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 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」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 10 月 1 日から 2017 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
2018 年 1 月 25 日

(*1) 制度発足時は「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）」の告示に基づいていましたが、現時点では次の告示に基づいています。
- 「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 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 13,523 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 4 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）から本四半期末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 37 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 33 件、合計 70 件でした。届出受付開始からの累計は 13,523 件で、内訳はソフトウェア製品に関するもの 3,895 件、ウェブサイトに関するもの 9,628 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	**37** 件	**3,895** 件
ウェブサイト	**33** 件	**9,628** 件
合計	**70** 件	**13,523** 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。本四半期末までの 1 就業日あたりの届出件数は 4.11 件[(*3)]でした。

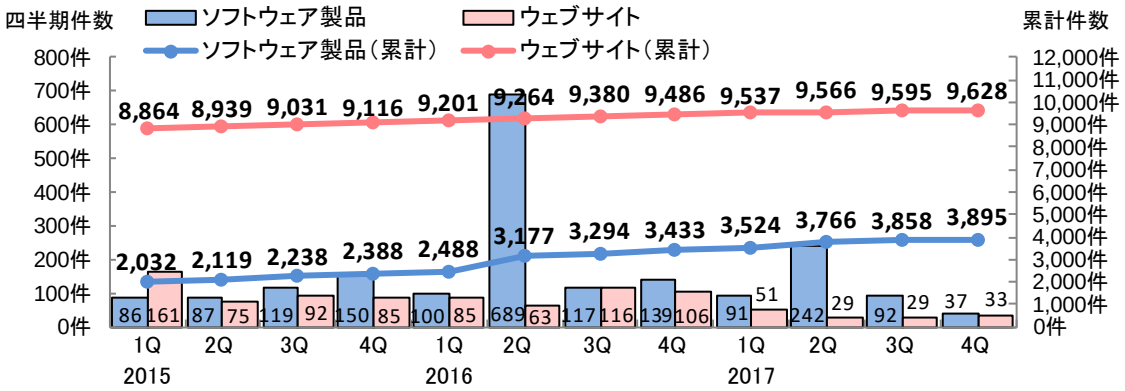


図1−1. 脆弱性の届出件数の四半期ごとの推移

表 1-2. 届出件数（過去 3 年間）

	2015 1Q	2Q	3Q	4Q	2016 1Q	2Q	3Q	4Q	2017 1Q	2Q	3Q	4Q
累計届出件数[件]	10,896	11,058	11,269	11,504	11,689	12,441	12,674	12,919	13,061	13,332	13,453	13,523
1 就業日あたり[件/日]	4.17	4.13	4.11	4.11	4.09	4.26	4.25	4.25	4.21	4.21	4.17	4.11

(*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。

また、図 1-2 は、届出受付開始から 2017 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年は、2008 年（2,622 件）でした。2017 年はソフトウェア製品が 462 件、ウェブサイトが 142 件の合計 604 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 割以上を占めています。またウェブサイトの届出は昨年に比べ半減しました。

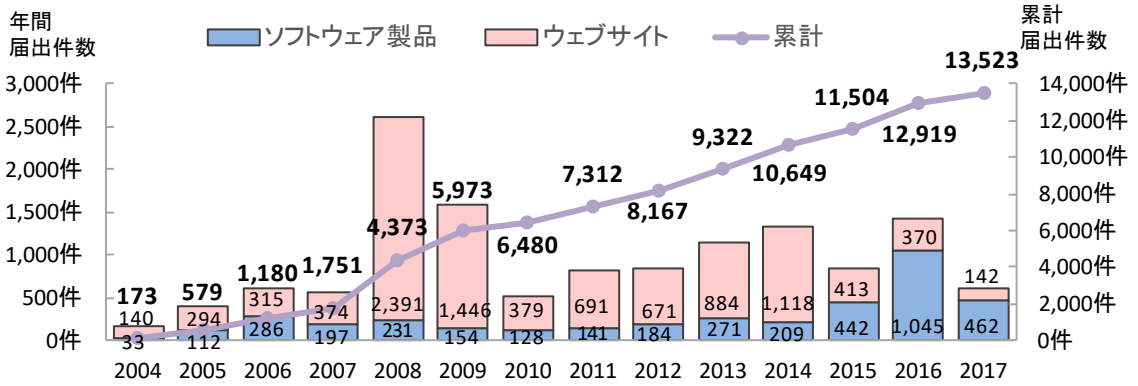


図1−2. 脆弱性関連情報の届出件数の年ごとの推移

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 8,809 件 ～

表 1-3 は本四半期、および届出受付開始から本四半期末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	**40** 件	**1,704** 件
ウェブサイト	**23** 件	**7,105** 件
合計	**63** 件	**8,809** 件

本四半期に JVN 公表したソフトウェア製品の件数は 40 件 (*4)（累計 1,704 件）でした。そのうち、6 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 5 件（13%）でした。

また、修正完了したウェブサイトの件数は 23 件（累計 7,105 件）でした。修正を完了した 23 件のうち、ウェブアプリケーションを修正したものは 19 件（82%）、当該ページを削除したものは 4 件（18%）で、運用で回避したものはありませんでした。なお、修正を完了した 23 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 14 件（61%）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（60 件中 33 件（55%））より増加しています。

また、図 1-3 は、届出開始から 2017 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年は 2009 年の 1,401 件でした。2017 年は、ソフトウェア製品が 322 件、ウェブサイトが 226 件の合計 548 件でした。2017 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。

(*4) P.12 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。

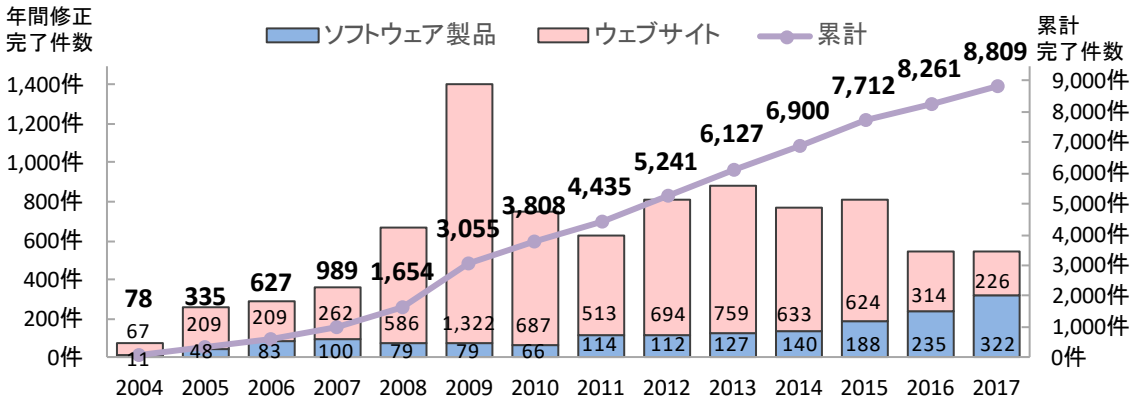


図1−3. 脆弱性関連情報の修正完了件数の年ごとの推移

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[(*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、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。本四半期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のは 230 件になります。また、2017 年 12 月に第 1 回目の公表判定委員会を開催し、4 件の脆弱性情報について判定しました。

(*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。

1-4. JVN で公表した脆弱性について

1-4-1. 複数の製品の DLL 読み込みの脆弱性

～ 影響を受ける製品が多い脆弱性、しかし悪用は困難 ～

2017 年に JVN（Japan Vulnerability Notes）にて公表された DLL 読み込みの脆弱性は 70 件で(表 1-4-1)それ以前（2016 年：42 件、2015 年：4 件）と比べて著しく増加しています。

