ソフトウェア等の脆弱性関連情報に関する届出状況

[2017 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」は、経済産業省の告示[(*1)]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（以降「IPA」）と一般社団法人 JPCERT コーディネーションセンター（以降「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、2017 年 4 月 1 日から 2017 年 6 月 30 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 7 月 26 日

(*1) 旧告示「ソフトウエア等脆弱性関連情報取扱基準」は廃止され、新たに以下の告示が定められました。
・「ソフトウエア製品等の脆弱性関連情報に関する取扱規程」（平成 29 年経済産業省告示第 19 号）
・「受付機関及び調整機関を定める告示」（平成 29 年経済産業省告示第 20 号）

目次

1. 2017 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 13,331 件 ～

表 1-1 は情報セキュリティ早期警戒パートナーシップ [(*2)]（以降「本制度」）における 2017 年第 2 四半期（以降「本四半期」）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）から本四半期までの累計を示しています。本四半期のソフトウェア製品に関する届出件数は 240 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 29 件、合計 269 件でした。届出受付開始からの累計は 13,331 件で、内訳はソフトウェア製品に関するもの 3,767 件、ウェブサイトに関するもの 9,564 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	本四半期件数	累計
ソフトウェア製品	**240** 件	**3,767** 件
ウェブサイト	**29** 件	**9,564** 件
合計	**269** 件	**13,331** 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。本四半期は、ウェブサイトに関する届出が前四半期の約半数に減少しました。一方で、製品に関する届出が前四半期の 2.5 倍に増加しました。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。本四半期までの 1 就業日あたりの届出件数は 4.21 件 [(*3)] でした。

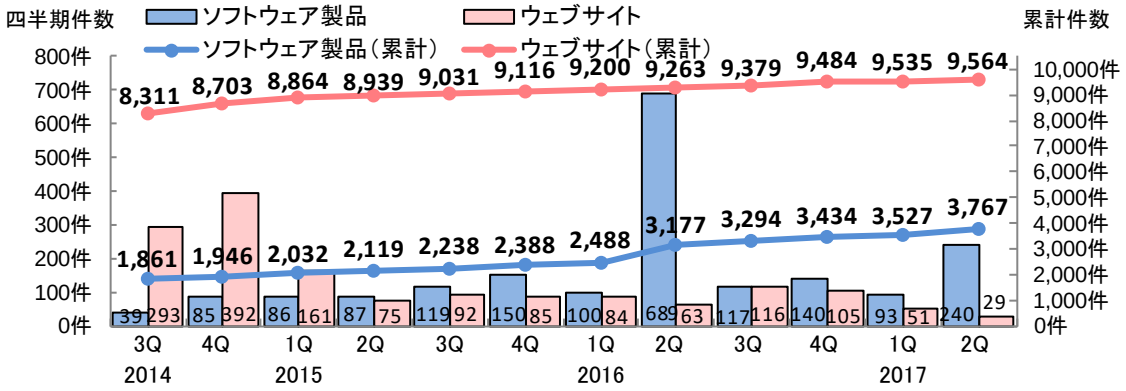


図1−1. 脆弱性の届出件数の四半期ごとの推移

表 1-2. 届出件数（過去 3 年間）

	2014 3Q	4Q	2015 1Q	2Q	3Q	4Q	2016 1Q	2Q	3Q	4Q	2017 1Q	2Q
累計届出件数[件]	10,172	10,649	10,896	11,058	11,269	11,504	11,688	12,440	12,673	12,918	13,062	13,331
1 就業日あたり[件/日]	4.07	4.16	4.17	4.13	4.11	4.11	4.09	4.26	4.25	4.25	4.21	4.21

(*2) 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

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

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 8,596 件 ～

表 1-3 は本四半期、および届出受付開始から本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	本四半期件数	累計
ソフトウェア製品	**145** 件	**1,574** 件
ウェブサイト	**38** 件	**7,022** 件
合計	**183** 件	**8,596** 件

本四半期に JVN 公表したソフトウェア製品の件数は 145 件 (*4)（累計 1,574 件）でした。そのうち、3 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 (*5) 以内のものは 36 件（25%）でした。

また、修正完了したウェブサイトの件数は 38 件（累計 7,022 件）でした。修正を完了した 38 件のうち、ウェブアプリケーションを修正したものは 31 件（82%）、当該ページを削除したものは 5 件（13%）で、運用で回避したものは 2 件（5%）でした。なお、修正を完了した 38 件のうち、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 (*6) 以内に修正が完了したものは 11 件（29%）でした。本四半期は、90 日以内に修正完了した割合が、前四半期（105 件中 88 件（84%））より減少しています。

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 (*7)。製品開発者名を公表後、3 ヶ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 (*8) で判定します。その判定を踏まえ、IPA が公表すると判定した脆弱性情報は JVN に公表されます。

本四半期は、1 件について製品開発者と連絡が取れたため調整を再開しました。連絡不能開発者として新たに製品開発者名を公表したものはありませんでした。また、公表判定委員会での判定を経て、脆弱性情報が JVN に公表したものはありませんでした。

2017 年 6 月末時点の連絡不能開発者の累計公表件数は 251 件、そのうち、製品情報を公表しているものは 205 件となりました。

(*4) P.7 表 2-3 参照

(*5) 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。

(*6) 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。

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

(*8) 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 が組織します。法律、サイバーセキュリティ、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ています。

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。2017 年 6 月末時点の届出の累計は 3,767 件で、本四半期に脆弱性対策情報を JVN 公表したものは 145 件（累計 1,574 件）でした。製品開発者が JVN 公表を行わず「個別対応」したものは 1 件（累計 37 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 85 件）でした。また「不受理」としたものは 5 件 (*9)（累計 391 件）、取扱い中は 1,680 件でした。1,680 件のうち、製品開発者と脆弱性対策情報の公表に向けた調整が再開したため、連絡不能開発者 (*10) 一覧から削除したものは 1 件です。2017 年 6 月末時点で 205 件 (*11) が連絡不能開発者一覧へ公表しています。

