# ソフトウェア等の脆弱性関連情報に関する活動報告レポート

## [2013 年第 4 四半期（10 月～12 月）]

### ソフトウェア等の脆弱性関連情報に関する活動報告レポートについて

独立行政法人情報処理推進機構（以下、IPA）と一般社団法人 JPCERT コーディネーションセンター（以下、JPCERT/CC）は、ソフトウェア等脆弱性関連情報取扱基準（経済産業省告示 第 235 号）に基づき、2004 年 7 月より脆弱性関連情報の届出業務を実施しています。

本レポートでは、2013 年 10 月 1 日から 2013 年 12 月 31 日までの間に受け付けた脆弱性関連情報の統計及び事例について紹介しています。

独立行政法人情報処理推進機構 技術本部 セキュリティセンター
一般社団法人 JPCERT コーディネーションセンター
2014 年 1 月 22 日

目次

## 1. 2013 年第 4 四半期　ソフトウェア等の脆弱性関連情報に関する届出状況

### 1-1. 脆弱性関連情報の届出状況

**～ 脆弱性の届出件数の累計が 9,333 件になりました ～**

「情報セキュリティ早期警戒パートナーシップ [*1]」（以降、本制度）における届出状況について、表 1-1 は 2013 年第 4 四半期の脆弱性関連情報の届出件数および届出受付開始（2004 年 7 月 8 日）から今四半期までの累計件数を示しています。今期のソフトウェア製品に関する届出件数は 88 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 219 件、合計 307 件でした。届出受付開始からの累計件数は 9,333 件で、内訳はソフトウェア製品に関するもの 1,749 件、ウェブサイトに関するもの 7,584 件でウェブサイトに関する届出が全体の 81%を占めています。

**表 1-1.　届出件数**

| 分類 | 今期件数 | 累計件数 |
|---|---|---|
| ソフトウェア製品 | **88** 件 | **1,749** 件 |
| ウェブサイト | **219** 件 | **7,584** 件 |
| 合計 | **307** 件 | **9,333** 件 |

図 1-1 [*2] のグラフは過去 3 年間の届出件数の四半期別推移を示したものです。今四半期のソフトウェア製品、ウェブサイトに関する届出はともに前四半期よりも減少しています。表 1-2 は過去 3 年間の四半期別の累計届出件数および 1 就業日あたりの届出件数の推移です。今四半期の 1 就業日あたりの届出件数は 4.03 [*3] 件でした。

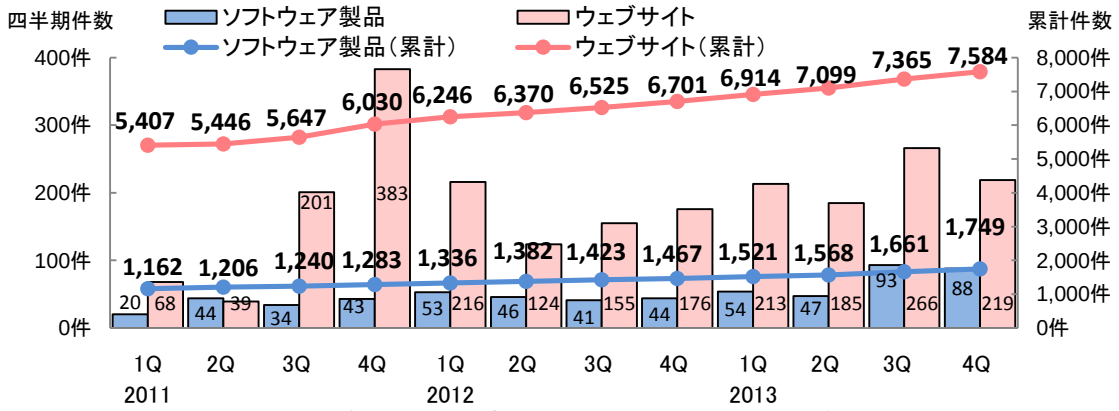



**図1−1.脆弱性関連情報の届出件数の四半期別推移**

**表 1−2. 届出件数（過去 3 年間）**

| | 2011 1Q | 2Q | 3Q | 4Q | 2012 1Q | 2Q | 3Q | 4Q | 2013 1Q | 2Q | 3Q | 4Q |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 累計届出件数[件] | 6,569 | 6,652 | 6,887 | 7,313 | 7,582 | 7,752 | 7,948 | 8,168 | 8,435 | 8,667 | 9,026 | 9,333 |
| 1就業日あたり[件/日] | 4.03 | 3.93 | 3.93 | 4.03 | 4.05 | 4.00 | 3.98 | 3.78 | 3.96 | 3.96 | 4.00 | 4.03 |

---

(*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) ソフトウェア等の脆弱性関連情報に関する活動報告レポート[2013 年第 3 四半期（7 月～9 月）]と比較し、図 1-1 のソフトウェア製品の届出件数について、2011 年第 4 四半期は既存の届出と同様の内容であることが判明したため 1 件減少、2013 年第 3 四半期は 1 つの届出に複数の脆弱性関連情報が記載されていたため 42 件増加しています。

(*3) 1 就業日あたりの届出件数は、「累計届出件数」/「届出受付開始からの就業日数」にて算出

また、図 1-2 は、届出受付開始から 2013 年 12 月末までの届出件数の年別推移です。過去、最も届出が多かったのは、2008 年（2,625 件）です。2013 年はソフトウェア製品が 282 件、ウェブサイトが 883 件の合計 1,165 件でした。**ソフトウェア製品の届出件数に関しては、過去最多だった 2006 年の 285 件に匹敵する件数です。**

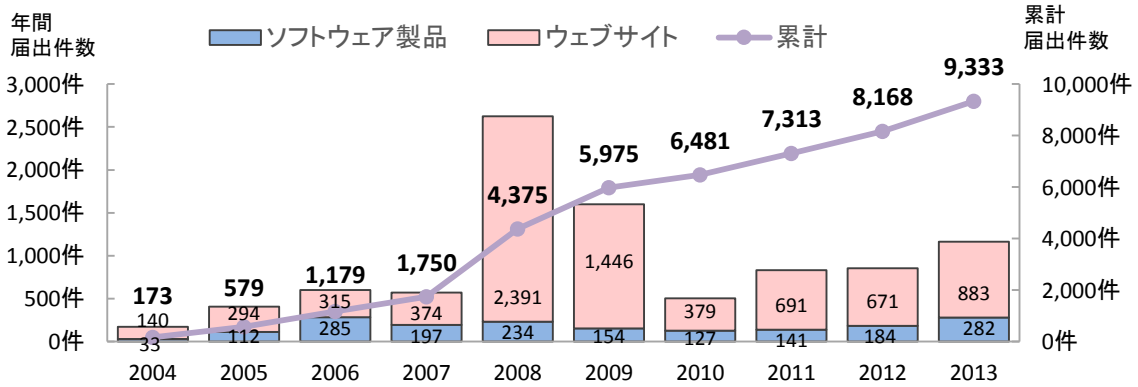



**図1−2. 脆弱性関連情報の届出件数の年別推移**

## 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 6,100 件を超えました～**

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 | 累計件数 |
|---|---|---|
| ソフトウェア製品 | **34** 件 | **819** 件 |
| ウェブサイト | **189** 件 | **5,308** 件 |
| 合計 | **223** 件 | **6,127** 件 |

ソフトウェア製品の脆弱性の届出のうち、製品開発者が修正を完了し、今四半期に JVN で対策情報を公表したものは 34 件 (*4)（累計 819 件）でした。四半期別修正完了件数は 2011 年以降 30 件前後で推移しており、今四半期は 34 件でした。(P9 図 2-12) そのうち、15 件が製品開発者自身から届けられた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公表までに 46 日 (*5) 以上経過したものは 19 件（56%）でした。

ウェブサイトの脆弱性関連情報の届出のうち、IPA がウェブサイト運営者に通知を行い、今四半期に修正を完了したものは 189 件（累計 5,308 件）でした。修正を完了した 189 件のうち、ウェブアプリケーションを修正したものが 175 件（93%）、当該ページを削除したもの 14 件（7%）でした。なお、修正を完了した 189 件のうち 32 件（17%）は、運営者へ脆弱関連情報を通知してから修正完了までに 91 日 (*6) 以上を要した届出です。今四半期は、修正完了までに 91 日以上を要した届出の割合が、前四半期（204 件中 48 件（24%））より減少しています。

(*4) 表 2-3 参照
(*5) 公表日の目安は、脆弱性関連情報の取扱を開始した日時から起算して 45 日後としています。
(*6) 対処の目安は、脆弱性関連情報の通知を受けてから、3 ヶ月以内としています。

また、図 1-3 は、届出開始から 2013 年 12 月末までの修正完了件数の年別推移を示しています。過去、1 年間で最も修正を完了した件数が多かったのは 2009 年（1,401 件）でした。2013 年の修正完了件数は、ソフトウェア製品が 127 件、ウェブサイトが 759 件の合計 886 件でした。**2013 年はソフトウェア製品の修正完了が、届出開始から最も多く行われた年となりました。**

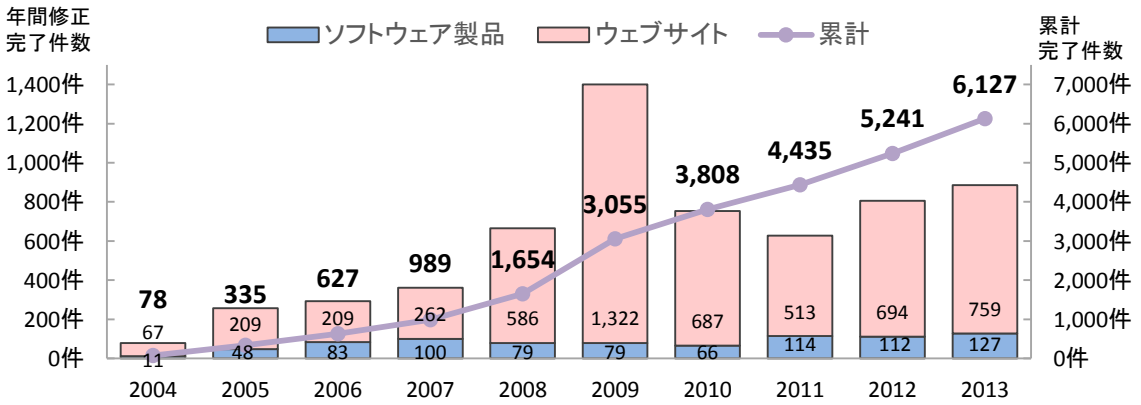



**図1-3. 脆弱性関連情報の修正完了件数の年別推移**

## 1-3. 調整不能案件の取扱い状況

本制度において届出を受け付けたソフトウェア製品の開発者に対して、一定期間にわたり連絡を試みても連絡が取れない製品開発者を「連絡不能開発者」と位置づけています。製品開発者と連絡をとる糸口を得るために、「連絡不能開発者一覧 (*7)」において段階的に製品開発者名と製品情報を公表し、製品開発者からの連絡および関係者からの情報提供を求めています。

