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

[2012 年第 4 四半期（10 月～12 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、ソフトウエ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。また、脆弱性に起因する被害の予防に資するため、四半期ごとに脆弱性関連情報の届出状況を公表しています。本レポートでは、2012 年 10 月 1 日から 2012 年 12 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
2013 年 1 月 28 日

目次

1. 2012 年第 4 四半期の注目すべき脆弱性

本章では、2012 年第 4 四半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。

1-1. HTTPS の設定不備の脆弱性について

～入力画面にも HTTPS の実施を～

HTTPS は、SSL（Secure Socket Layer）や TLS（Transport Layer Security）を用いて、ウェブブラウザとウェブサーバ間の通信を暗号化して通信内容を秘匿し、改ざんを防止するとともに、中間者攻撃を防止する手段です。この HTTPS は、ネットワーク盗聴やフィッシングサイト対策として、広く普及しています。

ウェブサイトで正しく HTTPS が導入されていないケースが報告されています。代表的な事案として、下記のようなケースが報告されています。

1)プライベートな CA 局から発行されたサーバ証明書が使用されている
2)サーバ証明書の有効期限が切れたまま使用され続けている
3)個人情報入力ページに HTTPS の導入がされていない

3)のケースにおいては、個人情報を送信するとき、送信先の URL が HTTPS のページであっても、その個人情報を利用者に入力させる画面の URL が HTTPS となるようにされていないケースが報告されています。このような状態でウェブサイトを運用すると、経路上で入力画面に改ざん等が行われた場合、ウェブ閲覧者は改ざんされたことに気付くことができず、結果として HTTPS を導入した効果の一つが無くなります。

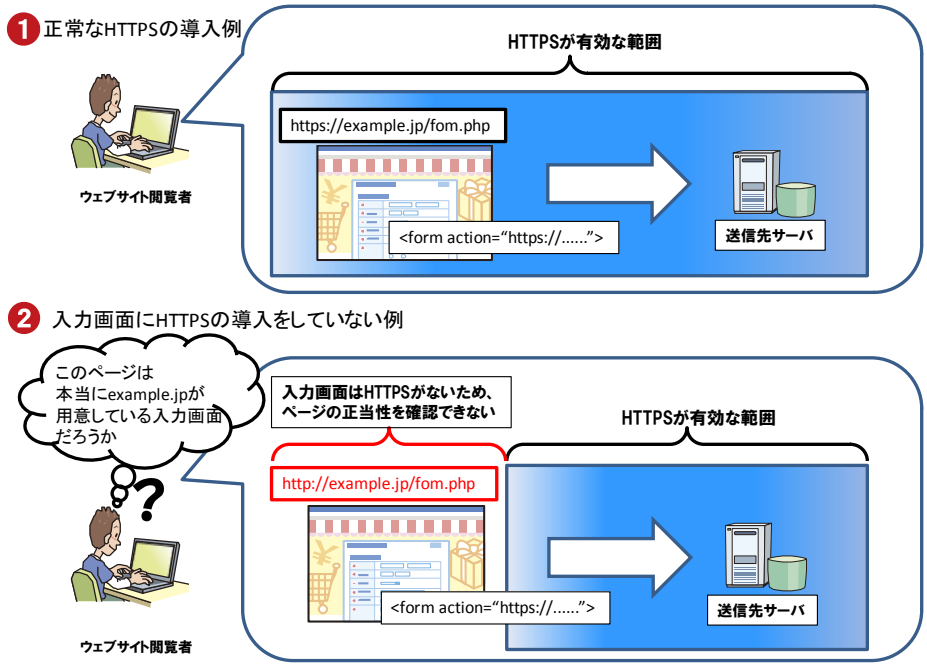


図1-1. 入力画面にHTTPSが導入されている場合といない場合の違いに関するイメージ

図 1-1 は正常な HTTPS の導入例と入力画面に HTTPS を導入しない例の違いを示しています。ウェブサイト運営者は、入力画面についても HTTPS を導入し、ウェブサイト閲覧者が安心して入力できる環境を構築しましょう。

また、HTTP Strict Transport Security(HSTS)というウェブサイトで常に HTTPS を使用するための仕組みを導入しているサイトもあります。対策の際に、この仕組みの導入についてもご検討ください。

1-2. DOM (*1) ベースのクロスサイト・スクリプティングの脆弱性について

図 1-2 は 2012 年に届出のあった DOM ベースのクロスサイト・スクリプティングの脆弱性の四半期別の届出件数を示しています。2012 年に、IPA に届出のあった DOM ベースのクロスサイト・スクリプティングの脆弱性は、全体で 130 件あり、その内 92 件は第 4 四半期に届出られたものでした。

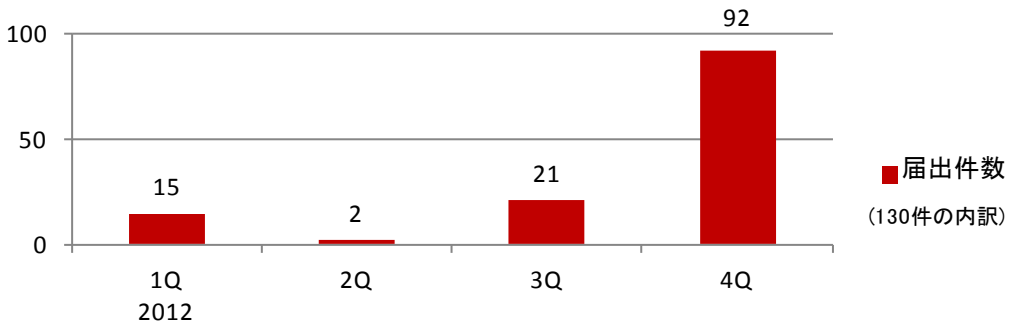


図1-2. 2012年のDOM Based XSSの届出件数

第 4 四半期の 92 件の中で最も多かった届出は、アクセス解析ソフトの JavaScript で実装された箇所に存在するもので、83 件でした。アクセス解析ソフトは、利用者のブラウザから送付されるウェブサイトのアクセス元を表すリファラ情報をアクセス解析に使用しています。届出では、JavaScript でリファラの情報を解析する処理にクロスサイト・スクリプティングの問題が内在していました。

攻撃シナリオとしては、攻撃者が作成した罠ページを被害者が訪れ、利用者のブラウザから送付されるリファラにスクリプトを含めることで、利用者のブラウザでスクリプトが実行され、悪意あるサイトなどへ誘導することが出来てしまいます。

DOM ベースのクロスサイト・スクリプティングにおいては、主に次のような対策を行い、適切に実装することを推奨します。

- **DOM 操作用のメソッドを使用する**
- **出力する内容（HTML なのか JavaScript コードなのか）に応じたエスケープ処理を施す**
- **JavaScript ライブラリの問題の場合は、ライブラリをアップデートする**

ウェブサイト運営者は上記の対策が実施済みであるかをご確認ください。

(*1) HTMLドキュメントやXMLドキュメントをアプリケーションから操作するためのアプリケーションプログラミングインターフェース（API）

2. 2012 年第 4 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

2-1. 脆弱性関連情報の届出状況

～ 脆弱性の届出件数の累計が 8,167 件になりました ～

IPAとJPCERT/CCは「情報セキュリティ早期警戒パートナーシップ (*2)」（以降、本制度）において届出を受け付けています。表 2-1 は 2012 年第 4 四半期のIPAへ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 44 件、ウェブサイト（ウェブアプリケーション）に関するもの 176 件、合計 220 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 1,467 件、ウェブサイトに関するもの 6,700 件、合計 8,167 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。

表 2-1.　届出件数

分類	今期件数	累計件数
ソフトウェア製品	**44** 件	**1,467** 件
ウェブサイト	**176** 件	**6,700** 件
合計	**220** 件	**8,167** 件

図 2-1 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 2-2 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 2012 年第 4 四半期末で 3.95 (*3) 件となっています。

