JPCERT-PR-2019-01
発行日 : 2019-01-16

JPCERT/CC 活動概要 [2018 年 10 月 1 日 ～ 2018 年 12 月 31 日]

活動概要トピックス

ートピック1ー 「2017 年度 CSIRT 構築および運用における実態調査」を公開

JPCERT/CC では、日本シーサート協議会（NCA）の協力のもと、国内の CSIRT の構築および運用における実態調査の結果をまとめた「2017 年度 CSIRT 構築および運用における実態調査」を 12 月 18 日に公開しました。

2017 年に、NCA は発足から 10 周年を迎え、発足時 6 組織だった会員数は、322 組織(2018 年 12 月 28 日現在)まで増加しており、国内の多くの組織で、「Computer Security Incident Response Team (CSIRT)」の構築や運用が進められています。その背景には、ランサムウエアの流布やリスト型攻撃、標的型攻撃など、昨今様々なサイバー攻撃が確認されていることがあります。また、2017 年 11 月に経済産業省が公開した「サイバーセキュリティ経営ガイドライン ver2.0」で、経営課題としてサイバーリスクへの対策の一つとして CSIRT の体制を整備するよう求めていることも、CSIRT の構築等に向けた動きを後押ししました。

このように前回調査から 2 年が経過する間に、CSIRT を備える組織が増え、サイバー攻撃手法も高度化するなど、取り巻く環境は大きく変化しています。JPCERT/CC では、新しい環境下での国内の CSIRT 活動の実態を明らかにするため、2015 年に次ぎ 2 回めのアンケート形式の調査を実施しました。

本報告書では、前回調査と同様に、CSIRT 構築および運用の実態を再確認することに加え、構築済の CSIRT が次のステップへ進むために取組むべき課題を分析し、その結果として、1) 他の組織の CSIRT との交流、2) インシデントの原因特定に向けたサービスの拡充、3) 事業継続と障害復旧計画への CSIRT としての関与、の 3 つを示しています。新たに CSIRT を構築しようとしている方々だけではなく、既に CSIRT を運用している組織を次の段階に向けて拡充する計画を検討している方々にも本書を役立てていただきたいと願っています。

2017 年度 CSIRT 構築および運用における実態調査
https://www.jpcert.or.jp/research/CSIRT-survey.html
https://www.jpcert.or.jp/research/20181218_CSIRT-survey2017.pdf

ートピック2ー　JPCERT/CC Eyes～JPCERT コーディネーションセンター公式ブログ～を開設

JPCERT/CC は、2018 年 10 月 23 日に JPCERT/CC 公式ブログ 「JPCERT/CC Eyes」を開設しました。JPCERT/CC で分析・調査した内容はもちろん、TSUBAME（インターネット定点観測システム）で観測された動向や国内外のイベントやカンファレンスの様子などをいち早くお届けするプラットフォームとして、情報発信に努めて参ります。
なお、これに伴い、これまで多くの皆さまにご愛読いただいてきた「分析センターだより」や「インシデントレスポンスだより」、「コラム」の各コンテンツを新ブログに一本化させていただきました。また、各コンテンツの過去の記事についても、新ブログに移し替えましたので、ご覧いただく際にはご留意ください。

JPCERT/CC Eyes～JPCERT コーディネーションセンター公式ブログ～（日本語版）
https://blogs.jpcert.or.jp/ja/

JPCERT/CC Eyes～JPCERT コーディネーションセンター公式ブログ～（英語版）
https://blogs.jpcert.or.jp/en/

事務所移転のお知らせ

JPCERT/CC は、2018 年 11 月 26 日に事務所を移転し、住所、電話番号等も変更になりました。
職員一同これを機に、気持ちを新たに、皆様のご期待にお応えできるよう一層の努力をいたす所存でございます。今後も倍旧のご支援ご指導を賜りますようお願い申し上げます。

所在地：〒103-0023
東京都中央区日本橋本町 4-4-2 東山ビルディング 8 階

Tel ：03-6271-8901
Fax：03-6271-8908

本活動は、経済産業省より委託を受け、「平成 30 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。

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 4,242 件、インシデント件数ベースでは 4,488 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 2,579 件でした。前四半期の 2,216 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/2019/IR_Report20190116.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

本四半期に報告が寄せられたフィッシングサイトの件数は 1,560 件で、前四半期の 1,302 件から 20%増加しました。また、前年度同期（852 件）との比較では、83%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	10 月	11 月	12 月	本四半期合計（割合）
国内ブランド	82	105	95	282(18%)
国外ブランド	301	330	354	985(63%)
ブランド不明（注 5）	70	133	90	293(19%)
全ブランド合計	453	568	539	1,560(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。

E コマースサイトを装ったフィッシングサイトに関する報告が前四半期に続き多く寄せられており、特定の国外ブランドのフィッシングサイトがその半数以上を占めています。
その中にはモバイル端末からアクセスした際にのみフィッシングサイトが表示されるものや、ブラウザの言語設定が日本語の場合にのみ表示されるものなど特定のユーザを標的としたものがいくつかありました。

国内ブランドのフィッシングサイトでは通信事業者、SNS、特定の宅配業者を装ったフィッシングサイトに関する報告が寄せられており、それぞれ次のような特徴がありました。

- 通信事業者を装ったフィッシングサイトについては大手携帯キャリアを狙ったものが前四半期に比べて増加している。また、正規のドメインを装った .com ドメインが多く各キャリアのフィッシングサイトが同一 IP アドレス上で稼働している場合もあった。
- SNS を装ったフィッシングサイトについてはホスティングサービスが無償で提供している .jp ドメインを使用したものが増加している。また、次のようにブランド名の後ろにランダムに選んだ複数の単語の羅列を添えたものをサブドメインに使用する特徴があった。

http://<ブランド名><単語の羅列>.<無料の jp ドメイン>/

- 特定の宅配業者を装ったフィッシングサイトについては、ドメインはブランド名の後ろに 2～4 文字の英小文字を足した .com ドメインが使用され、そのほとんどが中国のレジストラで取得されたドメインであった（詳しくは、4 章を参照）。また表示される Web ページにはいくつか種類があり、携帯番号の入力を求めるものや Apple ID とパスワードの入力を求めるもの、Android 端末でアクセスするとマルウエアがダウンロードされるものなどがあった。

フィッシングサイトの調整先の割合は、国内が 28%、国外が 72%であり、前四半期（国内が 27%、国外が 73%）と比べて国内への通知の割合が増加しました。

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、242 件でした。前四半期の 225 件から 8%増加しています。

10 月に、WordPress を使用した Web サイトに、不審な script タグや難読化された JavaScript が埋め込まれている事例を複数確認しました。それらのサイトにアクセスすると、パナマに割り当てられた同一の IP アドレスを持ち、.club や.site などのドメイン・アドレスが付与されたサイト上の URL を経由して複数回転送が行われた後、最終的には不審なサイトに転送され、広告や偽のシステム警告が表示されました。

12 月以降、Web ページ内の URL が、blueeyeswebsite[.]com といった URL に改ざんされているサイトを複数確認しています。改ざんされていた HTML ソースの例［図 1-1］に示します。script タグが改ざんされていることにより、ページにアクセスすると不正な JavaScript が読み込まれ、外部のサイトへの誘導が行われ、最終的に、広告を表示する不審なサイトに誘導されるようになっていました。改ざんされたサイトでは、script タグだけでなく、href タグなどの URL も改ざんされていました。また、blueeyeswebsite[.]com に誘導する難読化された JavaScript が Web ページに埋め込まれていた例も確認しています。

［図 1-1 Web ページ内の URL を改ざんされたサイトの HTML ソース］

1.1.1.3. その他

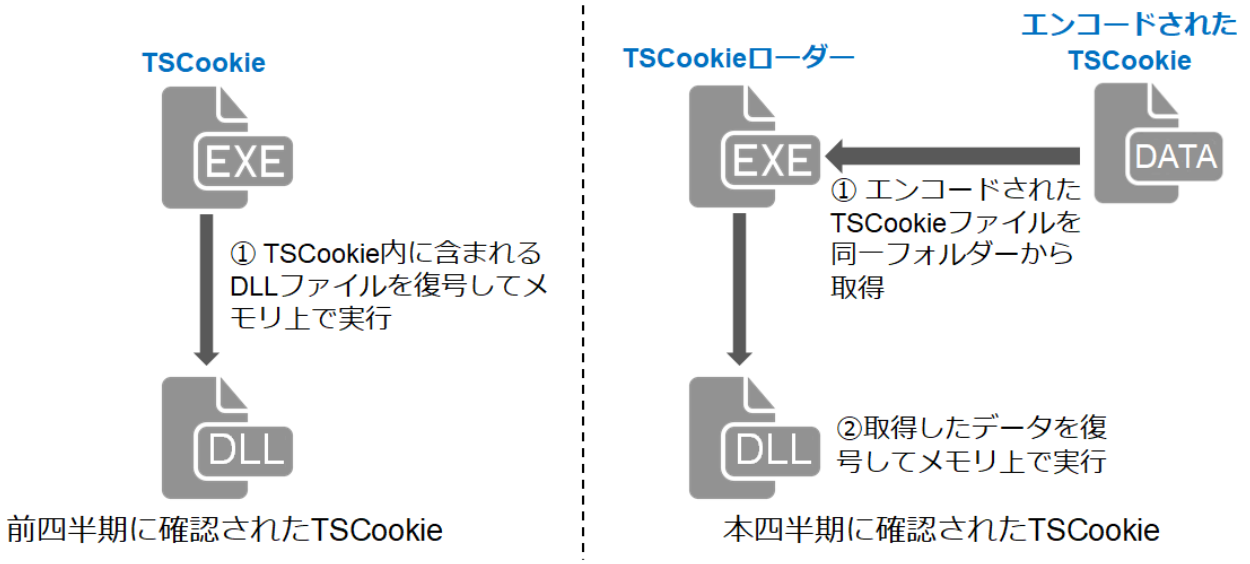
標的型攻撃に分類されるインシデントの件数は、4 件でした。前四半期の 7 件から 43%減少しています。本四半期に対応を依頼した組織はありませんでした。下に、確認されたインシデントを紹介します。

(1) マルウエア PlugX を用いた標的型攻撃

11 月に寄せられた報告には、PlugX と呼ばれるマルウエアが使用されていました。今回確認した PlugX はこれまで確認しているものと同様に 80/TCP、443/TCP に HTTP と独自プロトコルで C&C サーバと接続するといったものでした。その他にも攻撃者が使用したとみられる Mimikatz、secretdump といった認証情報を窃取するツールや RDP のセッションを多重化するツール、キーロガーなどが見つかっています。

