# ソフトウェア等の脆弱性関連情報の取扱いに関する届出状況

## [2016 年第 1 四半期（1 月～3 月）]

ソフトウェア等の脆弱性関連情報の取扱いに関する届出状況について

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、2016 年 1 月 1 日から 2016 年 3 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届出状況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 4 月 27 日

目次

## 1. 2016 年第 1 四半期　ソフトウェア等の脆弱性関連情報に関する届出状況

### 1-1. 脆弱性関連情報の届出状況

**～ 脆弱性の届出件数の累計は 11,677 件 ～**

表 1-1 は本制度 (*1) における届出状況です。2016 年第 1 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 100 件、ウェブアプリケーション（以降「ウェブサイト」）に関する届出は 85 件、合計 185 件でした。届出受付開始からの累計は 11,677 件で、内訳はソフトウェア製品に関するもの 2,476 件、ウェブサイトに関するもの 9,201 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 | **100** 件 | **2,476** 件 |
| ウェブサイト | **85** 件 | **9,201** 件 |
| 合計 | **185** 件 | **11,677** 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 4.17 (*2) 件でした。

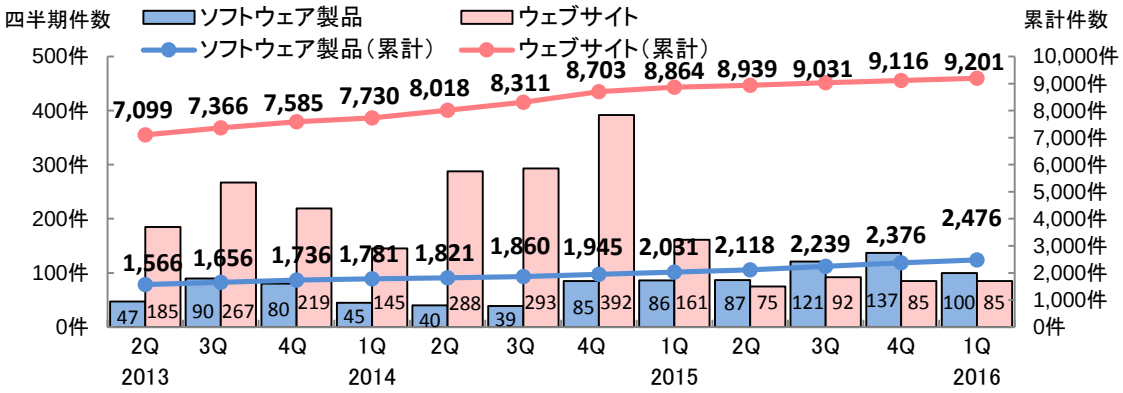



**図1−1. 脆弱性の届出件数の四半期ごとの推移**

**表 1-2. 届出件数（過去 3 年間）**

| | 2013 2Q | 3Q | 4Q | 2014 1Q | 2Q | 3Q | 4Q | 2015 1Q | 2Q | 3Q | 4Q | 2016 1Q |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 累計届出件数[件] | 8,665 | 9,022 | 9,321 | 9,511 | 9,839 | 10,171 | 10,648 | 10,895 | 11,057 | 11,270 | 11,492 | 11,677 |
| 1 就業日あたり[件/日] | 3.95 | 4.00 | 4.03 | 4.01 | 4.04 | 4.07 | 4.16 | 4.16 | 4.13 | 4.11 | 4.11 | 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
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

## 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 7,844 件～**

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 | **34** 件 | **1,181** 件 |
| ウェブサイト | **98** 件 | **6,663** 件 |
| 合計 | **132** 件 | **7,844** 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）。

今四半期に JVN 公表したソフトウェア製品の件数は 34 件 (*3)（累計 1,181 件）でした。そのうち、8 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 10 件（29%）でした。

また、修正完了したウェブサイトの件数は 98 件（累計 6,663 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 98 件のうち、ウェブアプリケーションを修正したものは 66 件（67%）、当該ページを削除したものは 32 件（33%）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 98 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 46 件（47%）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（84 件中 38 件（45%））より増加しています。

## 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、新たに 12 件について連絡が取れない製品開発者名を公表しました。製品開発者と連絡が取れ調整を再開したもの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。

2016 年 3 月末時点の連絡不能開発者の累計公表件数は 229 件、その内製品情報を公表しているものは 197 件となりました。

---

(*3) P.7 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。
(*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。

## 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。2016 年 3 月末時点の届出の累計は 2,476 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 1,181 件）でした。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 35 件）、製品開発者が「脆弱性ではない」と判断したものは 0 件（累計 80 件）、「不受理」としたものは 7 件 (*8)（累計 334 件）、取扱い中は 846 件でした。846 件のうち、連絡不能開発者 (*9) 一覧へ新規に公表したものは 12 件で、2016 年 3 月末時点で 188 件が公表中です。

