JPCERT CC®

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, o=Japan Computer Emergency Response Team Coordination Center, cn=Japan Computer Emergency Response Team Coordination Center, email=office@jpcert.or.jp
日付 : 2018.07.11 10:38:41 +09'00'

JPCERT-PR-2018-02
発行日 : 2018-4-12

JPCERT/CC 活動概要 [2018 年 1 月 1 日 ～ 2018 年 3 月 31 日]

活動概要トピックス

ートピック1ー　インターネットリスク可視化サービス Mejiro を公開

JPCERT/CC は 1 月 29 日にインターネットリスク可視化サービス Mejiro を公開しました。本サービスは、セキュリティインシデントの発生や事態の深刻化を引き起こすリスク因子の分布状況を、国や地域ごとに、ネットワークのサイズで相対化した Mejiro 指標を利用して可視化することにより、地域 CSIRT などにおけるセキュリティ課題の優先度付けのための参考情報を提供します。現時点での Mejiro は、SHODAN や Censys から 8 種類のリスク要因の情報を得て、5 種類のビューで可視化した結果を表示しています。さらに役立つサービスになるよう、利用者から寄せられたご意見やご要望を参考に、リスク要因の種類や表示ビューの機能および情報源などを拡充していく予定です。

Mejiro の詳細については、本報告書の 4.3.1 および次の Web ページをご参照ください。

実証実験:インターネットリスク可視化サービス—Mejiro—
https://www.jpcert.or.jp/research/mejiro.html

ートピック2ー　Japan Security Analyst Conference 2018 （JSAC2018）を開催

2018 年 1 月 25 日、東京お茶の水で JPCERT/CC 主催の「Japan Security Analyst Conference 2018（JSAC2018）」を開催しました。日々発生しかつ刻々と変化するサイバー攻撃によるインシデントの分析・対応を行うセキュリティアナリストの技術力向上を目的としたカンファレンスで、今回が初めての試みとなりました。
インシデント分析・対応に関連した技術や知見が共有される場が国内で少なかった状況を踏まえ、日本国内のセキュリティアナリストの底上げ行うために、国内のセキュリティアナリストが一同に介し、インシデント分析・対応に関連する技術的な知見を共有し、日本全体でサイバー攻撃に対抗することが必要であるとの思いから本イベントを開催いたしました。参加受付開始当初から多くの方に申し込みをいただき、カンファレンス当日には当初の予定人数を超える 481 名に参加していただきました。

事前の講演募集（CFP）に応募していただいた 24 件の中から選定された 10 件について講演が行われました。それぞれの講演では、マルウエア分析やフォレンジックといったセキュリティインシデント分析・対応に関する技術に関して、講演者独自の新しい技術的な知見や、分析をサポートするために講演者によって開発された分析ツールの紹介などが発表されました。

なお、JSAC2018 の講演資料は一部の講演を除いて公開しているほか、カンファレンスの様子を紹介した分析センターだより（前編、後編）も公開しています。

JPCERT/CC では、JSAC2018 に多くの方に参加していただいた実績を踏まえ、JSAC の継続的な開催について検討する他、インシデント分析・対応に関連したコミュニティに有益な情報発信や活動を今後も引き続き実施していく予定です。

Japan Security Analyst Conference 2018
https://www.jpcert.or.jp/event/jsac2018.html

Japan Security Analyst Conference 2018 開催レポート~前編~(2018-02-08)
https://www.jpcert.or.jp/magazine/acreport-jsac2018report1.html

Japan Security Analyst Conference 2018 開催レポート~後編~(2018-02-16)
https://www.jpcert.or.jp/magazine/acreport-jsac2018report2.html

ートピック3ー　制御システムセキュリティカンファレンス 2018 を開催

2018 年 2 月 7 日（水）に東京浅草橋で「制御システムセキュリティカンファレンス 2018」を開催しました。本カンファレンスは 2009 年 2 月から毎年開催してきており、今回で 10 回目を迎えました。前回開催した品川から会場を変更して定員が増えた今回は、290 名以上の方々にご来場いただきました。今年度はランサムウエアによる被害が国内の制御システムで発生したとの報道もあって関心が高く、参加申込数は来場募集の案内を行ってから早々に定員を超えました。制御システム利用会社のセキュリティ担当者や制御システムセキュリティに関するコンサルタント会社などから最新の制御システムセキュリティに関する情報や対策事例などを講演いただきました。参加者の所属による内訳は、アセットオーナが 33%、制御システム機器ベンダが 11%、システムベンダが 17%、エンジニアリング会社が 12%、研究者が 5%となりました。

制御システムセキュリティカンファレンス 2018
https://www.jpcert.or.jp/event/ics-conference2018.html

制御システムセキュリティカンファレンス 2018 講演資料
https://www.jpcert.or.jp/present/#year2018

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. 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 3,786 件、インシデント件数ベースでは 3,857 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 2,203 件でした。前四半期の 1,901 件と比較して 16%増加しています。「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/2018/IR_Report20180412.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 924 件で、前四半期の 852 件から 18%増加しました。また、前年度同期（707 件）との比較では、31%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	1 月	2 月	3 月	本四半期合計（割合）
国内ブランド	78	58	72	208(23%)
国外ブランド	174	212	178	564(61%)
ブランド不明 (注 5)	45	41	66	152(16%)
全ブランド合計	297	311	316	924(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。

前四半期と同様に、特定の海外ブランドのアカウント窃取を目的としたフィッシングサイトに関する報告が多く寄せられています。異なる見た目でありながら、同じサービスのアカウントを窃取するフィッシングサイトが複数確認されています。一つのフィッシングサイトが停止した後、同じサーバ上で新たに異なる見た目のフィッシングサイトが確認されるなど、攻撃者が共通していると見られるものもありました。

国内ブランドのフィッシングサイトでは、通信事業者、SNS、金融機関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サイトでは、ある 2 つのブランドに関する報告が多く、一方は海外の Web サイト作成サービスに設置され、もう一方は WordPress を使ったサイトに設置されるといった傾向が見られました。SNS を装ったフィッシングサイトは、ブランド名に 2、3 文字の英小文字を連結した.cn ドメインを使用したものが、本年度は継続して確認されています。金融機関を装ったフィッシングサイトでは、クレジットカード情報の窃取を目的としたものが大半を占めました。

フィッシングサイトの調整先の割合は、国内が 30%、国外が 70%であり、前四半期（国内 25%、国外 75%）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、268 件でした。前四半期の 276 件から 3%減少しています。

本四半期は、Google Chrome からアクセスしてきたユーザに不審なサイトへの誘導やポップアップの表示を行う、不正な JavaScript が埋め込まれる改ざんを確認しました。不審なポップアップが表示される改ざんとしては、Chrome のフォントパックのアップデートを装ってランサムウエアをダウンロードさせ、実行させるものが 2 月に確認されました。同様の手法は 2017 年 1 月ごろにも確認されていましたが、本

四半期には以前とは異なる種類のランサムウエアがダウンロードされるようになっていました。3 月に複数の国内サイトに埋め込まれていた JavaScript は、ページ上をクリックするとロシア語の国際化ドメイン名を使用した URL に誘導する仕組みになっていましたが、確認した時点では誘導先が名前解決できない状態になっており、どのような脅威があるかは分かりませんでした。改ざんされたサイトは CMS を使用しているものが多く、脆弱性を悪用した攻撃や、管理画面から不正にログインされてファイルを設置されることによって、不正なスクリプトを埋め込まれた可能性が考えられます。

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、6 件でした。前四半期の 9 件から 23%減少しています。本四半期は、対応を依頼した組織はありませんでした。

国内の複数の組織において、組織で利用しているクラウドサービスに不正にログインされ、サービスの悪用によるメールの送信や、クラウドストレージ上のファイルへのアクセスが行われたといった内容のインシデントが発生しており、本四半期に情報が寄せられました。

同様の被害を受けたいくつかの組織には、組織の認証ポータルを装ったフィッシングサイトに誘導するフィッシングメールが、他の国内組織から送り付けられていました。また、フィッシングメールの送信元になっていた組織も、以前に類似のフィッシングの被害を受けている場合がありました。クラウドサービスに不正にログインされた被害組織の調査では、攻撃者が一度の情報入力でログインに成功している形跡が確認されており、フィッシングなどで窃取したアカウント情報を使用して、不正アクセスを行った可能性があります。

不正アクセスは、海外のホスティングサービスや、匿名ネットワーク Tor のノードと見られる IP アドレスなどから行われていたことを確認しています。これらの IP アドレスの情報を国内の被害組織に共有したところ、いくつかの組織において、共通の海外 IP アドレスからのアクセスが見つかりました。

JPCERT/CC では、類似の被害を受けた複数の組織と連携し、攻撃の調査や、関連する組織への情報の展開を実施しています。

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 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。本四半期に発行したお知らせはありませんでした。

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：16 件（うち 4 件は更新情報）　https://www.jpcert.or.jp/at/

2018-01-10　Adobe Flash Player の脆弱性 (APSB18-01) に関する注意喚起 (公開)
2018-01-10　2018 年 1 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)
2018-01-11　Adobe Flash Player の脆弱性 (APSB18-01) に関する注意喚起 (更新)
2018-01-17　2018 年 1 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)
2018-01-17　ISC BIND 9 の脆弱性に関する注意喚起 (公開)
2018-01-17　Oracle WebLogic Server の脆弱性 (CVE-2017-10271) に関する注意喚起 (公開)
2018-02-02　Adobe Flash Player の未修正の脆弱性 (CVE-2018-4878) に関する注意喚起 (公開)
2018-02-07　Adobe Flash Player の未修正の脆弱性 (CVE-2018-4878) に関する注意喚起 (更新)

