Japan Computer Emergency Response Team Coordination Center

JPCERT CC®

JPCERT-PR-2017-03
発行日 : 2017-7-13

JPCERT/CC 活動概要 [2017 年 4 月 1 日 ～ 2017 年 6 月 30 日]

活動概要トピックス

ートピック1ー　ランサムウエア WannaCrypt について

2017 年 5 月 12 日より世界各国において WannaCrypt（または WannaCry）と呼ばれるランサムウエアの感染被害が多数報告され、英国、欧州をはじめとして医療機関等の公共サービスなどに大きな影響がおよびました。日本においても大手製造事業者や地方自治体、個人に感染被害があったことが報じられました。JPCERT/CC が海外のセキュリティ組織から提供された情報を分析したところ、日本国内でも、5 月 13 日の午前中の時点で約 2,000 台の感染があったことを確認しています。

全世界 150 か国のサーバや端末が感染したとされており、短期間でこれほど多数の機器が感染したのは、WannaCrypt がこれまでのランサムウエアと異なりワーム型のマルウエアであったことと、あらゆるネットワークに対してランダムに攻撃パケットを送出して感染させる機能をもっていたことが理由として挙げられます。

海外において被害が報告され始めた 12 日（金）［現地時間］は日本では週末の深夜でしたが、週明け 15 日（月）以降の被害組織等からの問い合わせに備えて、JPCERT/CC においては 5 月 13 日（土）より各国の専門機関等と情報共有を行い、14 日（日）に緊急の注意喚起を行いました。また、15 日より被害組織等からの相談を受け、提供いただいた検体の解析結果などから、17 日に注意喚起を更新し、感染経路やその対策について情報発信を行いました。

OS のアップデートなどが適切に行われず、感染拡大の原因となった脆弱性が残留するサーバなどは世界各国にまだ多く稼働していると推測され、JPCERT/CC では、WannaCrypt と同様に SMBv1 の脆弱性を悪用した他のサイバー攻撃を警戒するとともに、注意を呼び掛けています。

インターネット経由の攻撃を受ける可能性のある PC やサーバに関する注意喚起
https://www.jpcert.or.jp/at/2017/at170023.html

ートピック2ー　インシデントレスポンスだより公開開始

JPCERT/CC が対応している様々なインシデントの事例や傾向などを紹介する「インシデントレスポンスだより」を開始いたしました。

JPCERT/CC が設立当初から行ってきたインシデントレスポンスの事業では、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、被害組織に対する支援活動や関係組織への連絡などを行って被害の拡大を防止するとともに、適切な情報共有をとおして同様のインシデントの発生を抑止する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、インシデントレスポンスの現場で対応しているメンバーが、最新のインシデント事例や動向、調査方法などを執筆してまいります。企業や組織において情報セキュリティに携わる皆さまに向けて、インシデントの未然予防や早期解決を目的に、JPCERT/CC が見ている状況をタイムリーに公開してまいります。

2017 年 6 月に発行した第一回目は「Avalanche ボットネット解体により明らかになった国内マルウエア感染端末の現状」として、国際的な Avalanche ボットネット解体の取り組みにおける JPCERT/CC の活動と Avalanche ボットネットに関わる国内マルウエア感染端末の現状について紹介しました。

Avalanche ボットネット解体により明らかになった国内マルウエア感染端末の現状(2017-06-12)
https://www.jpcert.or.jp/magazine/irreport-avalanche.html

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. 主な執筆活動」、「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 5225 件、インシデント件数ベースでは 5365 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 2553 件でした。前四半期の 3077 件と比較して 17%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_Report20170413.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 736 件で、前四半期の 707 件から 4%増加しました。また、前年度同期（642 件）との比較では、15%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	4 月	5 月	6 月	本四半期合計（割合）
国内ブランド	52	69	88	209(28%)
国外ブランド	143	115	176	434(59%)
ブランド不明 (注 5)	30	37	26	93(13%)
全ブランド合計	225	221	290	736(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。

本四半期の国内ブランドのフィッシングサイトのうち、国内通信事業者または SNS のフィッシングサイトが 8 割以上を占めました。国内金融機関を装ったフィッシングサイトでは、クレジットカード番号の ID 登録サイトを装ったフィッシングサイトのみが確認され、その他の国内インターネットバンキングなどを装ったものはありませんでした。

国内通信事業者の Web メールのログイン画面を装ったサイトの多くは、侵入されたと見られる海外の Web サイトに設置されていました。特定のブランドを装ったフィッシングでは、Web フォームを作成する正規のサービスを使用して立ち上げられたフィッシングサイトに、短縮 URL から誘導するといった手法が共通して使用されていました。

SNS を装ったフィッシングサイトのほとんどは.cn ドメインを使用しており、ドメイン名は 4 月から 5 月初めにかけてはランダムな英字 5～6 文字、5 月半ば以降は被害ブランド名の後ろに英字 2～4 文字がついたドメイン名が使用されていました。また、多くのサイトで、香港の IP アドレスが使用されていました。

フィッシングサイトの調整先の割合は、国内が 26%、国外が 74%であり、前四半期（国内 27%、国外 73%）に比べ、国内での調整が増加しています。

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、461 件でした。前四半期の 967 件から 52%減少しています。

前四半期に引き続き、初回アクセス時にのみページ末尾に不正なスクリプトが埋め込まれる改ざんが観測されました。改ざんされたサイトに埋め込まれるスクリプトとして、フォントのアップデートのポップアップを表示するものや、Adobe Flash Player の脆弱性を使用した攻撃を行うサイトに誘導するものを確認

しており、いずれも最終的にランサムウエアがダウンロードされる仕組みになっていました。

初回アクセス時にのみ不正なスクリプトが埋め込まれる改ざんは、CMS を使用した Web サイトで多く確認されています。また、6 月初めごろから、WordPress 用プラグイン WP Job Manager の脆弱性によって画像ファイルを不正に設置されたとみられる国内サイトが多く確認されました。CMS およびそのプラグインの脆弱性は、改ざんなどの攻撃に悪用される可能性があるため、常に最新のバージョンのものを使用し、不要であれば削除するといった対策を行っておくことが重要です。

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、9 件でした。前四半期の 11 件から 18%減少しています。本四半期は、対応を依頼した組織は 2 件でした。

本四半期には、Daserf とよばれる HTTP ボットや wali とよばれるダウンローダなどを使用した標的型攻撃に関する報告が複数寄せられました。同種の標的型攻撃に関する報告は、昨年の 8 月ごろから寄せられています。

攻撃に使用されるマルウエアの感染経路の一つとして、資産管理ソフトの脆弱性が悪用されていることを確認しています。攻撃者はこの脆弱性を悪用した攻撃を、昨年の 6 月ごろから継続して行っている可能性があります。グローバル IP アドレスが割り当てられている PC 上で、脆弱性をもつバージョンの資産管理ソフトが攻撃パケットを受信すると、当該 PC がダウンローダに感染し、その後ダウンローダによって、HTTP ボットをダウンロードして実行します。

HTTP ボットは、攻撃者の C&C サーバから命令を受信し、PC から収集した情報を送信します。HTTP ボットの通信相手である C&C サーバに、国内の侵入された Web サーバが悪用されている例を多く確認しています。HTTP ボットは、感染 PC から収集した情報を C&C サーバに送信する際に、暗号化してはいますが HTTP リクエストのパラメータに埋め込むため、HTTP リクエストから暗号化された情報を取り出して復号することで、攻撃者が情報収集のために PC 上で行った操作などを確認できることがあります。

その他に、標的型攻撃と見られる、マルウエアが添付されたメールに関する報告が複数寄せられました。4 月後半に報告された標的型攻撃メールには、2017 年 4 月のアップデートで修正された Microsoft 製品の脆弱性（CVE-2017-0199）を悪用した攻撃を行うファイルが添付されていました。また、ダミーの文書ファイルとショートカットファイルが添付されており、ショートカットファイルを実行すると、最終的にボットの機能を持つマルウエアが実行され、PowerShell スクリプトによって追加のマルウエアがダウンロード、実行される攻撃手法も確認されています。この手法は、以前に見られた Asruex や ChChes といった HTTP ボットに感染させる標的型攻撃メールと類似しています。

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 33,000 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、本四半期は次のような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まとめ、次のようなお知らせとして発行しました。

発行件数：5 件　https://www.jpcert.or.jp/update/2017.html

2017-04-05　JPCERT/CC がランサムウエアの被害低減を目指す国際的なプロジェクト「No More Ransom」にサポートパートナーとして協力
2017-04-24　長期休暇に備えて 2017/04
2017-05-12　2015 年度 CSIRT 構築および運用における実態調査（英語版）を公開
2017-06-28　世界的に猛威を振るうランサムウエアへの注意