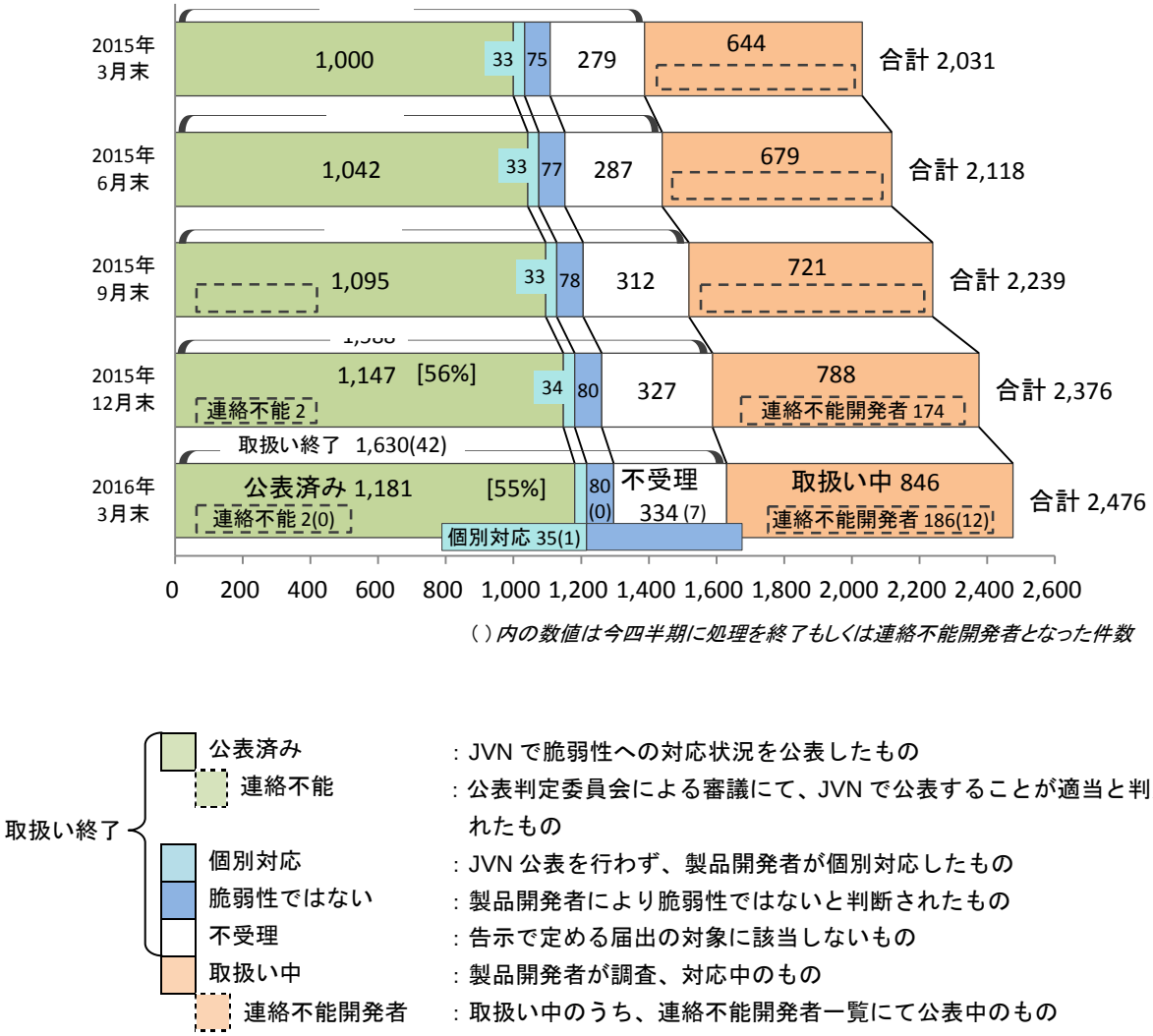






**図 2-1. ソフトウェア製品脆弱性の届出処理状況（四半期ごとの推移）**

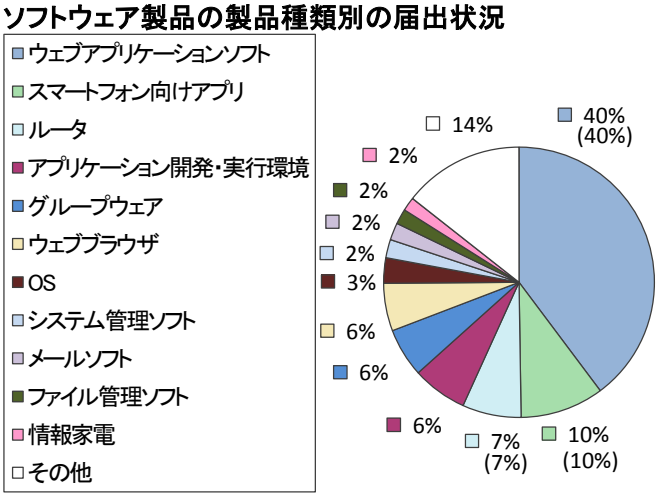
(*8) 内訳は今四半期の届出によるもの 1 件、前四半期までの届出によるもの 6 件。
(*9) 連絡不能開発者一覧への公表および一覧からの削除が複数回行われた製品開発者の公表回数は、その累計を計上しています。

今までに届出のあったソフトウェア製品の脆弱性 2,476 件のうち、不受理を除いた件数は 2,142 件でした。また、今四半期に届出のあった 100 件のうち、不受理を除いた件数は 99 件でした。以下に、不受理を除いた届出について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

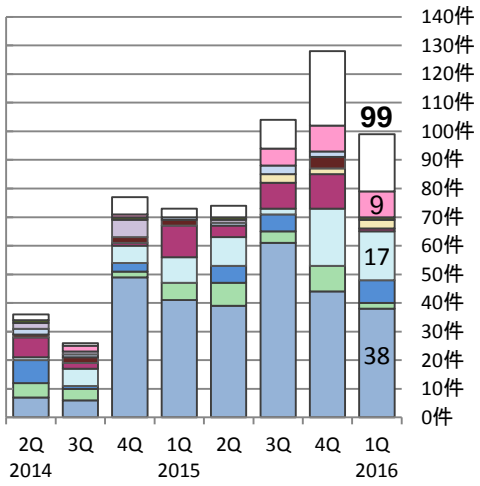
図 2-2、2-3 のグラフは、届出された脆弱性の製品種類別の分類です。図 2-2 は製品種類別割合を、図 2-3 は過去 2 年間の届出件数の推移を四半期ごとに示したものです。

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（38 件）」で、次いで多いのは、「ルータ（17 件）」「情報家電（9 件）」となっています。




※その他には、データベース、携帯機器などがあります。
（2,142件の内訳、グラフの括弧内は前四半期までの数字）

**図2-2. 届出累計の製品種類別割合**

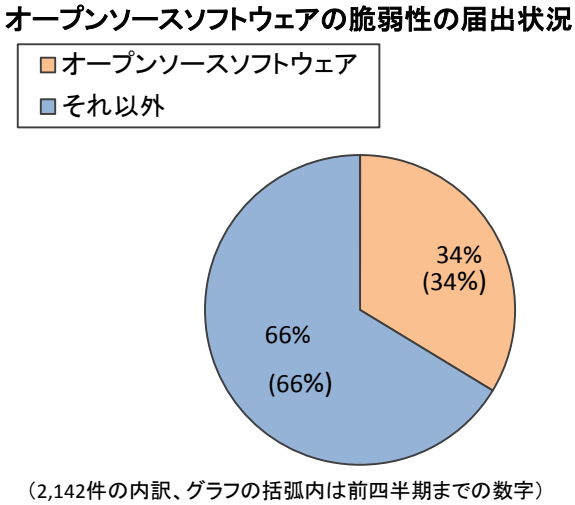



（過去2年間の届出内訳）

**図2-3. 四半期ごとの製品種類別届出件数**

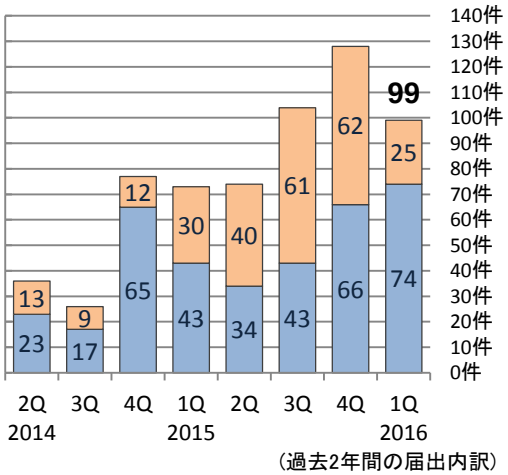
図 2-4、2-5 のグラフは、届出された製品のライセンスを「オープンソースソフトウェア」（OSS）と「それ以外」で分類しています。図 2-4 は届出累計の分類割合を、図 2-5 は過去 2 年間の届出件数の推移を四半期ごとに示したものです。

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 66%を占め、オープンソースソフトウェアの 2 倍以上となりました。




（2,142件の内訳、グラフの括弧内は前四半期までの数字）

**図2-4. 届出累計のオープンソースソフトウェア割合**



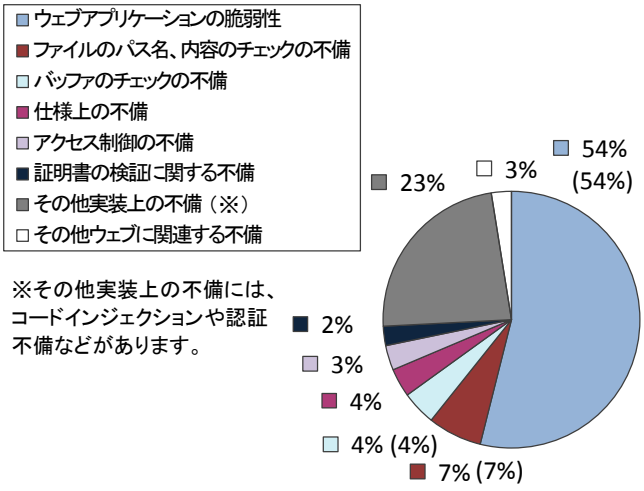

（過去2年間の届出内訳）

**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

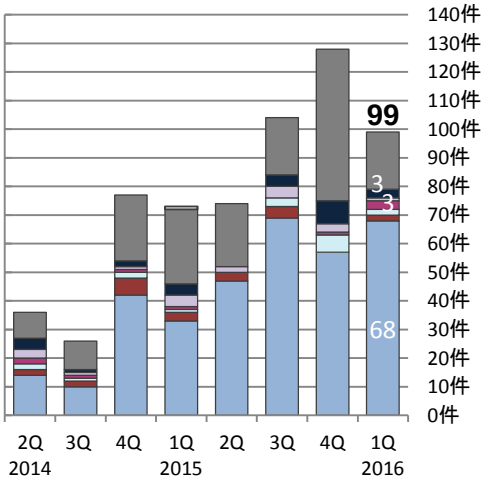
図 2-6、2-7 のグラフは、届出された脆弱性の原因を示しています。図 2-6 は届出累計の脆弱性の原因別割合を、図 2-7 は過去 2 年間の原因別の届出件数の推移を四半期ごとに示しています。累計では、「ウェブアプリケーションの脆弱性」が過半数を占めています。今四半期も「ウェブアプリケーションの脆弱性（68 件）」が最も多く、次いで「仕様上の不備（3 件）」「証明書の検証に関する不備（3 件）」となっています。

