JPCERT Coordination Center

JPCERT/CC 活動四半期レポート

2021 年 10 月 1 日 ～ 2021 年 12 月 31 日

一般社団法人 **JPCERT** コーディネーションセンター

2022 年 **1** 月 **20** 日

活動概要トピックス

ートピック1ー　JPCERT/CC Eyes「サイバー政策動向を知ろう Watch! Cyber World vol.1」を公開

JPCERT/CC は、サイバーセキュリティ政策に関する政府機関や国際機関、企業などのニュースを収集及び分析して、諸外国の動向を調査しています。この度、サイバーセキュリティ政策への関心を喚起することを目的に JPCERT/CC 公式ブログ JPCERT/CC Eyes にて、国連や諸外国の政策を解説する連載記事を開始しました。初号では、2021 年 7 月から 12 月までの約 6 カ月間の出来事で特に重要であると判断した、サイバー空間での課題に関する国連総会での議論と米国務省におけるサイバー関連部局の設置計画の 2 つの話題を取り上げました。

JPCERT/CC Eyes: サイバー政策動向を知ろう Watch! Cyber World vol.1
https://blogs.jpcert.or.jp/ja/2021/12/cyberworld1.html

政策面に馴染みの薄い方にも読みやすいように、この分野に詳しい犬のモチチローと好奇心旺盛な猫のマーシーという当連載オリジナルキャラクター間の会話の形式をとることにより、政府機関や国際機関、企業などの取り組みを易しい言葉で解説しています。また、セキュリティや脆弱性の情報には慣れ親しんでいても、サイバーセキュリティ政策の情報を日頃から積極的に収集してはいない読者を想定して、一次情報をすぐに確認できるよう、関連する Web ページへのリンクも添付しています。次号以降も引き続き当該分野に興味を抱いていただけるきっかけとなるような記事を配信していく予定です。

ートピック2ー　インシデント報告または脆弱性報告で顕著な貢献をいただいた方を顕彰するための賞（「ベストレポーター賞」）を制定し、初の贈呈を実施

インシデントや脆弱性といったサイバーセキュリティに関する問題をいち早く発見し正確な情報を提供いただける報告者（レポーター）の皆さまの活動は、JPCERT/CC がサイバーセキュリティにおける問題を解決する一連の活動を進めるために無くてはならないものです。またインシデントや脆弱性の数が増加し、また問題が複雑化し高度化している現状においては、レポーターの皆さまの協力を得てより多くの問題を迅速に解決していくことの重要性がさらに増してきています。このような状況を踏まえ JPCERT/CC では、日々情報を提供いただいている報告者の皆さまのお力添えに感謝の意をお伝えするとともに、その中でも特に優れた事例を広く世に知っていただく機会になればと考え、「ベストレポーター賞」を本年度から贈呈させていただくことにしました。

ベストレポーター賞は、インシデント報告と脆弱性報告のそれぞれの部門において、情報提供を通じて JPCERT/CC の活動に顕著な貢献をいただいた方に年 1 回、感謝の意を表し記念品を贈らせていただくものです。なお、インシデント報告部門ではインシデント報告の件数とその内容に基づいて、脆弱性報

告部門では JPCERT/CC や JVN に相談・報告をいただいた脆弱性情報の件数とその内容に基づいて、それぞれ受賞者を選定することにしています。
初回となる本年度は次の方々にベストレポーター賞をお贈りしました。

笹田 修平様（インシデント報告部門）
トレンドマイクロ株式会社　様（脆弱性報告部門）

笹田 修平様は、プライベートの活動を通じて、主として改ざんサイトやフィッシングサイトに関連する数多くのインシデントを報告していただきました。

トレンドマイクロ株式会社様は、製品開発者としての脆弱性対応の取り組みとして、社内外で発見された自社製品の脆弱性について報告を多数いただきました。なおトレンドマイクロ株式会社様への賞の贈呈に関する詳細と、自社製品の脆弱性届出についての JPCERT/CC の考えについては JPCERT/CC 公式ブログ JPCERT/CC Eyes で解説しています。

受賞者の皆さまをはじめ JPCERT/CC の活動に協力していただいている多くのレポーターの方々に改めて感謝申し上げます

JPCERT/CC ベストレポーター賞 2021
https://www.jpcert.or.jp/award/best-reporter-award/2021.html

JPCERT/CC Eyes 「2021 年度 ベストレポーター賞（脆弱性部門）をトレンドマイクロ株式会社に贈呈」
https://blogs.jpcert.or.jp/ja/2021/12/best-reporter-award-2021.html

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. 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 11,870 件、インシデント件数ベースでは 9,807 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 6,554 件でした。前四半期の 4,714 件と比較して 39%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/2022/IR_Report2021Q3.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 7,125 件で、前四半期の 6,311 件から 13%増加しました。また、前年度同期（5,015 件）との比較では、42%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	10 月	11 月	12 月	本四半期合計（割合）
国内ブランド	1,395	1,203	1,364	3,962（56%）
国外ブランド	732	839	835	2,406（34%）
ブランド不明 (注 5)	204	336	217	757（11%）
全ブランド合計	2,331	2,378	2,416	7,125

（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、ETC の利用照会サービスや EC サイトの会員用ログインページを装ったものが増加しています。それぞれ、前四半期と比較して ETC の利用照会サービスのフィッシングサイトが 6 倍、EC サイトを装ったものが 10 倍と大幅な件数の伸びがみられました。

他方、国外ブランドのフィッシングサイトは、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おり、報告件数上位ブランドの顔ぶれには変化がありませんでした。

フィッシングサイトテイクダウンのために調整したサイトの割合は、国内が 23%、国外が 77%であり、前四半期（国内が 23%、国外が 77%）と割合は同じでした。

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、906 件でした。前四半期の 579 件から 56%増加しています。

本四半期も、改ざんされた Web サイトから、不審な Web サイトへ転送される事例が複数報告されました。改ざんされた Web サイトにアクセスすると、［図 1-1］のような Location ヘッダーが挿入された、レスポンスが返り、それにより不審なサイトへリダイレクトされます。なお、このリダイレクトは、アクセス時の UserAgent が、iOS の Safari ブラウザーである場合のみ行われます。

```
Content-Length: 0
 X-Powered-By: PHP/7.4.12
 Server: Apache
 Connection: keep-alive
 Location: [redacted]
 Date: Thu, 02 Dec 2021 07:17:23 GMT
 Content-Type: text/html; charset=UTF-8
```

［図 1-1：不正な Location ヘッダーの例］

また，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前四半期から引き続き寄せられています。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

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、1 件でした。
次に、確認されたインシデントを紹介します。

(1) 「AppleJeus」と呼ばれる攻撃キャンペーンに関連する攻撃

本四半期は、AppleJeus と呼ばれる攻撃キャンペーンに関連する標的型攻撃の報告が寄せられました。この攻撃では、標的組織の社員に対して LinkedIn 経由でコンタクトし、マルウェアが埋め込まれたインストーラーを実行するように誘導するものです。インストーラーを実行した場合、UnionCrypto と呼ばれるマルウェアに感染します。

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：20 件（うち更新情報が 10 件）　https://www.jpcert.or.jp/at/

2021-10-01　SonicWall 製の SMA100 シリーズの脆弱性（CVE-2021-20034）に関する注意喚起（公開）
2021-10-06　Apache HTTP Server のパストラバーサルの脆弱性（CVE-2021-41773）に関する注意喚起（公開）
2021-10-08　Apache HTTP Server のパストラバーサルの脆弱性（CVE-2021-41773）に関する注意喚起（更新）
2021-10-13　Adobe Acrobat および Reader の脆弱性（APSB21-104）に関する注意喚起（公開）
2021-10-13　2021 年 10 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）
2021-10-20　2021 年 10 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）
2021-10-20　Movable Type の XMLRPC API における脆弱性（CVE-2021-20837）に関する注意喚起（公開）
2021-11-05　Movable Type の XMLRPC API における脆弱性（CVE-2021-20837）に関する注意喚起（更新）
2021-11-09　Movable Type の XMLRPC API における脆弱性（CVE-2021-20837）に関する注意喚起（更新）
2021-11-10　2021 年 11 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）
2021-11-16　Web メールサービスのアカウントを標的としたフィッシングに関する注意喚起（公開）
2021-11-25　Movable Type の XMLRPC API における脆弱性（CVE-2021-20837）に関する注意喚起（更新）
2021-12-11　Apache Log4j の任意のコード実行の脆弱性（CVE-2021-44228）に関する注意喚起（公開）
2021-12-13　Apache Log4j の任意のコード実行の脆弱性（CVE-2021-44228）に関する注意喚起（更新)
2021-12-15　2021 年 12 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）
2021-12-15　Apache Log4j の任意のコード実行の脆弱性（CVE-2021-44228）に関する注意喚起（更新）

2021-12-16　Movable Type の XMLRPC API における脆弱性（CVE-2021-20837）に関する注意喚起（更新）
2021-12-17　Movable Type の XMLRPC API における脆弱性（CVE-2021-20837）に関する注意喚起（更新）
2021-12-20　Apache Log4j の任意のコード実行の脆弱性（CVE-2021-44228）に関する注意喚起（更新）
2021-12-28　Apache Log4j の任意のコード実行の脆弱性（CVE-2021-44228）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：12 件　https://www.jpcert.or.jp/wr/

