IPA Information-technology Promotion Agency, Japan

JPCERT CC®

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

[2014 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、2014 年 1 月 1 日から 2014 年 3 月 31 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
2014 年 4 月 24 日

目次

1. 2014 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 9,517 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 2014 年第 1 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 44 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 145 件、合計 189 件でした。届出受付開始からの累計件数は 9,517 件で、内訳はソフトウェア製品に関するもの 1,788 件、ウェブサイトに関するもの 7,729 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	累計件数
ソフトウェア製品	**44** 件	**1,788** 件
ウェブサイト	**145** 件	**7,729** 件
合計	**189** 件	**9,517** 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減少しています。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。今四半期の 1 就業日あたりの届出件数は 4.01 [(*2)] 件でした。

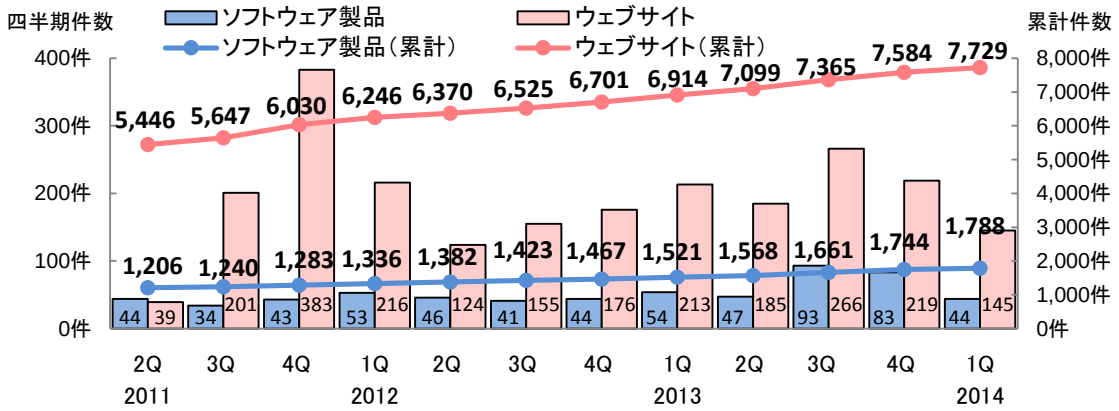


図1−1.脆弱性関連情報の届出件数の四半期別推移

表 1−2. 届出件数（過去 3 年間）

	2011 2Q	3Q	4Q	2012 1Q	2Q	3Q	4Q	2013 1Q	2Q	3Q	4Q	2014 1Q
累計届出件数[件]	6,652	6,887	7,313	7,582	7,752	7,948	8,168	8,435	8,667	9,026	9,328	9,517
1就業日あたり[件/日]	3.93	3.93	4.03	4.05	4.00	3.98	3.78	3.96	3.96	4.00	4.03	4.01

(*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 6,297 件となりました～

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	**32** 件	**851** 件
ウェブサイト	**138** 件	**5,446** 件
合計	**170** 件	**6,297** 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 JVN で対策情報を公表した四半期別の修正完了件数は、2011 年以降 30 件前後で推移しており今四半期は 32 件 (*3)（累計 851 件）でした。そのうち、7 件が製品開発者自身から届けられた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公表までに 46 日 (*4) 以上かかったものは 21 件（66%）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 138 件（累計 5,446 件）でした。修正を完了した 138 件のうち、ウェブアプリケーションを修正したもの 124 件（90%）、当該ページを削除したもの 13 件（9%）、運用で回避したもの 1 件（1%）でした。なお、修正を完了した 138 件のうち 60 件（43%）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（189 件中 32 件（17%））より増加しています。

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。その製品開発者への連絡の糸口を得るために、「連絡不能開発者一覧 (*6)」を公開しています。「連絡不能開発者一覧」では、「製品開発者名」をまず公表します。その後 3 ヵ月たっても製品開発者から応答が得られない場合、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、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

今四半期に新たに公表した「製品開発者名」は 8 件、「製品情報」は 16 件でした。

（2）　連絡不能開発者一覧の公表後の取扱い状況

今四半期に、製品開発者から応答があり調整を再開したのは 3 件（累計 21 件）、本制度における取扱いを終了したのは 0 件（累計 8 件）でした。依然として、131 件については、製品開発者と連絡がとれない状況です。

(*3)　表 2-3 参照
(*4)　公表日の目安は、脆弱性関連情報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、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. 脆弱性届出の傾向について

製品開発者自身によるソフトウェア製品の届出が増加傾向

～ 脆弱性対策情報を広く周知するため、本制度を活用して届出をする製品開発者が増加 ～

2013 年の 1 年間で、脆弱性として受理 (*7) したソフトウェア製品の届出は 245 件ありました。そのうち、31 件は製品開発者自身による届出で、ソフトウェア製品における届出の約 13%を占めています。2014 年第 1 四半期は、受理した届出 (*8) 42 件のうち、約 19%の 8 件が製品開発者からの届出で、ここ数年、一部の製品開発者が自身で届出を行うようになっていることが伺えます。

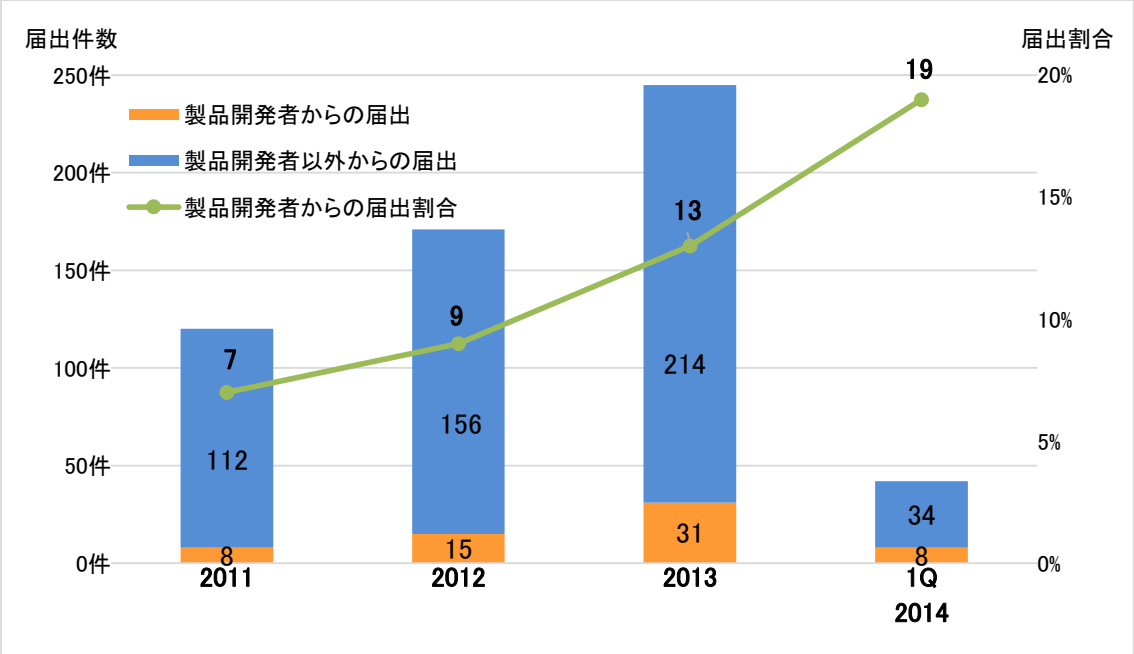


図 1-2. ソフトウェア製品の届出における製品開発者からの届出件数

製品開発者が自ら届出を行ったソフトウェア製品の脆弱性のうち、2014 年第 1 四半期に公表されたものはグループウェアやショッピングサイト構築システム、表計算ソフトの脆弱性、7 件で、表 1-4 の通りです。表計算ソフトの脆弱性 (*9) は、ゼロデイ攻撃に悪用される可能性が高いものでした。

表 1-4. 2014 年第 1 四半期に公表した製品開発者による脆弱性の届出

JVN公表日	JVN番号	脆弱性	CVSS 基本値
2014/2/26	JVN#71045461	サイボウズ ガルーンにおける SQL インジェクションの脆弱性	6.5
2014/2/26	JVN#26393529	サイボウズ ガルーンにおけるディレクトリトラバーサルの脆弱性	3.5
2014/2/26	JVN#24035499	サイボウズ ガルーンにおけるセッション管理不備の脆弱性	4.9
2014/1/28	JVN#28011378	三四郎シリーズにおいて任意のコードが実行される脆弱性	9.3
2014/1/28	JVN#91153528	サイボウズ ガルーン における複数の SQL インジェクションの脆弱性	6.5
2014/1/22	JVN#51770585	EC-CUBE における情報漏えいの脆弱性	5.0
2014/1/22	JVN#17849447	EC-CUBE における情報改ざんの脆弱性	5.0

