ソフトウェア等の脆弱性関連情報に関する届出状況

[2018 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(*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、2018 年 10 月 1 日から 2018 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 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
2019 年 1 月 24 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/ciadr/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 29 年経済産業省告示第 20 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 14,092 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 57 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 36 件、合計 93 件でした。届出受付開始からの累計は 14,092 件で、内訳はソフトウェア製品に関するもの 4,226 件、ウェブサイトに関するもの 9,866 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	**57** 件	**4,226** 件
ウェブサイト	**36** 件	**9,866** 件
合計	**93** 件	**14,092** 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 3.99 件 [*3] でした。

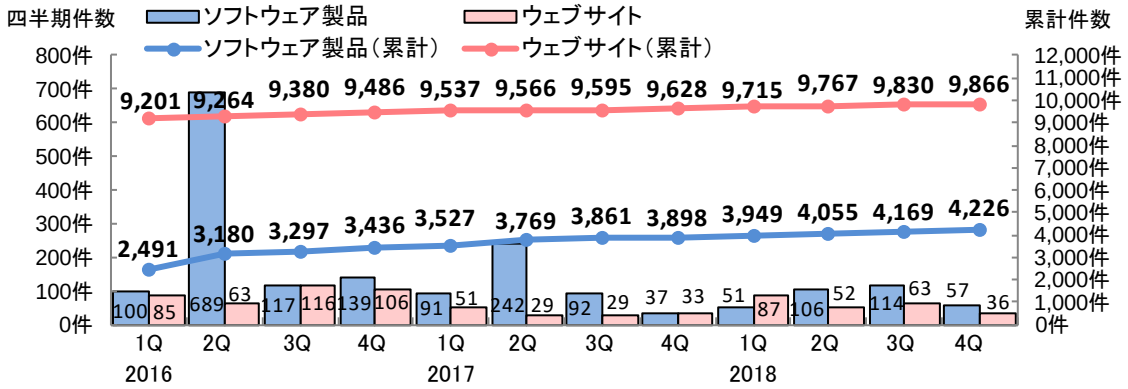


図1−1. 脆弱性の届出件数の四半期ごとの推移

表 1-2. 届出件数（過去 3 年間）

	2016 1Q	2Q	3Q	4Q	2017 1Q	2Q	3Q	4Q	2018 1Q	2Q	3Q	4Q
累計届出件数[件]	11,692	12,444	12,677	12,922	13,064	13,335	13,456	13,526	13,664	13,822	13,999	14,092
1就業日あたり[件/日]	4.09	4.26	4.25	4.25	4.21	4.21	4.17	4.11	4.08	4.06	4.03	3.99

[*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 2018 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。2018 年はソフトウェア製品が 328 件、ウェブサイトが 238 件の合計 566 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約 6 割を占めています。またウェブサイトの届出は昨年に比べ 1.7 倍ほど増加しました。

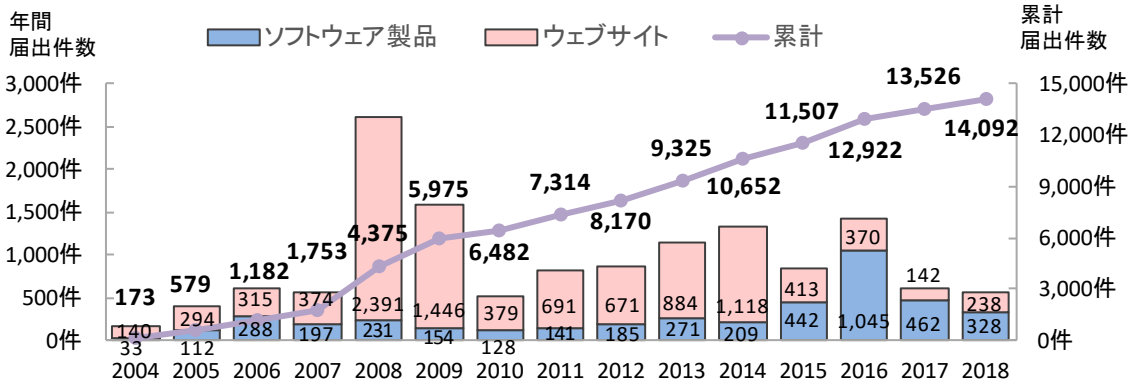


図1−2. 脆弱性の届出件数の年ごとの推移

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 9,282 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	**64** 件	**1,936** 件
ウェブサイト	**48** 件	**7,346** 件
合計	**112** 件	**9,282** 件

本四半期に JVN 公表したソフトウェア製品の件数は 64 件 (*4)（累計 1,936 件）でした。そのうち、15 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 18 件（28%）でした。また、JVN 公表前に重要インフラ事業者へ脆弱性対策情報を優先提供したのは、2 件（累計 3 件）でした (*5)。

修正完了したウェブサイトの件数は 48 件（累計 7,346 件）でした。修正を完了した 48 件のうち、ウェブアプリケーションを修正したものは 42 件（88%）、当該ページを削除したものは 6 件（12%）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 48 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 36 件（75%）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 33 件（31%））から増加しました。

また、図 1-3 は、届出開始から 2018 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。2018 年は、ソフトウェア製品が 232 件、ウェブサイトが 241 件の合計 473 件でした。

(*4) P.10 表 2-3 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。

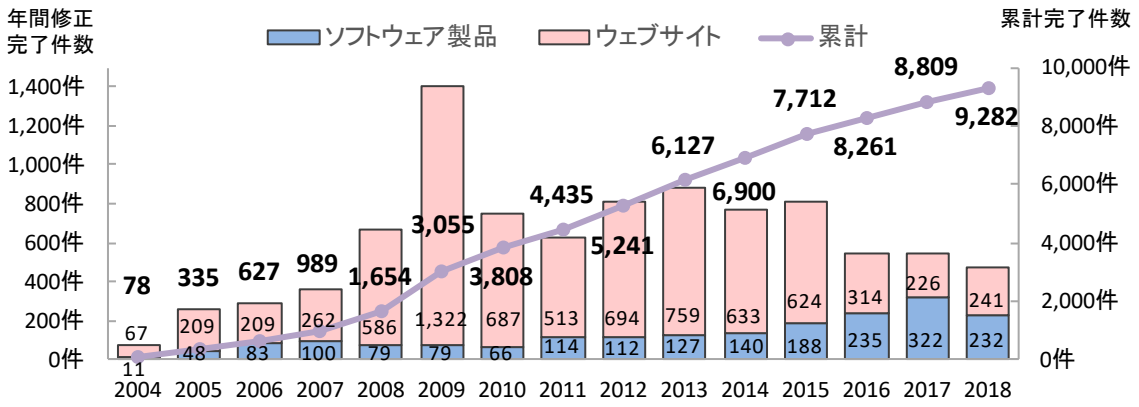


図1-3. 脆弱性の修正完了件数の年ごとの推移

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 件になります。

1-4. ウェブサイトに関する届出と対策の傾向について

1-4-1. 脆弱性対策に Web Application Firewall を活用するウェブサイト運営者が増加

2018 年において、ウェブサイトにおける「SQL インジェクション」の届出は、昨年のおよそ 2.5 倍となる 46 件でした。このうち、既に取扱いが終了しているものにおいて、およそ 30%がウェブサイト運営者より Web Application Firewall(以降、WAF)によって既に対策を行っている、または対策を行ったため、問題はないと回答があり、取扱いを終了したものでした。

届出されたウェブサイトを対象にしているため、一般的なウェブサイトにおける WAF の導入傾向と必ずしも一致しない可能性がありますが、この割合は、昨年の同回答の割合である 7%を大きく上回っており、2018 年は届出に対し、WAF によって脆弱性対策を行っているとしたウェブサイト運営者が特筆して多い傾向であったと言えます。なぜ 2018 年においてこれほどの増加がみられたのかについては不明ですが、ウェブアプリケーションを修正するよりも早く、安価に一定のセキュリティを確保することが可能であるとの考えから、WAF を採用するウェブサイト運営者が増加しているのではないかと推測されます。