2018-02-14　2018 年 2 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)
2018-02-14　Adobe Reader および Acrobat の脆弱性 (APSB18-02) に関する注意喚起 (公開)
2018-02-27　memcached のアクセス制御に関する注意喚起 (公開)
2018-02-28　memcached のアクセス制御に関する注意喚起 (更新)
2018-03-12　Mirai 亜種の感染活動に関する注意喚起 (更新)
2018-03-14　Adobe Flash Player の脆弱性 (APSB18-05) に関する注意喚起 (公開)
2018-03-14　2018 年 3 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)
2018-03-29　Drupal の脆弱性 (CVE-2018-7600) 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。本四半期における発行は次のとおりです。

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 70 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。

2018-01-11　担当者が選ぶ 2017 年重大ニュース
2018-01-17　Wi-Fi Alliance が WPA3 の概要を公開
2018-01-24　サイバーセキュリティ月間
2018-01-31　STOP. THINK. CONNECT. 啓発イベント
2018-02-07　IPA が「情報セキュリティ 10 大脅威 2018」を発表
2018-02-15　Weekly Report 2018-02-07 号に関するお詫び
2018-02-21　JPCERT/CC が「SSDP の応答情報を活用した Mirai 亜種感染機器の特定方法」を公開
2018-02-28　総務省が「サイバーセキュリティに関する総務大臣奨励賞」の受賞者の公表
2018-03-07　memcached のアクセス制御に関する注意喚起
2018-03-14　フィッシング対策協議会が「フィッシングサイトの早期検知に関する研究」を公開
2018-03-22　警察庁が「仮想通貨採掘ソフトウェア「Claymore（クレイモア）」を標的としたアクセスの増加等について」を公開
2018-03-28　警察庁が「平成 29 年中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

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：5 件　https://www.jpcert.or.jp/newsflash/

2018-02-09　Adobe Acrobat および Adobe Acrobat Reader のセキュリティアップデート予告について
2018-03-14　複数の Adobe 製品のアップデートについて
2018-03-19　BIND の "update-policy local;" の動作仕様変更について
2018-03-28　Apache Struts 2 の脆弱性 (S2-056 / CVE-2018-1327) について
2018-03-28　OpenSSL のアップデートについて

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) 分散型メモリキャッシュシステムとして使われる memcached のアクセス制御に関する情報発信
2018 年 2 月 21 日頃から 11211/UDP の通信ポートに対するスキャン活動が増加しており、JPCERT/CC においても外部組織からの情報提供およびインターネット定点観測システム (TSUBAME) の観測よりこの事象を確認しました。
当該通信ポートへのスキャン活動の通信を分析し、本スキャン活動が memcached を探すために行われている可能性があると推測しました。また、memcached を踏み台に悪用したとみられる DDoS 攻撃の報告が外部組織から JPCERT/CC にありました。
そうした攻撃の拡大が懸念されたため、JPCERT/CC では 2018 年 2 月 27 日に、memcached のアクセス制御に関する注意喚起を公開し、memcached の適切なアクセス制御の設定を呼びかけました。

memcached のアクセス制御に関する注意喚起
https://www.jpcert.or.jp/at/2018/at180009.html

(2) Adobe Flash Player の未修正の脆弱性に関する情報発信
KrCERT/CC より 2018 年 1 月 31 日に Adobe Flash Player の脆弱性 (CVE-2018-4878) に関する注意喚起が公開されました。その後、本脆弱性が韓国における標的型攻撃に使用されていたとの情報が海外の Web サイト上で公開され、また、アドビ社からは本脆弱性を修正したバージョンの公開予定が発表されました。

JPCERT/CC では、本脆弱性がリモートからのコード実行を可能にする脆弱性であり、さらに実際に本脆弱性が攻撃に利用されていることを踏まえ、2018 年 2 月 2 日に注意喚起を発行して、回避策の検討や修正バージョン公開後の速やかな適用を呼びかけました。

また、アドビ社から 2018 年 2 月 6 日（現地時間）に本脆弱性を修正したバージョンが公開されたため、注意喚起を更新し、早期の対策を呼びかけました。

Adobe Flash Player の未修正の脆弱性 (CVE-2018-4878) に関する注意喚起
https://www.jpcert.or.jp/at/2018/at180006.html

(3) Oracle WebLogic Server の脆弱性に関する情報発信
2017 年 10 月 18 日に修正バージョンが公開された Oracle WebLogic Server の脆弱性(CVE-2017-10271) について、2017 年 12 月頃、実証コードが公開され、本脆弱性を狙ったとみられるスキャンが増加しました。
JPCERT/CC でも本脆弱性を悪用した攻撃の報告を受け取っており、公開されている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、サーバ実行ユーザ権限で任意のコードを実行できることを確認しました。そのため、2018 年 1 月 17 日に、Oracle WebLogic Server の脆弱性 (CVE-2017-10271) に関する注意喚起を公開し、対策を呼びかけました。

Oracle WebLogic Server の脆弱性 (CVE-2017-10271) に関する注意喚起
https://www.jpcert.or.jp/at/2018/at180004.html

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。
2018 年 3 月末時点で、海外の 20 の経済地域の 26 組織に観測用センサーの設置への協力をいただいています。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、海外の 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

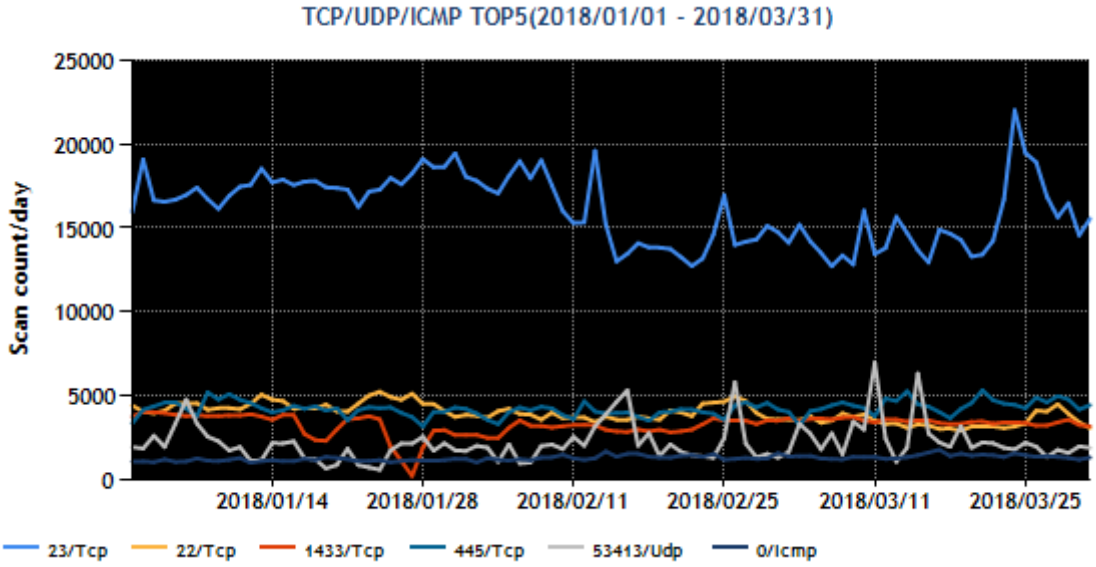
1.3.1. インターネット定点観測システム TSUBAME の観測データの活用

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 10 月から 12 月分のレポートを 2018 年 1 月 18 日に公開しました。

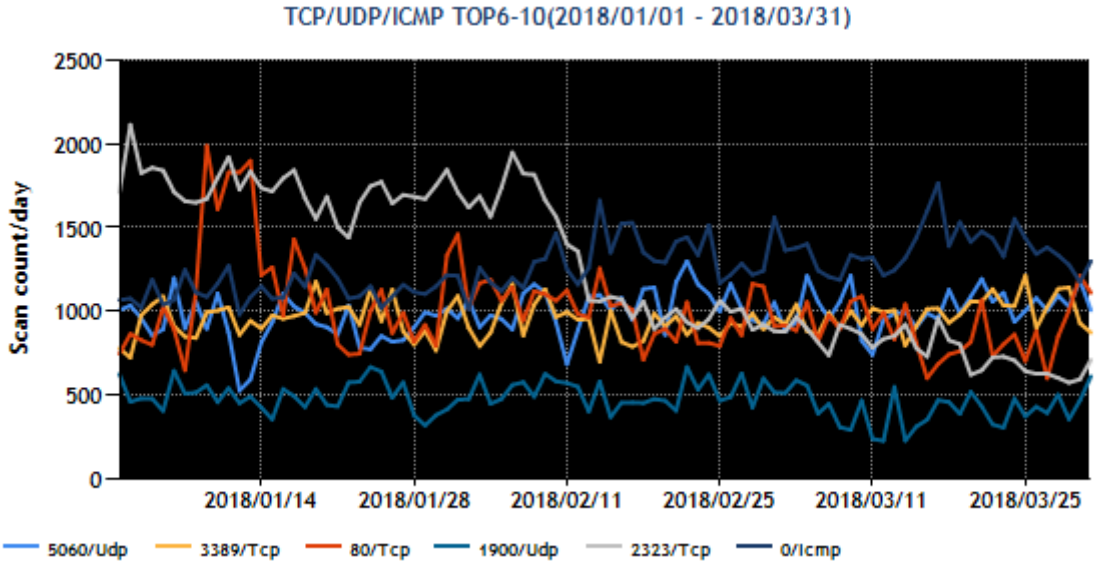
TSUBAME 観測グラフ
https://www.jpcert.or.jp/tsubame/index.html#examples
インターネット定点観測レポート（2017 年 10～12 月）
http://www.jpcert.or.jp/tsubame/report/report201710-12.html