(2) マルウエア TSCookie を用いた標的型攻撃

TSCookie は、2018 年 6 月末頃や 2018 年 8 月後半にも複数の組織に対してメールに添付されて送信されていたマルウエアです。11 月に寄せられた検体では、これまで確認していた TSCookie とは異なり、図 1-2 のように暗号化された TSCookie 本体とそれを読み込むローダーに分かれていました。また、ポート 443/TCP だけでなく、80/TCP に HTTP でも C&C サーバと通信する等、以前のものとは異なる特徴がみられました。



［図 1-2 TSCookie のファイル構成］

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：2 件　https://www.jpcert.or.jp/update/2018.html

2018-12-18　2017 年度 CSIRT 構築および運用における実態調査を公開
2018-12-18　長期休暇に備えて 2018/12

1.2.1.2. 注意喚起

深刻かつ影響範囲の広い脆弱性等が公表された場合には、「注意喚起」と呼ばれる情報を発行し、利用者に対して広く対策を呼びかけています。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：13 件（うち 1 件は更新情報）　https://www.jpcert.or.jp/at/

2018-10-02　Adobe Acrobat および Reader の脆弱性 (APSB18-30) に関する注意喚起 (公開)
2018-10-10　2018 年 10 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)
2018-10-17　2018 年 10 月 Oracle 製品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)
2018-10-19　2018 年 10 月 Oracle 製品のクリティカルパッチアップデートに関する注意喚起 (更新)
2018-10-26　Cisco Webex Meetings Desktop App および Cisco Webex Productivity Tools の脆弱性

(CVE-2018-15442) に関する注意喚起 (公開)
2018-11-14 Adobe Flash Player の脆弱性 (APSB18-39) に関する注意喚起 (公開)
2018-11-14 Adobe Acrobat および Reader の脆弱性 (APSB18-40) に関する注意喚起 (公開)
2018-11-14 2018 年 11 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)
2018-11-21 Adobe Flash Player の脆弱性 (APSB18-44) に関する注意喚起 (公開)
2018-12-06 Adobe Flash Player の脆弱性 (APSB18-42) に関する注意喚起 (公開)
2018-12-12 Adobe Acrobat および Reader の脆弱性 (APSB18-41) に関する注意喚起 (公開)
2018-12-12 2018 年 12 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)
2018-12-20 Microsoft Internet Explorer の脆弱性 (CVE-2018-8653) 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：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 99 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。

2018-10-03 ルートゾーン KSK ロールオーバーの鍵更新作業日時が決定
2018-10-11 仮想通貨を要求する日本語の脅迫メールについて
2018-10-17 「CODE BLUE 2018」開催
2018-10-24 PHP 5.6 系および 7.0 系が年内にサポート終了
2018-10-31 JPCERT/CC 公式ブログ「JPCERT/CC Eyes」開設
2018-11-07 JPCERT/CC が「マルウエア TSCookie の設定情報を正常に読み込めないバグ」に関するブログを公開
2018-11-14 NICT が「日本国内でインターネットに接続された IoT 機器等に関する事前調査」を実施
2018-11-21 IPA が「中小規模向け IoT 品質確認チェックリスト」を公開
2018-11-28 JPCERT/CC 事務所移転のお知らせ
2018-12-05 SecurityDay2018 開催のお知らせ
2018-12-12 「Hardening II SecurEach」に関するブログを公開
2018-12-19 長期休暇に備えて 2018/12
2018-12-27 JPCERT/CC が「2017 年度 CSIRT 構築および運用における実態調査」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 では、脆弱性やマルウエア、サイバー攻撃などに関する最新情報を、タイムリーにお届けしています。注意喚起とは異なり、発行時点では注意喚起の基準に満たない脆弱性の情報やセキュリティアップデート予告なども含まれます。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/

2018-10-10　複数の Adobe 製品のアップデートについて
2018-11-14　Adobe Photoshop CC のセキュリティアップデート (APSB18-43) について
2018-12-11　マルウエアへの感染を誘導し、仮想通貨を要求する脅迫メールについて
2018-12-19　Web Diary Professional を使用している Web サイトの改ざんについて

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) Adobe Flash Player の脆弱性に関する情報発信

Adobe より Adobe Flash Player に関する脆弱性の情報 (APSB18-42) が、2018 年 12 月 5 日（米国時間）に公開されました。この中で言及されている脆弱性 (CVE-2018-15982)を悪用すると、攻撃者が細工したコンテンツをユーザに開かせることで、任意のコードを実行することができます。また、Adobe は同脆弱性の悪用に関する報告を確認していると説明しています。JPCERT/CC では、公開されている実証コードにより脆弱性の悪用が可能なこと、さらに Flash Player を最新バージョンにアップデートすれば実証コードが動かなくなることを確認した上で、危険性の高い脆弱性であると判断し、注意喚起および早期警戒情報を発行し、早期の対策を呼びかけました。

Adobe Flash Player の脆弱性 (APSB18-42) に関する注意喚起
https://www.jpcert.or.jp/at/2018/at180048.html

(2) Oracle WebLogic Server の脆弱性に関する情報発信

JPCERT/CC は、2018 年 10 月 17 日に Oracle 製品のクリティカルパッチアップデートに関する注意喚起を発行しました。その後、同パッチアップデートで修正されていた Oracle Weblogic Server の脆弱性 (CVE-2018-3191、CVE-2018-3245) についての実証コードが、2018 年 10 月 19 日頃より Web 上で公開されていることを確認し、さらに JPCERT/CC が管理するセンサでも同脆弱性を持つノードを探索していると思われる通信を観測しました。JPCERT/CC にて公開されている実証コードを検証した結果、Oracle Weblogic Server が動作しているサーバに対し、細工したリクエストを T3 プロトコルで送信することで、任意のコードが実行可能であることを確認したことから、改めて早期警戒情報を発信し、早期の対策を呼びかけました。

2018 年 10 月 Oracle 製品のクリティカルパッチアップデートに関する注意喚起
https://www.jpcert.or.jp/at/2018/at180042.html

(3) 「2017 年度 CSIRT 構築および運用における実態調査」を公開

JPCERT/CC では、日本シーサート協議会（NCA）に加盟している CSIRT を対象にアンケート形式による CSIRT 構築および運用における実態調査を昨年度実施し、調査結果に対する分析をまとめた報告書を 12 月 18 日に公開しました。

CSIRT は、セキュリティインシデントの発生時に、組織が効果的に対処する際の要となる組織として、その構築や運用に注目が集まっています。高度化するサイバー攻撃手法など、取り巻く環境は日々変化しており、CSIRT の構築および運用にあたっては、実態を定期的に把握し、柔軟に対応することが重要となります。本報告書は、調査結果や JPCERT/CC が日々の活動で得た知見にもとづく分析結果を提示することにより、新たに CSIRT を構築しようとしている方々だけではなく、既に CSIRT を運用している組織においても次の段階に向けた検討に役立てていただくことを目的としています。CSIRT の構築や活動の改善の参考資料としてご活用ください。

2017 年度 CSIRT 構築および運用における実態調査
https://www.jpcert.or.jp/research/CSIRT-survey.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 12 月末時点で、海外の 21 の経済地域の 27 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

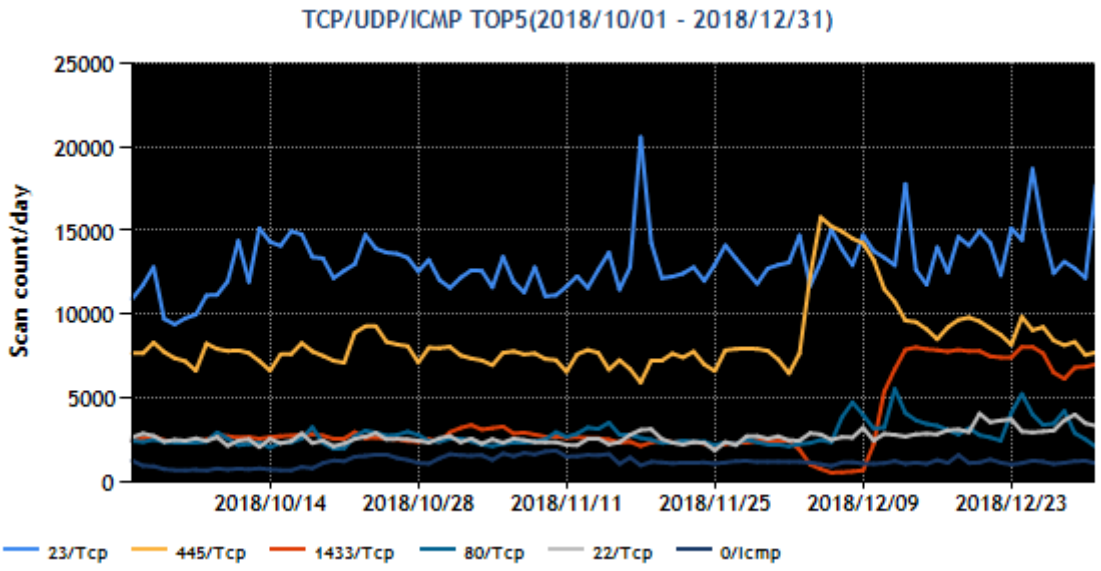
1.3.1. インターネット定点観測システム TSUBAME の観測データの活用

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、2018 年 7 月から 9 月分のレポートを 2018 年 10 月 18 日に公開しました。

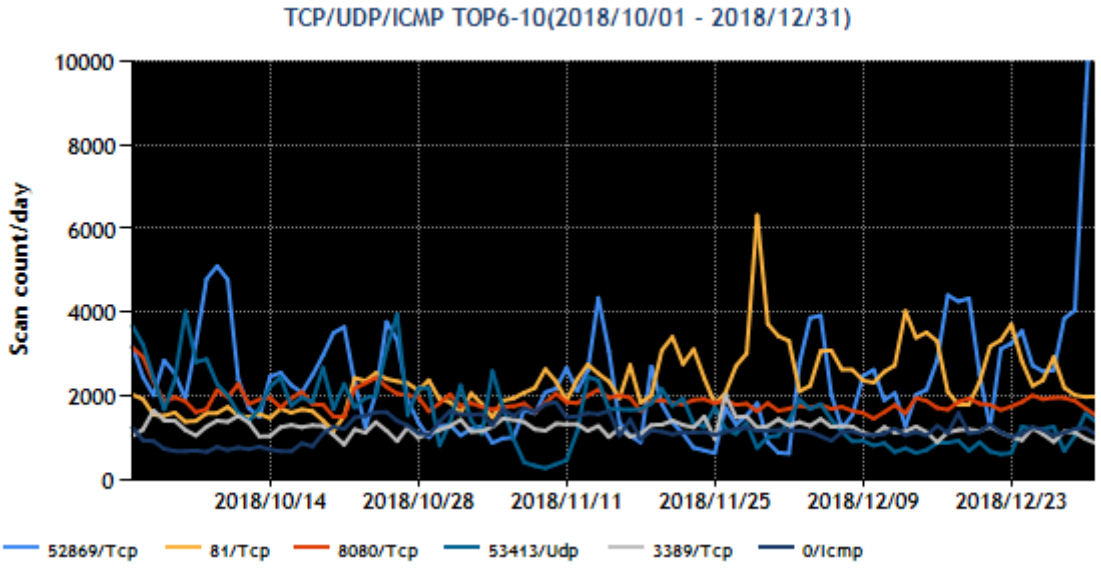
TSUBAME 観測グラフ
https://www.jpcert.or.jp/tsubame/index.html#examples
インターネット定点観測レポート（2018 年 7～9 月）
https://www.jpcert.or.jp/tsubame/report/report201807-09.html