表 1-4-1. JVN で公表された DLL 読み込みの脆弱性の一覧

#	JVN 番号	2017 年度に DLL の脆弱性対策情報が公開された製品	公開日
第１四半期（4 件）			
1	JVN#40667528	Norton Download Manager	2/10
2	JVN#86200862	7-ZIP32.DLL で作成された自己解凍書庫	2/17
3	JVN#88713190	PrimeDrive デスクトップアプリケーション のインストーラ	3/1
4	JVN#93699304	PhishWall クライアント Internet Explorer 版 のインストーラ	3/22
第２四半期（23 件）			
5	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	4/14
6	JVN#54268888	花子 を含む複数の製品	4/20
7	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	5/9
8	JVN#12493656	定量的プロジェクト管理ツール のインストーラ	5/19
9	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	5/25
10	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	5/25
11	JVN#92422409	商業登記電子認証ソフト のインストーラ	5/26
12	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	6/1
13	JVN#06770361	Tera Term のインストーラ	6/1
14	JVN#91170929	SaAT Netizen のインストーラ	6/2
15	JVN#08020381	SaAT Personal のインストーラ	6/2
16	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	6/2
17	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	6/8
18	JVN#31236539	[Simeji Windows 版(β)]文字入力システム のインストーラ	6/8
19	JVN#67305782	CASL II シミュレータ（自己解凍形式） のインストーラ	6/9
20	JVN#34508179	事前準備セットアップファイル のインストーラ	6/9
21	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	6/9
22	JVN#94771799	QuickTime for Windows のインストーラ	6/13
23	JVN#09293613	キャラミん OMP のインストーラ	6/23
24	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	6/26
25	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	6/28
26	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	6/30
27	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	6/30
第３四半期（34 件）			
28	JVN#06337557	国土交通省が提供する電子成果物作成支援・検査システム のインストーラおよびインストーラを含む自己解凍書庫	7/3
29	JVN#82120115	国土交通省国土技術政策総合研究所が提供する道路工事完成図等チェックプログラム のインストーラ	7/4
30	JVN#20409270	国土交通省国土技術政策総合研究所が提供する道路施設基本データ作成システム のインストーラ	7/4

#	JVN 番号	2017 年度に DLL の脆弱性対策情報が公開された製品	公開日
31	JVN#21369452	Lhaz と Lhaz+ のインストーラ、および Lhaz や Lhaz+ で作成された自己解凍書庫ファイル	7/7
32	JVN#21627267	Microsoft IME	7/7
33	JVN#29939155	ファイルコンパクトで作成された自己解凍書庫ファイル	7/10
34	JVN#81676004	Windows 版 Mozilla Firefox および Thunderbird のインストーラ	7/11
35	JVN#02852421	Yahoo!ツールバー（Internet explorer 版）のインストーラ	7/12
36	JVN#42031953	FileCapsule Deluxe Portable およびFileCapsule Deluxe Port-	7/13
37	JVN#61502349	アタッシェケース で作成された自己実行可能形式の暗号化ファイル	7/14
38	JVN#17523256	Tween のインストーラ	7/24
39	JVN#16136413	ソニー製 PaSoRi 関連ソフトウェアの複数のインストーラ	7/27
40	JVN#74554973	LhaForge のインストーラ	7/27
41	JVN#33797604	NFC ポートソフトウェアリムーバー	7/27
42	JVN#17788774	Baidu IME 文字入力システム のインストーラ	8/3
43	JVN#86724730	IP Messenger のインストーラ	8/3
44	JVN#81659403	Qua station 接続ツール（Windows 版）のインストーラ	8/8
45	JVN#53292345	定期報告書作成支援ツール	8/17
46	JVN#73559859	新・基幹統計報告データ入力用プログラム のインストーラ	8/17
47	JVN#71104430	新・石油輸入調査報告データ入力プログラム のインストーラ	8/17
48	JVN#23546631	新・緊急時報告データ入力プログラム のインストーラ	8/17
49	JVN#18641169	TypeA ご利用ソフト のインストーラおよびインストーラを含む自己解凍書庫	8/18
50	JVN#67954465	株式会社 NTT ドコモが提供するフォトコレクション PC ソフト の	8/22
51	JVN#30866130	商業登記電子認証ソフト のインストーラ	8/23
52	JVN#87540575	Optimal Guard のインストーラ	8/25
53	JVN#11601216	セキュリティ機能見張り番 のインストーラ	8/25
54	JVN#14658714	フレッツ・あずけ～る Windows 用 PC 自動バックアップツール の	8/25
55	JVN#14926025	フレッツインストールツール のインストーラ	8/25
56	JVN#36303528	セキュリティセットアップツール のインストーラおよびインス	8/25
57	JVN#22272314	フレッツ接続ツール のインストーラ	8/25
58	JVN#26115441	リモートサポートツール（遠隔サポートツール） のインストーラ	8/30
59	JVN#09769017	富士ゼロックス株式会社製の複数の製品	8/31
60	JVN#57205588	FENCE-Explorer のインストーラ	9/11
61	JVN#75929834	i-フィルター 6.0 のインストール プログラムおよびインストーラ	9/14
第４四半期（9 件）			
62	JVN#55516206	秘文 機密ファイル復号プログラム	10/11
63	JVN#58909026	秘文 機密ファイル復号プログラム	10/11
64	JVN#94056834	秘文 機密ファイルビューア のインストーラ	10/11
65	JVN#97243511	フレッツ簡単セットアップツール のインストーラ	11/2
66	JVN#71284826	HYPER SBI のインストーラ	11/9
67	JVN#08517069	Media Go および Music Center for PC のインストーラ	11/21
68	JVN#30352845	Windows 版公的個人認証サービス　利用者クライアントソフト	12/6
69	JVN#95423049	コンテンツ管理アシスタント for PlayStation のインストーラ	12/22
70	JVN#60695371	Music Center for PC のインストーラ	12/22

DLL 読み込みの脆弱性は、Windows アプリケーションの実行時の動作を悪用するものです。Windows アプリケーションは、実行時に同じフォルダーに格納されている DLL ファイルを優先的に読み込む動作をします。この動作を悪用し、同じフォルダーに悪意のあるコードを含む DLL ファイルを配置しておくことで、この DLL ファイルを読み込ませ実行させます。

この脆弱性は、ユーザの利用端末上で悪意のあるコードを実行されるという点では危険な脆弱性であると言えます。しかしながら、Windows アプリケーションの実行時に、同じフォルダーに悪意のある DLL ファイルを配置するという前提条件は現実的には厳しく、またユーザが適切に注意することで攻撃を防ぐことが可能であるため、実際に悪用され、被害が報告された事例はほとんど確認されていません。

IPA では、この脆弱性に関する注意喚起（【注意喚起】Windows アプリケーションの利用における注意）を実施し、一般の利用者向けに、この脆弱性に関する注意を広く呼び掛けました。

また、この脆弱性は産業制御システムで用いられる製品でも確認されています。米国 DHS(国土保安省)で制御システム・セキュリティを担当する ICS-CERT が、2017 年に公表した産業制御システムで用いられる製品における DLL 読み込みの脆弱性対策情報は 16 件でした。これについても、それ以前（2014 年：1 件、2015 年：5 件、2016 年：2 件、2017 年：16 件）と比べて増加傾向にあります。

このように、この脆弱性は攻撃のための前提条件が厳しいとはいえ、影響範囲は多岐にわたるものであり、攻撃が成功した際の影響も大きいものとなります。

利用者側で行える対策として、アプリケーションをダウンロードする場合は、新規に作成したフォルダーに保存する事や、既にダウンロードフォルダーに保存しているファイルを、別のフォルダーへ移動する等して、不審なファイルが存在しない環境で実行することがあげられます。また、止むを得ず他のファイルが存在するフォルダー内でアプリケーションを実行する場合は、同じフォルダー内に不審なファイルが存在しないか確認するといった対策を心がける必要があります。

1-4-2. システムに潜在する脆弱性を狙う攻撃に注意

～　古くから知られている脆弱性が残されていないか見直しを　～

日々新しい脆弱性やその攻撃手法が登場しており、最新のセキュリティ情報を収集することが重要です。しかし、その一方で古くから知られている脆弱性への対応も疎かにならないように注意しなければなりません。

2017 年には、XXE（XML External Entity）という脆弱性が届け出られました。この脆弱性は複数件届け出られており、そのうちの 1 件については既に対策が完了し、脆弱性対策情報が JVN において公表されている状況です。

XXE は、OWASP Top 10 - 2017 にて、セキュリティリスクの Top 10 に数えられており、何らかの形で XML を解析するほとんどすべての Web アプリケーションに影響する脆弱性です。