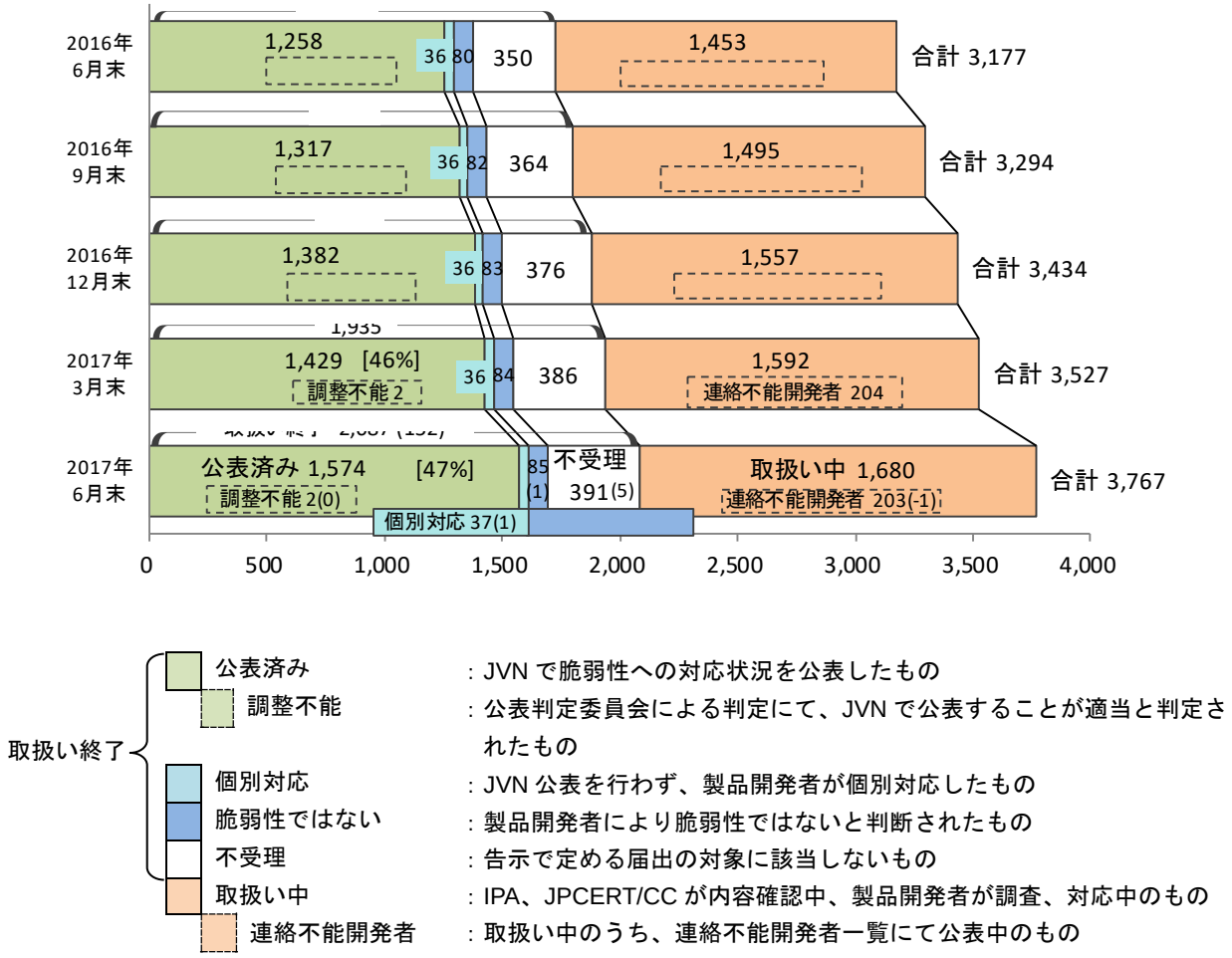


図 2-1. ソフトウェア製品脆弱性の届出処理状況（四半期ごとの推移）

(*9) 内訳は本四半期の届出によるもの 1 件、前四半期までの届出によるもの 4 件。
(*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た製品開発者の公表回数は、その累計を計上しています。
(*11) 連絡不能開発者一覧に公表中の件数は、図 2-1 の「調整不能」及び「連絡不能開発者」の合計です。

届出受付開始から本四半期までに届出のあったソフトウェア製品の脆弱性 3,767 件のうち、不受理を除いた件数は 3,376 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. ソフトウェア製品の種類別届出件数

図 2-2、2-3 は、届出された脆弱性の製品種類別の分類です。図 2-2 は製品種類別割合を、図 2-3 は過去 2 年間の届出件数の推移を四半期ごとに示しています。

累計では、「ウェブアプリケーションソフト」が最も多く 45%を占めています。本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（40 件）」が最も多く、次いで「ファイル管理ソフト（39 件）」「スマートフォン向けアプリ（15 件）」となっています。

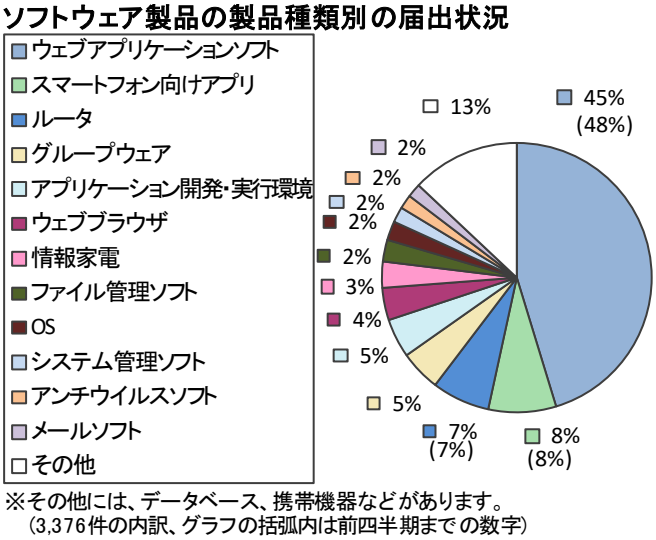


図2−2. 届出累計の製品種類別割合

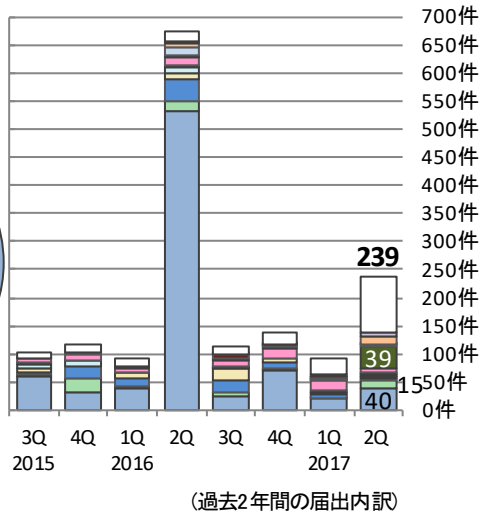


図2−3. 四半期ごとの製品種類別届出件数

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、本四半期は 82%、累計では 59%を占めています。

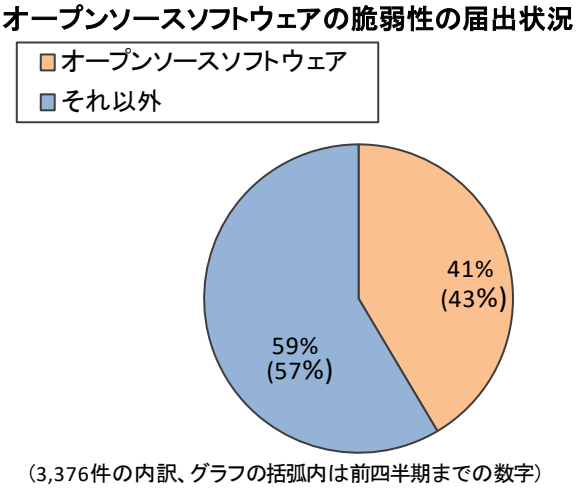


図2−4. 届出累計のオープンソースソフトウェア割合

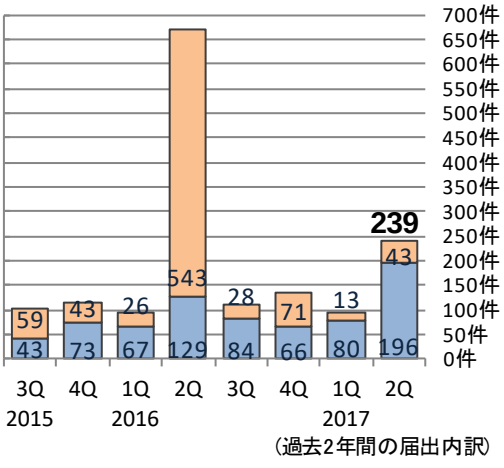


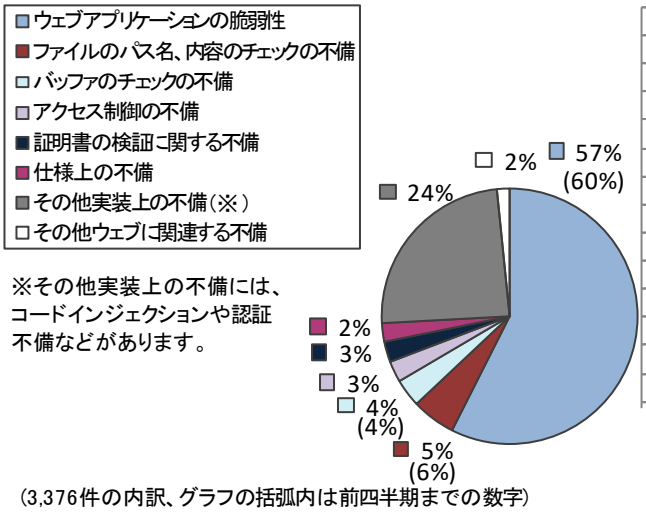
図2−5. 四半期ごとのオープンソースソフトウェア届出件数

2-1-3. 脆弱性の原因・影響別届出件数

図 2-6、2-7 は、届出された脆弱性の原因別の分類です。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[*12]。