**ソフトウェア製品の脆弱性の原因別の届出状況**




（2,142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**

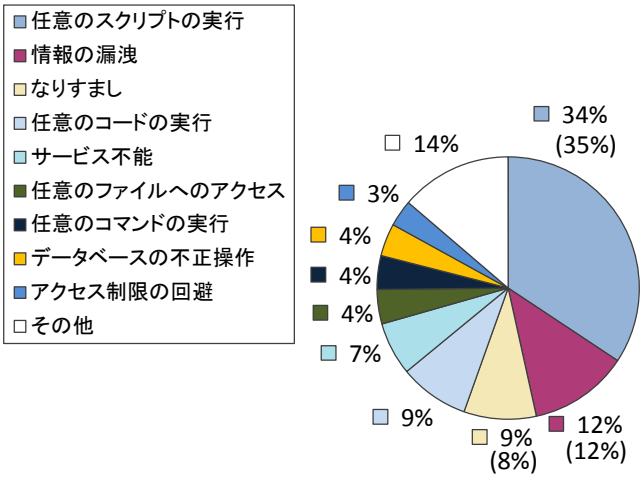



（過去2年間の届出内訳）

**図2-7. 四半期ごとの脆弱性の原因別届出件数**

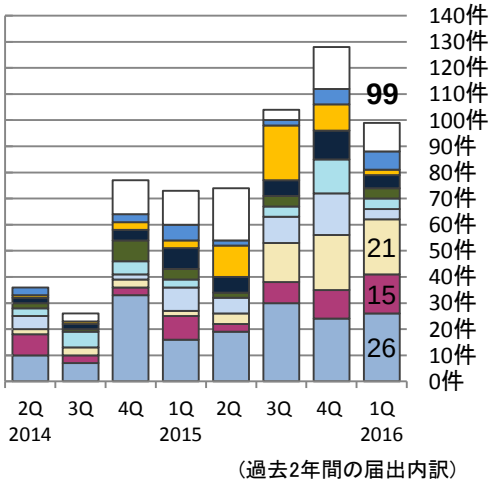
図 2-8、2-9 のグラフは、届出された脆弱性がもたらす影響を示しています。図 2-8 は届出累計の影響別割合を、図 2-9 は過去 2 年間の影響別届出件数の推移を四半期ごとに示しています。累計では「任意のスクリプトの実行」が最も多く、34%となっています。今四半期は、「任意のスクリプトの実行（26 件）」が最も多く、次いで多かったのは「なりすまし（21 件）」「情報の漏洩（15 件）」でした。

**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**




（2,142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.** JVN 公表状況別件数

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（1,181 件）について、図 2-10 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 2-1 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。

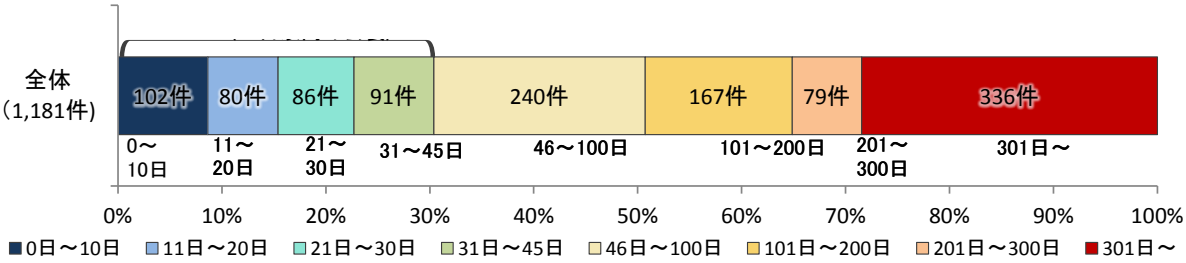



**図2−10. ソフトウェア製品の脆弱性公表日数**

**表 2-1. 45 日以内に JVN 公表した件数の割合推移（四半期ごと）**

| 2013 2Q | 3Q | 4Q | 2014 1Q | 2Q | 3Q | 4Q | 2015 1Q | 2Q | 3Q | 4Q | 2016 1Q |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 33% | 33% | 34% | 34% | 34% | 33% | 33% | 32% | 31% | 31% | 30% | 30% |

**2-1-5.** 調整および公表レポート数

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 [*10]。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 2-2、図 2-11 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 [*11] の推移等を示したものです。

**表 2-2. 脆弱性の提供元別 脆弱性公表レポート件数**

| | 情報提供元 | 今期件数 | 累計 |
|---|---|---|---|
| | 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 で公表した脆弱性レポート | 28 件 | 1,175 件 |
| | 海外 CSIRT 等から脆弱性情報の提供を受け JVN で公表した脆弱性レポート | 40 件 | 1,359 件 |
| | 合計 | 68 件 | 2,534 件 |

[*10] JPCERT/CC 活動概要 Page16～23（http://www.jpcert.or.jp/pr/2016/PR20160414.pdf）を参照下さい。
[*11] 2-1-5 は公表したレポートの件数をもとに件数を計上しています。複数の届出についてまとめ 1 件のレポートを公表する場合がある為、必ずしも JVN 公表した脆弱性の件数と一致するものではありません。

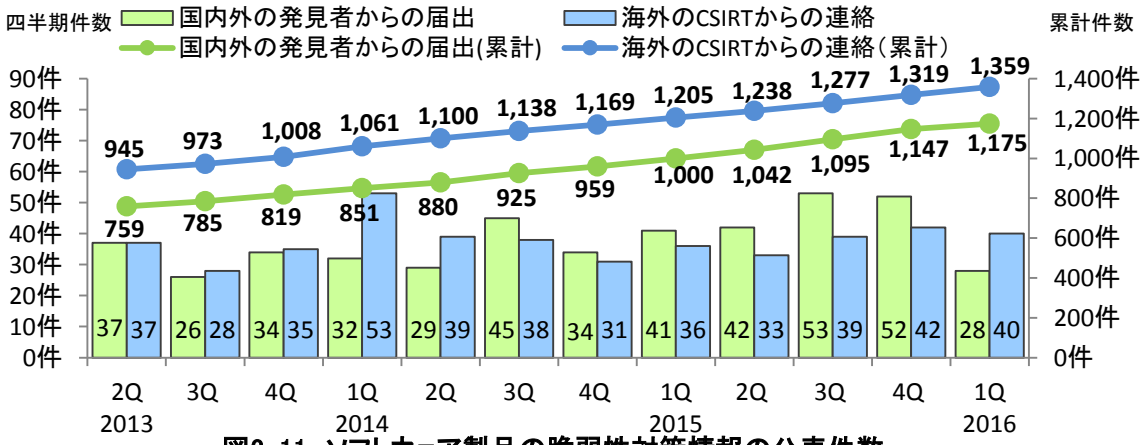



**図2−11. ソフトウェア製品の脆弱性対策情報の公表件数**

### （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

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 4 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 8 件（表 2-3 の#2）、組込みソフトウェア製品の脆弱性が 6 件（表 2-3 の#3）ありました。

