

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 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、2013 年 1 月 1 日から 2013 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。

目次

1. 2013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
1-1. 脆弱性関連情報の届出状況	1
1-2. 脆弱性の修正完了状況	2
1-3. 調整不能案件の取扱い状況	2
(1) 連絡不能開発者一覧の公表状況	2
1-4. 注目すべき脆弱性	3
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）	4
2-1. ソフトウェア製品の脆弱性	4
2-1-1. 処理状況	4
2-1-2. ソフトウェア製品の種類	5
2-1-3. 脆弱性の原因と脅威	6
2-1-4. 調整および公表状況	8
2-1-5. 調整不能案件の処理状況	13
(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	13
(2) 製品開発者情報の公開調査結果	13
2-2. ウェブサイトの脆弱性	14
2-2-1. 処理状況	14
2-2-2. 運営主体の種類	15
2-2-3. 脆弱性の種類と脅威	15
2-2-4. 修正完了状況	16
2-2-5. 取扱中の状況	18
3. 関係者への要望	19
3-1. ウェブサイト運営者	19
3-2. 製品開発者	19
3-3. 一般インターネットユーザー	19
3-4. 発見者	19
付表1. ソフトウェア製品 脆弱性の原因分類	20
付表2. ウェブサイト脆弱性の分類	21
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）	22

1. 2013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8,444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^(*)」(以降、本制度)における届出状況について、表1-1は2013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。今期の届出件数はソフトウェア製品に関するもの64件、ウェブサイト(ウェブアプリケーション)に関するもの213件、合計277件でした。届出受付開始からの累計件数は、ソフトウェア製品に関するもの1,531件、ウェブサイトに関するもの6,913件、合計8,444件となりました。ウェブサイトに関する届出が全体の82%を占めています。

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。

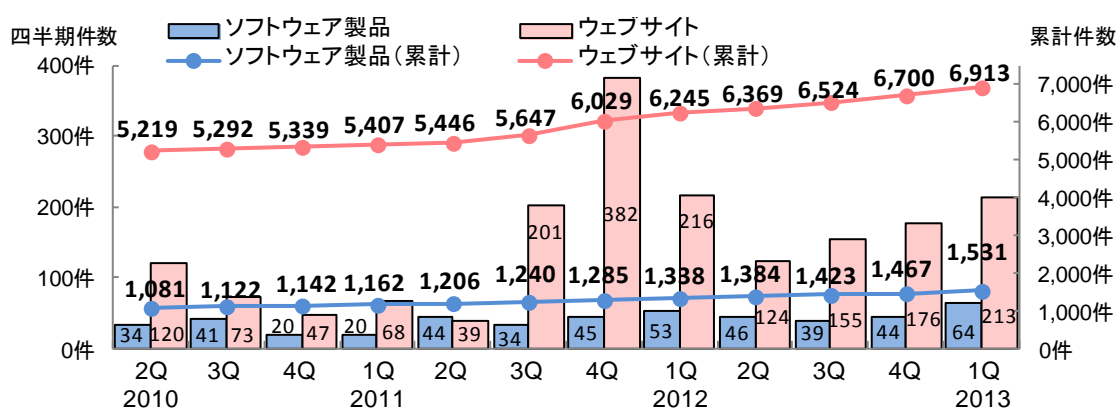


図1-1.脆弱性関連情報の届出件数の四半期別推移

表1-2. 届出件数(過去3年間)

	2010 2Q	3Q	4Q	2011 1Q	2Q	3Q	4Q	2012 1Q	2Q	3Q	4Q	2013 1Q
累計届出件数[件]	6,300	6,414	6,481	6,569	6,652	6,887	7,314	7,583	7,753	7,947	8,167	8,444
1就業日あたり[件/日]	4.32	4.22	4.10	4.01	3.92	3.91	4.01	4.03	3.99	3.96	3.95	3.97

(*) 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.jpccert.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5,400件を超過しました ～

表 1-3 は今四半期のソフトウェア製品とウェブサイトの修正完了件数および届出受付開始から今四半期までの累計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	30 件	722 件
ウェブサイト	196 件	4,745 件
合計	226 件	5,467 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 30 件^{(*)3} (累計 722 件) でした。2010 年第 4 四半期以降は修正完了件数が 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 30 件のうち、届出を受理してから公表までに 45 日^{(*)4} 以上経過したものは 28 件でした。

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 196 件 (累計 4,745 件) でした。修正を完了した 196 件のうち、ウェブアプリケーションを修正したものが 172 件 (88%)、当該ページを削除したものが 24 件 (12%) でした。なお、修正を完了した 196 件のうち 154 件 (79%) は、届出から 90 日^{(*)5} 以内に修正が完了しており、前四半期 (113 件中 63 件 (56%)) より早期に修正する増加しています。

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場合、その製品開発者を「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

今四半期に新たに公表した「製品開発者名」は 5 件 (累計 124 件) です。また、既に公表後一定期間 (約 3 ヶ月) が経過したものの連絡が取れず、広く関係者からの情報提供を求めるために「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)」を公表したものは 7 件 (累計 105 件) でした。製品開発者から応答があったのは 0 件 (累計 16 件) でした。これまでに製品開発者から応答があった 16 件のうち、7 件が本制度における取扱いを終了しました。今四半期末時点における公表中件数は、108 件となります。

^{(*)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

本節では、今期に届出のあった脆弱性関連情報の中で、注目すべき脆弱性「DNS の設定不備について」を紹介しています。ウェブサイト運営者は、下記の事例を参考に同様の脆弱性を作り込まない様に注意してください。

DNS (Domain Name System) は、ウェブサイトやメールをはじめとしたインターネットを支える技術の一つです。ウェブサイトにおいても DNS による名前解決は行われます。

ウェブサイトの名前解決に関する DNS の設定不備については、ウェブサイトの脆弱性として届出を受け付けています。今四半期には、この DNS の設定不備（「委譲」に関する設定が適切でないことに起因する問題）に関する届出がウェブサイト全体の 8% に当たる 15 件ありました。

大規模なウェブサイトの場合、ウェブサイトで利用するドメインを管理単位に分割してサブドメインを設ける構成をとることがあります。この際、DNS サーバ側に管理範囲を指定する為の委譲設定を行います。この委譲に関する設定が適切ではない場合、第三者が本来運用できないはずの DNS サーバを適切なサーバとして参照されてしまいます。

図 1-2 のように、第三者の DNS サーバが適切なウェブサイトの IP アドレスを返答しないように設定されてしまうことで、利用者は適切なアドレスにアクセスしているにもかかわらず、フィッシングサイトなど悪意あるページに誘導されてしまう場合があります。

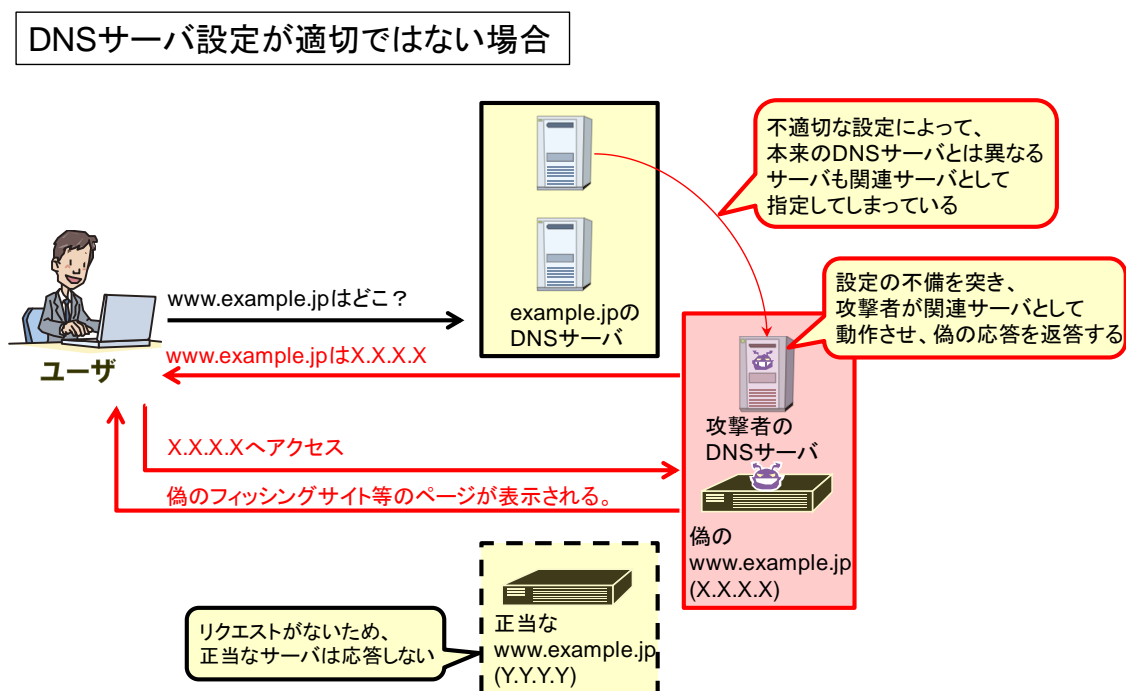


図 1-2. DNS サーバを適切に設定しない場合の危険性

このような状況になる原因は次のような場合が考えられます。

- ・ DNS 管理業者の変更やサーバ設定の更新時の設定変更忘れ
- ・ ミススペルなどの設定ミス (example.jp → exmaple.jp)

