ソフトウェア等の脆弱性関連情報に関する届出状況

[2016 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届出状況について

日本における公的な脆弱性関連情報の取扱制度である「情報セキュリティ早期警戒パートナーシップ（本報告書では本制度と記します）」は、「ソフトウエア等脆弱性関連情報取扱基準（2004 年経済産業省告示第 235 号改め、2014 年経済産業省告示第 110 号）」に基づき、2004 年 7 月より運用されています。本制度において、独立行政法人情報処理推進機構（以下、IPA）と一般社団法人 JPCERT コーディネーションセンター（以下、JPCERT/CC）は、脆弱性関連情報の届出の受付や脆弱性対策情報の公表に向けた調整などの業務を実施しています。

本報告書では、2016 年 10 月 1 日から 2016 年 12 月 31 日までの、脆弱性関連情報に関する届出状況について記載しています。

独立行政法人情報処理推進機構 技術本部 セキュリティセンター
一般社団法人 JPCERT コーディネーションセンター
2017 年 1 月 25 日

目次

1. 2016 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は 12,916 件 ～

表 1-1 は本制度 (*1) における 2016 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を示しています。今四半期のソフトウェア製品に関する届出件数は 138 件、ウェブアプリケーション（以降「ウェブサイト」）に関する届出は 104 件、合計 242 件でした。届出受付開始からの累計は 12,916 件で、内訳はソフトウェア製品に関するもの 3,433 件、ウェブサイトに関するもの 9,483 件でウェブサイトに関する届出が全体の約 7 割を占めています。

表 1-1. 届出件数

分類	今四半期件数	累計
ソフトウェア製品	**138** 件	**3,433** 件
ウェブサイト	**104** 件	**9,483** 件
合計	**242** 件	**12,916** 件

図 1-1 は過去 3 年間の届出件数の四半期ごとの推移を示したものです。今四半期はウェブサイトよりもソフトウェア製品に関して多くの届出がありました。表 1-2 は過去 3 年間の四半期ごとの届出の累計および 1 就業日あたりの届出件数の推移です。今四半期の 1 就業日あたりの届出件数は 4.25 (*2) 件でした。

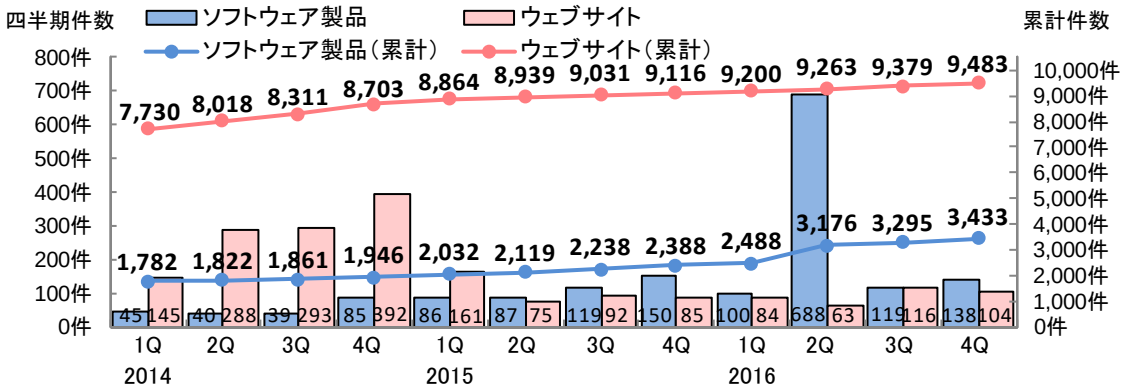


図1−1. 脆弱性の届出件数の四半期ごとの推移

表 1-2. 届出件数（過去 3 年間）

	2014 1Q	2Q	3Q	4Q	2015 1Q	2Q	3Q	4Q	2016 1Q	2Q	3Q	4Q
累計届出件数[件]	9,512	9,840	10,172	10,649	10,896	11,058	11,269	11,504	11,688	12,439	12,674	12,916
1 就業日あたり[件/日]	4.01	4.04	4.07	4.16	4.17	4.13	4.11	4.11	4.09	4.26	4.25	4.25

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

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

また、図 1-2 は、届出受付開始から 2016 年 12 月末までの届出件数の年ごとの推移です。過去、最も届出が多かったのは、2008 年（2,625 件）でした。2016 年はソフトウェア製品が 1,045 件、ウェブサイトが 367 件の合計 1,412 件でした。昨年に引き続きソフトウェア製品がウェブサイトの届出件数を上回り全体の 7 割以上を占め、ソフトウェア製品の届出件数が過去最多となりました。

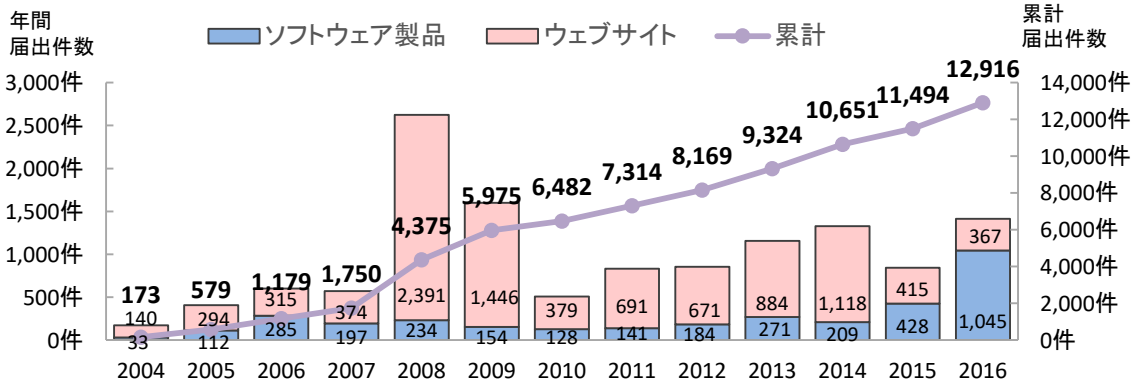


図1−2. 脆弱性関連情報の届出件数の年ごとの推移

1-2. 脆弱性の修正完了状況

～ ソフトウェア製品およびウェブサイトの修正件数は累計 8,261 件～

表 1-3 は今四半期、および届出受付開始から今四半期までのソフトウェア製品とウェブサイトの修正完了件数を示しています。ソフトウェア製品の場合、修正が完了すると JVN に公表しています（回避策の公表のみでプログラムの修正をしていない場合を含む）。

表 1-3. 修正完了（JVN 公表）

分類	今四半期件数	累計
ソフトウェア製品	**65** 件	**1,382** 件
ウェブサイト	**60** 件	**6,879** 件
合計	**125** 件	**8,261** 件

今四半期に JVN 公表したソフトウェア製品の件数は 65 件 (*3)（累計 1,382 件）でした。そのうち、20 件は製品開発者による自社製品の脆弱性の届出でした。なお、届出を受理してから JVN 公表までの日数が 45 日 (*4) 以内のものは 17 件（26%）でした。

また、修正完了したウェブサイトの件数は 60 件（累計 6,879 件）でした。修正を完了した 60 件のうち、ウェブアプリケーションを修正したものは 39 件（65%）、当該ページを削除したものは 21 件（35%）で、運用で回避したものは 0 件でした。なお、修正を完了した 60 件のうち、ウェブサイト運営者へ脆弱関連情報を通知してから 90 日 (*5) 以内に修正が完了したものは 43 件（72%）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（78 件中 46 件（59%））より増加しています。

また、図 1-3 は、届出開始から 2016 年 12 月末までの修正完了件数の年ごとの推移を示しています。過去、修正を完了した件数が最も多かったのは 2009 年の 1,401 件でした。2016 年は、ソフトウェア製品が 235 件、ウェブサイトが 314 件の合計 549 件でした。2016 年はソフトウェア製品の修正件数が最も多かった 1 年でした。

(*3) P.12 表 2-3 参照
(*4) JVN 公表日の目安は、脆弱性の取扱いを開始した日時から起算して 45 日後としています。
(*5) 対処の目安は、ウェブサイト運営者が脆弱性の通知を受けてから、3 ヶ月以内としています。

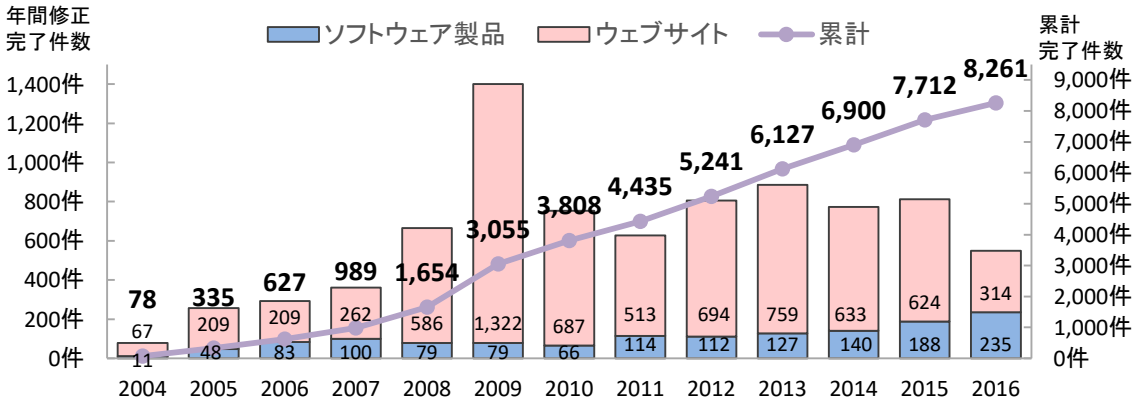


図1−3. 脆弱性関連情報の修正完了件数の年ごとの推移

1-3. 連絡不能案件の取扱状況

本制度では、調整機関から連絡が取れない製品開発者を「連絡不能開発者」と呼び、連絡の糸口を得るため、当該製品開発者名等を公表して情報提供を求めています(*6)。製品開発者名を公表後、3 ヵ月経過しても製品開発者から応答が得られない場合は、製品情報（対象製品の具体的な名称およびバージョン）を公表します。それでも応答が得られない場合は、情報提供の期限を追記します。情報提供の期限までに製品開発者から応答がない場合は、当該脆弱性情報の公表に向け、「情報セキュリティ早期警戒パートナーシップガイドライン」に定められた条件を満たしているかを公表判定委員会(*7)で審議します。公表が適当と判定された脆弱性情報は JVN に公表されます。

今四半期は、新たに 3 件について連絡が取れない製品開発者名を公表しました。また、3 件の製品開発者と連絡が取れ調整を再開しました。また、公表判定委員会での審議を経て、脆弱性情報が JVN に公表されたものはありませんでした。

2016 年 12 月末時点の連絡不能開発者の累計公表件数は 250 件、その内製品情報を公表しているものは 227 件となりました。

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

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

1-4. JVN で公表した脆弱性について

1-4-1. 複数の CMS プラグイン製品に含まれる脆弱性

～CMS 本体だけでなく、プラグイン製品も適切な脆弱性対策を～

2016 年は 190 件の脆弱性対策情報が JVN において公表し、そのうち CMS[8]本体の脆弱性は 8 件、プラグイン製品の脆弱性は 13 件でした(表 1-4-1)。CMS は一般的に、プラグイン製品を導入して機能を拡張するケースが多いため、プラグイン製品に対する脆弱性対策を実施することは重要です。

