ソフトウェア等の脆弱性関連情報の取扱いに関する活動報告レポート

[2014 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の取扱いに関する活動報告レポートについて

脆弱性関連情報の取扱いに関する活動は、ソフトウェア等脆弱性関連情報取扱基準（2004 年経済産業省告示第 235 号改め、2014 年経済産業省告示第 110 号）に基づき、関係者による情報セキュリティ早期警戒パートナーシップの枠組みの中で、脆弱性関連情報取扱制度（本報告書では本制度と記します）が 2004 年 7 月より運用されています。本制度において、独立行政法人情報処理推進機構（以下、IPA）と一般社団法人 JPCERT コーディネーションセンター（以下、JPCERT/CC）は、脆弱性関連情報の届出の受付や調整などの業務を実施しています。

本レポートでは、2014 年 10 月 1 日から 2014 年 12 月 31 日までの間に実施した、脆弱性関連情報の取扱いに関する活動及び脆弱性の傾向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
2015 年 1 月 28 日

目次

1. 2014 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受付状況

1-1. 脆弱性関連情報の届出受付状況

～ 脆弱性の届出件数の累計が 10,655 件になりました ～

表 1-1 は本制度[*1]における届出状況について、2014 年第 4 四半期の脆弱性関連情報（以降「脆弱性」）の届出件数および届出受付開始（2004 年 7 月 8 日）から今四半期までの累計を示しています。今期のソフトウェア製品に関する届出件数は 86 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 392 件、合計 478 件でした。届出受付開始からの累計は 10,655 件で、内訳はソフトウェア製品に関するもの 1,952 件、ウェブサイトに関するもの 8,703 件でウェブサイトに関する届出が全体の 82%を占めています。

表 1-1. 届出件数

分類	今期件数	累計
ソフトウェア製品	**86** 件	**1,952** 件
ウェブサイト	**392** 件	**8,703** 件
合計	**478** 件	**10,655** 件

図 1-1 のグラフは過去 3 年間の届出件数の四半期ごとの推移を示したものです。今四半期は、ソフトウェア製品に関する届出が前四半期の約 2 倍、ウェブサイトに関する届出が過去 3 年間で最多となりました。表 1-2 は過去 3 年間の四半期ごとの届出の累計および 1 就業日あたりの届出件数の推移です。今四半期の 1 就業日あたりの届出件数は 4.17 [*2] 件でした。

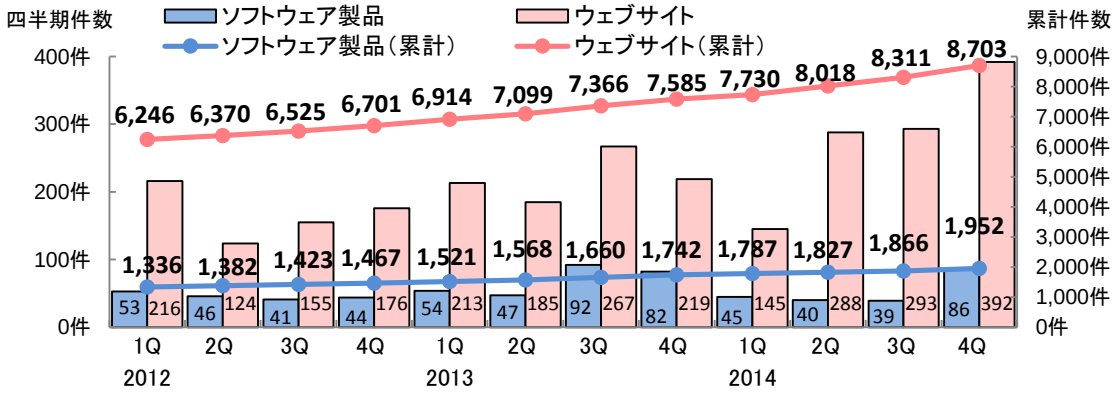


図1−1. 脆弱性の届出件数の四半期ごとの推移

表 1-2. 届出件数（過去 3 年間）

	2012 1Q	2Q	3Q	4Q	2013 1Q	2Q	3Q	4Q	2014 1Q	2Q	3Q	4Q
累計届出件数[件]	7,582	7,752	7,948	8,168	8,435	8,667	9,026	9,327	9,517	9,845	10,177	10,655
1 就業日あたり[件/日]	4.05	4.00	3.98	3.78	3.96	3.96	4.00	4.03	4.01	4.04	4.07	4.17

[*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

また、図 1-2 は、届出受付開始から 2014 年 12 月末までの届出件数の年ごとの推移です。過去、最も届出が多かったのは、2008 年（2,625 件）です。2014 年はソフトウェア製品が 210 件、ウェブサイトが 1,118 件の合計 1,328 件でした。**2010 年以降、届出件数は年々増加しており、2014 年は届出件数が届出受付開始以来 3 番目に多い年となりました。**

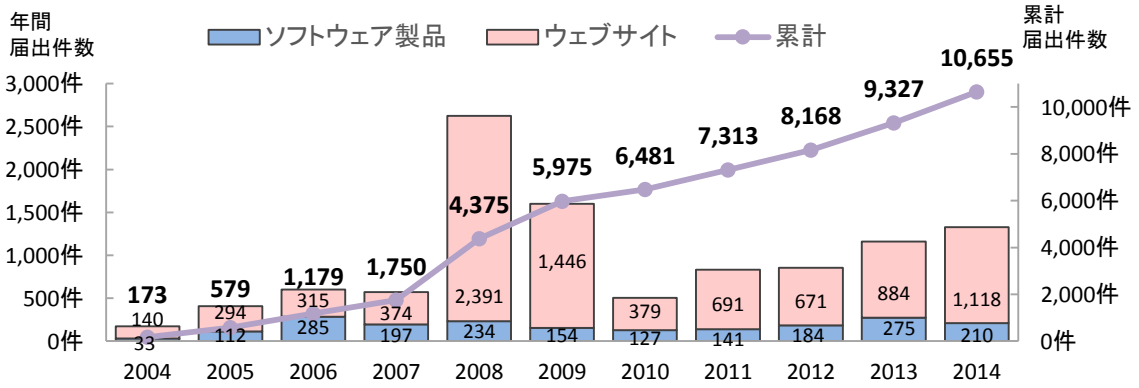


図1−2. 脆弱性関連情報の届出件数の年ごとの推移

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 6,900 件になりました～

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
ソフトウェア製品	**34** 件	**959** 件
ウェブサイト	**163** 件	**5,941** 件
合計	**197** 件	**6,900** 件

ソフトウェア製品の脆弱性の届出のうち、今四半期に脆弱性対策情報を JVN で公表した件数（回避策等の公表も修正完了とみなす）は 34 件 (*3)（累計 959 件）でした。そのうち、4 件が製品開発者による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 JVN 公表までの日数が 45 日 (*4) 以内だったのは 7 件（21%）でした。

ウェブサイトの脆弱性の届出のうち、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 163 件（累計 5,941 件）でした。修正を完了した 163 件のうち、ウェブアプリケーションを修正したものは 114 件（70%）、当該ページを削除したものは 49 件（30%）、運用で回避したものは 0 件でした。なお、修正を完了した 163 件のうちウェブサイト運営者へ脆弱関連情報を通知してから 90 日 (*5) 以内に修正が完了したのは 110 件（67%）でした。今四半期は、90 日以内に修正完了した割合が、前四半期（183 件中 142 件（78%））より減少しています。

(*3) P.12 表 2-3 参照
(*4) JVN 公表日の目安は、脆弱性の取扱いを開始した日時から起算して 45 日後としています。
(*5) 対処の目安は、ウェブサイト運営者が脆弱性の通知を受けてから、3 ヶ月以内としています。

また、図 1-3 は、届出開始から 2014 年 12 月末までの修正完了件数の年ごとの推移を示しています。過去、修正を完了した件数が最も多かったのは 2009 年の 1,401 件でした。2014 年は、ソフトウェア製品が 140 件、ウェブサイトが 633 件の合計 773 件でした。**2014 年はソフトウェア製品の修正が、最も多く完了した年となりました。これは、本制度が開始してから 10 年が経過し、「製品開発者の脆弱性に対する理解が浸透してきた」ためと考えられます。**

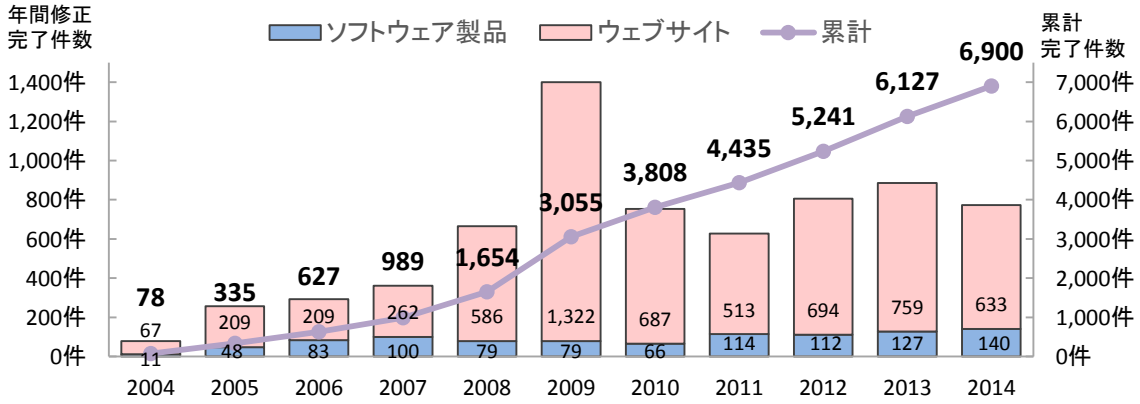


図1-3. 脆弱性関連情報の修正完了件数の年ごとの推移

1-3. 連絡不能案件の取扱状況

本制度では、連絡が取れない製品開発者を「連絡不能開発者」と呼び、連絡の糸口を得るため、まず最初に当該製品開発者名等を公表しています (*6)。製品開発者名を公表後、3 ヵ月経過しても製品開発者から応答が得られない場合は、その後製品情報（対象製品の具体的な名称およびバージョン）を公表します。それでも応答が得られない場合は、情報提供の期限を追記します。情報提供の期限までに製品開発者から応答がない場合は、当該脆弱性情報の公表に向け、「情報セキュリティ早期警戒パートナーシップガイドライン」に定められた公開条件を満たしているかを公表判定委員会 (*7) で審議します。公表が適当と判定された脆弱性情報は JVN に公表されます。

今四半期に新たに製品開発者名を公表したものは 12 件、製品開発者名に加え製品情報を追加公表したものは 8 件、2014 年 12 月末時点の連絡不能開発者の累計公表件数は 163 件となりました。また、2014 年 11 月に第 1 回目の公表判定委員会を開催し、4 件の脆弱性情報について審議しました。

(*6) 連絡不能開発者一覧：http://jvn.jp/reply/index.html
(*7) 連絡不能案件の脆弱性情報を公表するか否かを判定するために IPA が組織する。法律、情報セキュリティ、当該ソフトウェア製品分野の専門的な知識経験を有する専門家、かつ、当該案件と利害関係のない者で構成される。

1-4. 脆弱性の傾向について

ウェブサイトに潜むディレクトリ・トラバーサルの脆弱性の見つけ方に注意

～安全な手順、手法による脆弱性の発見を～

2014 年第 4 四半期には、ウェブサイト及びソフトウェア製品の届出は合計 478 件ありました。そのうちの約 30%を占めるのは、「ディレクトリ・トラバーサル」に関する脆弱性でした（図 1-4）。