詳細については、次のサイトを参考にしてください。

http://www.ipa.go.jp/security/event/2009/isec-semi/documents/2009tech2_v3.pdf

ウェブサイト運営者は、今一度 DNS サーバの設定を確認してください。

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 1 四半期に公表した脆弱性は 30 件（累計 722 件）です。また、製品開発者が「個別対応」したものは 2 件（累計 24 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 64 件）、「不受理」としたものは 4 件⁽⁷⁾（累計 210 件）、取扱い中は 511 件です。今四半期に、取扱い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⁽⁸⁾は 5 件です。2013 年 3 月末時点の連絡不能開発者公表数は 108 件になります。

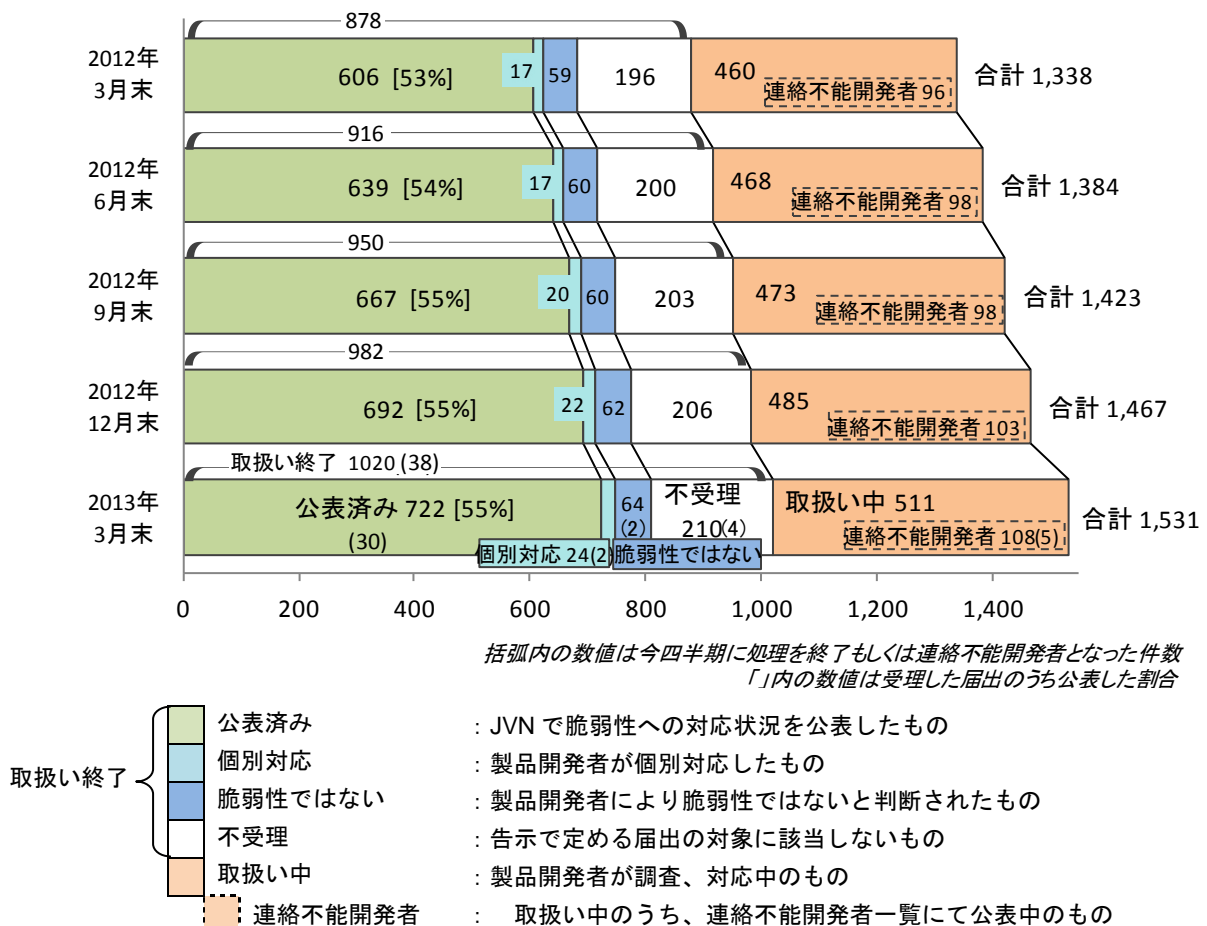


図 2-1.ソフトウェア製品 各時点における脆弱性関連情報の届出の処理状況

⁽⁷⁾ 今四半期の届出の中で不受理とした 1 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。

⁽⁸⁾ 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。

2-1-2. ソフトウェア製品の種類

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 1,531 件のうち、不受理を除いた 1,321 件について、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は、「ウェブアプリケーション」と「ウェブブラウザ」が共に増加しています。

ソフトウェア製品の製品種類別の届出状況

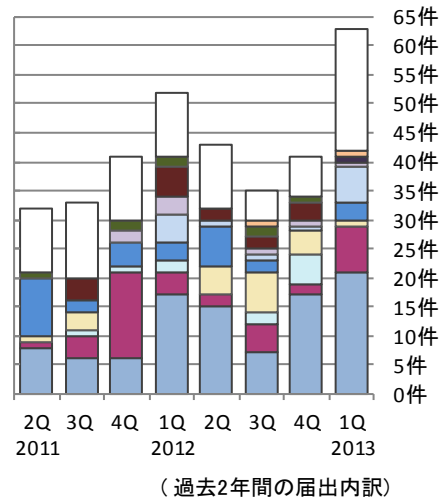
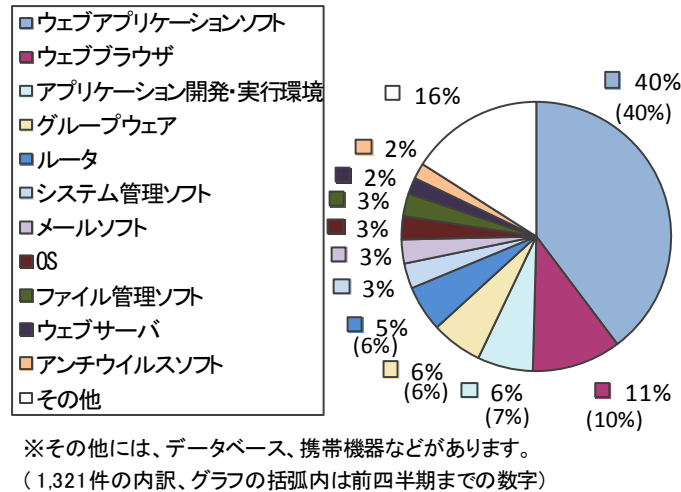


図2-2. 製品種類別の届出件数の割合 図2-3. 製品種類別の届出件数 (四半期別推移)

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 1,531 件のうち、不受理を除いた 1,321 件について、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は 33%となっています。また、今四半期はオープンソースソフトウェア以外（それ以外）の届出件数が 2 倍に増加しています。