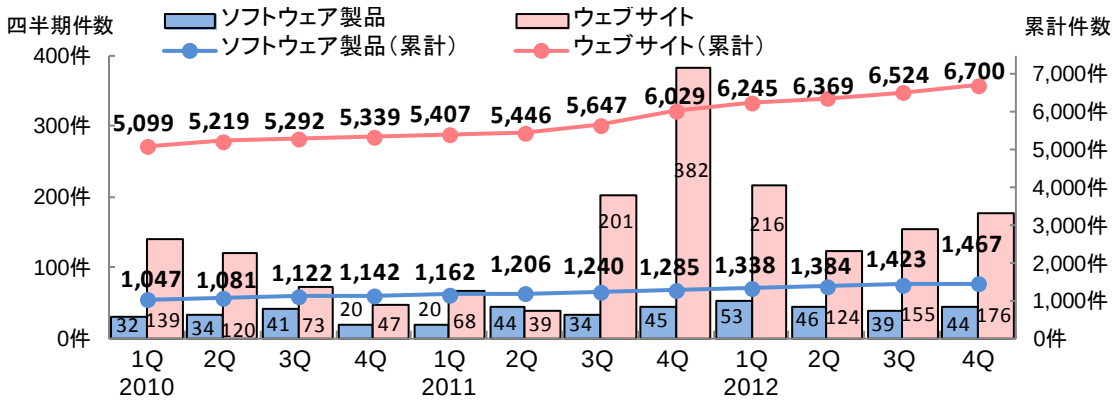


図2－1.脆弱性関連情報の届出件数の四半期別推移

表 2-2. 届出件数（過去 3 年間）

	2010 1Q	2Q	3Q	4Q	2011 1Q	2Q	3Q	4Q	2012 1Q	2Q	3Q	4Q
累計届出件数[件]	6,146	6,300	6,414	6,481	6,569	6,652	6,887	7,314	7,583	7,753	7,947	8,167
1就業日あたり[件/日]	4.40	4.32	4.22	4.10	4.01	3.92	3.91	4.01	4.03	3.99	3.96	3.95

(*2)　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

(*3)　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

2-2. 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 5,200 件を突破しました ～

表 2-3 は 2012 年第 4 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 2-3.　修正完了件数

分類	今期件数	累計件数
ソフトウェア製品	**25** 件	**692** 件
ウェブサイト	**113** 件	**4,549** 件
合計	**138** 件	**5,241** 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、2012 年第 4 四半期にJVNで対策情報を公表したものは 25 件 (*4)（累計 692 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 25 件のうち、届出を受理してから公表までに 45 日以上経過した届出は 18 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、2012 年第 4 四半期に修正を完了したものは 113 件（累計 4,549 件）でした。修正を完了した 113 件を、対策方法により分類すると、ウェブアプリケーションを修正したものが 92 件（81%）、当該ページを削除したものが 21 件（19%）、運用で回避したものが 0 件（0%）でした。なお、修正を完了した 113 件のうち 50 件（44%）は、届出から修正完了まで 90 日以上経過していました。

2-3. 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 (*5)」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 8 件（累計 119 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為に「製品開発者名」に加えて「製品情報（具体的な対象製品の名称およびバージョン）」を公表したものは 0 件（累計 98 件）でした。製品開発者から応答があったのは 3 件 (*6)（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、6 件が本制度における取扱いを終了しました。2012 年第 4 四半期末の公表中件数は、103 件となります。

(*4)　表 3-3 参照

(*5)　連絡不能開発者一覧：http://jvn.jp/reply/index.html

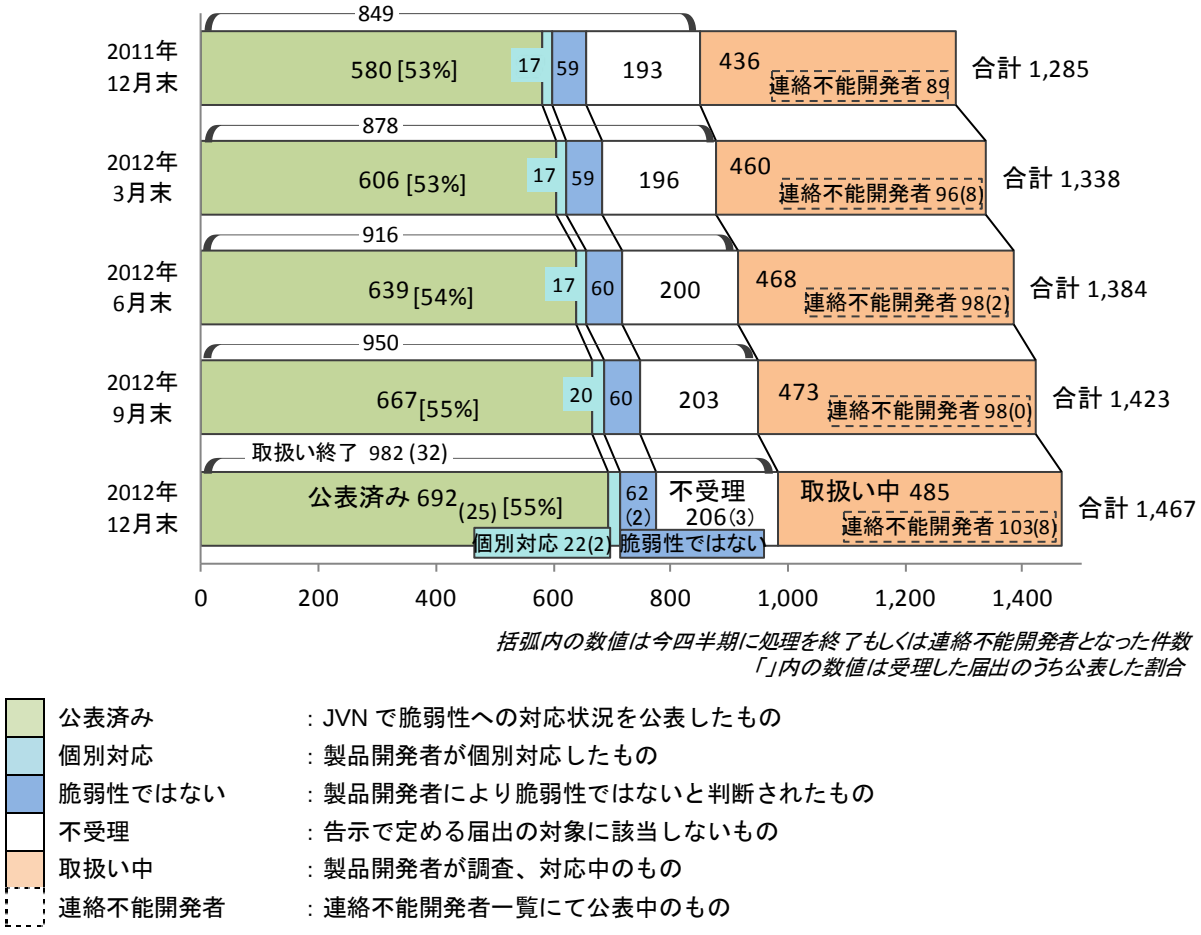
(*6)　2012 年第 3 四半期までに公表した 2 件、今四半期に公表した 1 件について、今四半期に製品開発者から応答がありました。

3. ソフトウェア等の脆弱性に関する届出の処理状況（詳細）

3-1. ソフトウェア製品の脆弱性の処理状況の詳細

3-1-1. ソフトウェア製品の脆弱性の処理状況

図 3-1 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。今四半期に公表した脆弱性は 25 件（累計 692 件）です。また、製品開発者が「個別対応」したものは 2 件（累計 22 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 62 件）、「不受理」としたものは 3 件 (*7)（累計 206 件）、取扱い中は 485 件です。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 (*8) は 8 件です。2012 年 12 月末時点の連絡不能開発者公表数は 103 件になります。



括弧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

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	：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	：連絡不能開発者一覧にて公表中のもの

図 3-1.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

3-1-2. 届出のあった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 IPA に届出のあったソフトウェア製品の脆弱性関連情報 1,467 件のうち、不受理を除いた 1,261 件について、図 3-2 のグラフは製品種類別の届出件数の割合を、図 3-3 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」が増加し、「ウェブブラウザ」が減少しています。

(*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 2 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。