**表 2-3. 2016 年第 1 四半期に JVN で公表した脆弱性**

| 項番 | 脆弱性 | セキュリティ上の問題点 | JVN 公表日 | CVSS 基本値 |
|---|---|---|---|---|
| 脆弱性の深刻度=レベル III（危険）、CVSS 基本値=7.0～10.0 | | | | |
| 1 | 「CLUSTERPRO X」におけるディレクトリ・トラバーサルの脆弱性 | クラスタリングソフト「CLUSTERPRO X」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。 | 2016 年 1 月 29 日 | 7.8 |
| 2 | EC-CUBE 用プラグイン「ヘルプ機能プラグイン」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「ヘルプ機能プラグイン」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。 | 2016 年 2 月 19 日 | 7.5 |
| 脆弱性の深刻度=レベル II（警告）、CVSS 基本値=4.0～6.9 | | | | |
| 3 | 「ＤＸライブラリ」におけるバッファオーバーフローの脆弱性 | Windows ソフトを開発するためのライブラリ「ＤＸライブラリ」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が実行される可能性がありました。 | 2016 年 1 月 5 日 | 6.8 |
| 4 | 「acmailer」における OS コマンド・インジェクションの脆弱性 | メール配信 CGI「acmailer」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。 | 2016 年 1 月 15 日 | 6.5 |
| 5 (#1) (#2) | 「H2O」における HTTP ヘッダ・インジェクションの脆弱性 | ウェブサーバソフト「H2O」には、HTTP ヘッダ・インジェクションの脆弱性がありました。このため、HTTP レスポンス分割攻撃によって、Cookie に任意の値が設定される可能性がありました。 | 2016 年 1 月 15 日 | 4.3 |
| 6 | iOS アプリ「ショッぷらっと」における SSL サーバ証明書の検証不備の脆弱性 | iOS アプリ「ショッぷらっと」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。 | 2016 年 1 月 18 日 | 4.0 |

| 項番 | 脆弱性 | セキュリティ上の問題点 | JVN 公表日 | CVSS 基本値 |
|---|---|---|---|---|
| 7 (#3) | バッファロー製の複数のネットワーク機器におけるクロスサイト・スクリプティングの脆弱性 | バッファロー製の複数のネットワーク機器には、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。 | 2016 年 1 月 22 日 | 4.3 |
| 8 (#3) | HOME SPOT CUBE における複数の脆弱性 | 無線 LAN ルータ「HOME SPOT CUBE」には、複数の脆弱性が存在しました。このため、第三者により任意の OS コマンドを実行されるなどの可能性がありました。 | 2016 年 1 月 27 日 | 5.2 |
| 9 (#1) | 「Vine MV」におけるクロスサイト・スクリプティングの脆弱性 | ミュージックビデオ自動生成アプリ「Vine MV」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。 | 2016 年 1 月 29 日 | 4.3 |
| 10 | 「JOB-CUBE」におけるクロスサイト・スクリプティングの脆弱性 | 求人サイト構築ソフト「JOB-CUBE」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。 | 2016 年 1 月 29 日 | 4.0 |
| 11 | iOS アプリ「Akerun - Smart Lock Robot」における SSL サーバ証明書の検証不備の脆弱性 | iOS アプリ「Akerun - Smart Lock Robot」には、SSL サーバ証明書の検証不備の問題が存在しました。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。 | 2016 年 2 月 12 日 | 4.0 |
| 12 (#2) | 「サイボウズ Office」におけるサービス運用妨害(DoS)の脆弱性 | グループウェア「サイボウズ Office」には、カスタムアプリに起因するサービス運用妨害(DoS)の脆弱性問題がありました。このため、当該製品を使用できなくなる可能性がありました。 | 2016 年 2 月 15 日 | 6.8 |
| 13 (#2) | 「サイボウズ Office」における情報漏えいの脆弱性 | グループウェア「サイボウズ Office」には、メール機能に情報漏えいの問題がありました。このため、ユーザにのみアクセス可能な画像ファイルが第三者に取得される可能性がありました。 | 2016 年 2 月 15 日 | 5.0 |
| 14 (#2) | 「サイボウズ Office」におけるアクセス制限回避の脆弱性 | グループウェア「サイボウズ Office」には、複数の機能にアクセス制限回避の問題がありました。このため、第三者によって、グループウェアの情報を閲覧される可能性がありました。 | 2016 年 2 月 15 日 | 5.5 |
| 15 (#2) | 「サイボウズ Office」におけるクロスサイト・スクリプティングの脆弱性 | グループウェア「サイボウズ Office」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。 | 2016 年 2 月 15 日 | 5.0 |
| 16 (#1) | 「baserCMS」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「baserCMS」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。 | 2016 年 2 月 19 日 | 6.5 |
| 17 | 「Internet Explorer」におけるクロスドメインポリシーを回避される脆弱性 | ウェブブラウザ「Internet Explorer」には、クロスドメインポリシーを回避される脆弱性がありました。このため、細工されたコンテンツを閲覧することで、ユーザがアクセスしている URL の情報を取得される可能性がありました。 | 2016 年 2 月 19 日 | 4.3 |
| 18 | Windows 版および MacOS 版「LINE」におけるサービス運用妨害(DoS)の脆弱性 | Windows 版および MacOS 版コミュニケーションソフト「LINE」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。 | 2016 年 2 月 19 日 | 4.0 |

| 項番 | 脆弱性 | セキュリティ上の問題点 | JVN 公表日 | CVSS 基本値 |
|---|---|---|---|---|
| 19 | 「Log-Chat」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「Log-Chat」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。 | 2016 年 2 月 22 日 | 5.0 |
| 20 (#3) | コレガ製の複数の無線 LAN ルータにおけるクロスサイト・リクエスト・フォージェリの脆弱性 | コレガ製の複数の無線 LAN ルータには、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。 | 2016 年 3 月 2 日 | 4.0 |
| 21 (#3) | 「Aterm WF800HP」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 | 無線 LAN ルータ「Aterm WF800HP」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。 | 2016 年 3 月 30 日 | 4.0 |
| 脆弱性の深刻度=レベル I（注意）、CVSS 基本値=0.0～3.9 | | | | |
| 22 (#3) | バッファロー製の複数のネットワーク機器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 | バッファロー製の複数のネットワーク機器には、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。 | 2016 年 1 月 22 日 | 2.6 |
| 23 | 「Microsoft Producer for Microsoft Office PowerPoint」におけるクロスサイト・スクリプティングの脆弱性 | ウェブページ生成ソフト「Microsoft Producer for Microsoft Office PowerPoint」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。 | 2016 年 2 月 12 日 | 2.6 |
| 24 (#2) | 「サイボウズ Office」における情報漏えいの脆弱性 | グループウェア「サイボウズ Office」には、情報漏えいの問題がありました。このため、クロスサイト・リクエスト・フォージェリ(CSRF)対策用のトークンが漏えいする可能性がありました。 | 2016 年 2 月 15 日 | 2.6 |
| 25 (#2) | 「サイボウズ Office」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 | グループウェア「サイボウズ Office」には、複数の機能にクロスサイト・リクエスト・フォージェリの問題がありました。このため、第三者により意図しない操作をさせられる可能性がありました。 | 2016 年 2 月 15 日 | 2.6 |
| 26 (#2) | 「サイボウズ Office」におけるオープンリダイレクトの脆弱性 | グループウェア「サイボウズ Office」には、ネット連携機能にオープンリダイレクトの問題がありました。このため、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ました。 | 2016 年 2 月 15 日 | 2.6 |
| 27 (#1) | WordPress 用プラグイン「WP Favorite Posts」におけるクロスサイト・スクリプティングの脆弱性 | WordPress 用プラグイン「WP Favorite Posts」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。 | 2016 年 3 月 24 日 | 2.6 |
| 28 (#3) | 「Aterm WG300HP」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 | 無線 LAN ルータ「Aterm WG300HP」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。 | 2016 年 3 月 30 日 | 2.6 |