これまで本制度を通じて届出された脆弱性情報のほとんどは、セキュリティの研究者等、特定の発見者によるものでした。発見者による自発的な届出は、IPA および JPCERT/CC を経由して製品開発者に通知され、製品開発者の速やかな対策実施後、JVN で対策情報が公表される、とい

(*7) 脆弱性届出件数から、IPA が脆弱性として認めて受理した件数を示す。届出の一部には、脆弱性ではないと判断し不受理とした届出が含まれている。

(*8) 受理した届出件数とは届出された件数（44 件）から不受理となった件数（2 件）を除いたもの。

(*9) 「三四郎」シリーズにおいて任意のコードが実行される脆弱性の対策について(JVN#28011378)
http://www.ipa.go.jp/security/ciadr/vul/20140128-jvn.html

う一連の運用が行われています。

脆弱性情報の取扱いにおいて、製品開発者自身で脆弱性を発見した場合、または製品開発者以外の第三者から本制度を経由せず直接、製品開発者に脆弱性が通知された場合は、製品開発者の判断により、製品開発者自身のウェブサイト等で対策情報が公表されることが一般的です。

前述のとおり、本制度では製品開発者によりソフトウェア製品の脆弱性対策が円滑に行われ、JVN
で対策情報が広く一般に周知されることで、ソフトウェア製品利用者の対策が促進される、という利点があります。

数年来、製品開発者による本制度への届出が増加しているその背景には、脆弱性対策情報を広く一般に周知、対策を推進するには、本制度の活用が有効であることが製品開発者に浸透してきていることが考えられます。

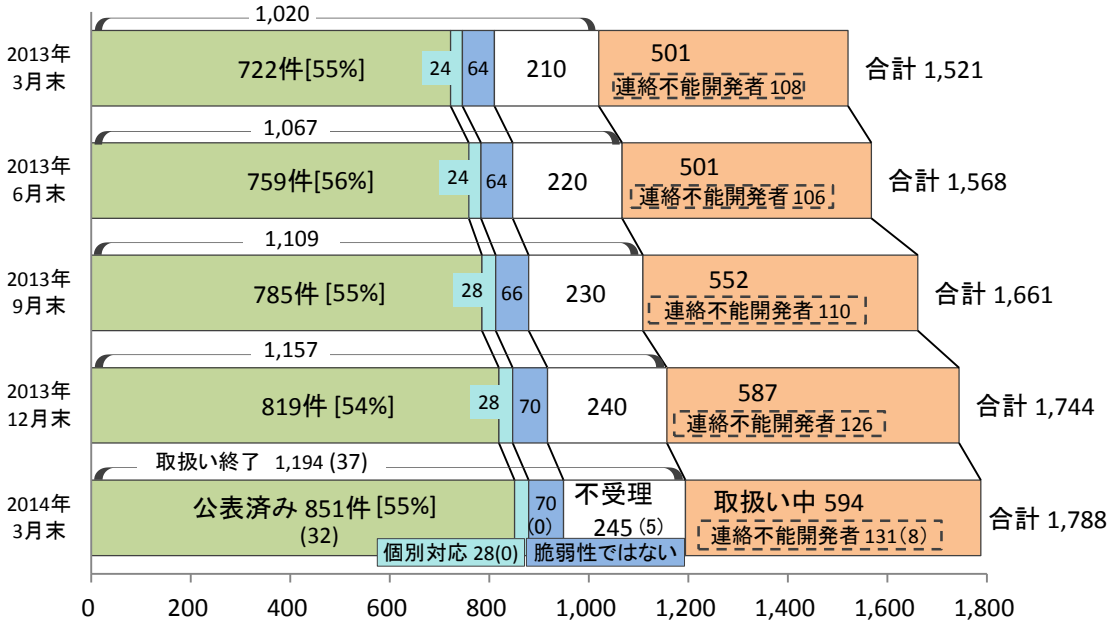
今後、さらに多くの製品開発者が脆弱性対策情報を広く一般に周知するため、本制度を活用すること、および組織のセキュリティ担当者が JVN を通じて脆弱性対策情報を積極的に収集することを期待します。

2. ソフトウェア等の脆弱性に関する届出状況（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、四半期別の処理状況の推移を示したものです。2014 年第 1 四半期末時点の届出件数は 1,788 件で、今四半期に公表した（修正完了した）脆弱性は 32 件（累計 851 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 28 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 70 件）、「不受理」としたものは 5 件 (*10)（累計 245 件）、取扱い中は 594 件でした。うち、連絡不能開発者一覧に公表した連絡不能開発者 (*11) は 8 件 (*12) で、2014 年 3 月末時点の連絡不能開発者公表数は 131 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

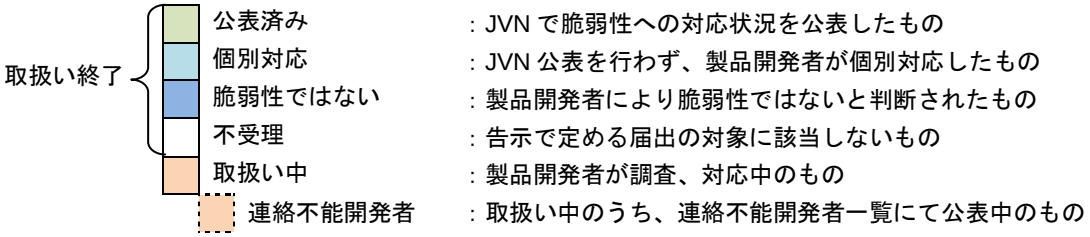


図 2-1. ソフトウェア製品脆弱性関連情報の届出処理状況（四半期別推移）

(*10) 今四半期の届出の中で不受理とした 2 件、前四半期までの届出の中で今四半期に不受理とした 3 件です。
(*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。
(*12) 今四半期に新たに 8 件公表し、製品開発者と調整を再開したため連絡不能開発者一覧から 3 件削除した。

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1,788 件のうち、不受理を除いた 1,543 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、図 2-3 のグラフは、届出された脆弱性の製品種類を示しています。図 2-2 は届出開始から今四半期末までの届出累計の割合を、図 2-3 は過去 2 年間の届出件数の推移を四半期別に示したものです。

累計では、「ウェブアプリケーションソフト」が最も多く 37%となっています。今四半期の届出件数は、「ウェブアプリケーションソフト」の届出が最も多くなっています。なお、今四半期は、既存の製品種類の分類に当てはまらない独自のサービスや機能を提供するスマートフォン向けアプリが多く届出されたため「その他」が多くなりました。

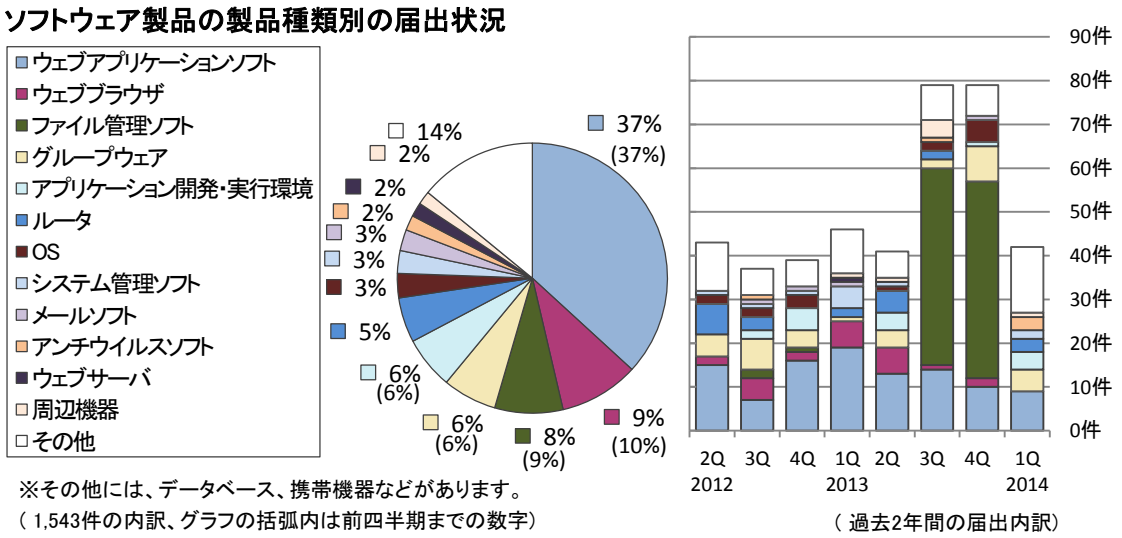


図2-2. 製品種類別の届出件数の割合

図2-3. 製品種類別の届出件数(四半期別推移)

