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

[2015 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

日本における公的な脆弱性関連情報の取扱制度である「情報セキュリティ早期警戒パートナーシップ（本報告書では本制度と記します）」は、「ソフトウエ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、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脆弱性対策情報の公表に向けた調整などの業務を実施しています。

本報告書では、2015 年 10 月 1 日から 2015 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記載しています。

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
2016 年 1 月 27 日

目次

1. 2015 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は 11,494 件 ～

表 1-1 は本制度[*1]における届出状況についてです。2015 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 134 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 87 件、合計 221 件でした。届出受付開始からの累計は 11,494 件で、内訳はソフトウェア製品に関するもの 2,376 件、ウェブサイトに関するもの 9,118 件でウェブサイトに関する届出が全体の約 8 割を占めています。

表 1-1. 届出件数

分類	今期件数	累計
ソフトウェア製品	**134** 件	**2,376** 件
ウェブサイト	**87** 件	**9,118** 件
合計	**221** 件	**11,494** 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。今四半期は前期同様、ソフトウェア製品に関する届出がウェブサイトに関する届出よりも多数を占めました。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 4.11 [*2] 件でした。

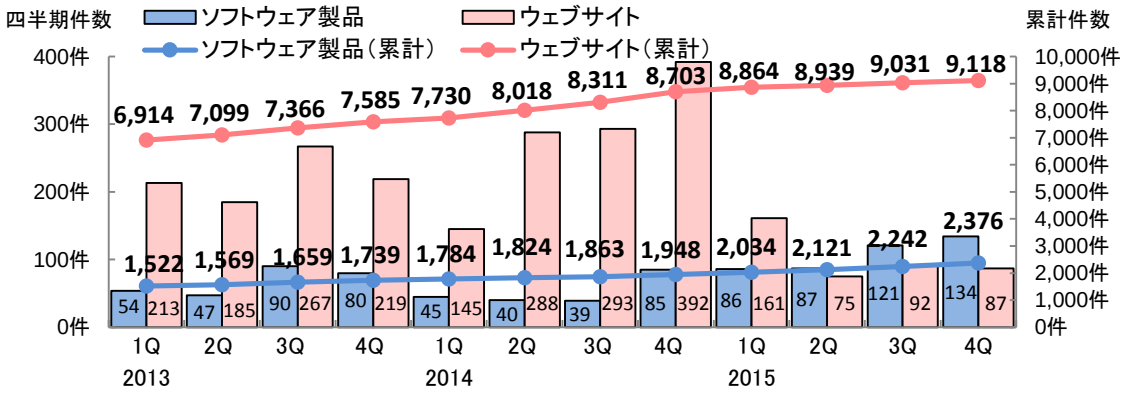


図1-1. 脆弱性の届出件数の四半期ごとの推移

表 1-2. 届出件数（過去 3 年間）

	2013 1Q	2Q	3Q	4Q	2014 1Q	2Q	3Q	4Q	2015 1Q	2Q	3Q	4Q
累計届出件数[件]	8,436	8,668	9,025	9,324	9,514	9,842	10,174	10,651	10,898	11,060	11,273	11,494
1 就業日あたり[件/日]	3.96	3.96	4.00	4.03	4.01	4.04	4.07	4.17	4.17	4.13	4.12	4.11

[*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
https://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 2015 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）でした。2015 年はソフトウェア製品が 428 件、ウェブサイトが 415 件の合計 843 件でした。また、今年はソフトウェア製品の届出件数が過去最多、かつウェブサイトより多い年となりました。

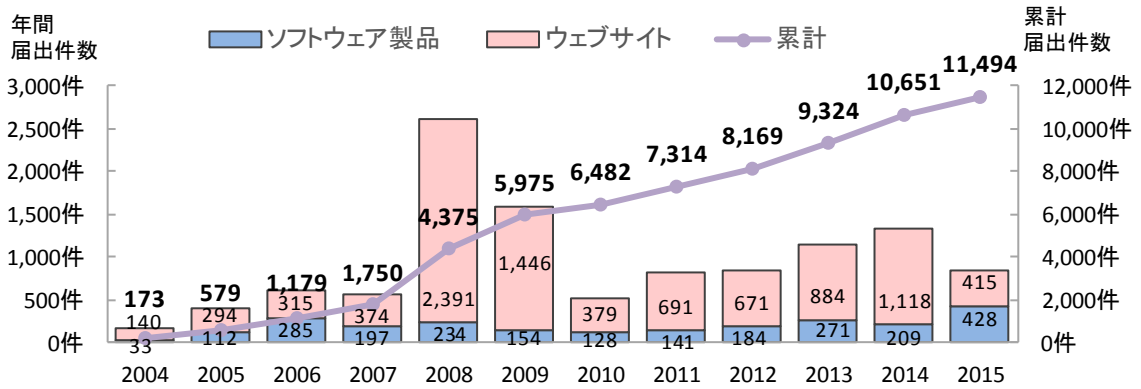


図1−2. 脆弱性関連情報の届出件数の年ごとの推移

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は累計 7,712 件～

表 1-3 は今四半期、および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。ソフトウェア製品の場合、修正が完了すると JVN に公表しています（回避策の公表のみでプログラムの修正をしていない場合を含む）。

表 1-3. 修正完了（JVN 公表）

分類	今期件数	累計
ソフトウェア製品	**52** 件	**1,147** 件
ウェブサイト	**84** 件	**6,565** 件
合計	**136** 件	**7,712** 件

今四半期に JVN 公表したソフトウェア製品の件数は 52 件 [*3]（累計 1,147 件）でした。そのうち、2 件は製品開発者による自社製品の脆弱性の届出でした。なお、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 9 件（17%）でした。

また、修正完了したウェブサイトの件数は 84 件（累計 6,565 件）でした。これらは届出を受け、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です。修正を完了した 84 件のうち、ウェブアプリケーションを修正したものは 59 件（70%）、当該ページを削除したものは 25 件（30%）で、運用で回避したものは 0 件でした。なお、修正を完了した 84 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 38 件（45%）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（129 件中 43 件（33%））より増加しています。

また、図 1-3 は、届出開始から 2015 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。2015 年は、ソフトウェア製品が 188 件、ウェブサイトが 624 件の合計 812 件でした。2015 年はソフトウェア製品の修正件数が、最も多かった 1 年でした。

[*3] P.10 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。

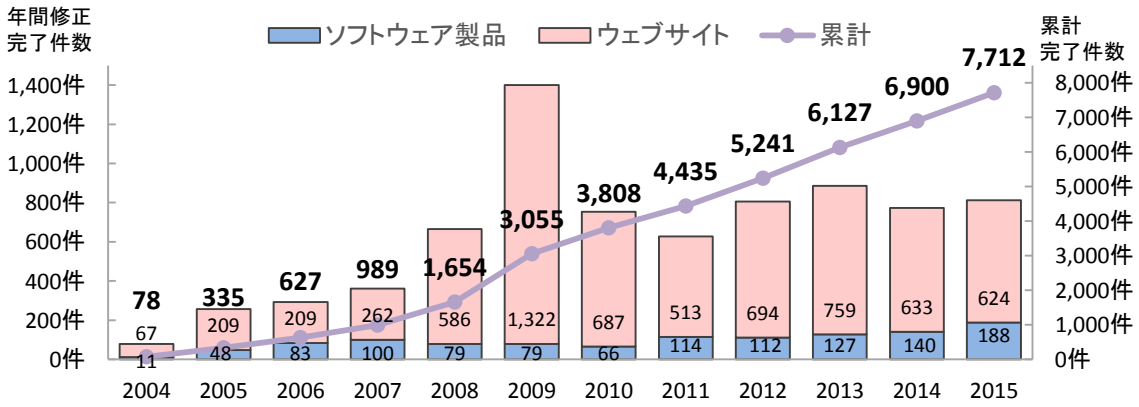


図1−3. 脆弱性関連情報の修正完了件数の年ごとの推移

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、当該製品開発者名等を公表して情報提供を求めています[(*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、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。

今四半期は、3 件について製品開発者と連絡が取れたため調整を再開しました。新たに連絡が取れない製品開発者名の公表はありませんでした。また、公表判定委員会での審議を経て、脆弱性情報が JVN に公表されたものもありませんでした。

2015 年 12 月末時点の連絡不能開発者の累計公表件数は 217 件、その内製品情報を公表しているものは 174 件となりました。

(*6) 連絡不能開発者一覧：https://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や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

7 社 [*8] のルータにクリックジャッキングの脆弱性

～組み込まれたウェブアプリケーションにもセキュリティ意識を～

2015 年第 4 四半期は、52 件の脆弱性対策情報が JVN に公表されました。そのうち 9 件（17%）は、家庭用ルータ、ネットワークカメラおよびファイアウォールといった組込み機器の脆弱性でした（表 1-4）。

表 1-4. 今四半期、JVN 公表された「組込み機器」に関連する脆弱性

公表日	JVN番号	製品の種類	タイトル
10月30日	JVN#48135658	ルータ	複数のルータ製品におけるクリックジャッキングの脆弱性
11月 6日	JVN#90135579	ファイアウォール	「SonicWall TotalSecure TZ 100 シリーズ」におけるサービス運用妨害 (DoS) の脆弱性
12月 9日	JVN#89965717	ルータ	「WL-330NUL」におけるクロスサイト・スクリプティングの脆弱性
12月 9日	JVN#34489380	ルータ	「WL-330NUL」において任意のコマンドを実行される脆弱性
12月 9日	JVN#85359294	ルータ	「WL-330NUL」におけるサービス運用妨害 (DoS) の脆弱性
12月 9日	JVN#69462495	ルータ	「WL-330NUL」における情報管理不備の脆弱性
12月25日	JVN#51349622	ルータ	「CG-WLBARGS 」における認証不備の脆弱性
12月25日	JVN#50775659	ルータ	「CG-WLBARAGM」がオープンプロキシとして機能してしまう問題
12月25日	JVN#51250073	ネットワークカメラ	「CG-WLNCM4G」がオープンリゾルバとして機能してしまう問題