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。

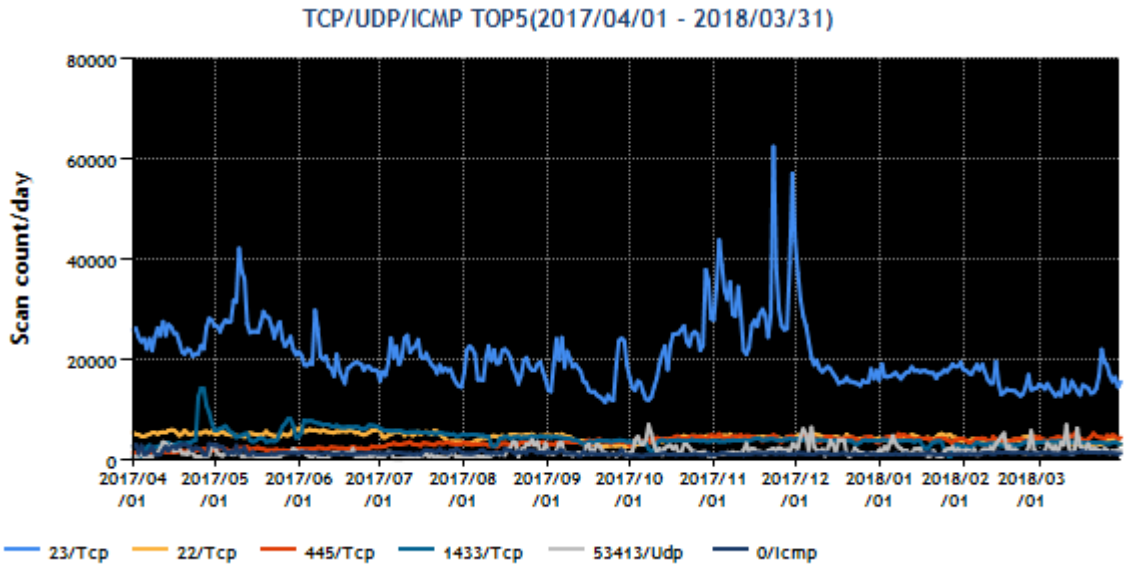


［図 1-1 宛先ポート別グラフ トップ 1-5（2018 年 1 月 1 日-3 月 31 日）］

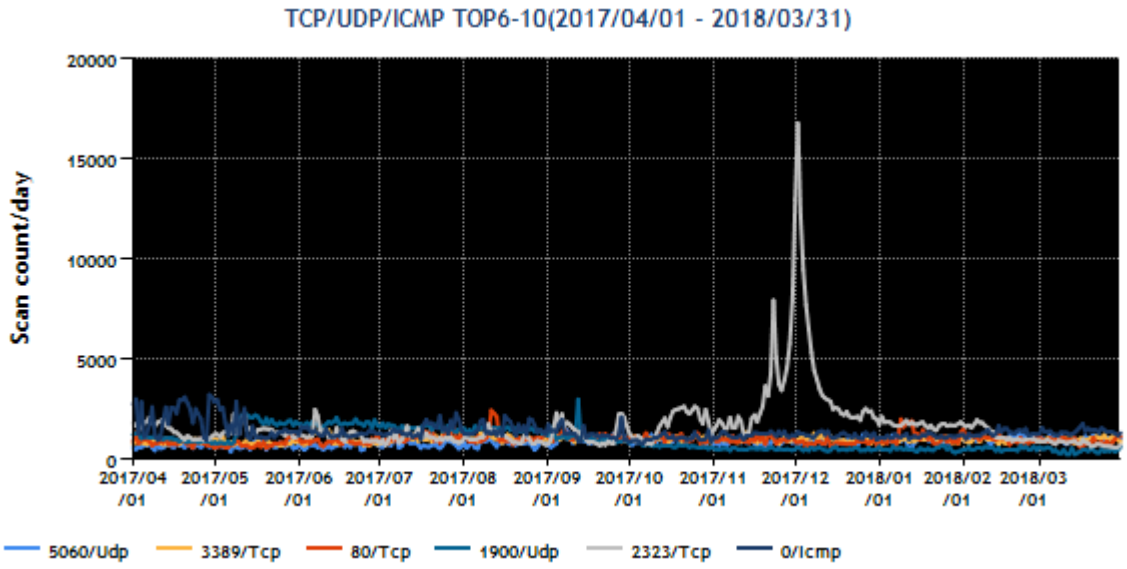


［図 1-2 宛先ポート別グラフ トップ 6-10（2018 年 1 月 1 日-3 月 31 日）］

また、過去 1 年間（2017 年 4 月 1 日-2018 年 3 月 31 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（2018 年 4 月 1 日-2018 年 3 月 31 日）］



［図 1-4 宛先ポート別グラフ トップ 6-10（2017 年 4 月 1 日-2018 年 3 月 31 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。2017 年 11 月頃から観測されていた、国内ベンダ製ルータが Mirai 等のマルウエアに感染して送信する 23/TCP や 2323/TCP 宛のパケットは、対策や機器の入れ替えなどが行われたため、パケットの送信元 IP アドレス数が徐々に減少しているようです。一方で、監視カメラやルータ、NAS といった専用機器から送信されたパケット数の減少は見られませんでした。送信元の機器が変わりましたが、本四半期も先四半期とほぼ同水準の数のパケットの送信が観測されました。

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応を行っています。本四半期における事例として、仮想サーバを管理するハイパーバイザーの管理 Web インターフェース経由で侵入されたインシデントについて次に述べます。

日本国内のある IP アドレスから、主に VNC サーバが使用すると思われるポートを探索する活動が 1 月中旬から TSUBAME で観測されました。当該 IP アドレスの管理者に連絡したところ、試験用に設置していた仮想サーバのインフラが侵害を受けていることがわかり、対応をしたとの返信を受領しました。報告によると、実際の運用とは異なるアクセス制御をして仮想サーバを試験的に使用していたところ、攻撃者に侵入されてしまったとのことでした。

このように JPCERT/CC では、観測したパケットの分析等を行い、必要に応じて関連する機器の管理者に調査を依頼するなど、感染した機器の発見やマルウエアの駆除等の、対策に努めています。

1.3.4. TSUBAME トレーニングの実施

本四半期は、台湾の CSIRT（TWNCERT, TWCERT/CC, EC-CERT）向けに、次の要領で TSUBAME トレーニングを実施しました。

日時：2018 年 1 月 19 日（金）
場所：台北
参加人数：27 名（TWNCERT、TWCERT/CC、 EC-CERT のメンバーが参加）
トレーニングの内容：
- TSUBAME プロジェクトの概要
- 機器や機器を対象とした探索活動の現状
- 演習
- 意見交換

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。

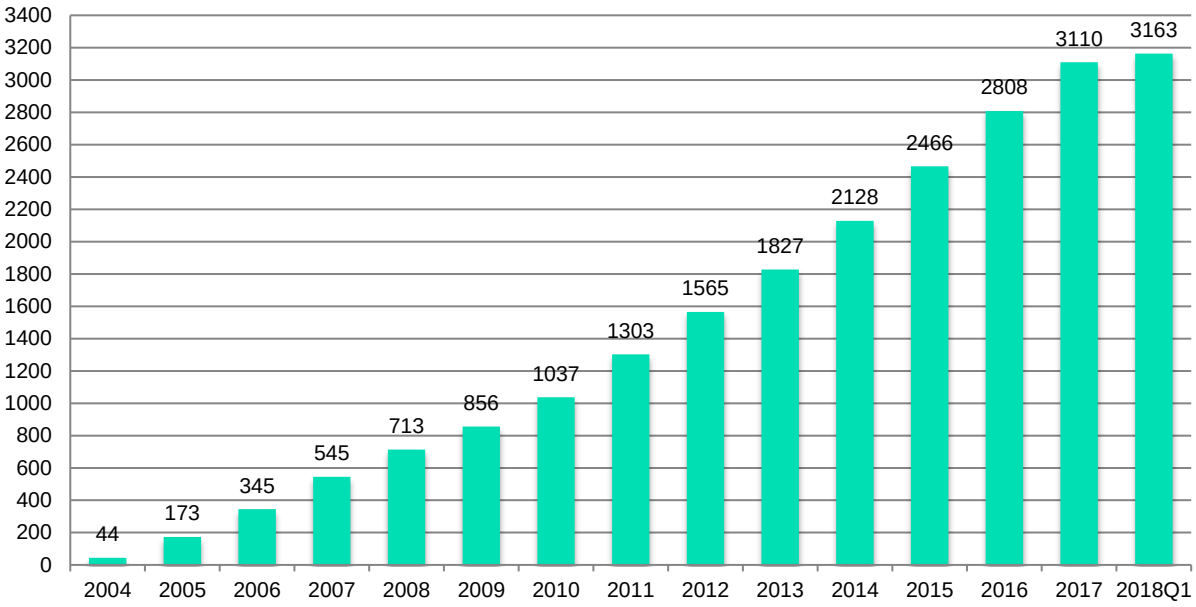
独立行政法人情報処理推進機構（IPA）脆弱性対策
https://www.ipa.go.jp/security/vuln/

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］を付与している）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］を付与している）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 53 件（累計 3,163）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/



