JPCERT/CC 活動四半期レポート

2023 年 10 月 1 日 ～ 2023 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

2024 年 1 月 18 日

目次

本活動は、経済産業省より委託を受け、「令和 5 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」、「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。

活動概要トピックス

－トピック1－　JPCERT/CC ベストレポーター賞 2023

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ご提供いただける報告者（レポーター）の皆さまは、サイバーセキュリティにおける問題解決に向けて JPCERT/CC が調整業務を的確に進めるための重要な情報源であり協力者でもあります。
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する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、日々情報をご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、特に優れた報告者の活動事例を広く世に知っていただく機会になればと考え、2021 年度に「ベストレポーター賞」を制定しました。
ベストレポーター賞では、インシデント報告と脆弱性報告の 2 つの部門を設けています。インシデントの報告、または、脆弱性情報の報告をいただいた方の中から、その件数や内容に基づいて JPCERT/CC の活動に顕著な貢献をされた方を選び、感謝の意を表して各賞を贈呈しています。

3 回目となる本年度は次の方にインシデント報告部門のベストレポーター賞をお贈りしました。脆弱性報告部門については該当者がありませんでした。

大学共同利用機関法人 高エネルギー加速器研究機構（KEK） 加茂 聡 様（インシデント報告部門）

加茂様は、自組織だけでなく外部の組織も対象にインシデントやフィッシングサイトなどについて日々調査、情報収集されています。そうした活動の中で発見された多数のインシデントを JPCERT/CC へご報告いただくとともに、活動から得られたインシデント発見手法と対応などについての知見を、学術系 CSIRT や、日本シーサート協議会、つくば SEC といったコミュニティーへ共有され、多くの組織のセキュリティ対策に貢献されました。

今回の受賞者をはじめとする、 JPCERT/CC の活動に日々ご協力いただいている多くのレポーターの方々にあらためて感謝申し上げます。

JPCERT/CC ベストレポーター賞 2023
https://www.jpcert.or.jp/award/best-reporter-award/2023.html

－トピック2－　製品開発者間の情報交換のための定期ミーティングを京都で開催

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。この活動には製品開発者のご協力が欠かせず、プロアクティブにご協力いただける製品開発者の皆さまを JPCERT/CC 製品開発者リストへ登録し連携体制を構築しています。
さらに、製品開発者リストに登録された皆さまとの情報交換・意見交換のためのミーティングを四半期ごとに開催しています。ミーティングでは、国内のさまざまな業種・業態の製品開発者が集い、製品脆弱性に関連する技術情報や動向などの情報交換、脆弱性情報流通業務に関する意見交換、製品開発者の PSIRT の整備や活動強化についての情報交換などを行っています。
こうしたミーティングで直接対話することは、JPCERT/CC にとっても、製品開発者の皆さまとの信頼を醸成し、脆弱性情報コーディネーションを円滑に進められるようにするためにとても重要です。従来は JPCERT/CC の事務所がある東京で開催していましたが、コロナ禍を経て、今年度からは Web 会議を併用したハイブリッド形式とし、地方に拠点を置く製品開発者にも参加しやすくなっていました。本四半期はこれをさらに推し進め、地方の開発者とのより直接的なコミュニケーションの機会を設けようと、12 月 15 日、初めての地方開催ミーティングをハイブリッド形式で実施しました。京都の会場には関西を拠点とする多くの製品開発者にお集まりいただき、活発な意見交換が行われました。
このミーティングの詳細については、「2.2.2. 製品開発者との定期ミーティング等の実施」をご参照ください。

JPCERT/CC では、今後も全国各地の製品開発者との連携を深めるため、地方開催のミーティングを実施していく計画です。

－トピック3－　JPCERT/CC が提案した 2 つのセッションが国連 IGF2023 に採択され運営と進行を担当

2023 年 10 月 8 日から 12 日まで京都で開催された第 18 回 Internet Governance Forum（IGF）において、JPCERT/CC が提案した 2 つのセッションが採択され、その実施にあたりオーガナイザーを務めました。「CSIRTs: A Global Dialogue with Cyber Incident Responders」というワークショップと、「Meeting Spot for CSIRT Practitioners: Share Your Experiences」というネットワーキングセッションです。
IGF は、国連加盟国をはじめとする政府や政府系組織だけでなく、民間セクター、技術コミュニティー、市民社会など、あらゆるステークホルダーが一堂に会してインターネットガバナンスに関して対話するために設けられた、国連が主催する大規模な国際会議です。JPCERT/CC はこれまでも IGF に継続的に参加し、インターネットガバナンスの議論を国内外に紹介するだけでなく、他の組織が運営するセッションに招かれ登壇してきましたが、今回はセッションの提案から運営と進行までを一貫して行いました。

どちらのセッションでも、国境を超えた連携が欠かせない CSIRT の役割や現在の課題について、講演者や聴講者と意見交換を行い、CSIRT および地域 CSIRT コミュニティーの存在をさまざまなステークホルダーに向けてアピールしました。JPCERT/CC は、サイバー空間のグローバルな取り決めや仕組み、実施体制についてセキュリティを推進する立場から意見を発信し、また、適切な情報を必要な人々に届けるなどのコーディネーションセンターとしての組織使命を果たすために、今後も IGF を含めたインターネットガバナンスに関する議論への参加を続けていきます。
2 つのセッションの詳細については次の JPCERT/CC Eyes の記事をご参照ください。

JPCERT/CC Eyes「国連 IGF2023 にて 2 つのセッションの運営と進行を務めました」
https://blogs.jpcert.or.jp/ja/2023/12/igf2023.html

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」という。）に関する報告は、報告件数ベースで 10,273 件、インシデント件数ベースでは 6,448 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 5,444 件でした。前四半期の 5,070 件と比較して 7%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、ウイルスなどのマルウェアが設置されたサイト、「scan」のアクセス元などの管理者などに対し、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 など）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/2023/IR_Report2023Q3.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 4,473 件で、前四半期の 4,754 件から 6%減少しました。また、前年度同期（6,266 件）との比較では、29%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数を添えて［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・国外ブランド別数］

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	894	1,047	855	2,796 (63%)
国外ブランド	371	278	467	1,116 (25%)
ブランド不明 (注 2)	188	230	143	561 (13%)
全ブランド合計	1,453	1,555	1,465	4,473

（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などの理由により、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。

JPCERT/CC が報告を受けたフィッシングサイトのうち、国外ブランド関連の報告では E コマースサイトを装ったものが 69.8%、国内ブランド関連の報告では金融関連のサイトを装ったものが 48.8%で、それぞれ最も多くを占めました。

海外ブランドでは、Amazon を装ったフィッシングサイトが全体の半数以上を占めました。
国内ブランドでは、総務省のマイナポイント事業や、ETC の利用照会サービスを装ったフィッシングサイトが多く報告されました。国内金融機関では、前四半期に引き続きエポスカード、イオンカード、そして三井住友カードを装ったフィッシングサイトが引き続き多く報告されました。前四半期と比較すると、セゾンカードや PayPay を装ったフィッシングサイト数の減少が目立ちました。

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 21%、国外が 79%であり、前四半期（国内が 25%、国外が 75%）と比較し国内の割合が増加しました。

1.1.1.2. Web サイト改ざん

本四半期に報告が寄せられた Web サイト改ざんの件数は、72 件でした。前四半期の 124 件から 42%減少しています。

本四半期は、不審なサイトへの転送させる Web サイトの改ざん事例を複数確認しました。改ざんされた Web サイトには［図 1-1］のようなスクリプトが設置されていて、初めてのアクセスだった場合にだけ不審なサイトに誘導する仕組みになっていました。なお、不審サイトは、ラッキービジター詐欺やブラウザーの通知機能を悪用するサイトであることを確認しています。

```
localStorage.setItem('test', 'testValue');

if ((localStorage.getItem('test') !== null) &&  (localStorage.getItem('click3') == null)){

    var click_r = false;
    document.addEventListener("click", function(){

    if(click_r == false){
    localStorage.setItem('click3', 'click3');
    window.open("[redacted]");
    click_r = true;
    }
    });
}
```

［図 1-1：不審なサイトを表示するスクリプト］

1.1.1.3. その他

本四半期に行った対応の例を紹介します。

(1) Proself の脆弱性（CVE-2023-45727）への対応

2023 年 10 月 10 日に、ノースグリッド社はオンラインストレージ構築パッケージ製品「Proself」における XML 外部実体参照（XXE）に関する脆弱性があることを公開しました。本脆弱性を悪用して、システム内の任意のファイルを外部へ送信する攻撃が確認されたことから JPCERT/CC でも 10 月 10 日に注意喚起を行いました。

Proself の XML 外部実体参照（XXE）に関する脆弱性を悪用する攻撃の注意喚起
https://www.jpcert.or.jp/at/2023/at230022.html

JPCERT/CC では、パッチ未適用と思われる国内の Proself を利用しているシステム管理者に対して通知を行いました。影響を受ける製品を利用している場合には速やかな対策をお願いします。また、すでに攻撃を受けている可能性もありますので、JPCERT/CC が公開しているインディケータ情報を参考に、不審な通信がないことを確認することを推奨します。

日本の組織を標的にした外部からアクセス可能な IT 資産を狙う複数の標的型サイバー攻撃活動に関する注意喚起
https://www.jpcert.or.jp/at/2023/at230029.html

(2) Cisco IOS XE の脆弱性（CVE-2023-20198）への対応

Cisco 社は、2023 年 10 月 16 日に Cisco IOS XE ソフトウェアの Web UI 機能に権限昇格の脆弱性があることを公開しました。これら脆弱性が悪用されると、認証されていない遠隔の第三者が最上位の特権アカウントを作成し当該システムを制御する可能性があることから、JPCERT/CC でも 10 月 18 日に注意喚起を行いました。

Cisco IOS XE の Web UI の脆弱性(CVE-2023-20198)に関する注意喚起
https://www.jpcert.or.jp/at/2023/at230025.html

JPCERT/CC には、本脆弱性を悪用してバックドアが設置された被害報告が国内外の組織から寄せられています。JPCERT/CC では、バックドアが設置されていると思われる国内のデバイスの管理者に対して通知を行いました。影響を受ける製品を利用している場合には速やかなアップデートをお願いします。

1.1.2. インシデントに関する情報提供のお願い

Web サイト改ざんなど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などの管理者への対応依頼など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、注意喚起など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など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などを対象とした「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 35,000 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）など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などが公表された場合には、「注意喚起」と呼ばれる文書を発行し、利用者に対して広く対策を呼びかけています。本四半期は次の注意喚起を発行しました。

発行件数：14 件（うち更新情報が 5 件）　https://www.jpcert.or.jp/at/

2023-10-10　Proself の XML 外部実体参照（XXE）に関する脆弱性を悪用する攻撃の注意喚起
2023-10-11　2023 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
2023-10-11　Citrix ADC および Citrix Gateway の脆弱性（CVE-2023-3519）に関する注意喚起（更新）
2023-10-18　2023 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
2023-10-18　Cisco IOS XE の Web UI における権限昇格の脆弱性（CVE-2023-20198）に関する注意喚起
2023-10-18　Proself の XML 外部実体参照（XXE）に関する脆弱性を悪用する攻撃の注意喚起（更新）
2023-10-20　Citrix ADC および Citrix Gateway の脆弱性（CVE-2023-4966）に関する注意喚起
2023-10-23　Cisco IOS XE の Web UI の脆弱性(CVE-2023-20198)に関する注意喚起（更新）
2023-10-26　Proself の XML 外部実体参照（XXE）に関する脆弱性を悪用する攻撃の注意喚起（更新）
2023-11-15　2023 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
2023-11-15　Adobe Acrobat および Reader の脆弱性（APSB23-54）に関する注意喚起
2023-11-16　日本の組織を標的にした外部からアクセス可能な IT 資産を狙う複数の標的型サイバー攻撃活動に関する注意喚起
2023-11-21　Citrix ADC および Citrix Gateway の脆弱性（CVE-2023-4966）に関する注意喚起（更新）
2023-12-13　2023 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

