Japan Computer Emergency Response Team Coordination Center

電子署名者 : Japan Computer Emergency Response Team Coordination Center
DN : c=JP, st=Tokyo, l=Chiyoda-ku, email=office@jpcert.or.jp, o=Japan Computer Emergency Response Team Coordination Center, cn=Japan Computer Emergency Response Team Coordination Center
日付 : 2017.10.11 14:53:07 +09'00'

JPCERT-PR-2017-04
発行日：2017-10-12

JPCERT/CC 活動概要 [2017 年 7 月 1 日 ～ 2017 年 9 月 30 日]

活動概要トピックス

ートピック1ー　サイバーセキュリティ対策活動への協力者に感謝状贈呈

JPCERT/CC は、国内のサイバーセキュリティインシデント（以下「インシデント」）による被害を低減するために、インシデントへの対応支援活動、インシデントを未然に防ぐための早期警戒活動、マルウエア分析、ソフトウエア製品等の脆弱性に関する調整活動などを行っています。これらの活動を円滑かつ効果的に進めるためには、情報提供等、さまざまな皆様からのご協力が欠かせません。

JPCERT/CC では、サイバーセキュリティ対策活動に対する皆様からの御好意と御力添えに深く思いをいたし、特に顕著なご貢献をいただいた方に感謝状を贈呈する制度を設けています。本年度は、長年にわたり脆弱性の探索や攻撃活動などの分析結果を JPCERT/CC に提供してこられ、さらに 2016 年には大規模な DDos 攻撃を引き起こしたマルウエア「Mirai」の分析と国内の被害低減に有用な情報を提供された株式会社クルウィットの 島村 隼平 様、および、自社で確認した APT 攻撃の詳細な情報や、脅威度の高い脆弱性について詳細な分析レポートを JPCERT/CC に提供され、国内の被害拡大を防ぐ活動に貢献された Recruit-CSIRT 様のお二方に対して、2017 年 7 月に感謝状と記念の盾を贈呈いたしました。

サイバーセキュリティ対策活動への協力者に感謝状贈呈
https://www.jpcert.or.jp/press/priz/2017/PR20170725-priz.html

ートピック2ー　継続する Web アプリケーションフレームワークの脆弱性報告を受けて

今日、多くの Web サーバが Web アプリケーションを用いてさまざまなコンテンツや機能を提供しています。Web アプリケーションの開発では、多くの場合、フレームワークが利用されています。広く利用されているフレームワークに、オープンソースソフトウエアとして提供されている Apache Struts や Apache Tomcat などがあります。これらのソフトウエアには深刻な脆弱性がたびたび報告されており、3 月に報告された Apache Struts2 の脆弱性を悪用した情報窃取などの被害が、その後の半年間に国内外で次々と公表されるという事態となりました。

オープンソースソフトウエアで脆弱性が報告されると、攻撃コードを含む詳細情報が広まって攻撃活動を助長させることがあります。さらに、Web アプリケーションフレームワークで作られた Web サーバの脆弱性の修正には、Web サーバの管理者だけでなく、Web アプリケーションの開発者の対応が必要となるため、想定以上に時間を要する傾向があります。したがって、新たな脆弱性が公表された時には、Web

サーバの管理者だけでなく Web アプリケーションの開発者にも適切な対応をしていただけるよう、正確な技術情報を迅速に伝えていく必要があります。

本四半期に JPCERT/CC では、Web サイト関連のソフトウエアの脆弱性に関して、1 件の Cyber News Flash と 3 件の注意喚起を発行しました。特に、本四半期に報告された脆弱性は、開発者からの公表から間もなく実証コードが公開されたことに加え、公表された修正内容についても新たな問題が指摘されたり、公表情報が複数回更新されたりしたため、Web サーバの管理者の方に混乱なく対応いただけるよう、最新の技術情報を提供できるよう努めました。これらの情報には、開発者からの公表情報だけでなく、JPCERT/CC による実証コードの確認結果や独自に収集した関連情報を含め、管理者や開発者が対応を進める上で参考となる技術情報を記載しています。JPCERT/CC が、本四半期に発行した Web サイト関連のソフトウエアの脆弱性に関する情報の詳細については「1.2.1. 情報提供」をご参照ください。

本活動は、経済産業省より委託を受け、「平成 29 年度サイバー攻撃等国際連携対応調整事業」として実施したものです。
ただし、「7.フィッシング対策協議会の会員組織向け活動」に記載の活動については、この限りではありません。また、「4.国際連携活動関連」、「9.主な講演活動」、「10. 主な執筆」、「11. 協力、後援」には、受託事業以外の自主活動に関する記載が一部含まれています。

JPCERT CC®

目次

1. 早期警戒

1.1. インシデント対応支援

JPCERT/CC が本四半期に受け付けたコンピュータセキュリティインシデント（以下「インシデント」）に関する報告は、報告件数ベースで 4,600 件、インシデント件数ベースでは 4,811 件でした(注 1)。

（注 1）「報告件数」は、報告者から寄せられた Web フォーム、メール、FAX による報告の総数を示します。また、「インシデント件数」は、各報告に含まれるインシデントの件数の合計を示し、1 つのインシデントに関して複数の報告が寄せられた場合にも 1 件のインシデントとして扱います。

JPCERT/CC が国内外のインシデントに関連するサイトとの調整を行った件数は 2,234 件でした。前四半期の 2,553 件と比較して 12%減少しています。「調整」とは、フィッシングサイトが設置されているサイトや、改ざんにより JavaScript が埋め込まれているサイト、ウイルス等のマルウエアが設置されたサイト、「scan」のアクセス元等の管理者等に対し、状況の調査や問題解決のための対応を依頼する活動です。

JPCERT/CC は、インターネット利用組織におけるインシデントの認知と対処、インシデントによる被害拡大の抑止に貢献することを目的として活動しています。国際的な調整・支援が必要となるインシデントについては、日本における窓口組織として、国内や国外（海外の CSIRT 等）の関係機関との調整活動を行っています。

インシデント報告対応活動の詳細については、別紙「JPCERT/CC インシデント報告対応レポート」をご参照ください。

JPCERT/CC インシデント報告対応レポート
https://www.jpcert.or.jp/pr/2017/IR_Report20170713.pdf

1.1.1. インシデントの傾向

1.1.1.1. フィッシングサイト

本四半期に報告をいただいたフィッシングサイトの件数は 1,011 件で、前四半期の 736 件から 37%増加しました。また、前年度同期（467 件）との比較では、116%の増加となりました。

本四半期のフィッシングサイトの報告件数を、装っていたブランドが国内か国外かで分けた内訳を添えて［表 1-1］に示します。

［表 1-1 フィッシングサイトの国内・国外ブランド別の件数］

フィッシングサイト	7 月	8 月	9 月	国内外別合計（割合）
国内ブランド	69	58	46	173(17%)
国外ブランド	196	253	237	686(68%)
ブランド不明 (注 5)	43	52	57	152(15%)
全ブランド合計	308	363	340	1,011(100%)

（注 2）「ブランド不明」は、報告されたフィッシングサイトが停止していた等の理由により、JPCERT/CC がブランドを確認することができなかったサイトの件数を示します。

本四半期は、攻撃者がフィッシング目的で新規にドメインの取得やサーバの利用契約をしたと見られるフィッシングサイトが多く確認され、その中には無料の SSL サーバ証明書を使用して HTTPS に対応しているフィッシングサイトも多くありました。

これまでのフィッシングサイトは、サーバ証明書を使用していないような一般の Web サイトにフィッシングのコンテンツが置かれたものが多く、HTTPS を使用するフィッシングサイトはあまり多くはありませんでした。最近では、無料で証明書を作成できるサービスや、証明書が用意される Web サイト作成サービス、CDN サービスなどがあるため、攻撃者にとっても、これらのサービスを悪用したり、サービスを利用しているサイトに侵入したりすることで、HTTPS のフィッシングサイトを立ち上げやすくなってきていると考えられます。したがって、これまではフィッシングサイトを見分ける手段の一つとして、URL が HTTPS であるか否かを Web ブラウザのアドレスバーで確認する方法がありましたが、今や HTTPS のサイトであっても注意が必要です。

国内ブランドのフィッシングサイトは、前四半期に引き続き、通信事業者の Web メールを装ったフィッシングサイトと、SNS を装ったフィッシングサイトに関する報告が多く寄せられました。国内通信事業者を装ったフィッシングでは、海外の無料 Web サイト作成サービスでサイトを立ち上げ、短縮 URL で誘導する手法が多く見られました。また、SNS を装ったフィッシングのほとんどは、.cn の下で正規サイトを装ったドメイン名を使用していました。

フィッシングサイトの調整先の割合は、国内が 24%、国外が 76%であり、前四半期（国内 26%、国外 74%）に比べ、国外への調整の割合が増加しています。

1.1.1.2. Web サイト改ざん

本四半期に報告が寄せられた Web サイト改ざんの件数は、254 件でした。前四半期の 461 件から 45%減少しています。

前四半期に比べて、改ざんされた Web サイトに関する報告が大幅に減少しました。原因としては、Web

サイトの改ざんを容易にするような新しい脆弱性が確認されなかったことや、マルウエアを配布する手段として、Web サイト改ざんによるドライブバイダウンロード攻撃よりも、ファイルを添付してメールで送る方法が主流になってきていることなどが考えられます。
8 月後半から、CMS を使用した Web サイトのページ末尾に埋め込まれた不正なスクリプトによってサポート詐欺サイトに誘導される事例を確認しています。サポート詐欺サイトは、PC がマルウエアに感染しているという偽の警告を表示し、マルウエアの削除手順について案内するため、表示されている電話番号に電話をかけるよう促すものでした。

1.1.1.3. その他

標的型攻撃に分類されるインシデントの件数は、7 件でした。前四半期の 9 件から 22%減少しています。本四半期は、対応を依頼した組織は 7 件でした。

7 月後半ごろ、標的型攻撃と見られるなりすましメールに関する報告が、複数の組織から寄せられました。これらの報告では、攻撃に使われた手口やファイルの名前に共通点が見られました。

報告を受けたなりすましメールの一つには ZIP ファイルが添付されており、展開すると、TXT ファイルに偽装したショートカットファイル（LNK ファイル）と、RTF 形式の文書ファイルが含まれていました。これらのファイルを開くと、海外のサーバから Powershell スクリプトをダウンロードして実行する仕組みになっていました。RTF ファイルには、2017 年 4 月に修正された Microsoft 製品の脆弱性（CVE-2017-0199）を悪用して、スクリプトをダウンロードし実行するコードが含まれていました。最終的にダウンロードされるスクリプトは、攻撃によって侵害した PC を操作するためのもので、そのコードは脆弱性診断などの目的で使用されるツールに類似していました。

また、報告された別のなりすましメールには、ファイルをダウンロードするためのリンクが記載されており、ダウンロードされる ZIP ファイルを展開すると、先に述べた事例と同様に RTF ファイルと LNK ファイルが含まれていました。こちらの RTF ファイルは無害なものでしたが、LNK ファイルをたどると、LNK ファイルで指定されたホストから Powershell スクリプトをダウンロードし、実行する仕組みになっていました。

これらのなりすましメールは、いずれも国内のメールサーバが配送元になっていました。JPCERT/CC から、なりすましメールの配送元サーバを管理していた組織に連絡したところ、アカウントが不正に使用されていたとの返信をいただきました。

1.1.2. インシデントに関する情報提供のお願い

Web サイト改ざん等のインシデントを認知された場合は、JPCERT/CC にご報告ください。JPCERT/CC では、当該案件に関して攻撃に関与してしまう結果となった機器等の管理者への対応依頼等の必要な調整を行うとともに、同様の被害の拡大を抑えるため、攻撃方法の変化や対策を分析し、随時、注意喚起等の情報発信を行います。

インシデントによる被害拡大および再発の防止のため、今後とも JPCERT/CC への情報提供にご協力をお願いいたします。

1.2. 情報収集・分析

JPCERT/CC では、国内の企業ユーザが利用するソフトウエア製品の脆弱性情報、国内のインターネットユーザが影響を受ける可能性のあるコンピュータウイルス、Web サイト改ざん等のサイバー攻撃に関する情報を収集し、分析しています。これらのさまざまな脅威情報を多角的に分析し、併せて脆弱性やウイルス検体の検証等も必要に応じて行っています。さらに、分析結果に応じて、国内の企業、組織のシステム管理者を対象とした「注意喚起」（一般公開）や、国内の重要インフラ事業者等を対象とした「早期警戒情報」（限定配付）等を発信することにより、国内におけるサイバーインシデントの発生・拡大の抑止を目指しています。

