JPCERT/CC 活動四半期レポート

2024 年 10 月 1 日～2024 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

2025 年 1 月 23 日

JPCERT CC®

目次

本活動は、経済産業省から委託を受け、「 令和 6 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、「3. 国内連携活動」「4. 国際連携活動」「8. その他の活動」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

2024 年度の JPCERT/CC ベストレポーター賞を贈呈

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皆さまは、JPCERT/CC が問題解決に向けて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、かつ問題が複雑化・高度化している現状においては、皆さまからの情報提供のご協力を得て、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に各賞を贈呈しています。

4 回目となる本年度は次の方にベストレポーター賞をお贈りしました。

株式会社マルスジャパン　力 美有樹 様（インシデント報告部門）

力様は、長年にわたってフィッシングサイトの調査活動をされており、稼働中のフィッシングサイトへの対応につながる詳細な分析を含む質の高い報告を多数いただきました。また、JPCERT/CC が運営するコミュニティーにおいても継続的に活動され、調査や分析等に関する有益な情報を共有いただきました。

春山 敬宏 様（脆弱性報告部門）

春山様は、ご自身が発見され報告いただいた脆弱性情報について、JPCERT/CC が海外を含む複数の製品開発者との調整を行うにあたり、それぞれの製品に応じた技術情報を提供され製品開発者の修正対応を支援いただきました。長期間に及ぶ調整にも粘り強く対応いただき、結果として複数の製品開発者による公表とご自身による発見者としての公表を同期して行うことができ、脆弱性調整における CVD（Coordinated Vulnerability Disclosure）の観点で模範的なケースの一つとなりました。また、JVN に掲載した当該脆弱性に関する技術解説（テクニカルアドバイザリ）も共同で執筆いただきました。

今回の受賞者をはじめ、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 2024
  https://www.jpcert.or.jp/award/best-reporter-award/2024.html

製品開発者間の情報交換のための定期ミーティングを名古屋で開催

JPCERT/CC では、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。ミーティングには国内のさまざまな業種・業態の製品開発者が参加され、製品脆弱性に関連する技術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。また、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な良好な関係を構築する場となることをも期しています。

前年度から、地方に拠点を置く製品開発者と直接対話する機会として東京以外でもミーティングを開催しています。本年度は 12 月 12 日に名古屋市内の会場を主会場としてハイブリッド形式で実施しました。主会場には東海地域だけでなくその他の地域を拠点とする製品開発者からも多数の PSIRT 担当者にお集まりいただき、Web 会議で参加された製品開発者も交えて活発な意見交換が行われ、PSIRT 担当者同士の横連携を深める機会となりました。

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、今後もさまざまな都市を訪れてミーティングを実施し、全国各地の製品開発者との連携を深めたいと考えています。

第 1 章

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 9,743 件、インシデント件数ベースでは 5,561 件でした[*1]。

JPCERT/CC が国内外のインシデントに関連するサイトとの調整を行った件数は 3,597 件でした。前四半期の 3,331 件と比較して 8% 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/2024/IR_Report2024Q3.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 4,780 件で、前四半期の 4,233 件から 13% 増加しました。また、前年同期（4,473 件）との比較では、7% の増加となりました。

[*1] **報告件数**は、報告者から寄せられた Web フォーム、メール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。

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	合計	割合
国内ブランド	1,177	1,179	1,334	3,690	77%
国外ブランド	163	173	168	504	11%
ブランド不明	279	124	183	586	12%
全ブランド合計	1,619	1,476	1,685	4,780	

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[*2]。

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 76.2%、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 61% で、それぞれ最も多くを占めました。

国外ブランドでは、Amazon を装ったフィッシングサイトが 6 割近くを占めました。国内ブランドでは、JCB、えきねっと、PayPay を装ったフィッシングサイトが多く報告されました。また、国内金融機関に関しては、JCB の他にアイフル、イオンカードを装ったフィッシングサイトが多く報告されました。サイトテイクダウンのために調整したフィッシングサイトの内訳は、国内が 36%、国外が 64% で、前四半期（国内が 36%、国外が 64%）と同じ割合でした。

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 53 件でした。前四半期の 93 件から 43% 減少しています。

本四半期は、EC サイトで商品購入時に入力したクレジットカード情報等を窃取する目的で、Web サイトを改ざんする事例を多数（19 件）確認しました。これは、2021 年に JPCERT/CC がブログで報告した 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事例と類似しており、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ました。

- JPCERT/CC Eyes「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」
  https://blogs.jpcert.or.jp/ja/2021/07/water_pamola.html

1.1.2 インシデント対応事例

本四半期に行った対応の例を紹介します。

[*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。

図 1.1 ユーザーの情報窃取を狙った JavaScript のコード

1.1.2.1 Ivanti Virtual Traffic Manager の脆弱性により侵害された可能性がある国内機器への通知

海外のセキュリティ組織から、Ivanti Virtual Traffic Manager の脆弱性（CVE-2024-7593）を悪用されて侵害を受けた可能性がある、日本国内の機器の IP アドレスが複数提供されました。

当該脆弱性については、対象となる機器を検索する方法と実証コードが公開されており、被害を受けた機器には特定の管理者ユーザーが作成されている可能性がありました。

JPCERT/CC では、IP アドレスを管理する組織に対して、機器に不正なアカウントが作成されていないか調査し、対策としてパッチの適用を検討するよう依頼しました。その結果、連絡が取れた組織から、不正なアカウントが存在しており削除した旨の返信を受領しました。

1.1.3 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・提供

JPCERT/CC は、インシデントなどによる被害の発生や拡大を防ぐために、脆弱性情報、脅威情報、セキュリティ情報などを収集・分析しています。分析の結果、インシデントなどによる被害の発生や拡大に対する蓋然性が高まったと判断した場合、「注意喚起」や「早期警戒情報」などの警戒情報やインシデントへの対処・対策のための情報提供を行っています。

1.2.1 情報収集・分析

JPCERT/CC が収集・分析する情報には、自ら収集した情報に加え、各地域や組織の CSIRT など関係機関を含む国内外の関連組織から受けた情報も含まれます。それらをもとに、サイバー攻撃で使われた脆弱性や攻撃手法、マルウェアなど、インシデントの発生や拡大につながる可能性がある情報について分析を行っています。

また、JPCERT/CC が提供した情報に対する各組織からのフィードバック情報を集計し、国内での影響把握と更なる情報の分析に役立てています。特に、早期警戒情報などを提供する Web ポータル「CISTA（Collective Intelligence Station for Trusted Advocates）」（1.2.3 参照）を介した各組織からのフィードバックは、他組織へも展開するなど有効活用しています。