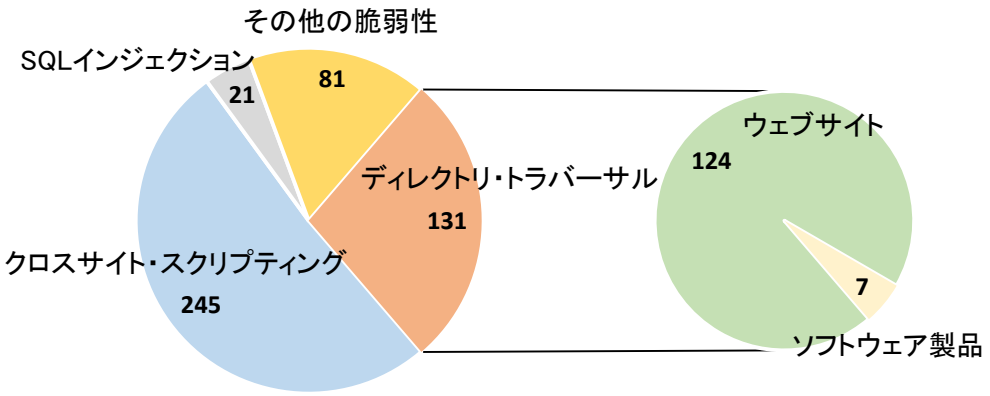


図1-4. 届出に対するディレクトリ・トラバーサルの届出の割合

「ディレクトリ・トラバーサル」の脆弱性とは

この脆弱性がウェブサイトに存在すると、悪意のある第三者に非公開のファイルにアクセスされてしまうなどのセキュリティ上の問題が生じます。詳細は次のとおりです（図 1-5）。

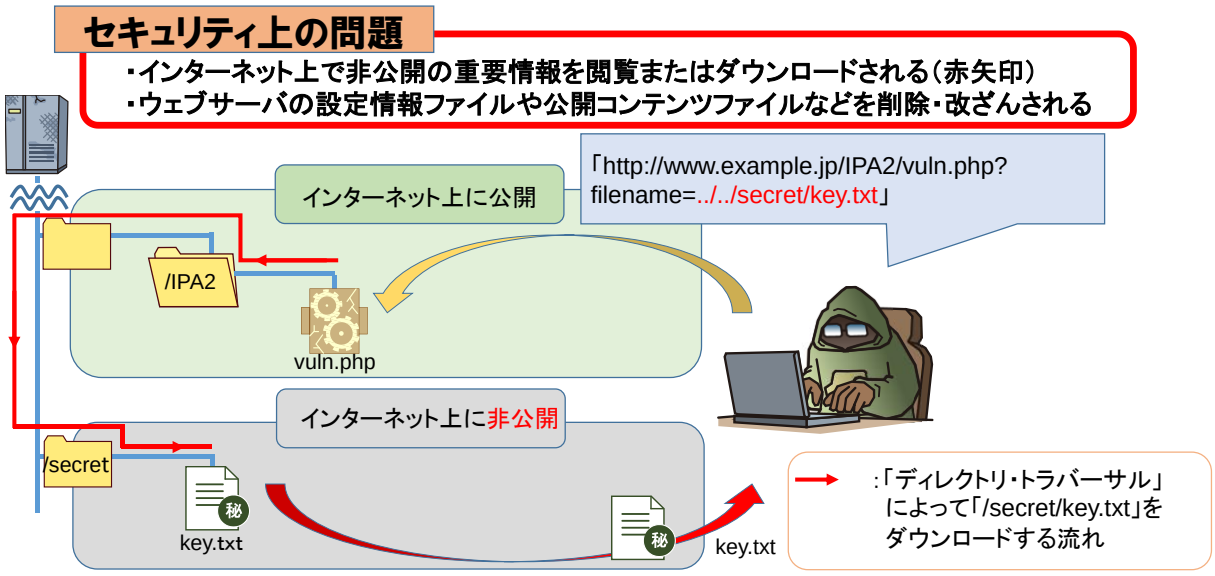


図1-5.「ディレクトリ・トラバーサル」の脆弱性の概要

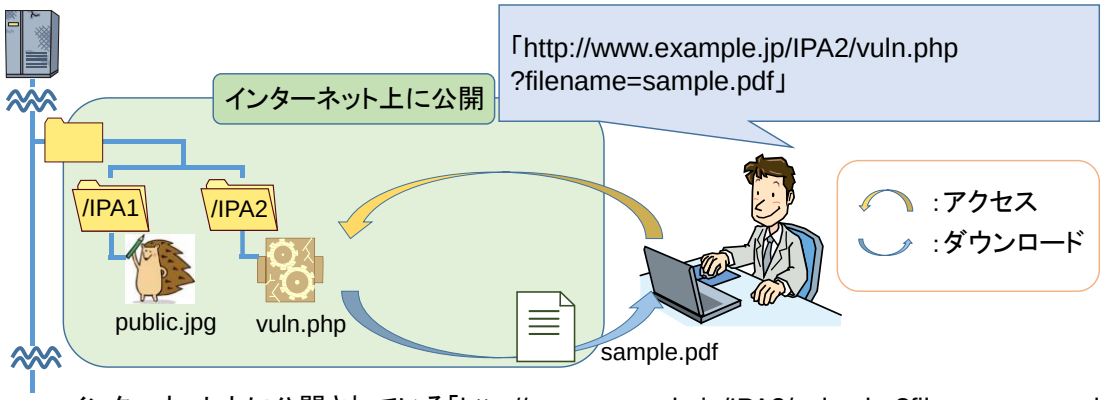
ウェブサイトにおける「ディレクトリ・トラバーサル」の脆弱性が作りこまれる原因は、ファイル名のチェックの不備にあります [*8]。

[*8] 「http://www.example.jp/IPA2/vuln.php?filename=sample.pdf」のように、パラメータ「filename」に「sample.pdf」とファイル名を直接指定している場合や、ファイル名に「../」やディレクトリ名を指定している実装において、ファイル名のチェックが不十分であること。

今期に比較的多く「ディレクトリ・トラバーサル」の脆弱性が届出されたのは、この脆弱性を意図せず作りこんでしまい、その脆弱性が未対策なままのウェブサイトが多く存在していたためと推測されます。前述のようなセキュリティ上の問題を引き起こさないよう、ウェブサイト運営者および、ウェブサイトの構築担当者は IPA が発行している「安全なウェブサイトの作り方」を参考にするなど適切な対策を行う必要があります。

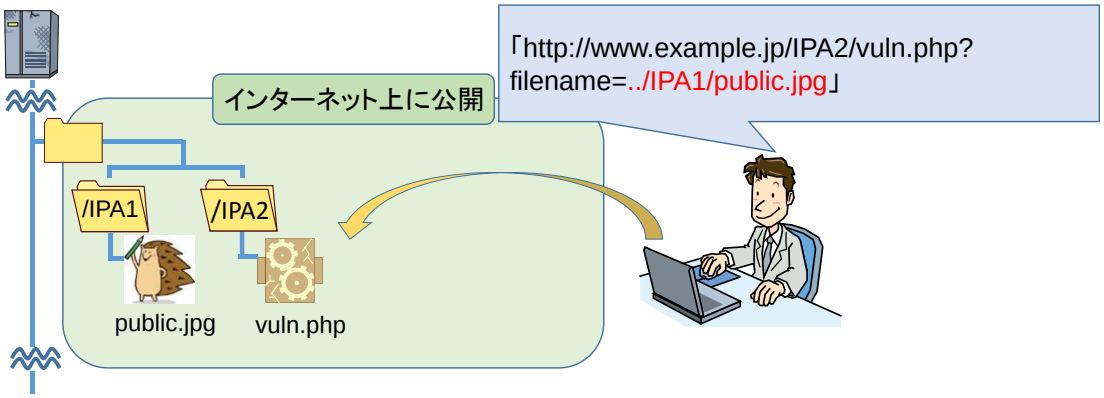
なお、「ディレクトリ・トラバーサル」の脆弱性を見つける場合は、安全な手順で行う必要があります。ウェブサイトに「ディレクトリ・トラバーサル」の脆弱性がある場合は、誤ってウェブサーバ上に存在する個人情報やウェブサーバの設定情報などといったインターネット上で非公開のファイルにアクセスしてしまう可能性があります。「ディレクトリ・トラバーサル」の脆弱性により、本来ファイルを閲覧する権限のない発見者がインターネット上で非公開なファイルを閲覧してしまうと、不正な行為であるとウェブサイト運営者にみなされる可能性があります。また場合によっては発見者とウェブサイト運営者との間でトラブルが生じる可能性があります。脆弱性の見つけ方は、次に示す安全な手順（図 1-6）で実施してください。なお、図 1-6 中の「vuln.php」は「ディレクトリ・トラバーサル」の脆弱性をもつ問題あるプログラムです。

1 現状把握：ウェブサイトの通常の動作確認



・インターネット上に公開されている「http://www.example.jp/IPA2/vuln.php?filename=sample.pdf」にウェブブラウザでアクセスすると、sample.pdf をダウンロードできることを確認する
・同時に「http://www.example.jp/IPA1/public.jpg」がインターネット上に公開されていることを確認する

2 脆弱性調査：インターネット上に公開されている異なるディレクトリのファイルにアクセス先を変更



「filename=sample.pdf」から「filename=../IPA1/public.jpg」へと文字を変更する

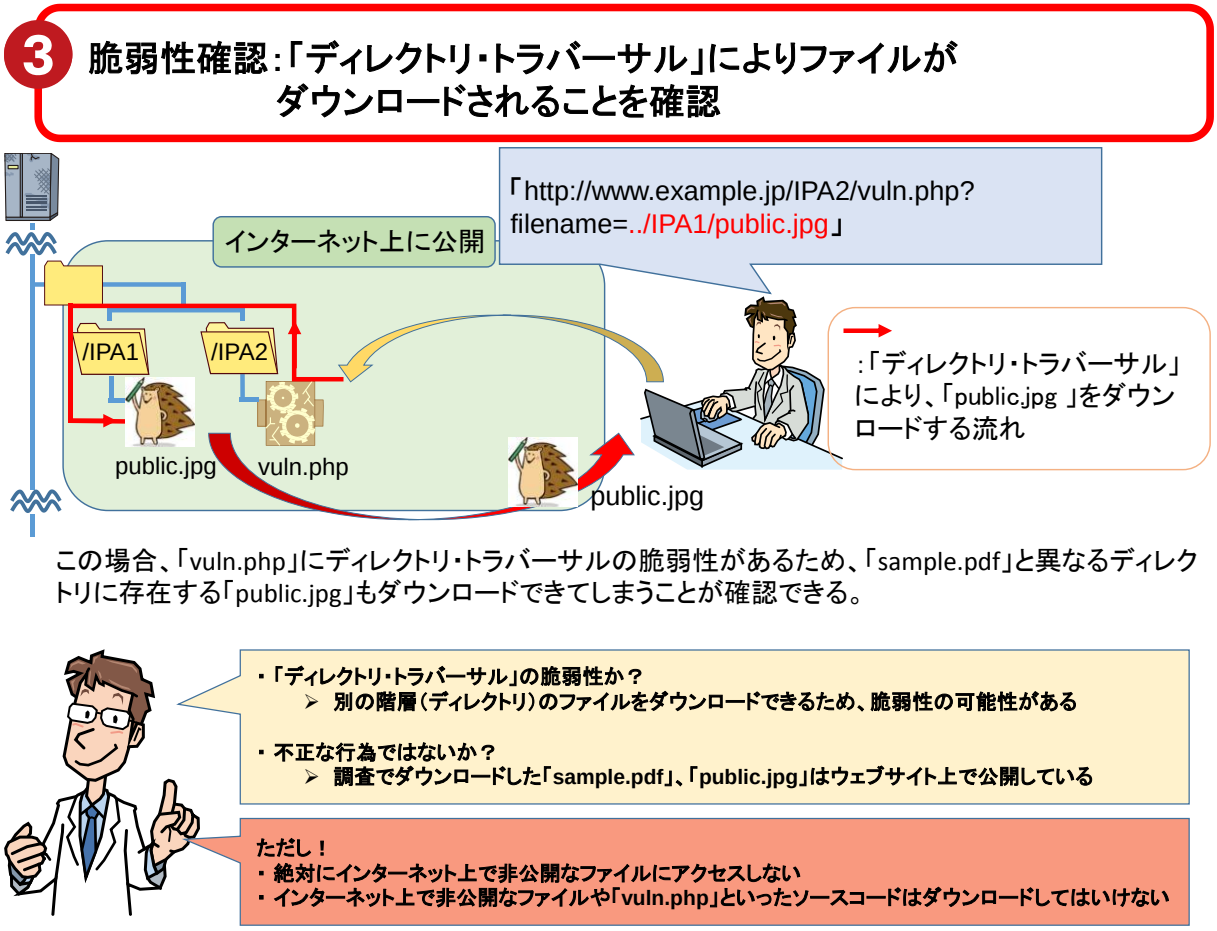


図1-6. 安全な「ディレクトリ・トラバーサル」の脆弱性の調査手順

図 1-6 の手順（3）ではサーバ上で公開していることをあらかじめ確認したファイル「public.jpg」をダウンロードしています。これは「ディレクトリ・トラバーサル」の安全な見つけ方です。しかし、図 1-5 にあるようにインターネット上で非公開とされているファイル名「../../secret/key.txt」を指定すると、「key.txt」がダウンロードできてしまうことがあります。非公開ファイルの不用意な閲覧は問題行為と解釈される可能性があり、図 1-5 に記載されている方法は行うべきではありません。