1.2.1. 情報提供

JPCERT/CC の Web ページ（https://www.jpcert.or.jp）や RSS、約 34,000 名の登録者を擁するメーリングリスト、早期警戒情報の提供用ポータルサイト WAISE（Watch and Warning Analysis Information for Security Experts）等を通じて情報提供を行いました。

1.2.1.1. JPCERT/CC からのお知らせ

JPCERT/CC で収集したセキュリティ関連情報のうち、各組織のセキュリティ対策に有用であると判断した情報を「お知らせ」としてまとめ公表しています。本四半期には次のようなお知らせを発行しました。

発行件数：1 件　https://www.jpcert.or.jp/update/2017.html

2017-08-01　STOP!! パスワード使い回し!!キャンペーン 2017 そのパスワードを知っているのは、本当にあなただけですか？

1.2.1.2. 注意喚起

注意喚起は深刻かつ影響範囲の広い脆弱性等について公表する情報です。本四半期は次のような注意喚起を発行しました。

発行件数：20 件（うち 6 件更新）　https://www.jpcert.or.jp/at/

2017-07-10　Apache Struts 2 の脆弱性 (S2-048) に関する注意喚起 (公開)
2017-07-11　Apache Struts 2 の脆弱性 (S2-048) に関する注意喚起 (更新)
2017-07-12　Adobe Flash Player の脆弱性 (APSB17-21) に関する注意喚起 (公開)

2017-07-12　2017 年 7 月マイクロソフトセキュリティ更新プログラムに関する注意喚起 (公開)
2017-07-13　ISC BIND 9 の脆弱性に関する注意喚起 (更新)
2017-07-18　Cisco WebEx Browser Extension の脆弱性 (CVE-2017-6753) に関する注意喚起 (公開)
2017-07-19　2017 年 7 月 Oracle Java SE のクリティカルパッチアップデートに関する注意喚起 (公開)
2017-08-09　Adobe Flash Player の脆弱性 (APSB17-23) に関する注意喚起 (公開)
2017-08-09　Adobe Reader および Acrobat の脆弱性 (APSB17-24) に関する注意喚起 (公開)
2017-08-09　2017 年 8 月マイクロソフトセキュリティ更新プログラムに関する注意喚起 (公開)
2017-08-30　Adobe Reader および Acrobat の脆弱性 (APSB17-24) に関する注意喚起 (更新)
2017-09-06　Apache Struts 2 の脆弱性 (S2-052) に関する注意喚起 (公開)
2017-09-06　Apache Struts 2 の脆弱性 (S2-052) に関する注意喚起 (更新)
2017-09-07　Apache Struts 2 の脆弱性 (S2-052) に関する注意喚起 (更新)
2017-09-12　NTT ドコモ Wi-Fi STATION L-02F の脆弱性に関する注意喚起 (公開)
2017-09-13　Adobe Flash Player の脆弱性 (APSB17-28) に関する注意喚起 (公開)
2017-09-13　2017 年 9 月マイクロソフトセキュリティ更新プログラムに関する注意喚起 (公開)
2017-09-13　Bluetooth の実装における脆弱性 "BlueBorne" に関する注意喚起 (公開)
2017-09-20　Apache Tomcat における脆弱性に関する注意喚起 (公開)
2017-09-25　Apache Tomcat における脆弱性に関する注意喚起 (更新)

1.2.1.3. Weekly Report

JPCERT/CC が収集したセキュリティ関連情報のうち重要と判断した情報の抜粋をレポートにまとめ、原則として毎週水曜日（週の第 3 営業日）に Weekly Report として発行しています。このレポートには、「ひとくちメモ」として、情報セキュリティに関する豆知識も掲載しています。本四半期における発行は次のとおりです。

発行件数：13 件　https://www.jpcert.or.jp/wr/

Weekly Report で扱った情報セキュリティ関連情報の項目数は、合計 13 件、「今週のひとくちメモ」のコーナーで紹介した情報は、次の 13 件でした。

2017-07-05　CyberNewsFlash を新設
2017-07-12　FIRST が「Guidelines and Practices for Multi-Party Vulnerability Coordination and Disclosure」を公開
2017-07-20　総務省が「サイバー攻撃（標的型攻撃）対策防御モデルの解説」を公開
2017-07-26　速やかにキャッシュ DNS サーバの設定の見直しを
2017-08-02　Web サイトへのサイバー攻撃に備えて
2017-08-09　警察庁のサイトを装う偽サイトに注意
2017-08-16　CSA ジャパンが「IoT へのサイバー攻撃仮想ストーリー集（第一版）」を公開
2017-08-23　マルウエア Datper をプロキシログから検知する方法
2017-08-30　JNSA が「セキュリティ知識分野（SecBoK）人材スキルマップ 2017 年版」を公開

2017-09-06　JIPDEC が「(平成 28 年度)「個人情報の取扱いにおける事故報告にみる傾向と注意点」」を公開
2017-09-13　警察庁が「平成 29 年上半期におけるサイバー空間をめぐる脅威の情勢等について」を公開
2017-09-21　フィッシング対策協議会が「SSL サーバー証明書に関する事業者ならびに利用者向けアンケートの調査結果」を公開
2017-09-27　NISC が「政府のサイバーセキュリティに関する予算」を公開

1.2.1.4. 早期警戒情報

JPCERT/CC では、生活や社会経済活動を支えるインフラ、サービスおよびプロダクト等を提供している組織の情報セキュリティ関連部署もしくは組織内 CSIRT に向けて、セキュリティ上の深刻な影響をもたらす可能性のある脅威情報やその分析結果、対策方法に関する情報等を「早期警戒情報」として提供しています。

早期警戒情報の提供について
https://www.jpcert.or.jp/wwinfo/

1.2.1.5. CyberNewsFlash

CyberNewsFlash は、情報収集・分析・情報発信を行っている早期警戒グループのメンバーが、最新のインシデント情報、対策情報、情報の読み方などをタイムリーにお届けする情報です。本四半期に公表した CyberNewsFlash は次のとおりです。

発行件数：4 件　https://www.jpcert.or.jp/newsflash/

2017-07-07　国内からの 22/TCP ポートへのアクセスの増加
2017-08-01　Web サイトへのサイバー攻撃に備えて
2017-09-20　マルウエアが仕込まれた「CCleaner」が配布されていた問題
2017-09-21　Phantom Squad を名乗る攻撃者からの DDoS 攻撃に関する情報

1.2.2. 情報収集・分析・提供（早期警戒活動）事例

本四半期における情報収集・分析・提供（早期警戒活動）の事例を紹介します。

(1) Cisco WebEx Browser Extension の脆弱性 (CVE-2017-6753) に関する情報発信
Cisco WebEx Browser Extension の脆弱性を狙った攻撃に関する注意喚起を 2017 年 7 月 18 日に公開しました。この脆弱性を悪用すると、Cisco WebEx Browser Extension をインストールした Windows PC 上で、遠隔の第三者が任意のコードを実行することができます。脆弱性の報告者からは、脆弱性についての詳細な情報が開示されており、攻撃者が脆弱性を悪用する可能性があったため、JPCERT/CC では注意喚起を発行し、早期の対策を呼びかけました。

(2) 国内からの 22/TCP ポートへのアクセスの増加

国内 IP から 22/TCP ポートへのアクセスの増加が、インターネット定点観測システム（TSUBAME）で観測され、このことについて 2017 年 7 月 7 日に CyberNewsFlash にて記事を公開しました。

22/TCP ポートへの国内からのアクセスの急増は 2017 年 6 月 13 日頃から観測されていますが、国外 IP からのアクセスには増減が見られません。そのことから国内に限った問題に起因する現象だと考えられ、公開した記事では、利用中の PC や危機について不審なソフトウエアやマルウエアがインストールされていないかなど、セキュアな状態が保たれているかを確認することを推奨しています。

1.3. インターネット定点観測

JPCERT/CC では、インターネット上に複数の観測用センサーを分散配置し、不特定多数に向けて発信されるパケットを収集するインターネット定点観測システム「TSUBAME」を構築し、運用しています。TSUBAME から得られる情報を、既に公開されている脆弱性情報やマルウエア、攻撃ツールの情報などと対比して分析することで、攻撃活動や攻撃の準備活動等の把握に努めています。

2007 年以降、TSUBAME の観測用センサーは、海外の National CSIRT 等の協力のもと、国外にも設置しています。JPCERT/CC はセンサーを設置した海外の National CSIRT 等と、国内外の観測データを共同で分析する「TSUBAME プロジェクト」を推進しています。

2017 年 9 月末時点で、海外の 20 の経済地域の 25 組織の協力のもとで観測用センサーが設置されています。さらなるセンサー設置地域の拡大と共同分析の深化を目指して、未参加の海外 National CSIRT 等に対して TSUBAME プロジェクトへの参加を呼びかけています。

TSUBAME プロジェクトの詳細については、次の Web ページをご参照ください。

TSUBAME（インターネット定点観測システム）
https://www.jpcert.or.jp/tsubame/index.html

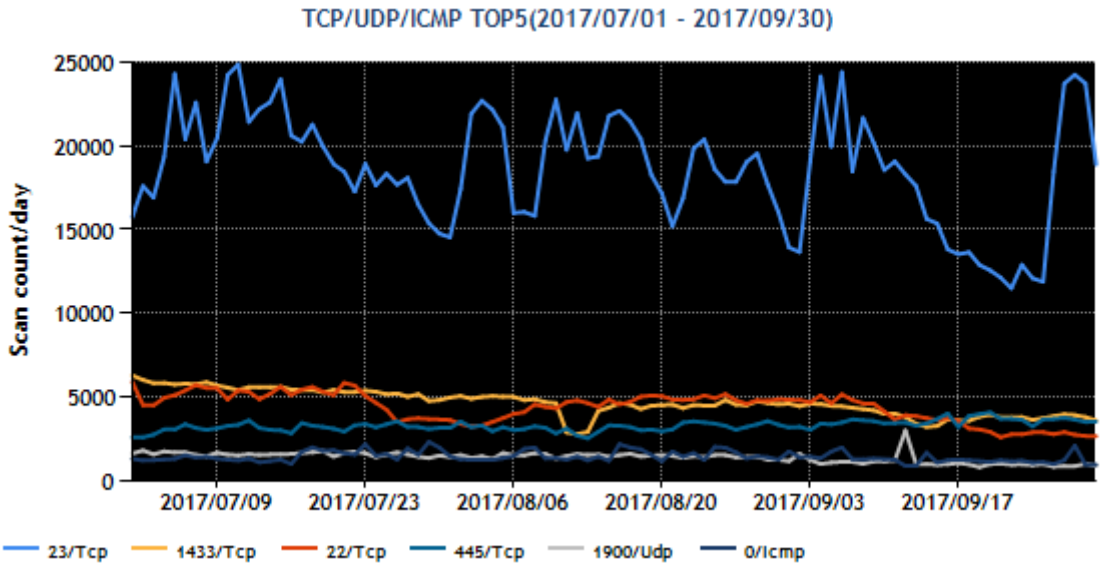
1.3.1. インターネット定点観測システム TSUBAME の観測データの活用

JPCERT/CC では、主に日本企業のシステム管理者の方々に、自組織のネットワークに届くパケットの傾向と比較していただけるよう、日本国内の TSUBAME のセンサーで受信したパケットを宛先ポート別に集計してグラフ化し、毎週月曜日に JPCERT/CC の Web ページで公開しています。また、四半期ごとに観測傾向や注目される現象を紹介する「インターネット定点観測レポート」を公開しており、2017 年 4 月から 6 月分のレポートを 2017 年 8 月 3 日に公開しました。