表 1-4-1. JVN で公表された CMS 本体、プラグイン製品の一覧

製品分類	項番	脆弱性	CVSS 基本値	JVN番号
CMS本体	1	baserCMS における OS コマンドインジェクションの脆弱性	6.5	JVN#69854312
	2	NetCommonsにおける権限昇格の脆弱性	5.5	JVN#00460236
	3	a-blog cms におけるクロスサイトスクリプティングの脆弱性	5.8	JVN#73166466
	4	a-blog cms におけるセッション管理不備の脆弱性	4.3	JVN#03975805
	5	Geeklog IVYWE版におけるクロスサイトスクリプティングの脆弱性	4.3	JVN#09836883
	6	baserCMS における複数の脆弱性	4.0	JVN#92765814
	7	SetucoCMSにおける複数の脆弱性	6.5	JVN#80157683
	8	DERAEMON-CMSにおけるクロスサイトスクリプティングの脆弱性	2.6	JVN#75396659
プラグイン製品	1	WordPress 用プラグイン「Ninja Forms」におけるPHPオブジェクト・インジェクションの脆弱性	6.8	JVN#44657371
	2	WordPress用プラグイン「Welcart e-Commerce」におけるPHPオブジェクト・インジェクションの脆弱性	6.8	JVN#47363774
	3	WordPress用プラグイン「WP-OliveCart」における複数の脆弱性	6.5	JVN#14567604
	4	WordPress用プラグイン「Welcart e-Commerce」におけるセッション管理不備の脆弱性	6.4	JVN#61578437
	5	WordPress用プラグイン「Welcart e-Commerce」におけるクロスサイト・スクリプティングの脆弱性	4.3	JVN#95082904
	6	WordPress用プラグイン「Welcart e-Commerce」におけるクロスサイト・スクリプティングの脆弱性	4.3	JVN#55826471
	7	WordPress用プラグイン「Markdown on Save Improved」におけるクロスサイト・スクリプティングの脆弱性	4.0	JVN#26026353
	8	WordPress用プラグイン「WP Favorite Posts」におけるクロスサイト・スクリプティングの脆弱性	2.6	JVN#86517621
	9	WordPressプラグイン「Nofollow Links」におけるクロスサイト・スクリプティングの脆弱性	2.6	JVN#13582657
	10	baserCMS用プラグイン「求人情報プラグイン」における複数の脆弱性	4.0	JVN#13288761
	11	baserCMS用プラグイン「メニューブックプラグイン」における複数の脆弱性	4.0	JVN#26627848
	12	baserCMS用プラグイン「ケースブックプラグイン」における複数の脆弱性	4.0	JVN#55801246
	13	「Geeklog IVYWE版」の複数のプラグインにおけるクロスサイト・スクリプティングの脆弱性	2.6	JVN#46087986

表 1-4-1 に記載されたプラグイン製品の脆弱性には、深刻度が高い PHP オブジェクト・インジェクションや SQL インジェクションの脆弱性も含まれています。これらの脆弱性を悪用された場合、任意の PHP コードを実行されたり、データベースを不正操作（取得、削除等）される可能性があり、プラグイン製品だけでなく CMS 本体にも影響が及び、ウェブページの改ざんや情報漏えいといった重大な被害が発生する場合があります(図 1-4-1)。

8 Content Management System の略称。インターネット上もしくはイントラネット上のウェブサイトのウェブページや画像などを「統合的」に管理し、ウェブサイトを構築するシステム。

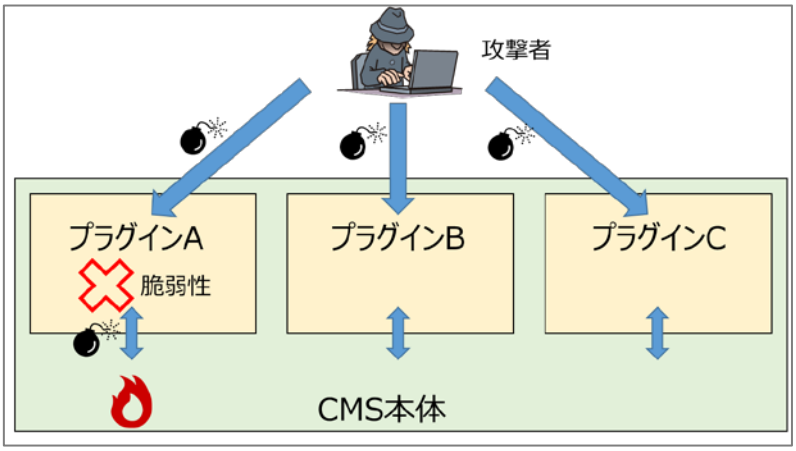


図 1-4-1. CMS プラグイン製品の脆弱性を悪用するイメージ図

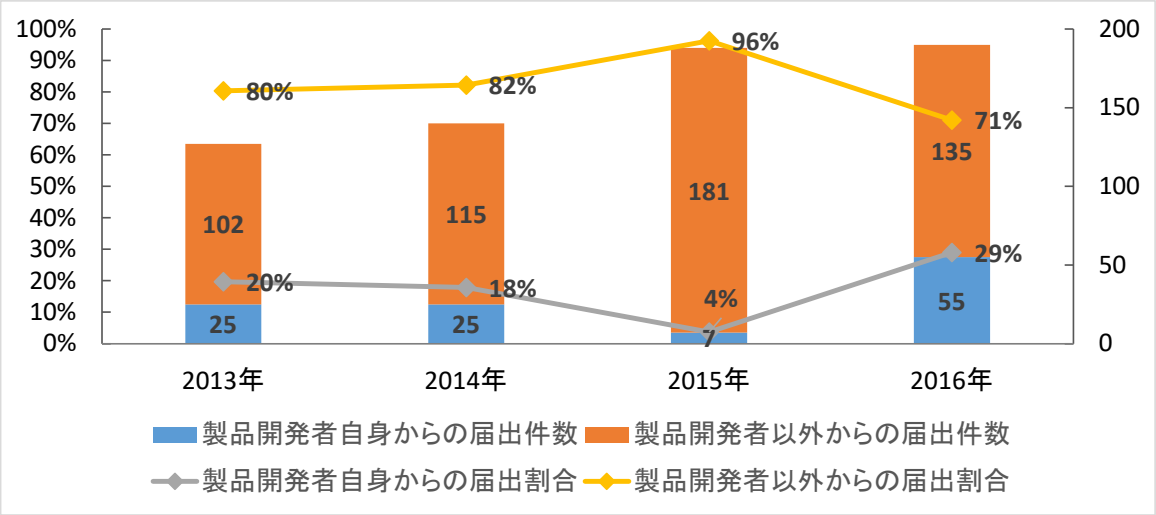
製品利用者は、CMS 本体だけでなく、利用しているプラグイン製品においても日頃から脆弱性対策情報を収集し、常に最新版のプラグイン製品を使うよう心がける必要があります。さらに、利用しているプラグイン製品の定期的な見直しを行い、利用していないプラグイン製品の削除といった運用も有効です。

なお、初期版のリリース以後ほとんどアップデートがされていないプラグイン製品は、脆弱性が放置されている可能性があり、注意が必要です。例えば、メンテナンス（バージョンアップ）が実施されている、または、リリースノート等で機能改善だけでなく脆弱性対策についても記載しているといった点も考慮して、プラグイン製品を選定し導入することが望ましいです。

1-4-2. ソフトウェア製品の自社届出件数の割合が過去最高件数

～製品開発者は積極的な脆弱性の対策と公表を～

2016 年で JVN 公表した脆弱性対策情報(190 件)のうち、55 件（約 30%）は、製品開発者自身（9 社）による自社製品の届出で、直近の 4 年間で件数が最も多く、割合も最も高くなりました(図 1-4-2)。近年では、脆弱性報奨金制度 [9]によって見つかった脆弱性対策情報を、一般利用者へ周知することを目的とし、製品開発者から本制度へ届出られていることが公表件数が増加した要因のひとつであると考えられます。



[9]製品開発者が自社製品の品質向上を主な目的として、ユーザ（バグハンター）による自社ソフトウェア製品における脆弱性の発見および報告を受付ける制度。製品開発者は、脆弱性の深刻度に応じて報奨金をユーザ（バグハンター）に支払う場合がある。

図 1-4-2. JVN で公表された製品開発者自身による届出件数の推移

JVN で公表された自社製品の届出 55 件のうち、CVSS 値が高い（深刻度 III）脆弱性は 4 件ありました(表 1-4-2)。

表 1-4-2. JVN で公表された製品開発者自身による届出（深刻度Ⅲ）

項番	脆弱性	CVSS 基本値
1	「SKYSEA Client View」において任意のコードが実行可能な脆弱性	10.0
2	「Deep Discovery Inspector」において任意のコードが実行可能な脆弱性	9.0
3	「WFS-SR01」において任意のコマンドを実行される脆弱性	7.5
4	「WFS-SR01」におけるアクセス制限不備の脆弱性	7.5

これら 4 件の脆弱性は、いずれも悪用された場合の影響が大きく、脆弱性の悪用が容易と考えられます。上記の項番 1 においては、製品開発者が脆弱性対策情報を公開するよりも前に、攻撃活動が観測されたことから、IPA では注意喚起を実施し、早急な対策の実施を呼びかけました [10]。なお、JPCERT/CC や警察庁セキュリティポータルサイト@police でも同様に注意喚起が行われました。悪用された場合の影響が大きい場合や、脆弱性の悪用が容易と考えられる脆弱性が見つかった場合、利用者に対して早急に対策実施を呼びかけ、被害を未然に防ぐことが、製品開発者のとるべき対応として重要となります。

製品開発者は自社製品に脆弱性が見つかった場合、修正を施すだけでなく、ウェブページ等で脆弱性対策情報を公開、周知する必要があります。これは、製品利用者に脆弱性対策を実施した事を周知しないと、脆弱性対策が実施されないためです。

さらに、JVN を活用して脆弱性対策情報を周知することで、より多くの製品利用者への周知することが可能です。

1-4-3. JVN で公表したソフトウェア製品種類ごとの内訳

～情報家電に潜む脆弱性に注意～

2012 年から 2016 年までの 5 年間で、755 件の脆弱性対策情報を JVN において公表しています。公表したソフトウェア製品を製品種類別に分類し、上位 5 種類を集計しています。 製品種類が、1 位のウェブアプリケーションソフトと 2 位のスマートフォン向けアプリケーションで、全体の約半数（49%）を占めています(図 1-4-3)。

順位	製品種類	件数
1	ウェブアプリケーションソフト	239 件（32%）
2	スマートフォン向けアプリ	126 件（17%）
3	グループウェア	80 件（11%）
4	アプリケーション開発・実行環境	61 件（8%）
5	ルータ	59 件（8%）