オープンソースソフトウェアの脆弱性の届出状況

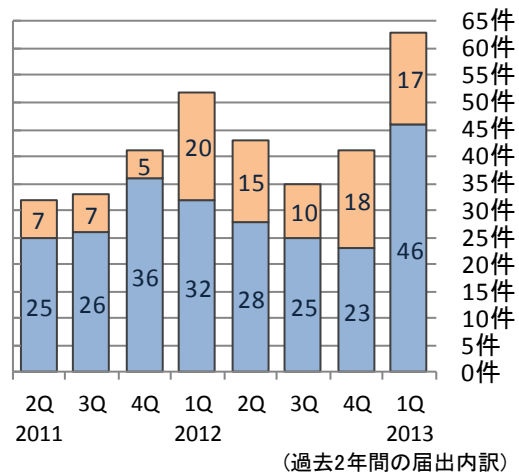
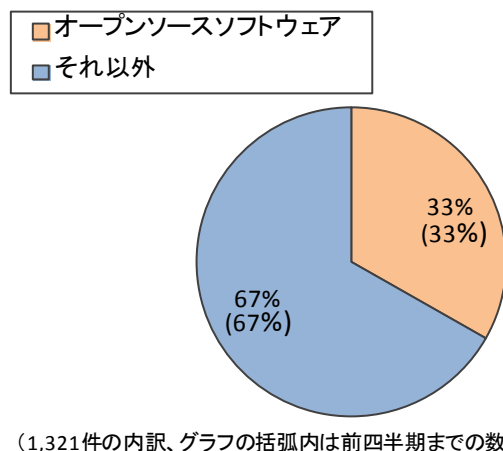


図2-4. オープンソースソフトウェアの届出件数の割合 図2-5. オープンソースソフトウェアの届出件数 (四半期別推移)

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 1,531 件のうち、不受理を除いた 1,321 件について、図 2-6 のグラフは過去 2 年間のスマートフォン向けアプリとそれ以外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処理状況を示したものです。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、届出されたスマートフォン向けアプリの脆弱性の 44% は対策が行われ JVN にて公表されています。

スマートフォン向けアプリの脆弱性の届出状況

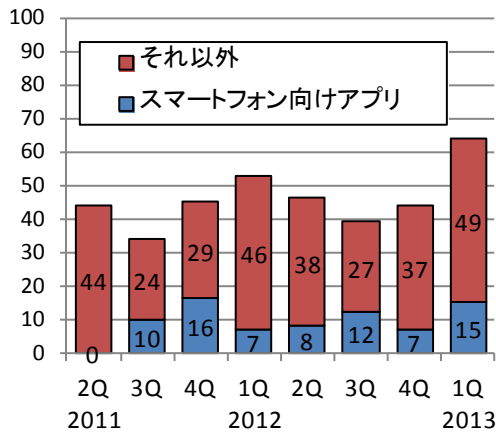


図2-6.スマートフォン向けアプリの届出件数(四半期別推移)

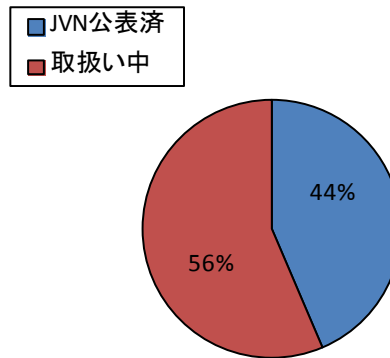
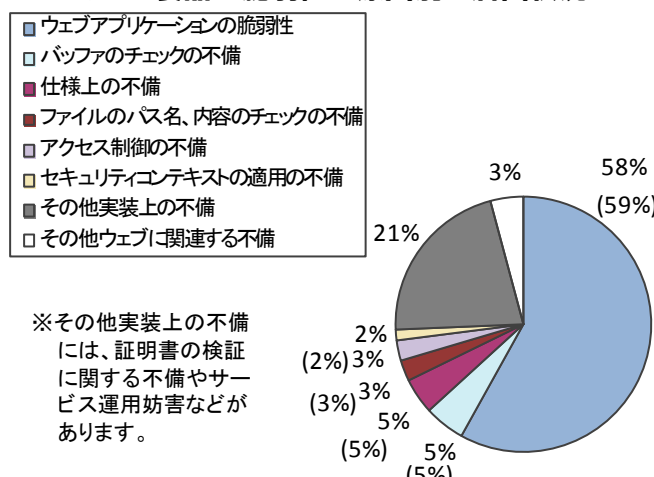


図2-7.スマートフォン向けアプリの処理状況

2-1-3. 脆弱性の原因と脅威

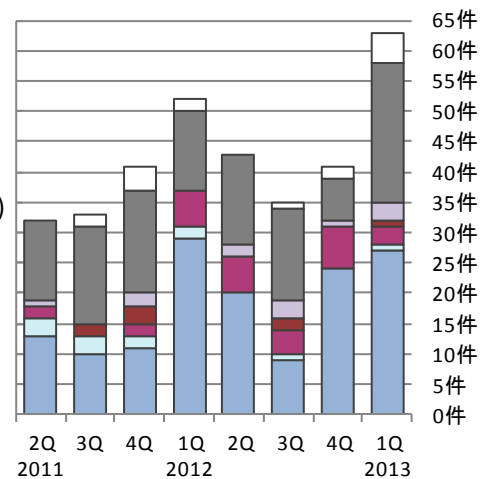
届出受付開始から今四半期までに届出のあったソフトウェア製品に関する脆弱性関連情報 1,531 件のうち、不受理を除いた 1,321 件について、図 2-8 のグラフは原因別の届出件数の割合を、図 2-9 のグラフは過去 2 年間の原因別届出件数の四半期別推移をそれぞれ示したものです。今四半期におけるソフトウェア製品の脆弱性の原因は、前四半期と同様に「ウェブアプリケーションの脆弱性」が最多となっています。

ソフトウェア製品の脆弱性の原因別の届出状況



(1,321 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

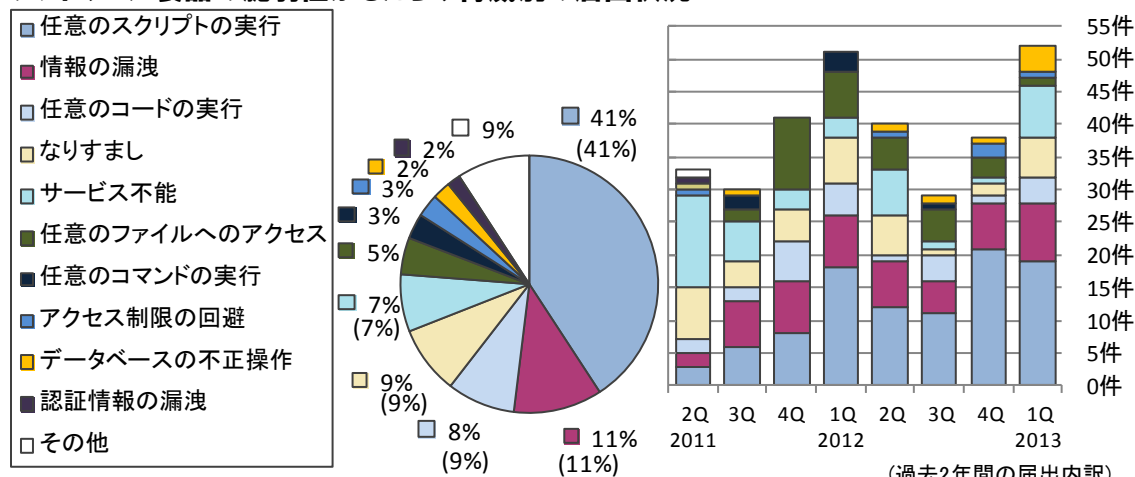


(過去2年間の届出内訳)

図2-9. 脆弱性の原因別の届出件数(四半期別推移)

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に関する脆弱性関連情報 1,531 件のうち、不受理を除いた 1,321 件について、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 年間の脅威別届出件数の四半期別推移をそれぞれ示したものです。「任意のスキプトの実行」が届出受付開始から今四半期までの届出のうち約 40%を占めています。また、今四半期は「任意のコードの実行」「なりすまし」「サービス不能」が増加し、「任意のスキプトの実行」が前四半期よりも減少しています。

ソフトウェア製品の脆弱性もたらす脅威別の届出状況



(1,321件の内訳、グラフの括弧内は前四半期までの数字)

図2-10. 脆弱性もたらす脅威別の届出件数の割合 図2-11. 脆弱性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⁽⁹⁾。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の中で、対策情報を公表した 1,629 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	30 件	722 件
②	海外 CSIRT 等と連携して公表したもの	34 件	907 件
合計		64 件	1,629 件

