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

[2014 年第 2 四半期（4 月～6 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（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 4 月 1 日から 2014 年 6 月 30 日までの間に実施した、脆弱性関連情報の取扱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 7 月 24 日

目次

1. 2014 年第 2 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
1-1. 脆弱性関連情報の届出受付状況 1
1-2. 脆弱性の修正完了状況 2
1-3. 連絡不能案件の取扱い状況 2
1-4. 脆弱性の傾向について 3
1-4-1.オープンソースソフトウェアの脆弱性の調整および公表 3
1-4-2.古いコンテンツ管理システムを利用するウェブサイトの改ざんの危険性 4
1-5. 経済産業省告示の改正および、「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の改訂 5
2. ソフトウェア等の脆弱性に関する取扱状況（詳細） 6
2-1. ソフトウェア製品の脆弱性 6
2-1-1. 処理状況 6
2-1-2. ソフトウェア製品別届出件数 7
2-1-3. 脆弱性の原因と脅威別件数 8
2-1-4. 調整および公表件数 10
2-1-5. 連絡不能案件の処理状況 15
2-2. ウェブサイトの脆弱性 16
2-2-1. 処理状況 16
2-2-2. 運営主体者別件数 17
2-2-3. 脆弱性の種類・脅威別届出 17
2-2-4. 修正完了状況 18
2-2-5. 取扱中の状況 20
3. 関係者への要望 21
3-1. ウェブサイト運営者 21
3-2. 製品開発者 21
3-3. 一般のインターネットユーザー 21
3-4. 発見者 21
付表 1. ソフトウェア製品の脆弱性の原因分類 22
付表 2. ウェブサイトの脆弱性の分類 23
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） . 24

1. 2014 年第 2 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 9,847 件になりました ～

本制度 (*1) における届出状況について、表 1-1 は 2014 年第 2 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 40 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 289 件、合計 329 件でした。届出受付開始からの累計は 9,847 件で、内訳はソフトウェア製品に関するもの 1,828 件、ウェブサイトに関するもの 8,019 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
ソフトウェア製品	**40** 件	**1,828** 件
ウェブサイト	**289** 件	**8,019** 件
合計	**329** 件	**9,847** 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。今四半期は前四半期と比較して、ソフトウェア製品に関する届出が減少し、ウェブサイトに関する届出が 2 倍に増加しています。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。

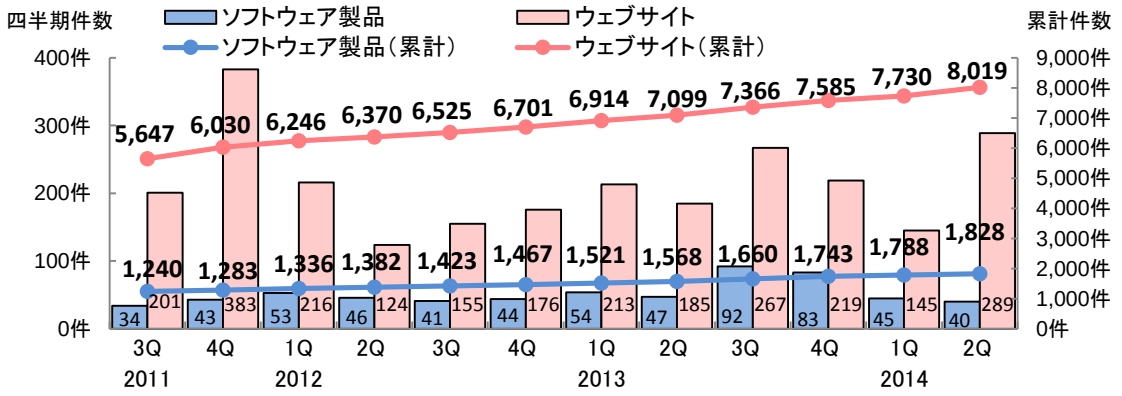


図1−1. 脆弱性関連情報の届出件数の四半期別推移

表 1−2. 届出件数（過去 3 年間）

	2011 3Q	4Q	2012 1Q	2Q	3Q	4Q	2013 1Q	2Q	3Q	4Q	2014 1Q	2Q
累計届出件数[件]	6,887	7,313	7,582	7,752	7,948	8,168	8,435	8,667	9,026	9,328	9,518	9,847
1就業日あたり[件/日]	3.93	4.03	4.05	4.00	3.98	3.78	3.96	3.96	4.00	4.03	4.01	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 6,475 件となりました～

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	**29** 件	**880** 件
ウェブサイト	**149** 件	**5,595** 件
合計	**178** 件	**6,475** 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 JVN で対策情報を公表した四半期別の修正完了件数は、2011 年以降 30 件前後で推移しており今四半期は 29 件 (*3)（累計 880 件）でした。そのうち、9 件が製品開発者自身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公表までの日数が 45 日 (*4) 以内だったのは 13 件（45%）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 149 件（累計 5,595 件）でした。修正を完了した 149 件のうち、ウェブアプリケーションを修正したもの 125 件（84%）、当該ページを削除したもの 24 件（16%）、運用で回避したもの 0 件でした。なお、修正を完了した 149 件のうち 95 件（64%）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 (*5) 以内の届出でした。今四半期は、90 日以内に修正完了した割合が、前四半期（138 件中 78 件（58%））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。「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ています。

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 13 件、製品開発者名に加え製品情報を追加公表したものは 7 件、2014 年 6 月末時点の「連絡不能開発者一覧」への公表件数は 144 件となりました。

(*3) 表 2-3 参照
(*4) 公表日の目安は、脆弱性関連情報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、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。
(*6) 連絡不能開発者一覧：http://jvn.jp/reply/index.html

1-4. 脆弱性の傾向について

1-4-1.オープンソースソフトウェアの脆弱性の調整および公表

～ 注目された Apache Struts、OpenSSL の脆弱性を JVN で公表 ～

表 1-4 は、2014 年第 2 四半期に JVN で脆弱性対策情報を公表した 29 件のうち、オープンソースソフトウェア（OSS）製品である 11 件の脆弱性を示しています。2014 年第 2 四半期は世界的に大きく注目された「Apache Struts」および「OpenSSL」などの深刻な脆弱性についても、本制度に基づき、製品開発者などと調整の上、JVN で公表しました。「Apache Struts」の脆弱性（JVN#19294237、CVE-2014-0112）は、CVE-2014-0094 の対策が不十分であったため問題が残存していました。攻撃に悪用された場合、ウェブサイトが改ざんされる可能性がありました。また、「OpenSSL」の脆弱性（JVN#61247051、CVE-2014-0224）は、中間者攻撃によって盗聴や改ざんに悪用できるため、暗号化を実現するソフトウェアの利用意義を揺るがす致命的な脆弱性でした。この様に、悪用された場合の影響が大きく、利用者の多いソフトウェア製品の脆弱性においても、発見者が本制度を活用することによって、より多くの製品開発者に脆弱性関連情報を適切に通知することができます。本制度は、利用者の円滑な脆弱性対策を促すことにも有効といえます。

表 1-4. 2014 年第 2 四半期に公表したオープンソースソフトウェアの脆弱性

公表日	JVN番号	深刻度	件名
6月24日	JVN#05329568	（警告）	WordPress 用プラグイン「Login rebuilder」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
6月20日	JVN#02213197	（注意）	「Webmin」におけるクロスサイト・スクリプティングの脆弱性
6月20日	JVN#49974594	（注意）	「Webmin」におけるクロスサイト・スクリプティングの脆弱性
6月20日	JVN#92737498	（警告）	「Usermin」におけるクロスサイト・スクリプティングの脆弱性
6月20日	JVN#48805624	（警告）	「Usermin」における OS コマンド・インジェクションの脆弱性
6月17日	JVN#30962312	（危険）	「TERASOLUNA Server Framework for Java(Web)」において ClassLoader が操作可能な脆弱性
6月13日	JVN#49154900	（警告）	「Spring Framework」におけるディレクトリ・トラバーサルの脆弱性
6月6日	JVN#61247051	（警告）	「OpenSSL」における Change Cipher Spec メッセージの処理に脆弱性
6月4日	JVN#54650130	（注意）	「SOY CMS」におけるクロスサイト・スクリプティングの脆弱性
4月25日	JVN#19294237	（危険）	「Apache Struts」において ClassLoader が操作可能な脆弱性
4月16日	JVN#93004610	（警告）	「Redmine」におけるオープンリダイレクトの脆弱性

図 1-2 は、過去 2 年間を四半期別に JVN で脆弱性対策情報を公表したソフトウェア製品の届出について、ライセンス別（オープンソースソフトウェア以外/オープンソースソフトウェア）の公表件数を示しています。過去 2 年間に公表した累計 241 件のうち、66 件（27%）が「オープンソースソフトウェア」でした。今四半期の「オープンソースソフトウェア」公表件数の割合は、過去 2 年間で、比較的多く、38%（公表件数 29 件のうち 11 件）でした。

