ソフトウェア等の脆弱性関連情報に関する届出状況

[2023 年第 1 四半期（1 月～3 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(*1)（以降「本制度」）」は、経済産業省の告示(*2)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、2023 年 1 月 1 日から 2023 年 3 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 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
2023 年 4 月 20 日

(*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/guide/vuln/partnership_guide.html
https://www.jpcert.or.jp/vh/index.html

(*2) 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 31 年経済産業省告示第 19 号）

目次

1. ソフトウェア等の脆弱性に関する取扱状況（概要）

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 18,027 件 ～

表 1-1 は本制度における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 94 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 90 件、合計 184 件でした。届出受付開始からの累計は 18,027 件で、内訳はソフトウェア製品に関するもの 5,448 件、ウェブサイトに関するもの 12,579 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	**94** 件	**5,448** 件
ウェブサイト	**90** 件	**12,579** 件
合計	**184** 件	**18,027** 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 3.96 件 [*3] でした。

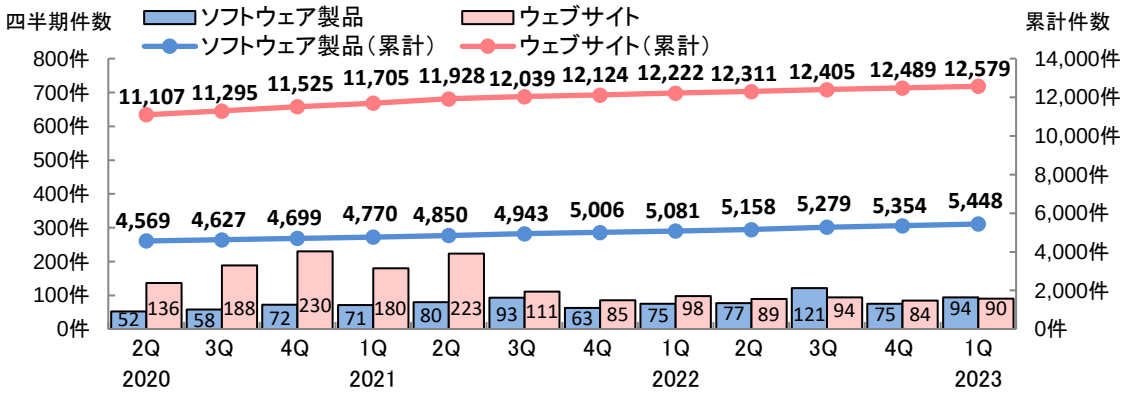


図1-1. 脆弱性の届出件数の四半期ごとの推移

表 1-2. 届出件数（過去 3 年間）

	2020 2Q	3Q	4Q	2021 1Q	2Q	3Q	4Q	2022 1Q	2Q	3Q	4Q	2023 1Q
累計届出件数[件]	15,676	15,922	16,224	16,475	16,778	16,982	17,130	17,303	17,469	17,684	17,843	18,027
1就業日あたり[件/日]	4.03	4.03	4.04	4.04	4.06	4.05	4.02	4.01	3.99	3.98	3.97	3.96

[*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 11,014 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（回避方法の策定のみでプログラムを修正しない場合を含む）、脆弱性情報や対策方法などを JVN に公表しています。

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	**43** 件	**2,531** 件
ウェブサイト	**64** 件	**8,483** 件
合計	**107** 件	**11,014** 件

本四半期に JVN 公表したソフトウェア製品の件数は 43 件 (*4)（累計 2,531 件）でした。そのうち、5 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 日以内のものは 7 件（16%）でした。また、JVN 公表前に重要インフラ事業者等へ脆弱性対策情報を優先提供したのは、2 件（累計 64 件）でした (*5)。

修正完了したウェブサイトの件数は 64 件（累計 8,483 件）でした。修正を完了した 64 件のうち、ウェブアプリケーションを修正したものは 61 件（95%）、当該ページを削除したものは 3 件（5%）で、運用で回避したものは 0 件（0%）でした。なお、修正を完了した 64 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 63 件（98%）でした。

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 件になります。

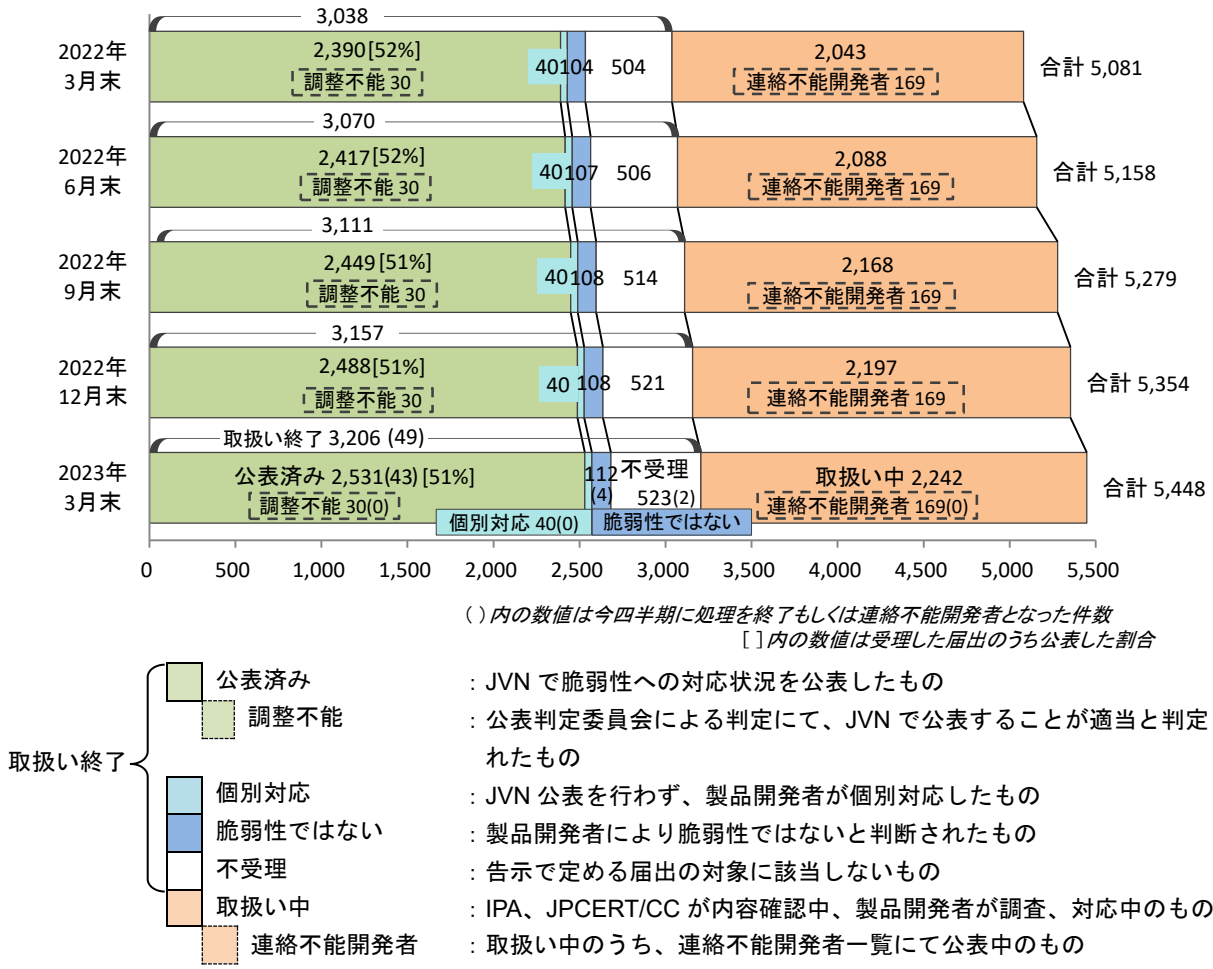
(*4) P.7 2-1-5 参照
(*5) P.13 2-1-6 参照
(*6) 対処の目安は、ウェブサイト運営者が脆弱性の通知を受けてから、3 ヶ月以内としています。
(*7) 連絡不能開発者一覧：https://jvn.jp/reply/index.html
(*8) 連絡不能案件の脆弱性情報を公表するか否かを判定するために IPA が組織します。法律、サイバーセキュリティ、当該ソフトウェア製品分野の専門的な知識や経験を有する専門家、かつ、当該案件と利害関係のない者で構成されています。