上記の赤枠はクリックジャッキングの脆弱性で、初の JVN 公表でした。また、この公表では複数の製品開発者のルータのクリックジャッキングの脆弱性が掲載されました [*9]。

クリックジャッキングの脆弱性とは、正常なページを装った悪意あるページを作成し、その上に利用者が本来目にするはずの正規のページを“透明化”し重ね、利用者に悪意あるページをクリック操作させようとする手口です。ルータのウェブ管理画面にクリックジャッキングの脆弱性が存在すると、利用者には正規のページが目に見えず、表示された悪意あるページをそうとは知らずクリックした場合、意図しない設定変更や操作を実行してしまう可能性があります。その結果、第三者にルータを不正利用される可能性があります。なお、IPA では 2013 年にクリックジャッキングの手口と対策を解説したレポートを公開していますので参考にしてください [*10]。

クリックジャッキングの脆弱性を悪用する攻撃は次の 2 つのページが用意されます。

1. 正常なページを装った悪意あるページ。利用者にはこのページが見えている。
   （図 1-4.ページ A）
2. 悪意により透明化させた正規のページ。
   （図 1-4.ページ B）

図 1-4 をもとに、利用者の操作イメージを記載します。たとえば、メール文中の URL をクリックするなど、何らかの手段で誘導され攻撃者が用意したウェブページにアクセスしてしまうと、表示されるのは悪意あるウェブページ（ページ A）です。しかし、実際にはページ A の手前に正規のページ B が表示されていますが、透明化されており利用者には見えていません。

図のように、ページ A には利用者がボタンをクリックしてしまいそうな「クリックで 5 万円プ

[*8] 2016 年 1 月 21 日時点の各社における当該脆弱性に関する情報を IPA が調べたもの。
[*9] JVN「JVN#48135658 複数のルータ製品におけるクリックジャッキングの脆弱性」
https://jvn.jp/jp/JVN48135658/index.html
[*10] IPA テクニカルウォッチ「知らぬ間にプライバシー情報の非公開設定を公開設定に変更されてしまうなどの『クリックジャッキング』に関するレポート」https://www.ipa.go.jp/about/technicalwatch/20130326.html

レゼント！」などと表示されています。もし利用者が表示されているページ A のボタンをクリックした場合、ページ A の手前に重ねられた透明の正規のページ B の「設定の初期化」をクリックしてしまうことになります。ページ B はルータの利用者に用意された正規のページですが、透明化されているため、利用者自らのクリックであるにもかかわらず、そうとは知らない間に設定が変更されてしまうことになります。（図 1-4）。

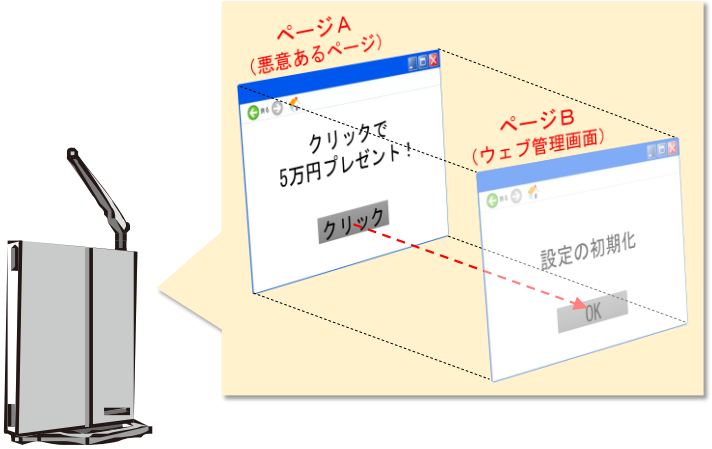


図 1-4. クリックジャッキングの脆弱性を悪用された場合のイメージ

既に市場に流通している組込み機器に脆弱性があった場合、利用者への修正プログラムの提供など、迅速な対策が難しい場合があります。また、利用者にも脆弱性対策の必要が生じます。開発者、利用者は以下の通り、それぞれの立場で求められる対策を行う必要があります。

・製品開発者

前述のようなルータのウェブ管理画面は機器に組み込まれたウェブアプリケーションといえます。機器の利用と管理を容易にするためのウェブアプリケーションの開発には、クリックジャッキングに限らず、脆弱性が作りこまれる可能性があります。組込み機器のウェブアプリケーション開発では要件定義、設計、開発といった各工程の仕様の明確化、出荷前検査等の対策が自組織のみならず委託先組織へも求められます。

また、脆弱性が見つかった場合、開発者は早急に修正（修正プログラムの提供）を行う必要があります。

IPA が行った調査で、セキュリティパッチの更新をしないと回答した人にその理由を聞いたところ、最多だったのは 30.5%の「書かれている内容がわからない」でした(*11)。このことから、開発者は修正パッチの作成・提供にとどまらず、利用者には修正プログラム適用の周知と必要性の啓発、さらに利用者が容易に適用できるような工夫が求められます(*12)。

・利用者

製品開発者による修正が行われた場合、製品開発者からの情報をもとに速やかに修正プログラムの適用を行うことが求められます。また、利用している製品について、製品開発者のサポートページを定期的に確認するといった行動が、早急な脆弱性対策につながります。

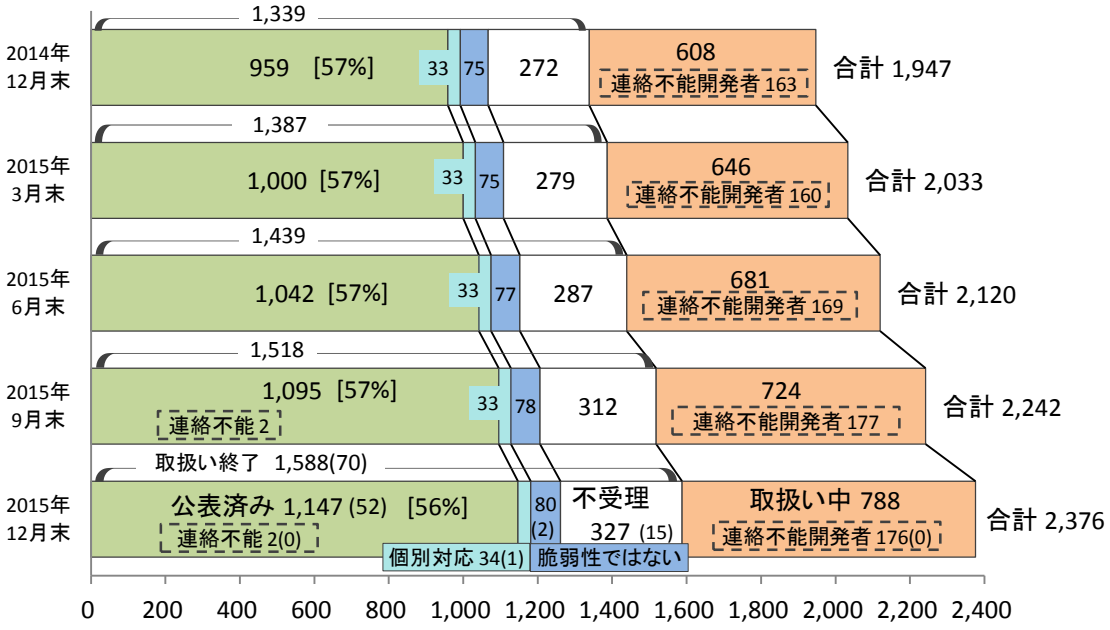
(*11) 「2015 年度情報セキュリティの脅威に対する意識調査」P76：
https://www.ipa.go.jp/security/fy27/reports/ishiki/index.html
(*12) 「ソフトウエア製品開発者による脆弱性対策情報の公表マニュアル」：
https://www.ipa.go.jp/files/000044734.pdf

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。2015 年 12 月末時点の届出の累計は 2,376 件で、今四半期に脆弱性対策情報を JVN 公表したものは 52 件（累計 1,147 件）でした。このうち、製品開発者が JVN 公表を行わず「個別対応」したものは 1 件（累計 34 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 80 件）、「不受理」としたものは 15 件 (*13)（累計 327 件）、取扱い中は 788 件でした。788 件のうち、連絡不能開発者 (*14) 一覧へ新規に公表したものは 0 件で、2015 年 12 月末時点で 176 件が公表中です。



( ) 内の数値は今四半期に処理を終了もしくは連絡不能開発者となった件数
[ ] 内の数値は受理した届出のうち公表した割合

取扱い終了
- 公表済み：JVN で脆弱性への対応状況を公表したもの
- 連絡不能：公表判定委員会による審議にて、JVN で公表することが適当と判定されたもの
- 個別対応：JVN 公表を行わず、製品開発者が個別対応したもの
- 脆弱性ではない：製品開発者により脆弱性ではないと判断されたもの
- 不受理：告示で定める届出の対象に該当しないもの
- 取扱い中：製品開発者が調査、対応中のもの
- 連絡不能開発者：取扱い中のうち、連絡不能開発者一覧にて公表中のもの

図 2-1. ソフトウェア製品脆弱性の届出処理状況（四半期ごとの推移）

(*13) 内訳は今四半期の届出によるもの 3 件、前四半期までの届出によるもの 12 件。
(*14) 連絡不能開発者一覧への公表および一覧からの削除が複数回行われ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、今までに届出のあったソフトウェア製品の脆弱性 2,376 件のうち、不受理を除いた 2,049 件の届出を分析した結果を記載します。

2-1-2. ソフトウェア製品種類別届出件数

図 2-2、2-3 のグラフは、届出された脆弱性の製品種類別の分類です。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 40%となっています。今四半期の届出件数で最も多いのも「ウェブアプリケーションソフト」で、次いで多いのは、「ウェブブラウザ」となっています。