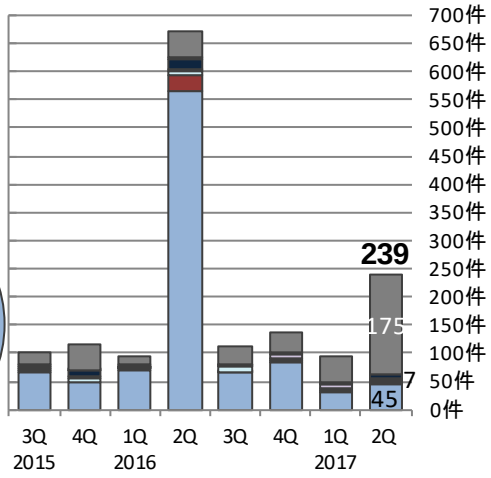
累計では、「ウェブアプリケーションの脆弱性」が過半数を占めています。本四半期は「その他実装上の不備（175 件）」が最も多く、次いで「ウェブアプリケーションの脆弱性（45 件）」「証明書の検証に関する不備（7 件）」となっています。

ソフトウェア製品の脆弱性の原因別の届出状況



（3,376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



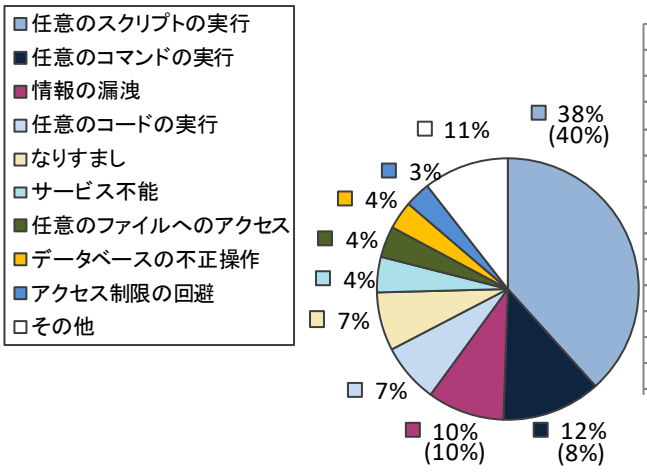
（過去2年間の届出内訳）

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別の分類です。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。

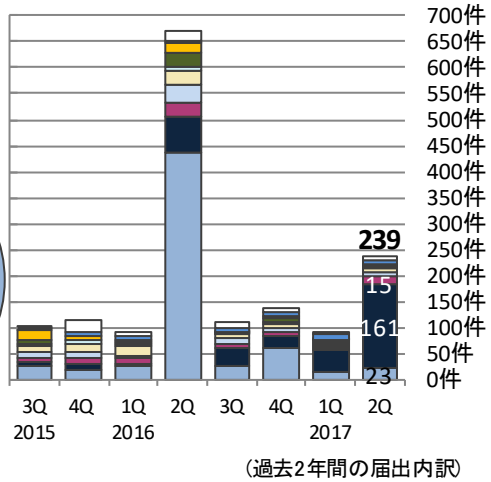
累計では「任意のスクリプトの実行」が最も多く、38%を占めています。本四半期は、「任意のコマンドの実行（161 件）」が最も多く、次いで「任意のスクリプトの実行（23 件）」「情報の漏洩（15 件）」でした。

ソフトウェア製品の脆弱性がもたらす影響別の届出状況



（3,376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

[*12] それぞれの脆弱性の詳しい説明については付表 1 を参照してください。

2-1-4. JVN 公表状況別件数

届出受付開始から本四半期までに対策情報を JVN 公表した脆弱性（1,574 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 31%、45 日を超過した件数は 69%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。

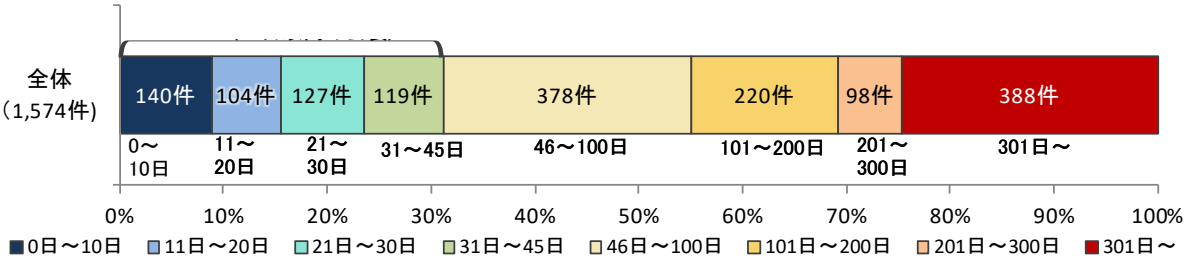


表 2-1. 45 日以内に JVN 公表した件数の割合推移（四半期ごと）

3Q	4Q	2015 1Q	2Q	3Q	4Q	2016 1Q	2Q	3Q	4Q	2017 1Q	2Q
33%	33%	32%	31%	31%	31%	30%	32%	32%	32%	32%	31%

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、本四半期の公表件数、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	本四半期件数	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	72 件	1,444 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	30 件	1,533 件
合計	102 件	2,977 件

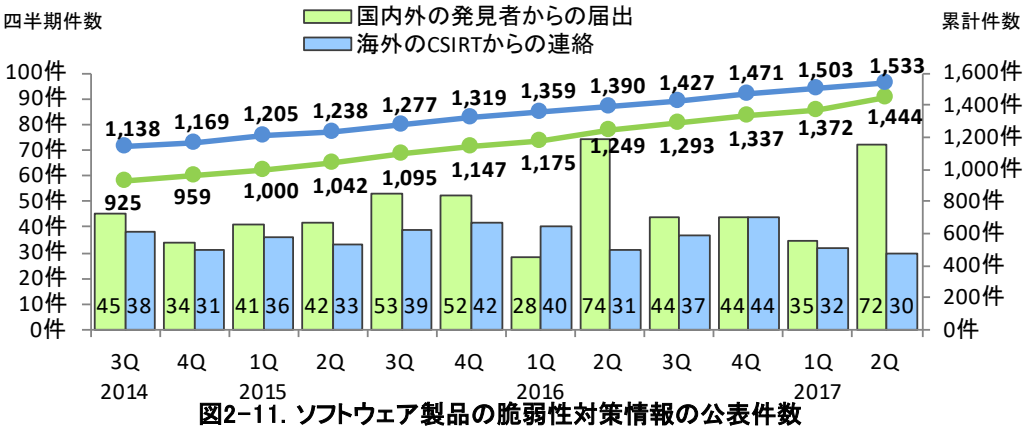


図2−11. ソフトウェア製品の脆弱性対策情報の公表件数

(*13) JPCERT/CC 活動概要 Page14～20（http://www.jpcert.or.jp/pr/2017/PR20170713.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、届出の JVN 公表件数と JVN 公表レポート数は異なる件数となります。

（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”脆弱性公表レポート

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、本四半期に 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 23 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 3 件（表 2-3 の#2）、組込みソフトウェア製品の脆弱性が 11 件（表 2-3 の#3）ありました。

