vuln_contents/

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

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

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

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。

⇒「TCP/IP に係る既知の脆弱性検証ツール」:
http://www.ipa.go.jp/security/vuln/vuln_TCPIP_Check.html

⇒「TCP/IP に係る既知の脆弱性に関する調査報告書」:
http://www.ipa.go.jp/security/vuln/vuln_TCPIP.html

⇒「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）」:
http://www.ipa.go.jp/security/fy22/reports/emb_app2010/

⇒「ファジング活用の手引き」、「ファジング実践資料」:
http://www.ipa.go.jp/security/vuln/fuzzing.html

3-3. 一般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

るまでの期間は第三者に漏れぬよう、適切に管理されることを求めます。

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

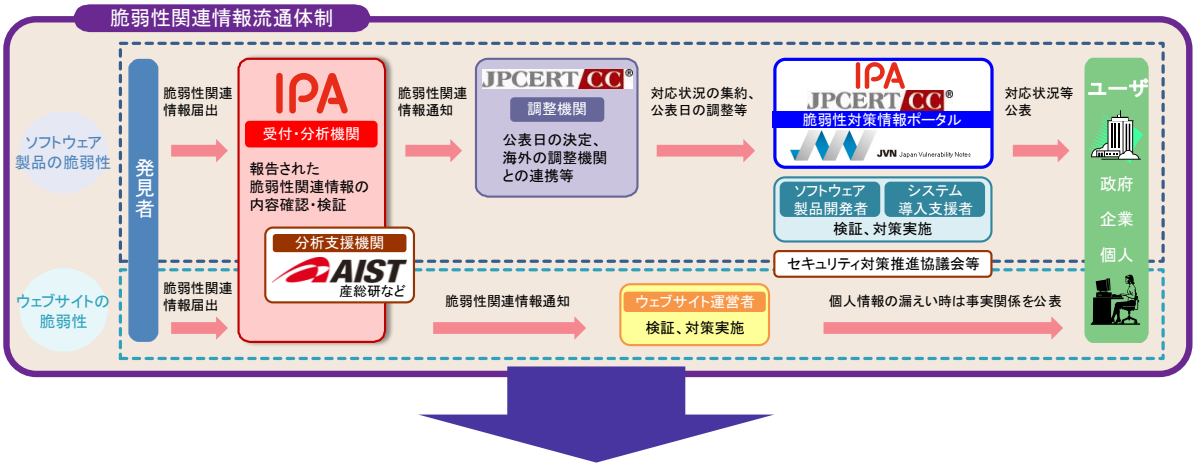
付表 2. ウェブサイトの脆弱性の分類

	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」（脆弱性関連情報取扱いの枠組み）



【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個人情報等需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:独立行政法人 産業技術総合研究所