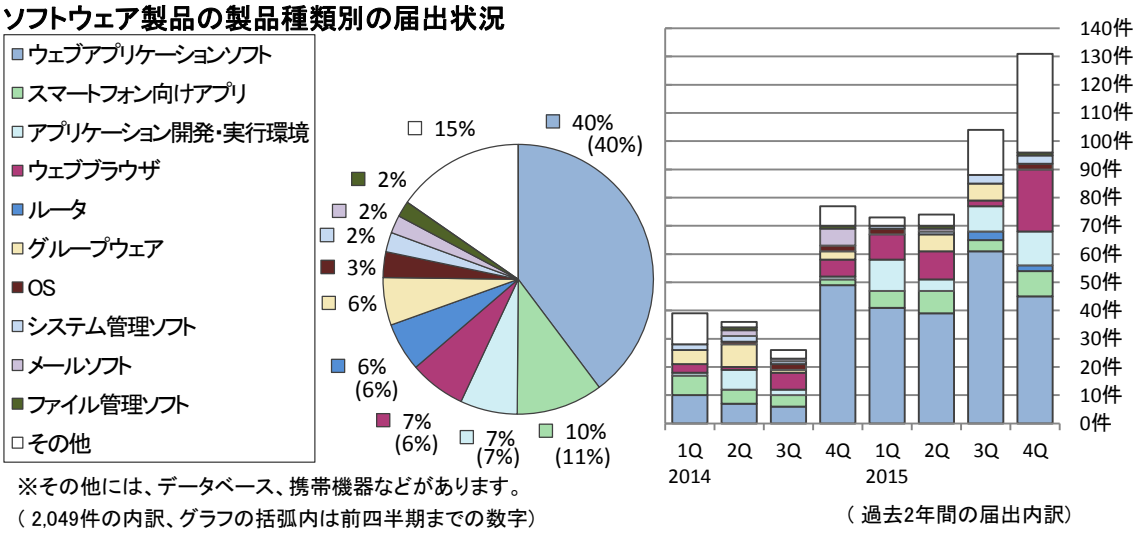


図2-2. 届出累計の製品種類別割合

図2-3. 四半期ごとの製品種類別届出件数

図 2-4、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。

累計の割合は、オープンソースソフトウェアではない「それ以外」が 67%を占め、四半期別で見ると、今四半期は過去 2 年間で初めてオープンソースソフトウェアを上回りました。

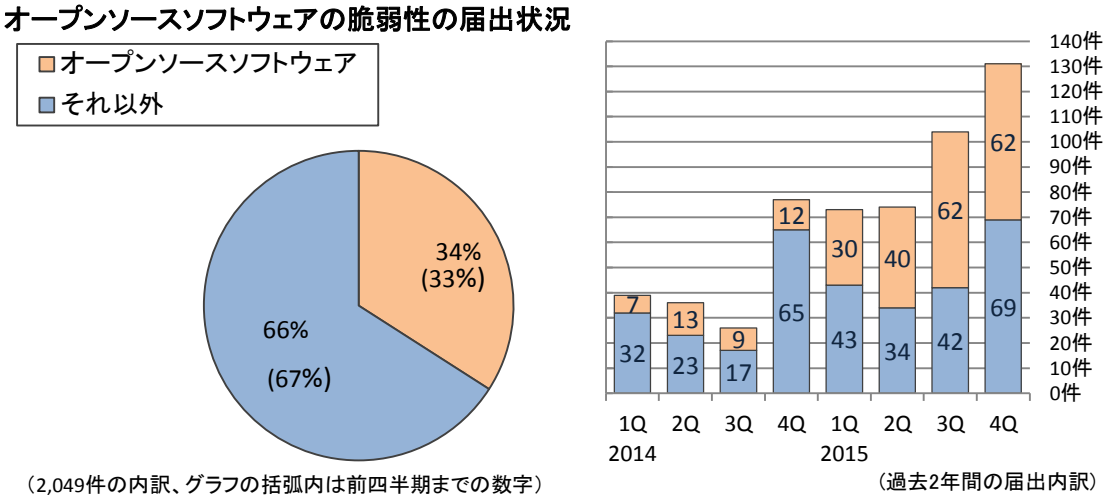


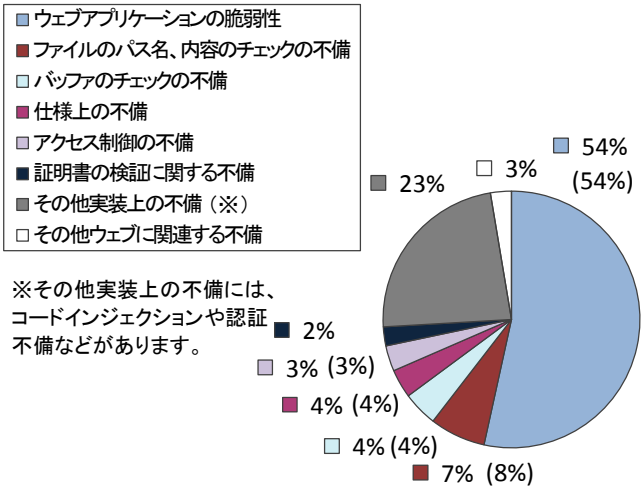
図2-4. 届出累計のオープンソースソフトウェア割合

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

2-1-3. 脆弱性の原因と影響別件数

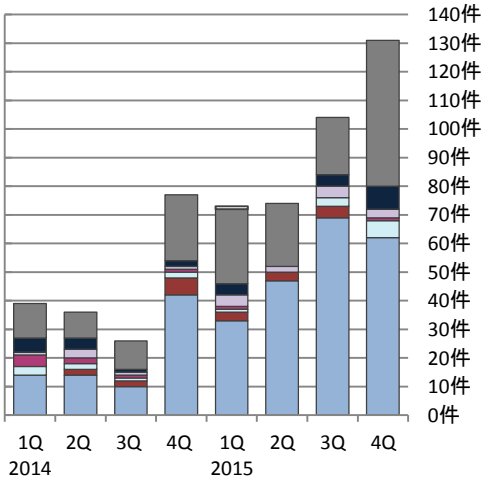
図 2-6、2-7 のグラフは、届出された脆弱性の原因を示しています。図 2-6 は届出累計の脆弱性の原因別割合を、図 2-7 は過去 2 年間の原因別の届出件数の推移を四半期ごとに示しています。累計では、「ウェブアプリケーションの脆弱性」が過半数を占めています。

ソフトウェア製品の脆弱性の原因別の届出状況



（2,049件の内訳、グラフの括弧内は前四半期までの数字）

図2-6. 届出累計の脆弱性の原因別割合

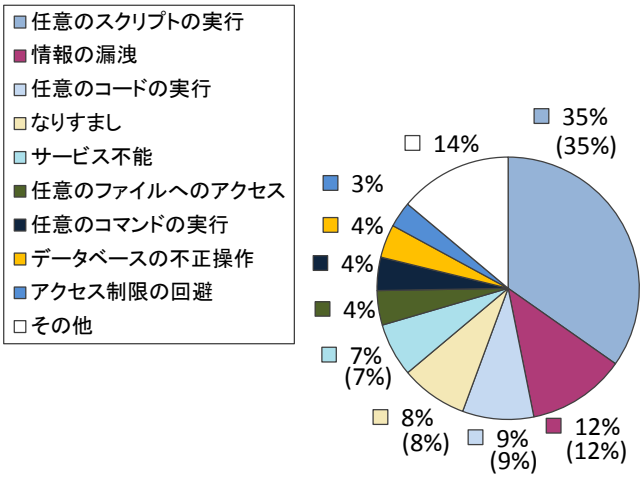


（過去2年間の届出内訳）

図2-7. 四半期ごとの脆弱性の原因別届出件数

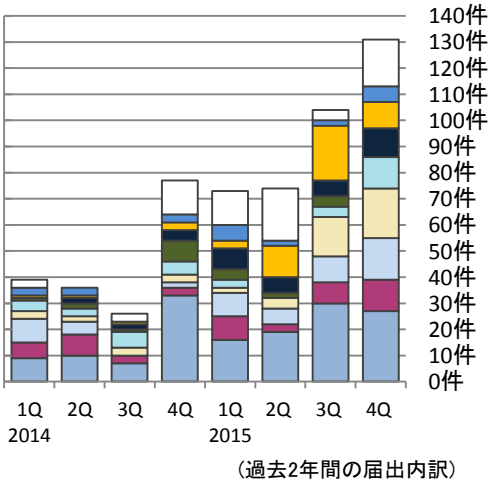
図 2-8、2-9 のグラフは、届出された脆弱性がもたらす影響を示しています。図 2-8 は届出累計の影響別割合を、図 2-9 は過去 2 年間の影響別届出件数の推移を四半期ごとに示しています。累計では「任意のスクリプトの実行」が最も多く、35%となっています。今四半期は、「任意のスクリプトの実行」が最も多く、次いで多かったのは「なりすまし」でした。

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



（2,049件の内訳、グラフの括弧内は前四半期までの数字）

図2-8. 届出累計の脆弱性がもたらす影響別割合



（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、国内外の関係者と脆弱性対策情報の公表に向けた調整を行っています[*15]。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 : https://jvn.jp/ ）に公表しています。表 2-1、図 2-10 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	52 件	1,147 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	42 件	1,319 件
	合計	94 件	2,466 件