表 2-3. 2017 年第 2 四半期に JVN で公表した脆弱性公表レポート

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)	JVN#17535578	「サイボウズ Office」における複数の脆弱性	2017 年 4 月 11 日	7.8
2 (#3)	JVN#85901441	東芝ライテック製「ホームゲートウェイ」における複数の脆弱性	2017 年 6 月 27 日	8.3
脆弱性の深刻度=レベル II（警告）、CVSS 基本値=4.0～6.9				
3	JVN#14396697	「CS-Cart」日本語版におけるアクセス制限不備の脆弱性	2017 年 4 月 6 日	5.0
4 (#1)	JVN#64451600	「Tablacus Explorer」におけるスクリプト・インジェクションの脆弱性	2017 年 4 月 7 日	6.8
5 (#3)	JVN#81024552	「WN-G300R3」における複数の脆弱性	2017 年 4 月 10 日	5.8
6	JVN#25598952	「CS-Cart」日本語版におけるアクセス制限不備の脆弱性	2017 年 4 月 10 日	5.0
7 (#1)	JVN#62392065	WordPress 用プラグイン「WP Statistics」におけるクロスサイト・スクリプティングの脆弱性	2017 年 4 月 13 日	5.0
8 (#1)	JVN#77253951	WordPress 用プラグイン「WP Statistics」におけるクロスサイト・スクリプティングの脆弱性	2017 年 4 月 13 日	5.0
9	JVN#05340816	東芝製メモリカード関連ソフトウェア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	2017 年 4 月 14 日	6.8
10 (#2) (#3)	JVN#86171513	「SEIL」シリーズルータにおけるサービス運用妨害(DoS)の脆弱性	2017 年 4 月 19 日	5.0
11 (#1)	JVN#18739672	WordPress 用プラグイン「Booking Calendar」におけるディレクトリ・トラバーサルの脆弱性	2017 年 4 月 20 日	5.0
12 (#1)	JVN#54762089	WordPress 用プラグイン「Booking Calendar」におけるクロスサイト・スクリプティングの脆弱性	2017 年 4 月 20 日	5.0
13	JVN#93931029	「風神ビュアー」におけるバッファオーバーフローの脆弱性	2017 年 4 月 20 日	5.1
14	JVN#54268888	「花子」を含む複数の製品における任意の DLL 読み込みに関する脆弱性	2017 年 4 月 20 日	6.8
15 (#3)	JVN#48790793	「WNC01WH」における OS コマンド・インジェクションの脆弱性	2017 年 4 月 21 日	5.2
16 (#1)	JVN#71572107	Windows 版「Vivaldi」のインストーラにおける実行ファイル読み込みの脆弱性	2017 年 4 月 25 日	6.8

項番	脆弱性識別番号	脆弱性	JVN 公表日	CVSS 基本値
17	JVN#87760109	「Nessus」におけるクロスサイト・スクリプティングの脆弱性	2017 年 5 月 9 日	4.0
18	JVN#39605485	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	2017 年 5 月 9 日	6.8
19 (#1)	JVN#51819749	「SOY CMS」におけるディレクトリ・トラバーサルの脆弱性	2017 年 5 月 11 日	6.5
20 (#1)	JVN#51978169	「SOY CMS」のインストーラにおけるクロスサイト・スクリプティングの脆弱性	2017 年 5 月 11 日	4.3
21	JVN#16248227	「PrimeDrive デスクトップアプリケーション」のインストーラにおける実行ファイル読み込みに関する脆弱性	2017 年 5 月 12 日	6.8
22 (#1)	JVN#96165722	WordPress 用プラグイン「WP Booking System」におけるクロスサイト・スクリプティングの脆弱性	2017 年 5 月 16 日	5.0
23 (#1)	JVN#85512750	「定量的プロジェクト管理ツール」におけるクロスサイト・スクリプティングの脆弱性	2017 年 5 月 19 日	4.0
24 (#1)	JVN#11326581	「定量的プロジェクト管理ツール」におけるクロスサイト・スクリプティングの脆弱性	2017 年 5 月 19 日	4.3
25 (#1)	JVN#12493656	「定量的プロジェクト管理ツール」のインストーラにおける任意の DLL 読み込みに関する脆弱性	2017 年 5 月 19 日	6.8
26 (#3)	JVN#91438377	「SSL Visibility Appliance」における RST パケットの生成に関する問題	2017 年 5 月 24 日	5.0
27	JVN#42164352	「GroupSession」におけるアクセス制限不備の脆弱性	2017 年 5 月 25 日	4.0
28	JVN#75514460	防衛装備庁が提供する電子入札・開札システムのインストーラにおける DLL 読み込みに関する脆弱性	2017 年 5 月 25 日	6.8
29	JVN#41185163	航空自衛隊が提供するスクリーンセーバーのインストーラにおける DLL 読み込みに関する脆弱性	2017 年 5 月 25 日	6.8
30	JVN#92422409	「商業登記電子認証ソフト」のインストーラにおける DLL 読み込みに関する脆弱性	2017 年 5 月 26 日	6.8
31	JVN#51274854	シャープ製住民基本台帳用 IC カードリーダライタ関連の複数のソフトウェアにおける DLL 読み込みに関する脆弱性	2017 年 6 月 1 日	6.8
32 (#1)	JVN#06770361	「Tera Term」のインストーラにおける DLL 読み込みに関する脆弱性	2017 年 6 月 1 日	6.8
33	JVN#91170929	「SaAT Netizen」のインストーラにおける DLL 読み込みに関する脆弱性	2017 年 6 月 2 日	6.8
34	JVN#08020381	「SaAT Personal」のインストーラにおける DLL 読み込みに関する脆弱性	2017 年 6 月 2 日	6.8
35	JVN#24087303	環境省が提供する「報告書作成支援ツール」のインストーラにおける任意の DLL 読み込みの脆弱性	2017 年 6 月 2 日	6.8
36 (#1)	JVN#98617234	WordPress 用プラグイン「Multi Feed Reader」における SQL インジェクションの脆弱性	2017 年 6 月 6 日	6.5
37	JVN#80238098	「脆弱性体験学習ツール AppGoat」において任意のコードが実行可能な脆弱性	2017 年 6 月 6 日	6.8

項番	脆弱性識別番号	脆弱性	JVN 公表日	CVSS 基本値
38	JVN#32120290	「脆弱性体験学習ツール AppGoat」における情報漏えいの脆弱性	2017 年 6 月 6 日	4.3
39	JVN#20870477	「脆弱性体験学習ツール AppGoat」において任意のコードが実行可能な脆弱性	2017 年 6 月 6 日	6.8
40	JVN#01404851	「脆弱性体験学習ツール AppGoat」において任意のコードが実行可能な脆弱性	2017 年 6 月 6 日	6.8
41	JVN#99737748	「AppCheck」における実行ファイル呼び出しに関する脆弱性	2017 年 6 月 7 日	6.8
42	JVN#52691241	国土地理院が提供する複数のソフトウェアのインストーラにおける任意の DLL 読み込みの脆弱性	2017 年 6 月 8 日	6.8
43	JVN#31236539	「[Simeji Windows 版(β)]文字入力システム」のインストーラにおける DLL 読み込みに関する脆弱性	2017 年 6 月 8 日	6.8
44	JVN#67305782	「CASL II シミュレータ（自己解凍形式）」のインストーラにおける DLL 読み込みに関する脆弱性	2017 年 6 月 9 日	6.8
45	JVN#34508179	「事前準備セットアップファイル」のインストーラにおける DLL 読み込みに関する脆弱性	2017 年 6 月 9 日	6.8
46	JVN#65154137	「電子納品チェックシステム（農林水産省農業農村整備事業版）」のインストーラにおける DLL 読み込みの脆弱性	2017 年 6 月 9 日	6.8
47	JVN#27198823	防衛装備庁が提供する「電子入札・開札システム」のインストーラにおける実行ファイル呼び出しに関する脆弱性	2017 年 6 月 12 日	6.8
48	JVN#25078144	「ソースコードセキュリティ検査ツール iCodeChecker」におけるクロスサイト・スクリプティングの脆弱性	2017 年 6 月 13 日	4.3
49 (#1)	JVN#79738260	WordPress 用プラグイン「WordPress Download Manager」における複数の脆弱性	2017 年 6 月 13 日	4.3
50	JVN#94771799	「QuickTime 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	2017 年 6 月 13 日	6.8
51 (#1)	JVN#56787058	WordPress 用プラグイン「WP Job Manager」におけるアクセス制限不備の問題	2017 年 6 月 15 日	5.0
52 (#3)	JVN#24348065	「HOME SPOT CUBE2」における複数の脆弱性	2017 年 6 月 20 日	5.8
53 (#3)	JVN#65411235	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クロスサイト・リクエスト・フォージェリの脆弱性	2017 年 6 月 20 日	4.0
54	JVN#09293613	「キャラミん OMP」のインストーラにおける任意の DLL 読み込みに関する脆弱性	2017 年 6 月 23 日	6.8
55	JVN#01775119	文部科学省が提供する「電子入札設定チェックツール」における DLL 読み込みに関する脆弱性	2017 年 6 月 26 日	6.8
56 (#1)	JVN#21174546	「Marp」の JavaScript 実行処理におけるアクセス制限不備の脆弱性	2017 年 6 月 28 日	6.8
57	JVN#79451345	「e-Tax ソフト (WEB 版) 事前準備セットアップ」のインストーラにおける DLL 読み込みに関する脆弱性	2017 年 6 月 28 日	6.8