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。
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/

1.2.1.3. 早期警戒情報

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 のうち、「早期警戒情報」の受け取りを希望して申し込みをいただいた方々に向けて、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「早期警戒情報」と呼ばれる情報を、各組織における必要性を勘案して提供しています。本四半期には 1 件の早期警戒情報を発信しました。
「早期警戒情報」の枠組みへの参加については次の Web ページを参考にご検討ください。

早期警戒情報
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：9 件（うち更新情報が 2 件）　https://www.jpcert.or.jp/newsflash/

2023-10-05　Apple 製品のアップデートについて（2023 年 10 月）
2023-10-11　Apple 製品のアップデートについて（2023 年 10 月）（更新）
2023-10-11　複数のアドビ製品のアップデートについて
2023-10-27　BIG-IP の脆弱性（CVE-2023-46747）について
2023-11-15　Intel 製品に関する複数の脆弱性について
2023-11-15　複数のアドビ製品のアップデートについて
2023-12-01　Apple 製品のアップデートについて（2023 年 12 月）
2023-12-13　Apple 製品のアップデートについて（2023 年 12 月）（更新）
2023-12-13　複数のアドビ製品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) 日本の組織を標的にした外部からアクセス可能な IT 資産を狙う複数の標的型サイバー攻撃活動に関する情報発信

2023 年 11 月 16 日、JPCERT/CC は、日本の組織を標的にした外部からアクセス可能な IT 資産を狙う複数の標的型サイバー攻撃活動に関する注意喚起を公開しました。
この注意喚起を出すことになった発端は SSL-VPN 用機器 ArrayAG シリーズの脆弱性を悪用した標的型攻撃でした。JPCERT/CC はこの攻撃の調査を 2023 年 5 月頃からサイバーセキュリティ協議会を通じて実施しました。その結果、この攻撃も、ノースグリッド社の Proself や Fortinet 社の FortiOS などの製品の脆弱性を悪用した攻撃も、同じ攻撃インフラから行われていることが判明しました。こうした経緯を経

て、複数の製品の類似した脆弱性を狙う攻撃活動に対して幅広く注意を促すことになりました。注意喚起では、複数の脆弱性情報とそれらに関連した攻撃のインディケータ情報を示して、外部からアクセス可能な機器に関する侵害の調査と適切な管理を促しています。また、今回の標的型サイバー攻撃との関連を確認している脆弱性の対象機器の他にも、今後の調査によってはさらに別の製品の脆弱性を悪用する攻撃が確認される可能性もあると JPCERT/CC は懸念しており、今回の標的型サイバー攻撃活動の動向を継続して注視するよう呼びかけました。

日本の組織を標的にした外部からアクセス可能な IT 資産を狙う複数の標的型サイバー攻撃活動に関する注意喚起
https://www.jpcert.or.jp/at/2023/at230029.html

(2) Proself の XML 外部実体参照（XXE）に関する情報発信

2023 年 10 月 10 日、株式会社ノースグリッドはオンラインストレージ構築パッケージ製品「Proself」の XML 外部実体参照（XXE）に関する脆弱性の情報を公表しました。同社によると、本脆弱性の悪用を含む一連の攻撃が確認されており、同社から利用者に対して、攻撃の影響を受けていないか確認するための調査の実施や、脆弱性の影響を緩和するための対策、アップデート版をリリースするまでの暫定対策方法の呼びかけが行われました。
JPCERT/CC は 2023 年 7 月に同製品で発見された別の深刻な脆弱性について、開発元との調整や製品の利用組織への通知支援を行いました。その際、該当の脆弱性に関する情報が伝わっていない利用組織が多く存在することを確認していました。そのため、今回の脆弱性をより多くの製品利用者に確認してもらうために、JPCERT/CC では開発元の情報公表と同日の 2023 年 10 月 10 日に注意喚起を公開し、問題の認識や調査、対策実施を広く呼びかけました。また、2023 年 10 月 18 日、26 日に XML 外部実体参照(XXE)の脆弱性に対するアップデートが公開されたため、注意喚起を更新し、アップデートの適用を呼びかけました。

Proself の XML 外部実体参照（XXE）に関する脆弱性を悪用する攻撃の注意喚起
https://www.jpcert.or.jp/at/2023/at230022.html

(3) Cisco IOS XE の Web UI における権限昇格の脆弱性（CVE-2023-20198）に関する情報発信

2023 年 10 月 16 日（現地時間）に Cisco は Cisco IOS XE ソフトウェアの Web UI 機能における権限昇格の脆弱性およびその悪用に関する情報を公表しました。
本脆弱性が悪用されると、同製品の Web UI 機能を有効にしている場合、同機能は同製品が接続されているネットワークに公開されていることになり、接続されているネットワークがインターネットや信頼できないネットワークである場合には、認証されていない第三者が、最上位の特権アカウントを作成し、当該システムを制御する可能性があります。
JPCERT/CC では、本脆弱性を悪用した攻撃による被害の報告を受けました。また、本脆弱性を悪用した

攻撃を受けて侵害されている可能性がある機器のリストの提供を受け、そのリストから、本脆弱性を悪用した攻撃を受けながら、攻撃に気づいていない国内組織が多数ありそうなことが推測されました。
そのため、広く問題の認識や調査を行い、被害の状況を確認し、対策を実施してもらうべく、10 月 18 日に注意喚起を公開しました。加えて、インターネット上のスキャン・パケットの分析から、本脆弱性を攻撃され侵害されていると推測される機器を保有している国内組織に対して、個別に通知を行い、被害の確認と脆弱性への対応を呼びかけました。
また 2023 年 10 月 23 日、Cisco がアドバイザリを更新し、確認された Cisco IOS XE への攻撃についての情報の追記や本脆弱性を修正したアップデートの公開を行ったため、JPCERT/CC でも注意喚起を更新し、アップデートの適用を呼びかけました。

Cisco IOS XE の Web UI の脆弱性(CVE-2023-20198)に関する注意喚起
https://www.jpcert.or.jp/at/2023/at230025.html

1.3. インターネット上の探索活動や攻撃活動に関する観測と分析

1.3.1. インターネット定点観測システム TSUBAME を用いた観測

JPCERT/CC では、不特定多数に向けて発信されるパケットを収集する観測用センサーを開発し、これを各地域に複数分散配置して、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。海外においても、ホスティングサービスなどを利用することにより、独自の観測センサーを配備しています。TSUBAME のセンサーで収集された観測結果は一つのデータベースにまとめて分析しています。これを、公開された脆弱性情報やマルウェア、攻撃ツールの情報などと対比することで、攻撃活動や攻撃の準備活動などを把握できる場合があり、グローバルな視野から攻撃活動など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

1.3.1.1. TSUBAME の観測データの活用

JPCERT/CC では、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」を公開しています。本四半期は、2023 年 7 月から 9 月の期間に関するレポートと、レポートで書き切れなかった内容を盛り込んだブログを公開しました。

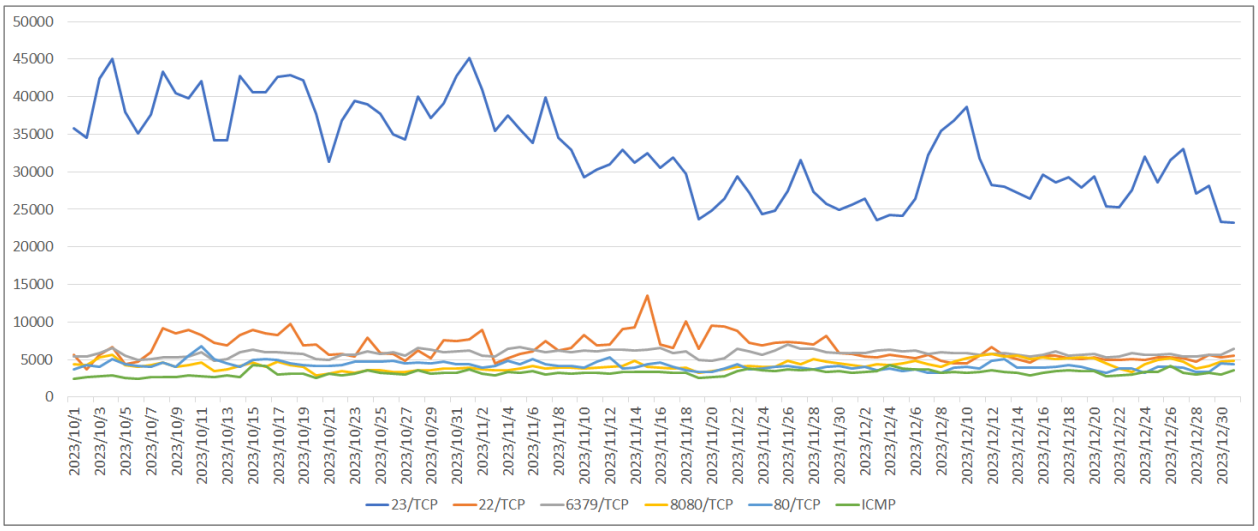
TSUBAME 観測グラフ
https://www.jpcert.or.jp/tsubame/index.html#examples

インターネット定点観測レポート（2023 年 7～9 月）
https://www.jpcert.or.jp/tsubame/report/report202307-09.html

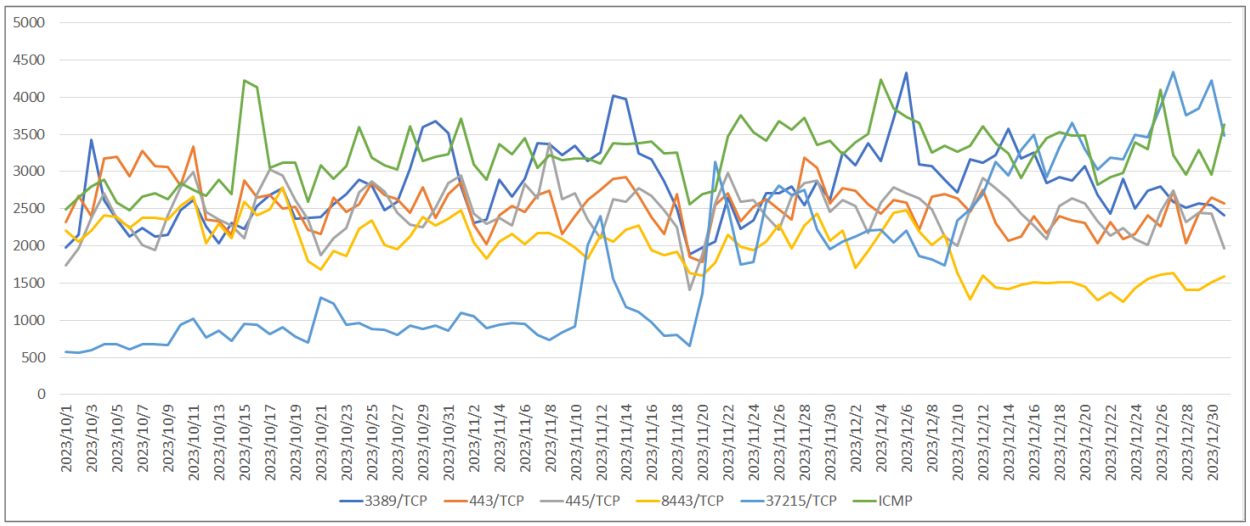
TSUBAME レポート Overflow（2023 年 7～9 月）
https://blogs.jpcert.or.jp/ja/2023/10/tsubame_overflow_2023-07-09.html

1.3.1.2. TSUBAME 観測動向

日本に設置されたセンサーが本四半期に観測した宛先ポートごとパケット数で上位 10 位になったものの本四半期における日々の増減を、上位 1～5 位と 6～10 位とに分けて［図 1-2］と［図 1-3］に示します。

