JPCERT/CC 活動四半期レポート

2021 年 4 月 1 日 ～ 2021 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

2021 年 7 月 15 日

活動概要トピックス

ートピック1ー　FIRST の理事に JPCERT/CC スタッフが当選

FIRST（Forum of Incident Response and Security Teams）は 2021 年 6 月現在、98 の国・地域から 585 の組織が加盟する世界最大の CSIRT コミュニティーです。その活動は、Board of Directors を構成する 10 名の理事により企画・立案されています。理事の任期は 2 年間で、半数の 5 名が毎年参加組織による選挙で選出されることになっています。オンラインにより行われた今年の選挙結果が 6 月 10 日の総会で発表され、JPCERT/CC から立候補していた国際部マネージャーの内田有香子が当選を果たしました。
理事の多くは欧米の組織に所属し、男性が多数を占めています。「アジア太平洋地域の組織に所属する女性理事として、この地域における議論の活性化や、新たな組織へのアウトリーチ、コロナ禍で停滞するイベントの再始動などの挑戦をとおして、FIRST の発展と活動の多様性の向上に貢献していきたい」と内田は抱負を述べました。
JPCERT/CC は、1998 年に日本で最初に FIRST に加盟して以来その活動に積極的に参加し、海外の CSIRT との連携を進めてきました。また、過去に FIRST 理事を務めたも職員も複数いました。今回の当選には、そうした実績を持つ JPCERT/CC へのコミュニティーの信頼感も寄与したと考えられます。

Board of Directors の他のメンバーや歴任者については、次の URL をご参照ください。

FIRST.Org,Inc., Board of Directors
https://www.first.org/about/organization/directors

ートピック2ー　JPCERT/CC を Root とする CNA 組織が 4 社に

JPCERT/CC は、脆弱性共通識別子 CVE の採番を行う CNA（CVE Numbering Authority）としてグローバルな脆弱性情報の円滑な流通に努めてきましたが、主要な製品開発者を CNA として認定し、CVE の採番を分散化する方針が打ち出されたことに伴い、Root CNA として、主に国内の製品開発者に呼びかけて CNA へ勧誘する等の取り組みを通じて CVE Program の安定的な運用を支えています。そうした取り組みが実を結び、今四半期には株式会社東芝が新たに CNA となり、前四半期までの 3 社とあわせて、JPCERT/CC を Root とする CNA が 4 社となりました。

2021 年 1 月には 152 社であった CNA 組織数は、7 月 10 日現在で 177 社に増加するなど分散化が進んでいますが、その多くが米国に偏在しています。特に米国以外の地域を中心に CNA の一層の拡充が課題となっており、その中で 6 月にスペインの Spanish National Cybersecurity Institute, S.A.（INCIBE）を Root に追加するなど努力が進められています。相次ぐ日本の CNA 組織の誕生は CVE Program からも歓迎されており、JPCERT/CC としても、脆弱性調整・情報流通に対する価値観を共有し、ともに脆弱性情

報に向き合うパートナーが増えることを喜ばしく思っています。

今後も、JPCERT/CC では引き続き CNA 組織の勧誘・育成に注力していくとともに、ローカライゼーションも含めた日本国内での運用体制の整備など CVE Program の普及活動を通じて、脆弱性情報のより一層効果的な流通経路の整備に努めてまいります。

NEC、CVE Numbering Authority（CNA）としての活動を開始
https://jpn.nec.com/cybersecurity/topics/2021/PR20210603_cna.html

東芝の CVE プログラム参画について
https://www.global.toshiba/jp/news/corporate/2021/06/news-20210616-01.html

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

ートピック3ー　JPCERT/CC 感謝状 2021

JPCERT/CC は、さまざまな国内のサイバー攻撃の被害を低減するために、インシデントへの対応支援活動、インシデントを未然に防ぐための早期警戒活動、マルウェア分析、ソフトウェア製品等の脆弱性に関する調整活動を行っています。これらの活動を円滑かつ効果的に進めるためには、皆さまからの情報提供やさまざまな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。

今年度は、JPCERT/CC が開催しているカンファレンス Japan Security Analyst Conference（JSAC）のプログラム選考委員の皆さまと、三菱電機 PSIRT 様に感謝状をお贈りいたしました。

本年度の感謝状をお贈りした方のうち、JSAC プログラム選考委員の皆さまは、カンファレンスを立ち上げた 2018 年当初からご協力いただいてきており、幅広いスキルレベルで実践に立つ情報が得られる質の高いプログラムの編成を通じたコンテンツの高度化だけでなく、国内外のセキュリティアナリストのコミュニティーに JSAC について広くお知らせいただいて知名度の向上を図るなど、カンファレンスのプレゼンス向上に大きく貢献いただきました。

［JSAC プログラム選考委員の皆さま］
新井 悠 様（株式会社 NTT データ）
石川 芳浩 様（株式会社ラック）
石丸 傑 様（株式会社カスペルスキー）
佐藤 元彦 様（伊藤忠商事株式会社）
鈴木 博志 様（株式会社インターネットイニシアティブ）
中津留 勇 様（セキュアワークス株式会社）
春山 敬宏 様（VMware, Inc）
山崎 輝 様（楽天グループ株式会社）

三菱電機 PSIRT 様は、PSIRT としての発足は 2019 年と比較的新しい組織ですが、発足以後、活発な活動を展開され、2019 年においては、自社製品の脆弱性届け出数が最も多い製品開発者の一つとして積極的に脆弱性への対応とその対策および情報公開を推進されています。また、脆弱性対策に関して製品開発者の視点から問題提起されるなど、JPCERT/CC の活動にもさまざまな気付きを与えていただきました。JPCERT/CC が行う脆弱性情報流通の活動へのこれまでの貢献とともに、成熟した PSIRT が保有する機能を発足当初から持ちあわせているだけでなく適切に機能させているなど、他の製品開発者の参考となる PSIRT 活動を展開されています。

今年度の感謝状贈呈の詳細と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 2021
https://www.jpcert.or.jp/press/priz/2021/PR20210624-priz.html

JPCERT/CC Eyes「JPCERT/CC 感謝状 2021～コロナ禍におけるご尽力に感謝を込めて～」
https://blogs.jpcert.or.jp/ja/2021/06/jpcertcc-priz-2021.html

目次

本活動は、経済産業省より委託を受け、「令和３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. 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 10,274 件、インシデント件数ベースでは 6,977 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 3,745 件でした。前四半期の 4,005 件と比較して 6%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/2021/IR_Report20210715.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 4,841 件で、前四半期の 4,831 件とほぼ同数でした。また、前年度同期（5,262 件）との比較では、8%の減少となりました。

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	894	817	1,021	2,732（56%）
国外ブランド	479	431	223	1,134（23%）
ブランド不明 (注 2)	227	403	349	975（20%）
全ブランド合計	1,600	1,651	1,593	4,841

（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。

国外ブランドを装ったフィッシングサイトは、特定の通販サイトに偽装したフィッシングサイトおよび、金融機関を装ったものが多く見られました。また、通信事業者の会員向けサイトを装ったものが、増加傾向にありました。

フィッシングサイトに使用されるドメインは、ランダムな文字列を用いた.com や.cn、.xyz、.top ドメインが多く使用されていました。また、1 つサーバー上に複数のブランドのフィッシングサイトが建てられおり、それぞれのサイトのサブドメインには正規サイトのドメインに似せた文字列が付けられているものもありました。

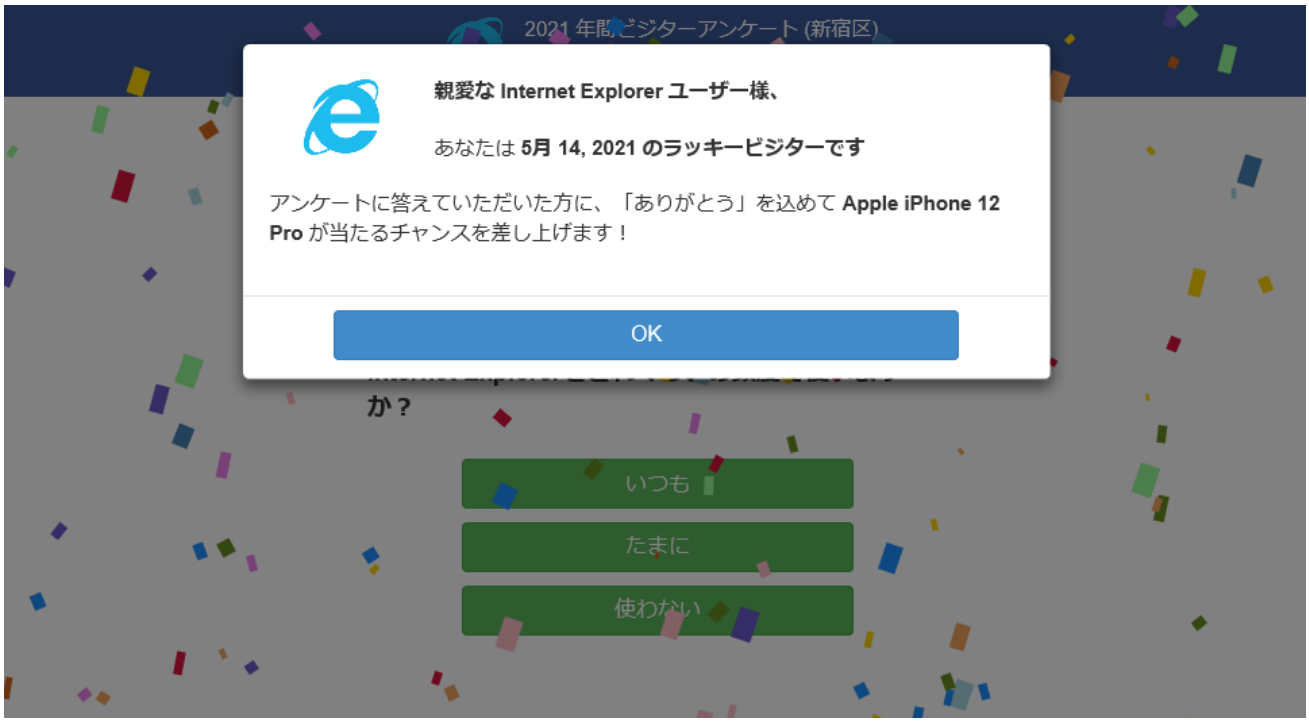
その他に、本四半期は Duck DNS を使ったフィッシングサイトの報告が多く寄せられました。Duck DNS は、無料のダイナミック DNS サービスで、短時間でサイトにアクセスできなくなることが多く、またサイトにアクセスするタイミングによってはメンテナンス中の画面やルーターの管理画面などが見えました。