### （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 40 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[*12] 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 | Eaglesoft (Patterson Dental) でパスワードがハードコードされている問題 | 注意喚起として掲載 |
| 2 | Node.js のパッケージマネージャ npm が不正なパッケージの動作を制限しない問題 | 注意喚起として掲載 |
| 3 | Granite Data Services に XML 外部実体参照 (XXE) に関する脆弱性 | 注意喚起として掲載 |
| 4 | 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 |
| 5 | DameWare Mini Remote Control 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 |
| 6 | 国内のウェブサイトに SQL インジェクションの脆弱性 | 注意喚起として掲載 |
| 7 | DTE Insight に情報漏えいの脆弱性 | 注意喚起として掲載 |
| 8 | Quagga 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 |
| 9 | ISC BIND にサービス運用妨害 (DoS) の脆弱性 | 注意喚起として掲載<br>複数製品開発者へ通知 |
| 10 | ISC DHCP にサービス運用妨害 (DoS) の脆弱性 | 注意喚起として掲載<br>複数製品開発者へ通知 |
| 11 | SSLv2 の暗号通信を解読可能な脆弱性 (DROWN 攻撃) | 注意喚起として掲載 |
| 12 | コンテンツデリバリネットワーク (CDN) に対するサービス運用妨害 (DoS) の問題 (Forwarding Loop 攻撃) | 注意喚起として掲載<br>複数製品開発者へ通知 |
| 13 | Internet Key Exchange (IKEv1, IKEv2) が DoS 攻撃の踏み台として使用される問題 | 複数製品開発者へ通知 |
| 14 | QNAP Signage Station と iArtist Lite に複数の脆弱性 | 注意喚起として掲載 |
| 15 | 無線接続するキーボードやマウスなどの入力機器が安全でない独自通信プロトコルを使用している問題 | 注意喚起として掲載 |
| 16 | Apache Tomcat の複数の脆弱性に対するアップデート | 注意喚起として掲載 |
| 17 | FlexNet Publisher の lmgrd 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 |
| 18 | Android Platform の URLConnection クラスに HTTP ヘッダインジェクションの脆弱性 | 複数製品開発者へ通知 |
| 19 | Swann NVW-470 に複数の脆弱性 | 注意喚起として掲載 |
| 20 | Zhuhai RaySharp 由来のファームウェアを使用しているデジタルビデオレコーダにパスワードがハードコードされている問題 | 複数製品開発者へ通知 |
| 21 | glibc 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<br>複数製品開発者へ通知 |
| 22 | Hirschmann Classic Platform スイッチの管理者パスワードが SNMP コミュニティ名を通じて漏えいする問題 | 注意喚起として掲載 |
| 23 | Cisco Adaptive Security Appliance (ASA) の IKEv1 と IKEv2 の処理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 |
| 24 | Comodo Chromodo に同一生成元ポリシーを適用していない問題および旧バージョンの Chromium を使用している問題 | 注意喚起として掲載 |
| 25 | Netgear NMS300 に任意のファイルアップロードとパストラバーサルの脆弱性 | 注意喚起として掲載 |

[*12] 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 |
|---|---|---|
| 26 | フィッシャープライス Smart Toy 向けウェブサービスにおいて認証なしで API を呼び出せる脆弱性 | 注意喚起として掲載 |
| 27 | OpenELEC と RasPlex に root の SSH パスワードがハードコードされている問題 | 注意喚起として掲載 |
| 28 | Huawei E5151 および Huawei E5186 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 |
| 29 | OpenSSL の DH プロトコルにおける脆弱性 | 注意喚起として掲載<br>複数製品開発者へ通知 |
| 30 | Harman AMX 製品がハードコードされたパスワードを使用する問題 | 注意喚起として掲載 |
| 31 | FFmpeg および Libav に情報漏えいの脆弱性 | 注意喚起として掲載<br>複数製品開発者へ通知 |
| 32 | Oracle Outside In 8.5.2 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 |
| 33 | 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 |
| 34 | 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<br>複数製品開発者へ通知 |
| 35 | OpenSSH のクライアントに複数の脆弱性 | 注意喚起として掲載<br>複数製品開発者へ通知 |
| 36 | ISC DHCP にサービス運用妨害 (DoS) の脆弱性 | 注意喚起として掲載<br>複数製品開発者へ通知 |
| 37 | Samsung 製ネットワークビデオレコーダーに複数の脆弱性 | 注意喚起として掲載 |
| 38 | Ipswitch WhatsUp Gold の XML オブジェクトのデシリアライズ処理に脆弱性 | 注意喚起として掲載 |
| 39 | Comcast XFINITY Home Security の無線接続が切断されたときの処理に問題 | 注意喚起として掲載 |
| 40 | 古野電気製 Voyage Data Recorder (VDR) にユーザ入力値を適切に検証しない脆弱性 | 特定製品開発者と調整 |

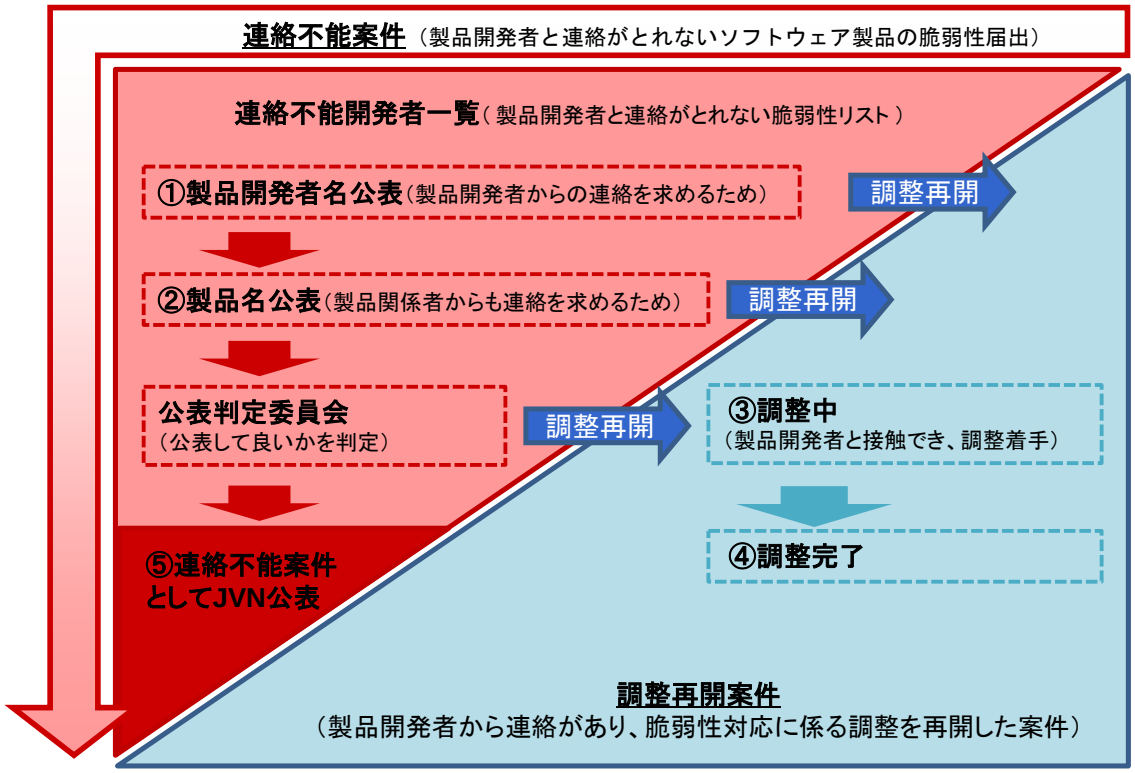
### 2-1-6. 連絡不能案件の処理状況

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、2016 年 3 月末までに、「連絡不能開発者」と位置づけて取扱った 229 件の処理状況の推移を示したものです。

「製品開発者名を公表（①）」について、今四半期は新たに 12 件公表しました。製品開発者名を公表しても製品開発者からの応答がないため追加情報として公表する「製品名公表（②）」について、今四半期は新たに公表した案件はありませんでした。また、製品開発者と調整が再開した「調整中（③）」および「調整が完了（④）」について、今四半期は変動がありませんでした。

この結果、2016 年 3 月末時点で連絡不能案件（①+②）は 186 件（前四半期は 174 件）、調整再開した案件（③+④）は 41 件（前四半期は 41 件）あります。

なお、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 公表に至った案件（⑤）について、今期に公表した案件はありませんでした。