Weekly Report で扱った情報セキュリティ関連情報の項目数は、合計 86 件、「今週のひとくちメモ」のコーナーで紹介した情報は、次の 12 件でした。

2021-10-06　総務省が「クラウドサービス提供における情報セキュリティ対策ガイドライン（第 3 版）」（案）に対する意見募集の結果および「クラウドサービス提供における情報セキュリティ対策ガイドライン（第 3 版）」の公開
2021-10-13　NOTICE の取組改善に向けた調査協力のお願いについて
2021-10-20　内閣サイバーセキュリティセンター（NISC）がランサムウェア特設ページ「ストップ！ランサムウェア」を公開
2021-10-27　JPCERT/CC が「2021 年 7 月から 9 月を振り返って」を公開
2021-11-04　「TRANSITS Workshop Online 2022 Winter」開催のお知らせ
2021-11-10　経済産業省および ICSCoE が「インド太平洋地域向け日米 EU 産業制御システムサイバーセキュリティウィーク」を実施
2021-11-17　JNSA が「オンライン身元確認(eKYC)金融事例調査報告書」を公開
2021-11-25　フィッシング対策協議会が「フィッシング対策セミナー2021 講演資料」を公開
2021-12-01　JPCERT/CC ベストレポーター賞 2021
2021-12-08　JPCERT/CC CSIRT マテリアルを更新
2021-12-15　制御システムセキュリティカンファレンス 2022 参加登録開始のお知らせ
2021-12-22　JPCERT/CC が「Apache Log4j2 の RCE 脆弱性（CVE-2021-44228）を狙う攻撃観測」を公開

1.2.1.3. 早期警戒情報

JPCERT/CC は、重要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 3 件）　https://www.jpcert.or.jp/newsflash/

2021-10-12　Apple 製品のアップデートについて（2021 年 10 月）
2021-10-13　Intel 製品に関する複数の脆弱性について
2021-10-15　複数のアドビ製品のアップデートについて
2021-10-18　2021 年 7 月から 9 月を振り返って
2021-10-27　Apple 製品のアップデートについて（2021 年 10 月）（更新）
2021-10-28　Apple 製品のアップデートについて（2021 年 10 月）（更新）
2021-10-28　複数のアドビ製品のアップデートについて
2021-11-10　複数のアドビ製品のアップデートについて
2021-11-10　Intel 製品に関する複数の脆弱性について
2021-11-12　Palo Alto Networks PAN-OS GlobalProtect ポータルおよびゲートウェイのメモリ破損の脆弱性（CVE-2021-3064）について
2021-12-14　Apple 製品のアップデートについて（2021 年 12 月）
2021-12-15　複数のアドビ製品のアップデートについて
2021-12-16　Apple 製品のアップデートについて（2021 年 12 月）（更新）
2021-12-23　2021 年 10 月から 12 月を振り返って
2021-12-24　2021 年 12 月に公表された Log4j の脆弱性について

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) Web メールサービスのアカウント情報を詐取しようとするフィッシングに関する情報発信

2021 年 6 月以降、Web メールサービスのアカウント情報の詐取を目的としたフィッシングに関する JPCERT/CC への報告が増加しました。11 月に入ってもその傾向が継続しており、JPCERT/CC は 11 月 16 日に注意喚起を公開しました。

本フィッシングキャンペーンでは、Web メールサービスのメンテナンスやお知らせなどをかたったメールが確認されており、メール本文中のリンクを開くと、Web メールサービスのログイン画面になりすました偽サイトに誘導されます。そのサイトでメールアドレスとパスワードなどを入力すると、攻撃者にアカウント情報が詐取されます。また、詐取された情報を使って乗っ取られたアカウントは、別のフィッシングメールを送るための踏み台として攻撃者に悪用されます。こうした状況から、被害の拡大を防ぐために本注意喚起を発行し、攻撃手法やアカウント情報を詐取された場合の影響を解説するとともに、被害を未然に防ぐ対策や、被害を受けてしまった場合の事後対応を紹介しています。

Web メールサービスのアカウントを標的としたフィッシングに関する注意喚起
https://www.jpcert.or.jp/at/2021/at210049.html

(2) Movable Type の XMLRPC API における脆弱性（CVE-2021-20837）に関する情報発信

2021 年 10 月 20 日、シックス・アパート株式会社から、Movable Type の XMLRPC API における OS コマンドインジェクションの脆弱性（CVE-2021-20837）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、遠隔の第三者が Movable Type で作られたコンテンツを搭載した Web サーバー上で任意の OS コマンドを実行する可能性があるため、JPCERT/CC は同日に注意喚起を公開しました。その後、JPCERT/CC では、10 月 26 日に本脆弱性を実証するコード（PoC）が公開されていることを確認しました。また、株式会社ラックによれば、10 月 27 日から本脆弱性をもつ環境を探索する通信が観測されるようになり、さらに 11 月 1 日には脆弱な環境に不審なファイルを配置することを目的とした通信が観測され、実際にファイルが配置される事例も見つかりました。こうした状況から、JPCERT/CC は 11 月 5 日に注意喚起を更新し、速やかに対策を適用するよう改めて呼び掛けました。2021 年 11 月 9 日、Movable Type をベースに開発された製品である PowerCMS の脆弱性（CVE-2021-20850）も公表されたため、こちらについても対策の適用を呼びかけました。

Movable Type の XMLRPC API における脆弱性（CVE-2021-20837）に関する注意喚起
https://www.jpcert.or.jp/at/2021/at210047.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 —

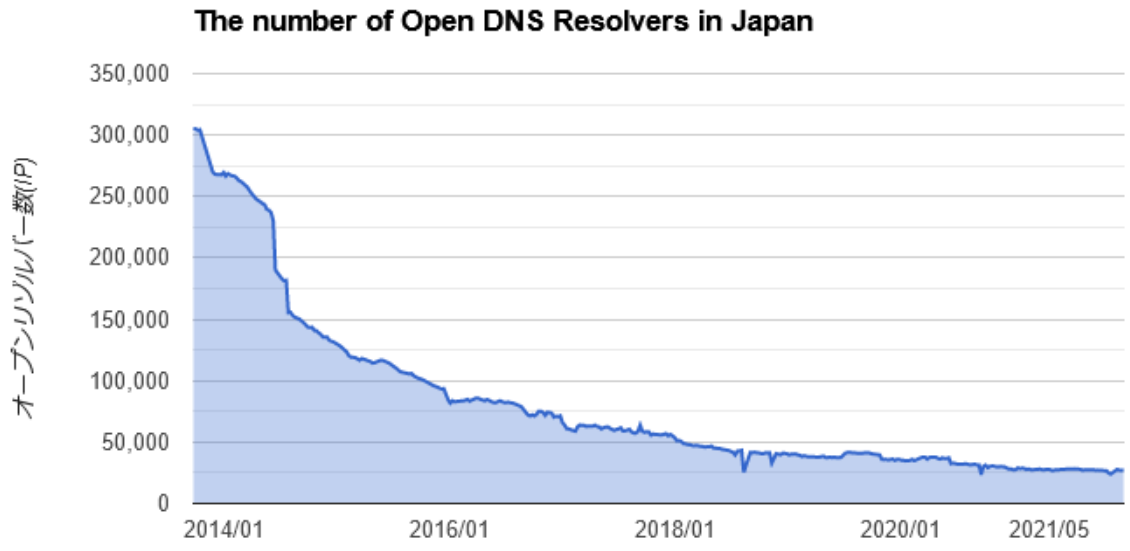
インターネットリスク可視化サービス Mejiro では、次のポートがインターネットに対して開いているノードを DoS リフレクション攻撃（DRDoS）に悪用される恐れのあるインターネット上のリスク要因と見なし、国や地域ごとにその分布状況を分析しています。

・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. オープンリゾルバー確認サイト

オープンリゾルバーとは、外部の不特定の IP アドレスからの再帰的な問い合わせを許可している DNS サーバーのことです。オープンリゾルバーの出現は、DNS サーバーのアクセス元制限不備や、ネットワーク機器やルーターにて管理者が気付かずに DNS 機能を有効にしてしまっていることなど、複数の原因が考えられます。世界的にも依然として このオープンリゾルバーを使って行う、Distributed Reflection Denial of Service （DRDoS） 攻撃がみられます。世界中に約 200 万ノードのオープンリゾルバーが存在しています。国内にも多数のオープンリゾルバーが存在しており、DRDoS に利用されていたとの報告を JPCERT/CC でも受け取ったことがあります。インターネットユーザー自らがオープンリゾルバーであるか否かを確認できるように、2013 年にオープンリゾルバー確認サイトを公開し、国内のインターネット利用者に対して、設定の確認を促しています。2013 年に確認を促し始めて以降、国内では徐々に減少してきており［図 1-2］、問題の改善が徐々に進んでいるものと考えられます。サイトサービス提供時から国内でのオープンリゾルバーのノード数は減少傾向であるものの、完全には無くなっていません。オープンリゾルバーの保有者には大きな被害がないので対策の動機づけが弱いのですが，踏み台にされて他者の攻撃に加担させられていることを説明するなどして、粘り強く対策を訴えていく必要があります。ユーザーの利便性を高め、より多くのインターネットユーザーが利用することを期待し、2021 年 12 月 14 日、オープンリゾルバー確認サイトに新しく 3 つの機能を追加しました。最近拡大している IPv6 の利用を踏まえ、接続元が IPv6 である場合に、IPv6 で表示を行う機能、複数の DNS サーバーが設定されている場合に、それぞれがオープンリゾルバーであるかの確認を行う機能、オープンリゾルバー確認サイト （コマンドライン版）での JSON 出力を行う機能を追加しました。
今後、Mejiro での国内のオープンリゾルバーに対する指標の状況や、オープンリゾルバー確認サイトからの知見を活かして、インターネットユーザーに向けて「オープンリゾルバー数０」を促していきたいと考えています。また、少しでも多くのインターネットユーザーにオープンリゾルバー確認サイトを利用していいただくとともに、オープンリゾルバーのリスクの周知に取り組んでいきたいと考えています。



［図 1-2：日本におけるオープンリゾルバーのノード数の変化］

参考文献

(1) オープンリゾルバー確認サイト
https://www.openresolver.jp/
(2) JPCERT/CC オープンリゾルバー確認サイト
https://www.jpcert.or.jp/magazine/security/openresolver.html
(3) 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/index.html