フィッシングサイトの調整先の割合は、国内が 19%、国外が 81%であり、前四半期（国内が 23%、国外が 77%）と比べて国外の調整が増加しました。

1.1.1.2. Web サイト改ざん

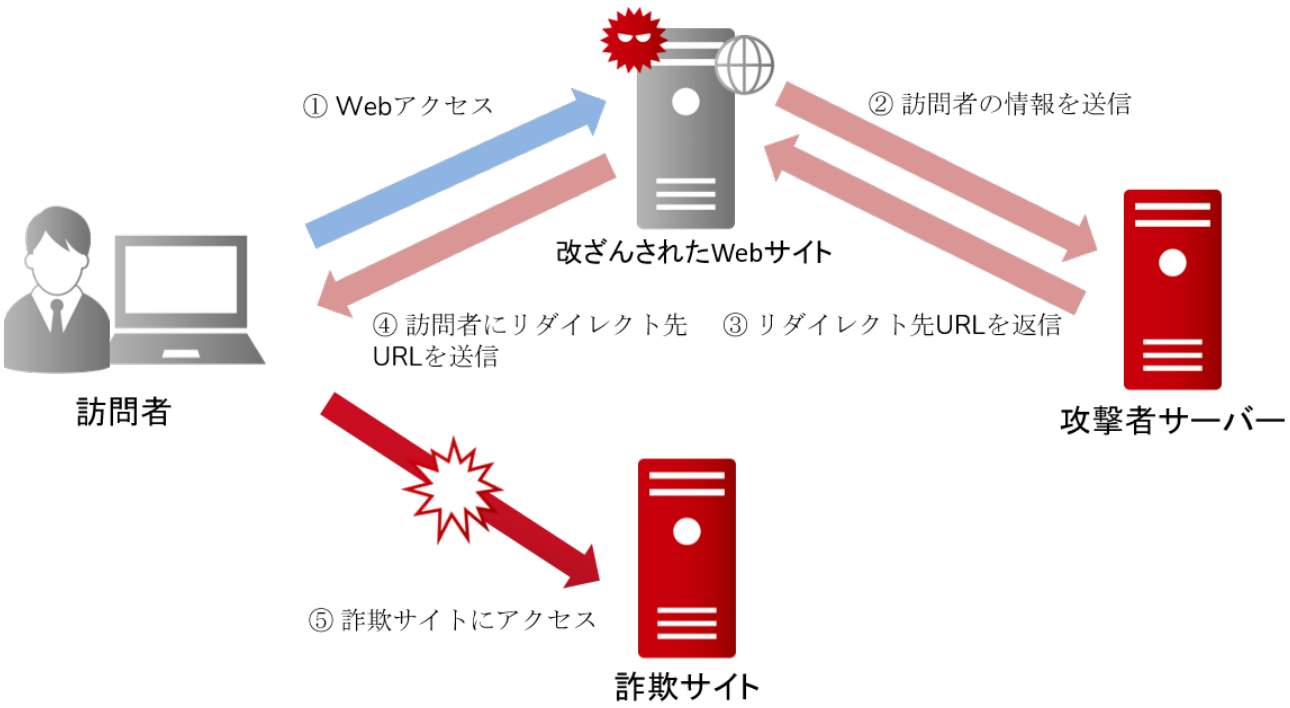
本四半期に報告が寄せられた Web サイト改ざんの件数は、251 件でした。前四半期の 282 件から 11%減少しています。

本四半期は、改ざんされた Web サイトから詐欺サイトや不審な商品販売サイトなどに誘導される報告が複数寄せられました。改ざんされた Web サイトには不正な PHP スクリプトが設置されており、そのスクリプトを利用して多数の不正なページが作成されます。［図 1-1］は、作成された不正なページにアクセスした際に表示されるラッキービジター詐欺ページの例です。



［図 1-1：転送先の詐欺サイトの例］

ページにアクセスすることで発生する転送までの流れは［図 1-2］のようになっています。



［図 1-2：詐欺サイトに転送するまでの流れ］

改ざんされた Web サイトにアクセスすると、訪問者の情報が攻撃者サーバーに送信されます。次に、攻撃者サーバーは訪問者の情報をもとに転送先となる URL をレスポンスとして返し、最終的に、この URL 宛に、改ざんされた Web サイトが訪問者を転送します。本攻撃の詳細については JPCERT/CC Eyes で解説しています。

JPCERT/CC Eyes「ラッキービジター詐欺で使用される PHP マルウェア」
https://blogs.jpcert.or.jp/ja/2021/06/php_malware.html

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、5 件でした。前四半期の 7 件から 29%減少しています。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

本四半期は、前四半期から引き続きマルウェア LODEINFO を使用した標的型攻撃の報告が寄せられました。マルウェア LODEINFO は、標的型攻撃メールに添付された Word ファイルを開いた際に、それに含まれる悪意のあるマクロが実行されることで感染します。

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や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 サイト改ざんなど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）など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や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. 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：18 件（うち更新情報が 5 件）　https://www.jpcert.or.jp/at/

2021-04-01　VMware vRealize Operations Manager などの複数の脆弱性に関する注意喚起（公開）
2021-04-14　2021 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）
2021-04-21　2021 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）
2021-04-21　Pulse Connect Secure の脆弱性（CVE-2021-22893）に関する注意喚起（公開）
2021-04-21　Trend Micro Apex One,Apex One SaaS およびウイルスバスター コーポレートエディションの脆弱性（CVE-2020-24557）に関する注意喚起（公開）
2021-04-22　Pulse Connect Secure の脆弱性（CVE-2021-22893）に関する注意喚起（更新）
2021-04-23　FileZen の脆弱性（CVE-2021-20655）に関する注意喚起（更新）
2021-04-30　ISC BIND 9 の複数の脆弱性に関する注意喚起（公開）
2021-05-06　Pulse Connect Secure の脆弱性（CVE-2021-22893）に関する注意喚起（更新）
2021-05-10　EC-CUBE のクロスサイトスクリプティングの脆弱性（CVE-2021-20717）に関する注意喚起（公開）
2021-05-12　Adobe Acrobat および Reader の脆弱性（APSB21-29）に関する注意喚起（公開）
2021-05-12　2021 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）
2021-05-26　VMware vCenter Server の複数の脆弱性（CVE-2021-21985、CVE-2021-21986）に関する注意喚起（公開）
2021-06-07　VMware vCenter Server の複数の脆弱性（CVE-2021-21985、CVE-2021-21986）に関する注意喚起（更新）
2021-06-09　Adobe Acrobat および Reader の脆弱性（APSB21-37）に関する注意喚起（公開）
2021-06-09　2021 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）
2021-06-11　Adobe Acrobat および Reader の脆弱性（APSB21-37）に関する注意喚起（更新）
2021-06-15　複数の EC-CUBE 3.0 系用プラグインにおけるクロスサイトスクリプティングの脆弱性に関する注意喚起（公開）

1.2.1.2. 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概要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 102 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。

2021-04-07　IPA が「企業ウェブサイトのための脆弱性対応ガイド」改訂版や研究会報告書などを公開
2021-04-14　IPA が「2020 年度サイバーセキュリティ経営ガイドライン実践のためのプラクティスの在り方に関する調査」報告書を公開
2021-04-21　JPCERT/CC が「2021 年 1 月から 3 月を振り返って」を公開
2021-04-28　経済産業省が「OSS の利活用及びそのセキュリティ確保に向けた管理手法に関する事例集」を公開
2021-05-12　経済産業省が「サイバーセキュリティ体制構築・人材確保の手引き」（第 1.1 版）を公開
2021-05-19　NISC が「次期サイバーセキュリティ戦略の骨子」を公開
2021-05-26　Internet Explorer 11 デスクトップアプリが 2022 年 6 月 15 日にサポート終了
2021-06-02　JNSA が「セキュリティ業務職種のキャリア展望について」を公開
2021-06-09　総務省が「テレワークセキュリティガイドライン（第 5 版）」を公開
2021-06-16　Japan Security Analyst Conference 2022 の CFP 募集開始
2021-06-23　「TRANSITS Workshop Online 2021 Summer」開催のお知らせ
2021-06-30　日本発の IoT 製品・システムを安全に実装するための国際規格について

1.2.1.3. 早期警戒情報

JPCERT/CC は、社重要社会インフラを支え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/

1.2.1.4. 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。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：15 件（うち更新情報が 1 件）　https://www.jpcert.or.jp/newsflash/

2021-04-08　Sensorweb 製 ScadaBR に任意のファイルをアップロードされる問題について
2021-04-14　複数のアドビ製品のアップデートについて
2021-04-15　2021 年 1 月から 3 月を振り返って
2021-04-15　GarageBand に関するアップデートについて
2021-04-27　複数の Apple 製品のアップデートについて
2021-04-28　2021 年 1 月から 3 月を振り返って（更新）
2021-05-06　複数の Apple 製品のアップデートについて
2021-05-12　複数のアドビ製品のアップデートについて
2021-05-12　Intel 製品に関する複数の脆弱性について
2021-05-19　Boot Camp に関するアップデートについて
2021-05-25　複数の Apple 製品のアップデートについて
2021-06-09　複数のアドビ製品のアップデートについて
2021-06-09　Intel 製品に関する複数の脆弱性について
2021-06-16　iOS に関するアップデートについて
2021-06-23　iMovie のアップデートについて

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) Pulse Connect Secure の脆弱性（CVE-2021-22893）に関する情報発信

2021 年 4 月 20 日（米国時間）、Pulse Secure 社から、VPN 製品の Pulse Connect Secure の脆弱性（CVE-2021-22893）に関する情報が公開されました。本脆弱性が悪用された場合、遠隔の第三者が認証を回避し、任意のコードを実行するなどの可能性があります。また、同日に FireEye がブログを公開し、本脆弱性や既知の Pulse Connect Secure の脆弱性を悪用した攻撃および侵害事例を複数確認していることを明らかにしました。この時点では脆弱性を修正するバージョンやパッチは公開されていませんでしたが、すでに脆弱性を悪用した攻撃が確認されていたため、JPCERT/CC は 2021 年 4 月 21 日に注意喚起を公開し、同製品のユーザーに向けて回避策の適用や侵害されていないことをツールで確認するよう呼び掛けました。その後、5 月 3 日（米国時間）に Pulse Secure 社から CVE-2021-22893 に対応した修正バージョンが公開されたため、注意喚起を

更新し修正バージョンの適用を呼び掛けました。

Pulse Connect Secure の脆弱性（CVE-2021-22893）に関する注意喚起
https://www.jpcert.or.jp/at/2021/at210019.html

(2) EC-CUBE の脆弱性（CVE-2021-20717）に関する情報発信

2021 年 5 月 7 日、株式会社イーシーキューブから、EC-CUBE のクロスサイトスクリプティングの脆弱性（CVE-2021-20717）に関する情報が公開されました。本脆弱性が悪用された場合、当該製品で作成された EC サイトの管理者のブラウザー上で任意のスクリプトが実行され、結果として当該 EC サイトへの不正アクセスや個人情報の窃取などが行われる可能性があります。同社によると本脆弱性を悪用する攻撃が確認されています。また、4 月 28 日（米国時間）にトレンドマイクロが、オンラインショップサイトを侵害する攻撃キャンペーン「Water Pamola」に関する情報を公開しており、その中で、最近の攻撃動向として日本国内のオンラインショップにおけるクロスサイトスクリプティングの脆弱性を悪用した攻撃手法について言及しています。
JPCERT/CC は、本脆弱性がすでに悪用されていることから 5 月 10 日に注意喚起を公開し、当該製品のユーザーに向けて早急に対策をとるよう呼び掛けました。また、株式会社イーシーキューブが公開している、すでに本脆弱性を悪用した攻撃を受けているか否かを確認する方法を参考情報として注意喚起に掲載しました。