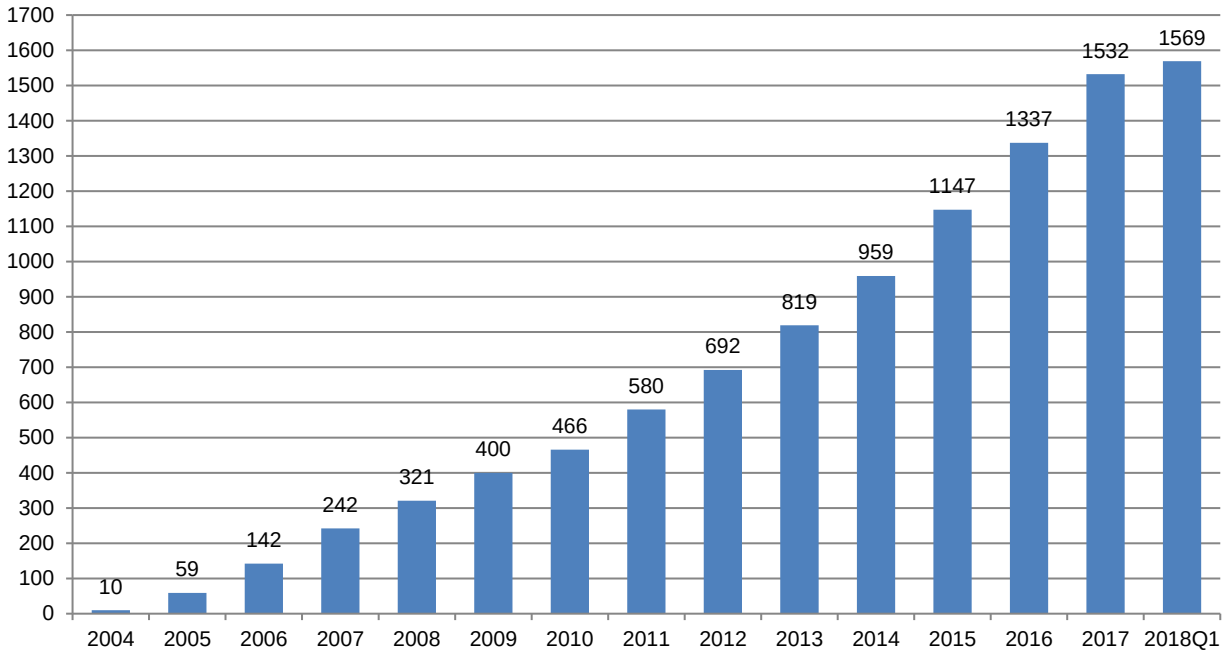
［図 2-1 JVN 公表累積件数］

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 37 件（累計 1,569 件）で、累計の推移は［図 2-2］に示すとおりです。本四半期に公表した 37 件すべてが単一の製品開発者の製品だけに影響を及ぼすもので、うち 29 件が国内製品開発者に関わるもの、8 件が海外の製品開発者に関わるかかわるものでした。また、29 件の国内製品開発者の製品に関する脆弱性情報のうち、1 件が自社製品の届出によるものでした。また国内製品開発者に関わる 29 件のうち 9 件が連絡不能開発者の提供する製品に関する公表でした。連絡不能開発者に関する詳細は、本報告書［2.1.3. 連絡不能開発者とそれに対する対応の状況等］に記載しています。

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 10 件と最も多く、次いでウェブアプリケーションが 6 件でした。Windows アプリケーションに関する公表は、2017 年第 2 四半期から非常に多く、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」と同じ仕組みで起こる Windows アプリケーションの脆弱性が多数みられました。これは、特定の発見者が、さまざまな Windows アプリケーションに対し同一の脆弱性が存在しないかを検証し、再現が確認されたものが順次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	10
ウェブアプリケーション	6
組込系	5
プラグイン	4
サーバ製品	3
Android アプリ	2
iOS アプリ	1
ウェブアプリケーションフレームワーク	1
ウェブブラウザ	1
開発ツール	1
グループウエア	1
データ処理ツール	1
フォームメール	1
計	37



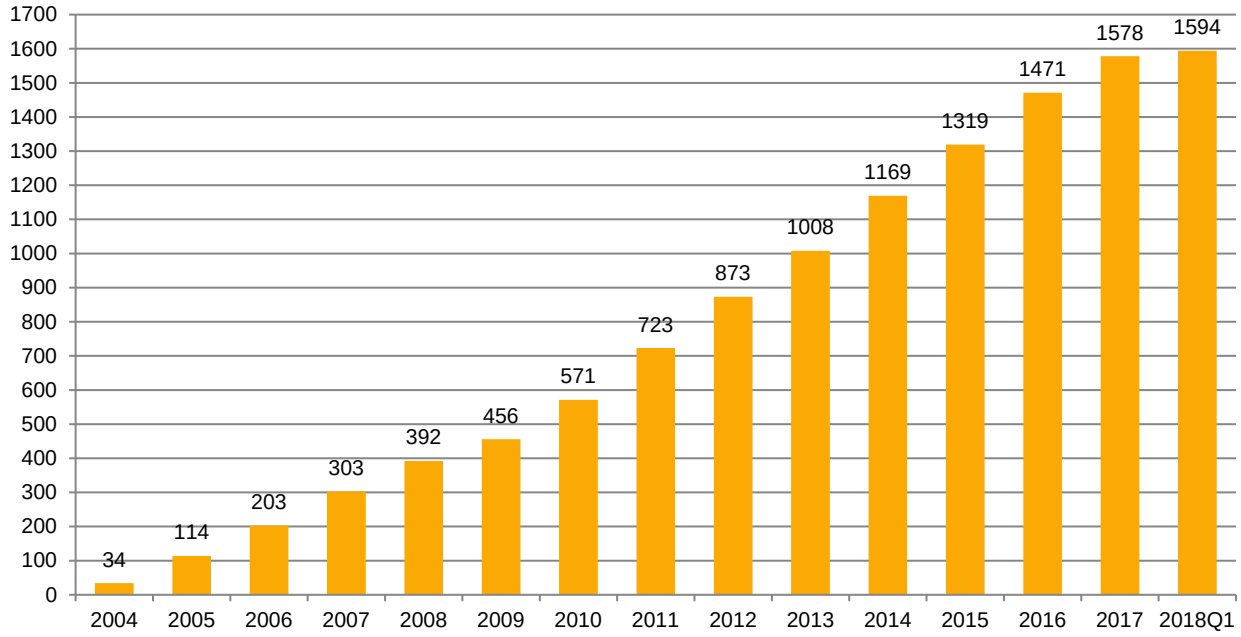
［図 2-2 公表を行った国内取扱脆弱性情報の累積件数］

本四半期に公表した国際取扱脆弱性情報は 16 件（累計 1,594 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。本四半期は、macOS アプリに関するものが 3 件と最も多く、前四半期に続き、DNS、ウェブサーブレットコンテナ、ライブラリ、サーバ製品、プロトコル実装、といった製品開発に使用されるソフトウエアやその実装に関する脆弱性の公表は合わせて 9 件ありました。
本四半期において特に目立った脆弱性は、米国 CERT/CC が 1 月 4 日に公表した「JVNVU#93823979 CPU に対するサイドチャネル攻撃」です。この情報は公表当日に翻訳し JVN にて公表しています。この脆弱性は、幅広いサービスや製品に影響を及ぼすことから、JVN 公表後、JPCERT/CC 製品開発者登録をしている複数の製品開発者へ通知し、ベンダ情報の掲載や情報提供等を呼びかけました。このほか本四半期の特徴として、16 件中 7 件の公表が製品開発者自身による脆弱性情報の公表依頼に基づくものであったことが挙げられます。このように、JPCERT/CC では、米国 CERT/CC をはじめとする海外調整機関に届け出られた脆弱性情報の日本国内への展開や調整、製品開発者自身からの告知を目的とした公表依頼の受付など、脆弱性情報の流通、調整および公表を幅広く行っています。

［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
macOS アプリ	3
DNS	2
ウェブサーブレットコンテナ	2
サーバ製品	2
VPN ソフトウエア	1
Windows OS	1
組込系	1
制御系製品	1
プロトコル	1
プロトコル実装	1
ライブラリ	1
計	16



［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、48 件（製品開発者数で 28 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 203 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場合、IPA が招集する公表判定委員会が妥当と判断すれば、公表できることに 2014 年から制度が改正されました。2015 年に 2 案件を公表し、2015 年以降、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きました。2017 年度においては、12 月に開催された公表判定委員会で 4 件が審議され、公表準備中であった 5 件と併せすべて公表すべきと判定されたため、2018 年 3 月 13 日に、これら 9 件を JVN にて公表しました。

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 14 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 45 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。

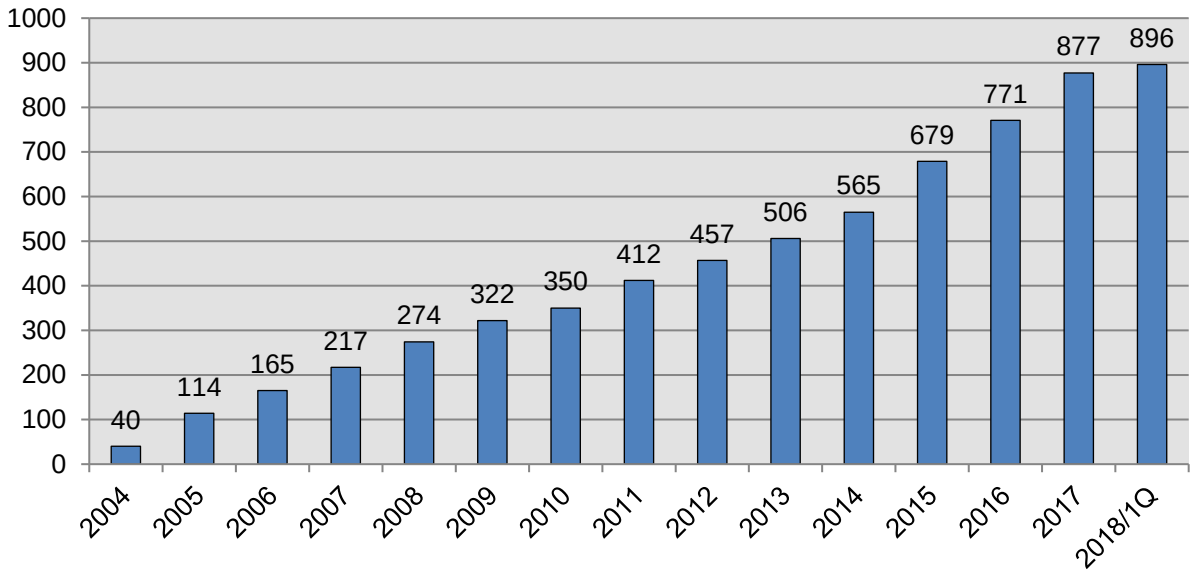
脆弱性情報取扱体制
http://www.meti.go.jp/policy/netsecurity/vulhandlingG.html
脆弱性情報コーディネーション概要
https://www.jpcert.or.jp/vh/

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、2018 年 3 月 31 日現在で 896 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. 製品開発者との定期ミーティングの実施