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。本四半期末時点の届出の累計は 5,448 件で、本四半期に脆弱性対策情報を JVN 公表したものは 43 件（累計 2,531 件）でした。そのうち、JVN 公表前に重要インフラ事業者等へ脆弱性対策情報を優先提供したものは 2 件（累計 64 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 40 件）、製品開発者が「脆弱性ではない」と判断したものは 4 件（累計 112 件）でした。また「不受理」としたものは 2 件 (*9)（累計 523 件）、「取扱い中」は 2,242 件でした。2,242 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 199 件 (*11) を連絡不能開発者一覧へ公表しています。



( ) 内の数値は今四半期に処理を終了もしくは連絡不能開発者となった件数
[ ] 内の数値は受理した届出のうち公表した割合

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が 0 件、前四半期以前の届出によるものが 2 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 5,448 件のうち、不受理を除いた件数は 4,925 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。

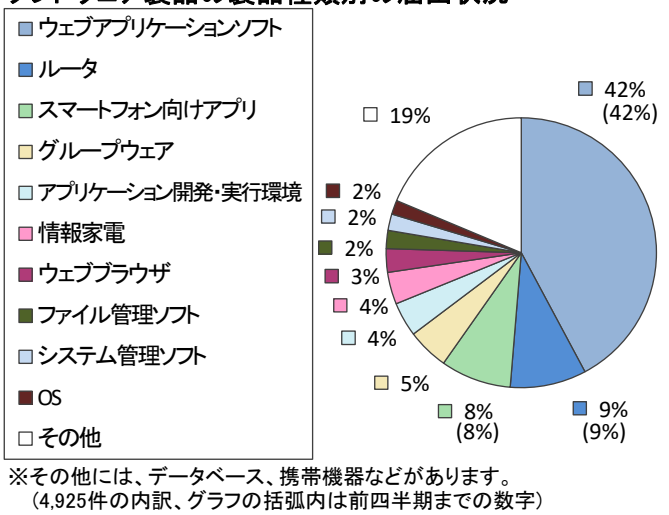
2-1-2. ソフトウェア製品の種類別届出件数

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 には過去 2 年間の四半期ごとの製品種類別届出件数の推移を示しています。

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（28 件）」が最も多く、次いで「ルータ（18 件）」となっています。

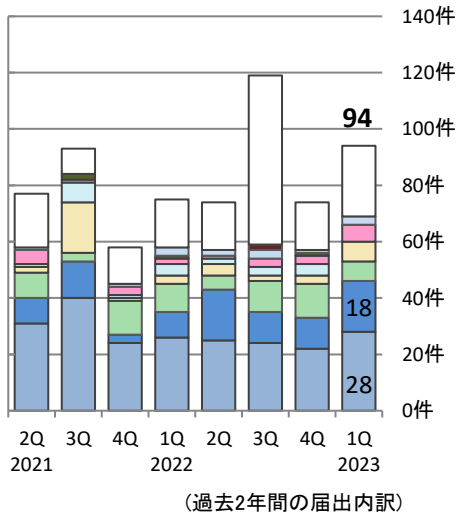
累計では、「ウェブアプリケーションソフト」が最も多く 42%を占めています。

ソフトウェア製品の製品種類別の届出状況



※その他には、データベース、携帯機器などがあります。
（4,925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



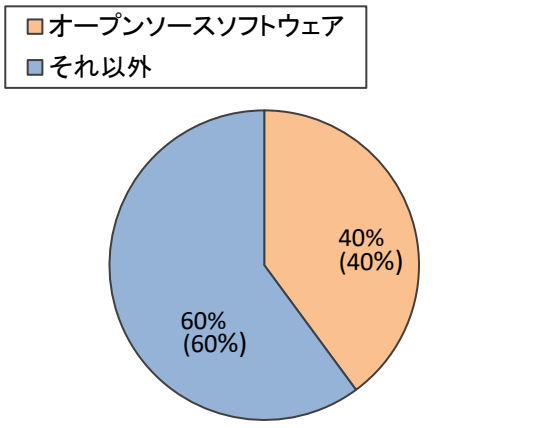
（過去2年間の届出内訳）

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 には過去 2 年間の四半期ごとの分類別届出件数の推移を示しています。

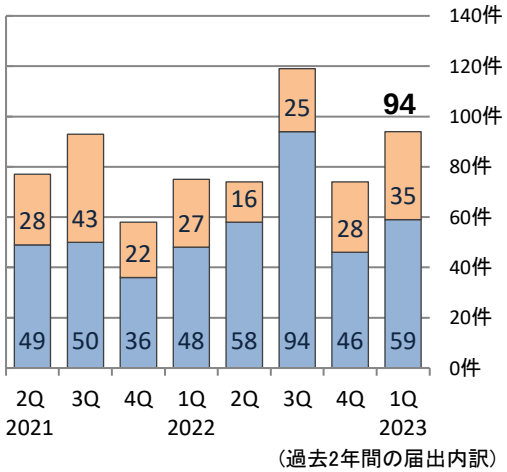
本四半期において「オープンソースソフトウェア」の届出は 35 件あり、累計では 40%を占めています。

オープンソースソフトウェアの脆弱性の届出状況



（4,925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）

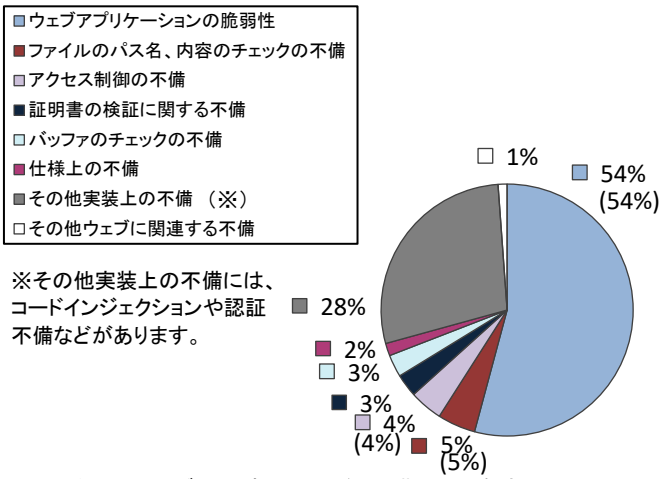
図2−5. 四半期ごとのオープンソースソフトウェア届出件数

2-1-3. 脆弱性の原因・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 には過去 2 年間の四半期ごとの原因別届出件数の推移を示しています[*12]。

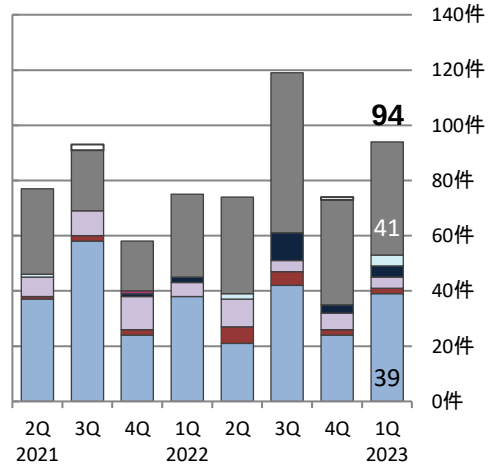
本四半期は「その他実装上の不備（41 件）」が最も多く、次いで「ウェブアプリケーションの脆弱性（39 件）」となっています。累計では、「ウェブアプリケーションの脆弱性」が 54%を占めています。

ソフトウェア製品の脆弱性の原因別の届出状況



（4,925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



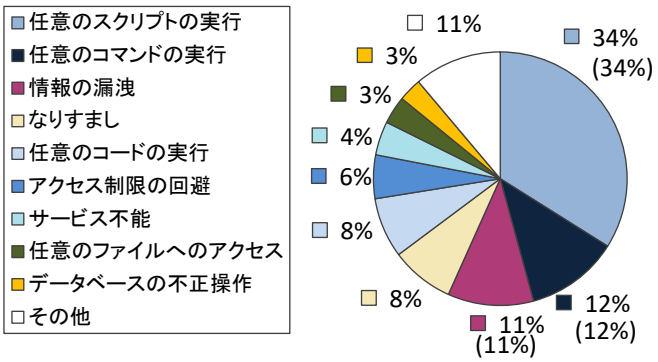
（過去2年間の届出内訳）

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 には過去 2 年間の四半期ごとの影響別届出件数の推移を示しています。