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 1-3］と［図 1-4］に示します。

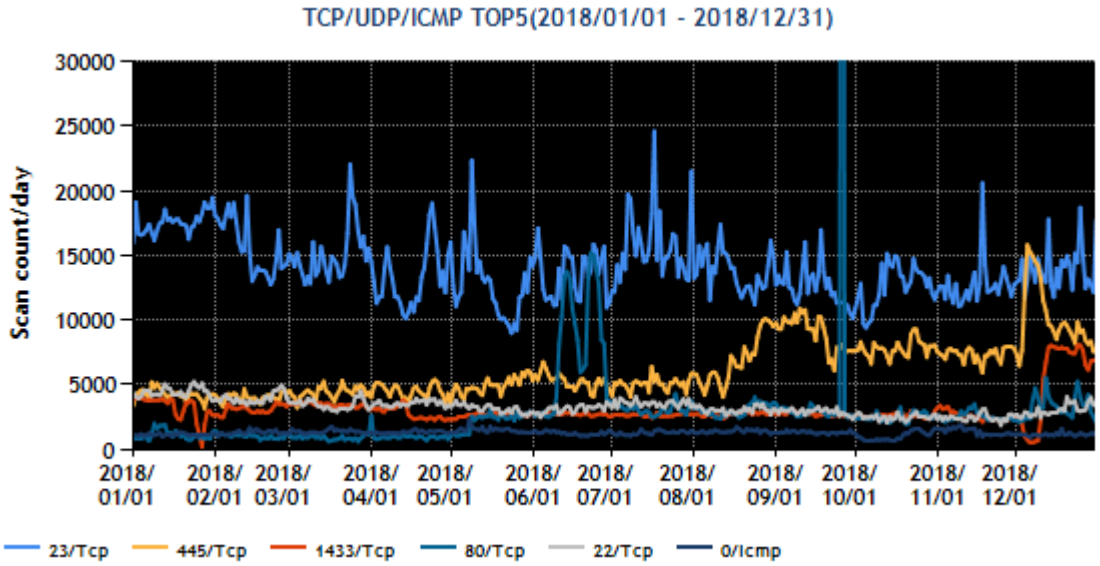


［図 1-3 宛先ポート別グラフ トップ 1-5（2018 年 10 月 1 日-12 月 31 日）］

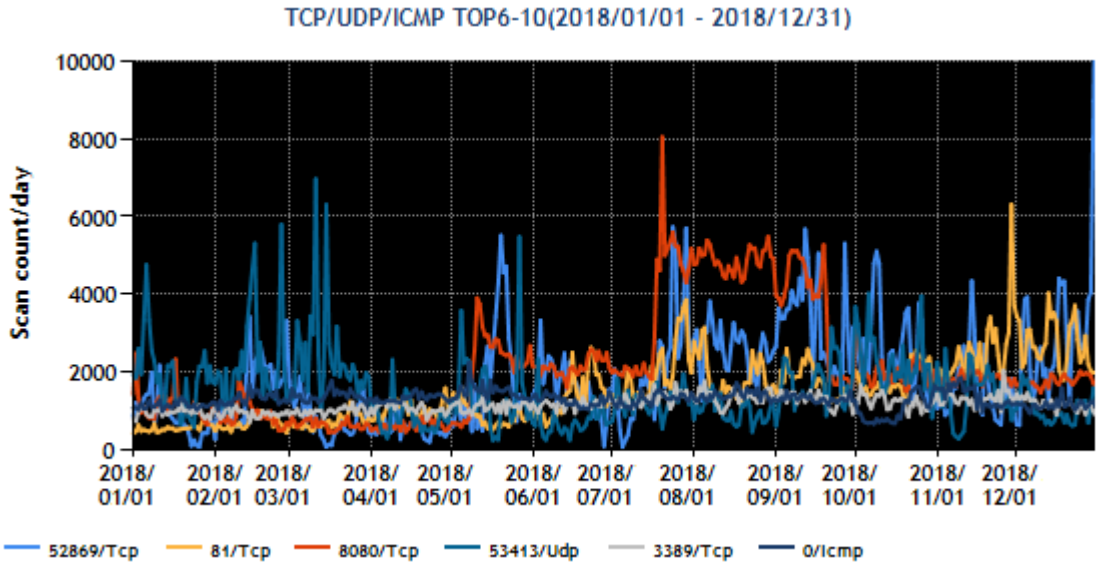


［図 1-4 宛先ポート別グラフ トップ 6-10（2018 年 10 月 1 日-12 月 31 日）］

また、過去 1 年間（2018 年 1 月 1 日-2018 年 12 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 1-5］と［図 1-6］に示します。



［図 1-5 宛先ポート別グラフ トップ 1-5（2018 年 1 月 1 日-12 月 31 日）］



［図 1-6 宛先ポート別グラフ トップ 6-10（2018 年 1 月 1 日-12 月 31 日）］

本四半期には、23/TCP 宛のパケット数が、ゆるやかに増減する、または突発的に増減するなどの目立った変化をしました。そうした変化が見られた送信元を調査したところ、その一部でルータや監視カメラ、レコーダー等の機器が設置されていることが分かりました。また、これらの機器が使用するポート宛のパケット数の一時的増加も観測されていました。これらの機器に関しては、すでに脆弱性情報や攻撃用コードが公開されています。攻撃者がこれらの機器で脆弱なまま放置されているものを攻撃するパケットを送り付け、その結果、マルウエアに感染した機器が 23/TCP 宛のパケットを送信し始めたものと考

えられます。

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、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、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。本四半期における主な対応事例として、Realtek 社の SDK の脆弱性を使用した機器がマルウエアに感染し、複数のポート番号宛のパケットを送信するインシデントについて次に述べます。

Realtek 社製の SDK から脆弱性 (CVE-2014-8361) を継承した、インターネットに接続された機器がマルウエアに感染し、広範囲の IP アドレスに Port23/TCP 等のポート宛のパケットを送信するという事象が、2017 年から 10 月 31 日頃から確認されました。
本四半期は、上述のような観測状況から、対策が行われていない機器が再度マルウエアに感染しパケットの送信元ホスト数が増加したものと推測されたため、それぞれの送信元ホストの IP アドレスの管理者に連絡を行いました。複数の管理者から返信があり、それにより対策の未実施機器を使用していたことが確認できました。

本攻撃ではマルウエアを外部サイトからダウンロードする手口を使用するため、マルウエアがダウンロードされるサイトの管理者にも連絡を行いました。
このように JPCERT/CC では、観測したパケットの分析等を行い、必要に応じて管理者への情報提供や、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. APCERT 年次総会での講演（2018 年 10 月 23 日）

TSUBAME プロジェクトにはアジア各国の CSIRT の協力が必要不可欠です。例年 APCERT 年次総会の期間内に TSUBAME Workshop を行いプロジェクトについての情報共有を図っています。
本四半期は APCERT 年次総会で講演し、TSUBAME ワーキンググループの活動を紹介しました。講演では、この 1 年間に観測された、脆弱なルータや監視カメラなどを探索する攻撃事例を振り返りました。これらの攻撃が、地域の境界を越えて行われていることを指摘し、メンバー間の情報共有を通じた対策を呼びかけました。

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。

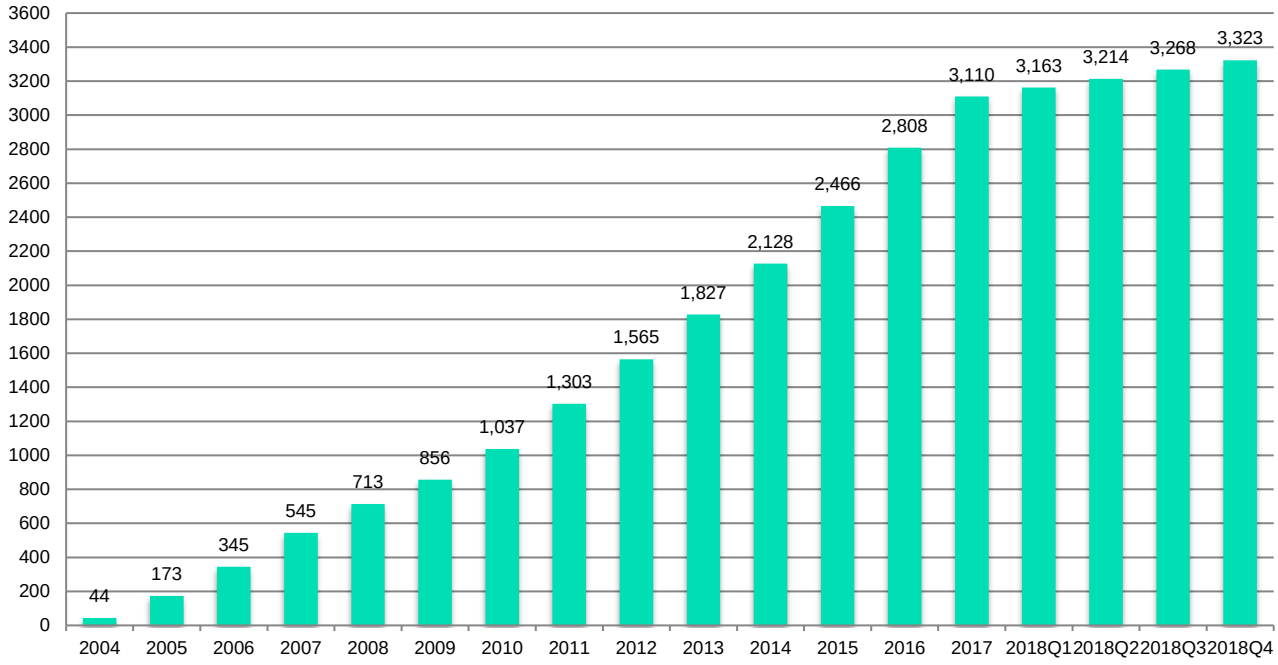
独立行政法人情報処理推進機構（IPA）脆弱性対策
https://www.ipa.go.jp/security/vuln/

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 55 件（累計 3,323 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］