XXE は Web アプリケーションが XML を解釈する際の処理を悪用して、リクエストを偽造する脆弱性および攻撃手法を指します。具体的には、XML で用いられる DTD と呼ばれるデータ型を定義するスキーマ言語に対し、不正な文字列を挿入することにより、XML を解析する Web アプリケーションを誤作動させ、本来意図されていない悪意のある操作を実行するものです。この脆弱性を悪用された場合、サーバ上の情報が漏えいしたり、サービス運用妨害 (DoS)等の攻撃を受けたりする可能性があります。(図 1-4-1)

XXE は他の脆弱性ほど一般的ではありませんが、新しい脆弱性というわけではなく、2000 年代前半から確認されていることから、むしろ古い脆弱性であると言えます。

しかし、多くの Web アプリケーションや製品には、脆弱性の残る古い XML 処理システムが残されており、攻撃が成功しやすいことから脅威として注目されています。

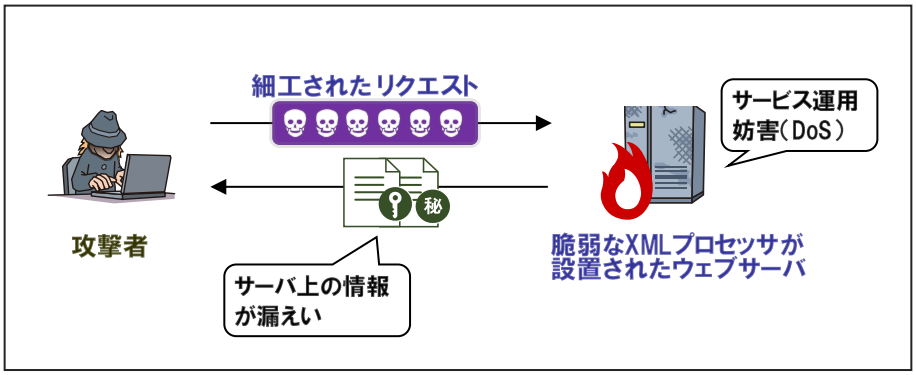


図 1-4-1. XXE の脆弱性を悪用するイメージ図

XXE の対策としては、DTD 自体の無効化、XML プロセッサ（XML パーサ）およびライブラリ（例えば libxml2 等）のアップグレード、サーバー側の入力検証（フィルタリング、またはサニタイズ）の実装等を製品開発者やウェブサイト運営者が適切に行う必要があります。製品開発者は、最新の脆弱性情報を収集して、自身が提供している製品について、影響が無いかを確認し、影響がある場合は脆弱性対策をして、利用者に修正版を提供してください。

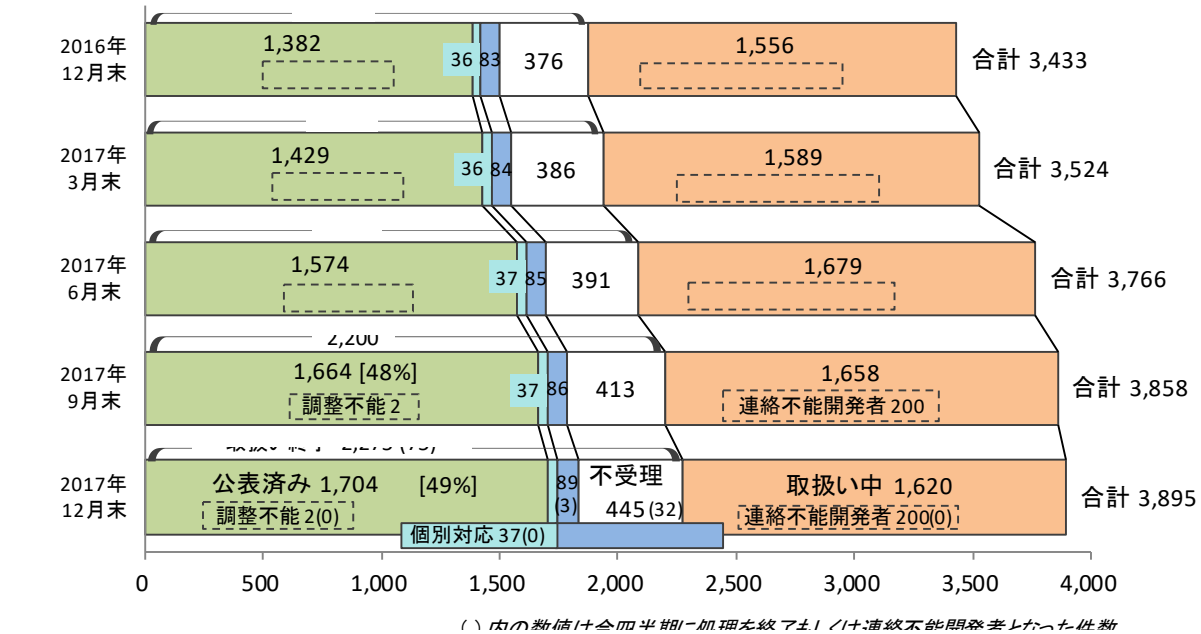
また、自社製品の脆弱性を自社内のみで見つけるのは困難な場合があります。製品の脆弱性は、製品の利用者やセキュリティ研究者等によって発見される場合もあるため、自社製品に脆弱性が発見された場合に備え、脆弱性情報を受け付ける窓口を設けておくことを推奨します。

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。本四半期末時点の届出の累計は 3,895 件で、本四半期に脆弱性対策情報を JVN 公表したものは 40 件（累計 1,704 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 37 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 89 件）でした。また「不受理」としたものは 32 件 (*9)（累計 445 件）、「取扱い中」は 1,620 件でした。1,620 件のうち、連絡不能開発者 (*10) 一覧へ新規に公表したものはありませんでした。本四半期末時点で 202 件 (*11) を連絡不能開発者一覧へ公表しています。



取扱い終了
- 公表済み：JVN で脆弱性への対応状況を公表したもの
  - 調整不能：公表判定委員会による判定にて、JVN で公表することが適当と判定されたもの
- 個別対応：JVN 公表を行わず、製品開発者が個別対応したもの
- 脆弱性ではない：製品開発者により脆弱性ではないと判断されたもの
- 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、JPCERT/CC が内容確認中、製品開発者が調査、対応中のもの
  - 連絡不能開発者：取扱い中のうち、連絡不能開発者一覧にて公表中のもの

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 2 件、前四半期までの届出によるもの 30 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末までに届出のあったソフトウェア製品の脆弱性 3,895 件のうち、不受理を除いた件数は 3,450 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（16 件）」が最も多く、次いで「ルータ（5 件）」「スマートフォン向けアプリ（2 件）」となっています。累計では、「ウェブアプリケーションソフト」が最も多く 47%を占めています。