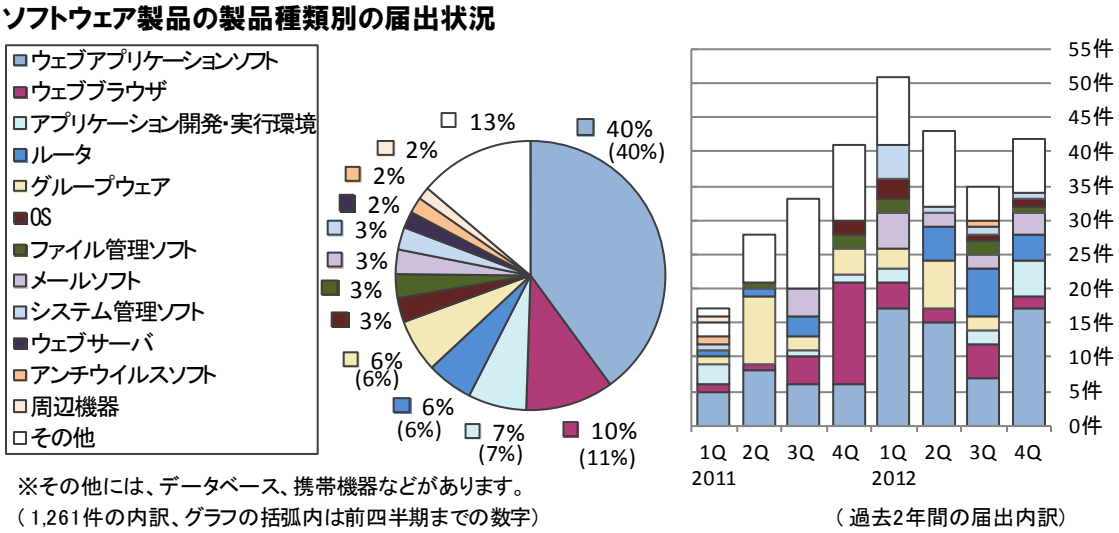


図3-2. 製品種類別の届出件数の割合　**図3-3. 製品種類別の届出件数（四半期別推移）**

届出受付開始から今四半期までに IPA に届出のあったソフトウェア製品の脆弱性関連情報 1,467 件のうち、不受理を除いた 1,261 件について、図 3-4 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 3-5 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約 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の届出が増加しています。

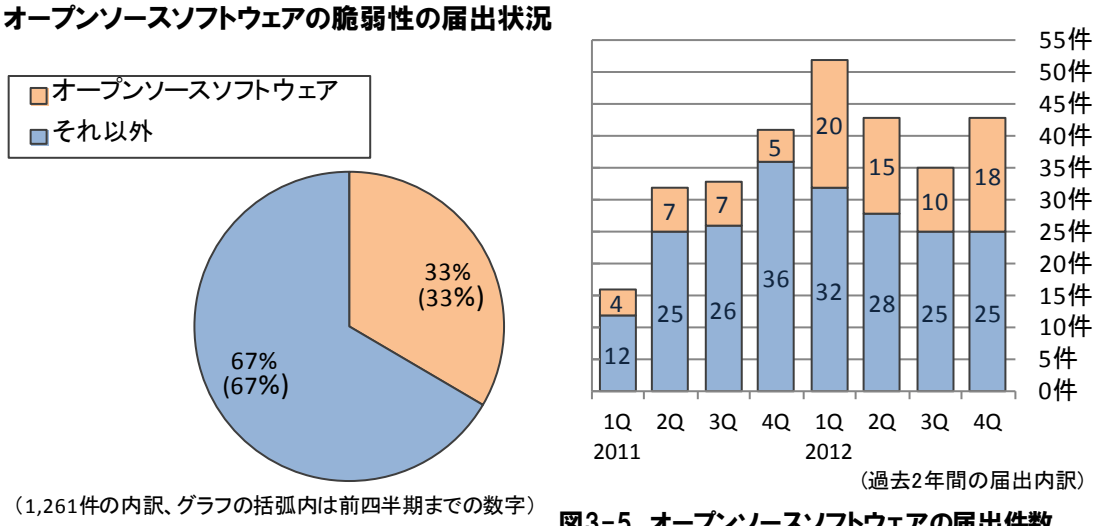


図3-4. オープンソースソフトウェアの届出件数の割合　**図3-5. オープンソースソフトウェアの届出件数（四半期別推移）**

届出受付開始から今四半期までに IPA に届出のあったソフトウェア製品の脆弱性関連情報 1,467 件のうち、不受理を除いた 1,261 件について、図 3-6 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 3-7 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約半数は対策が行われ JVN にて公表されている状況です。

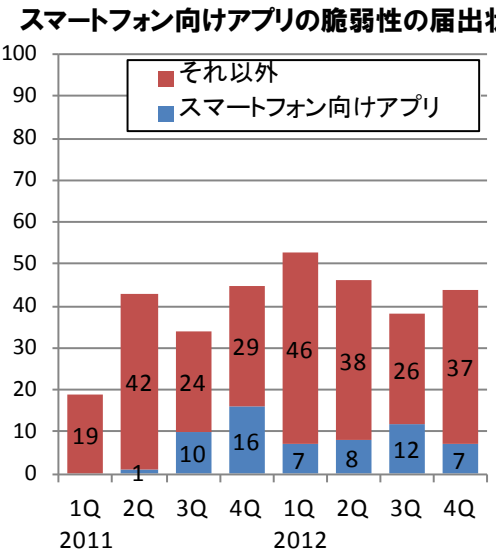


図3-6.スマートフォン向けアプリの届出件数（四半期別推移）

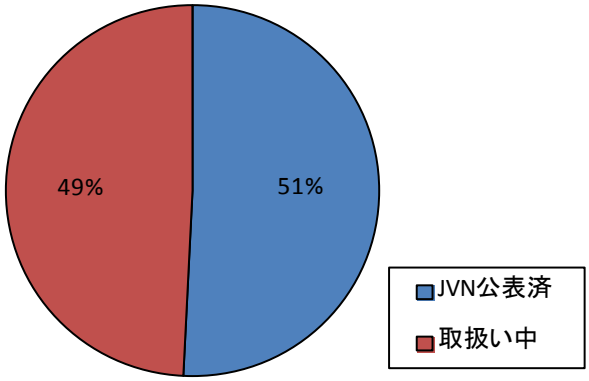


図3-7.スマートフォン向けアプリの処理状況

3-1-3. 脆弱性の原因と脅威

届出受付開始から今四半期までにIPA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 1,467 件のうち、不受理を除いた 1,261 件について、図 3-8 のグラフは原因別 (*9) の届出件数の割合を、図 3-9 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。

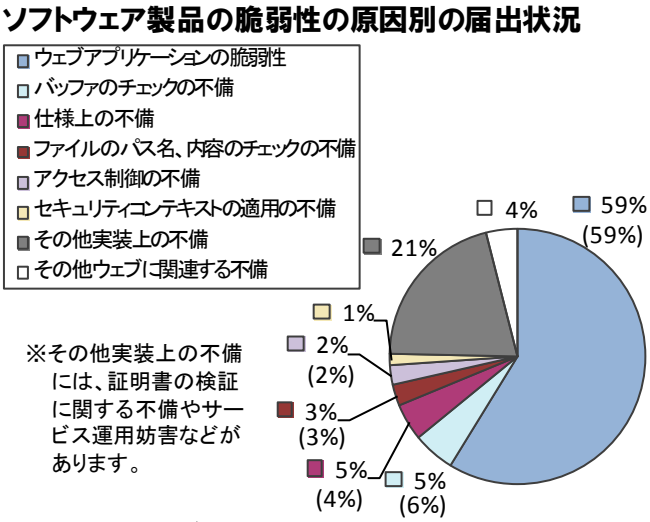


図3-8. 脆弱性の原因別の届出件数の割合

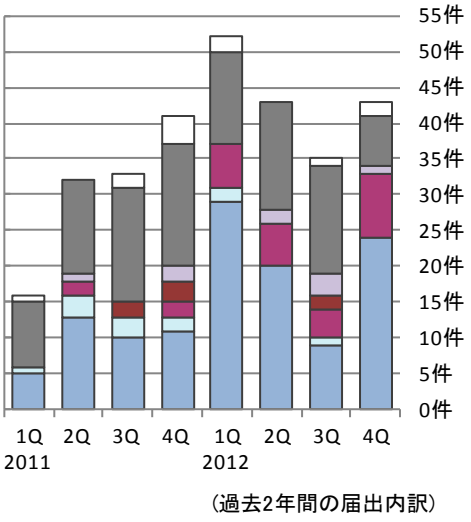
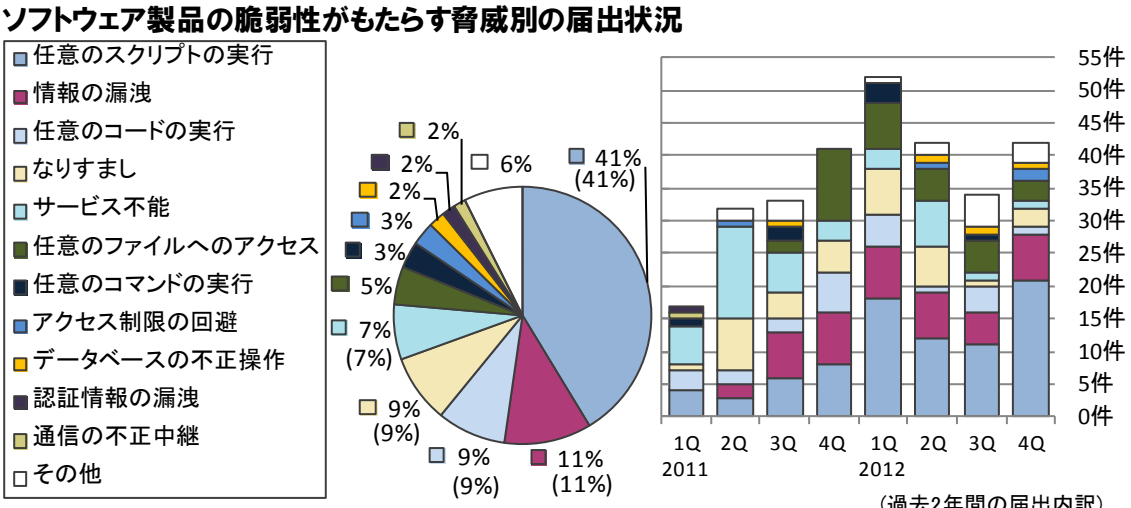