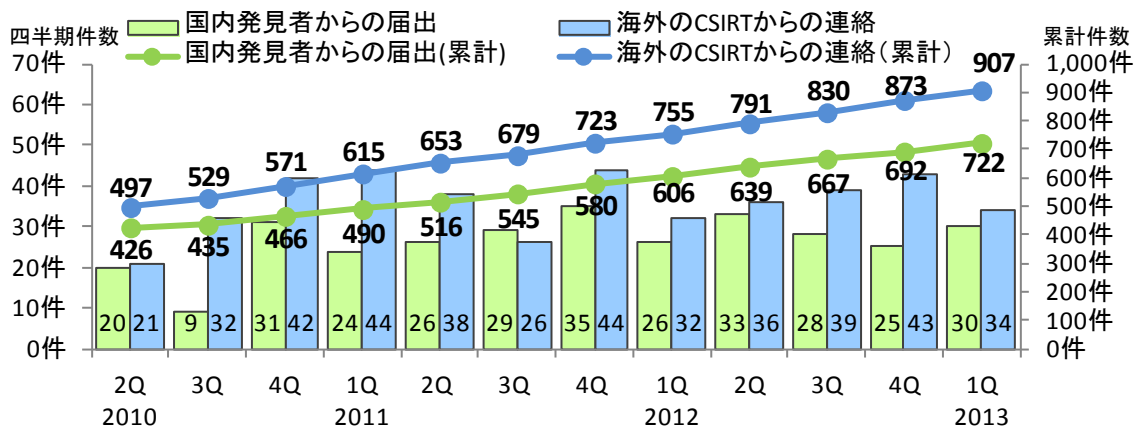


図 2-12. ソフトウェア製品の脆弱性対策情報の公表件数

(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 年間に於ける 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。

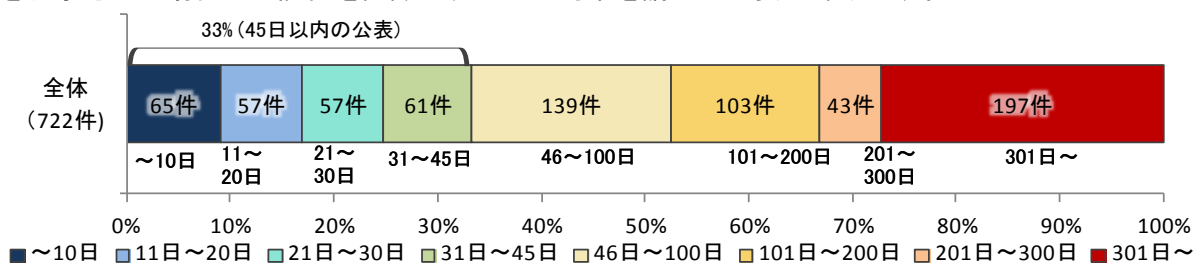


図 2-13. ソフトウェア製品の脆弱性公表日数

表 2-2. 45 日以内に公表した件数の割合推移 (四半期別)

2010 2Q	3Q	4Q	2011 1Q	2Q	3Q	4Q	2012 1Q	2Q	3Q	4Q	2013 1Q
36%	36%	38%	38%	36%	34%	33%	34%	34%	35%	34%	33%

⁽⁹⁾ JPCERT/CC 活動概要 Page15~18(<https://www.jpccert.or.jp/pr/2013/PR20130415.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 1 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）、組み込みソフトウェア製品の脆弱性が 2 件（表 2-3 の*3）ありました。

表 2-3. 2013 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 (*3)	NEC「Universal RAID Utility」におけるアクセス制限不備の脆弱性	RAID コントローラの管理ツール「Universal RAID Utility」には、アクセス制限不備の問題がありました。このため、第三者により当該製品で管理しているハードディスクに対して、任意の操作が実行される可能性がありました。	2013 年 2 月 21 日	9.0
2 (*3)	複数の Cisco 製品におけるサービス運用妨害 (DoS) の脆弱性	複数の Cisco 製品には、SSH 実装に不備がありました。このため、第三者によりサービス運用妨害 (DoS) 攻撃を受ける可能性がありました。	2013 年 3 月 7 日	7.8
3	「VxWorks」の SSH サーバ (IPSSH) におけるサービス運用妨害 (DoS) の脆弱性	組み込み用 OS「VxWorks」の SSH サーバ (IPSSH) には、認証リクエスト処理に不備がありました。このため、第三者により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。この問題は項番 4, 16, 17 とは異なる問題です。	2013 年 3 月 18 日	7.8
4	「VxWorks」の SSH サーバ (IPSSH) におけるサービス運用妨害 (DoS) の脆弱性	組み込み用 OS「VxWorks」の SSH サーバ (IPSSH) には、認証リクエスト処理に不備がありました。このため、第三者により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。この問題は項番 3, 16, 17 とは異なる問題です。	2013 年 3 月 18 日	7.8
脆弱性の深刻度=レベル II（警告）、CVSS 基本値=4.0~6.9				
5	「Documents Pro」(旧「Files HD」)におけるディレクトリ・トラバーサル脆弱性	iOS 向けのドキュメントビューア「Documents Pro」には、ディレクトリ・トラバーサル脆弱性がありました。このため、第三者により任意のファイルを閲覧されたり、削除されたりなどの操作が行われる可能性がありました。	2013 年 1 月 18 日	4.0
6	「μ-s」および「ネットマニア版 PHP ウェブログシステム」におけるクロスサイト・スクリプティング脆弱性	コンテンツ管理システム「μ-s」および「ネットマニア版 PHP ウェブログシステム」には、ウェブページを出力する際の処理に問題がありました。このため、第三者によりウェブページにスクリプトを埋め込まれる可能性がありました。	2013 年 1 月 22 日	4.3
7	「WebSphere Application Server (WAS)」におけるクロスサイト・スクリプティング脆弱性	アプリケーションサーバ「WebSphere Application Server (WAS)」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 1 月 25 日	4.3
8	「mora ダウンローダー」における実行ファイル読み込みに関する脆弱性	音楽データダウンロードソフト「mora ダウンローダー」には、実行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コードを実行される可能性がありました。	2013 年 2 月 7 日	5.1