### （1） 連絡不能開発者一覧の公表状況

今四半期は新たに「製品開発者名」16 件と、「製品情報（対象製品の具体的な名称およびバージョン）」を 4 件公表しました。これにより今四半期末時点の「連絡不能開発者一覧」の公表件数は、126 件となりました。

### （2） 連絡不能開発者一覧の公表後の取扱状況

今四半期は、製品開発者からの応答はありませんでした。また、これまでに応答があった 18 件のうち、8 件が本制度における取扱いを終了しました。

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

## 1-4. 脆弱性届出の傾向について

## 2013 年におけるソフトウェア製品の届出の約半数が Android アプリの脆弱性

**～ 開発者は Android OS が提供するアクセス制限機能を理解し、セキュアなコーディングを ～**

2013 年の 1 年間で、脆弱性として受理 (*8) したソフトウェア製品の届出は 253 件ありました。そのうち、117 件は Android 用のアプリケーション（以降、Android アプリ）で、ソフトウェア製品における届出の約半数を占めています。初めて届出のあった 2011 年からの経年で比較すると、昨年までは全体の 2 割に満たなかった Android アプリの脆弱性届出が 2013 年は急激に増えていることが見て取れます。

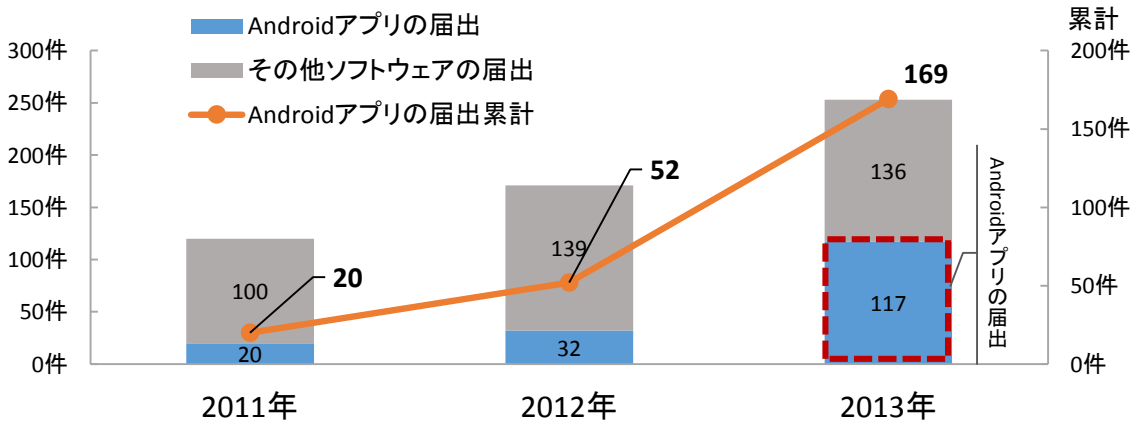



**図1-4. Androidアプリの届出件数の年別推移**

また、届出のあった Android アプリの脆弱性の内容は、表 1-4 の通りです。Android アプリの届出の累計は 169 件で「Android 特有の脆弱性 (*9)」が、全体の**約 3 割**を占めています。アプリの開発者は、従来のソフトウェア開発で作りこみ易い脆弱性に加えて、Android 特有の脆弱性についても注意が必要です。

**表 1-4. 届出のあった主な Android アプリの脆弱性の種類**

| 脆弱性の種類 | Android 特有の脆弱性 | 届出件数 |
|---|---|---|
| ファイルのアクセス制限不備 | ○ | 54 件 |
| 機能（コンポーネント）のアクセス制限不備 | ○ | |
| ログ出力に関する情報漏えい | ○ | |
| WebView クラスの実装不備 | ○ | |
| ディレクトリ・トラバーサルの脆弱性 | - | 115 件 |
| アドレスバーの偽装 | - | |
| SSL サーバ証明書の検証不備 | - | |
| データの暗号化不備 | - | |

また、IPA への届出では、Android アプリの脆弱性の届出が顕著に増加していますが、iOS などのスマートフォン上で動作する他のアプリにおいても類似の脆弱性が作り込まれる可能性があります。スマートフォンアプリの開発者は、IPA や JSSEC（一般社団法人日本スマートフォンセキュリティ協会）等で発信している資料 (*10) (*11) を参考に、脆弱性が作り込みにくいコーディングを心がけてください。

---

(*8) 脆弱性届出件数から、脆弱性として認められ、IPA で受理した件数を表す。届出の一部には、脆弱性ではないと判断し不受理とした届出が含まれている。

(*9) Android OS が提供するアクセス制限等の機能の理解不足に起因する脆弱性。

(*10) IPA テクニカルウォッチ 『Android アプリの脆弱性』に関するレポート
http://www.ipa.go.jp/about/technicalwatch/20120613.html

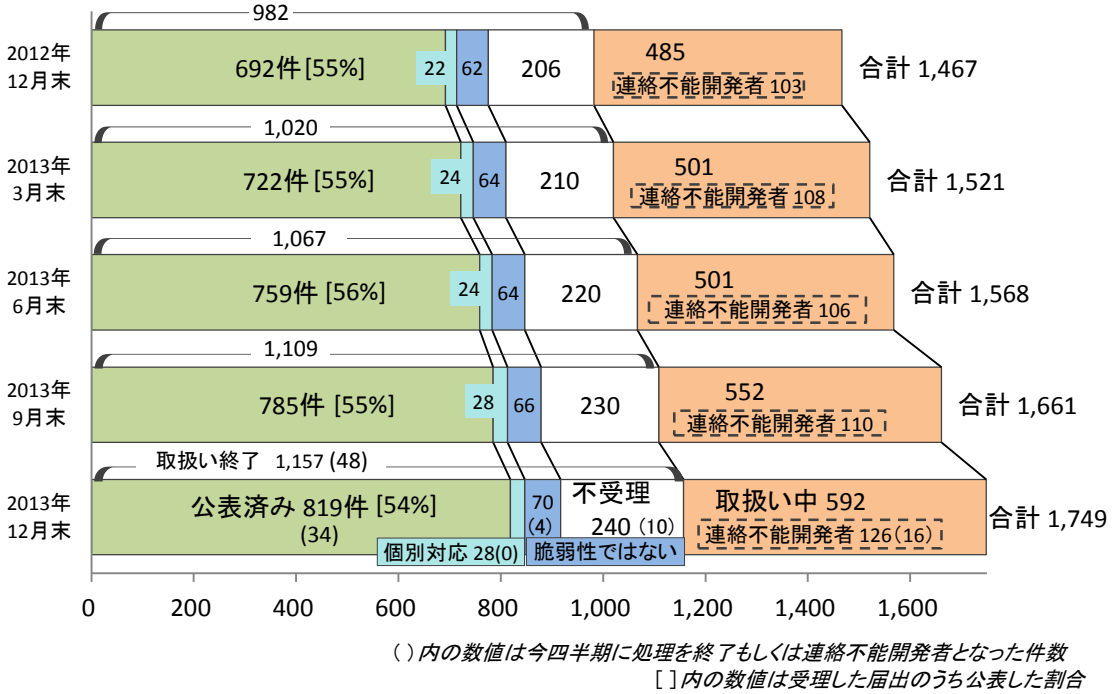
(*11) Android アプリのセキュア設計・セキュアコーディングガイド
http://www.jssec.org/report/securecoding.html

## 2. ソフトウェア等の脆弱性に関する届出状況（詳細）

### 2-1. ソフトウェア製品の脆弱性

#### 2-1-1. 処理状況

図 2-1 のグラフはソフトウェア製品の脆弱性関連情報の届出における、四半期別の処理状況の推移を示したものです。2013 年第 4 四半期末時点で取扱った届出件数は 1,749 件で、今四半期に公表した（修正完了した）脆弱性は 34 件（累計 819 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 0 件（累計 28 件）、製品開発者が「脆弱性ではない」と判断したものは 4 件（累計 70 件）、「不受理」としたものは 10 件 (*12)（累計 240 件）、取扱い中は 592 件でした。うち、取扱中の届出について連絡不能開発者一覧に公表した連絡不能開発者 (*13) は 16 件で、2013 年 12 末時点の連絡不能開発者公表数は 126 件になりました。




*( ) 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*

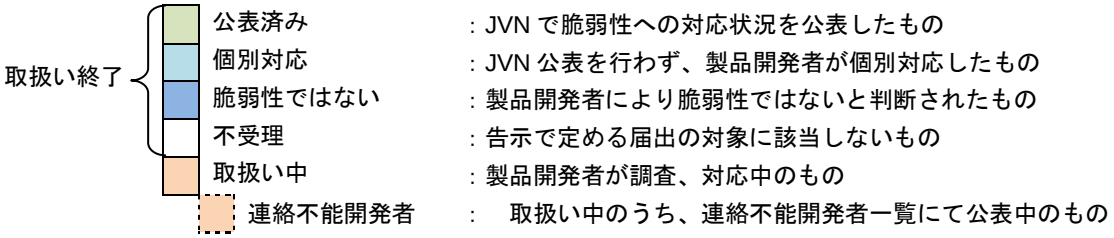



**図 2-1. 四半期別ソフトウェア製品脆弱性関連情報の届出の処理状況推移**

(*12) 今四半期の届出の中で不受理とした 8 件、前四半期までの届出の中で今四半期に不受理とした 2 件です。
(*13) 連絡不能開発者一覧への公表および一覧からの削除が複数回行われている製品開発者については、公表回数の累計を計上しています。

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関連情報1,749 件のうち、不受理を除いた 1,509 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 のグラフは製品種類別の割合を、図 2-3 は過去 2 年間を四半期別に推移をそれぞれ示したものです。

今四半期は「ファイル管理ソフト」が最も多く、これは前四半期からの傾向で、全体の 6 割弱を占めています。また、前四半期と比較して、「グループウェア」が多く届出されています。