図3-9. 脆弱性の原因別の届出件数（四半期別推移）

届出受付開始から今四半期までに IPA 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 1.467 件のうち、不受理を除いた 1,261 件について、図 3-10 のグラフは脅威別の届出件数の割合を、図 3-11 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。「任意のスクリプトの実行」が届出受付開始から今四半期までの届出のうち約 4 割を占めています。また、今四半期は「任意のスクリプトの実行」と「情報の漏洩」「なりすまし」が増加し、「任意

(*9) 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、回数の累計を計上しています。

のファイルへのアクセス」が前四半期よりも減少しています。



(1,261件の内訳、グラフの括弧内は前四半期までの数字)

図3-10. 脆弱性がもたらす脅威別の届出件数の割合

図3-11. 脆弱性がもたらす脅威別の届出件数(四半期別推移)

3-1-4. ソフトウェア製品の脆弱性情報の調整および公表状況

表 3-1 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(*10)。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 3-12 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 1,497 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 3-1. 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 IPA に届出があったもの、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	25 件	692 件
②	海外 CSIRT 等と連携して公表したもの	43 件	873 件
	合計	68 件	1,565 件

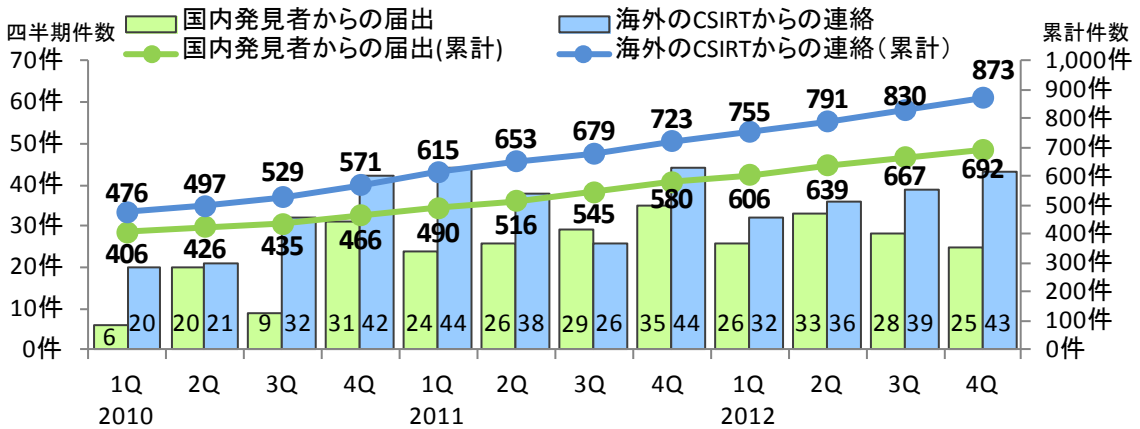


図3-12. ソフトウェア製品の脆弱性対策情報の公表件数

(*10) JPCERT/CC 活動概要 Page15~22（http://www.jpcert.or.jp/pr/2013/PR20130110.pdf）を参照下さい。

（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 3-1 の①）について、図 3-13 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 3-2 は過去 3 年間における 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 2012 年第 4 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。

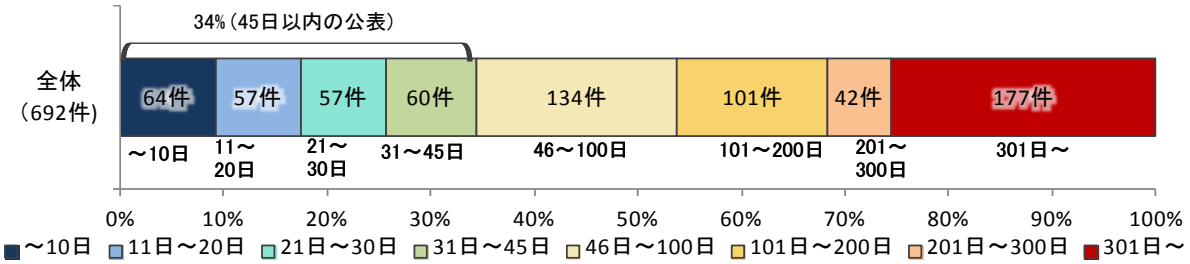


図3-13. ソフトウェア製品の脆弱性公表日数

表 3-2.　45 日以内に公表した件数の割合推移（四半期別）

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

表 3-3 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 11 件（表 3-3 の*1）、複数開発者・製品に影響がある脆弱性が 2 件（表 3-3 の*2）、組込みソフトウェア製品の脆弱性が 2 件（表 3-3 の*3）ありました。