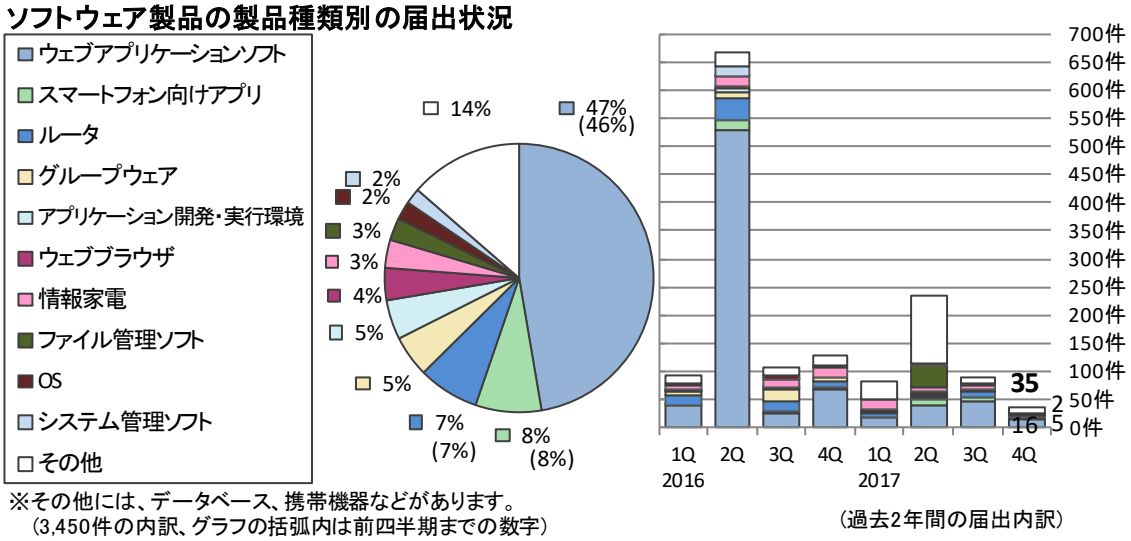


図2−2. 届出累計の製品種類別割合

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 51%、累計では 58%を占めています。

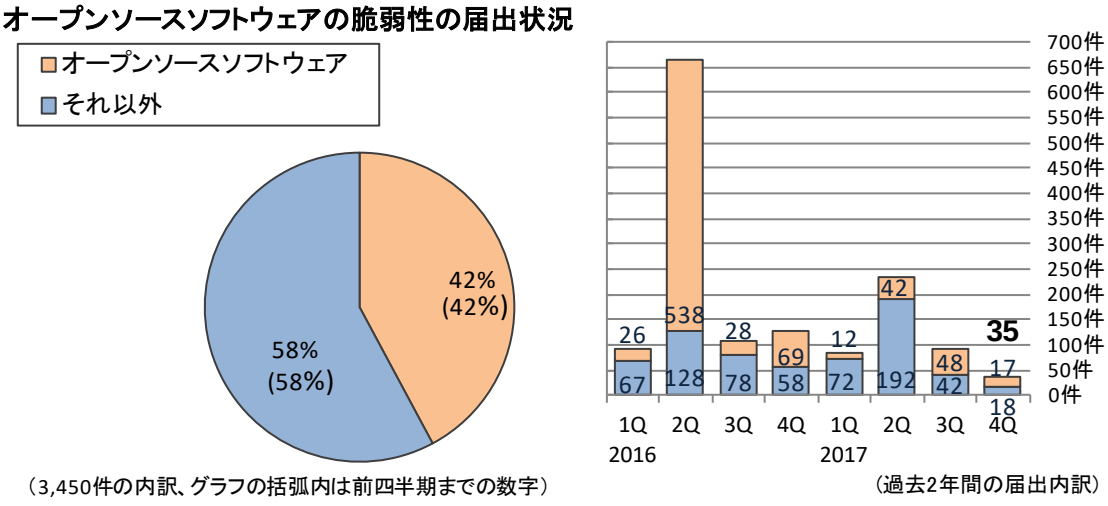


図2−4. 届出累計のオープンソースソフトウェア割合

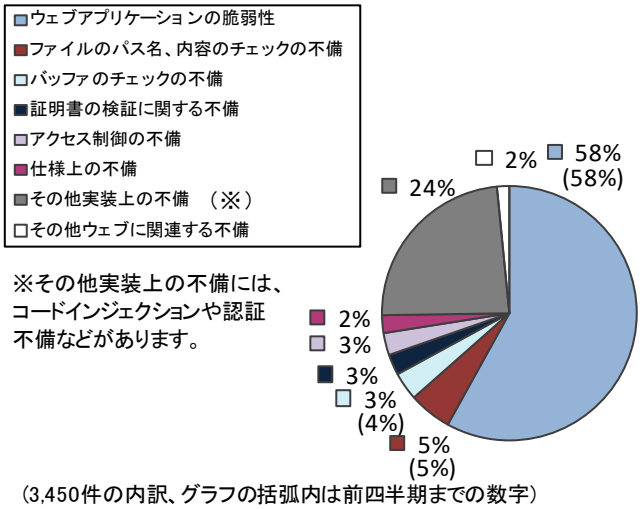
図2−5. 四半期ごとのオープンソースソフトウェア届出件数

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内訳です。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]。

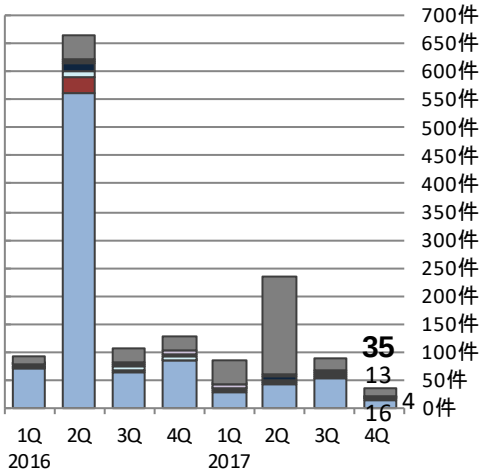
本四半期は「ウェブアプリケーションの脆弱性（16 件）」が最も多く、次いで「その他実装上の不備（13 件）」「アクセス制御の不備（4 件）」となっています。累計では、「ウェブアプリケーションの脆弱性」が過半数を占めています。

ソフトウェア製品の脆弱性の原因別の届出状況



（3,450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



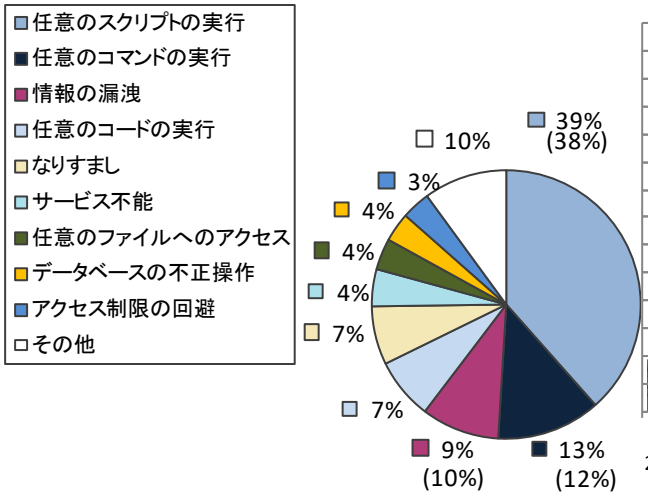
（過去2年間の届出内訳）

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内訳です。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。

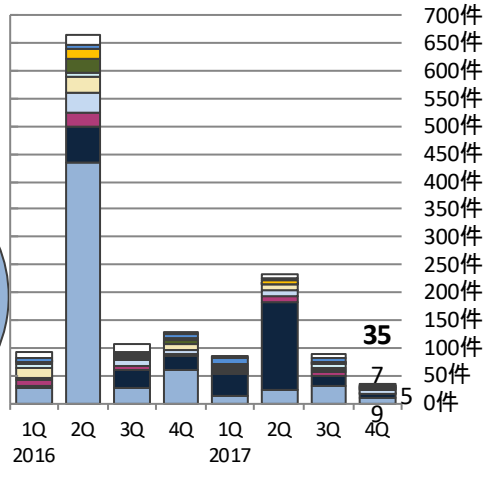
本四半期は、「任意のスクリプトの実行（9 件）」が最も多く、次いで「任意のコマンドの実行（7 件）」「任意のコードの実行（5 件）」でした。累計では「任意のスクリプトの実行」が最も多く、39%を占めています。

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



（3,450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

図 2-10 は、届出受付開始から本四半期末までに対策情報を JVN 公表した脆弱性（1,704 件）について、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 30%、45 日を超過した件数は 70%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。

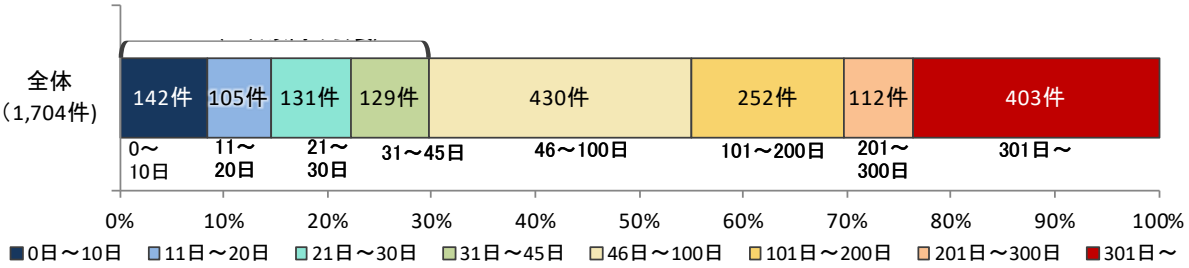


表 2-1. 45 日以内に JVN 公表した件数の割合推移（四半期ごと）

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

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	28 件	1,532 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	22 件	1,578 件
合計	50 件	3,110 件