EC-CUBE のクロスサイトスクリプティングの脆弱性（CVE-2021-20717）に関する注意喚起
https://www.jpcert.or.jp/at/2021/at210022.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、国や地域ごとにその分布状況を分析しています。

・19/udp（CHARGEN）
・53/udp（DNS）
・123/udp（NTP）
・161/udp（SNMP）
・445/tcp（MSDS）
・1900/udp（SSDP）
・5060/udp（SIP）

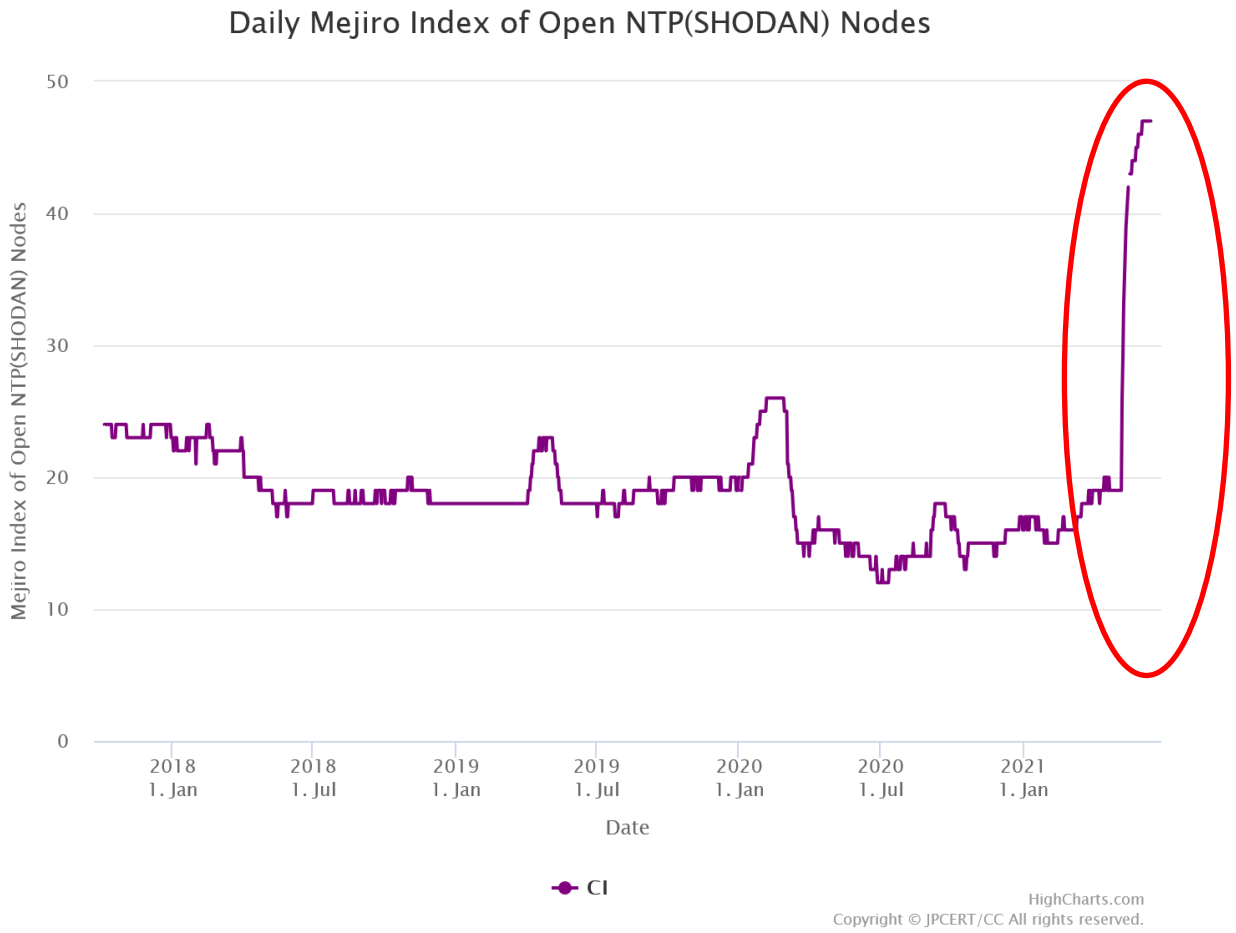
それらのノードの IP アドレスをもとにノードが設置された国・地域を判別して、リスク要因の分布状況を調べます。さらに、国・地域ごとのリスク要因となるノード数から、Mejiro 指標と呼ばれる指標値を算出します。各国・地域の Mejiro 指標の値を比較することで、それぞれの国・地域の相対的な特徴を明らかにして、対策の必要性や方向性を判断する参考にできると期待し、一般に公表しています。各国・地域の Mejiro 指標の値を比較することで、それぞれの国・地域の相対的な特徴が明らかになり、それを参考に対策の必要性や方向性を判断いただけることを期待しています。

1.3.1.2. Mejiro による観測動向

本四半期における Mejiro 指標の変化について、特徴的であったものを説明します。JPCERT/CC では、こうした情報を該当国・地域の National CSIRT に提供し、攻撃の事前把握や防止に努めています

(1) CL（コートジボアール）での 123/UDP での変化

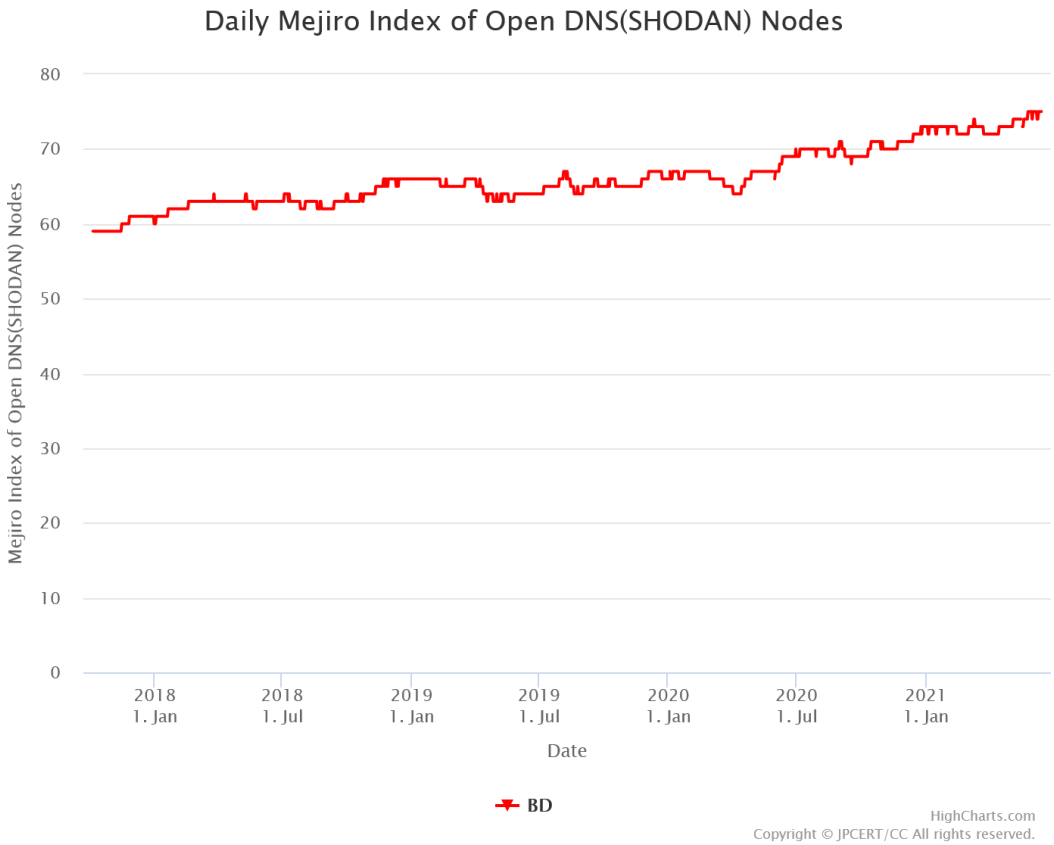
CL（コートジボアール）での 123/UDP に対する Mejiro 指標が、2021 年 5 月に 20 ポイント増加（[図 1-3]）しています。この変化は、約 2,500 ノードの増加に相当します。この変化の要因は不明です。一方で、123/UDP については、「インターネット定点観測レポート（2021 年 1～3 月）」が書いたように、TSUBAME の観測でも複数のスキャンが観測されていました。このスキャンの実行主体や狙いも不明です。引き続き調査の必要があります。



［図 1-3：ccTLD:CI Port:123/UDP の Mejiro 指標の変化］

(2) BD（バングラデシュ）でのオープンリゾルバーの増加

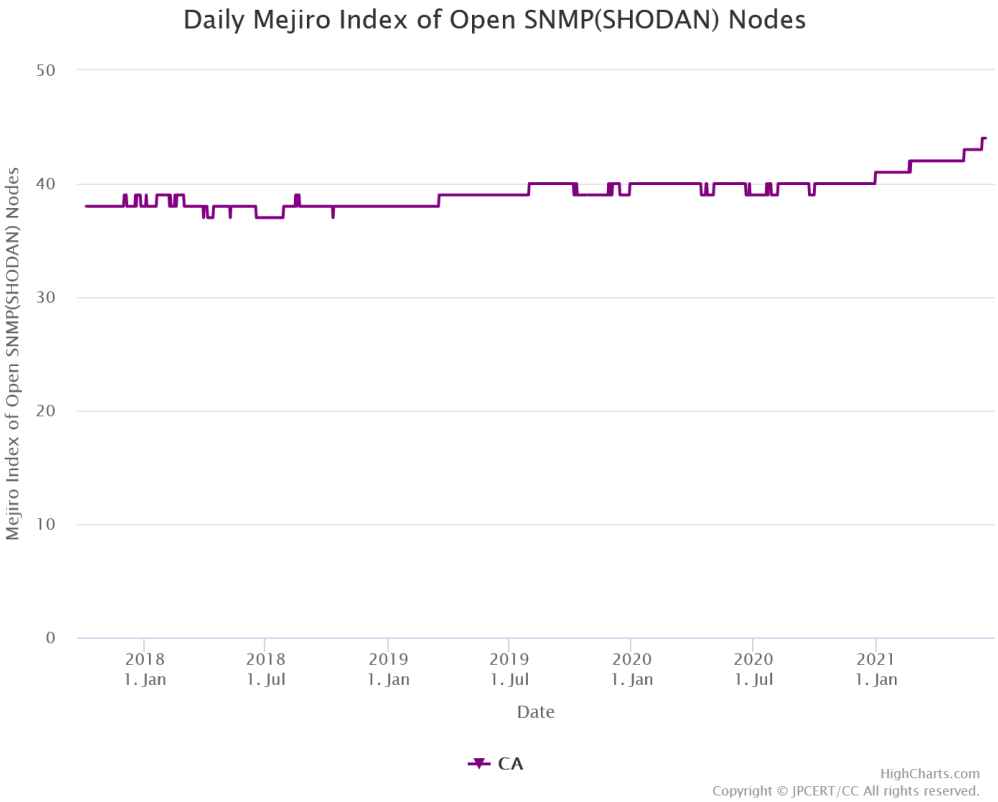
BD（バングラデシュ）の 53/UDP, オープンリゾルバーの Mejiro 指標について増加の傾向が続いています（[図 1-4]）。2 年間で 10 ポイント上昇しており、本四半期では 1.8 ポイント増加が見られます。