項番	脆弱性識別番号	脆弱性	JVN 公表日	CVSS 基本値
58	JVN#23389212	法務省が提供する「申請用総合ソフト」のインストーラにおける任意の DLL 読み込みに関する脆弱性	2017 年 6 月 30 日	6.8
59	JVN#45134765	法務省が提供する「PDF 署名プラグイン」のインストーラにおける任意の DLL 読み込みに関する脆弱性	2017 年 6 月 30 日	6.8
脆弱性の深刻度=レベル I（注意）、CVSS 基本値=0.0～3.9				
60	JVN#87770873	「CS-Cart」日本語版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	2017 年 4 月 6 日	2.6
61 (#1)	JVN#17633442	WordPress 用プラグイン「WP Statistics」におけるクロスサイト・スクリプティングの脆弱性	2017 年 4 月 10 日	2.6
62	JVN#82019695	「ASSETBASE」におけるクロスサイト・スクリプティングの脆弱性	2017 年 4 月 11 日	2.6
63 #3)	JVN#01537659	「WN-AC1167GR」におけるクロスサイト・スクリプティングの脆弱性	2017 年 4 月 14 日	1.4
64 (#3)	JVN#08740778	「NETGEAR ProSAFE Plus Configuration Utility」におけるアクセス制限不備の脆弱性	2017 年 4 月 18 日	2.9
65 (#1)	JVN#70411623	WordPress 用プラグイン「MaxButtons」におけるクロスサイト・スクリプティングの脆弱性	2017 年 5 月 16 日	2.6
66 (#1)	JVN#24834813	複数の BestWebSoft 製 WordPress 用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	2017 年 5 月 16 日	2.6
67 (#3)	JVN#46372675	「FlashAir」のフォトシェア機能におけるアクセス制限不備の脆弱性	2017 年 5 月 16 日	2.7
68 (#3)	JVN#81820501	「FlashAir」のフォトシェア機能に SSID およびパスワード固定の脆弱性	2017 年 5 月 16 日	3.3
69 (#1)	JVN#70951878	WordPress 用プラグイン「WP Live Chat Support」におけるクロスサイト・スクリプティングの脆弱性	2017 年 6 月 1 日	2.6
70 (#2)	JVN#56588965	Android アプリ「サイボウズ KUNAI for Android」におけるクロスサイト・スクリプティングの脆弱性	2017 年 6 月 12 日	2.6
71 (#1)	JVN#51355647	WordPress 用プラグイン「WP-Members」におけるクロスサイト・スクリプティングの脆弱性	2017 年 6 月 13 日	2.6
72 (#1)	JVN#73550134	WordPress 用プラグイン「Event Calendar WD」におけるクロスサイト・スクリプティングの脆弱性	2017 年 6 月 20 日	2.6

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

表 2-4、2-5 は、本四半期に 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。本四半期には、表 2-4 に示した脆弱性情報 28 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	ISC BIND に複数の脆弱性	複数製品開発者へ通知
2	ServerProtect for Linux における複数の脆弱性	特定製品製品開発者と調整
3	Deep Discovery Email Inspector に任意のコードが実行可能な脆弱性	特定製品製品開発者と調整
4	Deep Discovery Email Inspector に複数の脆弱性	特定製品製品開発者と調整
5	Apache HTTP Web Server における複数の脆弱性に対するアップデート	複数製品開発者へ通知
6	Acronis True Image に更新がセキュアに行われない脆弱性	注意喚起として掲載
7	Samsung Magician に更新がセキュアに行われない脆弱性	注意喚起として掲載
8	ISC BIND に複数の脆弱性	複数製品開発者へ通知
9	HPE SiteScope に複数の脆弱性	注意喚起として掲載
10	CalAmp LMU-3030 デバイスの SMS インターフェースに認証設定が行われていない脆弱性	注意喚起として掲載
11	libmtk 向けの httpd プラグインを使用する複数の WiMAX ルータに認証回避の脆弱性	複数製品開発者へ通知
12	Apache Tomcat にセキュリティ制限回避の脆弱性	複数製品開発者へ通知
13	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
14	スマートフォンアプリ「Space Coast Credit Union SCCU Mobile」における 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
15	iOS アプリ「Think Mutual Bank Mobile Banking App」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
16	Intel Active Management Technology (AMT) にアクセス制限不備の脆弱性	複数製品開発者へ通知
17	Ghostscript に任意のコードが実行可能な脆弱性	緊急案件として掲載 複数製品開発者へ通知
18	Portrait Displays SDK を使用して作成されたアプリケーションに任意のコードが実行可能な脆弱性	複数製品開発者へ通知
19	IBM Lotus Domino の IMAP サーバにスタックベースのバッファオーバーフローの脆弱性	注意喚起として掲載
20	ISC BIND に複数のサービス運用妨害 (DoS) の脆弱性	複数製品開発者へ通知
21	U818A WIFI に anonymous FTP でフルアクセス可能な脆弱性	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
22	Apache Tomcat の複数の脆弱性に対するアップデート	複数製品開発者へ通知
23	Microsoft OLE URL Moniker における遠隔の HTA データに対する不適切な処理	注意喚起として掲載
24	Java で実装された複数の Action Message Format (AMF3) ライブラリに脆弱性	注意喚起として掲載
25	Trend Micro Control Manager における SQL インジェクションの脆弱性	特定製品製品開発者と調整
26	Trend Micro Control Manager における複数の脆弱性	特定製品製品開発者と調整
27	Apple iOS におけるバッファオーバーフローの脆弱性	注意喚起として掲載
28	GIGABYTE BRIX のファームウェア保護機能に複数の脆弱性	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	制御システムを狙う CrashOverride マルウェアの脅威
2	Windows アプリケーションによる DLL 読み込みやコマンド実行に関する問題

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

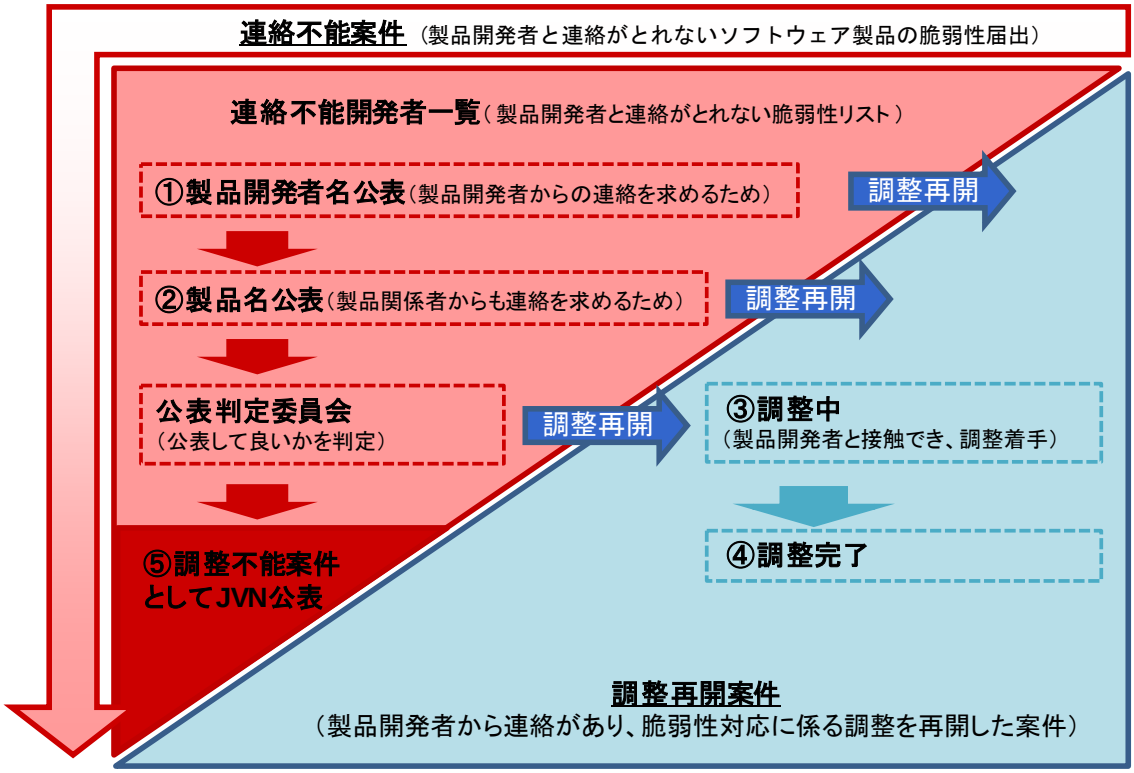
2-1-6. 連絡不能案件の処理状況

図 2-12 は、2011 年 9 月末から 2017 年 6 月末までに「連絡不能開発者」と位置づけて取扱った 251 件の処理状況の推移を示したものです。

「製品開発者名公表（①）」および、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、本四半期における新たな公表はありませんでした。また、製品開発者と調整が再開したもの（「調整中（③）」）は 1 件、本四半期の「調整完了（④）」については変動がありませんでした。