本四半期に収集した情報またはいただいたフィードバックのうち、特徴的なものを紹介します。

1.2.1.1 Fortinet 製 FortiManager における重要な機能に対する認証の欠如の脆弱性（CVE-2024-47575）

10 月 24 日、JPCERT/CC は FortiManager における重要な機能に対する認証の欠如の脆弱性（CVE-2024-47575）等に関する注意喚起を発行しました。以降、海外のパートナー組織からの情報提供や国内組織からのフィードバックをもとに、同脆弱性を悪用する攻撃に関する情報を、随時注意喚起に追記しました。さらに、11 月 15 日には同脆弱性の詳細を解説する情報、および、本脆弱性を実証するコード（Proof-of-Concept）などが公開されたことが判明したため、これらの情報を追記して注意喚起を更新し、警戒を呼びかけました。

1.2.1.2 Palo Alto Networks 製 PAN-OS の管理インタフェースにおける複数の脆弱性（CVE-2024-0012、CVE-2024-9474）

11 月 19 日、JPCERT/CC は、Palo Alto Networks 製 PAN-OS の管理 Web インタフェースにおける複数の脆弱性（CVE-2024-0012、CVE-2024-9474）を悪用する攻撃活動に関する情報を公開しました。注意喚起を発行した時点では、同脆弱性は限定的な攻撃で悪用されていると同社は公表していましたが、その翌日には、脆弱性の詳細を解説する情報が公開されたほか、その後新たに観測された攻撃活動を追跡していることが公表されました。JPCERT/CC は国内外の組織と連携し、同脆弱性の影響を受ける可能性があるホストや、すでに脆弱性を悪用する攻撃の被害を受けた可能性があるホストを調査し、被害の未然防止や最小化のため、影響を受けるホストの管理組織に対して個別に通知しました。

1.2.2 Web サイトでの情報提供

JPCERT/CC は、Web サイトで「注意喚起」「CyberNewsFlash」「Weekly Report」などの情報を公開しています。 RSS フィードを提供するとともに、メーリングリストの登録者（本四半期末時点で約 43,100 名）には一部の情報をメールでも配信しています。

1.2.2.1 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、10 件（うち更新情報が 4 件）発行しました。

- JPCERT/CC 注意喚起
  https://www.jpcert.or.jp/at/

2024-10-09 2024 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)

2024-10-24 Fortinet 製 FortiManager における重要な機能に対する認証の欠如の脆弱性（CVE-2024-47575）等に関する注意喚起 (公開)

2024-10-25 Fortinet 製 FortiManager における重要な機能に対する認証の欠如の脆弱性（CVE-2024-47575）等に関する注意喚起 (更新)

2024-11-01 Fortinet 製 FortiManager における重要な機能に対する認証の欠如の脆弱性（CVE-2024-47575）等に関する注意喚起 (更新)

2024-11-13 2024 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)

2024-11-15 Fortinet 製 FortiManager における重要な機能に対する認証の欠如の脆弱性（CVE-2024-47575）等に関する注意喚起 (更新)

2024-11-19 Palo Alto Networks 製 PAN-OS の管理インタフェースにおける複数の脆弱性（CVE-2024-0012、CVE-2024-9474）に関する注意喚起 (公開)

2024-11-20 Palo Alto Networks 製 PAN-OS の管理インタフェースにおける複数の脆弱性（CVE-2024-0012、CVE-2024-9474）に関する注意喚起 (更新)

2024-12-11 2024 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)

2024-12-11 Adobe Acrobat および Reader の脆弱性（APSB24-92）に関する注意喚起 (公開)

1.2.2.2 CyberNewsFlash

JPCERT/CC は、発行時点で注意喚起の基準に満たない脆弱性やマルウェア、サイバー攻撃に関する情報などを CyberNewsFlash として発信することがあります。本四半期は、1 件（うち更新情報が 1 件）発行しました。

- JPCERT/CC CyberNewsFlash
  https://www.jpcert.or.jp/newsflash/

2024-10-16 Check Point Software Technologies 社製品の VPN 機能における情報漏えいの脆弱性（CVE-2024-24919）について（更新）

1.2.2.3 Weekly Report

JPCERT/CC が収集したセキュリティ関連情報のうち重要と判断した情報の概要をレポートにまとめ、原則として毎週水曜日（各週の第 3 営業日）に Weekly Report として発行しています。本四半期は、13

件発行し、計 102 件のセキュリティ情報を提供しました。

- JPCERT/CC Weekly Report
  https://www.jpcert.or.jp/wr/

1.2.3 CISTA での情報提供

JPCERT/CC は、共有先を限定した情報共有のプラットフォーム「CISTA」を提供しています。「早期警戒情報」の受け取りを希望して申し込みいただいた方々に提供している登録制の Web ポータルで、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や組織内 CSIRT など約 1,240 組織との間で情報共有を行っています。「早期警戒情報」の枠組みに関する詳細は、次の Web ページをご確認ください。

- 早期警戒情報
  https://www.jpcert.or.jp/wwinfo/

CISTA では、JPCERT/CC が提供した情報に対して受信組織がポータル上でフィードバックの提供や返信を行うことができます。いただいたフィードバックや返信は、許された共有範囲などに応じて、他組織へも情報提供するなど還元しています。

1.2.3.1 早期警戒情報

収集した脆弱性情報や脅威情報などのうち、重要な情報インフラなどに重大な影響を及ぼす可能性があり、重要インフラなどを提供する組織に早期に共有すべきと判断したものを「早期警戒情報」として提供しています。本四半期には 2 件発信しました。

1.2.3.2 Analyst Note

収集した脆弱性情報や脅威情報などのうち、JPCERT/CC が注目すべきと考えたものを、毎日まとめて「Analyst Note」と呼ばれる情報として提供しています。本四半期には 62 件発信しました。

1.2.3.3 個別提供情報

収集した情報の中から、特定の組織に影響が及ぶと考えられる脆弱性情報および脅威情報について、個別に情報提供を行っています。例えば、深刻な脆弱性への対策を適用していない状態などの「脆弱なホスト」や、すでに脆弱性の悪用により不正プログラム設置や改ざん、認証情報が窃取されている可能性がある「侵害被疑のホスト」の利用組織などに対して情報を提供しています。なお、対象の組織へ CISTA で個別に情報を提供できない場合は、JPNIC WHOIS を利用して登録されている連絡先に通知する、あるいは ISP や保守ベンダーに通知を依頼する場合もあります。

11 月下旬、JPCERT/CC は、エンタープライズ向けの CMS である Sitecore における任意のファイル読み込みの脆弱性（CVE-2024-46938）に関する詳細情報が公開されていることを確認しました。調査の結果、CISTA の受信組織が管理するとみられるホストでも同製品が稼働している可能性があることを確認したため、CISTA で個別に通知しました。

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等を利用することにより、同様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等を把握できる場合があり、グローバルな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