［図 1-4：ccTLD:BD Port:53/UDP の Mejiro 指標の変化］

(3) CA（カナダ）での 161/UDP の増加

CA（カナダ）の 161/UDP についての Mejiro 指標も増加の傾向にあります（［図 1-5］）。本四半期では 1.6 ポイント増加しており、そのノードの中には、コミュニティー名が「***public***」に設定されているものも見つかりました。こういった機器はルーターに設定されている情報が閲覧されるだけではなく、DDoS の踏み台に悪用される恐れもあります。



［図 1-5：ccTLD:CA Port:161/UDP の Mejiro 指標の変化］

1.3.1.3. CyberGreen Institute のデータ提供の終了

CyberGreen Institute のデータは Mejiro のデータソースの 1 つとして、2019 年 3 月 18 日から Mejiro 指標に組み込まれていました。データ提供の契約が終了したため、2021 年 3 月 31 日をもって、Mejiro 指標を算出するデータソースから除外いたしました。Mejiro では新しいデータソースが見つかり次第、順次追加していく予定です。

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」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付くことがあります。
観測用センサーの設置に協力した各地域 National CSIRT 等とは、センサーの観測結果を一つのデータとして共有しデータの共同での分析や、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 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

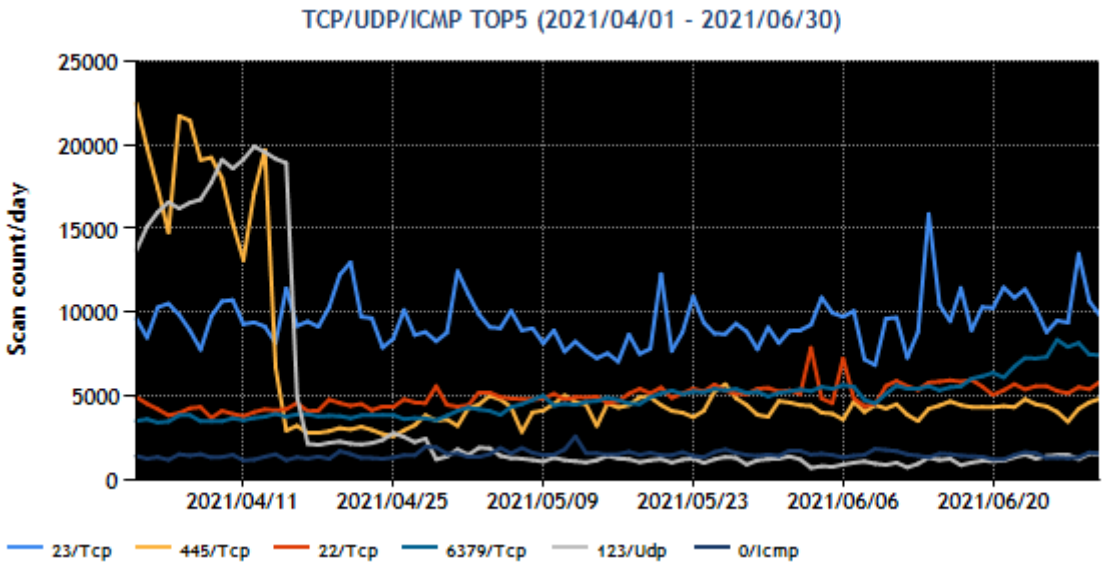
JPCERT/CC では、主に日本企業のシステム管理者の方々に、自組織のネットワークに届くパケットの傾向と比較していただけるよう、日本国内の TSUBAME のセンサーで受信したパケットを宛先ポート別に集計してグラフ化し、毎週月曜日に JPCERT/CC の Web ページで公開しています。また、四半期ごとに観測傾向や注目される現象を紹介する「インターネット定点観測レポート」を公開しており、2021 年 1 月から 3 月分のレポートを 2021 年 4 月 20 日に公開しました。

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

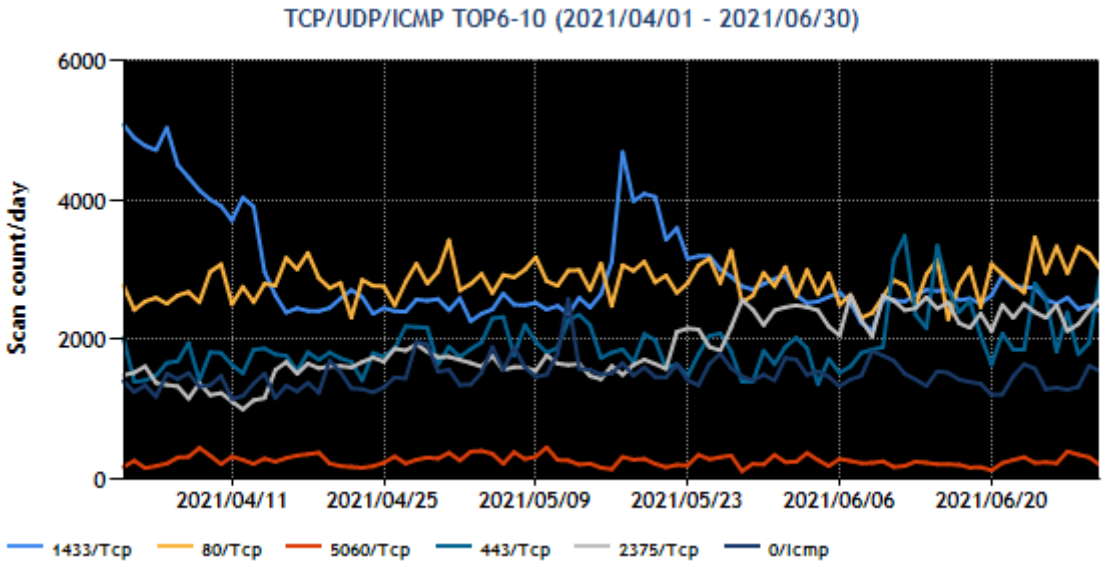
インターネット定点観測レポート（2021 年 1～3 月）
https://www.jpcert.or.jp/tsubame/report/report202101-03.html

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 1-6］と［図 1-7］に示します。

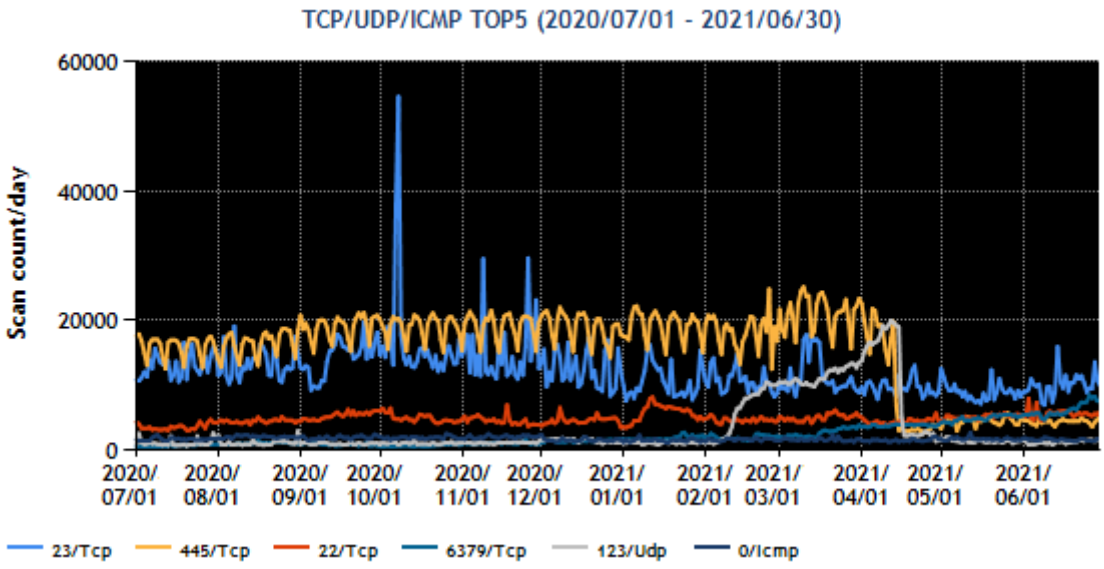


［図 1-6：宛先ポート別グラフ トップ 1-5（2021 年 4 月 1 日-6 月 30 日）］

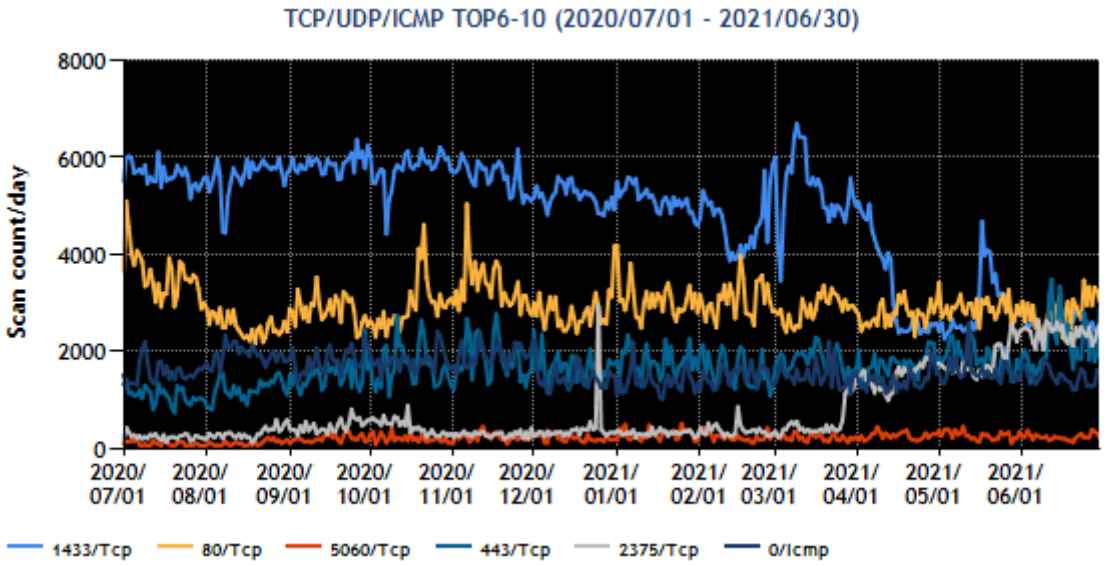


［図 1-7：宛先ポート別グラフ トップ 6-10（2021 年 4 月 1 日- 6 月 30 日）］

また、過去 1 年間（2020 年 7 月 1 日-2021 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（2020 年 7 月 1 日-2021 年 6 月 30 日）］



