JPCERT/CC 活動概要

2020 年 4 月 1 日 ～ 2020 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

2020 年 7 月 14 日

活動概要トピックス

ートピック1ー　「ビジネスメール詐欺の実態調査報告書 (英語版)」を公開

JPCERT/CC は、2020 年 3 月 25 日に公開した「ビジネスメール詐欺の実態調査報告書」を英訳し、6 月 11 日に公開しました。本報告書は、日本貿易会 ISAC、石油化学工業協会などの協力のもと、国内のビジネスメール詐欺（Business E-mail Compromise：BEC）の実態を調査し、その結果をまとめたものです。また、調査結果を踏まえて、BEC の被害を抑止するための取組み（対策）と発覚後の取組み（対応）を整理しています。

本調査は、国内組織における BEC の実態を明らかにし周知することで、国内組織における BEC 被害の抑止に寄与することを目的とし実施しました。本報告書を公開後も、BEC の被害事例に関する情報が継続して公開されており、また、日本語版の読者から英語版の発行のご要望をいただきましたので、国内組織以外にも広くご活用いただけるよう、英語版を公開するに至りました。

英語版の報告書は、海外の National CSIRT のウェブサイトでもご紹介いただき、既に多くの方にご利用いただいています。国内組織の海外拠点を含め、より多くの方に本書をご活用いただき、本書が BEC 被害の抑制に繋がることを願っています。

■Business E-mail Compromise Survey Report
https://www.jpcert.or.jp/english/pub/sr/BEC-survey.html

■ビジネスメール詐欺の実態調査報告書
https://www.jpcert.or.jp/research/BEC-survey.html

ートピック2ー　日本シーサート協議会が法人化

JPCERT/CC は 2020 年 4 月、緊密な連携体制の構築などを目的とした、一般社団法人日本コンピュータセキュリティインシデント対応チーム協議会（以下、日本シーサート協議会）を共同で設立しました。

2007 年の発足以来任意団体として活動をしてきた日本シーサート協議会は、2020 年 4 月より一般社団法人として本格的に活動を開始しました。JPCERT/CC は、共同設立組織の 1 つとして発足時から活動に協力してきました。また、発足からこの 3 月まで経済産業省の委託事業の一環として、国内 CSIRT 活動の定着化に向け、日本シーサート協議会事務局を担って参りました。

発足当初は、組織内 CSIRT の必要性も認知度も社会的に浸透しておらず、発足からおよそ 5 年が経過した 2012 年 3 月末時点で加盟組織は 27 組織でした。しかし、特定組織に対する官民を問わない標的型攻

撃など具体的な脅威への認識が自助活動としての CSIRT の必要性を高めました。活動 10 周年あたる 2017 年には 194 組織までになり、昨年度は加盟組織が 400 を超える規模となりました。この間、途絶えることなく継続的に活動を支えてきたそれぞれの時代の運営委員の皆様の熱意と自組織に対する危機意識を具体的な行動に移した会員の皆様の高い志が、任意団体として 13 年間の活動を支えてきたと感じます。この度、会員向けサービスの拡充や活動基盤をより柔軟に,強固に実施できる体制として一般社団法人化に移行されました。この法人化は、国内 CSIRT 活動の定着化という 13 年間の活動の大きな成果であると考えます。

日本シーサート協議会の活動が充実することは、日本の組織内 CSIRT が強い連携のもとで活動をしていることの現れでもあります。

今後も JPCERT/CC では、日本シーサート協議会と連携をとりながら国内の CSIRT 活動の浸透に努めていきたいと考えております。

一般社団法人日本コンピュータセキュリティインシデント対応チーム協議会
プレスリリース「一般社団法人化について」
https://www.nca.gr.jp/press/20200512.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 10,416 件、インシデント件数ベースでは 7,123 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 4,201 件でした。前四半期の 4,107 件と比較して 2%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_Report20200714.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 5,262 件で、前四半期の 3,839 件から 37%増加しました。また、前年度同期（1,947 件）との比較では、170%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	542	396	551	1,489(28%)
国外ブランド	892	1,153	1,220	3,265(62%)
ブランド不明 (注 5)	165	155	188	508(10%)
全ブランド合計	1,599	1,704	1,959	5,262

（注 2）「ブランド不明」は、報告されたフィッシングサイトが停止していた等の理由により、JPCERT/CC がブランドを確認することができなかったサイトの件数を示します。

前四半期に続き、国外ブランドは E コマースを装ったフィッシングサイト、国内は企業サイトを装ったフィッシングサイトの報告ものが多い増加傾向にあります。

また、報告いただいたフィッシングサイトの中には、URL の中にブランドとは関係のない「COVID-19」の文字列を使用し閲覧者の興味を引こうとしているものもいくつか見受けられました。

E コマースを装ったフィッシングサイトへの誘導方法は、主にメールが使用されており、ログインアカウントがあたかも不正利用されたかのように、「不正なログインを検知したので確認して欲しい」や「アカウントをロックしたので解除方法を案内します」などの文章と併せてフィッシングサイトへのリンクが本文に貼られているものが多く見受けられました。

国外ブランドを騙る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、.buzz ドメインが多く使われていました。
また、日本のホスティングサービスを悪用してフィッシングサイトが立てられているケースもいくつか確認されています。

フィッシングサイトの調整先の割合は、国内が 50%、国外が 50%であり、前四半期（国内が 38%、国外が 62%）と比べて国内への通知の割合が増加しました。

1.1.1.2. Web サイト改ざん

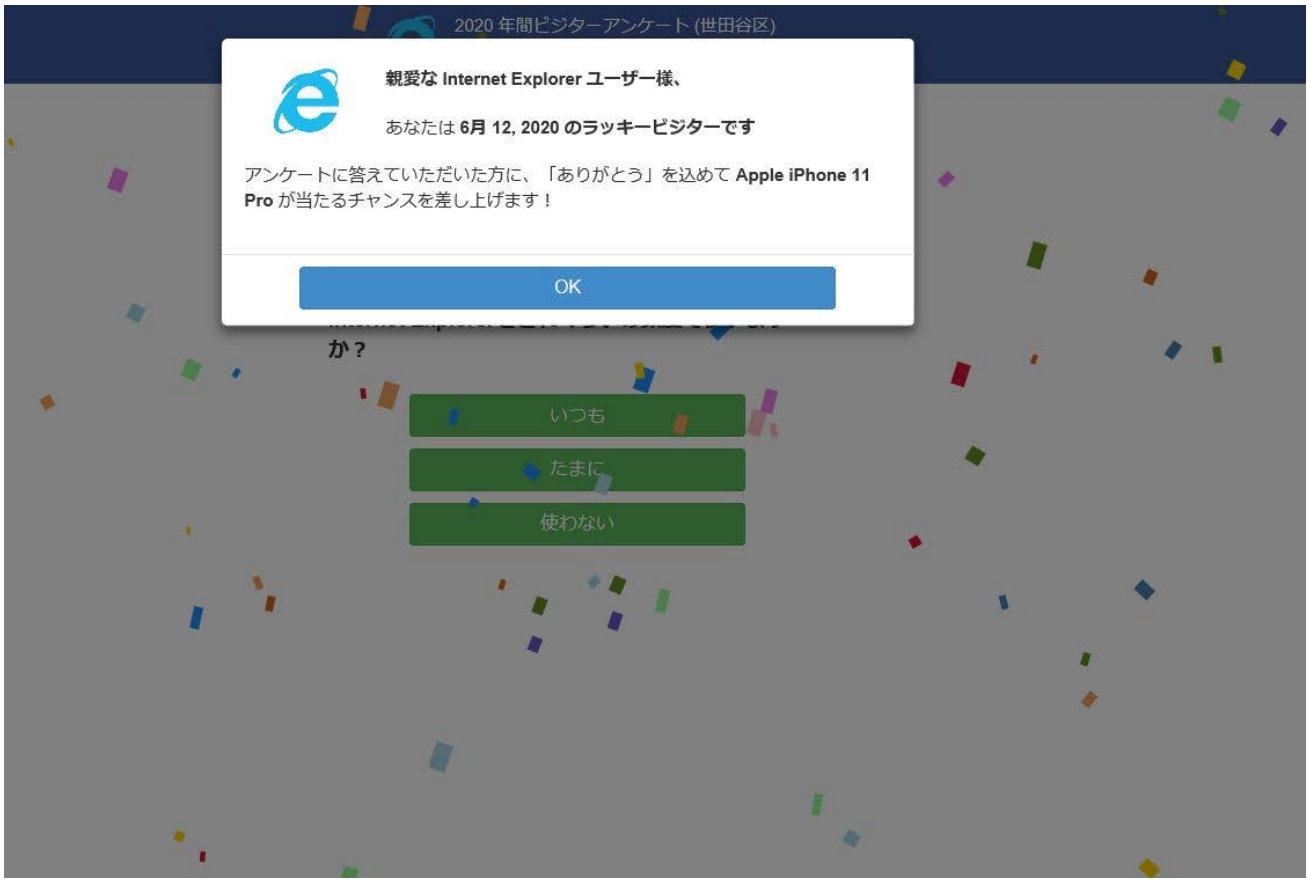
本四半期に報告が寄せられた Web サイト改ざんの件数は、291 件でした。前四半期の 192 件から 52%増加しています。