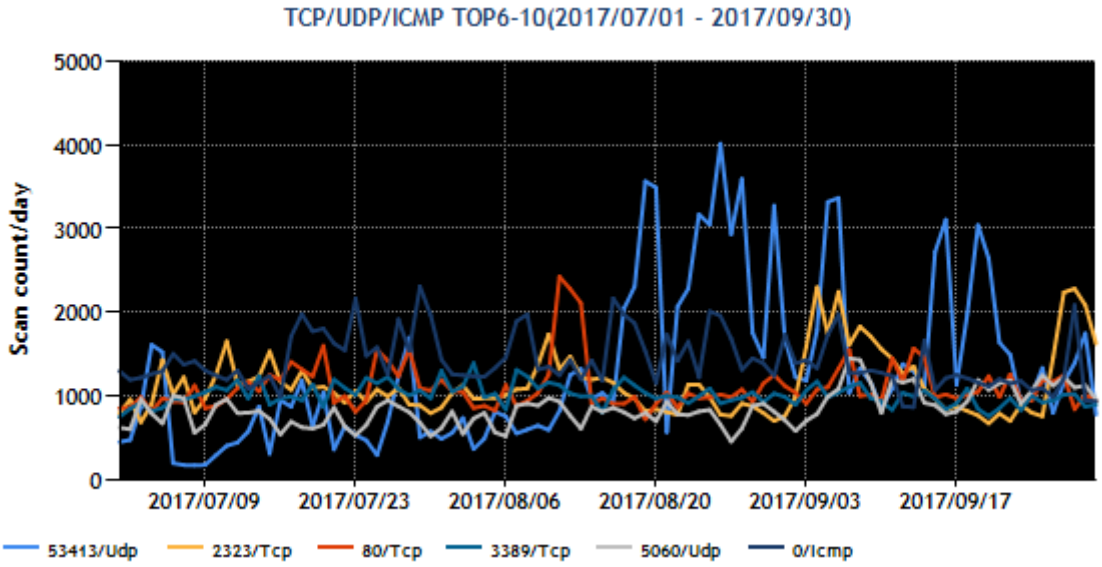
TSUBAME 観測グラフ
https://www.jpcert.or.jp/tsubame/index.html#examples
インターネット定点観測レポート（2017 年 4～6 月）
http://www.jpcert.or.jp/tsubame/report/report201704-06.html

1.3.2. 観測動向

本四半期に TSUBAME で観測された宛先ポート別パケット数の上位 1～5 位および 6～10 位を、［図 1-1］と［図 1-2］に示します。

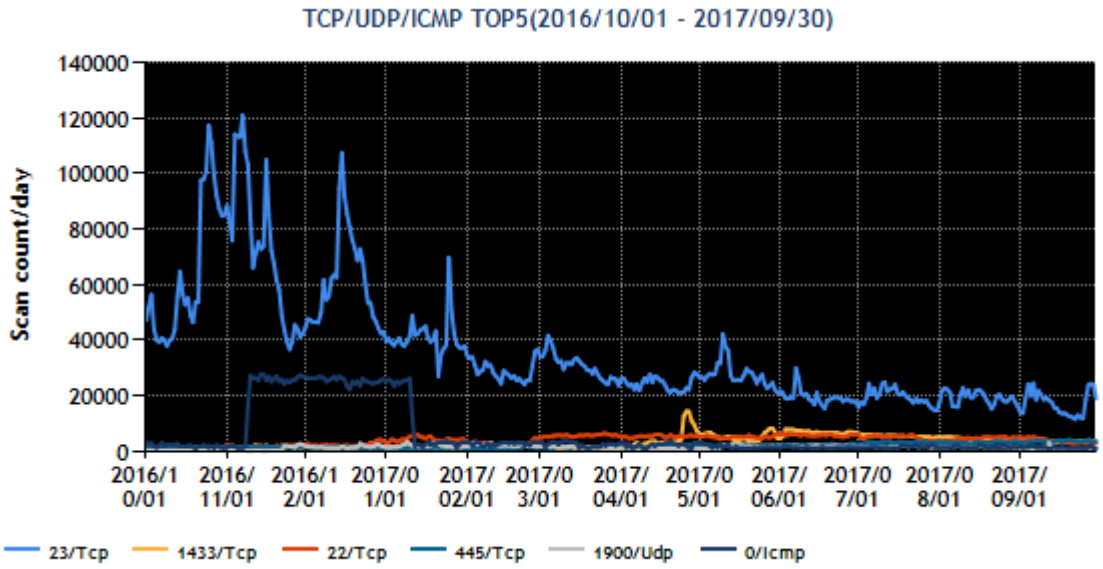


［図 1-1 宛先ポート別グラフ トップ 1-5（2017 年 7 月 1 日-9 月 30 日）］

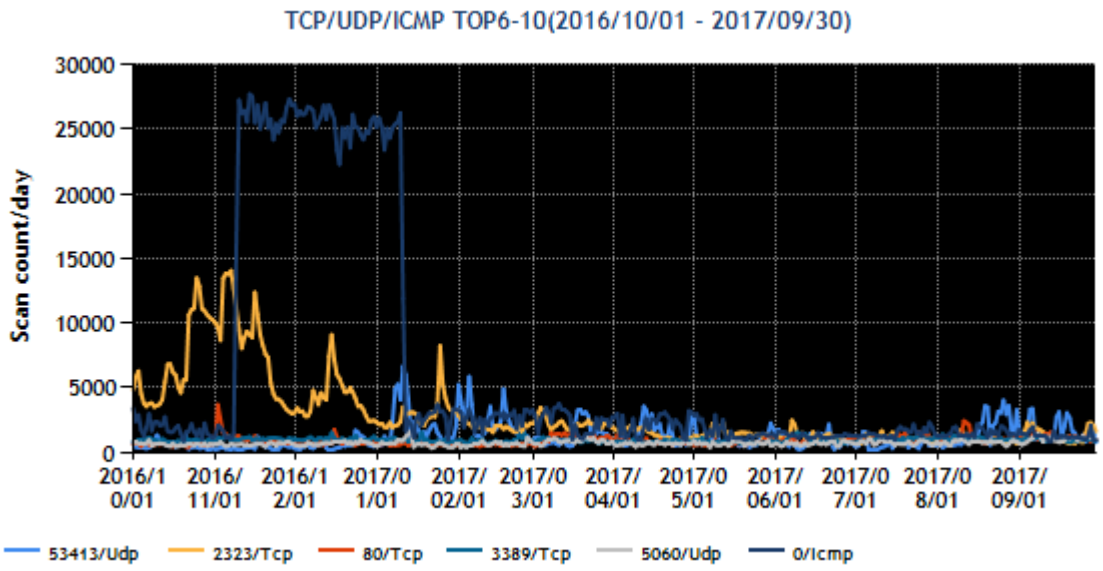


［図 1-2 宛先ポート別グラフ トップ 6-10（2017 年 7 月 1 日-9 月 30 日）］

また、過去 1 年間（2016 年 10 月 1 日-2017 年 9 月 30 日）における、宛先ポート別パケット数の上位 1～5 位および 6～10 位を［図 1-3］と［図 1-4］に示します。



［図 1-3 宛先ポート別グラフ トップ 1-5（2016 年 10 月 1 日-2017 年 9 月 30 日）］



［図 1-4 宛先ポート別グラフ トップ 6-10（2016 年 10 月 1 日-2017 年 9 月 30 日）］

本四半期は、23/TCP や 22/TCP のパケットが多く観測されました。これらのパケットは、調査の結果マルウエア（Mirai 等）に感染した監視カメラやルータ NAS など専用機器から送信されているとみられます。こうしたパケットは以前から観測されていましたが、送信元の機器は変化し続けています。その他、SQLServer をスキャンしていると見られるパケットが多く観測されました。また、WannaCrypt やその亜種に感染した PC から送信されているとみられるパケットも観測しています。

1.3.3. TSUBAME 観測データに基づいたインシデント対応事例

JPCERT/CC では、日々TSUBAME の観測情報を分析し、不審なパケットが見つかった場合に、必要に応じて送信元 IP アドレスの管理者に連絡する等の対処をしています。本四半期における主な対処事例を次に挙げます。

(1) 日本国内を送信元とし Port 22/TCP を宛先とするパケット観測に端を発するインシデント対応
6 月 12 日頃から、TSUBAME において、日本国内の IP アドレスを送信元とし、Port22/TCP を宛先とするパケットが観測され、これらのパケットを送信したホストの割合が一時期は国内の送信元ホスト数の 3 割に達しました。
送信元 IP アドレスに対して連絡を行う等の対応を行いつつ、詳細な調査を進めたところ、国内通信キャリアが販売するルータに脆弱性があることがわかりました。この脆弱性を悪用するマルウエアに感染すると、踏み台として第三者に攻撃パケットが送信される可能性が高いとの結論に達したため、IPA に情報の届出を行い、製品開発者による対策情報とともに 9 月 12 日に JVN で情報が公開されました。
JPCERT/CC では引き続き観測したパケットの分析等を行い、必要に応じて送信元 IP アドレスの管理者へ情報を提供して調査を依頼するなど、感染した機器の発見に努めています。また、ユーザからの問い合わせがあった場合には、問題の原因となっている技術的な内容や正しい設定方法などについて回答しています。

(2) オープンリゾルバとなっていて DDoS 攻撃に使用されうる機器についての対応
本四半期は、前四半期同様、DNS 応答パケットおよび DNS サービスのポートの不達を示す ICMP エラーパケットが多数観測されました。それらのパケットの送信元 IP アドレスのうち国内のものを調査したところ、インターネット側からの DNS のリクエストに応答するオープンリゾルバが見つかりました。観測されたパケットは、DNS 権威サーバに過剰な負荷をかけることを目的とした DDoS 攻撃の余波と推測されます。観測されたパケットの送信元 IP アドレスの管理者等に調査を依頼したところ、「DNS サーバやネットワーク機器の設定が不適切でオープンリゾルバになっていたことを確認し、必要な対応を行った」等の回答を得ています。

2. 脆弱性関連情報流通促進活動

JPCERT/CC は、ソフトウエア製品利用者の安全確保を図ることを目的として、発見された脆弱性情報を適切な範囲に適時に開示して製品開発者による対策を促進し、用意された対策情報と脆弱性情報を脆弱性情報ポータル JVN（Japan Vulnerability Notes ; 独立行政法人情報処理推進機構［IPA］と共同運営）を通じて公表することで広く注意喚起を行う活動を行っています。さらに、脆弱性を作り込まないためのセキュアコーディングの普及や、制御システムの脆弱性の問題にも取り組んでいます。

2.1. 脆弱性関連情報の取り扱い状況

2.1.1. 受付機関である独立行政法人情報処理推進機構（IPA）との連携

JPCERT/CC は、経済産業省告示「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。以下「本規程」）に基づいて製品開発者とのコーディネーションを行う「調整機関」に指定されています。本規程の受付機関に指定されている IPA から届出情報の転送を受け、本規程を踏まえて取りまとめられた「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（以下「パートナーシップガイドライン」）に従って、対象となる脆弱性に関係する製品開発者の特定、脆弱性関連情報の適切な窓口への連絡、開発者による脆弱性の検証等の対応や脆弱性情報の公表スケジュール等に関する調整を行い、原則として、調整した公表日に JVN を通じて脆弱性情報等を一般に公表しています。JPCERT/CC は、脆弱性情報の分析結果や脆弱性情報の取り扱い状況の情報交換を行う等、IPA と緊密な連携を行っています。なお、脆弱性関連情報に関する四半期ごとの届出状況については、次の Web ページをご参照ください。