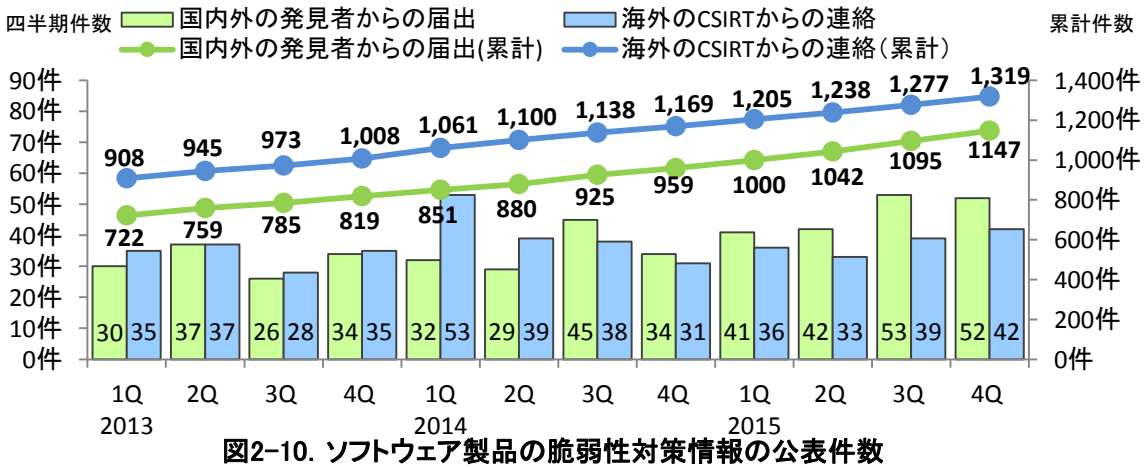


図2−10. ソフトウェア製品の脆弱性対策情報の公表件数

（1） JVN で公表するまでに要した日数で分類した“国内外の発見者および製品開発者から届出を受けた”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（1,147 件）について、図 2-11 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 30%、45 日を超過した件数は 70%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。

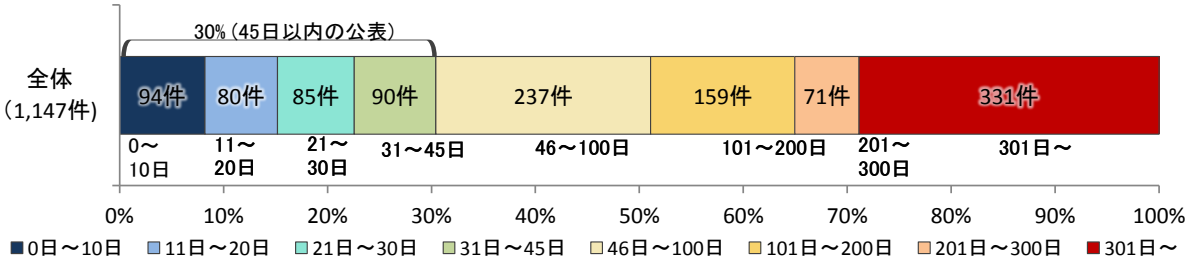


図2−11. ソフトウェア製品の脆弱性公表日数

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）

2013 1Q	2Q	3Q	4Q	2014 1Q	2Q	3Q	4Q	2015 1Q	2Q	3Q	4Q
33%	33%	33%	34%	34%	34%	33%	33%	32%	31%	31%	30%

[*15] JPCERT/CC 活動概要 Page16～23（https://www.jpcert.or.jp/pr/2016/PR20160114.pdf）を参照下さい。

表 2-3 は国内の発見者および製品開発者から受けた届出 52 件について、今四半期に JVN 公表した脆弱性を深刻度のレベル別に示しています。内訳はオープンソースソフトウェアに関する脆弱性が 23 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 2 件（表 2-3 の#2）、複数開発者・製品に影響がある脆弱性が 1 件（表 2-3 の#3）、組込みソフトウェア製品の脆弱性が 8 件（表 2-3 の#4）、制御システムの脆弱性が 1 件（表 2-3 の#5）ありました。

表 2-3. 2015 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（#5）	Canary Labs 製「Trend Web Server」におけるバッファオーバーフローの脆弱性	データ可視化ソフト「Trend Web Server」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。	2015 年 10 月 1 日	7.5
2（#2）	「サイボウズ ガルーン」において任意の PHP コードが実行される複数の脆弱性	グループウェア「サイボウズ ガルーン」には、任意の PHP コードが実行される脆弱性が複数存在しました。このため、当該製品にログイン可能なユーザによって、サーバ上で任意の PHP コードを実行される可能性がありました。	2015 年 10 月 7 日	8.5
3（#2）	「サイボウズ ガルーン」における LDAP 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、ログイン認証に起因する LDAP インジェクションの脆弱性が存在しました。このため、当該製品に不正にログインされたり、認証サーバの情報が漏えいしたりする可能性がありました。	2015 年 10 月 7 日	7.0
4（#1）	「縁 sys」における SQL インジェクションの脆弱性	グループウェア「縁 sys」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。	2015 年 10 月 29 日	7.5
5（#4）	「CG-WLBARGS」における認証不備の脆弱性	無線 LAN ルータ「CG-WLBARGS」には、認証不備の問題がありました。このため、第三者により管理画面にログインされる可能性がありました。	2015 年 12 月 25 日	10.0
脆弱性の深刻度=レベル II（警告）、CVSS 基本値=4.0～6.9				
6（#1）	「AjaXplorer」におけるディレクトリ・トラバーサルの脆弱性	ファイル共有ソフト「AjaXplorer」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、第三者によりサーバ上の任意のファイルを閲覧される可能性がありました。	2015 年 10 月 1 日	4.0
7（#1）	Windows 版「Python」における任意の DLL 読み込みに関する脆弱性	プログラミング言語「Python」には、DLL を読み込む際の検索パスに問題がありました。このため、第三者により任意のコードを実行される可能性がありました。	2015 年 10 月 1 日	6.8
8（#1）	「gollum」における任意のファイルを閲覧される脆弱性	wiki システム「gollum」サーバ上の任意のファイルを閲覧される脆弱性がありました。このため、遠隔の第三者によって、サーバ上の任意のファイルを閲覧される可能性がありました。	2015 年 10 月 2 日	4.3
9（#1）	「Dojo Toolkit」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作成ソフト「Dojo Toolkit」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。	2015 年 10 月 9 日	4.3
10（#1）	「phpRechnung」における SQL インジェクションの脆弱性	会計ソフト「phpRechnung」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。	2015 年 10 月 9 日	6.5