表 3-3. 2012 年第 4 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）	複数の京セラ製携帯端末におけるメール受信時に再起動する問題	京セラ株式会社の提供する複数の携帯端末には、メール受信時の処理に問題がありました。このため、第三者により携帯端末を再起動される可能性がありました。	2012 年 11 月 30 日	7.8
脆弱性の深刻度=レベル II（警告）、CVSS 基本値=4.0～6.9				
2	「MyWebSearch」におけるクロスサイト・スクリプティングの脆弱性	サイト内検索ソフト「MyWebSearch」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。	2012 年 10 月 5 日	4.3
3（*1）	「Smarty」におけるクロスサイト・スクリプティングの脆弱性	PHP 用のテンプレートエンジン「Smarty」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。	2012 年 10 月 10 日	4.3
4	「Safari」においてリモートからローカルファイルを読み取り可能な脆弱性	ウェブブラウザ「Safari」には、リモートからローカルファイルを読み取り可能な脆弱性がありました。これにより、第三者により利用者のコンピュータ内のファイルを取得される可能性がありました。	2012 年 10 月 23 日	4.3
5	「東京 BBS」におけるクロスサイト・スクリプティングの脆弱性	掲示板ソフトウェア「東京 BBS」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。	2012 年 10 月 26 日	4.3
6	Mac OS X の「OpenSSH」におけるサービス運用妨害 (DoS) の脆弱性	Mac OS X に同梱の SSH プロトコル利用ソフト「OpenSSH」には、パケットの受信する処理に問題がありました。このため、第三者により応答不能状態になる可能性がありました。	2012 年 10 月 31 日	5.0
7（*1）	「MosP 勤怠管理システム」におけるアクセス制限不備の脆弱性	勤怠管理システム「MosP 勤怠管理システム」には、アクセス制限不備の脆弱性が存在しました。このため、第三者により他のユーザの情報が取得される可能性がありました。	2012 年 11 月 02 日	4.0
8（*1）	「MosP 勤怠管理システム」における認証不備の脆弱性	勤怠管理システム「MosP 勤怠管理システム」には、認証不備の脆弱性が存在しました。このため、第三者により他のユーザになりすまされる可能性がありました。	2012 年 11 月 02 日	6.5
9（*1）	「Pebble」において記事が閲覧不能になる脆弱性	コンテンツ管理システム「Pebble」には、コメント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記事が閲覧不能にされる可能性がありました。	2012 年 11 月 02 日	5.0
10（*1）	「Pebble」における HTTP ヘッダ・インジェクションの脆弱性	コンテンツ管理システム「Pebble」には、HTTP ヘッダを出力する際の処理に問題がありました。このため、第三者により偽の情報が表示される可能性や任意のスクリプトが実行されてしまう可能性がありました。	2012 年 11 月 02 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
11 (*1)	「Pebble」におけるオープンリダイレクトの脆弱性	コンテンツ管理システム「Pebble」には、オープンリダイレクトの脆弱性が存在しました。このため、第三者により任意のウェブサイトにリダイレクトされる可能性がありした。	2012 年 11 月 02 日	4.3
12	「BeZIP 日本語対応版」におけるディレクトリ・トラバーサルの脆弱性	圧縮・展開ソフト「BeZIP 日本語対応版」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、第三者により任意のファイルが作成されたり、既存のファイルが書き換えられたりする可能性がありました。	2012 年 11 月 7 日	4.3
13 (*2) (*3)	Android OS を搭載した複数の端末におけるサービス運用妨害 (DoS) の脆弱性	Android OS を搭載した複数の端末は、特定のシステム領域を参照する際の処理に問題がありました。このため、第三者により当該製品が強制終了させられる可能性があります。	2012 年 11 月 14 日	5.4
14 (*1)	「BIGACE」におけるセッション固定の脆弱性	コンテンツ管理システム「BIGACE」には、セッション固定の脆弱性がありました。このため、第三者により登録ユーザになりすまされる可能性がありました。	2012 年 11 月 21 日	5.8
15	KENT-WEB 製「ACCESS REPORT」におけるクロスサイト・スクリプティングの脆弱性	アクセス解析ソフト「ACCESS REPORT」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上にスクリプトを埋め込まれる可能性がありました。項番 16 とは異なる問題です。	2012 年 12 月 6 日	5.0
16	KENT-WEB 製「ACCESS REPORT」におけるクロスサイト・スクリプティングの脆弱性	アクセス解析ソフト「ACCESS REPORT」には、クロスサイト・スクリプティングの問題がありました。このため、第三者によりウェブページ上にスクリプトを埋め込まれる可能性がありました。項番 15 とは異なる問題です。	2012 年 12 月 6 日	4.3
17 (*1)	「Welcart」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プラグイン「Welcart」には、ウェブページを出力する際の処理に問題がありました。このため、第三者によりウェブページ上にスクリプトを埋め込まれる可能性がありました。	2012 年 12 月 14 日	5.0
18 (*1)	「WikkaWiki」におけるクロスサイト・スクリプティングの脆弱性	Wiki 構築ソフト「WikkaWiki」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上にスクリプトを埋め込まれる可能性がありました。	2012 年 12 月 17 日	4.3
19	Android 版「Opera Mini ウェブブラウザ」および「Opera Mobile ウェブブラウザ」において任意のスクリプトが実行される脆弱性	ウェブブラウザ「Opera Mini ウェブブラウザ」および「Opera Mobile ウェブブラウザ」には、不正なスクリプトが実行される問題がありました。このため、第三者により指定されたウェブサイトの Cookie 情報を窃取される可能性がありました。	2012 年 12 月 20 日	4.0
脆弱性の深刻度=レベル I（注意）、CVSS 基本値=0.0～3.9				
20	「Android 版 Monaca デバッガー」における情報管理不備の脆弱性	デバッグアプリ「Android 版 Monaca デバッガー」には、情報管理不備の脆弱性がありました。このため、第三者によりアカウント情報やセッション ID 等の情報を取得される可能性がありました。	2012 年 11 月 16 日	2.6
21 (*1)	「Welcart」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	ショッピングサイト構築プラグイン「Welcart」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、第三者により購入手続きを終了される可能性がありました。	2012 年 12 月 14 日	2.6

項番	脆弱性	セキュリティ上の問題点	JVN 公表日	CVSS 基本値
22	「Boat Browser」および「Boat Browser Mini」における WebView クラスに関する脆弱性	ウェブブラウザ「Boat Browser」および「Boat Browser Mini」には、WebView クラス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のデータ領域にある情報が窃取される可能性がありました。	2012 年 12 月 20 日	2.6
23 (*1)	「concrete5」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「concrete5」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上にスクリプトを埋め込まれる可能性がありました。	2012 年 12 月 21 日	2.6
24	Android 版「ロケタッチ」における暗黙的 Intent の扱いに関する脆弱性	位置情報取得アプリ「ロケタッチ」には、暗黙的 Intent の扱いに関する問題がありました。このため、第三者により非公開の予定とするものを含めた位置情報を窃取される可能性がありました。	2012 年 12 月 21 日	2.6
25	Android 版「ロケタッチ」における情報管理不備の脆弱性	位置情報取得アプリ「ロケタッチ」には、ログ保存に関連する情報管理に問題がありました。このため、第三者により非公開の予定とするものを含めた位置情報を窃取される可能性がありました。	2012 年 12 月 21 日	2.6

（*1）：オープンソースソフトウェア製品の脆弱性
（*2）：複数開発者・製品に影響がある脆弱性
（*3）：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 3-4、表 3-5 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 43 件あり、うち表 3-4 には通常の脆弱性情報 40 件、表 3-5 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 3-4.米国CERT/CC [*11] 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	Cerberus FTP Server 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
2	複数のネットワークカメラに認証回避の脆弱性	注意喚起として掲載
3	ZENworks Asset Management に情報漏えいの脆弱性	注意喚起として掲載
4	OTRS 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
5	Mutiny にコマンドインジェクションの脆弱性	注意喚起として掲載
6	Adobe Shockwave Player に複数の脆弱性	注意喚起として掲載
7	複数の Broadcom 製無線チップセットにサービス運用妨害 (DoS) の脆弱性	複数製品開発者へ通知
8	複数の DomainKeys Identified Mail (DKIM) 実装に問題	注意喚起として掲載
9	HP/H3C 製および Huawei 製ネットワーク機器にアクセス制限不備の脆弱性	注意喚起として掲載
10	TomatoCart の PayPal Express Checkout モジュールに検証不備の脆弱性	注意喚起として掲載
11	CA ARCserve Backup において任意のコードが実行可能な脆弱性	注意喚起として掲載 特定製品開発者へ通知
12	CA ARCserve Backup にサービス運用妨害 (DoS) の脆弱性	注意喚起として掲載 特定製品開発者へ通知
13	Axigen Free Mail Server 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
14	Orion IPAM 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
15	Pattern Insight 製品に複数の脆弱性	注意喚起として掲載
16	FortiGate Unified Threat Management (UTM) の CA 証明書の取扱いに問題	注意喚起として掲載
17	複数の Symantec 製品に脆弱性	注意喚起として掲載 特定製品開発者へ通知
18	Sophos Antivirus に複数の脆弱性	注意喚起として掲載
19	VeriCentre に SQL インジェクションの脆弱性	注意喚起として掲載
20	FleetCommander に複数の脆弱性	注意喚起として掲載
21	Oberthur のスマートカードに問題	注意喚起として掲載
22	ArcGIS Server に SQL インジェクションの脆弱性	注意喚起として掲載
23	Vanilla Forums にアクセス制限不備の脆弱性	注意喚起として掲載
24	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 特定製品開発者へ通知
25	Novell File Reporter に複数の脆弱性	注意喚起として掲載
26	Autonomy Keyview IDOL ライブラリに複数の脆弱性	注意喚起として掲載
27	Samsung 製プリンタに SNMP コミュニティ文字列がハードコードされている問題	注意喚起として掲載 特定製品開発者へ通知

[*11] 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
28	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
29	Apple Safari における複数の脆弱性に対するアップデート	注意喚起として掲載
30	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
31	ManageEngine AssetExplorer 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
32	Qualcomm 製デバイスドライバを搭載した Android 端末に複数の脆弱性	注意喚起として掲載 複数製品開発者へ通知
33	D-Link DSL-2730u に OS コマンドインジェクションの脆弱性	注意喚起として掲載
34	IBM POWER5 のサービス・プロセッサーに権限昇格の脆弱性	注意喚起として掲載
35	Centreon にブラインド SQL インジェクションの脆弱性	注意喚起として掲載
36	Huawei E585 Pocket WiFi 2 に複数の脆弱性	注意喚起として掲載 複数製品開発者へ通知
37	Adobe Shockwave Player における Shockwave ランタイムのインストールに関する問題	注意喚起として掲載
38	Adobe Shockwave Player に旧バージョンの Flash ランタイムが同梱されている問題	注意喚起として掲載
39	Adobe Shockwave Player におけるプラグインモジュールのインストールに関する問題	注意喚起として掲載
40	Internet Explorer に任意のコードが実行される脆弱性	緊急案件として掲載 特定製品開発者へ通知