WAF は、ウェブアプリケーションの脆弱性を悪用した攻撃からウェブアプリケーションを保護するセキュリティ対策の一つです。WAF を導入することによって、ウェブサイトの安全性を向上させることが可能ですが、適切な運用が不可欠であり、万能というわけでもありません。

(*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。

以下では、WAF に実装されている「ブラックリスト」と「ホワイトリスト」の検査方式について、機能の概要と適切に運用するための注意点を簡単に解説します。

・ブラックリスト

「ブラックリスト」には、主にウェブアプリケーションの脆弱性を狙った攻撃通信に含まれる特徴的な値、またはパターンが定義されています。WAF は、WAF を通過する通信と「ブラックリスト」を照合し、合致した場合にその通信を不正な通信として検出します。

WAF は、機械的に通信の中身を検査しているため、「ブラックリスト」には、攻撃以外の通常通信を遮断してしまう誤検出のリスクがあります。また、既存の攻撃通信を基に定義されている特性上、未知の攻撃は防ぐことができません。最新の攻撃に対処するためには、開発元などから提供される最新のパターンファイルを常に適用する必要があります。

また、「ブラックリスト」では、膨大な数の検出パターンが定義されていますが、全てを有効にすることは、運用上、困難です。その理由は、照合するパターンが増えることで WAF の負荷が高くなり、ウェブサイトへのアクセスが遅延したり、誤検出のリスクを高めたりするためです。「ブラックリスト」の効果を十全に発揮させるためには、防御するウェブサイトの特性や存在する脆弱性に合わせ、適切に「ブラックリスト」の設定が調整されている必要があります。

・ホワイトリスト

「ホワイトリスト」では、ウェブサイトに対する通信における正しい値、またはパターンを定義します。WAF は、WAF を通過する通信と「ホワイトリスト」を照合し、合致しない場合にその通信を不正な通信として検出します。

「ホワイトリスト」は、正常な通信のみを定義しているため、未知の攻撃であっても防御することが可能です。ただし、「ホワイトリスト」は、どのような入力値であれば正常であるか定義しなければならない都合上、作成にはウェブアプリケーションに対する深い理解が不可欠です。また、ウェブアプリケーションの仕様変更などで値が変更になった場合は、都度、「ホワイトリスト」も修正を行わなければなりません。設定が適切ではない場合は、通常通信の遮断や、攻撃を検知できずに通過させてしまうリスクが生じます。

■WAF による脆弱性対策を行うにあたって

サービスの提供を止められないなどの理由により、すぐには脆弱性を修正できない状況下において、一定水準の安全性を確保するための対策として WAF は非常に有効です。ただし、WAF はウェブアプリケーションの実装面での根本的な対策ではなく、攻撃による影響を低減する運用面での対策となるため、ウェブアプリケーションに存在する脆弱性そのものが無くなるわけではありません。このため、脆弱性に対する対策として WAF を導入していたとしても、設定の内容や、攻撃の方法によっては、防御を回避され脆弱性を悪用されてしまうリスクが存在することを認識しておく必要があります。実際に、2018 年も WAF の設定に不備があったことで、攻撃を防御できず、ウェブサイトの脆弱性を悪用されてしまう事例がありました[(*9)]。

以上の点から、IPA では、WAF を導入している場合でも、ウェブアプリケーションの実装に脆弱性が存在している場合は、実装の修正による根本的な対策を実施することを推奨しています。なお、IPA では、WAF の理解を手助けするための資料として以下を公開しています。WAF を運用される際は、是非ご活用ください。

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

---

(*9) MS コンサルで会員情報 6000 件流出か　設定ミスが原因
https://www.nikkei.com/article/DGXMZO30514280V10C18A5000000/

1-4-2. 機密情報の意図しない公開に注意

2018 年において、個人情報やサーバのパスワードなどの機密情報を含むファイルを誤ってインターネット上に公開している「ファイルの誤った公開」に関する届出は、不受理となったものを除き、18 件でした。過去の届出傾向を見ると、2017 年の届出件数は 5 件と比較的少ない件数となっているものの、2016 年は 30 件もの届出を受け付けており、本来秘匿すべき情報を誤って公開しているウェブサイトが依然として存在することが伺えます。

この問題は、ウェブサイトにおけるアクセス制限などの設定不備に起因しています。ウェブサイトの新規公開や、利用するソフトウェアの入れ替えなど、多くの設定を必要とする作業では、このような設定不備が発生しやすく、特に注意が必要です。

誤ってインターネット上に機密情報を公開してしまうと、それらのファイルも検索エンジンのクローリングの対象となるため、ウェブサイトのドメイン名と、データファイルなどで使用されることの多い dat や csv などの拡張子や、「社外秘」「Confidential」などの特定のキーワードを組み合わせることで検索エンジンから容易に検索出来てしまう場合があります。この方法は、「検索エンジン・ハッキング」「Google ハッキング」等と呼ばれる攻撃に悪用される手段にもなっており、ファイルへアクセスされることで、個人情報漏洩などの重大なインシデントにつながる恐れがあります。

このような被害を避けるために、ウェブサイトにおける作業では、十分な確認プロセスを作業計画に組み込み、設定不備を未然に防ぐことが重要です。また、作業後も定期的に設定の見直し等を行い、公開を意図しないファイルが公開状態にないかを確認することが推奨されます。

なお、万が一、機密情報を誤って公開していることを確認した場合は、速やかに非公開へ変更すると共に、状況に応じて以下の対応を行います。

・キャッシュの削除を依頼する

対象のウェブページまたはファイルを非公開にしていても、キャッシュから情報が漏洩する可能性があります。そのため、ウェブサイト運営者は検索エンジンを運営する事業者へキャッシュされた機密情報を含むウェブページやファイルの削除を依頼します。

・個人情報保護委員会へ報告する

個人情報が漏洩した場合、ウェブサイト運営者は個人情報保護委員会に速やかに報告します。ただし、業種によっては、報告先が個人情報保護委員会ではない場合もあるため、報告を行う前に事業者毎に指定された報告先を確認してください。

報告先の概要 - 個人情報保護委員会
https://www.ppc.go.jp/files/pdf/180717_houkokusaki_gaiyou.pdf

・情報漏洩が発生した旨を公表する

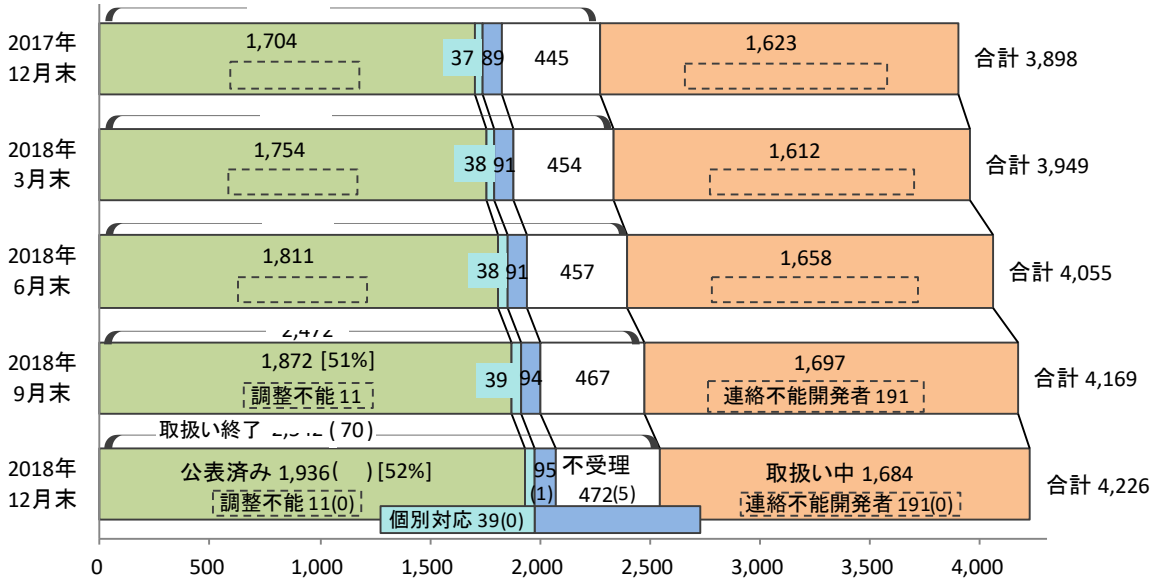
個人情報が漏洩した場合、ウェブサイト運営者は対象のウェブサイトにおいて個人情報漏洩が発生した旨を公表するようにしてください。公表することにより、漏洩した個人情報の悪用による二次被害を防止するとともに、同様の原因による個人情報の漏洩を予防することができます。