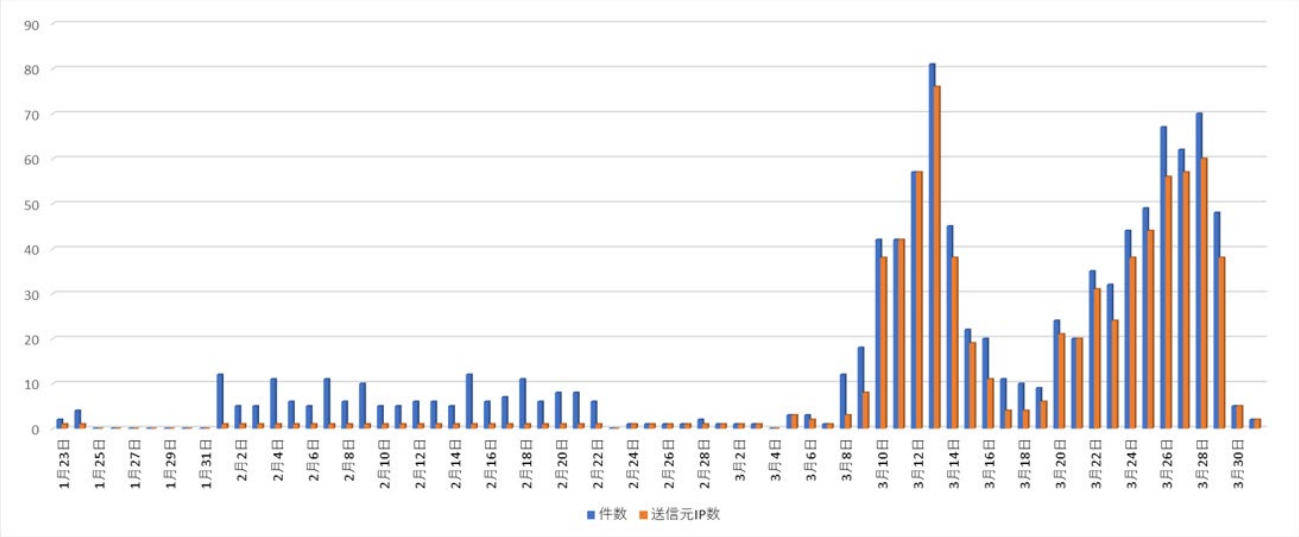
［図 1-9：宛先ポート別グラフ トップ 6-10（2020 年 7 月 1 日-2021 年 6 月 30 日）］

本四半期に最も多く観測されたパケットは 23/TCP（telnet-d）宛のものでした。2021 年 4 月 15 日より、445/TCP（Microsoft-ds）宛のパケット数が大きく減少し順位が入れ替わりました。445/TCP 宛のパケットが減少した理由は不明ですが、国内の送信元についてはその後もパケットを観測している送信元 IP アドレスがあるため、管理者に対してパケットが送信されている旨を通知しています。

1.3.2.4. 定点観測網の拡充に向けた運用とその分析

JPCERT/CC では、スキャン活動に関して、TSUBAME による観測だけでなく、スキャンに応答した場合に始まる攻撃の手口を捕捉したいと考え、攻撃者からの通信内容を低対話型ハニーポットにより観測するためのシステムを用意して、その有効性を確認するための運用を行っています。現在は、HTTP リクエストによる攻撃を収集し、分析を行っています。

低対話型ハニーポットにおいて 2021 年 1 月 23 日以降、Laravel の脆弱性（CVE-2021-3129）の悪用を試みる通信が観測されています。特に、2021 年 3 月 8 日頃から送信元 IP 数および送信件数が増加（[図 1-10]）し、日本国内から送信された通信も確認されました。
この通信は、Laravel がデバックモードで稼働しているサーバーに対して細工した POST リクエストを送信することで、サーバー上で任意のコード実行を可能にするものです。また、観測されたペイロードは、本脆弱性の発見者が公開した実証コードに含まれるペイロードと類似していました。
JPCERT/CC では、本脆弱性に関する情報提供を行うにあたり、攻撃が成立する条件等を、発見者により公開されている実証コードを用いて検証しました。検証結果については、CISTA を通じて Laravel の脆弱性（CVE-2021-3129）に関する検証レポートとして提供しました。



［図 1-10：Laravel の脆弱性（CVE-2021-3129）の悪用を試みる通信の観測件数推移］

また、HTTP プロトコル以外のプロトコルによる攻撃も観測できるよう複数のハニーポットの試用をはじめています。
SSH や RDP、FTP 等これまでは観測できなかった通信の収集を行っており、今後は、これらのプロトコルによる攻撃行為に関しても関係者に対策を促す準備を進める予定です。

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など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など、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/

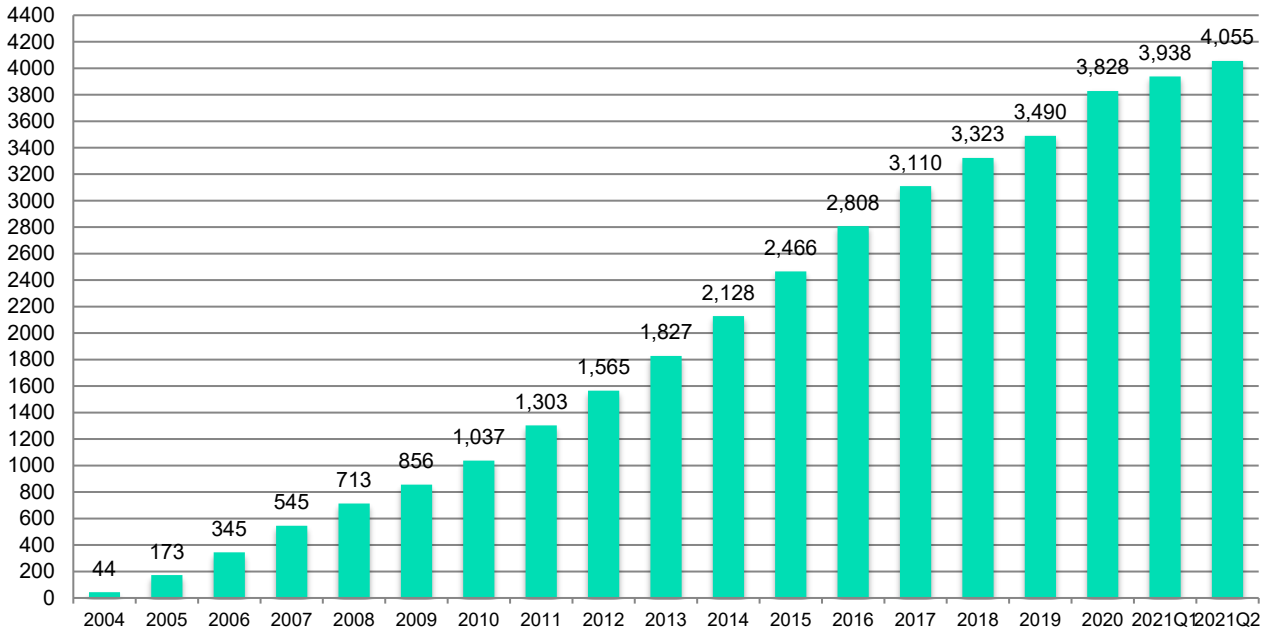
2.1.2. Japan Vulnerability Notes（JVN）において公表した脆弱性情報および対応状況

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 117 件（累計件 4,055）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/



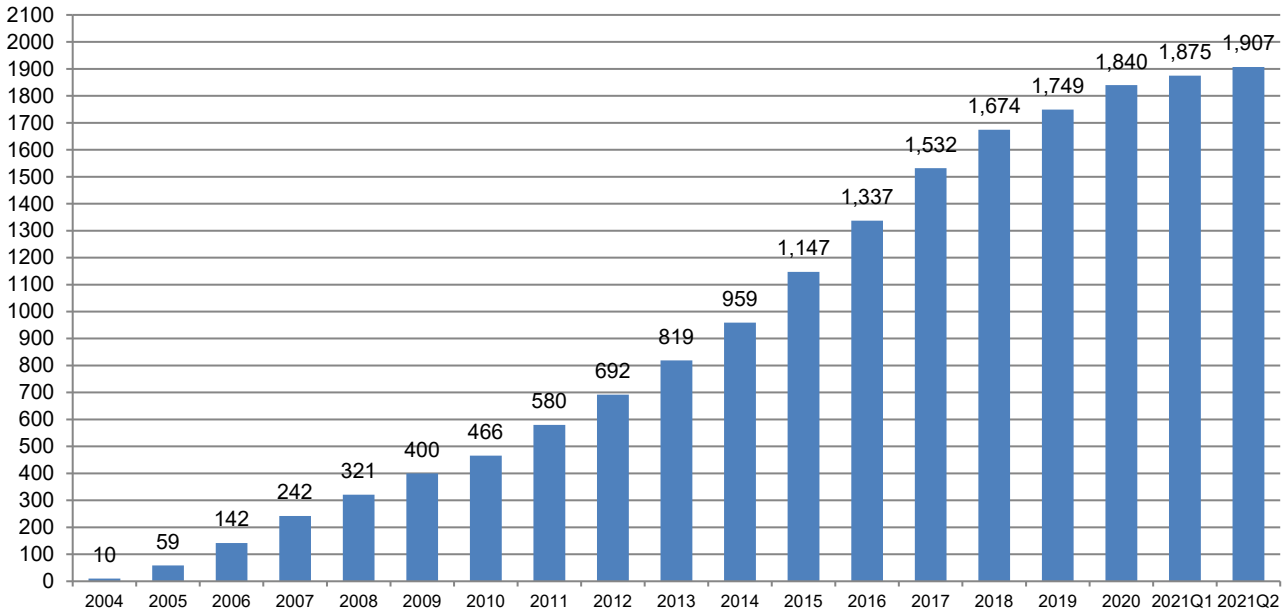
［図 2-1：JVN 公表累積件数］

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 32 件（累計 1,907 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 32 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 23 件（このうち自社製品の届け出によるものが 4 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 9 件ありました。また、悪用した攻撃が一部で観測されている脆弱性の情報を「緊急」として公表したものが 32 件中 2 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、プラグインが 7 件と最も多く、次いで CMS と組込系製品がそれぞれ 6 件、続いてスマートフォンアプリケーション 4 件、Windows アプリケーション、ウェブアプリケーション、マルチプラットフォームアプリケーションがそれぞれ 2 件、Android アプリケーション、アプリケーションフレームワーク、サーバー製品がそれぞれ 1 件でした。

［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
プラグイン	7
CMS	6
組込系製品	6
スマートフォンアプリケーション	4
Windows アプリケーション	2
ウェブアプリケーション	2
マルチプラットフォームアプリケーション	2
Android 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
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］