図 1-4-3. 2012 年から 2016 年の製品種類別公表件数上位 5 種類

5 位のルータにおいては、ルータ固有の機能に対する脆弱性ではなく、PC やスマートフォンのウェブブラウザなどからアクセス可能な管理用ウェブアプリケーションに対する脆弱性がほとん

[10] https://www.ipa.go.jp/security/ciadr/vul/20161222-jvn.html

どを占めています。このウェブアプリケーションの脆弱性が悪用されると、機器の設定を変更されたり、機器自体を乗っ取られたりするおそれがあります。

2016 年においては、ウェブカメラやフォトプレーヤーといった情報家電においても脆弱性対策情報を公表しています。近年は、冷蔵庫やエアコン、玄関の鍵など様々な機器をインターネットに接続し、遠隔地から操作を可能にする情報家電が普及し始めてきています。これらの情報家電においても、ウェブアプリケーションソフトが組み込まれていることが想定されます。

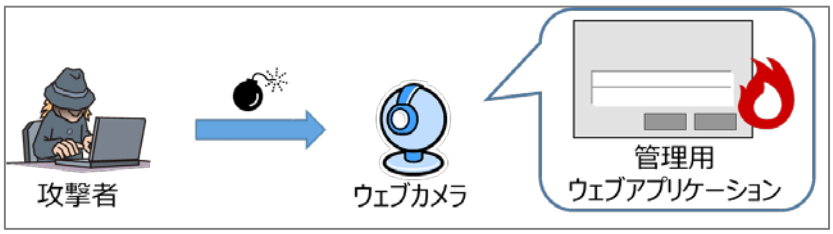


図 1-4-4. ウェブカメラの管理用ウェブアプリケーションの脆弱性を悪用するイメージ図

この様に、インターネットに接続する情報家電の普及に伴い、組み込まれているウェブアプリケーションの脆弱性が見つかることが、今後増加することと想定されるため、関係者は、次のように脆弱性対策を実施していく必要があります。

・製品開発者

PC 向けのウェブアプリケーションソフトと同じく、脆弱性対策を実施する必要があります。さらに、管理用ウェブアプリケーションの認証機能を強化する、不要なサービスは停止するといった対策を実施することで、攻撃者からの悪用を防ぐことができる可能性が高まります。また、ソフトウェアの自動更新といった機能、仕組みを導入することで、より効率的に製品利用者がソフトウェアの更新を実施することが期待できます。

・製品利用者

製品開発者が公開する脆弱性対策情報や JVN 等を日頃から確認し、製品開発者が提供するファームウェアのアップデートやパッチの適用を利用者自身が実施することによって、脆弱性を悪用した攻撃の被害を防ぐことができます。また、脆弱性を悪用されたことにより機器自体を乗っ取られた場合は、利用者自身が第三者に対する加害者となる場合があるため、脆弱性対策を実施する必要があります。

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 はソフトウェア製品の脆弱性届出の処理状況について、四半期ごとの推移を示しています。2016 年 12 月末時点の届出の累計は 3,433 件で、今四半期に脆弱性対策情報を JVN 公表したものは 65 件（累計 1,382 件）でした。製品開発者が JVN 公表を行わず「個別対応」したものは 0 件（累計 36 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 83 件）、「不受理」としたものは 12 件 (*11)（累計 376 件）、取扱い中は 1,556 件でした。1,556 件のうち、連絡不能開発者 (*12) 一覧へ新規に公表したものは 3 件で、2016 年 12 月末時点で 205 件が公表中です。

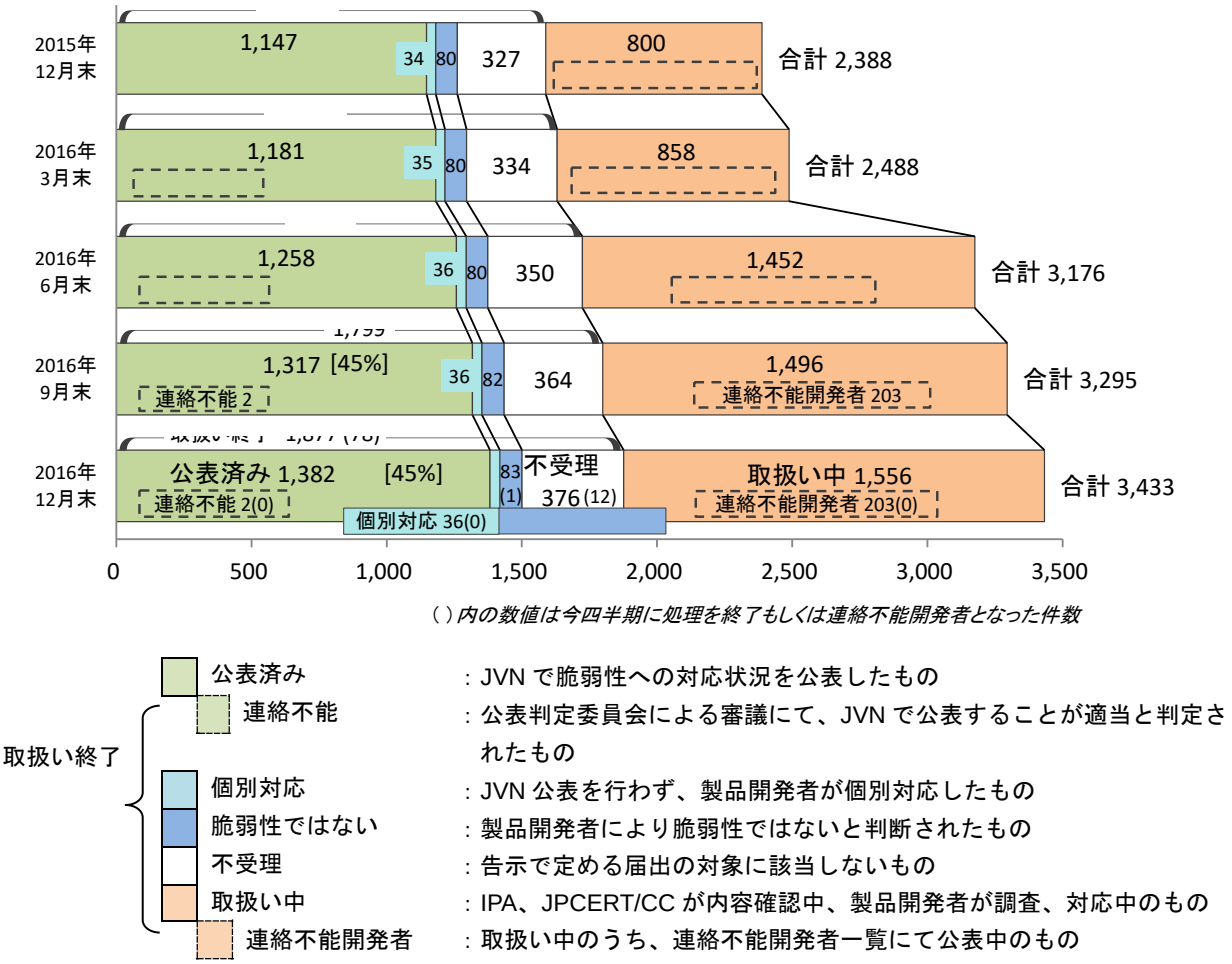


図 2-1. ソフトウェア製品脆弱性の届出処理状況（四半期ごとの推移）

(*11) 内訳は今四半期の届出によるもの 0 件、前四半期までの届出によるもの 12 件。

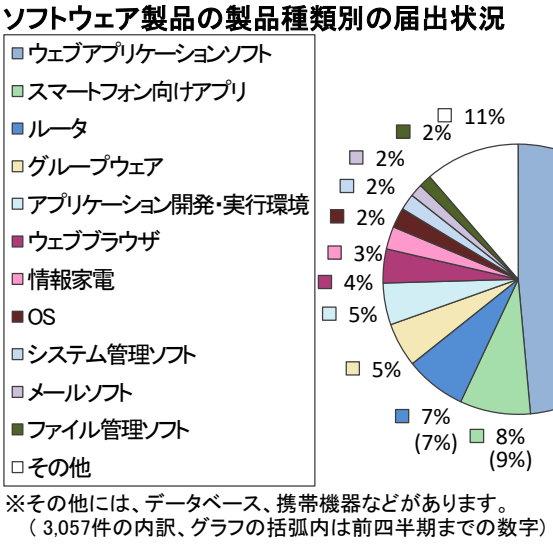
(*12) 連絡不能開発者一覧への公表および一覧からの削除が複数回行われた製品開発者の公表回数は、その累計を計上しています。

今までに届出のあったソフトウェア製品の脆弱性 3,433 件のうち、不受理を除いた件数は 3,057 件でした。以降、不受理を除いた届出について集計した結果を記載します。

2-1-2. ソフトウェア製品種類別届出件数

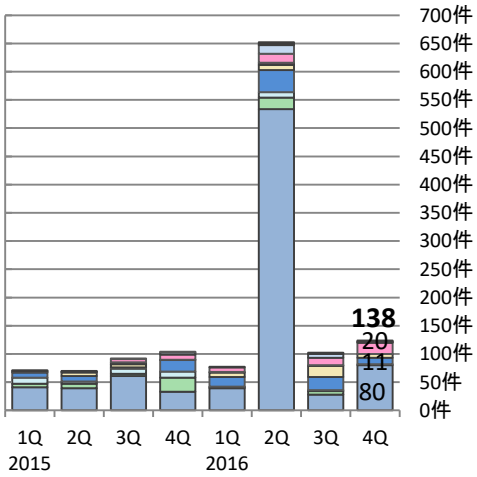
図 2-2、2-3 は、届出された脆弱性の製品種類別の内訳です。図 2-2 は製品種類別割合を、図 2-3 は過去 2 年間の届出件数の推移を四半期ごとに示したものです。

累計では、「ウェブアプリケーションソフト」が最も多く 49%となっています。今四半期の届出件数において「ウェブアプリケーションソフト（80 件）」が最も多く、次いで「情報家電（20 件）」「ルータ（11 件）」となっています。



※その他には、データベース、携帯機器などがあります。
（3,057件の内訳、グラフの括弧内は前四半期までの数字）

図2-2. 届出累計の製品種類別割合

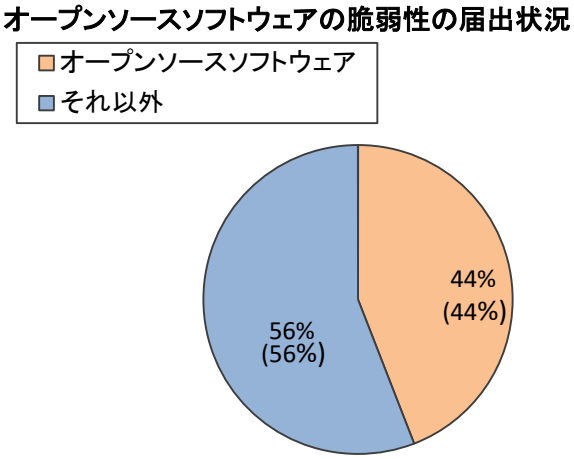


（過去2年間の届出内訳）

図2-3. 四半期ごとの製品種類別届出件数

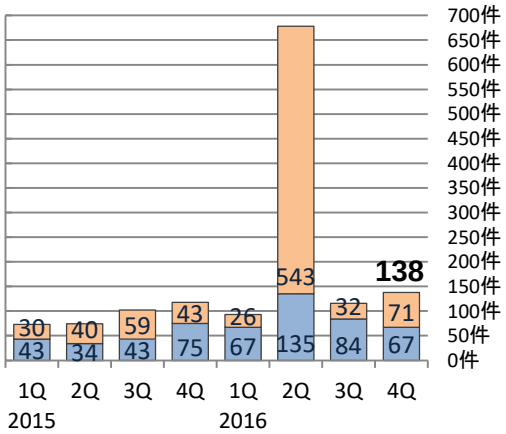
図 2-4、2-5 は、届出された製品をライセンスの形態により「オープンソースソフトウェア」（OSS）と「それ以外」で分類しています。図 2-4 は届出累計の分類割合を、図 2-5 は過去 2 年間の届出件数の推移を四半期ごとに示したものです。