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 4,226 件で、本四半期に脆弱性対策情報を JVN 公表したものは 64 件（累計 1,936 件）でした。そのうち、JVN 公表前に重要インフラ事業者へ脆弱性対策情報を優先提供したものは 2 件（累計 3 件）でした。製品開発者が JVN 公表を行わず「個別対応」したものは無く（累計 39 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 95 件）でした。また「不受理」としたものは 5 件 (*10)（累計 472 件）、「取扱い中」は 1,684 件でした。1,684 件のうち、連絡不能開発者 (*11) 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 (*12) を連絡不能開発者一覧へ公表しています。



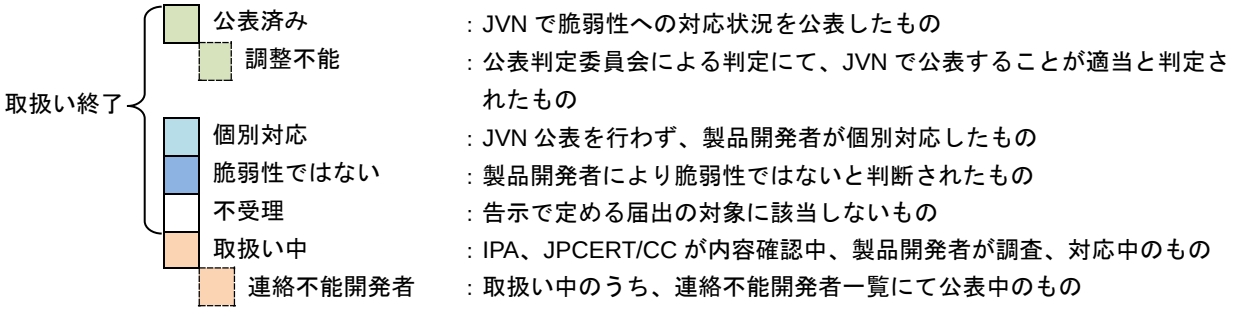


図 2-1. ソフトウェア製品脆弱性の届出処理状況（四半期ごとの推移）

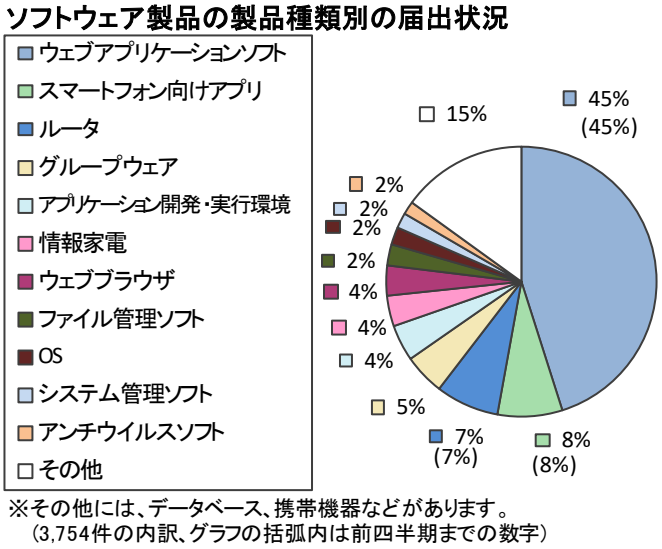
(*10) 内訳は本四半期の届出によるものが 1 件、前四半期以前の届出によるものが 4 件。
(*11) 連絡不能開発者一覧への公表および一覧からの削除が複数回行われた製品開発者の公表回数は、その累計を計上しています。
(*12) 連絡不能開発者一覧に公表中の件数は、図 2-1 の「調整不能」及び「連絡不能開発者」の合計です。

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 4,226 件のうち、不受理を除いた件数は 3,754 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

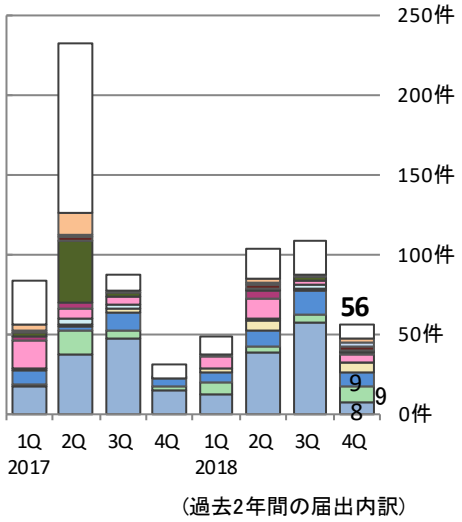
図 2-2、2-3 は、届出された脆弱性の製品種類別の内訳です。図 2-2 は製品種類別割合を、図 2-3 には過去 2 年間の四半期ごとの届出件数の推移を示しています。

本四半期の届出件数において「スマートフォン向けアプリ（9 件）」「ルータ（9 件）」が最も多く、次いで、「ウェブアプリケーションソフト（8 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 45%を占めています。



※その他には、データベース、携帯機器などがあります。
（3,754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

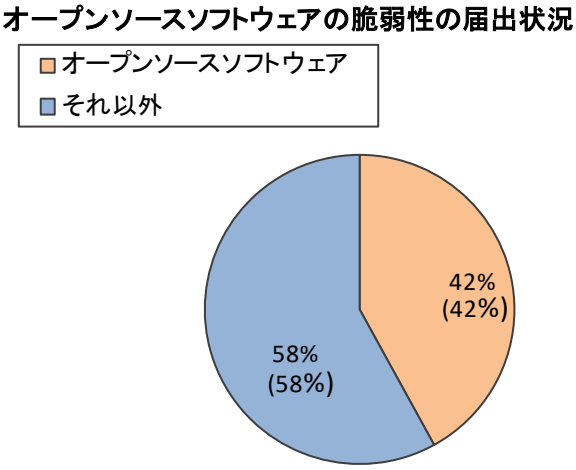


（過去2年間の届出内訳）

図2-3. 四半期ごとの製品種類別届出件数

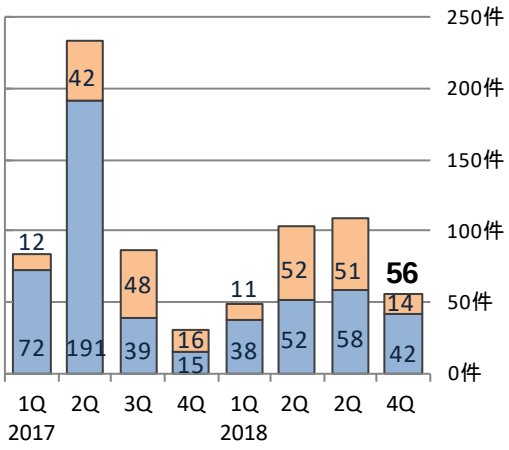
図 2-4、2-5 は、届出された製品をライセンスの形態により「オープンソースソフトウェア」（OSS）と「それ以外」で分類しています。図 2-4 は届出累計の分類割合を、図 2-5 には過去 2 年間の四半期ごとの届出件数の推移を示しています。