本四半期は、Web サイトに不正に埋め込まれたコードによって、いわゆる「当選詐欺」のサイトに転送させる事例を多く確認しています。多くの不審なコードが埋め込まれた Web サイトには、以下のような JavaScript が挿入されていたことを確認しています。

```
34  href="https://statcounter.com/" target="_blank"><img
35  class="statcounter"
36  src="https://c.statcounter.com/12180693/0/22249354/1/"
37  alt="web stats"></a></div></noscript>
38  <!-- End of Statcounter Code -->
39
40  <script>
41  setTimeout("location.href='http://www.jjokgo.xyz/jjgo'",300);
42  </script>
43
44  </head>
45
46  <body class="home blog">
47  <div id="page" class="hfeed site">
48      <a class="skip-link screen-reader-text" href="#content">Skip to content</a>
49
```

［図 1-1：挿入された JavaScript］

改ざんされた Web サイトに Web ブラウザーでアクセスすると、不正なサイトへの誘導が発生し、さらに誘導先のサイトでも、同様のコードや HTTP ステータスコード（300 番など）でリダイレクトさせることによって誘導が繰り返され、［図 1-2］のような当選詐欺のページが最終的に表示されることを確認しています。当選詐欺ページでは、個人情報の入力が求められるようになっており、個人情報の収集が目的と考えられます。



［図 1-2：最終的に表示される当選詐欺のページ］

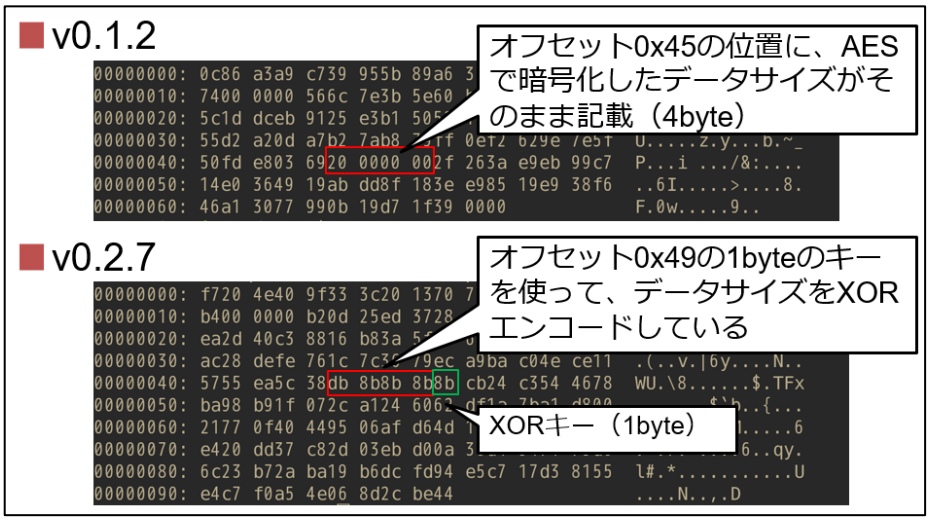
1.1.1.3. その他

標的型攻撃に分類されるインシデントの件数は、6 件でした。前四半期の 2 件から 200%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。

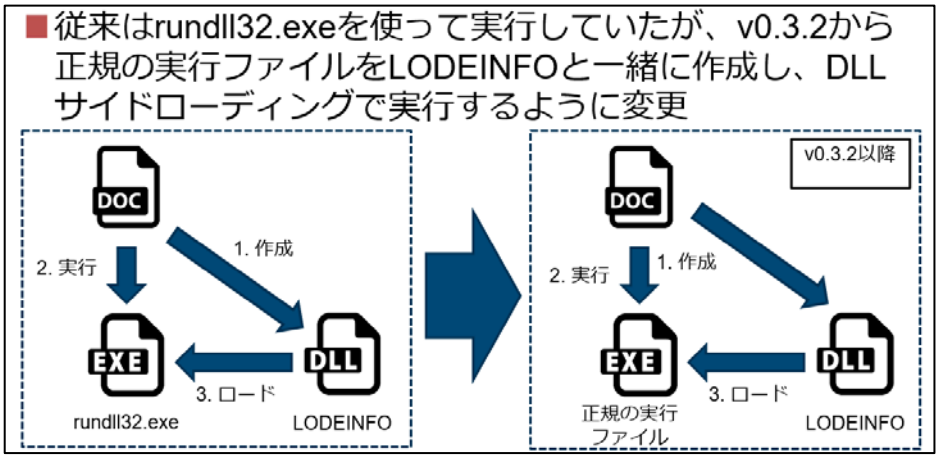
(1) マルウェア LODEINFO による攻撃

前四半期に続き、本四半期もマルウェア LODEINFO による標的型攻撃の報告が寄せられました。確認された手口は、悪意あるマクロが含まれた Word ファイルまたは Excel フィルを添付したメールにより、マルウェア LODEINFO に感染させるものでした。新型コロナウイルスに関する情報や、履歴書を装ったものなど、様々なメールや添付ファイルの内容を確認しています。

前四半期に投稿したブログで LODEINFO の詳細を解説していますが、本四半期に確認された LODEINFO はデータ送受信時のフォーマット（［図 1-3］参照）や実行方法（［図 1-4］参照）が変更されていました。活発にバージョンアップが行われており、引き続き警戒が必要です。



［図 1-3：データ送受信時のフォーマット変更］



［図 1-4：実行方法の変更］

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、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 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/

2020-04-15　2020 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)
2020-04-15　2020 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)
2020-04-16　2020 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 (更新)
2020-04-22　OpenSSL の脆弱性 (CVE-2020-1967) に関する注意喚起 (公開)
2020-05-02　Oracle WebLogic Server の脆弱性に関する注意喚起 (公開)
2020-05-07　SaltStack Salt の複数の脆弱性 (CVE-2020-11651, CVE-2020-11652) に関する注意喚起 (公開)
2020-05-13　Adobe Acrobat および Reader の脆弱性 (APSB20-24) に関する注意喚起 (公開)
2020-05-13　2020 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)

2020-05-21　ISC BIND 9 の脆弱性 (CVE-2020-8616, CVE-2020-8617) に関する注意喚起 (公開)
2020-05-21　Apache Tomcat の脆弱性 (CVE-2020-9484) に関する注意喚起 (公開)
2020-05-26　Apache Tomcat の脆弱性 (CVE-2020-9484) に関する注意喚起 (更新)
2020-06-10　Adobe Flash Player の脆弱性 (APSB20-30) に関する注意喚起 (公開)
2020-06-10　2020 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)

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：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 99 件、「今週のひとくちメモ」のコーナーで紹介した情報は、次の 12 件でした。

2020-04-01　JPCERT/CC 「ビジネスメール詐欺の実態調査報告書」を公開
2020-04-08　Youtube で Japan Security Analyst Conference 2020 講演動画を公開
2020-04-15　IPA が「脆弱性発見 報告のみちしるべ～発見者に知っておいて欲しいこと～」全 8 編を公開
2020-04-22　長期休暇に備えて 2020/04
2020-04-30　仮想通貨を要求する不審な脅迫メールに注意
2020-05-13　JPCERT/CC Eyes「SysmonSearch v2.0 リリース」を公開
2020-05-20　NICT が実践的サイバー防御演習「CYDER」の教材を期間限定で公開
2020-05-27　日本シーサート協議会が「シーサートワークショップ ～加盟希望組織向け説明会～（オンライン）2020 年 4 月開催報告」を公開
2020-06-03　IPA が「情報セキュリティ対策支援サイト」刷新版を公開
2020-06-10　IPA が「サイバーセキュリティ経営ガイドライン Ver 2.0」のプラクティス集を公開
2020-06-17　JPNIC が「DNS Abuse」に関する解説記事を公開
2020-06-24　Adobe Flash Player が 2020 年末でサポート終了