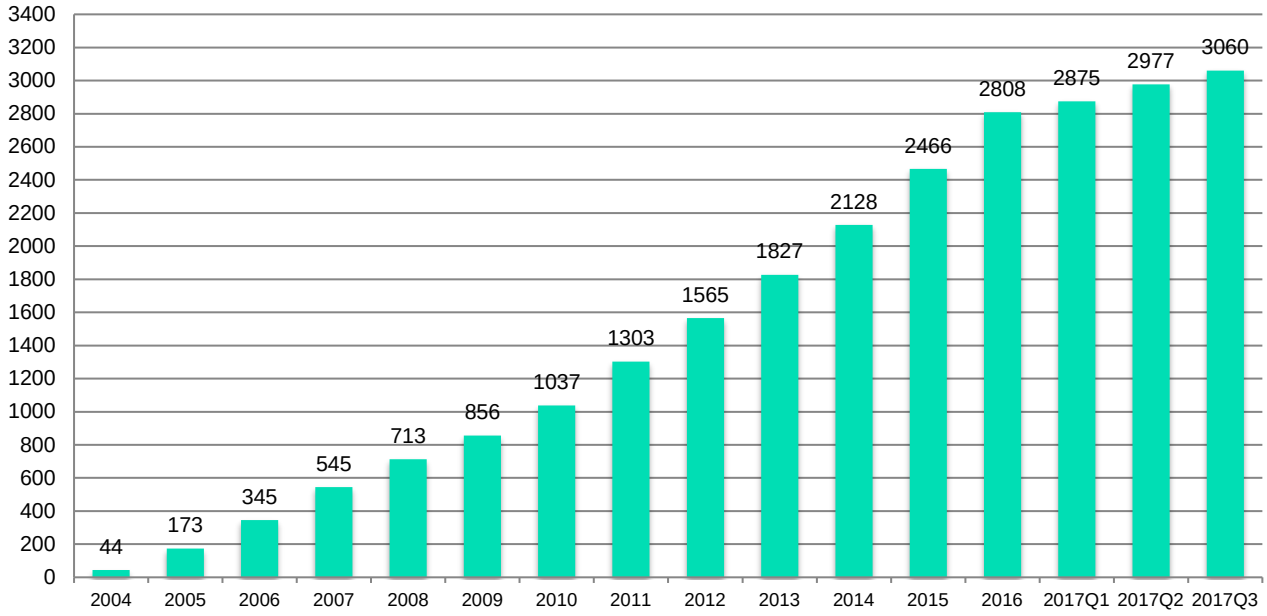
独立行政法人情報処理推進機構（IPA）脆弱性対策
https://www.ipa.go.jp/security/vuln/

2.1.2. Japan Vulnerability Notes（JVN）において公表した脆弱性情報および対応状況

JVN で公表している脆弱性情報は、本規程に従って国内で届け出られた脆弱性に関するもの（以下「国内取扱脆弱性情報」;「JVN#」に続く 8 桁の数字の形式の識別子［例えば、JVN#12345678 等］を付与）と、それ以外の脆弱性に関するもの（以下「国際取扱脆弱性情報」;「JVNVU#」に続く 8 桁の数字の形式の識別子［例えば、JVNVU#12345678 等］を付与）の 2 種類に分類されます。国際取扱脆弱性情報には、CERT/CC や NCSC-FI といった海外の調整機関に届け出られ国際調整が行われた脆弱性情報や海外の製品開発者から JPCERT/CC に直接届け出られた自社製品の脆弱性情報等が含まれます。なお、国際取扱脆弱性情報には、US-CERT からの脆弱性注意喚起の邦訳を含めていますが、これには「JVNTA」に続く 8 桁数字の形式の識別子［例えば、JVNTA#12345678］を使っています。

本四半期に JVN において公表した脆弱性情報は 83 件（累計 3,060 件）で、累計の推移は［図 2-1］に示すとおりです。本四半期に公表された個々の脆弱性情報に関しては、次の Web ページをご参照ください。

JVN(Japan Vulnerability Notes)
https://jvn.jp/



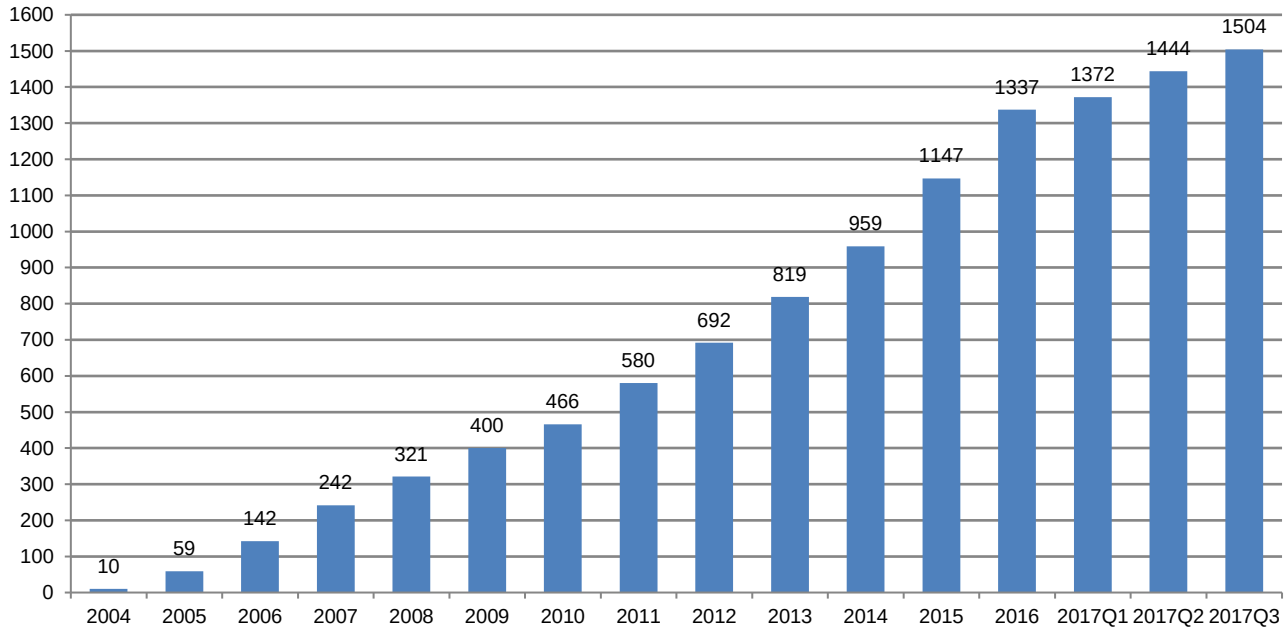
［図 2-1 JVN 公表累積件数］

本四半期において公表に至った脆弱性情報のうち、国内取扱脆弱性情報は 60 件（累計 1,504 件）で、累計の推移は［図 2-2］に示すとおりです。60 件のうち、50 件が国内製品開発者の製品、10 件が海外の製品開発者の製品でした。なお、本四半期においては、国内外の複数の製品開発者の製品に関連した脆弱性情報の公表はありませんでした。また、50 件の国内製品開発者の製品のうち、3 件が自社製品届出による脆弱性情報でした。

本四半期に公表した脆弱性の影響を受けた製品のカテゴリの内訳は、［表 2-1］のとおりでした。本四半期は前四半期同様に、Windows アプリケーションが 34 件と非常に多く、次いで無線 LAN ルータやネットワークカメラ等の組込み系製品が 15 件でした。Windows アプリケーションに関する公表は、前四半期から多く、2010 年に公表された「Windows アプリケーションにおける任意の DLL 読込みの脆弱性」と同じ機序で起こる Windows アプリケーションの脆弱性が多数みられました。また、行政機関が提供する Windows アプリケーションで見つかった脆弱性は、前四半期に続き本四半期も数多く公表されました。これは、特定の方が、さまざまな行政機関のソフトウエアについて脆弱性を探索し届け出られたことによるものです。

［表 2-1 公表を行った国内取扱脆弱性情報の件数の製品カテゴリ内訳］

製品分類	件数
Windows アプリケーション	34
組込系	15
プラグイン	5
グループウエア	2
ウェブアプリケーション	1
検索エンジン	1
スマホアプリ	1
CMS	1



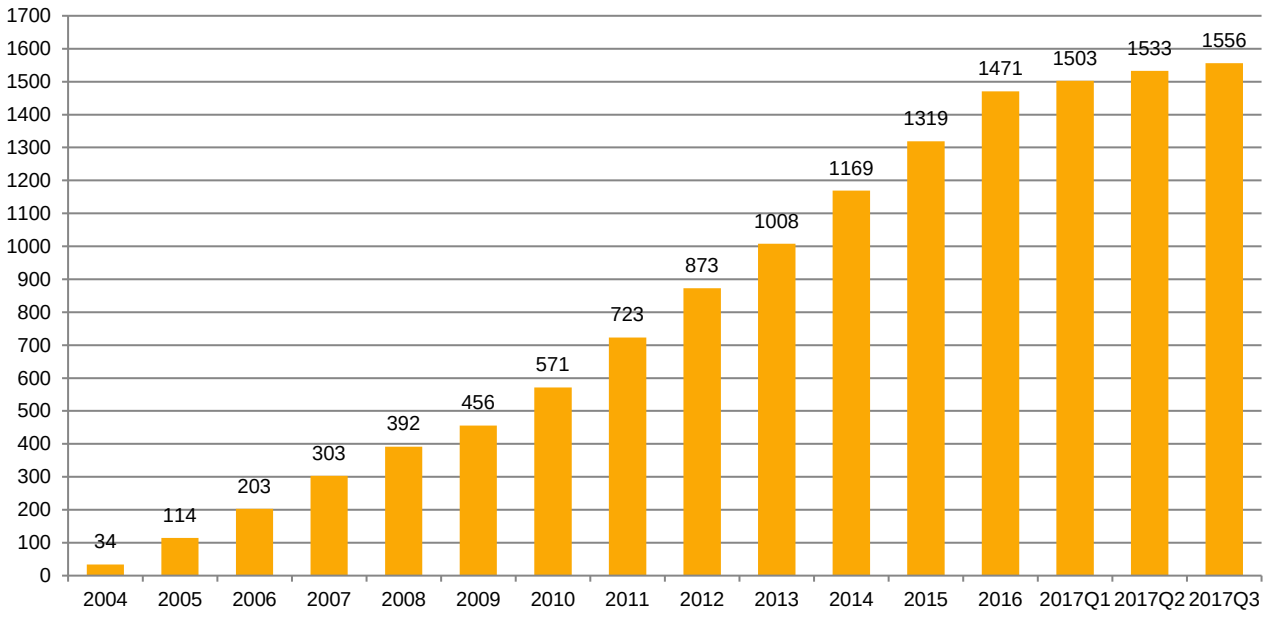
［図 2-2 公表を行った国内取扱脆弱性情報の累積件数］

本四半期に公表した国際取扱脆弱性情報は 23 件（累計 1,556 件）で、累計の推移は［図 2-3］に示すとおりです。

本四半期に公表した脆弱性の影響を受けた製品のカテゴリ内訳は、［表 2-2］のとおりでした。2016 年以降、多くの組込系製品に関する脆弱性情報を公表しており、本四半期においても 5 件のルータ機器等を含む組込系製品の脆弱性情報を公表しました。なお、本四半期には、ライブラリやウェブアプリケーションフレームワーク、ウェブサーブレットコンテナ、アプリケーションフレームワークといった製品開発に使用されるソフトウエアの脆弱性の公表が合計 8 件と比較的多く、このうち 3 件は、海外製品開発者自身による自社製品に関する脆弱性情報の公表依頼に基づくものでした。
国内製品開発者と同様に、海外製品開発者からも、自社製品の脆弱性情報が事前に JPCERT/CC に通知される事例が徐々に増えており、23 件中 5 件がこれに該当する公表事案でした。

［表 2-2 公表を行った国際取扱脆弱性情報の件数の製品カテゴリ内訳］

製品分類	件数
組込系	5
macOS アプリ	3
ライブラリ	3
ウェブアプリケーションフレームワーク	2
ウェブサーブレットコンテナ	2
その他(プロトコル実装)	2
Windows OS	1
Windows アプリケーション	1
アプリケーションフレームワーク	1
アンチウィルス製品	1
サーバ製品	1
マルチプラットフォームアプリケーション	1



［図 2-3 国際取扱脆弱性情報の公表累積件数］

2.1.3. 連絡不能開発者とそれに対する対応の状況等

本規程に基づいて報告された脆弱性について、製品開発者と連絡が取れない場合には、2011 年度以降、当該製品開発者名を JVN 上で「連絡不能開発者一覧」として公表し、連絡の手掛かりを広く求めています。これまでに 251 件（製品開発者数で 164 件）を公表し、45 件（製品開発者数で 27 件）の調整を再開することができ、脆弱性関連情報の取り扱いにおける「滞留」の解消に一定の効果を上げています。

本四半期に連絡不能開発者一覧に新たに掲載した案件はありませんでした。本四半期末日時点で、合計

206 件の連絡不能開発者案件を掲載しており、継続して製品開発者や関係者からの連絡および情報提供を呼びかけています。

こうした呼びかけによっても製品開発者と連絡が取れないケースの取り扱いについて、本規準およびパートナーシップガイドラインが 2014 年 5 月に改正され、利用者保護の観点から脆弱性情報を公表する手続きが定められました。この規定に従って、2014 年 11 月より公表判定委員会が定期的に開催されており、その審議により、これまでに 2 案件を公表し、その他に公表すべきと判定されている 5 案件の公表準備を進めています。 なお、2017 年度の公表判定委員会は、12 月に開催が予定されています。