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

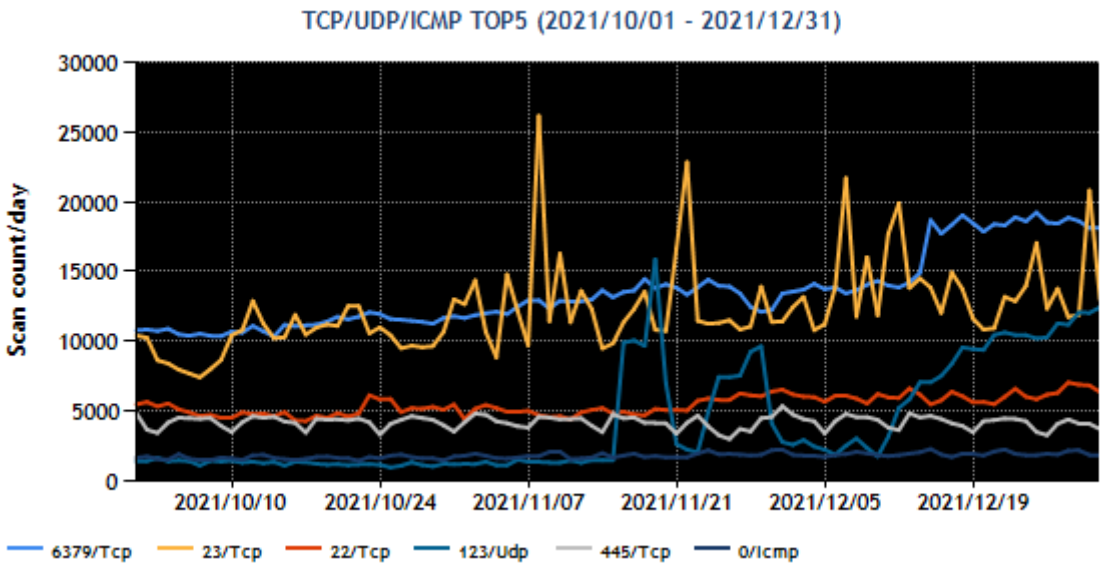
1.3.2.2. TSUBAME の観測データの活用

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 7 月から 9 月の期間に関するレポートを 2021 年 10 月 19 日に公開しました。またレポートに書き切れなかった内容を 2021 年 10 月 19 日にブログで公開しました。

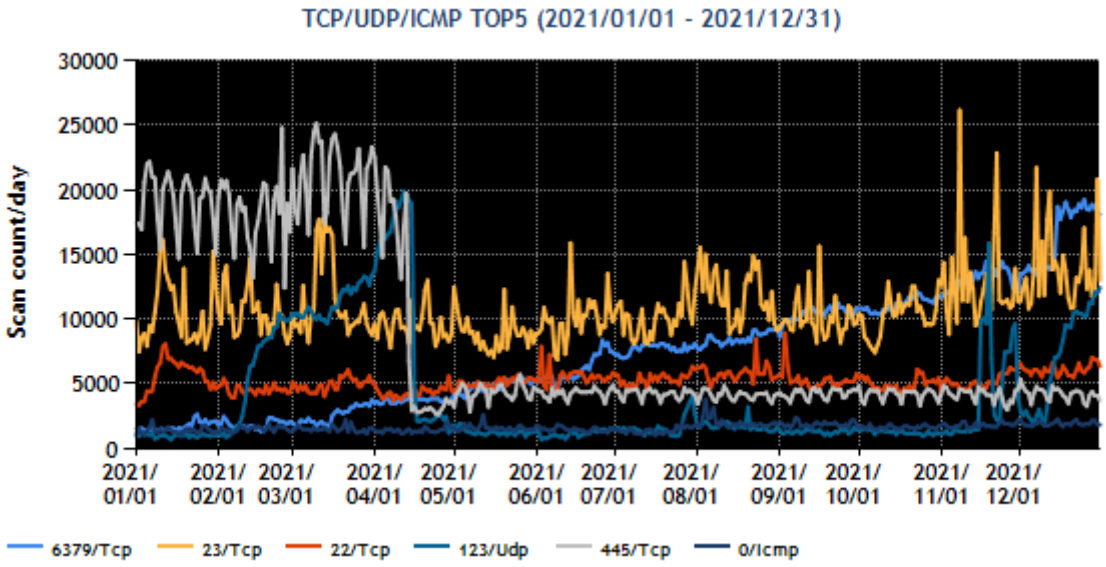
TSUBAME 観測グラフ
https://www.jpcert.or.jp/tsubame/index.html#examples
インターネット定点観測レポート（2021 年 7～9 月）
https://www.jpcert.or.jp/tsubame/report/report202107-09.html
TSUBAME レポート Overflow（2021 年 7～9 月）
https://blogs.jpcert.or.jp/ja/2021/10/tsubame_overflow_2021-07-09.html

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 位及び 6～10 位を［図 1-3］と［図 1-4］に示します。

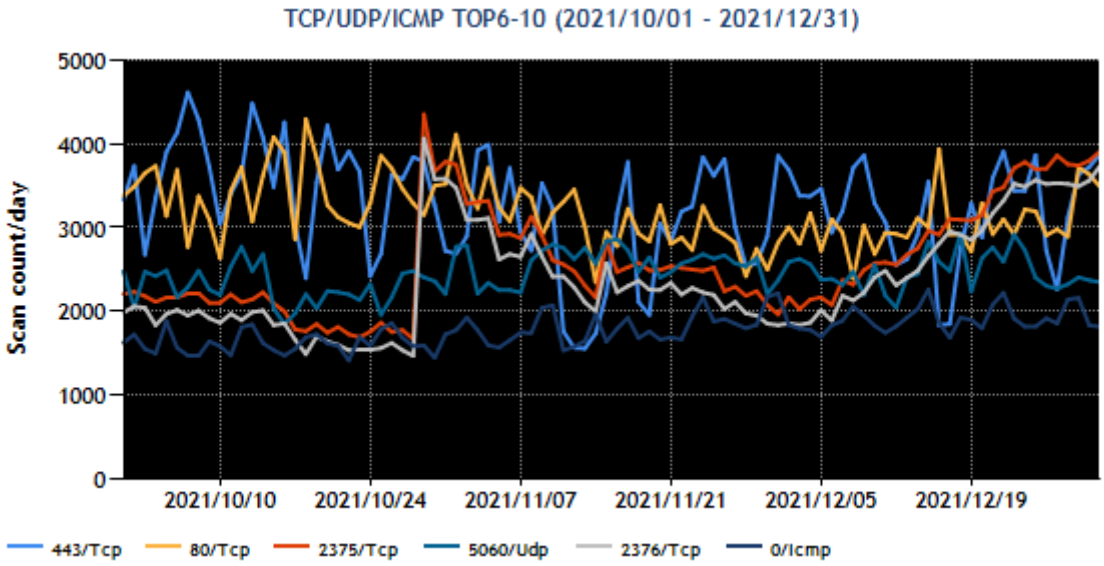


［図 1-3：宛先ポート別グラフ トップ 1-5（2021 年 10 月 1 日-12 月 31 日）］

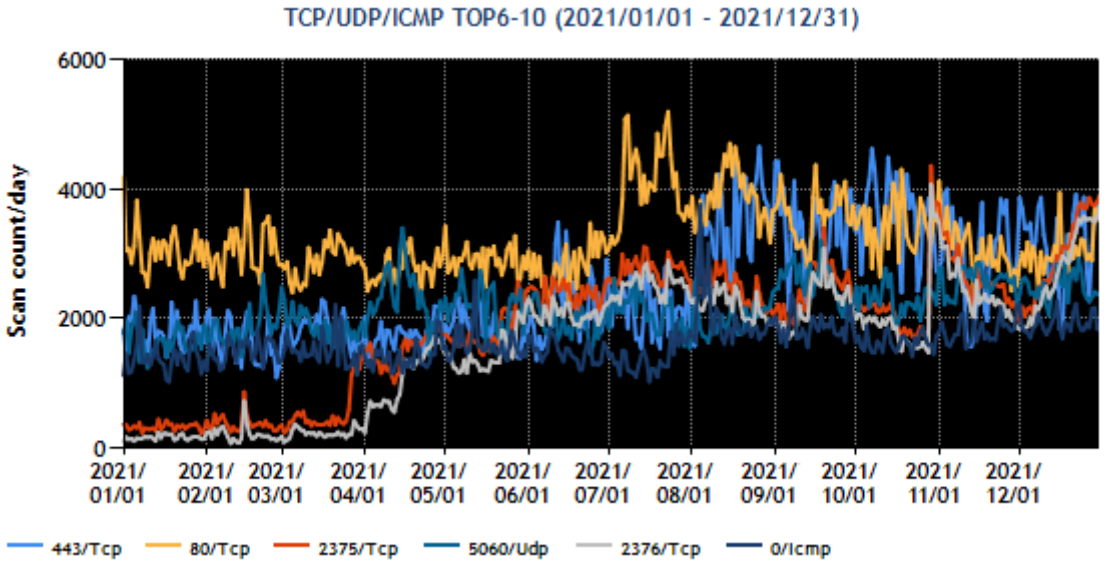


［図 1-4：宛先ポート別グラフ トップ 6-10（2021 年 10 月 1 日-12 月 31 日）］

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 位及び 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 1 月 1 日-12 月 31 日）］



［図 1-6：宛先ポート別グラフ トップ 6-10（2021 年 1 月 1 日-2021 年 12 月 31 日）］

本四半期に最も多く観測されたパケットは 6379/TCP（redis）宛の通信でした。それらの送信元の大半は中国に割り振られている IP アドレスであり、日本国内のものは数十件アドレスと少数でした。次いで多く観測されたパケットが 23/TCP（telnet）宛の通信です。また Docker が使用するポートへの通信（2375/TCP:9 番目、2376/TCP:10 番目）の推移にも注目しています。Redis と Docker 両方のポートに対してパケットを送ってきたホストが 3 割弱あることを確認しました。それ以外のポートに関しては特