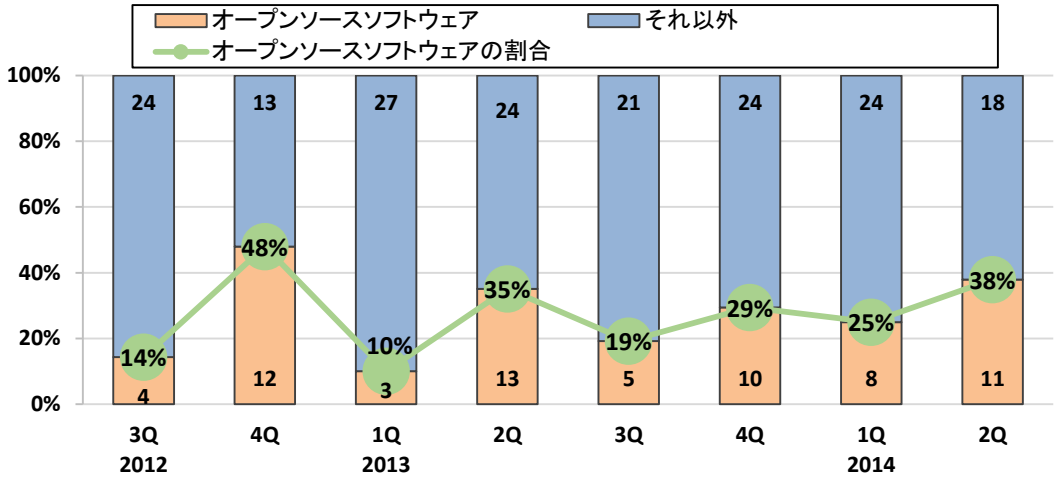


図 1-2. オープンソースとオープンソース以外の脆弱性公表件数

OSS 製品で脆弱性を発見した場合は、次の点を考慮し、対策に向けた手続きを行う必要があります。

・OSS 製品は、世界各地に在住する製品開発者が協力して開発しているため、多くの場合は国外の OSS 製品開発者のコミュニティに英語等で報告する必要がある
・OSS の脆弱性は OSS を利用（内包）しているソフトウェア製品にも影響を及ぼすため、OSS 製品開発者だけではなく、影響を受ける複数の製品開発者に報告することが望まれる

発見者がこれらに対応するのは大きな負担が掛かるという問題がありますが、本制度はその負担を軽減する解決策の一つです。本制度では、製品開発者との調整機関である JPCERT/CC を経由して製品開発者へ脆弱性情報を通知するため、脆弱性の発見者は、製品開発者と直接連絡をとる必要がありません。さらに、届出された脆弱性が複数のソフトウェア製品に影響を及ぼすと考えられる場合、JPCERT/CC が管理するリストに登録された製品開発者へ、脆弱性情報を展開しています。

そのため、脆弱性の発見者が本制度を利用した場合、負担を減らせるだけでなく、OSS を利用（内包）しているソフトウェアを開発する製品開発者等が、脆弱性の存在が公表される前に JPCERT/CC から脆弱性情報を受け取り、事前に OSS を利用（内包）した製品等への影響範囲の確認や修正ができる場合があります。脆弱性の修正後は、JVN で公表し、製品利用者へ早期に脆弱性対策情報を伝え、アップデートの適用を促すことができます。

今後も、発見者と製品開発者との調整に本制度が活用され、ソフトウェア製品の脆弱性対策が促進されることを期待します。

1-4-2.古いコンテンツ管理システムを利用するウェブサイトの改ざんの危険性

～ 狙われている脆弱性に対応できていないウェブサイトの危険性 ～

図 1-3 は、2013 年第 1 四半期から今四半期までに届出されたウェブサイトの届出のうち、古いバージョンのコンテンツ管理システム（以降、CMS）に起因する脆弱性の届出件数を示しています。本制度に届出されたウェブサイトの脆弱性 8,019 件のうち、不受理を除いた 7,842 件を調査したところ、241 件が古いバージョンの「Movable Type」や「WordPress」などの CMS の利用に起因する脆弱性でした。2013 年第 3 四半期以降、古いバージョンの CMS に起因する脆弱性が継続して届出されたため、IPA で古いバージョンの CMS を利用しているウェブサイトを調査しました。その結果、古いバージョンの「Movable Type」の利用に起因する脆弱性があるウェブサイト 71 件を発見し、本制度に届出を行ったため、今四半期の届出件数は 85 件と増加しました。

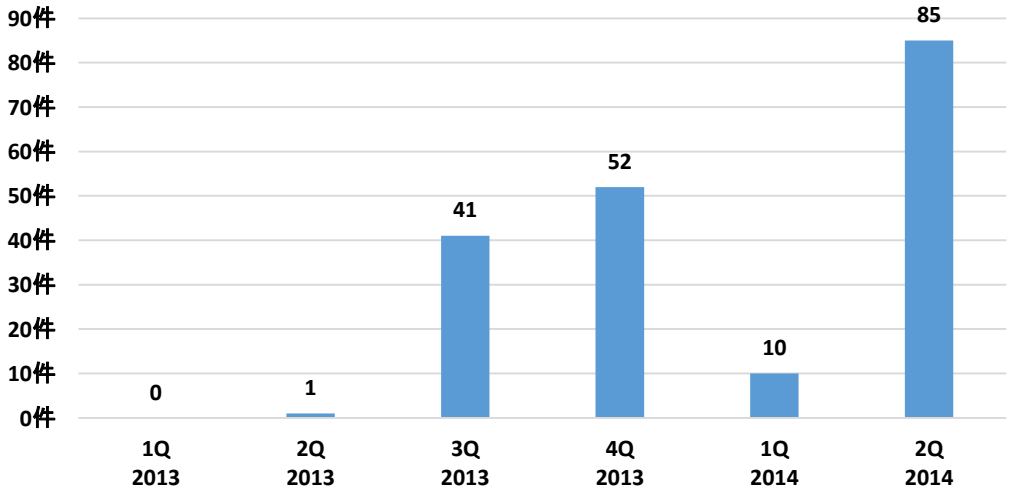


図 1-3. 古いバージョンのCMSの脆弱性を持つウェブサイトの届出件数

この様な届出状況の一方で、JPCERT/CC においては、「Movable Type」などの古いバージョンの CMS を使用しているウェブサイトが改ざんされるインシデントの報告を多数受領しており[*7]、ウェブサイトに不正なファイルが設置されるなどの改ざん事例が昨年より増加しているという現状があります。ウェブサイトの改ざん事例の全てが、脆弱性に起因するものであるとは断定できませんが、脆弱性を内在した状態でウェブサイトの運用を行っている場合、攻撃者によって脆弱性を突かれ、ウェブサイトが改ざんされるなどの被害を受ける可能性が高いことは明白です。

また、IPA から、古いバージョンの CMS を使用しているウェブサイト管理者に連絡した結果、「自組織のウェブサイトに CMS が使われているという認識がない」、「脆弱性がある古いバージョンの CMS を使用する危険性を認識していない」または「委託先との契約終了などの理由でウェブサイトの管理者が不在である」という状況が浮き彫りになりました。

これらの状況から、ウェブサイトの運営者においては、CMS に関わらず、ウェブサイトで利用しているソフトウェア製品を把握し、最新の状態を保つことで、脆弱性を悪用されるなどのリスクの低減に努める必要があります。また、ウェブサイトの管理者が不在等で適切な管理ができない場合は、現在契約しているウェブサイトホスティング業者や技術支援してくれるシステム構築業者にウェブサイトの適切な管理について、相談することを勧めます。ウェブサイトを適切に管理できない場合などは、ウェブサイト運営者だけでなくインターネット利用者全てに被害が及ぶため、ウェブサイト閉鎖などの検討が必要です。

1-5. 経済産業省告示の改正および、「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の改訂

5 月 14 日に、経済産業省の告示が改正されました。また、「情報システム等の脆弱性情報の取扱いに関する研究会」での検討結果を踏まえ、「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」を改訂し、5 月 30 日に公開しました[*8]。

[*7] 旧バージョンの Movable Type の利用に関する注意喚起:
https://www.jpcert.or.jp/at/2014/at140024.html

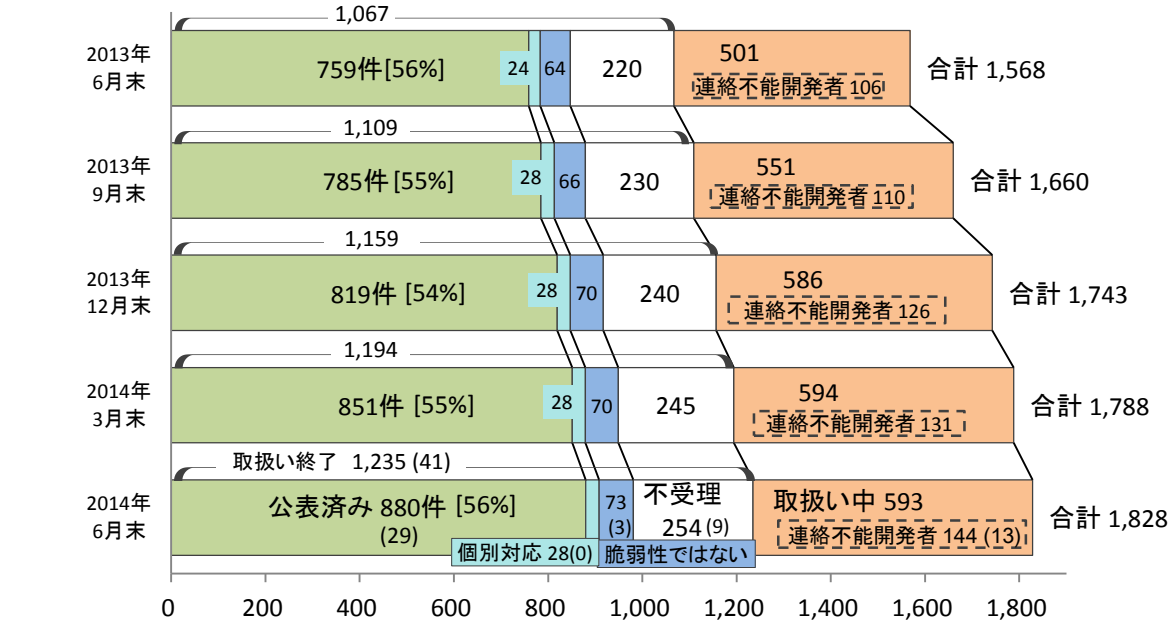
[*8] 「情報セキュリティ早期警戒パートナーシップガイドライン」の 2014 年版を公開:
http://www.ipa.go.jp/security/ciadr/partnership_guide.html