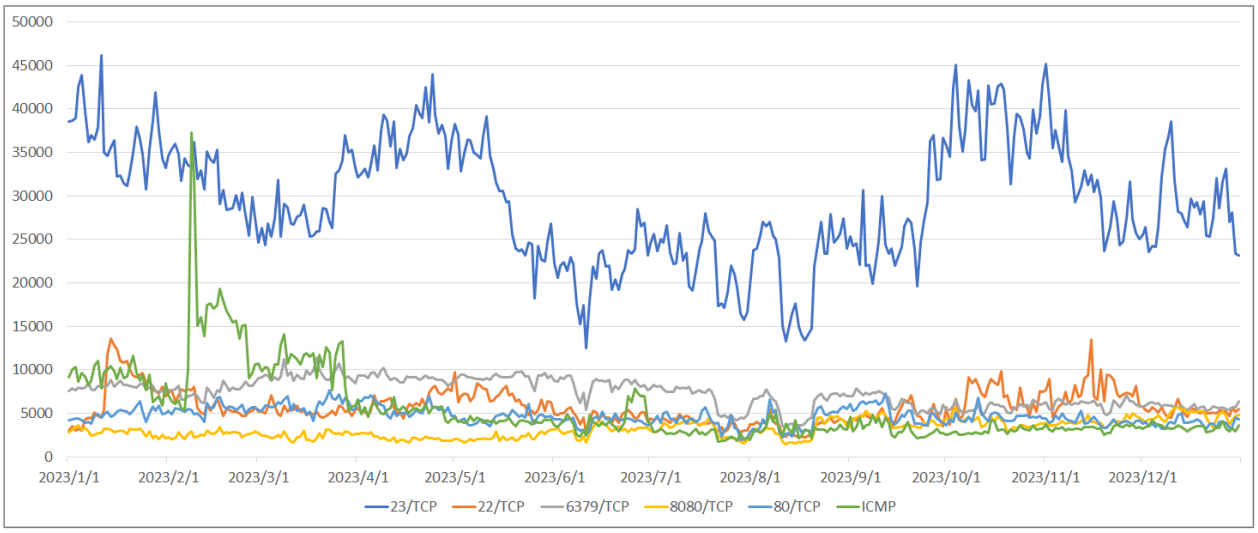


［図 1-2：TSUBAME で観測された宛先ポートの上位 1 位から 5 位のパケット数（2023 年 10 月 1 日-12 月 31 日)］

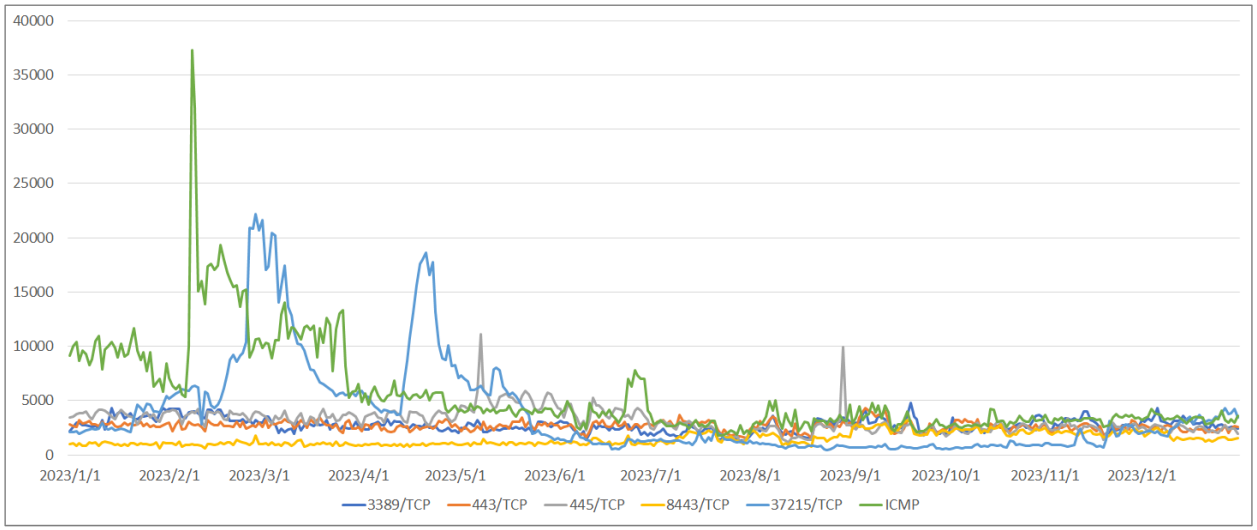


［図 1-3：TSUBAME で観測された宛先ポートの上位 6 位から 10 位のパケット数（2023 年 10 月 1 日-12 月 31 日)］

また、過去 1 年間（2023 年 1 月 1 日-12 月 31 日）の、宛先ポート別パケット数の上位 1～5 位および 6～10 位の観測数の推移を［図 1-4］と［図 1-5］に示します。



［図 1-4：TSUBAME で観測された宛先ポートの上位 1 位から 5 位のパケット数（2023 年 1 月 1 日-12 月 31 日)］



［図 1-5：TSUBAME で観測された宛先ポートの上位 6 位から 10 位のパケット数（2023 年 1 月 1 日-12 月 31 日)］

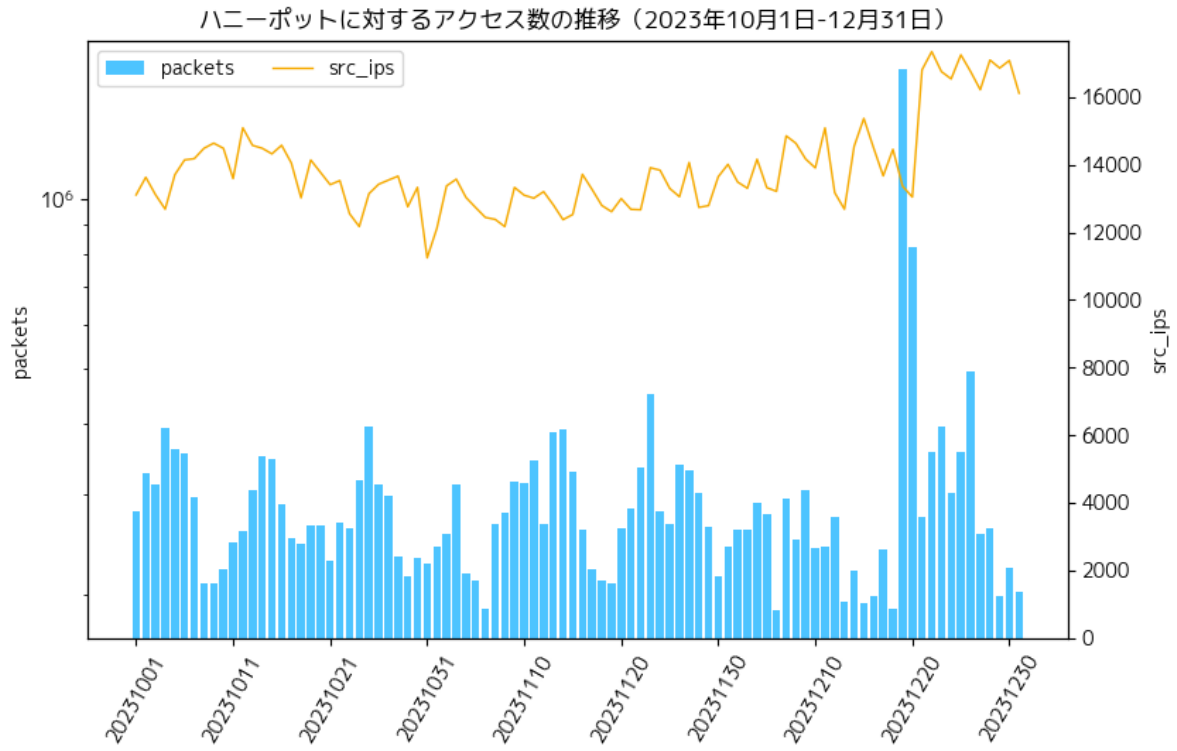
本四半期に最も多く観測されたパケットは 23/TCP（telnet）宛の通信でした。次いで、22/TCP（SSH）宛の通信が 6379/TCP と入れ替わり 2 番目になりました。4 番目と 5 番目に観測されたパケットは 80/TCP(http)、8080/TCP 宛の通信でした。

1.3.2. ハニーポットの運用とその分析

JPCERT/CC では、インターネット上に低対話型のハニーポットを設置して攻撃者から送られてくる種々の通信内容を収集し、攻撃活動を分析しています。

1.3.2.1. ハニーポット観測動向

本四半期にハニーポットで観測されたアクセス数の推移を［図 1-6］に示します。なお、図中の packets はアクセス数を、src_ips は送信元ホスト数を表します（以下同様）。