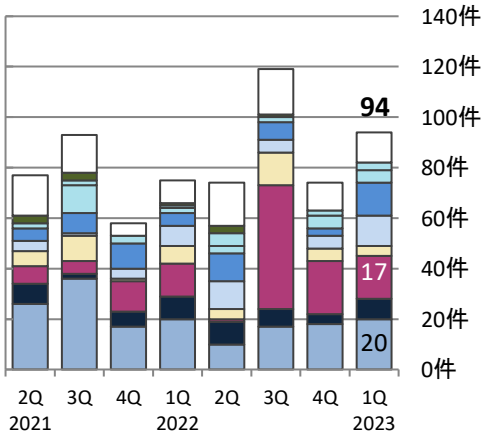
本四半期は、「任意のスクリプトの実行（20 件）」が最も多く、次いで「情報の漏洩（17 件）」でした。累計では「任意のスクリプトの実行」が最も多く、34%を占めています。

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



（4,925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（2,531 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 29%、45 日を超過した件数は 71%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。

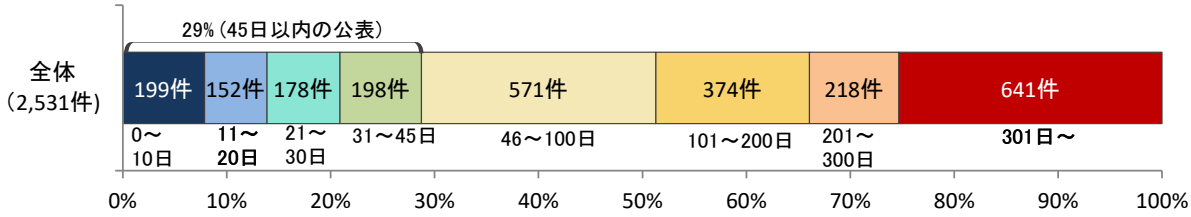


図2-10. ソフトウェア製品の脆弱性公表日数

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）

2020 2Q	3Q	4Q	2021 1Q	2Q	3Q	4Q	2022 1Q	2Q	3Q	4Q	2023 1Q
29%	29%	29%	29%	29%	29%	29%	29%	29%	29%	29%	29%

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取扱状況は、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	29 件	2,086 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	96 件	2,729 件
合計	125 件	4,815 件

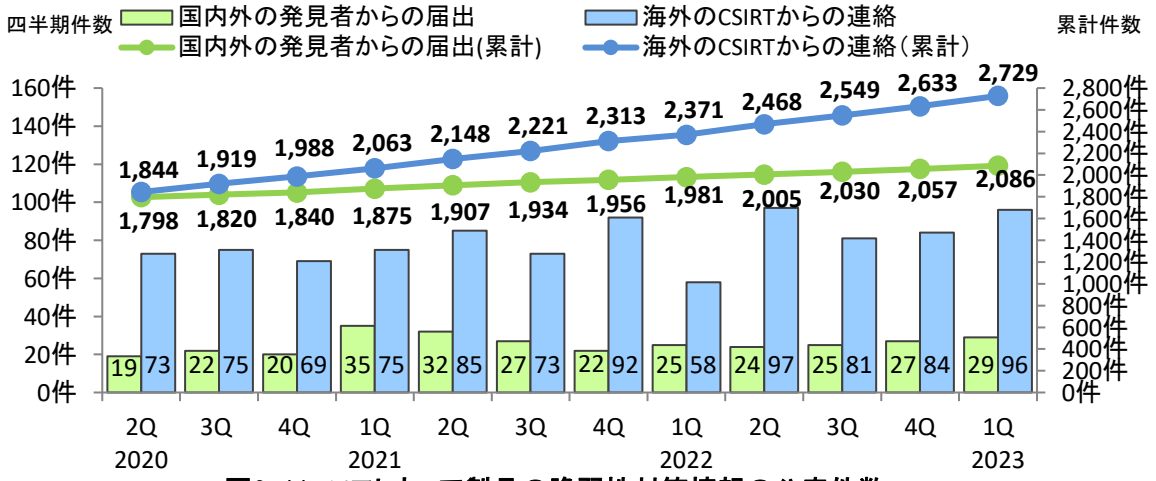


図2−11. ソフトウェア製品の脆弱性対策情報の公表件数

[*13] JPCERT/CC 活動四半期レポート [2023 年 1 月 1 日～2023 年 3 月 31 日] Page18～24（https://www.jpcert.or.jp/pr/）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） 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

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 12 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 5 件（表 2-3 の#2）、組み込みソフトウェア製品の脆弱性が 7 件（表 2-3 の#3）ありました。

表 2-3. 2023 年第 1 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 (#3)	JVN#99957889	「MAHO-PBX NetDevancer」シリーズにおける複数の脆弱性	2023 年 1 月 11 日	10.0
2 (#3)	JVN#57296685	ピクセラ製「PIX-RT100」における複数の脆弱性	2023 年 1 月 12 日	8.3
3 (#2)(#3)	JVN#40604023	セイコーソリューションズ製「SkyBridge MB-A100/A110/A200/A130」および「SkySpider MB-R210」における複数の脆弱性	2023 年 3 月 31 日	9.0
脆弱性の深刻度=レベル II（警告）、CVSS 基本値=4.0～6.9				
4 (#1)	JVN#16765254	「ruby-git」における複数のコード・インジェクションの脆弱性	2023 年 1 月 5 日	6.0
5 (#2)	JVN#55675303	デジタルアーツ製「m-FILTER」における認証不備の脆弱性	2023 年 1 月 6 日	4.3
6 (#3)	JVN#78481846	「TP-Link SG105PE」における認証回避の脆弱性	2023 年 1 月 11 日	4.3
7 (#1)	JVN#03832974	「pgAdmin 4」におけるオープンリダイレクトの脆弱性	2023 年 1 月 11 日	4.3
8 (#1)	JVN#31073333	WordPress 用プラグイン「Welcart e-Commerce」におけるディレクトリ・トラバーサルの脆弱性	2023 年 1 月 17 日	5.0
9 (#1)	JVN#05288621	「EasyMail」におけるクロスサイト・スクリプティングの脆弱性	2023 年 1 月 24 日	4.3
10	JVN#84642320	Android アプリ「スシロー」におけるログファイルからの情報漏えいの脆弱性	2023 年 1 月 31 日	4.9
11	JVN#11257333	スマートフォンアプリ「一蘭公式アプリ」におけるサーバ証明書の検証不備の脆弱性	2023 年 2 月 6 日	4.0
12	JVN#60320736	日本電気製「PC設定ツール」における重要な機能に対する認証の欠如の脆弱性	2023 年 2 月 10 日	6.8
13	JVN#60263237	「エレコム カメラアシスタント」および「QuickFileDealer」のインストーラにおける DLL 読み込みに関する脆弱性	2023 年 2 月 14 日	6.8
14	JVN#57224029	IT 資産管理ツール「SS1」および「らくらくPCクラウド」における複数の脆弱性	2023 年 3 月 1 日	5.0
15 (#1)(#2)	JVN#19872280	PostgreSQL 拡張モジュール「pg_ivm」における複数の脆弱性	2023 年 3 月 6 日	5.5
16 (#3)	JVN#62420378	TP-Link 製「T2600G-28SQ」における脆弱な SSH ホスト鍵使用	2023 年 3 月 17 日	4.6