オープンソースソフトウェアを除いた「それ以外」が、今四半期は 49%、累計では 56%を占めました。



（3,057件の内訳、グラフの括弧内は前四半期までの数字）

図2-4. 届出累計のオープンソースソフトウェア割合



（過去2年間の届出内訳）

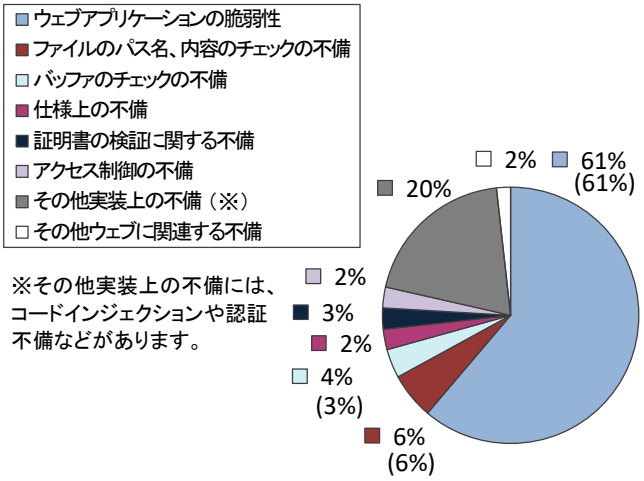
図2-5. 四半期ごとのオープンソースソフトウェア届出件数

2-1-3. 脆弱性の原因と影響別件数

図 2-6、2-7 は、届出された脆弱性の原因を示しています。図 2-6 は届出累計の脆弱性の原因別

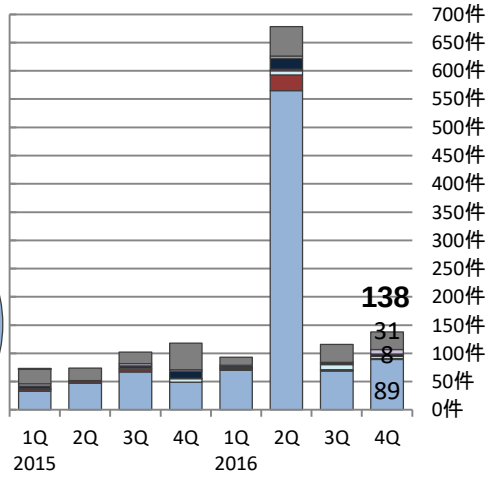
割合を、図 2-7 は過去 2 年間の原因別の届出件数の推移を四半期ごとに示しています。累計では、「ウェブアプリケーションの脆弱性」が過半数を占めています。今四半期も「ウェブアプリケーションの脆弱性（89 件）」が最も多く、次いで「その他実装上の不備（31 件）」「アクセス制御の不備（8 件）」となっています。

ソフトウェア製品の脆弱性の原因別の届出状況



（3,057件の内訳、グラフの括弧内は前四半期までの数字）

図2-6. 届出累計の脆弱性の原因別割合

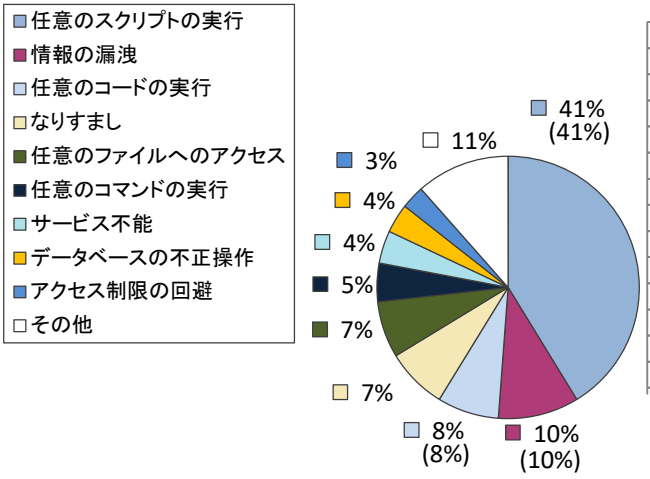


（過去2年間の届出内訳）

図2-7. 四半期ごとの脆弱性の原因別届出件数

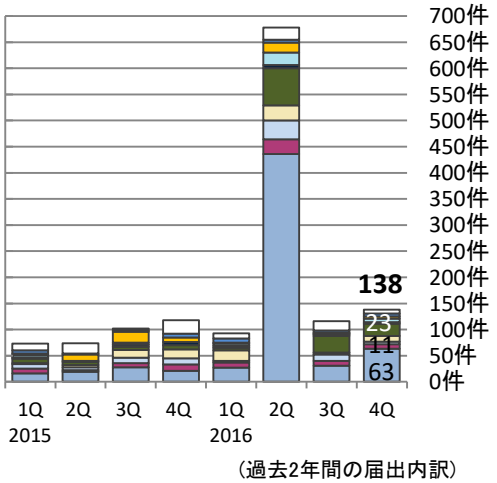
図 2-8、2-9 は、届出された脆弱性がもたらす影響を示しています。図 2-8 は届出累計の影響別割合を、図 2-9 は過去 2 年間の影響別届出件数の推移を四半期ごとに示しています。累計では「任意のスクリプトの実行」が最も多く、41%となっています。今四半期は、「任意のスクリプトの実行（63 件）」が最も多く、次いで「任意のファイルへのアクセス（23 件）」「なりすまし（11 件）」でした。

ソフトウェア製品の脆弱性がもたらす影響別の届出状況



（3,057件の内訳、グラフの括弧内は前四半期までの数字）

図2-8. 届出累計の脆弱性がもたらす影響別割合



（過去2年間の届出内訳）

図2-9. 四半期ごとの脆弱性がもたらす影響別届出件数

2-1-4. JVN 公表状況別件数

届出受付開始から今四半期までに対策情報を JVN 公表した脆弱性（1,382 件）について、図 2-10 は受理してから JVN 公表するまでに要した日数を示したものです。45 日以内は 32%、45 日を超過した件数は 68%でした。表 2-1 は過去 3 年間において 45 日以内に JVN 公表した件数の割合推移を四半期ごとに示したものです。製品開発者は脆弱性が悪用された場合の影響を認識し、迅速な対策を講じる必要があります。

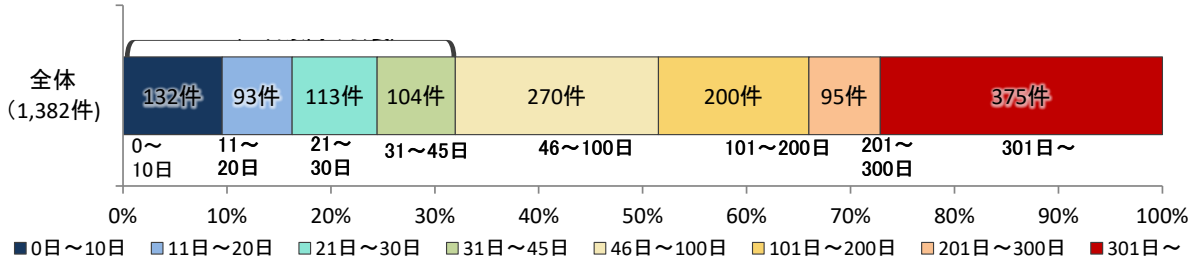


図2−10. ソフトウェア製品の脆弱性公表日数

表 2-1. 45 日以内に JVN 公表した件数の割合推移（四半期ごと）

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

2-1-5. 調整および公表レポート数

JPCERT/CC は、本制度に届け出られた脆弱性情報のほか、海外の製品開発者や CSIRT などからも脆弱性情報の提供を受けて、国内外の関係者と脆弱性対策情報の公表に向けた調整を行っています[(*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 : https://jvn.jp/ ）に公表しています。表 2-2、図 2-11 は、公表件数を情報提供元別に集計し、今四半期の公表件数、過去 3 年分の四半期ごとの公表件数[(*14)]の推移等を示したものです。

表 2-2. 脆弱性の提供元別 脆弱性公表レポート件数

情報提供元	今四半期件数	累計
国内外の発見者からの届出、製品開発者から自社製品の届出を受け JVN で公表した脆弱性レポート	44 件	1,337 件
海外 CSIRT 等から脆弱性情報の提供を受け JVN で公表した脆弱性レポート	44 件	1,471 件
合計	88 件	2,808 件

(*13) JPCERT/CC 活動概要 Page17～21（http://www.jpcert.or.jp/pr/2017/PR20170111.pdf）を参照下さい。
(*14) 2-1-5 は公表したレポートの件数をもとに件数を計上しています。複数の届出についてまとめ 1 件のレポートを公表する場合がある為、必ずしも JVN 公表した脆弱性の件数と一致するものではありません。

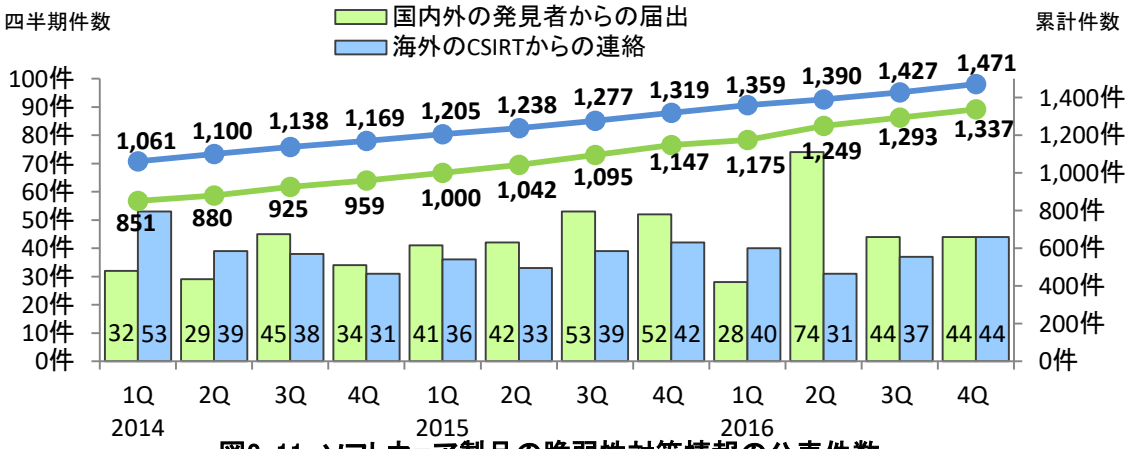


図2−11. ソフトウェア製品の脆弱性対策情報の公表件数

S

（1） JVN で公表した届出を深刻度で分類した“国内外の発見者および製品開発者から届出を受けた”脆弱性

表 2-3 は国内の発見者および製品開発者から受けた届出について、今四半期に JVN 公表した脆弱性を深刻度のレベル別に示しています。オープンソースソフトウェアに関する脆弱性が 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 19 件（表 2-3 の#2）、複数開発者・製品に影響がある脆弱性が 3 件（表 2-3 の#3）、組込みソフトウェア製品の脆弱性が 9 件（表 2-3 の#4）ありました。