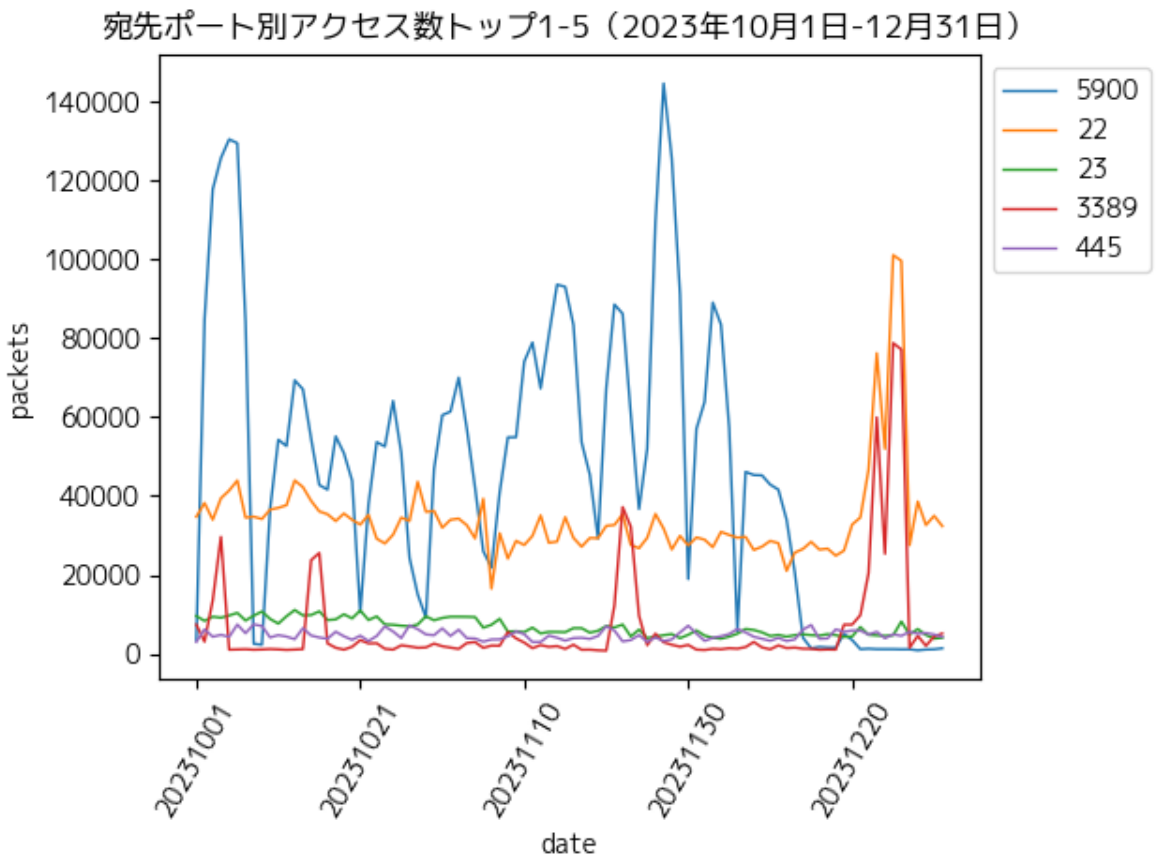


［図 1-6: ハニーポットに対するアクセス数の推移（2023 年 10 月 1 日-2023 年 12 月 31 日）］

また、ハニーポットで観測された宛先ポート別アクセス数の上位 1-5 位を［表 1-2］および［図 1-7］に示します。

［表 1-2: 宛先ポート別アクセス数 トップ 1-5（2023 年 10 月 1 日-12 月 31 日)］

#	宛先ポート	アクセス数
1	5900/TCP	4,349,008
2	22/TCP	3,151,382
3	23/TCP	623,492
4	3389/TCP	621,573
5	445/TCP	436,034



［図 1-7：宛先ポート別アクセス数 トップ 1-5（2023 年 10 月 1 日-12 月 31 日)］

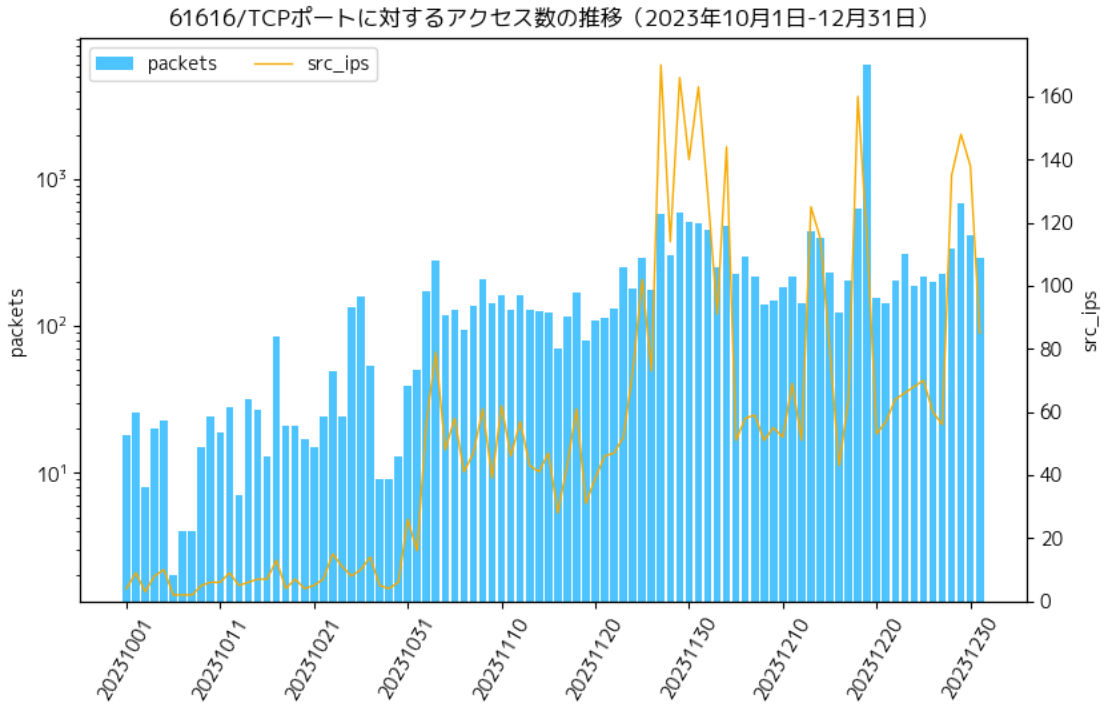
本四半期においては 5900/TCP ポートに対するアクセスが多く観測されています。これらの送信元ホストの多くは、Graynoise などのデータベースではスキャンツールである ZMap クライアントと推定されており、脆弱なサーバーを探索する目的でスキャンを行っているものと考えられますが、現時点では調査研究によるものか攻撃者によるものか判別することはできません。

ハニーポットでは、Shodan や Censys といった調査研究を目的としたスキャナーからのアクセスも多く観測されますが、それら調査研究目的のパケットと攻撃を目的としたパケットを区別することは難しく、

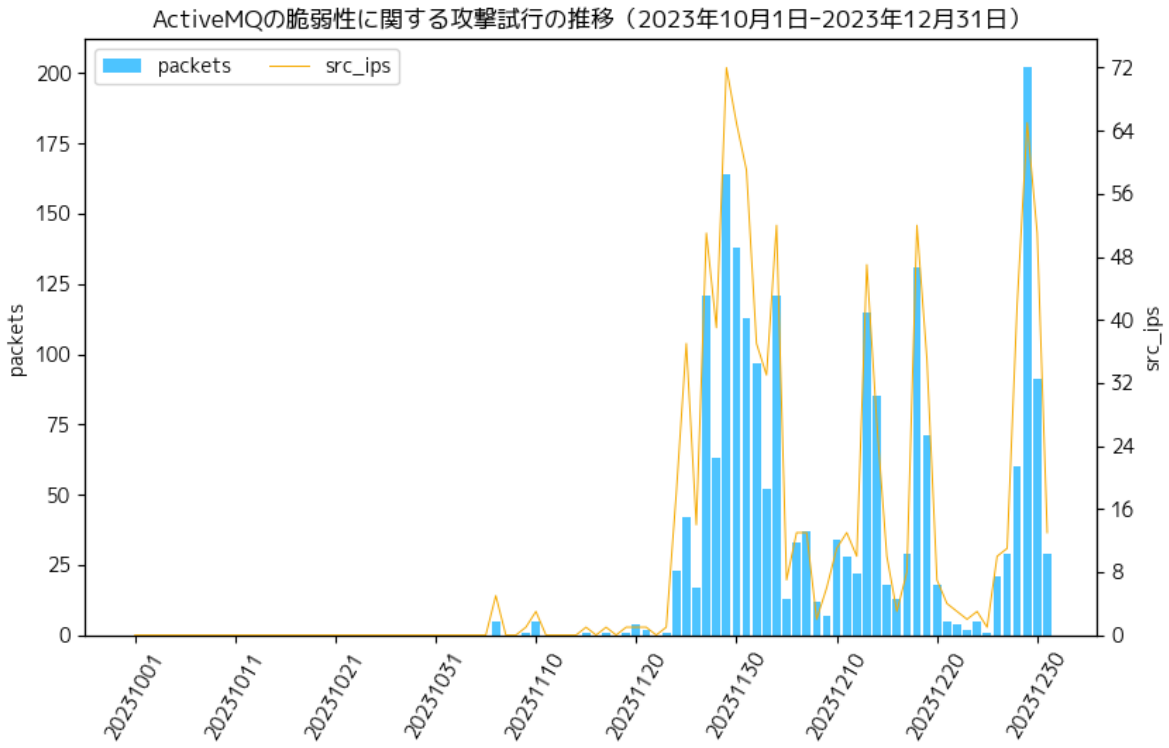
今後の課題となっています。

1.3.2.2. ActiveMQ の脆弱性に対する攻撃試行の観測

2023 年 11 月以降、JPCERT/CC で対応を行っていた ActiveMQ の脆弱性（CVE-2023-46604）に対する探索活動および攻撃試行を観測しています。同脆弱性は、10 月 26 日（米国時間）に公開されたものです。ActiveMQ が提供している OpenWire モジュールにおいては、初期状態で 61616/TCP ポートの待ち受けが有効になっており、JPCERT/CC では、11 月 2 日頃から 61616/TCP に対するアクセスの増加を観測しました［図 1-8］。
また、11 月 6 日からは本脆弱性の PoC に含まれる ClassPathXmlApplicationContext という文字列をペイロードに持ち、任意の Java クラスをインスタンス化することでコードを実行させようとしていると思われるパケットを観測しています［図 1-9］。



［図 1-8：61616/TCP ポートに対するパケット数の推移（2023 年 10 月 1 日-2023 年 12 月 31 日）］



［図 1-9：ActiveMQ の脆弱性に関する攻撃試行の推移（2023 年 10 月 1 日-2023 年 12 月 31 日）］

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）共同運営）を通じて公表することで広く注意を促す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. JPCERT/CC における脆弱性関連情報の取り扱い

JPCERT/CC では、寄せられた脆弱性関連情報に対して、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、製品開発者による脆弱性の検証や対処に向けた調整を行い、JVN を通じて脆弱性情報などを一般に公表しています。また、公表した脆弱性情報の国際的かつ効果的な情報流通のために、CVE（Common Vulnerabilities and Exposures）Program（個々の脆弱性を特定、記述、公に公表されたものをカタログ化することを使命として、専門家コミュニティーにより進められている国際的な活動。その事務局は米国の MITRE 社が務めています。）において配下の CNA を統括する Root の役割を担うとともに、CNA（CVE Numbering Authority、CVE 採番機関）として、CVE 番号の

付与を行っています。
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）に基づく「調整機関」として、製品開発者とのコーディネーションを行っています。調整機関としての活動は、この規定に基づく「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」という。）に沿って、脆弱性情報の「受付機関」である独立行政法人情報処理推進機構（IPA）と緊密に連携して進めています。
また、CERT/CC や CISA、NCSC-NL、NCSC-FI といった海外の調整組織との国際調整、国内外から寄せられる報告や調整依頼にも対応しています。

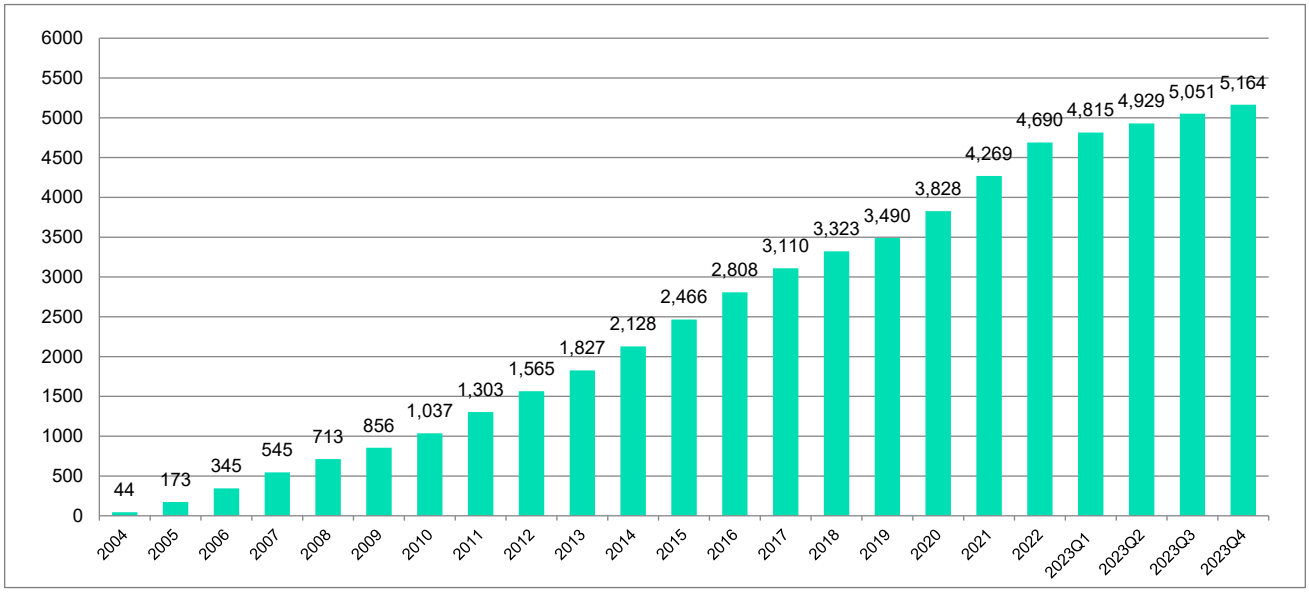
2.1.2. Japan Vulnerability Notes（JVN）において公表した脆弱性情報および対応状況