項番	脆弱性識別番号	脆弱性	JVN 公表日	CVSS 基本値
17	JVN#35246979	エレコム製法人向けアクセスポイント管理ツール「WAB-MAT」によって登録される Windows サービスの実行ファイルパスが引用符で囲まれていない脆弱性	2023 年 3 月 24 日	6.8
18 (#1)	JVN#61105618	「baserCMS」における任意のファイルをアップロードされる脆弱性	2023 年 3 月 27 日	4.0
19 (#1)	JVN#38170084	「HAProxy」における HTTP リクエスト・スマグリングの脆弱性	2023 年 3 月 31 日	5.1
脆弱性の深刻度=レベル I（注意）、CVSS 基本値=0.0～3.9				
20 (#1)(#2)	JVN#72418815	「Pgpool-II」における情報漏えいの脆弱性	2023 年 1 月 23 日	3.5
21 (#1)	JVN#01398015	「pgAdmin 4」におけるディレクトリ・トラバーサルの脆弱性	2023 年 1 月 24 日	2.1
22	JVN#22830348	富士フイルムビジネスイノベーション製ドライバー配布ツールにおける復元可能な形式でのパスワード保存の脆弱性	2023 年 1 月 31 日	2.1
23 (#3)	JVN#98612206	プラネックスコミュニケーションズ製 ネットワークカメラ「CS-WMV02G」における複数の脆弱性	2023 年 2 月 13 日	2.6
24	JVN#00712821	「tsClinical Define.xml Generator」および「tsClinical Metadata Desktop Tools」における XML 外部実体参照(XXE)に関する脆弱性	2023 年 2 月 14 日	1.2
25 (#1)	JVN#18765463	「SHIRASAGI」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	2023 年 2 月 22 日	3.5
26 (#1)	JVN#78253670	「web2py」の開発ツールにおけるオープンリダイレクトの脆弱性	2023 年 2 月 28 日	2.6
27 (#1)(#2)	JVN#04785663	「EC-CUBE」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	2023 年 2 月 28 日	3.5
28 (#3)	JVN#82424996	セイコーエプソン製プリンターおよびネットワークインターフェイス製品の「Web Config」における複数の脆弱性	2023 年 3 月 8 日	3.5
29	JVN#64453490	Android アプリ「Wolt ウォルト：フードデリバリー/出前」に外部サービスの API キーがハードコードされている問題	2023 年 3 月 13 日	2.1

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

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 96 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。

また、米国国土安全保障省傘下の CISA ICS が公開する ICSA（制御系製品に関する脆弱性情報）および ICSMA（医療機器に関する脆弱性情報）も JVN において注意喚起として掲載しています。

表 2-4. 海外 CSIRT 等と連携した脆弱性および注意喚起情報に対する対応状況

項番	脆弱性	対応状況
1	Apache Tomcat の JsonErrorReportValve におけるエスケープ処理不備の問題	製品開発者へ通知
2	複数の Hitachi Energy 製品における複数の脆弱性	注意喚起として掲載
3	OpenAM Web Policy Agent (OpenAM コンソーシアム版)におけるパストラバーサル脆弱性	製品開発者へ通知・調整
4	オムロン製 CX-Motion-MCH における初期化されていないポインタへアクセスする脆弱性	製品開発者へ通知・調整
5	Black Box 製 KVM エクステンダにおけるディレクトリトラバーサルの脆弱性	注意喚起として掲載
6	Siemens 製品に対するアップデート（2023 年 1 月）	注意喚起として掲載
7	Intel 製 oneAPI ツールキットにおける権限昇格の脆弱性	注意喚起として掲載
8	オムロン製 CP1L-EL20DR-D に利用可能なデバッグ機能が存在している脆弱性	製品開発者へ通知・調整
9	CLUSTERPRO X における複数の脆弱性	製品開発者へ通知・調整
10	Hitachi Energy 製 Lumada APM における不適切なアクセス制御の脆弱性	注意喚起として掲載
11	Johnson Controls 製 Metasys における認証情報の不十分な保護の脆弱性	注意喚起として掲載
12	SAUTER Controls 製 Nova 200-220 シリーズにおける複数の脆弱性	注意喚起として掲載
13	InHand Networks 製ルーターInRouter における複数の脆弱性	注意喚起として掲載
14	RONDS 製 Equipment Predictive Maintenance における複数の脆弱性	注意喚起として掲載
15	Sewio 製 RTLS Studio における複数の脆弱性	注意喚起として掲載
16	三菱電機製 MELSEC シリーズの WEB サーバ機能における認証回避の脆弱性	製品開発者へ通知・調整
17	複数の三洋電機製 CCTV ネットワークカメラにおけるクロスサイトリクエストフォージェリの脆弱性	注意喚起として掲載
18	GE Digital 製 Proficy Historian における複数の脆弱性	注意喚起として掲載
19	Netcomm 製ルータにおける複数の脆弱性	注意喚起として掲載
20	TP-Link 製ルータにおける複数の脆弱性	注意喚起として掲載
21	Apache HTTP Server 2.4 における複数の脆弱性に対するアップデート	製品開発者へ通知
22	Hitachi Energy 製 PCU400 における脆弱な OSS コンポーネントへの依存の問題	注意喚起として掲載
23	コンテック製 CONPROSYS HMI System (CHS)における複数の SQL インジェクションの脆弱性	製品開発者へ通知・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
24	オムロン製 CX-Motion Pro における XML 外部実体参照（XXE）の脆弱性	製品開発者へ通知・調整
25	SOCOMEC 製 MODULYS GP におけるパスワードに対する弱い暗号化使用の脆弱性	注意喚起として掲載
26	XINJE 製 XD/E Series PLC Program Tool における複数の脆弱性	注意喚起として掲載
27	三菱電機製 MELFA SD/SQ シリーズおよび F シリーズのロボットコントローラにおける認証回避の脆弱性	製品開発者へ通知・調整
28	ISC BIND における複数の脆弱性	製品開発者へ通知・調整
29	Landis+Gyr 製 E850 (ZMQ200)における検証や整合性確認をしていない Cookie への依存の脆弱性	注意喚起として掲載
30	GoAhead Web サーバを使用する Rockwell Automation 製品における複数の脆弱性	注意喚起として掲載
31	Sierra Wireless 製 ALEOS Software を実行する AirLink Router における複数の脆弱性	注意喚起として掲載
32	Snap One 製 Wattbox WB-300-IP-3 における複数の脆弱性	注意喚起として掲載
33	ECONOLITE 製 EOS における複数の脆弱性	注意喚起として掲載
34	Delta Electronics 製 CNCSoft および Screen Editor におけるスタックベースのバッファオバーフローの脆弱性	注意喚起として掲載
35	Delta Electronics 製 DOPSoft における複数の脆弱性	注意喚起として掲載
36	三菱電機製 GOT2000 シリーズおよび GT SoftGOT2000 の GOT Mobile 機能における複数の脆弱性	製品開発者へ通知・調整
37	ジェイテクトエレクトロニクス製 Screen Creator Advance 2 における複数の脆弱性	製品開発者へ通知・調整
38	Baicells 製 Nova におけるコマンドインジェクションの脆弱性	注意喚起として掲載
39	複数の Delta Electronics 製品における複数の脆弱性	注意喚起として掲載
40	EnOcean 製 SmartServer におけるハードコードされた認証情報の使用の脆弱性	注意喚起として掲載
41	OpenSSL に複数の脆弱性	製品開発者へ通知・調整
42	図研エルミック製 KASAGO における不十分なランダム値の使用の脆弱性	製品開発者へ通知・調整
43	Horner Automation 製 Cscape Envision RV における複数の脆弱性	注意喚起として掲載
44	Johnson Controls 製 System Configuration Tool（SCT）における複数の脆弱性	注意喚起として掲載
45	LS ELECTRIC 製 XBC-DN32U における複数の脆弱性	注意喚起として掲載
46	Xytronix Research & Design 製 X-400 および X-600M における複数の脆弱性	注意喚起として掲載
47	Weintek 製 EasyBuilder Pro におけるパストラバーサルの脆弱性	注意喚起として掲載
48	Siemens 製品に対するアップデート（2023 年 2 月）	注意喚起として掲載
49	Intel 製品に複数の脆弱性（2023 年 2 月）	注意喚起として掲載
50	ウイルスバスター ビジネスセキュリティおよびウイルスバスター ビジネスセキュリティサービスにおける複数の脆弱性	製品開発者へ通知・調整
51	BD 製 Alaris Infusion Central における復元可能な形式でのパスワード保存の脆弱性	注意喚起として掲載
52	Sub-IoT Open Source Stack for Dash7 Alliance Protocol 実装における境界外書き込みの脆弱性	製品開発者へ通知
53	Apache Tomcat の Apache Commons FileUpload におけるサービス運用妨害（DoS）の脆弱性	製品開発者へ通知
54	ウェブブラウザの権限機構におけるセキュリティ上の問題について	注意喚起として掲載
55	PTC 製 ThingWorx Edge C-SDK における複数の脆弱性	注意喚起として掲載
56	Hitachi Energy 製 Gateway Station における複数の脆弱性	注意喚起として掲載