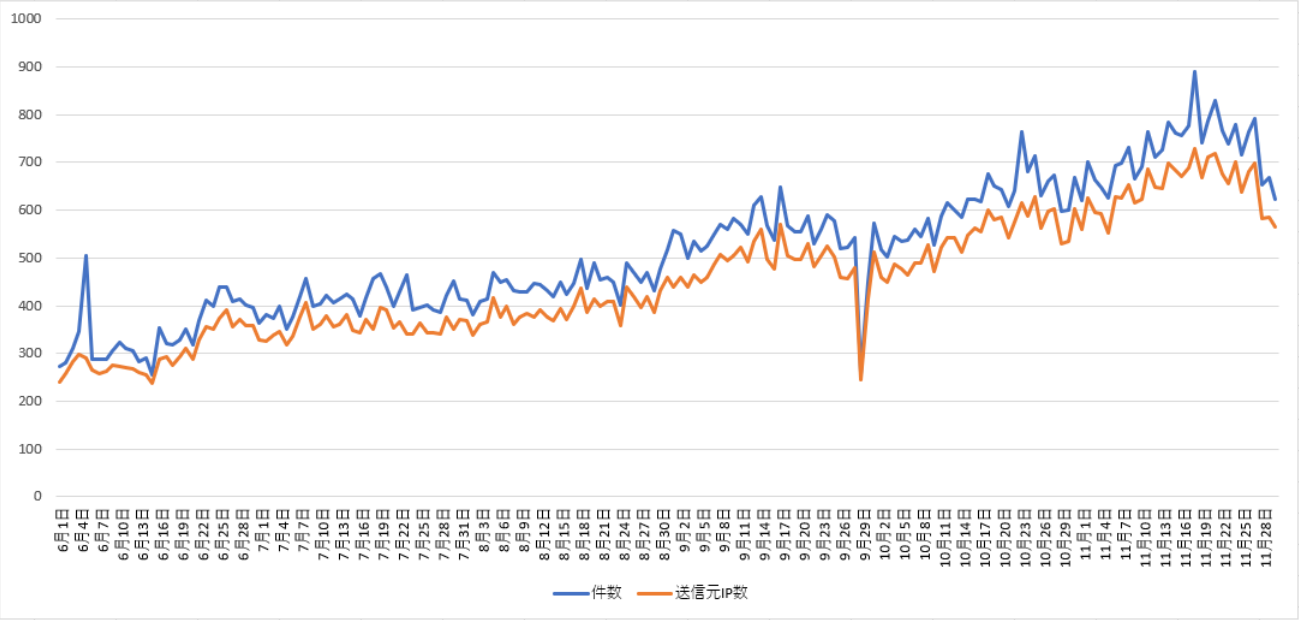
筆すべき変化はありませんでした。

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、スキャンに対する応答があった場合に行われる攻撃活動を捕捉したいとの考えから、低対話型ハニーポットを設置して攻撃者からの通信内容を収集しています。現在は、HTTP プロトコルとオープンソースのメモリ内データベース・システムである Redis が用いるプロトコル RESP（REdis Serialization Protocol）に応答するハニーポットを運用し、攻撃活動の通信を収集、分析しています。

(1) Redis に対する攻撃活動

前四半期に引き続き、今四半期においても低対話型ハニーポットにて 6379/TCP 宛の通信の増加が観測されています。



［図 1-7：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］

RESP に応答するハニーポットで収集した通信を分析した結果、観測した通信の送信元 IP アドレスの約 80%が、info（サーバーの情報を取得）や command（Redis コマンドの詳細を取得）といったスキャンを目的としたコマンドを送信していました。また、その他の送信元 IP アドレスからは、認証試行の通信や、Redis コマンドを用いてシステムに不正な cron を設定し、任意の OS コマンド実行やマルウェアのダウンロードを目的とした通信など、明らかに悪意のある攻撃もありました。

JPCERT/CC では、観測した通信のうち、数日間にわたりに攻撃を行う送信元ホスト及びマルウェアの配布元となっているホストに関して、テイクダウンに向けたコーディネーションを実施しました。

(2) Movable Type の XMLRPC API における脆弱性（CVE-2021-20837）の悪用を試みる通信

2021 年 10 月 20 日に公開された Movable Type の XMLRPC API における OS コマンドインジェクションの脆弱性（CVE-2021-20837）を悪用する通信を、HTTP プロトコルに応答する低対話型ハニーポットで観測しました。

不正な PHP ファイルをネットワーク経由で取得させようとする通信が観測され、ダウンロードするファイル名は攻撃事例として公開されているファイル名と同じものでした。

JAIPA（日本インターネットプロバイダー協会）の協力を得て、クラウドサービスを提供する各事業者に上記の観測情報を共有し、各事業者における対応に役立てていただきました。

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及び対応状況

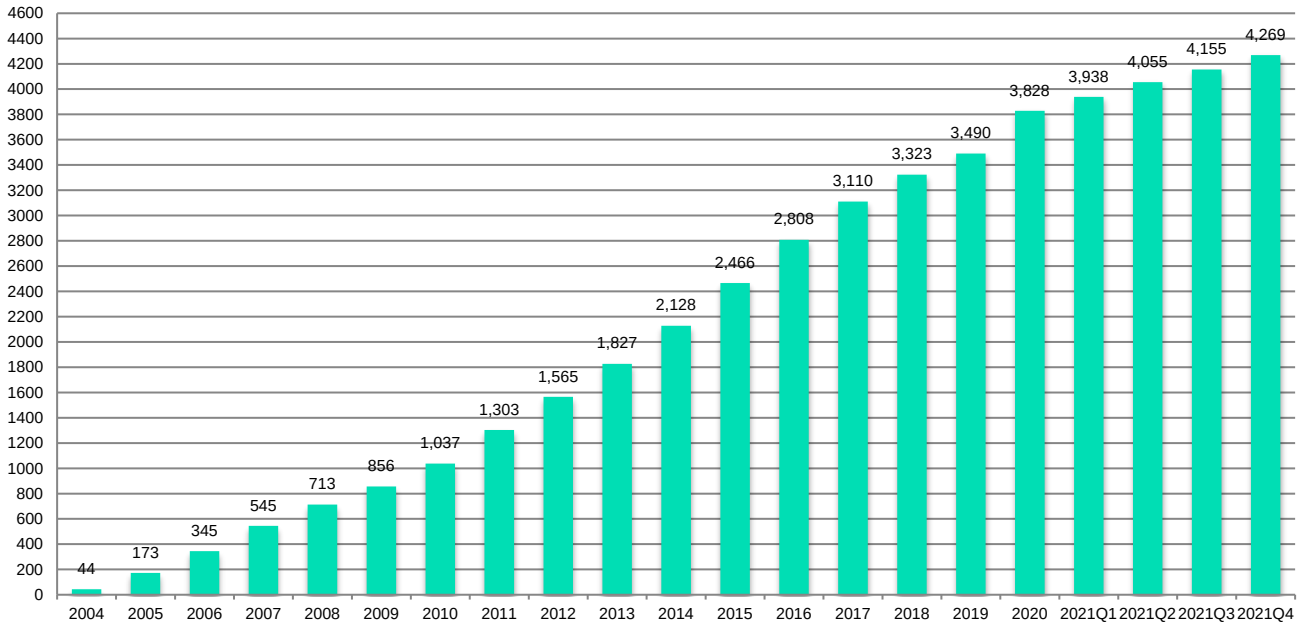
JVN で公表している脆弱性情報は、本規程に従って国内で届け出られた脆弱性に関するもの（以下、「国内取扱脆弱性情報」；「JVN#」に続く 8 桁の数字の形式の識別子［例えば、JVN#12345678 等］を付与し

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、海外の発見者から JPCERT/CC に直接届け出がなされた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 114 件（累計件 4,269）で、累計の推移は［図 2-1］に示すとおりです。本四半期に公表された個々の脆弱性情報に関しては、次の Web ページをご参照ください。

JVN（Japan Vulnerability Notes）
https://jvn.jp/



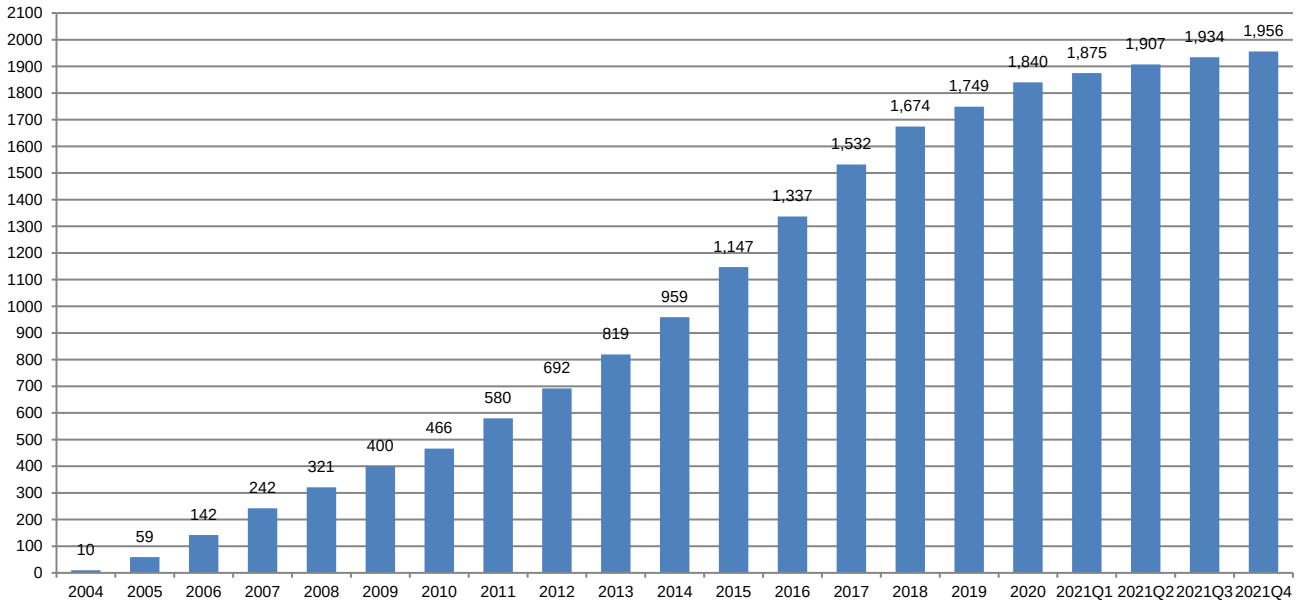
［図 2- 1：JVN 公表累積件数］

本四半期において公表に至った脆弱性情報のうち、国内取扱脆弱性情報は 22 件（累計 1,956 件）で、累計の推移は ［図 2-2］に示すとおりです。本四半期に公表した 22 件の内訳は、国内の単一の製品開発者の製品に影響を及ぼすものが 12 件（このうち自社製品の届け出によるものが 7 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、国内外の複数の製品開発者の製品に影響を及ぼすものが 1 件ありました。

