JPCERT/CC 活動概要

2020 年 7 月 1 日 ～ 2020 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

2020 年 10 月 15 日

活動概要トピックス

ー トピック 1ー 働き方の変動下におけるセキュリティ動向を総括し注意喚起

2020 年 4 月以降、新型コロナウイルス感染症（COVID-19）の影響によるテレワークの増加をはじめ働き方に変化が生じています。また、不規則な出勤体制やオフィスでの作業減少にともない、インシデントや脆弱性に対応しづらい状況が続いています。このような状況下で、2020 年 6 月以降、リモート接続が可能なシステムおよび製品の一部に深刻な脆弱性が多数確認されています。さらに、2020 年 7 月にはマルウェア Emotet（エモテット）が活動を再開し、感染に繋がるメールが確認されています。

こうした状況をふまえ、JPCERT/CC は、CyberNewsFlash「2020 年 4 月から 8 月を振り返って」を 8 月 24 日に公開しました。本ブログでは、2020 年 4 月以降に確認された、深刻かつ影響範囲の広い脆弱性情報や攻撃情報をまとめ、自組織が運用するサーバーやネットワーク機器の設定、アップデート状況を改めて見直すことや、Emotet の感染を防ぐための対策を検討するよう、広く注意を呼びかけました。また、脆弱性の影響を受ける製品およびバージョンを利用していることが確認できた組織や管理者に対して、個別通知の活動を行っております。

今後も不規則な勤務環境下でのセキュリティ対応の継続が予想されますが、JPCERT/CC では引き続き被害の抑制に繋がる情報発信や活動を実施してまいります。

CyberNewsFlash「2020 年 4 月から 8 月を振り返って」
https://www.jpcert.or.jp/newsflash/2020082401.html

ー トピック 2ー JPCERT/CC 感謝状 2020 ～脆弱性とインシデント報告に関連して 5 組織の方々に感謝状を贈呈

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」）による被害を低減するために、インシデントへの対応支援、インシデントを未然に防ぐための早期警戒情報の発信、マルウェア分析、ソフトウェア製品等の脆弱性の取り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、さまざまな皆さま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さまからの御厚意と御力添えに深く思いをいたし、特に大き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。

本年度の感謝状をお贈りした方のうち、NTT セキュアプラットフォーム研究所の秋山 満昭 様には、ソフトウェア製品等の脆弱性に関する調整活動において、関係者とのスムーズな調整やアドバイザリの作成などに多大なるご協力をいただき、従来の JPCERT/CC と対象ベンダーが 1 対 1 で行う調整だけではない、より多くの関係者を巻き込む新しい調整活動にお力添えいただきました。

株式会社インターネットイニシアティブ 九州支社の今井 健 様、理化学研究所の市原 卓 様、ヤフー株式会社の大角 祐介 様、伊藤忠商事株式会社 IT 企画部 ITCCERT 様には、マルウェアの分析や国内のサイバー攻撃による被害の低減につながる数多くのご報告をいただきました。

今年度、オンラインで行われた贈呈式の模様は JPCERT/CC 公式ブログ（JPCERT/CC Eyes）で紹介しています。

JPCERT/CC 感謝状 2020
https://www.jpcert.or.jp/press/priz/2020/PR20200917-priz.html

JPCERT/CC Eyes「JPCERT/CC 感謝状 2020～オンライン贈呈式にて」
https://blogs.jpcert.or.jp/ja/2020/09/jpcertcc-priz-2020.html

目次

本活動は、経済産業省より委託を受け、「令和２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、「6.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」、「8.主な講演活動」、「9.主な執筆」、「10.協力、後援」には、受託事業以外の自主活動に関する記載が一部含まれています。

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ー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 13,831 件、インシデント件数ベースでは 8,386 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 4,807 件でした。前四半期の 4,201 件と比較して 14%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ェ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/2020/IR_Report20201015.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 5,845 件で、前四半期の 5,262 件から 11%増加しました。また、前年度同期（3,457 件）との比較では、69%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］

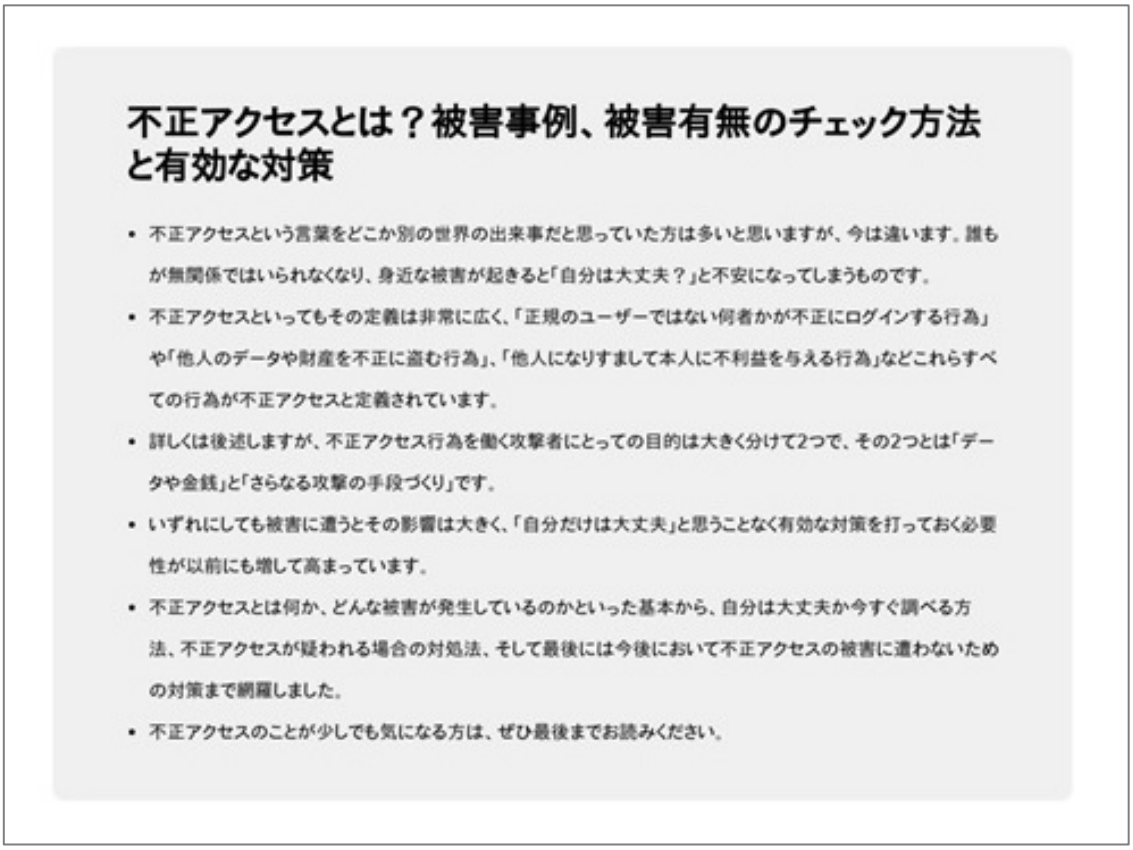
フィッシングサイト	7 月	8 月	9 月	本四半期合計（割合）
国内ブランド	590	607	846	2,043(35%)
国外ブランド	1,089	1,047	986	3,122(53%)
ブランド不明 (注 5)	163	195	322	680(12%)
全ブランド合計	1,842	1,849	2,154	5,845

（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。

国外ブランドについても国内ブランドについても、それぞれ特定の通販サイトを装ったフィッシングサイトのログイン画面を装ったものが非常に多く、ともに過半数を占めています。

その他に国内ブランドでは、国内の銀行やクレジットカード会社のオンラインサービスや、インターネットサービスプロバイダーなどが提供する Web メールのログイン画面を装ったものが増加傾向にありました。
また、フィッシングサイトのドメインには、正規サイトのドメインやブランド名に英数字を加えた.com や.top、.cn、.xyz ドメインが多く使われていました。

一部の国内の銀行を装ったフィッシングサイトの中には、PC 上のブラウザーからアクセスすると、スマートフォン等でアクセスした時とは異なる次のようなコンテンツを表示させるものもありました。



［図 1-1：PC 上のブラウザーからアクセスした際に表示されるコンテンツ］

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 50%、国外が 50%）と比べて国外への通知の割合が増加しました。

1.1.1.2. Web サイト改ざん

本四半期に報告が寄せられた Web サイト改ざんの件数は、374 件でした。前四半期の 291 件から 29%増加しています。

本四半期は、改ざんされた Web サイトから、次のような URL で示される Web サイトを経由し、不審なサイトに転送される報告が複数寄せられました。

```
https[:]//somelandingpage[.]live/?utm_campaign=<ランダムな英数字>&t=main7d
```

この転送は、検索エンジン経由でアクセスを行った場合にのみ発生し、Web ページに直接アクセスを行った場合には、無害なコンテンツが表示されるようになっていました。［図 1-2］は、改ざんされた Web ページを検索エンジン経由でアクセスした際に表示されるコンテンツの例です。

［図 1-2：転送コードの例］

今回報告のあった事例では、最終的に当選詐欺の Web サイトや、不審な商品販売サイトなどが表示されることを確認しています。

1.1.1.3. その他

標的型攻撃に分類されるインシデントの件数は、16 件でした。前四半期の 6 件から 167%増加しています。次に、確認されたインシデントを紹介します。

(1) Lazarus グループによる攻撃

本四半期には、Lazarus（Hidden Cobra とも言われる）と呼ばれる攻撃グループによる国内組織を狙った標的型攻撃の報告が寄せられました。攻撃には、ネットワーク侵入時には、侵入するために使われたマルウェアとは異なるものによって攻撃が行われていました。また、ネットワーク内で感染を広げるために、攻撃者は GitHub などで公開されているフリーのツールなどを使用していました。ネットワーク侵入後に使われるマルウェアについては公式ブログ「JPCERT/CC Eyes」で詳細を解説しています。