2. ソフトウェア等の脆弱性に関する取扱状況（詳細）

2-1. ソフトウェア製品の脆弱性

2-1-1. 処理状況

図 2-1 のグラフはソフトウェア製品の脆弱性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。2014 年 6 月末時点の届出の累計は 1,828 件で、今四半期に公表した（修正完了した）脆弱性は 29 件（累計 880 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 3 件（累計 73 件）、「不受理」としたものは 9 件 (*9)（累計 254 件）、取扱い中は 593 件でした。うち、連絡不能開発者一覧に公表した連絡不能開発者 (*10) は 13 件で、2014 年 6 月末時点の連絡不能開発者公表数は 144 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

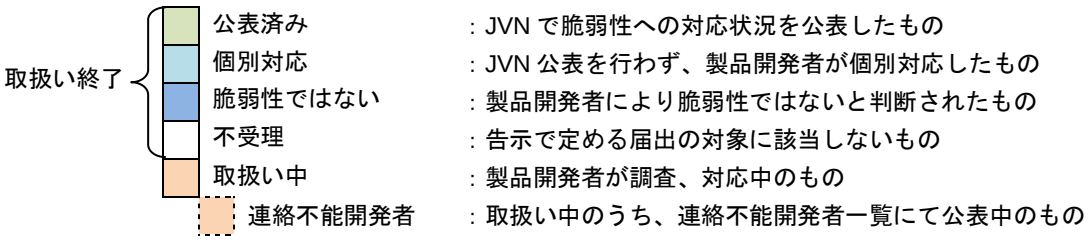


図 2-1. ソフトウェア製品脆弱性関連情報の届出処理状況（四半期別推移）

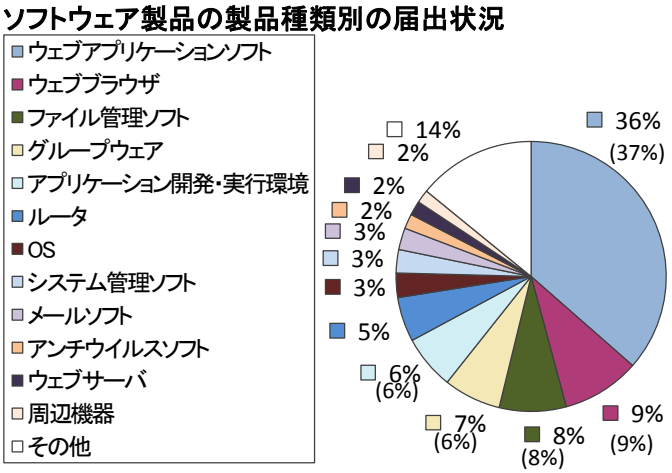
(*9) 今四半期の届出の中で不受理とした 3 件、前四半期までの届出の中で今四半期に不受理とした 6 件です。
(*10) 連絡不能開発者一覧への公表および一覧からの削除が複数回行われている製品開発者については、公表回数の累計を計上しています。

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1,828 件のうち、不受理を除いた 1,574 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

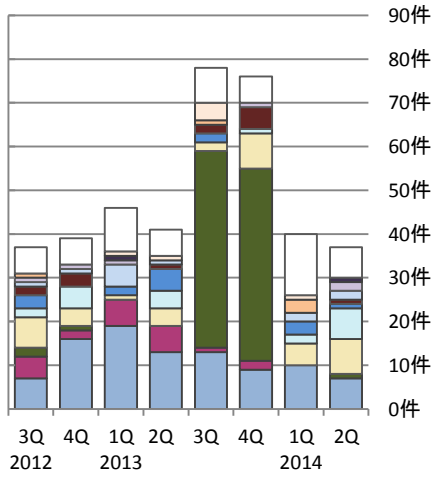
図 2-2、図 2-3 のグラフは、届出された脆弱性の製品種類別の分類を示しています。図 2-2 は届出受付開始から今四半期末までの製品種類別割合を、図 2-3 は過去 2 年間の届出件数の推移を四半期別に示したものです。

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、「グループウェア」が最も多く、次いで「ウェブアプリケーションソフト」と「アプリケーション開発・実行環境」が多くなっています。



※その他には、データベース、携帯機器などがあります。
（1,574件の内訳、グラフの括弧内は前四半期までの数字）

図2-2. 製品種類別の届出件数の割合

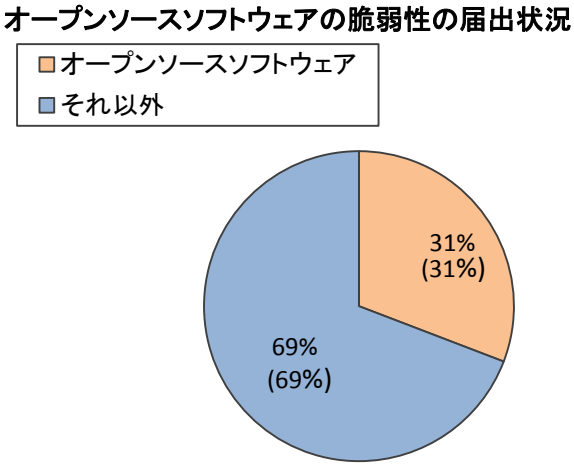


（過去2年間の届出内訳）

図2-3. 製品種類別の届出件数(四半期別推移)

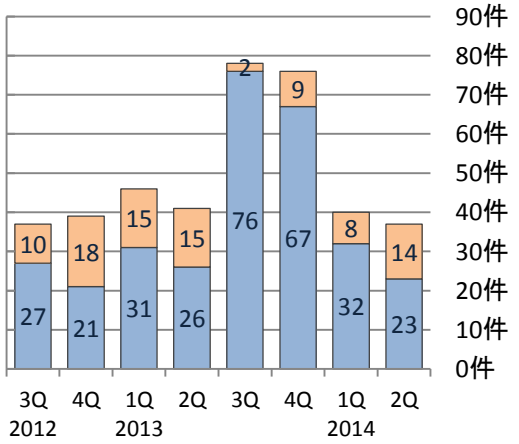
図 2-4、2-5 のグラフは、届出された脆弱性の製品ライセンスを「オープンソースソフトウェア」と「それ以外」で分類しています。図 2-4 は届出開始から今四半期末までの届出累計の分類割合を、図 2-5 は過去 2 年間の届出件数の推移を四半期別に示したものです。

累計では、オープンソースソフトウェアのが 31%を占めています。今四半期は、前四半期と比較してオープンソースソフトウェアの割合が増加しています。



（1,574件の内訳、グラフの括弧内は前四半期までの数字）

図2-4. オープンソースソフトウェアの届出件数の割合



（過去2年間の届出内訳）

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、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」で分類したものです。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 は届出開始から今四半期末までの届出について、公表までに要した日数の割合を示したものです。「スマホアプリ」に関する届出は、2013 年第 3 四半期と 2013 年第 4 四半期に急増しましたが、今四半期は 5 件に減少しました。

受理から 45 日以内に対策情報を公表した割合は「スマホアプリ」が 31%（前四半期は 40%）、「それ以外」が 34%（前四半期は 33%）でした。前四半期までは、「スマホアプリ」の方が早く対策される傾向にありましたが、今四半期は「それ以外」の対策がわずかに早くなっています。

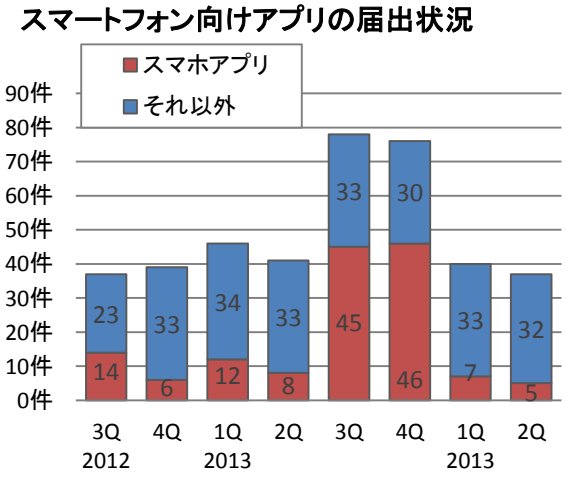


図2−6. スマートフォン向けアプリの届出件数（四半期別推移）

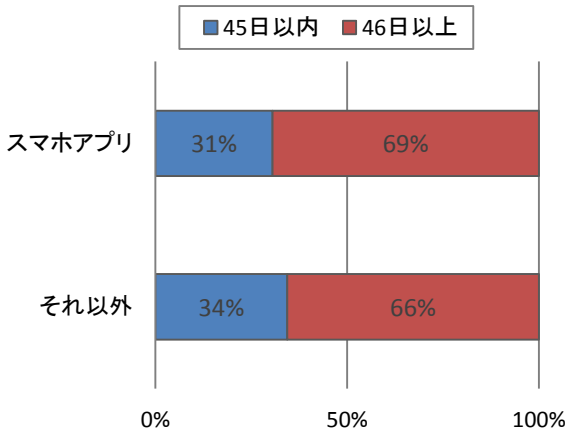


図2−7. .スマートフォン向けアプリとそれ以外の公表までの日数の割合

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 は届出開始から今四半期末までの届出累計原因別割合を、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たものです。累計では、「ウェブアプリケーションの脆弱性」が過半数を占めており、今四半期の届出件数も「ウェブアプリケーションの脆弱性」が最も多くなりました。