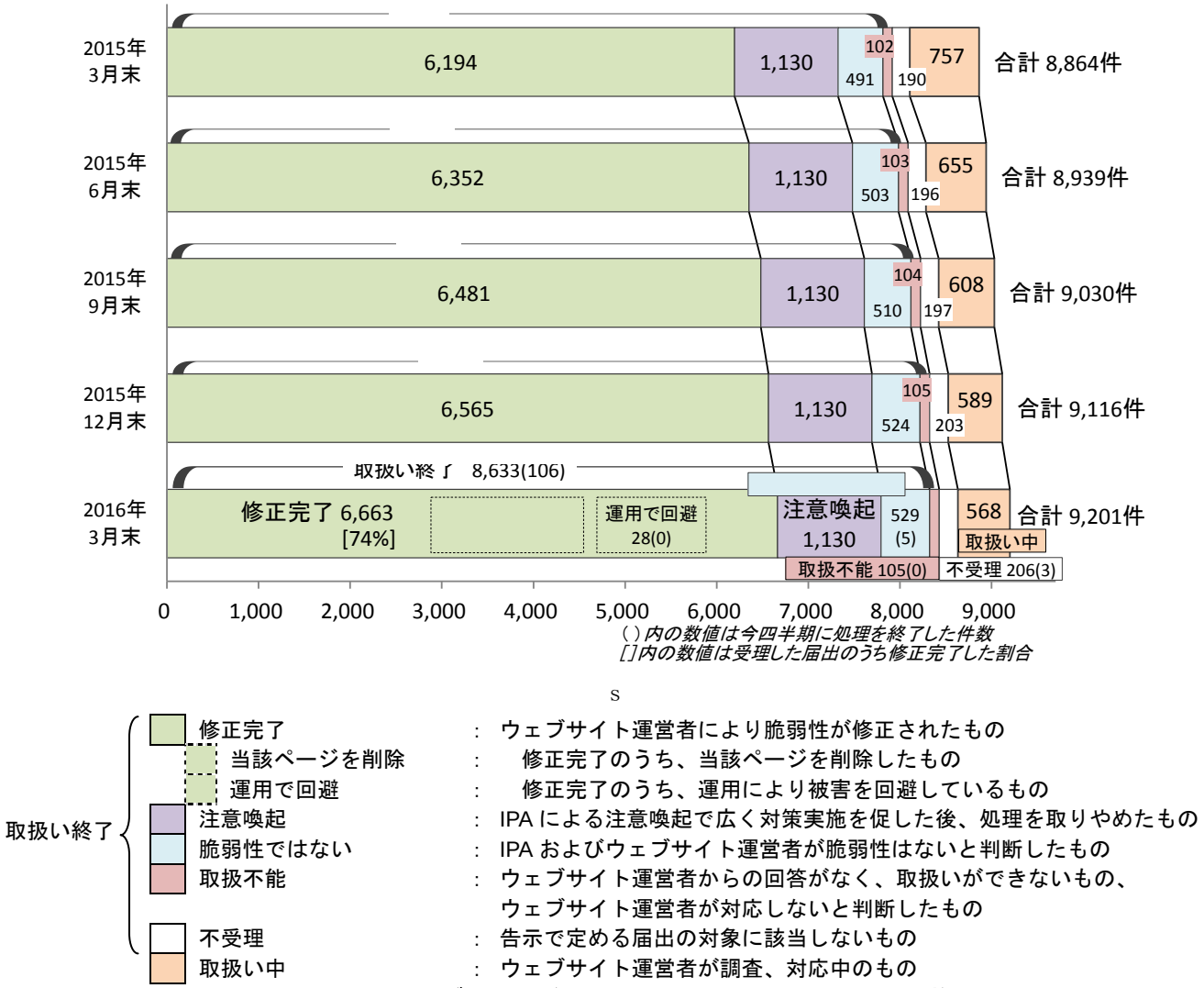

| | | | | |
|---|---|---|---|---|
| 2015年<br>第4四半期 | 174件<br>（①0件　②174件） | 41件<br>（③19件　④22件） | ⑤2件 | 合計<br>217件 |
| 2016年<br>第1四半期 | 186件<br>（①12件　②174件） | 41件<br>（③19件　④22件） | ⑤2件 | 合計<br>229件 |

**図2-12. 連絡不能案件の処理状況**

## 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。2016 年 3 月末時点の届出の累計は 9,201 件で、今四半期中に取扱いを終了したものは 106 件（累計 8,633 件）でした。このうち「修正完了」したものは 98 件（累計 6,663 件）、「注意喚起」により処理を取りやめたもの [*13] 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 5 件（累計 529 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 0 件（累計 105 件）でした。また「不受理」としたものは 3 件 [*14]（累計 206 件）でした。取扱いを終了した累計 8,633 件のうち「修正完了」「脆弱性ではない」の合計 7,192 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 32 件（累計 923 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**

[*13] 「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。

[*14] 内訳は今四半期の届出によるもの 2 件、前四半期までの届出によるもの 1 件。

今までに届出のあったウェブサイトの脆弱性 9,201 件のうち、不受理を除いた件数は 8,995 件でした。また、今四半期に届出のあった 85 件のうち、不受理を除いた件数は 84 件でした。以下に、不受理を除いた届出について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 84 件の約 7 割を企業が占めています。

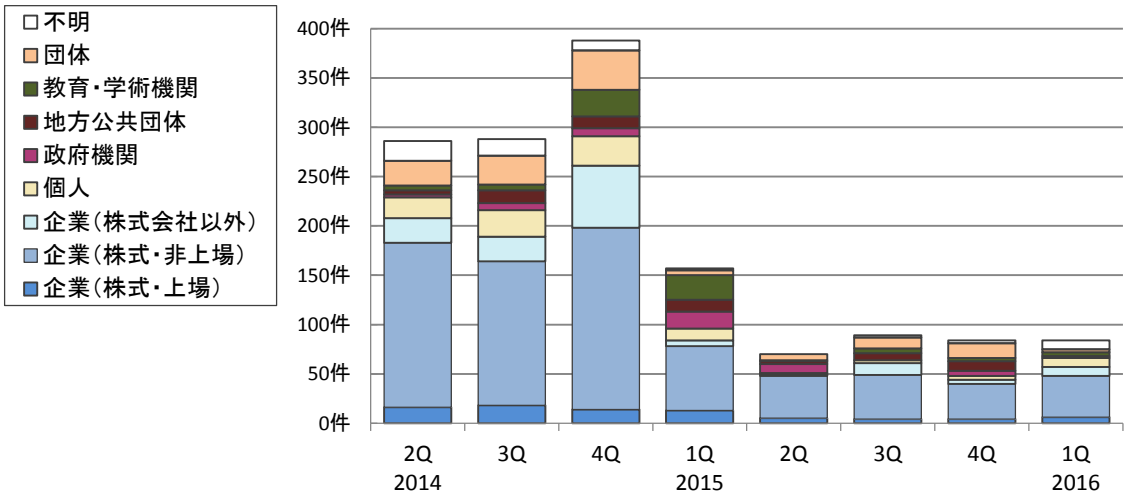



**図2−14. 四半期ごとの運営主体の種類別届出件数**

### 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[*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」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。今四半期は約 5 割を占める「クロスサイト・スクリプティング（40 件）」が最も多く、次いで「ファイルの誤った公開（22 件）」「SQL インジェクション（4 件）」となっています。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。