攻撃グループ Lazarus がネットワーク侵入後に使用するマルウェア
https://blogs.jpcert.or.jp/ja/2020/08/Lazarus_malware.html

(2) マルウェア Winnti を利用した攻撃

8 月頃に報告が寄せられた標的型攻撃ではマルウェア Winnti が使用されていました。複数のクラウドサーバーがマルウェア感染の被害にあっており、攻撃者が社内に設置されサーバーだけではなく、外部のクラウドサービスを利用したサーバーもターゲットにしていることがわかりました。

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、国内の企業ユーザーが利用するソフトウェア製品の脆弱性情報、国内のインターネットユーザーが影響を受ける可能性のあるコンピューターウイルス、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、あわせて脆弱性やウイルス検体の検証等も必要に応じて行っています。さらに、分析結果に応じて、国内の企業、組織のシステム管理者を対象とした「注意喚起」（一般公開）や、国内の重要インフラ事業者等を対象とした「早期警戒情報」（限定配付）等を発信することにより、国内におけるサイバーインシデントの発生・拡大の抑止を目指しています。

1.2.1. 情報提供

JPCERT/CC の Web ページ（https://www.jpcert.or.jp/）や RSS、約 33,000 名の登録者を擁するメーリングリスト、早期警戒情報の提供用ポータルサイト 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：13 件（うち更新情報が 2 件）　https://www.jpcert.or.jp/at/

2020-07-01　Microsoft Windows Codecs Library の脆弱性 (CVE-2020-1425, CVE-2020-1457) に関する注意喚起 (公開)
2020-07-06　複数の BIG-IP 製品の脆弱性 (CVE-2020-5902) に関する注意喚起 (公開)
2020-07-08　Microsoft Windows Codecs Library の脆弱性 (CVE-2020-1425, CVE-2020-1457) に関す

る注意喚起 (更新)
2020-07-14　複数の BIG-IP 製品の脆弱性 (CVE-2020-5902) に関する注意喚起 (更新)
2020-07-15　2020 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)
2020-07-15　2020 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)
2020-08-03　SKYSEA Client View の脆弱性 (CVE-2020-5617) に関する注意喚起 (公開)
2020-08-12　2020 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)
2020-08-12　Adobe Acrobat および Reader の脆弱性 (APSB20-48) に関する注意喚起 (公開)
2020-08-14　Apache Struts 2 の脆弱性 (S2-059、S2-060) に関する注意喚起 (公開)
2020-08-21　ISC BIND 9 に対する複数の脆弱性に関する注意喚起 (公開)
2020-09-09　2020 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)
2020-09-15　複数の MobileIron 製品の脆弱性に関する注意喚起 (公開)

1.2.1.3. Weekly Report

JPCERT/CC が収集したセキュリティ関連情報のうち重要と判断した情報の抜粋をレポートにまとめ、原則として毎週水曜日（週の第 3 営業日）に Weekly Report として発行しています。このレポートには、「ひとくちメモ」として、情報セキュリティに関する豆知識やお知らせ等も掲載しています。本四半期における発行は次のとおりです。

発行件数：14 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 98 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 14 件でした。

2020-07-01　IPA が「サイバーレスキュー隊（J-CRAT）活動状況 [2019 年度下半期]」を公開
2020-07-08　ICT-ISAC が「家庭内で安全快適に在宅勤務を行うためのリファレンスガイド」を公開
2020-07-15　Japan Security Analyst Conference 2021 の CFP 募集開始
2020-07-22　ISOG-J が「マネージドセキュリティサービス(MSS)選定ガイドライン Ver.2.0」を公開
2020-07-29　マルウエア Emotet の感染に繋がるメールの配布活動の再開について
2020-08-05　JPCERT/CC がログ分析トレーニング用コンテンツの公開
2020-08-13　JAIPA Cloud Conference 2020 開催のお知らせ
2020-08-19　ZeroShell の脆弱性を標的としたアクセスの観測について
2020-08-26　IPA が「【注意喚起】事業継続を脅かす新たなランサムウェア攻撃について」を公開
2020-09-02　「2020 年 4 月から 8 月を振り返って」を公開
2020-09-09　IPA が「情報セキュリティ白書 2020」を公開
2020-09-16　日本シーサート協議会が「新型ウイルス感染リスク禍における CSIRT 活動で考慮すべきこと」を公開
2020-09-25　「フィッシング対策セミナー 2020 (オンライン)」開催のお知らせ

2020-09-30　個人情報保護委員会が「テレワークに伴う個人情報漏えい事案に関する注意事項」を公開

1.2.1.4. 早期警戒情報

JPCERT/CC 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

JPCERT/CC は、脆弱性やマルウェア、サイバー攻撃などに関する最新情報を CyberNewsFlash としてタイムリーに発信しています。注意喚起とは異なり、発行時点で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：21 件（うち更新情報が 4 件）　https://www.jpcert.or.jp/newsflash/

2020-07-14　SAP NetWeaver Application Server Java の脆弱性 (CVE-2020-6287) について
2020-07-15　複数の Adobe 製品のアップデートについて
2020-07-20　マルウエア Emotet の感染に繋がるメールの配布活動の再開について
2020-07-22　複数の Adobe 製品のアップデートについて
2020-07-29　Magento に関するアップデート (APSB20-47) について
2020-07-29　マルウエア Emotet の感染に繋がるメールの配布活動の再開について (追加情報)
2020-08-12　Adobe Lightroom に関するアップデート (APSB20-51) について
2020-08-12　Citrix Endpoint Management のセキュリティアップデートについて
2020-08-13　Intel 製品に関する複数の脆弱性について
2020-08-20　IPA が「事業継続を脅かす新たなランサムウェア攻撃」に関する注意喚起を公開
2020-08-24　2020 年 4 月から 8 月を振り返って
2020-09-03　WordPress 用プラグイン File Manager の脆弱性について
2020-09-04　マルウェア Emotet の感染拡大および新たな攻撃手法について
2020-09-07　DDoS 攻撃を示唆して仮想通貨による送金を要求する脅迫行為 (DDoS 脅迫) について
2020-09-09　Intel 製品に関する複数の脆弱性について
2020-09-09　複数の Adobe 製品のアップデートについて

2020-09-11　複数のマイクロソフト社製品のサポート終了について
2020-09-14　WordPress 用プラグイン File Manager の脆弱性について (更新)
2020-09-16　Netlogon の特権の昇格の脆弱性 (CVE-2020-1472) への早急な対応を
2020-09-17　WordPress 用プラグイン File Manager の脆弱性について (更新)
2020-09-25　Netlogon の特権の昇格の脆弱性 (CVE-2020-1472) への早急な対応を (更新)

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) マルウェア Emotet に関する情報発信

マルウェア Emotet が感染拡大に繋がるメールの配布活動を 2020 年 7 月 17 日頃より再開し、これについて JPCERT/CC は、同月 CyberNewsFlash を発行し、注意を呼びかけました。Emotet は、情報窃取を行うだけでなく、感染端末から窃取した情報を用いてスパムメールを送信し、さらに感染拡大を試みます。Emotet の感染事例は 2019 年 10 月頃から日本国内でも報告が相次ぎ、JPCERT/CC では注意喚起やブログを公開して注意を呼びかけましたが、2020 年 2 月以降、Emotet の感染に繋がるメールの配布が観測されなくなり、活動が沈静化した状況が継続していました。

2020 年 7 月に観測されたメールは、以前に観測されていたメールと内容が似ており、中には感染端末から 2020 年 2 月以前に窃取した情報を用いて送信されたとみられるメールも確認されました。したがって、新たな感染を防ぐ対策だけでなく、以前に感染してしまった組織においても、窃取された可能性のある情報を利用した攻撃などに改めて警戒が必要です。

2020 年 9 月以降に、マルウェア Emotet に感染した国内ドメイン（.jp）のメールアドレスの急増を確認しました。メールの受信者に添付ファイルを実行させるための工夫や、検知回避のための手法の変化など、Emotet の感染を広げるための手口が巧妙化したことが確認されました。こうした状況から、国内におけるさらなる感染拡大を防ぐため、2020 年 9 月 4 日、JPCERT/CC は改めて CyberNewsFlash を公開し、警戒を呼びかけました。

マルウエア Emotet の感染に繋がるメールの配布活動の再開について (追加情報)
https://www.jpcert.or.jp/newsflash/2020072001.html

マルウェア Emotet の感染拡大および新たな攻撃手法について
https://www.jpcert.or.jp/newsflash/2020090401.html

(2) DDoS 攻撃をすると脅して仮想通貨による送金を要求する脅迫行（DDoS 脅迫）に関する情報発信

JPCERT/CC は 2020 年 8 月以降、DDoS 攻撃をすると脅して仮想通貨による送金を要求する脅迫行為に関する情報を複数確認しました。こうした脅迫行為は「DDoS 脅迫」「ransom DDoS」など

とも呼ばれ、攻撃者が標的の組織宛にメールを送り、指定する期間内に仮想通貨を支払わなければ、DDoS 攻撃を実行すると脅迫します。過去にも JPCERT/CC で DDoS 脅迫は確認しており、複数、注意喚起を公開している脅威ですが、2020 年においても引き続き観測されており、さまざまな国や地域の金融業、旅行業、小売業などを標的とした攻撃に関する情報が公表されています。

JPCERT/CC は、国内の組織を標的とした攻撃に関する情報も確認しており、国内の組織においても警戒が必要な状況であることから、2020 年 8 月以降に確認されている攻撃について、攻撃の流れ、手法や特徴を公開情報等をもとに整理し、参考情報として CyberNewsFlash を公開しました。

DDoS 攻撃を示唆して仮想通貨による送金を要求する脅迫行為 (DDoS 脅迫) について
https://www.jpcert.or.jp/newsflash/2020090701.html

(3) BIG-IP の脆弱性に関する情報発信

2020 年 7 月 1 日（米国時間）、F5 Networks から複数の BIG-IP 製品に影響する脆弱性（CVE-2020-5902）に関する情報が公開されました。本脆弱性の影響を受ける製品では、認証されていない遠隔の第三者 Traffic Management User Interface（TMUI）経由で任意のコードを実行するなどの可能性があります。

