Japan Computer Emergency Response Team Coordination Center

電子署名者 : Japan Computer Emergency Response Team Coordination Center
DN : c=JP, st=Tokyo, l=Chiyoda-ku, email=office@jpcert.or.jp, o=Japan Computer Emergency Response Team Coordination Center, cn=Japan Computer Emergency Response Team Coordination Center
日付 : 2014.10.23 09:45:50 +09'00'

# ソフトウェア等の脆弱性関連情報の取扱いに関する活動報告レポート

## [2014 年第 3 四半期（7 月～9 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

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

本レポートでは、2014 年 7 月 1 日から 2014 年 9 月 30 日までの間に実施した、脆弱性関連情報の取扱いに関する活動及び脆弱性の傾向について紹介しています。

独立行政法人情報処理推進機構 技術本部 セキュリティセンター
一般社団法人 JPCERT コーディネーションセンター
2014 年 10 月 23 日

目次

## 1. 2014 年第 3 四半期　ソフトウェア等の脆弱性関連情報に関する届出受付状況

### 1-1. 脆弱性関連情報の届出受付状況

**～ 脆弱性の届出件数の累計が 10,084 件になりました ～**

表 1-1 は本制度[*1]における届出状況について、2014 年第 3 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 39 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 200 件、合計 239 件でした。届出受付開始からの累計は 10,084 件で、内訳はソフトウェア製品に関するもの 1,866 件、ウェブサイトに関するもの 8,218 件でウェブサイトに関する届出が全体の 84%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 | **39** 件 | **1,866** 件 |
| ウェブサイト | **200** 件 | **8,218** 件 |
| 合計 | **239** 件 | **10,084** 件 |

図 1-1 のグラフは過去 3 年間の届出件数の四半期別推移を示したものです。ソフトウェア製品に関する届出は 2013 年第 3、第 4 四半期を除き、40 件前後で推移しています。今四半期のウェブサイトに関する届出は前四半期の約 7 割でした。表 1-2 は過去 3 年間の四半期別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 4.04 [*2] 件でした。

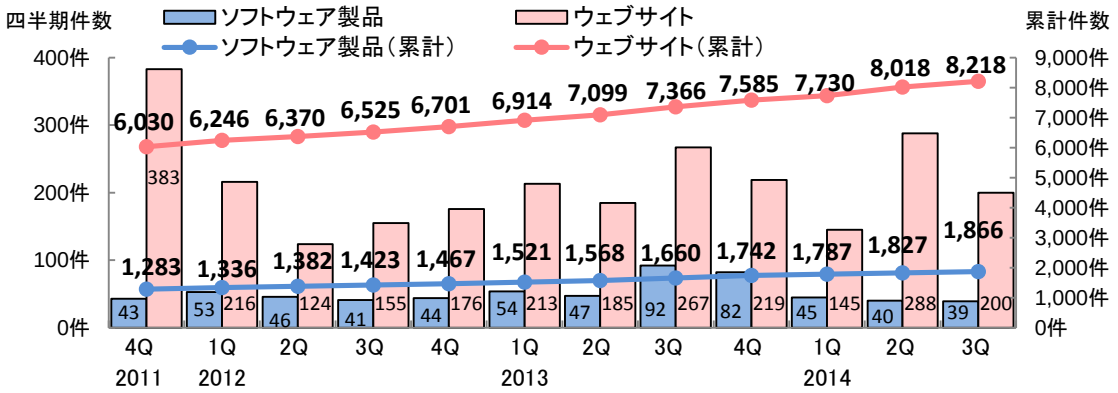



**図1−1. 脆弱性の届出件数の四半期別推移**

**表 1-2. 届出件数（過去 3 年間）**

| | 2011 4Q | 2012 1Q | 2Q | 3Q | 4Q | 2013 1Q | 2Q | 3Q | 4Q | 2014 1Q | 2Q | 3Q |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 累計届出件数[件] | 7,313 | 7,582 | 7,752 | 7,948 | 8,168 | 8,435 | 8,667 | 9,026 | 9,327 | 9,517 | 9,845 | 10,084 |
| 1 就業日あたり[件/日] | 4.03 | 4.05 | 4.00 | 3.98 | 3.78 | 3.96 | 3.96 | 4.00 | 4.03 | 4.01 | 4.04 | 4.04 |

---

[*1] 情報セキュリティ早期警戒パートナーシップガイドライン
http://www.ipa.go.jp/security/ciadr/partnership_guide.html
https://www.jpcert.or.jp/vh/index.html

[*2] 1 就業日あたりの届出件数は、「累計届出件数」/「届出受付開始からの就業日数」にて算出

## 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 6,703 件になりました～**

表 1-3 は今四半期と届出受付開始から今四半期までのソフトウェア製品とウェブサイトの修正完了件数を示しています。

**表 1-3. 修正完了件数**

| 分類 | 今期件数 | 累計 |
|---|---|---|
| ソフトウェア製品 | **45** 件 | **925** 件 |
| ウェブサイト | **183** 件 | **5,778** 件 |
| 合計 | **228** 件 | **6,703** 件 |

ソフトウェア製品の脆弱性の届出のうち、今四半期に脆弱性対策情報を JVN で公表したうち、修正が完了した件数は、過去最多の 45 件 (*3)（累計 925 件）でした。そのうち、8 件が製品開発者による自社製品の脆弱性の届出でした。また、届出を受理してから JVN 公表までの日数が 45 日 (*4) 以内だったのは 6 件（13%）でした。

ウェブサイトの脆弱性の届出のうち、IPA がウェブサイト運営者に通知を行い、今四半期に修正を完了したものは 183 件（累計 5,778 件）でした。修正を完了した 183 件のうち、ウェブアプリケーションを修正したものは 170 件（93%）、当該ページを削除したものは 13 件（7%）、運用で回避したものは 0 件でした。なお、修正を完了した 183 件のうち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 142 件（78%）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（149 件中 95 件（64%））より増加しています。

## 1-3. 連絡不能案件の取扱い状況

本制度では、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。その「連絡不能開発者」への連絡の糸口を得るために、「連絡不能開発者一覧 (*6)」を公表しています。「連絡不能開発者一覧」では、まず「製品開発者名」を公表します。その後 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、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、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ます。それでも情報が得られない場合、後述の情報公開に向けて情報提供の期限を追記します。

その結果、期限までに製品開発者と連絡がとれない場合は、利用者への被害低減のため脆弱性情報と対策検討の機会を提供することを目的に公表判定委員会 (*7) において当該脆弱性情報の公表について審議します。公表が妥当と判定されると当該脆弱性情報を JVN に公表します。

今四半期に「連絡不能開発者」と位置づけて新たに製品開発者名を公表したものは 8 件、製品開発者名に加え製品情報を追加公表したものは 12 件、2014 年 9 月末時点の「連絡不能開発者一覧」への累計公表件数は 151 件となりました。このうち、5 件について情報提供の期限を追記しました。

---

(*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。

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

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

## 1-4. 脆弱性の傾向について

### 1-4-1. SSL サーバ証明書の検証不備の脆弱性の調整及び公表

**～SSL サーバ証明書の検証不備の脆弱性が初めて JVN 公表されたのは 2008 年～**

2014 年第 3 四半期は、SSL サーバ証明書の検証 (*8) 不備の脆弱性について、JVN で脆弱性対策情報を 5 件公表しました。

また、今四半期は、CERT/CC から SSL サーバ証明書を適切に検証していない複数の Android アプリについての報告 (*9) もあり、世界中から注目を集めました。しかし、この問題は、Android アプリ特有のものではありません。実際、届出受付開始から今四半期までに JVN で公表された Android OS 以外のクライアントアプリケーションに存在した同種の脆弱性は 6 件で、Android OS を含めると 18 件が公表されています（表 1-4）。

また JVN で最初に公表されたのは 2008 年であったことから、この脆弱性は決して新しいものではないといえます。

**表 1-4. JVN 公表一覧**

| 公表日 | JVN番号 | 深刻度 | 対象製品名 |
|---|---|---|---|
| 2014年9月25日 | JVN#48270605 | 警告 | 「Yahoo!ボックス」(Android) |
| 2014年9月22日 | JVN#04560253 | 警告 | 「ゆこゆこ」(Android) |
| 2014年8月29日 | JVN#17637243 | 警告 | 「Kindle」(Android) |
| 2014年8月14日 | JVN#27702217 | 警告 | 「Ameba」(Android) |
| 2014年7月30日 | JVN#72950786 | 警告 | 「Outlook.com」(Android) |
| 2014年6月18日 | JVN#10603428 | 警告 | 「JR東日本アプリ」(Android) |
| 2014年3月17日 | JVN#16263849 | 警告 | 「出前館」(Android) |
| 2014年2月26日 | JVN#48810179 | 警告 | 「デニーズ」(Android) |
| 2013年11月22日 | JVN#97810280 | 警告 | 「KDrive個人版 PCクライアントソフト」 |
| 2013年8月19日 | JVN#75084836 | 注意 | 「Yahoo!ショッピング」(Android) |
| 2013年8月19日 | JVN#68156832 | 注意 | 「ヤフオク!」(Android・iOS) |
| 2013年6月7日 | JVN#39218538 | 注意 | 「ピザハット公式アプリ　宅配ピザのPizzaHut」(Android) |
| 2013年5月31日 | JVN#85812843 | 警告 | 「FileMaker Pro」 |
| 2012年5月25日 | JVN#39707339 | 警告 | 「Opera」 |
| 2012年4月26日 | JVN#82029095 | 警告 | 「spモードメールアプリ」(Android) |
| 2011年7月29日 | JVN#43105011 | 警告 | 「Android標準ブラウザ」(Android) |
| 2008年7月14日 | JVN#88676089 | 注意 | 「Safari」(iOS) |
| 2008年4月23日 | JVN#76788395 | 警告 | ソニー製「mylo COM-2」 |

製品開発者においては、HTTPS 通信を行う全てのクライアントアプリケーションに対して、「SSL サーバ証明書の検証不備の脆弱性」の有無について調査を行い、脆弱性があれば速やかに修正の上、脆弱性対策情報を公表する必要があります。

(*8) 個人情報など重要な情報を暗号化して送信する際に使用する通信において、通信先が信頼できるか確認し、通信の内容を傍受されないようにする仕組み。

(*9) http://www.kb.cert.org/vuls/id/582497

### 1-4-2. 情報家電をはじめとした組込み機器共通の脆弱性

**～組込まれた OS やソフトウェアに注意～**

2014 年度第 3 四半期のソフトウェア製品の届出のうち、インターネットに接続する、家庭用ルータ・IP カメラおよび、プリンタといった情報家電の届出が 10 件ありました。