JVN で公表している脆弱性情報は、次の 3 種類に分類されます。

- パートナーシップガイドラインに基づき報告された脆弱性関連情報に関するもの（「JVN#」に続く 8 桁の数字の形式の識別子を付与している；例：JVN#12345678）
- 国際調整や独自調整に基づく脆弱性情報（「JVNVU#」に続く 8 桁の数字の形式の識別子を付与している；例：JVNVU#12345678）
- 脆弱性情報に関連する技術情報や影響範囲が広く個別の製品の脆弱性情報という範疇を超えた情報など（「JVNTA」に続く 8 桁数字の形式の識別子を付与している；例：JVNTA#12345678）

本四半期に JVN において公表した脆弱性情報は 113 件（累計 5,164 件）で、累計の推移は［図 2-1］に示すとおりです。
本四半期に公表された個々の脆弱性情報に関しては、次の Web ページをご参照ください。

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



［図 2-1：JVN 公表累積件数］

本四半期において公表に至った脆弱性情報件数の内訳は次のとおりです。

- パートナーシップガイドラインに基づき報告された脆弱性情報に関するもの：28 件
- 国際調整や独自調整に基づく脆弱性情報に関するもの：84 件
- 脆弱性情報に関連する技術情報などに関するもの：1 件

なお、パートナーシップガイドラインに基づく脆弱性関連情報に関する四半期ごとの届出状況については、次の Web ページをご参照ください。

独立行政法人情報処理推進機構（IPA）ソフトウェア等の脆弱性関連情報に関する届出状況
https://www.ipa.go.jp/security/reports/vuln/software/index.html

本四半期に公表に至った脆弱性情報について、特徴があったものを紹介します。

(1) パートナーシップガイドラインに基づき報告された脆弱性関連情報における特徴的な事例

- JVN#95981460
  Proself における XML 外部実体参照（XXE）に関する脆弱性
  https://jvn.jp/jp/JVN95981460/

株式会社ノースグリッド社の提供するオンラインストレージサーバーProself における XML 外部実体参照（XXE)の脆弱性について同社から報告があり、それに基づいて JVN でアドバイザリを公表しました。

この脆弱性は、すでにサイバー攻撃に悪用されていることが確認されており、JPCERT/CC は、同社と協力して、注意喚起（JPCERT-AT-2023-0022　Proself の XML 外部実体参照（XXE）に関する脆弱性を悪用する攻撃の注意喚起　https://www.jpcert.or.jp/at/2023/at230022.html）を公表するとともに、同社から提供を受けた脅威情報の共有や対策を促す活動を情報専門組織間や利用組織に対して行いました。

(2) 国際調整または独自調整で取り扱った脆弱性における特徴的な事例

● JVNVU#98585341
Apache ActiveMQ にリモートコード実行の脆弱性
https://jvn.jp/vu/JVNVU98585341/

Apache Software Foundation から公開されているメッセージブローカーActiveMQ における脆弱性(CVE-2023）に関するアドバイザリです。本件は、Apache Software Foundation からのアナウンスや海外でのサイバー攻撃に関する公開情報に基づいて JPCERT/CC がアドバイザリを作成しました。さらに、当該製品を組み込んで自社製品を作っている可能性がある開発者のうち製品開発者リスト（https://www.jpcert.or.jp/vh/register.html）に登録済みの方々には参考情報としても通知しました。国内においても当該脆弱性を悪用したインシデントが報告されており、JPCERT/CC が運用するハニーポットでも脆弱性を悪用しようとする通信を確認しています。ActiveMQ を利用した製品を提供する製品開発者は、製品内部で利用している ActiveMQ をアップデートするなど、脆弱性への対策を進めることを強く推奨します。

● JVNVU#92152057
FXC 製無線 LAN ルータ「AE1021PE」および「AE1021」における OS コマンドインジェクションの脆弱性
https://jvn.jp/vu/JVNVU92152057/

FXC 社製情報コンセント対応型無線 LAN ルーターである「AE1021PE」および「AE1021」における OS コマンドインジェクションの脆弱性に関するアドバイザリです。当該脆弱性は、不正な通信の発見を糸口として、国内の研究者と海外の研究者により同時期に発見されました。本件の調整では JPCERT/CC が主導して、開発者や国内研究者、CISA、海外研究者との間の脆弱性情報や観測情報に関する情報共有、各々から公開する情報の内容と公開タイミングの調整を行いました。

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、52 件（製品開発者数で 32 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 199 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。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. 海外の脆弱性調整組織等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、米国の CISA および CERT/CC など各地域で脆弱性情報のコーディネーションを行っている海外の調整組織と協力関係を結び、脆弱性情報の円滑な国際的調整、情報流通などで相互に連携しています。また、FIRST（Forum of Incident Response and Security Teams）をはじめとする脆弱性に関わる国際的なコミュニティー活動に参加し、連携のための基盤づくりなどを行っています。本四半期の活動を次に紹介します。

(1) APCERT に脆弱性調整の課題に取り組むためのワーキンググループを設立

アジア太平洋地域には、国際的な脆弱性調整活動に参加する、また将来的にその可能性がある製品開発者や部品サプライヤーなどが数多く存在していますが、その中の多くは、脆弱性情報を受け取る窓口すら決まっていないなど、脆弱性ハンドリングへの準備が整っていない状況にあります。そのため、脆弱性情報への対応や情報流通を適切に行えないことが懸念されています。こうした状況を改善するため、JPCERT/CC では、インドの CERT-In、台湾の TWCERT/CC ならびに韓国の KrCERT/CC と協力し、アジア太平洋地域における CSIRT コミュニティーである APCERT（Asia Pacific Computer Emergency Response Team）にワーキンググループ「Coordinated Vulnerability Disclosure WG」を設立しました。本ワーキンググループでは、脆弱性調整や CNA（CVE Numbering Authority）についての情報共有や、アジア太平洋地域における脆弱性調整フレームワークの構築など脆弱性調整に関するさまざまな課題への取り組みが行われる予定です。

2.1.5. CNA としての活動

JPCERT/CC では、CVE Program の活動に協力し、国際的な脆弱性情報流通に資する上で、CNA として CVE ID の採番を行うことや、国内の製品開発者をスコープとする Root として活動を行っています。
JVN での脆弱性情報の公表に際しては 2008 年 5 月以降、他の CNA が採番するケースを除いて、CVE ID を付与しています。本四半期は、JVN で公表したものに 73 個の CVE 番号を付与しました。
CNA および CVE に関する詳細は、次の Web ページをご参照ください。

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

CVE Numbering Authorities
https://www.cve.org/PartnerInformation/Partner#CNA

About CVE
https://www.cve.org/About/Overview

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

(1) 横河電機が JPCERT/CC を Root とした CNA に

JPCERT/CC は日本国内の組織を対象スコープとした Root として、候補組織の勧誘やトレーニングなどを通じた CNA 作成活動を行っています。2023 年 10 月 24 日（米国時間）には、横河電機株式会社が JPCERT/CC を Root とした CNA として、新たに CVE Program に加わることになりました。これにより JPCERT/CC を Root とした CNA は計 8 組織となります。

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/

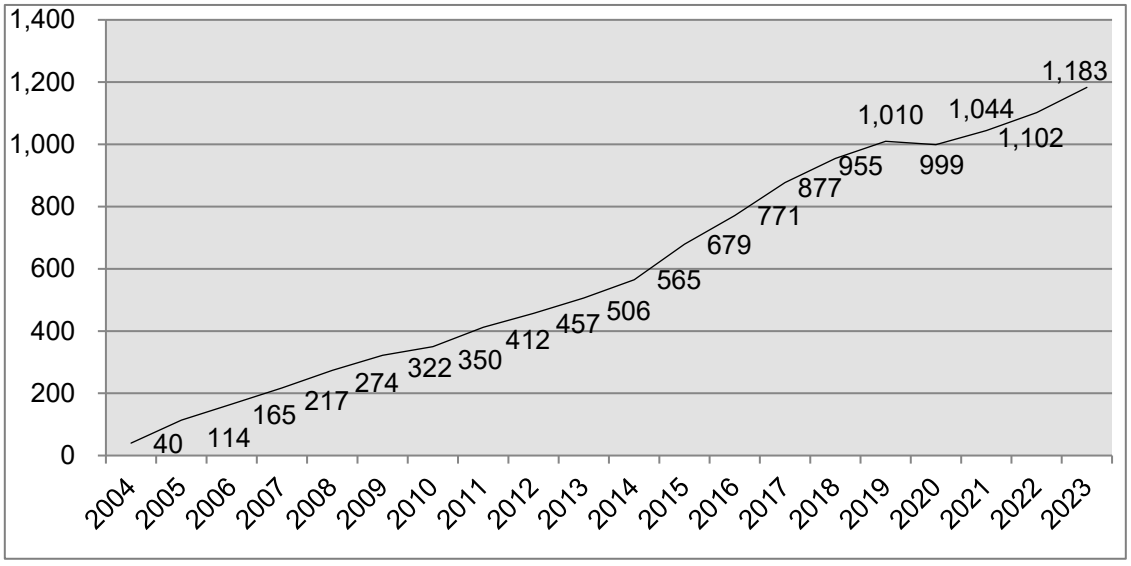
情報セキュリティ早期警戒パートナーシップガイドライン（2019 年版第 2 刷）
https://www.jpcert.or.jp/vh/partnership_guideline2019_r2.pdf

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、脆弱性情報の提供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 2-2］に示すとおり、2023 年 12 月 31 日現在で 1,183 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などを精査し、廃業や活動終了など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が反映されています。登録などの詳細については、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 2-2：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等の実施

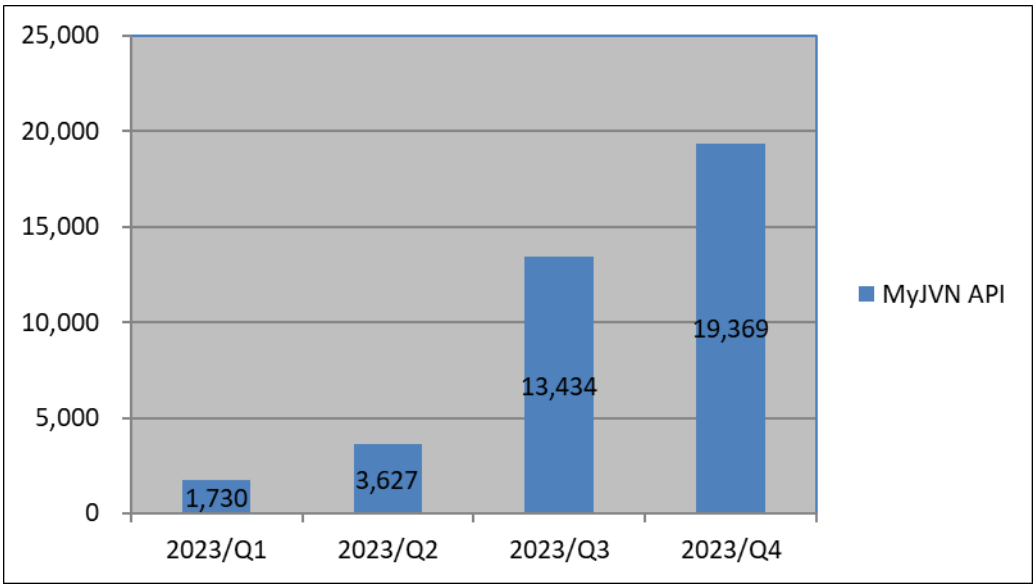
JPCERT/CC では、技術情報や脆弱性の動向などの情報交換や、脆弱性情報流通業務に関する製品開発者との意見交換、また、製品開発者間の情報交換を目的として、脆弱性情報流通の活動にご協力いただいている製品開発者の皆さまとの定期ミーティングや特定のテーマに関する個別ミーティングを開催しています。
本四半期においては、製品開発者登録ベンダー全体を対象とした定期ミーティングを 12 月 15 日に、主会場を京都に設け Web 会議とのハイブリッド形式で開催しました。関西地域を拠点とする製品開発者の PSIRT 担当者に多数お集まりいただき、他地域から Web 会議で参加いただいた製品開発者とあわせて意見交換を行いました。当日は、製品脆弱性を悪用する攻撃活動の観測状況の説明、SBOM に関する動向の紹介、さまざまな脆弱性評価指標（SVCC、CVSS v4.0、EPSS）についての説明、サプライチェーンを通じて複数の製品開発者に影響する脆弱性のコーディネーションにおける問題についての課題提起、製品開発者による PSIRT 活動の紹介、RFC1996 と security.txt についての説明、製品開発者による自社製品の脆弱性報告の手順紹介を行い、これらの議題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