図 2-4、2-5 のグラフは、届出された脆弱性の製品ライセンスを「オープンソースソフトウェア」と「それ以外」で示しています。図 2-4 は届出開始から今四半期末までの届出累計の割合を、図 2-5 は過去 2 年間の届出件数の推移を四半期別に示したものです。

累計では、オープンソースソフトウェアの届出が 31%を占めています。

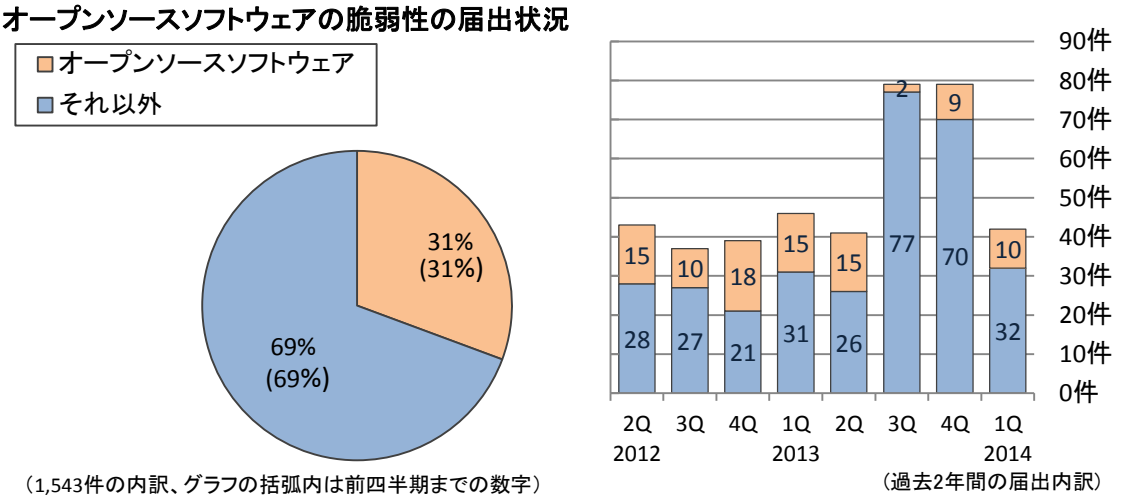


図2-4. オープンソースソフトウェアの届出件数の割合

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、図 2-7 のグラフは、届出された脆弱性の製品をスマートフォン向けアプリ（以降「スマホアプリ」）と「それ以外」で分類しています。図 2-6 は過去 2 年間の四半期別の届出件数の推移を、図 2-7 は届出開始から今四半期末までの届出が公表までに要した日数を示したものです。受理から 45 日以内に対策情報を公表した割合は「スマホアプリ」が 40%、「それ以外」が 33%となっており、「スマホアプリ」の方が早く対策される傾向にあります。

「スマホアプリ」に関する届出は、2013 年第 3 四半期と 2013 年第 4 四半期に急増しましたが、今四半期は 8 件に減少しました。

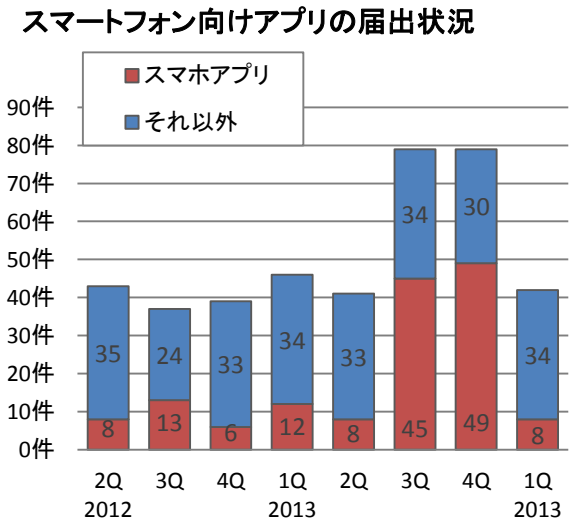


図2-6.スマートフォン向けアプリの届出件数（四半期別推移）

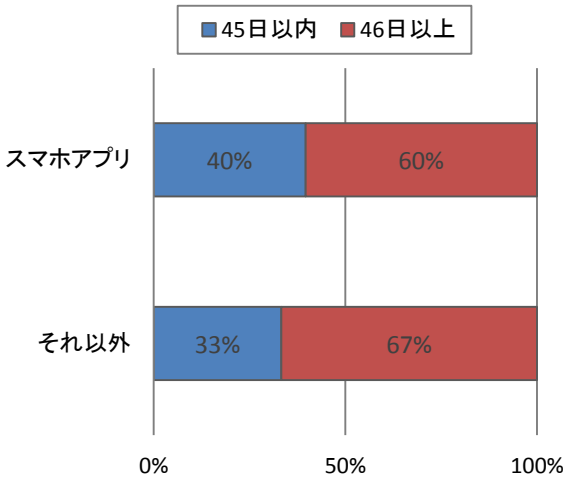
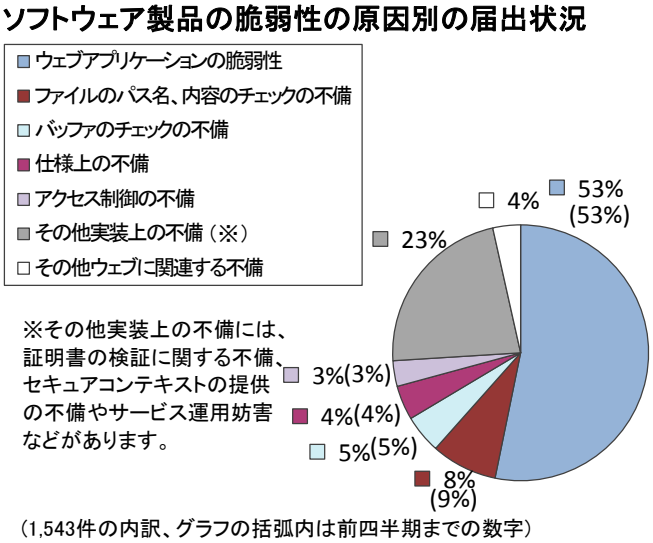


図2-7.スマートフォン向けアプリとそれ以外の公表までの日数

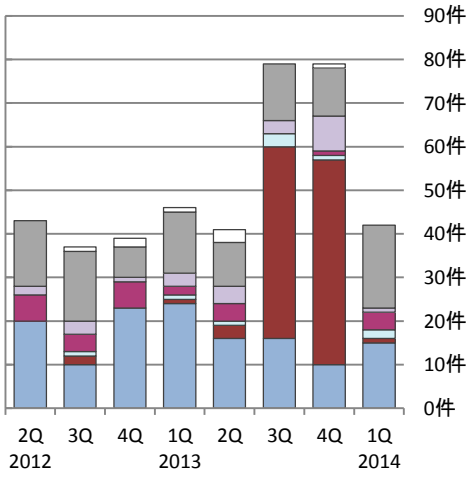
2-1-3. 脆弱性の原因と脅威別件数

図 2-8、図 2-9 のグラフは、届出された脆弱性の原因を示しています。図 2-8 は届出開始から今四半期末までの届出累計の割合を、図 2-9 は過去 2 年間の届出件数の推移を四半期別に示したものです。累計では、「ウェブアプリケーションの脆弱性」が過半数を占めており、今四半期の届出件数も「ウェブアプリケーションの脆弱性」が最も多くなりました。2013 第 3 四半期から 2013 第 4 四半期にかけて多く届出された「ファイルのパス名、内容のチェックの不備」は、大幅に減少しました。