情報家電には、低い開発コストでさまざまな機能を実現するため Linux などの汎用 OS やソフトウェアが組込まれています。そのため情報家電にも OS やソフトウェアに脆弱性が作りこまれてしまう可能性があります。例えば昨今の家庭用ルータには、PC やスマートフォンのウェブブラウザ上から詳細な設定をするためのウェブアプリケーションというソフトウェアが組込まれています。そのため、組込まれているウェブアプリケーションに脆弱性があると、その影響を受ける可能性があります。実際、前述の 10 件の届出のほとんどは、情報家電に組込まれているウェブアプリケーションに脆弱性がありました。なお、表 1-5 は、届出のあった情報家電の脆弱性の種類とその脅威例をまとめたものです。開発者は設計段階で、機器に組込む OS やソフトウェアに脆弱性が存在していないことの確認、開発段階では、機器に組込まれた OS やソフトウェアに脆弱性が存在しないかのテスト等を行い、脆弱性を作りこまないように注意する必要があります。

**表 1-5. 情報家電の脆弱性一覧**

| 届出された脆弱性の種類 | 脅威の例 | 製品の種類 |
|---|---|---|
| クロスサイト・スクリプティング | 偽のウェブページを表示される | 家庭用ルータ |
| クロスサイト・リクエスト・フォージェリ | 機器の設定情報を変更される | 家庭用ルータ |
| サービス運用妨害(DoS) | 機器が停止状態にされる | 家庭用ルータ、プリンタ |
| アクセス認証回避 | 機器を乗っ取られる | IP カメラ |
| 通信に関する不備 | 意図しないウェブサイトに接続される | 家庭用ルータ |

9 月 25 日（米国時間）に、CERT/CC より Linux など UNIX 系の OS に存在する bash というソフトウェアに関する脆弱性が報告されました[(*10)]。情報家電に組込まれている汎用 OS は Linux 系が一般的であることから、情報家電への影響の可能性が示唆されました。具体的な脅威には、情報漏えいや動作停止、ウイルス等悪意のあるプログラムのダウンロード、などが挙げられます。このように、OS やソフトウェアの脆弱性は、それを組込んだ機器にも影響がおよびます。今後インターネット接続が一般的となる情報家電は PC と同様に、前述の脅威がより現実のものとなることを考慮して、製品開発者は、開発、保守を行う必要があります。

また、情報家電に脆弱性が見つかった場合は、PC 等における他のソフトウェア製品と同様に、多くの場合利用者自身が製品開発者の提供するファームウェアやパッチを適用しなければなりません。情報家電の利用者は、製品開発者が提供するサポートサイトで脆弱性対策情報を確認するほか、JVN などでも情報を収集し、迅速かつ適切な対応が求められます。

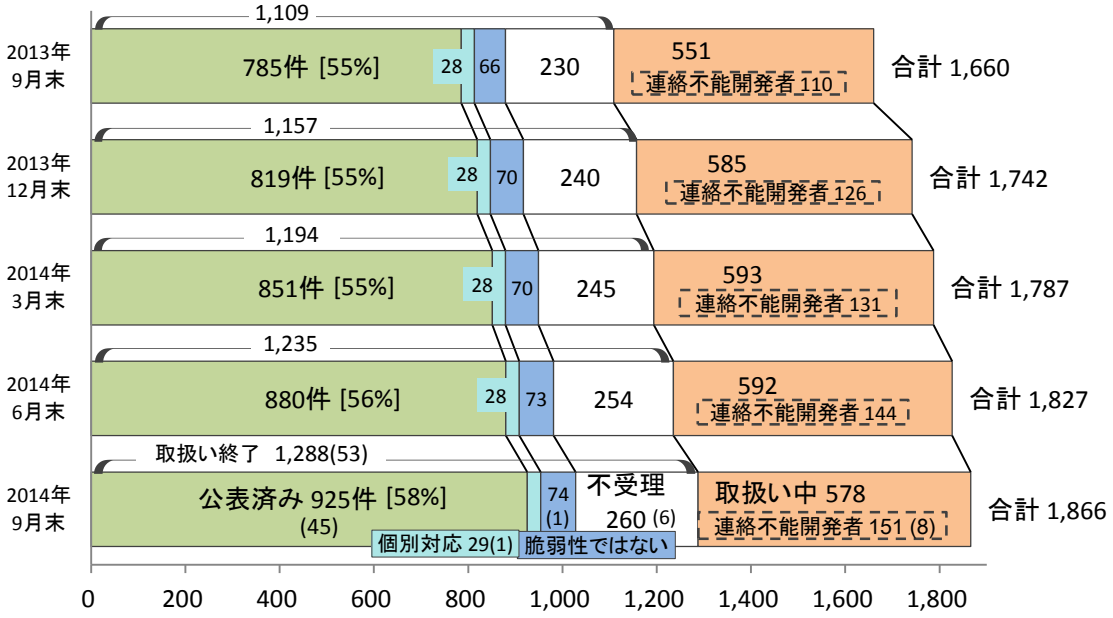
(*10) https://www.us-cert.gov/ncas/alerts/TA14-268A

## 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、四半期別の推移を示しています。2014 年 9 月末時点の届出の累計は 1,866 件で、今四半期に脆弱性対策情報を JVN 公表したものは 45 件（累計 925 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 1 件（累計 29 件）、製品開発者が「脆弱性ではない」と判断したものは 1 件（累計 74 件）、「不受理」としたものは 6 件 [*11]（累計 260 件）、取扱い中は 578 件でした。578 件のうち、連絡不能開発者 [*12] 一覧に公表したのは 8 件で、2014 年 9 月末時点の累計は 151 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

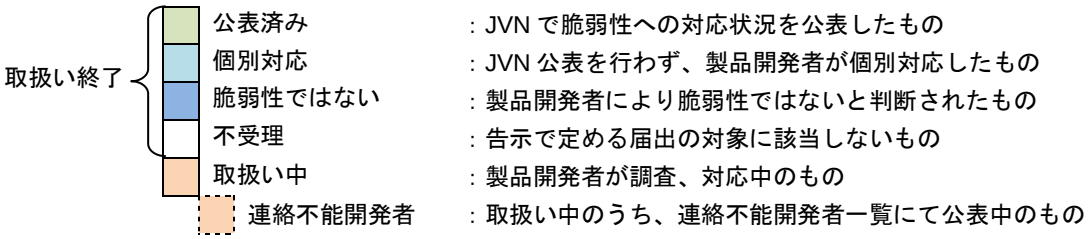



**図 2-1. ソフトウェア製品脆弱性の届出処理状況（四半期別推移）**

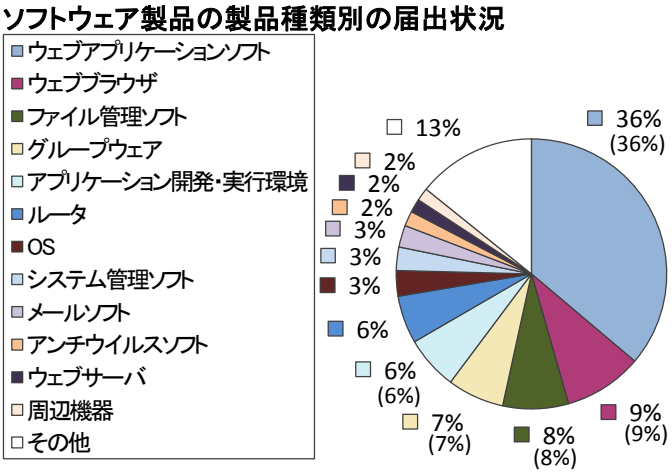
[*11] 内訳は今四半期の届出によるもの 4 件、前四半期までの届出によるもの 2 件。
[*12] 連絡不能開発者一覧への公表および一覧からの削除が複数回行われた製品開発者の公表回数は、その累計を計上しています。

以下に、届出受付開始から今四半期までに届出のあったソフトウェア製品の脆弱性 1,866 件のうち、不受理を除いた 1,606 件の届出を分析した結果を記載します。

### 2-1-2. ソフトウェア製品別届出件数

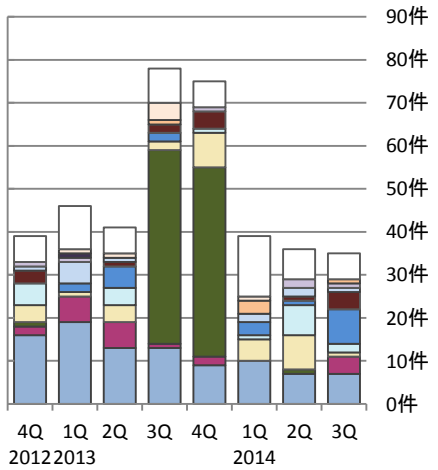
図 2-2、図 2-3 のグラフは、届出された製品の種類別の分類を示しています。図 2-2 は届出受付開始から今四半期末までの製品種類別割合を、図 2-3 は過去 2 年間の届出件数の推移を四半期別に示したものです。

累計では、「ウェブアプリケーションソフト」が最も多く 36%となっています。今四半期の届出件数は、「ルータ」が最も多く、次いで「ウェブアプリケーションソフト」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。
（1,606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**

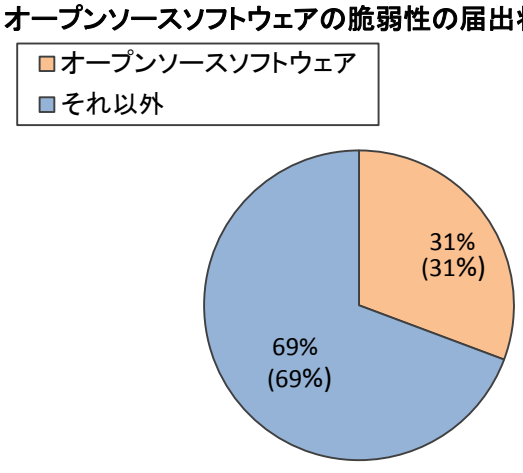



（過去2年間の届出内訳）

**図2-3. 四半期毎の製品種類別届出件数**

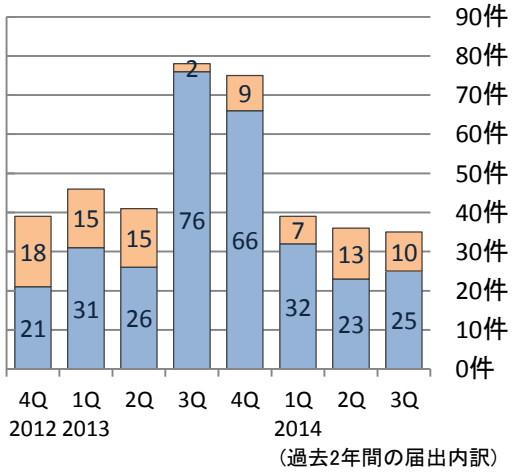
図 2-4、2-5 のグラフは、届出された製品のライセンスを「オープンソースソフトウェア」（OSS）と「それ以外」で分類しています。図 2-4 は届出受付開始から今四半期末までの届出累計の分類割合を、図 2-5 は過去 2 年間の届出件数の推移を四半期別に示したものです。