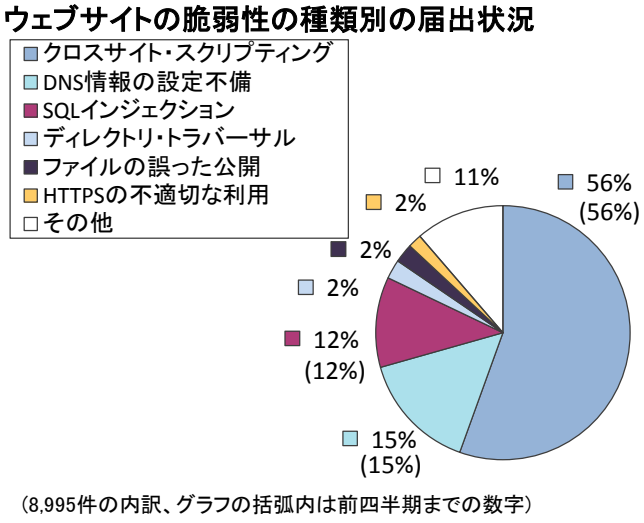



**図2−15. 届出累計の脆弱性の種類別割合**

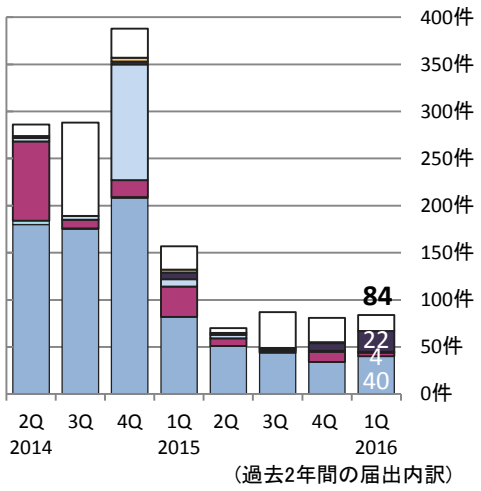


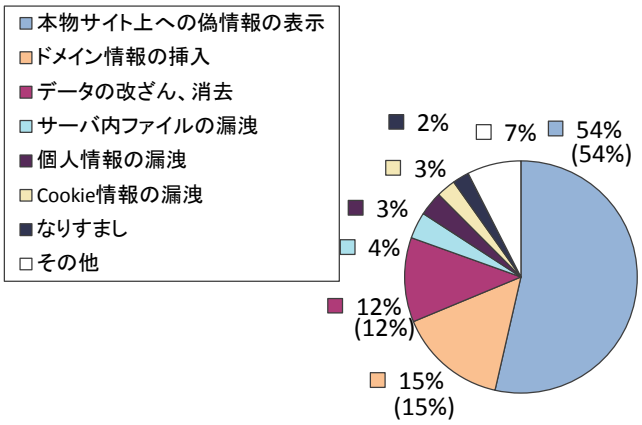

**図2−16. 四半期ごとの脆弱性の種類別届出件数**

[*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 2-17、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。

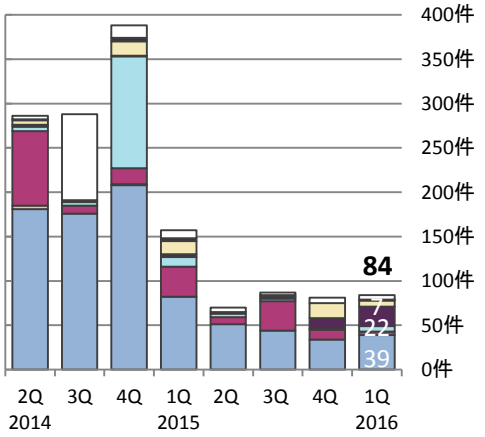
累計では、「本物サイト上への偽情報の表示」「ドメイン情報の挿入」「データの改ざん、消去」が全体の 8 割を占めています。これらは、「クロスサイト・スクリプティング」「DNS 情報の設定不備」「SQL インジェクション」などにより発生するものです。今四半期も「本物サイト上への偽情報の表示（39 件）」が最も多く、次いで「個人情報の漏洩（22 件）」「Cookie 情報の漏洩（7 件）」となっています。

**ウェブサイトの脆弱性がもたらす影響別の届出状況**




（8,995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。2016 年第 1 四半期に修正を完了した届出 98 件のうち 46 件（47%）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（84 件中 38 件）の 45%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。

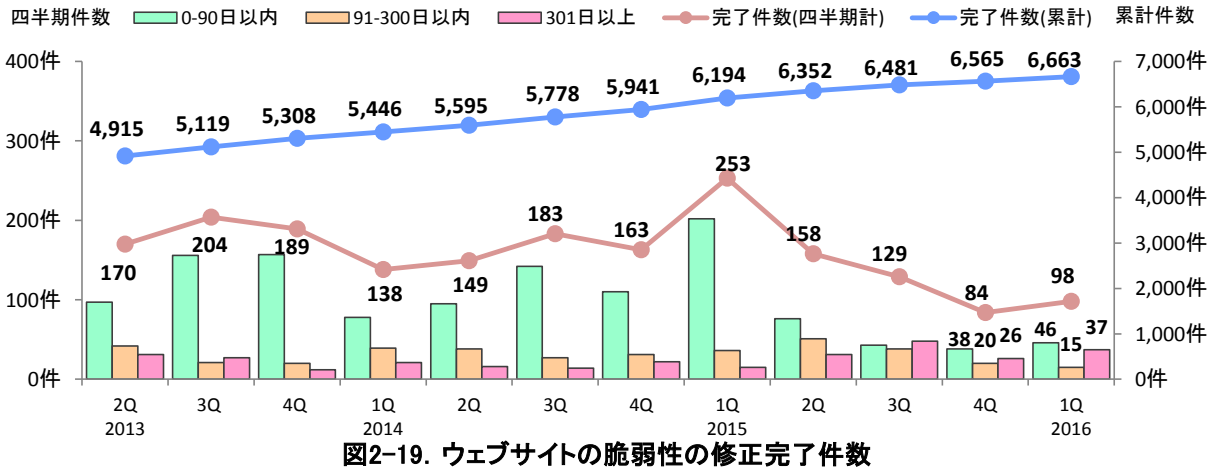



**図2−19. ウェブサイトの脆弱性の修正完了件数**

**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 2Q | 3Q | 4Q | 2014 1Q | 2Q | 3Q | 4Q | 2015 1Q | 2Q | 3Q | 4Q | 2016 1Q |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 修正完了件数 | 4,915 | 5,119 | 5,308 | 5,446 | 5,595 | 5,778 | 5,941 | 6,194 | 6,352 | 6,481 | 6,565 | 6,663 |
| 90 日以内の件数 | 3,244 | 3,400 | 3,557 | 3,635 | 3,730 | 3,872 | 3,982 | 4,184 | 4,260 | 4,303 | 4,341 | 4,387 |
| 90 日以内の割合 | 66% | 66% | 67% | 67% | 67% | 67% | 67% | 68% | 67% | 66% | 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 [*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。