（1,543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

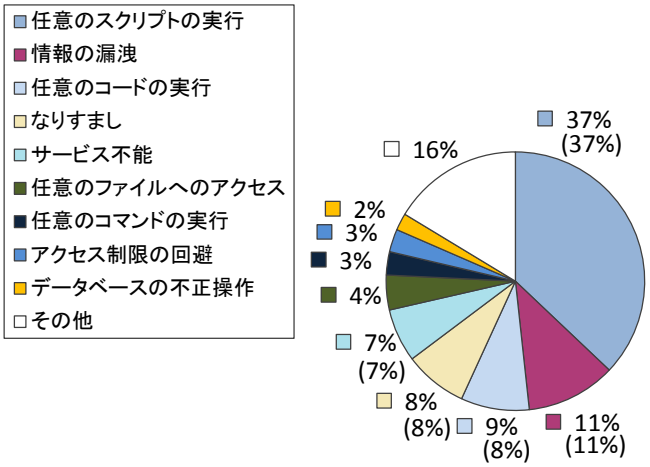


（過去2年間の届出内訳）

図2-9. 脆弱性の原因別の届出件数(四半期別推移)

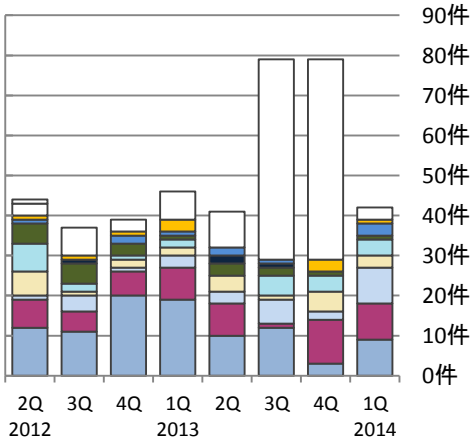
図 2-10、図 2-11 のグラフは、届出された脆弱性がもたらす脅威を示しています。図 2-10 は届出開始から今四半期末までの届出の割合を、図 2-11 は過去 2 年間の届出件数の推移を四半期別に示したものです。累計では、「任意のスクリプトの実行」が最も多く、全体の 37%となっています。今四半期は、「任意のスクリプト実行」「情報の漏洩」「任意のコード実行」が多く届出されました。「ファイルのパス名、内容のチェックの不備」がもたらす脅威が「その他」に分類されるため、「ファイルのパス名、内容のチェックの不備」の減少に伴い「その他」も減少しました。

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



（1,543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. 調整および公表件数

表 2-1 は情報の提供元別に、今期と累計の件数を示しています。JPCERT/CC は、情報の提供元別の 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[*13]。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、脆弱性情報の公表件数を国内および海外 CSIRT 等との連携によるものとに分け、過去 3 年分を四半期別に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	32 件	851 件
②	海外 CSIRT 等と連携して公表したもの	53 件	1,060 件
	合計	85 件	1,911 件

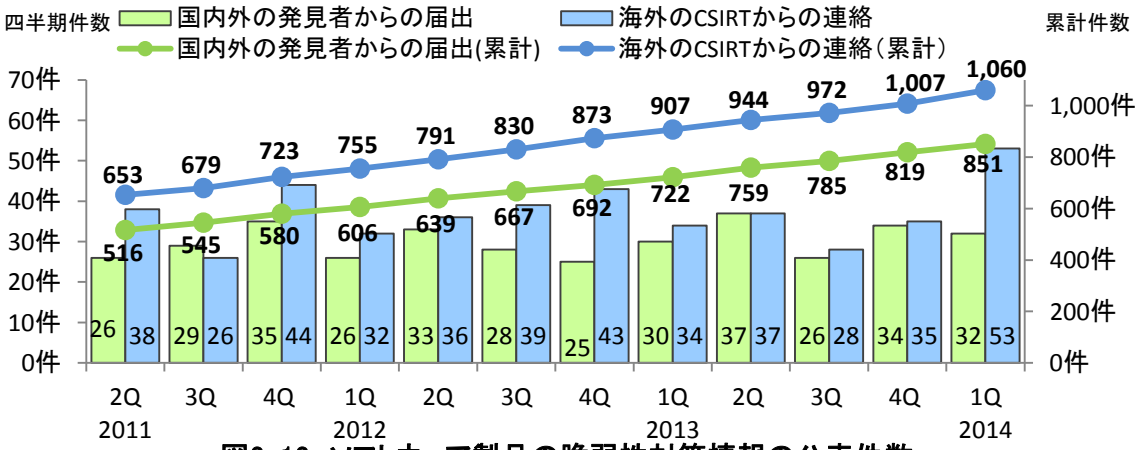


図2−12. ソフトウェア製品の脆弱性対策情報の公表件数

（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対策情報を公表した脆弱性（851 件）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 34%、45 日を超過した件数は 66%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。

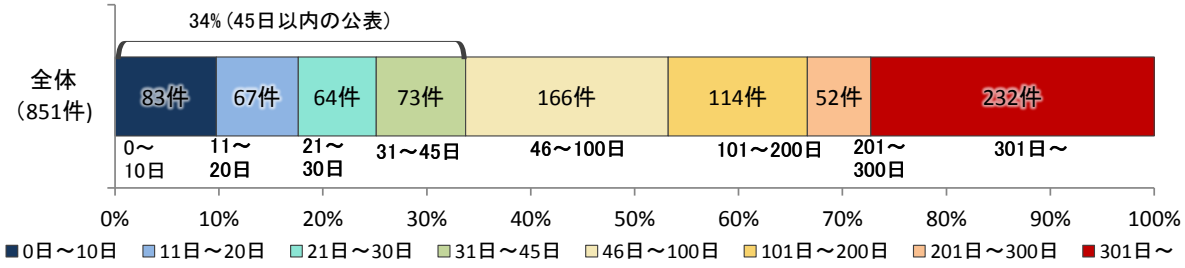


図2−13. ソフトウェア製品の脆弱性公表日数

表 2-2. 45 日以内に公表した件数の割合推移（四半期別）

2011 2Q	3Q	4Q	2012 1Q	2Q	3Q	4Q	2013 1Q	2Q	3Q	4Q	2014 1Q
36%	34%	33%	34%	34%	35%	34%	33%	33%	33%	34%	34%

[*13] JPCERT/CC 活動概要 Page15〜21（http://www.jpcert.or.jp/pr/2014/PR20140415.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のうち、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ものが 8 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 7 件（表 2-3 の*2）ありました。