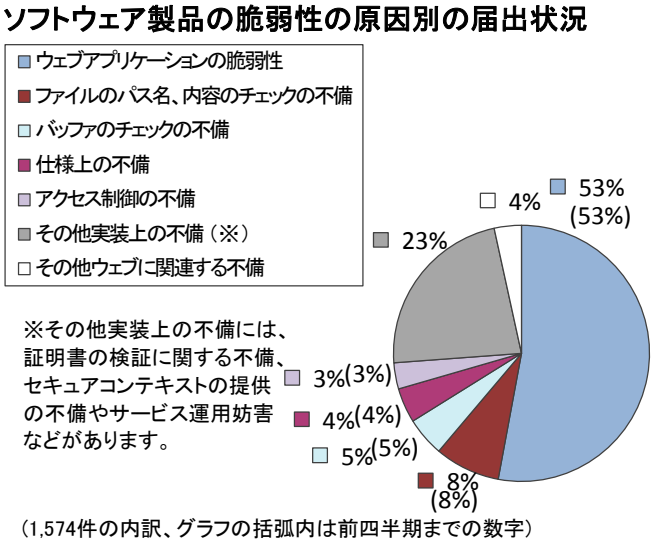


図2−8. 脆弱性の原因別の届出件数の割合

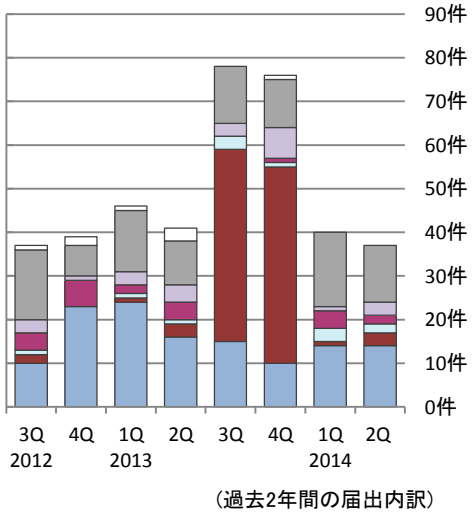
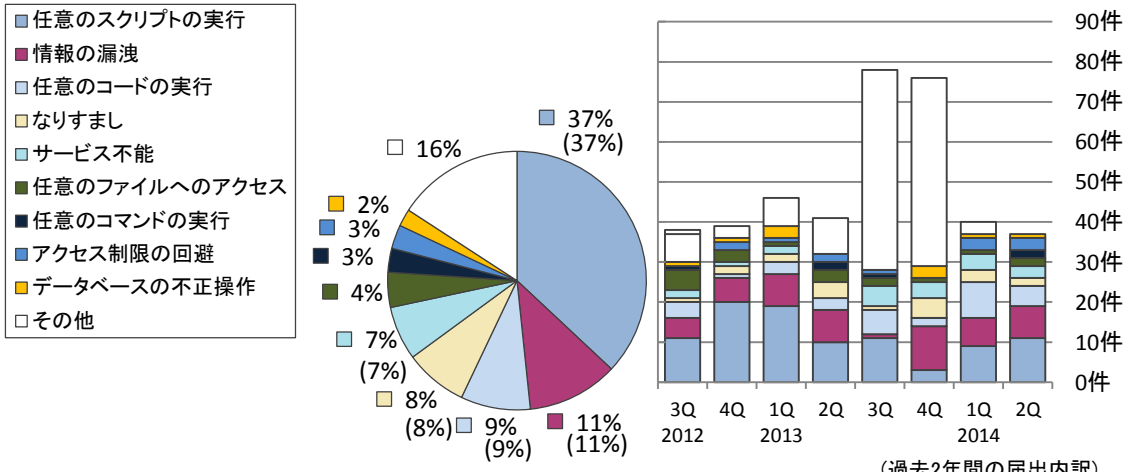


図2−9. 脆弱性の原因別の届出件数(四半期別推移)

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 は届出開始から今四半期末までの累計を脅威別の割合を、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たものです。今四半期は、「任意のスクリプト実行」が最も多く届出されましたが、累計でも、「任意のスクリプトの実行」が最も多く、全体の 37%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



（1,574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、情報の提供元別の 2 種類の脆弱性関連情報を、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[*11]。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 年分を四半期別の推移で示したものです。

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
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	29 件	880 件
②	海外 CSIRT 等と連携して公表したもの	39 件	1,099 件
	合計	68 件	1,979 件

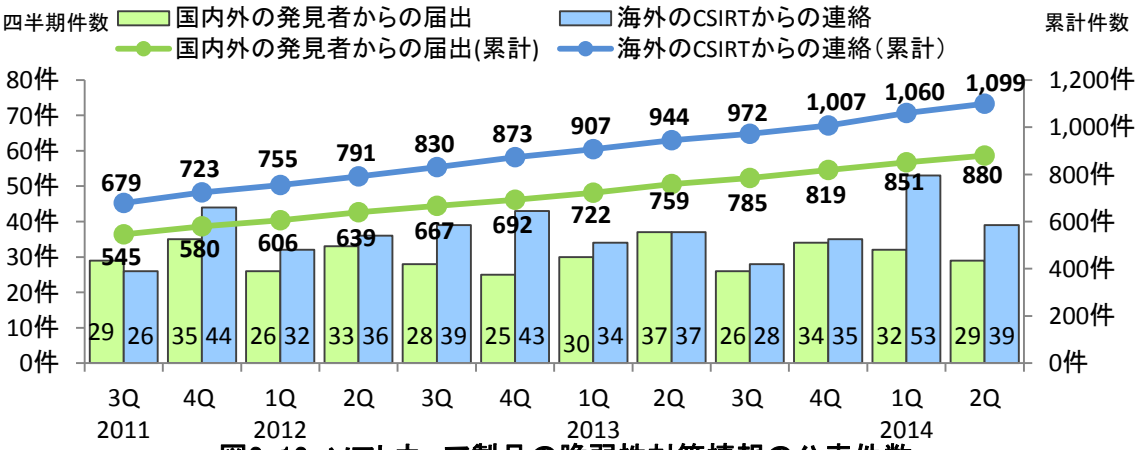


図2−12. ソフトウェア製品の脆弱性対策情報の公表件数

（1） 国内外の発見者および製品開発者からの届出により、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公表した脆弱性（880 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。

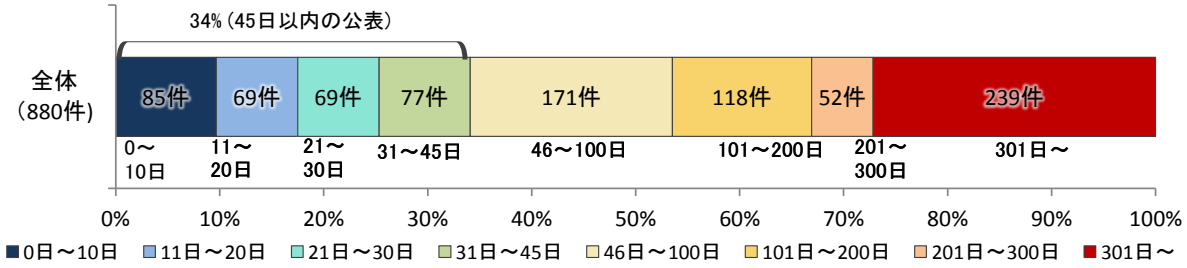


図2−13. ソフトウェア製品の脆弱性公表日数

表 2-2. 45 日以内に公表した件数の割合推移（四半期別）

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

[*11] JPCERT/CC 活動概要 Page15～21（http://www.jpcert.or.jp/pr/2014/PR20140710.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 9 件（表 2-3 の*2）、複数開発者・製品に影響がある脆弱性 2 件（表 2-3 の*3）、組込みソフトウェア製品の脆弱性が 2 件（表 2-3 の*4）ありました。