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 14 件あり、累計では 42%を占めています。



（3,754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）

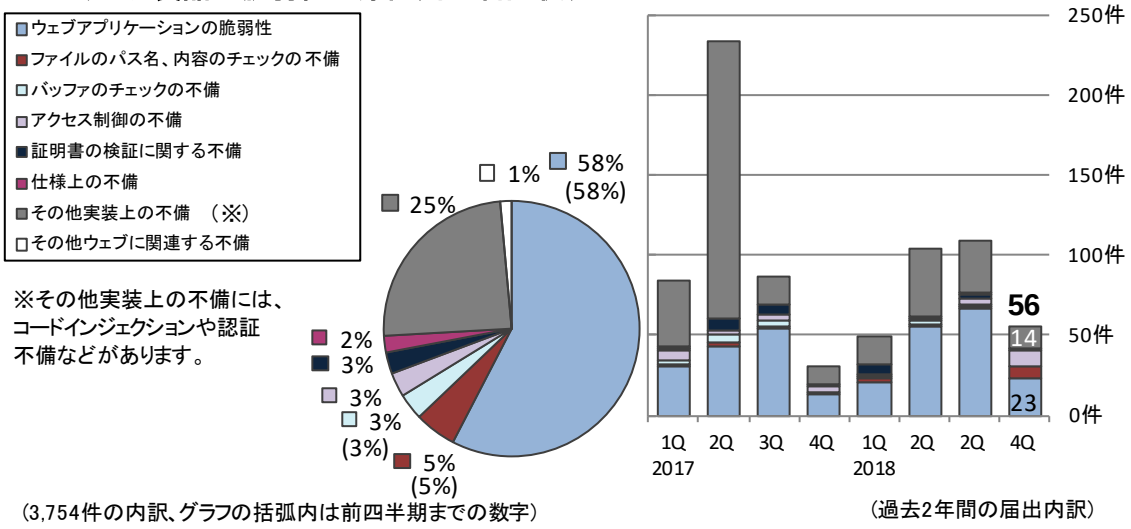
図2-5. 四半期ごとのオープンソースソフトウェア届出件数

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届出件数の推移を示しています[*13]。

本四半期は「ウェブアプリケーションの脆弱性（23 件）」が最も多く、次いで「その他実装上の不備（14 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 58%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



（3,754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

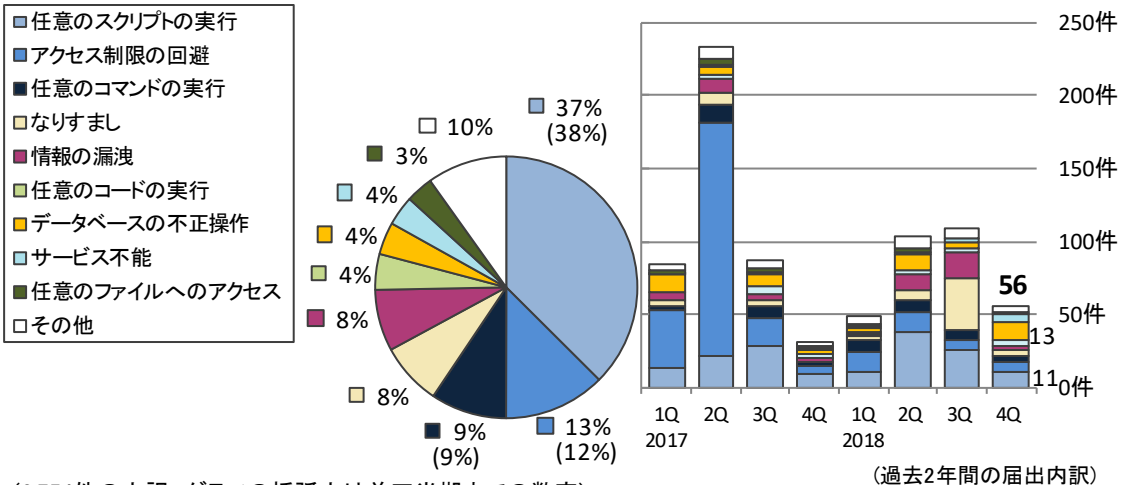
（過去2年間の届出内訳）

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届出件数の推移を示しています。

本四半期は、「データベースの不正操作（13 件）」が最も多く、次いで「任意のスクリプトの実行（11 件）」でした。累計では「任意のスクリプトの実行」が最も多く、37%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



（3,754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

[*13] 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（1,936 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。

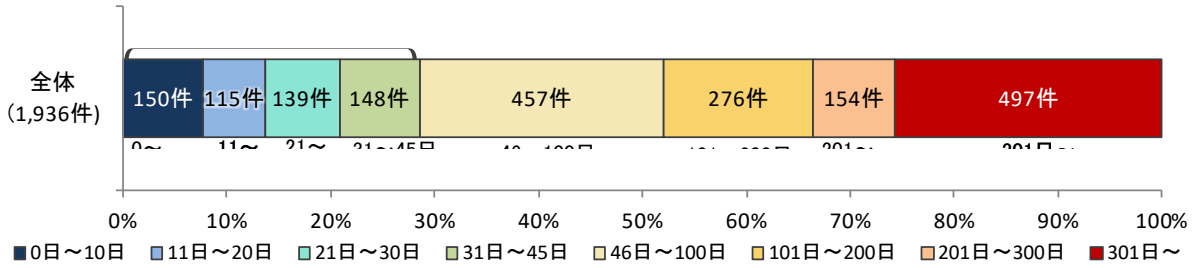


表 2-1. 45 日以内に JVN 公表した件数の割合推移（四半期ごと）

2016 1Q	2Q	3Q	4Q	2017 1Q	2Q	3Q	4Q	2018 1Q	2Q	3Q	4Q
30%	32%	32%	32%	32%	32%	30%	30%	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[(*14)]。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[(*15)]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	36 件	1,674 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	19 件	1,649 件
合計	55 件	3,323 件

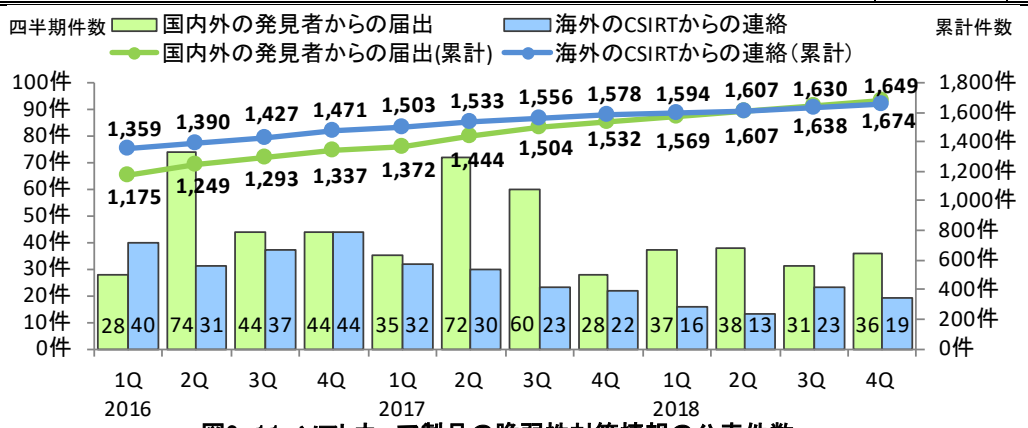


図2−11. ソフトウェア製品の脆弱性対策情報の公表件数

(*14) JPCERT/CC 活動概要 Page15～20（https://www.jpcert.or.jp/pr/2019/PR20190116.pdf）を参照下さい。
(*15) 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 11 件（表 2-3 の#1）、製品開発者自身から届けられた自社製品の脆弱性が 10 件（表 2-3 の#2）、複数開発者・製品に影響がある脆弱性が 1 件（表 2-3 の#3）、組込みソフトウェア製品の脆弱性が 5 件（表 2-3 の#4）ありました。