2.1.4. 海外 CSIRT との脆弱性情報流通協力体制の構築、国際的な活動

JPCERT/CC は、脆弱性情報の円滑な国際的流通のための脆弱性情報ハンドリングを行っている米国の CERT/CC、英国の NCSC、フィンランドの CERT-FI、オランダの NCSC-NL などの海外の調整機関と協力関係を結び連携して、それぞれが報告を受けた脆弱性情報の共有、各国の製品開発者への通知および対応状況の集約、脆弱性情報の公表時期の設定等の調整活動を行っています。さらに Android 関連製品や OSS 製品の脆弱性の増加に伴い、それらの製品開発者が存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 との連携も増えており、国際連携活動の幅が一層広がっています。また、米国の ICS-CERT との連携を 2013 年末に正式に開始し、本四半期までに合計 13 件の制御システム用製品の脆弱性情報を公表しており、新たな分野での国際的活動が定着したと言えます。

JPCERT/CC は、日本における脆弱性ハンドリングのコンタクトポイントとして、脆弱性情報ハンドリングにおける国際的活動を引き続き推進してまいります。

JVN 英語版サイト（https://jvn.jp/en）上の脆弱性情報も、日本語版とほぼ同時に公表しており、脆弱性情報の信頼できるソースとして、海外のセキュリティ関連組織等からも注目されています。

また、JPCERT/CC は、CNA（CVE Numbering Authorities）として認定されています。JPCERT/CC は、本四半期に JVN で公表したもののうち、国内で届出られた脆弱性情報に 89 個の CVE 番号を付与しました。2008 年以降においては、MITRE やその他の組織への確認や照合を必要とする特殊なケース（全体の 1 割弱）を除いて、JVN 上で公表する脆弱性のほぼすべてに CVE 番号が付与されています。

CNA および CVE に関する詳細は、次の Web ページをご参照ください。

News & Events “JPCERT/CC Becomes CVE Numbering Authority”
https://cve.mitre.org/news/archives/2010_news.html#jun232010a

CVE Numbering Authorities
https://cve.mitre.org/cve/cna.html

About CVE

https://cve.mitre.org/about/index.html

2.2. 日本国内の脆弱性情報流通体制の整備

JPCERT/CC では、本規程に従って、日本国内の脆弱性情報流通体制を整備しています。
詳細については、次の Web ページをご参照ください。

脆弱性情報取扱体制

http://www.meti.go.jp/policy/netsecurity/vulhandlingG.html

脆弱性情報コーディネーション概要

https://www.jpcert.or.jp/vh/

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（2017 年版）

https://www.jpcert.or.jp/vh/partnership_guideline2017.pdf

JPCERT/CC 脆弱性情報取扱いガイドライン（2017 年版）

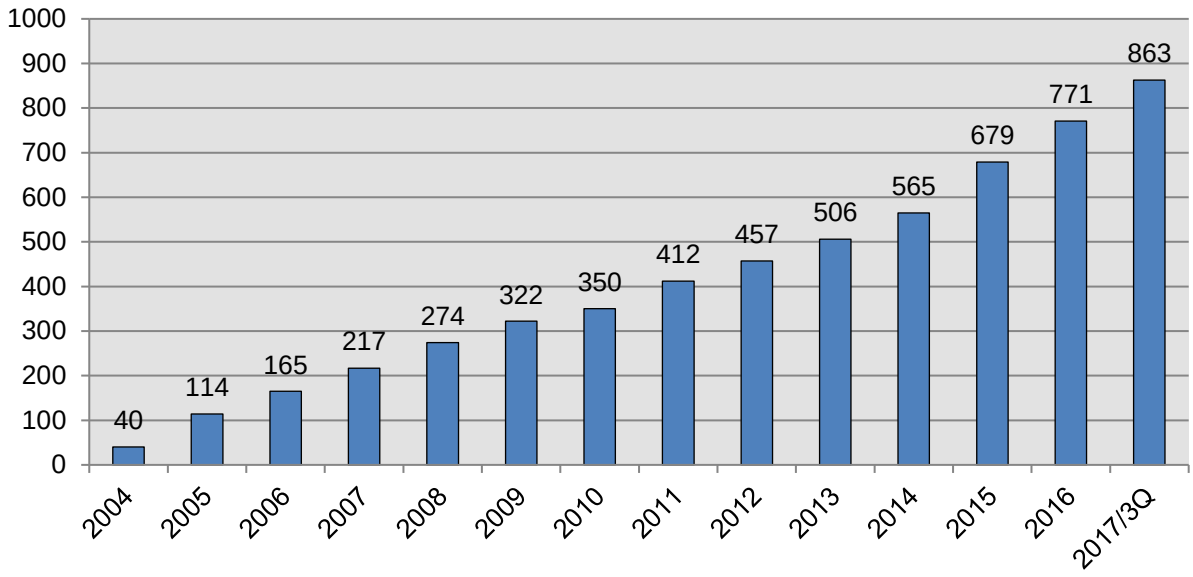
http://www.jpcert.or.jp/vh/vul-guideline2017.pdf

2.2.1. 日本国内製品開発者との連携

本規程では、脆弱性情報を提供する先となる製品開発者のリストを作成し、各製品開発者の連絡先情報を整備することが、調整機関である JPCERT/CC に求められています。JPCERT/CC では、製品開発者の皆さまに製品開発者リストへの登録をお願いしています。製品開発者の登録数は、[図 2-4] に示すとおり、2017 年 9 月 30 日現在で 863 となっています。
登録等の詳細については、次の Web ページをご参照ください。

製品開発者登録

http://www.jpcert.or.jp/vh/regist.html



［図 2-4 累計製品開発者登録数］

2.2.2. 脆弱性情報流通体制の普及啓発

オープンソースソフトウエアの作成と普及に係る開発者や企業などへ、日本国内の脆弱性情報流通体制の認知向上を図り、2017 年 8 月 4 日から 5 日にかけて開催された OpenSource Conference 2017 Kyoto へ参加しました。脆弱性情報ハンドリング業務内容と活動状況、セキュアコーディング、その他の JPCERT/CC の活動内容について紹介し、オープンソースソフトウエア分野における脆弱性対応等について出展コミュニティや一般来場者との意見交換、情報交換を行いました。

2.3. 脆弱性の低減方策の研究・開発および普及啓発

2.3.1. 講演活動

情報流通対策グループでは、脆弱なソフトウエアの解析等を通じて得られた脆弱性やその対策方法に関する知見を、広く一般のソフトウエア開発者の方々に伝えるための活動を行っています。

本四半期は、次の 3 件の講演を行いました。

講演日時: 7 月 23 日
講演タイトル: WordPress とバックアップの話
イベント名: WordBench 東京 7 月勉強会「夏の LT 大会！」

多くのサイトでデータベースのバックアップが外部からアクセス可能な場所に保存されていることを発見した、という最近のニュースを題材に、データバックアップ機能を提供する WordPress プラグインの使い方について注意するべきことを紹介しました。

講演日時: 8 月 5 日
講演タイトル: DLL 読み込みの問題を読み解く
イベント名: オープンソースカンファレンス 2017 Kyoto

Windows アプリケーションに潜む DLL 読み込みに関する脆弱性について、その仕組みと検証方法、ユーザにどんな影響があるのか、ユーザやソフトウエア開発者がとるべき対策について解説しました。

講演日時: 9 月 16 日
講演タイトル: 安全なプラグインに必要なこと: 脆弱性届出状況に見る傾向と対策
イベント名: WordCamp Tokyo 2017

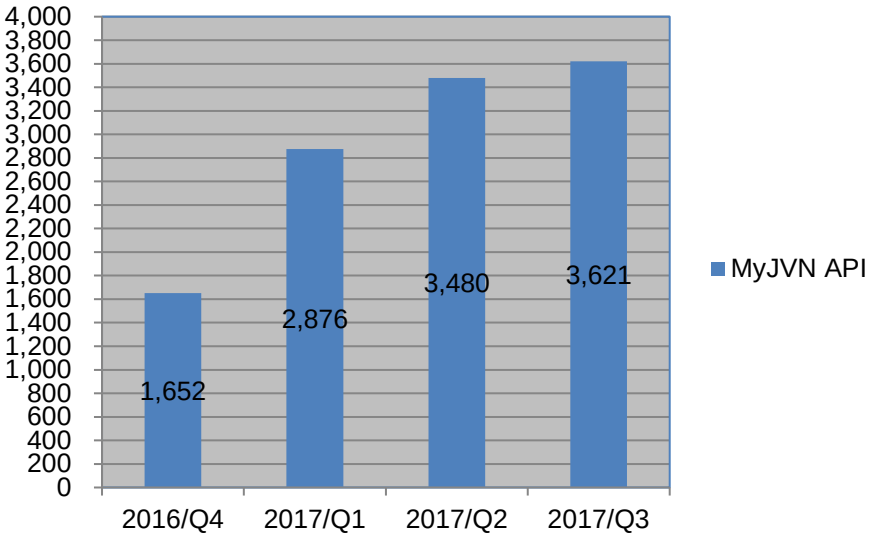
Wordpress プラグインに関する届出の状況を紹介するとともに、プラグイン開発者向けおよびサイト運営者向けに、JPCERT/CC が考えるベストプラクティスを提案し、コミュニティ内で議論を行いました。

2.4. VRDA フィードによる脆弱性情報の配信

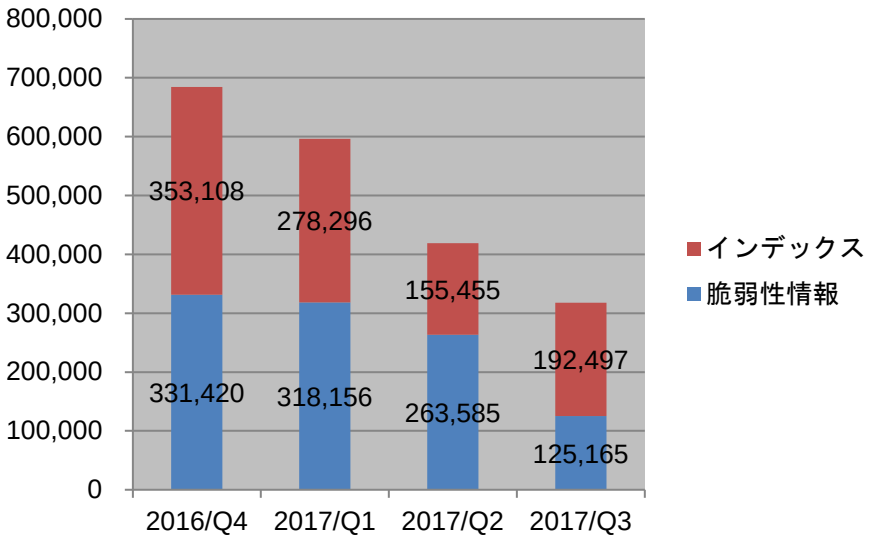
JPCERT/CC は、大規模組織の組織内 CSIRT 等での利用を想定して、KENGINE 等のツールを用いた体系的な脆弱性対応を可能とするため、IPA が運用する MyJVN API を外部データソースとして利用した、VRDA（Vulnerability Response Decision Assistance）フィードによる脆弱性情報の配信を行っています。VRDA フィードについての詳しい情報は、次の Web ページを参照ください。

VRDA フィード 脆弱性脅威分析用情報の定型データ配信
https://www.jpcert.or.jp/vrdafeed/index.html

四半期ごとに配信した VRDA フィード配信件数を［図 2-5］に、VRDA フィードの利用傾向を［図 2-6］と［図 2-7］に示します。［図 2-7］では、VRDA フィードインデックス（Atom フィード）と、脆弱性情報（脆弱性の詳細情報）の利用数を示します。VRDA フィードインデックスは、個別の脆弱性情報のタイトルと脆弱性の影響を受ける製品の識別子（CPE）を含みます。［図 2-7］では、HTML と XML の 2 つのデータ形式で提供している脆弱性情報について、データ形式別の利用割合を示しています。