この結果、2017 年 6 月末時点で連絡不能案件（①+②）は 203 件（前四半期は 204 件）、調整再開した案件（③+④）は 46 件となりました。

なお、公表判定委員会の判定にて 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、本四半期に公表した案件はありませんでした。



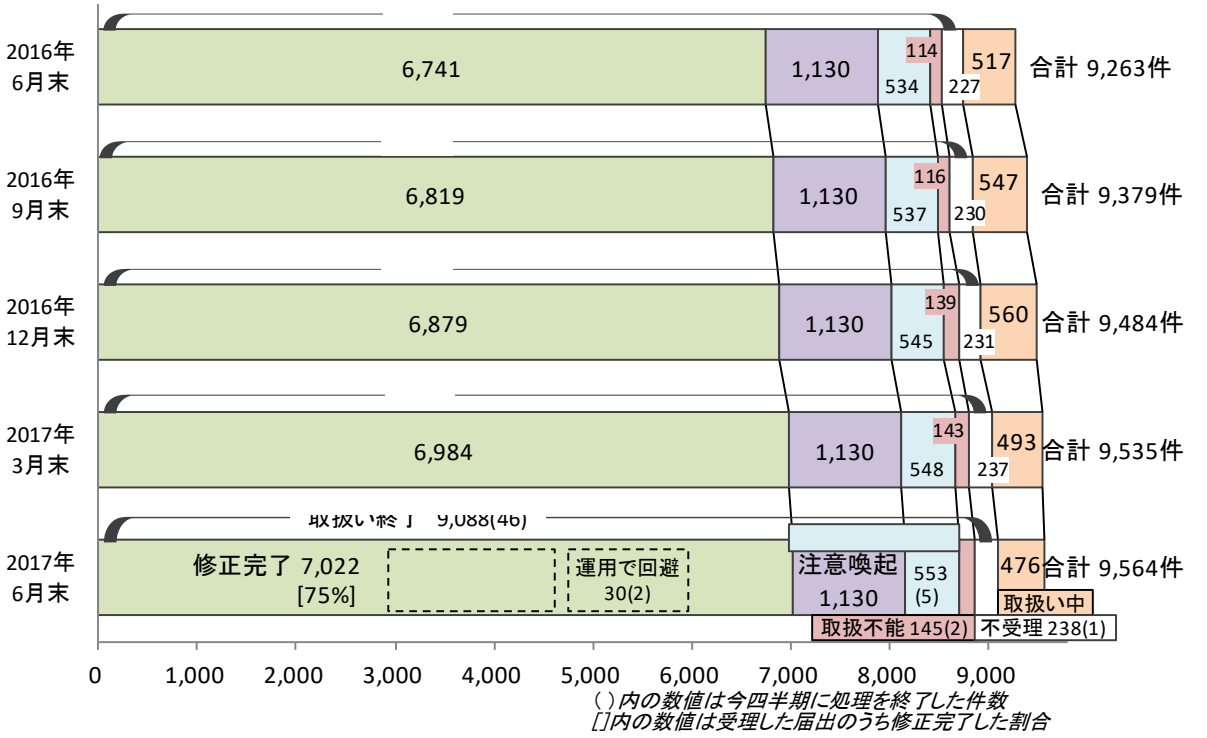
2017年 第1四半期	204件 （①1件　②203件）	45件 （③19件　④26件）	⑤2件	合計 251件
2017年 第2四半期	203件 （①1件　②202件）	46件 （③20件　④26件）	⑤2件	合計 251件

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。2017 年 6 月末時点の届出の累計は 9,564 件で、本四半期中に取扱いを終了したものは 46 件（累計 9,088 件）でした。このうち「修正完了」したものは 38 件（累計 7,022 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 5 件（累計 553 件）でした。ウェブサイト運営者への連絡手段がないなど「取扱不能」と判断したものは 2 件（累計 145 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。また「不受理」としたものは 1 件[*19]（累計 238 件）でした。取扱いを終了した累計 9,088 件のうち「修正完了」「脆弱性ではない」の合計 7,575 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 5 件（累計 1002 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 2 件（累計 30 件）でした。



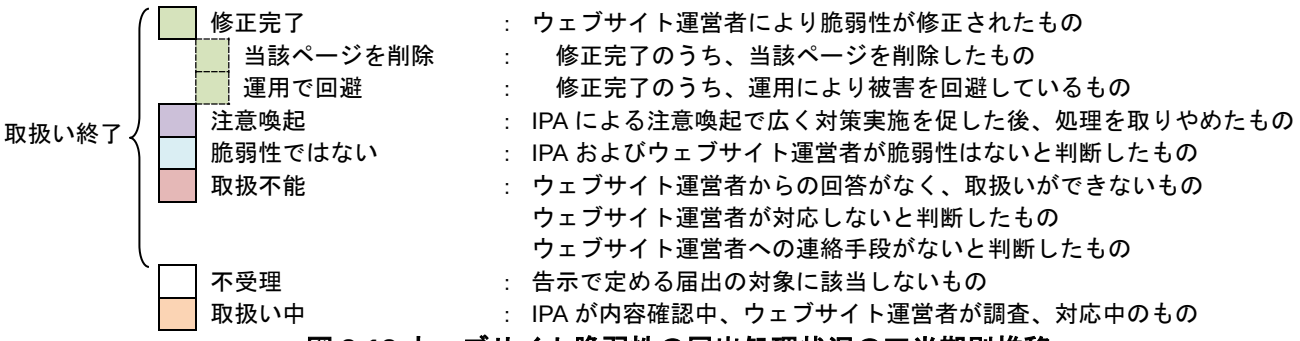


図 2-13.ウェブサイト脆弱性の届出処理状況の四半期別推移

[*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] 内訳は本四半期の届出によるもの 1 件、前四半期までの届出によるもの 0 件。

届出受付開始から本四半期までに届出のあったウェブサイトの脆弱性 9,564 件のうち、不受理を除いた件数は 9,326 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。本四半期は届出 28 件の約 9 割を企業が占めています。

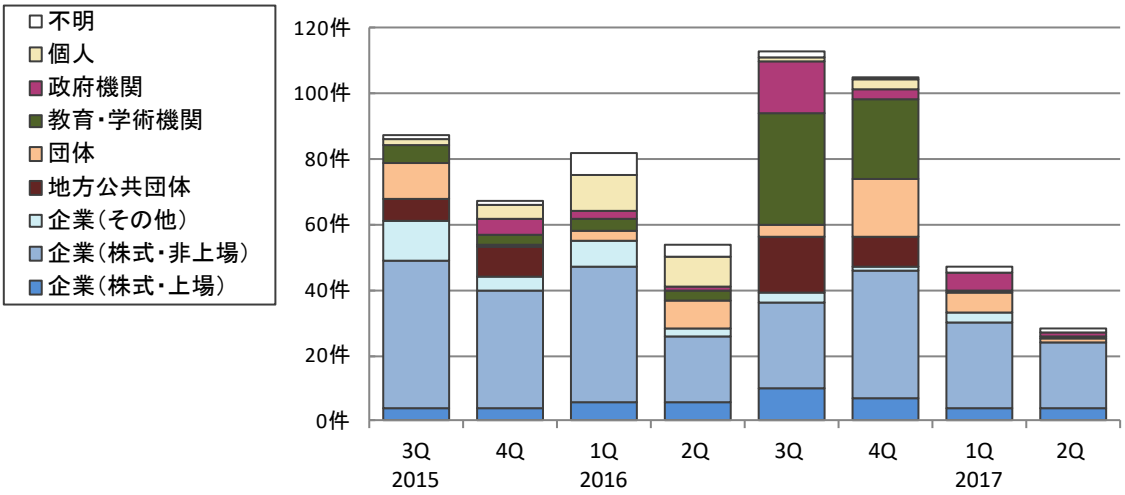


図2-14. 四半期ごとの運営主体の種類別届出件数

2-2-3. 脆弱性の種類・影響別届出件数

図 2-15、2-16 は、届出された脆弱性の種類別の分類です。図 2-15 は届出の種類別割合を、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。本四半期は約半数を占める「クロスサイト・スクリプティング（12 件）」が最も多く、次いで「SQL インジェクション（3 件）」となっています。なお、この統計は本制度における届出の傾向であり、世の中に存在する脆弱性の傾向と必ずしも一致するものではありません。