JPCERT/CC は、本脆弱性を実証したとするコードや、本脆弱性の影響を受ける機器を探索するスキャン、脆弱性の悪用を試みたと推察される通信を確認したため、2020 年 7 月 6 日に、本脆弱性に関する注意喚起を発行し、早期のアップデートを呼びかけました。また、2020 年 7 月 14 日に F5 Networks より本件に関する追加のアドバイザリが公開され、その確認を呼びかけるために注意喚起を更新しました。

複数の BIG-IP 製品の脆弱性 (CVE-2020-5902) に関する注意喚起
https://www.jpcert.or.jp/at/2020/at200028.html

1.3. インターネット上でリスク源となり得るノードの状態と活動を示す観測データの収集および分析

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ー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、サイバー空間全体の健全性を次の 2 つの側面から観測し分析しています。インターネット・ノード（以下「ノード」）のうち攻撃の踏み台として利用されやすいものの多寡と、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ー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 —

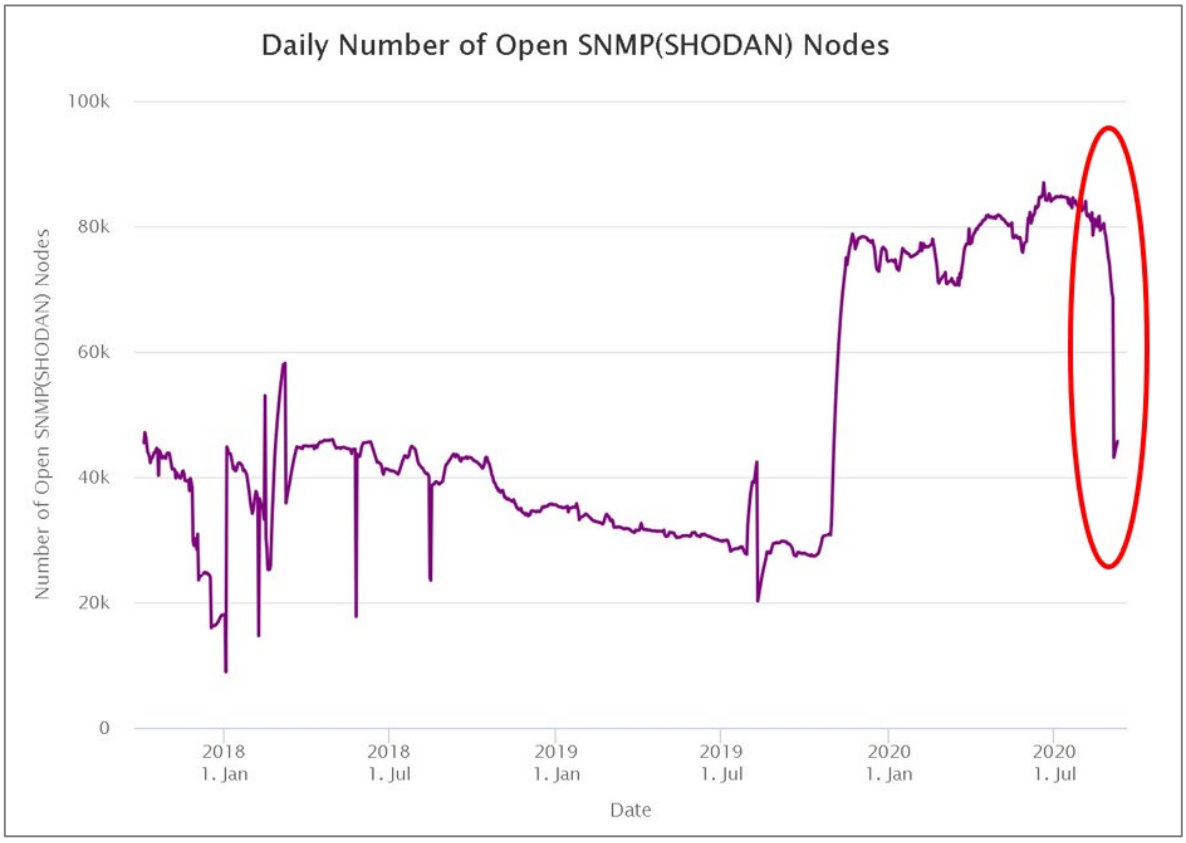
インターネットリスク可視化サービス Mejiro では、次のポートがインターネットに対して開いているノードを DoS リフレクション攻撃（DRDoS）に悪用される恐れのあるインターネット上のリスク要因と見なし、その国や地域ごとの分布状況を分析しています。

（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）

それらのノードの IP アドレスをもと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。さらに、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、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。

1.3.1.2. オープン SNMP のノード数減少について

JPCERT/CC 活動概要 [2020 年 1 月 1 日～2020 年 3 月 31 日] で、日本国内に割り当てられた IP アドレスをもつもので SNMP（161/Udp）に応答するノードの数が増加した問題について論じましたが、2020 年 7 月下旬ごろよりノード数が減少していることが確認できました。



［図 1-3：（例）フィリピンの ASN 別集計結果画面］

SNMP に応答するノード数の増加は、昨年 10 月頃から観測されるようになり、当該ノードが攻撃に悪用されることを懸念した JPCERT/CC では当該ノードの状況を調査するとともに、関係者に可能な限りの連絡を試みました。ノードの状況調査からは、SNMP だけでなく telnet（23/TCP）やアクセスすれば機器の設定を閲覧できるようなポートも開いたままになっていることが判明しました。関係者への連絡によって、当該機器の製造ベンダーに、当該ノードの設定を行っていた業者を特定するとともに JPCERT/CC からの指摘事項を当該業者に伝達していただくことになりました。7 月下旬以降の問題ノードの減少は、これが功を奏して、機器設定の是正が進んだことによるものと推測しています。
不要なポートをインターネットに向けて開放することが望ましくないことは言うまでもありませんが、中でも SNMP や DNS、NTP などのポートが解放されていると、重要インフラ等を含む他のサイトへの DDoS 攻撃に悪用される可能性が強く懸念されるところです。インターネット上には、そうした問題を抱えた多数のノードが存在しています。JPCERT/CC では、今後も継続的に Mejiro のデータを活用し

て、問題のあるノードの増加の気配をいち早く察知し、悪用される前に解決を促す活動を続けていきます。

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/

1.3.2. 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

1.3.2.1. 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ーを開発し、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」）を構築し運用しています。TSUBAME から得られる情報を、すでに公開されている脆弱性情報やマルウェア、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。
観測用センサーの設置に協力した 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

1.3.2.2. TSUBAME の観測データの活用

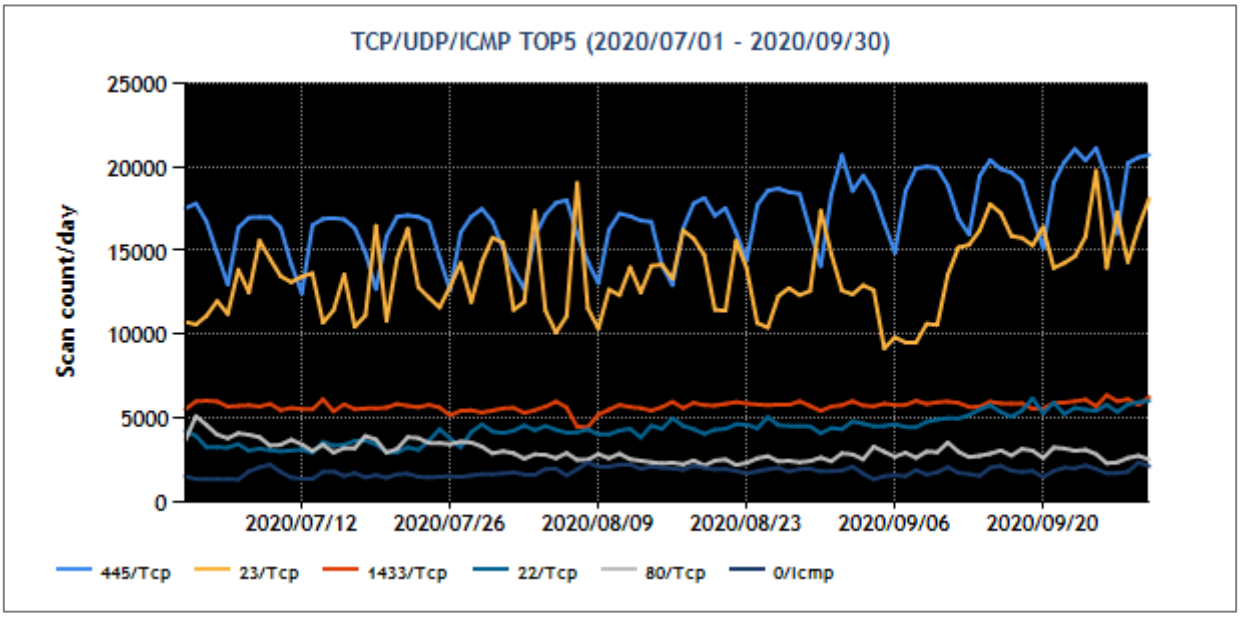
JPCERT/CC では、主に日本企業のシステム管理者の方々に、自組織のネットワークに届くパケットの傾向と比較していただけるよう、日本国内の TSUBAME のセンサーで受信したパケットを宛先ポート別に集計してグラフ化し、毎週月曜日に JPCERT/CC の Web ページで公開しています。また、四半期ごとに観測傾向や注目される現象を紹介する「インターネット定点観測レポート」を公開しており、2020 年 4 月から 6 月分のレポートを 2020 年 7 月 30 日に公開しました。