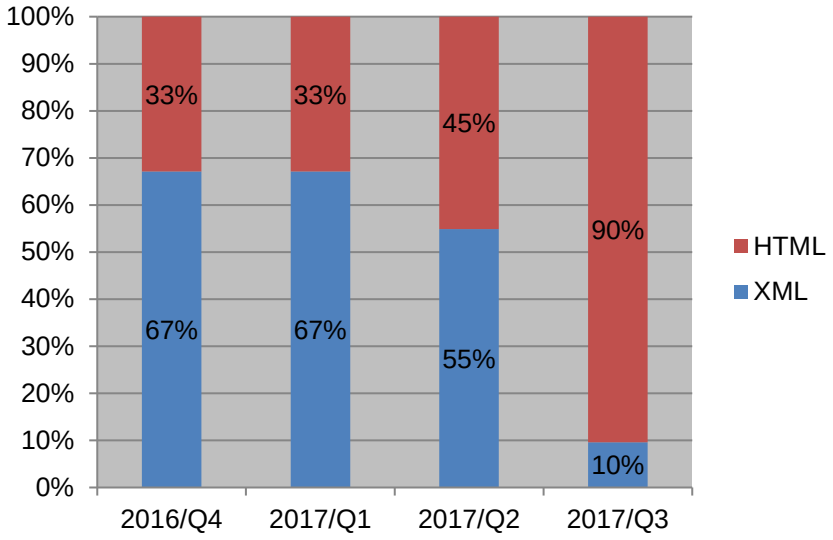


［図 2-5 VRDA フィード配信件数］



［図 2-6 VRDA フィード利用件数］

インデックスの利用数については、［図 2-6］に示したように、前四半期と比較し、約 24%減少しました。脆弱性情報の利用数についても、約 53%減少しました。



［図 2-7 脆弱性情報のデータ形式別利用割合］

脆弱性情報のデータ形式別利用傾向については、［図 2-7］に示したように、前四半期と比較し、XML 形式の割合が 45%減少しました。

3. 制御システムセキュリティ強化に向けた活動

3.1 情報収集分析

JPCERT/CC では、制御システムにおけるセキュリティインシデントに関わる事例や標準化活動の動向、その他セキュリティ技術動向に関するニュースや情報等を収集・分析し、必要に応じて国内組織等に情報提供を行っています。本四半期に収集・分析した情報は 455 件でした。このうち、国内の制御システム関係者に影響があり、注目しておくべき事案を「参考情報」として、制御システムセキュリティ情報共有コミュニティ（注 1）に提供しました。

（注 1）JPCERT/CC が運営するコミュニティで、制御システム関係者を中心に構成されています

本四半期に提供した参考情報は 9 件でした。

2017/07/07 【参考情報】米原子力に対するサイバー攻撃の件について
2017/07/24 【参考情報】海外の水道分野に対するサイバー攻撃の件について
2017/08/07 【参考情報】ニュージャージー州の原子力発電所へのハッキングの懸念について
2017/08/07 【参考情報】アイルランドの電力事業者へのサイバー攻撃について
2017/08/15 【参考情報】米 AW North Carolina 自動車部品工場におけるサイバー攻撃について
2017/08/15 【参考情報】ウクライナ郵便事業者の配送システムにおけるサイバー攻撃ついて
2017/08/15 【参考情報】太陽光発電システムの脆弱性について
2017/08/30 【参考情報】物流事業者における NotPetya サイバー攻撃の業績影響について
2017/09/07 【参考情報】エネルギー業界を標的にした Dragonfly による攻撃キャンペーンについて

また、海外での事例や、標準化動向などを JPCERT/CC からのお知らせとともに、制御システムセキュリティ情報共有コミュニティに登録いただいている関係者向けに月刊ニュースレターとして配信しています。本四半期は計 3 件を配信しました。

2017/07/06　制御システムセキュリティニュースレター 2017-0006
2017/08/07　制御システムセキュリティニュースレター 2017-0007
2017/09/05　制御システムセキュリティニュースレター 2017-0008

制御システムセキュリティ情報共有コミュニティには、制御システムセキュリティ情報提供用メーリングリストと制御システムセキュリティ情報共有ポータルサイト ConPaS があり、メーリングリストには現在 728 名の方にご登録いただいています。今期は、メーリングリスト利用登録の受付処理を自動化し、登録処理の迅速化をはかりました。あわせて、各サービス内容の充実を図り、さらなる利用を促進していく予定です。参加資格や申込み方法については、次の Web ページをご参照ください。

制御システムセキュリティ情報共有コミュニティ
https://www.jpcert.or.jp/ics/ics-community.html

3.2 制御システム関連のインシデント対応

本四半期における制御システムに関連するインシデントの報告件数は 0 件（0 IP アドレス）でした。
また、JPCERT/CC では SHODAN をはじめとするインターネット・ノード検索システム等のインターネット上の公開情報を分析し、外部から不正にアクセスされる危険性のある制御システム等を保有する国内の組織に対して情報を提供しています。
本四半期は、後者に関して 9 件の情報を提供しました。

3.3 関連団体との連携

SICE（計測自動制御学会）と JEITA（電子情報技術産業協会）、JEMIMA（日本電気計測器工業会）が定期的に開催している合同セキュリティ検討ワーキンググループに参加し、制御システムのセキュリティに関して専門家の方々と意見交換を行いました。

3.4 制御システム向けセキュリティ自己評価ツールの提供

JPCERT/CC では、制御システムの構築と運用に関するセキュリティ上の問題項目を抽出し、バランスの良いセキュリティ対策を行っていただくことを目的として、簡便なセキュリティ自己評価ツールである日本版 SSAT（SCADA Self Assessment Tool、申込み制）や J-CLICS（制御システムセキュリティ自己評価ツール、フリーダウンロード）を提供しています。本四半期は、日本版 SSAT に関して 5 件の利用申し込みがあり、直接配付件数の累計は、日本版 SSAT が 242 件となりました。

日本版 SSAT(SCADA Self Assessment Tool)
https://www.jpcert.or.jp/ics/ssat.html

制御システムセキュリティ自己評価ツール(J-CLICS)
https://www.jpcert.or.jp/ics/jclics.html

3.5 SICE Annual Conference および国際シンポジウムでの発表

JPCERT/CC では、制御システムネットワークやそこに接続された機器へのサイバー攻撃を検知・分析するため、制御システム向けにカスタマイズしたハニーポットに関する研究を行っています。その中間報告を論文にまとめて、9 月 20 日に開催された SICE Annual Conference で講演しました。講演では、制御システムにおいて想定されるサイバー攻撃の流れを説明し、同一ネットワークに存在する制御機器のプロファイルをハニーポットで模倣することにより攻撃者からのアクセスを誘導し、検知するための手法と、通信元(感染源)のプロファイルを目的としたカウンタースキャンを行うための手法について紹介しました。聴衆からは、制御システム特有のプロトコルのエミュレートや情報収集と共有に関して質問やコメントがありました。
また、併催された国際シンポジウムにおいては、「Safety with Security」と題したパネルディスカッションにパネラーとして参加し、制御システムに関する最近の脅威事例を紹介しました。制御システムは、インターネットに直結して運用していないとしても、社内ネットワーク上の他のシステムとデータをやり取りしている場合があり、他のネットワークとの接続点のセキュリティの確保が重要であると指摘しました。

4. 国際連携活動関連

4.1. 海外 CSIRT 構築支援および運用支援活動

海外の National CSIRT（Computer Security Incident Response Team）等のインシデント対応調整能力の向上を図るため、研修やイベントでの講演等を通じた CSIRT の構築・運用支援等を行っています。
本四半期は以下のとおり研修を行うとともに、新規の研修教材の開発を進めました。

4.1.1. ASEAN 政策担当者向けサイバーセキュリティ研修（7 月 13 日-14 日）

日本と ASEAN のサイバーセキュリティ政策担当者を集めて 7 月 13 日から 14 日にかけて東京で開催された The 3rd ASEAN-JAPAN Information Security Joint Working Group Meeting の機会を利用して、14 日午後、ASEAN のサイバーセキュリティ政策担当者約 20 名に向けて研修を行いました。
研修は「サイバー空間における規範と CSIRT の役割」と「TSUBAME で観測された WannaCry の状況」の 2 つのセッションで構成され、前者においては、サイバー空間における規範づくりや信頼醸成措置(CBM)の議論の現状を紹介するとともに、これらの議論が将来的にどう CSIRT に影響を与えるかを受講生とともに考察しました。後者においては、5 月に世界的な感染が確認されたランサムウエア WannaCry が、アジア・太平洋地域等を対象としたインターネット定点観測システム TSUBAME においてどのように見えたのかを、デモを交えて紹介しました。

4.2. 国際 CSIRT 間連携

国境をまたぐインシデントへのスムーズな対応等を目的に、JPCERT/CC は海外 CSIRT との連携強化を進めています。また、APCERT（4.2.1.参照）や FIRST（4.2.2.参照）で主導的な役割を担う等、多国間の CSIRT 連携の枠組みにも積極的に参加しています。

4.2.1. APCERT（Asia Pacific Computer Emergency Response Team）

JPCERT/CC は、2003 年 2 月の APCERT 発足時から継続して Steering Committee（運営委員会）のメンバーに選出されており、事務局も担当しています。APCERT の詳細および APCERT における JPCERT/CC の役割については、次の Web ページをご参照ください。

JPCERT/CC within APCERT
https://www.jpcert.or.jp/english/apcert/

4.2.1.1. APCERT Steering Committee 会議の実施

Steering Committee は 7 月 18 日と 9 月 13 日に電話会議を行い、今後の APCERT の運営方針等について議論しました。JPCERT/CC は Steering Committee メンバーとしてこれらの会議に参加すると同時に、事務局として会議運営をサポートしました。

4.2.1.2. CERT-In との APCERT 年次会合 2017 打ち合わせ（8 月 16 日）

JPCERT/CC は、APCERT 事務局として 8 月 16 日にデリー（インド）にある CERT-In のオフィスを往訪し、11 月に同市にて CERT-In が主催する APCERT 年次会合 2017 に向けた事前打ち合わせを行いました。

4.2.2. FIRST（Forum of Incident Response and Security Teams）

JPCERT/CC は、1998 年の加盟以来、FIRST の活動に積極的に参加しています。現在は JPCERT/CC の国際部シニアアナリスト 小宮山功一朗が FIRST の理事を務めており、四半期に一度開催されるシンポジウムの準備調整を主に担当しています。FIRST と理事の詳細については、次の Web ページをご参照ください。

FIRST
https://www.first.org/

FIRST.Org, Inc., Board of Directors
https://www.first.org/about/organization/directors

4.2.2.1. FIRST Regional Symposium for Asia-Pacific 参加（9 月 9 日-11 日）

9 月 9 日から 11 日にかけて台中（台湾）にて、FIRST が主催する FIRST Regional Symposium for Asia-Pacific が開催されました。JPCERT/CC 小宮山は FIRST 理事として、本イベントの企画・運営に携わりました。11 日に開催されたシンポジウムでは主に台湾の CSIRT スタッフや研究者による高度サイバー攻撃に関する知見の共有が行われました。また、それに先立って 9 日から 10 日にかけて JPCERT/CC 職員 2 名が講師となって、ネットワークフォレンジック研修を実施しました。

［図 4-1 研修の模様］

本イベントの詳細については、次の Web ページをご参照ください。

FIRST Regional Symposium for Asia-Pacific
https://www.first.org/events/symposium/taichung2017/program

4.2.3. 第 12 回 ASEAN CERTs Incident Drill（ACID）参加（9 月 11 日）

シンガポールの National CSIRT である SingCERT が主導し、ASEAN（東南アジア諸国連合）各国の CSIRT が合同で実施するサイバーインシデント演習である ACID（ASEAN CERTs Incident Drill）が 9 月 11 日に実施され、JPCERT/CC も参加しました。本演習は、国境を越えて発生するサイバーセキュリティインシデントに備え、ASEAN 加盟国および周辺各国の CSIRT 間の連携の強化を目的に毎年実施されており、今回で 12 回目になります。今年の演習は「不十分な権限設定とアクセスコントロールの危険性」をテーマに行われました。

4.2.4. 国際 CSIRT 間連携に係る国内外カンファレンス等への参加

4.2.4.1. PacNOG20（7 月 3 日-7 日）

スバ（フィジー）で開催された第 20 回 The Pacific Network Operators Group（PacNOG）会合（通称 PacNog20）の Network Security Workshop 等のイベントに参加し、フィジーやバヌアツなどの南太平洋地域におけるインターネット接続サービスの現状やセキュリティへの取り組み状況についての知見を得ました。また、この会合の機会を捉え、南太平洋地域の National CSIRT の構築状況等に関するヒアリングを行いました。ヒアリング結果は今後の CSIRT 構築支援活動に活かす予定です。PacNog20 については次の Web ページをご参照ください。