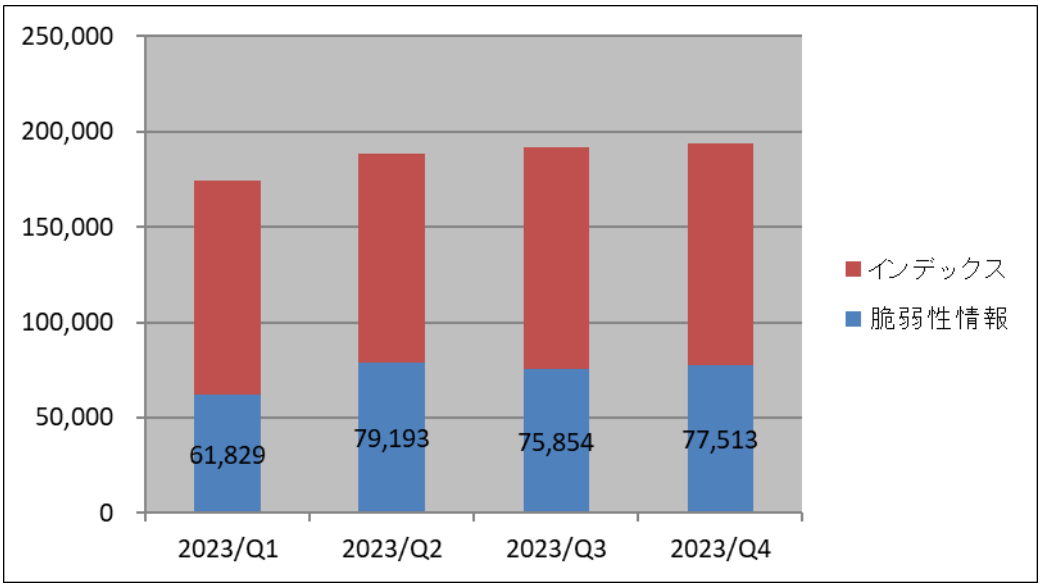
JPCERT/CC は、大規模組織の組織内 CSIRT などでの利用を想定して、ツールを用いた体系的な脆弱性対応を可能とするため、IPA が運用する MyJVN API を外部データソースとして利用した VRDA（Vulnerability Response Decision Assistance）フィードによる脆弱性情報の配信を行っています。VRDA フィードについての詳しい情報は、次の Web ページをご参照ください。

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 2-3］に、VRDA フィードの利用傾向を［図 2-4］と［図 2-5］に示します。［図 2-4］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 2-5］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。

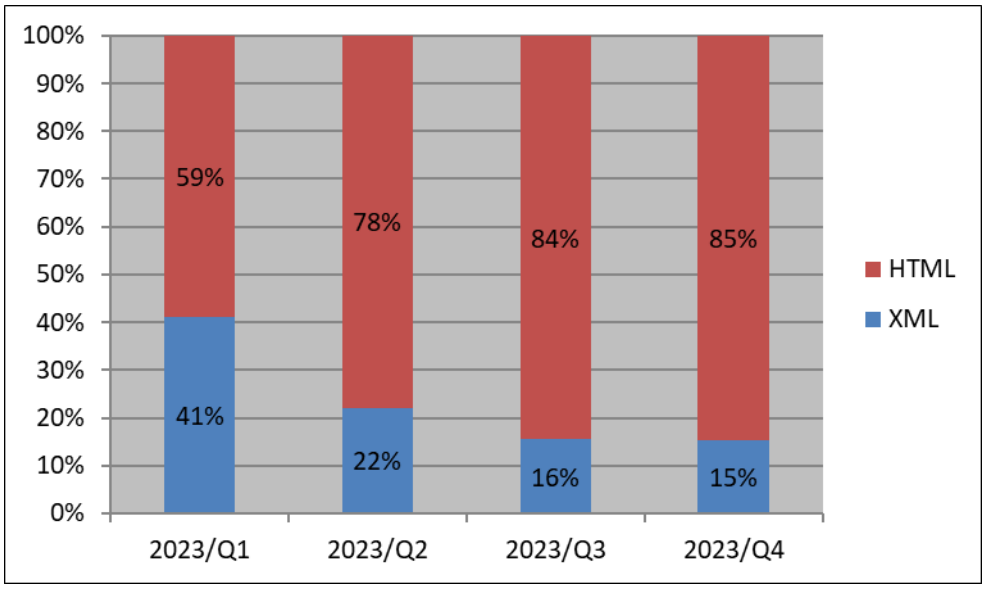


［図 2-3：VRDA フィード配信件数］



［図 2-4：VRDA フィード利用件数］

インデックスおよび脆弱性情報の利用数については、［図 2-4］に示したように、前四半期と比較し、大きな変化は見られませんでした。



［図 2-5：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 2-5］に示したように、前四半期と比較し、大きな変化は見られませんでした。

3. 制御システムに関するセキュリティ対策活動

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など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 172 件でした。

3.2. 情報提供

収集・分析した情報のうち、国内の制御システム関係者に影響があり注目すべきと判断したものを、情報に応じて適宜選んだ国内組織に「参考情報」として提供しています。

本四半期に提供した参考情報は 0 件でした。

また、2022 年度より、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「JPCERT/CC ICS Security Notes」を配信しています。

（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。

「JPCERT/CC ICS Security Notes」は、JPCERT/CC が収集した制御システムセキュリティ関連の公開情報のうち、特に着目していただきたい情報を選び、四半期にどのような動きがあったのかがわかるよう、次の形式にコンパクトにまとめたものです。

<< 1. ICS 関連の脆弱性情報 >>
- 脆弱性分析レポート（年 2 回公表予定）
  - ICS ユーザー組織の対策の参考として提供する JPCERT/CC が分析を行った ICS 関連製品の脆弱性分析レポート公表のお知らせ
- 脆弱性情報の一覧
  - JVN で公表した脆弱性情報のうち、ICS 関連製品の脆弱性情報の一覧

<< 2. ICS 関連の脅威情報 >>
- ICS 関連のインシデントやマルウェア等の脅威に関する情報

<< 3. ICS 関連のその他の情報 >>
- 調査レポートや国際標準、法規等、ICS セキュリティ対策の参考となるその他の情報

<< 4. JPCERT/CC からのお知らせ >>
- 脆弱性情報のご連絡、インシデント（セキュリティ事故）の調査やご相談などの連絡先、イベント告知等、JPCERT/CC からの各種お知らせ

<< 付録. JVN で掲載した ICS 脆弱性情報一覧>>
- JVN で公開された脆弱性情報のうち、ICS 関連製品の脆弱性情報をリスト形式で掲載

本四半期に提供した ICS Security Notes は次の 1 件でした。

2023-11-30　JPCERT/CC ICS Security Notes FY2023_#Q2

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を設けており、メーリングリストには現在 1,346 名に登録していただいています。参加資格や申し込み方法については、次の Web ページをご参照ください。

制御システムセキュリティ情報共有コミュニティー
https://www.jpcert.or.jp/ics/ics-community.html

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など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。

3.2.1. 注意喚起

本四半期に発行した注意喚起は 0 件でした。

3.2.2. 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。

3.2.3. ICS 脆弱性分析レポート

日々分析を行っている制御システム関連製品の脆弱性情報について、その分析結果を半期ごとに取りまとめ、その中から特に注目すべき情報を解説するレポートを公表する取り組みを 2021 年度から行っています。本レポートは、制御システムユーザー組織のセキュリティ担当者に向けて、制御システム関連製品の脆弱性情報を読み解く際や組織内で利用する制御システム製品の脆弱性への対応を検討する際の参考情報を提供することを目的としています。
本四半期は、2023 年度上期に公表された脆弱性情報の中から「KNX プロトコルを使用する製品に過度に制限されたアカウントロックアウトメカニズムの脆弱性（CVE-2023-4346）」に注目し、解説をしたレポートを 2023 年 11 月 30 日に公表しました。本脆弱性は、「機器にアクセスする際に使用するパスワードを設定した場合、そのパスワードを忘れてしまうとパスワードをリセットする手段がない」という、KNX プロトコルとは別にリセット機構を作り込むことを忘れていると起こり得る問題で、他の ICS プロトコルを使用する製品でも起こり得る問題です。アカウントロック機構が組み込まれた他の ICS プロトコルでも、ロックを解除する手段がないという問題を抱えている可能性があります。本レポートでは、ブルートフォース攻撃を防ぐためのアカウントロック機構が DoS 攻撃に悪用される可能性があり、さらに、ロック解除の仕組みが不適切だと DoS 攻撃の影響が長く続く、場合によっては永続する問題を、実際の脆弱性を例に説明しました。

ICS 脆弱性分析レポート ― 2023 年度上期 ―
https://www.jpcert.or.jp/ics/ics-vuls-analysis-report.html

3.3. 制御システム関連のインシデント対応

JPCERT/CC では、制御システム関連のインシデント報告を受け付け、いただいた報告内容に基づいて個別の対応を実施しています。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報告への対応件数は 1 件でした。報告内容は、インターネット経由でアクセス可能な制御システム関連製品に関するもので、報告にもとづいて調査および調整を進めました。

3.4. 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。

3.5. 制御システム向けセキュリティ自己評価ツールの提供

JPCERT/CC では、制御システムの構築と運用に関するセキュリティ上の問題項目を抽出し、バランスの良いセキュリティ対策を行っていただくことを目的として、簡便なセキュリティ自己評価ツールである日本版 SSAT（SCADA Self Assessment Tool：申し込み制）や J-CLICS（制御システムセキュリティ自己評価ツール）を無償で提供しています。本四半期は、日本版 SSAT に関する利用申し込みはなく、直接配付した件数の累計は、日本版 SSAT が 292 件のままでした。

日本版 SSAT（SCADA Self Assessment Tool）
https://www.jpcert.or.jp/ics/ssat.html

J-CLICS STEP1／STEP2（ICS セキュリティ自己評価ツール）
https://www.jpcert.or.jp/ics/jclics.html

J-CLICS 攻撃経路対策編（ICS セキュリティ自己評価ツール）
https://www.jpcert.or.jp/ics/jclics-attack-path-countermeasures.html

3.6. 連載「標準から学ぶ ICS セキュリティ」6 回目の記事を公表

JPCERT/CC では、IEC 62443 シリーズという貴重な情報源を現場の方々に少しでも役立てていただくために、その中に書かれている主なセキュリティ概念を順次取り上げて紹介する「標準から学ぶ ICS セキュリティ」と題した、気軽に読んでいただける連載を 2022 年 8 月に開始しました。

本四半期においては、12 月 14 日に「サービス事業者に対するセキュリティ要件」を公表しました。本書では、ICS に関するシステムインテグレーションや保守のサービス提供事業者に対してアセットオーナーが求めるセキュリティ要件を規定した IEC 62443-2-4 について、標準化の経緯と概要、現在検討中の改訂内容の一部などについて紹介しています。これで連載記事は 6 本となりました。