1.2.1.2. 注意喚起

深刻かつ影響範囲の広い脆弱性等について、次のような注意喚起情報を発行しました。

発行件数：13 件（うち 1 件更新）　https://www.jpcert.or.jp/at/

2017-04-12　Adobe Flash Player の脆弱性 (APSB17-10) に関する注意喚起 (公開)
2017-04-12　Adobe Reader および Acrobat の脆弱性 (APSB17-11) に関する注意喚起 (公開)
2017-04-12　2017 年 4 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)
2017-04-13　ISC BIND 9 に対する複数の脆弱性に関する注意喚起 (公開)
2017-04-19　2017 年 4 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)
2017-05-10　Adobe Flash Player の脆弱性 (APSB17-15) に関する注意喚起 (公開)
2017-05-10　2017 年 5 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)
2017-05-14　ランサムウエア "WannaCrypt" に関する注意喚起 (公開)
2017-05-17　ランサムウエア "WannaCrypt" に関する注意喚起 (更新)
2017-06-14　Adobe Flash Player の脆弱性 (APSB17-17) に関する注意喚起 (公開)
2017-06-14　2017 年 6 月マイクロソフトセキュリティリリースに関する注意喚起 (公開)
2017-06-28　インターネット経由の攻撃を受ける可能性のある PC やサーバに関する注意喚起 (公開)
2017-06-30　ISC BIND 9 の脆弱性に関する注意喚起 (公開)

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。

発行件数：12 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 12 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 12 件でした。

2017-04-05　Ruby 2.1 の公式サポート終了
2017-04-12　ビジネスメール詐欺に注意
2017-04-19　サポート対象外 OS の利用による脅威
2017-04-26　警察庁が「平成 28 年におけるコミュニティサイト等に起因する事犯の現状と対策につい

て」を公開
2017-05-10　IPA が「SECURITY ACTION」を開始
2017-05-17　ランサムウェア「WannaCrypt」が世界中で猛威を振るう
2017-05-24　ランサムウェア「WannaCrypt」が感染活動を継続
2017-05-31　Windows アプリケーションの DLL 読み込みに関する脆弱性について
2017-06-07　NICT がサイバー攻撃誘引基盤「STARDUST」(スターダスト) を開発
2017-06-14　FIRST が学習用のプラットフォームを公開
2017-06-21　フィッシング対策協議会が「フィッシング対策ガイドライン」の改訂版を公開
2017-06-28　ランサムウェア「WannaCry」の亜種によるものとみられるアクセスを確認

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/

1.2.2. 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。

【Samba の脆弱性に関する情報発信】
UNIX 系システム上のファイルやプリンタに Windows からアクセスするためのソフトウェア・モジュールである Samba の脆弱性 (CVE-2017-7494) に関するアドバイザリが 2017 年 5 月 24 日（現地時間）に公開されました。JPCERT/CC にて本脆弱性に関する実証コードの検証を行った結果、この脆弱性を悪用することで、共有フォルダへの書き込み権限のあるリモートのクライアントから、Samba の稼働するサーバ上で任意のコードが実行できることを確認しました。Samba は、組織内ネットワークにおいて、ファイルサーバや NAS などで広く使用されているため、本脆弱性の深刻度は高いと判断し、早期警戒情報を発行しました。

【英語版 CSIRT 構築および運用における実態調査の公開】
JPCERT/CC は、国内の CSIRT に関する実態調査レポートとして「2015 年度 CSIRT 構築および運用における実態調査」の英語版を 2017 年 6 月 29 日に公開しました。本調査は、日本シーサート協議会（NCA）に加盟している CSIRT に対し、組織体制やメンバー構成、ポリシーなど CSIRT の構築時に定義しておくべき項目を調査し、まとめたものです。当該調査において得られた知見を、日本国内のみならず海外にお

ける CSIRT 構築に活用していただくこと、海外の民間組織でセキュリティを担当している方々に日本の民間組織の取り組み事例を参考にしていただくことを目的として、英語版を公開しました。

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。

1.3.1. インターネット定点観測システム TSUBAME の運用、および観測データの活用

JPCERT/CC は、さまざまな地域に設置された観測用センサーを含むインターネット定点観測システム TSUBAME を構築運用するとともに、観測されたデータを各地域の CSIRT と共同で分析をするためのプロジェクトである TSUBAME プロジェクトの事務局を担当しています。2017 年 6 月末時点で、観測用センサーは 21 地域 26 組織に設置されています。今後も設置地域を拡大し、より充実したセンサー網の構築と共同分析の高度化を進めるべく、海外諸国のナショナル CSIRT 等に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。

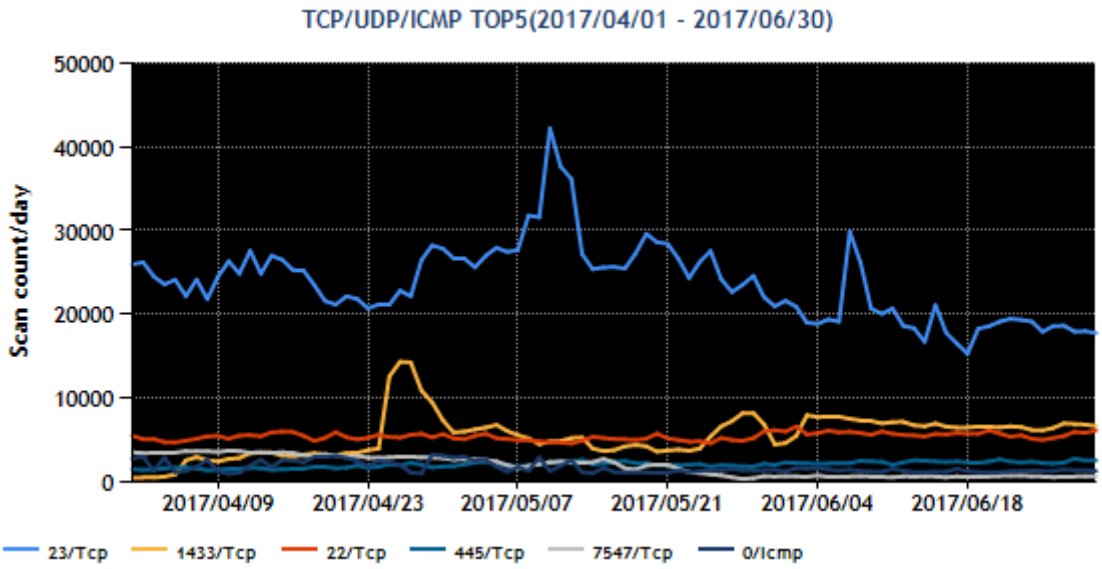
TSUBAME（インターネット定点観測システム）
https://www.jpcert.or.jp/tsubame/index.html

JPCERT/CC は、TSUBAME で収集したデータを宛先ポート番号や送信元地域ごとに分類して統計分析し、既知の脆弱性情報やマルウエア、攻撃ツール等との関連を考察することで、攻撃活動や準備活動の捕捉に努めています。

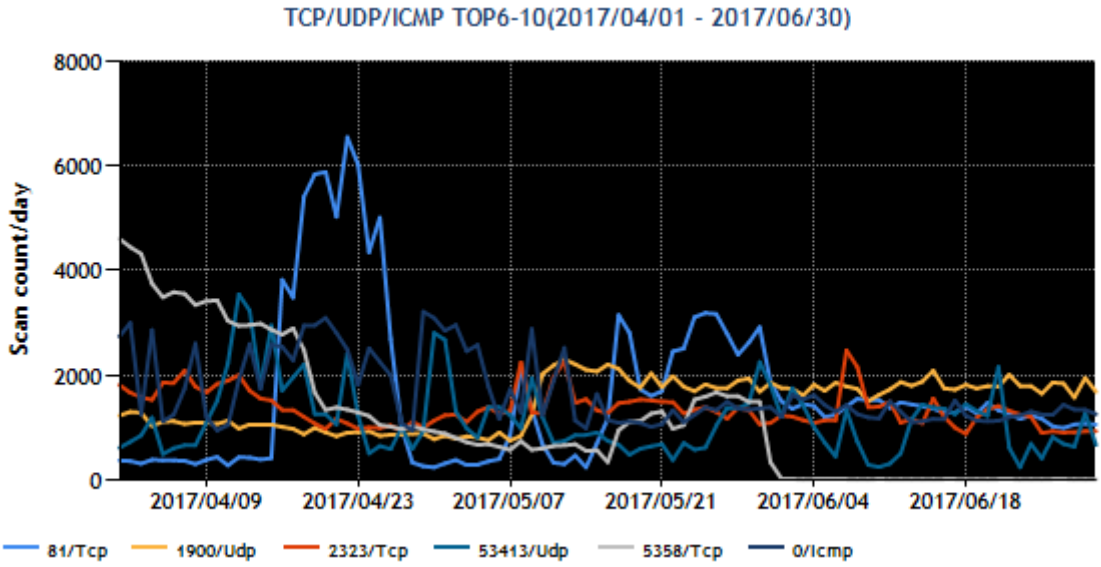
主に日本企業のシステム管理者等の方々に、自組織のネットワークに届くパケットの傾向と比較していただけるよう、日本国内のセンサーで受信したパケットを宛先ポート別に集計してグラフ化し、毎週月曜日に JPCERT/CC の Web ページで公開しています。また、四半期ごとに観測傾向や注目される現象を紹介する「インターネット定点観測レポート」を公開しており、2017 年 1 月から 3 月分のレポートを 2017 年 5 月 11 日に公開しました。