表 2-3. 2014 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 (*2)	「三四郎」シリーズにおいて任意のコードが実行される脆弱性	日本語表計算ソフト「三四郎」シリーズには、文書ファイルを読みこむ際の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を実行される可能性がありました。	2014 年 1 月 28 日	9.3
2	「Norman Security Suite」における権限昇格の脆弱性	アンチウイルスソフト「Norman Security Suite」には、権限昇格の脆弱性がありました。このため、第三者により権限を昇格され、任意のコードを実行される可能性がありました。	2014 年 2 月 26 日	7.2
脆弱性の深刻度=レベル II（警告）、CVSS 基本値=4.0～6.9				
3	aokitaka 製「解凍ツール」におけるディレクトリ・トラバーサルの脆弱性	Android 用ファイル展開ソフト aokitaka 製「解凍ツール」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。	2014 年 1 月 10 日	4.3
4	「tetra filer」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「tetra filer」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。	2014 年 1 月 10 日	4.3
5	「セキュリティーファイルマネージャー」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「セキュリティーファイルマネージャー」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。	2014 年 1 月 10 日	4.3
6	「NeoFiler」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「NeoFiler」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。	2014 年 1 月 10 日	4.3
7	「Sleipnir Mobile for Android」における位置情報漏えいの脆弱性	Android 用ウェブブラウザ「Sleipnir for Android」には、Geolocation API の取扱いに問題がありました。このため、ユーザの確認なしに、ユーザの位置情報が閲覧中のウェブサイトに送信される可能性がありました。	2014 年 1 月 22 日	4.3
8 (*1) (*2)	「EC-CUBE」における情報改ざんの脆弱性	ショッピングサイト構築ソフト「EC-CUBE」には、情報改ざんの脆弱性がありました。このため、ショッピングサイト利用者によって、他の利用者の登録情報を改ざんされる可能性がありました。	2014 年 1 月 22 日	5.0
9 (*1) (*2)	「EC-CUBE」における情報漏えいの脆弱性	ショッピングサイト構築ソフト「EC-CUBE」には、情報漏えいの脆弱性がありました。このため、ショッピングサイト利用者によって、他の利用者の登録情報を取得される可能性がありました。	2014 年 1 月 22 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
10	「SimZip (Simple Zip Viewer)」におけるディレクトリ・トラバーサルの脆弱性	Android 用ファイル圧縮展開ソフト「SimZip (Simple Zip Viewer)」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。	2014 年 1 月 22 日	4.3
11 (*1)	「OpenPNE」において任意の PHP コードが実行される脆弱性	コンテンツ管理ソフト「OpenPNE」には、Cookie ヘッダの処理に問題がありました。このため、第三者により任意の PHP コードが実行される可能性がありました。	2014 年 1 月 24 日	6.8
12 (*2)	「サイボウズ ガルーン」における SQL インジェクションの脆弱性	グループウェア「サイボウズ ガルーン」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。項番 23 とは異なる問題です。	2014 年 1 月 28 日	6.5
13	「Joyful Note」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「Joyful Note」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。	2014 年 1 月 31 日	5.0
14	「Opera browser for Android」における Intent スキーム URL 処理に関する脆弱性	Android 用ウェブブラウザ「Opera browser for Android」には、Intent スキーム URL 処理に問題がありました。このため、第三者により「Opera browser for Android」の Cookie ファイルが窃取される可能性がありました。	2014 年 2 月 6 日	4.3
15 (*1)	「phpMyFAQ」におけるクロスサイト・スクリプティングの脆弱性	FAQ サイト構築ソフト「phpMyFAQ」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。	2014 年 2 月 7 日	4.3
16 (*1)	「Apache Commons FileUpload」におけるサービス運用妨害 (DoS) の脆弱性	Java 用ライブラリ「Apache Commons FileUpload」には、マルチパートリクエストの処理に問題がありました。このため、第三者により「Apache Commons FileUpload」を使用したシステムを応答不能な状態にされる可能性がありました。	2014 年 2 月 10 日	5.0
17	「AutoCAD」において任意の VBScript が実行可能な脆弱性	CAD 用ソフト「AutoCAD」には、FAS ファイルを読み込む際の検索パスに問題がありました。このため、第三者により任意の VBScript コードを実行される可能性がありました。	2014 年 2 月 21 日	6.8
18	「AutoCAD」における DLL 読み込みに関する脆弱性	CAD 用ソフト「AutoCAD」には、DLL を読み込む際の検索パス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を実行される可能性がありました。	2014 年 2 月 21 日	6.8
19	「Blackboard Vista/CE」におけるクロスサイト・スクリプティングの脆弱性	学習管理システム「Blackboard Vista/CE」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。	2014 年 2 月 21 日	4.3
20 (*1)	「XooNIps」におけるクロスサイト・スクリプティングの脆弱性	XOOPS モジュール「XooNIps」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。	2014 年 2 月 26 日	4.3
21	Android 版アプリ「デニーズ」における SSL サーバ証明書の検証不備の脆弱性	Android 用ソフト「デニーズ」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解読などが行われる可能性がありました。	2014 年 2 月 26 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
22 (*2)	「サイボウズ ガルーン」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 ガルーン」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、任意のユーザになりすまされる可能性がありました。	2014 年 2 月 26 日	4.0
23 (*2)	「サイボウズ ガルーン」における SQL インジェクションの脆弱性	グループウェア「サイボウズ ガルーン」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。項番 12 とは異なる問題です。	2014 年 2 月 26 日	6.0
24	R-Company 製「Unzipper」におけるディレクトリ・トラバーサルの脆弱性	Android 用ファイル展開ソフト「Unzipper」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。	2014 年 3 月 17 日	4.3
25	Android 版アプリ「出前館」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「出前館」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解読などが行われる可能性がありました。	2014 年 3 月 17 日	4.0
26	「sp モードメール」において Java メソッドが実行される脆弱性	Android 用メールソフト「sp モードメール」には、Java 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。	2014 年 3 月 18 日	6.8
27 (*1)	「Silex」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「Silex」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。	2014 年 3 月 20 日	4.3
28	「ES File Explorer」におけるディレクトリ・トラバーサルの脆弱性	Android 用ファイル展開ソフト「ES File 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。	2014 年 3 月 20 日	4.3
脆弱性の深刻度=レベル I（注意）、CVSS 基本値=0.0～3.9				
29 (*1)	「phpMyFAQ」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	FAQ サイト構築ソフトウエア「phpMyFAQ」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。	2014 年 2 月 7 日	2.6
30 (*2)	「サイボウズ ガルーン」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「サイボウズ ガルーン」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取得される可能性がありました。	2014 年 2 月 26 日	3.5
31	「sp モードメール」における受信メールの添付ファイルへのアクセスに関する問題	Android 用メールソフト「sp モードメール」には、受信したメールの添付ファイルへのアクセス制限に関する問題がありました。このため、第三者により当該製品で受信したメールの添付ファイルを取得される可能性がありました。	2014 年 3 月 18 日	2.6
32	「sp モードメール」で作成中のメールへのアクセスに関する問題	Android 用メールソフト「sp モードメール」には、作成中のメールへのアクセス制限に関する問題がありました。このため、第三者により作成中のメールの内容を取得される可能性がありました。	2014 年 3 月 18 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

（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 53 件あり、うち表 2-4 には通常の脆弱性情報 52 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。これらの情報は、通常関係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 (*14) 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	BlogEngine.NET に情報漏えいの脆弱性	注意喚起として掲載
2	RealPlayer に複数の脆弱性	注意喚起として掲載
3	Synology DiskStation Manager にアクセス制御不備の脆弱性	注意喚起として掲載
4	QNAP QTS にディレクトリトラバーサルの脆弱性	注意喚起として掲載
5	VASCO IDENTIKEY Authentication Server に認証不備の脆弱性	注意喚起として掲載
6	libpng に NULL ポインタ参照の脆弱性	注意喚起として掲載
7	NTP が DDoS 攻撃の踏み台として使用される問題	複数製品開発者へ通知
8	Atmail Webmail Server に複数の脆弱性	注意喚起として掲載
9	ASUS 製無線 LAN ルータに静的な DNS レコードが登録されている問題	注意喚起として掲載
10	Dell の複数製品にサービス運用妨害(DoS)の脆弱性	注意喚起として掲載
11	MW6 Technologies の ActiveX コントロールに複数の脆弱性	注意喚起として掲載
12	Emerson Avocent MergePoint Unity 2016 にディレクトリ・トラバーサルの脆弱性	注意喚起として掲載
13	Avanset Visual CertExam Manager に SQL インジェクションの脆弱性	注意喚起として掲載
14	Thecus N8800 に複数の脆弱性	注意喚起として掲載
15	CS-Cart 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
16	Apple iTunes 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
17	Apple Pages における脆弱性に対するアップデート	注意喚起として掲載
18	Mozilla Thunderbird にメッセージ内の HTML 要素を適切にブロックしない脆弱性	注意喚起として掲載
19	Fail2ban にサービス運用妨害(DoS)の脆弱性	注意喚起として掲載
20	Lexmark 製レーザープリンタに複数の脆弱性	注意喚起として掲載
21	Inmarsat 衛星通信端末に複数の脆弱性	注意喚起として掲載
22	Media5 Mediatrix 4402 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
23	Visibility Software Cyber Recruiter に認証回避の脆弱性	注意喚起として掲載
24	ZTE ZXV10 W300 に認証情報がハードコードされている問題	注意喚起として掲載
25	Seowon Intech SWC - 9100 に複数の脆弱性	注意喚起として掲載
26	Fortinet FortiOS 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
27	Fortinet Fortiweb 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
28	Dell KACE K1000 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
29	BIG IP Edge Client における情報漏えいの脆弱性	注意喚起として掲載
30	DELL SonicWALL GMS/Analyzer/UMA 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
31	Internet Explorer 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
32	Microsoft XML DOM ActiveX コントロールに情報漏えいの脆弱性	注意喚起として掲載

(*14) 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。

項番	脆弱性	対応状況
33	Belkin WeMo Home Automation 製品に複数の脆弱性	注意喚起として掲載
34	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
35	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
36	Apple QuickTime 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
37	libpng におけるサービス運用妨害(DoS)の脆弱性	注意喚起として掲載
38	Synology DiskStation Manager に認証情報がハードコードされている問題	注意喚起として掲載
39	CMS Made Simple 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
40	Blue Coat ProxySG に脆弱性	注意喚起として掲載
41	Foscam FI8910W に認証回避の脆弱性	注意喚起として掲載
42	ZTE 製ケーブルモデム F460/F660 にバックドアの問題	注意喚起として掲載
43	Serena Dimensions CM web client に複数の脆弱性	注意喚起として掲載
44	Huawei E355 に認証回避の脆弱性	注意喚起として掲載
45	Aker Secure Mail Gateway 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
46	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
47	Apple TV 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
48	CENTUM CS 3000 操作監視機能に複数のバッファオーバーフローの脆弱性	特定製品開発者へ通知
49	WatchGuard Fireware XTM 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
50	Webmin 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
51	Virtual Access GW6110A に権限昇格の脆弱性	注意喚起として掲載
52	ManageEngine OpStor に複数の脆弱性	注意喚起として掲載