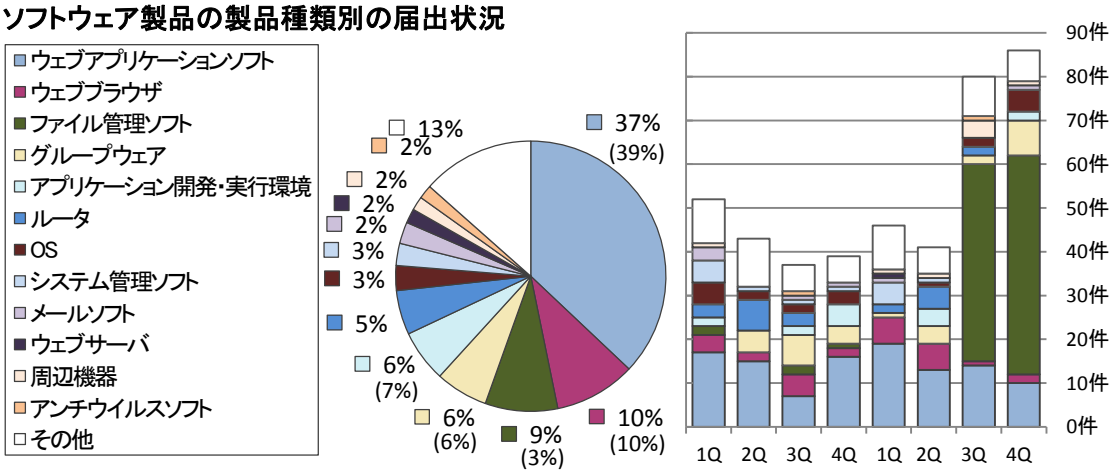



図2-2. 製品種類別の届出件数の割合




図2-3. 製品種類別の届出件数(四半期別推移)

図 2-4 のグラフはオープンソースソフトウェアとそれ以外のソフトウェアの割合を、図 2-5 は過去 2 年間の「オープンソースソフトウェア」と「それ以外」のソフトウェアの四半期別推移をそれぞれ示したものです。オープンソースソフトウェアの届出が占める割合は、今四半期までの累計で 31%となっています。

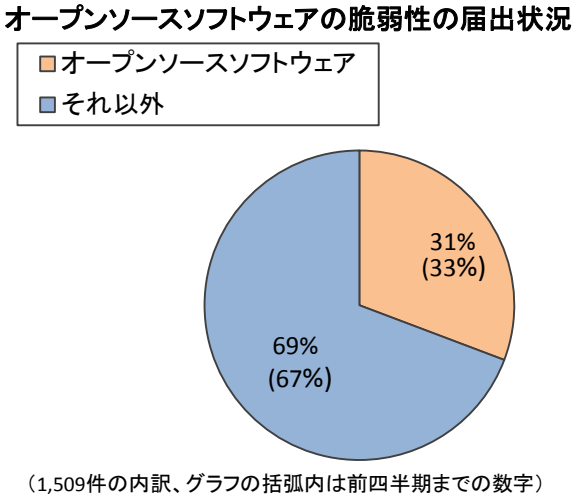



図2-4. オープンソースソフトウェアの届出件数の割合

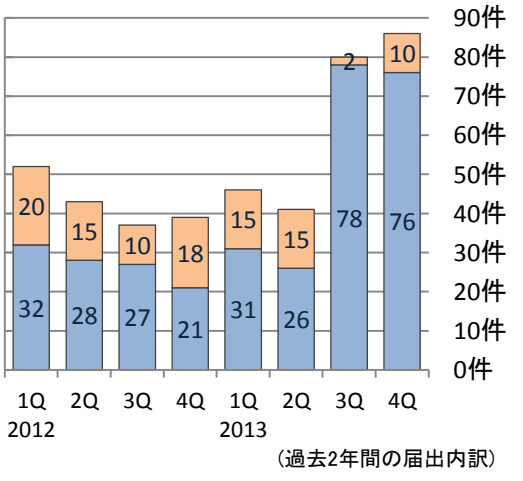



図2-5. オープンソースソフトウェアの届出件数（四半期別推移）

図 2-6 のグラフは過去 2 年間の「スマートフォン向けアプリ」と「それ以外」のソフトウェアの届出件数を四半期別に推移を、図 2-7 のグラフはスマートフォン向けアプリに関する届出の公表までに要した日数を示したものです。「スマートフォン向けアプリ」に関する届出は、2013 年第 3 四半期以降急増し、その割合も過半数を占めています。また、JVN で公表した脆弱性情報のうちスマートフォン向けアプリの届出は、40%が受理から 45 日以内に対策が行われており、それ以外のソフトウェア製品に比べて早めに対策される傾向にあります。

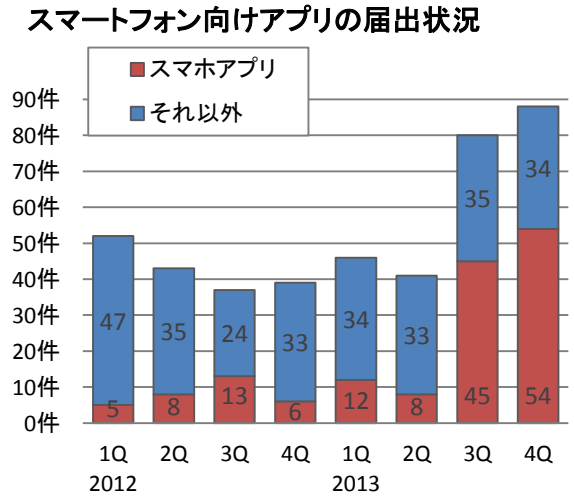



図2-6.スマートフォン向けアプリの届出件数（四半期別推移）

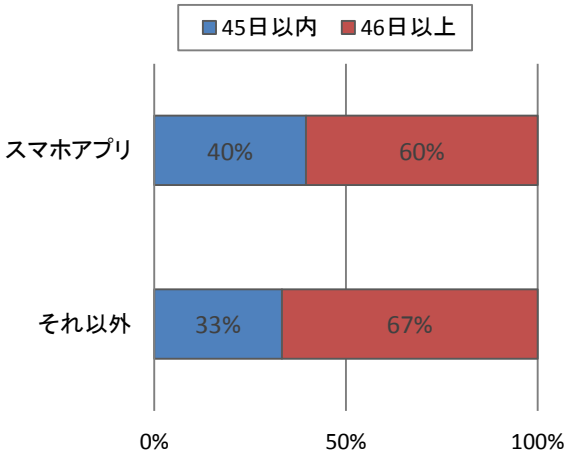
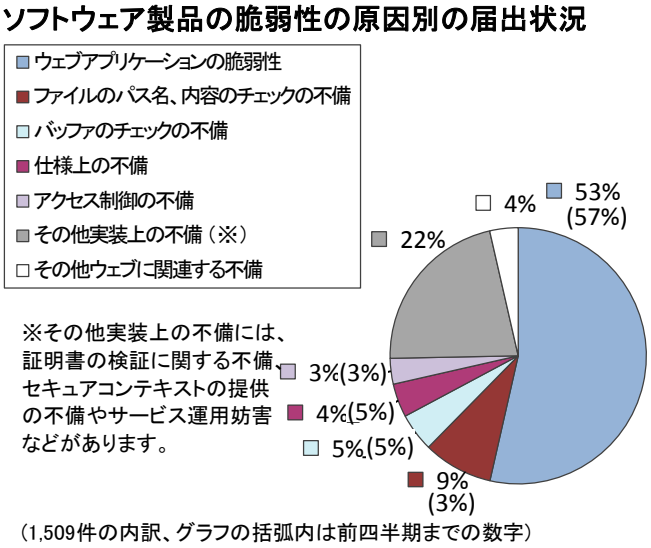



図2-7.スマートフォン向けアプリとそれ以外の公表までの日数

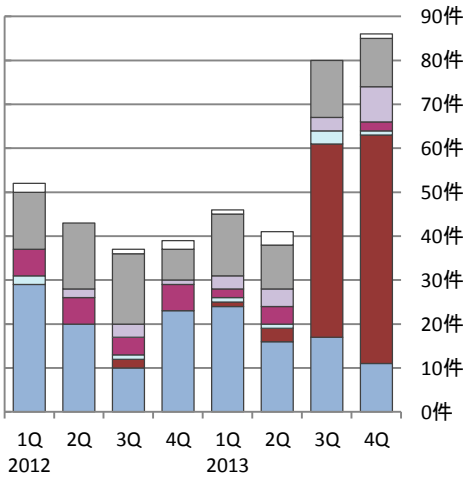
## 2-1-3. 脆弱性の原因と脅威別件数

図 2-8 のグラフは 2013 年第 4 四半期までの累計届出件数の原因別割合を、図 2-9 のグラフは過去 2 年間を四半期別に推移をそれぞれ示したものです。今四半期におけるの原因別の届出件数は、前四半期と同様に「ファイルのパス名、内容のチェックの不備」が最多となっています。




（1,509件の内訳、グラフの括弧内は前四半期までの数字）

図2-8. 脆弱性の原因別の届出件数の割合

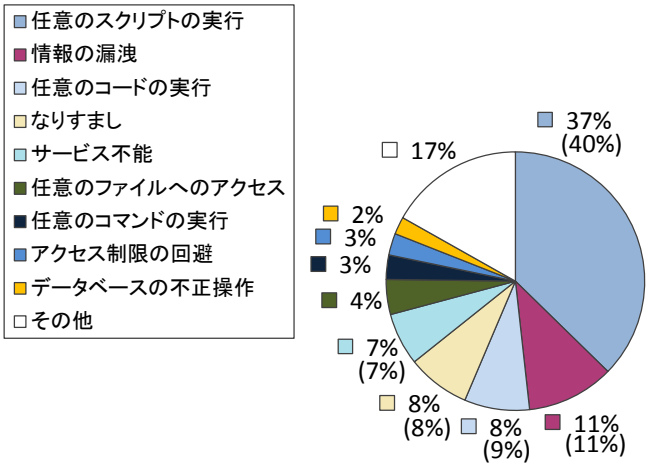



（過去2年間の届出内訳）

図2-9. 脆弱性の原因別の届出件数(四半期別推移)