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

2020-04-15　Intel 製品に関する複数の脆弱性について
2020-04-15　複数の Adobe 製品のアップデートについて
2020-04-16　長期休暇に備えて 2020/04
2020-04-17　Pulse Connect Secure の脆弱性への対策や侵害有無などの確認を
2020-04-30　複数の Adobe 製品のアップデートについて
2020-05-13　Adobe DNG Software Development Kit (SDK) に関するアップデート (APSB20-26) について
2020-05-21　複数の Adobe 製品のアップデートについて
2020-06-09　QNAP 社製 NAS および Photo Station に影響を与えるランサムウェアに関する情報について
2020-06-10　Intel 製品に関する複数の脆弱性について
2020-06-10　複数の Adobe 製品のアップデートについて
2020-06-17　複数の Adobe 製品のアップデートについて
2020-06-18　ISC BIND 9 における脆弱性 (CVE-2020-8618、CVE-2020-8619) について
2020-06-23　Magento に関するアップデート (APSB20-41) について
2020-06-30　Palo Alto Networks 製品の脆弱性 (CVE-2020-2021) 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) OpenSSL の脆弱性に関する情報発信

2020 年 4 月 21 日 (米国時間) 、OpenSSL Project から OpenSSL の脆弱性 (CVE-2020-1967) に関する情報が公開されました。OpenSSL は、SSL および TLS の機能を提供する、オープンソースのソフトウェアです。公開された情報によると、特定の条件下で脆弱な関数を呼び出すサーバ

一及びクライアントアプリケーションに対して、遠隔の第三者が細工したメッセージを送ることで、サービス運用妨害 (DoS) 攻撃を行う可能性があります。JPCERT/CC では、2020 年 4 月 22 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。

OpenSSL の脆弱性 (CVE-2020-1967) に関する注意喚起
https://www.jpcert.or.jp/at/2020/at200018.html

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

2020 年 4 月 30 日 (米国時間) 、Oracle は、Oracle WebLogic Server の脆弱性に関して、2020 年 4 月のクリティカルアップデートを適用するよう注意を呼びかける情報を公開しました。同社によると、2020 年 4 月 14 日 (米国時間) にリリースした 2020 年 4 月のクリティカルアップデートで修正した脆弱性を悪用するための複数の実証コードを確認しているとのことで、特に脆弱性 CVE-2020-2883 について注意を呼びかけています。本脆弱性が悪用された場合、リモートからの攻撃によって、不正な操作が実行されるなどの可能性があることから、JPCERT/CC では、2020 年 5 月 2 日に注意喚起を発行し、早急に対策や回避策の適用を行うよう呼びかけました。

Oracle WebLogic Server の脆弱性に関する注意喚起
https://www.jpcert.or.jp/at/2020/at200019.html

(3) SaltStack Salt の複数の脆弱性に関する情報発信

2020 年 4 月 30 日 (米国時間) 、SaltStack 社から、同社が提供する構成管理ツール Salt の複数の脆弱性 (CVE-2020-11651、CVE-2020-11652) に関する情報が公開されました。脆弱性が悪用された場合、リモートからの攻撃によって、認証なしでマスターサーバー上のユーザートークンが窃取されたり、管理対象サーバー上で任意のコマンドを実行されたりするなどの可能性があります。JPCERT/CC では、これらの脆弱性に関連する実証コードや、脆弱性を悪用したという情報が Web 上で公開されていることを確認した他、定点観測システム TSUBAME では、マスターサーバーが使用するポート (4505/TCP 宛、4506/TCP 宛) へのスキャンを確認しました。これらの状況から、本脆弱性を悪用される可能性があるため、2020 年 5 月 7 日に注意喚起を発行し、ユーザーに向けて早期のアップデートを呼びかけました。

SaltStack Salt の複数の脆弱性 (CVE-2020-11651, CVE-2020-11652) に関する注意喚起
https://www.jpcert.or.jp/at/2020/at200020.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」といいます)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。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. 描画スピードの向上と新機能追加

今年度、インターネットリスク可視化サービス Mejiro のリプレースを予定しており、5 月にこれに向けた準備作業に着手しました。リプレースでは、従来からの Mejiro 指標の提供に加えて、データーソースの追加や、データ取得のための API 機能の追加、National CSIRT 向けのポータルサイトを構築する予定です。新たなデーターソースとして、BinaryEdge を加え、SHODAN, Censys との件数を比較できるようにすることを計画しています。スキャン方法の異なる複数のデーターソースを組み合わせて分析することで、リスク要因の増減をより詳細に分析することができると期待しています。また、データーソースの追加等により Mejiro 指標が増えていくことや、独自に分析したいという要望に応える目的で、各国・地域での Mejiro 指標を取得しやすくするために、API の提供を予定しています。API を介して Mejiro のデータを取得し、同時に解析を行うということも可能になると考えています。
National CSIRT 向けのポータルサイトでは、そのチームの国・地域に属する ASN 毎での Mejiro 指標の提供を行うことを計画しています。これまで Mejiro では、各チームに対してデータの提供が困難であったことから、自らの国・地域でのより詳細な情報を知らせることで各チームの実施するクリーンアップ活動を活性化できるのではないかと考えています。これらの改善を 2020 年に終了し、2021 年初頭にリリースすることを目指しております。新しい Mejiro にご期待ください。

［図 1-5：（例）フィリピンの ASN 別集計結果画面］

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. 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

1.3.1. 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」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

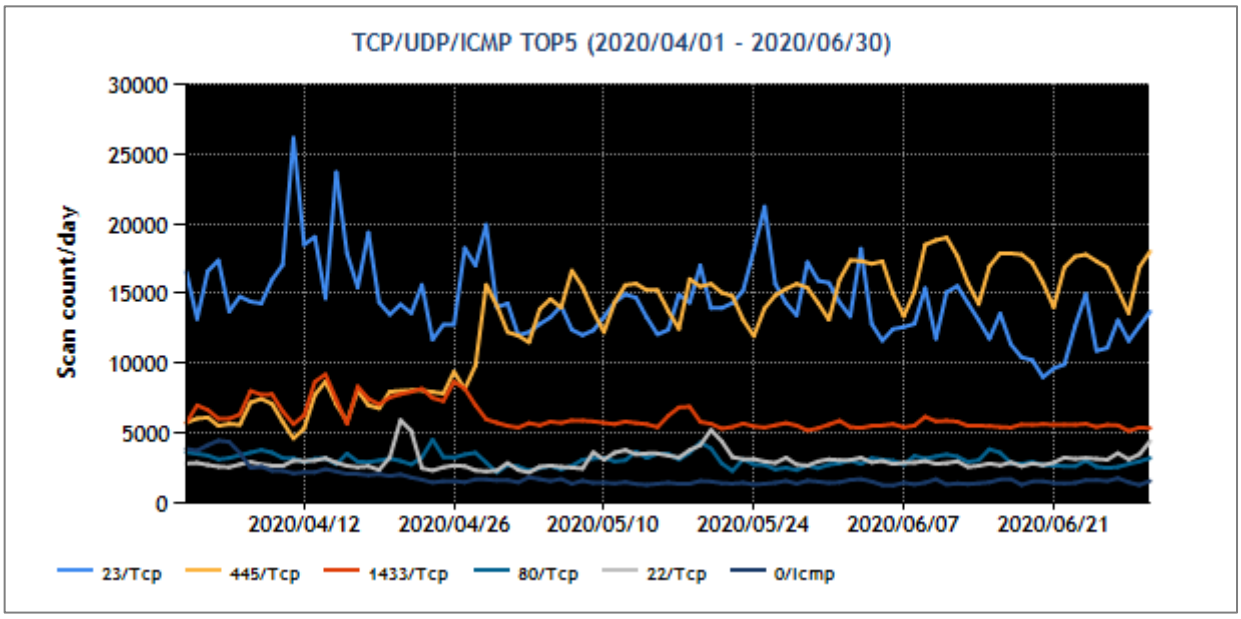
1.3.2. TSUBAME の観測データの活用

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 1 月から 3 月分のレポートを 2020 年 5 月 12 日に公開しました。