項番	脆弱性	セキュリティ上の問題点	JVN 公表日	CVSS 基本値
11 (#1)	「島根県 CMS」における SQL インジェクションの脆弱性	コンテンツ管理システム「島根県 CMS」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。	2015 年 10 月 9 日	6.5
12	iOS 版「Party Track SDK」におけるサーバ証明書の検証不備	効果測定システムをスマートフォンアプリに実装する「Party Track SDK」には、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なわれる可能性がありました。	2015 年 10 月 14 日	4.0
13 (#1)	「eXtplorer」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	ファイル管理ソフト「eXtplorer」には、クロスサイト・リクエスト・フォージェリの脆弱性が存在しました。このため、第三者により意図しない操作をさせられる可能性がありました。	2015 年 10 月 15 日	5.1
14	「アバスト」におけるディレクトリ・トラバーサルの脆弱性	アンチウイルスソフト「アバスト」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、第三者によりシステム上の任意のファイルを削除される可能性がありました。	2015 年 10 月 16 日	4.3
15 (#1)	「EC-CUBE」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システム「EC-CUBE」には、クロスサイト・リクエスト・フォージェリの脆弱性が存在しました。このため、第三者により意図しない操作をさせられる可能性がありました。	2015 年 10 月 26 日	5.1
16	スマートフォンアプリ「ANA」における SSL サーバ証明書の検証不備の脆弱性	スマートフォンアプリ「ANA」には、SSL 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解読などが行なわれる可能性がありました。	2015 年 10 月 28 日	4.0
17 (#1)	「縁 sys」における任意のファイルを作成される脆弱性	グループウェア「縁 sys」には、任意のファイルを作成される脆弱性がありました。このため、第三者によって、サーバ上に任意のファイルを作成される可能性がありました。	2015 年 10 月 29 日	6.5
18 (#1)	「縁 sys」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「縁 sys」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。	2015 年 10 月 29 日	4.3
19 (#1)	「縁 sys」におけるアクセス制限不備の脆弱性	グループウェア「縁 sys」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が管理しているファイルを取得される可能性がありました。	2015 年 10 月 29 日	5.0
20 (#1)	「ISUCON5 予選ポータル用 Web アプリケーション (eventapp)」における OS コマンド・インジェクションの脆弱性	ウェブアプリケーションのパフォーマンス改善コンテスト ISUCON5 の予選で使用されたソフト「ISUCON5 予選ポータル用 Web アプリケーション (eventapp)」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、当該製品にログインしているユーザにより任意の OS コマンドを実行させられる可能性がありました。	2015 年 11 月 2 日	6.5
21	TYPE-MOON 製の複数のゲーム製品における OS コマンド・インジェクションの脆弱性	TYPE-MOON 製の複数のゲーム製品には、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、細工されたセーブデータを読み込むことで、任意の OS コマンドを実行される可能性がありました。	2015 年 11 月 5 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
22	「SonicWall TotalSecure TZ 100 シリーズ」におけるサービス運用妨害(DoS)の脆弱性	UTM アプライアンス「SonicWall TotalSecure TZ 100 シリーズ」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。	2015 年 11 月 6 日	5.0
23 (#1)	「pWebManager」における OS コマンド・インジェクションの脆弱性	コンテンツ管理システム「pWebManager」には、OS コマンド･インジェクションの脆弱性の脆弱性がありました。このため、当該製品にログイン可能なユーザによって、任意の OS コマンドを実行される可能性がありました。	2015 年 11 月 13 日	6.5
24 (#1)	「アプリカン」におけるスクリプト・インジェクションの脆弱性	アプリケーション開発支援ソフト｢アプリカン｣には、SSID の処理に起因する、スクリプト・インジェクションの脆弱性がありました。このため、結果として任意の API を実行される可能性がありました。項番 25 とは異なる問題です。	2015 年 11 月 17 日	5.4
25 (#1)	「アプリカン」におけるスクリプト・インジェクションの脆弱性	アプリケーション開発支援ソフト｢アプリカン｣には、URL の処理に起因する、スクリプト・インジェクションの脆弱性がありました。このため、結果として任意の API を実行される可能性がありました。項番 24 とは異なる問題です。	2015 年 11 月 17 日	6.8
26	iOS アプリ「ぐるなび」における SSL サーバ証明書の検証不備の脆弱性	iOS アプリ「ぐるなび」には、SSL 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解読などが行なわれる可能性がありました。	2015 年 11 月 17 日	4.0
27	「Kirby」における任意のファイルを作成される脆弱性	コンテンツ管理システム「Kirby」には、任意のファイルを作成される脆弱性が存在しました。このため、結果として、任意の PHP コードを実行される可能性がありました。	2015 年 11 月 17 日	6.5
28 (#1)	「Void」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「Void」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。	2015 年 11 月 20 日	4.3
29	「ArcSight Management Center」および「ArcSight Logger」におけるクロスサイト・スクリプティングの脆弱性	ログ分析ソフト「ArcSight Management Center」および「ArcSight Logger」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。	2015 年 11 月 20 日	5.0
30	「ManageEngine Firewall Analyzer」におけるディレクトリ・トラバーサルの脆弱性	ログ解析ソフトウェア「ManageEngine Firewall Analyzer」には、ディレクトリ・トラバーサルの脆弱性がありました。このため、第三者によりファイルを閲覧される可能性がありました。	2015 年 11 月 27 日	4.0
31	「ManageEngine Firewall Analyzer」におけるアクセス制限不備の脆弱性	ログ解析ソフト「ManageEngine Firewall Analyzer」には、アクセス制限不備の脆弱性がありました。このため、第三者によって、当該製品のサーバログを取得される可能性がありました。	2015 年 11 月 27 日	5.0
32 (#1)	「Apache Cordova」におけるアクセス制限不備の脆弱性	アプリケーションフレームワーク｢Apache Cordova｣には、アクセス制限不備の脆弱性がありました。このため､ホワイトリストによるアクセス制限を回避される可能性がありました。	2015 年 11 月 27 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
33	「フレーム高速チャット」におけるクロスサイト・スクリプティングの脆弱性	チャット掲示板「フレーム高速チャット」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。	2015 年 11 月 30 日	4.3
34	「p++BBS」におけるクロスサイト・スクリプティングの脆弱性	チャット掲示板「p++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。	2015 年 11 月 30 日	5.0
35 （#1）	EC-CUBE 用プラグイン「管理画面表示制御プラグイン」における SQL インジェクションの脆弱性	EC-CUBE 用プラグイン「管理画面表示制御プラグイン」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。	2015 年 12 月 3 日	4.0
36	iOS アプリ「GANMA！」における SSL サーバ証明書の検証不備の脆弱性	iOS アプリ「GANMA！」には、SSL 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解読などが行なわれる可能性がありました。	2015 年 12 月 7 日	4.0
37	「アクセス解析」におけるクロスサイト・スクリプティングの脆弱性	アクセス解析サービス「アクセス解析」サービスを利用するための JavaScript 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。	2015 年 12 月 7 日	4.3
38 （#4）	「WL-330NUL」において任意のコマンドを実行される脆弱性	無線 LAN ルータ「WL-330NUL」には、任意のコマンドが実行される脆弱性がありました。このため、第三者によって、任意のコマンドを実行される可能性がありました。	2015 年 12 月 9 日	5.8
39 （#4）	「WL-330NUL」におけるクロスサイト・スクリプティングの脆弱性	無線 LAN ルータ「WL-330NUL」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。	2015 年 12 月 9 日	4.3
40 （#1）	「Zend Framework」における SQL インジェクションの脆弱性	ウェブアプリケーションフレームワーク「Zend Framework」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。	2015 年 12 月 11 日	6.8
41	「Adobe Flash Player」における iframe 内のコンテンツを上書きしてしまう問題	Flash コンテンツ再生用ソフトウェア「Adobe Flash Player」には、same-origin policy を迂回し、iframe 内のコンテンツを不正に上書きしてしまう問題がありました。このため、第三者により異なるドメイン上の情報を書き換えられる可能性がありました。	2015 年 12 月 17 日	5.8
42	「WinRAR」における実行ファイル読み込みに関する脆弱性	ファイル圧縮、解凍ソフト「WinRAR」には、実行ファイル読み込みに関する脆弱性が存在しました。このため、任意のファイルが実行される可能性がありました。	2015 年 12 月 17 日	5.1
43 （#1）	WordPress 用プラグイン「Welcart」における SQL インジェクションの脆弱性	WordPress 用プラグイン「Welcart」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。	2015 年 12 月 17 日	6.5
44 （#4）	「CG-WLBARAGM」がオープンプロキシとして機能してしまう問題	無線 LAN ルータ「CG-WLBARAGM」には、オープンプロキシとして機能してしまう問題がありました。このため、第三者により踏み台にされる可能性がありました。	2015 年 12 月 25 日	5.0

項番	脆弱性	セキュリティ上の問題点	JVN 公表日	CVSS 基本値
45 (#4)	「CG-WLNCM4G」がオープンリゾルバとして機能してしまう問題	無線 LAN ルータ「CG-WLNCM4G」には、オープンリゾルバとして機能してしまう問題がありました。このため、DNS リフレクター攻撃に悪用され、DDoS 攻撃に加担させられる可能性がありました。	2015 年 12 月 25 日	5.0
脆弱性の深刻度=レベルⅠ（注意）、CVSS 基本値=0.0～3.9				
46 (#1)	「Dotclear」におけるクロスサイト・スクリプティングの脆弱性	ウェブログ用ソフトウエア「Dotclear」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。	2015 年 10 月 2 日	2.6
47	Android アプリ「AirDroid」における暗黙的 Intent の扱いに関する脆弱性	Android アプリ「AirDroid」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、第三者により連絡先情報を窃取される可能性がありました。	2015 年 10 月 16 日	2.6
48 (#3) (#4)	複数のルータ製品におけるクリックジャッキングの脆弱性	複数のルータ製品の管理画面には、クリックジャッキングの脆弱性がありました。このため、ルータの管理画面上で意図しない操作をさせられる可能性がありました。	2015 年 10 月 30 日	2.6
49 (#1)	「HTML::Scrubber」におけるクロスサイト・スクリプティングの脆弱性	Perl モジュール「HTML::Scrubber」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。	2015 年 10 月 30 日	2.6
50	「OS X」におけるスリープモードからの復帰時の認証に関する問題	オペレーティングシステム「OS X」には、スリープモードからの復帰時の認証に関する問題がありました。このため、「Apple Remote Desktop」を使用していた場合、接続先の端末上で任意のコマンドを実行される可能性がありました。	2015 年 11 月 13 日	3.7
51 (#4)	「WL-330NUL」における情報管理不備の脆弱性	無線 LAN ルータ「WL-330NUL」には、情報管理不備の問題がありました。このため、第三者に WPA2-PSK のパスフレーズを取得される問題がありました。	2015 年 12 月 9 日	3.3
52 (#4)	「WL-330NUL」におけるサービス運用妨害(DoS)の脆弱性	無線 LAN ルータ「WL-330NUL」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。	2015 年 12 月 9 日	3.3

（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 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 42 件ありました。

Android 関連製品や OSS 製品の脆弱性の対策情報公表に向けた調整活動では、近年、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 [(*16)] 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	オムロン製 PLC および CX-Programmer に複数の脆弱性	特定製品開発者と調整
2	Datalex のエアライン予約ソフトウェアに認証回避の脆弱性	注意喚起として掲載

(*16) 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
3	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
4	QNAP QTS にパストラバーサルの脆弱性	注意喚起として掲載
5	ZyXEL NBG-418N、PMG5318-B20A および P-660HW-T1 ルータに複数の脆弱性	注意喚起として掲載
6	Voice over LTE (VoLTE) の実装に複数の脆弱性	複数製品開発者と調整
7	HP ArcSight Logger に複数の脆弱性	注意喚起として掲載
8	Medicomp MEDCIN Engine に複数の脆弱性	注意喚起として掲載
9	仮想マシンモニタ (VMM) のメモリ重複排除機能に脆弱性	注意喚起として掲載
10	HP Client Automation および Radia Client Automation にコード実行の脆弱性	注意喚起として掲載
11	HP Photosmart B210 の SMB サーバ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
12	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
13	EPSON Network Utility に権限昇格の脆弱性	注意喚起として掲載 特定製品開発者へ通知
14	HP ArcSight SmartConnector に複数の脆弱性	注意喚起として掲載
15	Qolsys IQ Panel に複数の脆弱性	注意喚起として掲載
16	MobaXterm 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
17	Commvault Edge Server に Cookie のデシリアライズ処理に関する脆弱性	注意喚起として掲載
18	ZTE 製の複数のルータ製品に脆弱性	注意喚起として掲載
19	Huawei HG532 シリーズルータ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
20	Apache Commons Collections ライブラリのデシリアライズ処理に脆弱性	注意喚起として掲載 複数製品開発者へ通知
21	ARRIS 製ケーブルモデムに複数の脆弱性	注意喚起として掲載
22	CSL DualCom GPRS CS2300-R に複数の脆弱性	注意喚起として掲載
23	Dell Foundation Services (DFS) がルート証明書と秘密鍵 (eDellRoot) をインストールする問題	注意喚起として掲載
24	Dell System Detect (DSD) がルート証明書と秘密鍵 (DSDTestProvider) をインストールする問題	注意喚起として掲載
25	組込み機器に固有でない X.509 証明書および SSH ホスト鍵を使用している問題	注意喚起として掲載
26	RSI Video Technologies の Videofied Frontel がセキュアでない独自プロトコルを使用する問題	注意喚起として掲載
27	Epiphany Cardio Server に SQL インジェクションおよび LDAP インジェクションの脆弱性	注意喚起として掲載
28	Lenovo Solution Center に権限昇格ほか複数の脆弱性	注意喚起として掲載 特定製品開発者へ通知
29	OpenSSL 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	TaxiHail に複数の脆弱性	注意喚起として掲載
31	Uptime Infrastructure Monitor (旧称 up.time) の Windows 向けエージェントに複数の脆弱性	注意喚起として掲載
32	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
33	ReadyNet WRT300N-DD に複数の脆弱性	注意喚起として掲載
34	Netgear WNR1000v3 に不十分なランダム値を使用している問題	注意喚起として掲載
35	Buffalo WZR-600DHP2 に不十分なランダム値を使用している問題	注意喚起として掲載 特定製品開発者へ通知