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「リモートサービスマネージャー」におけるサービス運用妨害(DoS)の脆弱性	管理ソフト「リモートサービスマネージャー」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「リモートサービスマネージャー」が稼働するサーバのリソースが枯渇する可能性がありました。	2014 年 4 月 18 日	7.1
2 (*1) (*3)	「Apache Struts」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開発支援フレームワーク「Apache Struts」には、ClassLoader が操作可能な脆弱性がありました。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 4 月 25 日	7.5
3 (*4)	「CN8000」におけるサービス運用妨害（DoS）の脆弱性	リモートアクセスユニット「CN8000」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「CN8000」を使用したシステムを応答不能な状態にされる可能性がありました。	2014 年 6 月 4 日	7.8
4 (*2)	複数のジャストシステム製品同梱のオンラインアップデートプログラムに任意のコード実行可能な脆弱性	複数のジャストシステム製品に同梱されているオンラインアップデートプログラムには電子署名の検証不備の問題がありました。このため、第三者により任意のコードが実行されてしまう可能性がありました。	2014 年 6 月 11 日	7.6
5 (*1) (*2)	「TERASOLUNA Server Framework for Java」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開発支援フレームワーク「TERASOLUNA Server Framework for Java(Web)」には、Apache Struts 1.2.9 の脆弱性に起因する 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 6 月 17 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	「SD Card Manager」におけるディレクトリ・トラバーサルの脆弱性	Android 用ファイル展開・管理ソフト「SD Card Manager」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 4 月 11 日	4.3
7	Android 版「CamiApp」における Content Provider のアクセス制限不備の脆弱性	Android 用データ管理ソフト「CamiApp」の Content Provider には、アクセス制限不備の脆弱性がありました。このため、第三者により当該製品のデータベースに格納された情報が、漏えいしたり改ざんされたりする可能性がありました。	2014 年 4 月 14 日	4.0
8 (*1)	「Redmine」におけるオープンリダイレクトの脆弱性	プロジェクト管理ソフト「Redmine」には、オープンリダイレクトの脆弱性がありました。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。	2014 年 4 月 16 日	4.3

項番	脆弱性	セキュリティ上の問題点	JVN 公表日	CVSS 基本値
9	「AndExplorer」におけるディレクトリ・トラバーサルの脆弱性	Android 用ファイル展開・管理ソフト「AndExplorer」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 4 月 18 日	4.3
10 (*2)	サイボウズ「リモートサービスマネージャー」におけるセッション固定の脆弱性	管理ソフト「リモートサービスマネージャー」には、セッション固定の脆弱性がありました。このため、第三者によりユーザになりすまされる可能性がありました。	2014 年 4 月 18 日	5.8
11 (*2)	東芝テック製「e-Studio シリーズ」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	複合機「e-Studio シリーズ」のウェブ管理画面には、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。	2014 年 4 月 18 日	4.0
12	「intra-mart」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開発支援フレームワーク「intra-mart」には、オープンリダイレクトの脆弱性がありました。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。	2014 年 5 月 8 日	4.3
13 (*1) (*3)	「OpenSSL」における Change Cipher Spec メッセージの処理に脆弱性	暗号通信ライブラリ「OpenSSL」には、初期 SSL/TLS ハンドシェイクにおける Change Cipher Spec メッセージの処理に脆弱性が存在しました。このため、サーバとクライアント間の SSL/TLS 通信が、中間者攻撃によって解読されたり、改ざんされたりする可能性がありました。	2014 年 6 月 6 日	4.0
14	「C-BOARD Moyuku」におけるクロスサイト・スクリプティングの脆弱性	電子掲示板ソフトウェア「C-BOARD Moyuku」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 6 月 11 日	4.3
15 (*1)	「Spring Framework」におけるディレクトリ・トラバーサルの脆弱性	ウェブアプリケーション開発支援フレームワーク「Spring Framework」には、ディレクトリ・トラバーサルの脆弱性がありました。このため、第三者によりサーバ上の任意のファイルにアクセスされる可能性がありました。	2014 年 6 月 13 日	5.0
16 (*2)	「SEIL」シリーズにおけるサービス運用妨害(DoS)の脆弱性	ルータ製品「SEIL」シリーズには、サービス運用妨害(DoS)の脆弱性がありました。このため、第三者により PPPAC 機能を用いて接続したセッションを切断されたり、接続の受付を停止させられたりする可能性がありました。	2014 年 6 月 13 日	5.0
17	Android 版アプリ「JR 東日本アプリ」における SSL サーバ証明書の検証不備の脆弱性	Android 版アプリ「JR 東日本アプリ」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 6 月 18 日	4.0
18 (*1)	「Usermin」における OS コマンド・インジェクションの脆弱性	ウェブメール管理ソフト「Usermin」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、第三者によって任意のコマンドを実行される可能性がありました。	2014 年 6 月 20 日	6.8
19 (*1)	「Usermin」におけるクロスサイト・スクリプティングの脆弱性	ウェブメール管理ソフト「Usermin」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 6 月 20 日	4.3

項番	脆弱性	セキュリティ上の問題点	JVN 公表日	CVSS 基本値
20 (*1)	WordPress 用プラグイン「Login rebuilder」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「Login rebuilder」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。	2014 年 6 月 24 日	4.0
21 (*2)	「Sophos Disk Encryption」における認証不備の脆弱性	ハードディスク暗号化ソフトウェア「Sophos Disk Encryption」には、認証不備の脆弱性がありました。このため、第三者によりコンピュータを操作される可能性がありました。	2014 年 6 月 24 日	4.7
22	「Web 給金帳」におけるクロスサイト・スクリプティングの脆弱性	明細書の電子化ソフト「Web 給金帳」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 6 月 25 日	4.3
23	「Web 給金帳」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	明細書の電子化ソフト「Web 給金帳」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。	2014 年 6 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				
24 (*2)	「サイボウズ ガルーン」の電話メモ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」の電話メモ機能には、ユーザからの入力を処理する部分に不備がありました。このため、第三者によりサービス運用妨害(DoS)状態にされる可能性がありました。	2014 年 4 月 30 日	3.5
25 (*2)	「サイボウズ ガルーン」の API 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 ガルーン」の API 利用時には、アクセス制限回避が可能な脆弱性がありました。このため、第三者により変更権限のないスケジュール情報を削除される可能性がありました。	2014 年 4 月 30 日	3.5
26 (*1)	「SOY CMS」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「SOY CMS」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 6 月 4 日	2.6
27 (*4)	Android 版アプリ「050 plus」における情報管理不備の脆弱性	Android 版アプリ「050 plus」には、当該製品が扱う情報の一部をシステムログに出力する問題が存在します。このため、Android 端末のログ情報を閲覧する権限のあるアプリケーションによって、当該製品が記録している情報の一部を取得される可能性がありました。	2014 年 6 月 17 日	2.6
28 (*1)	「Webmin」におけるクロスサイト・スクリプティングの脆弱性	ウェブベースのシステム管理ソフト「Webmin」には、ウェブページを出力する際の処理に問題がありました。このため、第三者によりウェブページにスクリプトを埋め込まれる可能性がありました。項番 29 とは異なる問題です。	2014 年 6 月 20 日	3.5
29 (*1)	「Webmin」におけるクロスサイト・スクリプティングの脆弱性	ウェブベースのシステム管理ソフト「Webmin」には、"referrer checking"が無効に設定されている場合において、ウェブページを出力する際の処理に問題がありました。このため、第三者によりウェブページにスクリプトを埋め込まれる可能性がありました。項番 28 とは異なる問題です。	2014 年 6 月 20 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 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 39 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において、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、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. 海外 CSIRT 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	Pearson eSIS 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
2	ZyXEL P660 シリーズにサービス運用妨害 (DoS) の脆弱性	注意喚起として掲載
3	Huawei Echo Life 光ルータ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
4	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
5	Websense TRITON Unified Security Center に情報漏えいの脆弱性	注意喚起として掲載
6	OpenSSL の heartbeat 拡張に情報漏えいの脆弱性	複数製品開発者へ通知
7	J2K-Codec に複数の脆弱性	注意喚起として掲載
8	Microsoft Office file format converter にメモリ破損の脆弱性	注意喚起として掲載
9	ZyXEL Wireless N300 NetUSB Router に複数の脆弱性	注意喚起として掲載
10	Fortinet FortiADC 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	Amtelco miSecureMessages に認証不備の脆弱性	注意喚起として掲載
12	PivotX に複数の脆弱性	注意喚起として掲載
13	PaperThin CommonSpot に複数の脆弱性	注意喚起として掲載
14	Ontario Systems Artiva Agency に認証不備の脆弱性	注意喚起として掲載
15	Xangati ソフトウェア製品に複数の脆弱性	注意喚起として掲載
16	Openfire にサービス運用妨害 (DoS) の脆弱性	注意喚起として掲載
17	Toshiba 4690 Operating System に脆弱性	特定製品開発者へ通知
18	IBM Notes および IBM Domino に問題	注意喚起として掲載
19	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
20	POCO C++ Libraries の NetSSL ライブラリにおけるワイルドカード証明書を適切に検証しない脆弱性	注意喚起として掲載
21	Internet Explorer に解放済みメモリ使用 (use-after-free) の脆弱性	緊急案件として掲載 特定製品開発者へ通知
22	Ignite Realtime Smack API に複数の脆弱性	注意喚起として掲載
23	Google 検索アプライアンス ダイナミック ナビゲーション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
24	Caldera に複数の脆弱性	注意喚起として掲載
25	Fortinet Fortiweb 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	注意喚起として掲載
26	Juniper ScreenOS におけるサービス運用妨害 (DoS) の脆弱性	注意喚起として掲載
27	Hanvon Face ID に認証欠如の問題	注意喚起として掲載
28	Internet Explorer 8 CMarkup における解放済みメモリ使用の脆弱性	特定製品開発者へ通知
29	Bizagi BPM Suite に複数の脆弱性	注意喚起として掲載
30	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
31	Alfresco Enterprise 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
32	Huawei E303 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	注意喚起として掲載