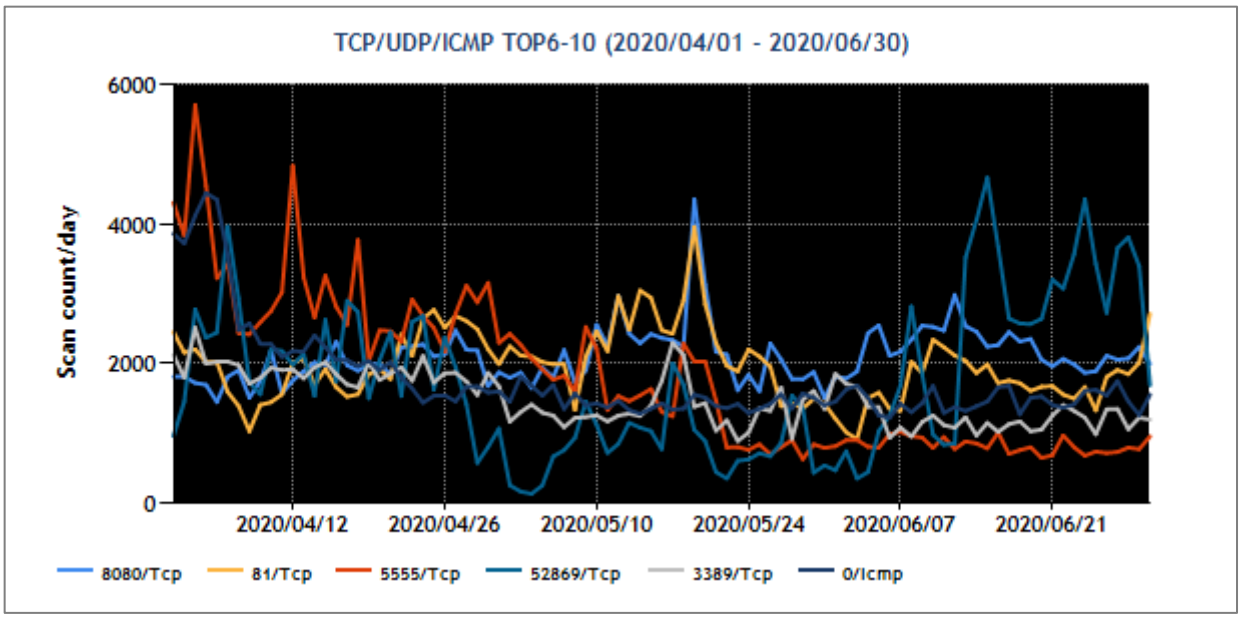
TSUBAME 観測グラフ
https://www.jpcert.or.jp/tsubame/index.html#examples
インターネット定点観測レポート（2020 年 1～3 月）
https://www.jpcert.or.jp/tsubame/report/report201907-09.html

1.3.3. 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 1-6］と［図 1-7］に示します。

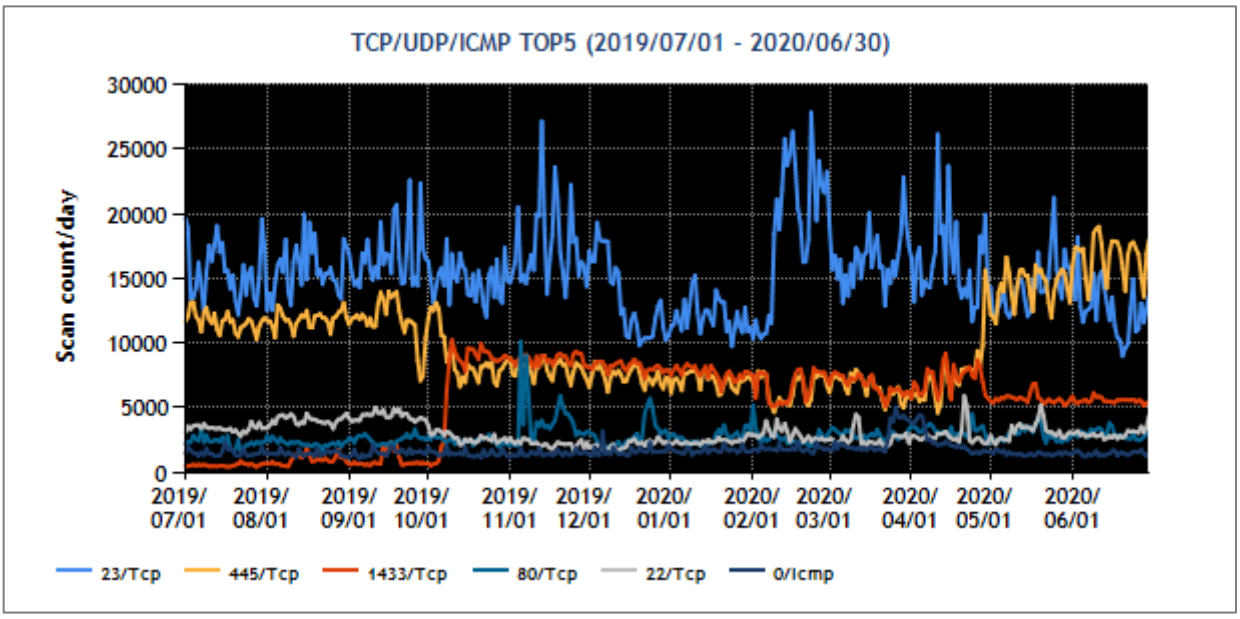


［図 1-6：宛先ポート別グラフ トップ 1-5（2020 年 4 月 1 日-6 月 30 日）］

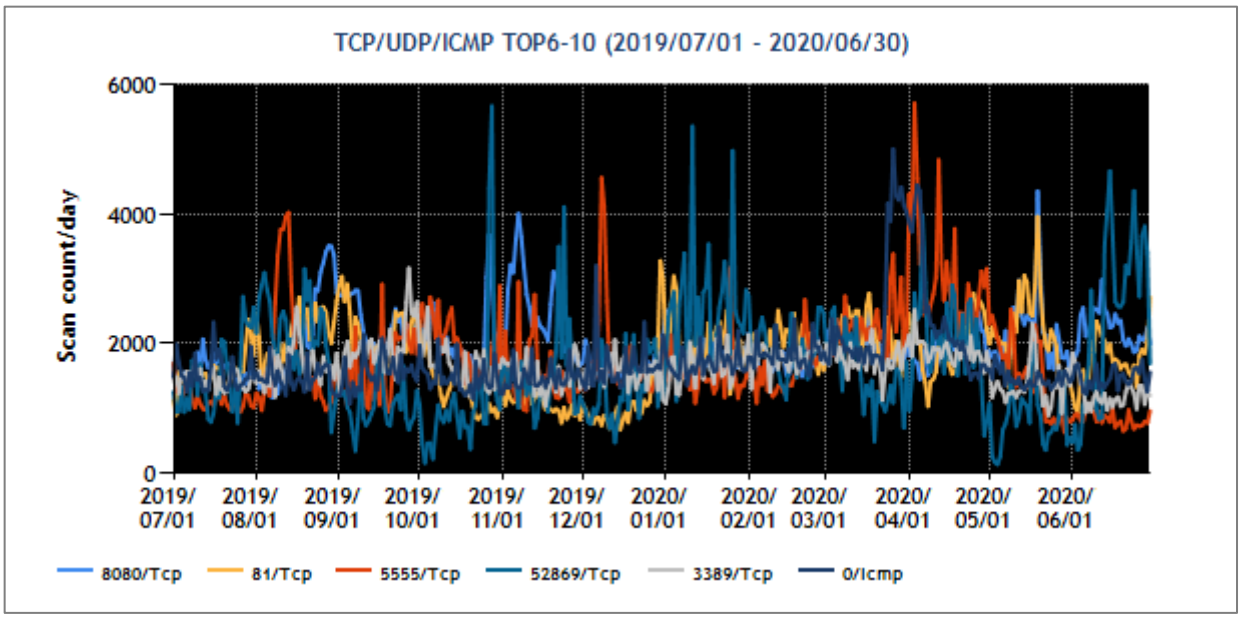


［図 1-7：宛先ポート別グラフ トップ 6-10（2020 年 4 月 1 日- 6 月 30 日）］

また、過去 1 年間（2019 年 7 月 1 日-2020 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 1-8］と［図 1-9］に示します。



［図 1-8：宛先ポート別グラフ トップ 1-5（2019 年 7 月 1 日-2020 年 6 月 30 日）］



［図 1-9：宛先ポート別グラフ トップ 6-10（2019 年 7 月 1 日-2020 年 6 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。2 番目に多かった 445/TCP 宛の通信は、4 月下旬から増加しています。445/TCP 宛通信の変化の背景には何らかのマルウェアの活動が関与しているのではないかと考え、送信元のユーザーに連絡を行いました。現時点では、攻撃手法やマルウェアにつながる情報は得られていません。

1.3.4. 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、スキャン活動の TSUBAME による観測に加えて、スキャンに応対があっ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 5 月 27 日～31 日にかけて、QNAP 社製 NAS および Photo Station の脆弱性 (NAS-QSA-20-02) を悪用しようとしたとみられる通信を観測しました。本通信は昨年度 2019 年 11 月 25 日に公表された脆弱性 (CVE-2019-7192、CVE-2019-7193、CVE-2019-7194、CVE-2019-7195) を狙ったランサムウェアと思われるもので、QNAP 社からは 2020 年 6 月 8 日にセキュリティアドバイザリが発行されています。観測した内容に基づき、CyberNewsFlash を公開しました。