項番	脆弱性	対応状況
36	Amped Wireless R10000 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	ZyXEL NBG-418N に複数の脆弱性	注意喚起として掲載
38	ISC BIND 9 に複数のサービス運用妨害 (DoS) の脆弱性	注意喚起として掲載 複数製品開発者へ通知
39	Ipswitch WhatsUp Gold に SQL インジェクションおよび複数のクロスサイトスクリプティングの脆弱性	注意喚起として掲載
40	Dovestones Software AD Self Password Reset に脆弱性	注意喚起として掲載
41	Juniper ScreenOS に複数の脆弱性	注意喚起として掲載
42	ISC Kea DHCP サーバにサービス運用妨害 (DoS) の脆弱性	注意喚起として掲載 複数製品開発者へ通知

2-1-5. 連絡不能案件の処理状況

図 2-12 は、2011 年 9 月末から始まった連絡不能案件取扱について、2015 年 12 月末までに、「連絡不能開発者」と位置づけて取扱った 217 件の処理状況の推移を示したものです。

今四半期は、連絡不能（新規公表）はありませんでしたが、前四半期に新規公表した 12 件について製品開発者と連絡がとれなかったため、追加情報を公表しました。一方で、連絡不能開発者一覧への掲載により、連絡不能（追加情報公表）の 3 件が製品開発者と連絡が取れ、脆弱性対策情報の公表に向け調整を再開しました。このため、連絡不能（追加情報公表）は差し引き 9 件の増加となりました。

この結果、調整再開した案件は 41 件（前四半期は 38 件）、連絡不能案件は 174 件（前四半期は 177 件）となりました。

今期「調整再開（調整完了）」した 2 件は JVN の公表に向け製品開発者と調整を行った結果、脆弱性対策情報の公表に至ったものです。なお、今期に公表判定委員会の審議にて JVN 公表が適当であると判定され JVN 公表に至ったものはありませんでした。

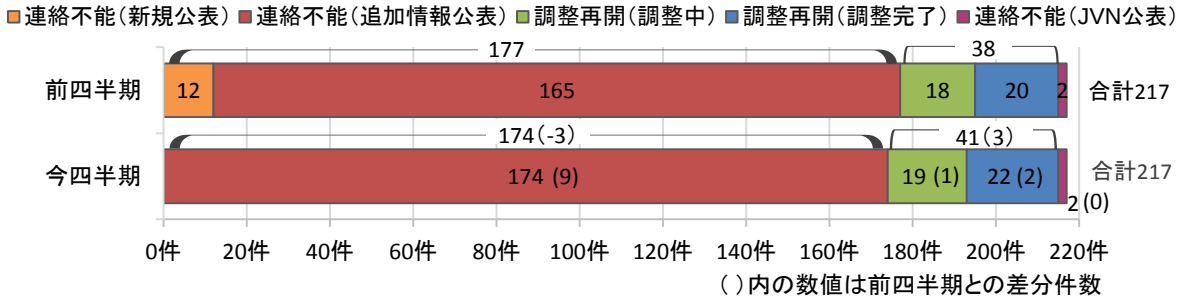
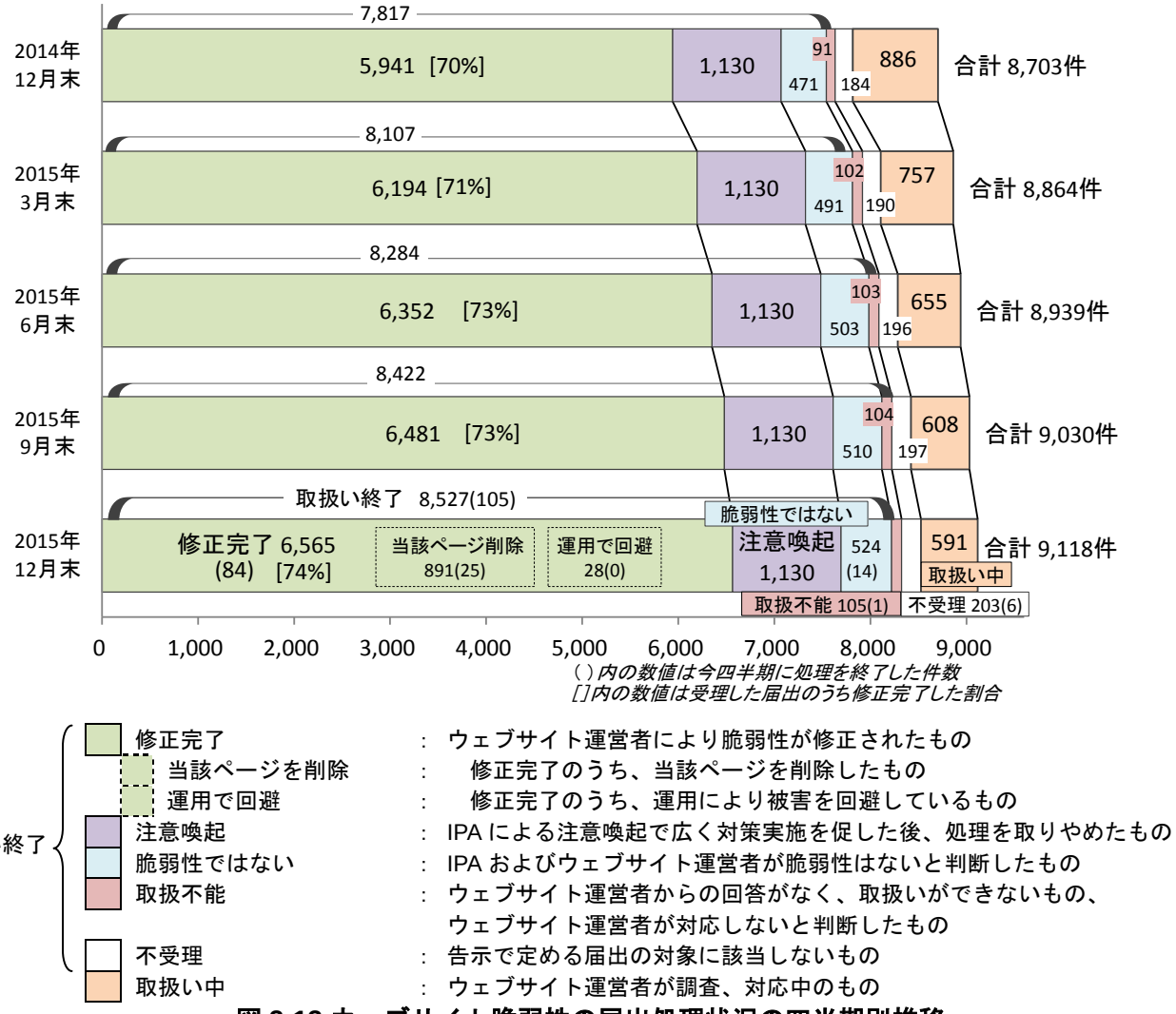


図2-12. 連絡不能開発者一覧の処理状況

2-2. ウェブサイトの脆弱性

2-2-1. 処理状況

図 2-13 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。2015 年 12 月末時点の届出の累計は 9,118 件で、今四半期中に取扱いを終了したものは 105 件（累計 8,527 件）でした。このうち「修正完了」したものは 84 件（累計 6,565 件）、「注意喚起」により処理を取りやめたもの [*17] 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 14 件（累計 524 件）でした。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に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 1 件（累計 105 件）でした。また「不受理」としたものは 6 件（累計 203 件）でした。取扱いを終了した累計 8,527 件のうち「修正完了」「脆弱性ではない」の合計 7,089 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たものです。なお「修正完了」のうち、ウェブサイト運営者が当該ページを削除したものは 25 件（累計 891 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 2-13.ウェブサイト脆弱性の届出処理状況の四半期別推移

[*17] 「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、効果的に周知徹底するため「注意喚起」を公表することがあります。そうした場合、「注意喚起」をもって届出の処理を取りやめます。

以下に、今までに届出のあったウェブサイトの脆弱性 9,118 件のうち、不受理を除いた 8,915 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 2-14 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。今四半期は届出 87 件の約 5 割を企業が占めています。