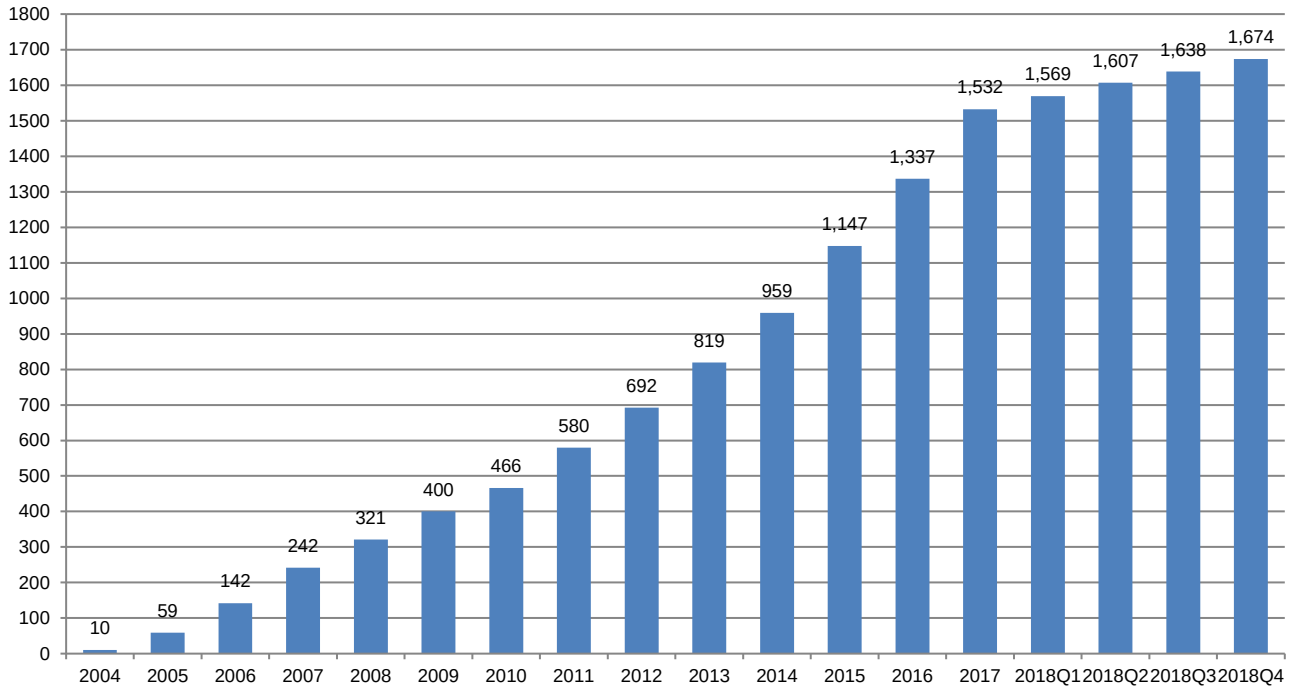
本四半期において公表に至った脆弱性情報のうち、国内取扱脆弱性情報は 36 件（累計 1,674 件）で、累計の推移は［図 2-2］に示すとおりです。本四半期に公表した 36 件の内訳は、国内の単一の製品開発者の製品に影響を及ぼすものが 22 件、海外の単一の製品開発者の製品に影響を及ぼすものが 12 件、国内の複数の製品開発者の製品に影響を及ぼすものが 2 件ありました。36 件うち 10 件が自社製品の届出によるものでした。自社製品における脆弱性の届出は年々増加しており、毎四半期に一定数の届出があります。

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］のとおりです。本四半期は前四半期同様に、Windows アプリケーションが 7 件と最も多く、2017 年第 2 四半期から継続して多数公表されています。これは、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 読込みの脆弱性」と同類の脆弱性をもつ Windows アプリケーションがあると考えた特定の発見者が、2017 年以降多数の Windows アプリケーションで検証を行い、脆弱性が確認されたものを順次届出たことに起因しています。

次いで本四半期の公表で多数を占めた製品カテゴリは、組込系（5 件）とグループウエア（5 件）でした。組込系製品の公表が比較的多いのは、特定の発見者が、組込系製品についての脆弱性を探索して順次届け出ていることによるもので、グループウエアに関しては、自社製品の脆弱性届出を継続的に行っている製品開発者がいる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	7
組込系	5
グループウエア	5
CMS	4
プラグイン	4
ウェブアプリケーション	3
アプライアンス	2
マルチプラットフォームアプリケーション	2
ミドルウエア	2
iOS アプリケーション	1
ライブラリ	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 19 件（累計 1,649 件）で、累計の推移は［図 2-3］に示すとおりです。

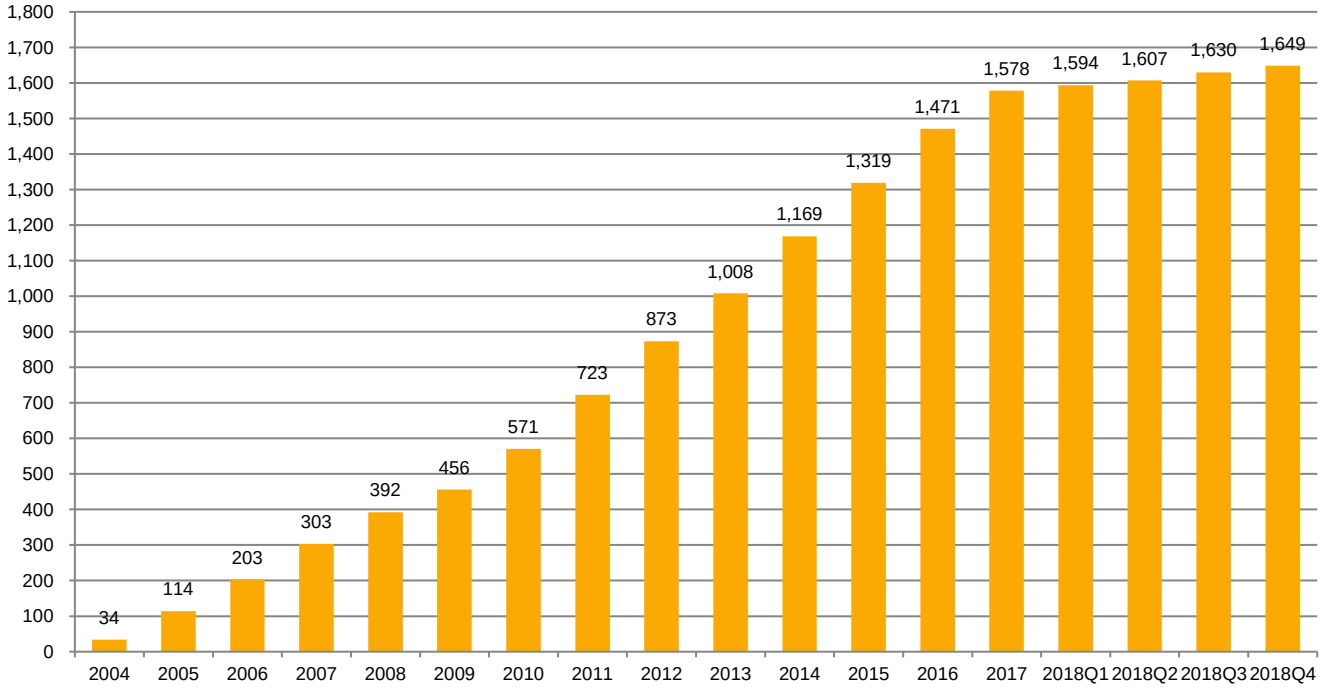
本四半期に公表した脆弱性の影響を受けた製品のカテゴリ内訳は、［表 2-2］のとおりです。本四半期は、組込系に関するものが 5 件と最も多く、これら 5 件のうち 2 件は、米国 CERT/CC、フィンランド

NCSC-FI、オランダ NCSC-NL、JPCERT/CC に国際展開され、各国の複数の製品開発者との事前調整を経て公表に至ったものです。5 件中 3 件は、CERT/CC が発行した注意喚起を、JPCERT/CC が翻訳し JVN にて注意喚起を行ったものです。

次いで多かったのは、macOS アプリケーションに関する脆弱性が 3 件、マルチプラットフォームアプリケーションに関する脆弱性が 3 件、制御系製品に関する脆弱性が 3 件でした。制御系製品に関する 3 件の公表の内訳は、米国 ICS-CERT からの国際展開および調整依頼を受け、国内製品開発者との調整を行い公表に至ったものが 2 件、制御系製品を開発する製品開発者が、自社製品に関する脆弱性情報を JVN で広く情報発信することを目的としたものが 1 件でした。
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
組込系	5
macOS アプリケーション	3
制御系製品	3
マルチプラットフォームアプリケーション	3
Android アプリケーション	1
API	1
ウェブサーブレットコンテナ	1
ウェブブラウザ	1
ミドルウエア	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、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。これまでに、公表判定委員会での審議を経て 11 件（製品開発者数で 8 件）を、JVN の「Japan Vulnerability Notes JP（連絡不能）一覧」に掲載しています。

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に、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 NCSC-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 21 件の制御システム用製品の脆弱性情報を公表しています。

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 72 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会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。

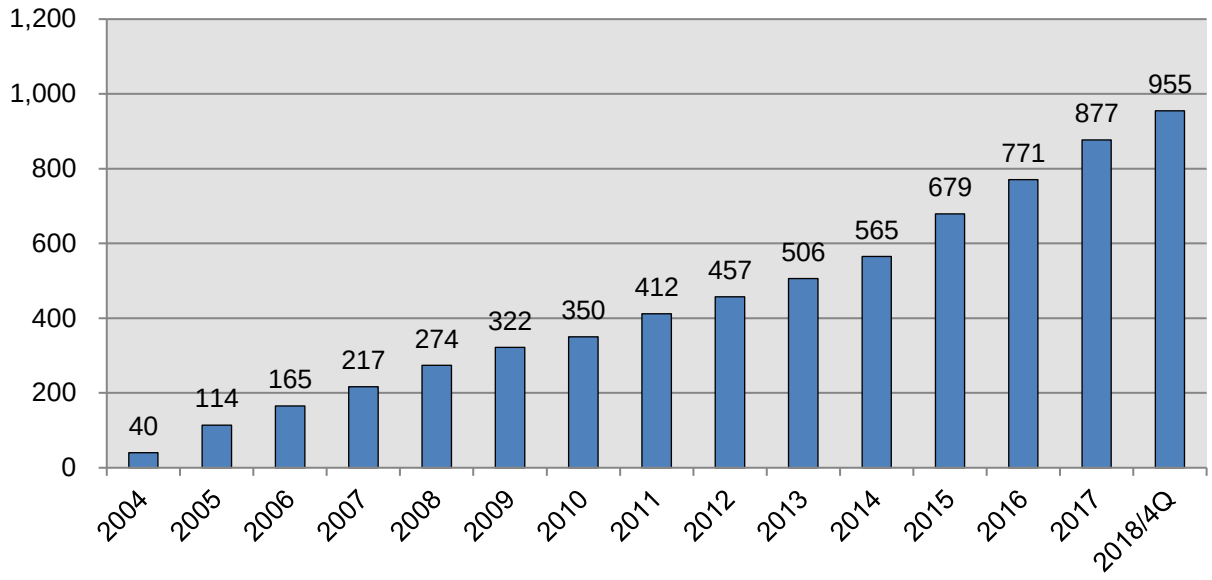
脆弱性情報取扱体制
http://www.meti.go.jp/policy/netsecurity/vulhandlingG.html
脆弱性情報コーディネーション概要
https://www.jpcert.or.jp/vh/