表 3-5.米国US-CERT [*12] 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	Microsoft 製品における複数の脆弱性に対するアップデート
3	Microsoft 製品における複数の脆弱性に対するアップデート

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

3-1-5. 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 3-14 は 2012 年第 4 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 2012 年第 3 四半期までで 111 件、今四半期に 8 件を公表し、合計 119 (*13) 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、2012 年第 4 四半期に「製品情報（具体的な対象製品の名称およびバージョン）」を公表した届出はありません。

（2） 製品開発者情報の公開調査結果

図 3-15 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。2012 年第 4 四半期は 3 件 (*14) の製品開発者から応答がありました。2012 年 12 月 28 日時点の公表中件数は、103 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 2012 年 12 月 31 日時点までに 16 件が調整を再開し、そのうち 6 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、2012 年 12 月 31 日時点で 103 件は依然として、製品開発者からの連絡が無い状況です。

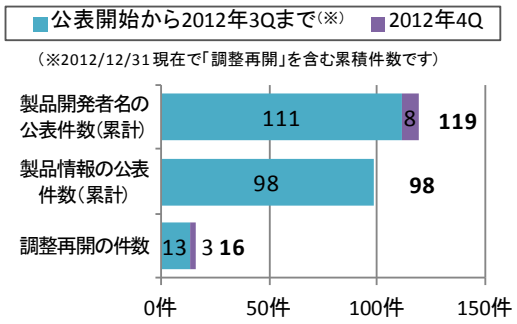


図3-14. 2012年4Qの公表および調整再開の状況

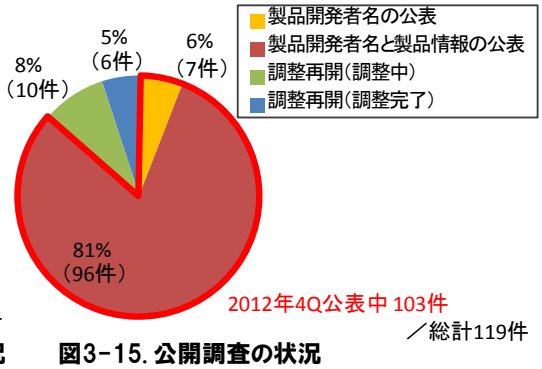


図3-15. 公開調査の状況

(*13) 過去に連絡不能開発者一覧に公表され、調整を再開し、再度連絡不能となったものは個別に計上しています。
(*14) 前四半期までに公表した 2 件および今四半期に公表した 1 件です。

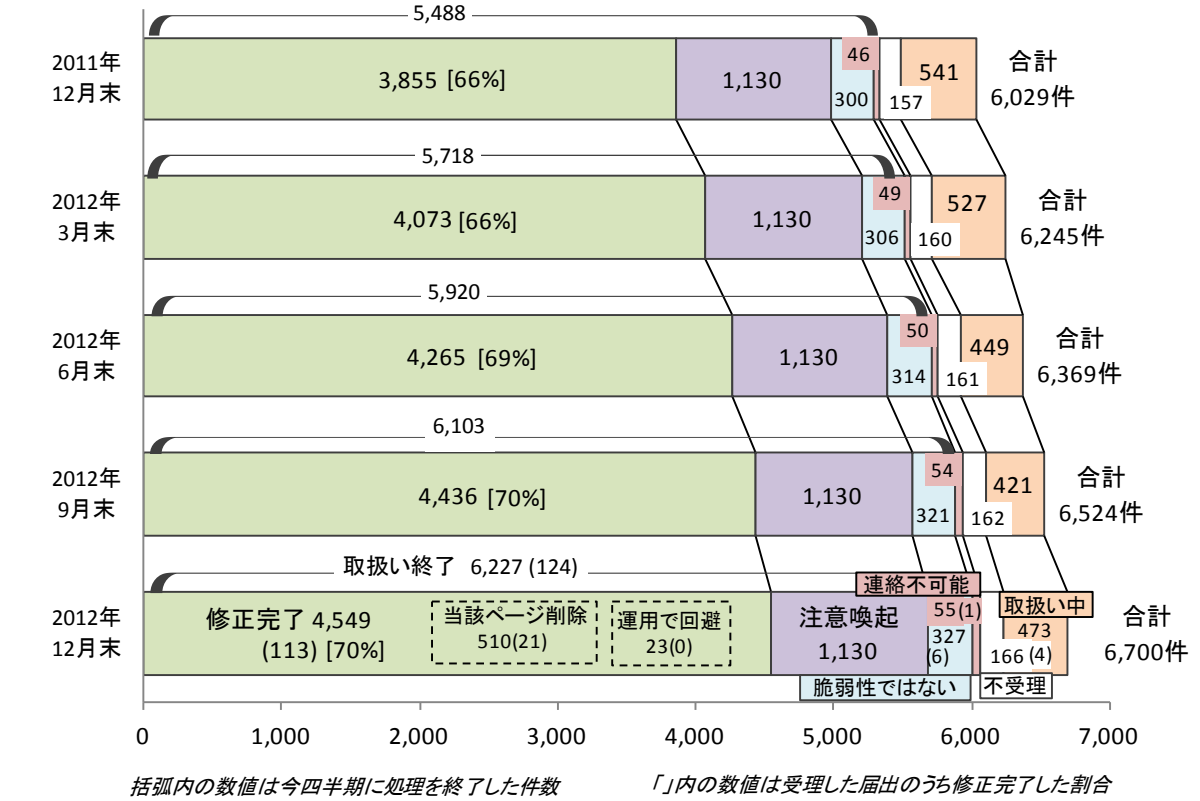
3-2. ウェブサイトの脆弱性の処理状況

3-2-1. ウェブサイトの脆弱性の処理状況

図 3-16 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 176 件（累計 6,227 件）でした。このうち「修正完了」したものは 113 件（累計 4,549 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 6 件（累計 327 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」なものは 1 件（累計 55 件）です。「不受理」としたものは 4 件（累計 166 件）でした。

取扱いを終了した累計 6,227 件のうち「注意喚起」「連絡不可能」「不受理」を除く累計 4,876 件（78%）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 21 件（累計 510 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。



括弧内の数値は今四半期に処理を終了した件数　　*「」内の数値は受理した届出のうち修正完了した割合*

①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
②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
③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
④連絡不可能	：	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
⑤不受理	：	告示で定める届出の対象に該当しないもの
⑥取扱い中	：	ウェブサイト運営者が調査、対応中のもの

図 3-16.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

3-2-2. ウェブサイトの運営主体の種類

図 3-17 のグラフは過去 2 年間に IPA 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。今四半期も企業が多く届出されています。

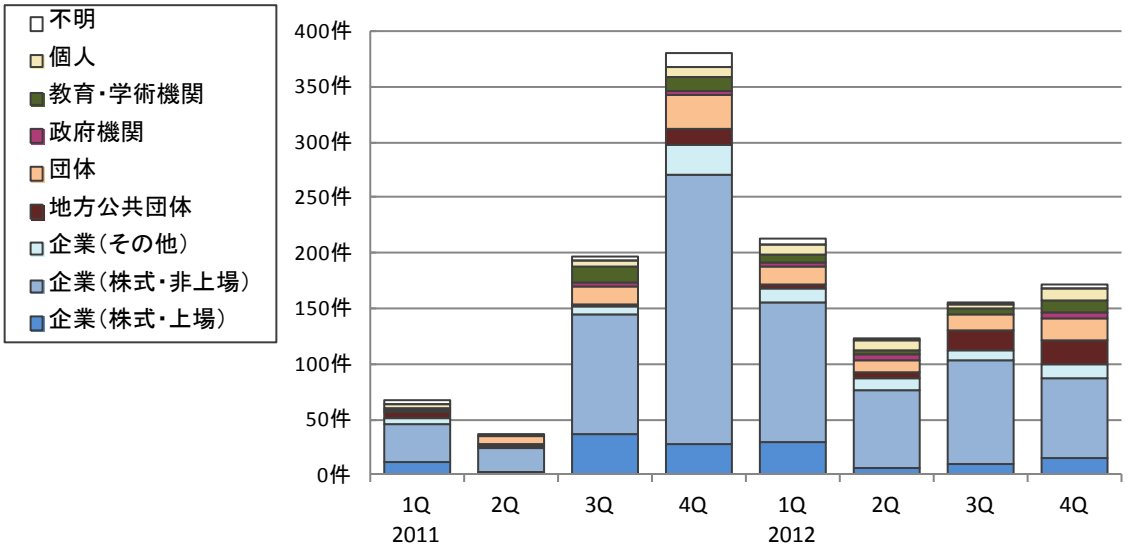
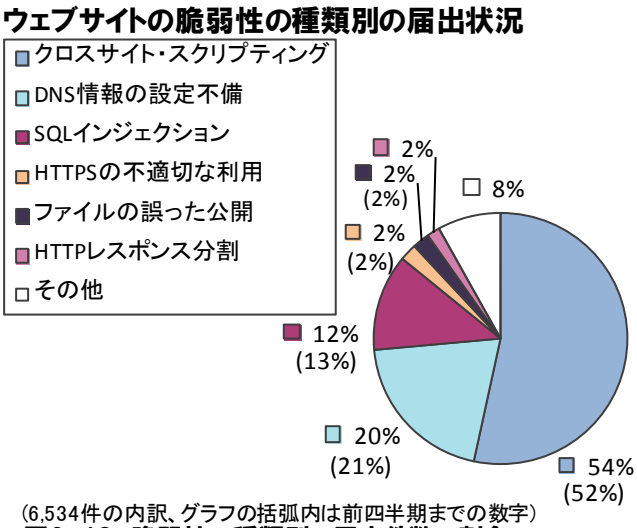