> QNAP 社製 NAS および Photo Station に影響を与えるランサムウェアに関する情報について
> https://www.jpcert.or.jp/newsflash/2020060901.html

また、脅威情報収集の対象となる攻撃通信の収集対象拡大を目的として、現在観測している HTTP プロトコル以外のプロトコルを観測するために、新たに SSH や RDP といったプロトコルが観測可能なハニーポットを新規に構築し、今後、評価を予定しています。

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。

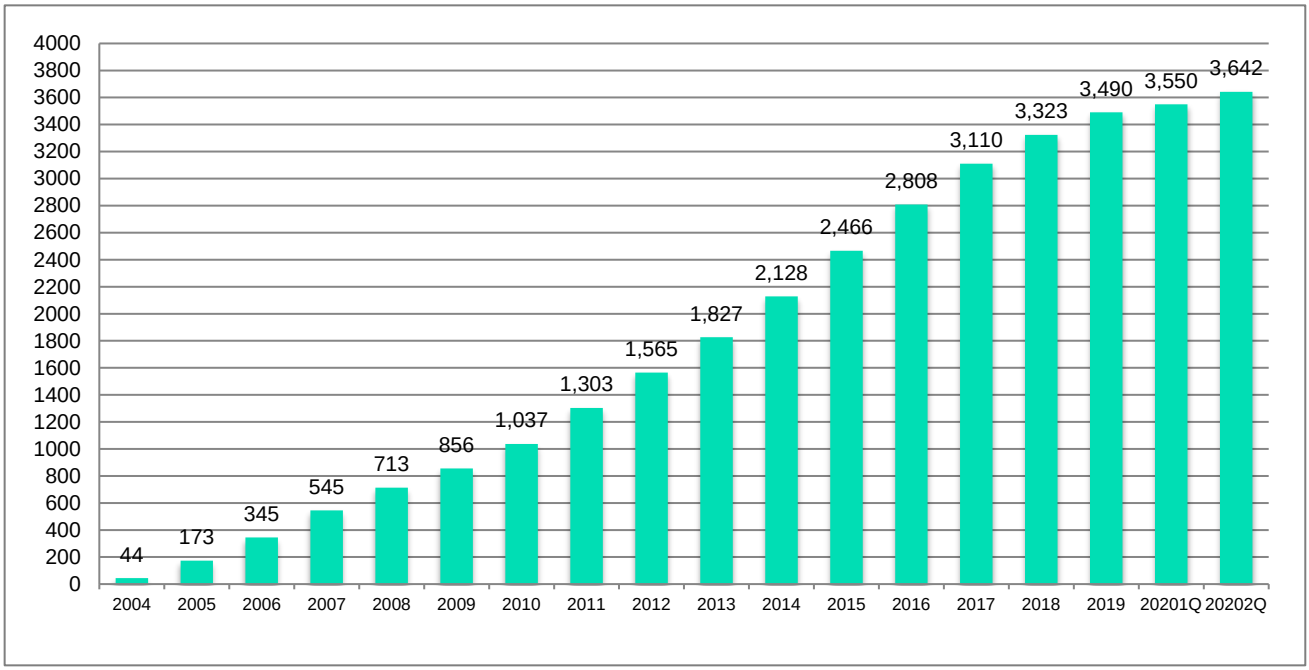
独立行政法人情報処理推進機構（IPA）脆弱性対策
https://www.ipa.go.jp/security/vuln/

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 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 92 件（累計 3,642 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/



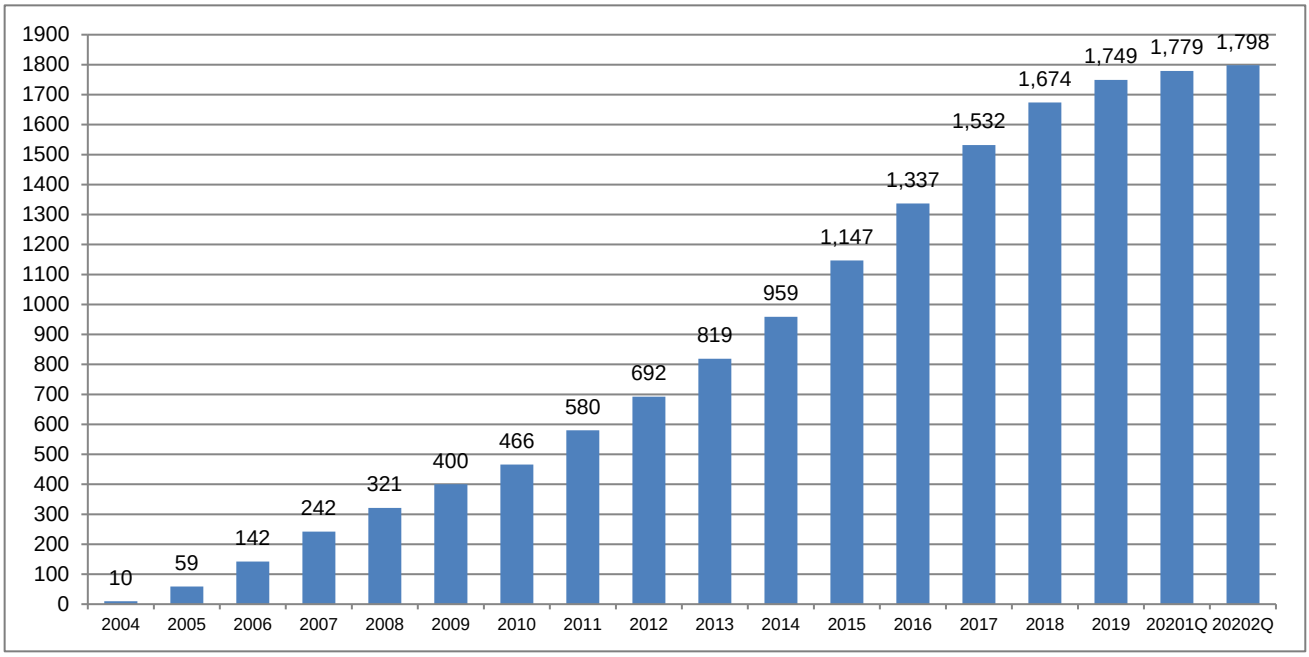
［図 2-1：JVN 公表累積件数］

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 19 件（累計 1,798 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 19 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 15 件（このうち自社製品の届出によるものが半数超となる 8 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 4 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、組込系製品が 5 件と最も多く、次いで CMS とグループウェアが 4 件ずつと他の製品に比べ多い状況でした。続いてプラグインが 3 件、IT 資産管理ツール、Windows アプリケーション、サーバー製品それぞれ 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
組込系製品	5
CMS	4
グループウェア	4
プラグイン	3
IT 資産管理ツール	1
Windows アプリケーション	1
サーバー製品	1