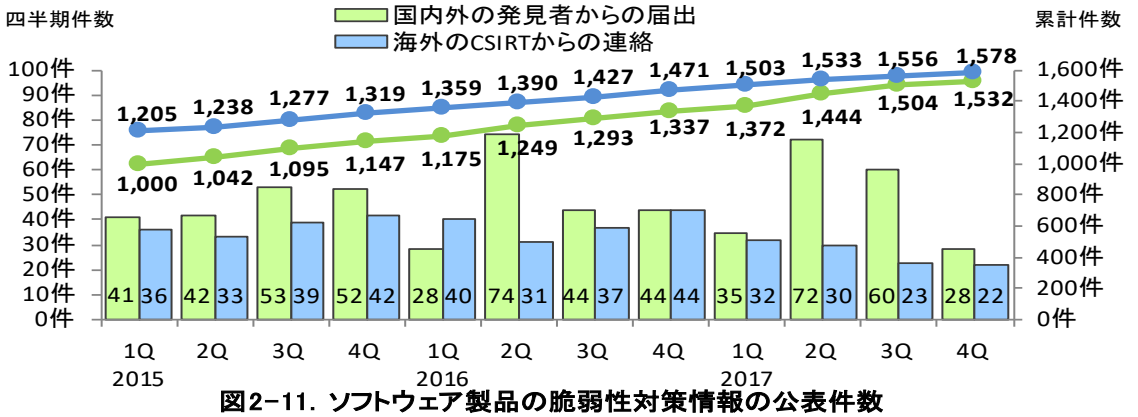


図2−11. ソフトウェア製品の脆弱性対策情報の公表件数

[*13] JPCERT/CC 活動概要 Page16～22（http://www.jpcert.or.jp/pr/2018/PR20180116.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 8 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）、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 6 件（表 2-4 の#4）ありました。

表 2-3. 2017 年第 4 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 (#4)	JVN#23367475	「Wi-Fi STATION L-02F」にバッファオーバーフローの脆弱性	2017 年 11 月 6 日	10.0
2	JVN#18420340	「BOOK☆WALKER for Windows/Mac」における複数の脆弱性	2017 年 11 月 14 日	7.1
3 (#4)	JVN#98295787	ワイヤレスモバイルストレージ「『デジ蔵 ShAirDisk』PTW-WMS1」における複数の脆弱性	2017 年 11 月 30 日	10.0
4	JVN#78501037	Movable Type 用プラグイン「A-Member」および「A-Reserve」における SQL インジェクションの脆弱性	2017 年 11 月 30 日	7.5
脆弱性の深刻度=レベル II（警告）、CVSS 基本値=4.0～6.9				
5 (#2)	JVN#14658424	「サイボウズ Office」におけるアクセス制限不備の脆弱性	2017 年 10 月 11 日	4.0
6	JVN#55516206	「秘文 機密ファイル復号プログラム」における DLL 読み込みに関する脆弱性	2017 年 10 月 11 日	6.8
7	JVN#58909026	「秘文 機密ファイル復号プログラム」における DLL 読み込みに関する脆弱性	2017 年 10 月 11 日	6.8
8	JVN#94056834	「秘文 機密ファイルビューア」のインストーラにおける DLL 読み込みおよび実行ファイル呼び出しに関する脆弱性	2017 年 10 月 11 日	6.8
9 (#4)	JVN#54795166	ホームユニット「KX-HJB1000」における複数の脆弱性	2017 年 10 月 17 日	6.5
10 (#1)	JVN#79546124	「OpenAM (オープンソース版)」における認証回避の脆弱性	2017 年 11 月 1 日	6.0
11	JVN#97243511	「フレッツ簡単セットアップツール」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 11 月 2 日	6.8
12	JVN#71284826	「HYPER SBI」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 11 月 9 日	6.8
13	JVN#29602086	「CS-Cart 日本語版」におけるクロスサイト・スクリプティングの脆弱性	2017 年 11 月 13 日	4.0
14 (#1)	JVN#05398317	WordPress 用プラグイン「TablePress」における XML 外部実体参照(XXE)処理の脆弱性	2017 年 11 月 14 日	4.0
15 (#4)	JVN#76382932	ロボット家電「COCOROBO」におけるセッション管理不備の脆弱性	2017 年 11 月 16 日	4.3
16	JVN#08517069	「Media Go」および「Music Center for PC」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 11 月 21 日	6.8

項番	脆弱性識別番号	脆弱性	JVN 公表日	CVSS 基本値
17 (#4)	JVN#73141967	「PWR-Q200」における DNS キャッシュポイズニングの脆弱性	2017 年 11 月 22 日	4.3
18 (#1)(#2)	JVN#71291160	「StreamRelay.net.exe」および「sDNSProxy.exe」におけるサービス運用妨害(DoS)の脆弱性	2017 年 11 月 29 日	5.0
19 (#4)	JVN#65994435	バッファロー製の複数の有線ブロードバンドルータに複数の脆弱性	2017 年 12 月 1 日	4.3
20	JVN#30352845	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 12 月 6 日	6.8
21 (#1)(#3)	JVN#67389262	「Qt for Android」における OS コマンド・インジェクションの脆弱性	2017 年 12 月 11 日	5.1
22 (#1)(#3)	JVN#27342829	「Qt for Android」における環境変数を改ざん可能な脆弱性	2017 年 12 月 11 日	5.1
23 (#1)(#2)	JVN#84182676	「H2O」における複数の脆弱性	2017 年 12 月 18 日	5.0
24(#1)	JVN#93333702	「OneThird CMS」にディレクトリ・トラバーサルの脆弱性	2017 年 12 月 19 日	4.0
25	JVN#95423049	「コンテンツ管理アシスタント for PlayStation」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 12 月 22 日	6.8
26	JVN#60695371	「Music Center for PC」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 12 月 22 日	6.8
27 (#1)(#3)	JVN#45494523	「MQTT.js」における PUBLISH パケットの扱いに関する問題	2017 年 12 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				
28	JVN#87886530	「LAN DISK コネクト」におけるサービス運用妨害(DoS)の脆弱性	2017 年 11 月 6 日	3.3

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

表 2-4 は、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おり、本四半期は脆弱性情報 22 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[*15]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	Dnsmasq に複数の脆弱性	複数製品開発者と調整
2	NXP Semiconductors 製 MQX RTOS における複数の脆弱性	注意喚起として掲載
3	AssetView および AssetView PLATINUM に複数の脆弱性	特定製品開発者と調整

[*15] 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
4	Adobe Flash Player に型の混同 (Type Confusion) の脆弱性	注意喚起として掲載
5	Infineon 製 RSA ライブラリが RSA 鍵ペアを適切に生成しない問題	注意喚起として掲載 複数製品開発者へ通知
6	Wi-Fi Protected Access II (WPA2) ハンドシェイクにおいて Nonce およびセッション鍵が再利用される問題	複数製品開発者と調整
7	「楽々はがき」および「楽々はがき セレクト for 一太郎」にメモリ破壊の脆弱性	特定製品開発者と調整
8	GNU Wget における複数のバッファオーバーフローの脆弱性	複数製品開発者と調整
9	Trend Micro Control Manager における複数の脆弱性	特定製品開発者と調整
10	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
11	IEEE P1735 に脆弱性	複数製品開発者と調整
12	Savitech 製 USB オーディオドライバがルート CA 証明書を許可なくインストールする問題	注意喚起として掲載
13	Packetbeat におけるサービス運用妨害 (DoS) の脆弱性	特定製品開発者と調整
14	Microsoft Office 数式エディタ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
15	Windows 8 およびそれ以降のバージョンにおいて、アドレス空間配置のランダム化が適切に行われない脆弱性	注意喚起として掲載
16	Install Norton Security for Mac 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
17	QND Advance/Standard におけるディレクトリトラバーサルの脆弱性	特定製品開発者と調整
18	Apple macOS High Sierra に無効化されているアカウントに対する認証回避の問題	注意喚起として掲載
19	Fluentd におけるエスケープシーケンスインジェクションの脆弱性	特定製品開発者と調整
20	複数の TLS 実装において Bleichenbacher 攻撃対策が不十分である問題	複数製品開発者と調整
21	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
22	InterScan Messaging Security Virtual Appliance における複数の脆弱性	特定製品開発者と調整