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

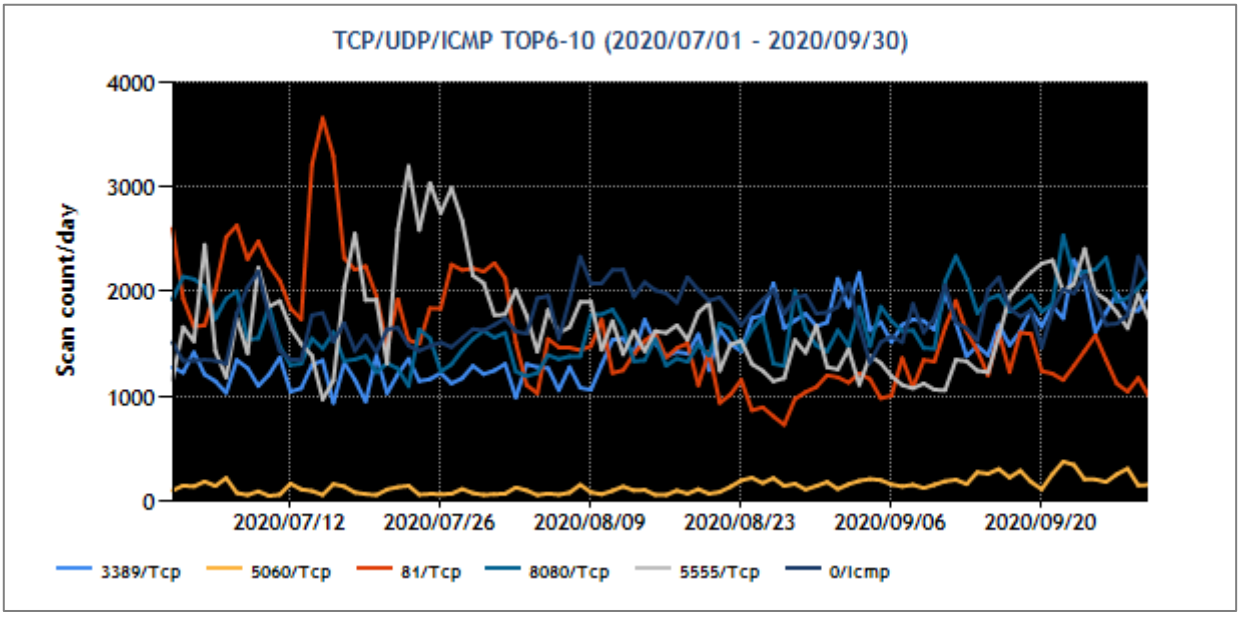
インターネット定点観測レポート（2020 年 4～6 月）
https://www.jpcert.or.jp/tsubame/report/report202004-06.html

1.3.2.3. 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 1-4 ］と［図 1-5］に示します。



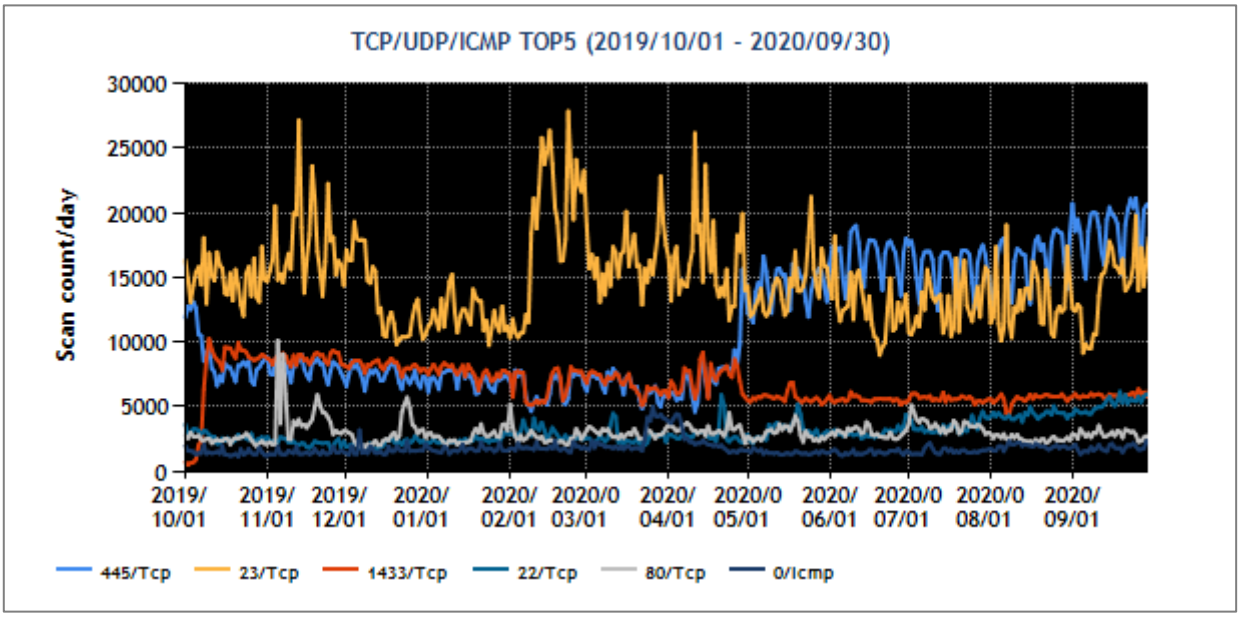
［図 1-4：宛先ポート別グラフ トップ 1-5（2020 年 7 月 1 日-9 月 30 日)］



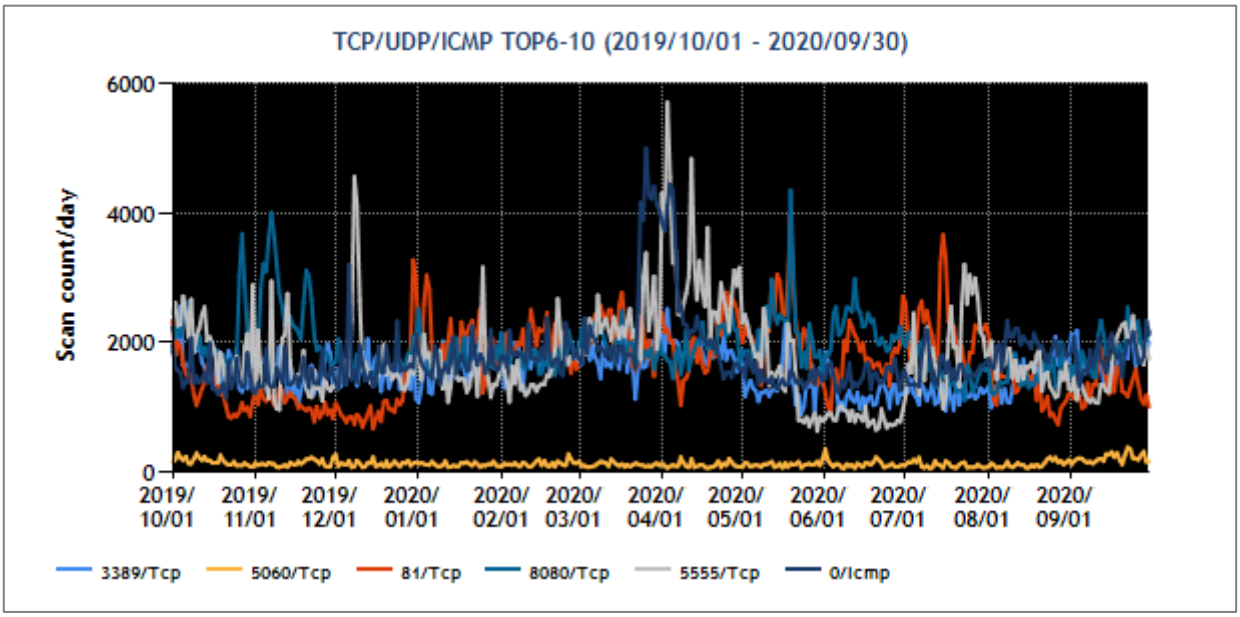
［図 1-5：宛先ポート別グラフ トップ 6-10（2020 年 7 月 1 日- 9 月 30 日)］

また、過去 1 年間（2019 年 10 月 1 日-2020 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 1-6］と［図 1-7］に示します。



［図 1-6：宛先ポート別グラフ トップ 1-5（2019 年 10 月 1 日-2020 年 9 月 30 日）］



［図 1-7：宛先ポート別グラフ トップ 6-10（2019 年 10 月 1 日-2020 年 9 月 30 日）］

本四半期に最も多く観測されたパケットは 445/TCP（microsoft-ds）宛のものでした。4 月下旬から増加し、本四半期末時点では 23/TCP（telnet）宛を上回っています。445/TCP 宛のスキャンの増加原因を考えると、過去の事案と同様に何らかのマルウェアが関与していることが考えられます。現時点では全容の解明に至っていませんが、通知した一部のユーザーからは、Windows サーバーがマイニングを行う

マルウェアに感染していたとの情報提供がありました。

1.3.2.4. 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、スキャン活動を TSUBAME によって観測することに加えて、スキャンに応対した場合に始まる攻撃活動を低対話型ハニーポットにより観測するための試作システムを用意して、その有効性を確認するための試験運用を行っています。試験運用では、簡単なシステムを構築して HTTP リクエストを収集し、それを分析しています。

2020 年 9 月 14 日～15 日にかけて、WordPress 用プラグイン File Manager の脆弱性（CVE-2020-25213）の悪用に向けたスキャンと思われる通信を観測しました。2020 年 9 月 14 日に修正された脆弱性（CVE-2020-25213）の影響を受ける PHP ファイルのスキャンと見られるものであり、当該ファイルの有無を確認後、攻撃を行う可能性が考えられます。観測した内容に基づき、CyberNewsFlash を公開しました。

WordPress 用プラグイン File Manager の脆弱性について
https://www.jpcert.or.jp/newsflash/2020090301.html