標準から学ぶ ICS セキュリティ
https://www.jpcert.or.jp/ics/information07.html

4. 国際連携活動

4.1. 海外 CSIRT 構築支援および運用支援活動

海外の National CSIRT など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などを通じた CSIRT の構築・運用支援を行っています。

4.2. 国際 CSIRT 間連携

国境をまたがって発生するインシデントへのスムーズな対応などを目的に、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など、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

APCERT の Steering Committee が、10 月 30 日に電話会議を行い、今後の APCERT の運営方針など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 年次総会 2023 への参加

APCERT の年次総会およびカンファレンスが 11 月 8 日と 9 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（33 チーム）のうち JPCERT/CC を含む 20 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、CyberSecurity Malaysia（マレーシア）、Sri Lanka CERT|CC（スリランカ）および JPCERT/CC がいずれも再選されました。議長チームおよび副議長チームの改選では、KrCERT/CC（韓国）が議長チームに、CyberSecurity Malaysia（マレーシア）が副議長チームにそれぞれ新たに選出されました。また、JPCERT/CC は事務局

に再選されました。JPCERT/CC は引き続き APCERT の事務局および Steering Committee メンバーとしてさまざまな活動をリードしてまいります。

4.2.2. 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、毎月のオンラインによる理事会に参加しました。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. 海外 CSIRT 等の来訪および往訪

4.3.1. ウズベキスタン UZCERT への訪問（10 月 2 日）

ウズベキスタンの UZCERT を訪問し、活動の状況についてヒアリングを行うとともに、今後の協力について意見交換を行いました。

4.3.2. シンガポール Cyber Security Agency の来訪（11 月 7 日）

シンガポールの Cyber Security Agency（CSA）の来訪に対応し、活動の状況についてヒアリングを行うとともに、今後の協力について意見交換を行いました。

4.4. その他国際会議への参加

4.4.1. Cyber Security Summit - Central Eurasia 2023 への参加（10 月 3 日）

ウズベキスタンの National Cyber Security Centre が主催するサイバーセキュリティに関する国際会議 Cyber Security Summit - Central Eurasia 2023 がウズベキスタンの首都タシケントで 10 月 3 日と 4 日に開催されました。JPCERT/CC は CSIRT、SOC、サイバーセキュリティセンターで提供すべきサービスや業務を整理する際に活用できるフレームワークについて講演を行いました。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。

Cyber Security Summit - Central Eurasia 2023
https://www.cybersecuritycentraleurasia.com/

世界の CSIRT から ～ウズベキスタン、モンゴル～
https://blogs.jpcert.or.jp/ja/2023/12/csirt-uz-mn.html

［図 4-1：イベントでの講演の様子］

4.4.2. MNSEC2023 への参加（10 月 5 日）

モンゴルの MNCERT/CC が主催するサイバーセキュリティカンファレンス MNSEC2023 が、モンゴルの首都ウランバートルで 10 月 5 日に開催されました。JPCERT/CC は、サイバーセキュリティにおける CSIRT の役割とその変遷に関する講演を行いました。
JPCERT/CC ではこの会議をモンゴルのサイバーセキュリティ専門家との関係強化を図る重要なイベントと捉えており、MNSEC が初めて開催された 2014 年以来、何度か講演してきました。今年の MNSEC カンファレンス会場に隣接した CTF 会場ではモンゴルの若手技術者が腕を競っており、またベンダーによるブースも立ち並んでいて、セキュリティコミュニティーの活動が充実していることを実感しました。
JPCERT/CC による講演は CSIRT やセキュリティ対策組織を構築する際にフレームワークを使用することの重要性を訴えるもので、会場からは技術的詳細などについて熱心な質問が寄せられました。

4.4.3. 日 ASEAN サイバーセキュリティ官民共同フォーラムへの参加（10 月 5～6 日）

日本政府が主催する「日 ASEAN サイバーセキュリティ官民共同フォーラム」が 10 月 5 日と 6 日に東京で開催されました。これは日 ASEAN 友好協力 50 周年を記念し、サイバーセキュリティ分野における日本と ASEAN 諸国との国際的な連携・取組を強化することを目的とした国際会議です。JPCERT/CC はインシデント対応における課題についてのパネルに登壇し、サイバー脅威の現状やそれをとりまく CSIRT の対応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。

日 ASEAN サイバーセキュリティ官民共同フォーラム
https://asean-cbp.org/ic-ajcc-program-jp/

4.4.4. IGF2023 への参加（10 月 8～12 日）

国連が主催する世界最大規模のインターネットガバナンスに関する国際会議 Internet Governance Forum（IGF）が 10 月 8 日から 12 日にかけて京都で開催されました。IGF とは、インターネットガバナンスに関して、国連加盟国をはじめとする政府や政府系組織だけでなく、民間セクター、技術コミュニティー、市民社会など、あらゆる立場のステークホルダーが一堂に会して対話するために設けられた、国連が主催する国際会議です。IGF2023 では 5 日間に 355 のセッションが行われ、178 カ国から 9,279 人が参加したと発表されています。
JPCERT/CC は「CSIRTs: A Global Dialogue with Cyber Incident Responders」ならびに「Meeting Spot for CSIRT Practitioners: Share Your Experiences」という 2 つのセッションでオーガナイザー（運営と進行）を務めました。国境を超えたグローバルな連携が欠かせない CSIRT コミュニティーの役割や現在の課題について、講演者や聴講者と意見交換を行い、サイバー空間における CSIRT の存在をさまざまな関係者（ステークホルダー）が参加する IGF の場でアピールしました。またそれ以外に 3 つのパネルディスカッションに登壇しました。
JPCERT/CC には、インターネット空間のグローバルな取り決め、仕組みや実施体制について、サイバーセキュリティを推進する立場からの意見を発信すること、またコーディネーションセンターとして適切な情報を必要な人々に届けることといった組織の使命があります。私たちはこれまで IGF に継続的に参加し、インターネットガバナンスの議論を国内外に紹介するだけでなく、関係組織が運営するセッションに招かれて登壇してきました。今回は登壇だけでなく、自らセッションを提案し、運営と進行まで行った点がこれまでとの最も大きな違いです。とりわけワークショップは過去最高の応募数（398 本）の中から約 5 倍の倍率をくぐり抜けて採択されました。

イベントに関する詳細は、次の Web ページをご参照ください。

IGF 2023
https://www.intgovforum.org/en/content/igf-2023

JPCERT/CC Eyes: 国連 IGF2023 にて 2 つのセッションの運営と進行を務めました
https://blogs.jpcert.or.jp/ja/2023/12/igf2023.html

［図 4-2：IGF セッションの様子］

4.4.5. GC3B への参加（11 月 29～30 日）

サイバーセキュリティの能力向上支援に関する国際会議 Global Conference on Cyber Capacity Building（GC3B）がガーナのアクラで、11 月 29 日と 30 日に開催されました。JPCERT/CC は AfricaCERT が主催する CSIRT の国際連携に関するパネルに登壇し、JPCERT/CC の活動や、APCERT を通した地域での連携などについて紹介しました。また、欧州連合の関係者が主催する、サイバーセキュリティ対応の規制についてのパネルに登壇し、日本におけるインシデント対応のベストプラクティスや課題を述べました。
GC3B は米国の国務省、世界銀行、サイバーピースインスティテュートなどがサポートする新しい会議です。サイバーレジリエンスに関するキャパビルについてグローバルな情報共有を図るという目的で、この度発足され、今回が初回会合になります。会議ではアクラ宣言とよばれる共同文書がガーナ大統領によって発表されました。次回は 2025 年 5 月にスイスで開催されることが決まっています。

GC3B の詳細については、次の Web ページをご参照ください。

Global Conference on Cyber Capacity Building
https://gc3b.org/

［図 4-3：GC3B の様子］

4.5. 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）で検討されている標準化作業の一部と、WG4（セキュリティコントロールとサービスに関する標準化を担当）で検討されているインシデント管理に関する標準の改定に、情報処理学会の情報規格調査会を通じて参加しています。
本四半期は、WG4 で作業中の「インシデント管理に関する標準（ISO/IEC 27035）」の新しいパート（パート 4（コーディネーション））の作成について、現在 DIS ステージにある文書に対する日本からの回答処理作業に協力しました。

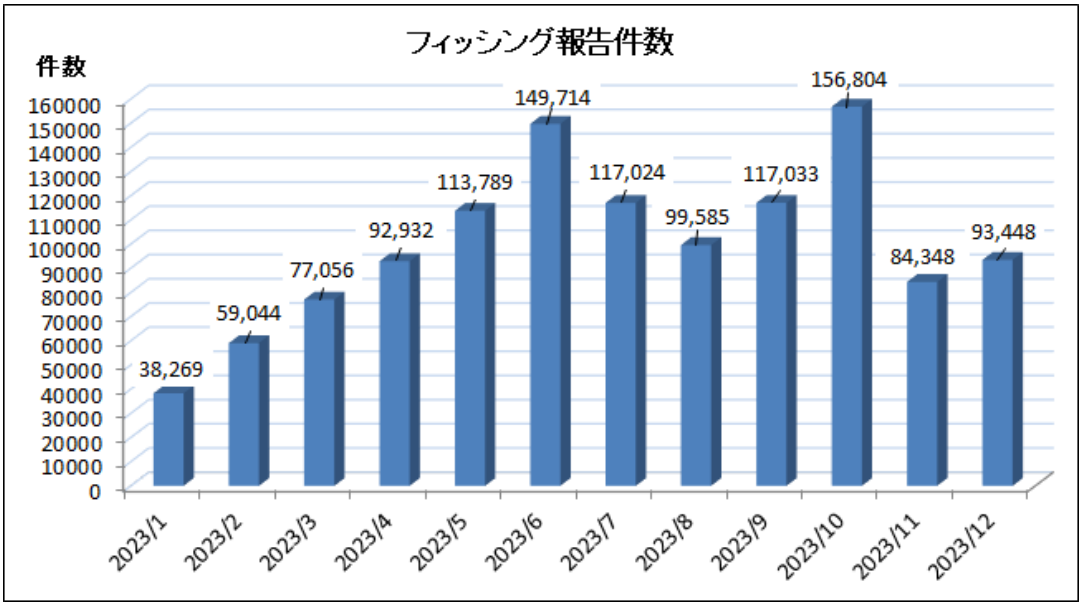
5. フィッシング対策協議会事務局の運営

フィッシング対策協議会（本節において、以下「協議会」という。）は、フィッシングに関する情報収集・提供と動向分析、技術・制度的対応の検討など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など、一部のワーキンググループの運営などを行っています。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、フィッシングサイトを停止するための調整などを行っています。

5.1. フィッシングに関する報告・問い合わせの受付

フィッシング報告件数は、10 月に過去最高の報告件数を記録し、その後も多数の報告を受けました。



［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最も多く、全体の約 30.0%を占めています。ついで、「ETC サービス」をかたるフィッシングの報告も多く、全体の約 27.0%を占めていました。