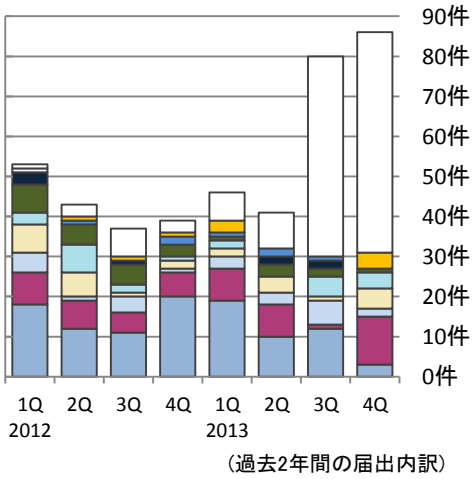
図 2-10 のグラフは 2013 年第 4 四半期までの脅威別の割合を、図 2-11 は過去 2 年間を脅威別に四半期別で推移をそれぞれ示したものです。届出受付開始から今四半期までの累計で、「任意のスクリプトの実行」が最も多く、全体の約 40%を占めています。また、「ファイルのパス名、内容のチェックの不備」がもたらす脅威である、任意のファイルの閲覧・改ざん・削除が「その他」に分類されるため、今四半期も前四半期と同様に「その他」が最多となっています。

**ソフトウェア製品の脆弱性がもたらす脅威別の届出状況**




（1,509件の内訳、グラフの括弧内は前四半期までの数字）

**図2-10. 脆弱性がもたらす脅威別の届出件数の割合**




（過去2年間の届出内訳）

**図2-11. 脆弱性がもたらす脅威別の届出件数（四半期別推移）**

### 2-1-4. 調整および公表件数

表 2-1 は情報の提供元別に、今期と累計の件数を示しています。JPCERT/CC は、2 種類の脆弱性関連情報について、日本国内の製品開発者や関係者との調整、および海外 CSIRT の協力のもと海外の製品開発者との調整を行っています[*14]。これらの脆弱性関連情報に対する製品開発者の対応状況は、IPA と JPCERT/CC が共同運営している脆弱性対策情報ポータルサイト JVN（Japan Vulnerability Notes）（URL： http://jvn.jp/ ）において公表しています。図 2-12 のグラフは、脆弱性情報の公表件数を国内および海外 CSIRT 等との連携によるものとに分け、過去 3 年分を四半期別に推移を示したものです。

**表 2-1. 脆弱性関連情報の提供元別 脆弱性公表件数**

| | 情報提供元 | 今期件数 | 累計件数 |
|---|---|---|---|
| ① | 国内外の発見者から届出があったもの、および製品開発者自身から自社製品の脆弱性、対策方法について届出を受けたもの | 34 件 | 819 件 |
| ② | 海外 CSIRT 等と連携して公表したもの | 35 件 | 1,007 件 |
| | 合計 | 69 件 | 1,826 件 |

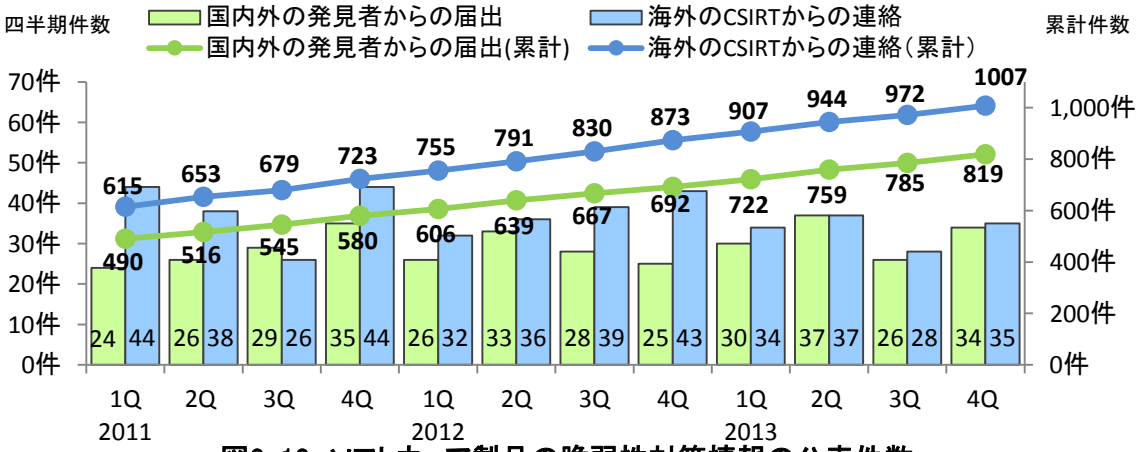



**図2-12. ソフトウェア製品の脆弱性対策情報の公表件数**

### （1） 国内外の発見者および製品開発者から届出があり、公表した脆弱性

届出受付開始から今四半期までに届出のあったソフトウェア製品の脆弱性関連情報（819 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。表 2-2 は過去 3 年間において 45 日以内に公表した件数の割合推移を四半期別に示したものです。45 日以内に公表した件数は今四半期で 34%、45 日を超過した件数は 66%です。製品開発者は脆弱性を攻撃された場合の危険性を認識し、迅速な対策を講じる必要があります。

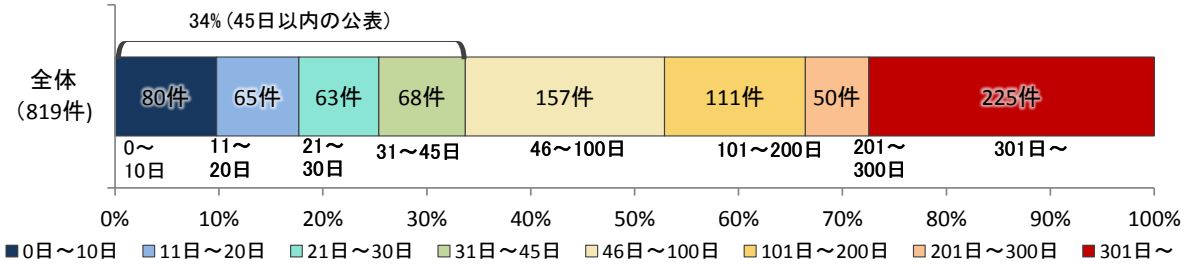



**図2-13. ソフトウェア製品の脆弱性公表日数**

**表 2-2. 45 日以内に公表した件数の割合推移（四半期別）**

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

[*14] JPCERT/CC 活動概要 Page15～21(http://www.jpcert.or.jp/pr/2014/PR20140116.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 11 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 11 件（表 2-3 の*2）、複数開発者・製品に影響がある脆弱性 3 件（表 2-3 の*3）、組込みソフトウェア製品の脆弱性が 6 件（表 2-3 の*4）ありました。