累計では、オープンソースソフトウェアが 31%を占めました。件数では今四半期のオープンソースソフトウェアの数が、前四半期と比較して少なくなりました。




（1,606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. 四半期毎のオープンソースソフトウェア届出件数**

図 2-6、図 2-7 のグラフは、ソフトウェア製品の届出をスマートフォン向けアプリ（以降「スマホアプリ」）と「それ以外」で分類しています。図 2-6 は過去 2 年間の四半期別の届出件数の推移を、図 2-7 は届出受付開始から今四半期末までの届出について、JVN 公表までに要した日数の割合を示しています。「スマホアプリ」に関する届出は、2013 年第 3、第 4 四半期に急増しましたが、それ以降は 5 件前後となっています。

受理から 45 日以内に対策情報を JVN 公表した割合は「スマホアプリ」が 28%（前四半期は 31%）、「それ以外」が 34%（前四半期は 34%）でした。

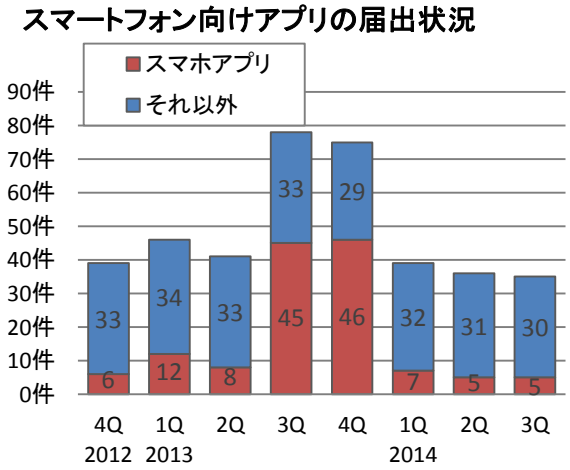



**図2-6. 四半期毎のスマートフォン向けアプリ届出件数**

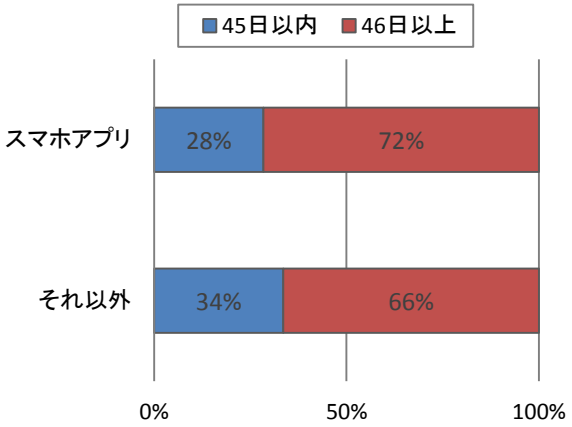
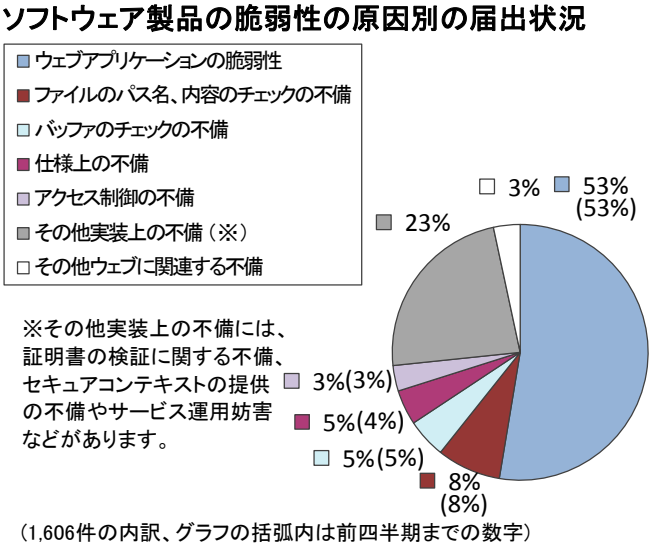



**図2-7. .スマートフォン向けアプリとそれ以外のJVN公表までの日数の割合**

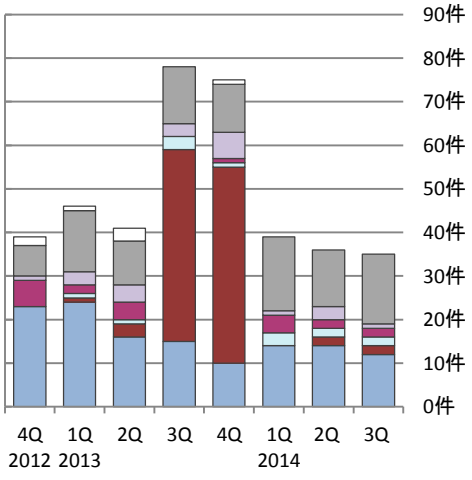
### 2-1-3. 脆弱性の原因と脅威別件数

図 2-8、図 2-9 のグラフは、届出された脆弱性の原因を示しています。図 2-8 は届出受付開始から今四半期末までの届出累計の脆弱性の原因別割合を、図 2-9 は過去 2 年間の原因別の届出件数の推移を四半期毎に示しています。累計では、「ウェブアプリケーションの脆弱性」が過半数を占めています。また、今四半期の届出件数は「その他実装上の不備」が最多でした。これは今四半期にスマホアプリや組込み機器、OS 等、様々な製品に対する届出があったためです。




（1,606件の内訳、グラフの括弧内は前四半期までの数字）

**図2-8. 届出累計の脆弱性の原因別割合**

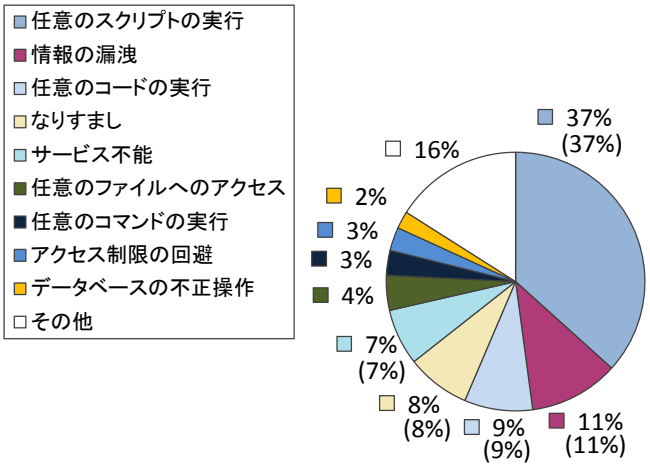



（過去2年間の届出内訳）

**図2-9. 四半期毎の脆弱性の原因別届出件数**

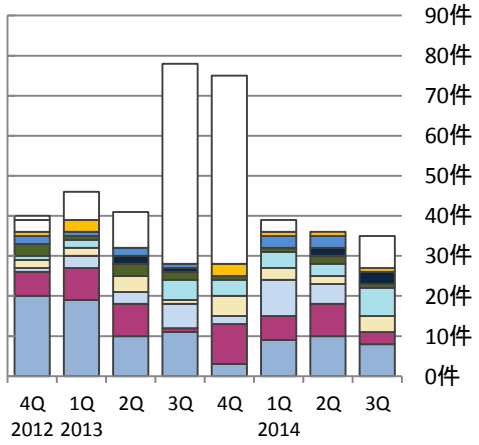
図 2-10、図 2-11 のグラフは、届出された脆弱性がもたらす脅威を示しています。図 2-10 は届出受付開始から今四半期末までの届出累計の脅威別割合を、図 2-11 は過去 2 年間の脅威別届出件数の推移を四半期毎に示しています。累計では「任意のスクリプトの実行」が最も多く、次いで「情報の漏洩」となっています。今四半期は、「任意のスクリプト実行」が最も多く、次いで「サービス不能」が多く届出されました。なお、2013 年第 3、第 4 四半期の「その他」が多いのは、「ファイルのパス名、内容のチェックの不備」によりもたらされる脅威が「その他」に分類されたためです。

**ソフトウェア製品の脆弱性がもたらす脅威別の届出状況**




(1,606件の内訳、グラフの括弧内は前四半期までの数字)

**図2-10. 届出累計の脆弱性がもたらす脅威別割合**




(過去2年間の届出内訳)

**図2-11. 四半期毎の脆弱性がもたらす脅威別届出件数**

### 2-1-4. 調整および公表件数

表 2-1 は脆弱性情報の提供元別に、今期と累計の件数を示しています。JPCERT/CC は、脆弱性情報の提供元別に日本国内の製品開発者や関係者、および海外 CSIRT の協力のもと海外の製品開発者と調整を行っています[*13]。これらの脆弱性に対する製品開発者の対応状況は、IPA と JPCERT/CC が共同運営している脆弱性対策情報ポータルサイト JVN（Japan Vulnerability Notes）（URL：http://jvn.jp/ ）に公表しています。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、連携先別に集計し、過去 3 年分を四半期別の推移で示したものです。

**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 | 45 件 | 925 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 | 38 件 | 1,138 件 |
| | 合計 | 83 件 | 2,062 件 |