PacNog20
https://www.pacnog.org/pacnog20/

4.2.4.2. 2017 APISC Security Training Course 参加（7 月 31 日-8 月 4 日）

韓国のソウルにおいて開催された 2017 APISC Security Training Course に参加しました。本研修は、CSIRT オペレーション等に関する知識の習得を目的として韓国の Korea Internet & Security Agency（KISA）および KrCERT/CC が主催したもので、アジアだけでなく、ヨーロッパ、中米、アフリカ地域の情報セキュリティ関係者が受講生として招かれました。JPCERT/CC も、日本のインターネットセキュリティへの取り組み状況等についての発表を行うとともに、受講生として CSIRT 構築・機能強化やインシデント対応のあり方などについての議論に参加しました。

4.2.4.3. 第五回 日中韓 サイバーセキュリティインシデント対応年次会合（9 月 6 日-7 日）

日中韓の National CSIRT（JPCERT/CC、CNCERT/CC、KrCERT/CC）による「日中韓 サイバーセキュリティインシデント対応年次会合」が 9 月 6 日から 9 月 7 日にかけてソウルで開催されました。本会合は、2011 年 12 月に三者が締結した覚書（MOU）に基づき毎年開催されています。
本会合では、前回の会合以降の、日中韓に影響を及ぼす重大なサイバーセキュリティインシデントにおける National CSIRT 間の連携実績を振り返るとともに、対応した主要なインシデントや各種取り組み等を各 CSIRT が報告しました。また、昨年度に引き続き、脆弱性コーディネーションにおける連携を進めるため、この分野における各 CSIRT の持つ役割や権限等について詳細に確認するなどしました。

4.3. CyberGreen

国際的なプロジェクトである CyberGreen は、インターネット全体の健全性とリスクを評価する指標を用いて各国／地域間で比較を行い、各国の CSIRT や ISP、セキュリティベンダーといった技術パートナーが、それぞれの担当領域の指標値を向上させる施策に努めることを通じて、より効率的に健全なサイバー空間を実現することを目的としています。2015 年 11 月に設立された日本発の国際 NPO である CyberGreen Institute がプロジェクトの中心を担っています。本四半期、JPCERT/CC は、CyberGreen Institute が収集したデータの今後の商用利用を見据え、データの検索条件や抽出方法の改善などデータを

利用する立場から提案を行いました。

CyberGreen Institute については、次の Web ページをご参照ください。
https://www.cybergreen.net/

4.4. ブログや Twitter を通した情報発信

英語ブログ（http://blog.jpcert.or.jp/）や Twitter（@jpcert_en）を通して、日本やアジア太平洋地域の情報セキュリティに関する状況や JPCERT/CC の活動等について英文による情報発信を継続して行っています。本四半期は次の記事をブログに掲載しました。

Clustering Malware Variants Using “impfuzzy for Neo4j” （7 月 5 日）
http://blog.jpcert.or.jp/2017/07/clustering-malw-5a14.html

What the Avalanche Botnet Takedown Revealed: Banking Trojan Infection in Japan（8 月 4 日）
http://blog.jpcert.or.jp/2017/08/what-the-avalanche-botnet-takedown-revealed-banking-trojan-infection-in-japan.html

Detecting Datper Malware from Proxy Logs（8 月 21 日）
http://blog.jpcert.or.jp/2017/08/detecting-datper-malware-from-proxy-logs.html

Chase up Datper’s Communication Logs with Splunk/Elastic Stack（9 月 27 日）
http://blog.jpcert.or.jp/2017/09/chase-up-datper-bba7.html

5. 日本シーサート協議会（NCA）事務局運営

5.1. 概況

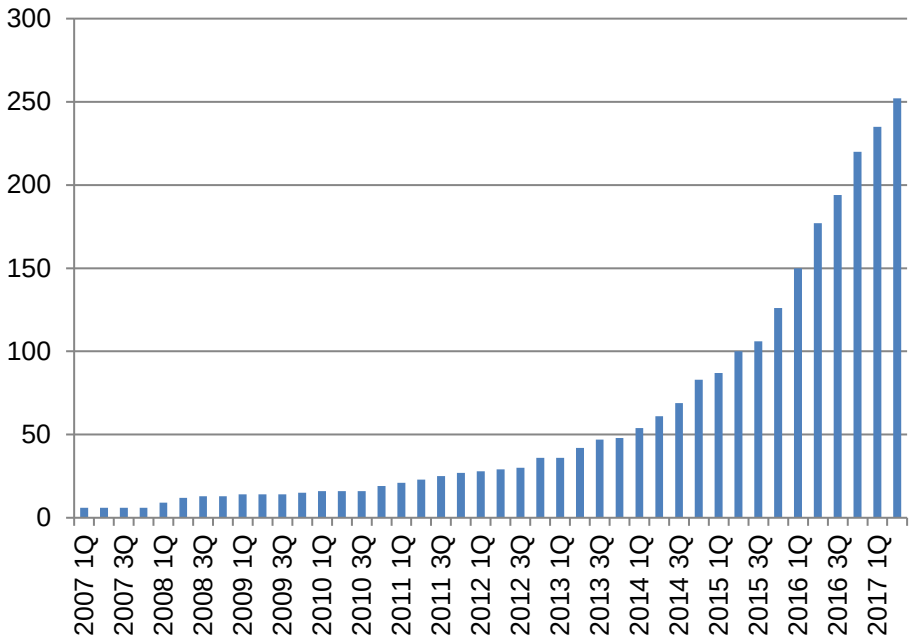
日本シーサート協議会（NCA：Nippon CSIRT Association）は、国内のシーサート（CSIRT：Computer Security Incident Response Team）組織が互いに協調し、連携して共通の問題を解決する場として設立されました。その事務局として、JPCERT/CC は、NCA の Web サイトの管理や更新を通じた広報活動、協議会の問い合わせ窓口やメーリングリストを含む会員情報の管理、加盟のためのガイダンスの実施および手続きの運用を担当するとともに、自らも会員として協議会の活動に参加しています。

本四半期には、次の 18 組織（括弧内はシーサート名称）が新規に NCA に加盟しました。

株式会社パソナグループ (Pasona-CSIRT)
大塚製薬株式会社 (Otsuka-CSIRT)
日東電工株式会社 (Nitto-CSIRT)
株式会社アイネス (INES-SIRT)

株式会社 富士通エフサス (FSAS-CSIRT)
アステラス製薬株式会社 (Astellas-CSIRT)
学校法人 工学院大学 (KU-CSIRT)
アーバーネットワークス株式会社 (ASERT Japan)
YKK 株式会社 (YKK-CSIRT)
富士電機　株式会社 (Fe-CSIRT)
西日本旅客鉄道株式会社 (JRW-CSIRT)
株式会社　コンシスト (Con-SIRT)
住友ベークライト株式会社 (SUMIBE-CSIRT)
JXTG ホールディングス株式会社 / JX アイティソリューション株式会社 (JXTG-SEC)
株式会社ジェイティービー (JTB-CSIRT)
国立大学法人東京海洋大学 (KAIYODAI CSIRT)
鉄道情報システム株式会社 (JRS-CSIRT)
一般財団法人　ITS サービス高度化機構 (ITS-TEA.SIRT)

本四半期末時点で 252 の組織が加盟しています。これまでの参加組織数の推移は［図 5-1］のとおりです。



［図 5-1 日本シーサート協議会 加盟組織数の推移］

5.2. 第 13 回総会および第 18 回シーサートワーキンググループ会

第 13 回総会および第 18 回シーサートワーキンググループ会を次のとおり開催しました。

日時：2017 年 8 月 25 日
場所：ヒューリックホール&カンファレンス

第 13 回総会では、前任の次の 3 名の運営委員が立候補し、会員の信任を得て再選されました。
HIRT　寺田真敏氏
MBSD-SIRT　大河内 智秀氏
専門委員　乾 奈津子氏

第 18 回シーサートワーキンググループ会は、日本シーサート協議会の会員および協議会への加盟を前提に組織内シーサートの構築を検討している組織が参加する会合です。会合では、各ワーキンググループからの活動報告や、新しく加盟した 12 チームによる自組織のシーサートの概要紹介に加えて、次の 3 つの講演がおこなわれました。

講演 1
「皆に役立つ 4 つのキーワード ～10 年後の協議会へのメッセージ～」
寺田 真敏氏　運営委員長（日本シーサート協議会）

講演 2
「進化しつづける CSIRT をめざして：高信頼性組織化の視点から」
中西 晶氏（明治大学　経営学部　教授）

講演 3
「大学組織における CSIRT の悩みと暗号学視点から見た電子文書長期保存の考え方」
猪俣 敦夫氏（東京電機大学 教授）

5.3. 日本シーサート協議会　運営委員会

本四半期は、次のとおり 3 回の運営委員会と 1 回の臨時運営員会を開催しました。

第 122 回運営委員会
日時：2017 年 4 月 26 日（水）16:00 - 18:00
場所：HIRT

第 123 回運営委員会
日時：2017 年 8 月 21 日（月）16:00 - 18:00
場所：JPCERT/CC

臨時運営委員会
日時：2017 年 8 月 28 日（月）16:00 - 18:00
場所：JPCERT/CC

第 124 回運営委員会
日時：2017 年 9 月 27 日（水）16:00 - 18:00
場所：JPCERT/CC

日本シーサート協議会の活動の詳細については、次の Web ページをご参照ください。

日本シーサート協議会
http://www.nca.gr.jp/

6. フィッシング対策協議会事務局の運営

JPCERT/CC は、フィッシング対策協議会（以下「協議会」）の事務局を担当しており、経済産業省からの委託により、協議会における各ワーキンググループ活動の運営や、一般消費者からのフィッシングに関する報告・問い合わせの受付、報告に基づいたフィッシングサイトに関する注意喚起等の活動を行っています。

6.1 情報収集 / 発信の実績

本四半期は、協議会 Web サイトや会員向けメーリングリストを通じて、フィッシングに関するニュースや緊急情報を 20 件発信しました。

本四半期は、Amazon、Apple 等の E コマースサイトをかたりクレジットカード情報を不正に詐取するフィッシングの報告が増加しています。中でも Apple をかたるフィッシングでは、フィッシングサイトの短縮 URL をメール本文や添付ファイルに記載し、1 日から数日ごとにリダイレクト先を変更するタイプが多く、メール文面もさまざまなパターンが報告されました。また LINE をかたるフィッシングについても、前四半期に続き、継続して多くの報告が寄せられました。これらのサービスは利用者数も多く、影響範囲も大きいため、緊急情報を発行し注意を促しました。また、名前をかたられた各事業者に、フィッシングメールの内容やフィッシングサイトの URL 等の関連情報を提供しました。

本四半期は、合計 13 件の緊急情報を協議会 Web サイト上に掲載し、広く注意を喚起しました。その内訳は次のとおりです。

ライセンス更新をかたるフィッシング関連：1 件
SNS サービスをかたるフィッシング関連：2 件

クレジットカード会社をかたるフィッシング関連：2 件

E コマースサイトをかたるフィッシング関連：8 件

例として、［図 6-1］に Apple をかたるフィッシング (2017/07/05)の注意喚起の内容を示します。

［図 6-1 Apple をかたるフィッシング (2017/07/05) ］

https://www.antiphishing.jp/news/alert/apple_20170705.html

これらのフィッシングサイトについては、JPCERT/CC のインシデント対応支援活動を通じて、サイト停止の調整を行いました。

6.2. フィッシングサイト URL 情報の提供

協議会の会員のうち、フィッシング対策ツールバーやウイルス対策ソフト等を提供している事業者と、フィッシングに関する研究を行っている学術機関に対し、協議会に報告されたフィッシングサイトの URL を集めたリストを提供しています。この URL 情報の提供は、各社の製品においてブラックリストに登録する等、ユーザ保護に向けた取り組みへの活用や、研究教育機関における関連研究への利用を目的としています。本四半期末の時点で 37 組織に対し URL 情報を提供しており、今後も提供先を順次拡大していく予定です。