**表 2-3. 2013 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（*2）（*3） | 複数製品で使用されている「International Components for Unicode (ICU)」に解放済みメモリ使用 (use-after-free) の脆弱性 | Unicode ライブラリ「International Components for Unicode (ICU)」には、解放済みメモリ使用 (use-after-free) の脆弱性がありました。このため、第三者によりサービス運用妨害 (DoS) 攻撃を受けるなどの可能性がありました。 | 2013 年 10 月 30 日 | 7.5 |
| 2（*1） | 「Tiki Wiki CMS Groupware」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「Tiki Wiki CMS Groupware」には、SQL 文を組み立てる処理に問題がありました。このため、第三者により任意の SQL 命令を実行される可能性がありました。 | 2013 年 11 月 5 日 | 7.5 |
| 3（*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こ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を実行される可能性がありました。 | 2013 年 11 月 12 日 | 9.3 |
| 4（*4） | D-Link「DES-3800」シリーズにおけるサービス運用妨害 (DoS) の脆弱性 | ネットワークスイッチ「DES-3800」シリーズには、Web マネージャーの機能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。 | 2013 年 11 月 22 日 | 7.8 |
| 5（*4） | Juniper「ScreenOS」におけるサービス運用妨害 (DoS) の脆弱性 | セキュリティ製品用 OS「ScreenOS」には、パケットの取扱いに不備がありました。このため、第三者により当該 OS を組み込んだセキュリティ製品を停止させられる可能性がありました。 | 2013 年 12 月 13 日 | 7.8 |
| 脆弱性の深刻度=レベル II（警告）、CVSS 基本値=4.0～6.9 | | | | |
| 6 | 「Accela BizSearch」におけるクロスサイト・スクリプティングの脆弱性 | 検索ソフト「Accela BizSearch」には、ウェブページを出力する際の処理に問題がありました。このため、第三者によりウェブページにスクリプトを埋め込まれる可能性がありました。 | 2013 年 10 月 4 日 | 4.3 |
| 7（*4） | 「HDL-A」および「HDL2-A」シリーズにおけるセッション管理に関する脆弱性 | ファイルサーバ「HDL-A」および「HDL2-A」シリーズには、ログイン画面のセッション管理に関する処理に問題がありました。このため、第三者にユーザになりすまされ当該製品にアクセスされる可能性がありました。 | 2013 年 10 月 18 日 | 4.0 |
| 8（*4） | 「RockDisk」におけるクロスサイト・スクリプティングの脆弱性 | ファイルサーバ「RockDisk」には、ウェブページを出力する際の処理に問題がありました。このため、第三者によりウェブページにスクリプトを埋め込まれる可能性がありました。 | 2013 年 10 月 29 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 |
|---|---|---|---|---|
| 9 (*2) (*3) | 複数製品で使用されている「International Components for Unicode (ICU)」にサービス運用妨害 (DoS) の脆弱性 | Unicode ライブラリ「International Components for Unicode (ICU)」には、競合状態 (race condition) 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、第三者によりサービス運用妨害 (DoS) 攻撃を受ける可能性がありました。 | 2013 年 10 月 30 日 | 6.8 |
| 10 | 「改造版 TOWN」におけるクロスサイト・スクリプティングの脆弱性 | CGI ゲーム「改造版 TOWN」には、ウェブページを出力する際の処理に問題がありました。このため、第三者によりウェブページにスクリプトを埋め込まれる可能性がありました。 | 2013 年 11 月 7 日 | 4.3 |
| 11 (*1) | 「Page Scroller」におけるクロスサイト・スクリプティングの脆弱性 | スクリプト「Page Scroller」には、既知のクロスサイト・スクリプティングの脆弱性を持つ jQuery を同梱していました。このため、第三者によりウェブページにスクリプトを埋め込まれる可能性がありました。 | 2013 年 11 月 7 日 | 4.3 |
| 12 (*1) | 「EC-CUBE」における情報漏えいの脆弱性 | ショッピングサイト構築システム「EC-CUBE」には、エラーログの出力に問題があり、情報漏えいの脆弱性が存在しました。このため、第三者により運営者しか知りえない情報を取得されてしまう可能性がありました。 | 2013 年 11 月 20 日 | 4.3 |
| 13 (*1) | 「EC-CUBE」における情報漏えいの脆弱性 | ショッピングサイト構築システム「EC-CUBE」には、情報漏えいの脆弱性が存在しました。このため、第三者により当該製品の絶対パスを取得されてしまう可能性がありました。 | 2013 年 11 月 20 日 | 5.0 |
| 14 (*1) | 「EC-CUBE」における情報漏えいの脆弱性 | ショッピングサイト構築システム「EC-CUBE」には、フロント機能の処理に問題があり、情報漏えいの脆弱性が存在しました。このため、第三者により他のショッピングサイト利用者の登録情報を取得されたり、改ざんされたりする可能性がありました。 | 2013 年 11 月 20 日 | 5.5 |
| 15 (*1) | 「EC-CUBE」におけるクロスサイト・スクリプティングの脆弱性 | ショッピングサイト構築システム「EC-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。 | 2013 年 11 月 20 日 | 4.3 |
| 16 (*4) | D-Link「DES-3800」シリーズにおけるサービス運用妨害 (DoS) の脆弱性 | ネットワークスイッチ「DES-3800」シリーズには、SSH の実装に不備がありました。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。 | 2013 年 11 月 22 日 | 6.8 |
| 17 | 「KDrive 個人版 PC クライアントソフト」における SSL サーバ証明書の検証不備の脆弱性 | オンラインストレージ KDrive 用ソフト「KDrive 個人版 PC クライアントソフト」には、SSL サーバ証明書の検証不備の脆弱性がありました。このため、中間者攻撃による暗号通信の解読などが行われる可能性がありました。 | 2013 年 11 月 22 日 | 4.0 |
| 18 (*2) | 「改造版 TOWN」におけるディレクトリ・トラバーサルの脆弱性 | CGI ゲーム「改造版 TOWN」には、ディレクトリ・トラバーサルの脆弱性が存在しました。第三者によりサーバ上の任意のファイルを取得される可能性がありました。 | 2013 年 11 月 29 日 | 5.0 |
| 19 (*2) | 「サイボウズ ガルーン」における複数のクロスサイト・スクリプティングの脆弱性 | グループウェア「サイボウズ ガルーン」には、ウェブページを出力する際の処理に問題がありました。このため、第三者によりウェブページにスクリプトを埋め込まれる可能性がありました。 | 2013 年 12 月 3 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 |
|---|---|---|---|---|
| 20 (*2) | 「サイボウズ ガルーン」における SQL インジェクションの脆弱性 | グループウェア「サイボウズ ガルーン」には、SQL 文を組み立てる処理に問題がありました。このため、第三者により任意の SQL 命令を実行される可能性がありました。 | 2013 年 12 月 3 日 | 6.0 |
| 21 (*2) | 「サイボウズ ガルーン」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 ガルーン」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、第三者により当該製品が動作しているサーバの CPU に負荷をかけられる可能性がありました。 | 2013 年 12 月 3 日 | 4.3 |
| 22 (*2) | 「サイボウズ ガルーン」におけるメールヘッダ・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、電話メモのメール転送処理に不備がありました。このため、第三者により転送されるメールのヘッダが細工される可能性がありました。 | 2013 年 12 月 3 日 | 4.0 |
| 23 (*2) | 「サイボウズ ガルーン」におけるセッション固定の脆弱性 | グループウェア「サイボウズ ガルーン」には、セッション固定の脆弱性がありました。このため、第三者により登録ユーザになりすまされる可能性がありました。 | 2013 年 12 月 3 日 | 5.8 |
| 24 (*1) (*3) (*4) | 「Android OS」において任意の Java のメソッドが実行される脆弱性 | 「Android OS」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 Android OS の機能を起動されたり、任意のコードを実行されたりする可能性がありました。 | 2013 年 12 月 17 日 | 6.8 |
| 25 | 「IrfanView」におけるバッファオーバーフローの脆弱性 | 画像ビューアソフト「IrfanView」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。 | 2013 年 12 月 24 日 | 6.8 |
| 26 (*2) | 「サイボウズ ガルーン」における SQL インジェクションの脆弱性 | グループウェア「サイボウズ ガルーン」には、SQL 文を組み立てる処理に問題がありました。このため、第三者により任意の SQL 命令を実行される可能性がありました。 | 2013 年 12 月 25 日 | 6.5 |
| 27 (*2) | 「サイボウズ ガルーン」のケータイ機能における認証回避の脆弱性 | グループウェア「サイボウズ ガルーン」には、認証処理に不備がありました。このため、第三者によりログイン認証を回避される可能性がありました。 | 2013 年 12 月 25 日 | 5.8 |
| 脆弱性の深刻度=レベル I（注意）、CVSS 基本値=0.0～3.9 | | | | |
| 28 (*1) | 「Tiki Wiki CMS Groupware」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「Tiki Wiki CMS Groupware」には、ウェブページを出力する際の処理に問題がありました。このため、第三者によりウェブページにスクリプトを埋め込まれる可能性がありました。 | 2013 年 11 月 5 日 | 2.6 |
| 29 | 「ASP.NET」におけるオープンリダイレクトの脆弱性 | ウェブアプリケーションフレームワーク「ASP.NET」のログインコンポーネントには、オープンリダイレクトの脆弱性が存在しました。このため、第三者により任意のウェブサイトにリダイレクトされる可能性がありました。 | 2013 年 11 月 15 日 | 2.6 |
| 30 (*1) | 「EC-CUBE」におけるクロスサイト・スクリプティングの脆弱性 | ショッピングサイト構築システム「EC-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。 | 2013 年 11 月 20 日 | 2.6 |
| 31 (*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。 | 2013 年 11 月 20 日 | 2.6 |

| 項番 | 脆弱性 | セキュリティ上の問題点 | JVN 公表日 | CVSS 基本値 |
|---|---|---|---|---|
| 32 | 「サイボウズ デヂエ」におけるクロスサイト・スクリプティングの脆弱性 | Web データベース「サイボウズ デヂエ」には、ウェブページを出力する際の処理に問題がありました。このため、第三者によりウェブページにスクリプトを埋め込まれる可能性がありました。 | 2013 年 12 月 10 日 | 2.6 |
| 33 (*1) | 「VMware ESX および ESXi」において任意のファイルにアクセス可能な問題 | 仮想化ソフトウェア（ハイパーバイザー）「VMware ESX および ESXi」には、仮想マシンファイル記述子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ファイルが読みとられる可能性がありました。 | 2013 年 12 月 24 日 | 2.1 |
| 34 | 「HP Autonomy Ultraseek」におけるクロスサイト・スクリプティングの脆弱性 | 検索ソフト「HP Autonomy Ultraseek」には、特定の文字コードの処理に問題がありました。このため、第三者によりウェブページにスクリプトを埋め込まれる可能性がありました。 | 2013 年 12 月 26 日 | 2.6 |

（*1）：オープンソースソフトウェア製品の脆弱性
（*2）：製品開発者自身から届けられた自社製品の脆弱性
（*3）：複数開発者・製品に影響がある脆弱性
（*4）：組込みソフトウェアの脆弱性

### （2） 海外 CSIRT 等と連携して公表した脆弱性

表 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 35 件あり、うち表 2-4 には通常の脆弱性情報 33 件、表 2-5 には対応に緊急を要する Technical Cyber Security Alert の 2 件を示しています。これらの情報は、通常関係する登録済み製品開発者へ通知したうえ、JVN に掲載しています。

**表 2-4.米国 CERT/CC (*15) 等と連携した脆弱性関連情報および対応状況**

| 項番 | 脆弱性 | 対応状況 |
|---|---|---|
| 1 | マルチコア CPU の共有 L3 キャッシュに対するサイドチャネル攻撃 | 注意喚起として掲載 |
| 2 | baramundi Management Suite に複数の脆弱性 | 注意喚起として掲載 |
| 3 | ASUS Wireless-N150 Router RT-N10E に認証回避の脆弱性 | 注意喚起として掲載 |
| 4 | McAfee Agent にサービス運用妨害(DoS)の脆弱性 | 注意喚起として掲載 |
| 5 | 無線 LAN アクセスポイント ZoneFlex 2942 に認証回避の脆弱性 | 注意喚起として掲載 |
| 6 | HR Systems Strategies の info:HR に認証情報の管理に関する脆弱性 | 注意喚起として掲載 |
| 7 | Oracle Outside In 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 |
| 8 | SAP Sybase Adaptive Server Enterprise に XML インジェクションの脆弱性 | 注意喚起として掲載 |
| 9 | 複数の D-Link 製ルータに認証回避の脆弱性 | 注意喚起として掲載 |
| 10 | Oracle Outside In 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 |
| 11 | Watchguard Extensible Threat Management (XTM)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 | JavaServer Faces に複数の脆弱性 | 注意喚起として掲載 |
| 13 | DrayTek Vigor2700 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 |
| 14 | 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 |
| 15 | TVT TD-2308SS-B 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 |

(*15) CERT/Coordination Center：1988 年のウイルス感染事件を契機に米国カーネギーメロン大学に設置された CSIRT。

| 項番 | 脆弱性 | 対応状況 |
|---|---|---|
| 16 | Tyler Technologies TaxWeb に複数の脆弱性 | 注意喚起として掲載 |
| 17 | Cisco Identity Services Engine に脆弱性 | 注意喚起として掲載 |
| 18 | Openbravo ERP に情報漏えいの脆弱性 | 注意喚起として掲載 |
| 19 | Joomla!にファイルアップロードに関する脆弱性 | 注意喚起として掲載 |
| 20 | NAS4Free にコードインジェクションの脆弱性 | 注意喚起として掲載 |
| 21 | Tiki Wiki CMS Groupware 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 |
| 22 | Attachmate Verastream Host Integrator に任意のファイルを上書き可能な脆弱性 | 注意喚起として掲載 |
| 23 | IBM Tivoli Federated Identity Manager および IBM Tivoli Federated Identity Manager Business Gateway にオープンリダイレクトの脆弱性 | 注意喚起として掲載 |
| 24 | 信頼できないパラメータを使用して生成した Dual_EC_DRBG の出力結果が推測可能な問題 | 注意喚起として掲載 |
| 25 | EMC Documentum 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 |
| 26 | Adobe ColdFusion に複数の脆弱性 | 注意喚起として掲載 |
| 27 | Thomson Reuters Velocity Analytics Vhayu Analytic Server にコードインジェクションの脆弱性 | 注意喚起として掲載 |
| 28 | EMC Document Sciences xPression に複数の脆弱性 | 注意喚起として掲載 |
| 29 | AT&T Connect Participant Application for Windows 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 |
| 30 | NagiosQL 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 |
| 31 | SketchUp Viewer 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 |
| 32 | 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 |
| 33 | Apple Motion における任意のコード実行の脆弱性に対するアップデート | 注意喚起として掲載 |