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）
https://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 12 月 31 日現在で 955 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
https://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 11 月 12 日に開催したミーティングでは、ネットワーク定点観測からみえる IoT 製品等の脆弱性

動向や事例、脆弱性報告者による脆弱性発見手法の紹介、これまでに CVE 番号が割り当てられた脆弱性全体の傾向分析など、技術的な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

脆弱性コーディネーショングループでは、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: 11 月 16 日
講演タイトル: インターネットとセキュリティと JPCERT/CC
イベント名: 早稲田大学基幹理工学部「サイバー攻撃対策技術の基礎」科目

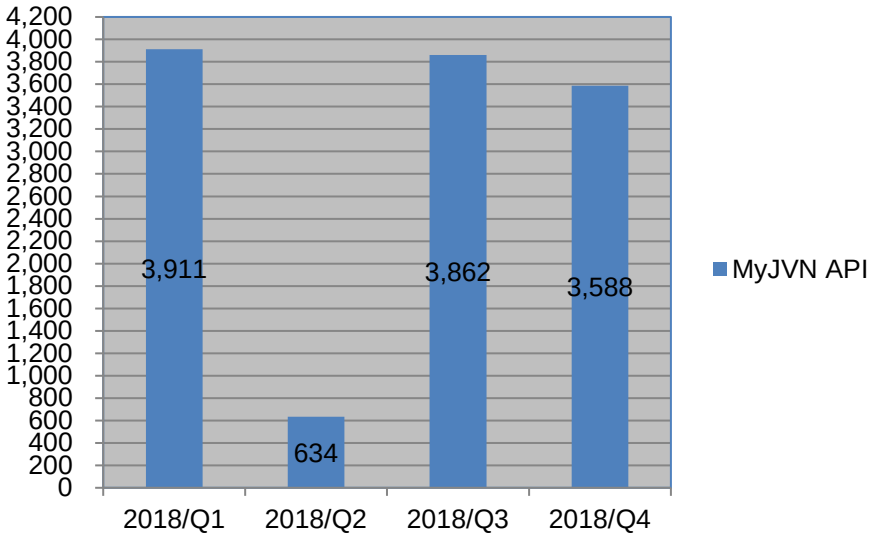
本講演は、早稲田大学基幹理工学部が開講している「サイバー攻撃対策技術の基礎」科目の講義の一部を、講師派遣依頼を受けて担当したものです。セキュリティインシデントと CSIRT、JPCERT/CC の組織概要と活動内容、および、ソフトウエアの脆弱性とその修正を目指して行うコーディネーション活動の 3 項目について解説しました。

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、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。

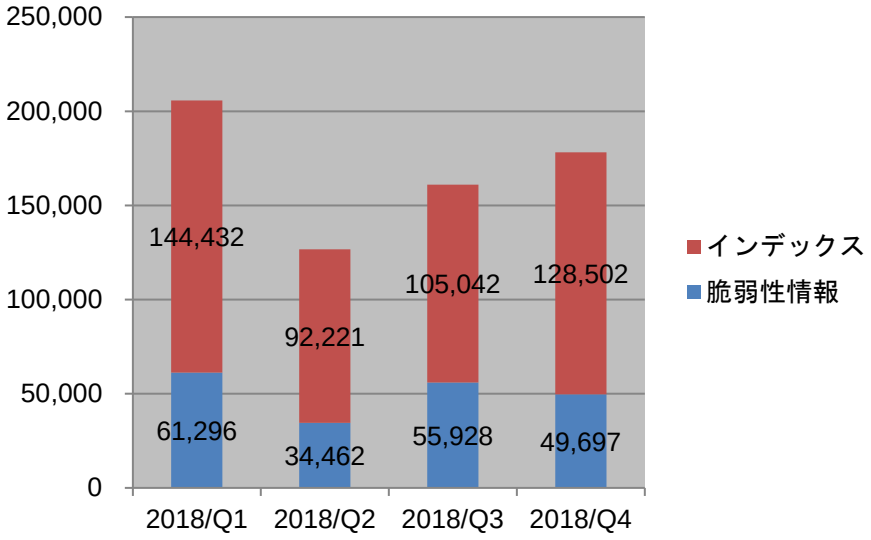
VRDA フィード 脆弱性脅威分析用情報の定型データ配信
https://www.jpcert.or.jp/vrdafeed/index.html

四半期ごとに配信した VRDA フィード配信件数を［図 2-6］に、VRDA フィードの利用傾向を［図 2-7］と［図 2-8］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 2-8］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。



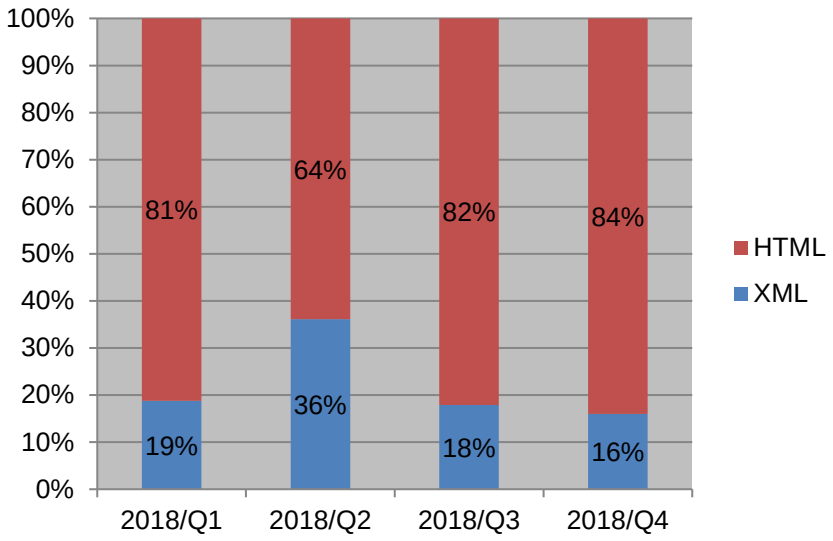
［図 2-6 VRDA フィード配信件数］

VRDA フィード配信件数については、第 2 四半期の配信件数が大幅に減少していますが、これは同四半期に実施された VRDA フィード配信用システムの一部改訂作業におけるデータ更新の停止が伴ったことが原因です。



［図 2-7 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 2-7］に示したように、前四半期と比較し、約 22%増加しました。脆弱性情報の利用数については、約 11%減少しました。



［図 2-8 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 2-8］に示したように、前四半期と比較し、大きな変化は有りませんでした。

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 499 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 4 件でした。

2018/10/16 【参考情報】Auto-Maskin 社の船舶エンジン関連製品の複数の脆弱性について
2018/10/16 TRITON の亜種に関するインディケータ提供について
2018/10/31 【参考情報】NERC がサプライチェーンのセキュリティリスク管理に関する 3 つの CIP を公表
2018/11/21 【参考情報】米国のプラム島で行われた電力システムのサイバー演習について

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。

2018/10/11 制御システムセキュリティニュースレター 2018-0009
2018/11/08 制御システムセキュリティニュースレター 2018-0010
2018/12/07 制御システムセキュリティニュースレター 2018-0011

制御システムセキュリティ情報共有コミュニティでは、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 のサービスを設けており、メーリングリストには現在 908 名の方にご登録いただいています。今後も両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活動として、インシデント報告の受付と、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を行っています。本四半期における活動は次のとおりでした。

(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システムの情報（23 IP アドレス）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 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 265 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

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。

4.1.1. アフリカ CSIRT 構築支援

4.1.1.1. AFRINIC 29 への参加

チュニジアで開催された AFRINIC-29 に、アフリカ CSIRT 構築支援の一環として参加しました。AFRINIC-29 は、AFRINIC（African Network Information Centre）が主催する、アフリカのインターネットの普及/構築に携わる産官学の多様な人々を対象としたイベントです。アフリカの ICT における技術動向や政策等に関して、国際コミュニティとの交流を図るとともに、現状と課題について話し合うことを目的に 2004 年から毎年 2 回開催（前期は Africa Internet Summit（AIS）と同時開催）されており、今回で 29 回目になります。11 月 26 日から 11 月 30 日のイベント中に 254 名が参加しました。
JPCERT/CC は、AfricaCERT（アフリカコンピュータ緊急対応チーム）から依頼を受けて、情報技術の向上を目的としたワークショップにおいて OSINT（オープンソースインテリジェンス）トレーニングを行いました。地元のチュニジアからの参加者を中心に 20 名がこれを受講しました。

［図 4-1　OSINT についてのトレーニング風景写真］

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っています。JPCERT/CC では、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、同地域の技術力の向上と連携の基盤づくりを目的に、CSIRT の構築・運営とそれを支える人材の育成に 2010 年から取り組んでいます。

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、APCERT について 2003 年 2 月の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、また、その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 年次総会 2018 への参加

アジア太平洋地域の CSIRT コミュニティである APCERT の年次総会が中国の上海で開催されました。APCERT の主要メンバーであるオペレーショナルメンバー（全 30 チーム）のうち JPCERT/CC を含む 27 チームが参加しました。
APCERT 年次総会は、各経済地域における最近のインターネットセキュリティ動向、インシデント対応の事例、調査・研究活動等を共有することを目的に、毎年開催されています。今年のテーマは”Strengthen information sharing for effective and cooperative emergency response” でした。開催概要は次のとおりです。

1) 日程：
10/21（日） 午前：APCERT ワーキンググループ会合
午後：APCERT チームビルディングイベント
10/22（月） 午前：トレーニングワークショップ（Microsoft 社）
午後：APCERT Steering Committee 会議
10/23（火） 午前：メンバー向けカンファレンス（Closed Conference）
午後：APCERT 年次総会（Annual General Meeting）
10/24（水） 終日：一般公開講演（Open Conference）

2) 会場：Westin Bund Center, Shanghai

3) 主な決定事項等：
APCERT Steering Committee および年次総会では、APCERT の運営規約(Operational Framework)を改正