JPCERT/CC では、技術情報やセキュリティ・脆弱性の動向などの情報交換や、脆弱性情報ハンドリング業務に関する製品開発者との意見交換、また、製品開発者間の情報交換を目的として、脆弱性情報ハンドリングにご協力いただいている製品開発者の皆さまとのミーティングを定期的に開催しています。
2018 年 3 月 23 日に開催したミーティングでは、脆弱性の取り扱い状況、政府機関および重要インフラ事業者向けの情報提供の取り組み、製品開発者における脆弱性対応事例、CSAJ/Software ISAC の活動紹介等のトピックを中心にプログラムを構成し、各テーマについて講演と意見交換を行いました。

［図 2-5 製品開発者との定期ミーティングの様子］

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

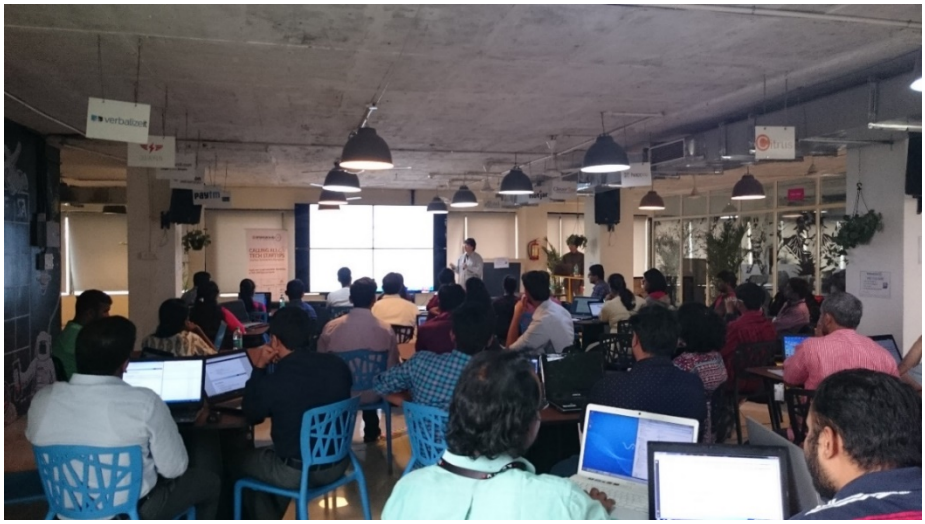
情報流通対策グループでは、脆弱なソフトウエアの解析等を通じて得られた脆弱性やその対策方法に関する知見を、広く一般のソフトウエア開発者の方々に伝えるための活動を行っています。

本四半期は、次の 1 件の講演を行いました。

講演日時: 2 月 12 日（デリー）、2 月 15 日（ベンガルール）
講演タイトル: Android Secure Coding
イベント名: Workshop on Android Security & Secure Coding

インドの national CERT である CERT-In の協力のもと、インドのデリーおよびベンガルールにて Android セキュアコーディングセミナーを実施しました。
半日コースとして企画したこのセミナーでは、最初に Android アプリを巡るセキュリティ動向を紹介した後、具体的な脆弱性事例やその対策としてのコーディングテクニックについて解説しました。さらに、脆弱性を作り込んだサンプルアプリを参加者に配布し、コードレビューにより脆弱性を発見し修正案を検討する演習を行いました。

［図 2-6 デリーでのセミナーの様子］



［図 2-7 ベンガルールでのセミナーの様子］

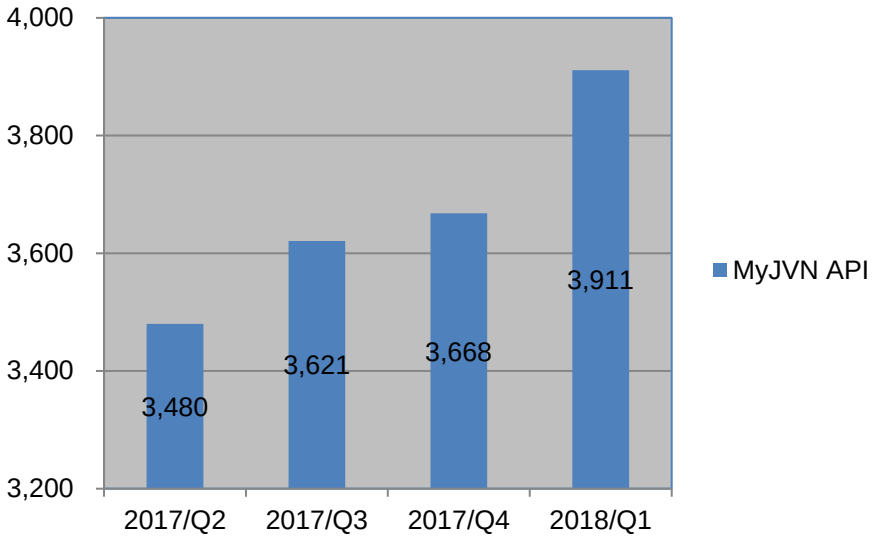
デリーのセミナーでは政府関係組織の方々の参加が多く、ベンガルールのセミナーではスタートアップ企業で働くエンジニアの方々に多く参加いただきました。セミナーの内容は、Activity や Content Provider の export 設定、ローカルファイルの取り扱い、証明書検証、WebView コンポーネントの使用上の注意など、Android アプリ開発を日々行っているエンジニアにとってはごく基本的な内容でしたが、どちらのセミナーにおいても、講義から演習まで熱心に取り組んでいただきました。

2.4. VRDA フィードによる脆弱性情報の配信

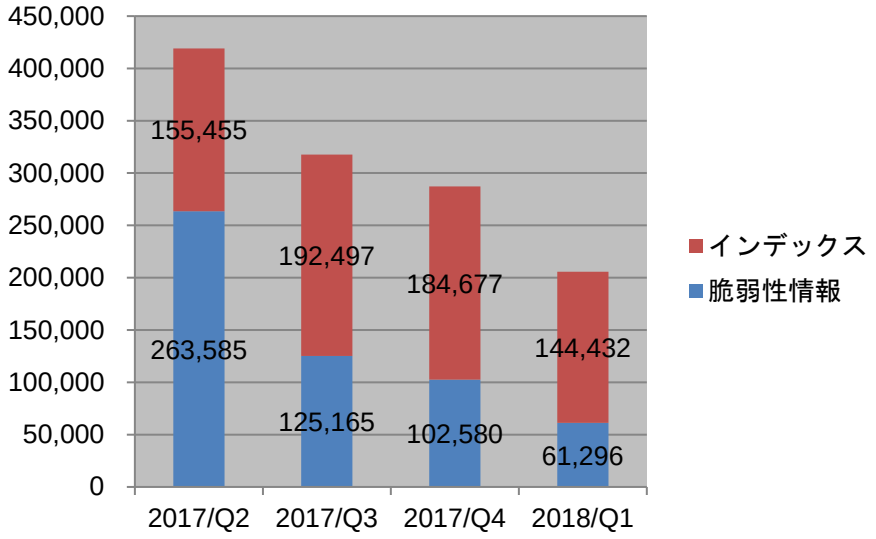
JPCERT/CC は、大規模組織の組織内 CSIRT 等での利用を想定して、ツールを用いた体系的な脆弱性対応を可能とするため、IPA が運用する MyJVN API を外部データソースとして利用した、VRDA（Vulnerability Response Decision Assistance）フィードによる脆弱性情報の配信を行っています。VRDA フィードについての詳しい情報は、次の Web ページを参照ください。

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 2-8］に、VRDA フィードの利用傾向を［図 2-9］と［図 2-10］に示します。［図 2-10］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 2-10］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。

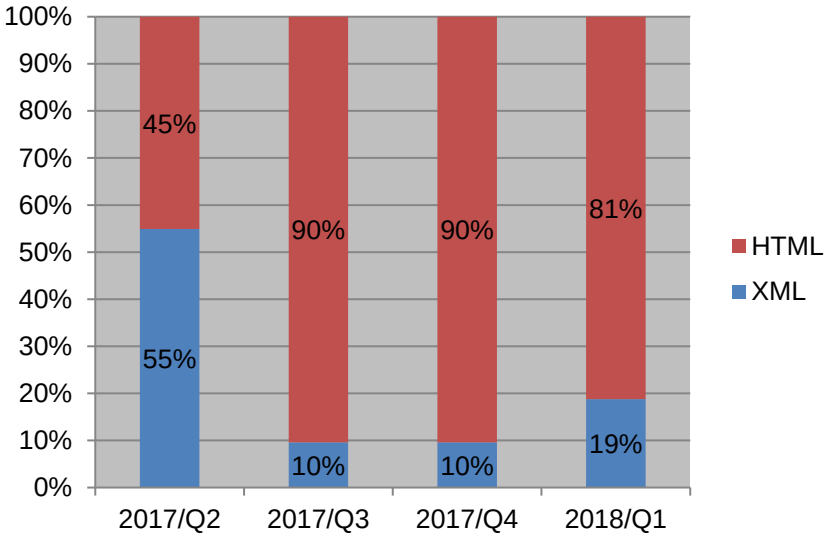


［図 2-8 VRDA フィード配信件数］



［図 2-9 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 2-9］に示したように、前四半期と比較し、約 22%減少しました。脆弱性情報の利用数についても、約 40%減少しました。



［図 2-10 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 2-10］に示したように、前四半期と比較し、目立った変化は見られませんでした。

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 367 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。

2018/02/22 【参考情報】ライセンス管理システムに関する脆弱性
2018/03/19 【参考情報】米国エネルギー業界およびその他重要インフラを標的としたサイバー活動について (TA18-074A)
2018/03/20 【参考情報】サウジアラビアの石油化学工場へのサイバー攻撃について

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。

2018/01/12　制御システムセキュリティニュースレター 2017-0012
2018/02/05　制御システムセキュリティニュースレター 2018-0001
2018/03/07　制御システムセキュリティニュースレター 2018-0002

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 824 名の方にご登録いただいています。今後も各サービスの充実を図り、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