TSUBAME 観測グラフ
https://www.jpcert.or.jp/tsubame/index.html#examples

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。

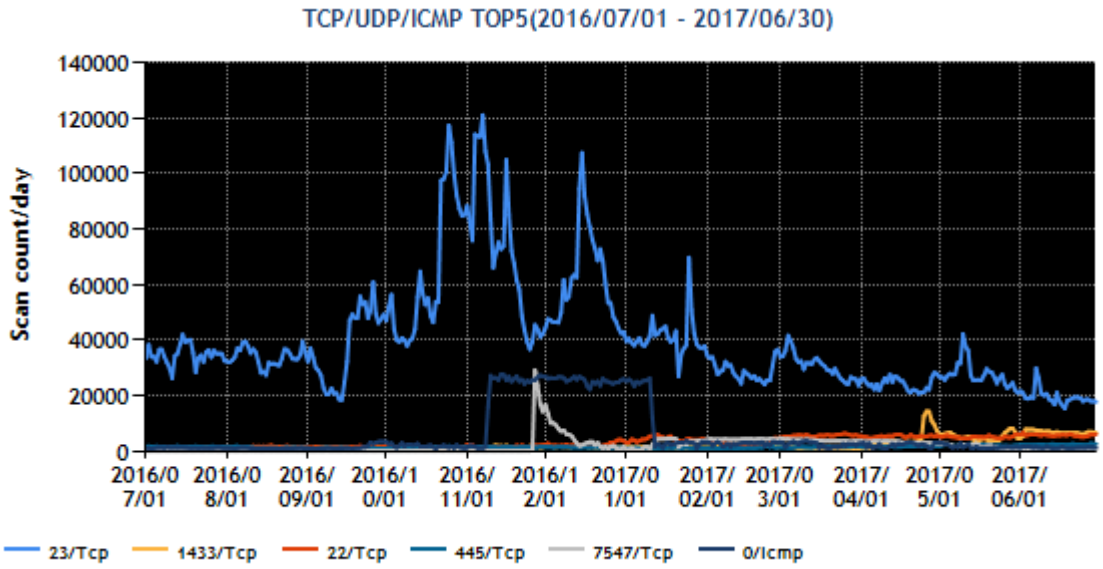


［図 1-1 宛先ポート別グラフ トップ 1-5（2017 年 4 月 1 日-6 月 30 日）］

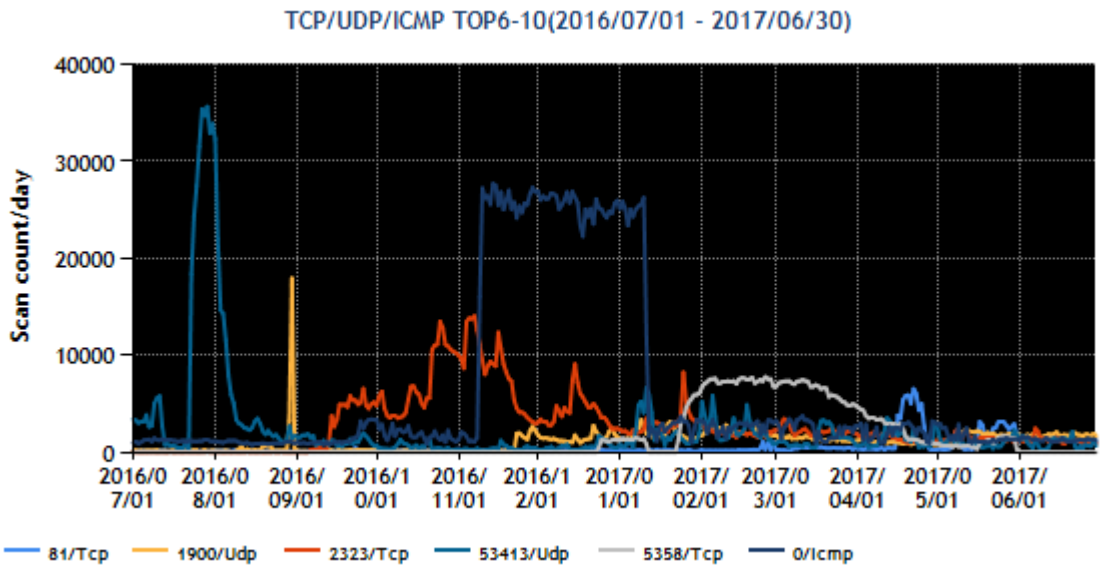


［図 1-2 宛先ポート別グラフ トップ 6-10（2017 年 4 月 1 日-6 月 30 日）］

また、過去 1 年間（2016 年 7 月 1 日-2017 年 6 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 7 月 1 日-2017 年 6 月 30 日)］



［図 1-4 宛先ポート別グラフ トップ 6-10（2016 年 7 月 1 日-2017 年 6 月 30 日)］

本四半期は、23/TCP、22/TCP 宛のパケットが多く観測されました。それらのパケットは、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、遠隔操作のための SSH サーバ等のサービスをスキャンしていると見られるパケットが継続して観測されています。

1.3.2. 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) 国内外の機器を主な対象とした探索活動についての対応
複数の日本国内外の IP アドレスを送信元とし、23/TCP、2323/TCP、5358/TCP、7547/TCP 等、遠隔ログインや機器の API 等が使用する Port 宛てのパケットが前四半期に引き続き観測されました。これらの Port に対するパケットは、Mirai 等のマルウエアが他の専用機器をマルウエアに感染させる活動と関連していると考えられます。これらのマルウエアに感染した機器からは、探索パケットが送信されます。送信元 IP アドレスを調査したところ、マルウエアに感染した複数のベンダの機器が見つかりました。その中には、今回初めて感染を確認した機器も含まれており、マルウエアに感染する機器の種類が拡大している可能性が示唆されます。JPCERT/CC では、攻撃対象となる専用機器の変化に注目し対象となった製造ベンダへの情報提供を行ったり、送信元 IP アドレスに対しての連絡を行ったりといった対応を行いました。

(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、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扱状況

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。

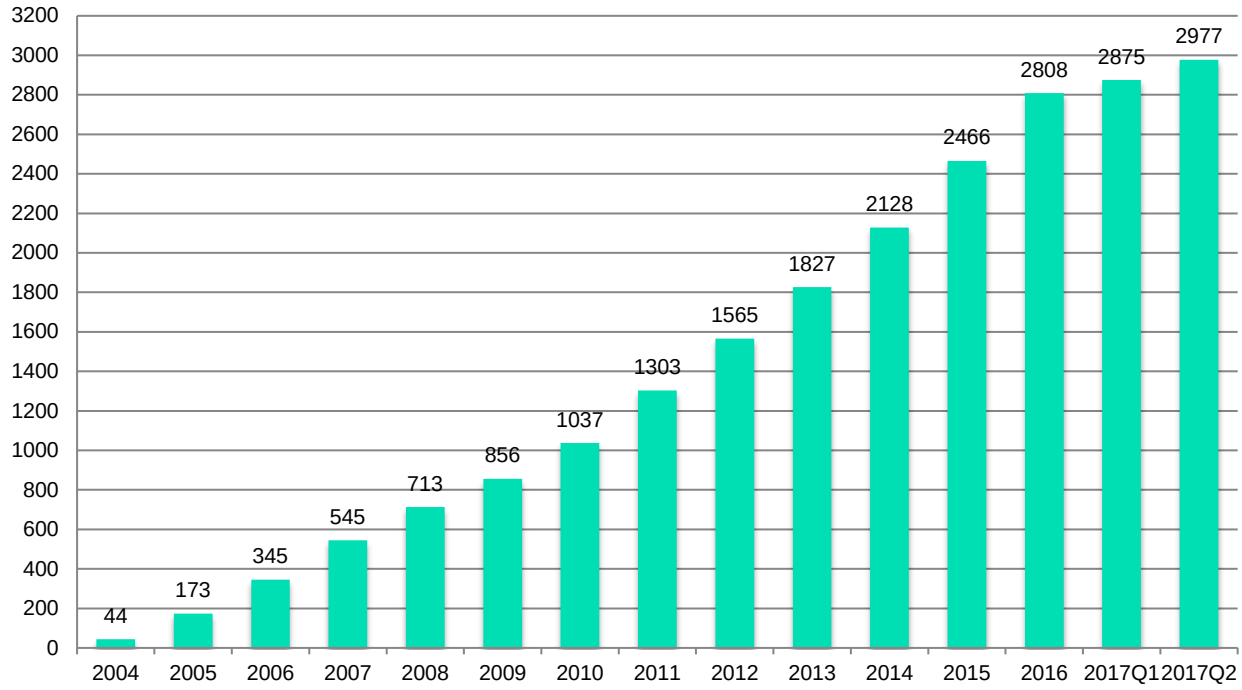
独立行政法人情報処理推進機構（IPA）脆弱性対策
https://www.ipa.go.jp/security/vuln/

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 102 件（累計 2,977 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/