1.3.1.1 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います。また、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」を四半期ごとに公開しています。本四半期は、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「TSUBAME レポート Overflow」を公開しました。

- インターネット定点観測レポート（2024 年 7〜9 月）
  https://www.jpcert.or.jp/tsubame/report/report202407-09.html
- TSUBAME レポート Overflow（2024 年 7〜9 月）
  https://blogs.jpcert.or.jp/ja/2024/11/tsubame_overflow_2024-07-09.html

1.3.1.2 TSUBAME 観測動向

日本に設置されたセンサーが観測したパケットを宛先ポートで分けた時に、本四半期の総パケット数で上位 10 位になった宛先ポートについて、日々のパケット数の増減を上位 1〜5 位と 6〜10 位とに分けて図 1.2 と図 1.3 に示します。

また、過去 1 年間（2024 年 1 月 1 日〜2024 年 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。

本四半期に最も多く観測されたパケットは 23/TCP（telnet）宛ての通信でした。10 月 10 日頃を境に、徐々に減少してきています。2 番目に多かったのは 8728/TCP 宛ての通信でした。 4 位の 22/TCP（ssh）は一時的にパケット数が増加する現象が見られ、5 位から浮上して 6379/TCP（redis）と入れ替わりました。

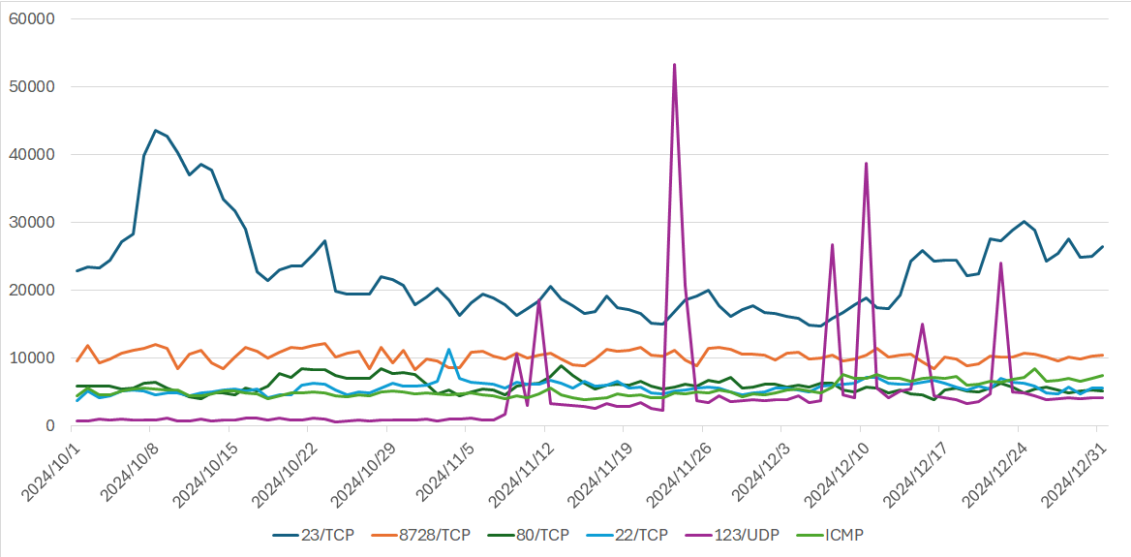

図 1.2 TSUBAME で観測された宛先ポートの上位 1 位から 5 位のパケット数
（2024 年 10 月 1 日～12 月 31 日）

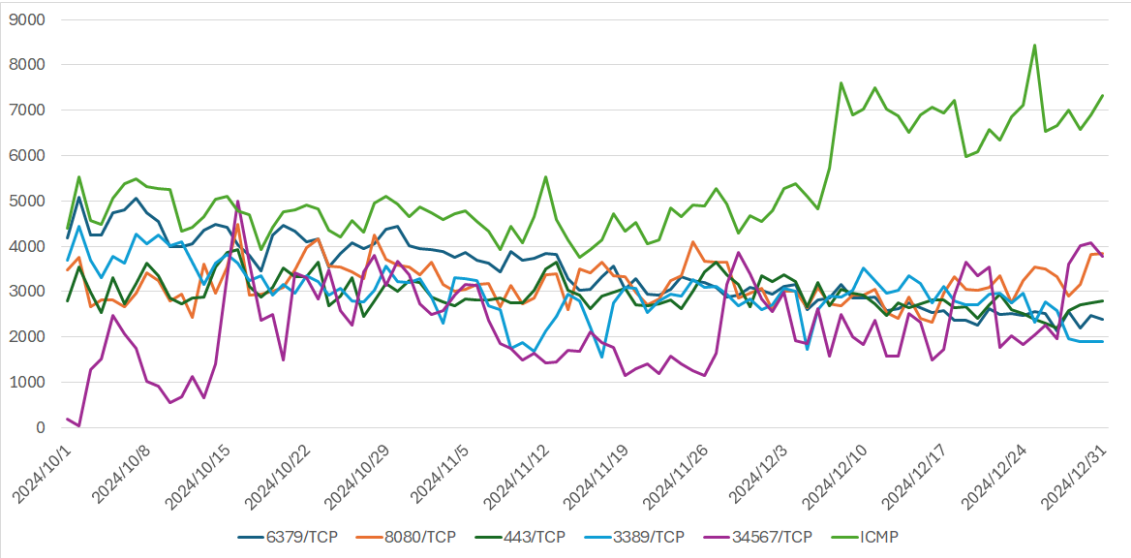

図 1.3 TSUBAME で観測された宛先ポートの上位 6 位から 10 位のパケット数
（2024 年 10 月 1 日～12 月 31 日）

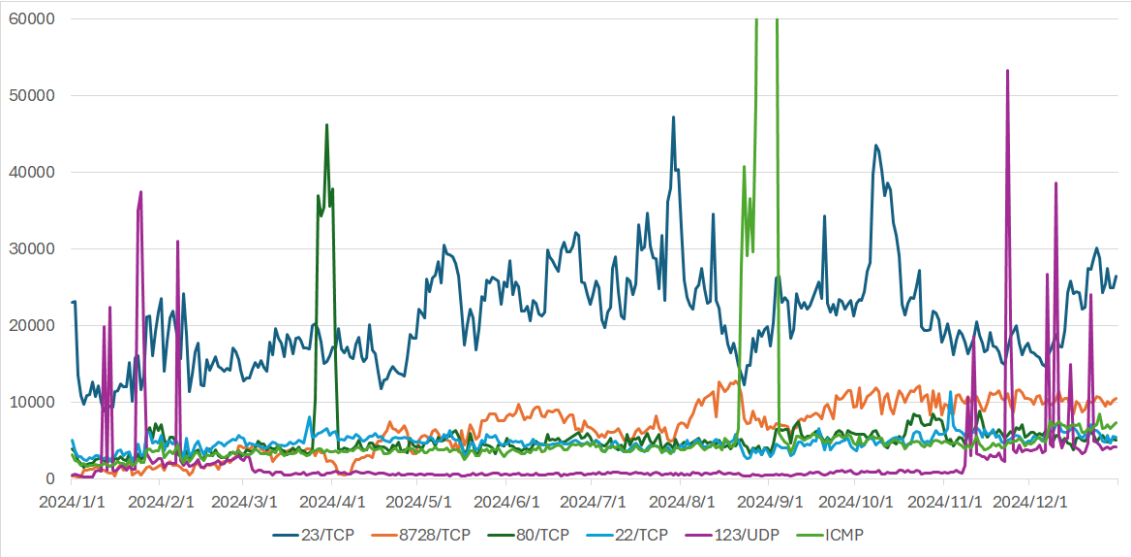

図 1.4 TSUBAME で観測された宛先ポートの上位 1 位から 5 位のパケット数
（2024 年 1 月 1 日～2024 年 12 月 31 日）