項番	脆弱性	対応状況
57	Trend Micro Apex One および Trend Micro Apex One SaaS における複数の脆弱性	製品開発者へ通知・調整
58	トレンドマイクロ製ウイルスバスター クラウドにおける複数の脆弱性	製品開発者へ通知・調整
59	三菱電機製 MELSEC iQ-F シリーズにおける認証情報の平文保存の脆弱性	製品開発者へ通知・調整
60	Edgecross 基本ソフトウェア Windows 版における複数の脆弱性	製品開発者へ通知・調整
61	ジェイテクトエレクトロニクス製 Kostac PLC Programming Software における複数の脆弱性	製品開発者へ通知・調整
62	Medtronic 製臨床医アプリにおける未検証のパスワード変更の脆弱性	注意喚起として掲載
63	Rittal 製 CMC III における不適切なアクセス制御の脆弱性	注意喚起として掲載
64	BaiCells 製 Nova および Neutrino におけるコマンドインジェクションの脆弱性	注意喚起として掲載
65	Trusted Computing Group の TPM2.0 実装における複数の脆弱性	製品開発者へ通知・調整
66	バッファロー製ネットワーク機器における複数の脆弱性	製品開発者へ通知・調整
67	Apache HTTP Server 2.4 における複数の脆弱性に対するアップデート	製品開発者へ通知
68	Hitachi Energy 製 Relion 670, 650 および SAM600-IO Series におけるデータの信頼性確認が不十分な脆弱性	注意喚起として掲載
69	Step Tools 製 ifcmesh ライブラリにおける NULL ポインタ参照の脆弱性	注意喚起として掲載
70	ABB 製 S+ Operations における不適切な認証の脆弱性	注意喚起として掲載
71	B&R Industrial Automation 製 System Diagnostics Manager におけるクロスサイトスクリプティングの脆弱性	注意喚起として掲載
72	Akuvox 製 E11 における複数の脆弱性	注意喚起として掲載
73	オムロン製 SYSMAC CJ/CS/CP シリーズに不適切なアクセス制御の脆弱性	製品開発者へ通知・調整
74	AVEVA Plant SCADA および AVEVA Telemetry Server における不適切な認可の脆弱性	注意喚起として掲載
75	GE Digital 製 iFIX におけるコードインジェクションの脆弱性	注意喚起として掲載
76	Autodesk 製 FBX SDK における複数の脆弱性	注意喚起として掲載
77	Siemens 製品に対するアップデート（2023 年 3 月）	注意喚起として掲載
78	Rockwell Automation 製 Modbus TCP Server AOI における情報漏えいの脆弱性	注意喚起として掲載
79	Honeywell 製 OneWireless Wireless Device Manager における複数の脆弱性	注意喚起として掲載
80	コンテック製 CONPROSYS IoT ゲートウェイ製品における複数の脆弱性	製品開発者へ通知・調整
81	Rockwell Automation 製 ThinManager ThinServer における複数の脆弱性	注意喚起として掲載
82	VISAM 製 VBASE における複数の XML 外部実体参照（XXE）に関する脆弱性	注意喚起として掲載
83	Delta Electronics 製 InfraSuite Device Master における複数の脆弱性	注意喚起として掲載
84	Keysight Technologies 製 N6854A Geolocation Server における信頼できないデータのデシリアライゼーションの脆弱性	注意喚起として掲載
85	OpenSSL の X.509 ポリシー制限の検証における過剰なリソース消費の問題	製品開発者へ通知・調整
86	Apache Tomcat における保護されていない認証情報の送信の脆弱性	製品開発者へ通知
87	ProPump and Controls 製 Osprey Pump Controller における複数の脆弱性	注意喚起として掲載
88	ABB 製 Pulsar Plus Controller における複数の脆弱性	注意喚起として掲載
89	Schneider Electric 製 IGSS における複数の脆弱性	注意喚起として掲載
90	SAUTER 製 EY-modulo 5 Building Automation Stations における複数の脆弱性	注意喚起として掲載
91	CP Plus 製 KVMS Pro における認証情報の不十分な保護の脆弱性	注意喚起として掲載

項番	脆弱性	対応状況
92	RoboDK における重要なリソースに対する不適切なアクセス権の割り当ての脆弱性	注意喚起として掲載
93	OpenSSL に複数の脆弱性（Security Advisory [28th March 2023]）	製品開発者へ通知・調整
94	ジェイテクトエレクトロニクス製 Screen Creator Advance 2 におけるメモリバッファエラーの脆弱性	製品開発者へ通知・調整
95	コンテック製 CONPROSYS HMI System(CHS)における SQL インジェクションの脆弱性	製品開発者へ通知・調整
96	Hitachi Energy 製 IEC 61850 MMS-Server におけるリソースの不適切なシャットダウンまたはリリースの脆弱性	注意喚起として掲載

2-1-6. 優先情報提供の実施状況

2018 年 4 月から、脆弱性による国民の日常生活に必要不可欠なサービスへの被害を低減するために、これらのサービスを提供する重要インフラ事業者等 (*16) に対して脆弱性対策情報を JVN 公表前に優先的に提供しています。本四半期に優先情報提供したものは、電力分野 1 件、政府機関 1 件で、累計では 64 件（電力分野 37 件、政府機関 27 件）でした。

(*16) 内閣サイバーセキュリティセンター（NISC）の最新の「重要インフラの情報セキュリティ対策に係る行動計画」で定める重要インフラ事業者等とします。

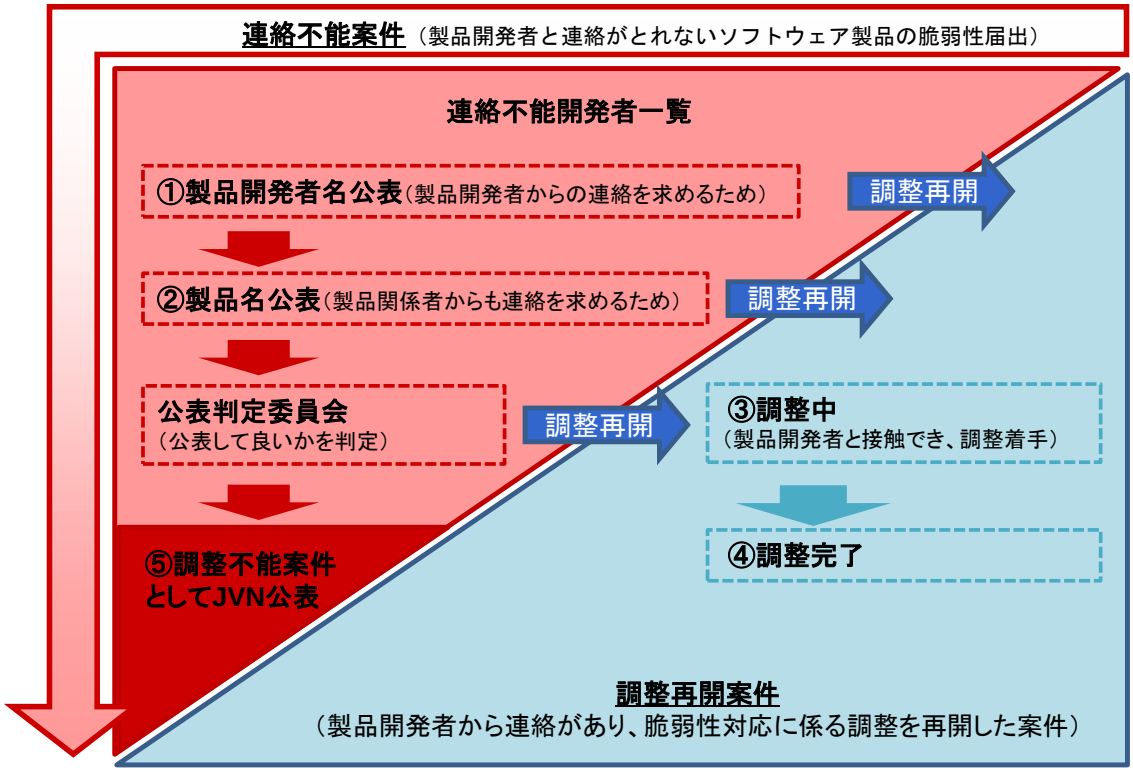
2-1-7. 連絡不能案件の処理状況

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 169 件、調整再開した案件（③+④）は 52 件、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）は 30 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。