し、会議の定足数などを見直しました。
メンバー向けカンファレンスにおいては、IoT 機器を介したインシデントの動向や、APCERT メンバーが国内の事業者向けに行っているサイバー演習の取り組み、また標的型攻撃をはじめとしたサイバー攻撃情報の分析について様々なツールを用いた工夫などが紹介されました。また JPCERT/CC からも TSUBAME の活動成果の報告や、最近の観測動向などについて講演を行いました。
一般公開講演においては、CSIRT の技術担当者や民間企業の専門家から、最新の攻撃手法についての分析事例や、ハニーネットを活用したインシデント観測事例などの紹介がありました。
任期満了を迎えた Steering Committee の半数のメンバーの改選選挙では、ACSC（オーストラリア）、CNCERT/CC（中国）、KrCERT/CC（韓国）、TWNCERT（台湾）が再選されました。また、APCERT 議長チームおよび副議長チームの改選が行われ、ACSC が議長チームとして、MyCERT（マレーシア）が副議長チームとしてそれぞれ再選されました。JPCERT/CC は、引き続き APCERT の事務局および Steering Committee メンバーとしてさまざまな活動をリードしてまいります。

［図 4-2　APCERT 年次総会集合写真］

APCERT 年次総会についての詳細は、次の Web ページをご参照ください。

APCERT Annual General Meeting & Conference 2018
http://apcert2018.cert.org.cn/index

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。本四半期は、JPCERT/CC が支援したベトナムの VNCERT が FIRST に加盟を果たしました。

FIRST 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. Kyiv 2018 UNDP/FIRST Technical Colloquium への参加（10 月 9-11 日）

JPCERT/CC は 10 月 9 日から 11 日までウクライナのキエフで開催された FIRST TC に参加しました。また元 FIRST 理事の小宮山がその準備を支援しました。このイベントは FIRST と国連開発計画(UNDP)の共催で、主に東欧諸国から 40 名程度が参加しました。

4.2.2.2. FIRST Regional Symposium での講演（10 月 25 日）

JPCERT/CC は 10 月 25 日に中国の上海で開催された FIRST Regional Symposium の Plenary session で、標的型攻撃に関するログ分析のために開発したツール SysmonSearch について講演しました。本講演では、SysmonSearch を使って行うログの可視化やフィルタリングの方法についてデモンストレーションを交えて解説しました。

［図 4-3　講演風景］

4.3. CyberGreen

国際的なプロジェクトである CyberGreen は、指標を用いて各国／地域インターネット全体の健全性を評価して比較し、各国の CSIRT や ISP、セキュリティベンダーが、関連する指標値を向上させる施策についてグッド・プラクティスを学びあい、目標を明確化することを通じて、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。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、前四半期に続き本四半期においても継続して提案を行いました。

CyberGreen Institute
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

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 の英語版を公開したことにより、海外のセキュリティ関係者に Mejiro で見るインターネット健全性について説明することができるようになりました。今後は.Mejiro 指標を使って各国で抱えるリスクの説明とインターネット空間のクリーンアップ活動を進めていきたいと思います。本四半期はモンゴルとインドネシアのイベントで講演を行いましたので、報告いたします。

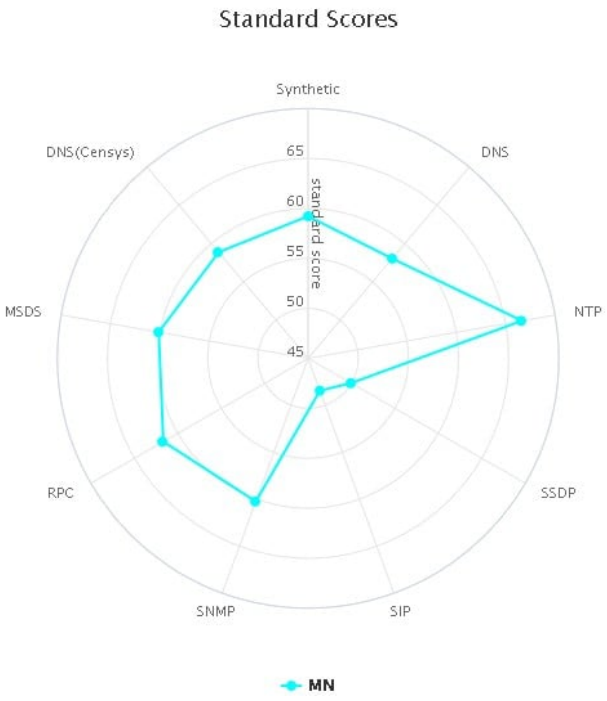
4.3.1.1. MNSEC 2018 での講演

モンゴル国内で最大の情報セキュリティ関連のイベントである MNSEC が 10 月 4 日と 10 月 5 日の 2 日間に渡って開かれました。JPCERT/CC はインターネットリスク可視化サービス—Mejiro（以下、Mejiro）についての講演を 10 月 4 日に行いました。

MNSEC2018
https://mncert.org/mnsec/home

［図 4-4　MNSEC 講演写真］

この講演では、Mejiro 英語版が公開されたことと、Mejiro で見たモンゴルのインターネット健全性を紹介しました。モンゴルの Mejiro 指標は DNS, NTP, SNMP, RPC, MSDS のプロトコルで平均よりも高い値を示しています（図 4-5 参照）。これは、設定が不適切で DDoS 攻撃の踏み台になりえる端末の台数の、モンゴルに割り当てられた IP アドレス数に対する割合が世界の平均と比べて大きく、攻撃のための基盤として悪用されるリスクが高いということです。



［図 4-5 モンゴルの Mejiro 指標］

4.3.1.2. codeBALI 2018 でのトレーニングと講演

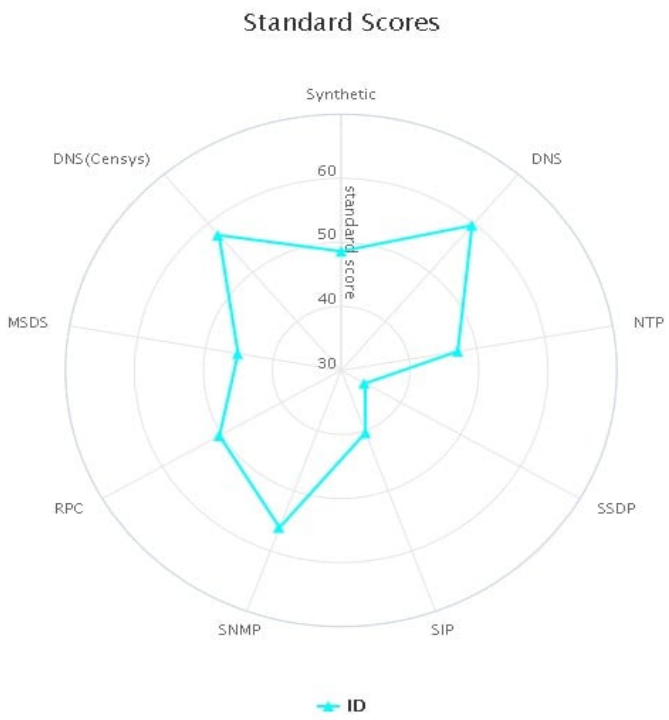
codeBALI はインドネシアと日本、両国の産官学が協力し、年に一度バリ島で開かれるカンファレンスです。JPCERT/CC が行っている情報収集方法を基にした解析手法などの OSINT トレーニングを 10 月 9 日に、Mejiro についての講演を 10 月 10 日の codeBALI カンファレンスで行いました。

［図 4-6　OSINT についてのトレーニング風景写真］

6 時間に渡ったトレーニングでは、参加者から講師へ活発な質問がありました。また参加者の過去の経験や現在の課題などが共有され、双方向のコミュニケーションを行うことができました。

前述のモンゴルで行われた MNSEC に続き、インドネシア バリ島でも Mejiro 英語版の公開を紹介すると共に Mejiro で見るインドネシアのインターネット健全性について講演を行いました。

codeBALI2018
https://www.codebali.net/



［図 4-7 インドネシアの Mejiro 指標］

国が変わると各プロトコルのリスクの度合いが変わります。図 4-7 のとおりインドネシアでは DNS と SNMP プロトコルのリスクノードが多く存在していることがわかります。こういったリスクノードを 1 つ 1 つ減らしていく活動が重要であることを参加者に伝えました。

［図 4-8　codeBALI 講演写真］

4.4. その他国際会議への参加

4.4.1. H-ISAC Workshop での講演（10 月 17 日）

米国を拠点にグローバルに活動する医療セクターの ISAC（Information Sharing and Analysis Center）である H-ISAC （Health Information Sharing and Analysis Center）のワークショップが東京で開催され、JPCERT/CC は最近のインシデント動向や海外組織との連携について講演しました。

HITCON Pacific での講演（12 月 13－14 日）

台湾国内の最大級のセキュリティイベントである Hitcon Pacific が 12 月 13 日と 12 月 14 日の 2 日間に渡って開催されました。JPCERT/CC は、“Not just a ‘incident responder’ : Ever-changing Nature of CERTs/CSIRTs”と題して、変わりつつある CSIRT に求められる役割について講演しました。

［図 4-9　HITCON 講演風景］

4.4.2. The Global Commission on the Stability of Cyberspace（GCSC）への参加

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 2017 年 3 月に立ち上がりました。その中には技術、法律、インターネットガバナンスなどの分野ごとにオープンな議論を行うことを目的とする 4 つのワーキンググループが設けられています。技術ワーキンググループではメーリングリストでの議論や調査の仕様作成などを行っており、JPCERT/CC の小宮山が副議長としてこれに関与しています。
本四半期はメーリングリストでの議論などを通じて、2018 年 9 月にシンガポールで実施された会合の成果文書を作成しました。同文書は次の Web ページで一般公開されています。

Global Commission Introduces Six Critical Norms Towards Cyber Stability
https://cyberstability.org/news/global-commission-introduces-six-critical-norms-towards-cyber-stability/

加えてこれら国際的な規範の議論の実態を、日本国内の関係者に伝えることを目的として、2018 年 11 月 1-2 日に東京で開催されたセキュリティカンファレンス Code Blue で“Reading the norms of cyberspace - New role of technician community -”と題した講演を行いました。

4.4.3. 海外 CSIRT 等の来訪および往訪

4.4.3.1. ウズベキスタン UZ-CERT 往訪（10 月 2 日）

ウズベキスタンの UZ-CERT（ウズベキスタンコンピュータ緊急対応チーム）を訪問し、活動の状況についてヒアリングを行うとともに、今後の協力について意見交換を行いました。

4.4.3.2. ウズベキスタン UZ-CERT 来訪（10 月 30 日）

ウズベキスタンの UZ-CERT（ウズベキスタンコンピュータ緊急対応チーム）が来訪し、活動の状況についてヒアリングを行うとともに、今後の協力について意見交換を行いました。