表 2-3. 2018 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	JVN#00344155	「Denbun」における複数の脆弱性	2018 年 10 月 4 日	7.5
2 (#2)	JVN#95355683	「FileZen」における複数の脆弱性	2018 年 10 月 15 日	10.0
3 (#2)	JVN#83739174	「サイボウズ メールワイズ」におけるディレクトリ・トラバーサルの脆弱性	2018 年 11 月 14 日	7.8
4 (#2)	JVN#15232217	「サイボウズ Office」における複数のディレクトリ・トラバーサルの脆弱性	2018 年 11 月 14 日	7.8
5 (#2)	JVN#16697622	「サイボウズ デヂエ」におけるディレクトリ・トラバーサルの脆弱性	2018 年 11 月 14 日	7.8
6 (#2)(#4)	JVN#55263945	「RICOH Interactive Whiteboard」における複数の脆弱性	2018 年 11 月 27 日	10.0
7 (#4)	JVN#99810718	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	2018 年 12 月 19 日	8.3
8 (#1)(#2)	JVN#13199224	「PgpoolAdmin」におけるアクセス制限不備の脆弱性	2018 年 12 月 21 日	7.5
脆弱性の深刻度=レベル II（警告）、CVSS 基本値=4.0～6.9				
9	JVN#77885134	「Baidu Browser」のインストーラにおける DLL 読み込みに関する脆弱性	2018 年 10 月 3 日	6.8
10	JVN#36623716	「Music Center for PC」にソフトウェアアップデート時のダウンロードファイル検証不備の脆弱性	2018 年 10 月 9 日	5.1
11 (#1)	JVN#14323043	「Metabase」におけるクロスサイト・スクリプティングの脆弱性	2018 年 10 月 11 日	4.3
12 (#1)	JVN#49995005	「OpenAM (オープンソース版)」におけるセッション管理不備の脆弱性	2018 年 10 月 12 日	4.0
13 (#1)	JVN#36343375	「YukiWiki」における複数の脆弱性	2018 年 10 月 19 日	4.3
14	JVN#58005743	「Symantec Web Isolation」におけるクロスサイト・スクリプティングの脆弱性	2018 年 10 月 19 日	4.3
15	JVN#60702986	「BlueStacks App Player」におけるアクセス制限不備の脆弱性	2018 年 10 月 24 日	5.8
16 (#1)	JVN#59394343	「OpenDolphin」における複数の脆弱性	2018 年 10 月 26 日	6.5

項番	脆弱性識別番号	脆弱性	JVN 公表日	CVSS 基本値
17	JVN#96551318	「iOS メール App」におけるサービス運用妨害(DoS)の脆弱性	2018 年 11 月 2 日	5.0
18 (#1)	JVN#75738023	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	2018 年 11 月 2 日	4.0
19	JVN#15709478	「『セキュリティ対策ツール』に対する Windows10 Fall Creators Update 向け修正モジュール」のインストーラにおける DLL 読み込みに関する脆弱性	2018 年 11 月 9 日	6.8
20 (#1)	JVN#85760090	WordPress 用プラグイン「LearnPress」における複数の脆弱性	2018 年 11 月 9 日	6.5
21 (#4)	JVN#65082538	パナソニック製「BN-SDWBP3」における複数の脆弱性	2018 年 11 月 20 日	5.8
22	JVN#78422300	「マーケットスピード」のインストーラにおける DLL 読み込みに関する脆弱性	2018 年 11 月 28 日	6.8
23 (#2)	JVN#36895151	パナソニック製アプリケーションが登録する一部の Windows サービスにおいて実行ファイルのパスが引用符で囲まれていない脆弱性	2018 年 11 月 29 日	4.6
24 (#4)	JVN#89767228	セイコーエプソン製の複数のプリンタおよびスキャナにおける複数の脆弱性	2018 年 12 月 6 日	4.3
25	JVN#32155106	「i-FILTER」における複数の脆弱性	2018 年 12 月 7 日	4.3
26 (#2)	JVN#23161885	「サイボウズ リモートサービス」における複数の脆弱性	2018 年 12 月 10 日	6.5
27 (#2)	JVN#25385698	「サイボウズ Garoon」におけるアクセス制限回避の脆弱性	2018 年 12 月 10 日	5.0
28 (#4)	JVN#87535892	「Aterm WF1200CR」および「Aterm WG1200CR」における複数の脆弱性	2018 年 12 月 14 日	5.8
29 (#3)	JVN#69812763	「cordova-plugin-ionic-webview」におけるパス・トラバーサルの脆弱性	2018 年 12 月 21 日	4.3
30 (#1)	JVN#27052429	WordPress 用プラグイン「Google XML Sitemaps」におけるクロスサイト・スクリプティングの脆弱性	2018 年 12 月 25 日	4.0
31	JVN#33677949	「マッピングツール」のインストーラにおける DLL 読み込みに関する脆弱性	2018 年 12 月 25 日	6.8
32 (#1)	JVN#96493183	「GROWI」におけるクロスサイト・スクリプティングの脆弱性	2018 年 12 月 26 日	4.0
脆弱性の深刻度=レベル I（注意）、CVSS 基本値=0.0～3.9				
33 (#1)	JVN#73794686	「User-friendly SVN」におけるクロスサイト・スクリプティングの脆弱性	2018 年 10 月 9 日	2.6
34	JVN#21528670	「SecureCore Standard Edition」における認証不備の脆弱性	2018 年 10 月 24 日	2.1
35	JVN#37943805	「Confluence Server」におけるスクリプト・インジェクションの脆弱性	2018 年 10 月 29 日	3.5
36 (#1)(#2)	JVN#25359688	「EC-CUBE」におけるオープンリダイレクトの脆弱性	2018 年 11 月 28 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 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 19 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	Auto-Maskin DCU 210E、RP 210E および Marine Pro Observer App に複数の脆弱性	注意喚起として掲載
2	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
3	Intel 製品に複数の脆弱性	注意喚起として掲載
4	オムロン製 CX-Supervisor に複数の脆弱性	特定製品開発者と調整
5	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
6	Apache Tomcat JK mod_jk Connector にパストラバーサルの脆弱性	注意喚起として掲載 複数製品開発者へ通知
7	Texas Instruments 製マイクロコントローラ CC2640 および CC2650 に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
8	Cisco ASA および FTD の SIP インスペクション機能におけるサービス運用妨害 (DoS) の脆弱性	注意喚起として掲載
9	LogonTracer に複数の脆弱性	特定製品開発者と調整
10	自己暗号化ドライブ製品における複数の脆弱性	複数製品開発者と調整
11	Android アプリ「みずほ銀行　みずほダイレクトアプリ」における SSL サーバ証明書の検証不備の脆弱性	特定製品開発者と調整
12	オムロン製 CX-One に複数の脆弱性	特定製品開発者と調整
13	Adobe Flash Player および Flash Player Installer に脆弱性	注意喚起として掲載
14	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
15	Pixar Tractor 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
16	Internet Explorer の JScript スクリプトエンジンにおけるメモリ破損の脆弱性	注意喚起として掲載
17	横河電機製 Vnet/IP オープン通信ドライバにサービス運用妨害 (DoS) の脆弱性	特定製品開発者と調整
18	MsiAdvertiseProduct における権限昇格の脆弱性	注意喚起として掲載
19	ファイルシステムドライバ Dokan におけるスタックバッファオーバーフローの脆弱性	注意喚起として掲載

[*16] JPCERT/CC 製品開発者リスト：https://jvn.jp/nav/index.html

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[17]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 件でした。