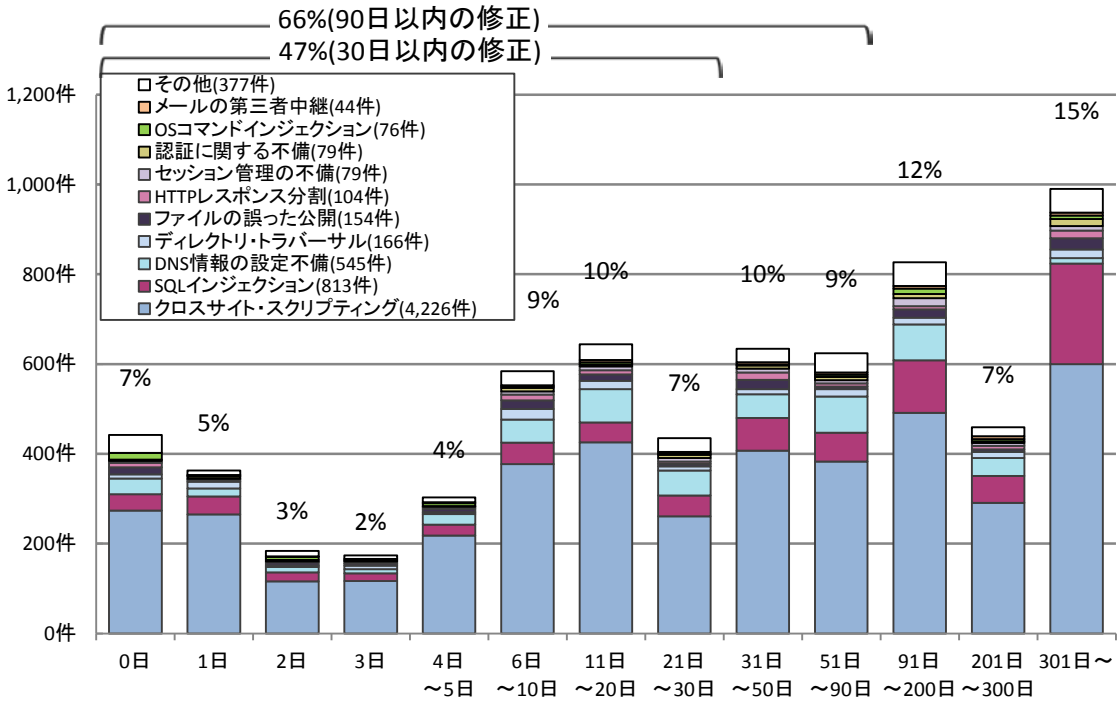



**図2-20. ウェブサイトの修正に要した日数**

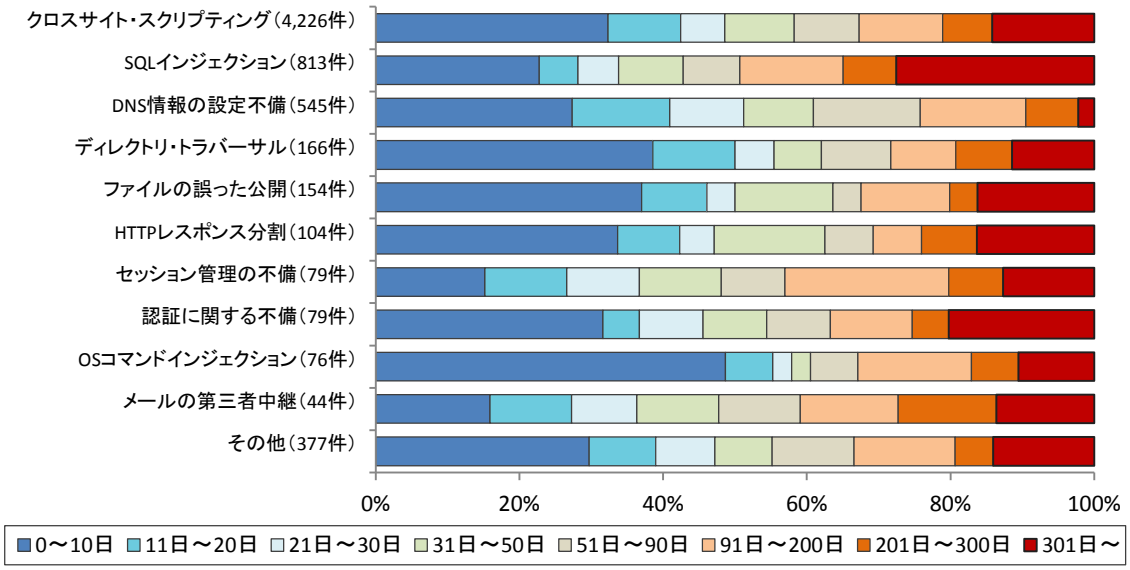



**図2-21. ウェブサイトの修正に要した脆弱性種類別の日数の傾向**

[*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. 長期化している届出の取扱い経過日数

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 436 件（前四半期は 473 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。

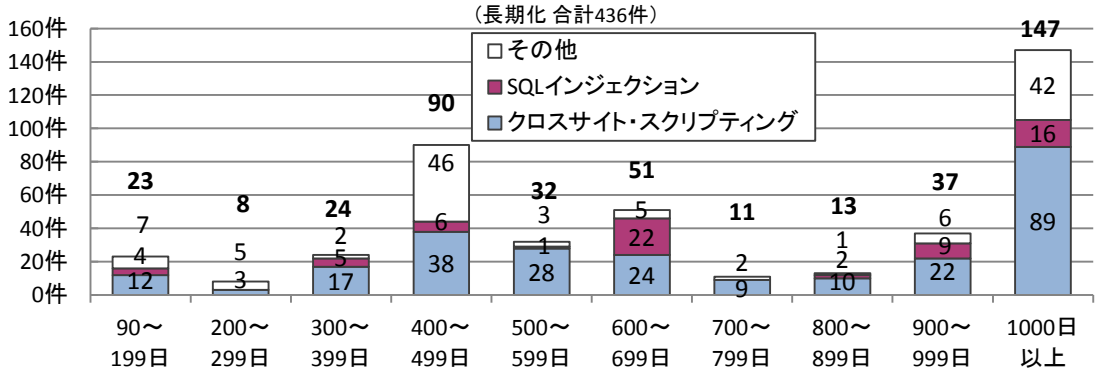



**図2−22. 取扱いが長期化(90日以上経過)しているウェブサイトの経過日数と脆弱性の種類**

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 2Q | 3Q | 4Q | 2015 1Q | 2Q | 3Q | 4Q | 2016 1Q |
|---|---|---|---|---|---|---|---|---|
| 取扱い中の件数 | 596 | 676 | 886 | 757 | 655 | 608 | 589 | 568 |
| 長期化している件数 | 353 | 402 | 446 | 415 | 562 | 504 | 473 | 436 |
| 長期化している割合 | 59% | 59% | 50% | 55% | 86% | 83% | 80% | 77% |

## 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

⇒「IPA 脆弱性対策コンテンツリファレンス」https://www.ipa.go.jp/files/000051352.pdf

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<br>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<br>通信の不正中継<br>なりすまし<br>任意のスクリプトの実行<br>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<br>価格等の改ざん<br>サービス不能<br>資源の枯渇<br>重要情報の漏洩<br>情報の漏洩<br>セッション・ハイジャック<br>通信の不正中継<br>なりすまし<br>任意のコマンドの実行<br>任意のスクリプトの実行<br>任意のファイルへのアクセス<br>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<br>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<br>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<br>情報の漏洩<br>任意のコードの実行<br>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<br>任意のコードの実行<br>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<br>サービス不能<br>資源の枯渇<br>任意のファイルへのアクセス<br>認証情報の漏洩 |

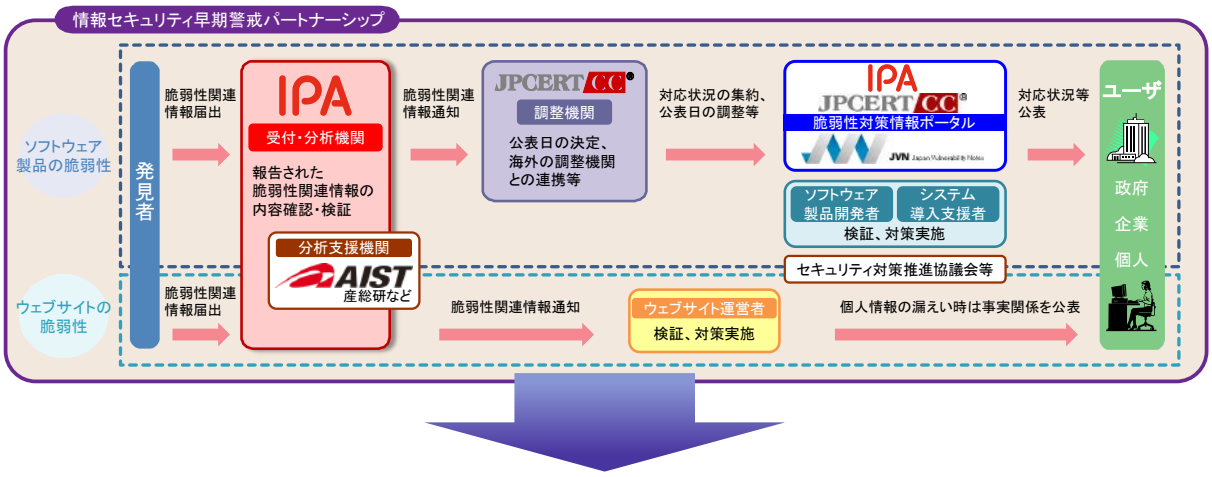
**付表 2. ウェブサイトの脆弱性の分類**

| | 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<br>サーバ内ファイルの漏洩<br>データの改ざん、消去<br>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<br>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<br>個人情報の漏洩<br>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<br>サーバ内ファイルの漏洩<br>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<br>サーバ内ファイルの漏洩<br>個人情報の漏洩<br>データの改ざん、消去<br>なりすまし<br>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<br>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<br>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