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	「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。	2013 年 2 月 8 日	6.5
10	「imgboard」におけるクロスサイト・スクリプティングの脆弱性	画像共有掲示板ソフト「imgboard」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 2 月 14 日	4.3
11	「3DM」(3ware Disk Manager) におけるディレクトリ・トラバーサル脆弱性	RAID コントローラの管理ツール「3DM (3ware Disk Manager)」には、ディレクトリ・トラバーサル脆弱性がありました。このため、第三者によりサーバ内の任意のファイルを取得される可能性がありました。	2013 年 2 月 15 日	5.0
12 (*2)	複数のジャストシステム製品において任意のコードが実行される脆弱性	複数のジャストシステム製品には、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、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 2 月 26 日	6.8
13	「dopvCOMET*」におけるクロスサイト・スクリプティング脆弱性	アクセス解析ソフト「dopvCOMET*」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 2 月 28 日	4.3
14	「dopvSTAR*」におけるクロスサイト・スクリプティング脆弱性	アクセス解析ソフト「dopvSTAR*」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 2 月 28 日	4.3
15	「Kingsoft Writer」におけるバッファオーバーフロー脆弱性	ドキュメント編集ソフト「Kingsoft Writer」には、バッファオーバーフロー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 3 月 1 日	6.8
16	「VxWorks」の SSH サーバ (IPSSH) におけるサービス運用妨害 (DoS) の脆弱性	組込み用 OS「VxWorks」の SSH サーバ (IPSSH) には、pty リクエスト処理に不備がありました。このため、第三者により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。この問題は項番 3, 4, 17 とは異なる問題です。	2013 年 3 月 18 日	6.8
17	「VxWorks」の SSH サーバ (IPSSH) におけるサービス運用妨害 (DoS) の脆弱性	組込み用 OS「VxWorks」には、SSH セッションが確立した直後の処理に不備がありました。このため、第三者により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。この問題は項番 3, 4, 16 とは異なる問題です。	2013 年 3 月 18 日	6.8
18	「VxWorks」の WebCLI におけるサービス運用妨害 (DoS) の脆弱性	組込み用 OS「VxWorks」の WebCLI には、コマンド文字列の解析処理に不備がありました。このため、第三者により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。	2013 年 3 月 18 日	6.8
19	「VxWorks Web Server」におけるサービス運用妨害 (DoS) の脆弱性	組込み用 OS「VxWorks」の Web Server には、URL 解析処理に不備がありました。このため、第三者により「VxWorks Web Server」を応答不能な状態にされる可能性がありました。	2013 年 3 月 18 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
20	複数の NEC 製モバイルルータにおけるクロスサイト・リクエスト・フォージェリの脆弱性	複数の NEC 製モバイルルータにクロスサイト・リクエスト・フォージェリの脆弱性がありました。このため、第三者により設定の初期化や再起動をさせられる可能性がありました。	2013年 3月19日	4.0
21	「Lotus Domino」におけるサービス運用妨害 (DoS) の脆弱性	グループウェア「Lotus Domino」には、HTTP リクエストの処理に不備がありました。このため、第三者によって「Lotus Domino」のサービスを停止される可能性がありました。	2013年 3月28日	5.0
脆弱性の深刻度=レベル1 (注意)、CVSS 基本値=0.0~3.9				
22	「Documents Pro」(旧「Files HD」)におけるクロスサイト・スクリプティングの脆弱性	iOS 向けのドキュメントビューア「Documents Pro」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 1月18日	2.6
23	Android 版「ウェザーニュースタッチ」において位置情報をログに出力する脆弱性	Android 向けの天気予報アプリ「ウェザーニュースタッチ」には、位置情報をログに出力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が記録した位置情報を取得される可能性がありました。	2013年 1月31日	2.6
24	「サイボウズ ガルーン」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 ガルーン」には出力する文字列のエスケープ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 2月8日	2.6
25	Android 版「GREE (グリーン)」におけるディレクトリ・トラバーサル脆弱性	Android 向けのゲームアプリ「GREE (グリーン)」には、ディレクトリ・トラバーサル脆弱性がありました。このため、第三者により当該製品のデータ領域にある情報を取得される可能性がありました。	2013年 2月14日	2.6
26	「Simeji」におけるアクセス制限不備の脆弱性	Android 端末用の日本語入力ソフトウェア「Simeji」には、アクセス制限不備の脆弱性がありました。このため、第三者により当該製品のデータ領域にある情報を取得される可能性がありました。	2013年 3月26日	2.6
27	「ArtIME 日本語入力」におけるアクセス制限不備の脆弱性	Android 端末用の日本語入力ソフトウェア「ArtIME 日本語入力」には、アクセス制限不備の脆弱性がありました。このため、第三者により当該製品のデータ領域にある情報を取得される可能性がありました。	2013年 3月26日	2.6
28	「COBIME」におけるアクセス制限不備の脆弱性	Android 端末用の日本語入力ソフトウェア「COBIME」には、アクセス制限不備の脆弱性がありました。このため、第三者により当該製品のデータ領域にある情報を取得される可能性がありました。	2013年 3月26日	2.6
29 (*1)	「OpenWnn フリック入力対応版」におけるアクセス制限不備の脆弱性	Android 端末用の日本語入力ソフトウェア「OpenWnn フリック入力対応版」には、アクセス制限不備の脆弱性がありました。このため、第三者により当該製品のデータ領域にある情報を取得される可能性がありました。	2013年 3月26日	2.6
30	Android 版「OpenWnn」におけるアクセス制限不備の脆弱性	Android 端末用の日本語入力ソフトウェア「OpenWnn」の Android 版には、アクセス制限不備の脆弱性がありました。このため、第三者により当該製品のデータ領域にある情報を取得される可能性がありました。	2013年 03月29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) : 組み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 34 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 9 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 ⁽¹⁰⁾ 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	Ruby on Rails に複数の脆弱性	注意喚起として掲載
2	BigAnt IM Message Server および関連コンポーネントに複数の脆弱性	注意喚起として掲載
3	Dell OpenManage Server Administrator 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	TL-WR841N に情報漏えいの脆弱性	注意喚起として掲載
5	DOMIT! RSS を使用している製品に情報漏えいの脆弱性	注意喚起として掲載
6	Foxit Advanced PDF Editor 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
7	WebYaST にホスト一覧を改ざんされる脆弱性	注意喚起として掲載
8	Ruby on Rails の JSON 解析処理に脆弱性	注意喚起として掲載
9	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
10	Portable SDK for UPnP にバッファオーバーフローの脆弱性	複数製品開発者へ通知
11	Nuance 製品に脆弱性	注意喚起として掲載
12	Adobe Reader および Acrobat に脆弱性	注意喚起として掲載
13	CS-Cart に検証不備の脆弱性	注意喚起として掲載
14	Dell PowerConnect 6248P にサービス運用妨害 (DoS) の脆弱性	注意喚起として掲載
15	GroundWork Monitor Enterprise に複数の脆弱性	注意喚起として掲載
16	HP LaserJet Pro シリーズにアクセス制限不備の脆弱性	注意喚起として掲載
17	Apple OS X Server 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
18	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
19	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
20	Fiery 2.0 Print Controller に脆弱性	注意喚起として掲載
21	Verizon FiOS Actiontec ルータ MI424WR-GEN3I にクロスサイトリクエストフォージェリの脆弱性	注意喚起として掲載
22	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
23	askiaweb に複数の脆弱性	注意喚起として掲載
24	NVIDIA 製ビデオカードのディスプレイドライバに複数の脆弱性	注意喚起として掲載
25	Core FTP 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

⁽¹⁰⁾ 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 ^(*) 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 製品における複数の脆弱性に対するアップデート
2	Oracle Java 7 に脆弱性
3	Microsoft 製品における CVE-2012-4792 に対するアップデート
4	Oracle Java 7 に複数の脆弱性
5	Adobe 製品に複数の脆弱性
6	Microsoft 製品の複数の脆弱性に対するアップデート
7	Oracle Java に複数の脆弱性
8	Oracle Java に複数の脆弱性
9	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前四半期までで 119 件、今四半期に 5 件を公表し、合計 124 件となりました。このうち、16 件が調整を再開しています。また、今四半期に「製品情報（対象製品の具体的な名称およびバージョン）」を公表した届出は 7 件あり、合計 105 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された連絡不能開発者の調査状況を示しています。今四半期は製品開発者からの応答はありませんでした。今四半期末時点の公表中件数は、108 件です。また、「連絡不能開発者一覧」の公表開始（2011 年 9 月 29 日）から今四半期末時点までに 16 件が調整を再開し、そのうち 7 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」の公表開始から 1 年以上が経過しましたが、今四半期末時点で 108 件は依然として、製品開発者からの連絡が無い状況です。

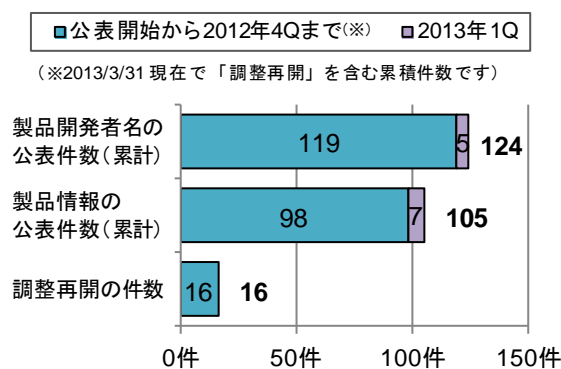


図2-14. 2013年1Qの公表および調整再開の状況

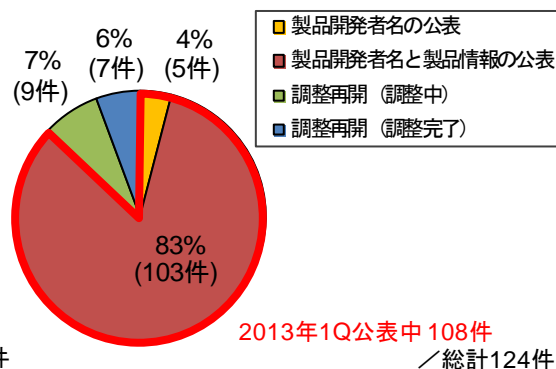


図2-15. 公開調査の状況

(*) 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、今四半期中に処理を終了したものは 212 件（累計 6,439 件）でした。このうち「修正完了」したものは 196 件（累計 4,745 件）、ウェブサイトが利用しているソフトウェア製品の修正プログラムが適用されていない問題について、IPA による「注意喚起」で広く対策実施を促した後に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 10 件（累計 337 件）でした。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手段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「連絡不可能」なもの 4 件（累計 59 件）です。「不受理」としたものは 2 件⁽¹²⁾（累計 168 件）でした。