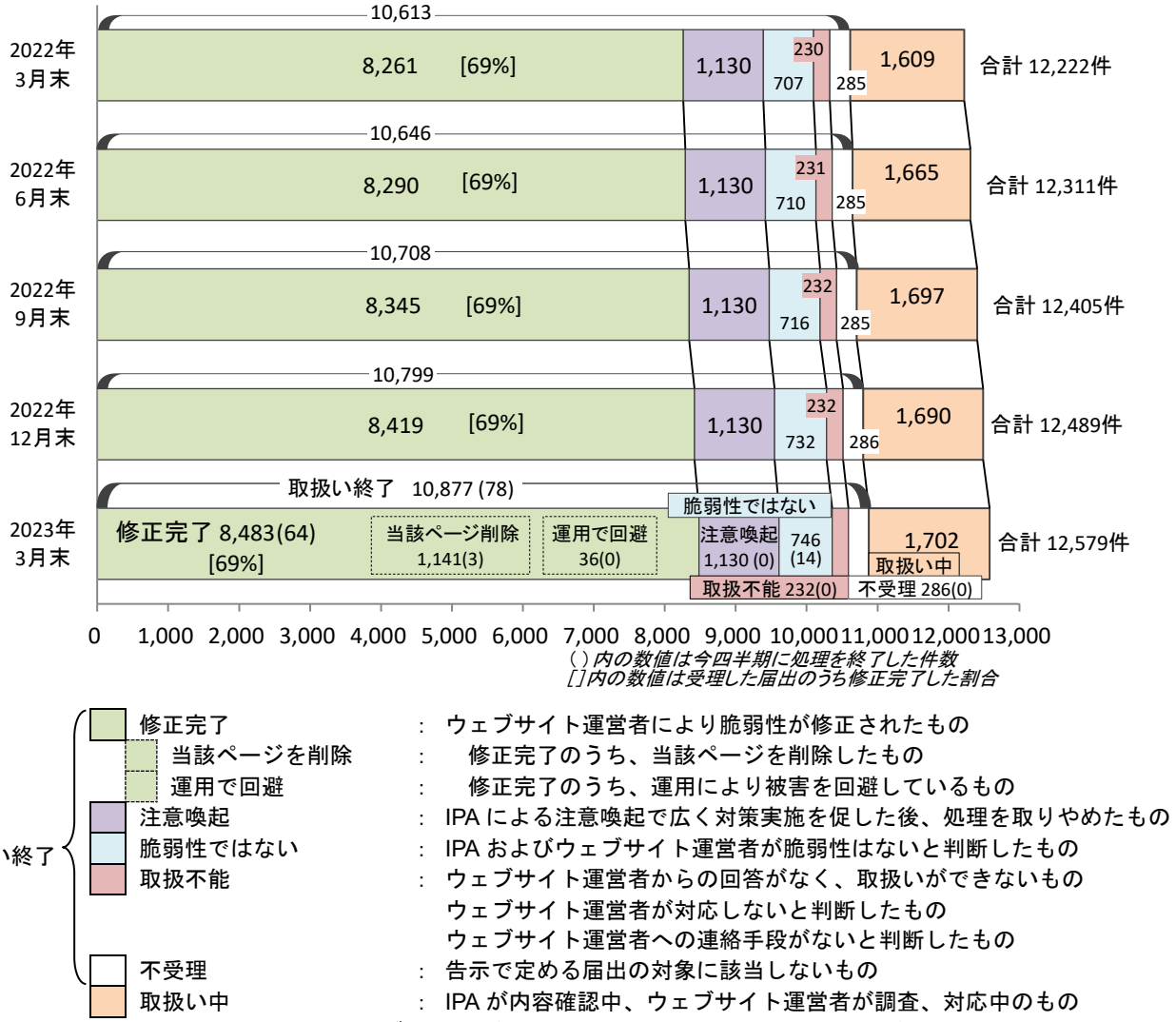
2022年 第4四半期	169件 （①1件　②168件）	52件 （③20件　④32件）	⑤30 件	合計 251件
2023年 第1四半期	169件 （①1件　②168件）	52件 （③20件　④32件）	⑤30 件	合計 251件

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 12,579 件で、本四半期中に取扱いを終了したものは 78 件（累計 10,877 件）でした。このうち「修正完了」したものは 64 件（累計 8,483 件）、「注意喚起」により処理を取りやめたもの[*17]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 14 件（累計 746 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 0 件（累計 232 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 0 件[*18]（累計 286 件）でした。取扱いを終了した累計 10,877 件のうち「修正完了」「脆弱性ではない」の合計 9,229 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 3 件（累計 1,141 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 36 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

[*17] 「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。

[*18] 内訳は本四半期の届出によるもの 0 件、前四半期以前によるものが 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 12,579 件のうち、不受理を除いた件数は 12,293 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 90 件あり、そのうち約 7 割を企業が占めています。

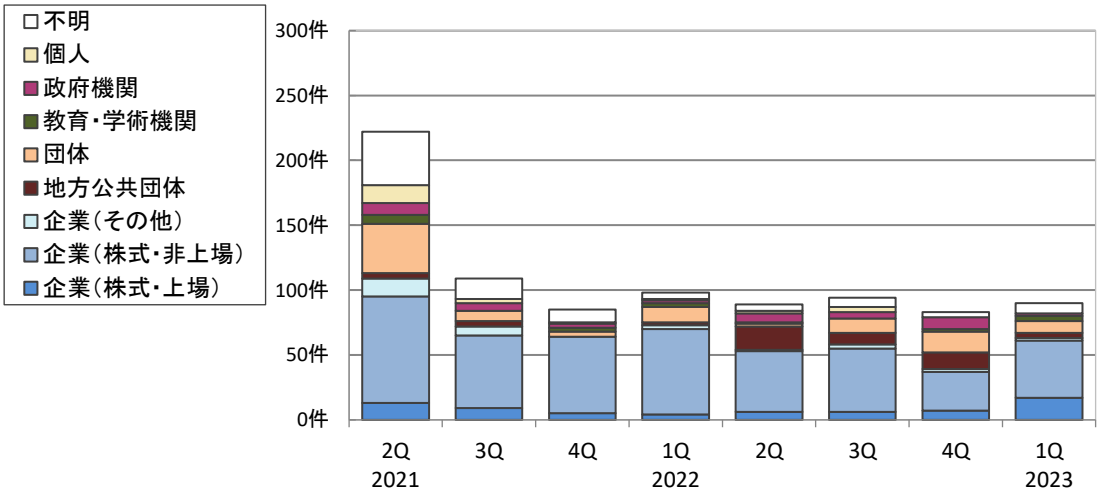


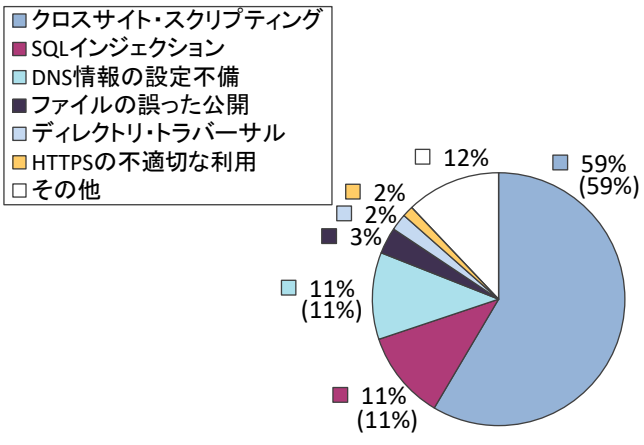
図2-14. 四半期ごとの運営主体の種類別届出件数

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 には過去 2 年間の四半期ごとの種類別届出件数の推移を示しています[*19]。

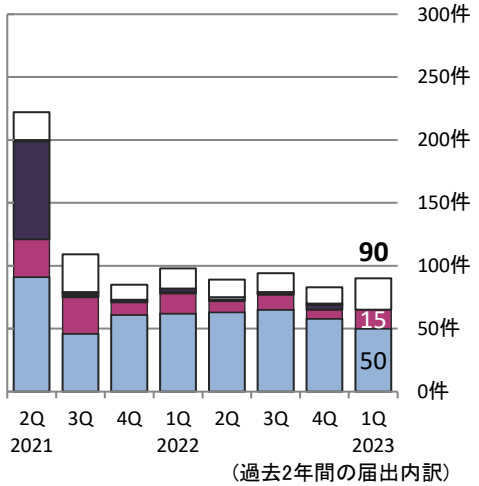
本四半期は「クロスサイト・スクリプティング（50 件）」が最も多く、次いで「SQL インジェクション（15 件）」となっています。累計では、「クロスサイト・スクリプティング」だけで 59%を占めており、次いで「SQL インジェクション」と「DNS 情報の設定不備」が 11%となっています。「DNS 情報の設定不備」は、2008 年から 2009 年にかけて多く届出されたものが反映されています。なお、この統計値の利用にあたっては、本制度における届出の傾向であることにご留意ください。