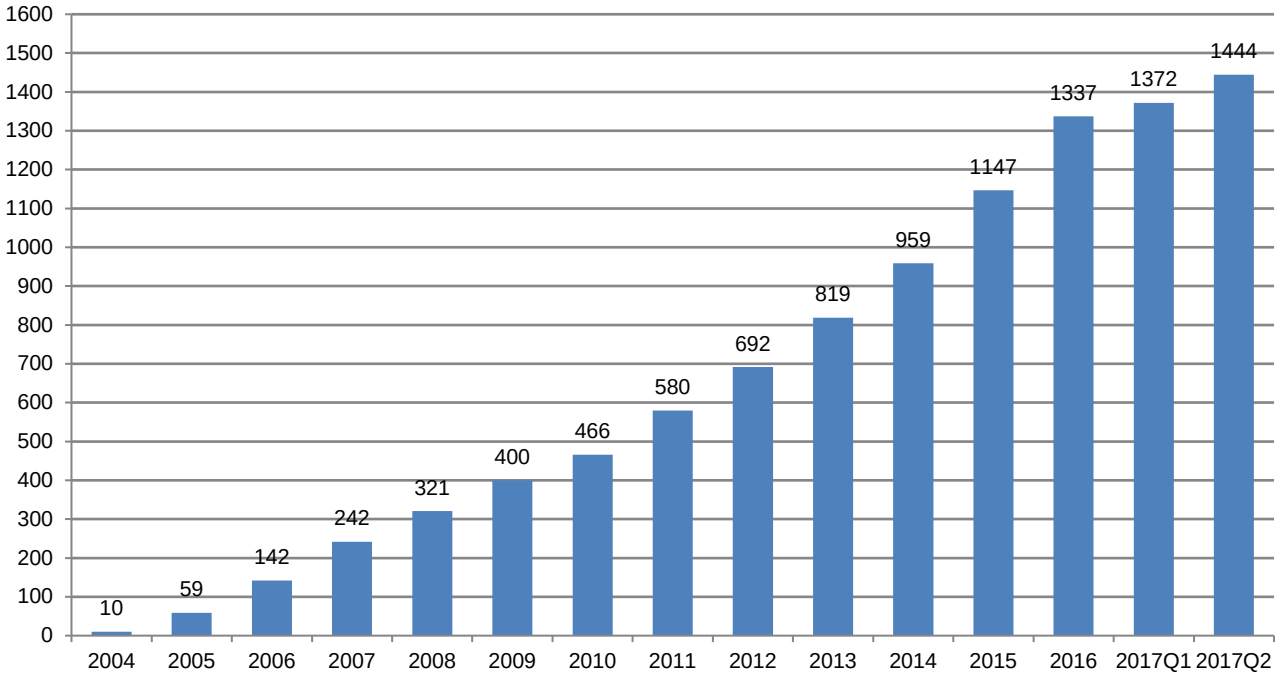
［図 2-1　JVN 公表累積件数］

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 72 件（累計 1,444 件）で、累計の推移は［図 2-2］に示すとおりです。72 件のうち、47 件が国内製品開発者の製品、25 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、47 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情報の件数の、影響を受けた製品のカテゴリ別の内訳は、［表 2-1］のとおりでした。本四半期は、Windows アプリケーションが 32 件と非常に多く、次いで WordPress プラグイン、無線 LAN ルータ等の組込み系製品が比較的多い状況でした。本四半期において Windows アプリケーションに関する公表が多かったのは、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 読み込みの脆弱性と同じ機序で脆弱な Windows アプリケーションが、最初の報告から 7 年経過した今日になって、多数発見・届出されたからです。行政機関が提供する Windows アプリケーションに関する脆弱性の公表も本四半期は特に多くありました。これは、行政機関のソフトウエアの脆弱性に関心をもった特定の発見者によって関する脆弱性が検出、届出さ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別内訳］

製品分類	件数
Windows アプリケーション	32
プラグイン	14
組込系	10
CMS	5
ウェブアプリケーション	4
グループウエア	2
マルチプラットフォームアプリケーション	2
Android アプリ	1
IT 資産管理ツール	1
セキュリティアプライアンス	1



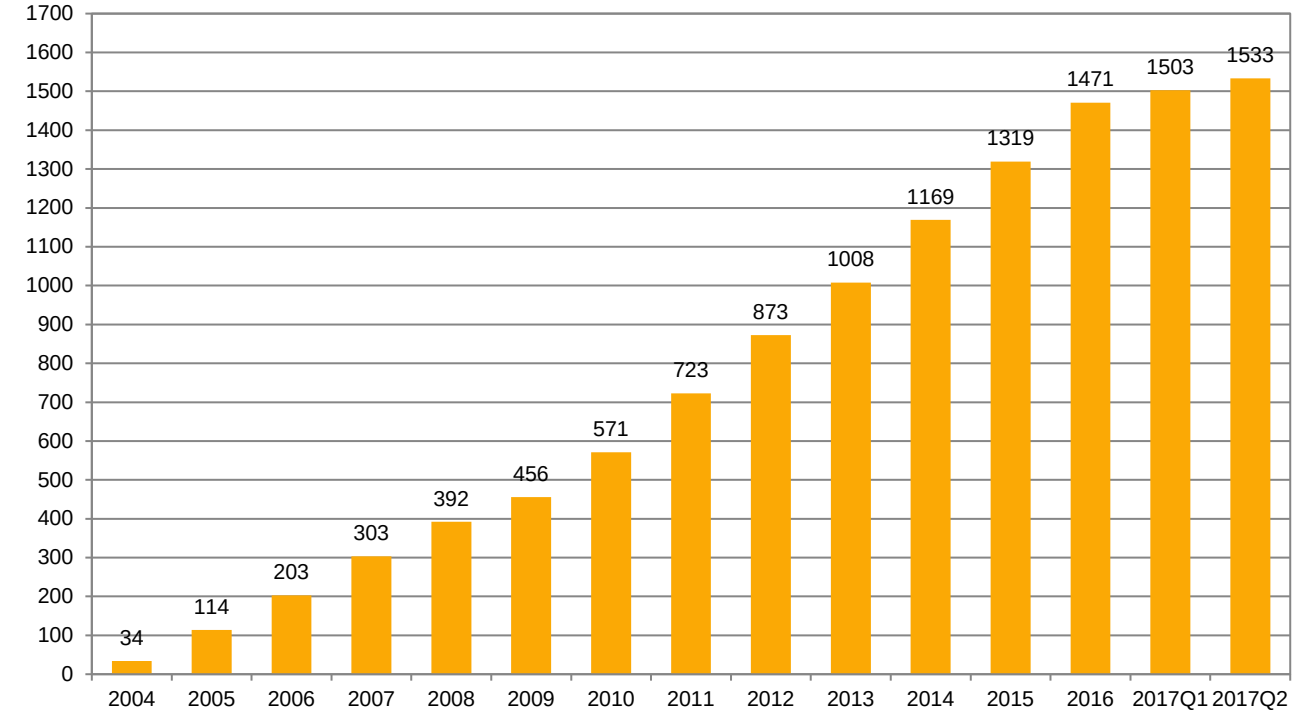
［図 2-2 公表を行った国内取扱脆弱性情報の累積件数］

本四半期に公表した国際取扱脆弱性情報は 30 件（累計 1,533 件）で、累計の推移は［図 2-3］に示すとおりです。この 30 件には、JPCERT/CC が独自に注意喚起として 5 月 25 日に公表したテクニカルアラート「Windows アプリケーションによる DLL 読み込みやコマンド実行に関する問題」と米国 US-CERT が 6 月 13 日に公表したテクニカルアラートを JPCERT/CC が日本語訳して公表した「制御システムを狙う CrashOverride マルウェアの脅威」の 2 件が含まれます。

本四半期に公表した脆弱性情報の、影響を受けた製品のカテゴリ別内訳は、［表 2-2］のとおりでした。2016 年以降、非常に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。アンチウィルス製の公表も 5 件と本四半期は多くありましたが、これらはすべて自社製品の脆弱性に関する公表依頼でした。昨今、国内製品開発者と同様に、海外製品開発者からも、自社製品の脆弱性対応に関する事前通知等が JPCERT/CC に報告される事例が徐々に増えており、本四半期においては、12 件の自社製品における脆弱性情報の通知を受け、JVN にて公表しました。

［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別内訳］

製品分類	件数
アンチウィルス製品	5
組込系	5
DNS	3
Windows アプリケーション	2
ウェブサーブレットコンテナ	2
サーバ製品	2
マルチプラットフォームアプリケーション	2
ライブラリ	2
iOS	1
iOS アプリ	1
macOS 等複数の Apple 製品	1
SDK	1
Windows OS	1
スマホアプリ	1
制御系	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。

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 等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 87 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。

5 月 23 日から 24 日にかけて、MITRE と共同で CNA Training を開催しました。このトレーニングは、アジア地域に拠点を持つ新しく CNA になった組織および今後 CNA になることを検討している、調整機関および製品を開発している組織を対象にしたもので、日本国内からは 5 組織、海外からは 4 組織が参加しました。トレーニングの前半では CNA として期待される役割などを中心に解説が行われ、後半では、公開されている脆弱性情報をもとに CVE データベースに登録するための CVE Entry を作成するハンズオンを行いました。