「SQL インジェクション」(*9) などウェブサイトにおける他の脆弱性にもいえることですが、脆弱性は安全な方法で見つけてください。脆弱性を見つける前には「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」(*10) の「発見者が心得ておくべき法的な論点」を参考にして、その見つけ方が安全であるか、今一度確認してください。なお、「ディレクトリ・トラバーサル」の脆弱性を届ける場合は、前述の手順（1）～（3）を脆弱性の証拠として提出してください。

(*9) 「SQL インジェクション」の脆弱性の届出において、認証回避やサーバ上のファイル削除・改ざんなどの行為をしたと認められる内容の届出は受け付けていません。

(*10) 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

2. ソフトウェア等の脆弱性に関する取扱状況（詳細）

2-1. ソフトウェア製品の脆弱性

2-1-1. 処理状況

図 2-1 のグラフはソフトウェア製品の脆弱性届出の処理状況について、四半期ごとの推移を示しています。2014 年 12 月末時点の届出の累計は 1,952 件で、今四半期に脆弱性対策情報を JVN 公表したものは 34 件（累計 959 件）でした。また、製品開発者が JVN 公表を行わず「個別対応」したものは 4 件（累計 33 件）、製品開発者が「脆弱性ではない」と判断したものは 1 件（累計 75 件）、「不受理」としたものは 12 件 (*11)（累計 272 件）、取扱い中は 613 件でした。613 件のうち、連絡不能開発者 (*12) 一覧へ新たに公表したのは 12 件で、2014 年 12 月末時点の累計は 163 件になりました。

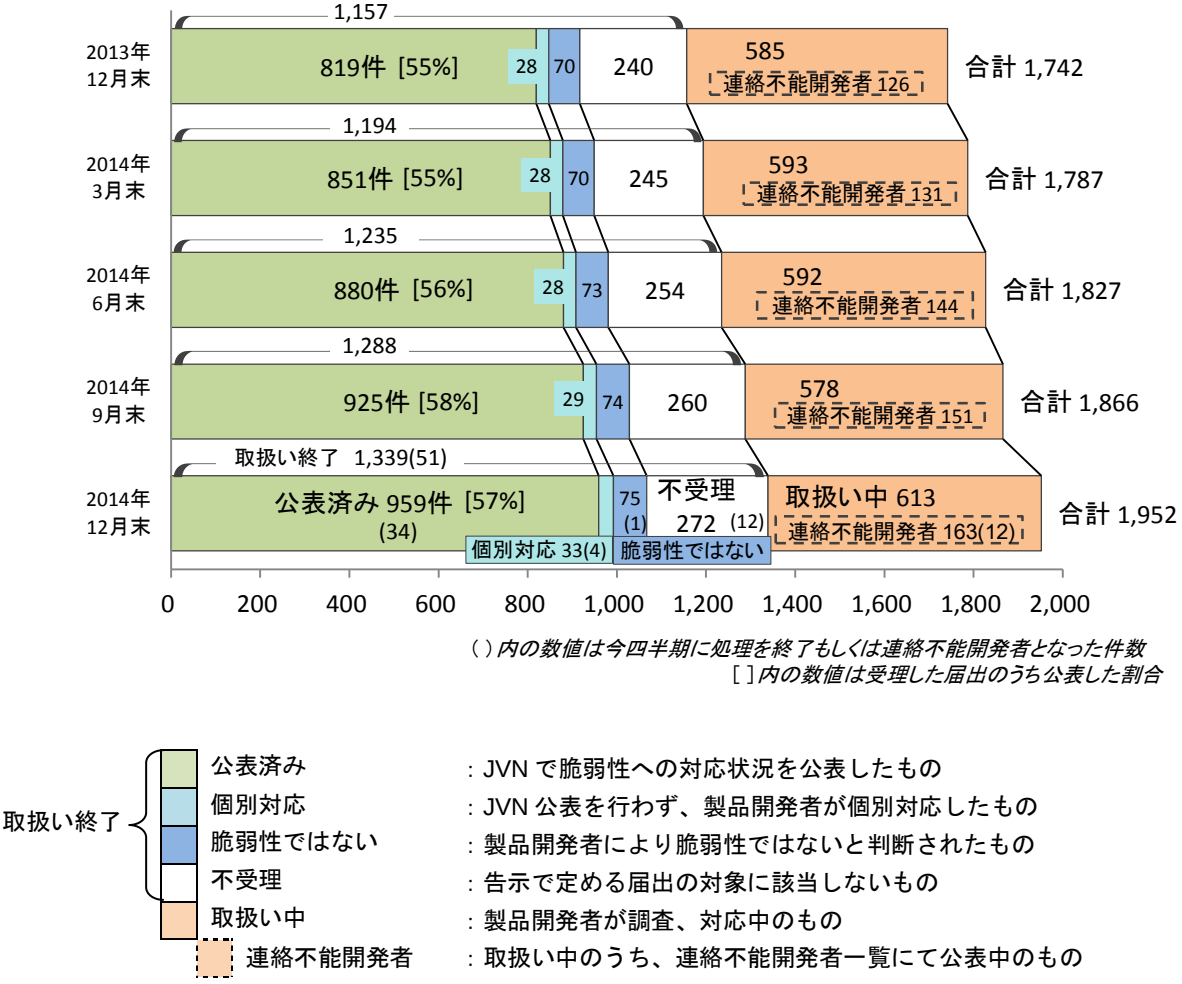


図 2-1. ソフトウェア製品脆弱性の届出処理状況（四半期ごとの推移）

(*11) 内訳は今四半期の届出によるもの 4 件、前四半期までの届出によるもの 8 件。
(*12) 連絡不能開発者一覧への公表および一覧からの削除が複数回行われた製品開発者の公表回数は、その累計を計上しています。

以下に、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 1,952 件のうち、不受理を除いた 1,680 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、届出された製品の種類別の分類を示しています。図 2-2 は製品種類別割合を、図 2-3 は過去 2 年間の届出件数の推移を四半期ごとに示したものです。

累計では、「ウェブアプリケーションソフト」が最も多く 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」が最も多く、次いで「ルータ」となっています。

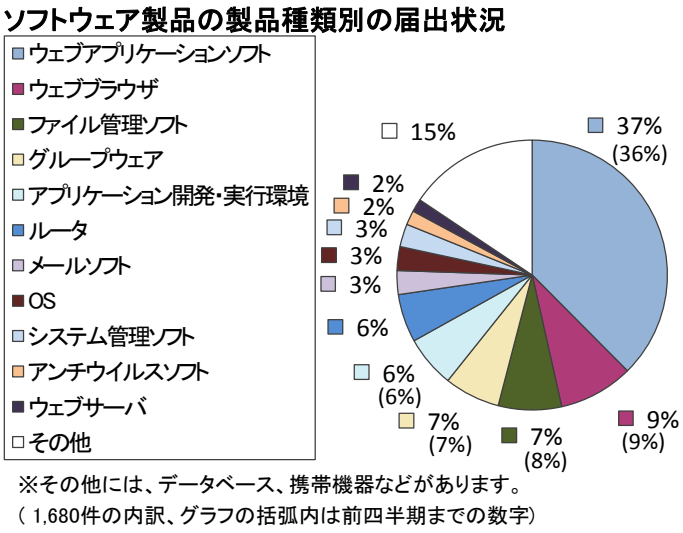


図2-2. 届出累計の製品種類別割合

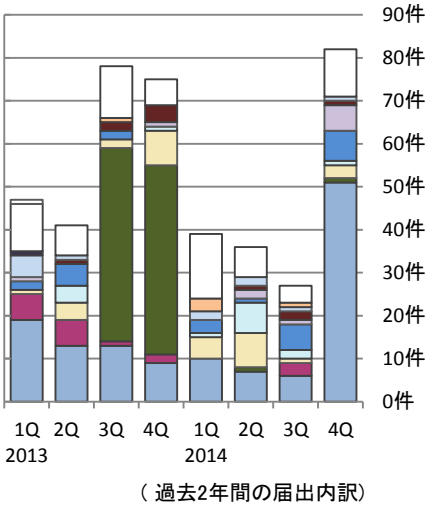


図2-3. 四半期ごとの製品種類別届出件数

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

累計では、オープンソースソフトウェアが 30%を占めています。オープンソースソフトウェアの件数は、2013 第 3 四半を除き 10 件前後で推移しています。

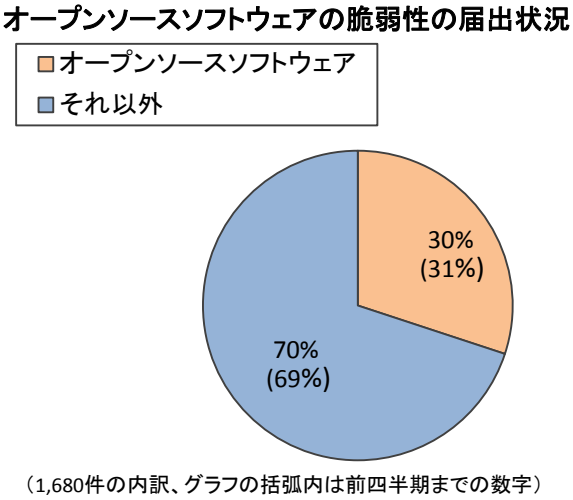


図2-4. 届出累計のオープンソースソフトウェア割合

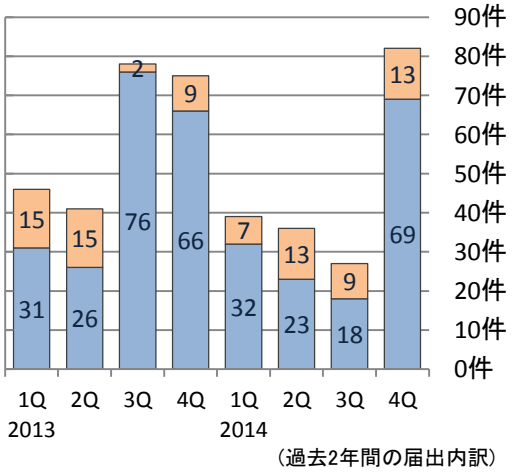


図2-5. 四半期ごとのオープンソースソフトウェア届出件数

図 2-6、図 2-7 のグラフは、ソフトウェア製品の届出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 年間の四半期ごとの届出件数の推移を、図 2-7 は届出受付開始から今四半期末までの届出累計について、JVN 公表までに要した日数の割合を示しています。「スマホアプリ」に関する届出は、2013 年第 3、第 4 四半期に急増しましたが、それ以降は 5 件前後となっています。