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	Microsoft Windows XP および Office 2003 のサポート終了について

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

2-1-5. 調整不能案件の処理状況別件数

（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「連絡不能開発者一覧」を 2011 年 9 月 29 日に公開して以来の公表件数です。今四半期の新たな公表数は、8 件、累計 152 件 [*16] でした。「連絡不能開発者一覧」に公表後、調整を再開できたのは今四半期、3 件、累計 21 件です。

（2） 製品開発者情報の公開調査結果

図 2-15 は前述の連絡不能開発者 152 件についての公開調査の結果です。152 件のうち 86%にあたる 131 件が連絡不能開発者で、依然として、製品開発者と連絡がとれない状況です。また、今四半期末までに調整を再開した 21 件のうち、本制度における取扱いを終了したのは 8 件、残り 13 件は引き続き調整中です。

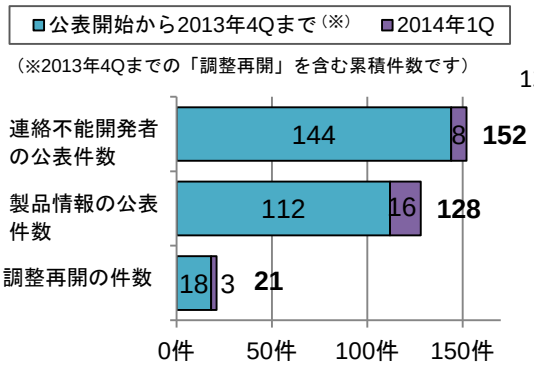


図2-14. 2014年1Qの公表および調整再開の状況

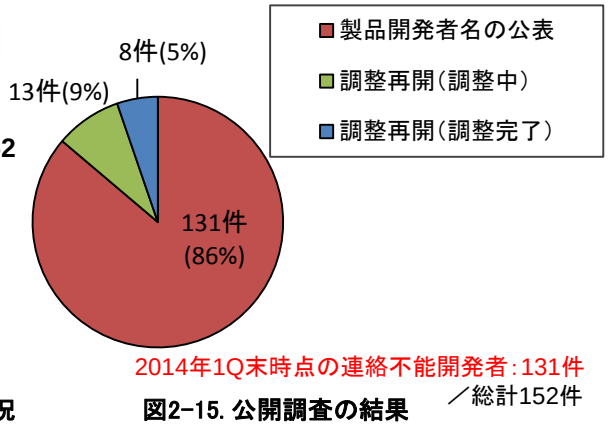


図2-15. 公開調査の結果

[*16] 調整再開した件数を含んだ製品開発者名の公表件数の累計です。

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 160 件（累計 7,240 件）でした。このうち「修正完了」したものは 138 件（累計 5,446 件）、注意喚起により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 13 件（累計 414 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」を行った上で、処理を取りやめるという本制度の運用に則ったものです。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ないなどの理由により「取扱不能」となったものは 5 件（累計 74 件）でした。「不受理」としたものは 4 件（累計 176 件）でした。取扱いを終了した累計 7,240 件のうち「注意喚起」「取扱不能」「不受理」を除く累計 5,860 件（81%）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が確認されています。

「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 13 件（累計 612 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 1 件（累計 28 件）でした。

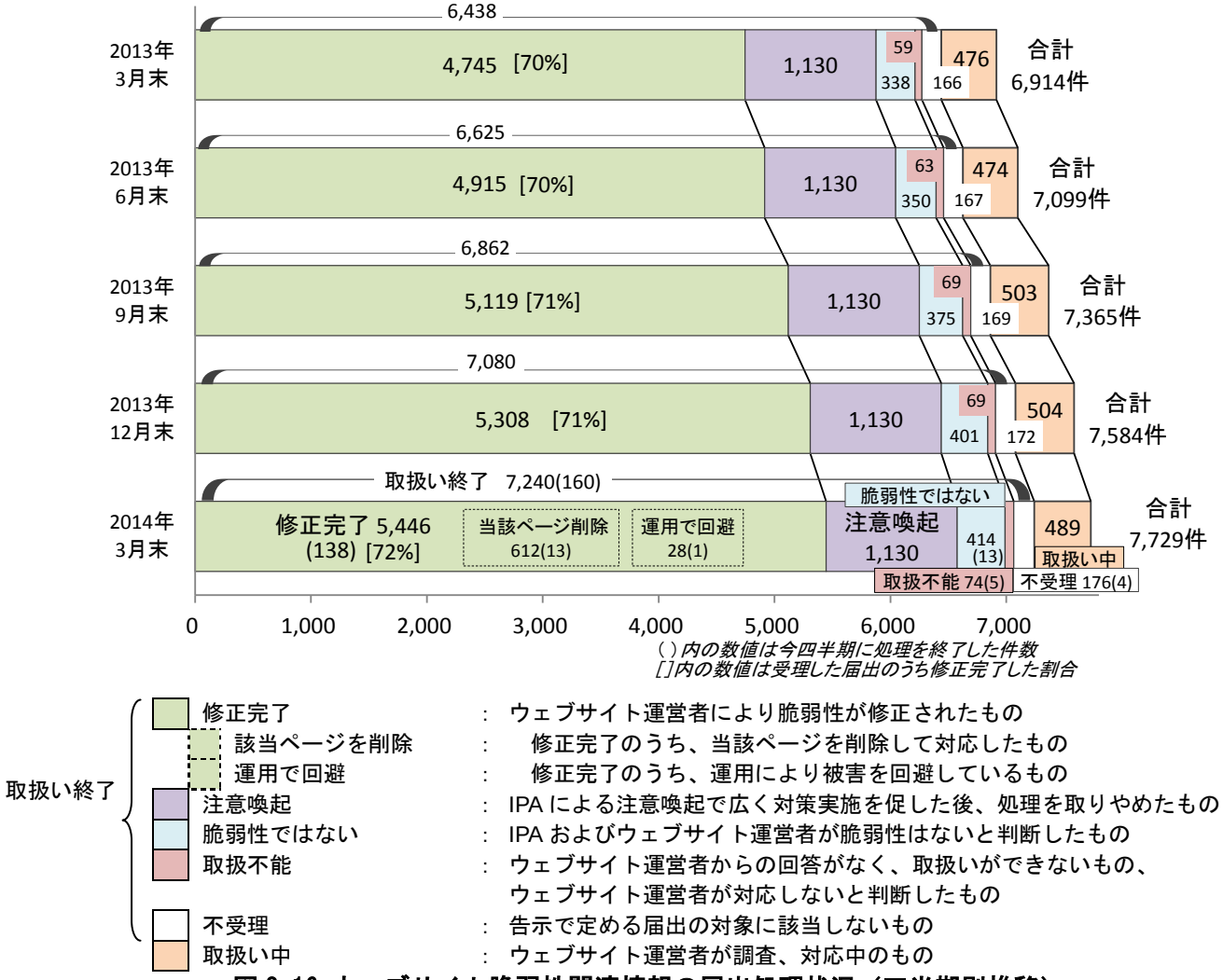


図 2-16. ウェブサイト脆弱性関連情報の届出処理状況（四半期別推移）

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 7,729 件のうち、不受理を除いた 7,553 件の届出を分析した結果を記載します。

2-2-2. 運営主体者別件数

図 2-17 のグラフは、届出されたウェブサイトにおける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別に示しています。今四半期は「企業（株式・非上場）」が最も多く、企業が全体の約 8 割を占めています。