また、現在観測している HTTP プロトコル以外のプロトコルに対する攻撃等の脅威動向を調査できるように、複数のハニーポットプログラムの試験を実施しています。今期で試験した 16 種類のハニーポットのうち、6 種類のハニーポットにおいて国内 IP からのスキャン活動を確認しました。マルウェアの感染など、何らかの異常が疑わしい場合などに、取得した通信内容に基づいて通信元への通知を進められるよう、評価や分析を続けていきます。

2. 脆弱性関連情報流通促進活動

JPCERT/CC は、ソフトウェ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、脆弱性情報と製品開発者が用意した対策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。本規程で受付機関に指定されている IPA から届け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け出状況については、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/

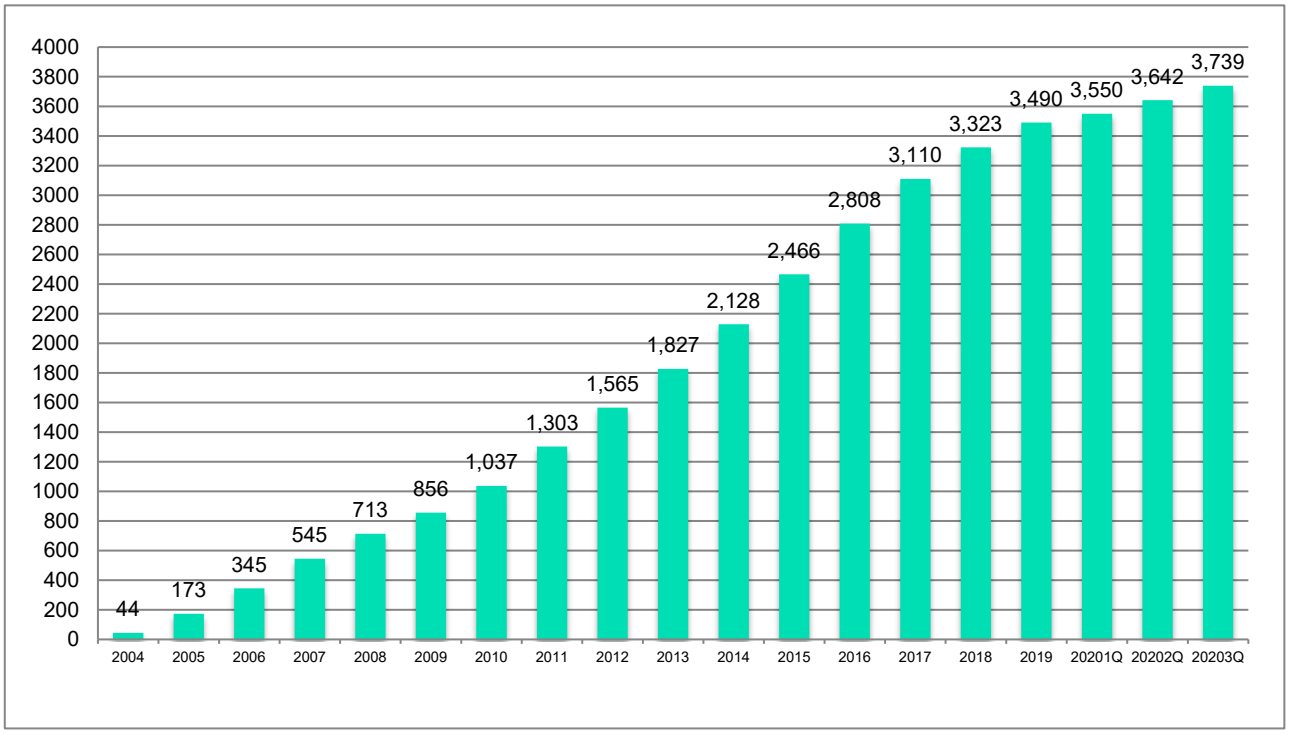
2.1.2. Japan Vulnerability Notes（JVN）において公表した脆弱性情報および対応状況

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 CISA ICS 、NCSC-NL、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等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 97 件（累計 3,739 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/



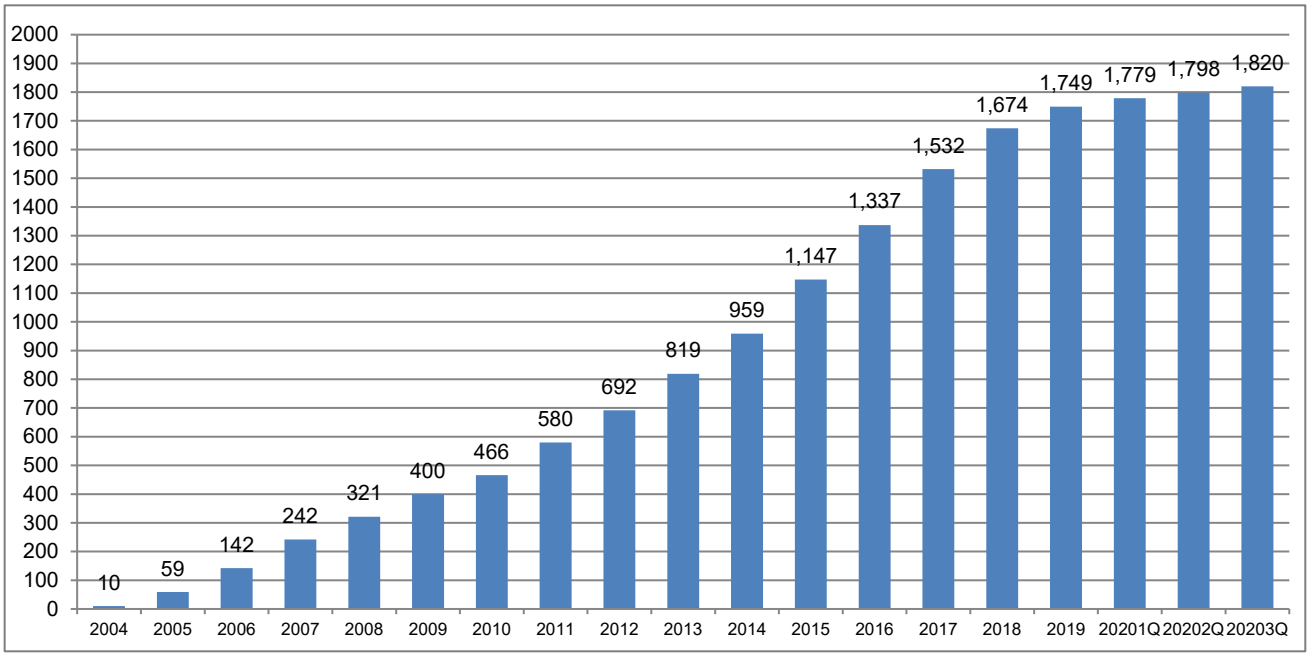
［図 2-1：JVN 公表累積件数］

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 22 件（累計 1,820 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 22 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 19 件（このうち自社製品の届け出によるものが 5 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 2 件、国内外の複数の製品開発者の製品に影響を及ぼすものが 1 件ありました。

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ーごとの内訳は、［表 2-1］のとおりです。本四半期は、サーバー製品が 4 件と最も多く、次いで Android アプリケーションと CMS が 3 件ずつと他の製品に比べ多い状況でした。続いてウェブアプリケーション、組込系製品、制御系製品が 2 件、IT 資産管理ツール、Windows アプリケーション、アプリケーションフレームワーク、スマートフォンアプリケーション、プラグイン、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ー内訳］

製品分類	件数
サーバー製品	4
Android アプリケーション	3
CMS	3
ウェブアプリケーション	2
組込系製品	2
制御系製品	2
IT 資産管理ツール	1
Windows アプリケーション	1
アプリケーションフレームワーク	1
スマートフォンアプリケーション	1
プラグイン	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 75 件（累計 1,919 件）で、累計の推移は［図 2-3］に示すとおりです。75 件のうち 71 件はアドバイザリとして公表したもので、4 件は Technical Alert として公表したものでした。71 件のアドバイザリのうち、海外調整機関や製品開発者等からの届け出によるものおよび製品開発者による脆弱性情報公開の事前通知によるものは 19 件、国内外の発見者からの届け出による

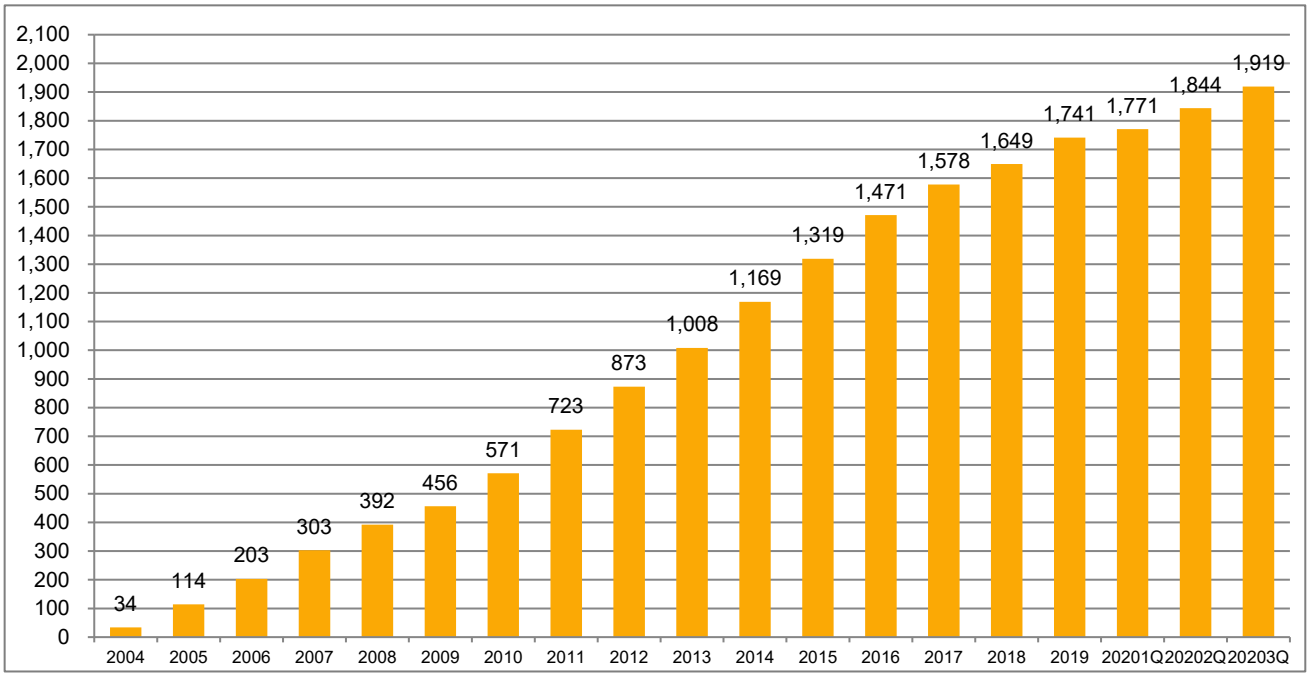
ものは 3 件でした。

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ー内訳は、［表 2-2］のとおりです。本四半期は、制御系製品に関するものが 48 件と最も多く、次いで多かったのは、医療機器、アンチウイルス製品に関するものでそれぞれ 5 件ずつでした。続いてプロトコルに関するものが 4 件、macOS、組込系製品に関するものがそれぞれ 3 件、CMS、DNS、ウェブサーブレットコンテナー、サーバー製品、ドライバー、ファームウェアに関するものおよびその他がそれぞれ 1 件でした。