**表 2-5.米国 US-CERT [(*16)] と連携した脆弱性関連情報および対応状況**

| 項番 | 脆弱性 |
|---|---|
| 1 | Microsoft 製品の複数の脆弱性に対するアップデート |
| 2 | Microsoft 製品の複数の脆弱性に対するアップデート |

(*16) United States Computer Emergency Readiness Team：米国の政府系 CSIRT。

### 2-1-5. 調整不能案件の処理状況別件数

#### （1） 連絡不能開発者一覧（製品開発者名および製品情報）の公表状況

図 2-14 は今四半期の連絡不能開発者一覧(製品開発者名および製品情報)の公表件数と今四半期までの累計件数を示しています。「連絡不能開発者一覧」にある「製品開発者名」の公表件数の累計は 144 件で、今四半期は、新たに「製品開発者名」を 16 件公表し、「製品開発者名」に加えて「製品情報（対象製品の具体的な名称およびバージョン）」を 4 件公表しています。このうち 18 件が調整を再開しています。

#### （2） 製品開発者情報の公開調査結果

図 2-15 は今四半期までに公表した連絡不能開発者の公開調査の結果を示しています。今四半期末時点の公開中の連絡不能開発者件数は、126 件です。また、「連絡不能開発者一覧」の公開開始（2011 年 9 月 29 日）から今四半期末時点までに 18 件が調整を再開し、製品開発者と調整を完了した累計 8 件が本制度における取扱いを終了しました。「連絡不能開発者一覧」の公開開始から 2 年が経過しましたが、今四半期末時点で 126 件は依然として、製品開発者と連絡がとれない状況です。

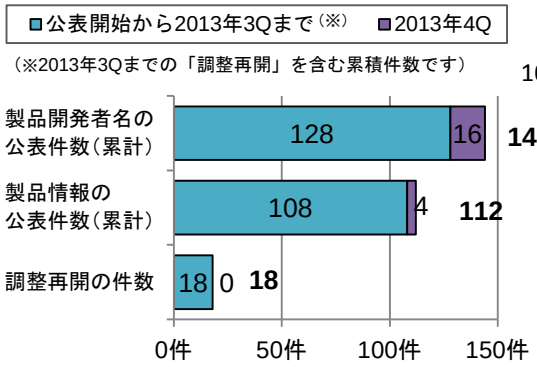



図2-14. 2013年4Qの公表および調整再開の状況

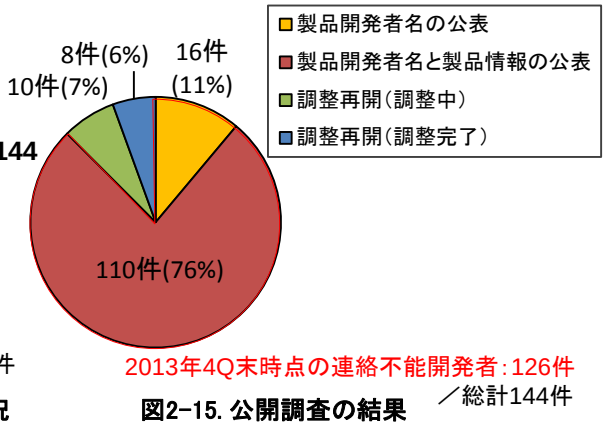


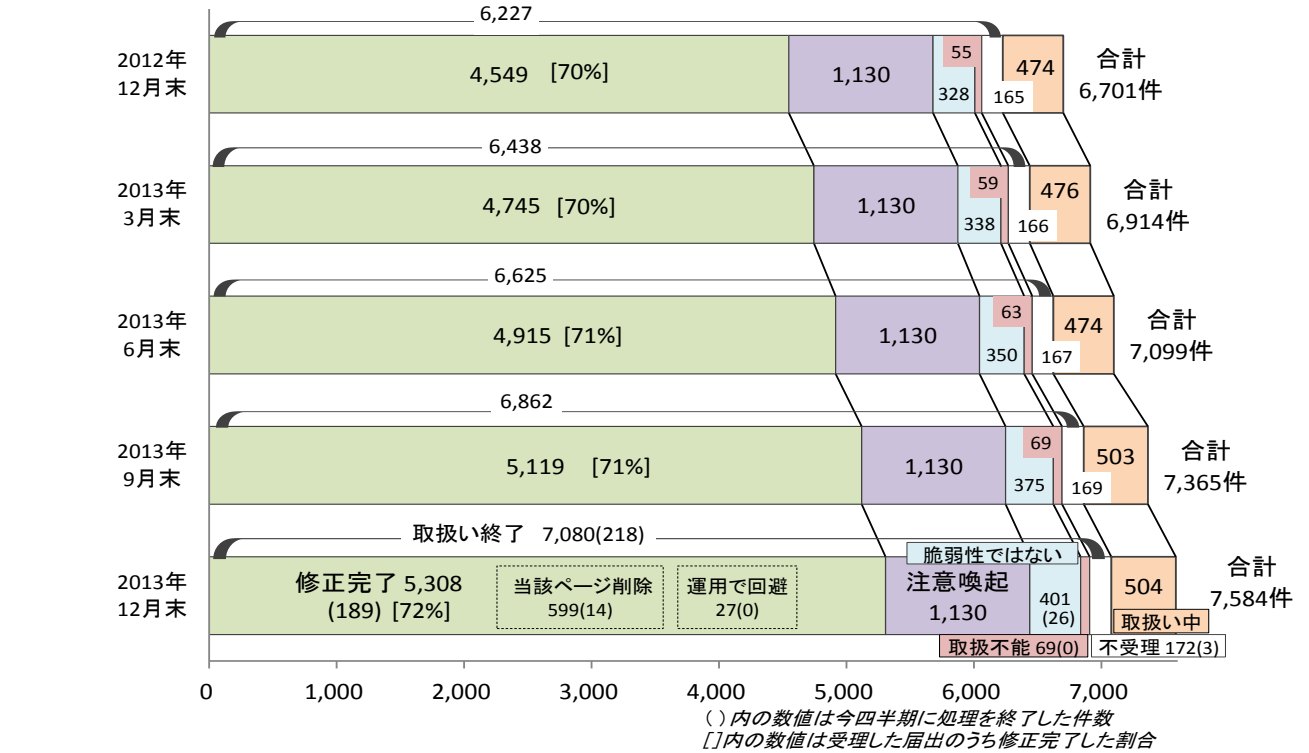

図2-15. 公開調査の結果

## 2-2. ウェブサイトの脆弱性

### 2-2-1. 処理状況

図 2-16 はウェブサイトの脆弱性関連情報の届出における、処理状況の推移を示したものです。ウェブサイトの脆弱性について、今四半期中に取扱いを終了したもの 218 件（累計 7,080 件）でした。このうち「修正完了」したものは 189 件（累計 5,308 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 26 件（累計 401 件）でした。処理の取りやめとは、例えば 1 つの脆弱性が多数のウェブサイトに存在するという届出があった場合「注意喚起」を行った上で、処理を取りやめるという本制度の運用に則ったものです。なお、メールでウェブサイト運営者と連絡が取れない場合は電話や郵送で連絡を試みるなどの対応をしていますが、それでもウェブサイト運営者と連絡が取れずに「取扱不能」となったものは 0 件（累計 69 件）でした。「不受理」としたものは 3 件 (*17)（累計 172 件）でした。取扱いを終了した累計 7,080 件のうち「注意喚起」「取扱不能」「不受理」を除く累計 5,709 件（81%）は、ウェブサイト運営者からの報告もしくは IPA の判断により指摘した点が解消されていることが確認されています。

「修正完了」したもののうち、ウェブサイト運営者が当該ページを削除することにより対応したものは 14 件（累計 599 件）、ウェブサイト運営者が運用により被害を回避しているものは 0 件（累計 27 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
  - 該当ページを削除 : 修正完了のうち、当該ページを削除して対応したもの
  - 運用で回避 : 修正完了のうち、運用により被害を回避しているもの
- 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 2-16. ウェブサイト 各四半期時点での脆弱性関連情報の届出の処理状況**

(*17) 今四半期の届出の中で不受理とした 8 件、前四半期までの届出の中で今四半期に不受理とした 2 件です。

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関連情報 7,584 件のうち、不受理を除いた 7,412 件の届出を分析した結果を記載します。

### 2-2-2. 運営主体者別件数

図 2-17 のグラフは過去 2 年間の運営主体者別届出件数を四半期で推移を示しています。今四半期は「教育・学術機関」が急増しています。

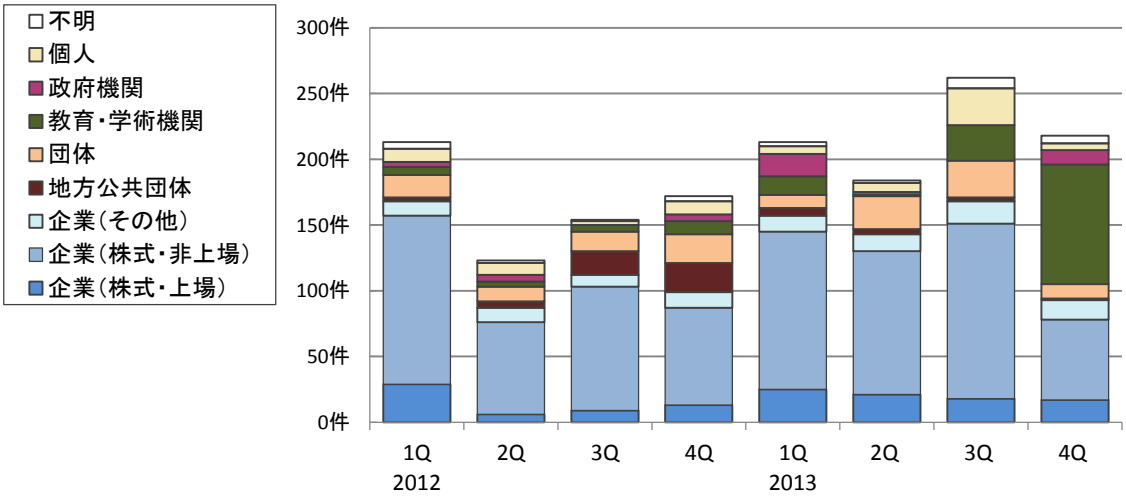
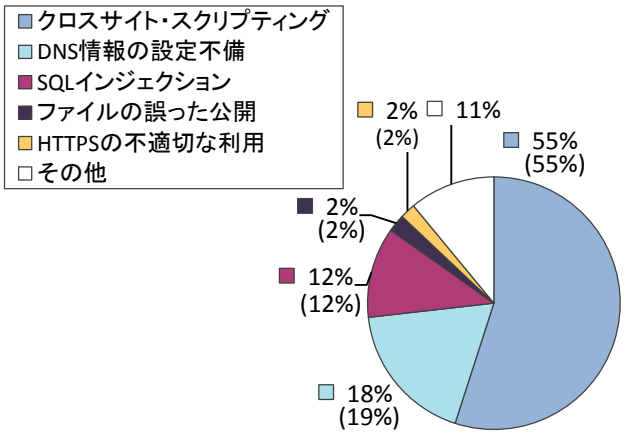