［図 2-2：公表を行った国内取扱脆弱性情報の累積件数］

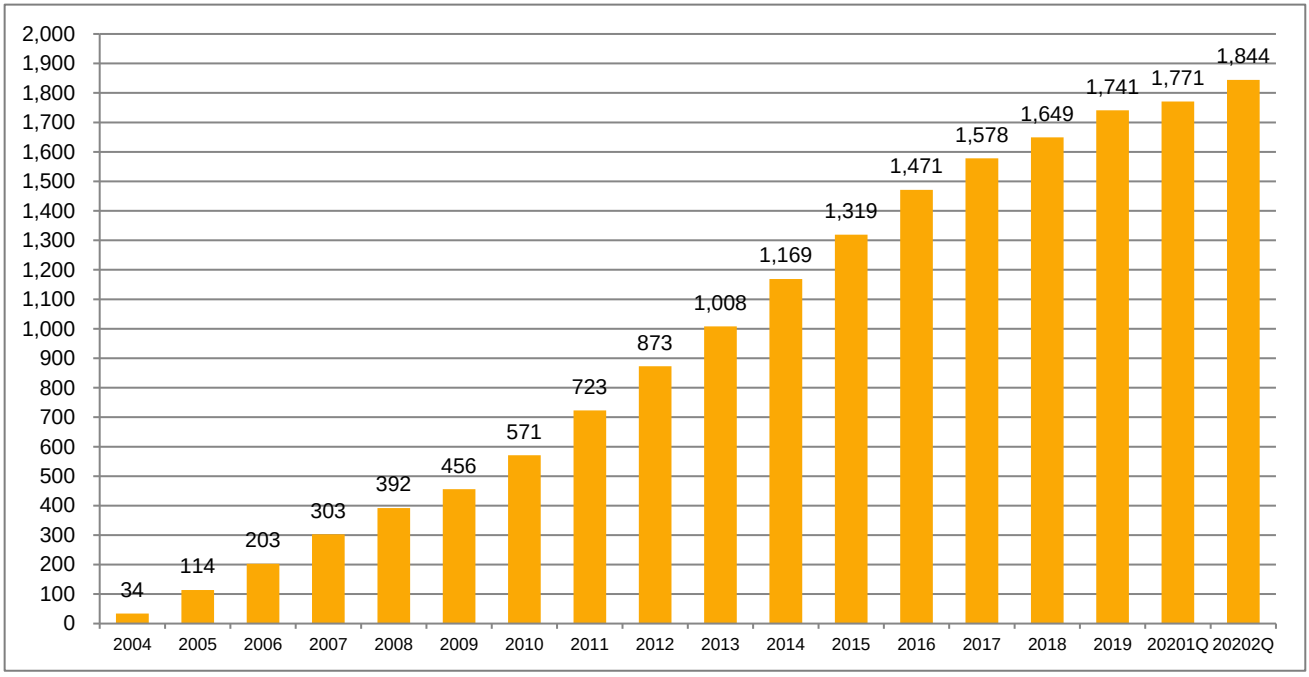
本四半期に公表した国際取扱脆弱性情報は 73 件（累計 1,844 件）で、累計の推移は［図 2-3］に示すとおりです。本四半期 2020 年 4 月 1 日より、JPCERT/CC では、米国国土安全保障省傘下の CISA ICS が公開する ICSA（制御系製品に関する脆弱性情報）および ICSMA（医療機器に関する脆弱性情報）を邦訳し、国際取扱脆弱性情報にふくめ JVN にて注意喚起として公開することにいたしました。本四半期の国際取扱脆弱性情報の公開数が前四半期と比較すると極めて大きく 73 件となったのはそのためです。
73 件のうち、海外調整機関や製品開発者等からの届出によるものおよ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 22 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、上述のとおり ICSA および ICSMA の注意喚起公開を開始したことにより制御系製品に関するものが 46 件と最も多く、次いで多かったのは、医療機器、macOS、プロトコルに関するものでそれぞれ 5 件ずつでした。続いて組込系製品に関するものが 4 件、DNS、Windows アプリケーション、ウェブサーブレットコンテナがそれぞれ 2 件、そしてライブラリ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	46
macOS	5
医療機器	5
プロトコル	5
組込系製品	4
DNS	2
Windows アプリケーション	2
ウェブサーブレットコンテナ	2
ライブラリ	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 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 40 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/

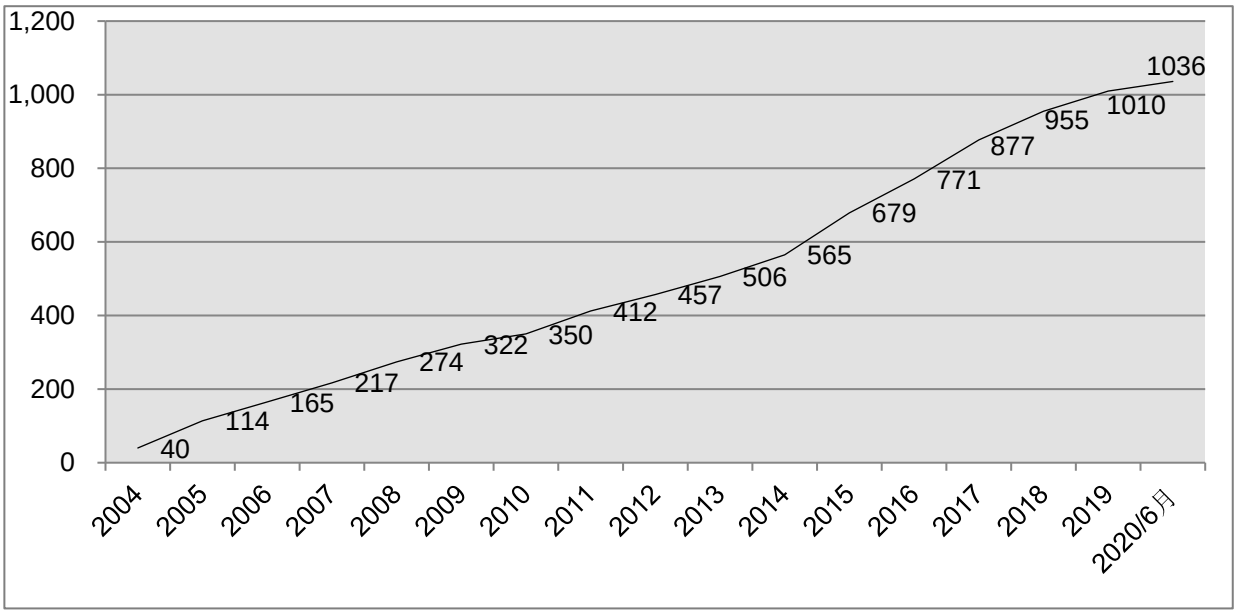
情報セキュリティ早期警戒パートナーシップガイドライン（2019 年版）
https://www.jpcert.or.jp/vh/partnership_guideline2019.pdf

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

2.2.1. 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 6 月 30 日現在で 1,036 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



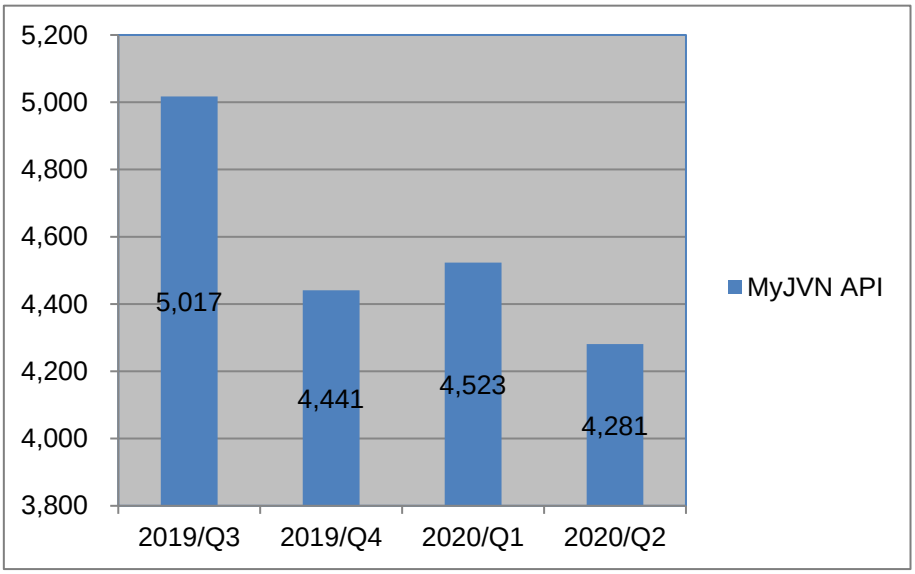
［図 2-4：累計製品開発者登録数］

2.3. VRDA フィードによる脆弱性情報の配信

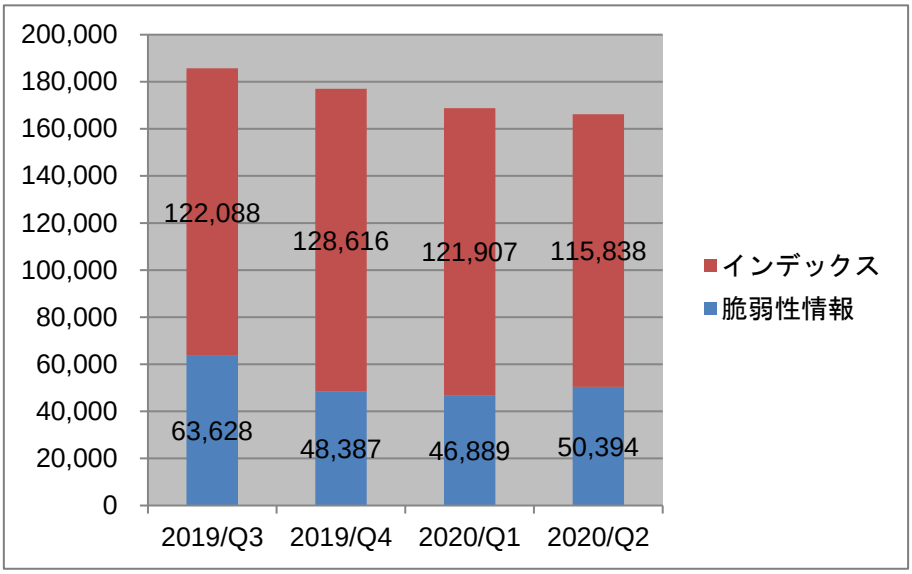
JPCERT/CC は、大規模組織の組織内 CSIRT 等での利用を想定して、ツールを用いた体系的な脆弱性対応を可能とするため、IPA が運用する MyJVN API を外部データソースとして利用した、VRDA（Vulnerability Response Decision Assistance）フィードによる脆弱性情報の配信を行っています。VRDA フィードについての詳しい情報は、次の Web ページを参照ください。