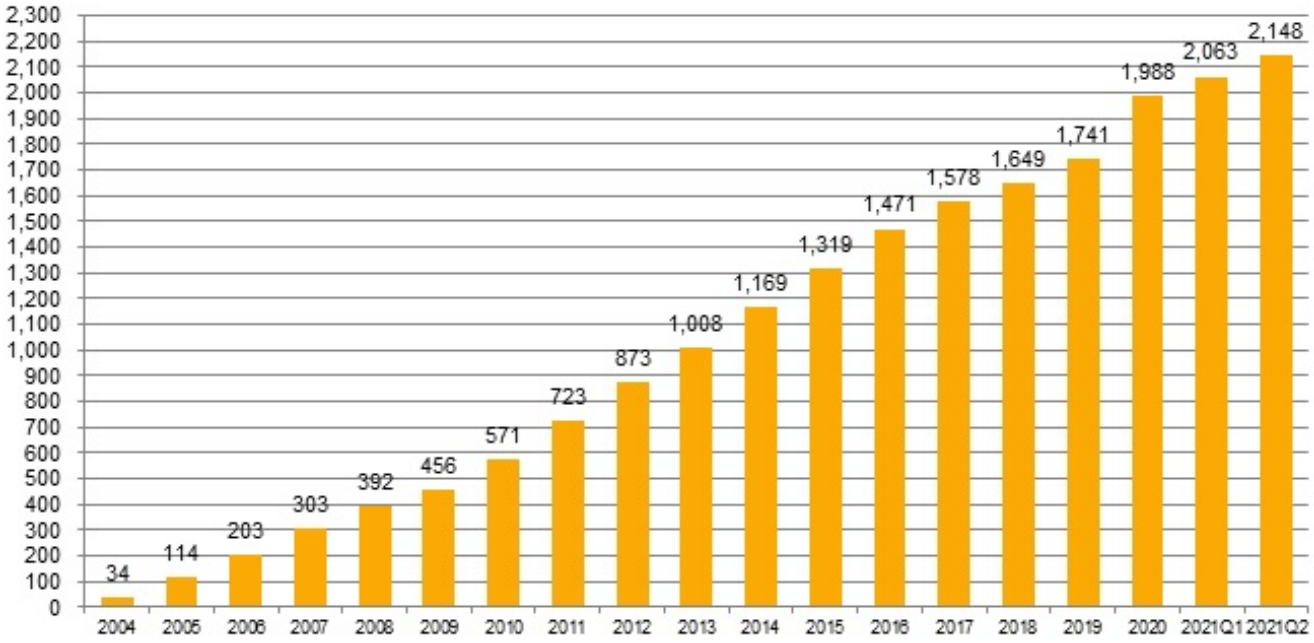
本四半期に公表した国際取扱脆弱性情報は 85 件（累計 2,148 件）で、累計の推移は［図 2-3］に示すとおりです。85 件のアドバイザリのうち、海外調整機関や製品開発者等からの届け出によるものおよび製品開発者による脆弱性情報公開の事前通知によるものは 18 件、国内外の発見者からの届け出によるものは 5 件、JPCERT/CC が注意喚起として発行したものは 1 件でした。また、攻撃観測を伴う脆弱性情報を「緊急」として公表したものが 85 件中 2 件ありました。

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内訳は、［表 2-2］のとおりです。本四半期は、制御系製品が 59 件と最も多く、次いでアンチウイルス製品が 8 件、組込系製品が 6 件、医療機器が 3 件、DNS、サーバー製品、マルチプラットフォームアプリケーションに関するものがそれぞれ 2 件、プロトコル、ライブラリ、その他に関するものがそれぞれ 1 件でした。

本四半期も、国際取扱脆弱性情報の中には、製品開発者自身が届け出たものや、自社製品に関する脆弱性情報を公開に先立って JPCERT/CC へ事前に通知したものが比較的多く見られました。このような製品開発者自身から広く一般への告知を目的としたものも含めて、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	59
アンチウイルス製品	8
組込系製品	6
医療機器	3
DNS	2
サーバー製品	2
マルチプラットフォームアプリケーション	2
プロトコル	1
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、50 件（製品開発者数で 30 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 200 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ように 2014 年から制度が改正されました。本年度においては、前四半期に公表判定委員会が開催され、そこで連絡不能開発者一覧に掲載されている 10 件の製品について審議し、9 件については公表が妥当と判定がされ、前四半期の 3 月 25 日にそれら 9 件を公表し、さらに、製品開発者との最終確認を行う必要が生じた 1 件に関して本四半期の 4 月 22 日に JVN にて公表しました。これまでに公表判定委員会での審議を経て累計で 30 件（製品開発者数で 19 件）を JVN の「Japan Vulnerability Notes JP（連絡不能）一覧」に掲載しています。

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

Japan Vulnerability Notes JP（連絡不能）一覧
https://jvn.jp/adj/

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など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 49 個の CVE 番号を付与しました。

最初は CVE 番号の付与を、MITRE 社から番号プールの提供を受けて、その中から採番することにより実施していましたが、2010 年 6 月には CNA（CVE Numbering Authorities）として CVE 番号を付与し始めました。2018 年には Root CNA に指定され、新しい CNA の招致やトレーニングなどの活動も行っています。こうした活動の結果として、前四半期までに三菱電機株式会社、株式会社 LINE、日本電気株式会社（NEC）の 3 社が JPCERT/CC を Root とする CNA として登録されました。本四半期においては新たに、株式会社東芝が 4 社目の CNA として登録されました。また、同じ Root CNA である米国の MITRE 社ならびに CISA ICS とともに、CVE Program への関与や成り立ちなどに関する話をした Podcast エピソード「Partnering with the CVE Program - Episode 3」が 4 月に公開されたほか、5 月には各国の CNA が集う CVE Summit という会合にて、JPCERT/CC の Root CNA 活動に関する発表を行いました。

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

JPCERT/CC Eyes「CNA 活動レポート ～日本の 2 組織が新たに CNA に参加～」
https://blogs.jpcert.or.jp/ja/2020/12/cna-2cna.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/vulinfo.html

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

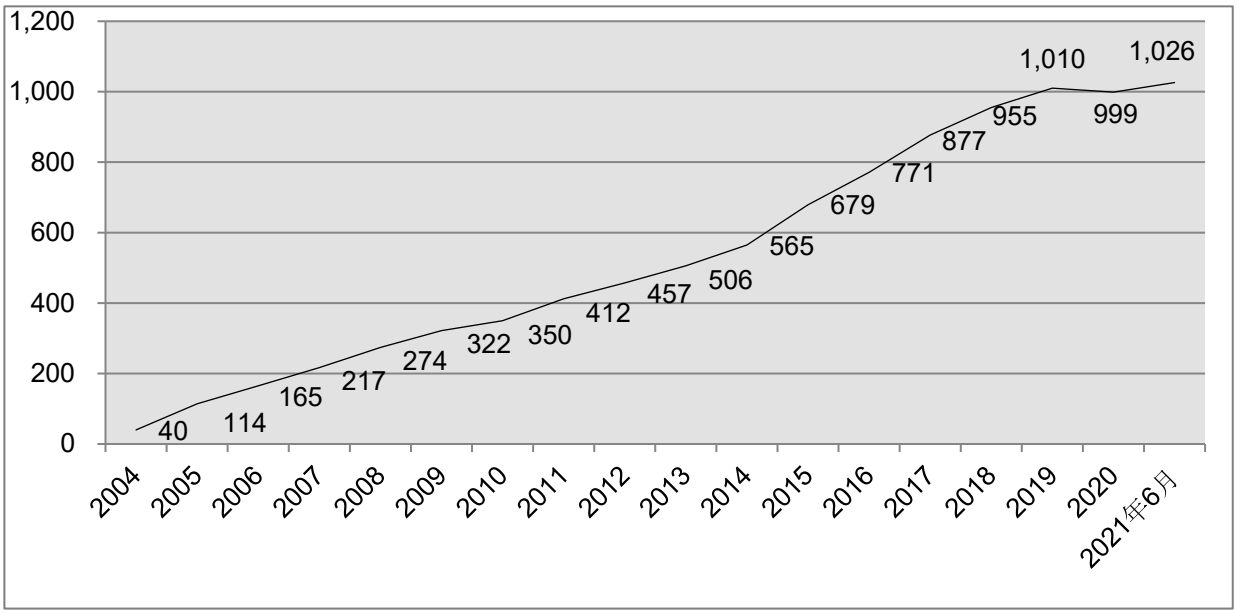
情報セキュリティ早期警戒パートナーシップガイドライン（2019 年版）
https://www.jpcert.or.jp/vh/partnership_guideline2019.pdf

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、2021 年 6 月 30 日現在で 1,026 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］

2.2.2. 製品開発者との定期ミーティングの実施

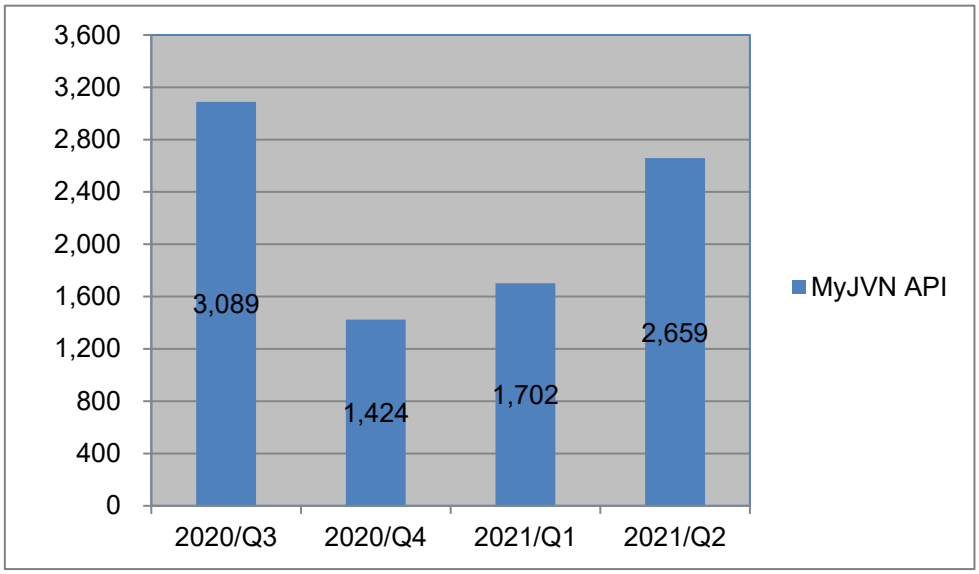
JPCERT/CC では、技術情報やセキュリティ・脆弱性の動向などの情報交換や、脆弱性情報ハンドリング業務に関する製品開発者との意見交換、また、製品開発者間の情報交換を目的として、脆弱性情報ハンドリングにご協力いただいている製品開発者の皆さまとのミーティングを定期的に開催しています。
新型コロナウイルスの流行状況を鑑み、昨年度よりオンライン形式にてミーティングを開催しています。本四半期は 5 月 28 日にミーティングを開催し、脆弱性を悪用する攻撃活動の観測状況、PSIRT 向け演習プログラム、JVN 掲載項目の変更などのプログラム構成で、参加者との意見交換を行いました。