本四半期に公表した脆弱性の影響を受けた製品のカテゴリーごとの内訳は、［表 2-1］のとおりです。本四半期は、CMS が 5 件と最も多く、次いで組込系製品とプラグインがそれぞれ 4 件、続いてサーバー製品が 3 件、Android アプリケーション、アンチウイルス製品、ウェブアプリケーション、開発支援、グループウェア、スマートフォンアプリケーションがそれぞれ 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
CMS	5
組込系製品	4
プラグイン	4
サーバー製品	3
Android アプリケーション	1
アンチウイルス製品	1
ウェブアプリケーション	1
開発支援	1
グループウェア	1
スマートフォンアプリケーション	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 92 件（累計 2,313 件）で、累計の推移は［図 2-3］に示すとおりです。92 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及び製品

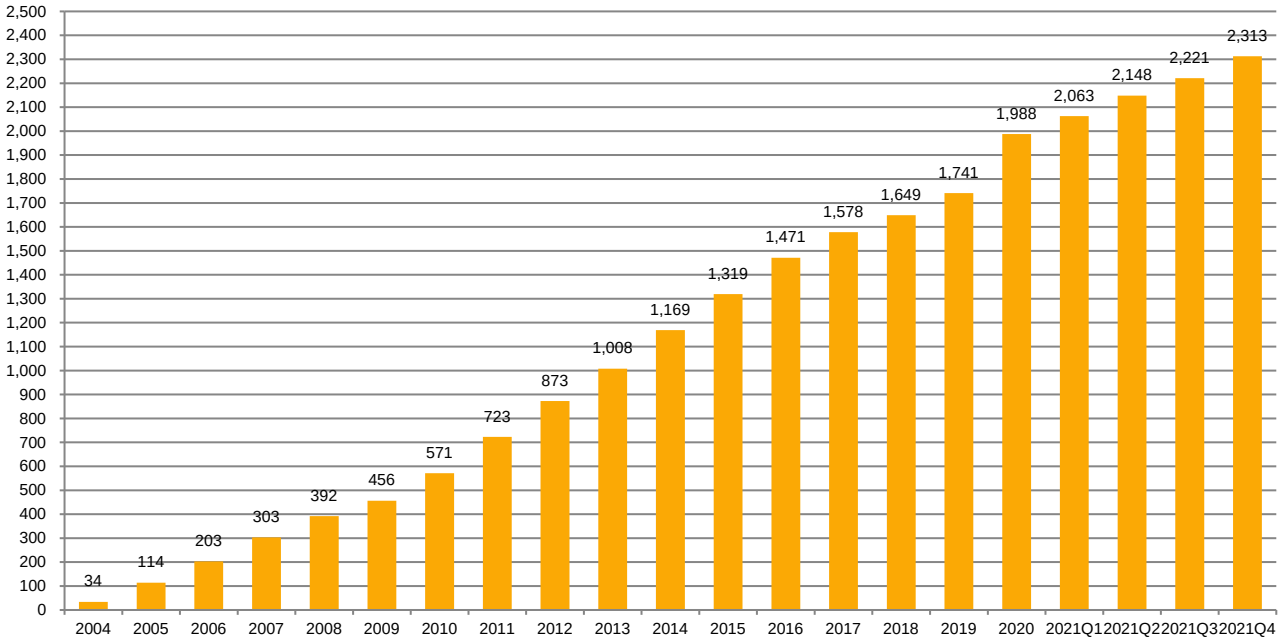
開発者による脆弱性情報公開の事前通知によるものは 22 件（このうち複数製品開発者の製品に影響を及ぼすものは 5 件）、国内外の発見者からの届け出によるものは 7 件、JPCERT/CC が注意喚起として発行したものは 63 件（このうち Technical Alert は 1 件）でした。

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 65 件と最も多く、次いで医療機器と組込系製品がそれぞれ 7 件、ライブラリが 3 件、アンチウイルス製品、開発支援、サーバー製品がそれぞれ 2 件、DNS、macOS アプリケーション、ウェブサーブレットコンテナ、認証ソフトウェアがそれぞれ 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。また、国内外の発見者からの届け出によるものも、本四半期においては比較的多くありました。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や、国内外の発見者から直接 JPCERT/CC に届け出られるもの等も含めて、脆弱性情報の流通、調整及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	65
医療機器	7
組込系製品	7
ライブラリ	3
アンチウイルス製品	2
開発支援	2
サーバー製品	2
DNS	1
macOS アプリケーション	1
ウェブサーブレットコンテナ	1
認証ソフトウェア	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及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。これまでに 2015 年度、2017 年度、2019 年度に公表判定委員会が開催され、そこでの審議を経て、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 及び 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及び対応状況の集約、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に 45 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、製品開発者を新しい CNA に招致する活動やトレーニングなどの活動も行っています。CNA 招致活動の結果として、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、パナソニック株式会社を新たに CNA として迎え、現在 5 社が、CNA として自社製品における脆弱性に対し CVE を採番しています。
CNA 及び 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/

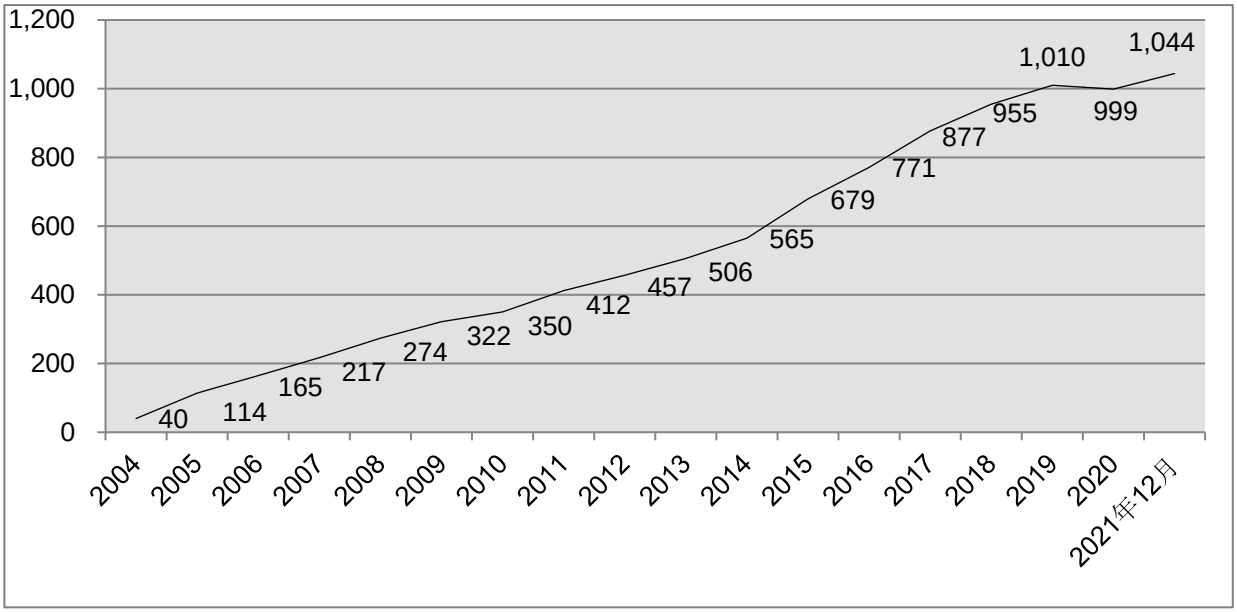
情報セキュリティ早期警戒パートナーシップガイドライン（2019 年版）
https://www.jpcert.or.jp/vh/partnership_guideline2019.pdf

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 12 月 31 日現在で 1,044 となっています。今四半期は製品開発者リストに登録されている製品開発者の活動状況等を精査し、廃業や活動終了等のため今後の脆弱性対応を期待できない製品開発者の登録を抹消しました。上記の登録数にはこの登録抹消に伴う減少分を反映しています。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のミーティングに変更しています。本四半期は 11 月 12 日に開催し、組み込み／制御システム開発におけるサプライチェーンを含む脆弱性情報流通の問題、CNA（CVE Numbering Authority）の活動状況、VINCE と呼ばれる情報連携ツールを使った国際的な製品開発者間の脆弱性情報連携などについて、参加者との意見交換を行いました。