**図2-17. ウェブサイトの運営主体の種類別の届出件数(四半期別推移)**

### 2-2-3. 脆弱性の種類・脅威別届出

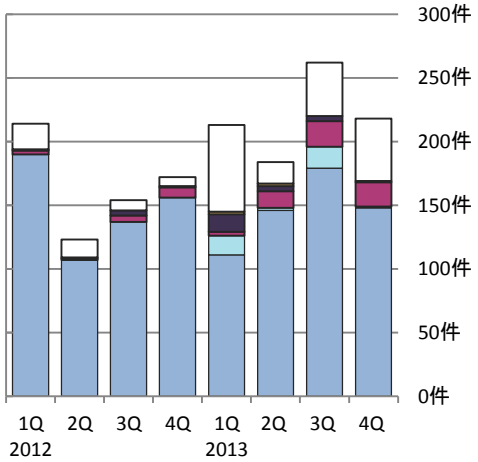
図 2-18 のグラフは届出受付開始から 2013 年第 4 四半期までの脆弱性の種類別の割合を、図 2-19 のグラフは過去 2 年間の脆弱性の種類別を四半期で推移をそれぞれ示したものです[*18]。図 2-18 の脆弱性の種類別では届出の多い「クロスサイト・スクリプティング」「DNS 情報の設定不備」「SQL インジェクション」の 3 種類で全体の 85%を占めています。また、2008 年第 3 四半期から 2009 年第 3 四半期にかけて多く届出のあった「DNS 情報の設定不備」の届出は、2009 年第 4 四半期以降はありませんでしたが、図 2-19 で示すとおり 2013 年の第 1 四半期および第 3 四半期に届出がありました。今四半期も「クロスサイト・スクリプティング」の届出が最も多く約 7 割を占めています。しかし、この統計はあくまでも届出された情報の傾向であり、必ずしも世の中に存在する脆弱性の傾向と一致するとは限りません。

**ウェブサイトの脆弱性の種類別の届出状況**




(7,412件の内訳、グラフの括弧内は前四半期までの数字)

**図2-18. 脆弱性の種類別の届出件数の割合**

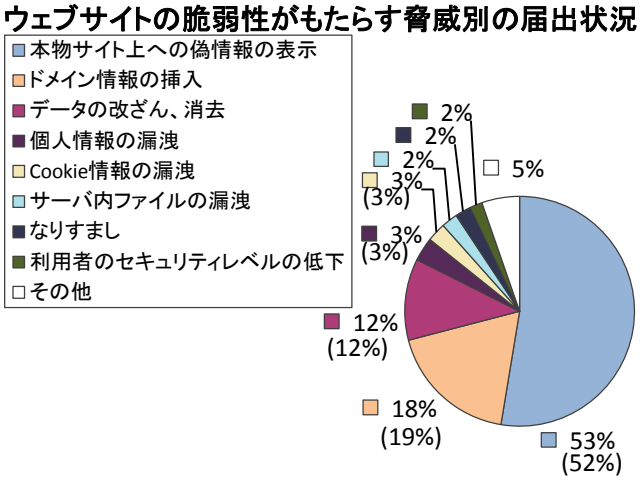



(過去2年間の届出内訳)

**図2-19. 脆弱性の種類別の届出件数 (四半期別推移)**

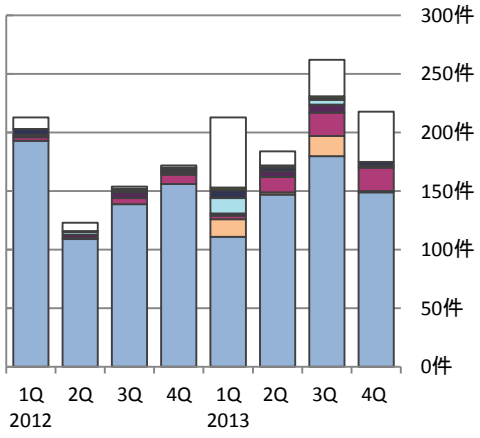
[*18] それぞれの脆弱性の詳しい説明については付表 2 を参照してください。

図 2-20 のグラフは 2013 年第 4 四半期までの脅威別の割合を、図 2-21 のグラフは過去 2 年間の脅威別届出件数を四半期で推移をそれぞれ示したものです。「クロスサイト・スクリプティング」「DNS 情報の設定不備」「SQL インジェクション」などにより発生する、「本物サイト上での偽情報の表示」「ドメイン情報の挿入」「データの改ざん、消去」が全体の 83%を占めています。




(7,412件の内訳、グラフの括弧内は前四半期までの数字)

**図2-20. 脆弱性がもたらす脅威別の届出件数の割合**




(過去2年間の届出内訳)

**図2-21. 脆弱性がもたらす脅威別の届出件数 (四半期別推移)**

## 2-2-4. 修正完了状況

図 2-22 のグラフは、過去 3 年間のウェブサイトの脆弱性の修正完了件数について四半期ごとに示しています。2013 年第 4 四半期の修正を完了した 189 件のうち 32 件（17%）は、運営者へ脆弱関連情報を通知してから修正完了までに 91 日以上を要した届出です。今四半期は、修正完了までに 91 日以上を要した届出の割合が、前四半期（204 件中 48 件（24%））より減少しています。表 2-6 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関連情報を通知してから、90 日以内に修正が完了した件数の割合を四半期ごとに示したものです。

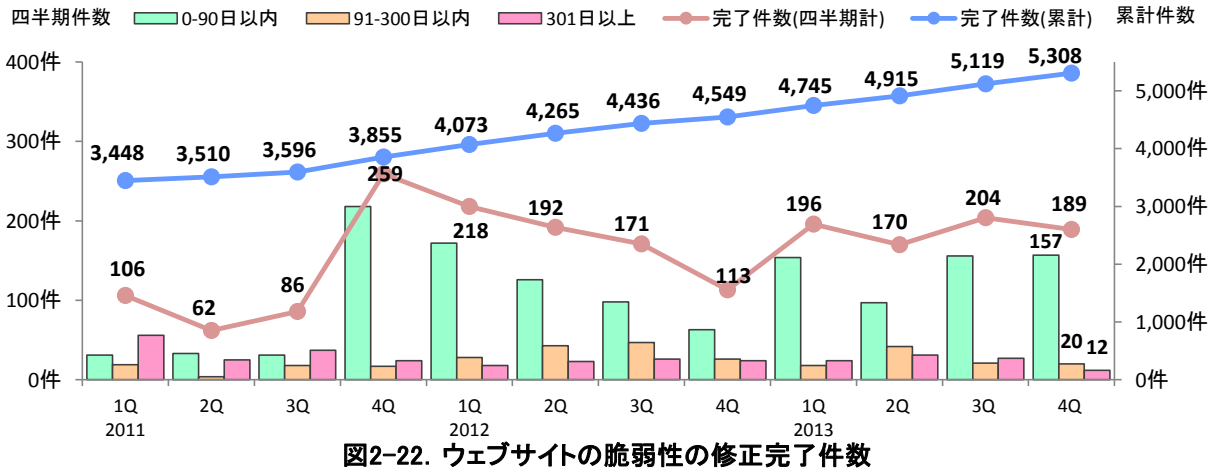



**図2-22. ウェブサイトの脆弱性の修正完了件数**

**表 2-6. 90 日以内に修正完了した件数および割合の推移**

| | 2011 1Q | 2Q | 3Q | 4Q | 2012 1Q | 2Q | 3Q | 4Q | 2013 1Q | 2Q | 3Q | 4Q |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 修正完了件数 | 3,448 | 3,510 | 3,596 | 3,855 | 4,073 | 4,265 | 4,436 | 4,549 | 4,745 | 4,915 | 5,119 | 5,308 |
| 90 日以内の件数 | 2,252 | 2,285 | 2,316 | 2,534 | 2,706 | 2,832 | 2,930 | 2,993 | 3,147 | 3,244 | 3,400 | 3,557 |
| 90 日以内の割合 | 65% | 65% | 64% | 66% | 66% | 66% | 66% | 66% | 66% | 66% | 66% | 67% |

図 2-23 および図 2-24 は、ウェブサイト運営者に脆弱性関連情報を通知してから修正されるまでに要した日数を脆弱性の種類別に分類し、その傾向を示したものです[*19]。全体の 47%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。