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

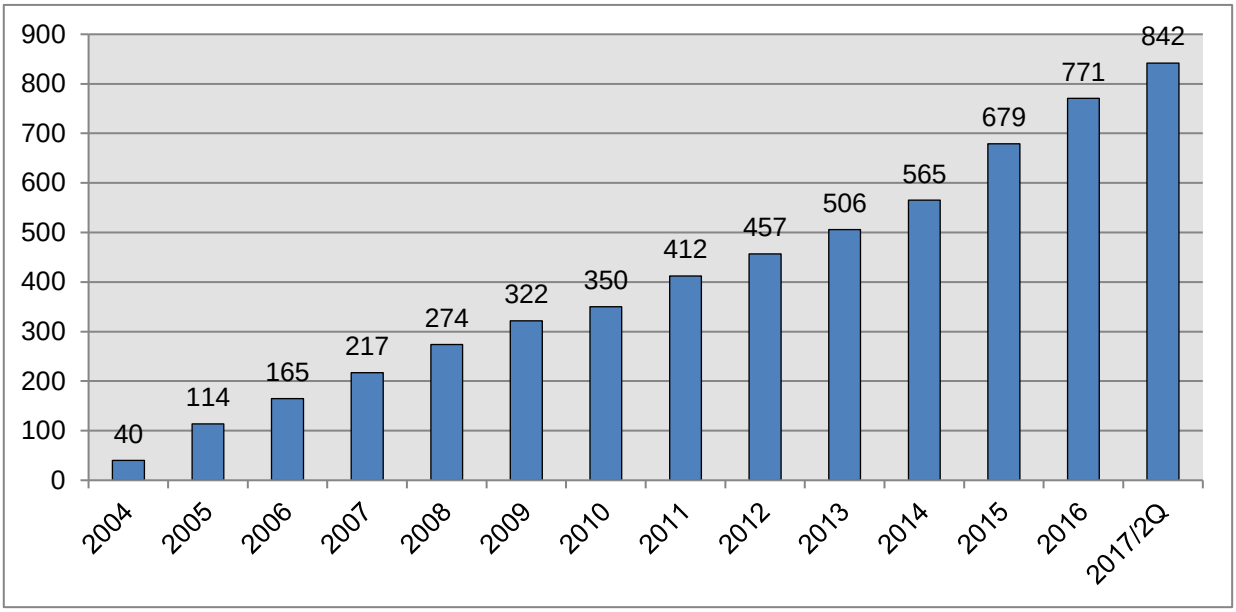
JPCERT/CC では、本規程に従って、日本国内の脆弱性情報流通体制を整備しています。
詳細については、次の Web ページをご参照ください。

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 6 月 30 日現在で 842 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. 「JPCERT/CC 脆弱性情報取扱いガイドライン」および「JPCERT/CC 製品開発者リスト登録規約」の改訂

2016 年度の「情報システム等の脆弱性情報の取扱いに関する研究会」において検討された結果を踏まえ、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が改訂され、5 月 30 日に公表されました。 これを受け JPCERT/CC では、「JPCERT/CC 脆弱性関連情報取扱いガイドライン」を改訂し、6 月 22 日に公表しました。 このガイドライン改訂では、パートナーシップガイドラインの改訂を受けて脆弱性の影響度に応じた取扱いに関する記述を追加したほか、現在の脆弱性情報ハンドリングの実態に即した記述の修正をおこなっています。
また「JPCERT/CC 製品開発者リスト登録規約」の改訂案を 6 月 22 日に公表しました。この改訂案においても、告示の改正を反映したほか、現在の脆弱性情報ハンドリングの実態に即した修正を加えています。この改訂案は、製品開発者リスト登録ベンダから 1 ヶ月間意見を求めた後、大きな問題点の指摘がなければ、所定の手続きを経て、新たな登録規約となる予定です。
これらの改訂内容の詳細につきましては、次の Web ページをご参照ください。

JPCERT/CC 脆弱性情報取り扱いガイドライン(2017 年 6 月 22 日公開)
http://www.jpcert.or.jp/vh/vul-guideline2017.pdf

「JPCERT コーディネーションセンター製品開発者リスト登録規約（変更案）」についてのお知らせ
http://www.jpcert.or.jp/vh/regist-notice2017.html

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 2 件の講演を行いました。

講演日時: 5 月 22 日
講演タイトル: Data Breach and Vulnerability Assessment
イベント名: 東京大学公共政策大学院 ”Introduction to Cybersecurity for Policy Administrators” 第 7 回講義

2004 年から運用を開始した日本の脆弱性届出制度と情報セキュリティ早期警戒パートナーシップのこれまでと現状を振り返り、グローバルな脆弱性情報流通の変化について紹介しました。

講演日時: 4 月 24 日
講演タイトル: CERT コーディングスタンダードのご紹介
～脆弱性を生まないセキュアコーディングのために～
イベント名: コーディング技法で守るモビリティ社会のセキュリティ
（情報処理推進機構 ソフトウェア高信頼化センター）
http://sec.ipa.go.jp/seminar/20170424.html

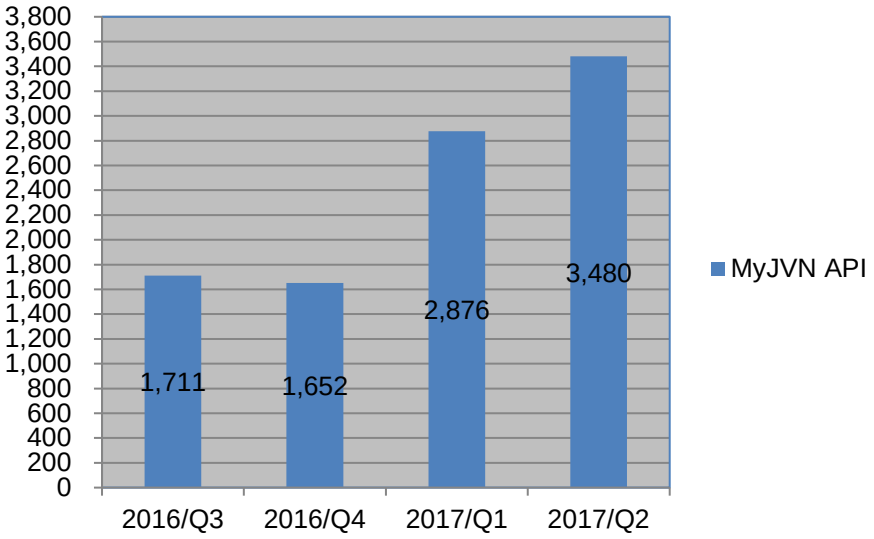
情報処理推進機構ソフトウェア高信頼化センター（IPA/SEC）が、自動車業界や組み込み分野に関係するソフトウェア技術者を対象に開催した、「コーディング技法で守るモビリティ社会のセキュリティ」と題したセミナーにおいて、JPCERT/CC は、CMU SEI の CERT 部門が作成しているコーディング規約集「SEI CERT コーディングスタンダード」の活動概要を紹介するとともに、JPCERT/CC で行っている日本語化の取り組みや日本語版について紹介しました。

2.4. VRDA フィードによる脆弱性情報の配信

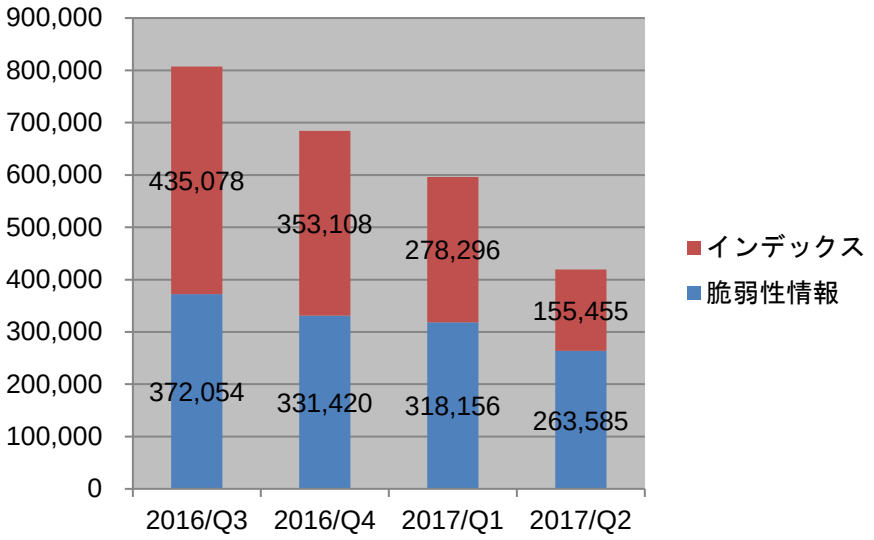
JPCERT/CC は、大規模組織の組織内 CSIRT 等での利用を想定して、KENGINE 等のツールを用いた体系的な脆弱性対応を可能とするため、IPA が運用する MyJVN API を外部データソースとして利用した、VRDA（Vulnerability Response Decision Assistance）フィードによる脆弱性情報の配信を行っています。VRDA フィードについての詳しい情報は、次の Web ページを参照ください。

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 2-6］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。