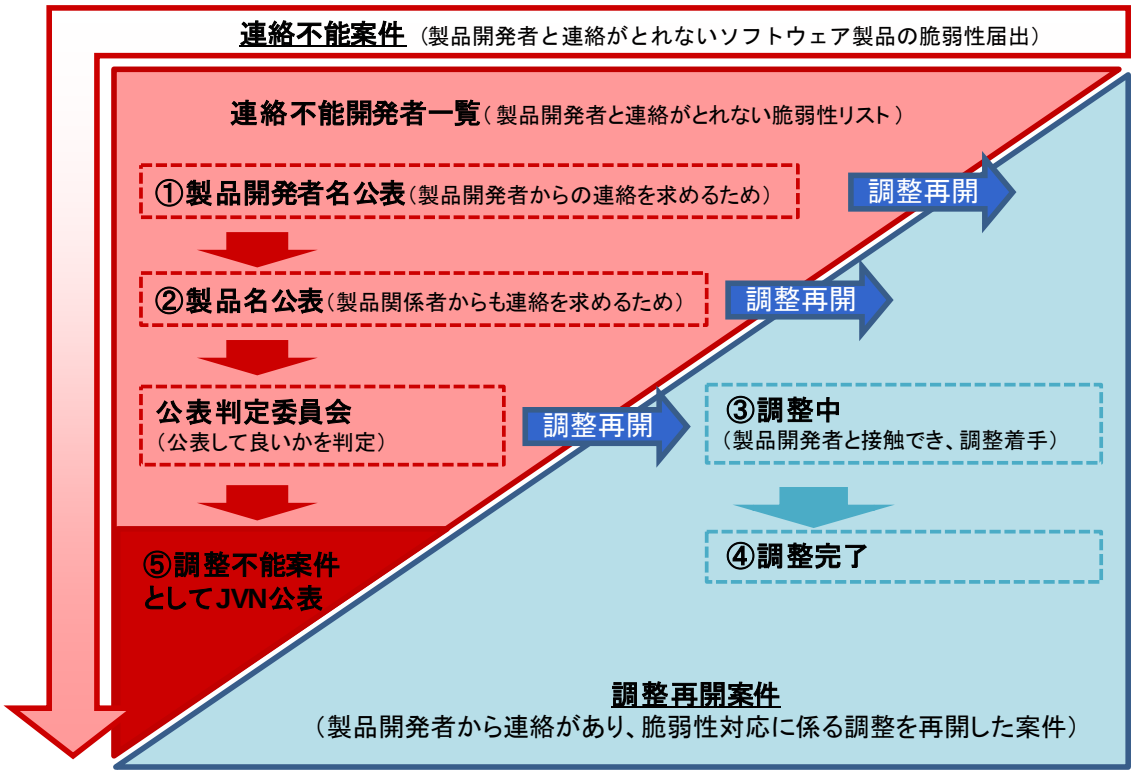
2-1-6. 連絡不能案件の処理状況

図 2-12 は、2011 年 9 月末から本四半期末までに「連絡不能開発者」と位置づけて取り扱った 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）」）および本四半期の「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、本四半期末時点で連絡不能案件（①+②）は 200 件（前四半期 200 件）、調整再開した案件（③+④）は 49 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。



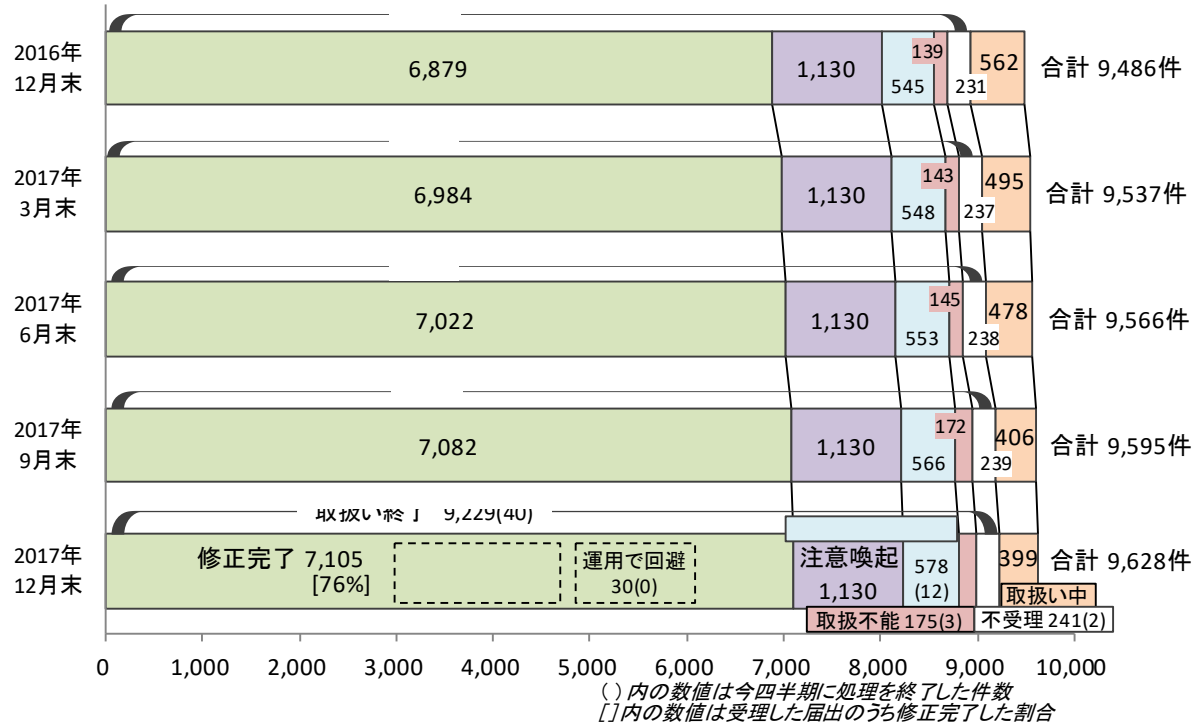
2017年 第3四半期	200件 （①1件　②199件）	49件 （③23件　④26件）	⑤2件	合計 251件
2017年 第4四半期	200件 （①1件　②199件）	49件 （③23件　④26件）	⑤2件	合計 251件

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。本四半期末時点の届出の累計は 9,628 件で、本四半期中に取扱いを終了したものは 40 件（累計 9,229 件）でした。このうち「修正完了」したものは 23 件（累計 7,105 件）、「注意喚起」により処理を取りやめたもの[*16]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 12 件（累計 578 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 3 件（累計 175 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 2 件[*17]（累計 241 件）でした。取扱いを終了した累計 9,229 件のうち「修正完了」「脆弱性ではない」の合計 7,683 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 4 件（累計 1,021 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 30 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
  ウェブサイト運営者への連絡手段が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

[*16] 「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。

[*17] 内訳は本四半期の届出によるもの 2 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末までに届出のあったウェブサイトの脆弱性 9,628 件のうち、不受理を除いた件数は 9,387 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。本四半期は届出が 31 件あり、そのうち約 7 割を企業が占めています。