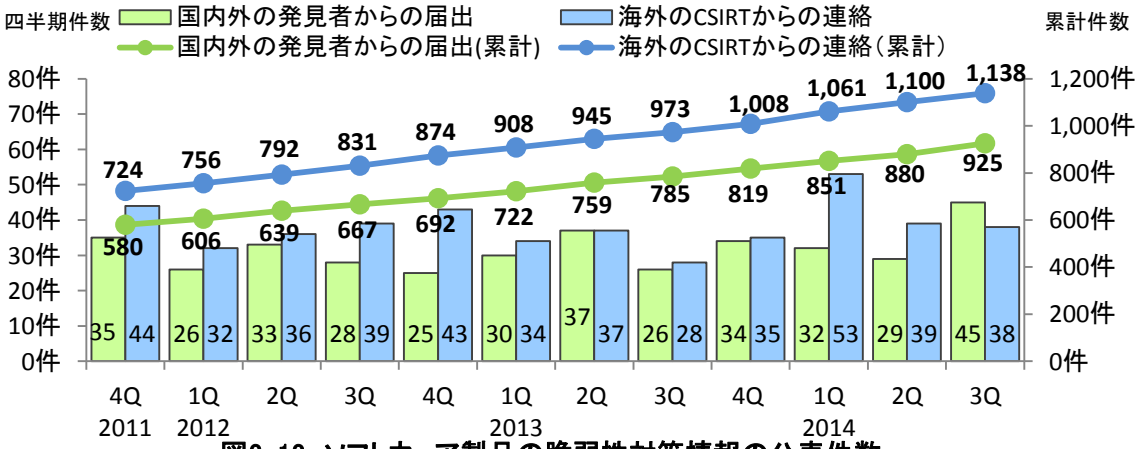



**図2-12. ソフトウェア製品の脆弱性対策情報の公表件数**

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

届出受付開始から今四半期までに対策情報を JVN 公表した脆弱性（925 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 JVN 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 日以内は 33%、45 日を超過した件数は 67%です。製品開発者は脆弱性が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。

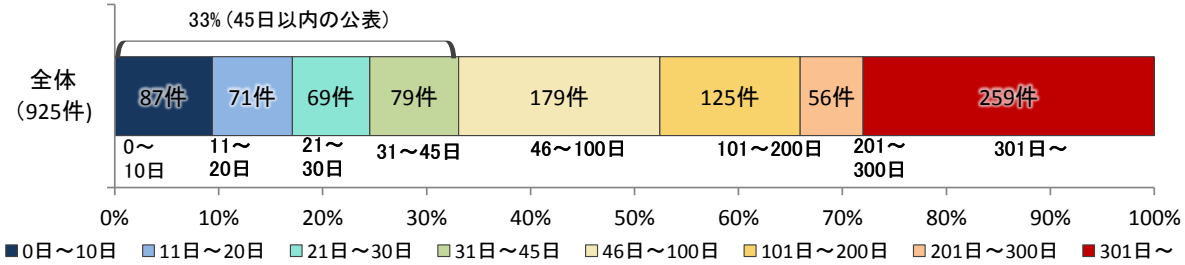



**図2-13. ソフトウェア製品の脆弱性公表日数**

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

| 2011 4Q | 2012 1Q | 2Q | 3Q | 4Q | 2013 1Q | 2Q | 3Q | 4Q | 2014 1Q | 2Q | 3Q |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 33% | 34% | 34% | 35% | 34% | 33% | 33% | 33% | 34% | 34% | 34% | 33% |

[*13] JPCERT/CC 活動概要 Page16～23（http://www.jpcert.or.jp/pr/2014/PR20141009.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 45 件のうち、今四半期に JVN 公表した脆弱性を深刻度別に示しています。オープンソースソフトウェアに関するものが 12 件（表 2-3 の*1）、組込みソフトウェア製品の脆弱性が 4 件（表 2-3 の*3）、制御システムの脆弱性に関するものが 1 件（表 2-3 の*4）ありました。また、製品開発者自身から届けられた自社製品の脆弱性は 9 件（表 2-3 の*2）でした。

**表 2-3. 2014 年第 2 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） | 「サイボウズ ガルーン」において任意のコマンドが実行される脆弱性 | グループウェア「サイボウズ ガルーン」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、サーバ上で任意のコマンドを実行される可能性がありました。 | 2014 年 7 月 15 日 | 10.0 |
| 2（*1） | 「S2Struts」において ClassLoader が操作可能な脆弱性 | ウェブアプリケーションフレームワーク「S2Struts」には、Apache Struts の脆弱性(CVE-2014-0114)に起因する ClassLoader が操作可能な脆弱性が存在していました。このため、第三者により情報を窃取されたり、任意のコードを実行されたりするなどの可能性がありました。 | 2014 年 7 月 15 日 | 7.5 |
| 3（*4） | 「TrendLink」の ActiveX コントロールにおける任意のプログラムが実行される脆弱性 | データ分析支援ツール「TrendLink」には、ファイルの書き込みを適切に制限していない脆弱性がありました。このため第三者によって、任意のファイルをシステム上に書き込まれ、その結果、任意のコードを実行される可能性がありました。 | 2014 年 7 月 25 日 | 8.5 |
| 4（*3） | 「Dominion KX2-101」におけるサービス運用妨害(DoS)の脆弱性 | ネットワーク機器「Dominion KX2-101」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、細工されたパケットを受信することで、サービス不能な状態にされる可能性がありました。 | 2014 年 8 月 12 日 | 7.8 |
| 5 | 「Advance-Flow」における SQL インジェクションの脆弱性 | 電子承認システム「Advance-Flow」には、SQL 文を組み立てる処理に問題がありました。このため、第三者により任意の SQL 命令を実行される可能性がありました。 | 2014 年 8 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 | | | | |
| 6（*3） | 「SX-2000WG」におけるサービス運用妨害(DoS)の脆弱性 | ネットワーク機器「SX-2000WG」には、TCP Option ヘッダの取扱いに問題がありました。このため、第三者により応答不能な状態にされる可能性がありました。項番 7 とは異なる問題です。 | 2014 年 7 月 2 日 | 5.0 |
| 7（*3） | 「SX-2000WG」におけるサービス運用妨害(DoS) の脆弱性 | ネットワーク機器「SX-2000WG」には、IP パケットの処理機能に問題がありました。このため、第三者により応答不能な状態にされる可能性がありました。項番 6 とは異なる問題です。 | 2014 年 7 月 2 日 | 5.0 |
| 8 | 「Becky! Internet Mail」におけるバッファオーバーフローの脆弱性 | メールクライアントソフト「Becky! Internet Mail」には、POP3 サーバからのレスポンスの処理に起因するバッファオーバーフローの脆弱性がありました。このため、第三者により任意のコードを実行される可能性がありました。 | 2014 年 7 月 8 日 | 5.1 |
| 9（*2） | 「サイボウズ ガルーン 3 連携 API」におけるアクセス制限回避の脆弱性 | サイボウズ ガルーン API「サイボウズ ガルーン 3 連携 API」にはアクセス制限を回避される脆弱性がありました。このため、第三者により利用権限のない機能にアクセスされる可能性がありました。 | 2014 年 7 月 15 日 | 5.5 |

| 項番 | 脆弱性 | セキュリティ上の問題点 | JVN 公表日 | CVSS 基本値 |
|---|---|---|---|---|
| 10 | 「多機能メールフォームフリー」におけるクロスサイト・スクリプティングの脆弱性 | メールフォームソフト「多機能メールフォームフリー」には、ウェブページを出力する際の処理に問題がありました。このため、第三者によりウェブページにスクリプトを埋め込まれる可能性がありました。 | 2014 年 7 月 16 日 | 4.3 |
| 11 | 「File Explorer」におけるディレクトリ・トラバーサルの脆弱性 | Android 用ファイル管理ソフト「File Explorer」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作成されたり既存のファイルを上書きされたりする可能性がありました。 | 2014 年 7 月 18 日 | 4.3 |
| 12 (*1) | 「FuelPHP」において任意のコードが実行される脆弱性 | ウェブアプリケーションフレームワーク「FuelPHP」には、Request_Curl クラスの処理に問題がありました。このため、第三者により任意のコードが実行される可能性がありました。 | 2014 年 7 月 18 日 | 5.1 |
| 13 | 「PerlMailer」におけるクロスサイト・スクリプティングの脆弱性 | メールフォームソフト「PerlMailer」には、ウェブページを出力する際の処理に問題がありました。このため、第三者によりウェブページにスクリプトを埋め込まれる可能性がありました。 | 2014 年 7 月 29 日 | 4.3 |
| 14 | 「acmailer」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 | メールフォームソフト「acmailer」の複数の cgi 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、第三者により登録されている情報の改ざんや削除、管理者権限が奪われる可能性がありました。 | 2014 年 7 月 29 日 | 5.1 |
| 15 (*2) (*3) | アイ・オー・データ機器製の複数の IP カメラにおける認証回避の脆弱性 | アイ・オー・データ機器製の複数の IP カメラには、認証回避の脆弱性がありました。このため、第三者により認証情報を含む設定内容を窃取される可能性がありました。 | 2014 年 7 月 29 日 | 6.4 |
| 16 | Android 版「Outlook.com」における SSL サーバ証明書の検証不備の脆弱性 | Android 用メールクライアントソフト「Outlook.com」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。 | 2014 年 7 月 30 日 | 4.0 |
| 17 (*2) | 「ServerView Operations Manager」におけるクロスサイト・スクリプティングの脆弱性 | サーバ監視ソフトウェア「ServerView Operations Manager」には、ウェブページを出力する際の処理に問題がありました。このため、第三者によりウェブページにスクリプトを埋め込まれる可能性がありました。 | 2014 年 8 月 1 日 | 4.3 |
| 18 (*1) | 「Piwigo」におけるクロスサイト・スクリプティングの脆弱性 | 画像管理ソフトウェア「Piwigo」には、ウェブページを出力する際の処理に問題がありました。このため、第三者によりウェブページにスクリプトを埋め込まれる可能性がありました。 | 2014 年 8 月 8 日 | 4.3 |
| 19 (*1) | 「Piwigo」における SQL インジェクションの脆弱性 | 画像管理ソフトウェア「Piwigo」には、SQL 文を組み立てる処理に問題がありました。このため、第三者により任意の SQL 命令を実行される可能性がありました。 | 2014 年 8 月 8 日 | 6.0 |
| 20 | Android 版「Ameba」における SSL サーバ証明書の検証不備の脆弱性 | Android 用 SNS アプリ「Ameba」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。 | 2014 年 8 月 14 日 | 4.0 |
| 21 (*1) | 「Shutter」における SQL インジェクションの脆弱性 | 写真共有ソフトウェア「Shutter」には、SQL 文を組み立てる処理に問題がありました。このため、第三者により任意の SQL 命令を実行される可能性がありました。 | 2014 年 8 月 15 日 | 5.1 |