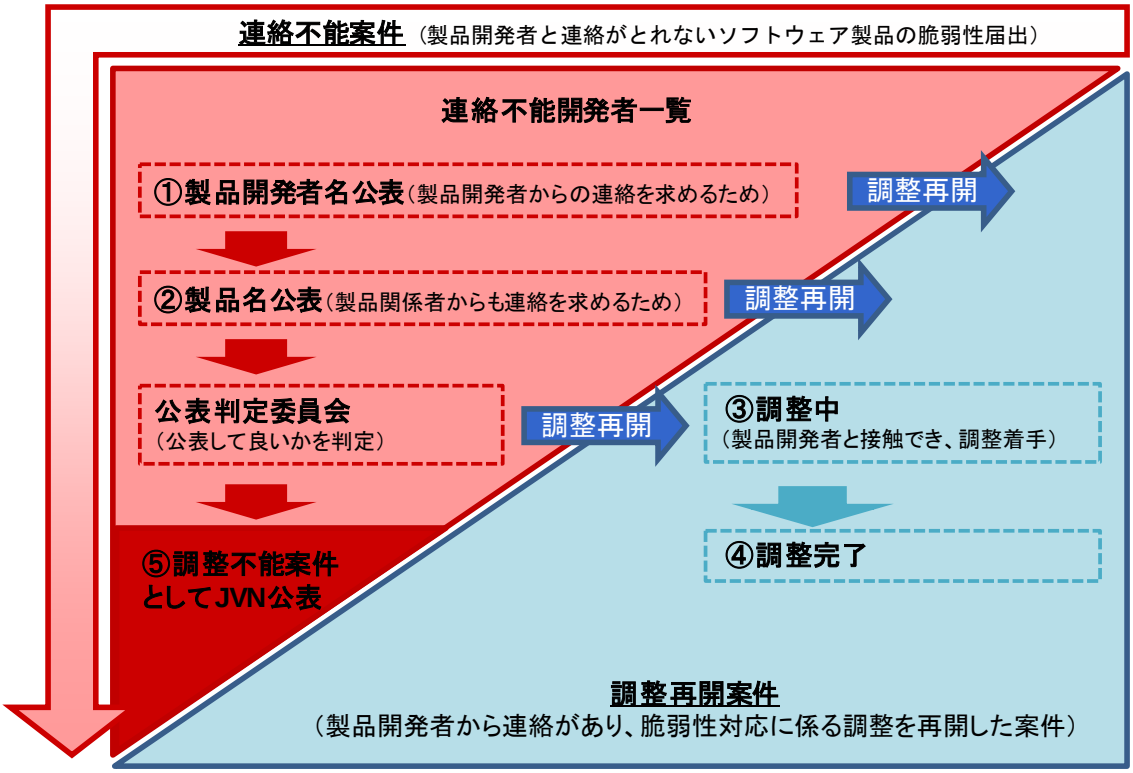
2-1-7. 連絡不能案件の処理状況

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 191 件、調整再開した案件（③+④）は 49 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 11 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。



2018年 第3四半期	191件 （①1件 ②190件）	49件 （③23件 ④26件）	⑤ 11 件	合計 251件
2018年 第4四半期	191件 （①1件 ②190件）	49件 （③23件 ④26件）	⑤11 件	合計 251件

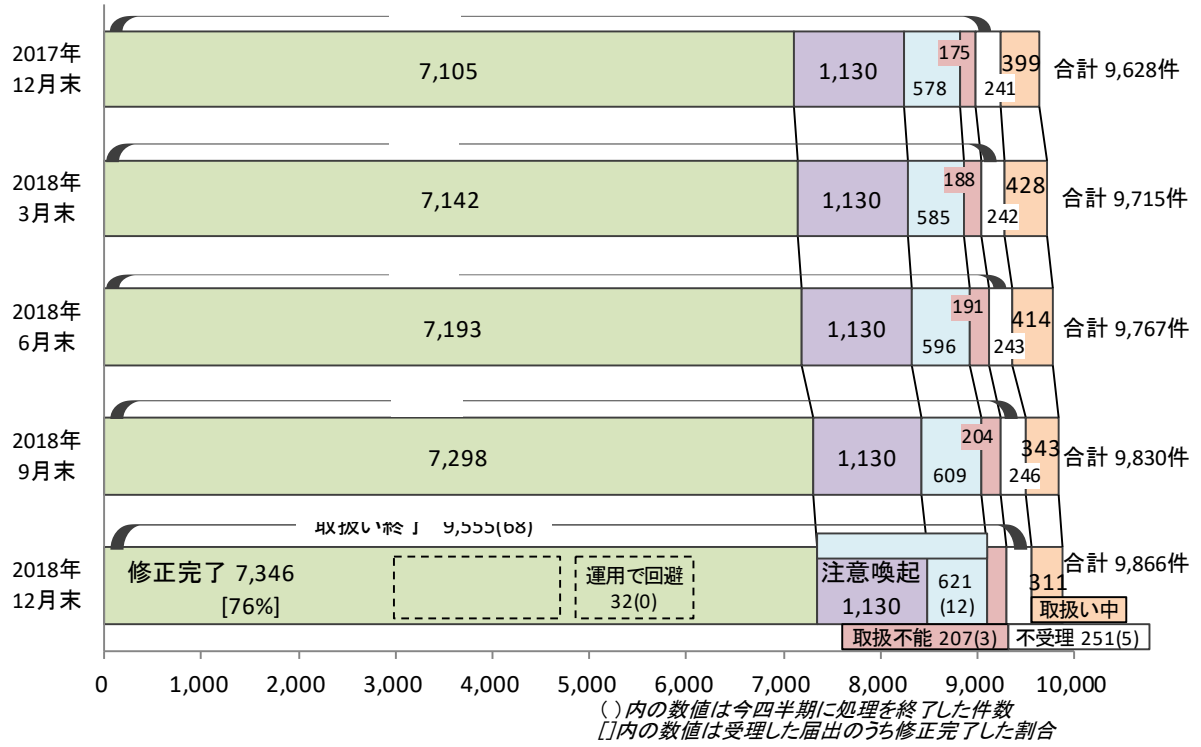
図2-12. 連絡不能案件の処理状況

[17] 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とします。

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 9,866 件で、本四半期中に取扱いを終了したものは 68 件（累計 9,555 件）でした。このうち「修正完了」したものは 48 件（累計 7,346 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 12 件（累計 621 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 207 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 5 件[*19]（累計 251 件）でした。取扱いを終了した累計 9,555 件のうち「修正完了」「脆弱性ではない」の合計 7,967 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 6 件（累計 1,086 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 32 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

[*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 4 件、前四半期以前によるものが 1 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 9,866 件のうち、不受理を除いた件数は 9,615 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 32 件あり、そのうち約 4 割強を企業が占めています。

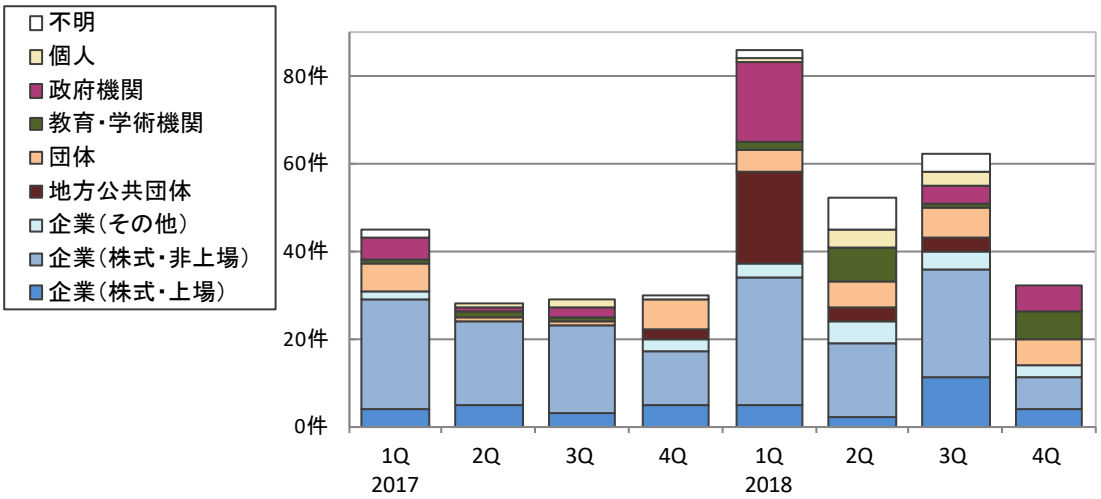


図2−14. 四半期ごとの運営主体の種類別届出件数

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届出件数の推移を示しています[*20]。

本四半期は「クロスサイト・スクリプティング（19 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 55%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。