表 2-3. 2016 年第 2 四半期に JVN で公表した脆弱性

項番	脆弱性識別番号	脆弱性	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) (#4)	JVN#18228200	「WFS-SR01」における複数の脆弱性	2016 年 11 月 2 日	7.5
2 (#2)	JVN#84995847	「SKYSEA Client View」において任意のコードが実行可能な脆弱性	2016 年 12 月 22 日	10.0
脆弱性の深刻度=レベル II（警告）、CVSS 基本値=4.0～6.9				
3 (#2)	JVN#06726266	「サイボウズ Office」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	2016 年 10 月 3 日	4.0
4 (#2)	JVN#07148816	「サイボウズ Office」における複数のアクセス制限不備の脆弱性	2016 年 10 月 3 日	4.0
5 (#2)	JVN#10092452	「サイボウズ Office」におけるサービス運用妨害(DoS)の脆弱性	2016 年 10 月 3 日	6.8
6 (#3)	JVN#20786316	「Cryptography API: Next Generation (CNG)」におけるサービス運用妨害(DoS)の脆弱性	2016 年 10 月 7 日	4.3
7 (#1)	JVN#80157683	「SetucoCMS」における複数の脆弱性	2016 年 10 月 7 日	6.5
8	JVN#70380788	「BASP21」におけるメールヘッダ・インジェクションの脆弱性	2016 年 10 月 13 日	5.8
9	JVN#63012325	「e-Tax ソフト」のインストーラにおける DLL 読み込みに関する脆弱性	2016 年 10 月 18 日	6.8
10	JVN#03251132	「Evernote for Windows」のインストーラにおける DLL 読み込みに関する脆弱性	2016 年 10 月 18 日	6.8

項番	脆弱性識別番号	脆弱性	JVN 公表日	CVSS 基本値
11 (#1)	JVN#14567604	WordPress 用プラグイン「WP-OliveCart」における複数の脆弱性	2016 年 10 月 20 日	6.5
12 (#1)	JVN#76780067	「7-Zip for Windows」のインストーラにおける DLL 読み込みに関する脆弱性	2016 年 10 月 26 日	6.8
13 (#2)	JVN#27260483	スマートフォンアプリ「mobiGate」における SSL サーバ証明書の検証不備の脆弱性	2016 年 11 月 1 日	4.0
14	JVN#91002412	Windows 版「公的個人認証サービス　利用者クライアントソフト」のインストーラにおける DLL 読み込みに関する脆弱性	2016 年 11 月 1 日	6.8
15 (#4)	JVN#25060672	コレガ製の複数の無線 LAN ルータにおけるクロスサイト・スクリプティングの脆弱性	2016 年 11 月 11 日	4.3
16 (#4)	JVN#23823838	「CG-WLR300NX」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	2016 年 11 月 11 日	4.0
17 (#4)	JVN#23549283	「CG-WLR300NX」におけるアクセス制限不備の脆弱性	2016 年 11 月 11 日	5.4
18 (#1)	JVN#05493467	「シンプル携帯チャット」におけるクロスサイト・スクリプティングの脆弱性	2016 年 11 月 25 日	5.0
19 (#2)	JVN#20252219	Android アプリ「kintone mobile for Android」における SSL サーバ証明書の検証不備の脆弱性	2016 年 11 月 28 日	4.0
20 (#4)	JVN#25059363	アイ・オー・データ製の複数のネットワークカメラ製品に複数の脆弱性	2016 年 11 月 30 日	5.2
21	JVN#08868688	日本年金機構製の複数のインストーラにおける DLL 読み込みに関する脆弱性	2016 年 12 月 1 日	6.8
22 (#4)	JVN#40613060	「WNC01WH」における複数の脆弱性	2016 年 12 月 2 日	6.2
23	JVN#28151745	「Sleipnir for Mac」におけるアドレス表示偽装の脆弱性	2016 年 12 月 7 日	4.3
24 (#2)	JVN#16781735	「サイボウズ デヂエ」における複数のアクセス制限不備の脆弱性	2016 年 12 月 12 日	6.4
25 (#1)	JVN#78980598	「Apache ActiveMQ」におけるクロスサイト・スクリプティングの脆弱性	2016 年 12 月 13 日	4.0
26 (#2)	JVN#14631222	「サイボウズ ガルーン」における複数のアクセス制限不備の脆弱性	2016 年 12 月 19 日	4.0
27 (#2)	JVN#16200242	「サイボウズ ガルーン」におけるディレクトリ・トラバーサルの脆弱性	2016 年 12 月 19 日	4.0
28 (#2)	JVN#17980240	「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	2016 年 12 月 19 日	6.5
29 (#1) (#2)	JVN#44566208	「H2O」における解放済みメモリ使用(use-after-free)の脆弱性	2016 年 12 月 22 日	6.4
30 (#1)	JVN#90813656	Windows 版「Wireshark」における任意ファイルが削除される問題	2016 年 12 月 26 日	4.0
31 (#1) (#3)	JVN#96681653	「WinSparkle」におけるレジストリ値を検証しない問題	2016 年 12 月 26 日	4.0

項番	脆弱性識別番号	脆弱性	JVN 公表日	CVSS 基本値
脆弱性の深刻度=レベルⅠ（注意）、CVSS 基本値=0.0～3.9				
32 （#4）	JVN#46351856	「L-04D」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	2016 年 10 月 3 日	2.6
33 （#2）	JVN#08736331	「サイボウズ Office」におけるメールヘッダ・インジェクションの脆弱性	2016 年 10 月 3 日	2.6
34 （#2）	JVN#09736331	「サイボウズ Office」における情報漏えいの脆弱性	2016 年 10 月 3 日	2.6
35 （#2）	JVN#11288252	「サイボウズ Office」における意図しないファイルをダウンロードさせられる脆弱性	2016 年 10 月 3 日	3.5
36 （#1）	JVN#32504719	「Usermin」におけるクロスサイトスクリプティングの脆弱性	2016 年 10 月 7 日	2.6
37 （#4）	JVN#34103586	アイ・オー・データ製の複数のネットワークカメラ製品における情報漏えいの脆弱性	2016 年 11 月 11 日	3.3
38 （#4）	JVN#92237169	「CG-WLR300NX」におけるクロスサイト・スクリプティングの脆弱性	2016 年 11 月 11 日	2.7
39 （#1）	JVN#75396659	「DERAEMON-CMS」におけるクロスサイト・スクリプティングの脆弱性	2016 年 11 月 15 日	2.6
40 （#2）	JVN#42070907	複数のソニー製ビデオ会議システムにおける認証不備の脆弱性	2016 年 12 月 15 日	2.9
41 （#2）	JVN#12281353	「サイボウズ ガルーン」におけるクロスサイト・スクリプティングの脆弱性	2016 年 12 月 19 日	2.6
42 （#2）	JVN#13218253	「サイボウズ ガルーン」における情報漏えいの脆弱性	2016 年 12 月 19 日	2.6
43 （#2）	JVN#15222211	「サイボウズ ガルーン」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	2016 年 12 月 19 日	2.6
44 （#1） （#3）	JVN#38755305	「BlueZ」付属のユーティリティにおけるバッファオーバーフローの脆弱性	2016 年 12 月 22 日	3.5

（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、2-5 は、今四半期に JPCERT/CC が海外 CSIRT 等と連携して取り扱った脆弱性の公表ないし対応の状況を示しています。今四半期には、表 2-4 に示した脆弱性情報 42 件と、表 2-5 に示した Alert [*15]（注意喚起情報）の 2 件を公表しました。

Android 関連製品や OSS を組み込んだ製品の脆弱性に関する調整活動では、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 との連携が近年増えています。これらの情報は、JPCERT/CC 製品開発者リスト [*16] に登録された製品開発者へ通知したうえ、JVN に掲載しています。

表 2-4. 海外 CSIRT 等と連携した脆弱性および対応状況

項番	脆弱性	対応状況
1	PHPMailer 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
2	Apache HTTP Web Server 2.4 における複数の脆弱性に対するアップデート	特定製品開発者と調整 複数製品開発者へ通知
3	複数の Apple 製品における脆弱性に対するアップデート	注意喚起として掲載
4	McAfee VirusScan Enterprise for Windows にメモリ破損の脆弱性	注意喚起として掲載
5	EpubCheck に XML 外部実体参照 (XXE) に関する脆弱性	注意喚起として掲載
6	Adobe Flash Player における解放済みメモリ使用 (use-after-free) の脆弱性	特定製品開発者と調整 緊急案件として掲載
7	Apache Tomcat に情報漏えいの脆弱性	特定製品開発者と調整 複数製品開発者へ通知
8	複数の Apple 製品における脆弱性に対するアップデート	注意喚起として掲載
9	McAfee Virus Scan Enterprise for Linux に複数の脆弱性	注意喚起として掲載
10	複数の NETGEAR 製ルータに脆弱性	注意喚起として掲載
11	PHP FormMail Generator で作成した PHP コードに複数の脆弱性	注意喚起として掲載
12	ForeScout CounterACT SecureConnector エージェントに権限昇格の脆弱性	注意喚起として掲載
13	BSD libc 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
14	SunGard eTRAKiT に SQL インジェクションの脆弱性	注意喚起として掲載
15	三菱電機 MELSEC-Q シリーズの Ethernet インターフェースモジュールに複数の脆弱性	特定製品開発者と調整
16	Android アプリ「株式会社三菱東京ＵＦＪ銀行」に SSL/TLS ダウングレード攻撃が可能となる脆弱性	特定製品開発者と調整
17	Apache HTTP Web Server の HTTP/2 プロトコルの処理にサービス運用妨害 (DoS) の脆弱性	特定製品開発者と調整 複数製品開発者へ通知
18	Mozilla Firefox における解放済みメモリ使用 (use-after-free) の脆弱性	注意喚起として掲載
19	ソニー製の複数のネットワークカメラ製品に脆弱性	特定製品開発者と調整
20	Apache Tomcat の複数の脆弱性に対するアップデート	特定製品開発者と調整 複数製品開発者へ通知
21	NTP.org の ntpd に複数の脆弱性	注意喚起として掲載
22	Ragentek 製のコードを使用した Android 端末の OTA アップデートに中間者攻撃が可能な脆弱性	注意喚起として掲載