JPCERT/CC は、制御システム関連のインシデント対応の分野で、インシデント報告の受付、およびインターネットからアクセスできる可能性がある制御システムの探索とそれら制御システムを保有している国内の組織に対する情報提供の 2 つの活動を展開しています。本四半期における活動は次のとおりです。

(1) インシデント報告の受付

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。

(2) インシデント未然防止活動

SHODAN をはじめとするインターネット・ノード検索システムで公開されている情報を分析し、インターネット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が含まれていないかを調査しています。本四半期に発見した 8 件（15 IP アドレス）のシステムの情報を、それぞれのシステムを保有する国内の組織に対して提供しました。

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 9 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 257 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カンファレンス 2018 の開催

2018 年 2 月 7 日（水）に東京浅草橋で、290 名を超える方々にご来場いただき、「制御システムセキュリティカンファレンス 2018」を開催しました。本カンファレンスは 2009 年 2 月から毎年開催しており、今回で 10 回目を迎えました。今年度はランサムウエアによる被害が国内の制御システムで発生したとの報道もあって関心が高く、定員を上回る参加申込をいただきました。昨年に続き、講演の一部を公募し、制御システムにおけるサイバー脅威の動向や、自己評価ツール結果に基づく制御システム利用企業におけるセキュリティ対策の取り組み、新しい技術の研究開発などでプログラムを構成しました。詳細については次の Web ページをご参照ください。

制御システムセキュリティカンファレンス 2018
https://www.jpcert.or.jp/event/ics-conference2018.html

制御システムセキュリティカンファレンス 2018 講演資料
https://www.jpcert.or.jp/present/#year2018

［図 3-1 制御システムセキュリティカンファレンス 2018 講演風景］

［表 3-1 制御システムセキュリティカンファレンス・プログラム構成］

(1)「IPA 産業サイバーセキュリティセンターが目指す先」 独立行政法人情報処理推進機構　田辺　雄史
(2)「制御システム・セキュリティの現在と展望～この 1 年間を振り返って～」 JPCERT/CC　顧問　宮地　利雄
(3)「産業用ロボットのセキュリティリスク検証からみえること」 トレンドマイクロ株式会社　上田　勇貴
(4)「制御システムにおけるサイバーリスクマネジメント態勢の確立と事例紹介」 KPMG コンサルティング株式会社　保坂　範和
(5)「生産工場制御システム向けサイバー攻撃対策の取組み～JPCERT アセスメント推進事例～」 大陽日酸株式会社　中辻　利一
(6)「制御システムにおける Deception System と早期警戒網について」 JPCERT/CC　阿部　真吾

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・運用支援を行っています。本四半期は新規の研修教材の開発を進めました。

4.1.1. JICA 情報セキュリティ能力向上研修における CSIRT 運用支援（2 月 2 日）

JPCERT/CC は、カンボジア、インドネシア、ミャンマー、パプアニューギニア、フィリピン、タイ、ベトナムの 7 ヶ国の National CSIRT や関係組織の IT 担当者 11 名を対象に、独立行政法人国際協力機構（JICA）が開催した「ASEAN 地域のサイバー セキュリティ対策強化のための政策能力向上」の実施に協力し、研修生を JPCERT/CC に招いて JPCERT/CC の活動、重要インフラ防護や標的型攻撃への取り組み、最新のインシデント動向等について講義し、National CSIRT としての活動状況について理解を深めていただきました。

4.1.2. ネパールにおける研修実施（2 月 22 日）

2018 年 2 月 22 日にネパールの首都カトマンズで Information Technology Security Emergency Response Team Nepal（ITSERT-NP）に対して Open Source Intelligence（OSINT）のトレーニングを行いました。ITSERT-NP のコミュニティに参加している組織のメンバー12 人に対して OSINT の概論の講義とバングラデシュ中央銀行の不正送金事件を題材にした OSINT ワークショップを行いました。ネパールの銀行も 2017 年 10 月に不正送金の被害にあっており、参加者は熱心に研修に取り組みました。

4.2. 国際 CSIRT 間連携

国境をまたいで発生する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、1 月 16 日に電話会議を、また APRICOT 2018 の開催にあわせて 2 月 23 日にカトマンズで会議をそれぞれ行い、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. APCERT メンバーとしての会議出席

2 月 19 日から 28 日にかけてカトマンズで、アジア太平洋地域におけるインターネット運用技術者に向けた国際会合である APRICOT 2018 が開催され、その一環として 2 月 24 日に FIRST Technical Colloquium（TC）が実施されました。APCERT メンバーとして FIRST TC の運営をサポートしました。APRICOT 2017 および FIRST TC についての詳細は、次の Web ページをご参照ください。

APRICOT 2017
https://2018.apricot.net/

Ho Chi Minh City 2017 FIRST Technical Colloquium
https://2018.apricot.net/program/schedule/#/day/6/first-tc-plenary

4.2.1.3. APCERT サイバー演習（APCERT Drill）2017 への参加（3 月 7 日）

本演習は、アジア太平洋地域で発生し、国境を越えて広範囲に影響を及ぼすインシデントへの対応における CSIRT 間の連携の強化ならびにサイバー攻撃を受けた際により迅速に対応するための APCERT 加盟組織の能力の向上を目的として、毎年実施されています。
14 回目となる今回のサイバー演習は「IoT に関するマルウエアによって引き起こされるデータ漏洩」をテーマに実施されました。脆弱性を悪用して IoT 機器を感染させてボットネットを形成し、それを踏み台として大規模な DDoS 攻撃を仕掛ける Mirai マルウエアなど、IoT 機器を利用した新たな脅威が広まっています。今回はこうした状況を踏まえて、テーマが設定され、演習シナリオが作成されました。参加組織は関係する組織とのインシデント情報のやり取りやマルウエアおよびログの分析など、インシデント対応の手順を確認しました。本演習には、APCERT 加盟組織のうち 20 経済地域から 27 チーム、および OIC-CERT（The Organisation of the Islamic Cooperation - Computer Emergency Response Teams）からエジプト、ナイジェリア、パキスタン、モロッコ、オマーンの 5 チームが参加しました。
JPCERT/CC は、APCERT 事務局ならびに演習ワーキンググループ（Drill Working Group）のメンバーとして、シナリオの議論や運営において主導的な役割を果たしました。また、プレーヤー（演習者）として参加するとともに、コントローラ（Exercise Control: ExCon）と呼ばれる演習の進行調整役も務めました。
APCERT Drill 2018 についての詳細は、次の Web ページをご参照ください。

APCERT Drill 2018 – Data Breach via Malware on IoT
http://www.apcert.org/documents/pdf/APCERTDrill2018PressRelease.pdf

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 の国際部マネージャ 小宮山功一朗が FIRST の理事を務めており、本四半期は 2 月 5 日から 9 日にかけてハンブルグで、3 月 12 日から 13 日に大阪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。また四半期に一度開催されるシンポジウムの準備調整を進めました。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 PSIRT Technical Colloquium 2018 への参加（2 月 27 日-28 日）

2 月 27 日から 28 日にかけてアトランタで開催された FIRST PSIRT Technical Colloquium 2018 に参加し、製品の脆弱性に対応する PSIRT（製品セキュリティインシデント対応チーム）の活動の取り組みについて発表を聴講しました。また参加している PSIRT と主に JPCERT/CC が行う脆弱性情報ハンドリングに関する情報共有を行いました。FIRST PSIRT Technical Colloquium 2018 の詳細については、次の Web ページをご参照ください。

PSIRT Technical Colloquium 2018
https://www.first.org/events/colloquia/atlanta2018/

4.2.2.2. Osaka 2018 FIRST Technical Colloquium 参加（3 月 14 日-16 日）

3 月 14 日から 16 日にかけて大阪で開催された Osaka 2018 FIRST Technical Colloquium に参加しました。JPCERT/CC は、Global Vulnerability Reporting Summit にて脆弱性ハンドリング業務について講演したほか、プログラム委員として当日の運営をサポートしました。Osaka 2018 FIRST Technical Colloquium の詳細は次の Web ページをご参照ください。

Osaka 2018 FIRST Technical Colloquium
https://www.first.org/events/colloquia/osaka2018/

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。前四半期より、JPCERT/CC は、CyberGreen Institute が収集したデータに対し、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っていますが、本四半期においても継続して提案を行いました。