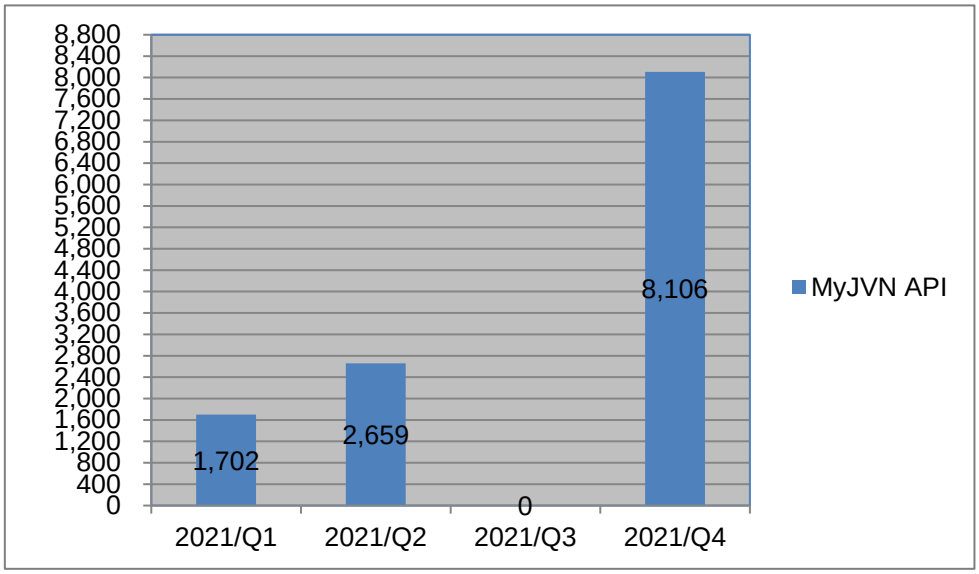
2.3. VRDA フィードによる脆弱性情報の配信

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

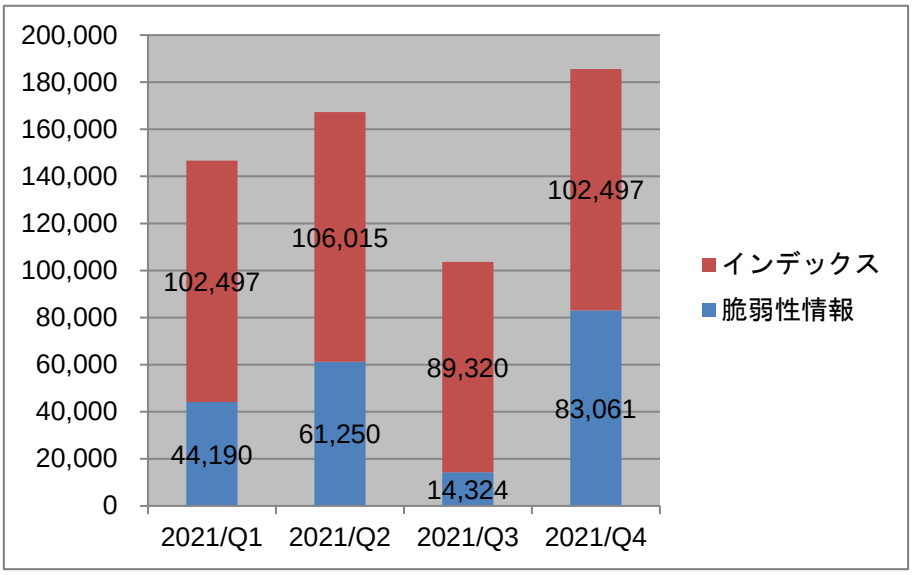
四半期ごとに配信した VRDA フィード配信件数を［図 2- 5］に、VRDA フィードの利用傾向を［図 2- 6］と［図 2- 7］に示します。［図 2- 6］では、VRDA フィードインデックス（Atom フィード）と、脆弱

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］

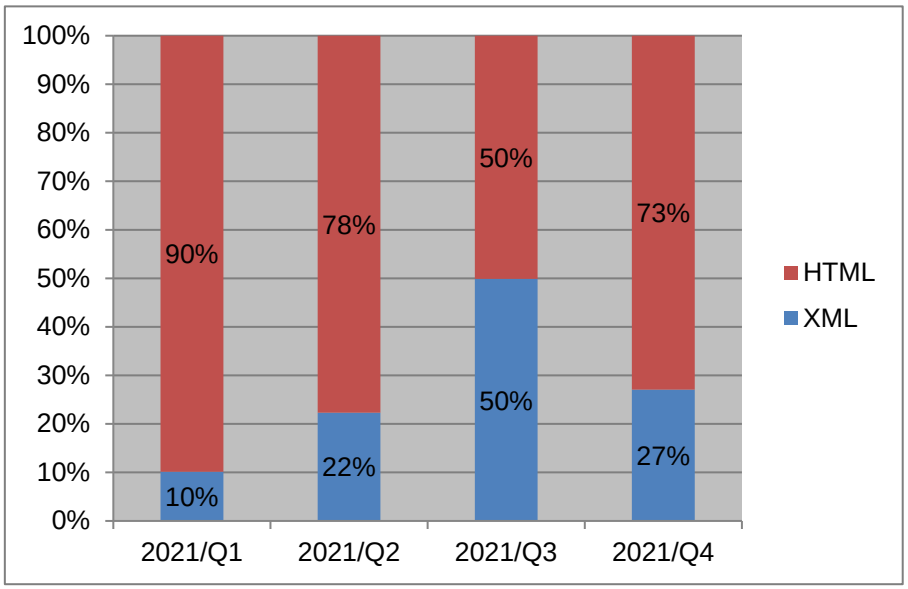
VRDA フィード配信件数については、［図 2- 5］に示したように前四半期は配信件数が 0 となっています。これは VRDA フィード配信用システムの障害により、期間中データ更新が停止していたことが原因です。障害期間中の未配信情報は、本四半期に配信しました。



［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 15%増加しまし

た。脆弱性情報の利用数については、約 580%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 23%減少しました。

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 316 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 2 件でした。

2021/11/01　MTS（Maritime Transportation System）のサイバーリスクに対処するための提言をまとめた報告書を米 Atlantic Council が公表
2021/11/01　電力業界の OT セキュリティを強化するための手法を米 DOE が公表

また、海外での事例や、標準化動向などを JPCERT/CC からのお知らせとともに、制御システムセキュリティ情報共有コミュニティー（注1）に登録いただいている関係者向けに月刊ニュースレターとして配信しています。

本四半期は 2 件を配信しました。

2021/10/11　制御システムセキュリティニュースレター 2021-0009
2021/11/10　制御システムセキュリティニュースレター 2021-0010

（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。JPCERT/CC では、制御システムセキュリティ情報共有コミュニティーに向けて、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 1,236 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

これら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 1 件でした。

2021/12/16　Apache Log4j の任意のコード実行の脆弱性の影響を受ける制御システム製品に関する注意喚起

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次の 1 件でした。

2021/11/25　JVNTA#94851885：Apache log4net における XML 外部実体参照（XXE）の脆弱性

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、悪用された場合の影響が大きいため、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) Apache log4net における XML 外部実体参照（XXE）の脆弱性

2021 年 10 月 26 日、CERT@VDE より、Pepperl+Fuchs 社製の複数 DTM 関連製品及び Visunet に XML 外部実体参照（XXE）の脆弱性に関する情報が公表されました。この脆弱性は 2017 年 9 月に発見された Microsoft .NET Framework 向けのオープンソースのロギングライブラリである Apache Log4net の XML 外部実体参照（XXE）の脆弱性に起因するものでした。同社から公表された脆弱性情報の中にはフィールド機器とオートメーションシステムの間でデータ交換を行うための標準規格である FDT 技術に沿って実装された製品があります。FDT2.0 では、Microsoft .NET Framework での実装が求められていることから、同社では FDT/DTM の実装において、ログ出力の仕組みに log4net を採用したものと考えられます。FDT 技術を採用する制御システムベンダーが多く、他の制御システムベンダーにおいても同様に Apache log4net を採用したソフトウェアを提供している可能性があります。

影響を受けるバージョンの log4net が組み込まれたアプリケーションでは、外部エンティティと同名のエンティティを定義した XML ファイルの文書型定義（DTD）を Log4net の設定ファイルとして読み込むと、外部エンティティを参照すべきであっても定義されたエンティティを参照してしまう問題が存在します。そのため、攻撃者によって細工された外部エンティティが定義されている XML ファイルを log4net の設定ファイルとして読み込まれると、攻撃者による任意のコードが当該アプリケーションと同じ権限で実行される可能性があります。また、SSRF（Server Side Request Forgery）攻撃に使用される可能性もあります。

JPCERT/CC では、本脆弱性に関する PoC コードが 2021 年 5 月に公開されていること、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ており、制御システム関連ソフトウェアの影響があることも鑑み、制御システムベンダーを含むソフトウェア開発者、改めての注意を喚起する目的で 11 月 25 日に JVN で本脆弱性情報を公表しました。

(2) Apache Log4j の任意のコード実行の脆弱性の影響を受ける制御システム製品に関する注意喚起

2021 年 12 月 11 日、JPCERT/CC では、「Apache Log4j の任意のコード実行の脆弱性（CVE-2021-44228）に関する注意喚起」を Web サイトにて公表し、2021 年 12 月 13 日に JVN にて脆弱性情報を公表いたしました。

Java ベースのオープンソースのロギングライブラリの Apache Log4j には、任意のコード実行の脆弱性があります。Apache Log4j が動作するサーバーにおいて、遠隔の第三者が本脆弱性を悪用する細工したデータを送信することで、任意のコードを実行される可能性があります。

JPCERT/CC では、本脆弱性の影響を受ける制御システム製品に関する情報が複数の制御システム製品ベンダーから公表されていることを確認し、12 月 16 日にメーリングリストや ConPaS を通じて制御システムユーザー等に向けて注意を喚起しました。

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 に関する利用申し込みはなく、直接配付件数の累計 287 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