[*15] US-CERT が公表した注意喚起情報
[*16] JPCERT/CC 製品開発者リスト：https://jvn.jp/nav/index.html

項番	脆弱性	対応状況
23	WordPress 用プラグイン NextGEN Gallery に PHP ファイルインクルージョンの脆弱性	注意喚起として掲載
24	OpenSSL に複数の脆弱性	特定製品開発者と調整 複数製品開発者へ通知
25	D-Link 製ルータの HNAP サービス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
26	ISC BIND の DNAME レコードを含む応答パケットの処理に脆弱性	特定製品開発者と調整 緊急案件として掲載 複数製品開発者へ通知
27	複数の Apple 製品における脆弱性に対するアップデート	注意喚起として掲載
28	Apache Tomcat の複数の脆弱性に対するアップデート	特定製品開発者と調整 複数製品開発者へ通知
29	TrackR Bravo に複数の脆弱性	注意喚起として掲載
30	Zizai Tech Nut に複数の脆弱性	注意喚起として掲載
31	iTrack Easy に複数の脆弱性	注意喚起として掲載
32	複数の Apple 製品の脆弱性に対するアップデート	注意喚起として掲載
33	Linux カーネルのメモリサブシステムに実装されている copy-on-write 機構に競合状態が発生する脆弱性	緊急案件として掲載
34	Synology 製の複数の NAS サーバに機器共通の認証情報が設定されている問題	注意喚起として掲載
35	Green Packet DX-350 に機器共通の認証情報が設定されている問題	注意喚起として掲載
36	Intellian Satellite TV および Satellite Communications に機器共通の認証情報が設定されている問題	注意喚起として掲載
37	NUUO Titan NVR NT-4040 に機器共通の認証情報が設定されている問題	注意喚起として掲載
38	ISC BIND 9 にサービス運用妨害 (DoS) の脆弱性	特定製品開発者と調整 複数製品開発者へ通知
39	ASUS RP-AC52 に複数の脆弱性	注意喚起として掲載
40	MatrixSSL に複数の脆弱性	注意喚起として掲載
41	Animas OneTouch Ping に複数の脆弱性	注意喚起として掲載
42	iOS 版「U by BB&T」に SSL サーバ証明書の検証不備の脆弱性	注意喚起として掲載

表 2-5.米国 US-CERT [*17] と連携した注意喚起情報

項番	脆弱性
1	細工された PDF による情報詐取について
2	Mirai 等のマルウェアで構築されたボットネットによる DDoS 攻撃の脅威

[*17] United States Computer Emergency Readiness Team：米国の政府系 CSIRT。

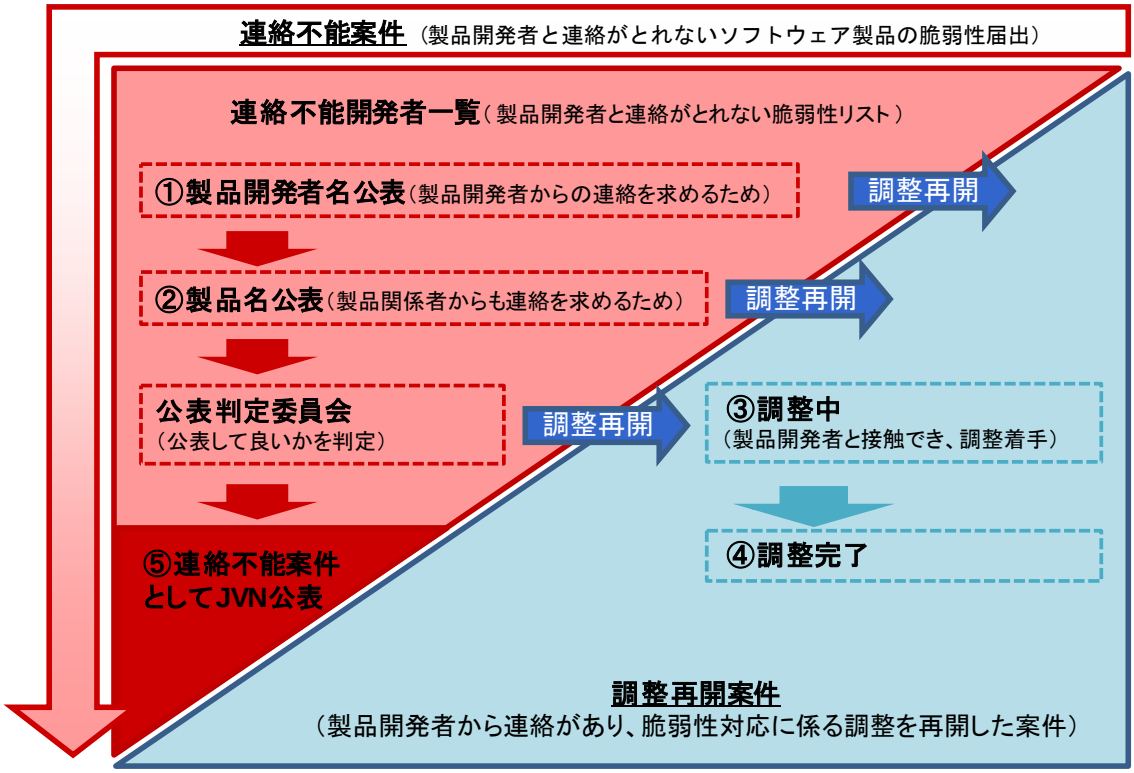
2-1-6. 連絡不能案件の処理状況

図 2-12 は、2011 年 9 月末から 2016 年 12 月末までに「連絡不能開発者」と位置づけて取扱った 250 件の処理状況の推移を示したものです。

「製品開発者名を公表（①）」について、今四半期は新たに 3 件公表しました。製品開発者名を公表しても製品開発者からの応答がないため追加情報として公表する「製品名公表（②）」について、今四半期は新たに 5 件公表しました。また、製品開発者と調整が再開したもの（「調整中（③）」）は 3 件あり、今四半期は「調整が完了（④）」について変動がありませんでした。

この結果、2016 年 12 月末時点で連絡不能案件（①+②）は 203 件（前四半期は 203 件）、調整再開した案件（③+④）は 45 件となりました。

なお、公表判定委員会の審議にて JVN 公表が適当であると判定され JVN 公表に至った案件（⑤）について、今四半期に公表した案件はありませんでした。



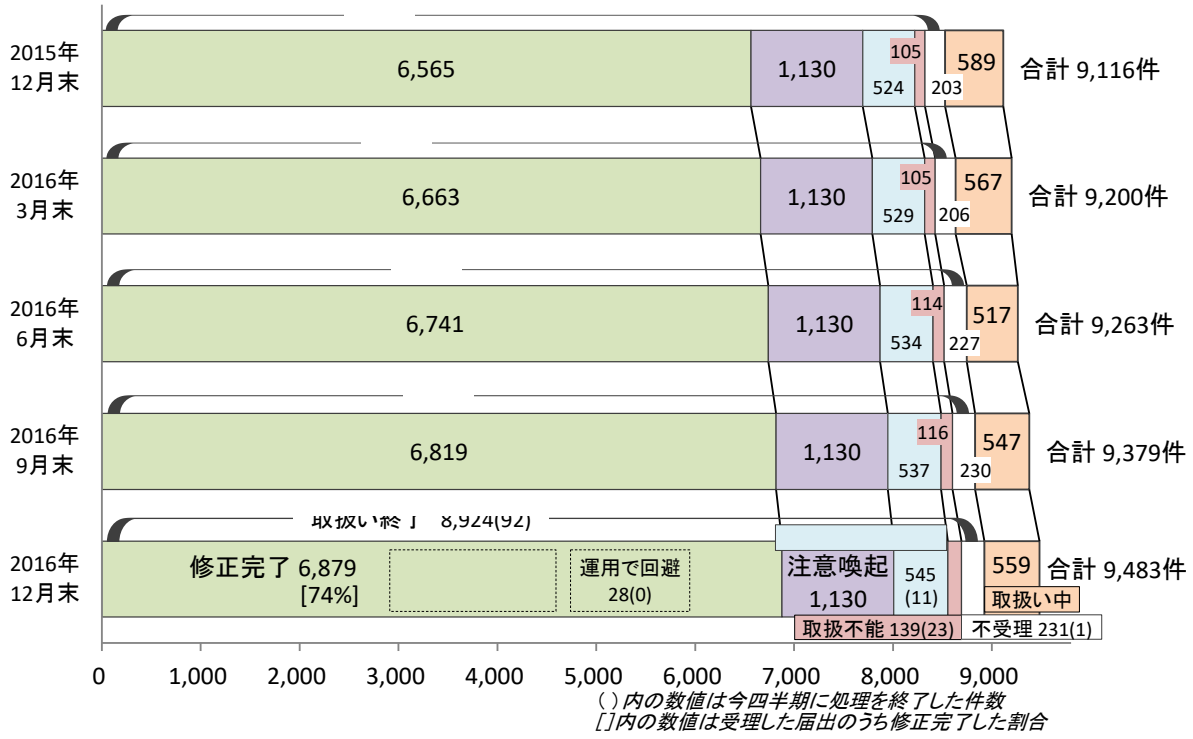
2016年 第3四半期	203件 （①5件　②198件）	42件 （③19件　④23件）	⑤2件	合計 247件
2016年 第4四半期	203件 （①3件　②200件）	45件 （③22件　④23件）	⑤2件	合計 250件

図2-12. 連絡不能案件の処理状況

2-2. ウェブサイトの脆弱性

2-2-1. 処理状況

図 2-13 は、ウェブサイトの脆弱性届出の処理状況について、四半期ごとの推移を示したものです。2016 年 12 月末時点の届出の累計は 9,483 件で、今四半期中に取扱いを終了したものは 92 件（累計 8,924 件）でした。このうち「修正完了」したもの 60 件（累計 6,879 件）、「注意喚起」により処理を取りやめたもの[*18] 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 11 件（累計 545 件）でした。なお、ウェブサイト運営者への連絡は通常メールで行い、連絡が取れない場合に電話や郵送での連絡も行っています。しかしウェブサイト運営者への連絡手段がない場合などは「取扱不能」案件に分類しています。今四半期の件数は 23 件（累計 139 件）でした。また「不受理」としたものは 1 件[*19]（累計 231 件）でした。取扱いを終了した累計 8,924 件のうち「修正完了」「脆弱性ではない」の合計 7,424 件は全て、ウェブサイト運営者からの報告もしくは IPA の判断により指摘した点が解消されていることが確認されたものです。なお「修正完了」のうち、ウェブサイト運営者が当該ページを削除したものは 21 件（累計 989 件）、ウェブサイト運営者が運用により被害を回避したものは 0 件（累計 28 件）でした。



取扱い終了
- 修正完了 : ウェブサイト運営者により脆弱性が修正されたもの
  - 当該ページを削除 : 修正完了のうち、当該ページを削除したもの
  - 運用で回避 : 修正完了のうち、運用により被害を回避しているもの
- 注意喚起 : IPA による注意喚起で広く対策実施を促した後、処理を取りやめたもの
- 脆弱性ではない : IPA およびウェブサイト運営者が脆弱性はないと判断したもの
- 取扱不能 : ウェブサイト運営者からの回答がなく、取扱いができないもの、ウェブサイト運営者が対応しないと判断したもの