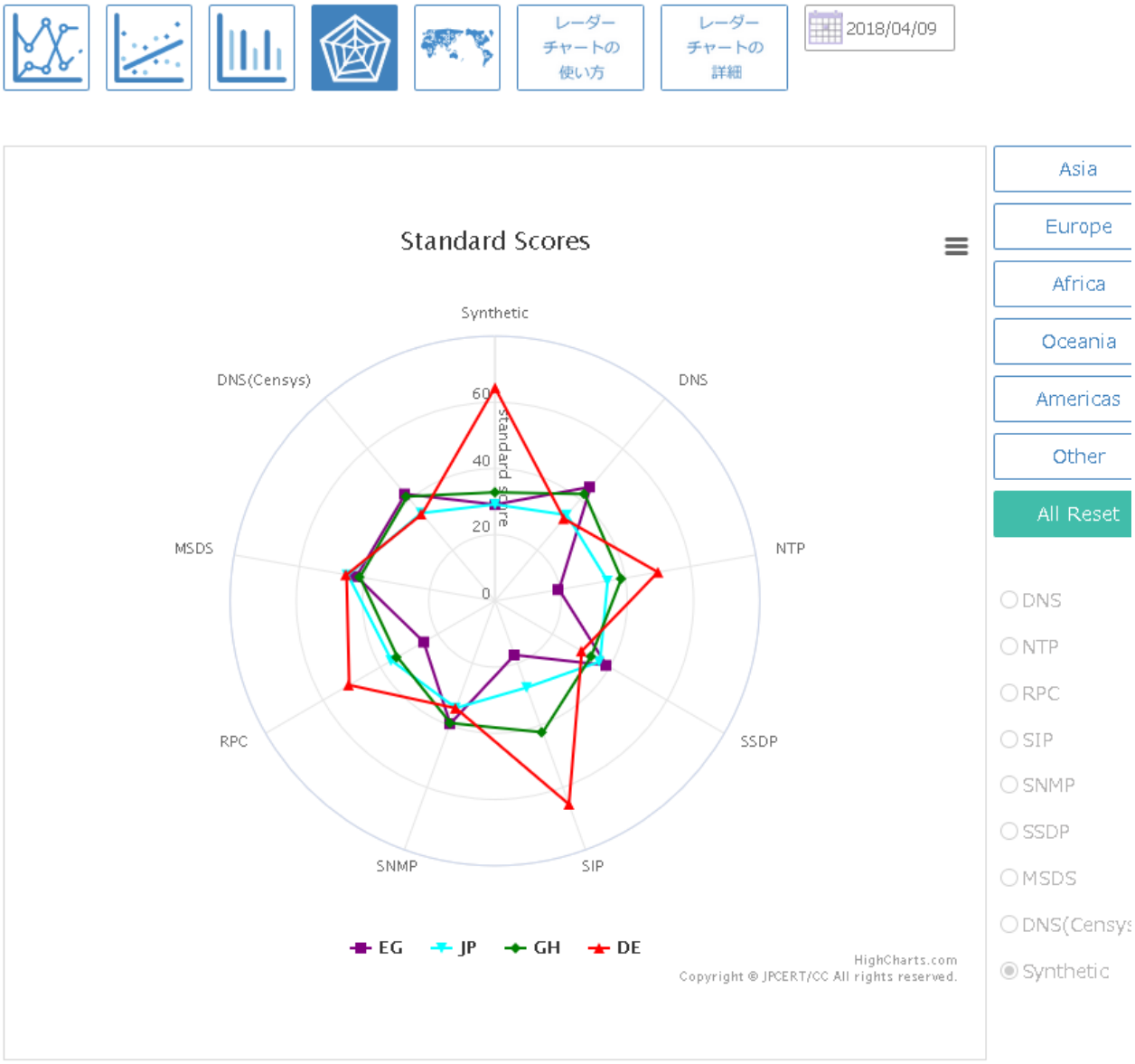
CyberGreen Institute については、次の Web ページをご参照ください。
https://www.cybergreen.net/

4.3.1. インターネットリスク可視化サービス Mejiro

1 月 29 日にインターネットリスク可視化サービスを提供するポータル Mejiro を公開しました。インターネット上には、サイバー攻撃の踏み台あるいは標的とされやすいなど、サイバー・インシデントの引き金となり事態を深刻化させる、さまざまなリスク要因が存在しています。こうしたリスク要因が国・地域ごとに、どの程度散在しているかを可視化し表示する Web サービスが Mejiro です。現時点では、悪用されることの多い 6 種類（DNS,NTP,RPC,SIP,SNMP,SSDP）のリフレクション型 DDoS 攻撃の踏み台となり得る機器と、WannaCry などのワームに感染しやすい特定の Windows の脆弱性を持つ機器を、表示対象のリスク要因とし、SHODAN から 7 種類（DNS,NTP,RPC,SIP,SNMP,SSDP,MSDS）、Censys から 1 種類（DNS）の計 8 種類の情報を得て表示しています。

国・地域ごとに、リスク要因の数の対数値を縦軸、割り当てられた IP アドレスの数の対数値を横軸として、両対数グラフ上にプロットすると回帰直線からの乖離の分布が正規分布に近いことに着目して、回帰直線からの乖離の偏差値を「Mejiro 指標」と名付け、Mejiro での可視化に使うことにしました。Mejiro 指標を用いることにより、国・地域のインターネット接続機器の多少によらず同じ土俵でリスク要因の多少を国・地域間で比較することができるようになるとともに、リスク要因の多少が他の国・地域と比較した相対値として表現されることになるので、リスク要因ごとの Mejiro 指標を比較することにより、当該国・地域において注力すべきセキュリティ課題の優先度付けにも役立つと期待されます。

現在のところ、Mejiro では 5 種類のビューによる可視化機能を提供しています。時系列グラフ（期間でのリスク要因の増減）と、散布図（リスク要因の数と IP アドレスの数）、ヒストグラム（指標値の分布を見る）、レーダーチャート（指標値を比較する）、ワールドマップバブル（世界地図上での指標値）です。例



［図 4-1 Mejiro のレーダーチャート表示］

として、エジプトと日本、ガーナ、ドイツの 4 ヶ国のリスク要因を Mejiro のレーダーチャートで表示した結果を［図 4-1］に示します。このように、割り当てられている IP アドレスの数の比が 100:50:10:1 と大きく異なっている日本とドイツ、エジプト、ガーナの 4 つの ccTLD 間で、9 種類のリスク要因それぞれの相対的に期待される水準に対する実態を直感的に比較評価することができます。

JPCERT/CC では、地域 CSIRT が Mejiro を活用することにより、インターネット全体のリスク要因の低減に向けて、相互にグッド・プラクティスを学び合い切磋琢磨していくことを願って Mejiro を公開しま

した。Mejiro の機能については、利用者からのご意見やご要望を参考に、引き続き拡充を図っていく予定です。

4.4. その他国際会議への参加

4.4.1. イスラエル CyberTech への参加および講演（1 月 30-31 日）

1 月 29 日から 31 日かけて、テルアビブで開催された CyberTech に参加しました。会期中に開かれた”Tomorrow World Cyber Management”の分科会にて JPCERT/CC の活動について講演しました。

4.4.2. 海外 CSIRT 等の来訪および往訪

4.4.2.1. CERT-IL 往訪（1 月 31 日）

CERT-IL（イスラエルコンピュータ緊急対応チーム）を往訪し、今後の協力関係等について議論を行いました。同組織は FIRST のメンバーとしても活動しており、イスラエルでの今後のイベント開催などについて協議しました。

4.4.2.2. VNCERT 往訪（3 月 8 日）

VNCERT（ベトナムコンピュータ緊急対応チーム）を往訪し、今後の能力構築支援等について意見交換を行い、今後も活動を通して密な連携を維持していくことを確認しました。

4.5. 国際標準化活動

IT セキュリティ分野の標準化を行うための組織 ISO/IEC JTC-1/SC27 で進められている標準化活動のうち、作業部会 WG3（セキュリティの評価・試験・仕様）で検討されている脆弱性の開示と取り扱いに関する標準の改定と、WG4（セキュリティコントロールとサービス）で検討されているインシデント管理に関する標準の改定に、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。

昨年 10 月末から 11 月初旬にかけてベルリンで開催された標準化会議において合意された方針に基づいて、脆弱性の開示（ISO/IEC 29147）と脆弱性の取扱手順（ISO/IEC 30111）の改定草案をプロジェクト・エディタが修正し、事務局を通じて配布することになっていました。しかしながら、この作業が遅れており、修正草案の配布がないまま次の標準化会議を 4 月に迎えることになりそうです。

4.6. 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。

Investigate Unauthorised Logon Attempts using LogonTracer（1 月 25 日）
http://blog.jpcert.or.jp/2017/11/visualise-event-logs-to-identify-compromised-accounts---logontracer-.html

Identify Mirai Variant Infected Devices from SSDP Response（2 月 20 日）
http://blog.jpcert.or.jp/2017/12/research-report-released-detecting-lateral-movement-through-tracking-event-logs-version-2.html

Malware “TSCookie”（3 月 6 日）
http://blog.jpcert.or.jp/2018/03/malware-tscooki-7aa0.html

5. 日本シーサート協議会（NCA）事務局運営

5.1. 概況

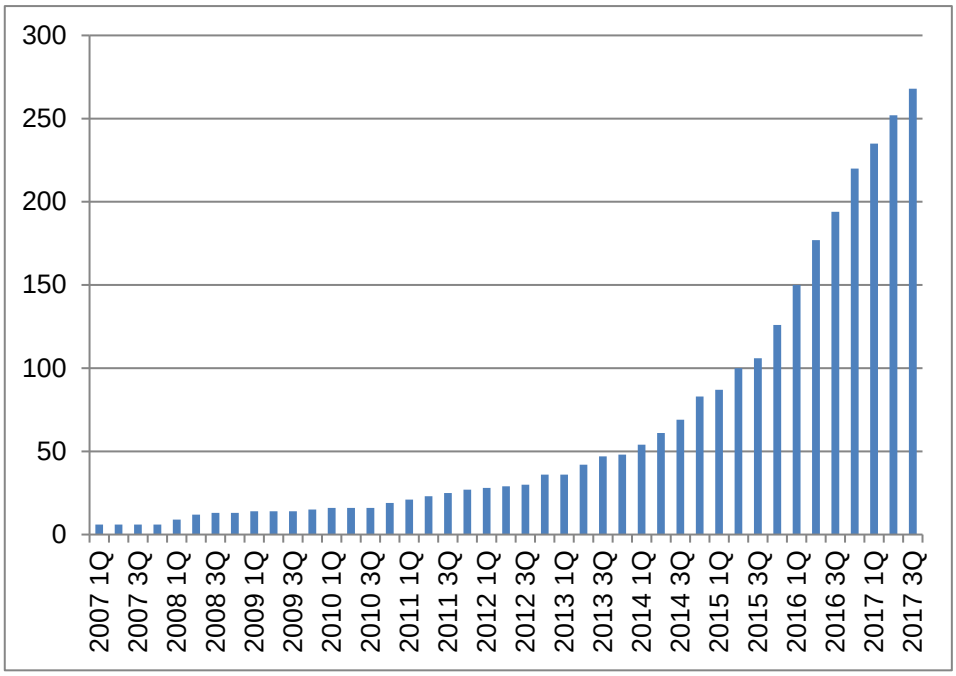
日本シーサート協議会（NCA：Nippon CSIRT Association）は、国内のシーサート（CSIRT：Computer Security Incident Response Team）組織が互いに協調し、連携して共通の問題を解決する場として 2007 年に設立されました。その事務局として、JPCERT/CC は、NCA の Web サイトの管理や更新を通じた広報活動、協議会の問合せ窓口やメーリングリストを含む会員情報の管理、加盟のためのガイダンスの実施および手続きの運用を担当するとともに、自らも会員として協議会の活動に参加しています。さらに、2016 年 8 月からは運営委員としても JPCERT/CC 職員（山本 健太郎）が NCA の運営に携わっています。