図3−17. ウェブサイトの運営主体の種類別の届出件数（四半期別推移）

3-2-3. ウェブサイトの脆弱性の種類と脅威

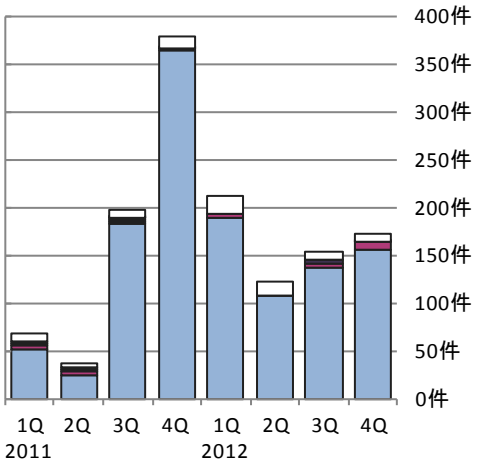
届出受付開始から今四半期までにIPAに届出のあったウェブサイトの脆弱性関連情報 6,700 件のうち、不受理を除いた 6,534 件について、図 3-18 のグラフは脆弱性の種類別の届出件数の割合を、図 3-19 は過去 2 年間の脆弱性の種類別届出件数の四半期別推移をそれぞれ示したものです[*15]。脆弱性の種類は届出の多い「クロスサイト・スクリプティング」「DNS情報の設定不備」「SQLインジェクション」の 3 種類の脆弱性が全体の 86%を占めています。2008 年第 3 四半期から 2009 年第 3 四半期にかけて多く届出のあった「DNS情報の設定不備」は、2009 年第 4 四半期以降は届出がありません。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 70%以上を占めています。しかし、この統計はあくまでIPAに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。

[*15] 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。



(6,534件の内訳、グラフの括弧内は前四半期までの数字)

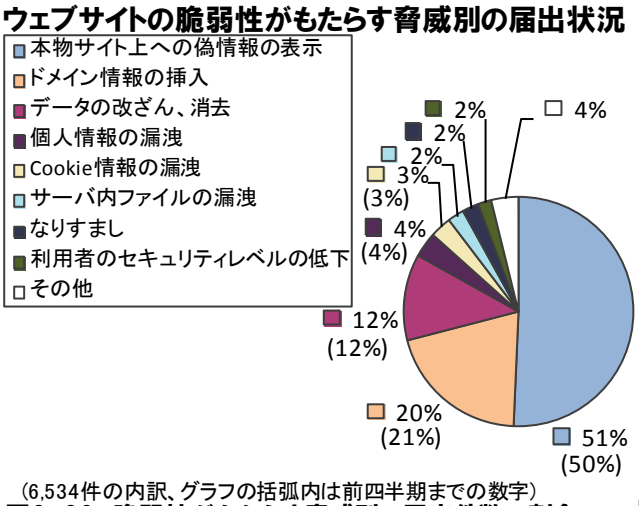
図3-18. 脆弱性の種類別の届出件数の割合



(過去2年間の届出内訳)

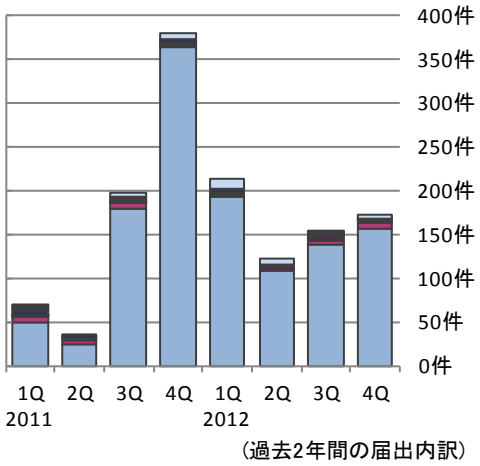
図3-19. 脆弱性の種類別の届出件数
(四半期別推移)

届出受付開始から今四半期までに IPA に届出のあったウェブサイトの脆弱性関連情報 6,700 件のうち、不受理を除いた 6,534 件について、図 3-20 のグラフは脅威別の届出件数の割合を、図 3-21 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。



(6,534件の内訳、グラフの括弧内は前四半期までの数字)

図3-20. 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3-21. 脆弱性がもたらす脅威別の届出件数
(四半期別推移)

3-2-4. ウェブサイトの脆弱性の修正完了状況

図 3-22 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 3-6 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（7 割弱程度）に大きな変動はありません。

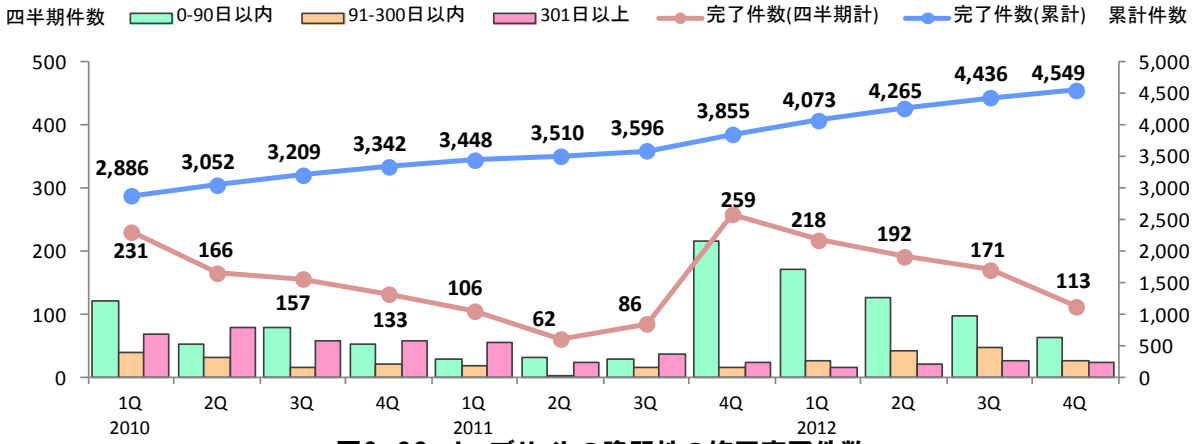


図3-22. ウェブサイトの脆弱性の修正完了件数

表 3-6. 90 日以内に修正完了した件数および割合の推移

	2010 1Q	2Q	3Q	4Q	2011 1Q	2Q	3Q	4Q	2012 1Q	2Q	3Q	4Q
修正完了件数	2,886	3,052	3,209	3,342	3,448	3,510	3,596	3,855	4,073	4,265	4,436	4,549
90 日以内の件数	2,028	2,082	2,163	2,216	2,247	2,280	2,311	2,528	2,700	2,825	2,924	2,987
90 日以内の割合	70%	68%	67%	66%	65%	65%	64%	66%	66%	66%	66%	66%

図 3-23 および図 3-24 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[(*16)]。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。