項番	脆弱性	対応状況
33	Dell ML6000 と Quantum Scalar i500 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
34	複数製品の UEFI ファームウェアの実装に脆弱性	注意喚起として掲載
35	Cisco AsyncOS 製品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
36	Symantec Web Gateway に複数の脆弱性	注意喚起として掲載
37	F5 ARX Data Manager に SQL インジェクションの脆弱性	注意喚起として掲載
38	Belkin N150 における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
39	SpamTitan 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

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 6 月末までに、「連絡不能開発者」と位置づけて取扱った 165 件の処理状況の推移を示したものです。

2014 年 6 月末時点での処理状況は、165 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 21 件（前四半期は 21 件）、連絡が取れずに「連絡不能開発者一覧」に公表しているのは 144 件（前四半期は 131 件）です。

製品開発者から連絡があり調整を再開した 21 件の内訳は、今四半期に新たに調整が再開した「調整中」は 0 件で 11 件が継続して調整中、製品開発者と調整再開後に本制度における取扱いを終了した「調整完了」は 2 件増加し、累計 10 件となりました。

「連絡不能開発者一覧」に公表中の 144 件の内訳は、前期から繰り越された連絡不能案件 131 件と今四半期に新たに製品開発者名を公表した「新規公表」が 13 件です。前四半期に新規公表した 7 件は連絡が取れない状態が継続したため製品情報を追加公表し、連絡不能「追加情報公表」となりました。

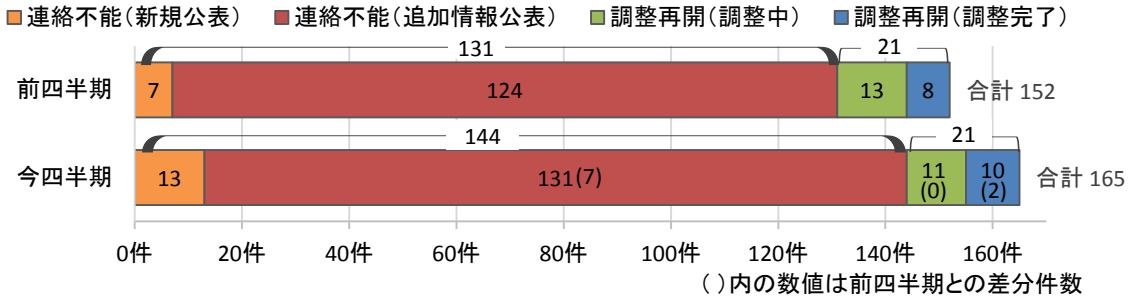


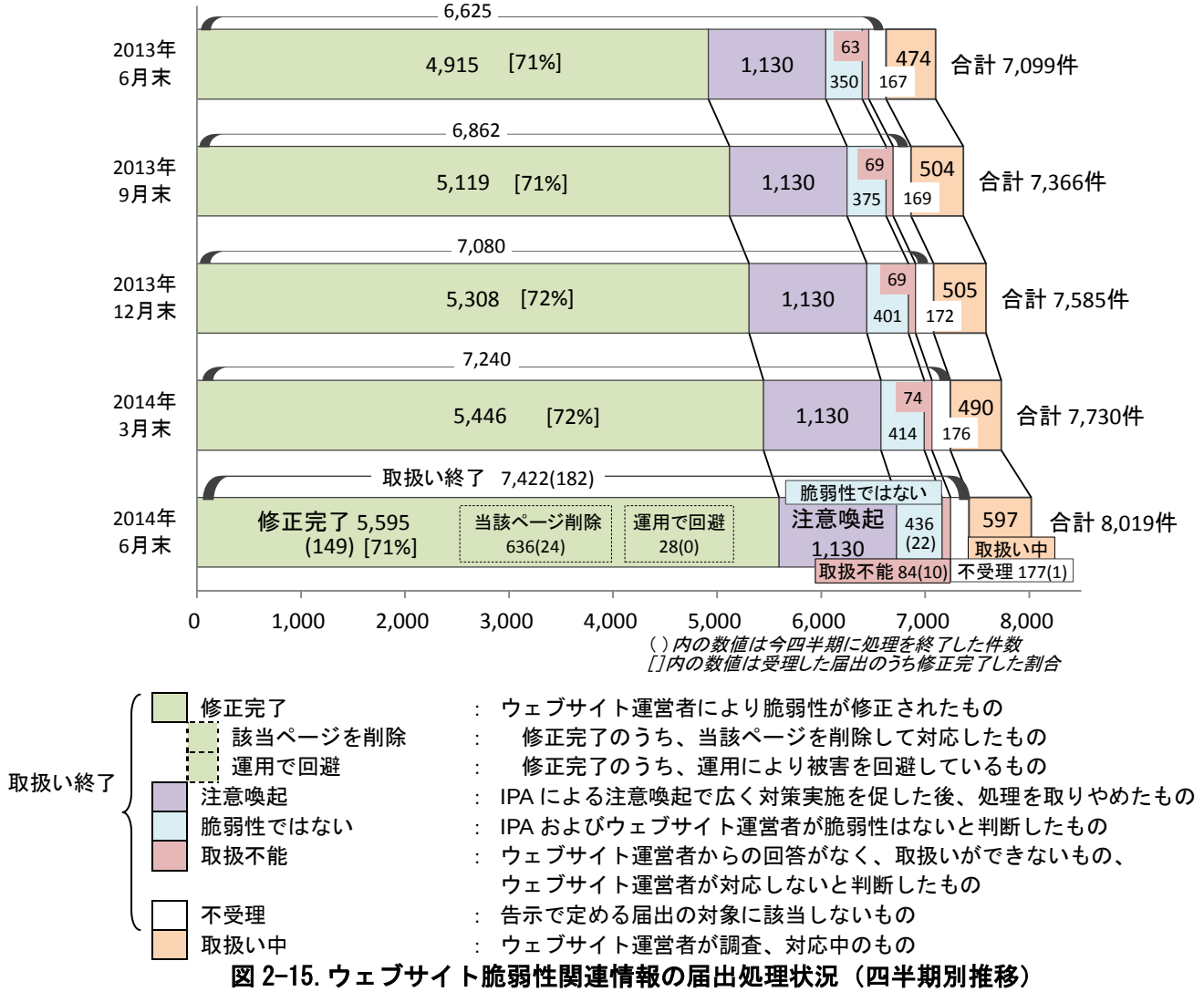
図2-14. 連絡不能開発者一覧の処理状況

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、はウェブサイト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。2014 年 6 月末時点の届出の累計は 8,019 件で、今四半期中に取扱いを終了したもの 182 件（累計 7,422 件）でした。このうち「修正完了」したものは 149 件（累計 5,595 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 22 件（累計 436 件）でした。処理の取りやめとは、例えばウェブサイトで利用しているソフトウェア製品の修正プログラムが適用されていないなど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、届出以外のウェブサイト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ます。なお、ウェブサイト運営者への連絡は通常メールで、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。ウェブサイト運営者と連絡が取れない場合などは「取扱不能」案件となり、今期その件数は 10 件（累計 84 件）でした。「不受理」としたものは 1 件（累計 177 件）でした。取扱いを終了した累計 7,422 件のうち「注意喚起」「取扱不能」「不受理」を除く累計 6,031 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」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 24 件（累計 636 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 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
  - 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 2-15. ウェブサイト脆弱性関連情報の届出処理状況（四半期別推移）

以下に、届出受付開始から今四半期までに届出のあったウェブサイトの脆弱性関連情報 8,019 件のうち、不受理を除いた 7,842 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 2-16 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「企業（株式・非上場）」が最も多く、企業が全体の約 7 割を占めています。

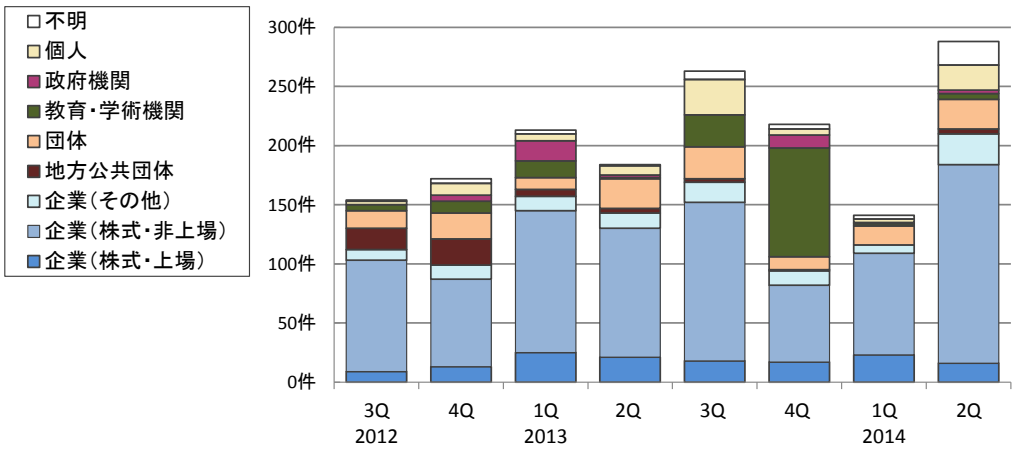


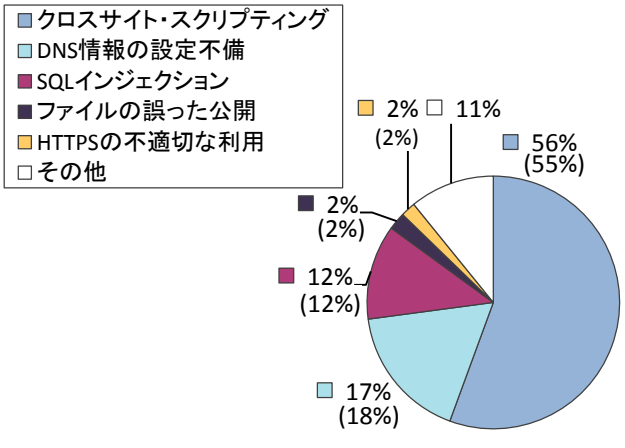
図2-16. 運営主体の種類別の届出件数(四半期別推移)