| 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 | Android 版アプリ「Kindle」における SSL サーバ証明書の検証不備の脆弱性 | Android 用電子書籍ビューア「Kindle」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。 | 2014 年 8 月 29 日 | 4.0 |
| 23 | 「EmFTP」における実行ファイル読み込みに関する脆弱性 | FTP/SFTP クライアント「EmFTP」には、ファイルの読み込み処理に問題があり、実行ファイルなどの意図しないファイルを読み込んでしまう脆弱性がありました。このため、第三者により任意のコードを実行される可能性がありました。 | 2014 年 9 月 4 日 | 5.1 |
| 24 | 「WisePoint」におけるセッション固定の脆弱性 | ワンタイムパスワード認証システム「WisePoint」には、セッション固定の脆弱性がありました。このため、第三者により当該製品の登録ユーザになりすまされる可能性がありました。 | 2014 年 9 月 4 日 | 5.8 |
| 25 (*1) | 「Movable Type」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「Movable Type」には、ウェブページを出力する際の処理に問題がありました。このため、第三者によりウェブページにスクリプトを埋め込まれる可能性がありました。 | 2014 年 9 月 9 日 | 4.0 |
| 26 | 複数の「Adobe」製品のヘルプページにおけるクロスサイト・スクリプティングの脆弱性 | 複数の「adobe」製品のヘルプページには、クロスサイト・スクリプティングの脆弱性がありました。このため、第三者によりウェブページにスクリプトを埋め込まれる可能性がありました。 | 2014 年 9 月 12 日 | 4.3 |
| 27 | 「365 Links」シリーズにおけるクロスサイト・スクリプティングの脆弱性 | リンク集作成ツール「365 Links」シリーズには、ウェブページを出力する際の処理に問題がありました。このため、第三者によりウェブページにスクリプトを埋め込まれる可能性がありました。 | 2014 年 9 月 17 日 | 4.3 |
| 28 | 「ゆこゆこ」における SSL サーバ証明書の検証不備の脆弱性 | Android 用宿泊予約アプリ「ゆこゆこ」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盗聴などが行なわれる可能性がありました。 | 2014 年 9 月 22 日 | 4.0 |
| 29 | 「Safari」におけるアプリケーションキャッシュの取扱いに関する問題 | ウェブブラウザ「Safari」には、アプリケーションキャッシュの取扱いに関する問題がありました。このため、ウェブサイト側からユーザの識別をされる可能性がありました。 | 2014 年 9 月 25 日 | 5.0 |
| 30 (*1) | WordPress 用プラグイン「N-Media file uploader」におけるアップロードされたファイルの取扱いに関する脆弱性 | WordPress 用ファイルアップロードプラグイン「N-Media file uploader」には、アップロードされたファイルの取扱いに関する脆弱性がありました。このため、第三者によりサーバ上で任意のコマンドを実行される可能性がありました。 | 2014 年 9 月 25 日 | 5.0 |
| 31 | エスリンク製 Android アプリ「ファイルマネージャー」におけるディレクトリ・トラバーサルの脆弱性 | Android 用ファイル管理ソフト「ファイルマネージャー」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作成されたり既存のファイルを上書きされたりする可能性がありました。 | 2014 年 9 月 25 日 | 4.3 |
| 32 | iOS 版「jigbrowser+」における同一生成元ポリシー回避の脆弱性 | iOS 用ウェブブラウザ「jigbrowser+」には、ウェブページの読み込み処理に問題がありました。このため、第三者により異なるドメイン上の情報を取得される可能性がありました。 | 2014 年 9 月 25 日 | 5.8 |

| 項番 | 脆弱性 | セキュリティ上の問題点 | JVN 公表日 | CVSS 基本値 |
|---|---|---|---|---|
| 33 (*2) | 「Yahoo!ボックス (Android 版)」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管理アプリ「Yahoo!ボックス (Android 版)」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。 | 2014 年 9 月 25 日 | 4.0 |
| 脆弱性の深刻度=レベル I（注意）、CVSS 基本値=0.0～3.9 | | | | |
| 34 (*2) | 「サイボウズ ガルーン」の地図検索機能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 ガルーン」の地図検索機能には、ウェブページを出力する際の処理に問題がありました。このため、第三者によりウェブページにスクリプトを埋め込まれる可能性がありました。 | 2014 年 7 月 15 日 | 3.5 |
| 35 (*2) | 「サイボウズ ガルーン」のお知らせポートレット機能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 ガルーン」のお知らせポートレット機能には、ウェブページを出力する際の処理に問題がありました。このため、第三者によりウェブページにスクリプトを埋め込まれる可能性がありました。 | 2014 年 7 月 15 日 | 3.5 |
| 36 (*2) | 「サイボウズ ガルーン」において他のユーザのポートレット設定へアクセス可能な脆弱性 | グループウェア「サイボウズ ガルーン」には、他のユーザのポートレット機能へアクセス可能な脆弱性がありました。このため、他のユーザによって、ポートレットの設定を編集される可能性がありました。 | 2014 年 7 月 15 日 | 3.5 |
| 37 (*2) | 「サイボウズ ガルーン」のメッセージ機能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 ガルーン」のメッセージ機能には、ウェブページを出力する際の処理に問題がありました。このため、第三者によりウェブページにスクリプトを埋め込まれる可能性がありました。 | 2014 年 7 月 15 日 | 3.5 |
| 38 | 「Meridian」におけるクロスサイト・スクリプティングの脆弱性 | 証券取引用ソフト「Meridian」には、ウェブページを出力する際の処理に問題がありました。このため、第三者によりウェブページにスクリプトを埋め込まれる可能性がありました。 | 2014 年 7 月 18 日 | 2.6 |
| 39 | 「GOM Player」におけるサービス運用妨害 (DoS)の脆弱性 | 動画再生ソフトウェア「GOM Player」には、スキン用画像ファイルの処理に問題がありました。このため、細工された画像ファイルを読み込むことで、当該製品を起動できない状態にされる可能性がありました。 | 2014 年 8 月 6 日 | 2.6 |
| 40 (*1) | 「Piwigo」におけるクロスサイト・スクリプティングの脆弱性 | 画像管理ソフトウェア「Piwigo」には、ウェブページを出力する際の処理に問題がありました。このため、第三者によりウェブページにスクリプトを埋め込まれる可能性がありました。 | 2014 年 8 月 8 日 | 2.6 |
| 41 (*1) | 「Shutter」におけるクロスサイト・スクリプティングの脆弱性 | 写真共有ソフトウェア「Shutter」には、ウェブページを出力する際の処理に問題がありました。このため、第三者によりウェブページにスクリプトを埋め込まれる可能性がありました。 | 2014 年 8 月 15 日 | 2.6 |
| 42 (*1) | WordPress 用テーマ「Cakifo」におけるクロスサイト・スクリプティングの脆弱性 | WordPress 用のテーマ「Cakifo」には、ウェブページを出力する際の処理に問題がありました。このため、第三者によりウェブページにスクリプトを埋め込まれる可能性がありました。 | 2014 年 8 月 18 日 | 3.5 |
| 43 (*1) | 「MailPoet Newsletters」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 | WordPress 用プラグイン「MailPoet Newsletters」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。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。 | 2014 年 8 月 26 日 | 2.6 |
| 44 | Android 版「Bump」における暗黙的 Intent の扱いに関する脆弱性 | Android 版アプリ「Bump」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。 | 2014 年 9 月 19 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 |
|---|---|---|---|---|
| 45 (*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ェア「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。 | 2014 年 9 月 19 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）：組込みソフトウェアの脆弱性
（*4）：制御システムの脆弱性

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

表 2-4 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 38 件ありました。近年、Android 関連製品や OSS 製品の脆弱性に対する調整活動では、製品開発者が所在するアジア圏の調整機関、特に韓国の KrCERT/CC や中国の CNCERT/CC、台湾の TWNCERT との連携が増えています。これらの情報は、JPCERT/CC 製品開発者リスト (*14) 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 | 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 |
| 2 | Netgear GS105PE Prosafe Plus Switch に認証情報がハードコードされている問題 | 注意喚起として掲載 |
| 3 | Autodesk VRED に OS コマンドインジェクションの脆弱性 | 注意喚起として掲載 |
| 4 | CENTUM を含む複数の YOKOGAWA 製品にバッファオーバーフローの脆弱性 | 特定製品開発者へ通知 |
| 5 | AVG Safeguard および AVG Secure Search の ActiveX コントロールに任意のコードを実行される脆弱性 | 注意喚起として掲載 |
| 6 | Liferay Portal に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 |
| 7 | Raritan PX Power Distribution ソフトウェアに cipher zero 攻撃を受ける脆弱性 | 注意喚起として掲載 |
| 8 | Datum Systems の衛星モデムに複数の脆弱性 | 注意喚起として掲載 |
| 9 | Kaseya エージェントドライバーに NULL ポインタ参照の脆弱性 | 注意喚起として掲載 |
| 10 | Huawei E355 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 |
| 11 | MicroPact icomplaints 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 |
| 12 | Resin Pro に Unicode 文字を適切に変換しない問題 | 注意喚起として掲載 |
| 13 | TestRail 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 |
| 14 | BulletProof FTP Client 2010 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 |
| 15 | Omron NS シリーズ HMI に複数の脆弱性 | 特定製品開発者へ通知 |
| 16 | Sabre AirCentre Crew ソリューションに SQL インジェクションの脆弱性 | 注意喚起として掲載 |
| 17 | Silver Peak VX に複数の脆弱性 | 注意喚起として掲載 |
| 18 | Symantec Endpoint Protection 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 |
| 19 | UEFI EDK2 の Capsule Update 処理に複数の脆弱性 | 複数製品開発者へ通知 |