2.3. VRDA フィードによる脆弱性情報の配信

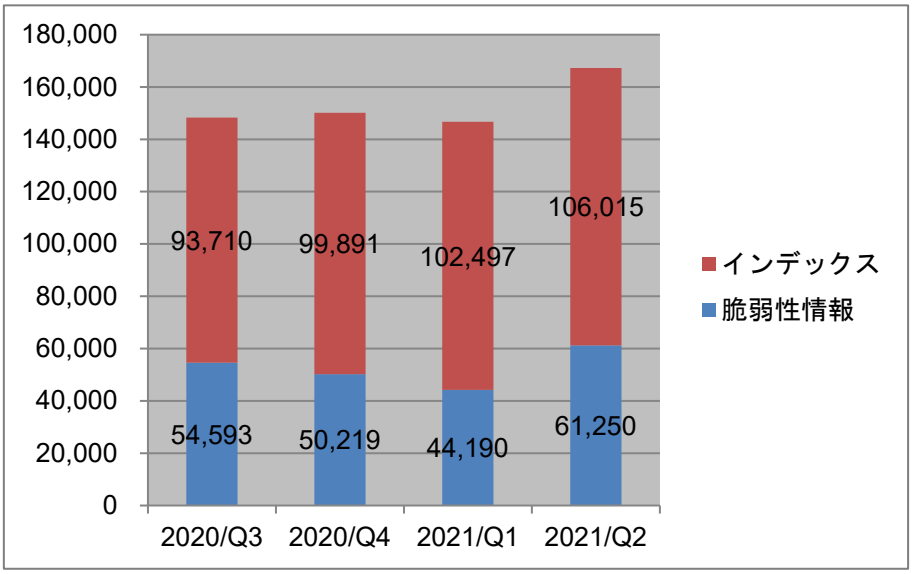
JPCERT/CC は、大規模組織の組織内 CSIRT 等での利用を想定して、ツールを用いた体系的な脆弱性対応を可能とするため、IPA が運用する MyJVN API を外部データソースとして利用した、VRDA（Vulnerability Response Decision Assistance）フィードによる脆弱性情報の配信を行っています。VRDA フィードについての詳しい情報は、次の Web ページを参照ください。

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。

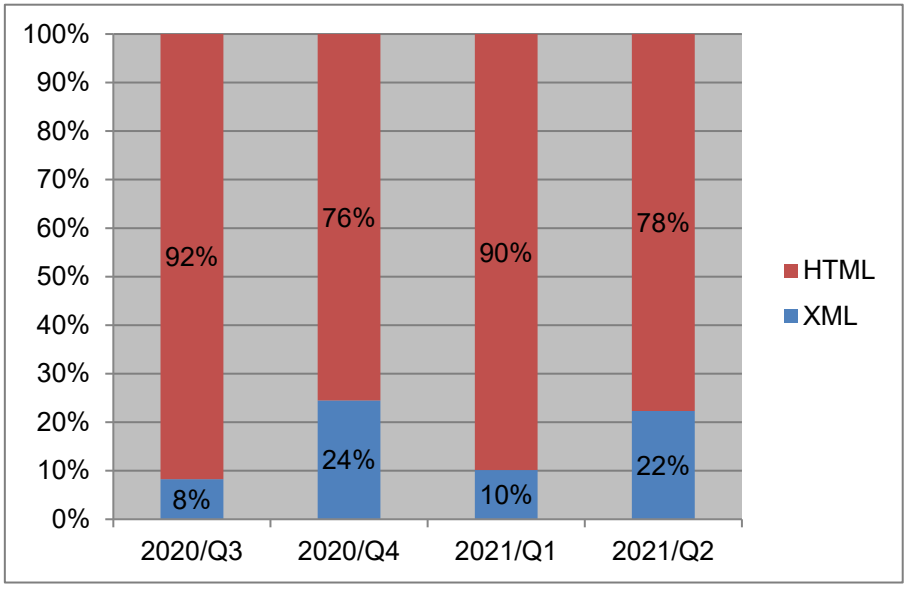


［図 2-5：VRDA フィード配信件数］



［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、約 3%増加しました。
脆弱性情報の利用数については、約 39%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 12%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などを収集・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 296 件でした。

3.1.1. 情報提供

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 1 件でした。

2021/05/25 【参考情報】石油・ガス業界向けサイバーレジリエンス強化のホワイトペーパーについて

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。

2021/04/09 制御システムセキュリティニュースレター 2021-0003
2021/05/10 制御システムセキュリティニュースレター 2021-0004
2021/06/04 制御システムセキュリティニュースレター 2021-0005

制御システムセキュリティ情報共有コミュニティーとして、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 1,199 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

上記の情報提供以外にも、制御システムに関連するソフトウェアや機器において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。また、発行時点で注意喚起の基準に満たないものの国内で利用が認められる制御システムに関連する製品の脆弱性情報も対策に留意いただくため、情報提供しています。

3.1.1.1. 注意喚起

本四半期に発行した注意喚起は 0 件でした。

3.1.1.2. その他、留意いただくべき脆弱性情報

CyberNewsFlash を通じて発信した件数：1 件

2021/04/08　Sensorweb 製 ScadaBR に任意のファイルをアップロードされる問題について

JVN を通じて発信した件数：3 件

2021/04/08　JVNVU#90815335: Softing AG 製 OPC Toolbox における複数の脆弱性
2021/05/12　JVNVU#98262671: Advantech 製 WebAccess/HMI Designer に任意コード実行の脆弱性
2021/05/12　JVNVU#92650134: Delta Electronics 製 DOPSoft に境界外読み取りの脆弱性

3.1.2. 提供情報の事例紹介

本四半期における情報収集・分析・提供した事例を紹介します。これらの脆弱性情報は、すぐに悪用される可能性は低いものの、国内の利用者に向けて注意を促す目的で発信いたしました。

(1) Advantech 製 WebAccess/HMI Designer に任意コード実行の脆弱性

2021 年 4 月 21 日、海外セキュリティ組織より、Advantech 製 WebAccess/HMI Desinger におけるメモリ破損の脆弱性に関する情報が公開され、2021 年 4 月 28 日に同製品に関する追加の脆弱性情報が当該セキュリティ組織より公開されました。この脆弱性を悪用しようとする第三者が細工して提供したファイルをユーザーが読み込んだ場合、第三者が組み込んだ任意のコードが実行されます。

JPCERT/CC では、本脆弱性が調整機関とベンダーとの調整において報告から一定期間を経過したことにより、調整機関に本脆弱性を報告した発見者から情報公開されたことを確認し、5 月 12 日に JVN で脆弱性情報を発信しました。

JVNVU#98262671　Advantech 製 WebAccess/HMI Designer に任意コード実行の脆弱性
https://jvn.jp/vu/JVNVU98262671/index.html

(2) Delta Electronics 製 DOPSoft に境界外読み取りの脆弱性に関する情報発信

2021 年 5 月 6 日、海外セキュリティ組織より、Delta Electronics 製 DOPSoft における境界外読み取りの脆弱性に関する情報が公開されました。この脆弱性を悪用しようとする第三者が細工して提供したファイルをユーザーが読み込んだ場合、第三者が組み込んだ任意のコードが実行されます。

JPCERT/CC では、本脆弱性が調整機関とベンダーとの調整において報告から一定期間を経過したことにより、調整機関に本脆弱性を報告した発見者から情報公開されたことを確認し、5 月 12 日に JVN で脆弱性情報を発信しました。

JVNVU#92650134　Delta Electronics 製 DOPSoft に境界外読み取りの脆弱性
http://jvn.jp/vu/JVNVU92650134/index.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を行っています。本四半期における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。

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 3 件の利用申込みがあり、直接配付件数の累計は、日本版 SSAT が 285 件でした。

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カンファレンス

2021 年 2 月 12 日（金）にオンライン開催した「制御システムセキュリティカンファレンス 2021」に関する英語版ブログ記事を 4 月 1 日（木）に公開しました。2020 年の制御システムセキュリティ全体の動向や、スマート家電の製品安全とセキュリティに関する考え方や取り組み、国内制御システムユーザー組織の取り組みや課題など、同カンファレンスで行われた 6 つの講演の概要を海外の制御システムセキュリティ関係者に向けて紹介しています。

JPCERT/CC Eyes：ICS Security Conference 2021
https://blogs.jpcert.or.jp/en/2021/04/ics-conference2021.html

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。

4.1.1. フィリピン CERT-PH に対する TSUBAME トレーニング

JPCERT/CC は 4 月 21 日にフィリピンの CERT-PH に対して TSUBAME センサーの運用およびデータの活用方法に関するトレーニングをオンラインで開催しました。

4.1.2. ベトナム向け CSIRT トレーニング

JPCERT/CC は、独立行政法人国際協力機構（JICA）がベトナムに対して行っている「サイバーセキュリティに関する能力向上プロジェクト」に協力し、6 月 15 日から 18 日にかけてオンラインでトレーニングを実施しました。同国からは情報セキュリティ庁 Authority of Information Security（AIS）、National CSIRT である VNCERT/CC、関連する省庁や通信事業者に所属する技術者など 29 名が参加しました。JPCERT/CC は CSIRT 運用の基礎や日本のインシデント動向に加えて、TSUBAME の活用方法や Mejiro で観測できるインターネット上のリスク状況などについて講演を行いました。本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。

独立行政法人国際協力機構（JICA）
https://www.jica.go.jp/

サイバーセキュリティに関する能力向上プロジェクト
https://www.jica.go.jp/project/vietnam/052/outline/index.html

［図 4-1: 研修の様子］

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 において、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、6 月 2 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。2020 年版の報告書は、JPCERT/CC を含む 30 のオペレーショナルメンバーが寄稿し、4 月 27 日に公開されました。

［図 4-2: APCERT 年次報告書表紙］

APCERT Annual Report 2020
https://www.apcert.org/documents/pdf/APCERT_Annual_Report_2020.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. 33rd Annual FIRST Conference

第 33 回 FIRST 年次会合は、新型コロナウイルス感染拡大の影響を受けて、福岡での予定をオンライン開催に切り替えて、6 月に行われました。日本や海外の National CSIRT や民間企業の CSIRT を含むサイバーセキュリティの専門家が、各自の CSIRT 運用に係る技術やインシデント対応事例を紹介しました。

第 33 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。

33rd Annual FIRST Conference
https://www.first.org/conference/2021/program

4.2.2.2. FIRST の理事に当選

FIRST の活動の企画・立案等を行う Board of Directors を構成する 10 名の理事は、参加組織による選挙によって選出されます。今回の選挙は事前にオンライン投票が行われ、6 月 10 日の総会で結果が発表されました。その結果、JPCERT/CC 国際部マネージャーの内田有香子が当選を果たしました。今後 2 年間の任期をとおして、FIRST の運営に携わり、CSIRT 間の国際連携の活性化に貢献してまいります。Board of Directors のメンバーについては、次の URL をご参照ください。

FIRST.Org,Inc., Board of Directors
https://www.first.org/about/organization/directors

4.3. その他国際会議への参加

4.3.1. Locked Shields への参加

4 月 13 日から 16 日にかけて、NATO サイバー防衛協力センター（Cooperative Cyber Defence Centre of Excellence : CCDCOE）が主催する国際的なサイバー演習 Locked Shields 2021 にリモートで参加しました。JPCERT/CC は日本の政府・重要インフラ事業者の参加者とともにブルーチームの一員として、インシデントの対応およびフォレンジックや法務・広報の課題に取り組みました。Locked Shields の詳細については、次の URL のブログで公開している参加記をご参照ください。

Locked Shields
https://ccdcoe.org/exercises/locked-shields/

JPCERT/CC Eyes「Locked Shields 2021 参加記」
https://blogs.jpcert.or.jp/ja/2021/05/locked-shields-2021.html

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・仕様に関する標準化を担当）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。