2-2-3. 脆弱性の種類・脅威別届出

図 2-17、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 (*12) 。

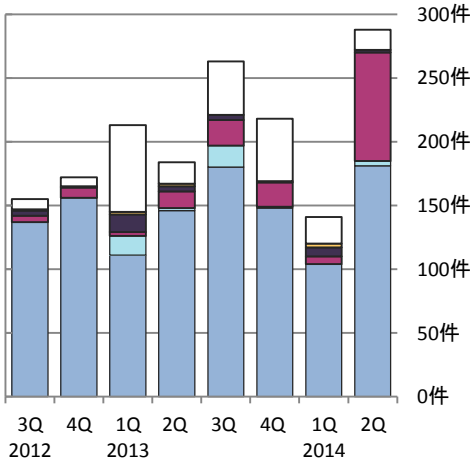
累計では、「クロスサイト・スクリプティング」だけで 56%を占めており、次いで「DNS 情報の設定不備」「SQL インジェクション」となっています。「DNS 情報の設定不備」は累計 18%ありますが、2008 年から 2009 年にかけて多く届出されたのが反映されたものです。今四半期は「SQL インジェクション」の届出が急増しています。なお、この統計は本制度における届出の傾向であり、世の中に存在する脆弱性の傾向と必ずしも一致するものではありません。

ウェブサイトの脆弱性の種類別の届出状況



(7,842件の内訳、グラフの括弧内は前四半期までの数字)

図2-17. 脆弱性の種類別の届出件数の割合



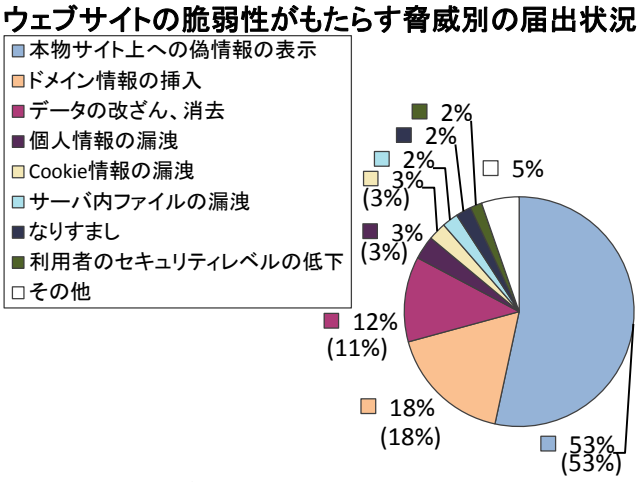
(過去2年間の届出内訳)

図2-18. 脆弱性の種類別の届出件数 (四半期別推移)

(*12) 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。

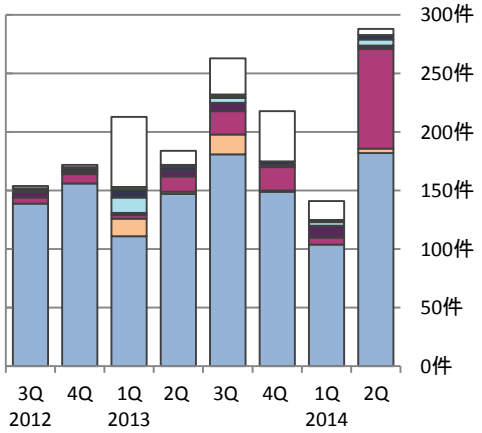
図 2-19、図 2-20 のグラフは、届出された脆弱性がもたらす脅威を示しています。図 2-19 は届出開始から今四半期末までの届出の割合を、図 2-20 は過去 2 年間の届出件数の推移を四半期別に示したものです。

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、「SQL インジェクション」の届出の増加に伴い「データの改ざん、消去」が増加しています。



(7,842件の内訳、グラフの括弧内は前四半期までの数字)

図2-19. 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2-20. 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 2-21 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 2 四半期に修正を完了した 149 件のうち 95 件（64%）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（138 件中 78 件（57%））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関連情報を通知してから、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たものです。

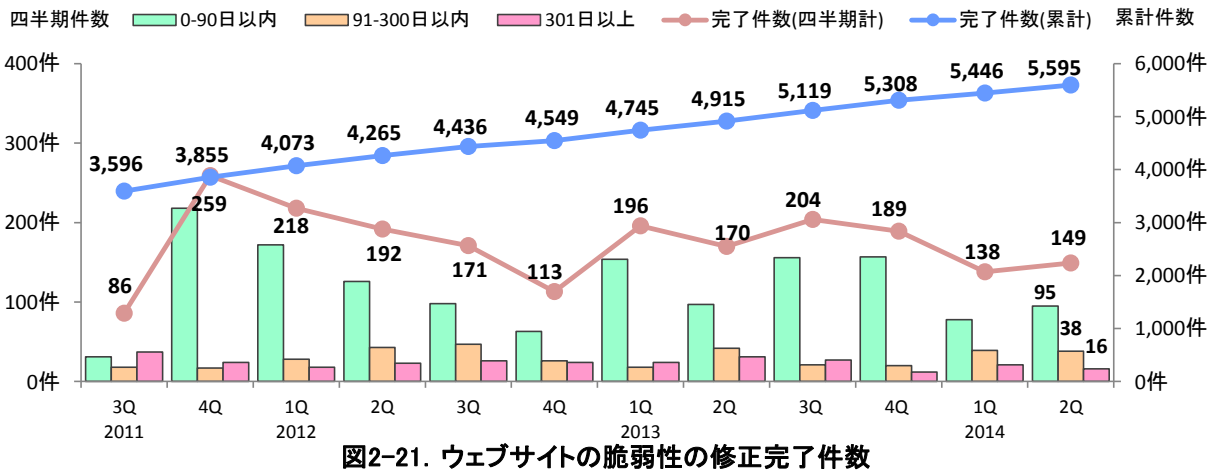


図2-21. ウェブサイトの脆弱性の修正完了件数

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 3Q	4Q	2012 1Q	2Q	3Q	4Q	2013 1Q	2Q	3Q	4Q	2014 1Q	2Q
修正完了件数	3,596	3,855	4,073	4,265	4,436	4,549	4,745	4,915	5,119	5,308	5,446	5,595
90 日以内の件数	2,316	2,534	2,706	2,832	2,930	2,993	3,147	3,244	3,400	3,557	3,635	3,730
90 日以内の割合	64%	66%	66%	66%	66%	66%	66%	66%	66%	67%	67%	67%

図 2-22、図 2-23 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[(*13)]。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。