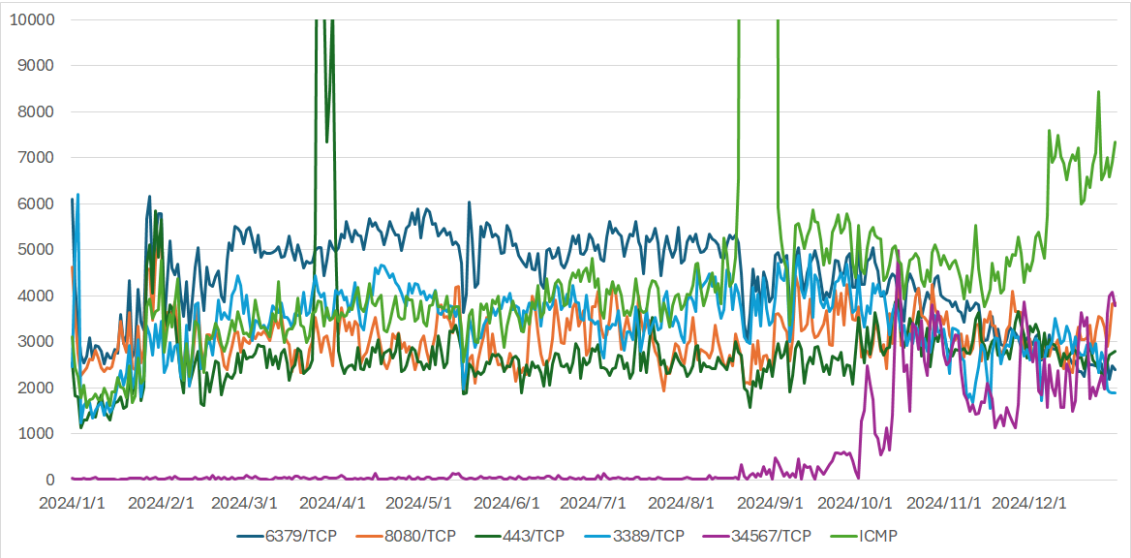

図 1.5 TSUBAME で観測された宛先ポートの上位 6 位から 10 位のパケット数
（2024 年 1 月 1 日～2024 年 12 月 31 日）

第 2 章

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、独立行政法人情報処理推進機構（IPA）と共同運営している脆弱性情報ポータル JVN（Japan Vulnerability Notes）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等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、公表されたものをカタログ化することを使命として、1999 年から専門家コミュニティーにより進められてきた国際的な活動。米国の MITRE 社が事務局を務めている）において、配下の CNA（CVE Numbering Authority、CVE 採番機関）を統括する Root の役割を担うとともに、自ら CNA 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、最終改正令和 6 年経済産業省告示第 93 号（以下、「本規程」という。））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、この規程に基づく「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 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。

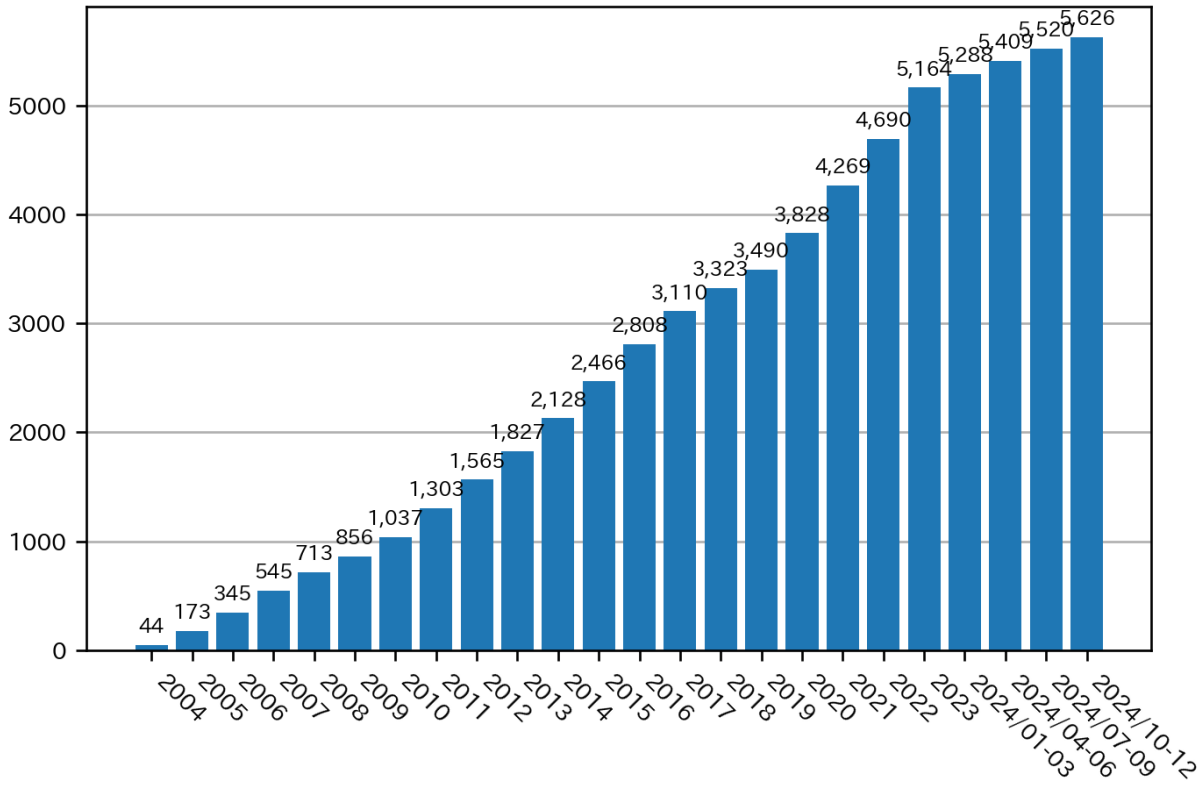

図 2.1 JVN 公表累積件数

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（「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）
- パートナーシップガイドラインを介さず、報告者、製品開発者、海外の調整機関などから連絡を受けた脆弱性情報（「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）
- 通信プロトコルやプログラミング言語標準の問題など個別の製品の脆弱性情報という範疇を超えた情報等（「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 106 件（累計 5,626 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/