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。

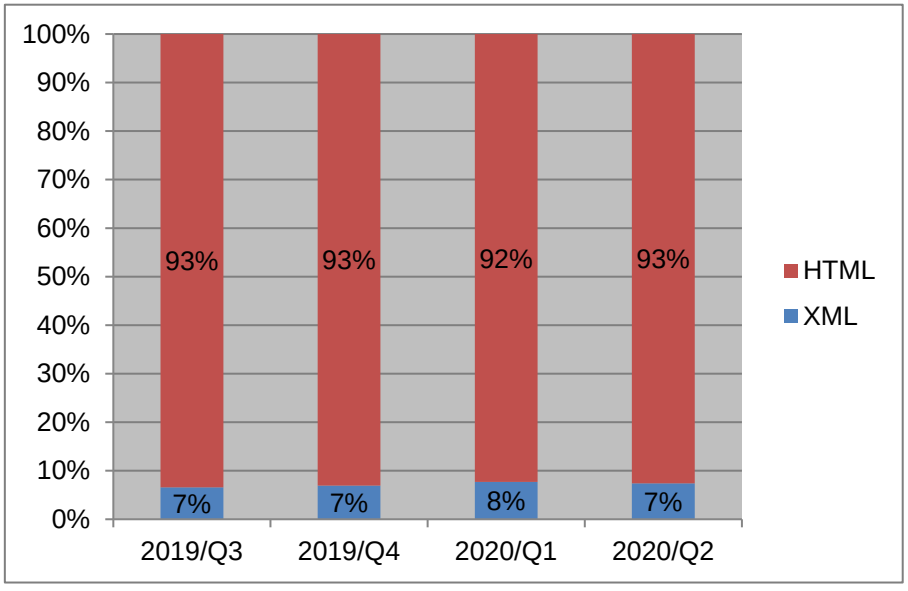


［図 2-5：VRDA フィード配信件数］



［図 2-6：VRDA フィード利用件数］

インデックスの利用数および脆弱性情報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、大きな変化は見られませんでした。



［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 255 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 2 件でした。

2020/05/13 【参考情報】ホルムズ海峡にあるイランの主要な港へのサイバー攻撃について
2020/05/22 【参考情報】米国 MTS-ISAC の設立に関するニュースリリースが公表された件について

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。

2020/04/06 制御システムセキュリティニュースレター 2020-0003
2020/05/11 制御システムセキュリティニュースレター 2020-0004
2020/06/05 制御システムセキュリティニュースレター 2020-0005

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 1,123 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 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、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 4 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

本四半期は、新型コロナウイルスの感染防止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、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、4 月 1 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 年次報告書の公開

APCERT では毎年春に、前年の APCERT 全体および各オペレーショナルメンバーの活動をまとめた年次報告書をまとめ、Web サイト上に掲載しています。各オペレーショナルメンバーの報告には、組織概要、インシデント対応実績、国内でのセキュリティ啓発事業など、それぞれの組織の活動を紹介した内容が含まれています。2019 年版の報告書は、JPCERT/CC を含む 29 のオペレーショナルメンバーが寄稿し、5 月 28 日に公開されました。

[図 4-1: APCERT 年次報告書表紙]

APCERT Annual Report 2019
https://www.apcert.org/documents/pdf/APCERT_Annual_Report_2019.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. 32nd Annual FIRST Conference Montreal の延期

6 月 21 日から 26 日にかけて、カナダのモントリオールで開催が予定されていた第 32 回 FIRST カンファレンスは、新型コロナウイルスの感染拡大の影響を受けて、11 月に延期されることになりました。

32nd Annual FIRST Conference Montreal
https://www.first.org/conference/2020/

4.3. 講演活動

4.3.1. 東京大学公共政策大学院での講演（5 月 19 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 間の協力関係等に次いで、サイバー脅威情報の収集・分析活動や脆弱性情報のハンドリング等の JPCERT/CC の主な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 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。

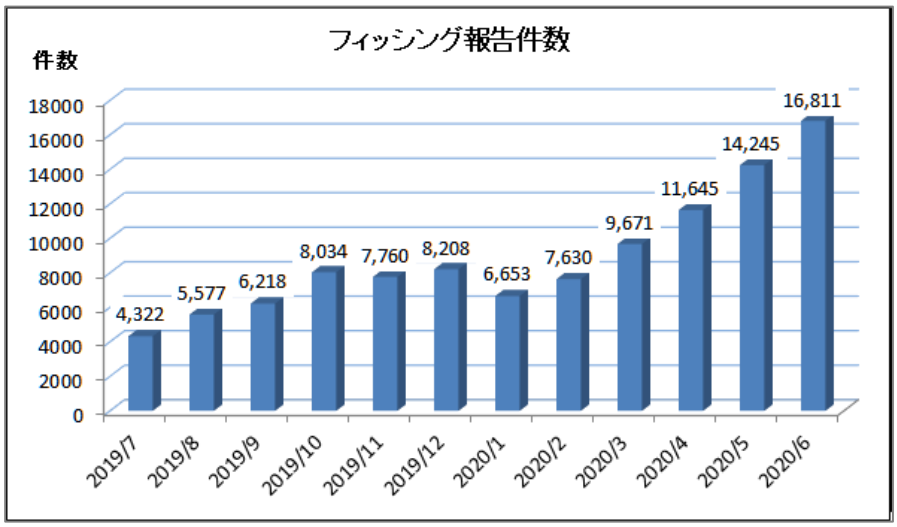
本四半期中 4 月にロシアのペテルスブルグで開催予定であった会議は、新型コロナウイルス感染の世界的な広がりの影響で中止され、オンライン会議で議論を進め結論を国際投票により確定させる形式で行われました。「複数の開発者が関与する脆弱性の開示と取扱」に関しては案件主査から技術文書の作成が提案され、コンビーナによって承認されました。今後は、調査期間が延長されるとともに、技術文書の作成期間となります。

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、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・問合せの受付

本四半期のフィッシング報告件数は、毎月過去の報告数を更新し、前年同期の約 4.5 倍となり高い数値となりました。（[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、Apple、LINE、楽天をかたるフィッシングの報告が多く、この 4 ブランドの報告で全体の約 85 %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