本四半期も、国際取扱脆弱性情報において、製品開発者自身による届け出や、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。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、調整および公開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ー内訳］

製品分類	件数
制御系製品	48
アンチウイルス製品	5
医療機器	5
プロトコル	4
macOS	3
組込系製品	3
CMS	1
DNS	1
ウェブサーブレットコンテナー	1
サーバー製品	1
ドライバー	1
ファームウェア	1
その他	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。

連絡不能開発者一覧
https://jvn.jp/reply/index.html

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 および CISA ICS、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。

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 では、2008 年 5 月以降 JVN 英語版サイトの公開を機に CVE 採番を行っており、Primary CNA である 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 番号を付与しています。本四半期には、JVN で公表したもののうち国内で届け出られた脆弱性情報に 32 個の CVE 番号を付与しました。

2010 年 6 月からは CNA（CVE Numbering Authorities）として活動するとともに、主に製品開発者を対象として CNA への勧誘、トレーニングなども行っています。

CNA および CVE に関する詳細は、次の Web ページをご参照ください。

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/

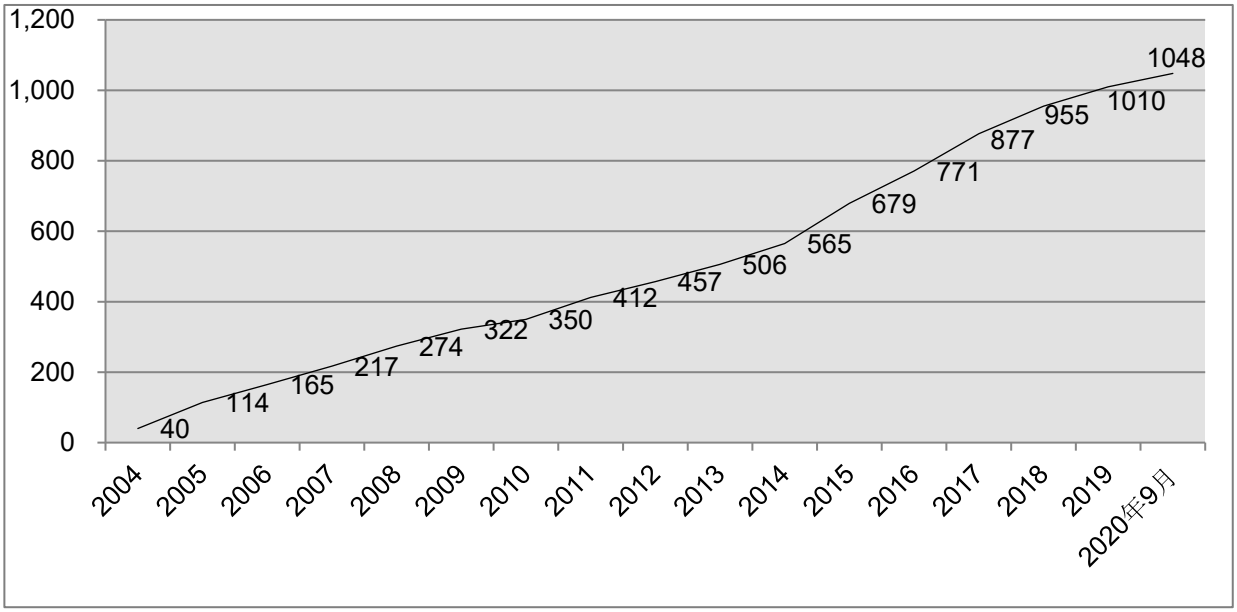
情報セキュリティ早期警戒パートナーシップガイドライン（2019 年版）
https://www.jpcert.or.jp/vh/partnership_guideline2019.pdf

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

2.2.1. 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、2020 年 9 月 30 日現在で 1,048 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. 脆弱性の低減方策の研究・開発および普及啓発

2.3.1. 講演活動

早期警戒グループでは、脆弱なソフトウェ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ェア開発者の方々に伝えるための活動を行っています。

本四半期は次の 2 件の講演を行いました。

(1) 国立情報学研究所トップエスイー2020「セキュアプログラミング」
（2020 年 7 月 22 日、8 月 5 日、8 月 19 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ました。

- 7 月 22 日「セキュアプログラミング - イントロダクション」
- 8 月 5 日「Web 脆弱性とセキュアプログラミング」
- 8 月 19 日「Web 脆弱性検査」

今年度は Zoom を用いたオンライン講義となりました。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) 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 26 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、ソフトウェア開発者向け啓発活動の一環として次の講義を行いました。

- 総論 ： セキュアシステム設計・開発
- セキュアプログラミング演習（Web アプリケーション）

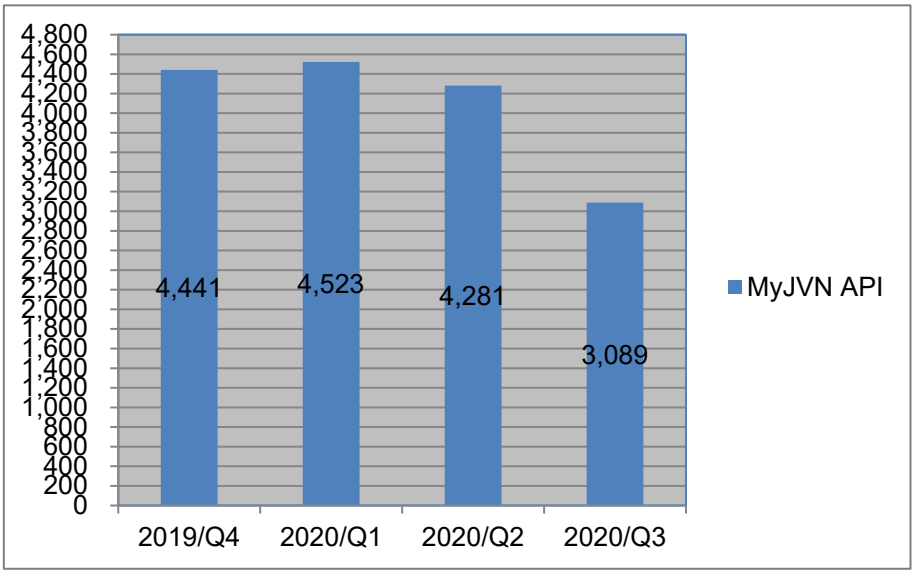
今年度は Zoom を用いたオンライン講義となりました。Web アプリケーションの脆弱性を悪用する攻撃やその対策について、サンプルアプリケーションを用いた実習を行いました。

2.4. VRDA フィードによる脆弱性情報の配信

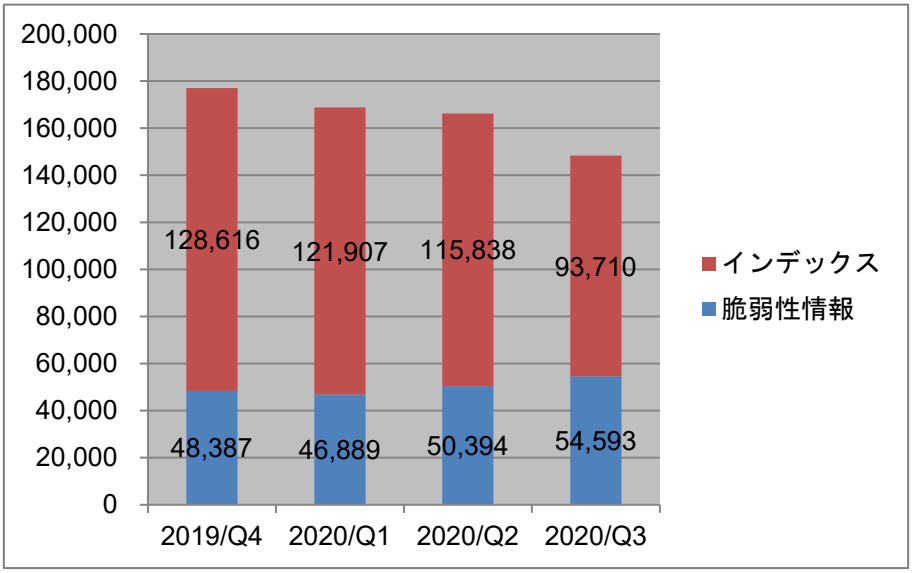
JPCERT/CC は、大規模組織の組織内 CSIRT 等での利用を想定して、ツールを用いた体系的な脆弱性対応を可能とするため、IPA が運用する MyJVN API を外部データソースとして利用した、VRDA（Vulnerability Response Decision Assistance）フィードによる脆弱性情報の配信を行っています。VRDA フィードについての詳しい情報は、次の Web ページを参照ください。