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：21 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：85 件
- 脆弱性情報に関連する技術情報等に関するもの：0 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）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、特徴のあったものを紹介します。

2.1.2.1 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

- JVN#46615026
  アイ・オー・データ製ルーター UD-LT1 および UD-LT1/EX における複数の脆弱性
  https://jvn.jp/jp/JVN46615026/

株式会社アイ・オー・データ機器が提供するルーター製品 3 件の脆弱性情報に関するアドバイザリです。本件は JPCERT/CC が報告者から脆弱性報告を受け製品開発者と調整を進めている最中に、同脆弱性を悪用した攻撃が行われている可能性を確認したと製品開発者から報告を受けました。これを受け、本アドバイザリ公表時には、製品開発者同意のもと、アドバイザリの表題に「緊急」と表示し、本文中で攻撃が観測されていることを書き添えました。パートナーシップガイドラインでも触れていますが、すでに攻撃に悪用されている脆弱性を公表する場合は、攻撃の存在をアドバイザリ上で示すことで製品利用者に早期対応を促しています。また、3 件の脆弱性の修正ファームウェアは同時に提供されませんでした。すでに脆弱性が悪用されている状況を鑑み、1 件の脆弱性の修正ファームウェアの準備が整った段階で、残り 2 件についてはワークアラウンド（軽減策）を示した上でまとめてアドバイザリを公表。その後、残りの修正ファームウェアが提供された段階でアドバイザリを更新することによって攻撃の被害の軽減に努めました。このように、悪用被害拡大を抑止するため、段階的な情報公開を実施することがあります。

2.1.2.2 国際調整または独自調整で取り扱った脆弱性

- JVNVU#91741031
  CUPS における複数の脆弱性
  https://jvn.jp/vu/JVNVU91741031/

インターネット印刷プロトコル（IPP）の実装である CUPS 内の複数パッケージの脆弱性情報（入力値を適切に無害化しないために任意のコードまたはコマンド実行の可能性がある）が OpenPrinting から公開されたことを契機に、これらパッケージを利用した印刷システムなどの開発者へ周知するため、本アドバイザリを公表しました。この脆弱性は、複数の開発者の製品に継承され、それらの製品の多数の利用者が影響を受けることが懸念されたため、本アドバイザリの公表をそうした開発者にも通知し注意喚起をしました。JPCERT/CC は報告された脆弱性を解決するために開発者と協力し製品利用者に向けて

修正や対策情報を公表するだけでなく、JVN 以外で公開された脆弱性情報の影響も検討し、必要に応じて JVN でのアドバイザリ公表や開発者への連絡を行っています。このため、さまざまな脆弱性の影響や関連する開発者を正しく判断できるように日頃から開発者との連携を心がけています。本件においても、開発者への照会から CUPS 関連パッケージが広範囲に展開・利用されていることを確認できました。また、開発者からは本脆弱性情報公表に至るまでの過程が分かりづらかったなどの意見をいただき、脆弱性情報の受け手にとっては公表に至るまでに関係者がやり取りした内容や時系列も大事な情報であると認識し、何をどこまで公表するべきかなど、脆弱性調整の難しさを改めて感じる案件となりました。

2.1.3 連絡不能開発者対応

パートナーシップガイドライン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、公表判定委員会での諮問等による連絡不能開発者案件を公表するための手順（2014 年 5 月告示・ガイドライン改正）に沿って対応を行うケースがあります。 JPCERT/CC ではこの手順に基づき、該当する製品開発者名の連絡の手掛かりを広く求めるための「連絡不能開発者一覧」と、公表判定委員会で公表が妥当と判定された脆弱性を、製品利用者に向けて周知するための「Japan Vulnerability Notes JP（連絡不能）一覧」を JVN 上で公表しています。本四半期においては、「連絡不能開発者一覧」および「Japan Vulnerability Notes JP（連絡不能）一覧」の新規公表は 0 件です。

- 連絡不能開発者一覧
  https://jvn.jp/reply/
- Japan Vulnerability Notes JP（連絡不能）一覧
  https://jvn.jp/adj/

2.1.4 脆弱性調整および情報流通に関する国際的な協力体制の構築

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し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。

2.1.4.1 APCERT AGM & Conference 2024 への参加

11 月 5 日から 7 日に、アジアパシフィックの CSIRT コミュニティーが主催する APCERT AGM & Conference 2024 が台湾の台北で開催されました。本会合では、JPCERT/CC が作成した製品開発者向けのガイダンス資料をもとに、日本国内の脆弱性コーディネーションを改善する取り組みについて説明する講演を行いました。当該会合の詳細については、次の Web ページをご参照ください。

- APCERT AGM & Conference 2024, Power of Together: More Than the Sum of AP CERTs/CSIRTs.
  https://apcert2024con.org.tw/

2.1.5　CNA としての活動

JPCERT/CC では、CVE Program の活動に参加し、国際的な脆弱性情報流通において、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 として活動をしています。

JVN で公表する脆弱性情報には 2008 年 5 月以降、他の CNA が採番したケースを除き、JPCERT/CC が採番した CVE ID を付与してきました。本四半期は、54 件の脆弱性に CVE ID 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
- Overview About the CVE Program
  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

2.1.5.1　オムロン株式会社が 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等を通じた CNA の設立を促進するための活動を行っています。本四半期においては、10 月 22 日（米国時間）に、オムロン株式会社が 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。これによって JPCERT/CC を Root とした CNA は計 10 組織となりました。

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（2024 年版）
  https://www.jpcert.or.jp/vh/partnership_guideline2024.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