- 不受理 : 告示で定める届出の対象に該当しないもの
- 取扱い中 : IPA が内容確認中、ウェブサイト運営者が調査、対応中のもの

図 2-13.ウェブサイト脆弱性の届出処理状況の四半期別推移

[*18] 「多数のウェブサイトにおいて利用されているソフトウェア製品に修正プログラムが適用されていない」といった届出があった場合、効果的に周知徹底するため「注意喚起」を公表することがあります。そうした場合、「注意喚起」をもって届出の処理を取りやめます。

[*19] 内訳は今四半期の届出によるもの 0 件、前四半期までの届出によるもの 1 件。

今までに届出のあったウェブサイトの脆弱性 9,483 件のうち、不受理を除いた件数は 9,252 件でした。以降、不受理を除いた届出について集計した結果を記載します。

2-2-2. 運営主体の種類別の届出件数

図 2-14 は、届出された脆弱性のウェブサイト運営主体の種類について、過去 2 年間の届出件数の推移を四半期ごとに示しています。今四半期は届出 104 件の約 4 割を企業が占めています。

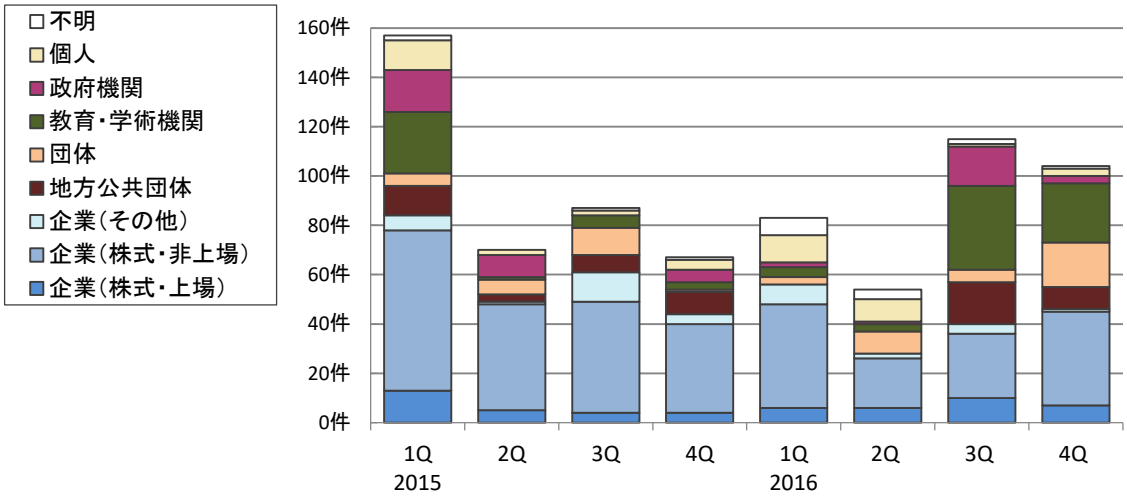
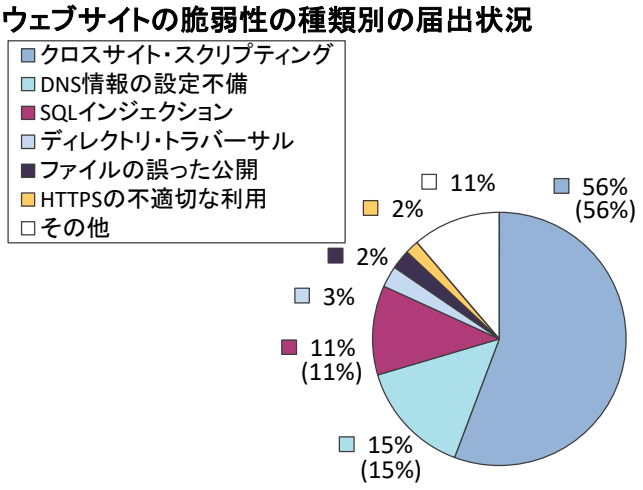


図2-14. 四半期ごとの運営主体の種類別届出件数

2-2-3. 脆弱性の種類・影響別届出

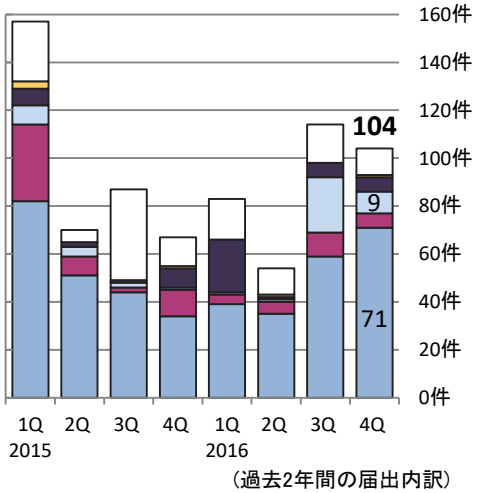
図 2-15、2-16 は、届出された脆弱性の種類を示しています。図 2-15 は今までの届出累計の割合を、図 2-16 は過去 2 年間の届出件数の推移を四半期ごとに示しています[*20]。

累計では、「クロスサイト・スクリプティング」だけで 56%を占めており、次いで「DNS 情報の設定不備」「SQL インジェクション」となっています。「DNS 情報の設定不備」の 15%は、2008 年から 2009 年にかけて多く届出されたものが反映されています。今四半期は約 7 割を占める「クロスサイト・スクリプティング（71 件）」が最も多く、次いで「ディレクトリ・トラバーサル（9 件）」となっています。なお、この統計は本制度における届出の傾向であり、世の中に存在する脆弱性の傾向と必ずしも一致するものではありません。



（9,252件の内訳、グラフの括弧内は前四半期までの数字）

図2-15. 届出累計の脆弱性の種類別割合



（過去2年間の届出内訳）

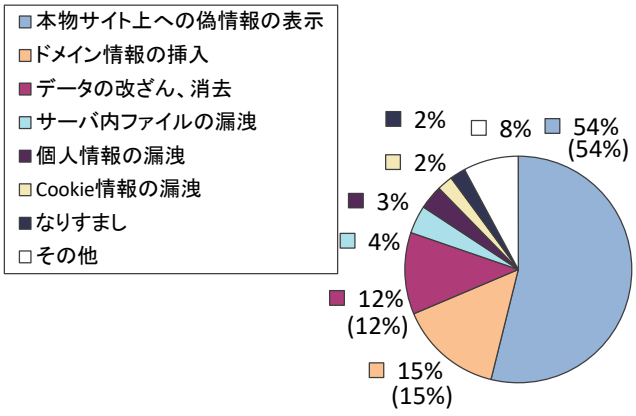
図2-16. 四半期ごとの脆弱性の種類別届出件数

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

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

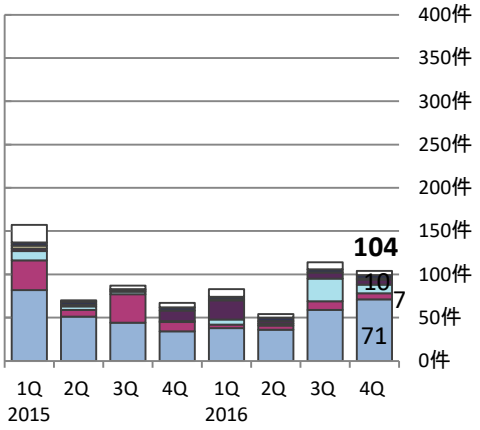
累計では、「本物サイト上への偽情報の表示」「ドメイン情報の挿入」「データの改ざん、消去」が全体の 8 割を占めています。これらは、「クロスサイト・スクリプティング」「DNS 情報の設定不備」「SQL インジェクション」などにより発生するものです。今四半期は「本物サイト上への偽情報の表示（71 件）」が最も多く、次いで「サーバ内ファイルの漏洩（10 件）」「データの改ざん、消去（7 件）」となっています。

ウェブサイトの脆弱性がもたらす影響別の届出状況



（9,252件の内訳、グラフの括弧内は前四半期までの数字）

図2−17. 届出累計の脆弱性がもたらす影響別割合



（過去2年間の届出内訳）

図2−18. 四半期ごとの脆弱性がもたらす影響別届出件数

2-2-4. 修正完了状況

図 2-19 は、過去 3 年間のウェブサイトの脆弱性の修正完了件数を四半期ごとに示しています。2016 年第 4 四半期に修正を完了した届出 60 件のうち 43 件（72%）は、運営者へ脆弱関連情報を通知してから 90 日以内に修正が完了しました。この割合は、前四半期（78 件中 46 件）の 59%より増加しています。表 2-6 は、過去 3 年間に修正が完了した全届出のうち、ウェブサイト運営者に通知してから、90 日以内に修正が完了した脆弱性の累計およびその割合を四半期ごとに示したものです。今四半期の割合は 66%でした。

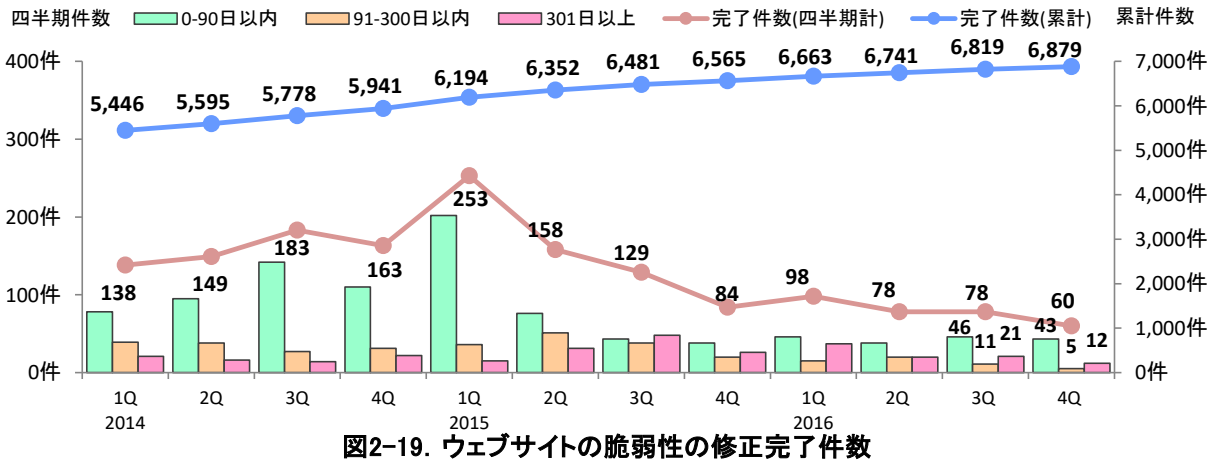


図2−19. ウェブサイトの脆弱性の修正完了件数

表 2-6. 90 日以内に修正完了した累計およびその割合の推移

	2014 1Q	2Q	3Q	4Q	2015 1Q	2Q	3Q	4Q	2016 1Q	2Q	3Q	4Q
修正完了件数	5,446	5,595	5,778	5,941	6,194	6,352	6,481	6,565	6,663	6,741	6,819	6,879
90 日以内の件数	3,635	3,730	3,872	3,982	4,184	4,260	4,303	4,341	4,387	4,425	4,471	4,514
90 日以内の割合	67%	67%	67%	67%	68%	67%	66%	66%	66%	66%	66%	66%