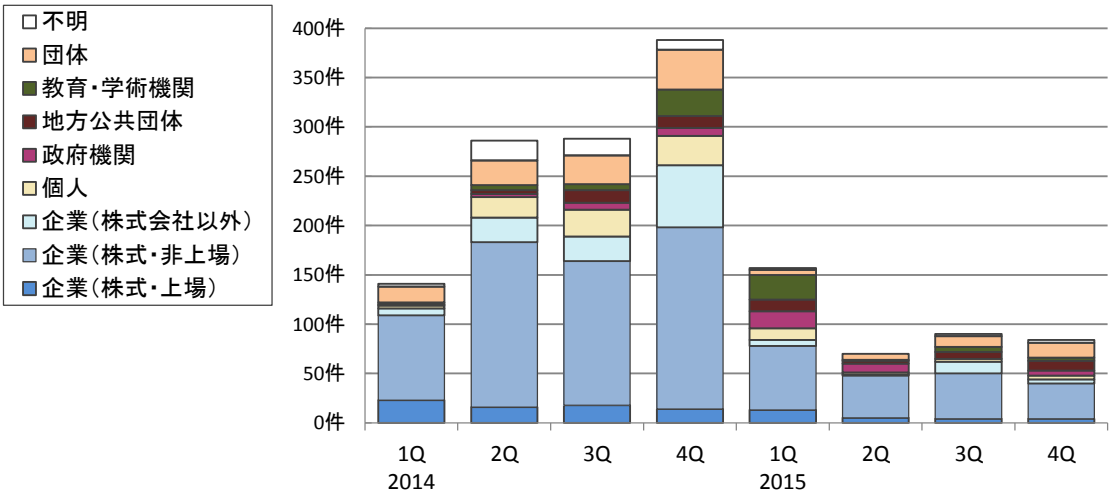


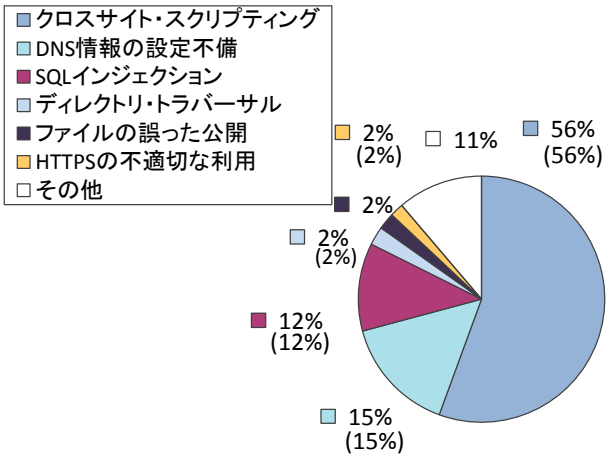
図2-14. 四半期ごとの運営主体の種類別届出件数

2-2-3. 脆弱性の種類・影響別届出

図 2-15、2-16 のグラフは、届出された脆弱性の種類を示しています。図 2-15 は今までの届出累計の割合を、図 2-16 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[*18]。

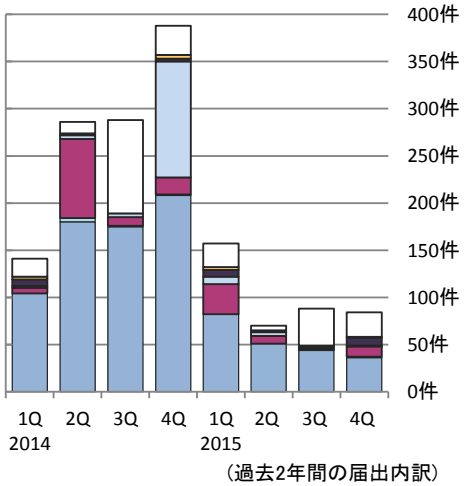
累計では、「クロスサイト・スクリプティング」だけで 56%を占めており、次いで「DNS 情報の設定不備」「SQL インジェクション」となっています。「DNS 情報の設定不備」の 15%は、2008 年から 2009 年にかけて多く届出されたのが反映されたものです。今四半期の傾向は約 4 割を占める「クロスサイト・スクリプティング」と「その他」が多く、後者は“古いバージョンのソフトウェア製品の利用”という内容が過半数を占めています。なお、この統計は本制度における届出の傾向であり、世の中に存在する脆弱性の傾向と必ずしも一致するものではありません。

ウェブサイトの脆弱性の種類別の届出状況



（8,915件の内訳、グラフの括弧内は前四半期までの数字）

図2-15. 届出累計の脆弱性の種類別割合



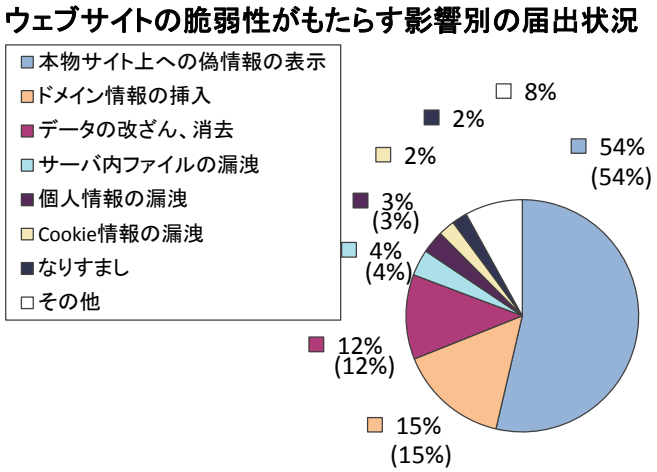
（過去2年間の届出内訳）

図2-16. 四半期ごとの脆弱性の種類別届出件数

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

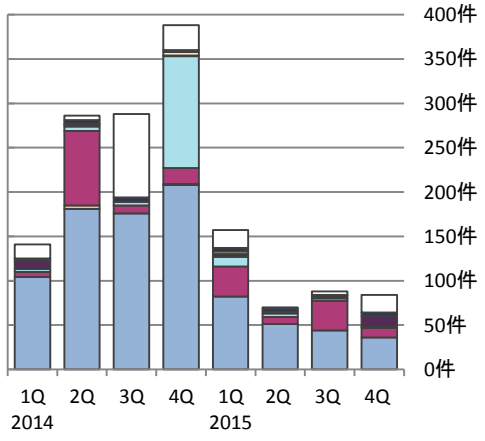
図 2-17、2-18 のグラフは、届出された脆弱性がもたらす影響別の分類です。図 2-17 は届出の影響別割合を、図 2-18 は過去 2 年間の届出件数の推移を四半期ごとに示しています。

累計では、「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。これらは、「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ものです。



(8,915件の内訳、グラフの括弧内は前四半期までの数字)

図2-17. 届出累計の脆弱性がもたらす影響別割合



(過去2年間の届出内訳)

図2-18. 四半期ごとの脆弱性がもたらす影響別届出件数

2-2-4. 修正完了状況

図 2-19 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。2015 年第 4 四半期に修正を完了した届出 84 件のうち 38 件（45%）は、運営者へ脆弱関連情報を通知してから 90 日以内に修正が完了しました。この割合は、前四半期（129 件中 43 件）の 33%より増加しています。

表 2-6 は、過去 3 年間に修正が完了した全届出のうち、ウェブサイト運営者に通知してから、90 日以内に修正が完了した脆弱性の累計およびその割合を四半期ごとに示したものです。今期の割合は 66%でした。

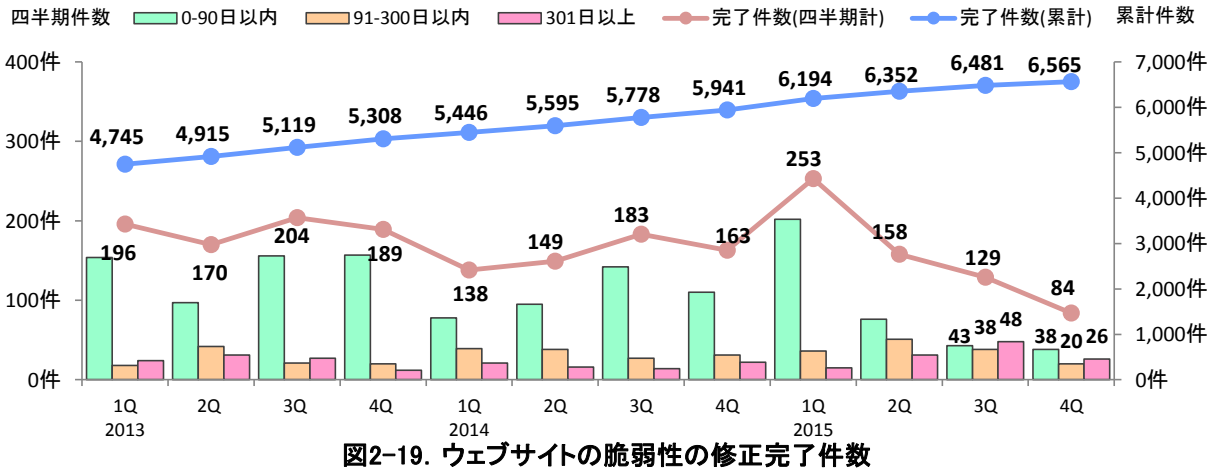


図2-19. ウェブサイトの脆弱性の修正完了件数

表 2-6. 90 日以内に修正完了した累計およびその割合の推移

	2013 1Q	2Q	3Q	4Q	2014 1Q	2Q	3Q	4Q	2015 1Q	2Q	3Q	4Q
修正完了件数	4,745	4,915	5,119	5,308	5,446	5,595	5,778	5,941	6,194	6,352	6,481	6,565
90 日以内の件数	3,147	3,244	3,400	3,557	3,635	3,730	3,872	3,982	4,184	4,260	4,303	4,341
90 日以内の割合	66%	66%	66%	67%	67%	67%	67%	67%	68%	67%	66%	66%

図 2-20、2-21 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 [*19]。全体の 47%の届出が 30 日以内、全体の 66%の届出が 90 日以内に修正されています。