(*14) 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 |
|---|---|---|
| 20 | Cobham SATCOM 製品のウェブインターフェースのパスワード復元メカニズムに脆弱性 | 注意喚起として掲載 |
| 21 | Cobham thraneLINK デバイスのファームウェアアップデート機能に脆弱性 | 注意喚起として掲載 |
| 22 | Cobham Sailor の衛星通信用端末に認証情報がハードコードされている問題 | 注意喚起として掲載 |
| 23 | Cobham Sailor 6000 シリーズの衛星通信用端末に認証情報がハードコードされている問題 | 注意喚起として掲載 |
| 24 | Cobham Aviator 衛星通信用端末に複数の脆弱性 | 注意喚起として掲載 |
| 25 | Iridium Pilot と OpenPort に複数の脆弱性 | 注意喚起として掲載 |
| 26 | OpenSSL クライアントにナルポインタ参照の脆弱性 | 複数製品開発者へ通知 |
| 27 | 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 |
| 28 | 複数の Android アプリに SSL 証明書を適切に検証しない脆弱性 | 注意喚起として掲載 |
| 29 | Netmaster 製ケーブルモデム CBW700N における情報漏えいの脆弱性 | 注意喚起として掲載 |
| 30 | Arris 製ケーブルモデム Touchstone DG950A に情報漏えいの脆弱性 | 注意喚起として掲載 |
| 31 | Netgear ProSafe Plus Configuration Utility に管理パスワード漏えいの脆弱性 | 注意喚起として掲載 |
| 32 | CacheGuard OS にクロスサイトリクエストフォージェリの脆弱性 | 注意喚起として掲載 |
| 33 | Embarcadero Delphi と C++Builder の VCL 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 |
| 34 | CENTUM および Exaopc において任意のファイルにアクセス可能な脆弱性 | 特定製品開発者へ通知 |
| 35 | 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 |
| 36 | FortiGate および FortiWiFi アプライアンスに複数の脆弱性 | 注意喚起として掲載 |
| 37 | Mozilla Network Security Services (NSS) に RSA 署名検証不備の脆弱性 | 注意喚起として掲載 |
| 38 | GNU Bash に OS コマンドインジェクションの脆弱性 | 緊急案件として掲載<br>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 2-14 は、2011 年 9 月末から 2014 年 9 月末までに、「連絡不能開発者」と位置づけて取扱った 173 件の処理状況の推移を示したものです。

2014 年 9 月末時点での処理状況は、173 件のうち、製品開発者との調整が再開したため連絡不能開発者一覧から削除したものは 22 件（前四半期は 21 件）で、引き続き公表しているものは 151 件（前四半期は 144 件）となりました。このうち、5 件について、連絡期限を追記しました。

「連絡不能」は、前期からの繰り越し 143 件と、今四半期に「新規公表」8 件の累計 151 件となりました。このうち、前四半期に新規公表したうち 13 件は今期、12 件の連絡が取れなかったため製品情報を追加する「追加情報公表」となり、1 件が調整を再開しました。

また、「調整再開（調整中）」の件数は新たに「連絡不能」から追加された 1 件、および製品開発者との調整完了が 1 件あり、今期は差引き 11 件でした。一方、「調整再開（調整完了）」は 1 件増加し、「調整再開」の合計は 22 件となりました。

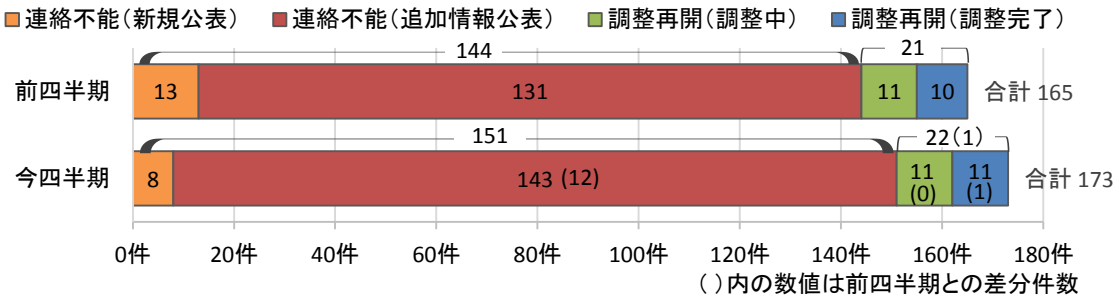



**図2-14. 連絡不能開発者一覧の処理状況**

## 2-2. ウェブサイトの脆弱性

### 2-2-1. 処理状況

図 2-15 のグラフは、ウェブサイトの脆弱性届出の処理状況について、四半期別の推移を示したものです。2014 年 9 月末時点の届出の累計は 8,218 件で、今四半期中に取扱いを終了したものは 213 件（累計 7,635 件）でした。このうち「修正完了」したものは 183 件（累計 5,778 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 20 件（累計 456 件）でした。“「注意喚起」により処理を取りやめる”とは、多数のウェブサイトにおいて利用されているソフトウェア製品に修正プログラムが適用されていない、といった届出があった場合、届出されたウェブサイト以外でも影響を受ける可能性があるため、「注意喚起」で広く対策を呼びかけた上で処理を取りやめたものです。なお、ウェブサイト運営者への連絡は通常メールで行い、連絡が取れない場合は電話や郵送での連絡も行っています。しかしウェブサイト運営者への連絡手段がない場合などは「取扱不能」案件となります。今期その件数は 4 件（累計 88 件）でした。また「不受理」としたものは 6 件 [*15] （累計 183 件）でした。取扱いを終了した累計 7,635 件のうち「修正完了」「脆弱性ではない」の合計 6,234 件は全て、ウェブサイト運営者からの報告もしくは IPA の判断により指摘した点が解消されていることが確認されています。「修正完了」のうち、ウェブサイト運営者が当該ページの削除により対応したものは 13 件（累計 649 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。

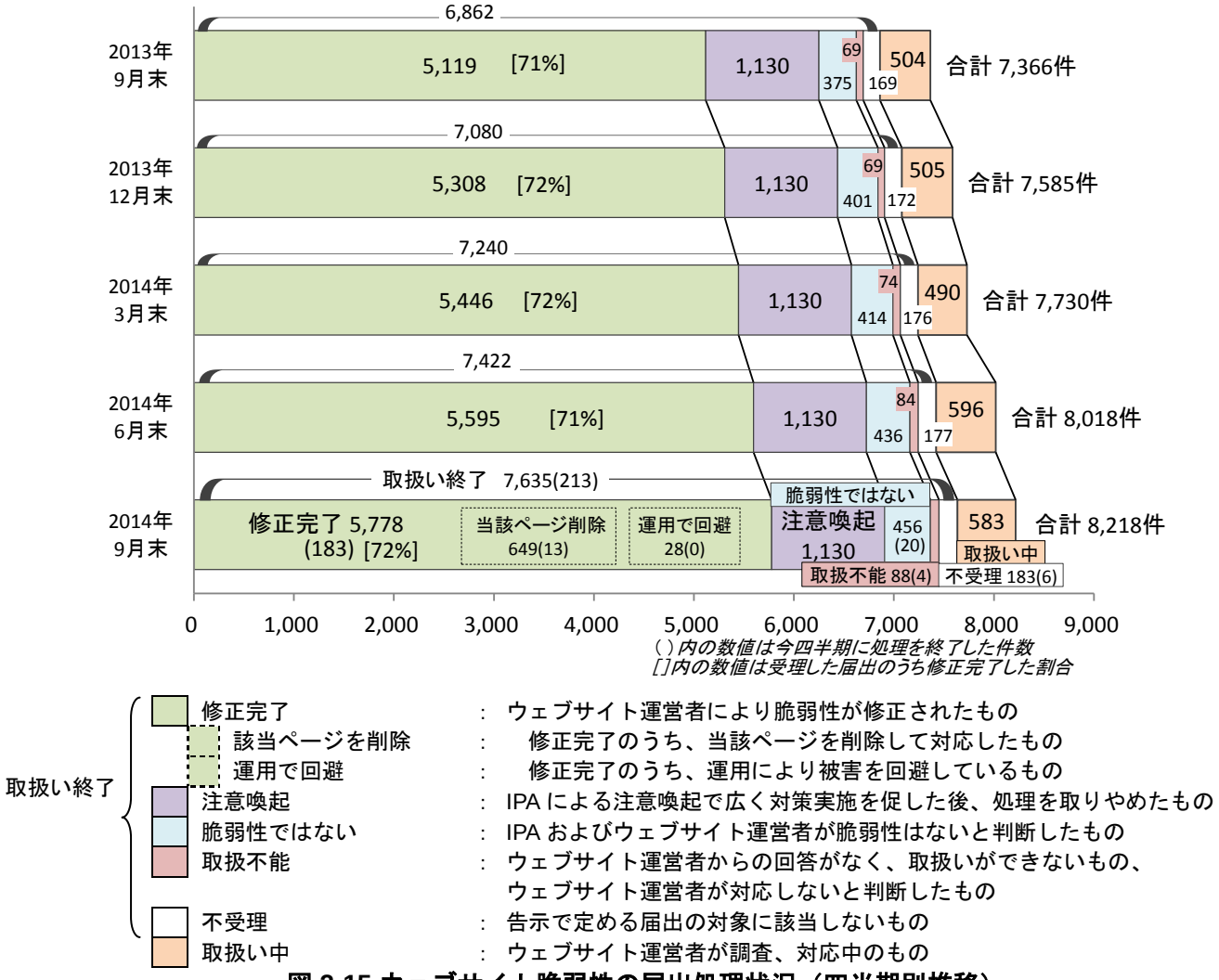



**図 2-15.ウェブサイト脆弱性の届出処理状況（四半期別推移）**

[*15] 今四半期の届出の中で不受理とした 5 件、前四半期までの届出の中で今四半期に不受理とした 1 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 8,218 件のうち、不受理を除いた 8,035 件の届出を分析した結果を記載します。

### 2-2-2. 運営主体の種類別の届出件数

図 2-16 のグラフは、届出されたウェブサイトにおける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別に示しています。今四半期は全体の約 8 割を「企業（株式・非上場）」が占めています。