5.2. 情報収集／発信

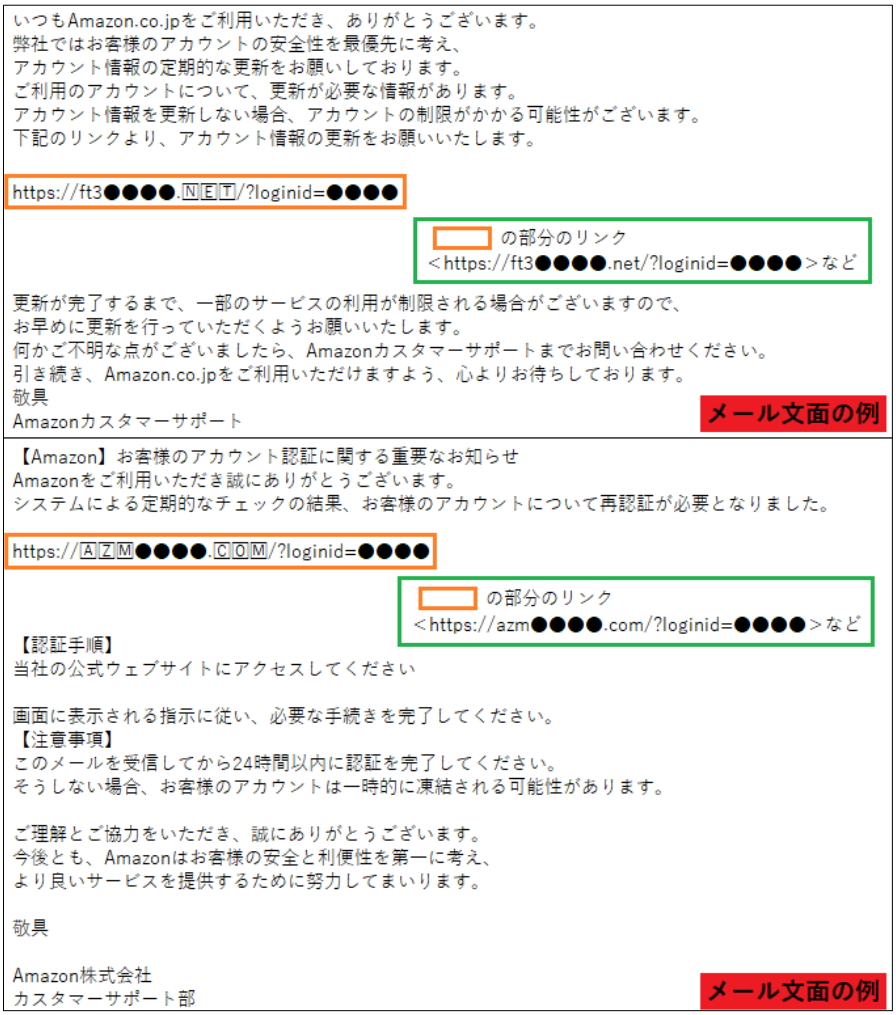
5.2.1. フィッシングの動向等に関する情報発信

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緊急情報を計 10 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。

- セディナカードをかたるフィッシング：1 件
- URL に飾り文字などが含まれたフィッシング：1 件
- MyJCB 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
- URL に特殊な IP アドレス表記を用いたフィッシング：1 件
- マイナポータル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
- S/MIME 電子署名ファイルが添付されたフィッシング：1 件

本四半期の報告件数は、10 月に過去最高件数を記録した後に、次の 2 カ月間は減少するものの引き続き多数の報告を受け付けました。
セキュリティ機構による検知の回避を目的としていると考えられる URL に飾り文字を使用したケース（[図 5-2]）や、特殊な表記の IP アドレスを含む URL を用いたものなど、本四半期もさまざまな手段を用いてフィッシングメールを受信させようとする試みを確認しました。
また、メールを開封させるために偽の S/MIME 署名ファイル「smime.p7s」を添付したフィッシングメールが報告されました（[図 5-3]）。これは、S/MIME 検証ができないメーラーで、署名されたメールを受信した場合に電子署名を添付ファイルの形で表示する動作を模倣したものであり、ユーザーが署名付きの正規のメッセージであると誤認して開封することを狙っています。「smime.p7s」が添付されている場合は正規メールであると説明している事業者もいますが、こうした事例が出現する中では見直しが必要です。



［図 5-2：URL に飾り文字などが含まれたフィッシングメールの例 ］

https://www.antiphishing.jp/news/alert/decourl_20231017.html

［図 5-3：S/MIME 電子署名ファイルが添付されたフィッシングメールの例 ］

https://www.antiphishing.jp/news/alert/myna_20230911.html

5.2.2. 定期報告

報告されたフィッシングサイト数を含む、毎月の活動報告などを協議会の Web サイトで次のとおり公開しています。

協議会 Web ページ
https://www.antiphishing.jp/

協議会 Web ページ
https://www.antiphishing.jp/

2023 年 10 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/202310.html

2023 年 11 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/202311.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などである協議会の会員などに対し、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 56 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、協議会の会員を中心とする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。
本四半期は、2024 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、法制度の整備状況などについて情報共有しつつ、事業者および一般消費者が講ずべきフィッシング対策などについて議論しました。

- 技術・制度検討ワーキンググループ会合（第 3 回）
  日時：2023 年 10 月 31 日（火）15:00-17:30
- 技術・制度検討ワーキンググループ会合（第 4 回）
  日時：2023 年 12 月 1 日（金） 10:00-12:00

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・運営方針の決定などを行う運営委員会を次のとおり開催しました。

- 第 112 回運営委員会（オンライン）
  2023 年 10 月 19 日（木）16:00 - 18:00

- 第 113 回運営委員会（オンライン）
  2023 年 11 月 16 日（木）16:00 - 18:00

- 第 114 回運営委員会（オンラインおよび JPCERT/CC 会議室）
  2023 年 12 月 21 日（木）16:00 - 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などの会合の開催を支援しました。

- 学術研究ワーキンググループ会合
  日時：10 月- 12 月　毎週火曜日 9：00 - 9：30（オンライン）

- 証明書普及促進ワーキンググループ会合
  日時：11 月 17 日　16：00 - 18：00（オンラインおよび JPCERT/CC 会議室）

- 被害情報共有ワーキンググループ　ワークショップ＋Tea Party 開催
  日時：10 月 2 日　13：00 - 17：00（株式会社マクニカ 品川オフィス）

- フィッシング対策セミナー2023（オンライン）
  日時：11 月 10 日（金）10：00 - 17：30

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、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、および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。

2023-10-17
JPCERT/CC インシデント報告対応レポート［2023 年 7 月 1 日～2023 年 9 月 30 日］
https://www.jpcert.or.jp/pr/2023/IR_Report2023Q2.pdf

2023-12-14
JPCERT/CC Incident Handling Report [July 1, 2022 - September 30,2022]
https://www.jpcert.or.jp/english/doc/IR_Report2023Q2_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と照らし合わせて、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。

2023-10-31
JPCERT/CC インターネット定点観測レポート［2023 年 7 月 1 日～2023 年 9 月 30 日］
https://www.jpcert.or.jp/tsubame/report/report202307-09.html
https://www.jpcert.or.jp/tsubame/report/TSUBAME_Report2023Q2.pdf

2023-12-14
JPCERT/CC Internet Threat Monitoring Report [July 1, 2022 - September 30,2022]
https://www.jpcert.or.jp/english/doc/TSUBAMEReport2023Q2_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。

2023-10-19
ソフトウェア等の脆弱性関連情報に関する届出状況［2023 年第 3 四半期（7 月～9 月）］
https://www.jpcert.or.jp/pr/2023/vulnREPORT_2023q3.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：6 件　https://blogs.jpcert.or.jp/ja/

2023-10-25　フィッシングサイト経由の認証情報窃取とドメイン名ハイジャック事件
2023-10-31　TSUBAME レポート　Overflow（2023 年 7～9 月）
2023-11-10　RFC 9116「security.txt」の紹介（2022 年 8 月）の続報
2023-12-05　国連 IGF2023 にて 2 つのセッションの運営と進行を務めました
2023-12-05　サイバー攻撃被害に係る情報の意図しない開示がもたらす情報共有活動への影響について
2023-12-19　世界の CSIRT から ～ウズベキスタン、モンゴル～

英語版発行件数：2 件 https://blogs.jpcert.or.jp/en/

2023-11-07　Credential Theft and Domain Name Hijacking through Phishing Sites
2023-12-14　TSUBAME Report Overflow (Jul-Sep 2023)

8. 主な講演活動

(1) 佐々木 勇人（政策担当部長兼早期警戒グループマネージャー 脅威アナリスト）：
「最近のインシデント対応現場の情勢から見えてくるサイバー攻撃対策の注意点について」
第 32 回クレジットセプター運営会議（主催：日本クレジット協会、講演日：2023 年 10 月 2 日）

(2) 宮地 利雄（技術顧問）：
「プラントやインフラの制御システムへのサイバー攻撃事例と防御対策」
SICE 九州フォーラム（主催：計測自動制御学会、講演日：2023 年 10 月 13 日）
(3) 小宮山 功一朗（国際部部長）：
「One Internet という思想の行き詰まり。では、いくつに分割すればよいのだろうか？」
Security Days Fall 2023（主催：ナノオプト・メディア、講演日：2023 年 10 月 19 日）
(4) 佐々木 勇人（政策担当部長兼早期警戒グループマネージャー 脅威アナリスト）：
「『能動的サイバー防御』で何ができるようになるのか、何に備えるか」
JPRS ユーザー会 意見交換会（主催：JPRS ユーザー会、講演日：2023 年 10 月 20 日）
(5) 佐々木 勇人（政策担当部長兼早期警戒グループマネージャー 脅威アナリスト）：
「脆弱性を悪用する事案に関する情報を巡る課題～『サイバー攻撃被害に係る情報の共有・公表ガイダンス』から～」
組込みシステムセキュリティ委員会（主催：組込みシステム技術協会、講演日：2023 年 11 月 9 日）
(6) 佐々木 勇人（政策担当部長兼早期警戒グループマネージャー 脅威アナリスト）：
「被害公表が新たな“被害”にならないための被害公表の在り方について」
官民連携ネットワーク合同協議会（主催：栃木県警察本部警備部警備第一課、講演日：2023 年 11 月 10 日）
(7) 横井 逸人（早期警戒グループ 脅威アナリスト）：
「教育機関におけるサイバーセキュリティ」
令和 5 年度情報セキュリティセミナー（主催：筑波大学情報環境機構、講演日：2023 年 11 月 16 日）
(8) 輿石 隆（早期警戒グループ 脅威アナリスト）：
「コーディネーションセンターというお仕事」
InternetWeek2023「セキュリティの仕事、どんなことをしているの？どうしたらなれるの？」
（主催：日本ネットワークインフォメーションセンター、講演日 2023 年 11 月 17 日）
(9) 田中 信太郎（インシデントレスポンスグループリーダー インシデントコーディネーター）：
「abuse 窓口への連絡」
InternetWeek2023「Abuse 対応の理論と実践 ～abuse 対応はじめの 1 歩～」（主催：日本ネットワークインフォメーションセンター、講演日 2023 年 11 月 17 日）
(10) 佐條 研（インシデントレスポンスグループリーダー マルウェアアナリスト）：
「近年の標的型攻撃の手口の変化と課題」
NANO OPT Media Online セミナー（主催：ナノオプト・メディア、配信日：2023 年 11 月 22 日～2023 年 12 月 20 日）
(11) 戸田 洋三（早期警戒グループ シニアテクニカルリード）：
「脆弱性対応からセキュア開発へ　JPCERT/CC の経験から」
ソフトウェア品質向上セミナー（主催：テクマトリックス、講演日：2023 年 12 月 1 日）
(12) 小宮山 功一朗（国際部部長）：
「最新の脅威動向から情報共有・被害公表の課題を再考する」
Security Summit' 23（主催：グーグル・クラウド・ジャパン、講演日：2023 年 12 月 13 日）

9. 協力、後援

本四半期は次の行事の開催に協力または後援などを行いました。

(1) Cybersecurity Awards 2023
（主催：デジタル制作フォーラム、応募期間：2023 年 11 月 1 日～2023 年 12 月 31 日、表彰：2024 年 3 月）
(2) 第 20 回デジタル・フォレンジック・コミュニティ 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／デジタル・フォレンジック・コミュニティ 2023 実行委員会、開催日：2023 年 12 月 4 日～2023 年 12 月 5 日）
(3) Security Management Conference 2023 Winter
（主催：SB クリエイティブ、開催日：2023 年 12 月 13 日～2023 年 12 月 14 日）

■インシデントの対応依頼、情報のご提供　：info@jpcert.or.jp
　　：https://www.jpcert.or.jp/form/
■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