取扱いを終了した累計 6,439 件のうち「注意喚起」「連絡不可能」「不受理」を除く累計 5,802 件（79%）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た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 24 件（累計 534 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 0 件（累計 23 件）でした。

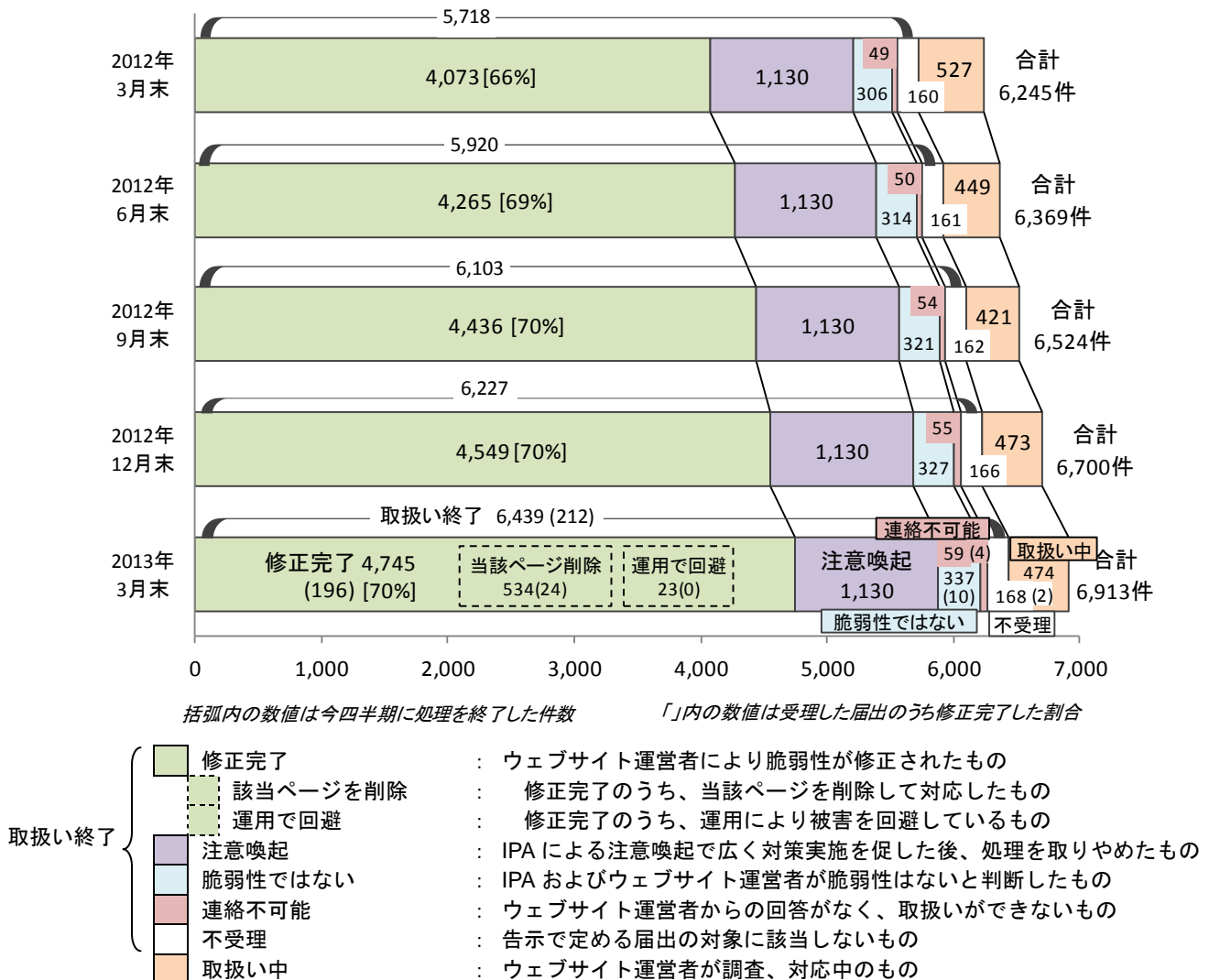


図 2-16. ウェブサイト各時点における脆弱性関連情報の届出の処理状況

⁽¹²⁾ 今四半期の届出の中で不受理とした 1 件、前四半期までの届出の中で今四半期に不受理とした 1 件です。

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脆弱性関連情報のうち、不受理を除いたウェブサイトの運営主体の種類別届出件数の四半期別推移を示しています。今四半期も企業への届出が多数を占めています。

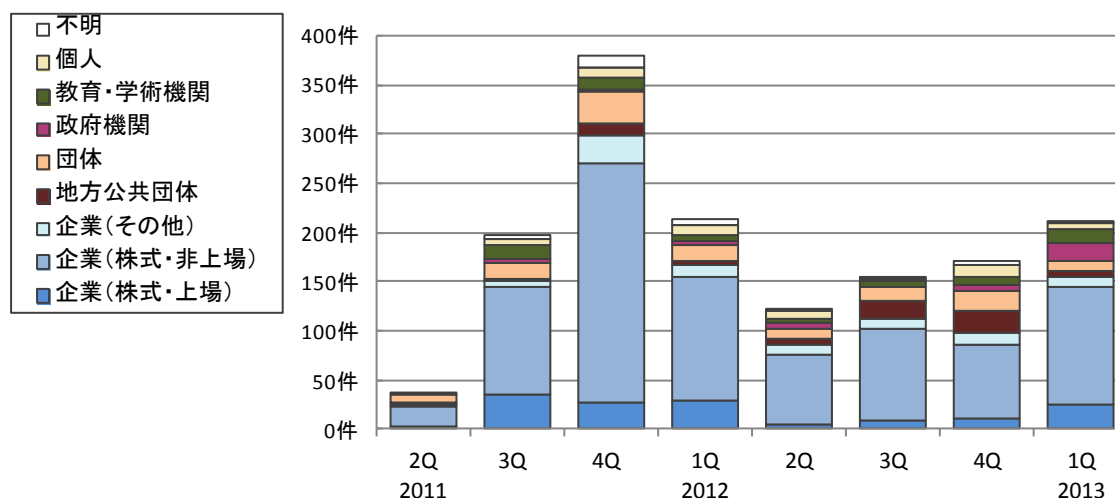
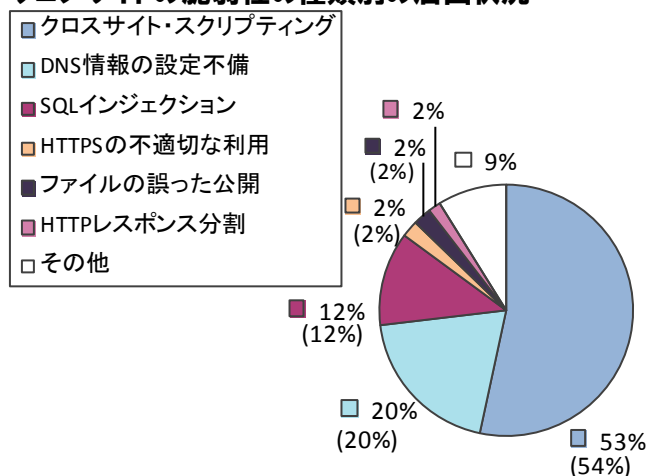


図2-17. ウェブサイトの運営主体の種類別の届出件数 (四半期別推移)