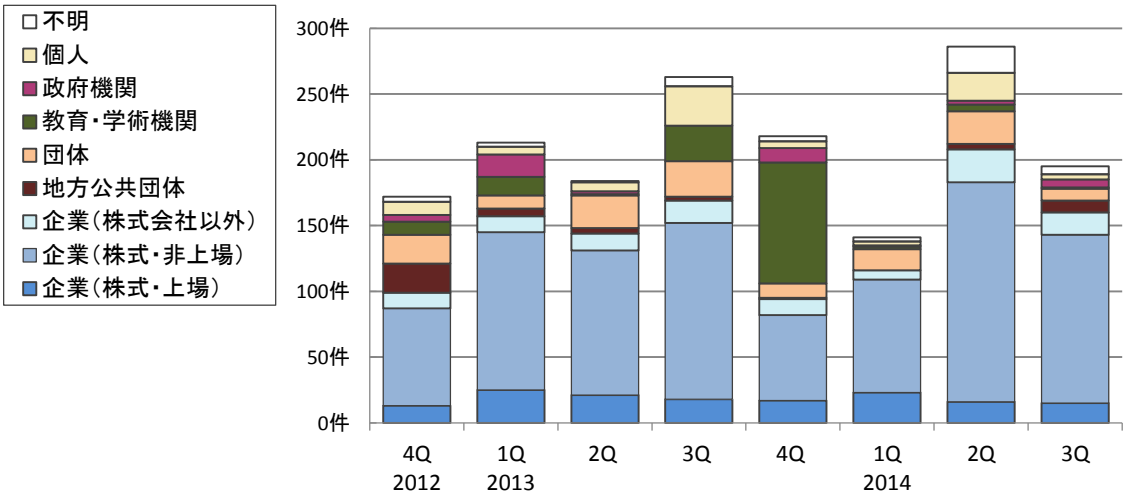


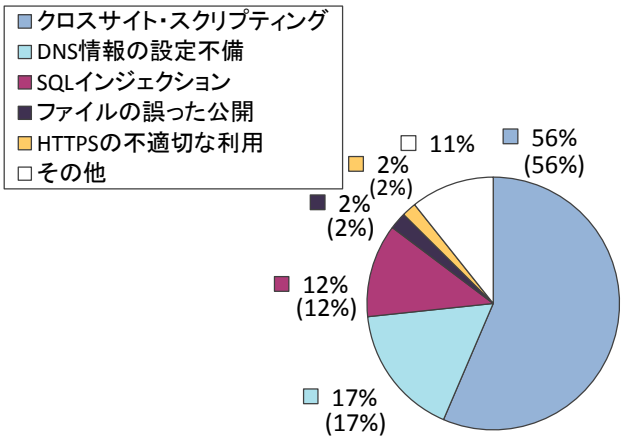

**図2-16. 四半期毎の運営主体の種類別届出件数**

### 2-2-3. 脆弱性の種類・脅威別届出

図 2-17、図 2-18 のグラフは、届出された脆弱性の種類を示しています。図 2-17 は届出受付開始から今四半期末までの届出累計の割合を、図 2-18 は過去 2 年間の届出件数の推移を四半期別に示しています [*16]。

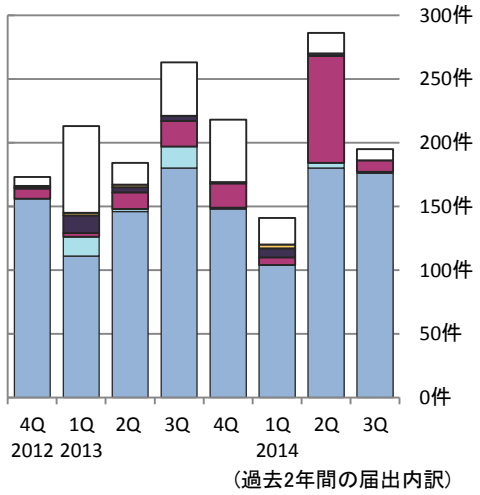
累計では、「クロスサイト・スクリプティング」だけで 56%を占めており、次いで「DNS 情報の設定不備」「SQL インジェクション」となっています。「DNS 情報の設定不備」は 17%ありますが、2008 年から 2009 年にかけて多く届出されたのが反映されたものです。今四半期は「クロスサイト・スクリプティング」が約 9 割を占めています。なお、この統計は本制度における届出の傾向であり、世の中に存在する脆弱性の傾向と必ずしも一致するものではありません。

**ウェブサイトの脆弱性の種類別の届出状況**




（8,035件の内訳、グラフの括弧内は前四半期までの数字）

**図2-17. 届出累計の脆弱性の種類別割合**



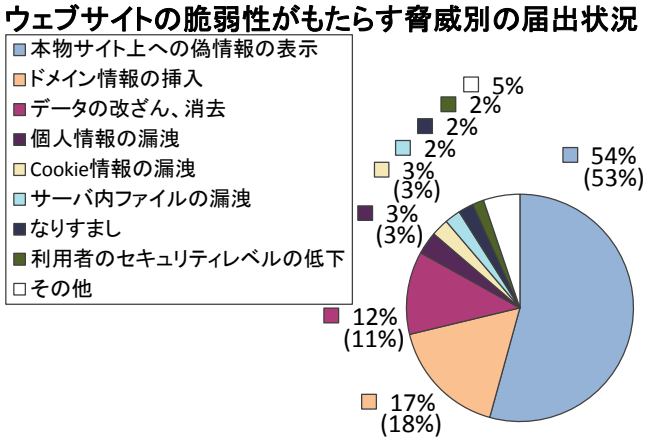

（過去2年間の届出内訳）

**図2-18. 四半期毎の脆弱性の種類別届出件数**

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

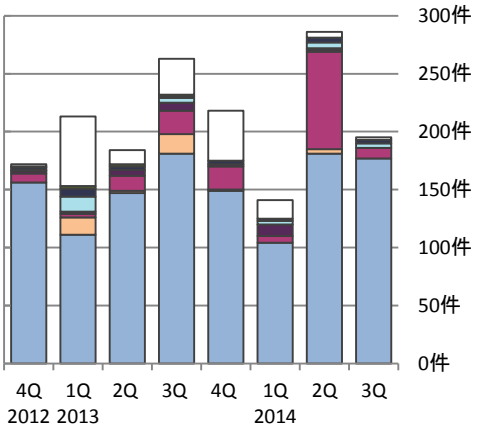
図 2-19、図 2-20 のグラフは、届出された脆弱性がもたらす脅威別の分類です。図 2-19 は届出受付開始から今四半期末までの届出の割合を、図 2-20 は過去 2 年間の届出件数の推移を四半期別に示しています。

累計では、「クロスサイト・スクリプティング」「DNS 情報の設定不備」「SQL インジェクション」などにより発生する、「本物サイト上での偽情報の表示」「ドメイン情報の挿入」「データの改ざん、消去」が全体の 8 割を占めています。今四半期は、「クロスサイト・スクリプティング」が多く届出されたため「本物サイト上での偽情報の表示」が約 9 割を占めており、前四半期に多く届出された「データの改ざん、消去」は前四半期の 1 割程に減少しています。




(8,035件の内訳、グラフの括弧内は前四半期までの数字)

**図2-19. 届出累計の脆弱性がもたらす脅威別割合**




(過去2年間の届出内訳)

**図2-20. 四半期毎の脆弱性がもたらす脅威別届出件数**

### 2-2-4. 修正完了状況

図 2-21 のグラフは、過去 3 年間のウェブサイトの脆弱性の修正完了件数を四半期ごとに示しています。2014 年第 3 四半期に修正を完了した 183 件のうち 142 件（78%）は、運営者へ脆弱関連情報を通知してから修正完了までの日数が 90 日以内の届出です。今四半期は、90 日以内に修正完了した届出の割合が、前四半期（149 件中 95 件（64%））より増加しています。

表 2-5 は、過去 3 年間の修正が完了した全届出のうち、ウェブサイト運営者に脆弱性を通知してから、90 日以内に修正が完了した累計および割合を四半期ごとに示しています。

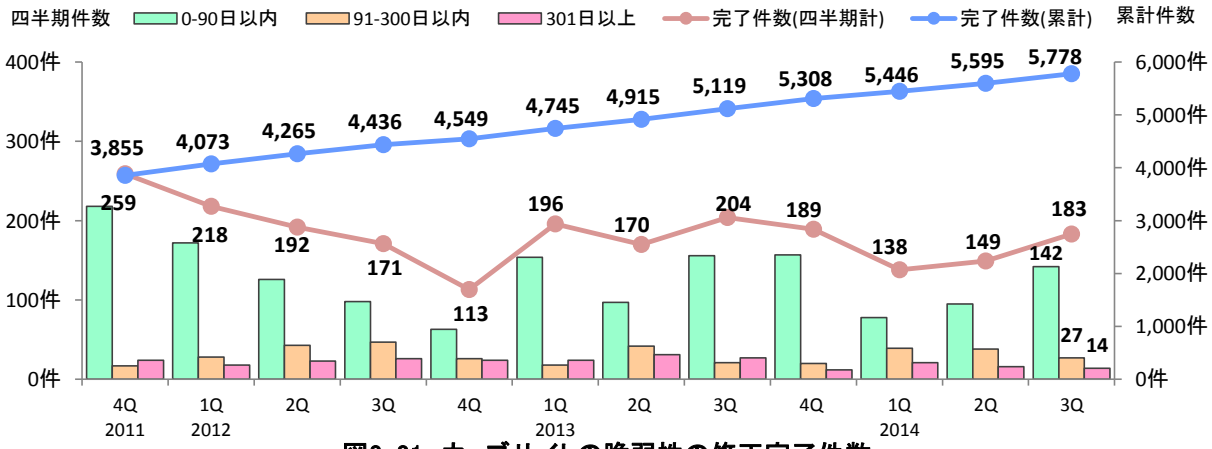



**図2-21. ウェブサイトの脆弱性の修正完了件数**

**表 2-5. 90 日以内に修正完了した累計およびその割合の推移**

| | 2011 4Q | 2012 1Q | 2Q | 3Q | 4Q | 2013 1Q | 2Q | 3Q | 4Q | 2014 1Q | 2Q | 3Q |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 修正完了件数 | 3,855 | 4,073 | 4,265 | 4,436 | 4,549 | 4,745 | 4,915 | 5,119 | 5,308 | 5,446 | 5,595 | 5,778 |
| 90 日以内の件数 | 2,534 | 2,706 | 2,832 | 2,930 | 2,993 | 3,147 | 3,244 | 3,400 | 3,557 | 3,635 | 3,730 | 3,872 |
| 90 日以内の割合 | 66% | 66% | 66% | 66% | 66% | 66% | 66% | 66% | 67% | 67% | 67% | 67% |

図 2-22、図 2-23 は、ウェブサイト運営者に脆弱性を通知してから修正されるまでに要した日数を脆弱性の種類別に分類し、その傾向を示しています[*17]。全体の 48%の届出が 30 日以内、全体の 67%の届出が 90 日以内に修正されています。