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

四半期ごとに配信した VRDA フィード配信件数を［図 2-5］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。

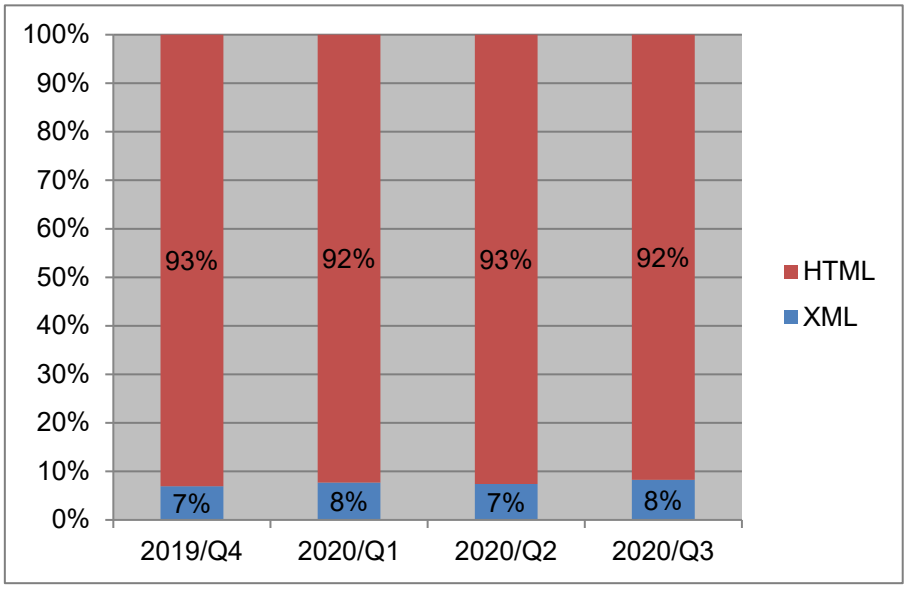


［図 2-5：VRDA フィード配信件数］



［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 19%減少しました。脆弱性情報の利用数については、約 8%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、大きな変化は見られませんでした。

3. 制御システムセキュリティ強化に向けた活動

3.1. 情報収集分析

JPCERT/CC では、制御システムにおけるセキュリティに関わるインシデント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 207 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、その情報を必要とする国内組織に提供しました。

本四半期に提供した参考情報は 3 件でした。

2020/08/27 【参考情報】NERC および NIST が NERC CIP v5 と NIST CSF v1.1 の対応表を公表した件について
2020/08/31 【参考情報】機器に組みこまれた NIC のベンダーを特定する方法を示したホワイトペーパーを FERC と NERC が公表
2020/09/03 【参考情報】OpenFMB に適用可能なセキュリティ対策について検証した結果をまとめた報告書を NIST が公表

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ー（注 1）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。

（注 1）JPCERT/CC が運営するコミュニティーで、制御システム関係者を中心に構成されています。

本四半期は計 3 件を配信しました。

2020/07/06　制御システムセキュリティニュースレター 2020-0006
2020/08/07　制御システムセキュリティニュースレター 2020-0007
2020/09/10　制御システムセキュリティニュースレター 2020-0008

制御システムセキュリティ情報共有コミュニティーでは、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 1,144 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。参加資格や申し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ー
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 1 件（1 IP アドレス）でした。報告内容はインターネットからアクセス可能な制御システムに関するもので、その報告に基づいて調査と調整を行いました。報告者にその結果をお伝えし、本件についての調整を完了しました。

(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は 0 件（0 IP アドレス）でした。

3.3. 関連団体との連携

SICE（計測自動制御学会）と JEITA（電子情報技術産業協会）、JEMIMA（日本電気計測器工業会）が定期的に開催している合同セキュリティ検討ワーキンググループに参加し、制御システムのセキュリティに関して専門家の方々と意見交換を行いました。

3.4. 制御システム向けセキュリティ自己評価ツールの提供

JPCERT/CC では、制御システムの構築と運用に関するセキュリティ上の問題項目を抽出し、バランスの良いセキュリティ対策を行っていただくことを目的として、簡便なセキュリティ自己評価ツールである日本版 SSAT（SCADA Self Assessment Tool：申し込み制）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 に関する利用申込みはなく、直接配付件数の累計は 280 件のままでした。

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 では、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行ってきました。この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 なども参考にして、JPCERT/CC が独自の評価指針に基づいて行う制御システム向けのセキュリティアセスメントです。制御システム利用組織において制御システムのセキュリティ対策の現状把握や課題抽出などに活用していただくことを想定しています。

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、制御システムのセキュリティ対策にお役立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。

今年度は、アセスメントサービスの改善およびアセスメント実施後の組織の取り組みに関する実態把握を目的として、過去にアセスメントを実施した組織に対してアンケートおよびヒアリングを行っています。本四半期は 1 組織にアンケートおよびヒアリングを実施しました。

4. 国際連携活動関連

本四半期も引き続き、新型コロナウイルス感染症対策の観点から世界の多くの国で国外への渡航制限が敷かれ、予定されていた多くの国際会議が中止・延期ないしオンラインでの開催に変更されました。

4.1. 海外 CSIRT 構築支援および運用支援活動

海外の National CSIRT 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、アジア太平洋地域の CSIRT コミュニティーである APCERT について 2003 年 2 月の発足時から継続して Steering Committee（運営委員会）のメンバーに選出されており、また、その事務局も担当しています。APCERT の詳細および APCERT における JPCERT/CC の役割については、次の Web ページをご参照ください。

JPCERT/CC within APCERT
https://www.jpcert.or.jp/english/apcert/

4.2.1.1. APCERT 年次総会 2020 への参加

APCERT の年次総会が 9 月 29 日に開催されました。新型コロナウイルス感染症拡大の影響により、APCERT の年次総会としては初めてのオンライン開催となりました。今年は年次総会のみを実施し、これまで併設されていた講演やワークショップ等を含むカンファレンスセッションについては 2021 年に延期することとなりました。年次総会には APCERT の主要メンバーであるオペレーショナルメンバー（33 チーム）のうち JPCERT/CC を含む 27 チームが参加しました。
任期を満了する半数の Steering Committee メンバーの改選選挙では、ACSC（オーストラリア）、CNCERT/CC（中国）、KrCERT/CC（韓国）、TWNCERT（台湾）が再選されました。また、議長チームおよび副議長チームの改選が行われ、CyberSecurity Malaysia（マレーシア）が議長チームとして、CNCERT/CC が副議長チームとしてそれぞれ再選されました。JPCERT/CC は、引き続き APCERT の事務局および Steering Committee メンバーとしてさまざまな活動をリードしてまいります。

4.2.1.2. APCERT Steering Committee 会議の実施

Steering Committee は、8 月 5 日と 9 月 23 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。本四半期は国内の企業の FIRST 新規加盟に関するサポートを実施しました。
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. TRAFFIC LIGHT PROTOCOL (TLP) FIRST Standards Definitions and Usage Guidance の日本語訳公開

さまざまな組織のインシデント対応チーム間の相互協力を促進するため、インシデント対応の標準化を進めています。その一環として、FIRST 加盟組織は特定のテーマについて議論する SIG（Special Interest Groups）を立ち上げ、インシデント対応チーム間の相互協力を促進する基準の開発が奨励されています。このうち、TLP（Traffic Light Protocol）SIG では、機微な情報の取り扱い基準を示すことで的確な情報の共有を手助けする、TLP の定義を決定する役割を担っています。 TLP は、信号機の色である赤黄緑の 3 色に白を加えた 4 つで、情報の取扱区分を直感的に理解しやすく表示する方法です。「TRAFFIC LIGHT PROTOCOL（TLP）FIRST Standards Definitions and Usage Guidance」は、TLP に関する定義や利用方法、注意事項を述べた文書で、情報の発信者および受信者が情報共有の際に留意すべき点をまとめています。

「TRAFFIC LIGHT PROTOCOL (TLP) FIRST Standards Definitions and Usage Guidance - Version 1.0」は、JPCERT/CC が翻訳を行い、NTT-CERT および Panasonic PSIRT によるレビューを経て、FIRST の Web サイトに公開されました。

TRAFFIC LIGHT PROTOCOL (TLP) FIRST Standards Definitions and Usage Guidance - Version 1.0 日本語版
https://www.first.org/tlp/docs/tlp-v1-jp.pdf

4.3. その他国際会議への参加

4.3.1. 第 8 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 24 日-25 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 24 日から 25 日にかけてオンラインで開催されました。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、前年の会合以降の、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り組み等をそれぞれの CSIRT が報告しました。特に、新型コロナウイルス感染症に関連したサイバー攻撃の状況や各組織の行った対処の取り組みについて活発に意見を交わしました。

4.3.2. EU CYBER FORUM での講演（9 月 17 日）

JPCERT/CC は European Union Institute for Security Studies（欧州安全保障研究所）などが主催する EU CYBER FORUM の複数のパネルディスカッションにオンラインで参加しました。このうち、”International security and emergency response cooperation”と題したセッションでは、海外の National CSIRT 担当者とともに新型コロナウイルス感染症対応下での CSIRT および CSIRT コミュニティーでの活動について紹介し、また、”Youth Cyber Forum”では主に若年層をターゲットとしたサイバーセキュリティ啓発活動の日本における状況について紹介しました。

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 で検討されている「複数の開発者が関与する脆弱性の開示と取扱」の標準化作業と、WG4（セキュリティコントロールとサービスに関する標準化を担当）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。