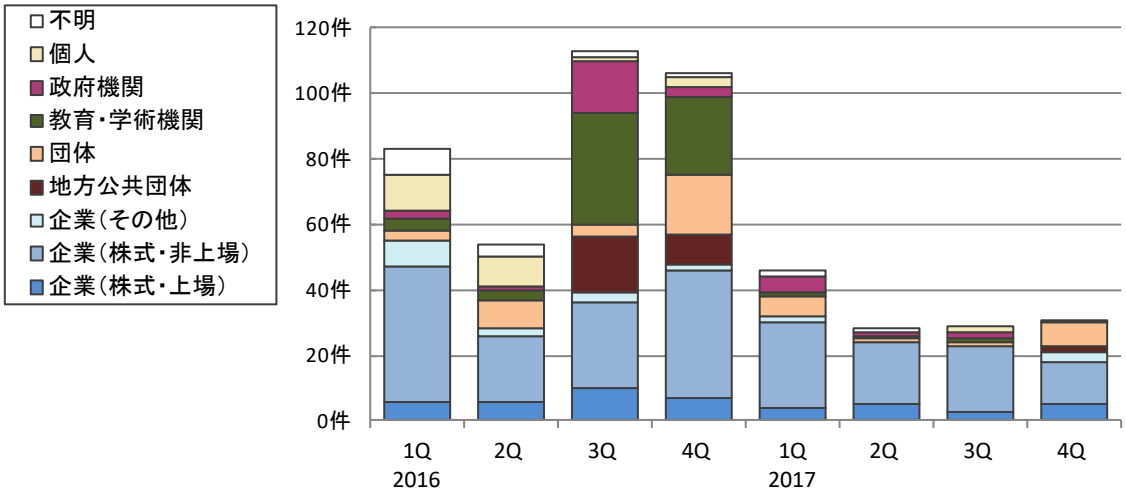
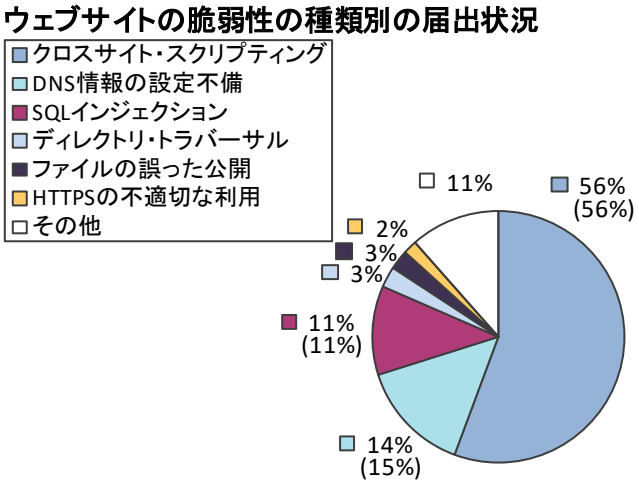


図2−14. 四半期ごとの運営主体の種類別届出件数

2-2-3. 脆弱性の種類・影響別届出件数

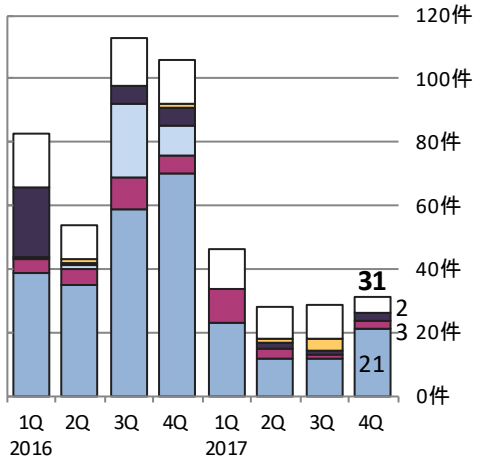
図 2-15、2-16 は、届出された脆弱性の種類別の内訳です。図 2-15 は届出の種類別割合を、図 2-16 は過去 2 年間の届出件数の推移を四半期ごとに示しています[*18]。

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（21 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。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 14%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。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。



(9,387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



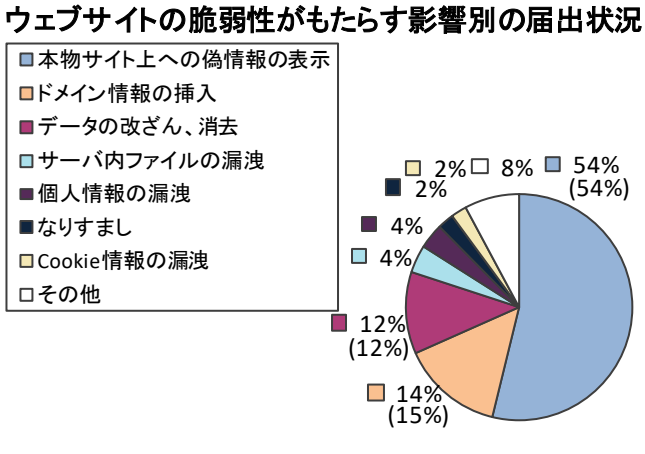
(過去2年間の届出内訳)

図2−16. 四半期ごとの脆弱性の種類別届出件

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

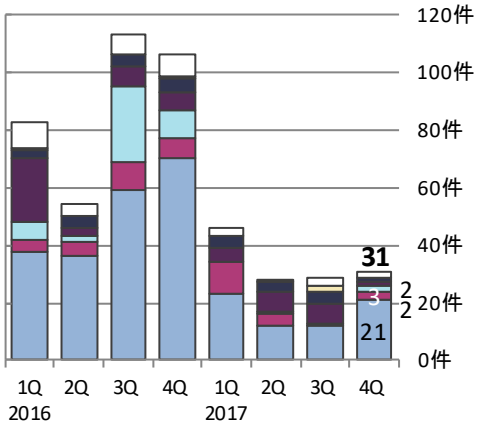
図 2-17、2-18 は、届出された脆弱性がもたらす影響別の内訳です。図 2-17 は届出の影響別割合を、図 2-18 は過去 2 年間の届出件数の推移を四半期ごとに示しています。

本四半期は「本物サイト上への偽情報の表示（21 件）」が最も多く、次いで「データの改ざん、消去（3 件）」「サーバ内ファイルの漏洩（2 件）」および「なりすまし（2 件）」となっています。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。



（9,387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 23 件のうち 14 件（61%）は、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 日以内に修正が完了しました。この割合は、前四半期（60 件中 33 件）の 55%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。本四半期の割合は 66%でした。

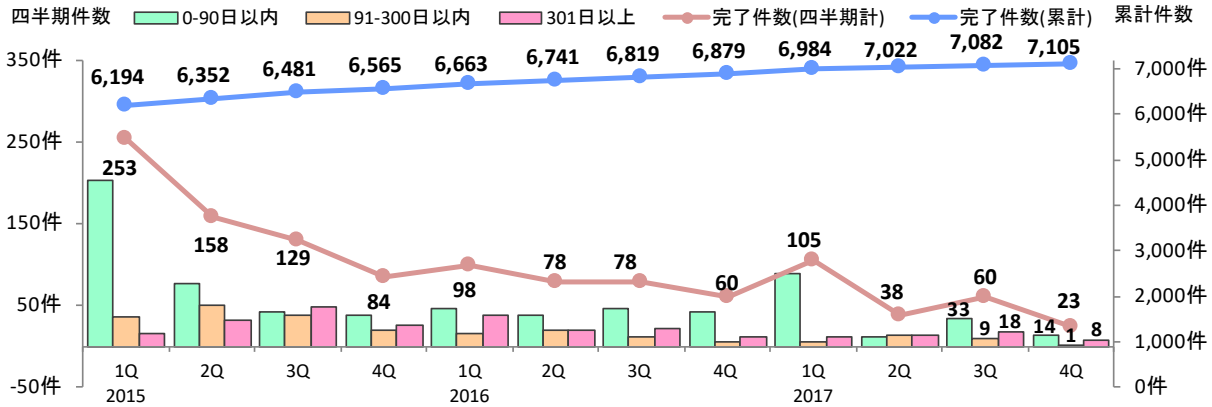


図2-19. ウェブサイトの脆弱性の修正完了件数

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

	2015 1Q	2Q	3Q	4Q	2016 1Q	2Q	3Q	4Q	2017 1Q	2Q	3Q	4Q
修正完了件数	6,194	6,352	6,481	6,565	6,663	6,741	6,819	6,879	6,984	7,022	7,082	7,105
90 日以内の件数	4,184	4,260	4,303	4,341	4,387	4,425	4,471	4,514	4,602	4,613	4,646	4,660
90 日以内の割合	68%	67%	66%	66%	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[*19]。全体の 48%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。