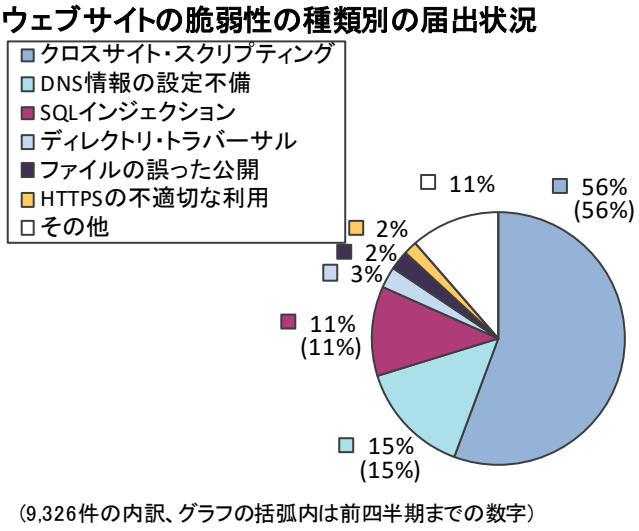


図2-15. 届出累計の脆弱性の種類別割合

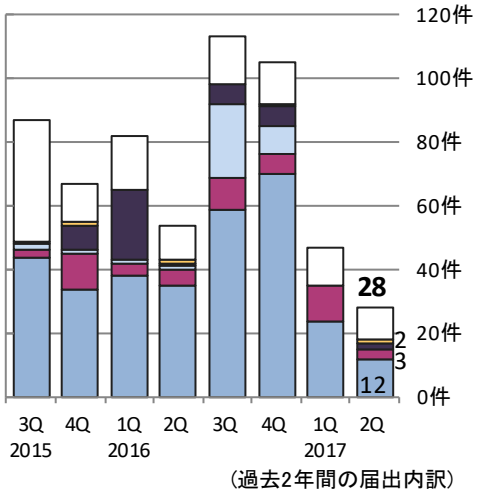


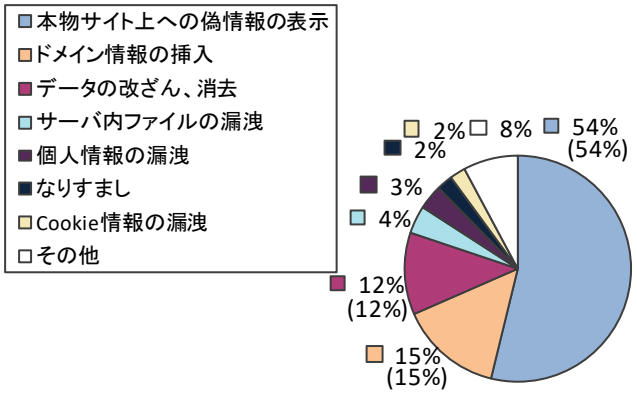
図2-16. 四半期ごとの脆弱性の種類別届出件数

[*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。

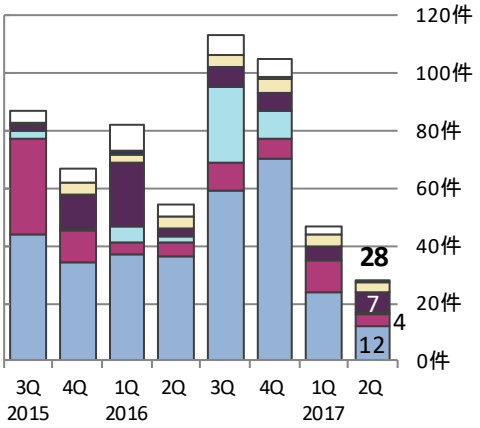
累計では、「本物サイト上への偽情報の表示」「ドメイン情報の挿入」「データの改ざん、消去」が全体の 8 割を占めています。これらは、「クロスサイト・スクリプティング」「DNS 情報の設定不備」「SQL インジェクション」などにより発生するものです。本四半期は「本物サイト上への偽情報の表示（12 件）」が最も多く、次いで「個人情報の漏洩（7 件）」「データの改ざん、消去（4 件）」となっています。

ウェブサイトの脆弱性がもたらす影響別の届出状況



(9,326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。本四半期に修正を完了した届出 38 件のうち 11 件（29%）は、運営者へ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ました。この割合は、前四半期（105 件中 88 件）の 84%より減少しています。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。本四半期の割合は 66%でした。

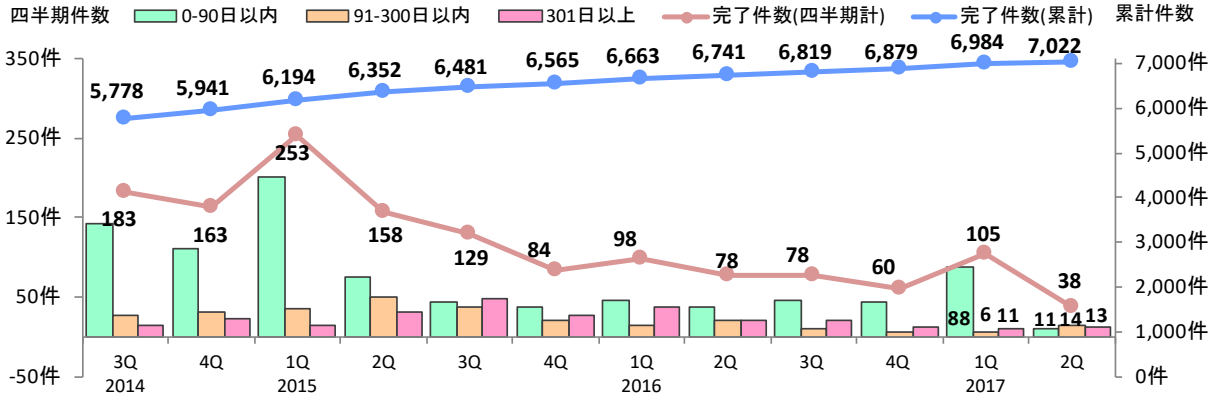


図2-19. ウェブサイトの脆弱性の修正完了件数

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 3Q	4Q	2015 1Q	2Q	3Q	4Q	2016 1Q	2Q	3Q	4Q	2017 1Q	2Q
修正完了件数	5,778	5,941	6,194	6,352	6,481	6,565	6,663	6,741	6,819	6,879	6,984	7,022
90 日以内の件数	3,872	3,982	4,184	4,260	4,303	4,341	4,387	4,425	4,471	4,514	4,602	4,613
90 日以内の割合	67%	67%	68%	67%	66%	66%	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。