受理から 45 日以内に対策情報を JVN 公表した割合は「スマホアプリ」が 27%（前四半期は 28%）、「それ以外」が 33%（前四半期は 34%）でした。

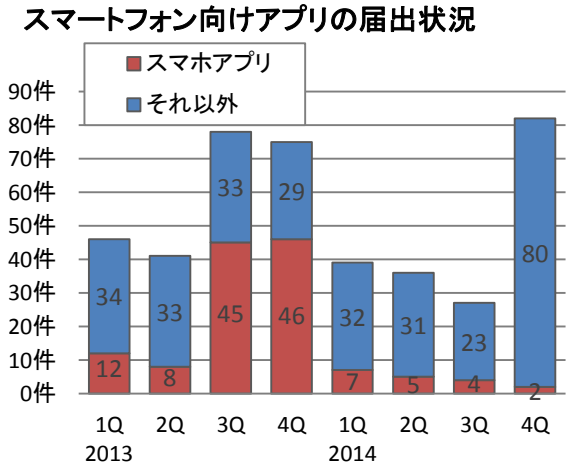


図2-6. 四半期ごとのスマートフォン向けアプリ届出件数

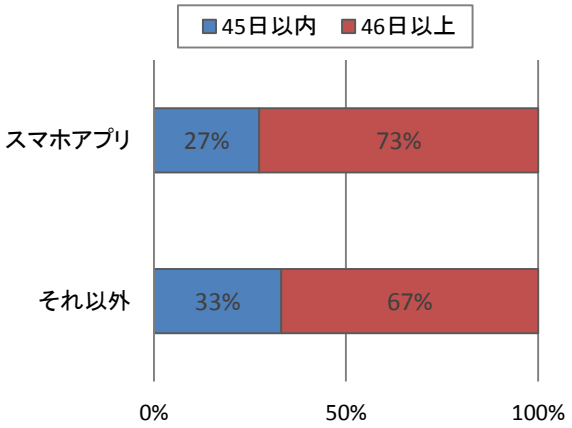
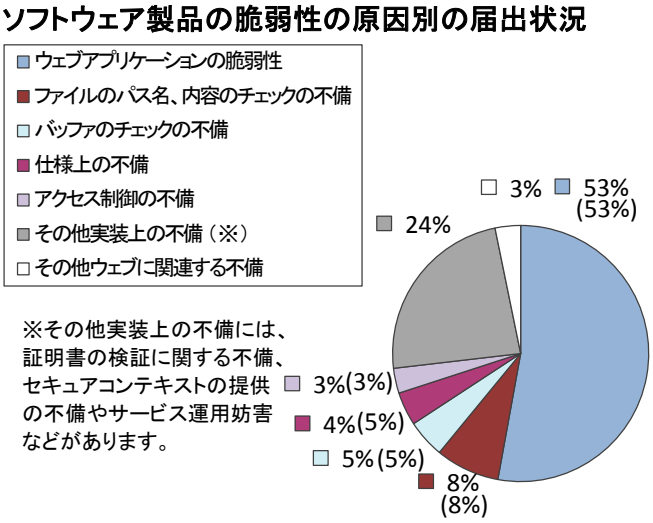


図2-7. スマートフォン向けアプリとそれ以外のJVN公表までの日数の割合

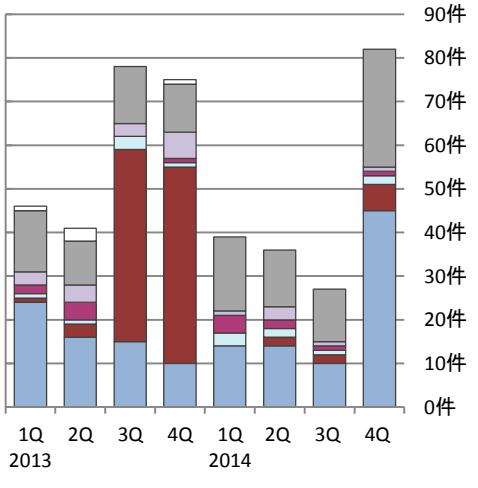
2-1-3. 脆弱性の原因と影響別件数

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 は届出累計の脆弱性の原因別割合を、図 2-9 は過去 2 年間の原因別の届出件数の推移を四半期ごとに示しています。累計では、「ウェブアプリケーションの脆弱性」が過半数を占めています。また、今四半期の届出件数は「ウェブアプリケーションの脆弱性」が最多でした。



（1,680件の内訳、グラフの括弧内は前四半期までの数字）

図2-8. 届出累計の脆弱性の原因別割合

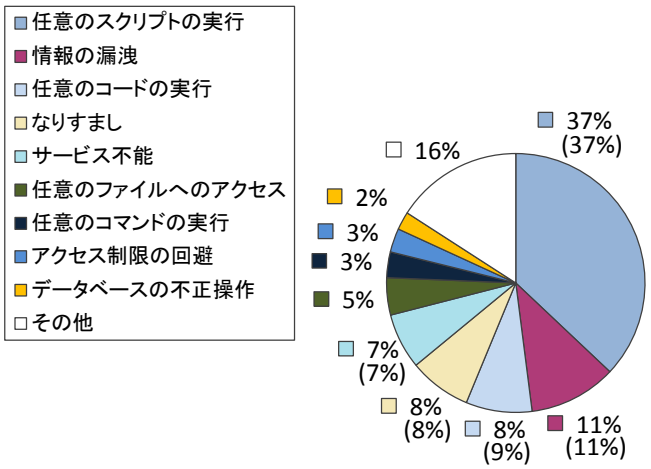


（過去2年間の届出内訳）

図2-9. 四半期ごとの脆弱性の原因別届出件数

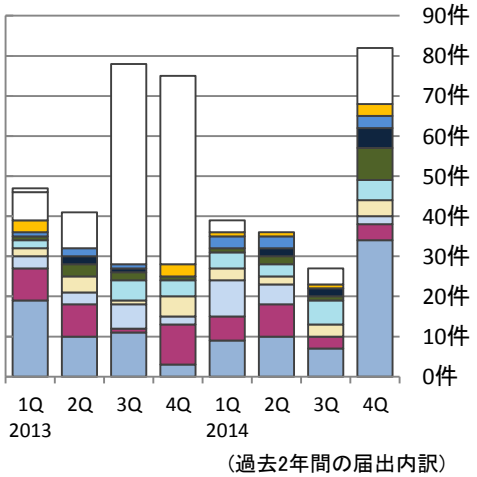
図 2-10、図 2-11 のグラフは、届出された脆弱性がもたらす影響を示しています。図 2-10 は届出累計の影響別割合を、図 2-11 は過去 2 年間の影響別届出件数の推移を四半期ごとに示しています。累計では「任意のスクリプトの実行」が最も多く、次いで「情報の漏洩」となっています。今四半期は、「任意のスクリプト実行」が最も多く、次いで「任意のファイルへのアクセス」が多く届出されました。なお、2013 年第 3、第 4 四半期の「その他」が多いのは、「ファイルのパス名、内容のチェックの不備」によりもたらされる影響が「その他」に分類されたためです。

ソフトウェア製品の脆弱性がもたらす影響別の届出状況



（1,680件の内訳、グラフの括弧内は前四半期までの数字）

図2-10. 届出累計の脆弱性がもたらす影響別割合



（過去2年間の届出内訳）

図2-11. 四半期ごとの脆弱性がもたらす影響別届出件数

2-1-4. 調整および公表件数

JPCERT/CC は、本制度に届け出られた脆弱性情報のほか、海外の製品開発者や CSIRT などからも脆弱性情報の提供を受けて、国内外の関係者と調整を行っています。これらの脆弱性に対する製品開発者の対応状況は、IPA と JPCERT/CC が共同運営している脆弱性対策情報ポータルサイト JVN（Japan Vulnerability Notes）（URL：http://jvn.jp/ ）に公表しています。表 2-1、図 2-12 のグラフは、公表件数を情報提供元別に集計し、今四半期の公表件数、過去 3 年分の四半期ごとの公表件数の推移等を示したものです。

表 2-1. 脆弱性の提供元別 脆弱性公表件数

	情報提供元	今期件数	累計
①	国内外の発見者からの届出、製品開発者から自社製品の届出を受け JVN で公表した脆弱性	34 件	959 件
②	海外 CSIRT 等から脆弱性情報の提供を受け JVN で公表した脆弱性	31 件	1,169 件
	合計	65 件	2,128 件

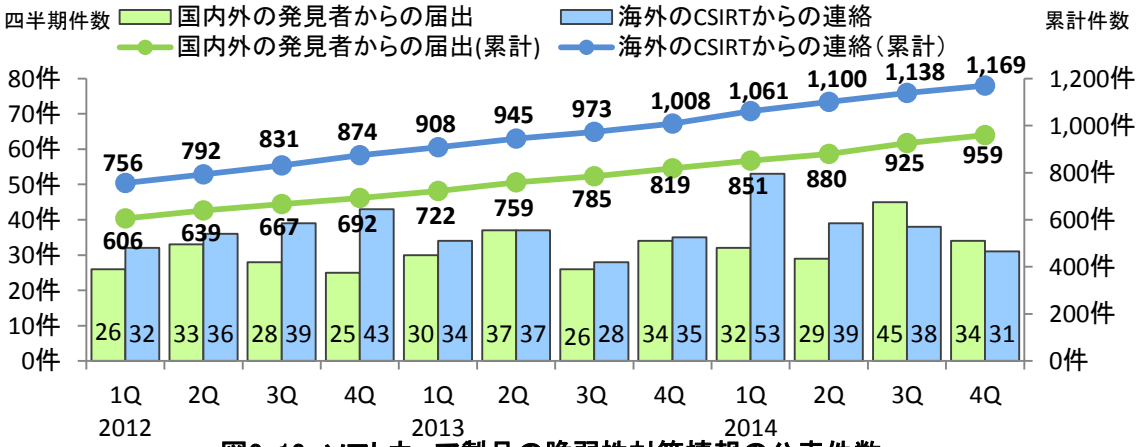


図2-12. ソフトウェア製品の脆弱性対策情報の公表件数

（1） 国内外の発見者および製品開発者から届出を受け JVN で公表した脆弱性

届出受付開始から今四半期までに対策情報を JVN 公表した脆弱性（959 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。45 日以内は 33%、45 日を超過した件数は 67%でした。表 2-2 は過去 3 年間において 45 日以内に JVN 公表した件数の割合推移を四半期ごとに示したものです。製品開発者は脆弱性が悪用された場合の影響を認識し、迅速な対策を講じる必要があります。

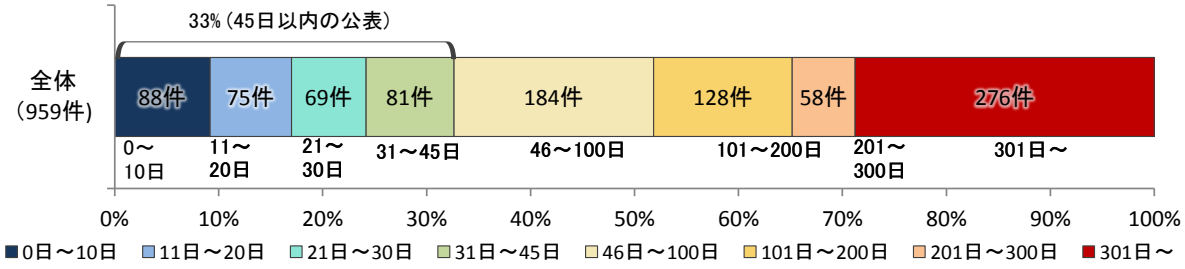


図2-13. ソフトウェア製品の脆弱性公表日数

表 2-2. 45 日以内に JVN 公表した件数の割合推移（四半期ごと）

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

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 34 件のうち、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 9 件（表 2-3 の*1）、複数開発者・製品に影響がある脆弱性が 2 件（表 2-3 の*2）、組込みソフトウェア製品の脆弱性が 10 件（表 2-3 の*3）、制御システムの脆弱性に関するものが 1 件（表 2-3 の*4）ありました。