本四半期には、次の 17 組織（括弧内はシーサート名称）が新規に NCA の一般会員となりました。

トヨタコネクティッド株式会社 (TC-SIRT)
株式会社 LIXIL (LIXIL-CSIRT)
NTT テクノクロス株式会社 (TX-CSIRT)
株式会社　ビックカメラ (BICSIRT)
共同印刷株式会社 (TOMOWEL-CSIRT)
株式会社ＡＩＲＤＯ (ADO-CSIRT)
株式会社ワコールホールディングス (Wacoal-SIRT)
慶應義塾大学(WIDE プロジェクト) (WIRT)
一般財団法人 国際ビジネスコミュニケーション協会 (IIBC-SIRT)
国立大学法人 九州工業大学 (Kyutech CSIRT)
KNT CT ホールディングス株式会社 (KNT-CT CSIRT)
株式会社オージス総研 (OGIS-CSIRT)
オムロン株式会社 (OMRON-SIRT)
都築電気株式会社 (TSUZUKI-CSIRT)
オリックス株式会社 (ORIX-SIRT)

株式会社クボタ (Kubota-CSIRT)
ポケットカード株式会社 (PCC-CSIRT)

本四半期末時点で 284（一般会員 283、オブザーバ 1）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 20 回シーサートワーキンググループ会

第 20 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：2018 年 3 月 26 日
場所：大崎ブライトコアホール

シーサートワーキンググループ会は、NCA の会員および NCA 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 16 チームによる自組織のシーサートの概要紹介に加えて、次の講演がおこなわれました。

演題　：「インシデント対応訓練手法検討 WG の活動紹介～机上演習ガイドと NISC/NCA 連携演習の活用に向けて～」
講演者：Fuji Xerox CERT 増田 佳弘 氏、Canon-CSIRT 羽場 満 氏

5.3. 日本シーサート協議会　運営委員会

本四半期は、次のとおり計 3 回の運営委員会を開催しました。

第 128 回運営委員会
開催日時：2018 年 1 月 24 日（水）16:00 - 18:00
開催場所：NTT-CERT

第 129 回運営委員会
開催日時：2018 年 2 月 21 日（水）16:00 - 18:00
開催場所：JSOC

第 130 回運営委員会
開催日時：2018 年 3 月 28 日（水）16:00 - 18:00
開催場所：HIRT

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（本節の以下において「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。また、協議会が報告を受けたフィッシングサイトについて、JPCERT/CC に報告しており、これを受けて JPCERT/CC が、サイトを停止するための調整をインシデント対応支援活動の一環として行っています。

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計 22 件（ニュース：7 件、緊急情報：15 件）発信しました。

本四半期も前四半期に引き続き、Apple や Amazon、大手クレジットカード会社等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および LINE をかたりアカウント情報を詐取するフィッシングに

ついて、多くの報告が寄せられました。これらのサービスも含め、利用者数が多く、影響範囲も大きい報告については緊急情報として Web サイトに適宜掲載し、広く注意を喚起しました。その件数と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
仮想通貨関連サービスをかたるフィッシング関連：1 件
オンラインサービスをかたるフィッシング関連：4 件
通信事業者をかたるフィッシング関連：1 件
業界団体名をかたるフィッシング関連：1 件

本四半期の特筆すべきフィッシング事案としては、Netflix をかたるフィッシングがありました。Netflix は米国の映像ストリーミング配信等のサービス事業者で、日本でも数年前からサービスが開始され、ユーザ数が増加しています。これまで協議会では、Netflix をかたる英語のフィッシングメールの報告はありましたが、本四半期に、日本語のフィッシングメールおよびフィッシングサイトの報告が初めて寄せられました。同報告は 2 月 23 日に緊急情報として協議会 Web サイトに掲載し、広く注意を喚起しました。

［図 6-1 Netflix をかたるフィッシングサイト ］

https://www.antiphishing.jp/news/alert/netflix_20180223.html

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 31 の会員、もしくは、オブザーバに対し 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) 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）
2018 年 2 月 13 日 イーコマースフェア 2018「最新のフィッシング動向と対策について」

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/
2018 年 1 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201801.html
2018 年 2 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201802.html
2018 年 3 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201803.html

7. フィッシング対策協議会の会員組織向け活動

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。ここでは本四半期における会員組織向けの活動の一部について記載します。

7.1 運営委員会開催

本四半期においては、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。

第 58 回運営委員会
日時：2018 年 1 月 12 日 16:00 - 18:00
場所：株式会社日立システムズ

第 59 回運営委員会
日時：2018 年 2 月 16 日 16:00 - 18:00
場所：マホロバ・マインズ三浦

第 60 回運営委員会
日時：2018 年 3 月 9 日 16:00 - 18:00
場所：トッパン・フォームズ株式会社

7.2 フィッシング対策勉強会 第 2 回会合

協議会会員向けに、フィッシング対策勉強会 第 2 回会合を次のとおり開催しました。

フィッシング対策勉強会 第 2 回会合
日時：2018 年 2 月 16 日 10:00 - 12:00
場所：三菱総合研究所 本社 会議室 CR-DE
プログラム： 講演 1: なりすまし対策技術の最新動向:DMARC を中心として
株式会社インターネットイニシアティブ 櫻庭秀次 様

講演 2：Phishing の世界的トレンドを振り返る - Phishkit からわかること-
株式会社カスペルスキー 大沼千亜希様

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運用の一端を 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 4 四半期（10 月～12 月)]
（2018 年 1 月 25 日）
https://www.jpcert.or.jp/press/2018/vulnREPORT_2017q4.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 10～12 月)
（2018 年 1 月 18 日）
https://www.jpcert.or.jp/tsubame/report/report201710-12.html
https://www.jpcert.or.jp/tsubame/report/TSUBAMEReport2017Q3.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 4 件の記事を公開しました。

(1) LogonTracer を用いた不正ログオンの調査(2018-01-24)

JPCERT/CC が 2017 年 11 月 28 日に公開したイベントログの分析をサポートするツール「LogonTracer」を用いた不正アクセスの特定方法を紹介しています。LogonTracer と合わせてご活用ください。

LogonTracer を用いた不正ログオンの調査(2018-01-24)
https://www.jpcert.or.jp/magazine/acreport-logontracer2.html

(2) Japan Security Analyst Conference 2018 開催レポート~前編(2018-02-08)・後編(2018-02-16)~

JPCERT/CC が 2018 年 1 月 25 日に御茶ノ水ソラシティカンファレンスセンターで開催した Japan Security Analyst Conference 2018 （JSAC2018）の各講演の概要を前後編の 2 回に分けて紹介しています。

Japan Security Analyst Conference 2018 開催レポート~前編~(2018-02-08)
https://www.jpcert.or.jp/magazine/acreport-jsac2018report1.html

Japan Security Analyst Conference 2018 開催レポート~後編~(2018-02-16)
https://www.jpcert.or.jp/magazine/acreport-jsac2018report2.html

(3) プラグインをダウンロードして実行するマルウエア TSCookie(2018-03-01)

マルウエア「TsCookie」は国内組織を狙った標的型攻撃で確認したマルウエアで、JPCERT/CC では 2018 年 1 月にこのマルウエアを使った攻撃を確認しています。本記事では TsCookie の挙動の概要や通信リクエストの特徴などを解説しています。また、TsCookie の設定ファイルを抽出するツールも公開していますので、記事と合わせてご活用ください。

プラグインをダウンロードして実行するマルウエア TSCookie (2018-03-01)
https://www.jpcert.or.jp/magazine/acreport-tscookie.html

9. 主な講演活動

(1) 竹田 春樹（分析センター　マネージャー）：
「サイバー攻撃の最新動向とその対策～インシデント対応時に必要なこと～」
サイバーリーズン・ジャパン セキュリティ対策セミナー,2018 年 2 月 2 日

(2) 洞田 慎一（早期警戒グループ　マネージャー）：
「CSIRT 構築・運用」
KIIS サイバーセキュリティ研究会 セキュリティ人材育成プログラム,2018 年 2 月 2 日

(3) 輿石 隆（早期警戒グループ）：
「高度化するサイバー攻撃の脅威と対策」
栃木県警サイバー犯罪対策室　サイバーセキュリティ研修会，2018 年 2 月 20 日

(4) 輿石 隆（早期警戒グループ）：
「IoT セキュリティ評価のためのチェックリストを使った取り組み」
JNSA IoT セキュリティ WG セミナー，2018 年 2 月 26 日

(5) 佐々木 勇人（早期警戒グループ リーダー）：
「2017 年度のサイバー脅威を振り返り～金融先物取引業界への攻撃事例の解説と対策から～」
金融先物取引業協会 会員セミナー，2018 年 2 月 28 日

(6) 森崎 樹弥（早期警戒グループ）：
「情報セキュリティ最新動向 - Meltdown / Spectre 問題について -」
JAIPA 第 49 回 ISP＆クラウド事業者の集い in 下関,2018 年 3 月 8 日

(7) 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）：
「JPCERT/CC から見た IoT をめぐる脅威の現状～インシデント対応体制構築のポイント～」
日経産業新聞フォーラム, 2018 年 3 月 29 日

10. 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) 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

(2) 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：2018年1月24日

(3) 第2回重要インフラサイバーセキュリティコンファレンス
主　催：重要インフラサイバーセキュリティコンファレンス実行委員会、株式会社インプレス
開催日：2018年2月15日

(4) Security Days Spring 2018
主　催：株式会社ナノ・オプトメディア
開催日：2018年2月16日～3月9日

(5) JSSECセキュリティフォーラム2018
主　催：一般社団法人日本スマートフォンセキュリティ協会（JSSEC）
開催日：2018年3月9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