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、多くの国際会議がオンラインで開催されました。

4.1. 海外 CSIRT 構築支援及び運用支援活動

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、研修会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. ベトナム向けマルウェア解析トレーニング

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、12 月 7 日から 10 日にかけてオンラインでトレーニングを実施しました。同国の情報セキュリティ庁 Authority of Information Security（AIS）や、National CSIRT である VNCERT/CC に所属する技術者など 20 名が参加しました。JPCERT/CC はマルウェア解析に必要な環境構築の手法や、静的及び動的な解析技術に関するハンズオンを交えた講義を行いました。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

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 の詳細及び 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、12 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。

4.2.2. 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

4.3. その他国際会議への参加

4.3.1. 第 9 回 日中韓 サイバーセキュリティインシデント対応年次会合の開催（10 月 13 日～14 日）

JPCERT/CC と CNCERT/CC、KrCERT/CC による「日中韓　サイバーセキュリティインシデント対応年次会合」が 10 月 13 日から 14 日にかけてオンラインで開催されました。
本会合では、前年の会合以降の日中韓に影響を及ぼす重大なサイバーセキュリティインシデントにおける 3 組織間の連携実績を振り返るとともに、対応した主要なインシデントや各種取り組み等をそれぞれの CSIRT が報告しました。特に、昨今被害が拡大しているランサムウェアによるインシデントや各組織の行った取り組みについて活発に意見を交わしました。

4.3.2. TWCERT 2021 台灣資安通報應變年會でのパネル登壇（11 月 3 日）

台湾の TWCERT/CC が主催する年次カンファレンスである「台灣資安通報應變年會」が 11 月 3 日オンラインで開催され、JPCERT/CC は国際 CSIRT 間連携をテーマとしたパネルに登壇しました。CERT-In（インド）、ThaiCERT（タイ）の担当者とともに、各国の CERT の運営の形態やインシデントの動向などについて意見を述べました。イベントの詳細については、次の Web ページをご参照ください。

TWCERT 2021 台灣資安通報應變年會
https://www.informationsecurity.com.tw/seminar/2021twcert/

4.3.3. HITCON2021 参加（11 月 26 日～27 日）

台湾のセキュリティカンファレンス HITCON が 11 月 26 日～27 日に開催され、オンラインで配信されました。JPCERT/CC は攻撃グループ Lazarus による標的型攻撃に関する分析について発表を行いました。イベントの詳細については、次の Web ページをご参照ください。

HITCON 2021
https://hitcon.org/2021/

4.3.4. Internet Governance Forum (IGF) 2021 参加（12 月 6 日～10 日）

国連主催のインターネットガバナンスに関する国際会議である IGF2021 が、12 月 6 日から 10 日にかけてポーランドのカトヴィツェで開催され、オンラインでも配信されました。JPCERT/CC はサイバー空間における中立性に関するパネルに登壇し、ヨーロッパやラテンアメリカの代表的な専門家と意見を交わしました。パネルの詳細については、次の Web ページをご参照ください。

IGF 2021 WS #187 Exploring Neutrality: A Multistakeholder Cyber Norms Dialogue
https://www.intgovforum.org/multilingual/content/igf-2021-ws-187-exploring-neutralitya-multistakeholder-cyber-norms-dialogue

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。

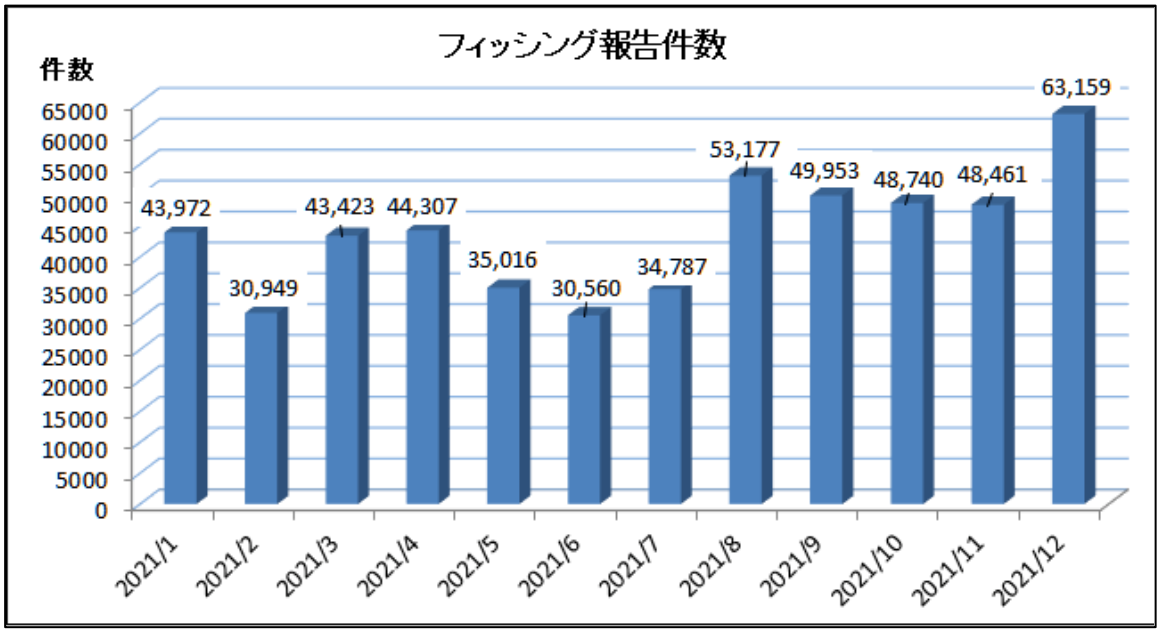
コエディターとして DTR：Draft Technical Report（技術報告書原案）の作成を分担していた WG3「複数の開発者が関与する脆弱性の開示と取扱」については、10 月の国際会議において国際投票時に提出されたコメントの処理が行われ、全体会議でコメントに対処した文書を技術報告書として公開することが承認されました。WG4「インシデント管理に関する標準」については、引き続きの標準文書の改訂に伴う CD 文書の作成ならびに新しいパートの WD 文書の作成が行われており、全体会議においては改訂に伴う CD 文書に対するコメント処理が行われました。また改訂文書のうち「Part2: インシデント対応のための計画及び準備の指針」については DIS：Draft International Standard（国際規格原案）のプロセスに進むことになりました。

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、9 月から 4 万件後半が続いていましたが、12 月にこれまでの最多記録を更新しました。



［図 5-1：1 年間のフィッシング報告件数（月別）］

報告件数の内訳では、Amazon をかたるフィッシングの報告数が引き続き多く、全体の約 27.9%を占めています。次いで、メルカリ、三井住友カード、ETC サービス、楽天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 68.1%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及び緊急情報を計 17 件（ニュース：1 件、緊急情報：21 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。詳細は次のとおりです。

- さくらインターネットをかたるフィッシング ：1 件
- お名前.com 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
- ファミリーマートをかたるフィッシング ：1 件
- Xserver をかたるフィッシング ：1 件
- UCS 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
- 三菱 UFJ 銀行をかたるフィッシング ：1 件
- 明治安田生命をかたるフィッシング ：1 件
- DMM をかたるフィッシング ：1 件
- Mastercard をかたるフィッシング ：1 件
- au および KDDI をかたるフィッシング ：1 件
- Joshin web をかたるフィッシング ：1 件
- 東京都水道局をかたるフィッシング ：1 件
- 住友生命をかたるフィッシング ：1 件
- アフラックをかたるフィッシング ：1 件
- ラクマをかたるフィッシング ：1 件
- ヤマダデンキをかたるフィッシング ：1 件
- 朝日生命をかたるフィッシング ：1 件
- Paidy をかたるフィッシング：1 件
- えきねっと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（40 種類）をかたるフィッシングの報告が多く寄せられました。また、これまでまったく報告がなかった保険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]：保険ブランドをかたるフィッシングの例）。それ以外では、メルカリを模した偽サイトへ誘導するフィッシングの報告が多く寄せられ、Amazon に次ぐ報告件数となりました。（[図 5-3：メルカリをかたるフィッシングの例]）