表 2-3. 2014 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	「GIGAPOD」におけるサービス運用妨害(DoS)の脆弱性	ファイルサーバソフト「GIGAPOD」には、Apache HTTP Server の脆弱性(CVE-2011-3192)に起因するサービス運用妨害(DoS)の脆弱性がありました。このため、第三者により応答不能な状態にされる可能性がありました。	2014 年 10 月 16 日	7.8
2（*3）	「QNAP QTS」における OS コマンド・インジェクションの脆弱性	Turbo NAS 用の OS「QTS」には、GNU Bash の脆弱性(JVNVU#97219505)に起因する OS コマンド・インジェクションの脆弱性がありました。このため、第三者によりサーバ上で任意のコマンドを実行される可能性がありました。	2014 年 10 月 28 日	10.0
3（*2）	複数のサイボウズ製品におけるバッファオーバーフローの脆弱性	複数のサイボウズ製品には、バッファオーバーフローの脆弱性がありました。このため、第三者により応答不能な状態にされたり、任意のコードを実行されたりする可能性がありました。	2014 年 11 月 11 日	9.0
4（*2）	「一太郎」シリーズにおいて任意のコードが実行される脆弱性	ワープロソフト「一太郎」シリーズには、文書ファイルを読み込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が実行される可能性がありました。	2014 年 11 月 13 日	9.3
5（*3）	「ARROWS Me F-11D」における任意の領域にアクセス可能な脆弱性	Android 端末「ARROWS Me F-11D」には、当該製品の任意の領域にアクセス可能な脆弱性がありました。このため、第三者により当該製品に内蔵されているフラッシュメモリの内容を取得されたり、改ざんされたりする可能性がありました。	2014 年 12 月 2 日	7.2
6	i-HTTPD 付属「ファイルアップロード BBS」において任意のコマンドが実行される脆弱性	掲示板ソフト「ファイルアップロード BBS」には、SSI ディレクティブが記載されたファイルの処理に不備がありました。このため、サーバ上で任意のコマンドを実行される可能性がありました。	2014 年 12 月 9 日	7.5
7（*3）	アライドテレシス製の複数の製品におけるバッファオーバーフローの脆弱性	アライドテレシス製のルータおよびスイッチには、バッファオーバーフローの脆弱性がありました。このため、第三者により任意のコードを実行される可能性がありました。	2014 年 12 月 18 日	10.0
脆弱性の深刻度=レベル II（警告）、CVSS 基本値=4.0～6.9				
8（*3）	「Huawei E5332」におけるサービス運用妨害(DoS)の脆弱性	ネットワーク機器「Huawei E5332」には、サービス運用妨害(DoS)の脆弱性がありました。このため、第三者により応答不能な状態にされる可能性がありました。項番 9 とは異なる問題です。	2014 年 10 月 10 日	5.5
9（*3）	「Huawei E5332」におけるサービス運用妨害(DoS)の脆弱性	ネットワーク機器「Huawei E5332」には、サービス運用妨害(DoS)の脆弱性がありました。このため、第三者により応答不能な状態にされる可能性がありました。項番 8 とは異なる問題です。	2014 年 10 月 10 日	5.5

項番	脆弱性	セキュリティ上の問題点	JVN 公表日	CVSS 基本値
10 (*1)	「BirdBlog」におけるクロスサイト・スクリプティングの脆弱性	ウェブログシステム「BirdBlog」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 10 月 16 日	4.3
11 (*1)	「Aflax」におけるクロスサイト・スクリプティングの脆弱性	JavaScript ライブラリ「Aflax」には、クロスサイト・スクリプティングの脆弱性がありました。このため、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 10 月 16 日	4.3
12	Android 版「スマ保」における SSL/TLS サーバ証明書の検証不備の脆弱性	保健サービス管理アプリ「スマ保」には、SSL/TLS サーバ証明書の検証不備の脆弱性が存在しました。このため、中間者攻撃による暗号通信の盗聴などが行われる可能性がありました。	2014 年 10 月 23 日	4.0
13 (*1)	「OpenAM」におけるサービス運用妨害(DoS)の脆弱性	アクセス管理ソフト「OpenAM」には、Cookie の処理に不備がありました。このため、第三者により応答不能な状態にされる可能性がありました。	2014 年 11 月 10 日	6.8
14 (*1)	「Direct Web Remoting (DWR)」における XML 外部実体参照(XXE)に関する脆弱性	ウェブアプリケーションフレームワーク「Direct Web Remoting (DWR)」には、XML 外部実体参照(XXE)に関する脆弱性がありました。このため、第三者によりサーバ上の任意のファイルを読みとられる可能性がありました。	2014 年 11 月 14 日	5.8
15 (*1)	「Direct Web Remoting (DWR)」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「Direct Web Remoting (DWR)」には、クロスサイト・スクリプティングの脆弱性がありました。このため、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 11 月 14 日	4.3
16	「iLogScanner」におけるクロスサイト・スクリプティングの脆弱性	ウェブサイトの攻撃兆候検出ツール「iLogScanner」には、クロスサイト・スクリプティングの脆弱性がありました。このため、第三者により検出結果の HTML ファイルにスクリプトを埋め込まれる可能性がありました。	2014 年 11 月 14 日	5.0
17 (*1)	BSD 系 OS におけるサービス運用妨害(DoS)の脆弱性	FreeBSD、NetBSD、OpenBSD などの Net/2 をベースにした BSD 系 OS には、TCP セッションタイマーの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な状態にされる可能性がありました。	2014 年 11 月 21 日	4.3
18 (*3)	「SEIL」シリーズルータにおけるサービス運用妨害(DoS)の脆弱性	ルータ「SEIL」シリーズには、NTP リクエストの処理に問題がありました。このため、第三者によりリソースを消費されたり、踏み台として DDoS 攻撃に悪用されたりする可能性がありました。	2014 年 12 月 1 日	5.0
19 (*3)	「SEIL」シリーズルータにおけるサービス運用妨害 (DoS) の脆弱性	ルータ「SEIL」シリーズには、特定のパケット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を再起動させられる可能性がありました。	2014 年 12 月 1 日	5.0
20 (*3)	Texas Instruments 「OMAP モバイル・プロセッサ」の Syslink ドライバにおける複数のデータ検証不備の脆弱性	プロセッサ間通信用の Syslink ドライバには、複数のデータ検証不備の脆弱性がありました。このため、第三者によりカーネルメモリの内容を取得されたり、任意のコードを実行され root 権限を取得されたりする可能性がありました。	2014 年 12 月 2 日	6.2
21 (*3)	富士通製の複数の Android 端末における OS コマンド・インジェクションの脆弱性	富士通製の複数の Android 端末には、OS コマンド・インジェクションの脆弱性がありました。このため、第三者により当該製品の root 権限を取得されたり、任意の OS コマンドを実行されたりする可能性がありました。	2014 年 12 月 2 日	6.2

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 (*1)	「DBD::PgPP」における SQL インジェクションの脆弱性	Perl モジュール「DBD::PgPP」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。	2014 年 12 月 3 日	6.8
23	KENT-WEB 製「Clip Board」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「Clip Board」には、クロスサイト・スクリプティングの脆弱性がありました。このため、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 12 月 4 日	4.3
24	「i-HTTPD」におけるクロスサイト・スクリプティングの脆弱性	ウェブサーバソフト「i-HTTPD」には、ウェブページを出力する際の処理に問題がありました。このため、第三者によりウェブページにスクリプトを埋め込まれる可能性がありました。項番 26 とは異なる問題です。	2014 年 12 月 9 日	4.3
25	i-HTTPD 付属「おまけ 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「おまけ 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。	2014 年 12 月 9 日	5.0
26	「i-HTTPD」におけるクロスサイト・スクリプティングの脆弱性	ウェブサーバソフト「i-HTTPD」には、ウェブページを出力する際の処理に問題がありました。このため、第三者によりウェブページにスクリプトを埋め込まれる可能性がありました。項番 24 とは異なる問題です。	2014 年 12 月 12 日	4.3
27 (*1)	「LinPHA」におけるクロスサイト・スクリプティングの脆弱性	画像ファイル管理ソフト「LinPHA」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 12 月 9 日	4.3
28	Android 版「TSUTAYA アプリ」における任意の Java のメソッドが実行される脆弱性	Android アプリ「TSUTAYA アプリ」には任意の Java のメソッドが実行される脆弱性がありました。このため、第三者により当該製品の権限で実行可能な任意の Java メソッドを実行される可能性がありました。	2014 年 12 月 18 日	5.8
29	「WBS ガントチャート for JIRA」におけるクロスサイト・スクリプティングの脆弱性	課題管理ツール JIRA 用プラグイン「WBS ガントチャート for JIRA」には、ウェブページを出力する際の処理に問題がありました。このため、第三者によりウェブページにスクリプトを埋め込まれる可能性がありました。項番 34 とは異なる問題です。	2014 年 12 月 18 日	4.0
脆弱性の深刻度=レベル I（注意）、CVSS 基本値=0.0～3.9				
30 (*4)	「FAST/TOOLS」における XML 外部実体参照処理の脆弱性	SCADA ソフト「FAST/TOOLS」には、XML 外部実体参照(XXE)に関する脆弱性がありました。このため、第三者によりサーバ上の任意のファイルを読みとられる可能性や応答不能な状態にされる可能性がありました。	2014 年 11 月 28 日	2.4
31 (*3)	「LG Electronics 製モバイルアクセスルータ」にアクセス制限不備の脆弱性	「LG Electronics 製モバイルアクセスルータ」のウェブ管理インターフェースには、アクセス制限不備の脆弱性がありました。このため、第三者により認証を回避して機器が保持している情報を取得される可能性がありました。	2014 年 12 月 2 日	3.3
32	Android 版「拡散性ミリオンアーサー」における情報管理不備の脆弱性	Android 用ゲームアプリ「拡散性ミリオンアーサー」には、認証情報の管理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認証情報を取得される可能性がありました。	2014 年 12 月 4 日	2.6
33 (*1)	「Chyrp」におけるクロスサイト・スクリプティングの脆弱性	ブログサイト構築ソフト「Chyrp」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 12 月 10 日	3.5

項番	脆弱性	セキュリティ上の問題点	JVN 公表日	CVSS 基本値
34	「WBS ガントチャート for JIRA」におけるクロスサイト・スクリプティングの脆弱性	課題管理ツール JIRA 用プラグイン「WBS ガントチャート for JIRA」には、エクスポートする際の処理に問題がありました。このため、第三者によりウェブページにスクリプトを埋め込まれる可能性がありました。項番 29 とは異なる問題です。	2014 年 12 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）：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
（*4）：制御システムの脆弱性

（2） 海外 CSIRT 等から脆弱性情報の提供を受け JVN で公表した脆弱性

表 2-4、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 31 件あり、表 2-4 は通常の脆弱性情報 30 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。

近年、Android 関連製品や OSS 製品の脆弱性に対する調整活動では、製品開発者が所在するアジア圏の調整機関、特に韓国の KrCERT/CC や中国の CNCERT/CC、台湾の TWNCERT との連携が増えています。これらの情報は、JPCERT/CC 製品開発者リスト [*13] に登録された製品開発者へ通知したうえ、JVN に掲載しています。

表 2-4. 海外 CSIRT 等と連携した脆弱性および対応状況

項番	脆弱性	対応状況
1	Brocade Vyatta 5400 vRouter に複数の脆弱性	注意喚起として掲載
2	HP System Management Homepage (SMH) にクロスサイトスクリプティングの脆弱性	注意喚起として掲載
3	NetComm NB604N に格納型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	Rejetto HFS (HTTP File Server) に null バイトの取扱いに関する脆弱性	注意喚起として掲載
5	Cryoserver における権限昇格の脆弱性	注意喚起として掲載
6	BMC Track-It! に複数の脆弱性	注意喚起として掲載
7	IBM WebSphere Application Server に複数の脆弱性	注意喚起として掲載
8	SSLv3 プロトコルに暗号化データを解読される脆弱性(POODLE 攻撃)	注意喚起として掲載 複数製品開発者へ通知
9	複数の Apple 製品の脆弱性に対するアップデート	注意喚起として掲載
10	Centreon に複数の脆弱性	注意喚起として掲載
11	複数の NAT-PMP デバイスが WAN 側から操作可能な問題	注意喚起として掲載 複数製品開発者へ通知
12	GNU Wget にシンボリックリンクの扱いに関する問題	注意喚起として掲載
13	drchrono Electronic Health Record (EHR) のウェブアプリケーションに複数の脆弱性	注意喚起として掲載
14	Linksys SMART WiFi 対応ファームウェアに複数の脆弱性	注意喚起として掲載
15	uIP と lwIP の DNS リゾルバにキャッシュポイズニングの脆弱性	注意喚起として掲載
16	Android 版 IBM Notes Traveler クライアントに HTTP 経由でユーザ認証情報を送信する問題	注意喚起として掲載
17	Microsoft Secure Channel (Schannel) に任意のコード実行が可能な脆弱性	緊急案件として掲載
18	Microsoft Windows OLE ライブラリに任意のコード実行が可能な脆弱性	緊急案件として掲載