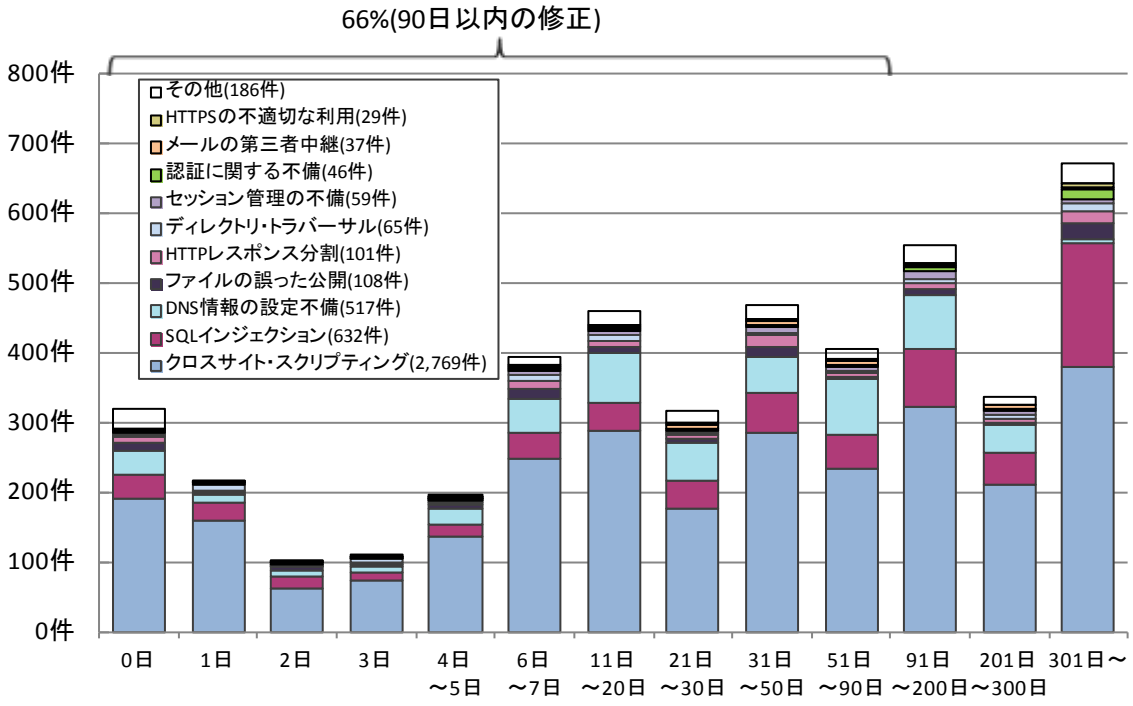


図3-23.ウェブサイトの修正に要した日数

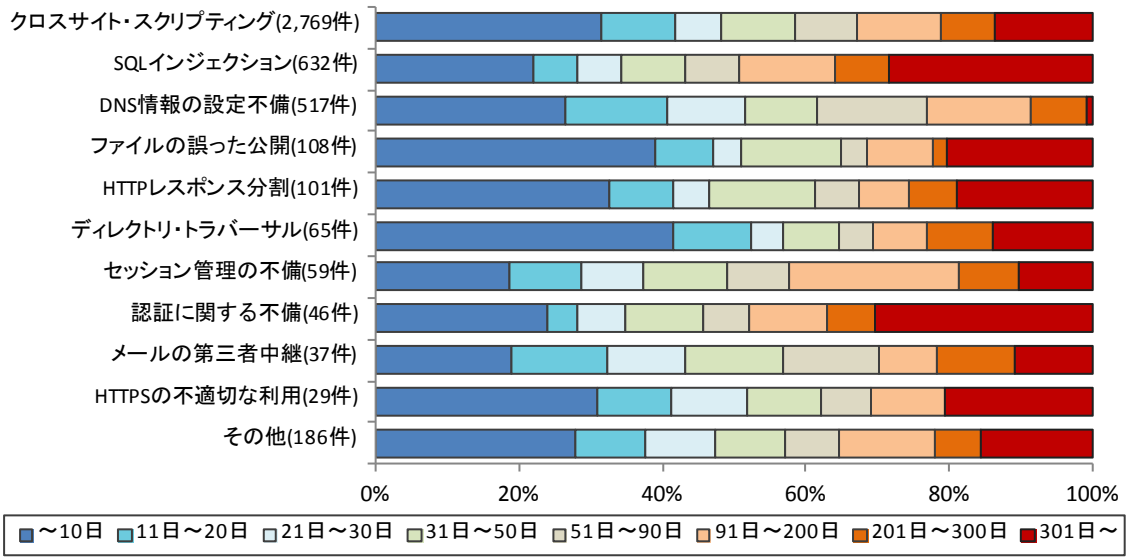


図3-24.ウェブサイトの修正に要した脆弱性種類別の日数の傾向

(*16) 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。

3-2-5. ウェブサイトの脆弱性の取扱中の状況

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 3-25 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 53 件、200 日から 299 日のものは 36 件など、これらの合計は 296 件（前四半期は 302 件）です。前四半期末までの取扱い長期化 302 件のうち今四半期に 48 件が取扱い終了となった一方、新たに 42 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 6 件減少しました。

表 3-7 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、200 日から 299 日に達したもの、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 8 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。

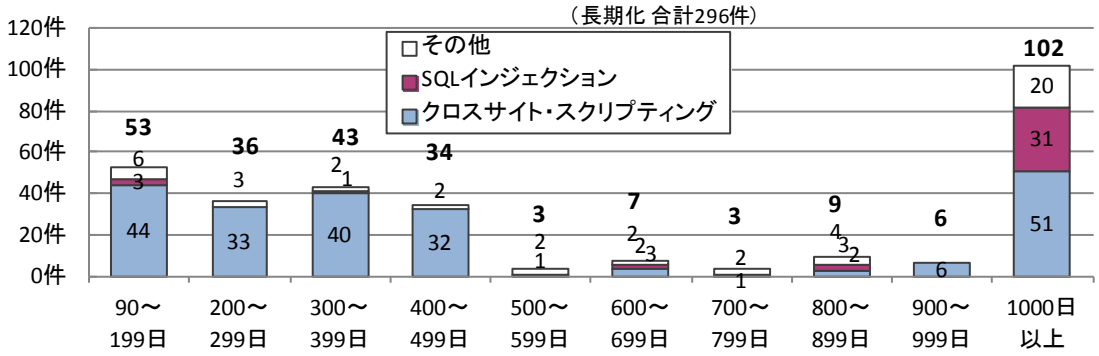


図3-25.取扱いが長期化（90日以上経過）しているウェブサイトの経過日数と脆弱性の種類

表 3-7. 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 1Q	2Q	3Q	4Q	2012 1Q	2Q	3Q	4Q
取扱い中件数	388 件	344 件	435 件	541 件	527 件	449 件	423 件	473 件
長期化している件数	309 件	289 件	228 件	237 件	298 件	318 件	302 件	296 件
長期化している割合	80%	84%	53%	44%	57%	71%	71%	63%

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修正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。

4. 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。

4-1. 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

4-2. 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

4-3. 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。

4-4. 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

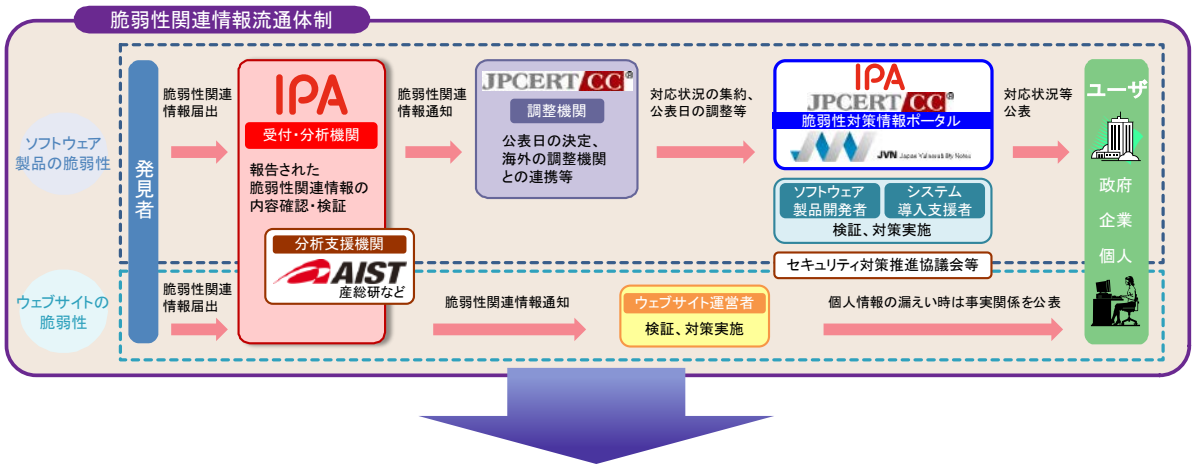
付表 2. ウェブサイト脆弱性の分類

	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