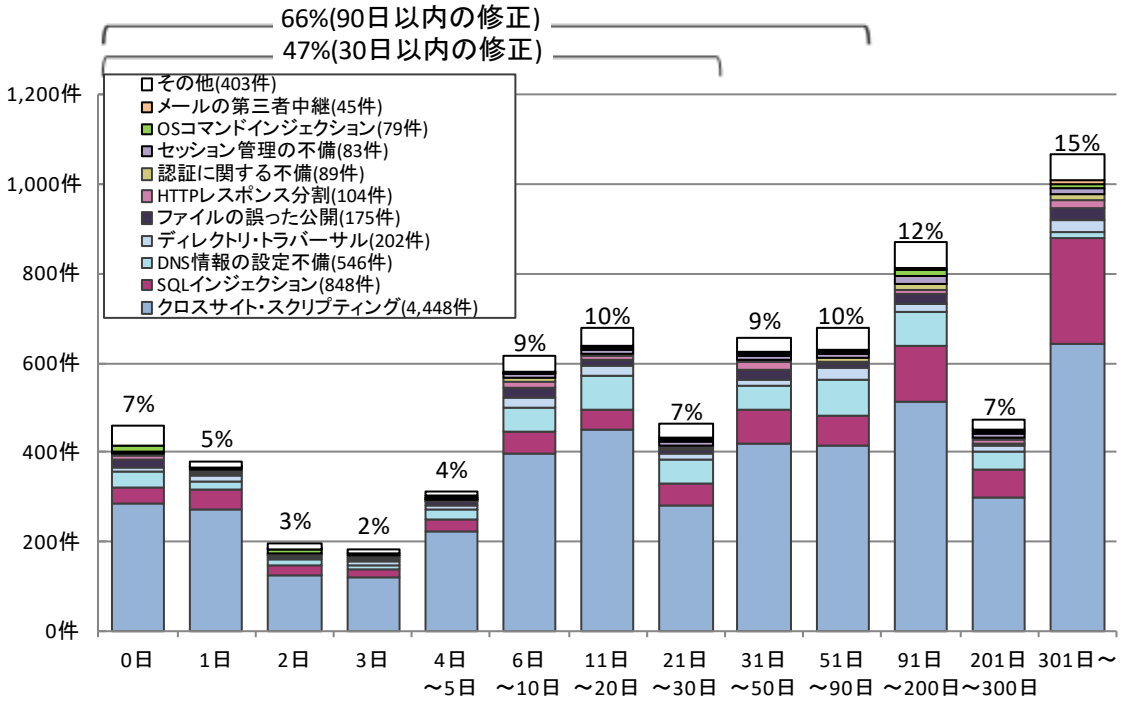


図2-20. ウェブサイトの修正に要した日数

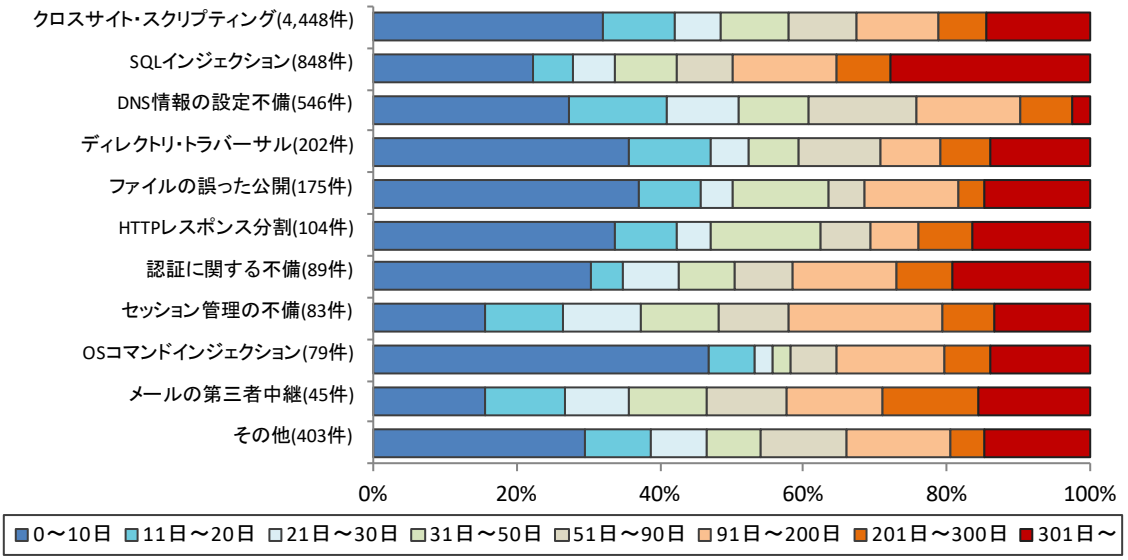


図2-21. ウェブサイトの修正に要した脆弱性種類別の日数の傾向

[*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 日は脆弱性関連情報を通知した当日に修正されたもの、または運営者へ脆弱性関連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ない場合、IPA は 1～2 ヶ月毎にメールや電話、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 376 件（前四半期は 387 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 17%を占めています。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。

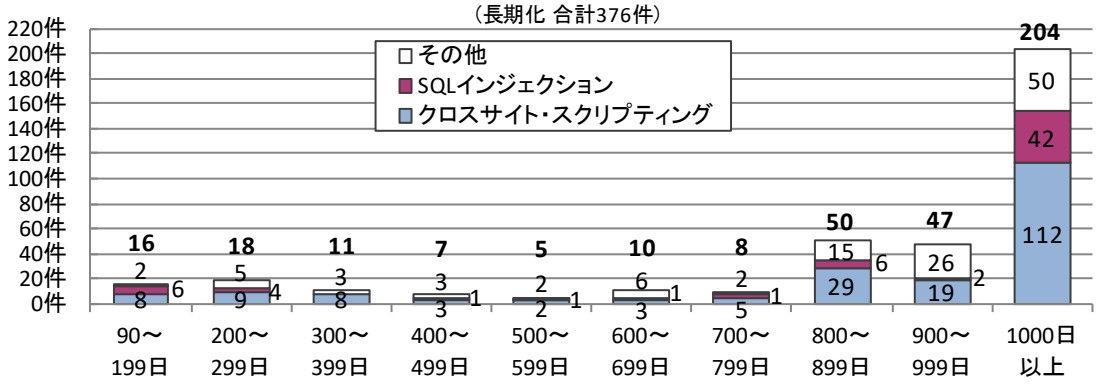


図2-22. 取扱いが長期化(90日以上経過)している届出の取扱経過日数と脆弱性の種類

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 3Q	4Q	2016 1Q	2Q	3Q	4Q	2017 1Q	2Q
取扱い中の件数	608	591	567	517	547	560	493	476
長期化している件数	504	473	436	401	388	374	387	376
長期化している割合	83%	80%	77%	78%	71%	67%	78%	79%

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：製品出荷前に未知の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

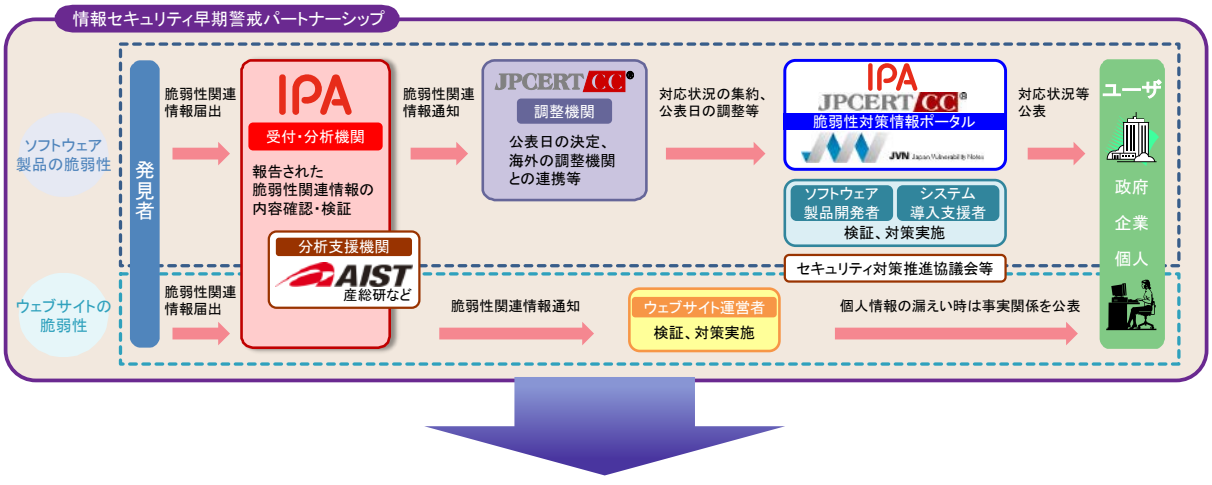
付表 2. ウェブサイトの脆弱性の分類

	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