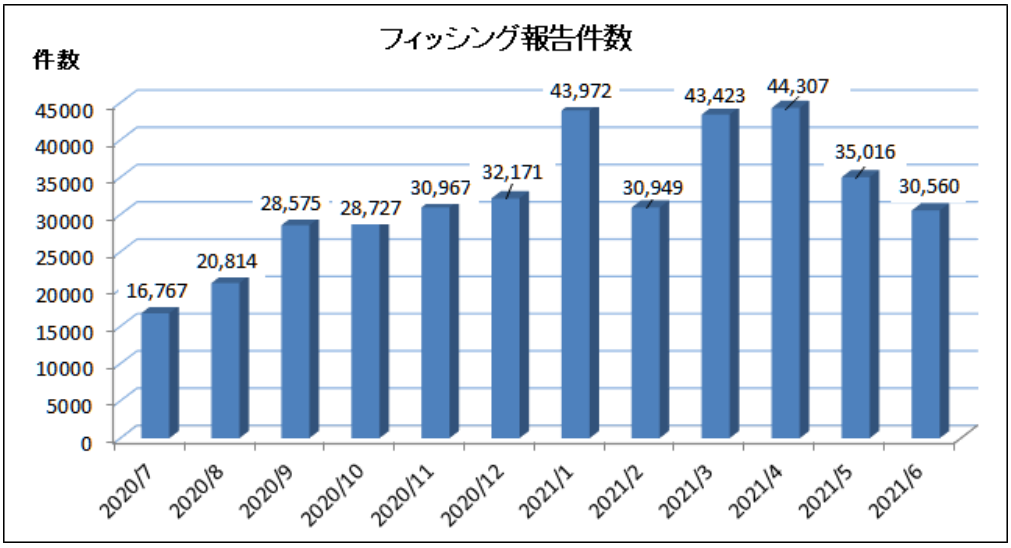
前回に引き続きオンライン形式で 4 月に開催された SC27 の作業部会の国際会議に参加しました。会議期間中、WG3 では「複数の開発者が関与する脆弱性の開示と取扱」に関して、前四半期に提出した技術報告書の WD：Working draft（作業原案）へのコメント寄稿者との個別会議に参加しコメントや WD 内容に関する議論を行いました。そして WG3 本会議において、技術報告書の作成が正式に承認されました。WG4 では「インシデント管理に関する標準」文書に関して、既存の標準文書の改訂について作成中の CD 文書へのコメントの採決作業をプロジェクト個別会議にて行いました。また WG4 総会では、同標準の新しいパートの WD 文書作成および、既存標準の改訂に関する CD 文書の作成が引き続き行われる旨が決定されました。

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・問い合わせの受付、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、前期に引き続き 4 月は 4 万件を超えたものの、5 月、6 月は 3 万件台となりました。（[図 5-1]）報告件数の減少は、中国から大量に配信されるフィッシングメール数が減っていることが原因と考えられますが、5 月の長期休暇（労働節 5/1~5/5）などが影響している可能性もあり、この減少傾向が続くのかどうかは注視が必要です。



［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 をかたるフィッシングの報告数が、前四半期と比較して減少したものの引き続き多く、全体の約 45.3%を占めています。次いで、楽天、三井住友カード、MICARD、三菱 UFJ ニコスをかたるフィッシングの報告が多く、この 5 ブランドに関連する報告が全体の約 74.6%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 24 件（ニュース：0 件、緊急情報：24 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。

- bitFlyer をかたるフィッシング：1 件
- ビューカードをかたるフィッシング：1 件
- 東京電力をかたるフィッシング：1 件
- ほくせんカードをかたるフィッシング：1 件
- bitbank をかたるフィッシング：1 件
- JP BANK カードをかたるフィッシング：1 件
- au をかたるフィッシング：1 件
- 三井住友トラストクラブをかたるフィッシング：1 件
- 鹿児島銀行をかたるフィッシング：1 件

- ETC 利用照会サービスをかたるフィッシング：1 件
- OC カード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
- イオンカードをかたるフィッシング：1 件
- ファミマ T カード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
- NTT ドコモをかたるフィッシング：1 件
- Evernote をかたるフィッシング：1 件
- セディナ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
- ビックカメラ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
- エムアイカードをかたるフィッシング：1 件
- りそなカード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
- Spotify をかたるフィッシング：1 件
- ゆめカードをかたるフィッシング：1 件
- PayPay 銀行をかたるフィッシング：1 件

本四半期は、前期に引き続きクレジットカードブランドをかたるフィッシングの報告が多く（34 ブランド）寄せられました。しばらく、あるいは、これまでまったく報告がなかったカードブランドをかたるフィッシングの報告も受領しています（[図 5-2]）。これらカードブランドをかたるフィッシングの特徴として、メール文面が共通しており、ブランド名（社名）の部分を変えて送られるケースが多く、またそのほとんどが差出人も正規のメールアドレス （ドメイン） を使用した「なりすまし」メールであることを確認しています。

また、スミッシング（ショートメッセージサービス（SMS）を使用したフィッシング）の報告も続いています。宅配便の不在通知を装うものに加えて、Amazon やドコモ、クレジットカードブランドをかたるショートメッセージのフィッシングも報告されています。

フィッシング以外では、ビットコインを要求する脅迫メール（セクストーションメール）の報告が多数、寄せらせました。

［図 5-2：クレジットカードブランドをかたるフィッシングサイトの例 ］

https://www.antiphishing.jp/news/alert/micard_20210615.html

［図 5-3：スミッシング（ショートメッセージ）の例 ］

https://www.antiphishing.jp/news/alert/nttdocomo_20210527.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/

2021 年 4 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/202104.html

2021 年 5 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/202105.html

2021 年 6 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/202106.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など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 47 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

2020 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 2021 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 2021」を 2021 年 6 月 1 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 ページを参照ください。

フィッシング対策ガイドライン 2021 年度版
https://www.antiphishing.jp/report/guideline/antiphishing_guideline2021.html

利用者向けフィッシング詐欺対策ガイドライン 2021 年度版
https://www.antiphishing.jp/report/guideline/consumer_guideline2021.html

フィッシングレポート 2021
https://www.antiphishing.jp/report/wg/phishing_report2021.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 86 回運営委員会
  2021 年 4 月 7 日（水）15:30-18:00

- 第 87 回運営委員会
  2021 年 4 月 22 日（木）15:30-18:00

- 第 88 回運営委員会
  2021 年 5 月 26 日（水）9:30-12:00

- 第 89 回運営委員会
  2021 年 6 月 24 日（木）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。

- 第 2 回フィッシング対策勉強会（オンライン）
  日時：2021 年 4 月 8 日（金）13:00 - 15:00

- 2021 年度総会（オンライン）
  日時：2021 年 6 月 11 日（金）13:00 - 15:00

※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等の成果物の公開支援

本四半期においては、次のようなワーキンググループ等の成果物の公開を支援しました。

証明書普及促進 WG

- Google Chrome における混在コンテンツのブロック（2021/04/01）
  https://www.antiphishing.jp/news/info/Chrome_MixedContents_20210401.html

7. 公開資料

本章では JPCERT/CC が本四半期に公開した調査・研究の報告書や論文、セミナー資料を一覧にまとめています。

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の受付、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。そうした活動の概要を紹介するために、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て、邦文および英文のレポートとして公表しています。

2021-04-15
JPCERT/CC インシデント報告対応レポート［2021 年 1 月 1 日～2021 年 3 月 31 日］
https://www.jpcert.or.jp/pr/2021/IR_Report20210415.pdf

2021-06-25
JPCERT/CC Incident Handling Report [January 1 , 2021 - March 31, 2021]
https://www.jpcert.or.jp/english/doc/IR_Report2020Q4_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。こうしたインターネット定点観測の結果を四半期ごとにまとめて邦文および英文のレポートとして公表しています。

2021-04-20
JPCERT/CC インターネット定点観測レポート［2021 年 1 月 1 日～2021 年 3 月 31 日］
https://www.jpcert.or.jp/tsubame/report/report202101-03.html
https://www.jpcert.or.jp/tsubame/report/TSUBAMEReport2020Q4.pdf

2021-06-25
JPCERT/CC Internet Threat Monitoring Report [January 1, 2021 - March 31, 2021]
https://www.jpcert.or.jp/english/doc/TSUBAMEReport2020Q4_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。この制度の運用に関連した前四半期の活動実績と、同期間中に公表された脆弱性に関する注目すべき動向をまとめてレポートとして公表しています。

2021-04-22
ソフトウェア等の脆弱性関連情報に関する届出状況［2021 年第 1 四半期（1 月～3 月）］
https://www.jpcert.or.jp/pr/2021/vulnREPORT_2021q1.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 10 件の記事を公表しました。

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

2021-05-18	Locked Shields 2021 参加記
2021-05-20	仮想通貨マイニングツールの設置を狙った攻撃
2021-06-01	ラッキービジター詐欺で使用される PHP マルウェア
2021-06-24	JPCERT/CC 感謝状 2021～コロナ禍におけるご尽力に感謝を込めて～
2021-06-30	CSIRT 研修レポ：ベトナム VNCERT/CC 編

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

2021-04-01　ICS Security Conference 2021

2021-05-18　JPCERT/CC participated in the Locked Shields 2021
2021-05-27　Attacks Embedding XMRig on Compromised Servers
2021-06-04　PHP Malware Used in Lucky Visitor ScamNEW
2021-06-30　CSIRT Training to VNCERT/CC with JICA

8. 主な講演活動

(1) 佐々木 勇人（早期警戒グループマネージャー）：
「最近のサイバー攻撃動向とインシデント対応のポイントについて～2020 年度の JPCERT/CC の活動から～」
宮城県サイバーセキュリティ協議会総会（主催：宮城県サイバーセキュリティ協議会、開催日：2021 年 5 月 14 日）

(2) 洞田 慎一（早期警戒グループ担当部門長）：
「リモート環境下でのインシデント対応への課題」
第 25 回 サイバー犯罪に関する白浜シンポジウム（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：2021 年 5 月 21 日）

(3) 輿石 隆（早期警戒グループ 脅威アナリスト）：
「ゲーム演習で学ぶ CSIRT のうごき」
日本青年会議所主催クロストークイベント（主催：日本青年会議所、開催日：2021 年 5 月 28 日）

(4) 石井 泰鷹（早期警戒グループ 脆弱性アナリスト）：
「サイバー攻撃の脅威に対する認識が高まるクロストーク」
日本青年会議所主催クロストークイベント（主催：日本青年会議所、開催日：2021 年 5 月 28 日）

(5) 小島 和浩（早期警戒グループ 脅威アナリスト）：
「Analyzing and Sharing information about threats and vulnerabilities」
東大公共政策大学院講義（主催：東京大学公共政策大学院、開催日：2021 年 6 月 1 日）

(6) 佐々木 勇人（早期警戒グループマネージャー）：
「クラウドサービスのインシデント対応をめぐる「モヤモヤ」～JPCERT/CC のインシデント対応事例より～」
Cloud Operators Day2021（主催：Cloud Operator Days Tokyo 2021 実行委員会、Cloud Native Telecom Operator Meetup 実行委員会、開催日：2021 年 6 月 30 日）

9. 協力、後援

本四半期は次の行事開催に協力または後援等を行いました。

(1) Interop Tokyo 2021
主　催：Interop Tokyo 実行委員会
開催日：2021 年 4 月 14 日（水）～16 日（金）

(2) 第 25 回 サイバー犯罪に関する白浜シンポジウム
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：2021 年 5 月 20 日（木）、21 日（金）

(3) セキュリティフォーラム 2021 オンライン
共　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：2021 年 6 月 9 日（水）

■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