2-2-3. 脆弱性の種類と脅威

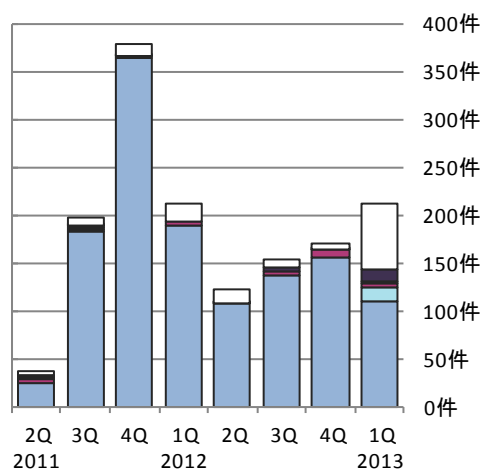
届出受付開始から今四半期までに届出のあったウェブサイトの脆弱性関連情報 6,913 件のうち、不受理を除いた 6,745 件について、図 2-18 のグラフは脆弱性の種類別の届出件数の割合を、図 2-19 は過去 2 年間の脆弱性の種類別届出件数の四半期別推移をそれぞれ示したものです⁽¹³⁾。脆弱性の種類は届出の多い「クロスサイト・スクリプティング」「DNS 情報の設定不備」「SQL インジェクション」の 3 種類の脆弱性が全体の 85% を占めています。2008 年第 3 四半期から 2009 年第 3 四半期にかけて多く届出のあった「DNS 情報の設定不備」は、2009 年第 4 四半期以降は届出がありませんでしたが、今四半期で 15 件の届出がありました。2011 年第 1 四半期以降、継続して「クロスサイト・スクリプティング」の脆弱性が 50% 以上を占めています。しかし、この統計はあくまで届出されたものの情報であり、この内訳が世の中に存在する脆弱性の傾向と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



(6,745 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



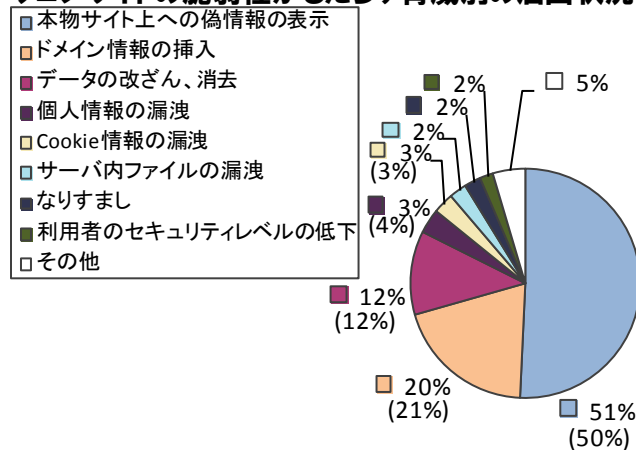
(過去2年間の届出内訳)

図2-19. 脆弱性の種類別の届出件数 (四半期別推移)

⁽¹³⁾ 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。

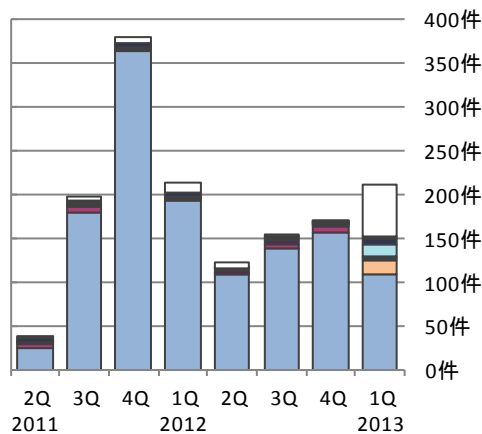
届出受付開始から今四半期までに届出のあったウェブサイトの脆弱性関連情報 6,913 件のうち、不受理を除いた 6,745 件について、図 2-20 のグラフは脅威別の届出件数の割合を、図 2-21 は過去 2 年間の脅威別届出件数の四半期別推移をそれぞれ示したものです。「クロスサイト・スクリプティング」「DNS 情報の設定不備」「SQL インジェクション」などにより発生する、「本物サイト上への偽情報の表示」「ドメイン情報の挿入」「データの改ざん、消去」が全体の 83% を占めています。

ウェブサイトの脆弱性もたらす脅威別の届出状況



(6,745 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。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。2011 年以降について「90 日以内」に修正が完了した割合（約 7 割弱）に大きな変動はありません。

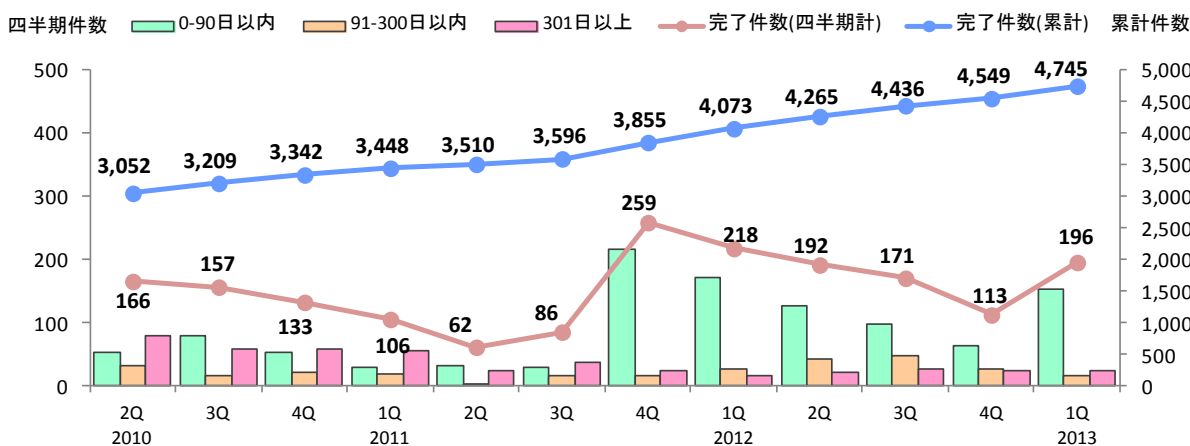


図 2-22. ウェブサイトの脆弱性の修正完了件数

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 2Q	3Q	4Q	2011 1Q	2Q	3Q	4Q	2012 1Q	2Q	3Q	4Q	2013 1Q
修正完了件数	3,052	3,209	3,342	3,448	3,510	3,596	3,855	4,073	4,265	4,436	4,549	4,745
90 日以内の件数	2,082	2,163	2,216	2,247	2,280	2,311	2,528	2,700	2,826	2,924	2,987	3,141
90 日以内の割合	68%	67%	66%	65%	65%	64%	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⁽¹⁴⁾。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。