図 2-20、2-21 は、ウェブサイト運営者に脆弱性を通知してから修正されるまでに要した日数を脆弱性の種類別に分類し、その傾向を示しています[*21]。全体の 47%の届出が 30 日以内、全体の 66%の届出が 90 日以内に修正されています。

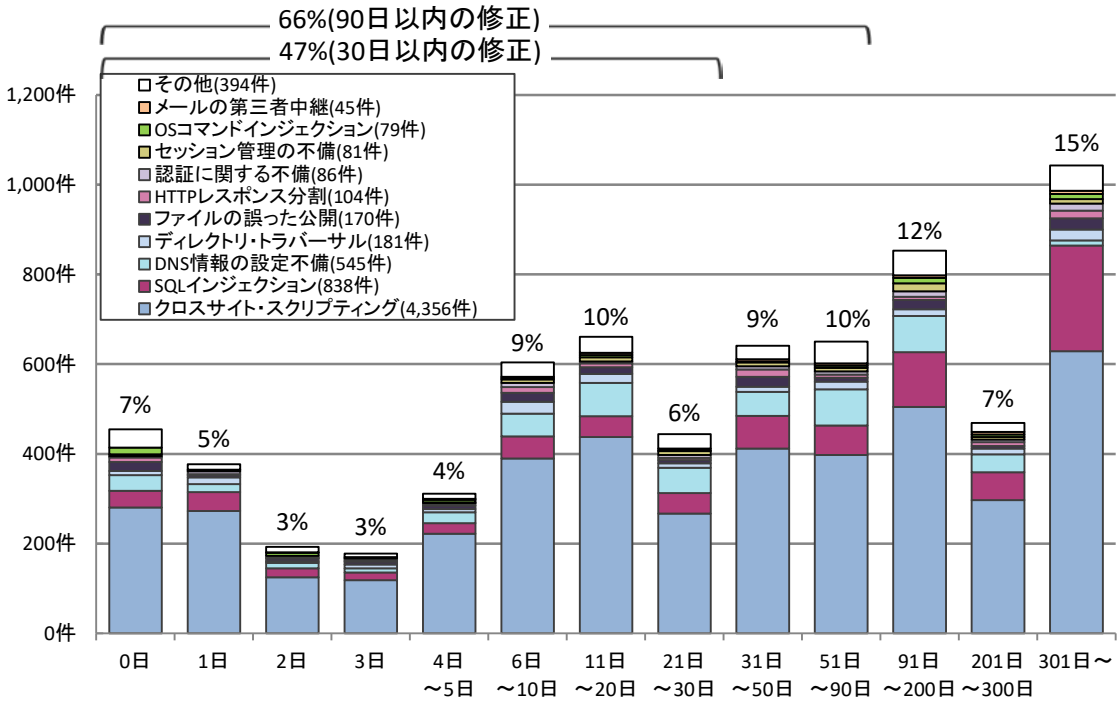


図2-20. ウェブサイトの修正に要した日数

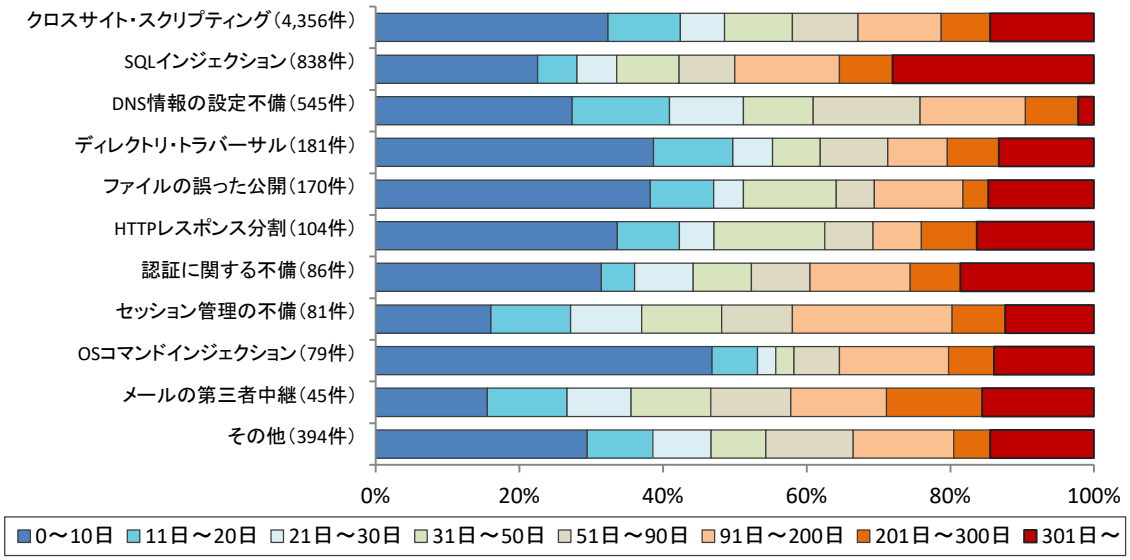


図2-21. ウェブサイトの修正に要した脆弱性種類別の日数の傾向

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

2-2-5. 長期化している届出の取扱い経過日数

ウェブサイト運営者から脆弱性を修正した旨の報告が無い場合、IPA は 1～2 ヶ月毎に電子メールや電話、郵送などの手段でウェブサイト運営者に繰り返し連絡を試み、脆弱性対策の実施を促しています。

図 2-22 は、ウェブサイトの脆弱性のうち、取扱いが長期化（IPA からウェブサイト運営者へ脆弱性を通知してから、90 日以上修正した旨の報告が無い）しているものについて、経過日数別の件数を示したものです。これらの合計は 374 件（前四半期は 388 件）と減少しています。これらのうち、SQL インジェクションという深刻度の高い脆弱性の割合は全体の約 15%を占め、この脆弱性は、ウェブサイトの情報が窃取されてしまうなどの危険性が高いものです。

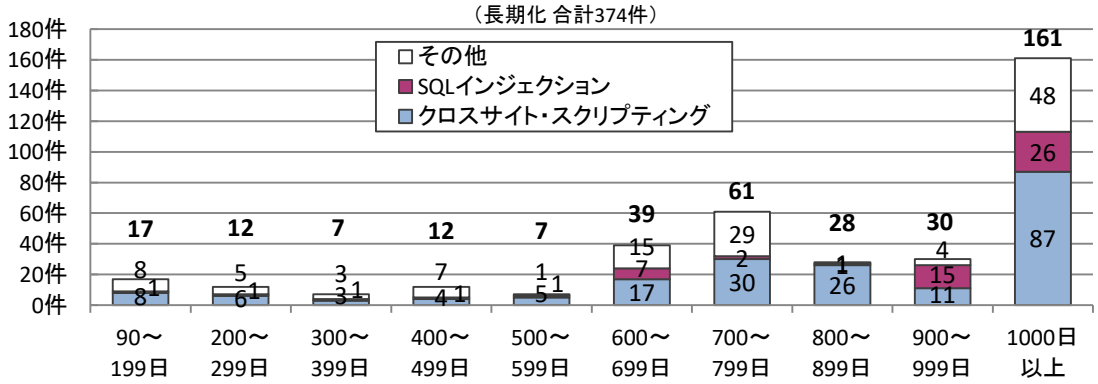


図2−22. 取扱いが長期化(90日以上経過)しているウェブサイトの経過日数と脆弱性の種類

表 2-7 は、過去 2 年間の四半期末時点で取扱い中の届出と、取扱いが長期化している届出の件数および、その割合を示しています。

表 2-7. 取扱いが長期化している届出件数および割合の四半期ごとの推移

	2015 1Q	2Q	3Q	4Q	2016 1Q	2Q	3Q	4Q
取扱い中の件数	757	655	608	591	568	517	547	559
長期化している件数	415	562	504	473	436	401	388	374
長期化している割合	55%	86%	83%	80%	77%	78%	71%	67%

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次のとおりです。

3-1. ウェブサイト運営者

多くのウェブサイトで利用しているソフトウェア製品に脆弱性が発見されています。自身のウェブサイトでどのようなソフトウェア製品を利用しているか把握し、脆弱性対策を実施する事が必要です。脆弱性の理解・対策にあたっては、次の IPA が提供するコンテンツが利用できます。

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

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

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

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

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

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

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

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

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

3-2. 製品開発者

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

なお、製品開発にあたっては、次のコンテンツが利用できます。

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

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

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

3-3. 一般のインターネットユーザー

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

なお、一般インターネットユーザー向けには、次のツールを提供しています。

⇒「MyJVN 脆弱性対策情報収集ツール」: 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

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

3-4. 発見者

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

付表 1. ソフトウェア製品の脆弱性の原因分類

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

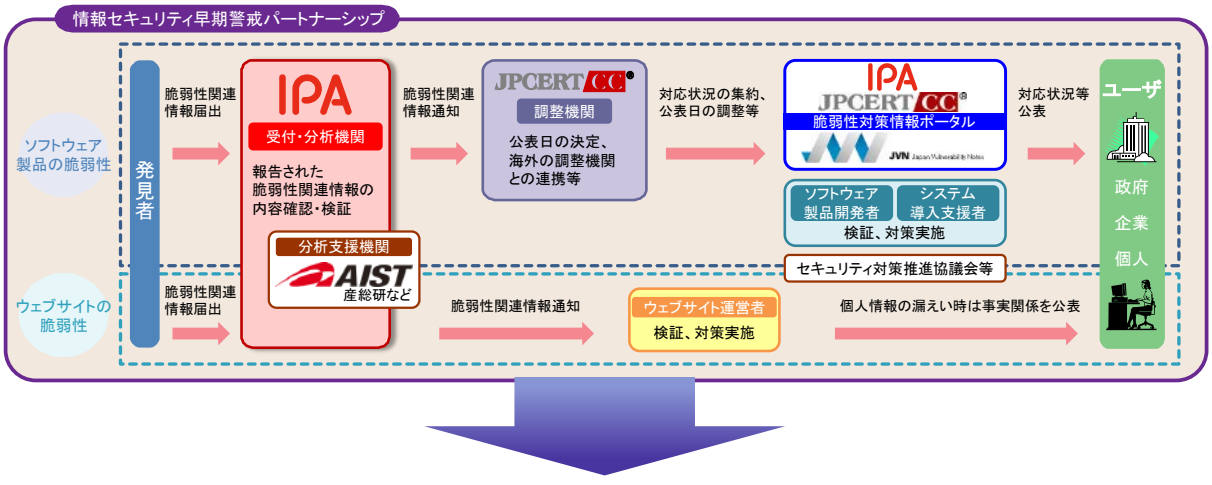
付表 2. ウェブサイトの脆弱性の分類

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

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

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

付図１．「情報セキュリティ早期警戒パートナーシップ」（脆弱性関連情報の取扱制度）



【期待効果】

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

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