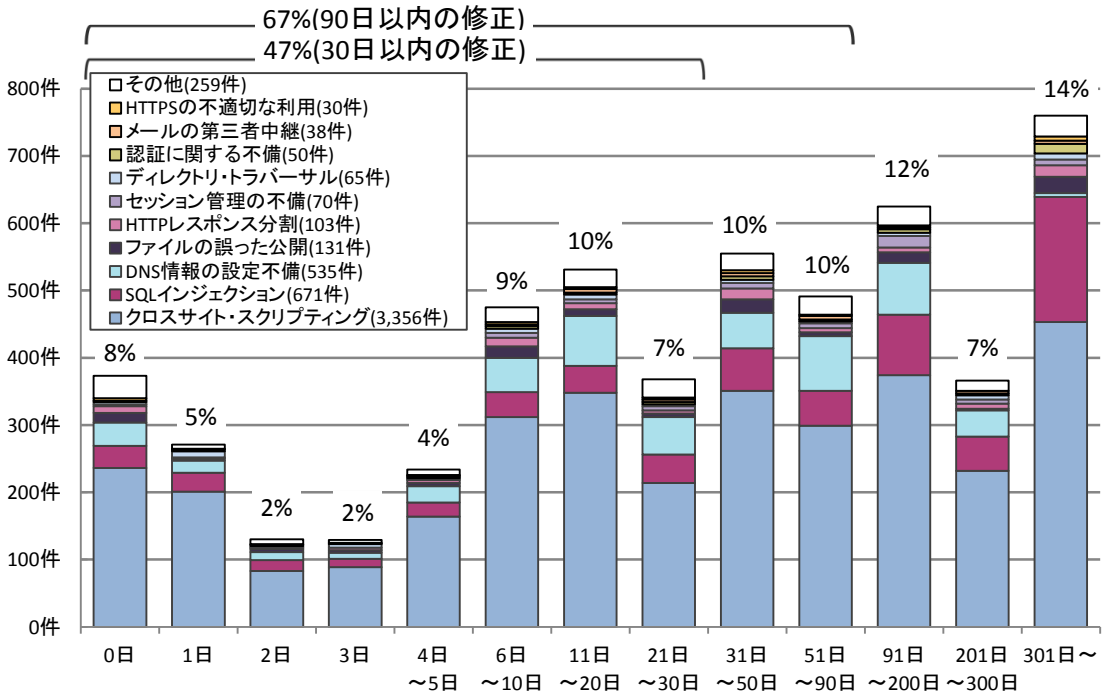



**図2-23.ウェブサイトの修正に要した日数**

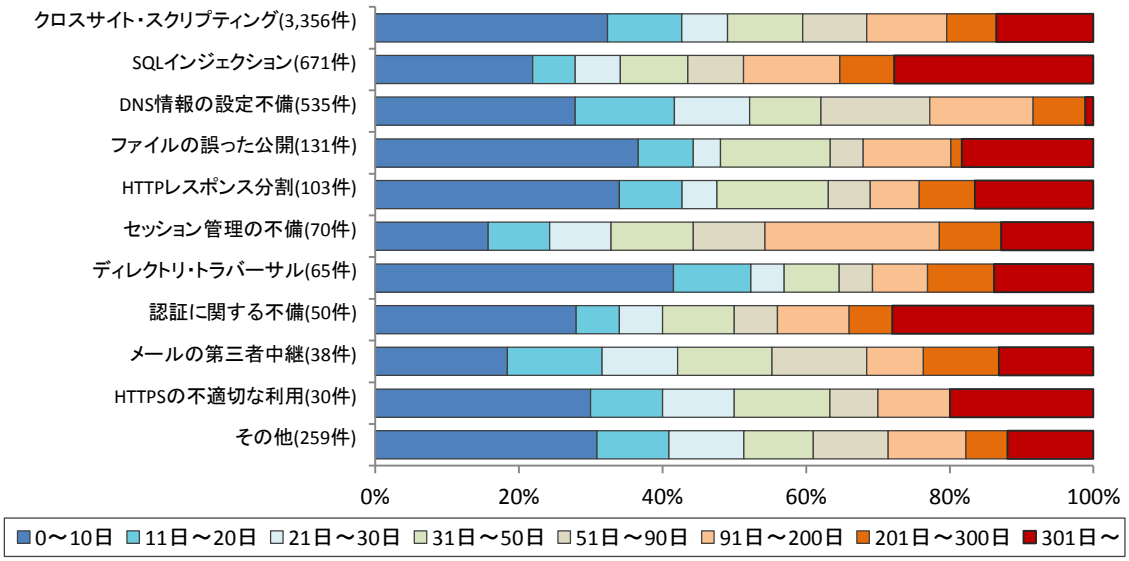



**図2-24.ウェブサイトの修正に要した脆弱性種類別の日数の傾向**

[*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通知が無い場合、IPA は運営者に脆弱性が悪用されて攻撃された場合の危険性を分かりやすく解説し、1～2 ヶ月毎に電子メールや電話、郵送などの手段で運営者に連絡を試み、脆弱性対策の実施を促しています。

図 2-25 は、ウェブサイトの脆弱性関連情報のうち、取扱いが長期化（IPA からウェブサイト運営者へ脆弱性関連情報を通知してから、90 日以上脆弱性を修正した旨の報告が無い）しているものについて、経過日数別の件数を示したものです。経過日数が 90 日から 199 日に達したものは 96 件、200 日から 299 日のものは 28 件など、これらの合計は 358 件（前四半期は 302 件）です。また、1000 日以上経過している届出脆弱性には、SQL インジェクションなどの比較的危険度の高い脆弱性が含まれており、速やかな対策が望まれます。

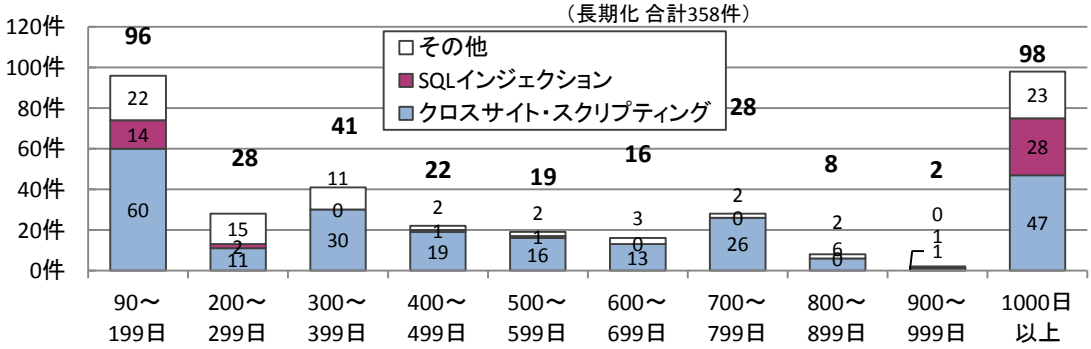



**図2-25.取扱いが長期化(90日以上経過)しているウェブサイトの経過日数と脆弱性の種類**

表 2-7 は、過去 2 年間の四半期末時点で取扱い中の届出について、取扱いが長期化している届出件数および、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別推移**

| | 2012 1Q | 2Q | 3Q | 4Q | 2013 1Q | 2Q | 3Q | 4Q |
|---|---|---|---|---|---|---|---|---|
| 取扱い中件数 | 527 件 | 449 件 | 423 件 | 473 件 | 474 件 | 473 件 | 503 件 | 504 件 |
| 長期化している件数 | 298 件 | 318 件 | 302 件 | 296 件 | 301 件 | 307 件 | 302 件 | 358 件 |
| 長期化している割合 | 57% | 71% | 71% | 63% | 64% | 65% | 60% | 71% |

ウェブサイトの情報が盗まれてしまう可能性のある SQL インジェクションのように、取扱いが長期化しているものの中には深刻度の高い脆弱性もあります。ウェブサイト運営者は脆弱性を攻撃された場合の影響を認識し、迅速な対策を講じる必要があります。

## 3. 関係者への要望

脆弱性の修正促進のための、各関係者への要望は以下のとおりです。

### 3-1. ウェブサイト運営者

多くのウェブサイトで利用しているソフトウェアに脆弱性が発見されています。自身のウェブサイトでどのようなソフトウェアを利用しているかを把握し、脆弱性対策を実施することが必要です。

なお、脆弱性の理解にあたっては、以下の IPA が提供するコンテンツが利用できます。

⇒「知っていますか？脆弱性（ぜいじゃくせい）」： http://www.ipa.go.jp/security/vuln/vuln_contents/

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

また、対策実施にあたっては、以下のコンテンツが利用できます。

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

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

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

また、ウェブサイトの脆弱性診断実施にあたっては、以下のコンテンツが利用できます。

⇒「ウェブ健康診断仕様」: http://www.ipa.go.jp/security/vuln/websecurity.html

### 3-2. 製品開発者

JPCERT/CC は、ソフトウェア製品の脆弱性関連情報を、「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。

⇒「TCP/IP に係る既知の脆弱性検証ツール」:
http://www.ipa.go.jp/security/vuln/vuln_TCPIP_Check.html

⇒「TCP/IP に係る既知の脆弱性に関する調査報告書」:
http://www.ipa.go.jp/security/vuln/vuln_TCPIP.html

⇒「組込みシステムのセキュリティへの取組みガイド（2010 年度改訂版）」:
http://www.ipa.go.jp/security/fy22/reports/emb_app2010/

⇒「ファジング活用の手引き」、「ファジング実践資料」:
http://www.ipa.go.jp/security/vuln/fuzzing.html

### 3-3. 一般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の期間は第三者に漏れぬよう、適切に管理されることを求めます。

**付表 1. ソフトウェア製品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 |

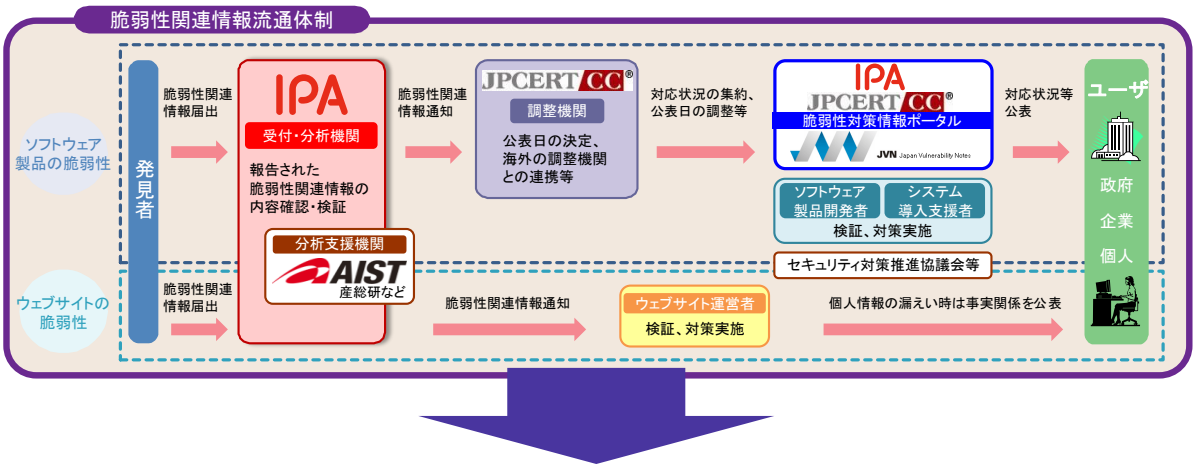
**付表 2. ウェブサイトの脆弱性の分類**

| | 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