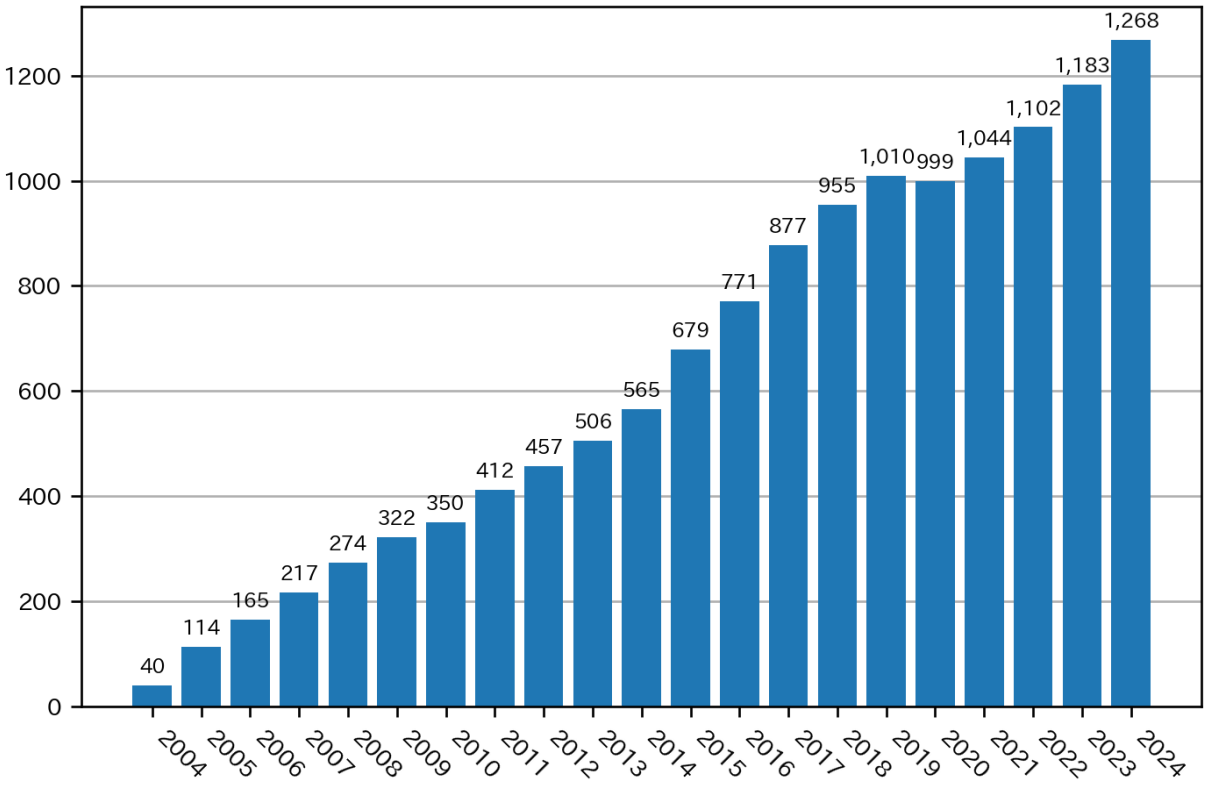

図 2.2 製品開発者登録数

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、本四半期末時点で 1,268 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

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 12 月 12 日に、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主会場を名古屋に設けハイブリッド形式で開催しました。東海地域だけでなくその他地域を拠点とする製品開発者からも多数の PSIRT 担当者にお集まりいただき、オフライン参加者も交えて意見交換を行いました。ミーティングでは、製品に対する安全とセキュリティの両面からのアプローチ、製品開発

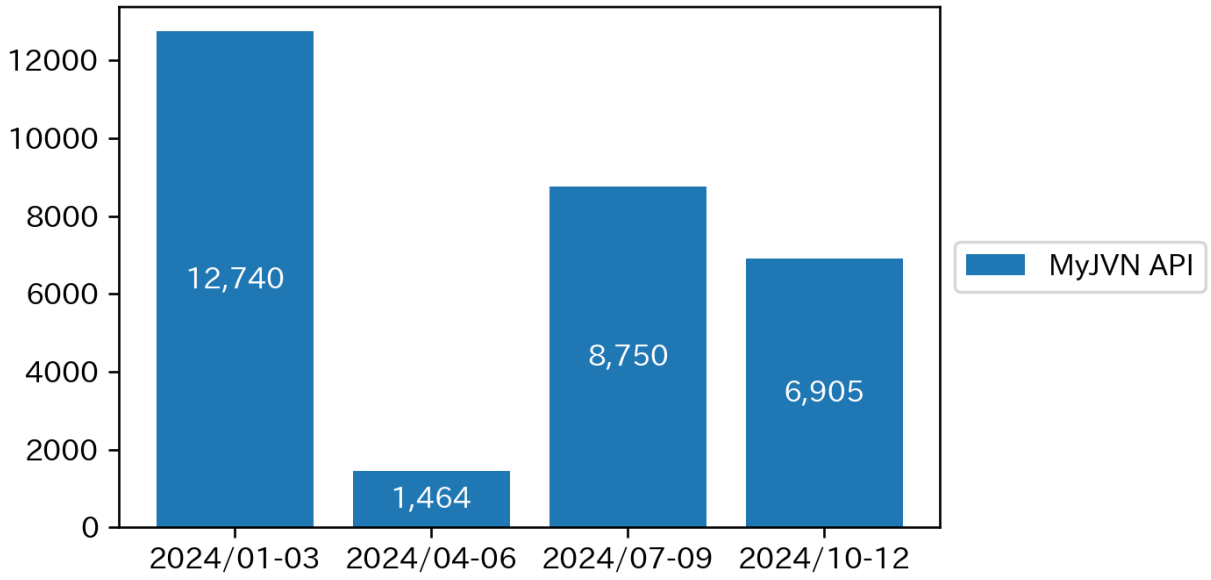

図 2.3 VRDA フィード配信件数

者による PSIRT 活動紹介、JVN の脆弱性公表ページの閲覧数の推移からの考察、脆弱性アドバイザリの高品質化の取り組み、CVSS v4 に関する説明、過去の定期ミーティングのアンケート結果の振り返りといったテーマで、参加者との意見交換を行いました。

2.3 VRDA フィードによる脆弱性情報の配信

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

- 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。

インデックス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、約 7% 減少しました。脆弱性情報の利用数については、約 20% 減少しました。