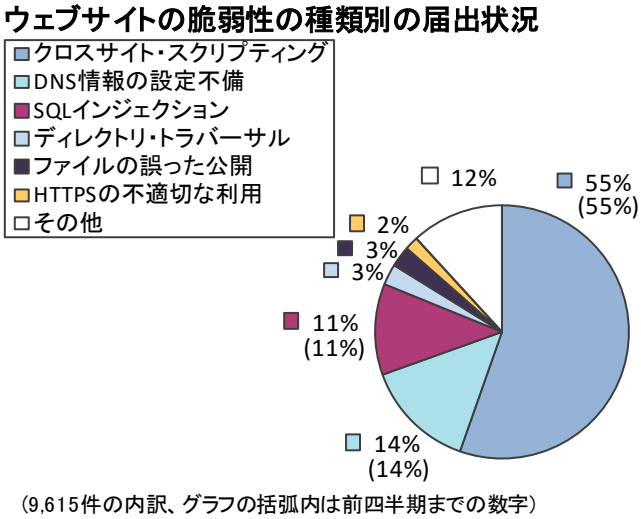


図2−15. 届出累計の脆弱性の種類別割合

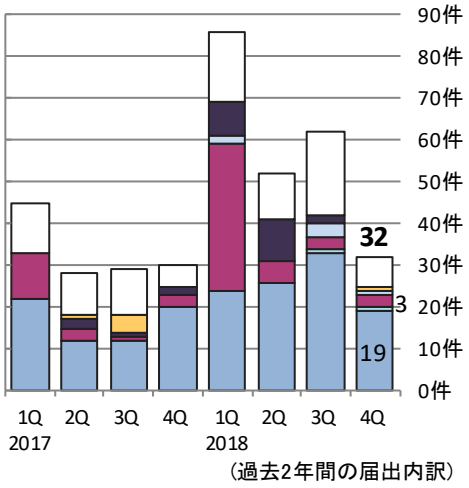
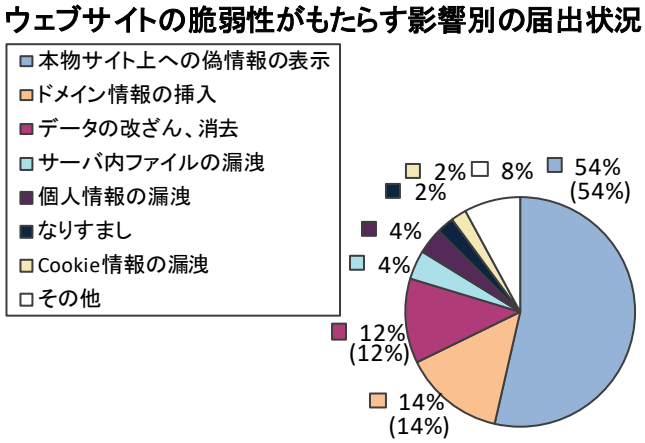


図2−16. 四半期ごとの脆弱性の種類別届出件数

[*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。

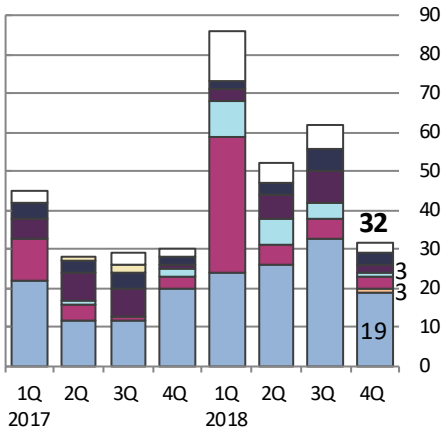
図 2-17、2-18 は、届出された脆弱性がもたらす影響別の内訳です。図 2-17 は届出の影響別割合を、図 2-18 には過去 2 年間の四半期ごとの届出件数の推移を示しています。

本四半期は「本物サイト上への偽情報の表示（19 件）」が最も多く、次いで「データの改ざん、消去（3 件）」、「なりすまし（3 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」が全体の約 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。



（9,615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 48 件のうち 36 件（75%）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（105 件中 33 件）の 31%から増加しました。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 65%でした。

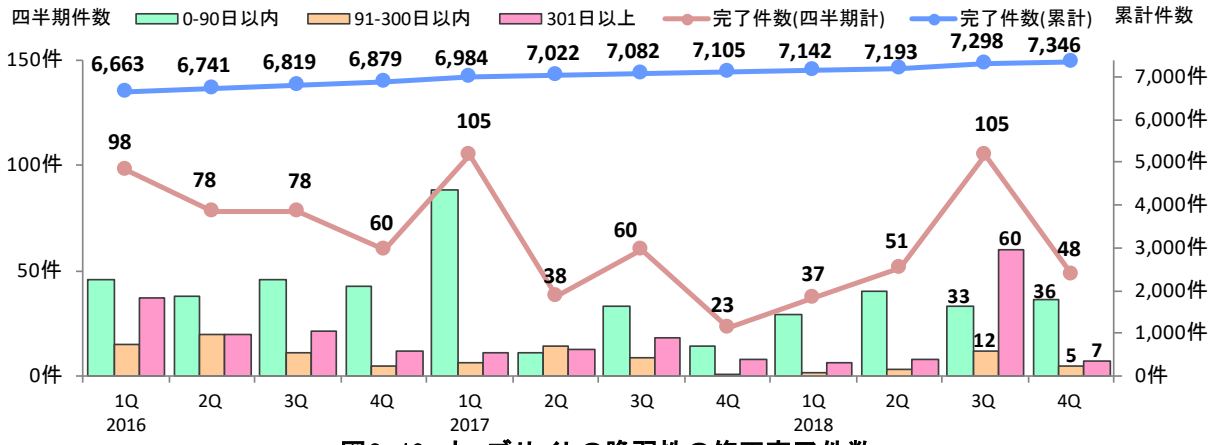


図2−19. ウェブサイトの脆弱性の修正完了件数

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

	2016 1Q	2Q	3Q	4Q	2017 1Q	2Q	3Q	4Q	2018 1Q	2Q	3Q	4Q
修正完了件数	6,663	6,741	6,819	6,879	6,984	7,022	7,082	7,105	7,142	7,193	7,298	7,346
90 日以内の件数	4,387	4,425	4,471	4,514	4,602	4,613	4,646	4,660	4,689	4,729	4,762	4,798
90 日以内の割合	66%	66%	66%	66%	66%	66%	66%	66%	66%	66%	65%	65%