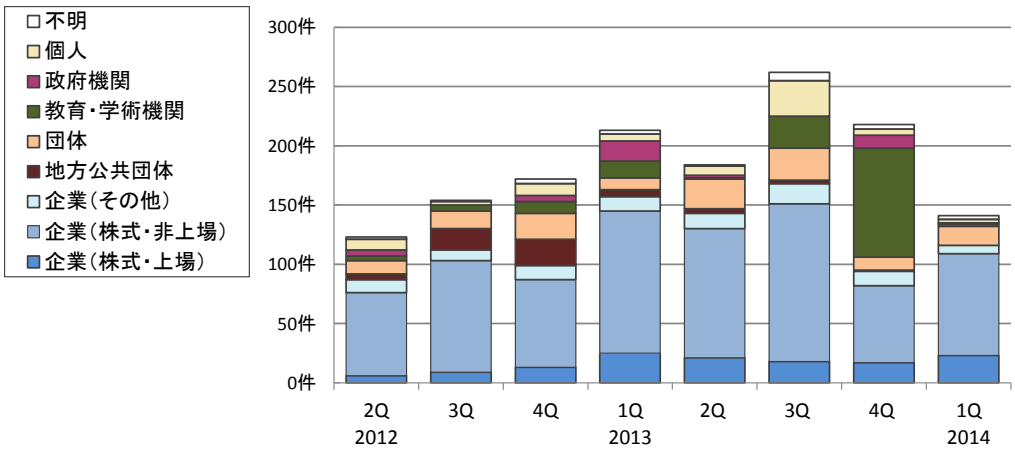


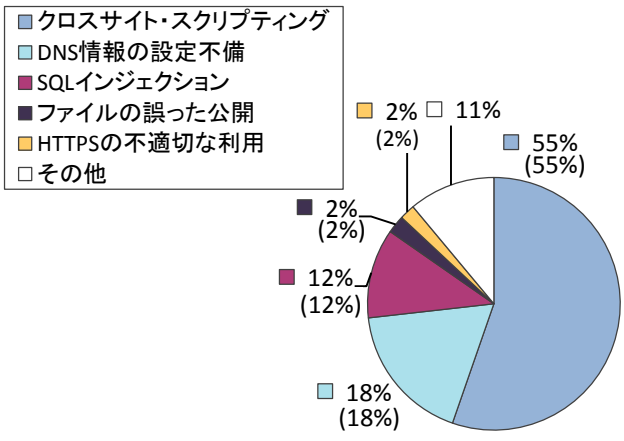
図2-17. 運営主体の種類別の届出件数(四半期別推移)

2-2-3. 脆弱性の種類・脅威別届出

図 2-18、図 2-19 のグラフは、届出された脆弱性の種類を示しています。図 2-18 は届出開始から今四半期末までの届出累計の割合を、図 2-19 は過去 2 年間の届出件数の推移を四半期別に示しています[*17]。

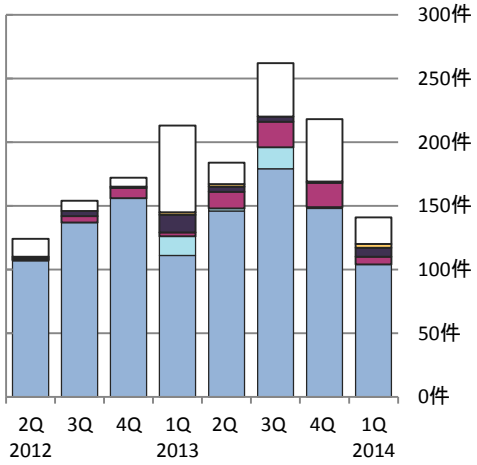
累計では、「クロスサイト・スクリプティング」だけで 55%を占めており、次いで「DNS 情報の設定不備」「SQL インジェクション」となっています。「DNS 情報の設定不備」は累計 18%ありますが、2008 年から 2009 年にかけて多く届出されたのが反映されたものです。「クロスサイト・スクリプティング」は、2011 年第 3 四半期から 2012 年第 4 四半期まで全体の約 9 割を占めていましたが、2013 年第 1 四半期以降は他の脆弱性の種類の件数が増加しています。なお、この統計はあくまでも届出の傾向であり、世の中に存在する脆弱性の傾向と必ずしも一致するものではありません。

ウェブサイトの脆弱性の種類別の届出状況



(7,553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



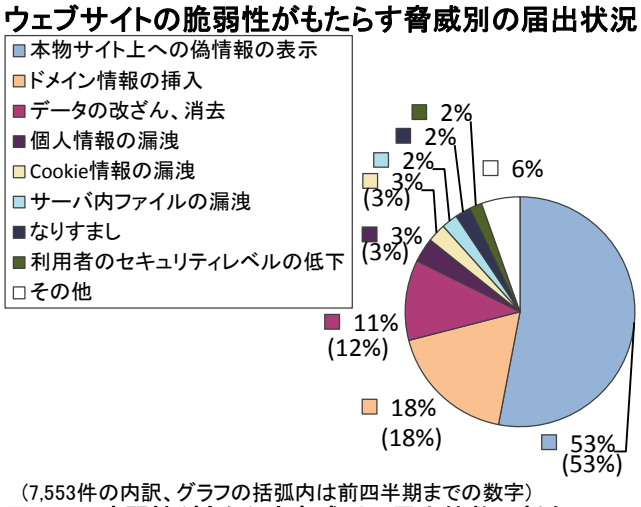
(過去2年間の届出内訳)

図2-19. 脆弱性の種類別の届出件数 (四半期別推移)

[*17] 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。

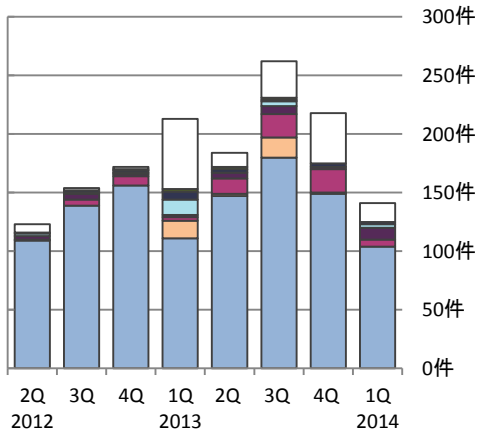
図 2-20、図 2-21 のグラフは、届出された脆弱性がもたらす脅威を示しています。図 2-20 は届出開始から今四半期末までの届出の割合を、図 2-21 は過去 2 年間の届出件数の推移を四半期別に示したものです。

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 82%を占めています。



（7,553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、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。2014 年第 1 四半期に修正を完了した 138 件のうち 60 件（43%）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（189 件中 32 件（17%））より増加しています。表 2-6 は、過去 3 年間の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累計件数および割合を四半期ごとに示したものです。

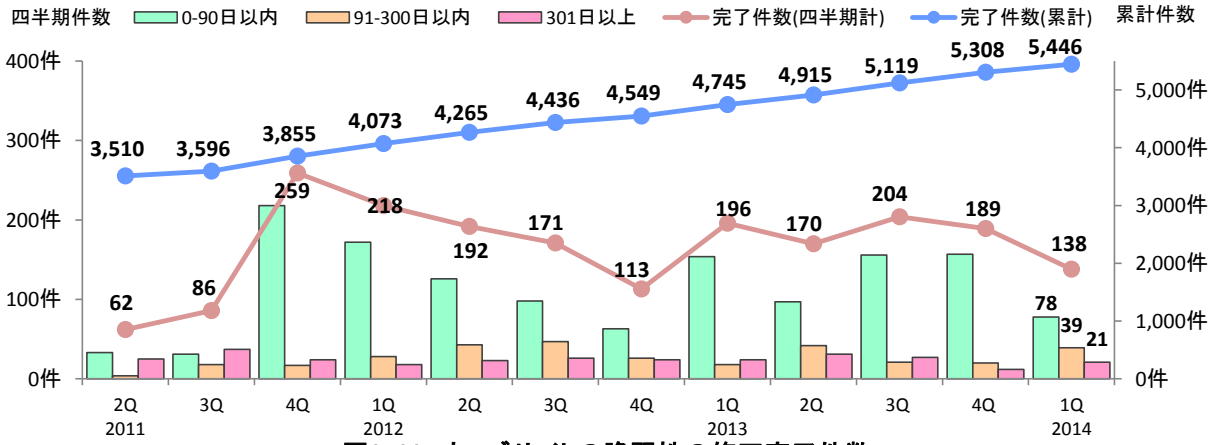


図2-22. ウェブサイトの脆弱性の修正完了件数

表 2-6. 90 日以内に修正完了した累計件数およびその割合の推移

	2011 2Q	3Q	4Q	2012 1Q	2Q	3Q	4Q	2013 1Q	2Q	3Q	4Q	2014 1Q
修正完了件数	3,510	3,596	3,855	4,073	4,265	4,436	4,549	4,745	4,915	5,119	5,308	5,446
90 日以内の件数	2,285	2,316	2,534	2,706	2,832	2,930	2,993	3,147	3,244	3,400	3,557	3,635
90 日以内の割合	65%	64%	66%	66%	66%	66%	66%	66%	66%	66%	67%	67%

図 2-23、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を脆弱性の種類別に分類し、その傾向を示したものです[*18]。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。