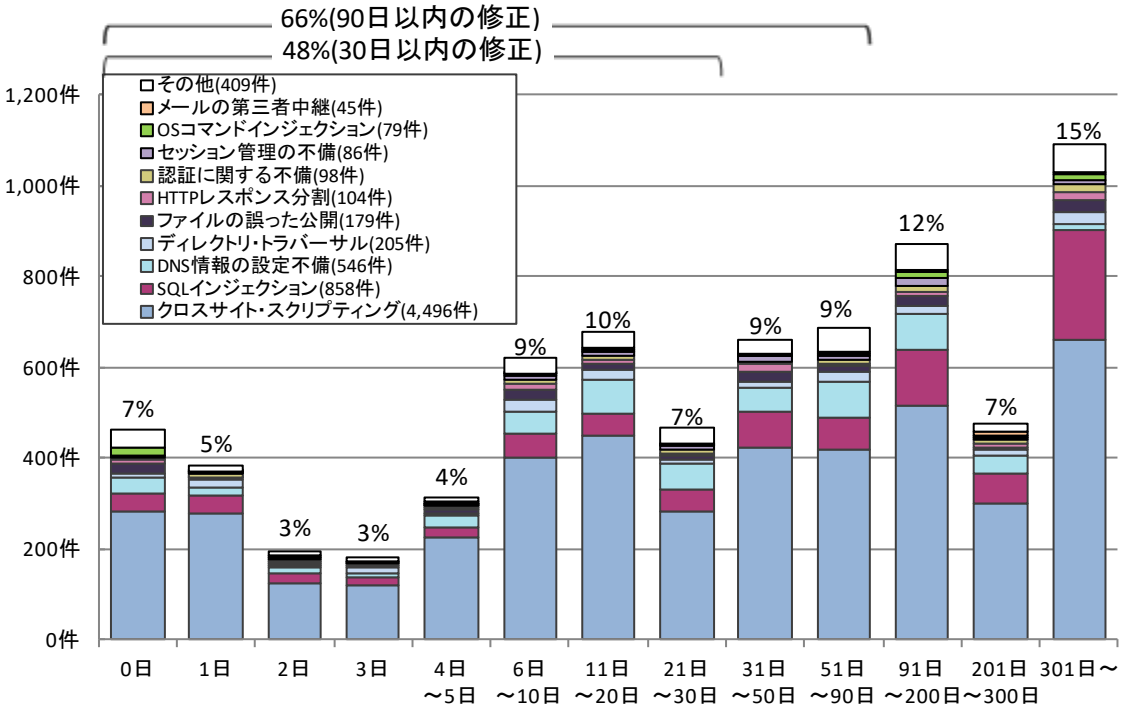


図 2-20. ウェブサイトの修正に要した日数

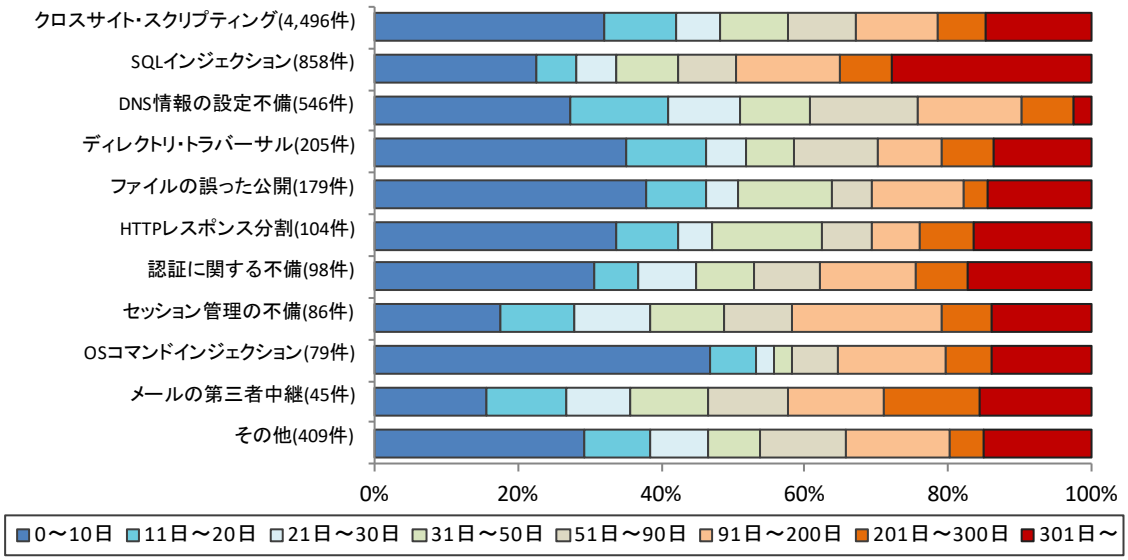


図 2-21. ウェブサイトの修正に要した脆弱性種類別の日数の傾向

[*19] 運営者から修正完了の報告があったもの、および、脆弱性が修正されたと IPA で判断したものも含めて示しています。なお、0 日は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、取扱いが長期化しているもの（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 日以上修正した旨の報告が無い）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 333 件（前四半期は 342 件）となり前四半期より減少しています。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 18%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。

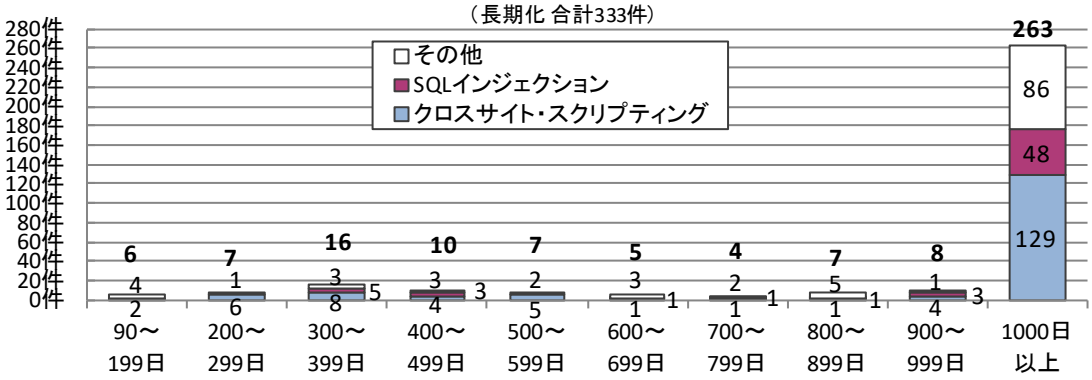


図2−22. 取扱いが長期化(90日以上経過)している届出の取扱経過日数と脆弱性の種類

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

	2016 1Q	2Q	3Q	4Q	2017 1Q	2Q	3Q	4Q
取扱い中の件数	568	518	548	561	494	477	406	399
長期化している件数	436	401	388	374	387	376	342	333
長期化している割合	77%	78%	71%	67%	78%	79%	84%	83%

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

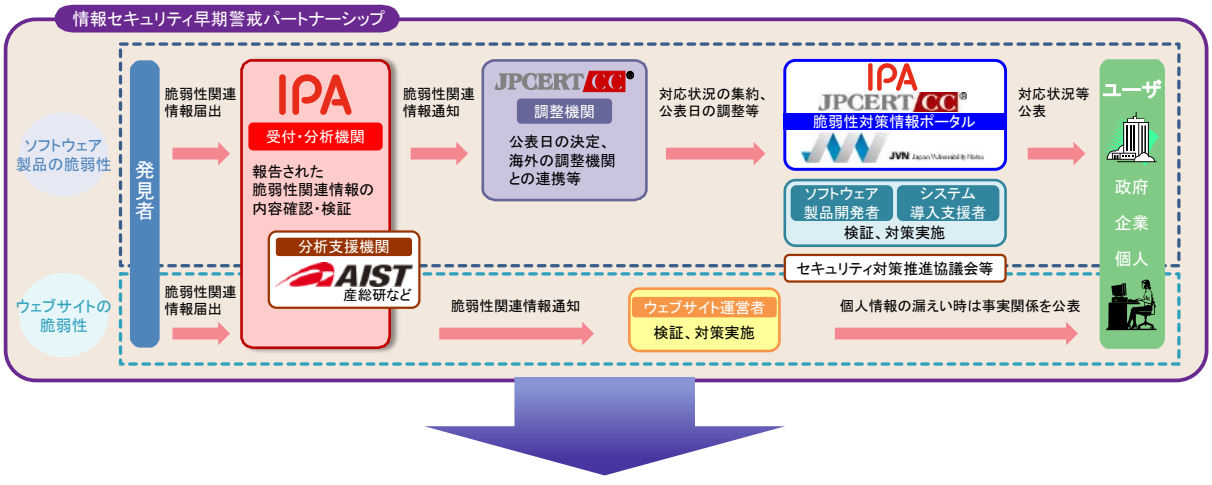
付表 2. ウェブサイトの脆弱性の分類

	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