4.4.3.3. バヌアツ CERT VU 来訪（11 月 13 日）

今年バヌアツに設立された CERT VU（バヌアツコンピュータ緊急対応チーム）が来訪し、活動の進捗についてヒアリングを行いました。

4.4.3.4. メキシコ CERT-MX 往訪（11 月 19 日）

「平成 30 年度中南米 CSIRT 動向調査」のプロジェクトの一環として、メキシコの CERT-MX（メキシココンピュータ緊急対応チーム）を訪問し、施設を見学するとともに設立背景や活動の詳細についてヒアリングを行いました。

4.4.3.5. ブラジル CERT.br 往訪（11 月 22 日）

「平成 30 年度中南米 CSIRT 動向調査」のプロジェクトの一環として、ブラジルの CERT.br（ブラジルコンピュータ緊急対応チーム）を訪問し、施設を見学するとともに設立背景や活動の詳細についてヒアリングを行いました。

4.4.3.6. チュニジア TunCERT 往訪（11 月 28 日）

チュニジアの TunCERT（チュニジアコンピュータ緊急対応チーム）を訪問し、活動の状況についてヒアリングを行うとともに、今後の協力について意見交換を行いました。

4.4.3.7. ベトナム VNCERT 来訪（12 月 4 日）

ベトナム VNCERT（ベトナムコンピュータ緊急対応チーム）が来訪し、日本国内の CSIRT の活動状況について説明を行いました。

4.4.3.8. 台湾 TWNCERT 往訪（12 月 11 日）

台湾の TWNCERT（台湾コンピュータ緊急対応チーム）を訪問し、活動の状況についてヒアリングを行うとともに、今後の協力について意見交換を行いました。

4.4.3.9. ベトナム VNCERT、AIS 往訪（12 月 13 日）

ベトナム VNCERT（ベトナムコンピュータ緊急対応チーム）、AIS（情報セキュリティ庁）を訪問し、インシデントの対応状況についての確認や、今後の協力の分野について議論しました。

4.4.3.10. フィンランド NCSC-FI 来訪（12 月 14 日）

フィンランドの NCSC-FI（National Cyber Security Centre Finland）が来訪し、活動の状況について意見交換を行いました。

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。
脆弱性関連のうち、脆弱性の開示（ISO/IEC 29147）については、8 月 7 日から 10 月 2 日まで最終国際標準草案(FDIS；Final draft of international standard)が国際投票に付され、すべての参加国の賛同を得ました。本案に対して、JPCERT/CC からも参加した 9 月 30 日から 10 月 4 日までイェービク(ノルウェイ)で開催された SC27 の WG 会議で若干の修正を加えた後，新しい国際標準として 10 月下旬から公表されています。
また、脆弱性の取扱手順（ISO/IEC 30111）については 10 月 31 日から 2019 年 1 月 23 日まで国際標準草案(DIS；Draft of international standard)が国際投票に付されており、JPCERT/CC では、これに対する

日本の対応方針案をまとめて情報規格調査会に提案しました。

5. 日本シーサート協議会（NCA）事務局運営

5.1. 概況

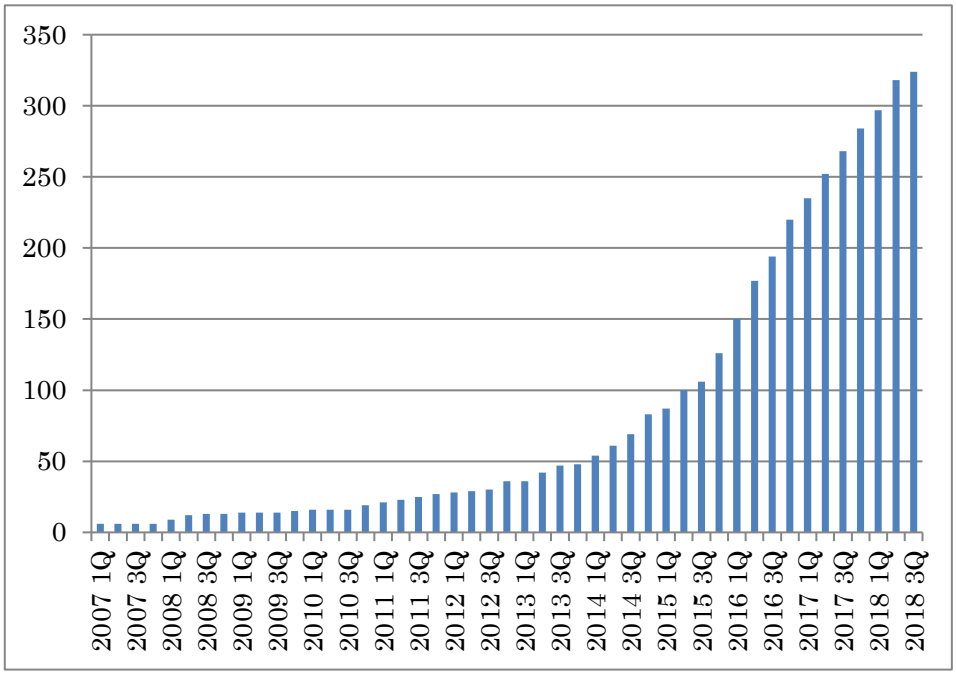
日本シーサート協議会（NCA：Nippon CSIRT Association；本節の以下において「協議会」）は、国内のシーサート（CSIRT：Computer Security Incident Response Team）組織が互いに協調し、連携して共通の問題を解決する場として 2007 年に設立されました。その事務局として、JPCERT/CC は、NCA の Web サイトの管理や更新を通じた広報活動、協議会の問合せ窓口やメーリングリストを含む会員情報の管理、加盟のためのガイダンスの実施および手続きの運用を担当するとともに、自らも会員として協議会の活動に参加しています。

本四半期には、次の 10 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。

株式会社エムティーアイ (MTI-CSIRT)
株式会社インテージホールディングス (ITGG-CSIRT)
株式会社フロムスクラッチ (b-dash-CSIRT)
SKY 株式会社 (Sky-SIRT)
東邦ガス株式会社 (THG CSIRT)
北海道電力株式会社 (TOMARI-CSIRT)
株式会社 LIFULL (LIFULL-CSIRT)
株式会社 システムエグゼ (EXE-CSIRT)
株式会社神戸デジタル・ラボ (KDL-SIRT)
株式会社コナミデジタルエンタテインメント (KDE-CSIRT)

本四半期末時点で※324（一般会員 322、協力会員 2）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。

※集計は協議会 Web の掲載時期をもとに実施。実際の加盟承認時期と若干のタイムラグが生じる場合があります。



［図 5-1 日本シーサート協議会 加盟組織数の推移］

5.2. 第 23 回シーサートワーキンググループ会

第 23 回シーサートワーキンググループ会が次のとおり開催されました。JPCERT/CC は事務局としてこの開催のための各種サポートを行いました。

日時：2018 年 12 月 6 日（木）
場所：工学院大学新宿キャンパス 3F

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、次の講演が行われました。

演題 1 ：「「CSIRT に向いている人の適性判断」資料の NCA 内部公開について」
講演者：SoftBank CSIRT 松本 勝之 氏

演題 2 ：「SIM3 使ってみたら・・・」
講演者：AT-CSIRT 小村 誠一 氏

演題 3 ：「CSIRT Framework 日本語版の紹介・・・その後」
講演者：NCA 専門委員 石塚 元 氏

演題 4 ：「FIRST の教育コンテンツと活用方法の紹介」
講演者：Fuji Xerox CERT 増田 佳弘 様 、NTT-CERT 小崎 武博 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 137 回運営委員会
開催日時：2018 年 10 月 24 日（水）16:00 - 18:00
開催場所：JPCERT/CC

第 138 回運営委員会
開催日時：2018 年 11 月 21 日（水）16:00 - 18:00
開催場所：Canon-CSIRT

第 139 回運営委員会
開催日時：2018 年 12 月 19 日（水）16:00 - 18:00
開催場所：TM-SIRT

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。また、協議会は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

6.1.1 フィッシングの動向等に関する情報発信

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 17 件（ニュース：6 件、緊急情報：11 件）発信しました。

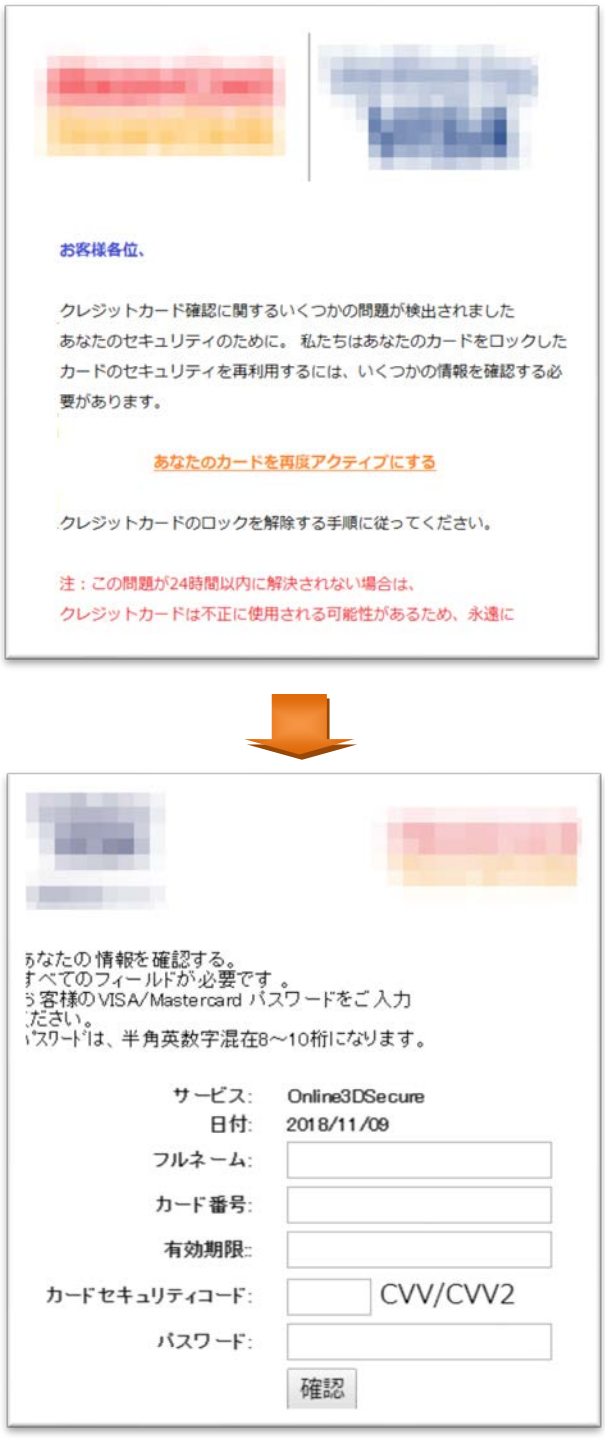
前四半期に引き続き、本四半期も Apple や Amazon、LINE、クレジットカード会社などをかたりクレジットカード情報を詐取するフィッシングの報告が多く寄せられました。また、佐川急便の不在通知メールサービスを装ったショートメッセージ（SMS）から誘導されるフィッシングも続いており注意を呼びかけました。また、キャリア決済の不正利用を目的としたモバイルキャリアをかたるフィッシングサイトの報告も続きました。フィッシングに対する心構えがないスマートフォンユーザを広範囲に狙っていると考えられます。