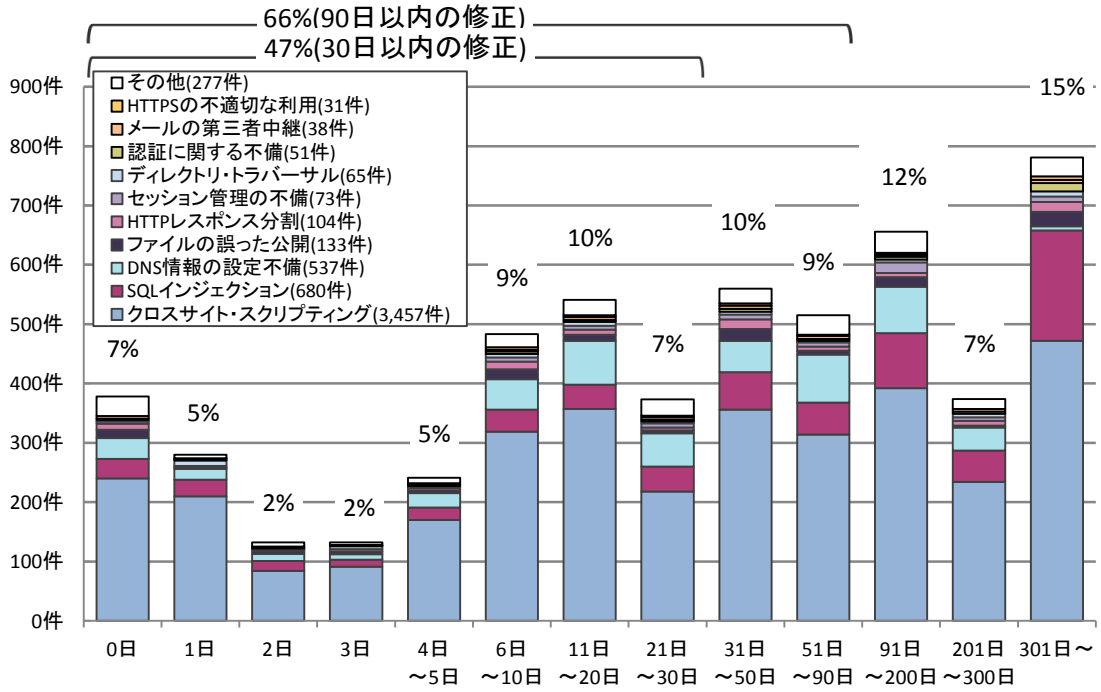


図2-23.ウェブサイトの修正に要した日数

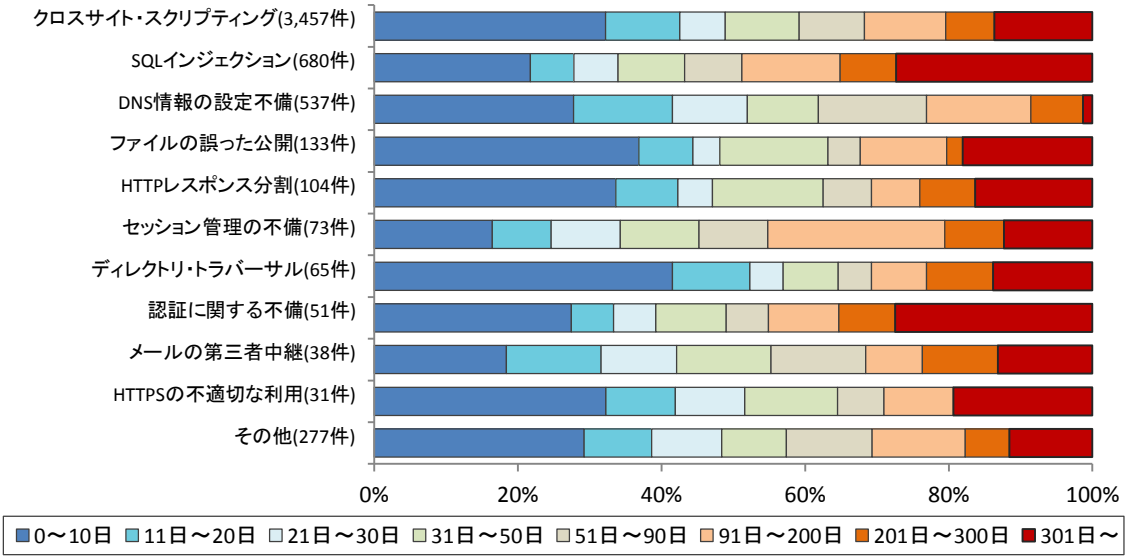


図2-24.ウェブサイトの修正に要した脆弱性種類別の日数の傾向

[*18] 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 66 件、200 日から 299 日のものは 81 件など、これらの合計は 357 件（前四半期は 358 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。

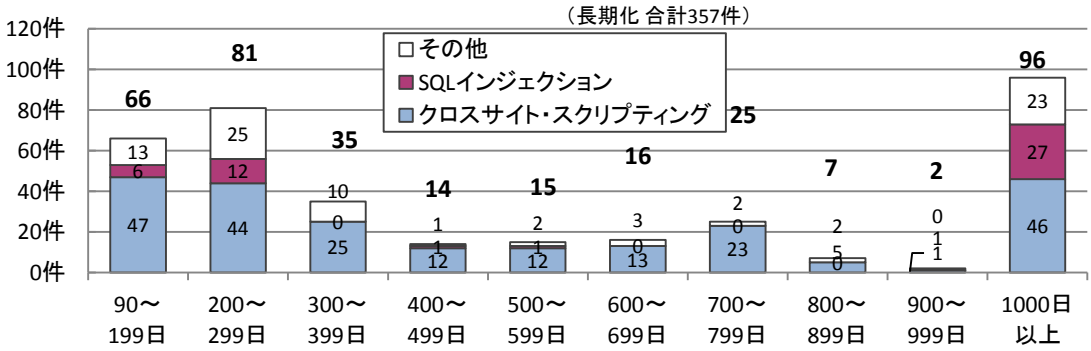


図2−25.取扱いが長期化(90日以上経過)しているウェブサイトの経過日数と脆弱性の種類

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、その割合を示しています。

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

	2012 2Q	3Q	4Q	2013 1Q	2Q	3Q	4Q	2014 1Q
取扱い中の件数	449 件	423 件	473 件	474 件	473 件	503 件	504 件	489 件
長期化している件数	318 件	302 件	296 件	301 件	307 件	302 件	358 件	357 件
長期化している割合	71%	71%	63%	64%	65%	60%	71%	73%

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

⇒「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）:
http://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）」:
http://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」:
http://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」:
http://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

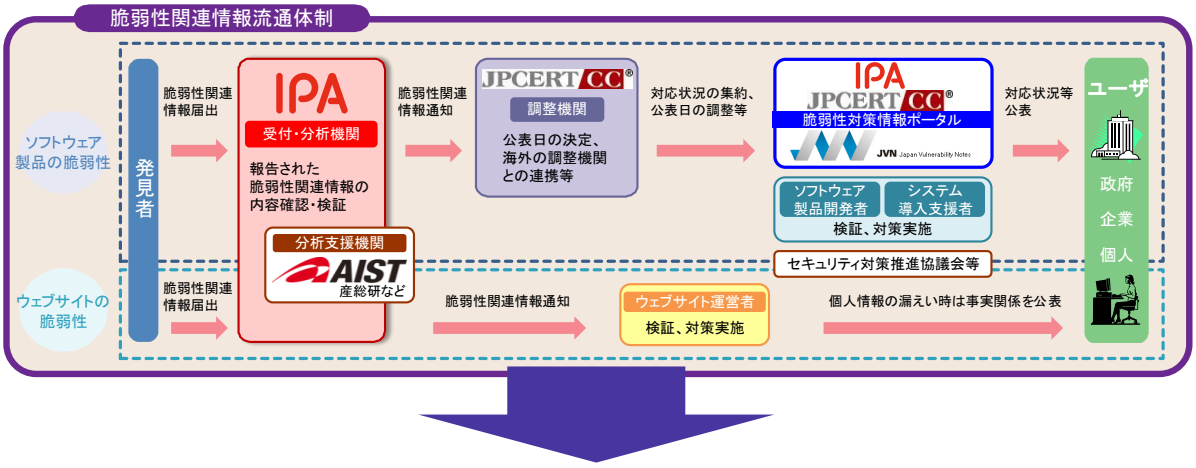
付表 2. ウェブサイトの脆弱性の分類

	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