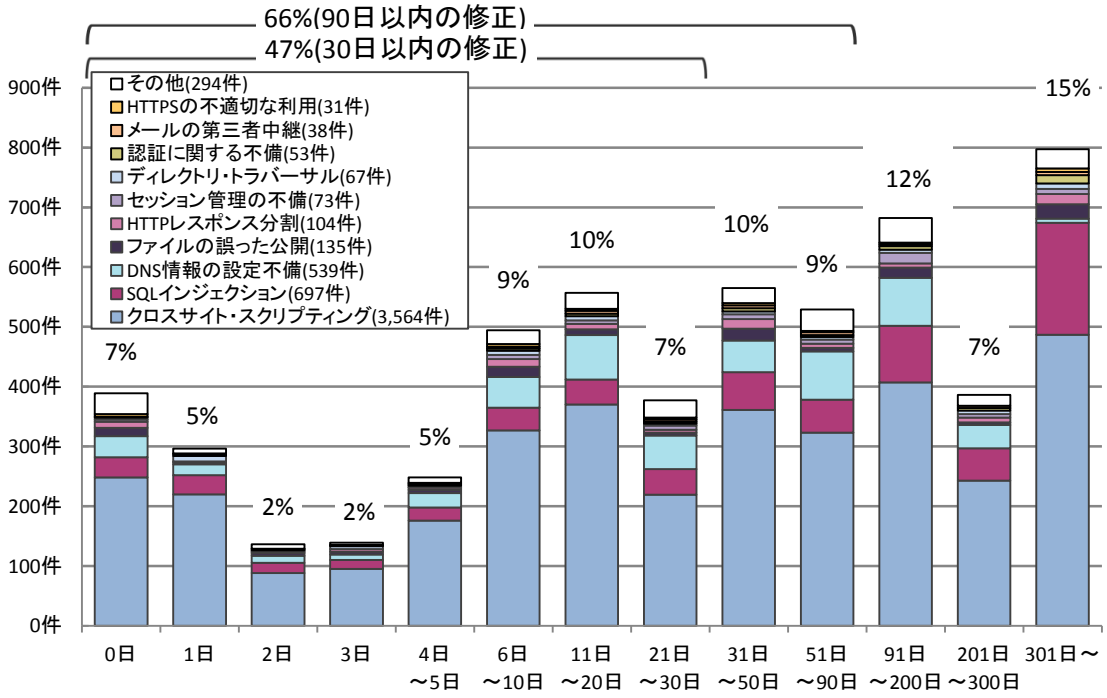


図2-22. ウェブサイトの修正に要した日数

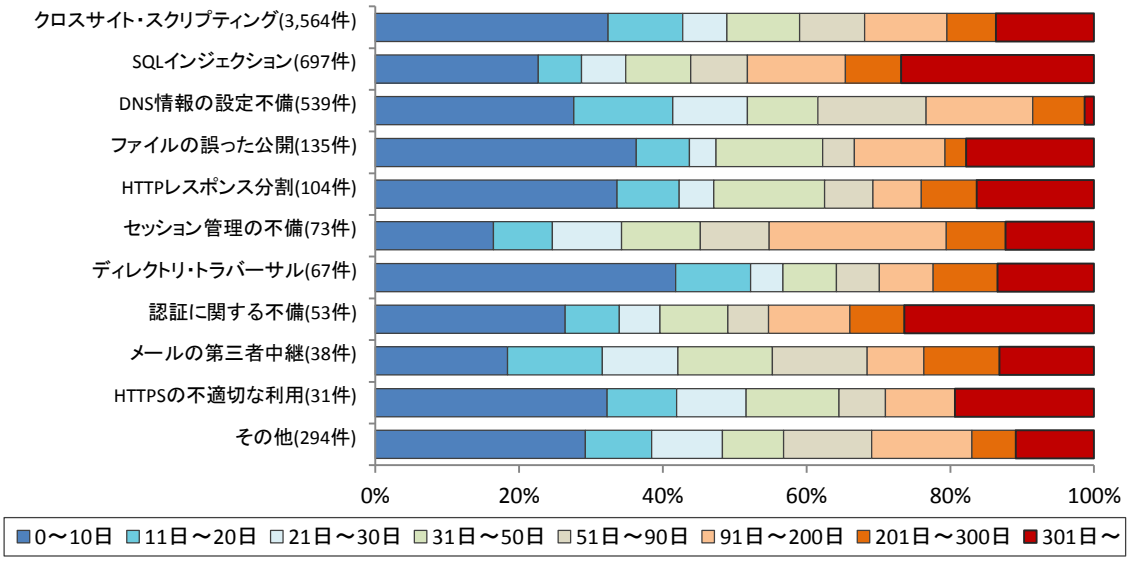


図2-23. ウェブサイトの修正に要した脆弱性種類別の日数の傾向

(*13) 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、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 48 件、200 日から 299 日のものは 43 件など、これらの合計は 353 件（前四半期は 357 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 SQL インジェクションのように深刻度の高い脆弱性も多く含まれています。

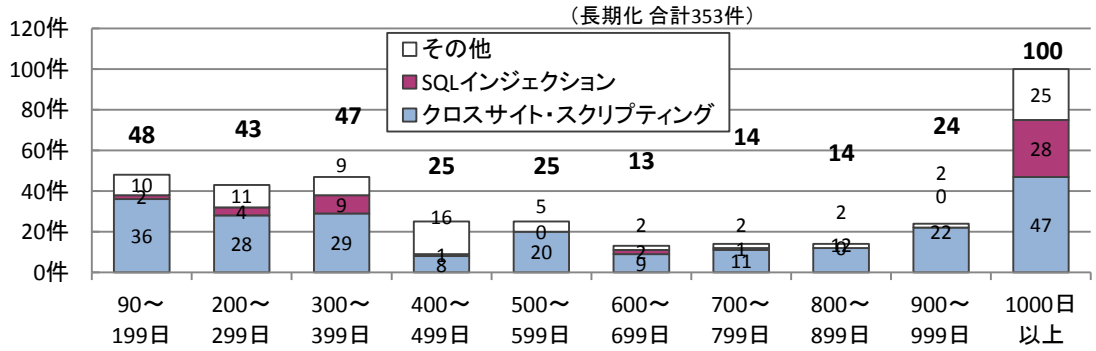


図2-24. 取扱いが長期化(90日以上経過)しているウェブサイトの経過日数と脆弱性の種類

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 2-6. 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 3Q	4Q	2013 1Q	2Q	3Q	4Q	2014 1Q	2Q
取扱い中の件数	423	473	474	473	503	504	489	597
長期化している件数	302	296	301	307	302	358	357	353
長期化している割合	71%	63%	64%	65%	60.0%	71%	73%	59%

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の期間は第三者に漏れないよう、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 想定された脅威
1	アクセス制御の不備	アクセス制御を行うべき個所において、アクセス制御が欠如している。	設定情報の漏洩 通信の不正中継 なりすまし 任意のスクリプトの実行 認証情報の漏洩
2	ウェブアプリケーションの脆弱性	ウェブアプリケーションに対し、入力された情報の内容の解釈や認証情報の取扱い、出力時の処理に問題がある。「クロスサイト・スクリプティング」攻撃や「SQL インジェクション」攻撃などに利用されてしまう。	アクセス制限の回避 価格等の改ざん サービス不能 資源の枯渇 重要情報の漏洩 情報の漏洩 セッション・ハイジャック 通信の不正中継 なりすまし 任意のコマンドの実行 任意のスクリプトの実行 任意のファイルへのアクセス 認証情報の漏洩
3	仕様上の不備	RFC 等の公開された規格に準拠して、設計、実装した結果、問題が生じるもの。	サービス不能 資源の枯渇
4	証明書の検証に関する不備	ウェブブラウザやメールクライアントソフトに証明書を検証する機能が実装されていない、または、検証が正しく行われずに、偽の証明書を受けいれてしまう。	証明書の確認不能 なりすまし
5	セキュリティコンテキストの適用の不備	本来、厳しい制限のあるセキュリティコンテキストで取り扱うべき処理を、緩い制限のセキュリティコンテキストで処理してしまう。	アプリケーションの異常終了 情報の漏洩 任意のコードの実行 任意のスクリプトの実行
6	バッファのチェックの不備	想定外の長さの入力が行われた場合に、長さをチェックせずバッファに入力してしまう。「バッファオーバーフロー」攻撃に利用されてしまう。	サービス不能 任意のコードの実行 任意のコマンドの実行
7	ファイルのパス名、内容のチェックの不備	処理の際のパラメータとして指定されているディレクトリ名やファイル名、ファイルの内容をチェックしていない。任意のディレクトリのファイルを指定できてしまい、「ディレクトリ・トラバーサル」攻撃に利用されてしまう。また、破損したファイルや不正に書き換えられたファイルを処理した際に不具合が生じる。	アプリケーションの異常終了 サービス不能 資源の枯渇 任意のファイルへのアクセス 認証情報の漏洩

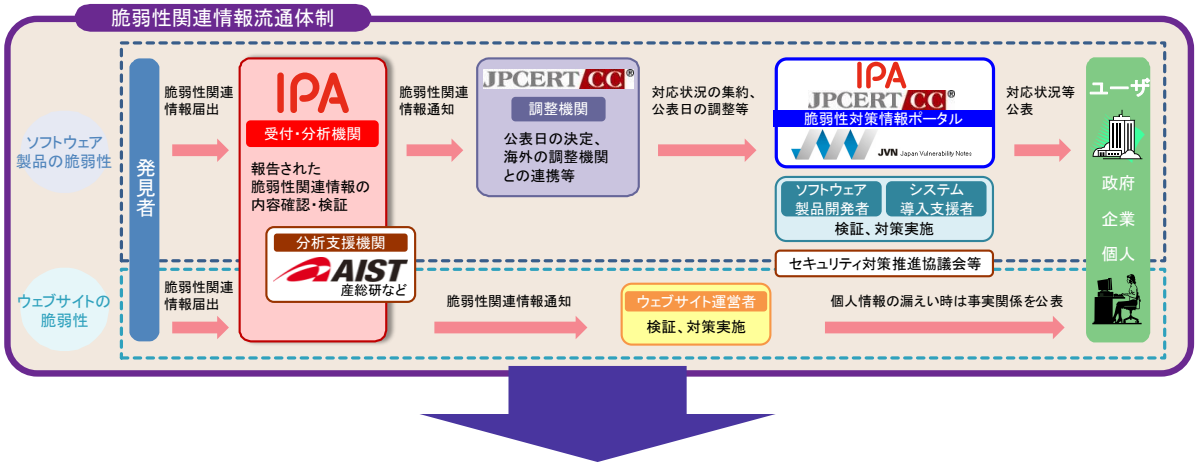
付表 2. ウェブサイトの脆弱性の分類

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

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

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

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



【期待効果】
①製品開発者及びウェブサイト運営者による脆弱性対策を促進
②不用意な脆弱性関連情報の公表や脆弱性の放置を抑制
③個人情報等需要情報の流出や重要システムの停止を予防

※IPA:独立行政法人情報処理推進機構, JPCERT/CC:一般社団法人 JPCERTコーディネーションセンター、産総研:独立行政法人 産業技術総合研究所