ウェブサイトの脆弱性の種類別の届出状況



（12,293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



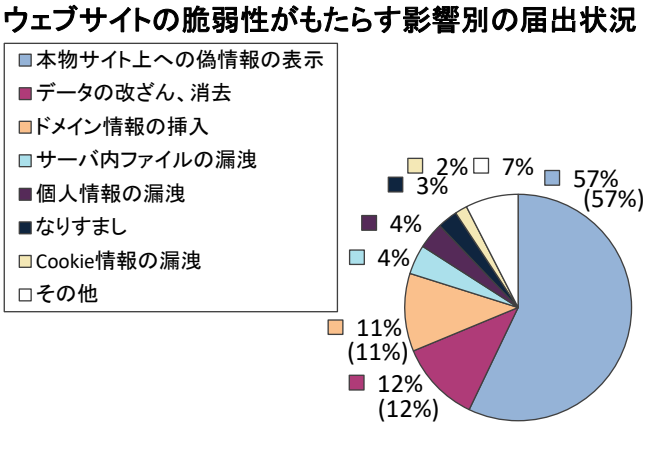
（過去2年間の届出内訳）

図2-16. 四半期ごとの脆弱性の種類別届出件数

[*19] 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。

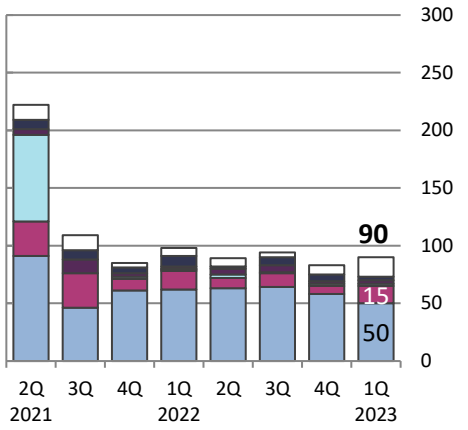
図 2-17、2-18 は、届出された脆弱性がもたらす影響別の内訳です。図 2-17 は届出の影響別割合を、図 2-18 には過去 2 年間の四半期ごとの影響別届出件数の推移を示しています。

本四半期は「本物サイト上への偽情報の表示（50 件）」が最も多く、次いで「データの改ざん、消去（15 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」、「データの改ざん、消去」、「ドメイン情報の挿入」が全体の約 8 割を占めています。これらは、脆弱性の種類別割合で上位を占めた「クロスサイト・スクリプティング」「SQL インジェクション」「DNS 情報の設定不備」などにより発生するものです。



（12,293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 64 件のうち 63 件（98%）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。表 2-5 は、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過去 3 年間において四半期ごとに示したものです。本四半期の割合は 69%でした。

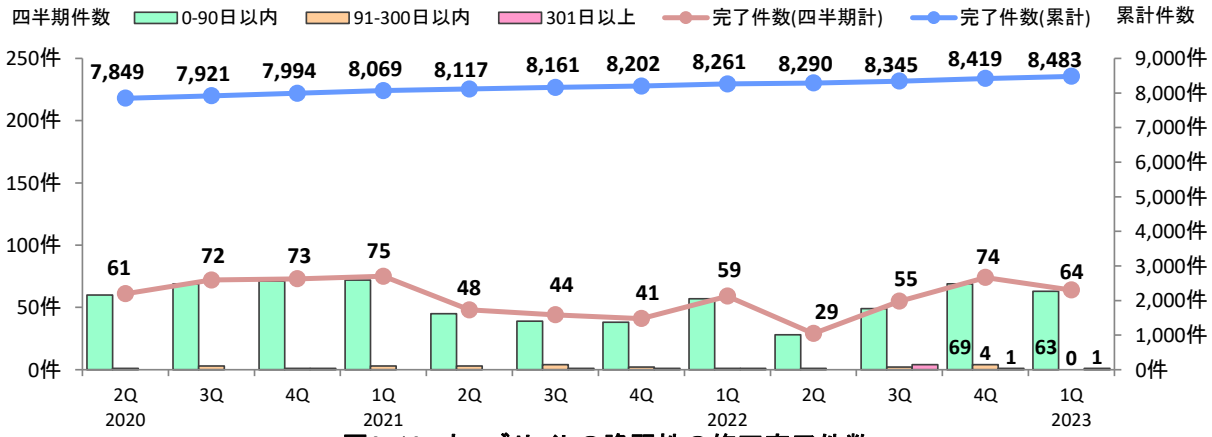


図2-19. ウェブサイトの脆弱性の修正完了件数

表 2-5. 90 日以内に修正完了した累計およびその割合の推移

	2020 2Q	3Q	4Q	2021 1Q	2Q	3Q	4Q	2022 1Q	2Q	3Q	4Q	2023 1Q
修正完了件数	7,849	7,921	7,994	8,069	8,117	8,161	8,202	8,261	8,290	8,345	8,419	8,483
90 日以内の件数	5,264	5,333	5,404	5,476	5,521	5,560	5,598	5,655	5,683	5,732	5,801	5,864
90 日以内の割合	67%	67%	68%	68%	68%	68%	68%	68%	69%	69%	69%	69%

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[*20]。全体の 51%の届出が 30 日以内、全体の 69%の届出が 90 日以内に修正されています。