利用者数が多く、影響範囲も大きい報告については、緊急情報を 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。

MUFG カードをかたるフィッシング件：1 件
Amazon をかたるフィッシング：4 件
Apple をかたるフィッシング：1 件
PayPal をかたるフィッシング：1 件
OMC Plus をかたるフィッシング：1 件
3D セキュア（本人認証サービス）の認証情報を詐取することを目的としたフィッシング：1 件
全国銀行協会をかたるフィッシング件：1 件
三井住友銀行をかたるフィッシング：1 件

本四半期の特筆すべきフィッシング事案として、3D セキュア（本人認証サービス）の認証情報を詐取することを目的としたフィッシングがありました。3D セキュアはクレジットカード決済をより安全に行うためにクレジットカード会社が推奨する本人認証サービスです。決済時にクレジットカードに表示されている情報に加えて、利用者本人しか知らないパスワードを合わせて認証に利用することで安全性を高めていますが、このパスワードの詐取を狙ったものになります。
3D セキュアは旅行会社でのオンライン決済時の本人認証サービスとして導入されていることが多く、日本サイバー犯罪センター (JC3) からも 10 月 18 日に、フィッシングなどにより詐取されたクレジットカード情報が旅行サービス（宿泊施設、航空券、テーマパークのチケット等）の不正購入に利用されているという注意喚起が行われています。協議会への報告も少数ながら続いていることから、今後も注意が必要です。

参考情報: 日本サイバー犯罪センター（JC3）：不正トラベル対策の実施
https://www.jc3.or.jp/topics/travel_fraud.html



［図 6-1 3D セキュア（本人認証サービス）の認証情報を詐取することを目的としたフィッシングサイト ］

https://www.antiphishing.jp/news/alert/3dsecure_20181109.html

6.1.2 定期報告

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 10 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201810.html
2018 年 11 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201811.html
2018 年 12 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201812.html

6.1.3 フィッシングサイト URL 情報の提供

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やフィッシングに関する研究を行っている学術機関等に該当する協議会の会員に対し、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。これは、フィッシング対策製品の強化や、関連研究の促進を目的としたものです。本四半期末の時点で 38 組織に対し URL 情報を提供しており、今後も要望に応じて提供を拡充する予定です。

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独自の活動を、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 65 回運営委員会
日時：2018 年 10 月 12 日 16:00 - 18:00
場所： 株式会社日立システムズ

第 66 回運営委員会
日時：2018 年 12 月 7 日 15:00 - 17:00
場所：株式会社日本レジストリサービス（JPRS）大阪オフィス

7.2 ワーキンググループ会合等 開催支援

本四半期においては、次のとおり開催された協議会のワーキンググループ等の会合の開催の支援と参加を行いました。

技術・制度検討ワーキンググループ会合
日時：2018 年 10 月 17 日 16:00 - 18:00
場所：JPCERT/CC

認証方法調査・推進ワーキンググループ会合
日時：2018 年 10 月 30 日 15:00 - 17:00
場所：アルプス電気本社ビル内

フィッシング対策セミナー2018
日時：2018 年 11 月 2 日 13:00 - 18:00
場所：大崎ブライトコアホール
https://www.antiphishing.jp/news/event/antiphishing_seminar2018.html

技術・制度検討ワーキンググループ会合
日時：2018 年 11 月 28 日 16:00 - 18:00
場所：三菱総合研究所会議室

認証方法調査・推進ワーキンググループ会合
日時：2018 年 12 月 10 日 15:00 - 17:00
場所：アルプス電気本社ビル内

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。

ソフトウェア等の脆弱性関連情報に関する届出状況[2018 年第 3 四半期（7 月～9 月）]
（2018 年 10 月 24 日）
https://www.jpcert.or.jp/press/2018/vulnREPORT_2018q3.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(2018 年 7～9 月)
（2018 年 10 月 18 日）
https://www.jpcert.or.jp/tsubame/report/report201807-09.html
https://www.jpcert.or.jp/tsubame/report/TSUBAMEReport2018Q2.pdf

8.3. JPCERT/CC Eyes～JPCERT コーディネーションセンター公式ブログ～

2018 年 10 月 23 日に JPCERT/CC は、JPCERT コーディネーションセンター公式ブログ「JPCERT/CC Eyes」を開設しました。本ブログは、これまで同様に JPCERT/CC が分析・調査した内容はもちろん、TSUBAME（インターネット定点観測システム）で観測された動向や国内外のイベントやカンファレンスの様子などをいち早くお届けするプラットフォームです。
なお、これに伴い、これまで多くの皆さまにご愛読いただいてきた「分析センターだより」や「インシデントレスポンスだより」、「コラム」の各コンテンツグは新ブログに一本化させていただきました。また、各コンテンツの過去の記事についても、新ブログに移し替えましたので、ご覧いただく際にはご留意く

ださい。本四半期においては次の 9 件の記事を公開しました。

日本語版発行件数：6 件　https://blogs.jpcert.or.jp/ja/

2018-10-23　JPCERT コーディネーションセンター公式ブログ 「JPCERT/CC Eyes」を開設しました！
2018-10-30　マルウエア TSCookie の設定情報を正常に読み込めないバグ
2018-11-06　“渡り鳥”Mejiro モンゴル～バリ島 10,000km の旅
2018-12-06　Hardening II SecurEach に参加しました
2018-12-20　国際カンファレンス講演記 ～Black Hat USA, BSides LV, CODE BLUE～
2018/12/25　アフリカ CSIRT 構築支援 ~チュニジア編~

英語版発行件数：3 件 https://blogs.jpcert.or.jp/en/

2018-10-23　Welcome to New JPCERT/CC Blog site!
2018-11-12　Bug in Malware “TSCookie” - Fails to Read Configuration –
2018-11-27　“Mejiro” – A bird of Passage over 10,000km from Mongolia to Bali –

9. 主な講演活動

(1) 真鍋 敬士（理事・最高技術責任者）：
「サイバーインシデントの傾向とその対策」
NXTWORK 2018 for Japan Partners,2018 年 10 月 3 日
(2) 森 淳太朗（早期警戒グループ）：
「情報セキュリティ研修【基礎編】」
目黒区役所研修，2018 年 10 月 15 日
(3) 真鍋 敬士（理事・最高技術責任者）：
「最近のサイバー攻撃の傾向と国内における取組」
総務省 情報システム統一研修「情報セキュリティ運用」 ，2018 年 10 月 22 日、12 月 18 日
(4) 洞田 慎一（早期警戒グループ マネージャー）：
「大学等におけるサイバー攻撃事例から考えるインシデントへの対応」
北海道大学 役員・部局長/情報セキュリティ管理者向けセミナー,2018 年 10 月 16 日
(5) 米澤 詩歩乃（早期警戒グループ）：
「最近のサイバー攻撃の動向と対策について」
建設コンサルタンツ協会 平成 30 年度情報セキュリティ講習会,2018 年 10 月 31 日
(6) 宮地利雄 (技術顧問)：
「制御システムにおけるサイバーセキュリティの動向」
計測自動制御学会 プラント運転の安全と高度化を考える講演会, 2018 年 11 月 6 日

(7) 森崎 樹弥（早期警戒グループ）：
「最新のサイバー攻撃動向から考えるインシデントレスポンス」
鹿児島県情報サービス産業協会主催セミナー,2018 年 11 月 16 日

(8) 宮地利雄 (技術顧問)：
「安全計装システムを狙ったマルウエア Hatman について」
石油化学工業協会・情報セキュリティ WG&情報セキュリティ対応部会の合同会合, 2018 年 11 月 19 日

(9) 洞田 慎一（早期警戒グループ マネージャー）：
「Society5.0 社会における IoT をとりまくセキュリティの現状と対策への考え方」
第 10 回 TCG 日本支部(JRF)公開ワークショップ,2018 年 11 月 22 日

(10) 輿石 隆（早期警戒グループ）：
「迫りくる標的型攻撃に備えて」
Internet Week 2018,2018 年 11 月 28 日

(11) 真鍋 敬士（理事・最高技術責任者）：
「サイバーセキュリティにおける脅威と取り組み」
ラック＆アカマイ・テクノロジーズ事例セミナー,2018 年 11 月 29 日

(12) 真鍋 敬士（理事・最高技術責任者）：
「サイバーインシデントの最新動向と各組織に期待される取り組み」
Canon Security Days,2018 年 12 月 5 日

(13) 河野 一之（制御システムセキュリティグループ）：
「製造業の制御システムユーザが実践すべき産業用 IoT 導入時のセキュリティ対策の第一歩とは」
ひろしま AI・IoT 進化型ロボット展示会,2018 年 12 月 13 日

(14) 藤井 吉弘（制御システムセキュリティグループ）：
「JPCERT/CC における ICS セキュリティに対する取り組みについて」
日本ガス協会 2018 年度ガスセプター会議,2018 年 12 月 14 日

10. 主な執筆活動

(1) 中谷 昌幸、秋田 卓（制御システムセキュリティグループ）：
「制御システムセキュリティアセスメントサービス」
工業技術社 月刊計装 11 月号,2018 年 10 月 10 日

(2) 河野 一之（制御システムセキュリティグループ）：
「アセットオーナーのための工場における産業用 IoT 導入時のセキュリティ対策ガイド」
工業技術社 月刊計装 12 月号,2018 年 11 月 10 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) 第14回IPAひろげよう情報モラル・セキュリティコンクール2018
主　催：IPA 独立行政法人 情報処理推進機構
開催日：2018年6月1日～2019年3月31日

(2) Hardening Project 2018
主　催：Web Application Security Forum Hardening Project実行委員会,内閣府 沖縄総合事務局
開催日：2018年7月～11月

(3) 第18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　迷惑メール対策委員会
開催日：2018年11月8日

(4) 第10回TCG日本支部(JRF)公開ワークショップ
主　催：TCG日本支部
開催日：2018年11月22日

(5) CODE BLUE2018
主　催：CODE BLUE 実行委員会
開催日：2018年11月27日～11月30日

(6) Internet Week2018
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(JPNIC)
開催日：2018年11月27日～11月30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　：secure-coding@jpcert.or.jp
■公開資料、講演依頼、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