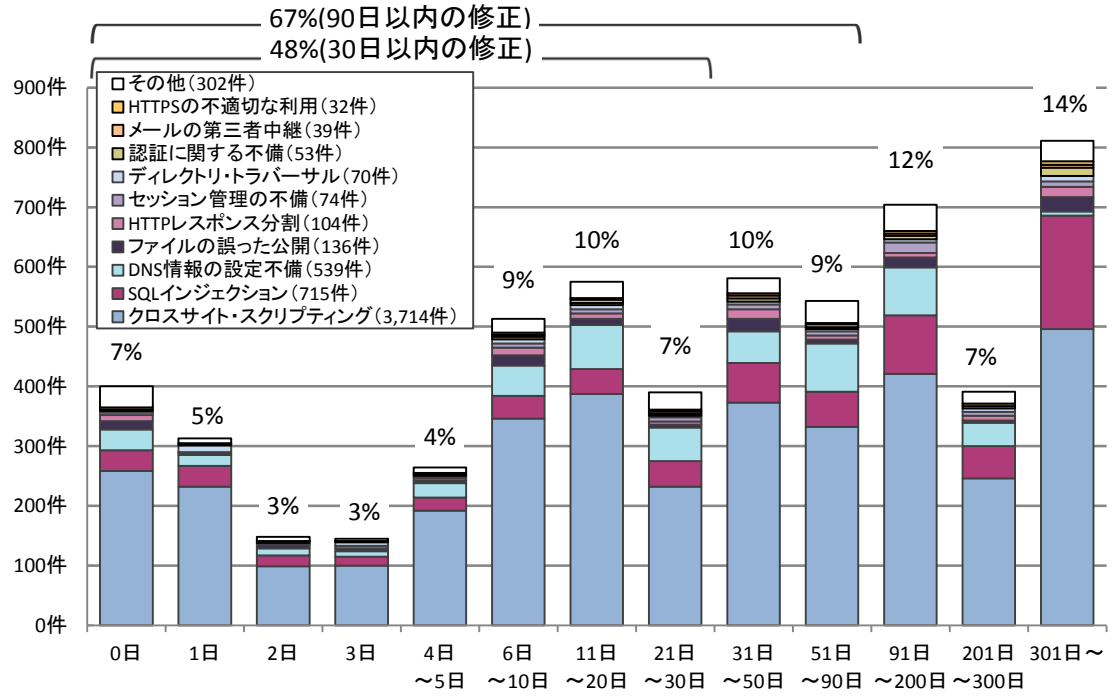



**図2-22. ウェブサイトの修正に要した日数**

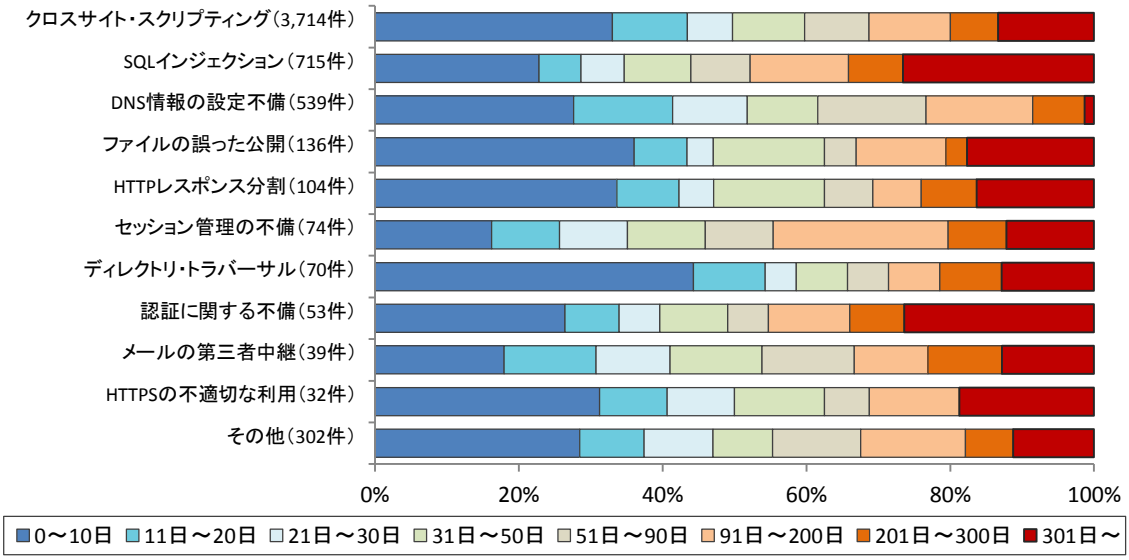



**図2-23. ウェブサイトの修正に要した脆弱性種類別の日数の傾向**

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

### 2-2-5. 取扱中の状況

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

図 2-24 は、ウェブサイトの脆弱性のうち、取扱いが長期化（IPA からウェブサイト運営者へ脆弱性を通知してから、90 日以上脆弱性を修正した旨の報告が無い）しているものについて、経過日数別の件数を示したものです。これらの合計は 402 件（前四半期は 353 件）です。

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

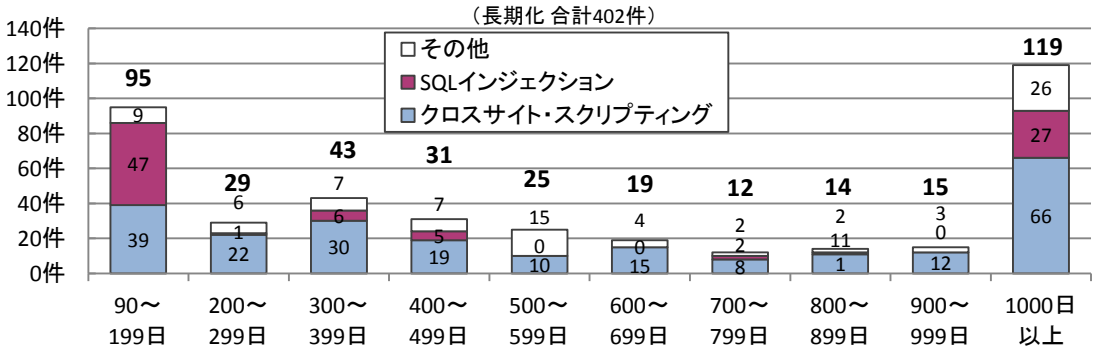



**図2-24. 取扱いが長期化(90日以上経過)しているウェブサイトの経過日数と脆弱性の種類**

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

**表 2-6. 取扱いが長期化している届出件数および割合の四半期別推移**

| | 2012 4Q | 2013 1Q | 2Q | 3Q | 4Q | 2014 1Q | 2Q | 3Q |
|---|---|---|---|---|---|---|---|---|
| 取扱い中の件数 | 473 | 474 | 473 | 504 | 505 | 490 | 596 | 583 |
| 長期化している件数 | 296 | 301 | 307 | 302 | 358 | 357 | 353 | 402 |
| 長期化している割合 | 63% | 64% | 65% | 60.0% | 71% | 73% | 59% | 69% |

## 3. 関係者への要望

脆弱性の修正促進のための、各関係者への要望は以下のとおりです。

### 3-1. ウェブサイト運営者

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

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

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

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

また、対策実施にあたっては、以下のコンテンツが利用できます。

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

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

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

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

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

⇒「動画で知ろう！クロスサイト・スクリプティングの被害！」（約 7 分）:
http://www.ipa.go.jp/security/keihatsu/videos/index.html#eng

### 3-2. 製品開発者

JPCERT/CC は、ソフトウェア製品の脆弱性関連情報を、「製品開発者リスト」に基づき、一般公表日の調整等を行います。迅速な調整が進められるよう、「製品開発者リスト」に登録してください（URL：https://www.jpcert.or.jp/vh/regist.html）。また、製品開発者自身が自社製品の脆弱性関連情報を発見した場合も、対策情報を利用者へ周知するために JVN を活用することができます。JPCERT/CC もしくは IPA へ連絡してください。

なお、製品開発にあたっては、以下のコンテンツが利用できます。

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

⇒「ファジング：製品出荷前に機械的に脆弱性をみつけよう」:
http://www.ipa.go.jp/security/vuln/fuzzing.html

⇒「Android アプリの脆弱性の学習・点検ツール AnCoLe」:
http://www.ipa.go.jp/security/vuln/ancole/index.html

### 3-3. 一般のインターネットユーザー

JVN や IPA、JPCERT/CC など、脆弱性情報や対策情報を公表しているウェブサイトを参照し、パッチの適用など、自発的なセキュリティ対策を日ごろから心がける必要があります。ソフトウェアを利用する場合は、脆弱性対策を実施してから利用してください。

なお、一般インターネットユーザー向けには、以下のツールを提供しています。

⇒「MyJVN 情報収集ツール」: http://jvndb.jvn.jp/apis/myjvn/mjcheck.html
脆弱性対策情報を効率的に収集するためのツール。

⇒「MyJVN バージョンチェッカ」: http://jvndb.jvn.jp/apis/myjvn/vccheck.html
利用者の PC、サーバ上にインストールされたソフトウェア製品のバージョンを容易にチェックする等の機能。

### 3-4. 発見者

脆弱性関連情報の適切な流通のため、届出した脆弱性関連情報については、脆弱性が修正されるまでは、第三者に漏れないよう、適切に管理してください。

**付表 1. ソフトウェア製品の脆弱性の原因分類**

| | 脆弱性の原因 | 説明 | 届出において<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 |

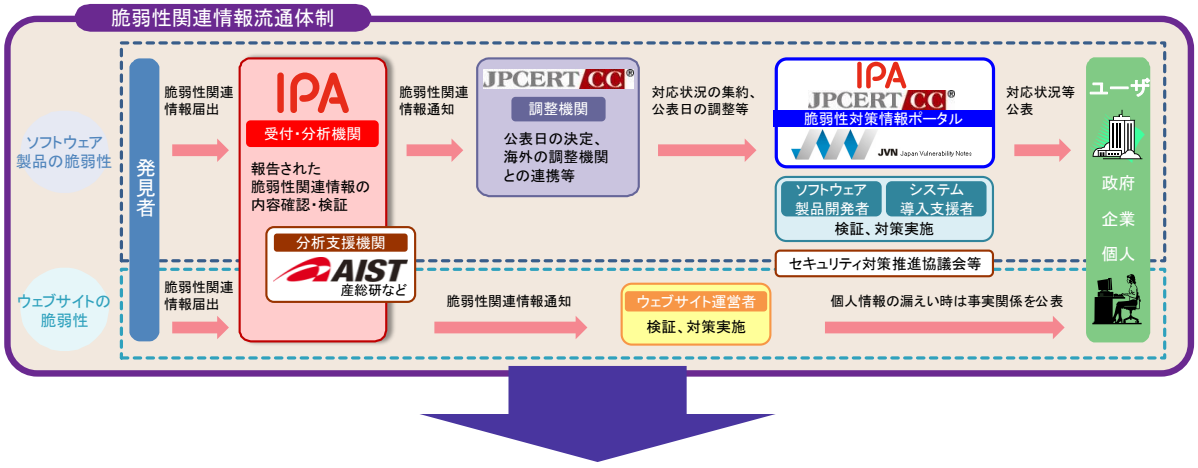
**付表 2. ウェブサイトの脆弱性の分類**

| | 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