[*13] JPCERT/CC 製品開発者リスト：https://jvn.jp/nav/index.html。

項番	脆弱性	対応状況
19	Microsoft Windows の Kerberos Key Distribution Center (KDC) に Privilege Attribute Certificate (PAC) 署名検証不備の脆弱性	緊急案件として掲載
20	Zenoss Core に複数の脆弱性	注意喚起として掲載
21	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
22	ISC BIND 9 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
23	再帰的名前解決を行う DNS リゾルバの実装に名前解決を無限に繰り返す問題	注意喚起として掲載 複数製品開発者へ通知
24	Honeywell OPOS Suite にスタックバッファオーバーフローの脆弱性	注意喚起として掲載
25	EMC Documentum シリーズの製品に複数の脆弱性	注意喚起として掲載
26	CA Release Automation (旧 CA LISA Release Automation) に複数の脆弱性	注意喚起として掲載
27	複数の Dell iDRAC 製品にセッション管理に関する脆弱性	注意喚起として掲載
28	AppsGeyser で作成される Android アプリケーションに SSL 証明書の検証不備の脆弱性が作り込まれる問題	注意喚起として掲載
29	Network Time Protocol daemon (ntpd) 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
30	複数のブロードバンドルータに、脆弱性が存在するバージョンの Allegro RomPager を使用している問題	注意喚起として掲載 複数製品開発者へ通知

表 2-5.米国 US-CERT [*14] 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	Apple iOS に対する攻撃手法 Masque Attack

2-1-5. 連絡不能案件の処理状況

図 2-14 は、2011 年 9 月末から 2014 年 12 月末までに、「連絡不能開発者」と位置づけて取扱った 185 件の処理状況の推移を示したものです。

2014 年 12 月末時点での処理状況は、185 件のうち、製品開発者との調整が再開したため連絡不能開発者一覧から削除したものは前四半期と変わらず 22 件で、製品開発者と連絡が取れないため公表しているものは 163 件（前四半期は 151 件）となりました。

「連絡不能」は、前期からの繰り越し 151 件と、今四半期の「新規公表」12 件の累計 163 件となりました。このうち、前四半期に新規公表した 8 件は製品開発者と連絡が取れなかったため製品情報を追加する「追加情報公表」となりました。

また、「調整再開」22 件のうち 1 件は、製品開発者との調整を経て脆弱性対策情報の公表を完了したため、「調整再開（調整中）」から「調整再開（調整完了）」となりました。

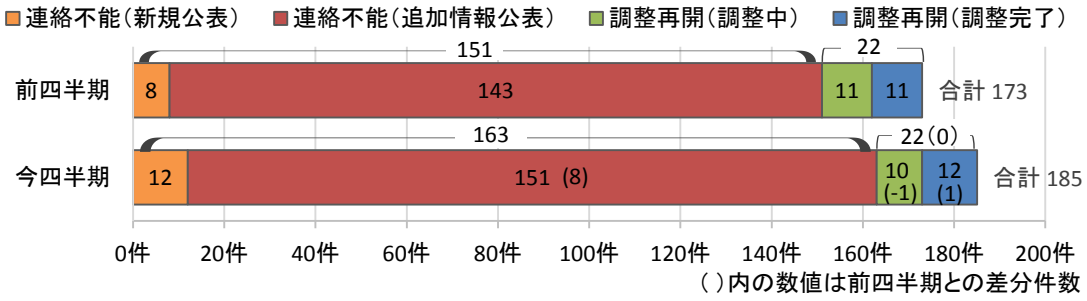


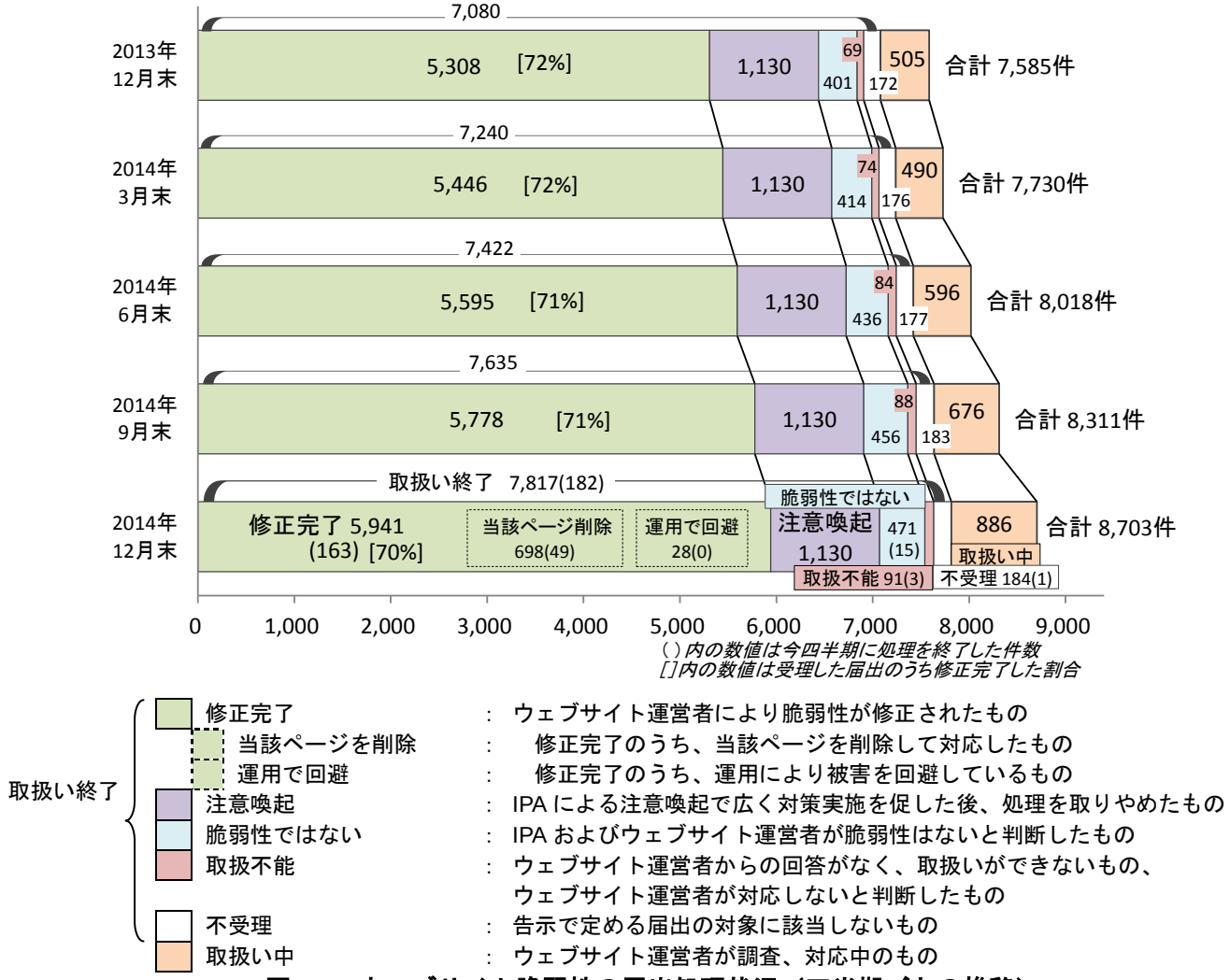
図2-14. 連絡不能開発者一覧の処理状況

[*14] 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 2-15 のグラフは、ウェブサイトの脆弱性届出の処理状況について、四半期ごとの推移を示したものです。2014 年 12 月末時点の届出の累計は 8,703 件で、今四半期中に取扱いを終了したものは 182 件（累計 7,817 件）でした。このうち「修正完了」したものは 163 件（累計 5,941 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 15 件（累計 471 件）でした。“「注意喚起」により処理を取りやめる”とは、多数のウェブサイトにおいて利用されているソフトウェア製品に修正プログラムが適用されていない、といった届出があった場合、届出されたウェブサイト以外でも影響を受ける可能性があるため、「注意喚起」で広く対策を呼びかけた上で処理を取りやめたものです。なお、ウェブサイト運営者への連絡は通常メールで行い、連絡が取れない場合は電話や郵送での連絡も行っています。しかしウェブサイト運営者への連絡手段がない場合などは「取扱不能」案件となります。今期その件数は 3 件（累計 91 件）でした。また「不受理」としたものは 1 件（累計 184 件）でした。取扱いを終了した累計 7,817 件のうち「修正完了」「脆弱性ではない」の合計 6,412 件は全て、ウェブサイト運営者からの報告もしくは IPA の判断により指摘した点が解消されていることが確認されています。「修正完了」のうち、ウェブサイト運営者が当該ページの削除により対応したものは 49 件（累計 698 件）、ウェブサイト運営者が運用により被害を回避したものは 0 件（累計 28 件）でした。



取扱い終了
- 修正完了 ： ウェブサイト運営者により脆弱性が修正されたもの
  - 当該ページを削除 ： 修正完了のうち、当該ページを削除して対応したもの
  - 運用で回避 ： 修正完了のうち、運用により被害を回避しているもの
- 注意喚起 ： IPA による注意喚起で広く対策実施を促した後、処理を取りやめたもの
- 脆弱性ではない ： IPA およびウェブサイト運営者が脆弱性はないと判断したもの
- 取扱不能 ： ウェブサイト運営者からの回答がなく、取扱いができないもの、ウェブサイト運営者が対応しないと判断したもの
- 不受理 ： 告示で定める届出の対象に該当しないもの
- 取扱い中 ： ウェブサイト運営者が調査、対応中のもの

図 2-15.ウェブサイト脆弱性の届出処理状況（四半期ごとの推移）

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 8,703 件のうち、不受理を除いた 8,519 件の届出を分析した結果を記載します。

2-2-2. 運営主体の種類別の届出件数

図 2-16 のグラフは、届出された脆弱性のウェブサイト運営主体の種類について、過去 2 年間の届出件数の推移を四半期ごとに示しています。今四半期は全体の約 7 割を企業が占めています。

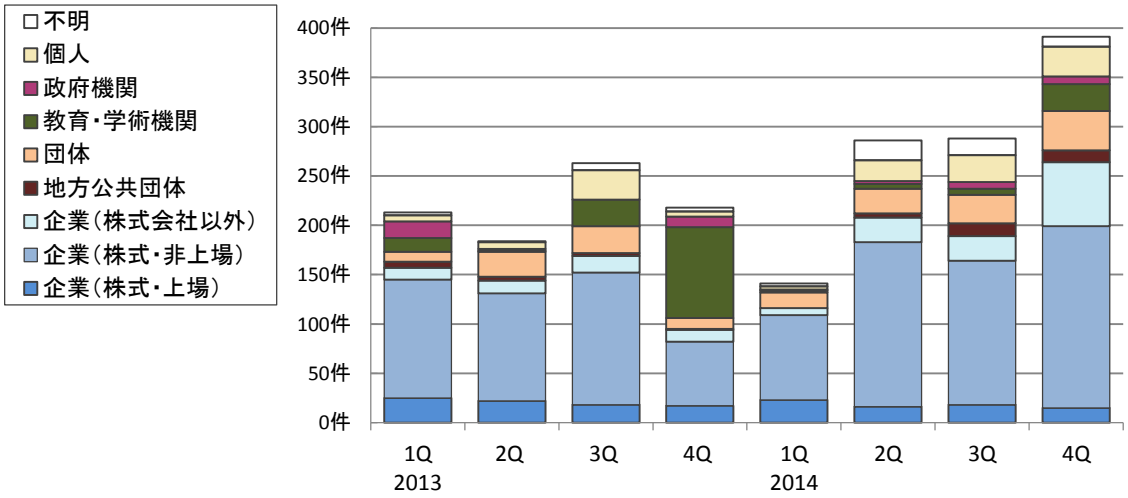


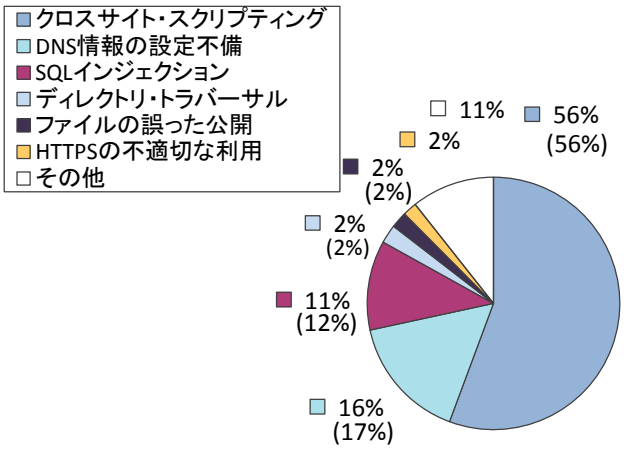
図2-16. 四半期ごとの運営主体の種類別届出件数

2-2-3. 脆弱性の種類・影響別届出

図 2-17、図 2-18 のグラフは、届出された脆弱性の種類を示しています。図 2-17 は届出受付開始から今四半期末までの届出累計の割合を、図 2-18 は過去 2 年間の届出件数の推移を四半期ごとに示しています[*15]。