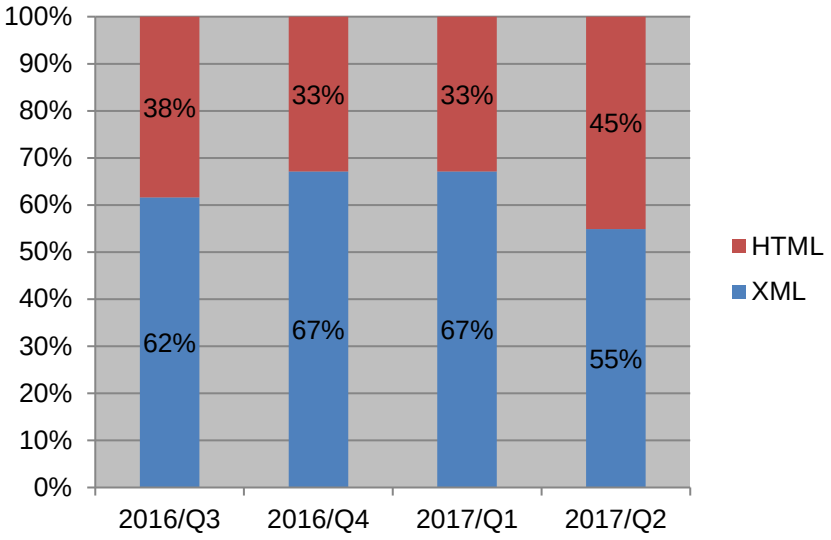


［図 2-5 VRDA フィード配信件数］



［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 44%減少しました。脆弱性情報の利用数についても、約 17%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、HTML 形式の割合が 12%増加しました。

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。本四半期で収集・分析した情報は 512 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 3 件でした。

2017/04/24 【参考情報】Bosch 社 車載製品の脆弱性について
2017/04/26 【参考情報】Hyundai Motor America 社 車載製品の脆弱性について
2017/06/13 【参考情報】2016 年のウクライナでのサイバー攻撃に使用されたマルウエアに関する情報

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。

2017-04-07　制御システムセキュリティニュースレター 2017-0003
2017-05-09　制御システムセキュリティニュースレター 2017-0004
2017-06-02　制御システムセキュリティニュースレター 2017-0005

制御システムセキュリティ情報共有コミュニティには、現在 713 名の方にご登録いただいています。今後も内容の充実を図っていく予定です。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 1 件（58IP アドレス）で、国内の研究者からの報告でした。インターネットからアクセスできる制御システム関連機器に関して注意を促して欲しいとの報告でした。
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。
以上に関する本四半期の情報提供は 17 件でした。

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 8 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 237 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 制御システムセキュリティアセスメントサービスの実施

JPCERT/CC は、日本国内の制御システムセキュリティの実態把握と利用組織におけるセキュリティの向上を目的として、2016 年 12 月より制御システムセキュリティアセスメントサービスを行っています。（2017 年 7 月現在、募集を行っておりません）
前四半期に事前調整と事前説明を行った 2 組織に対して、サイトアセスメントを実施しました。また、前四半期にサイトアセスメントを行った組織を含めた 5 組織に対して、サイトアセスメント結果と発見事項などをまとめたレポートの報告会を行いました。サービス開始から累計 6 組織に対してサイトアセスメントを行いました。

制御システムセキュリティアセスメントサービス
https://www.jpcert.or.jp/ics/ics-assessment.html

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、トレーニングやイベントでの講演等を通じた CSIRT の構築・運用支援を行っています。

4.1.1. アフリカ CSIRT 構築支援（5 月 24 日-25 日）

情報セキュリティに関する制度や技術が成長段階にある国・地域等からのサイバー攻撃は日本のインターネットユーザの脅威の一つとなります。急速なインターネット普及が予想されるアフリカ地域に起因するインシデントの増加に備え、事態が発生した際に迅速かつ円滑な対応ができるよう、同地域の育成と連携の基盤づくりを目的に、JPCERT/CC では 2010 年から CSIRT の構築・運営とそれらを支える人材の育成に取り組んできました。
その一環として本四半期においては、ケニアの首都ナイロビで開催された Africa Internet Summit（AIS）'17 に参加しました。AIS は AfNOG（African Network Operators' Group）と AFRINIC（The African Network Information Centre）が共同で主催する、アフリカのインターネットの発展に携わる産官学を対象としたイベントで、アフリカの ICT における技術動向や政策等に関して、現状や課題を国際コミュニティとともに協議することを目的に 2013 年から毎年開催されています。今年は 5 月 21 日から 6 月 2 日まで開催されました。
JPCERT/CC は、AfNOG のメンバーである AfricaCERT（Africa Computer Emergency Response Teams）

から依頼を受けて、AIS'17 の期間中の 5 月 24 日、25 日にログ解析トレーニングを行いました。本トレーニングには、ケニア、ナイジェリア、ガーナ等から約 20 名が参加しました。

［図 4-1　ログ解析トレーニング参加者との集合写真］

AIS'17 および AfricaCERT の詳細については、次の Web ページをご参照ください。

Africa Internet Summit '17
https://internetsummitafrica.org/

AfricaCERT
https://www.africacert.org/home/

4.2. 国際 CSIRT 間連携

インシデント対応における連携強化および各国のインターネット環境の整備や情報セキュリティ関連活動の取り組み状況の共有を目的として、海外の National CSIRT との連携を強化するための活動を行っています。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、継続して APCERT の事務局を担当しています。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 4 月 19 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。

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

JPCERT/CC は、FIRST の活動に 1998 年の加盟以来、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。本四半期は 4 月 3 日から 6 日にかけてクアラルンプール（マレーシア）で開催された理事会に出席し、組織運営に関わる議論に参画しました。
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 Technical Colloquium への参加（5 月 22 日）

5 月 22 日に青島（中国）で開催された Qingdao 2017 FIRST Technical Colloquium に参加し、各国の関連組織の活動事例や脅威情報共有の取り組みについて、情報を収集しました。イベントの詳細は、次の Web ページをご参照ください。

Qingdao 2017 FIRST Technical Colloquium
https://www.first.org/events/colloquia/qingdao2017

4.2.2.2. 29th Annual FIRST Conference San Juan への参加（6 月 11 日-16 日)

第 29 回 FIRST 年次会合が 6 月 11 日から 16 日にかけてプエルトリコのサンファンで開催されました。本会合は、サイバーインシデントの予防、対応、技術分析等に関する最新動向の情報交換およびインシデント対応チームの連携強化を目的に毎年開催されています。今年は ” Fighting Pirates and Privateers”のテーマの下に多種多様なトピックが取り上げられ、68 の国と地域から約 725 名が参加しました。

JPCERT/CC は、6 月 16 日に“APT Log Analysis - Tracking Attack Tools by Audit Policy and Sysmon -”と題して講演を行いました。マルウエアに感染したマシンを侵入の起点とし、組織内の至るところを侵害するようなサイバー攻撃では、多くの場合、攻撃者は特定のツールを使用しますが、この過程で、どこにどのようなログが残るのか、またどのような設定をすれば十分な情報を含むログを取得できるようになるのかを調査した研究結果を発表しました。

さらに、この機会を利用し、世界各国の National CSIRT や製品ベンダの CSIRT 等と個別に意見を交換するとともに、脆弱性ハンドリングや情報交換ポリシー等に関する SIG（Special Interest Group）やアジア太平洋地域の National CSIRT の集いに参加し、各分野の活動について情報を共有しました。このような会合への参加をとおした、各地域間の情報共有の促進や信頼関係の醸成によって、国際間でのインシデント対応調整がより円滑に進められるよう今後も活動してまいります。第 29 回 FIRST 年次会合についての詳細は、次の Web ページをご参照ください。

29th Annual FIRST Conference San Juan
https://www.first.org/conference/2017

4.2.3. 国際 CSIRT 間連携に係る国内外カンファレンス等への参加

4.2.3.1. CNCERT/CC 年次会合への参加（5 月 23 日-24 日）

5 月 23 日から 24 日にかけて青島で開催された CNCERT/CC（National Computer network Emergency Response technical Team / Coordination Center of China）の年次会合に参加し、中国でのインシデント動向や脅威動向、サイバーセキュリティの取り組み等に関する情報を収集しました。また、現在対応している案件等について、関連組織と意見交換を行いました。

4.2.3.2. CERT-EE Symposium 2017 への参加（5 月 29 日-30 日）

5 月 29 日から 30 日にかけてエストニアのタリンで CERT-EE（CERT Estonia）が主催する CERT-EE Symposium 2017 に参加し、北欧、バルト三国、東ヨーロッパ地域の CSIRT をはじめ、研究者や企業のサイバーセキュリティへの取り組み等について情報を収集しました。

4.2.3.3. The Global Commission on the Stability of Cyberspace（GCSC）公聴会への参加（6 月 2 日）

2017 年 3 月にサイバー空間における規範を議論する場として The Global Commission on the Stability of Cyberspace (GCSC) が立ち上がりました。その中に設けられた、複数の分野ごとにオープンな議論を行うことを目的とするワーキンググループの副議長に JPCERT/CC の小宮山が就任しております。6 月 2 日には、エストニアのタリンで当該分野の専門家を集めた GCSC の公聴会が開かれ、小宮山が一部のセッションのモデレータを務めました。GCSC の詳細は、次の Web ページをご参照ください。

The Global Commission on the Stability of Cyberspace (GCSC)
https://cyberstability.org/

4.2.3.4. National CSIRT Meeting（6 月 16-17 日）

第 29 回 FIRST 年次会合に引き続き、米国 CERT/CC が主催する National CSIRT Meeting（NatCSIRT）2017 がプエルトリコのサンファンで開催されました。本会合は、世界各国の National CSIRT が一堂に会し、国を代表するインシデント対応チームとしての活動計画や課題を共有し、開発ツールや共同プロジェクト、調査研究等に関して発表や議論することを目的に毎年開催されており、今年で 12 回目を迎えました。今回は 38 の国と地域から 83 名が参加しました。JPCERT/CC は、NatCSIRT の場でパネルセッションに参加し、日本の脆弱性ハンドリングの枠組みについて発表しました。NatCSIRT についての詳細は、次の Web ページをご参照ください。