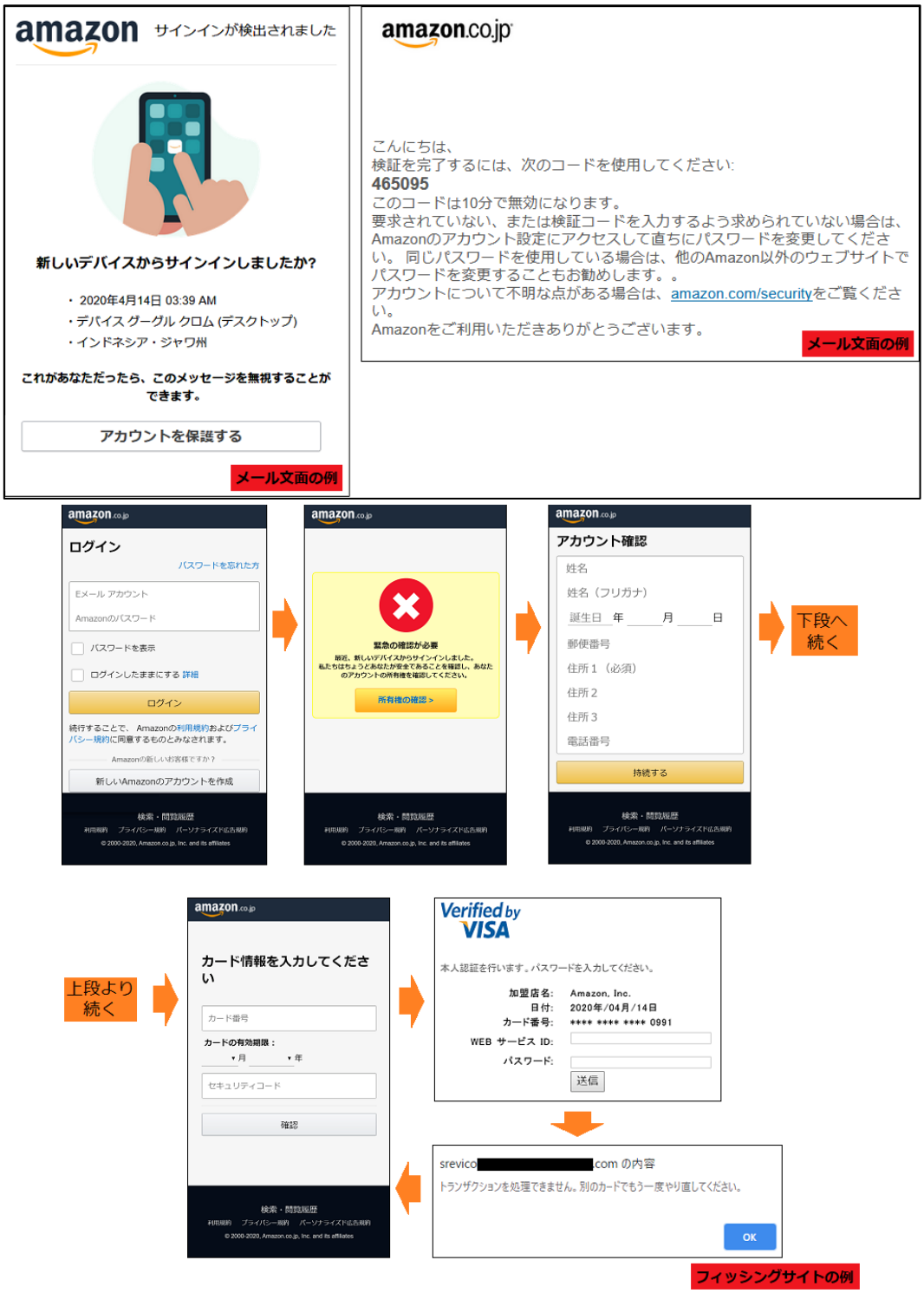
本四半期は、協議会 Web サイトや会員向けメーリングリストを通じて、フィッシングに関するニュースおよび緊急情報を計 18 件（ニュース：2 件、緊急情報：16 件）発信しました。
利用者が多いサービスに関する、影響範囲が大きいと思われるフィッシングについては、緊急情報を Web サイトに適宜掲載し、広く注意を喚起しました。その内訳は次のとおりです。

- 楽天をかたるフィッシング：2 件
- メルカリをかたるフィッシング：1 件
- Amazon をかたるフィッシング：3 件
- NTT ドコモをかたるフィッシング：1 件
- au をかたるフィッシング：2 件
- 千葉銀行をかたるフィッシング：1 件
- ヨドバシカメラをかたるフィッシング：1 件
- 住信 SBI ネット銀行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
- LINE をかたるフィッシング：1 件
- アメリカン･エキスプレス･カード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

本四半期は新型コロナウイルス感染症に係る緊急事態宣言により、不要不急の外出自粛、店舗・施設の営業自粛などが要請され、オンラインショッピングの利用機会が増えた時期でしたが、この状況を狙ったかのように、フィッシング報告においても Amazon や楽天などのショッピングサイトをかたるものが非常に増えました。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、宅配業者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。

フィッシングサイトへ誘導する方法としては、大手 SNS サービスで使われる短縮 URL や、大手メール配信サービスのトラッキング用 URL をフィッシングメール内に記載し、リダイレクトでフィッシングサイトへ誘導するタイプが増えました。これらは正規サービスの URL と区別がつかず、セキュリティフィルタをすり抜ける可能性があるため、注意が必要です。

フィッシング以外では、マスク等の衛生用品を販売するショップを装った偽ショッピングサイトへ誘導するメールや、給付金や補助金の申請を促すメール、ビットコインで寄付や納税を求める不審なメール等が確認されました。



［図 5-2：Amazon 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/amazon_20200414.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 4 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/202004.html

2020 年 5 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/202005.html

2020 年 6 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/202006.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 43 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 フィッシング対策啓発文書の公開

2019 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定を進めた、「フィッシング対策ガイドライン 2020 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 2020」を 2020 年 6 月 2 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 2020 年度版
https://www.antiphishing.jp/report/guideline/antiphishing_guideline2020.html

利用者向けフィッシング詐欺対策ガイドライン 2020 年度版
https://www.antiphishing.jp/report/guideline/consumer_guideline2020.html

フィッシングレポート 2020
https://www.antiphishing.jp/report/wg/phishing_report2020.html

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 77 回運営委員会
  日時：2020 年 4 月 9 日(木) 16:00-18:00
  場所：オンライン
- 第 78 回運営委員会
  日時：2020 年 5 月 8 日 15:00-17:20
  場所：オンライン
- 第 79 回運営委員会
  日時：2020 年 6 月 26 日 16:00-18:00
  場所：オンライン

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：2020 年 5 月 19 日 13:00-14:00
  場所：オンライン
- 学術研究プロジェクト会合
  日時：2020 年 5 月 26 日 13:00-14:00
  場所：オンライン
- 学術研究プロジェクト会合
  日時：2020 年 6 月 2 日 11:00-12:00
  場所：オンライン
- 学術研究プロジェクト会合
  日時：2020 年 6 月 9 日 11:00-12:00
  場所：オンライン
- 学術研究プロジェクト会合
  日時：2020 年 6 月 16 日 11:00-12:00
  場所：オンライン

- 学術研究プロジェクト会合
  日時：2020 年 6 月 23 日 11:00-12:00
  場所：オンライン
- 学術研究プロジェクト会合
  日時：2020 年 6 月 30 日 11:00-12:00
  場所：オンライン
- 証明書普及促進 WG 会合
  日時：2020 年 6 月 2 日 16:00-18:00
  場所：オンライン
- 2020 年度総会
  日時：2020 年 6 月 11 日 15:00 - 17:00
  場所：オンライン

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。

2020-04-14 JPCERT/CC インシデント報告対応レポート [2020 年 1 月 1 日～2020 年 3 月 31 日]
https://www.jpcert.or.jp/pr/2020/IR_Report20200414.pdf

2020-06-19 JPCERT/CC Incident Handling Report [January 1, 2020 - March 31, 2020]
https://www.jpcert.or.jp/english/doc/IR_Report2019Q4_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。

2020-05-12　JPCERT/CC インターネット定点観測レポート [2020 年 1 月 1 日～2020 年 3 月 31 日]
https://www.jpcert.or.jp/tsubame/report/report202001-03.html
https://www.jpcert.or.jp/tsubame/report/TSUBAMEReport2019Q4.pdf

2020-06-19　JPCERT/CC Internet Threat Monitoring Report [January 1, 2020 ～ March 31, 2020]
https://www.jpcert.or.jp/english/doc/TSUBAMEReport2019Q4_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。

2020-05-14　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 1 四半期（1 月～3 月）]
https://www.jpcert.or.jp/press/2020/vulnREPORT_2019q4.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通して、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 13 件の記事を公開しました。

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

2020-06-23　Volatility Plugin をバージョン 3 対応にする方法
2020-06-11　マルウエア LODEINFO の進化
2020-05-11　おすすめのセキュリティカンファレンス
2020-04-30　SysmonSearch v2.0 リリース
2020-04-23　LogonTracer v1.4 リリース
2020-04-02　IE の脆弱性 (CVE-2020-0674) と Firefox の脆弱性 (CVE-2019-17026) を悪用する攻撃

英語版発行件数：6 件 https://blogs.jpcert.or.jp/en/

2020-06-19　Evolution of Malware LODEINFO
2020-05-14　3 Recommended International Cyber Security ConferencesNEW

2020-04-30　SysmonSearch v2.0 ReleasedNEW
2020-04-23　LogonTracer v1.4 ReleasedNEW
2020-04-06　Attacks Simultaneously Exploiting Vulnerability in IE (CVE-2020-0674) and Firefox (CVE-2019-17026)
2020-04-03　Attacks Exploiting Vulnerabilities in Pulse Connect Secure

8. 主な講演活動

(1) 中野 巧（国際部 渉外担当）、伊藤 智貴（早期警戒グループ 国際連携スペシャリスト）、
小島 和浩（早期警戒グループ　脅威アナリスト）：
「JPCERT/CC Activities」
東京大学公共政策大学院,2020 年 5 月 19 日

9. 主な執筆活動

(1) 中井 尚子（インシデントレスポンスグループ）：
「情報発信とフィードバック」
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 News & Views vol.1764
2020 年 4 月 15 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) 第 15 回情報危機管理コンテスト
主　催：サイバー犯罪に関する白浜シンポジウム実行委員会
開催日：2020 年 4 月 11 日～5 月 23 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