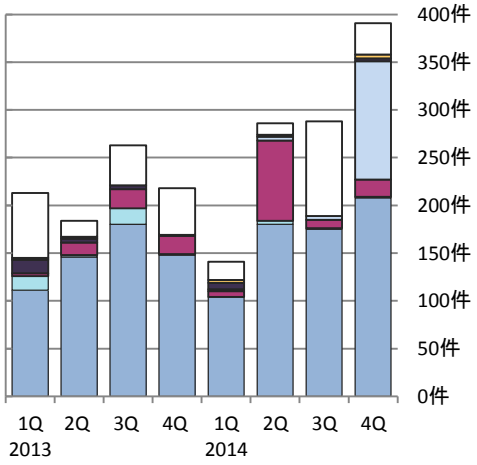
累計では、「クロスサイト・スクリプティング」だけで 56%を占めており、次いで「DNS 情報の設定不備」「SQL インジェクション」となっています。「DNS 情報の設定不備」は 16%ありますが、2008 年から 2009 年にかけて多く届出されたのが反映されたものです。今四半期は「ディレクトリ・トラバーサル」の届出が急増し、「クロスサイト・スクリプティング」に匹敵する件数となりました。なお、この統計は本制度における届出の傾向であり、世の中に存在する脆弱性の傾向と必ずしも一致するものではありません。

ウェブサイトの脆弱性の種類別の届出状況



(8,519件の内訳、グラフの括弧内は前四半期までの数字)

図2-17. 届出累計の脆弱性の種類別割合



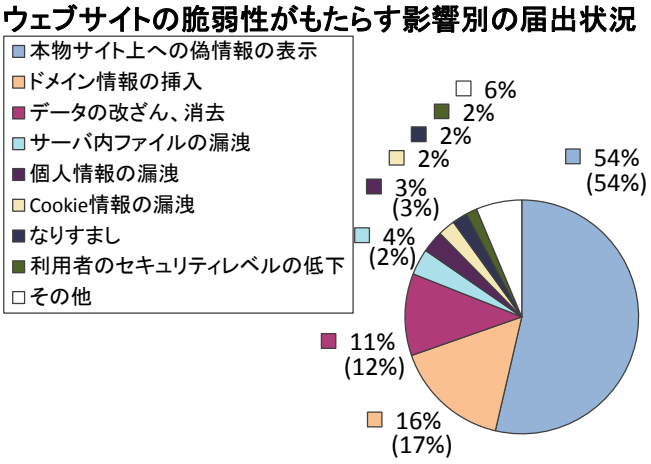
(過去2年間の届出内訳)

図2-18. 四半期ごとの脆弱性の種類別届出件

[*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。

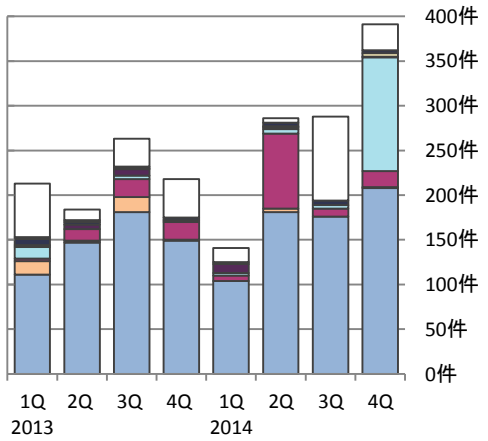
図 2-19、図 2-20 のグラフは、届出された脆弱性がもたらす影響別の分類です。図 2-19 は届出の影響別割合を、図 2-20 は過去 2 年間の届出件数の推移を四半期ごとに示しています。

累計では、「クロスサイト・スクリプティング」「DNS 情報の設定不備」「SQL インジェクション」などにより発生する、「本物サイト上での偽情報の表示」「ドメイン情報の挿入」「データの改ざん、消去」が全体の 8 割を占めています。今四半期は、「サーバ内ファイルの漏洩」が急増しました。これは、今四半期に「ディレクトリ・トラバーサル」の脆弱性が多く届出されたためです。



(8,519件の内訳、グラフの括弧内は前四半期までの数字)

図2-19. 届出累計の脆弱性がもたらす影響別割合



(過去2年間の届出内訳)

図2-20. 四半期ごとの脆弱性がもたらす影響別届出件数

2-2-4. 修正完了状況

図 2-21 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 4 四半期に修正を完了した 163 件のうち 110 件（67%）は、運営者へ脆弱関連情報を通知してから修正完了までの日数が 90 日以内の届出です。今四半期は、90 日以内に修正完了した届出の割合が、前四半期（183 件中 142 件（78%））より減少しています。

表 2-5 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を通知してから、90 日以内に修正が完了した累計および割合を四半期ごとに示しています。

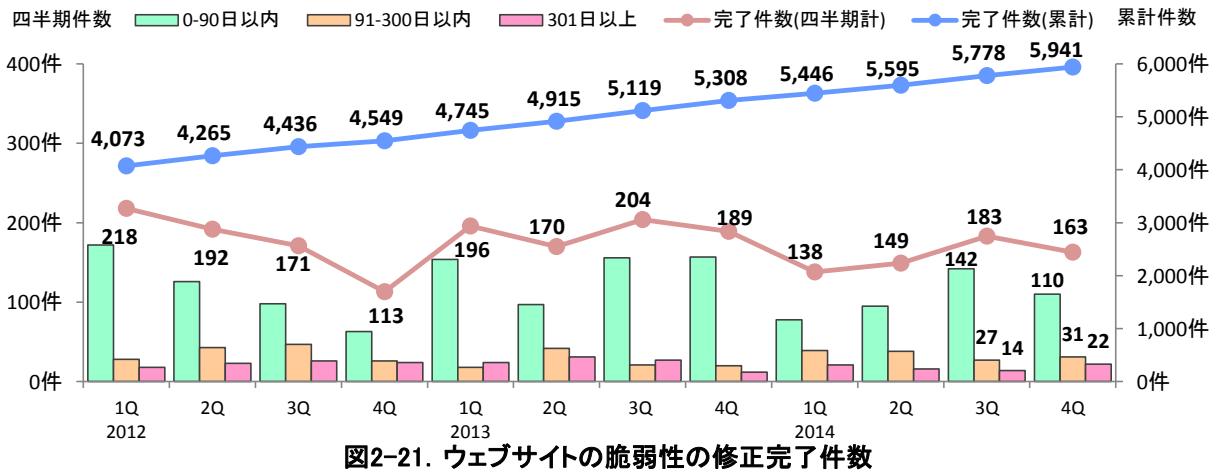


図2-21. ウェブサイトの脆弱性の修正完了件数

表 2-5. 90 日以内に修正完了した累計およびその割合の推移

	2012 1Q	2Q	3Q	4Q	2013 1Q	2Q	3Q	4Q	2014 1Q	2Q	3Q	4Q
修正完了件数	4,073	4,265	4,436	4,549	4,745	4,915	5,119	5,308	5,446	5,595	5,778	5,941
90 日以内の件数	2,706	2,832	2,930	2,993	3,147	3,244	3,400	3,557	3,635	3,730	3,872	3,982
90 日以内の割合	66%	66%	66%	66%	66%	66%	66%	67%	67%	67%	67%	67%

図 2-22、図 2-23 は、ウェブサイト運営者に脆弱性を通知してから修正されるまでに要した日数を脆弱性の種類別に分類し、その傾向を示しています[(*16)]。全体の 48%の届出が 30 日以内、全体の 67%の届出が 90 日以内に修正されています。

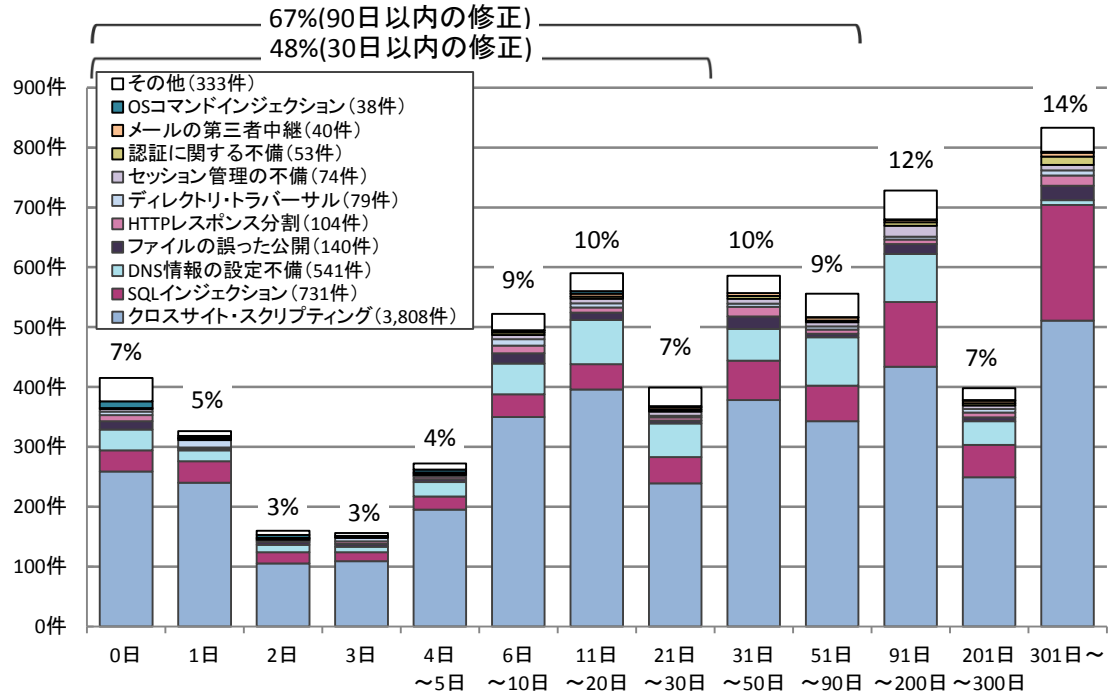


図2-22. ウェブサイトの修正に要した日数

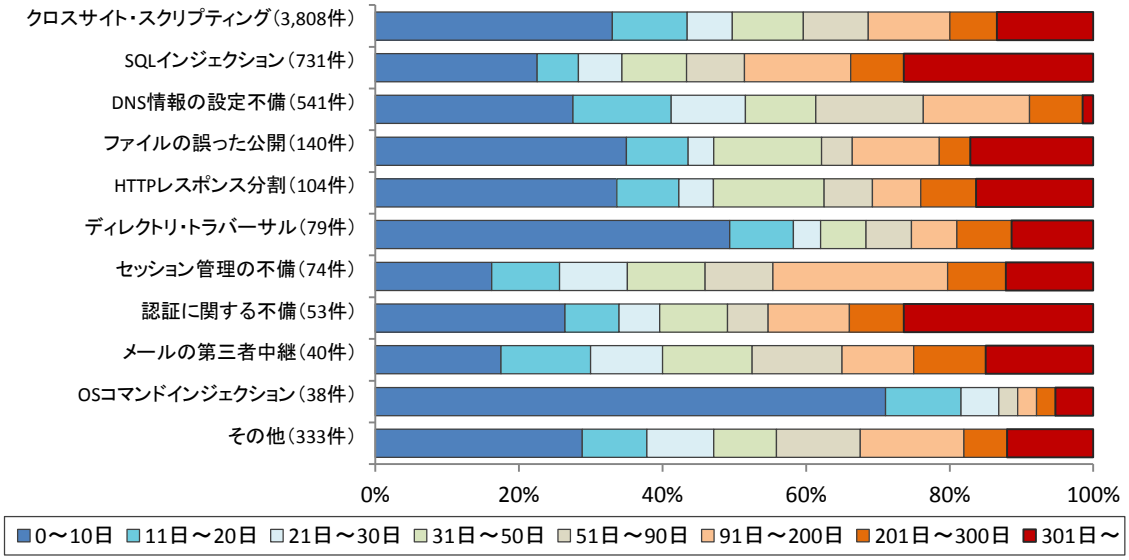


図2-23. ウェブサイトの修正に要した脆弱性種類別の日数の傾向

(*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。

2-2-5. 取扱中の状況

ウェブサイト運営者から脆弱性を修正した旨の報告が無い場合、IPA はウェブサイト運営者に 1～2 ヶ月毎に電子メールや電話、郵送などの手段でウェブサイト運営者に連絡を試み、脆弱性が悪用されて攻撃を受けた場合の危険性を分かりやすく解説し、脆弱性対策の実施を促しています。