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。

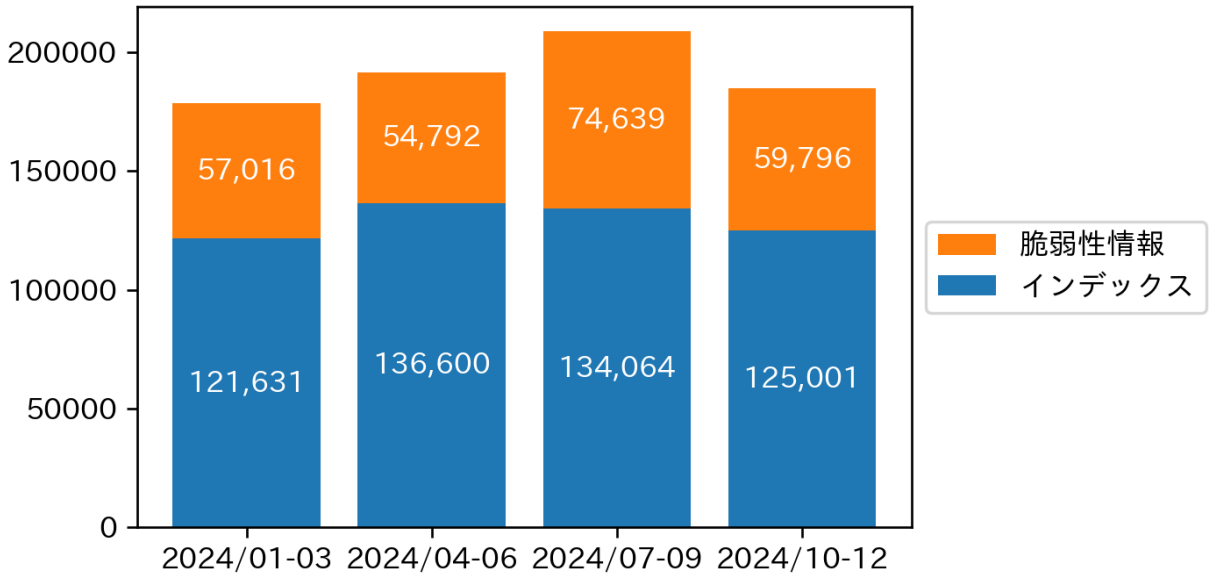

図 2.4 VRDA フィード利用件数

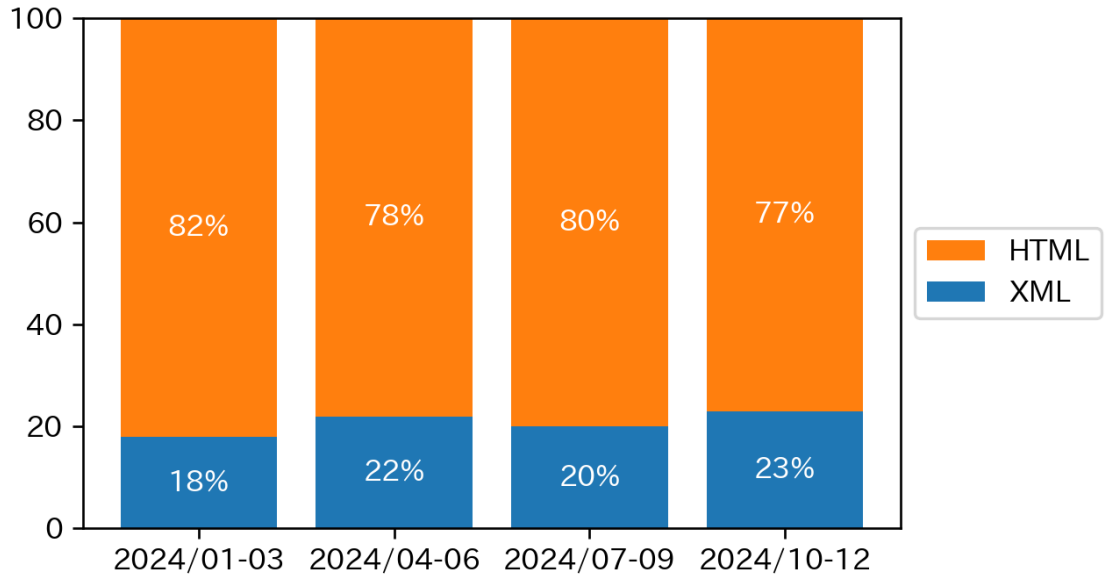

図 2.5 脆弱性情報のデータ形式別利用割合

第 3 章

国内連携活動

先に述べたような調整業務を円滑に進めるために、各組織の CSIRT やサイバーセキュリティ課題に取り組んでいる業界団体等の組織の協力を必要とする場合があります。そのような場合に備えて、JPCERT/CC では、そうした組織とセキュリティ状況に関する情報や認識の共有に平常時から努め、緊急時の連携が円滑にできるようにするための環境づくりに取り組んでいます。

3.1 業界団体やコミュニティー等との連携活動

サイバーセキュリティに関する取り組みを行っている各業界の ISAC や CEPTOAR などの組織や、業界団体、学会等が開催する集まりに参加し、意見交換や講演等を行っています。本四半期には次のような活動を行いました。

3.1.1 貿易会 ISAC

11 月 15 日に開催された技術部会に参加し、「最近のサイバー攻撃動向」という演題で講演を行いました。また、12 月 20 日に開催された実務部会では「2024 年の攻撃の技術的傾向から見た、情報共有や制度上の対応の傾向と対策」という演題で講演を行いました。

3.1.2 SICE/JEITA/JEMIMA セキュリティ調査研究合同 WG

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セキュリティ調査研究合同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。

3.1.3 セプターカウンシル運営委員会

JPCERT/CC は、セプターカウンシルの活動に参加しワーキンググループ活動の支援や情報提供等を行うとともに、内閣サイバーセキュリティセンター（NISC）と共同でセプターカウンシルの事務局業務を支援しています。本四半期においては、12 月 2 日に開催された第 78 回セプターカウンシル運営委員会

で、「FortiManager の重要な機能に対する認証の欠如の脆弱性（CVE-2024-47575）について」と題し情報提供を行うとともに、標的型攻撃に関する情報共有体制（C4TAP）の運用状況について報告しました。

3.2 国内関係機関との連携強化および情報交換の環境整備

3.2.1 早期警戒情報提供先との連携促進

ポータルサイト CISTA の登録組織に対し、早期警戒情報等の提供に加えて、情報共有や意見交換のための機会を設けています。会合をオフラインで開催するなどして組織間の交流を促すとともに、参加組織にもご講演をいただくなど、双方向の対話の活性化に努めています。なお、本四半期において新たに 14 組織が CISTA に登録されました。

3.2.2 製造業の制御システムセキュリティ担当者向け課題検討グループ

JPCERT/CC では、製造業を中心とした制御システムセキュリティ担当者による課題検討グループを主催しています。このグループでは、制御システムセキュリティに関する共通課題について、JPCERT/CC と参加組織とが協働し、実務ベースで実践的な検討を行っています。

なお、本四半期末時点で 32 組織が参加しています。

3.3 情報・ツール等の提供

3.3.1 制御システムセキュリティ情報提供用メーリングリスト

JPCERT/CC では制御システムセキュリティ情報提供用メーリングリストを設けており、本四半期末時点で 1,599 名に登録していただいています。対象者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
  https://www.jpcert.or.jp/ics/ics-community.html

現在、制御システムセキュリティ情報提供用メーリングリストに登録いただいている方には、「JPCERT/CC ICS Security Notes」を配信しています。