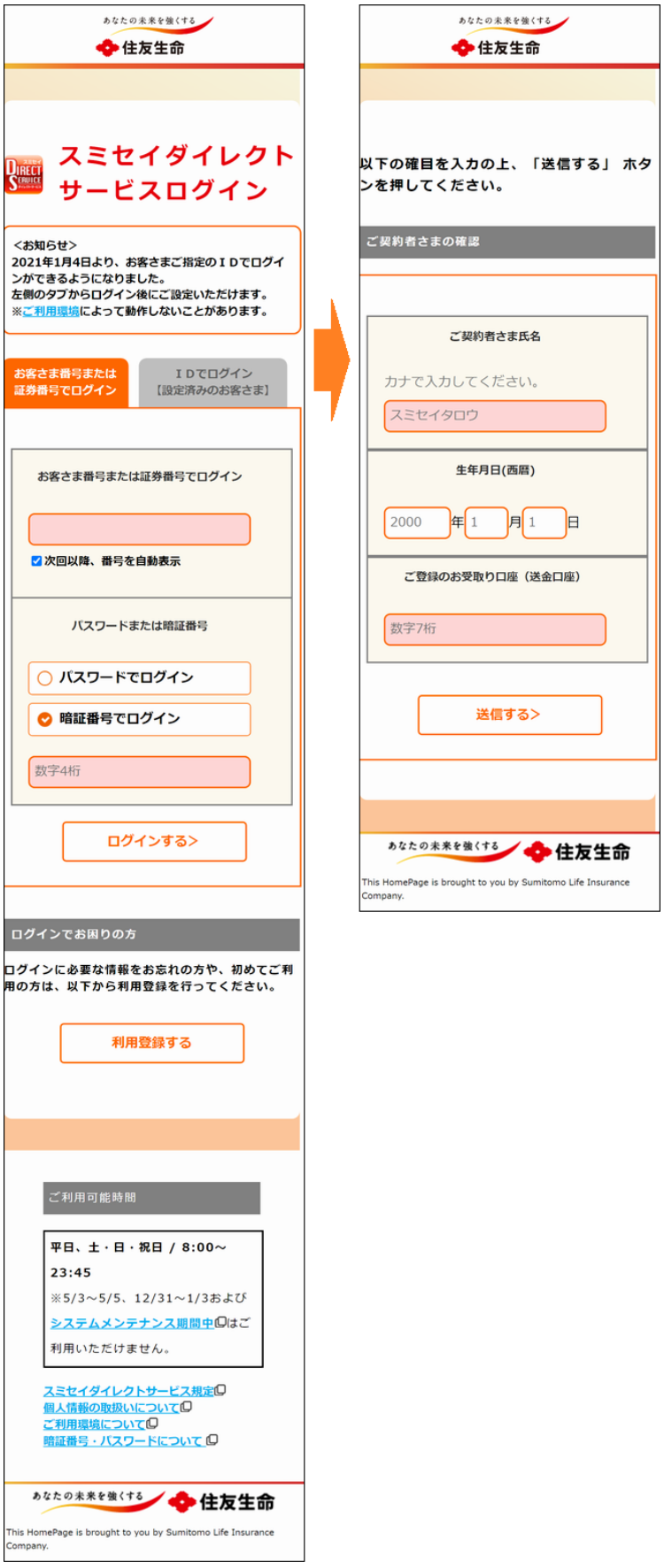
これら大量配信されるフィッシングメールが、依然として正規のメールアドレス （ドメイン） を差出人とした「なりすまし」メールであることから、受信者による判別を容易にするために、送信ドメイン認証

技術を活用するよう協議会として呼び掛けています。

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。以前からある、宅配便の不在通知をかたるものに加えて、Amazon、モバイルキャリアをかたるメッセージを多く確認しています。

フィッシング以外では、ビットコインを要求するセクストーションメールの報告が多数、寄せられています。

※セクストーション…性（sex）と Extortion（ゆすり）を併せた造語。実際には行っていないのに、受信者のデバイスをハッキングして、裸の画像や猥褻サイトの閲覧履歴などの性的情報を入手したと偽り、それを暴露すると脅かして、仮想通貨を要求する詐欺行為。



［図 5-2：保険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/sumisei_20211208.html

［図 5-3：メルカリをかたるフィッシングサイトの例 ］
https://www.antiphishing.jp/news/alert/mercari_20211006.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 10 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/202110.html

2021 年 11 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/202111.html

2021 年 12 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/202112.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 49 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及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、事業者及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 3 回）
  日時：2021 年 10 月 21 日 13:00-15:00

- 技術・制度検討 WG 会合（第 4 回）
  日時：2021 年 11 月 24 日 14:00-16:00

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 92 回運営委員会（オンライン）
  2021 年 10 月 28 日（木）15:30-18:00

- 第 93 回運営委員会（オンライン）
  2021 年 11 月 25 日（木）15:30-18:00

- 第 94 回運営委員会（一部オフライン　JPCERT/CC 開催）
  2021 年 12 月 23 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：10 月-12 月　毎週火曜日 9：00 - 9：30

- 証明書普及促進 WG（第 4 回）
  日時：2021 年 11 月 9 日（月）16：00 - 18：00

- 証明書普及促進 WG（第 5 回）
  日時：2021 年 12 月 13 日（月）16：00 - 18：00

- フィッシング対策セミナー2021
  日時：2021 年 11 月 5 日（金）10：00 - 16：45

※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。

STOP. THINK. CONNECT.普及啓発 WG

- 『第 17 回 IPA「ひろげよう情報モラル・セキュリティコンクール」2021』 の優秀賞を選出
  https://www.antiphishing.jp/news/info/ipa_competition2021.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。

2021-10-14
JPCERT/CC インシデント報告対応レポート［2021 年 7 月 1 日～2021 年 9 月 30 日］
https://www.jpcert.or.jp/pr/2021/IR_Report20211014.pdf

2021-12-10
JPCERT/CC Incident Handling Report [July 1, 2021 - September 30, 2021]
https://www.jpcert.or.jp/english/doc/IR_Report2021Q2_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。

2021-10-19
JPCERT/CC インターネット定点観測レポート［2021 年 7 月 1 日～2021 年 9 月 30 日］
https://www.jpcert.or.jp/tsubame/report/report202107-09.html
https://www.jpcert.or.jp/tsubame/report/TSUBAMEReport2021Q2.pdf

2021-12-10
JPCERT/CC Internet Threat Monitoring Report [July 1, 2021 - September 30, 2021]
https://www.jpcert.or.jp/english/doc/TSUBAMEReport2021Q2_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。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。

2021-10-21
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（7 月～9 月）］
https://www.jpcert.or.jp/pr/2021/vulnREPORT_2021q3.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 10 件の記事を公表しました。

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

2021-10-19	TSUBAME レポート Overflow（2021 年 7～9 月）
2021-10-26	攻撃グループ LuoYu が使用するマルウェア WinDealer
2021-12-02	2021 年度 ベストレポーター賞（脆弱性部門）をトレンドマイクロ株式会社に贈呈
2021-12-17	Apache Log4j2 の RCE 脆弱性（CVE-2021-44228）を狙う攻撃観測
2021-12-21	サイバー政策動向を知ろう Watch! Cyber World vol.1
2021-12-23	モバイル端末を狙うマルウェアへの対応 FAQ

英語版発行件数：4 件 https://blogs.jpcert.or.jp/en/

2021-10-04	Malware Gh0stTimes Used by BlackTech
2021-10-26	How to Use Volatility 3 Offline
2021-12-10	TSUBAME Report Overflow (Jul–Sep 2021)
2021-12-22	Observation of Attacks Targeting Apache Log4j2 RCE Vulnerability (CVE-2021-44228)

8. 主な講演活動

(1) 森 克宏（サイバーメトリクスグループ 情報セキュリティアナリスト）：
「JPCERT/CC の活動について」
総務省総合通信局 サイバーセキュリティ研修課 講義 （主催：総務省 情報通信政策研究所研修部、開催日：2021 年 10 月 5 日）

(2) 佐々木 勇人（早期警戒グループ マネージャー）：
「いつか来る「いざ」という時に備えて～被害者としてだけではないインシデント対応のポイント～」
山形県インターネット防犯連絡協議会総会 （主催：山形県インターネット防犯連絡協議会、開催日：2021 年 10 月 26 日）

(3) 伊藤 智貴（早期警戒グループ 国際連携スペシャリスト）：
パネルディスカッション「Root Roundup Discussion Panel」
CVE Global Summit – Fall 2021（主催：CVE Program、開催日：2021 年 10 月 26 日～27 日）

(4) 土居 毅彦（早期警戒グループ 脅威アナリスト）：
「SSL-VPN 製品の脆弱性および脅威動向」
NANO OPT Media Online（主催：株式会社ナノオプト・メディア 、開催日：2021 年 11 月 4 日）

(5) 輿石 隆 （早期警戒グループ 脅威アナリスト）：
「サイバー攻撃２０２１ - 昨今のサイバー攻撃動向とその対応 -」
Internet Week 2021（主催：一般社団法人日本ネットワークインフォメーションセンター（JPNIC）、開催日：2021 年 11 月 16 日）

(6) 中井 尚子（インシデントレスポンスグループ）：
「従来の攻撃プラットフォームがモバイルに変わりつつある現状と要因について」
Internet Week 2021（主催：一般社団法人日本ネットワークインフォメーションセンター（JPNIC）、開催日：2021 年 11 月 25 日）

(7) 河野 一之（制御システムセキュリティ対策グループ マネージャー）：
「製造現場に産業用 IoT を導入する際のセキュリティ対策の第一歩 -産業用 IoT を活用した事業の推進をセキュアに進めるために -」
オープンリサーチ 2021（主催：千葉県産業支援技術研究所、開催日（オンライン配信期間）：2021 年 11 月 25 日～12 月 9 日）

(8) 小宮山 功一朗（国際部 部長）：
ワークショップ「Exploring Neutrality:A Multistakeholder Cyber Norms Dialogue」
IGF 2021（主催：IGF Japan、開催日：2021 年 12 月 8 日）

(9) 小宮山 功一朗（国際部 部長）：
「日本のサイバーセキュリティ事情」
Keio-Columbia Cyber Dialogue session 12 月会合（主催：慶應大学・コロンビア大学 、開催日：2021 年 12 月 14 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) Security Days Fall 2021
主　催：株式会社ナノオプト・メディア
開催日：2021 年 9 月 24 日（金）～10 月 8 日（金）

(2) 第 21 回迷惑メール対策カンファレンス
主　催：一般財団法人インターネット協会（IAjapan）
開催日：2021 年 11 月 11 日（木）～12 日（金）

(3) Internet Week2021
主　催：一般社団法人日本ネットワークインフォメーションセンター（JPNIC）
開催日：2021 年 11 月 16 日（火）～19 日（金）、22 日（月）、24 日（水）～26 日（金）

(4) HardeningProject2021
主　催：HardeningProject 運営委員
開催日：2021 年 11 月 17 日（水）～20 日（土）、27 日（土）

(5) デジタル・フォレンジック・コミュニティ 2021 in TOKYO
主　催：特定非営利活動法人デジタル・フォレンジック研究会
　　コミュニティ 2021 実行委員会
開催日：2021 年 12 月 6 日（木）～7 日（火）

(6) オーストラリア外務貿易省日豪交流基金助成金によるサイバーセキュリティ分野の多様性促進を目的とした日豪協力の学際的パネルディスカッション
主　催：クイーンズランド大学、株式会社 BLUE
開催日：2021 年 12 月 8 日（木）、15 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