NatCSIRT 2017
https://www.cert.org/natcsirt/

4.3. CyberGreen

CyberGreen は、インターネット全体の健全性とリスクを各国／地域間で比較可能にする指標を用いて、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と連携し、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に実施している国際的なプロジェクトです。
2015 年 11 月に設立された日本発の国際 NPO である CyberGreen Institute を中心にプロジェクトが推進されており、本四半期、JPCERT/CC では CyberGreen Institute とともに収集する計測データの質・量の増強やグリーンインデックスの計算方法・可視化等の改良を進めました。CyberGreen および CyberGreen Institute については、次の Web ページをご参照ください。

CyberGreen Institute
https://www.cybergreen.net/

4.4. 国際標準化活動

IT 分野の標準化を行うための組織 ISO/IEC JTC 1/SC27 で進められている情報セキュリティに関する技術の標準化のうち、作業部会 WG3（セキュリティの評価・試験・仕様）における脆弱性の開示と取り扱いに関する標準の改定活動と、WG4（セキュリティコントロールとサービス）におけるインシデント管理に関する標準の改定活動に情報処理学会の情報規格調査会を通じて参加しています。

今四半期は、4 月にニュージーランドのハミルトン市で開催された標準化会議に参加しました。

WG3 では、脆弱性の開示（ISO/IEC 29147）の改定標準の第 1 次 CD（委員会草案）について各国から提出されたコメントについて検討が行われ、DIS（国際標準草案）段階に進むことになりました。また、脆弱性の取扱手順（ISO/IEC 30111）については、事前に第 1 次 CD が用意されなかったため、進捗はなく、次回の国際会議から議論が始まることになります。

WG4 では、改定に伴いシリーズ化されたインシデント管理に関する一連の標準のうち、セキュリティオペレーションセンター（SOC）におけるインシデント管理について標準化を検討してきましたが、これについては検討を終了することになりました。一方、過去にプロジェクトがキャンセルされたインシデント対応のオペレーションに関するガイドライン（ISO/IEC 27035-3）について、適用範囲を見直し、再度標準化を行う方向で各国の合意が得られ、引き続き検討を行うことになります。

4.5. その他の活動ブログや 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。

RedLeaves - Malware Based on Open Source RAT （4 月 3 日）
http://blog.jpcert.or.jp/2017/04/redleaves---malware-based-on-open-source-rat.html

Volatility Plugin for Detecting RedLeaves Malware（5 月 2 日）
http://blog.jpcert.or.jp/2017/05/volatility-plugin-for-detecting-redleaves-malware.html

Fact-finding Report on the Establishment and Operation of CSIRTs in Japan（5 月 12 日）
http://blog.jpcert.or.jp/2017/05/fact-finding-report-on-the-establishment-and-operation-of-csirts-in-japan.html

Research Report Released: Detecting Lateral Movement through Tracking Event Logs（6 月 12 日）
http://blog.jpcert.or.jp/2017/06/1-ae0d.html

5. 日本シーサート協議会（NCA）事務局運営

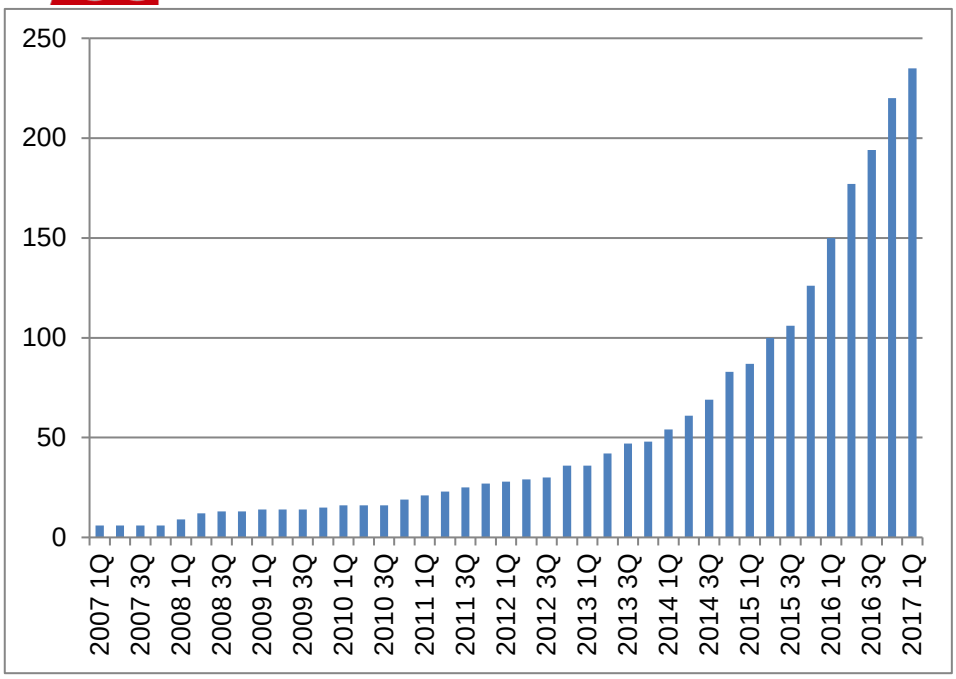
5.1. 概況

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、協議会の問合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 16 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。

小林製薬株式会社 (Kobayashi-SIRT)
清水建設株式会社 (Shimz-SIRT)
株式会社 資生堂 (Shiseido CSIRT)
株式会社ワンビシアーカイブズ (W-CSIRT)
SG ホールディングス株式会社 (SGH-CSIRT)
東京急行電鉄株式会社 (TKK-CSIRT)
ＮＴＴファイナンス株式会社 (NF-CSIRT)
株式会社　UR システムズ (URS-CSIRT)
遠州鉄道株式会社 (Entetsu-SIRT)
カブドットコム証券株式会社 (k.CSIRT)
ソニーペイメントサービス株式会社 (SPSV-CSIRT)
新日鐵住金株式会社 (NSG-CSIRT)
株式会社ＪＦＲ情報センター (JFRIC-CSIRT)
株式会社 Imperva Japan (Imperva JP-CSIRT)
株式会社東京証券取引所 (JPX-CSIRT)
国立大学法人　九州大学 (Qdai CSIRT)

本四半期末時点で 235 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 17 回シーサートワーキンググループ会

第 17 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 6 月 30 日
場所：近畿大学　東大阪キャンパス（KINDAI-CSIRT）

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方々が参加する会合です。会合では、4 つのワーキンググループの活動報告や、組織内シーサートの構築や運用に関する課題や意見の交換等が行われ、新しく加盟した 8 チームが自組織のシーサートの概要を紹介しました。
また、会場をお借りした近畿大学の井口 信和　教授から「本学の ICT の取組みについて」の講演をしていただきました。

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 回の運営委員会を開催しました。

第 119 回運営委員会
日時：2017 年 4 月 26 日（水）16:00 - 18:00
場所：JPCERT/CC

第 120 回運営委員会

日時：2017 年 5 月 31 日（水）16:00 - 18:00

場所：トレンドマイクロ株式会社

第 121 回運営委員会

日時：2017 年 6 月 28 日（水）16:00 - 18:00

場所：ヤフー株式会社

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・問合せの受付、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 21 件発信しました。

本四半期は、MUFG カードをかたるフィッシング事案が初めて報告されました。このほか、Amazon、Apple 等を含む E コマースサイトをかたりクレジットカード情報を詐取するフィッシングの報告が増加しています。特に Amazon や Apple の Web サイトは利用者数が非常に多いため、緊急情報を発行し注意を促しました。また LINE をかたるフィッシングについて、本四半期も継続して多くの報告が寄せられました。協議会では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。