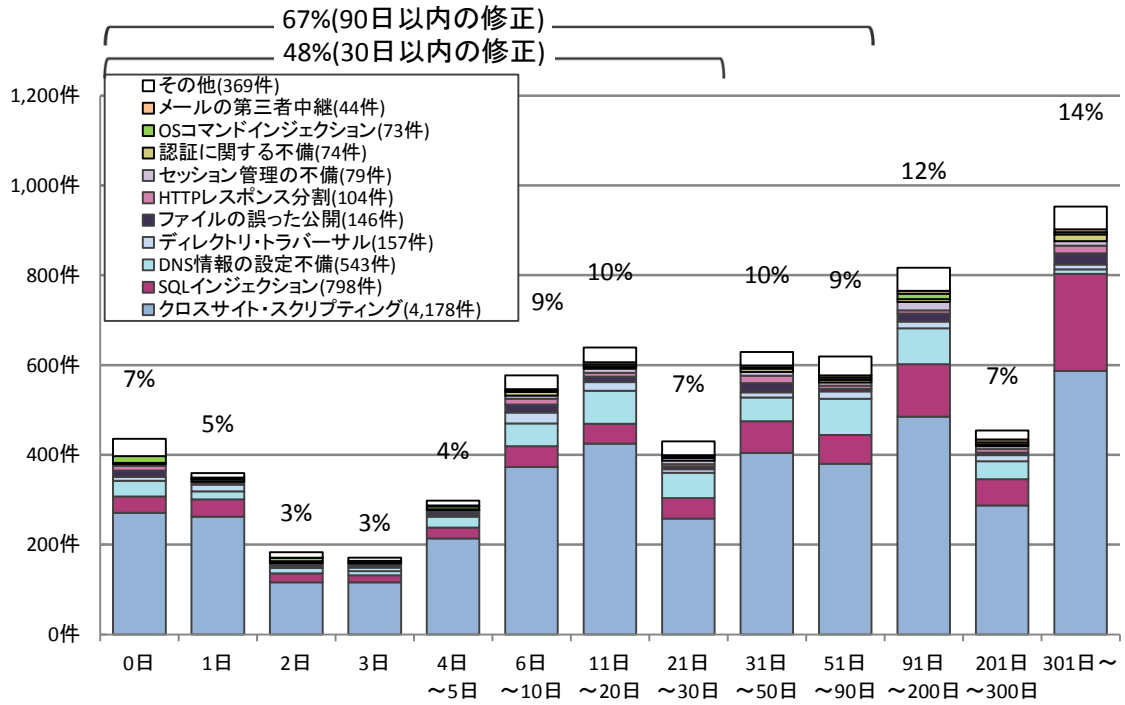


図2-20. ウェブサイトの修正に要した日数

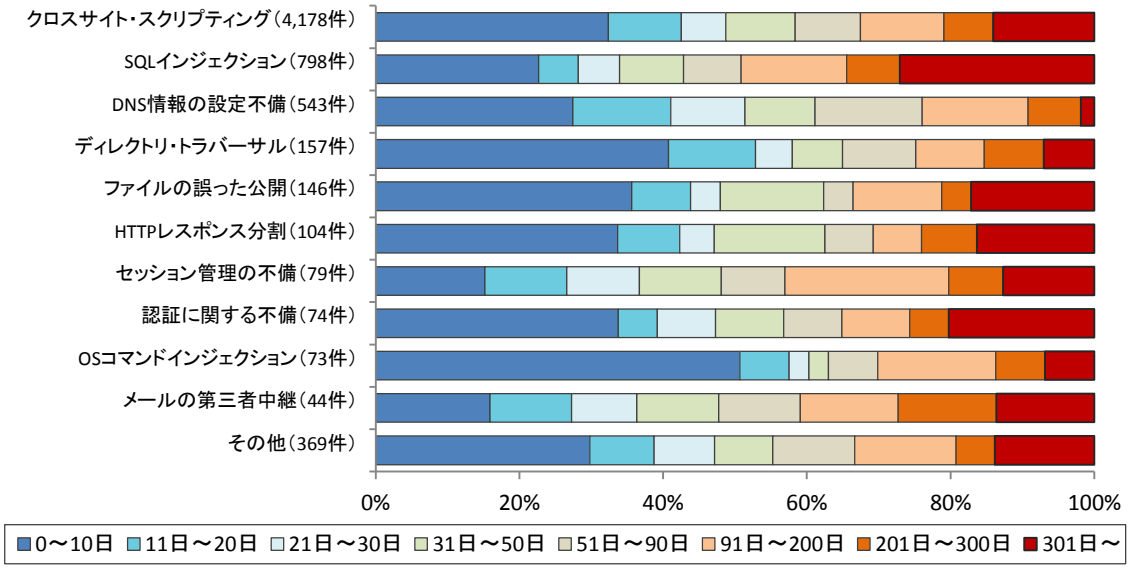


図2-21. ウェブサイトの修正に要した脆弱性種類別の日数の傾向

[*19] 運営者から修正完了の報告があったもの、および、脆弱性が修正されたと IPA で判断したものも含めて示しています。なお、0 日は詳細情報を通知した当日に修正されたもの、または運営者へ詳細情報を通知する前に修正されたものです。

2-2-5. 取扱中の状況

ウェブサイト運営者から脆弱性を修正した旨の報告が無い場合、IPA は 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繰り返し連絡を試み、脆弱性対策の実施を促しています。

図 2-22 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 473 件（前四半期は 504 件）と減少しています。

これは、取扱いが長期化しているウェブサイトについて、既にウェブサイトが閉鎖、もしくは問題のあるページが削除されていることを確認したものについて取扱いを終了としたためです。

またウェブサイトの情報が窃取されてしまうなどの危険性がある、SQL インジェクションという深刻度の高い脆弱性が含まれる割合は全体の約 15%を占めています。

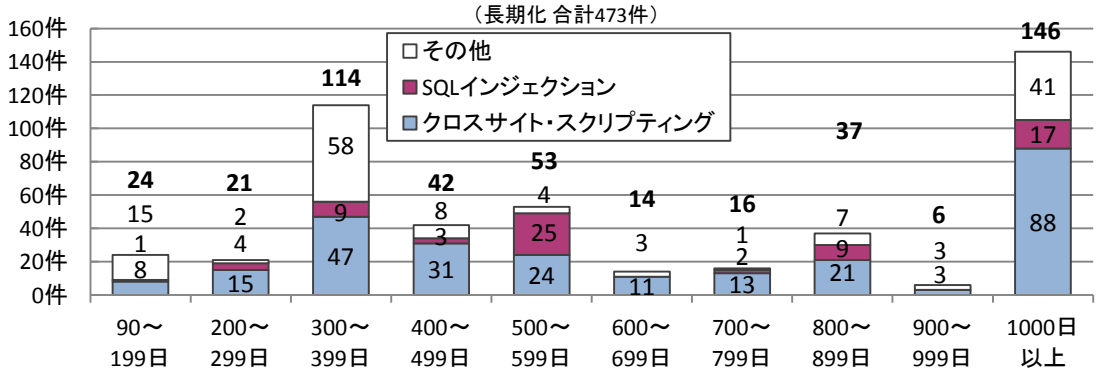


図2−22. 取扱いが長期化(90日以上経過)しているウェブサイトの経過日数と脆弱性の種類

表 2-7 は、過去 2 年間の四半期末時点で取扱い中の届出と、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 2-7. 取扱いが長期化している届出件数および割合の四半期ごとの推移

	2014 1Q	2Q	3Q	4Q	2015 1Q	2Q	3Q	4Q
取扱い中の件数	490	596	676	886	757	655	608	591
長期化している件数	357	353	402	446	415	562	504	473
長期化している割合	73%	59%	59%	50%	55%	86%	83%	80%

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把握し、脆弱性対策を実施する事が必要です。脆弱性の理解・対策にあたっては、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）」： https://www.ipa.go.jp/security/vuln/vuln_contents/

⇒「安全なウェブサイト運営入門」： https://www.ipa.go.jp/security/vuln/7incidents/

⇒「安全なウェブサイトの作り方」: https://www.ipa.go.jp/security/vuln/websecurity.html

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

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

⇒「安全なウェブサイトの構築と運用管理に向けての 16 ヶ条 ～セキュリティ対策のチェックポイント～」
https://www.ipa.go.jp/security/vuln/websitecheck.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」: https://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）:
https://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）」:
https://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」:
https://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」:
https://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

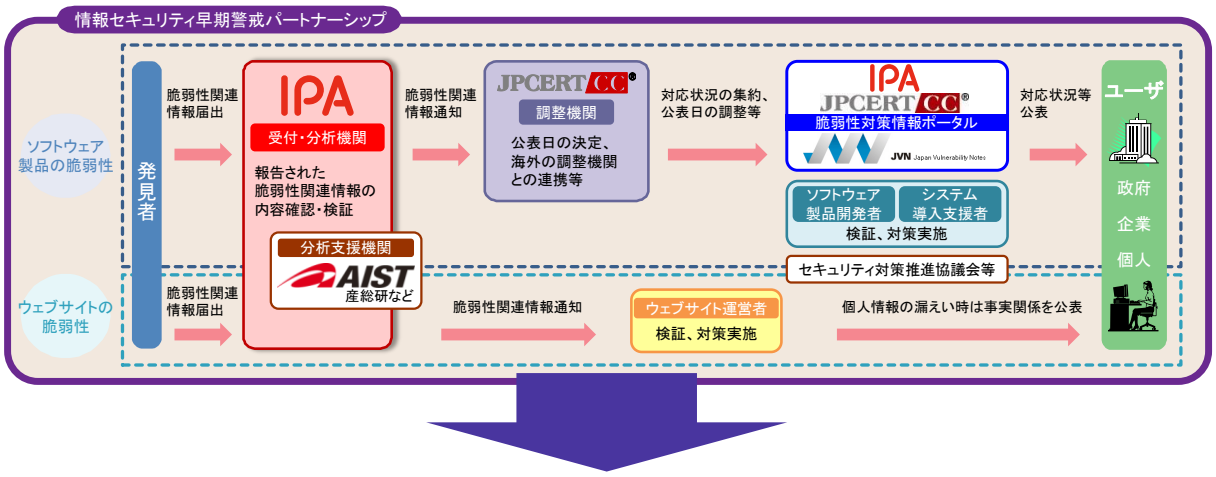
付表 2. ウェブサイトの脆弱性の分類

	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」（脆弱性関連情報の取扱制度）



【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個人情報等重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：国立研究開発法人産業技術総合研究所