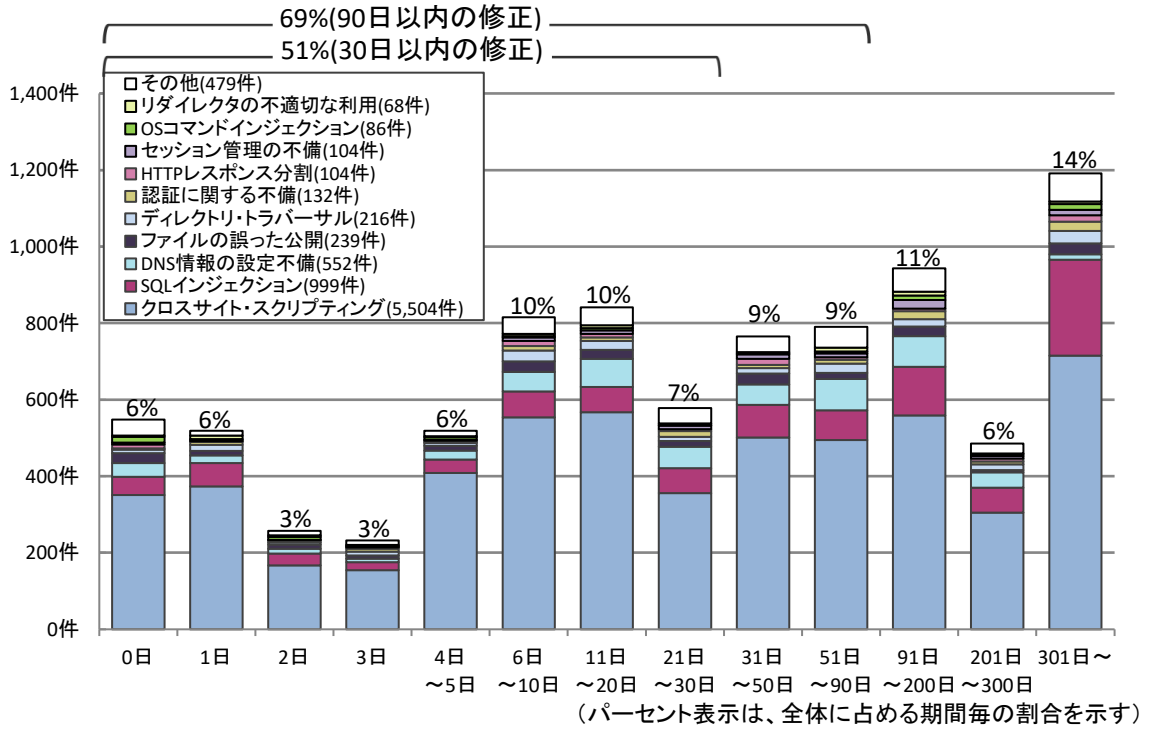


図2-20. ウェブサイトの修正に要した日数

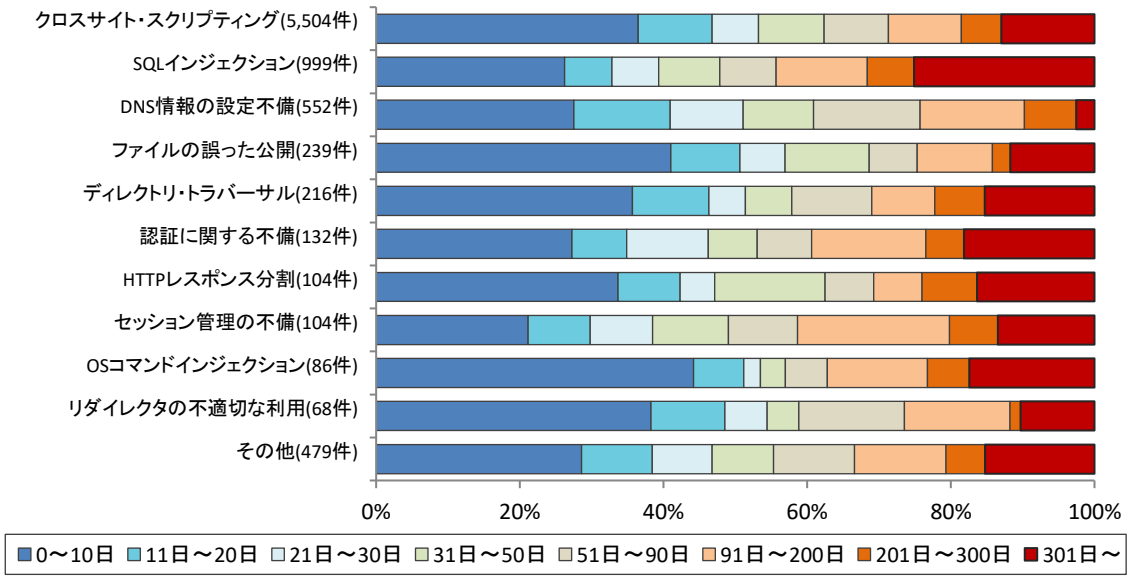


図2-21. ウェブサイトの修正に要した脆弱性種類別の日数の傾向

[*20] 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 714 件（前四半期は 644 件）となり前四半期より増加しています。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 20%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。

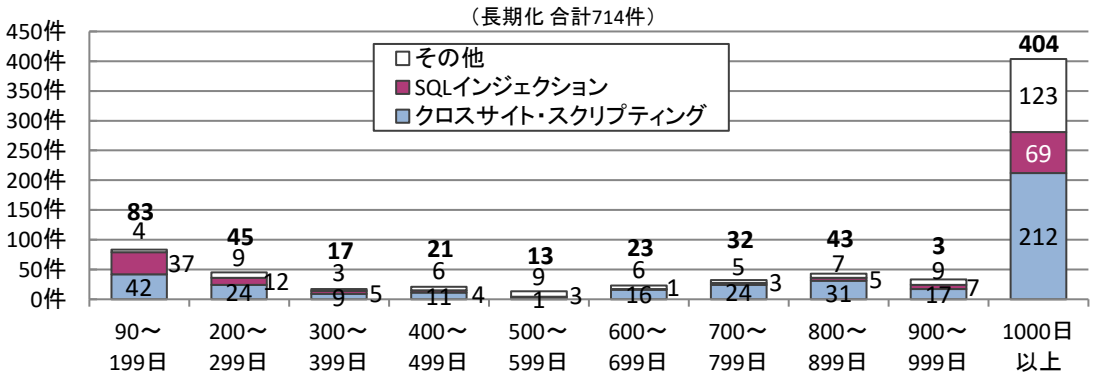


図2−22. 取扱いが長期化(90日以上経過)している届出の取扱経過日数と脆弱性の種類

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

表 2-6. 取扱いが長期化している届出件数および割合の四半期ごとの推移

	2021 2Q	3Q	4Q	2022 1Q	2Q	3Q	4Q	2023 1Q
取扱い中の件数	1,482	1,542	1,573	1,609	1,665	1,697	1,690	1,702
長期化している件数	516	534	551	563	585	615	644	714
長期化している割合	35%	35%	35%	35%	35%	36%	38%	42%

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. 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。

⇒「IoT 開発におけるセキュリティ設計の手引き」: https://www.ipa.go.jp/security/iot/iotguide.html

⇒「IoT 製品・サービス脆弱性対応ガイド」:
https://www.ipa.go.jp/security/todokede/vuln/ug65p90000019gda-att/000065095.pdf

⇒「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/contents.html

⇒「脆弱性対処に向けた製品開発者向けガイド」: https://www.ipa.go.jp/security/guide/vuln/forvendor.html

3-2. 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。

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

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

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

⇒「安全なウェブサイトの運用管理に向けての 20 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/websecurity/sitecheck.html

⇒「IPA 脆弱性対策コンテンツリファレンス」:
https://www.ipa.go.jp/security/guide/hjuojm0000007uwy-att/000051352.pdf

⇒「サーバ用オープンソースソフトウェアに関する製品情報およびセキュリティ情報」:
https://www.ipa.go.jp/security/vuln/oss/sw_security_info.html

⇒「安全なウェブサイト運営にむけて ～ 企業ウェブサイトのための脆弱性対応ガイド ～」:
https://www.ipa.go.jp/archive/files/000089537.pdf

⇒「ウェブサイト運営者向けセキュリティ問い合わせ窓口設置の手引き」:
https://www.ipa.go.jp/security/todokede/vuln/ug65p90000019gda-att/000096758.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/about.html

⇒「動画で知ろう！クロスサイト・スクリプティングの被害！」（情報セキュリティ技術解説映像-脆弱性対策：ウェブアプリケーション）: https://www.ipa.go.jp/security/videos/list.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 バージョンチェッカ for .NET」: https://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。

また、一般インターネットユーザー向けに次のコンテンツを公開しています。

⇒「ネット接続製品の安全な選定・利用ガイド -詳細版-」(動画付き) :

https://www.ipa.go.jp/security/guide/vuln/forconsumer.html

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。

なお、発見者向けに以下のコンテンツを公開しています。

⇒「脆弱性関連情報として取り扱えない場合の考え方の解説」:

https://www.ipa.go.jp/security/todokede/vuln/handling_notaccept.html

⇒「脆弱性発見・報告のみちしるべ～発見者に知っておいて欲しいこと～」（情報セキュリティ技術解説映像-脆弱性報告）: https://www.ipa.go.jp/security/videos/list.html

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

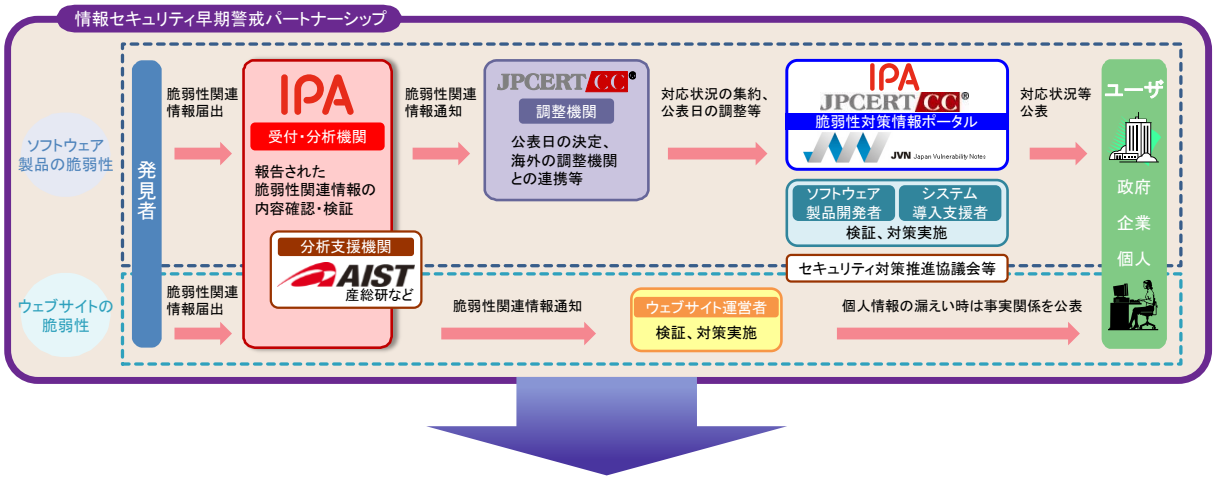
付表 2. ウェブサイトの脆弱性の分類

	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