また、合計 10 件の緊急情報を協議会の Web 上で公開し、広く注意を喚起しました。その内訳は次のとおりです。

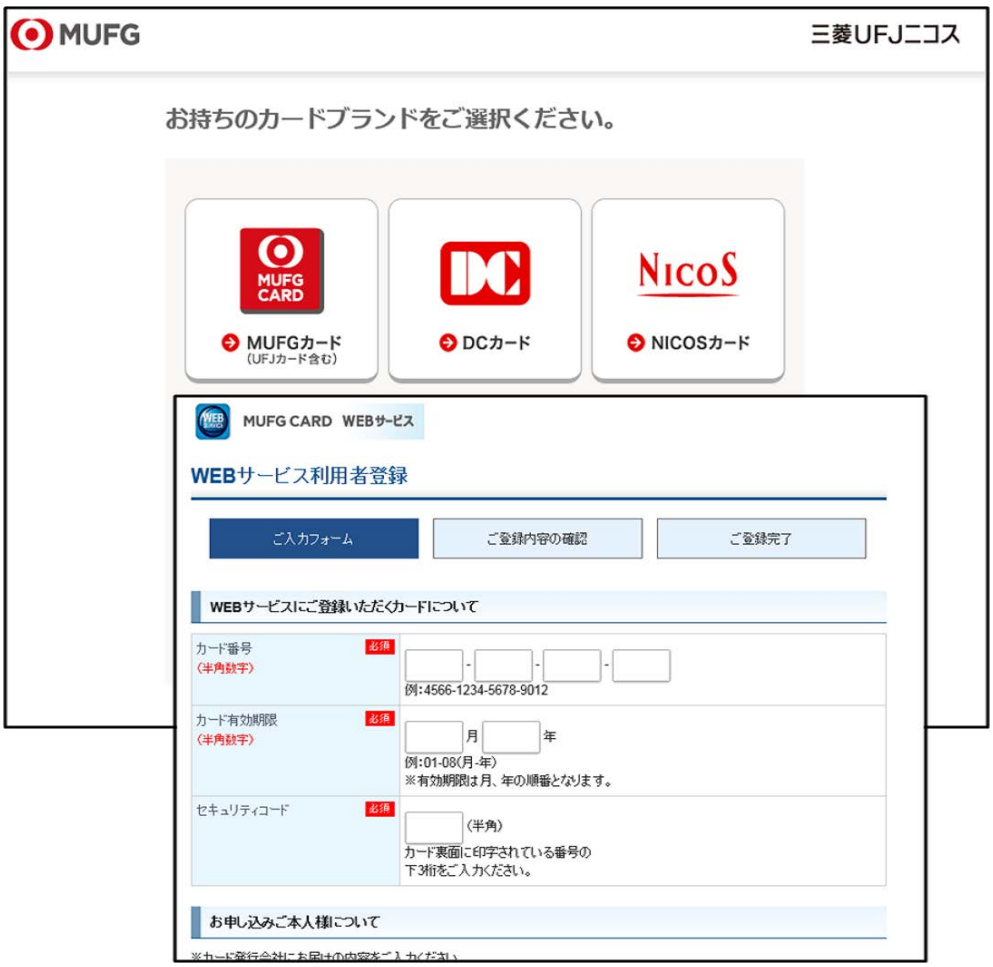
ライセンス更新をかたるフィッシング関連：1 件

SNS サービスをかたるフィッシング関連：1 件

クレジットカード会社をかたるフィッシング関連：5 件

E コマースサイトをかたるフィッシング関連：1 件

例として、［図 6-1］に[更新] MUFG カードをかたるフィッシング (2017/05/15)の注意喚起の内容を示します。



［図 6-1］[更新] MUFG カードをかたるフィッシング (2017/05/15)
https://www.antiphishing.jp/news/alert/mufgcard_20170515.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 23 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に関する動向を紹介し、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) 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）
「Phishing Trends in Japan and the Counteraction Taken as the Council of Anti-Phishing Japan」
Symposium on Electronic Crime Research, APWG , 2017 年 4 月 25 日

(2) 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）
「フィッシングの動向について 2017」
一般社団法人日本インターネットプロバイダー協会（JAIPA）地域 ISP 部会、2017 年 5 月 17 日

(3) 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）
「最新のフィッシングの動向 2017」
法務省・地方法務局職員セキュリティ研修、2017 年 5 月 24 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 4 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201704.html
フィッシング対策協議会 2017 年 5 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201705.html
フィッシング対策協議会 2017 年 6 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201706.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 49 回運営委員会
日時：2017 年 4 月 13 日 16:00 - 18:00
場所：NTT コミュニケーションズ株式会社

フィッシング対策協議会 第 50 回運営委員会
日時：2017 年 5 月 10 日 16:00 - 18:00
場所：株式会社日立システムズ

フィッシング対策協議会 第 51 回運営委員会
日時：2017 年 6 月 9 日 16:00 - 18:00
場所：トレンドマイクロ株式会社

7.2 フィッシング対策協議会　2017 年度総会

フィッシング対策協議会 2017 年度総会を次のとおり開催しました。

日時：2017 年 6 月 21 日 15:00 - 17:00
場所：エッサム神田ホール 2 号館 5 階会議室
議事：第 1 号議案　会則改定の件
第 2 号議案　運営委員選任の件
第 3 号議案　2016 年度決算報告書承認の件
第 4 号議案　2017 年度活動計画と会費収入の執行予算案承認の件
2018 年度に向けて会員種別の変更について
stopthinkconnect.jp サイト改ざんの報告とリニューアルサイトの紹介
APWG 「Symposium on Electronic Crime Research (eCrime 2017)」出張報告

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、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）等に基づき、2004 年 7 月からそれぞれ受付機関および調整機関として脆弱性関連情報流通制度の一端を担っています。
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 1 四半期（1 月～3 月）]
（2017 年 4 月 26 日）
https://www.jpcert.or.jp/press/2017/vulnREPORT_2017q1.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 1～3 月)
（2017 年 5 月 11 日）
https://www.jpcert.or.jp/tsubame/report/report201701-03.html
https://www.jpcert.or.jp/tsubame/report/TSUBAMEReport2016Q4.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 2 件の記事を公開しました。

(1) オープンソースの RAT を改良したマルウエア RedLeaves(2017-04-03)

2016 年以降、新たに標的型攻撃で確認されているマルウエア RedLeaves の動作の概要や、分析により判明した RedLeaves と PlugX との関連性、RedLeaves のベースとなった RAT について紹介しました。

オープンソースの RAT を改良したマルウエア RedLeaves(2017-04-03)
https://www.jpcert.or.jp/magazine/acreport-redleaves.html

(2) マルウエア RedLeaves を検知する Volatility Plugin(2017-05-02)

海外で観測されたマルウエア RedLeaves の感染事例では、自身を削除するためディスク上には存在せず、メモリ上やプロキシなどのネットワークから調査を行う必要がある点が言及されています。本記事では、RedLeaves への感染をメモリ上から発見するためのツールの公開（github で公開）および使用方法について紹介しました。

マルウエア RedLeaves を検知する Volatility Plugin(2017-05-02)
https://www.jpcert.or.jp/magazine/acreport-redleaves2.html

8.4 コラム「偽 JPCERT ドメイン名を取り戻すための 60 日間～ドメイン名紛争処理をしてみた～」

JPCERT/CC のものと錯誤されかねないドメイン名(jpcert.org)が何者かにより 2017 年 2 月 10 日に登録されたことが判明しました。これが悪事に使われることを懸念して、JPCERT/CC は紛争調停機関に申し立てを行い、当該ドメインを利用する権利を登録者から取り上げて獲得することに成功しました。同様の状況に陥った組織に参考にしていただけるよう、jpcert.org を JPCERT/CC の管理下とするまでの体験記を、ドメイン名紛争手続きのしくみの解説を交えしながらコラムとしてまとめました。

偽 JPCERT ドメイン名を取り戻すための 60 日間～ドメイン名紛争処理をしてみた～
https://www.jpcert.or.jp/column/udrp.html

9. 主な講演活動

(1) 椎木 孝斉（分析センター 分析センター長）：
「JPCERT/CC の活動と最近のサイバー攻撃の傾向」
「シマンテック　インターネットセキュリティ脅威レポート」記者発表会,2017 年 4 月 26 日

(2) 佐藤 祐輔（エンタープライズサポートグループ リーダー）：
「高度サイバー攻撃(APT)対応のための演習プログラム」
情報セキュリティ EXPO IPA ブース, 2017 年 5 月 10 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」
マネジメントシステム評価センター セミナー, 2017 年 5 月 12 日

(4) 洞田 慎一（早期警戒グループ マネージャー）：
「高等教育機関を狙うサイバー攻撃への対策」
私立大学キャンパスシステム研究会第六分科会, 2017 年 5 月 23 日

(5) 久保 啓司（インシデントレスポンスグループ マネージャー）：
「APT 攻撃への対応体制－インシデントレスポンスの現場から－」
日経 BP 経営課題解決シンポジウム, 2017 年 5 月 24 日

(6) 竹田 春樹（分析センター マネージャー）：
「実践インシデント対応 -侵入された痕跡を発見せよ-」
Internet Week ショーケース, 2017 年 6 月 2 日

(7) 洞田 慎一（早期警戒グループ マネージャー）：
「サイバー攻撃の傾向と対応について　Open Source Intelligence 概説」
警察大学校, 2017 年 6 月 8 日

(8) 真鍋 敬士（理事・最高技術責任者）：
「2020 年の CSIRT 間情報共有　～王道と覇道～」
Interop Tokyo2017, 2017 年 6 月 9 日

(9) 久保 啓司（インシデントレスポンスグループ マネージャー）：
「WannaCry がおしえてくれたこと」
Interop Tokyo2017, 2017 年 6 月 9 日

(10) 阿部 真吾（制御システムセキュリティ対策グループ 情報セキュリティアナリスト）、輿石 隆（早期警戒グループ 情報セキュリティアナリスト）：
「Hardening 1010 Cash Flow における JPCERT/CC について」
Hardening Project 2017, 2017 年 6 月 23 日

10. 主な執筆活動

(1) 小宮山 功一朗（国際部・エンタープライズサポートグループ マネージャー）：
「サイバー人材　アフリカに必要」
読売新聞社「論点」,2017 年 5 月 12 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) Internet Week ショーケースin名古屋

主　催：一般社団法人日本ネットワークインフォメーションセンター

開催日：2017年6月1日～2日

(2) Interop Tokyo 2017

主　催：Inlerop Tokyo実行委員会

開催日：2017年6月7日～9日

(3) 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

■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