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。

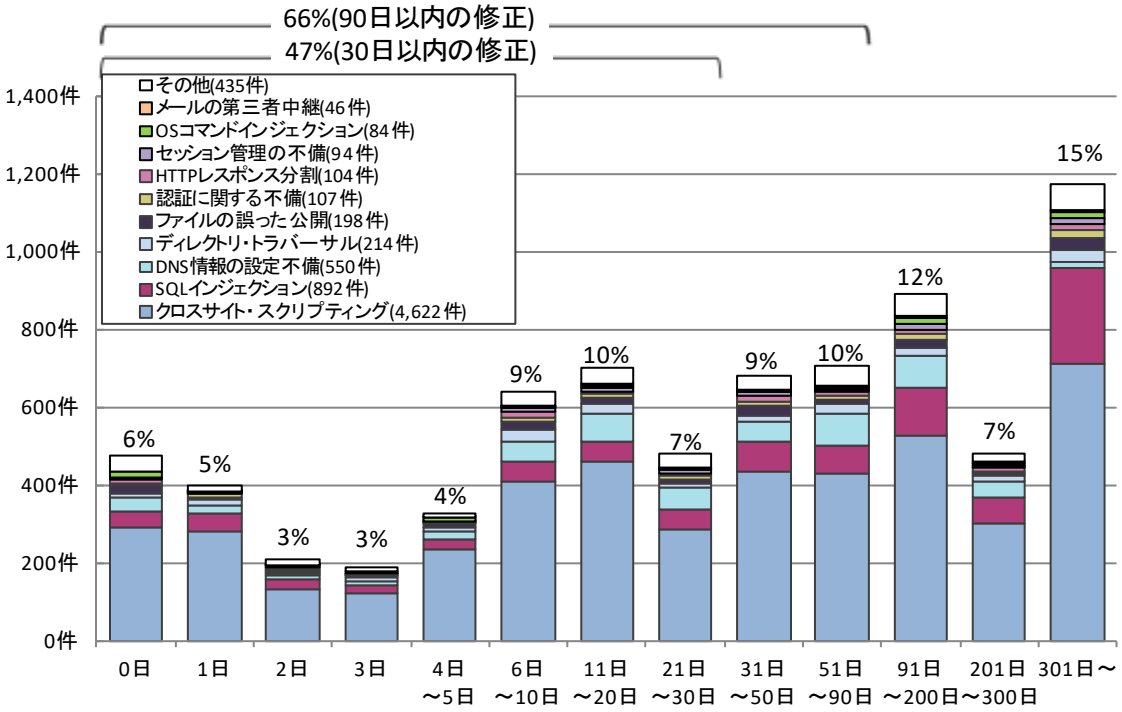


図2-20. ウェブサイトの修正に要した日数

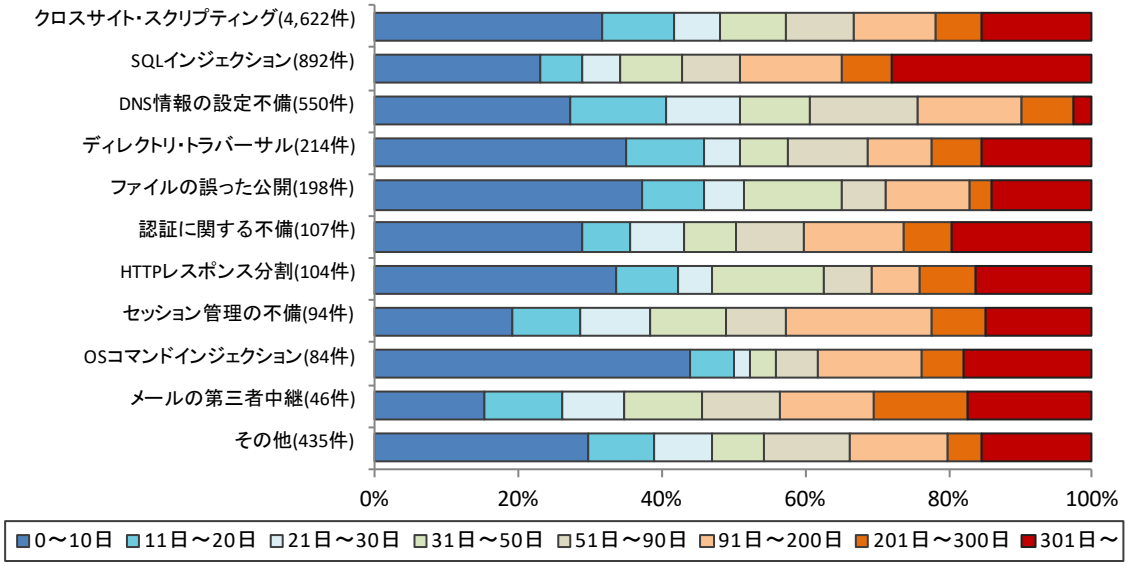


図2-21. ウェブサイトの修正に要した脆弱性種類別の日数の傾向

[*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 265 件（前四半期は 259 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 23%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。

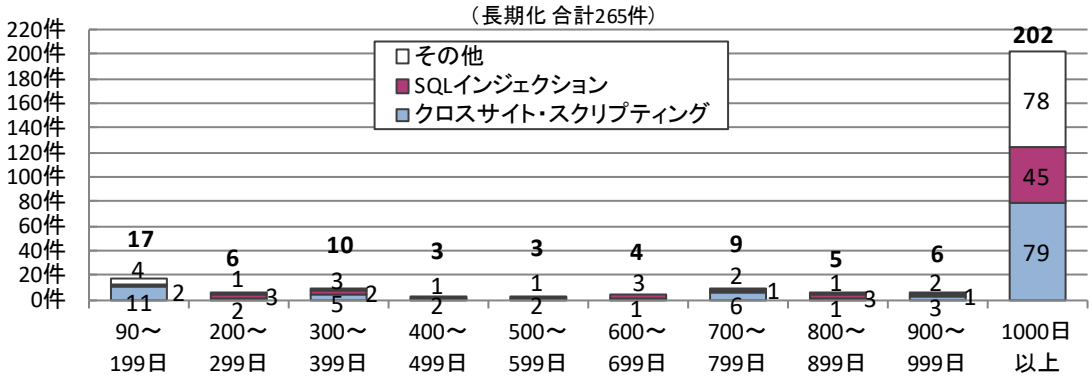


図2−22. 取扱いが長期化(90日以上経過)している届出の取扱経過日数と脆弱性の種類

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

	2017 1Q	2Q	3Q	4Q	2018 1Q	2Q	3Q	4Q
取扱い中の件数	495	478	406	399	428	413	342	311
長期化している件数	387	376	342	333	329	334	259	265
長期化している割合	78%	79%	84%	83%	77%	81%	76%	85%

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/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

⇒「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ページ」
https://www.ipa.go.jp/security/announce/sw_security_info.html

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。

⇒「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/files/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.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 脆弱性対策情報フィルタリング収集ツール（mjcheck3）」: https://jvndb.jvn.jp/apis/myjvn/mjcheck3.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」: https://jvndb.jvn.jp/apis/myjvn/vccheck.html

⇒「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。

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/vuln/report/notice/handling_notaccept.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

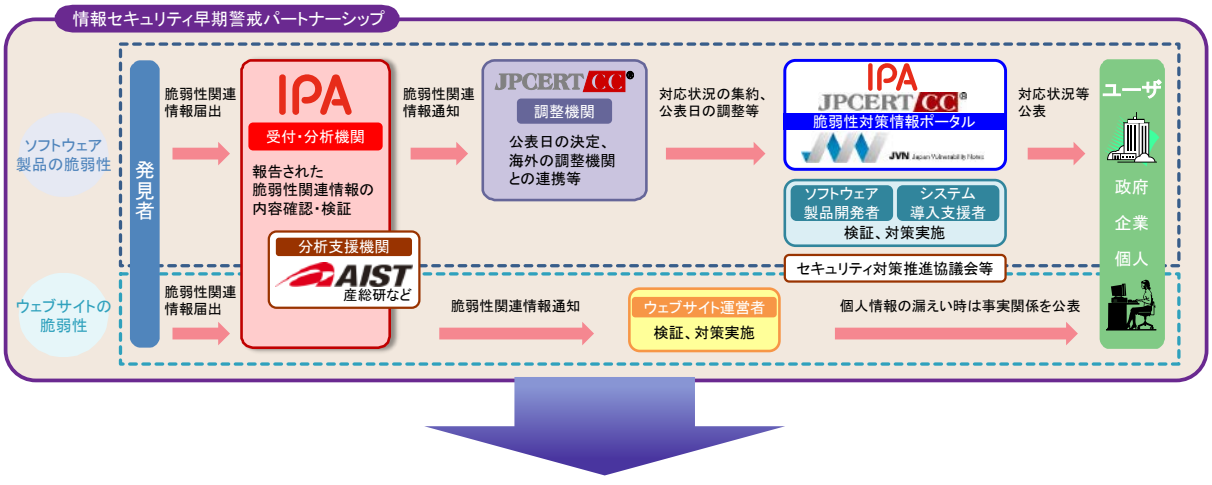
付表 2. ウェブサイトの脆弱性の分類

	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