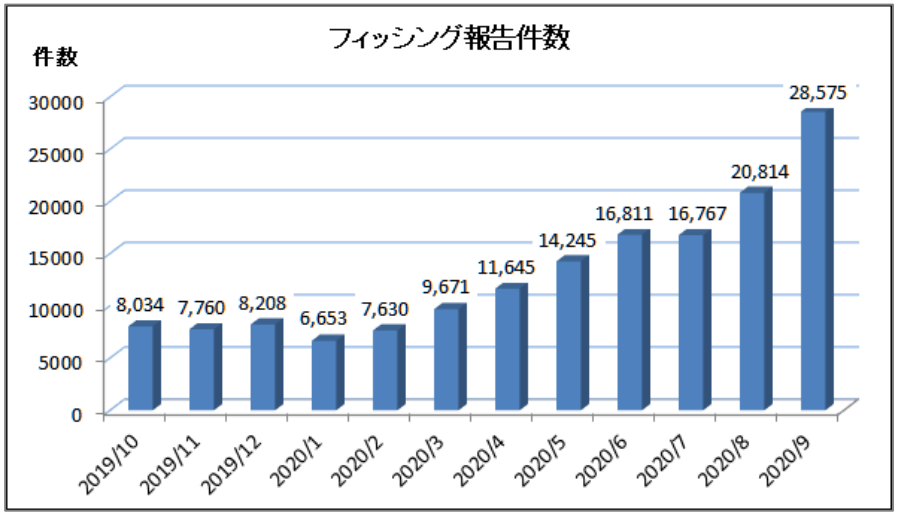
本四半期中 9 月には、ポーランドのワルシャワで開催予定であった会議が、前回に引き続き新型コロナウイルス感染症対策としてオンライン形式に変更して開催されました。「複数の開発者が関与する脆弱性の開示と取扱」に関しては技術文書の作成が 9 月から開始され、技術文書へ項目の追加を提案した Contribution（寄書）を提出しました。

5. フィッシング対策協議会事務局の運営

フィッシング対策協議会（本節の以下において「協議会」）は、フィッシングに関する情報収集・提供と動向分析、技術・制度的対応の検討等を行う会員組織です。JPCERT/CC は、経済産業省からの委託により、協議会の活動のうち、一般消費者からのフィッシングに関する報告・問い合せの受付、フィッシングサイトに関する注意喚起等、一部のワーキンググループ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、Web サイトを停止するための調整等を行っています。

5.1. フィッシングに関する報告・問い合わせの受付

本四半期のフィッシング報告件数は、2020 年初から報告件数がほぼ毎月 20 %程度の増加を続けており、2020 年 8 月には、ひと月で 2 万件を超え、さらに 9 月は 3 万件に迫る非常に多くの報告が寄せられました。（[図 5-1]）



［図 5-1：1 年間のフィッシング報告件数（月別）］

報告件数の内訳は、Amazon、LINE、楽天および楽天カードをかたるフィッシングの報告が多く、この 4 ブランドに関連する報告が全体の約 87.2 %を占めました。

5.2 情報収集 / 発信

5.2.1 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 8 件（ニュース：0 件、緊急情報：8 件）発信しました。
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。その内訳は次のとおりです。

- セブン銀行をかたるフィッシング：1 件
- 宅配便の不在通知を装うフィッシング：3 件
- BTCBOX をかたるフィッシング：2 件
- 三井住友銀行および三井住友カード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

本四半期も前四半期に引き続き、新型コロナウイルス感染症の流行の影響でオンラインショッピングの利用機会が増えたとみられ、Amazon や楽天などのショッピングサイトをかたるフィッシング報告が非常に多く寄せられました。いずれも、ログイン情報のみならず、住所や電話番号などの個人情報ならびにクレジットカード情報の入力を促されるものでした。

また、オンラインショッピングで購入した商品を受け取る機会が増えたためか、宅配便の不在通知をよそおう SMS から誘導されるフィッシングに関する相談も増えました。この宅配便の不在通知をよそおう SMS は 2018 年から断続的に報告が続いており、当初は宅配業者をかたるフィッシングサイトで携帯電話番号と SMS 認証コードを詐取して、キャリア決済を不正利用することを目的としていました。本四半期では同文面の SMS から金融機関をかたるフィッシングサイトへ誘導されることを確認しています。

また、本四半期は正規サービスのドメインを差出人メールアドレスに使用した「なりすまし」フィッシングメールが急増しました。このような「なりすまし」メールに対しては、組織として行う対策である DMARC 等の送信ドメイン認証技術を導入することで、正規の送信元から送られたか否かを受信側で検証し、なりすまされた被害組織が宣言しているポリシーに沿ってフィルタリング等を行うことも可能です。国内のサービス事業者や組織におけるメールセキュリティ対策として、さらなる普及が望まれます。

また、一度に大量送信されるタイプのフィッシングメールについては、迷惑メールフィルター機能などを有効にすることで、そのほとんどが迷惑メールフィルターに検知されていることを確認しており、利用者側のフィッシング対策として迷惑メールフィルター機能は有効と考えられます。

［図 5-2：宅配便の不在通知を装う SMS とフィッシングサイト ］

https://www.antiphishing.jp/news/alert/fuzaiSMS_20200709.html

5.2.2. 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/

2020 年 7 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/202007.html

2020 年 8 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/202008.html

2020 年 9 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/202009.html

5.2.3 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アンチウイルス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 46 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。

5.2.4 フィッシング対策ガイドライン等の改定作業

「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を作成・改訂を行う作業部会です。
今期は、2021 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 WG 会合
  日時：2020 年 8 月 26 日 15:00-17:00

6. 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。

6.1. 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 80 回運営委員会
  日時：2020 年 7 月 28 日(火) 15:30-18:00

- 第 81 回運営委員会
  日時：2020 年 9 月 15 日(火) 15:30-18:00

6.2. 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イベントやワーキンググループ等の会合の開催を支援しました。

- 学術研究プロジェクト会合
  日時：7 月　　毎週火曜日 11:00-11:00
  　　8 月-9 月　毎週火曜日 11:30-11:00

※運営委員会およびワーキンググループ会合等はすべてオンライン開催

6.3. ワーキンググループの成果物の公開支援

本四半期においては、次のとおりワーキンググループの成果物の公開を支援しました。

- 証明書普及促進 WG
  サーバ証明書の有効期限の短縮について
  https://www.antiphishing.jp/news/info/20200714.html

  【更新】主要ブラウザのセキュリティ強化に対する施策について
  https://www.antiphishing.jp/news/info/2020824.html

- 認証方法調査・推進 WG
  インターネットサービス利用者に対する 「認証方法」に関するアンケート調査結果報告書を公開
  http://www.antiphishing.jp/news/info/20200909.html

7. 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。

7.1. 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ー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、インシデントの傾向やインシデント対応事例を四半期ごとにまとめたものです。

2020-07-14　JPCERT/CC インシデント報告対応レポート [2020 年 4 月 1 日～2020 年 6 月 30 日]
https://www.jpcert.or.jp/pr/2020/IR_Report20200714.pdf

2020-09-10　JPCERT/CC Incident Handling Report [April 1, 2020 - June 30, 2020]
https://www.jpcert.or.jp/english/doc/IR_Report2020Q1_en.pdf

7.2. インターネット定点観測レポート

JPCERT/CC では、インターネット上に複数のセンサーを分散配置し、不特定多数に向けて発信されるパケットを継続して収集するインターネット定点観測システム「TSUBAME」を構築・運用しています。脆弱性情報、マルウェ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。

2020-07-30　JPCERT/CC インターネット定点観測レポート [2020 年 4 月 1 日～2020 年 6 月 30 日]
https://www.jpcert.or.jp/tsubame/report/report202004-06.html
https://www.jpcert.or.jp/tsubame/report/TSUBAMEReport2020Q1.pdf

2020-09-10　JPCERT/CC Internet Threat Monitoring Report [April 1, 2020 - June 30, 2020]
https://www.jpcert.or.jp/english/doc/TSUBAMEReport2020Q1_en.pdf

7.3. 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、ソフトウェ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、同期間中に届け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。

2020-07-28　ソフトウェア等の脆弱性関連情報に関する届出状況[2020 年第 2 四半期 (4 月～6 月)]
https://www.jpcert.or.jp/press/2020/vulnREPORT_2020q2.pdf

7.4. 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、国内外のイベントやカンファレンスの様子などを JPCERT/CC のアナリスト一人一人の眼をとおして、いち早くお届けする読み物です。
本四半期においては次の 7 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/

2020-07-28　ログ分析トレーニング用コンテンツの公開
2020-08-31　攻撃グループ Lazarus がネットワーク侵入後に使用するマルウェア
2020-09-29　攻撃グループ Lazarus が使用するマルウェア BLINDINGCAN
2020-09-30　JPCERT/CC 感謝状 2020～オンライン贈呈式にて

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

2020-07-01　Migrate Volatility Plugins 2 to 3
2020-08-31　Malware Used by Lazarus after Network Intrusion
2020-09-29　BLINDINGCAN - Malware Used by Lazarus -

8. 主な講演活動

(1) 洞田 慎一（早期警戒グループ担当部門長 兼 サイバーメトリクスグループ部門長・マネージャー）：
「リモート環境のサイバー攻撃への悪用と対策」
CRC セキュリティ講習会,共通基盤研究施設計算科学センター, 2020 年 9 月 18 日
(2) 佐々木 勇人（早期警戒グループマネージャー）：
「インシデント対応能力を上げて「新しい働き方」を支えよう！～2020 年上半期を振り返る」
日経 BP 情報セキュリティ戦略セミナー　ニュー・ノーマル時代のサイバーセキュリティ対策, 2020 年 9 月 29 日

9. 主な執筆活動

(1) 内田 有香子（国際部マネージャー）：
「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 2020,2020 年 9 月 3 日

10. 協力、後援

本四半期の行事開催に協力または後援等を行いました。

(1) JAIPA Cloud Conference 2020
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：2020 年 9 月 2 日(水)
(2) セキュリティフォーラム２０２０
主　催：一般社団法人日本スマートフォンセキュリティ協会（JSSEC）
一般社団法人セキュア IoT プラットフォーム協議会（SIOTP 協議会）
開催日：2020 年 9 月 3 日(木)
(3) 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：2020 年 9 月 3 日(木)

■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ーのお問い合わせ　：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