6.3. 講演活動

協議会ではフィッシングの動向を紹介し、効果的な対策を呼び掛けるための講演活動を行っています。本四半期は次の講演を行いました。

(1) 村上 晃（エンタープライズサポートグループ　部門長）
　駒場 一民（エンタープライズサポートグループ　情報セキュリティアナリスト）
　「フィッシング対策ガイドライン全体説明」
　フィッシング対策ガイドライン実践セミナー 2017 , 2017 年 8 月 10 日

6.4. フィッシング対策協議会の活動実績の公開

協議会の Web サイトにおいて、報告されたフィッシングサイト数を含む、毎月の活動報告等を公開しています。詳細については、次の Web ページをご参照ください。

フィッシング対策協議会 Web ページ
https://www.antiphishing.jp/
フィッシング対策協議会 2017 年 7 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201707.html
フィッシング対策協議会 2017 年 8 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201708.html
フィッシング対策協議会 2017 年 9 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201709.html

7. フィッシング対策協議会の会員組織向け活動

フィッシング対策協議会では、経済産業省から委託された活動のほかに、協議会の会員組織向けの活動を、運営委員会の決定に基づいて行っています。

7.1 運営委員会開催

本四半期においては、フィッシング対策協議会の活動の企画・運営方針の決定等を行う運営委員会を次のとおり開催しました。

フィッシング対策協議会 第 52 回運営委員会
日時：2017 年 7 月 14 日 16:00 - 18:00
場所：アルプス　システム　インテグレーション株式会社

フィッシング対策協議会 第 53 回運営委員会
日時：2017 年 8 月 4 日 16:00 - 18:00
場所：トッパン・フォームズ株式会社

フィッシング対策協議会 第 54 回運営委員会
日時：2017 年 9 月 8 日 16:00 - 18:00
場所：GMO グローバルサイン株式会社

7.2 フィッシング対策ガイドライン実践セミナー 2017 開催

フィッシング対策ガイドライン実践セミナー 2017 を次のとおり開催しました。
本セミナーでは 2017 年 6 月に改訂版を公開したフィッシング対策ガイドラインの内容とフィッシング対策への活用について解説しました。

フィッシング対策ガイドライン実践セミナー 2017
日時：2017 年 8 月 10 日 14:00 - 17:00
場所：日立システムズ　ソリューションスクエア東京
東京都品川区大崎 1-2-1 大崎フロントタワー

8. 公開資料

JPCERT/CC が本四半期に公開した調査・研究の報告書や論文、セミナー資料は次のとおりです。

8.1 脆弱性関連情報に関する活動報告レポート

IPA と JPCERT/CC は、それぞれ受付機関および調整機関として、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）等に基づく脆弱性関連情報流通制度の一端を 2004 年 7 月から担っています。
本レポートは、この制度の運用に関連した前四半期の活動実績と、同期間中に届出ないし公表された脆弱性に関する注目すべき動向についてまとめたものです。

ソフトウエア等の脆弱性関連情報に関する届出状況[2017 年第 2 四半期（4 月～6 月）]
（2017 年 7 月 26 日）
https://www.jpcert.or.jp/press/2017/vulnREPORT_2017q2.pdf

8.2 インターネット定点観測レポート

JPCERT/CC では、インターネット上に複数のセンサーを分散配置し、不特定多数に向けて発信されるパケットを継続して収集するインターネット定点観測システム「TSUBAME」を構築・運用しています。脆弱性情報、マルウエアや攻撃ツールの情報などを参考に、収集したデータを分析することで、攻撃活動やその準備活動の捕捉に努めています。
本レポートは、インターネット定点観測の結果を四半期ごとにまとめたものです。

インターネット定点観測レポート(2017 年 4～6 月)
（2017 年 8 月 3 日）
https://www.jpcert.or.jp/tsubame/report/report201704-06.html
https://www.jpcert.or.jp/tsubame/report/TSUBAMEReport2017Q1.pdf

8.3 分析センターだより

JPCERT/CC では、インシデントに関連して収集または報告いただいた情報をもとに、攻撃に用いられた手法やその影響を把握するため、アーティファクトの調査・分析を行っています。また、分析技術の普及や技術者の育成にも努めており、その一環として日々のアーティファクト分析業務の中で感じたこと、発見したことを「分析センターだより」として発信しています。本四半期においては次の 3 件の記事を公開しました。

(1) impfuzzy for Neo4j を利用したマルウエア分析(2017-07-03)
大量のマルウエアをすべて手動で分析するのは現実的に難しいため、ツールによって分類作業を自動化し、分析すべき新種のマルウエアを抽出したり、マルウエアの変化を検知したりすることが重要で

す。この記事では、マルウエアをクラスタリングするツール「impfuzzy for Neo4j」を活用してマルウエア「Emdivi」90 検体を用いて分析した事例を紹介しました。

impfuzzy for Neo4j を利用したマルウエア分析(2017-07-03)
https://www.jpcert.or.jp/magazine/acreport-impfuzzy_neo4j-2.html

(2) マルウエア Datper をプロキシログから検知する(2017-08-17)
マルウエア「Datper」は主に日本国内の組織を標的とした攻撃に使われてきたマルウエアで、JPCERT/CC では 2016 年 6 月頃からこのマルウエアを使った攻撃を確認してきました。Datper を用いた一連の攻撃は、侵入の発見や検知が難しく、攻撃の早期発見や被害の未然防止が難しいのが現状です。こうした状況を改善する一助として、本記事では、Datper を通信の特徴から検知する方法を紹介しています。

マルウエア Datper をプロキシログから検知する(2017-08-17)
https://www.jpcert.or.jp/magazine/acreport-datper.html

(3) マルウエア Datper の痕跡を調査する～ログ分析ツール（Splunk・Elastic Stack）を活用した調査～(2017-09-25)
プロキシサーバのログなどに含まれるマルウエア Datper の通信を検知するための Python スクリプトを活用し、ログ分析ツールで Datper の通信を調査するための環境設定方法を紹介しました。高いマーケットシェアを持つ「Splunk」またはオープンソフトウェアの「Elastic Stack（Elasticsearch、Logstash、Kibana）」のいずれかを使って Datper の通信ログを抽出できるよう、それぞれについて方法を解説しています。

マルウエア Datper の痕跡を調査する～ログ分析ツール（Splunk・Elastic Stack）を活用した調査～(2017-09-25)
https://www.jpcert.or.jp/magazine/acreport-search-datper.html

8.4 インシデントレスポンスだより

JPCERT/CC は、設立当初から国内外から日本に関係するコンピュータセキュリティインシデントの報告を受け付け、その対応の支援、状況の把握をおこない、国内全体の被害拡大防止の活動を行っています。「インシデントレスポンスだより」では、日々現場で起こるインシデントへの対応を支援している、インシデントレスポンスグループのメンバーが、最新のインシデント事例や動向、調査方法など実際にインシデントに対応するなかで見えた状況をタイムリーに紹介しています。本四半期においては次の 1 件の記事を公開しました。

(1) インターネット上に公開されてしまったデータベースのダンプファイル(2017-08-08)
2017 年 6 月下旬にドイツのセキュリティ研究者より、日本国内の多数の Web サイトで、データベースのダンプファイルが外部から閲覧できる状態にあるとの報告を受けました。JPCERT/CC ではサイ

バー攻撃の可能性を懸念しつつ、提供いただいた情報をもとに該当する Web サイトの管理者に連絡し、状況を確認していただきました。本記事は、この問題について確認できた状況を紹介しています。

インターネット上に公開されてしまったデータベースのダンプファイル(2017-08-08)
https://www.jpcert.or.jp/magazine/irreport-Unsecured_Databases.html

9. 主な講演活動

(1) 佐々木 勇人（早期警戒グループ リーダー）：
「サイバー攻撃の最新動向とインシデント対応のポイント」
第 5 回埼玉県自治体 ICT セミナー,2017 年 7 月 7 日

(2) 真鍋 敬士（理事・最高技術責任者）：
「デジタル変革時代のサイバーセキュリティ対策」
Cyber Security Dialogue, 2017 年 7 月 18 日

(3) 竹田 春樹（分析センター マネージャー）：
「サイバー攻撃の動向とその対策」
株式会社サイバー・ソリューションズユーザ総会, 2017 年 7 月 19 日

(4) 佐々木 勇人（早期警戒グループ リーダー）：
「サイバー攻撃の最新動向とインシデント対応のポイント」
AGS 株式会社「サイバー攻撃の脅威セキュリティ対策セミナー」, 2017 年 7 月 19 日

(5) 小宮山 功一朗（エンタープライズサポートグループ マネージャー）：
「グローバルなサイバーセキュリティのおしごと」
セキュリティ・キャンプ全国大会 2017,2017 年 8 月 14 日

(6) 久保 正樹（情報流通対策グループ マネージャー）：
「リクルートテクノロジーズが、とある IT 資産管理ソフトウェアの脆弱性を発見し、修正されるまで」
@IT 編集部主催セミナー「連日の「深刻な脆弱性」どう向き合い、どう対応するか」, 2017 年 8 月 30 日

(7) 洞田 慎一（早期警戒グループ マネージャー）：
「Web サイトへのサイバー攻撃に備えて」
平成 29 年度 JR 西日本グループ CSIRT メンバー向けセキュリティ研修, 2017 年 9 月 8 日

(8) 竹田 春樹（分析センター マネージャー）：
「サイバー攻撃の脅威の現状と検討すべき対策~ 通信の特徴から見る課題 ~」
サイバーセキュリティテクノロジー最前線 セミナー, 2017 年 9 月 14 日

(9) 洞田 慎一（早期警戒グループ マネージャー）：
「調査から見えてくる EC サイトを取り巻く情報漏えいのリスク」
日経 BP 社・情報セキュリティ戦略セミナー2017, 2017 年 9 月 20 日

(10) 村上 晃（経営企画室、エンタープライズサポートグループ部門長）：
「もはや境界線では守れないクラウド/IoT 時代に求められる新たな制御モデルと CSIRT」
ITmedia Executive PowerBreakfast, 2017 年 9 月 21 日

(11) 洞田 慎一（早期警戒グループ マネージャー）：

「自動車を取り巻くサイバーセキュリティ」

「情報共有による脅威へのリスク低減～ 製品が引き起こすサイバーセキュリティの課題を例に考える ～」

DNV GL 車載セキュリティセミナー, 2017 年 9 月 25 日

10. 主な執筆活動

(1) 内田 有香子（国際部）：

情報セキュリティ白書 2017「2.3.5　アジア太平洋地域での CSIRT の動向」

2017 年 7 月 1 日

11. 協力、後援

本四半期は、次の行事の開催に協力または後援をしました。

(1) Hardening Project 2017

主　催：Hardening Project実行委員会

開催日：2017年6月23日～11月25日

(2) JAIPA Cloud Conference 2017

主　催：一般社団法人 日本インターネットプロバイダー協会 クラウド部会

開催日：2017年7月19日

(3) 第13回IPAひろげよう情報モラル・セキュリティコンクール2017

主　催：IPA（独立行政法人情報処理推進機構）

開催日：2017年6月1日～2018年3月31日

(4) RSAサイバーセキュリティワークショップ

主　催：EMCジャパン株式会社 RSA事業本部

開催日：2017年9月8日

(5) Security Days Fall 2017 / Email Security Conference 2017 / ID Management Conference 2017

主　催：株式会社ナノ・オプトメディア

開催日：2017年9月26日～9月29日

(6) IAjapan 第16-17回 迷惑メール対策カンファレンス

主　催：一般財団法人インターネット協会（IAjapan）

開催日：2017年9月26日～9月29日

■インシデントの対応依頼、情報のご提供
info@jpcert.or.jp
https://www.jpcert.or.jp/form/
■制御システムに関するインシデントの対応依頼、情報のご提供
icsr-ir@jpcert.or.jp
https://www.jpcert.or.jp/ics/ics-form.html
■脆弱性情報ハンドリングに関するお問い合わせ　：vultures@jpcert.or.jp
■制御システムセキュリティに関するお問い合わせ　：icsr@jpcert.or.jp
■セキュアコーディングセミナのお問い合わせ　：seminar-secure@jpcert.or.jp
■公開資料、講演依頼、資料使用、その他のお問い合わせ：pr@jpcert.or.jp

■PGP 公開鍵について　：https://www.jpcert.or.jp/jpcert-pgp.html