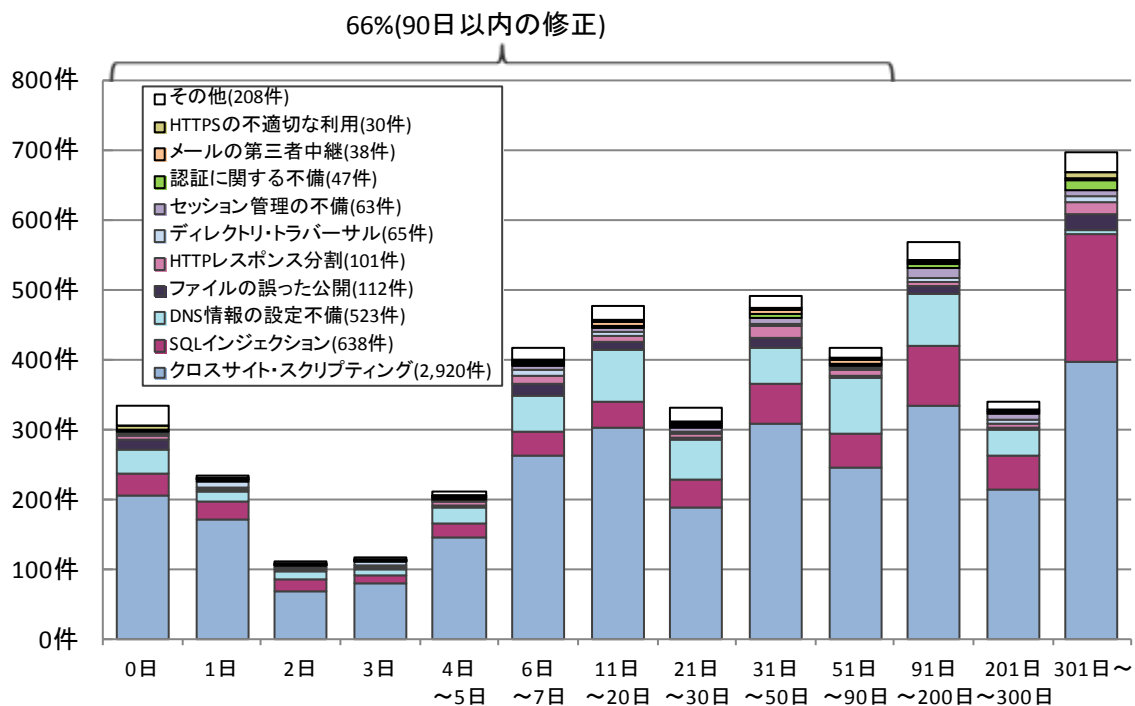


図2-23.ウェブサイトの修正に要した日数

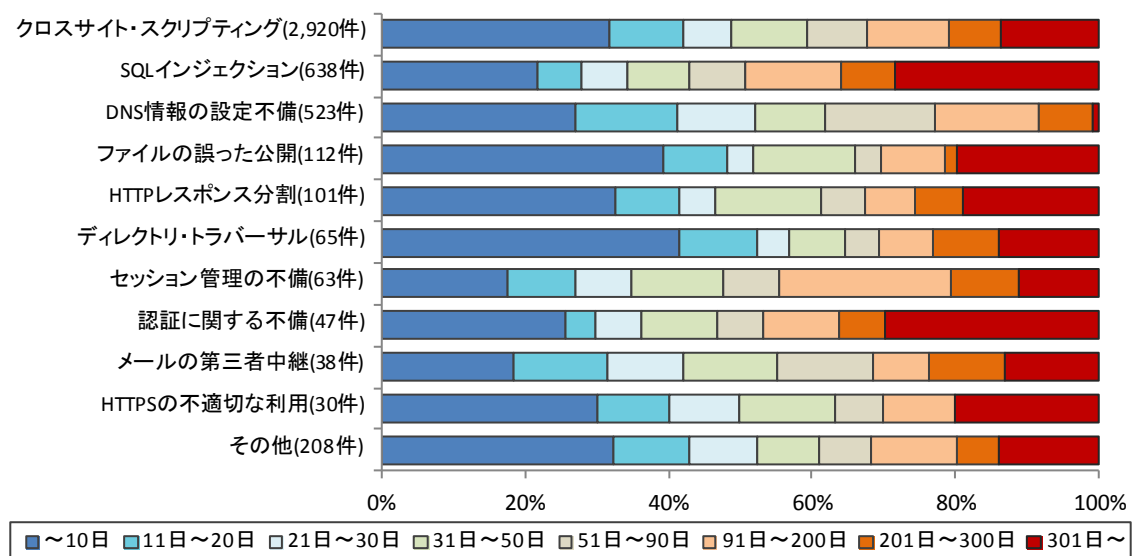


図2-24.ウェブサイトの修正に要した脆弱性種類別の日数の傾向

⁽¹⁴⁾ 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 は脆弱性が攻撃された場合の危険性を分かりやすく解説することや、1～2 か月毎に電子メールや電話、郵送などの手段で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 45 件、200 日から 299 日のものは 40 件など、これらの合計は 301 件（前四半期は 296 件）です。前四半期末までの取扱い長期化 296 件のうち今四半期に 34 件が取扱い終了となった一方、新たに 39 件が 90 日以上経過し取扱い長期化に加わり、合計で前四半期から取扱い長期化の件数が 5 件増加しました。

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。今四半期は経過日数が 90 日から 199 日に達したものの、300 日から 399 日に達したものがいずれも前四半期よりも減少しています。一方、400 日から 499 日に達したものが前四半期の 10 倍に増加しています。これは、2011 年第 3 四半期以降の届出が、修正されずに長期化したためです。

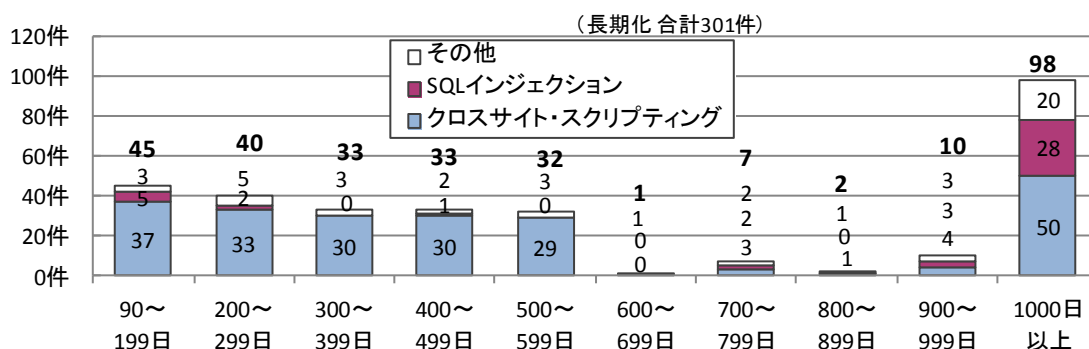


図2-25.取扱いが長期化(90日以上経過)しているウェブサイトの経過日数と脆弱性の種類

表 2-7. 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 2Q	3Q	4Q	2012 1Q	2Q	3Q	4Q	2013 1Q
取扱い中件数	344 件	435 件	541 件	527 件	449 件	423 件	473 件	474 件
長期化している件数	289 件	228 件	237 件	298 件	318 件	302 件	296 件	301 件
長期化している割合	84%	53%	44%	57%	71%	71%	63%	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、深刻度の高い脆弱性でも取扱いが長期化しているものがあります。ウェブサイト運営者は脆弱性を攻撃された場合の影響度を認識し、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の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について、「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。迅速な調整を進められるよう、「製品開発者リスト」へ登録ください（URL：<https://www.jpcert.or.jp/vh/regist.html>）。また、製品開発者自身が自社製品に関する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。脆弱性があるソフトウェアを使い続けることは避けなければなりません。

なお、MyJVN（URL：<http://jvndb.jvn.jp/apis/myjvn/>）で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 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 任意のスキプトの実行 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 任意のスキプトの実行 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、偽の証明書を受け入れてしまう。	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 任意のスキプトの実行
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

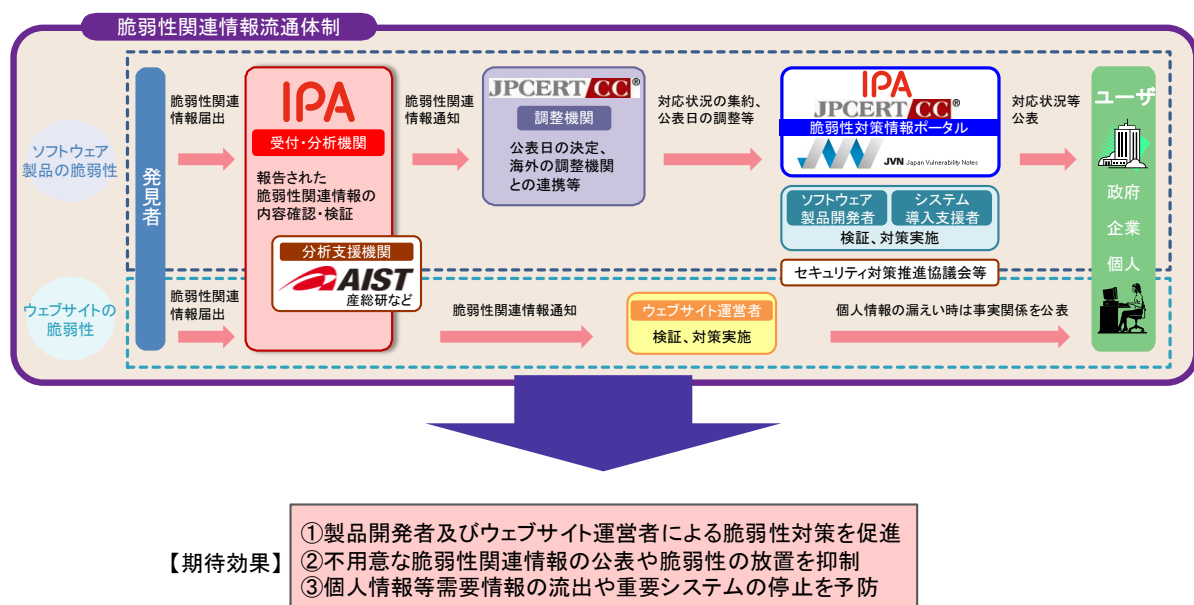
付表 2. ウェブサイト脆弱性の分類

	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)



※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