図 2-24 は、ウェブサイトの脆弱性のうち、取扱いが長期化（IPA からウェブサイト運営者へ脆弱性を通知してから、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。これらの合計は 448 件（前四半期は 402 件）です。

取扱いが長期化しているものの中には、ウェブサイトの情報が盗まれてしまうなどの危険性がある、深刻度の高い SQL インジェクションという脆弱性も多く含まれています。

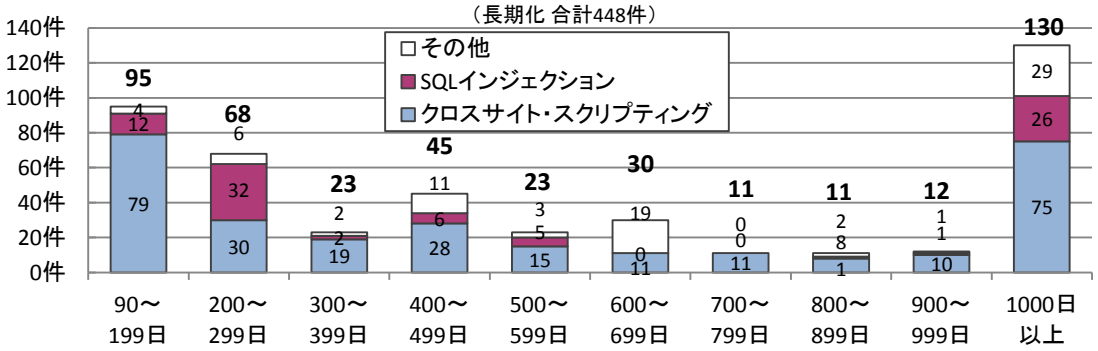


図2−24. 取扱いが長期化(90日以上経過)しているウェブサイトの経過日数と脆弱性の種類

表 2-6 は、過去 2 年間の四半期末時点で取扱い中の届出と、取扱いが長期化している届出の件数および、その割合を示しています。

表 2-6. 取扱いが長期化している届出件数および割合の四半期ごとの推移

	2013 1Q	2Q	3Q	4Q	2014 1Q	2Q	3Q	4Q
取扱い中の件数	474	473	504	505	490	596	676	886
長期化している件数	301	307	302	358	357	353	402	448
長期化している割合	64%	65%	60%	71%	73%	59%	59%	51%

3. 関係者への要望

脆弱性の修正促進のための、各関係者への要望は以下のとおりです。

3-1. ウェブサイト運営者

多くのウェブサイトで利用しているソフトウェア製品に脆弱性が発見されています。自身のウェブサイトでどのようなソフトウェア製品を利用しているかを把握し、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は、第三者に漏れないよう、適切に管理してください。

付表 1. ソフトウェア製品の脆弱性の原因分類

	脆弱性の原因	説明	届出において 想定された脅威
1	アクセス制御の不備	アクセス制御を行うべき個所において、アクセス制御が欠如している。	設定情報の漏洩 通信の不正中継 なりすまし 任意のスクリプトの実行 認証情報の漏洩
2	ウェブアプリケーションの脆弱性	ウェブアプリケーションに対し、入力された情報の内容の解釈や認証情報の取扱い、出力時の処理に問題がある。「クロスサイト・スクリプティング」攻撃や「SQL インジェクション」攻撃などに利用されてしまう。	アクセス制限の回避 価格等の改ざん サービス不能 資源の枯渇 重要情報の漏洩 情報の漏洩 セッション・ハイジャック 通信の不正中継 なりすまし 任意のコマンドの実行 任意のスクリプトの実行 任意のファイルへのアクセス 認証情報の漏洩
3	仕様上の不備	RFC 等の公開された規格に準拠して、設計、実装した結果、問題が生じるもの。	サービス不能 資源の枯渇
4	証明書の検証に関する不備	ウェブブラウザやメールクライアントソフトに証明書を検証する機能が実装されていない、または、検証が正しく行われずに、偽の証明書を受けいれてしまう。	証明書の確認不能 なりすまし
5	セキュリティコンテキストの適用の不備	本来、厳しい制限のあるセキュリティコンテキストで取り扱うべき処理を、緩い制限のセキュリティコンテキストで処理してしまう。	アプリケーションの異常終了 情報の漏洩 任意のコードの実行 任意のスクリプトの実行
6	バッファのチェックの不備	想定外の長さの入力が行われた場合に、長さをチェックせずバッファに入力してしまう。「バッファオーバーフロー」攻撃に利用されてしまう。	サービス不能 任意のコードの実行 任意のコマンドの実行
7	ファイルのパス名、内容のチェックの不備	処理の際のパラメータとして指定されているディレクトリ名やファイル名、ファイルの内容をチェックしていない。任意のディレクトリのファイルを指定できてしまい、「ディレクトリ・トラバーサル」攻撃に利用されてしまう。また、破損したファイルや不正に書き換えられたファイルを処理した際に不具合が生じる。	アプリケーションの異常終了 サービス不能 資源の枯渇 任意のファイルへのアクセス 認証情報の漏洩

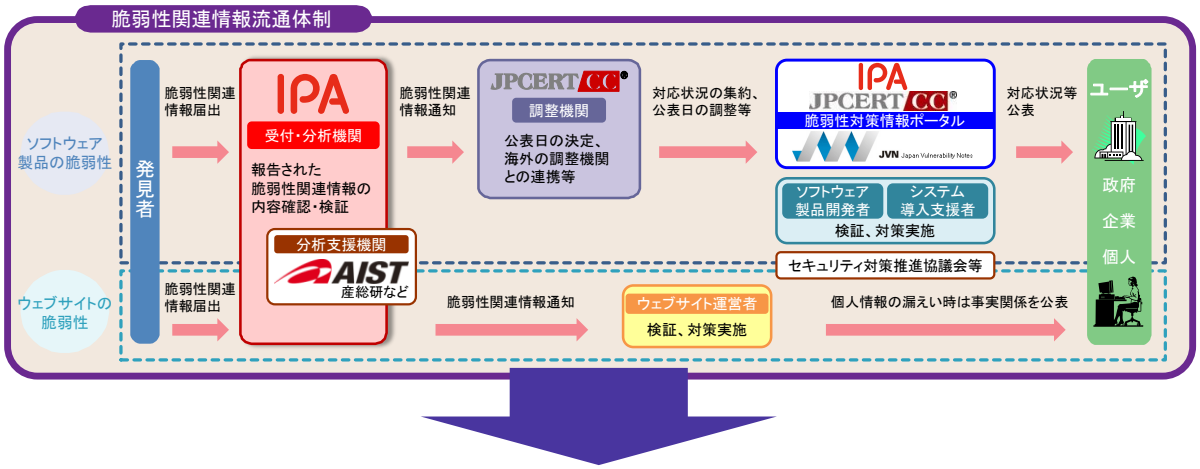
付表 2. ウェブサイトの脆弱性の分類

	脆弱性の種類	深刻度	説明	届出において想定された脅威
1	ファイルの誤った公開	高	一般に公開すべきでないファイルが公開されており、自由に閲覧できる状態になっている	個人情報の漏洩 サーバ内ファイルの漏洩 データの改ざん、消去 なりすまし
2	パス名パラメータの未チェック	高	ユーザからの入力を処理する際のパラメータとして指定されているファイル名を、ユーザが変更し、ウェブサーバ上の任意のディレクトリのファイルを指定できてしまう	サーバ内ファイルの漏洩
3	ディレクトリ･トラバーサル	高	ウェブサーバ上のディレクトリのアクセス権を超えて、本来許可されている範囲外のディレクトリにアクセスできる	個人情報の漏洩 サーバ内ファイルの漏洩
4	セッション管理の不備	高	セッション管理に、推測可能な情報を使用しているため、他のユーザの情報が容易に推測でき、他のユーザになりすまして、サービスを利用することができる	Cookie 情報の漏洩 個人情報の漏洩 なりすまし
5	SQL インジェクション	高	入力フォームなどへ SQL コマンド（データベースへの命令）を入力し、データベース内の情報の閲覧、更新、削除などができる	個人情報の漏洩 サーバ内ファイルの漏洩 データの改ざん、消去
6	DNS 情報の設定不備	高	DNS サーバに不適切な情報が登録されているため、第三者がそのドメイン名の持ち主であるかのようにふるまえてしまう	ドメイン情報の挿入
7	オープンプロキシ	中	外部の第三者により、他のサーバへのアクセスを中継するサーバとして利用され、不正アクセスなどの際にアクセス元を隠すための踏み台にされてしまう	踏み台
8	クロスサイト･スクリプティング	中	ユーザの Cookie 情報を知らないうちに転送させたり、偽の情報を表示させたりするような罠のリンクをユーザにクリックさせ、個人情報等を盗むことができる	Cookie 情報の漏洩 サーバ内ファイルの漏洩 個人情報の漏洩 データの改ざん、消去 なりすまし 本物サイト上への偽情報の表示
9	クロスサイト・リクエスト・フォージェリ	中	ユーザを罠のページに誘導することで、そのユーザが登録済みのサイトにひそかにアクセスさせ、登録情報の変更や商品の購入をさせることができる	データの改ざん、消去
10	HTTP レスポンス分割	中	攻撃者がユーザに対し、悪意のある要求をウェブサーバに送信するように仕向けることで、ウェブサーバからの応答を分割させて応答内容をすり替え、ユーザに対して偽のページを表示させることができる	ウェブキャッシュ情報のすり替え
11	セキュリティ設定の不適切な変更	中	ユーザに対し、ソフトウェアをインストールさせたり、ブラウザのセキュリティレベルを下げるよう指示することでクライアント PC のセキュリティ設定を低下させる	利用者のセキュリティレベルの低下
12	リダイレクタの不適切な利用	中	ウェブサーバに設置したリダイレクタが悪意あるリンクへの踏み台にされたり、そのウェブサイト上で別のサイト上のページを表示させられてしまう	踏み台 本物サイト上への偽情報の表示

	脆弱性の種類	深刻度	説明	届出において想定された脅威
13	フィルタリングの回避	中	ウェブサイトのサービスやブラウザの機能として提供されているフィルタリング機能が回避される問題。これにより、本来制限されるはずのウェブページを閲覧してしまう	利用者のセキュリティレベルの低下 なりすまし
14	OS コマンド・インジェクション	中	攻撃者がウェブアプリケーションを介してウェブサーバの OS コマンドを実行できてしまい、サーバ内ファイルの閲覧やシステム操作、不正なプログラムの実行などを行われてしまう	任意のコマンドの実行
15	メールの第三者中継	低	利用者が入力した内容を管理者が指定したメールアドレスに送信する機能で、外部の利用者が宛先メールアドレスを自由に指定できてしまい、迷惑メール送信の踏み台に悪用される	メールシステムの不正利用
16	HTTPS の不適切な利用	低	HTTPS による暗号化をしているが、暗号の選択や設定が十分でなかったり、ウェブサイトでのユーザへの説明に間違いがある、または、ウェブサイトの設計上、ユーザから証明書が確認できない	なりすまし
17	価格等の改ざん	低	ショッピングサイトにおいて、価格情報等が利用者側で書き換えられる。書き換えによる被害は、ウェブサイト側に限定される	データの改ざん

・API : Application Program Interface
・CGI : Common Gateway Interface
・DNS : Domain Name System
・HTTP : Hypertext Transfer Protocol
・HTTPS : Hypertext Transfer Protocol Security
・ISAKMP : Internet Security Association Key Management Protocol
・MIME : Multipurpose Internet Mail Extension
・RFC : Request For Comments
・SQL : Structured Query Language
・SSI : Server Side Include
・SSL : Secure Socket Layer
・TCP : Transmission Control Protocol
・URI : Uniform Resource Identifier
・URL : Uniform Resource Locator

付図１．「情報セキュリティ早期警戒パートナーシップ」（脆弱性関連情報取扱いの枠組み）



【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