3.3.2 JPCERT/CC ICS Security Notes

「JPCERT/CC ICS Security Notes」は、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四半期ごとに配信するもので、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、対象期間にどのような動きがあったのかがわかるよう、コンパクトにまとめたものです。「JPCERT/CC ICS Security Notes」の配信内容については次の 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
  https://www.jpcert.or.jp/ics/ics-community.html

本四半期に提供した ICS Security Notes は次のとおりです。

- 2024-10-18 JPCERT/CC ICS Security Notes FY2024_#Q2

3.3.3 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。

- 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

第 4 章

国際連携活動

4.1 海外 CSIRT 構築支援および運用支援活動

JPCERT/CC は、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。

4.2 国際 CSIRT 間連携

JPCERT/CC は、複数国に影響が生じるインシデントへのスムーズな対応等を目的に、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）

APCERT は 2003 年 2 月に発足したアジア太平洋地域の CSIRT コミュニティーです。JPCERT/CC は、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 は 10 月 25 日に電話会議を行い、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。

図 4.1 カンファレンスオープニングの模様（TWCERT/CC Web サイトより）

4.2.1.2　APCERT 年次総会およびカンファレンス 2024 への参加（11 月 5 日～8 日）

11 月 5 日から 8 日にかけて、APCERT の年次総会およびカンファレンスが台湾の台北で開催されました。対面での開催は 2019 年のシンガポール以来 5 年ぶりです。今年は “Power of Together: More Than the Sum of AP CERTs/CSIRTs” というテーマのもと、APCERT のメンバー・パートナー組織や台湾のサイバーセキュリティコミュニティーの代表者ら 200 名程度が参加しました。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 15 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 4 チームの改選選挙では、ACSC（オーストラリア）、CNCERT/CC（中国）、KrCERT/CC（韓国）、TWCERT/CC（台湾）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 が議長チームに再選され、副議長チームには新たに ACSC が選出されました。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。 FIRST Regional Symposium との共催イベントとして行われた 7 日の Open Conference では、冒頭で FIRST 理事である JPCERT/CC 国際部マネージャーの内田有香子があいさつを述べ（図 4.1）、セッション本編では JPCERT/CC が作成に取り組んでいる脆弱性コーディネーター向けのガイドラインについて早期警戒グループの木村浩樹が紹介しました。

- APCERT AGM & Conference
  https://apcert2024con.org.tw/
- 2024 APCERT & FIRST Regional Symposium for Asia Pacific
  https://www.first.org/events/symposium/asia-pacific2024/

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、国際部マネージャー 内田が 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 等の来訪および訪問

4.3.1 ベルギーサイバーセキュリティセンター（CCB）の来訪（11 月 13 日）

ベルギーのサイバーセキュリティセンターが JPCERT/CC オフィスを訪問しました。活動の状況についてヒアリングを受けるとともに、今後の協力について意見交換を行いました。

4.3.2 ラトビア CERT.LV の来訪（11 月 13 日）

ラトビアの CERT.LV が JPCERT/CC オフィスを訪問しました。活動の状況についてヒアリングを受けるとともに、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 IGF2024 への参加（12 月 15 日〜19 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 12 月 15 日から 19 日にかけてサウジアラビアのリヤドで開催されました（図 4.2）。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、国際会議です。世界の多様な国・地域から 11,000 名以上が参加登録し、6,000 名以上が現地参加しました。 JPCERT/CC はこの会議に参加し、情報収集を図るとともに、BFP Cybersecurity Panel と題したセッションに登壇し、サイバー分野の能力開発支援について日本の事例を紹介しました。IGF2024 については次の Web ページをご参照ください。

- IGF 2024
  https://igfriyadh2024.sa/

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。

図 4.2 IGF2024 の会場の様子

本四半期は、WG3 においては 10 月初旬に開催された国際会議に参加し、情報収集に努めました。

第 5 章

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（本章および次章において、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・問い合わせの受け付け、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フィッシング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・問い合わせの受け付け

フィッシング報告件数は、前四半期から引き続き増加しており、12 月は過去最大の報告件数を記録しました。過去 1 年間のフィッシング報告件数の推移は図 5.1 に示すとおりです。

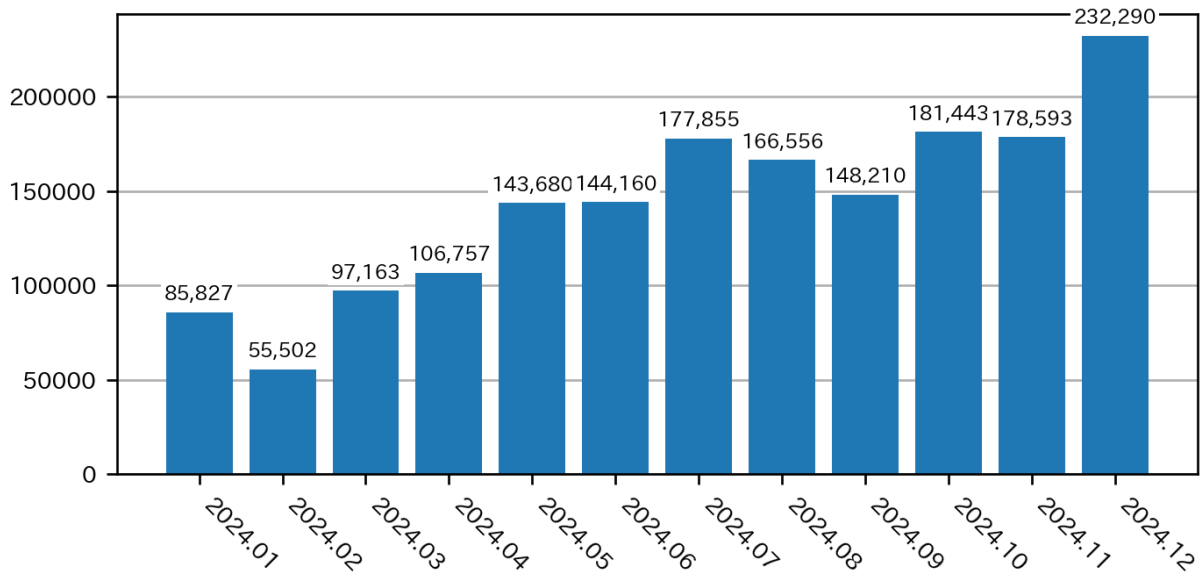

図 5.1 フィッシング報告件数

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 21.5% を占めました。次いで、「MyJCB」をかたるフィッシングの報告も多く、全体の約 8.7% 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緊急情報を 9 件発信しました。

利用者が多いサービスに関する、影響範囲が広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。

- JCB をかたるフィッシング：1 件
- アイフルをかたるフィッシング：1 件
- プロミスをかたるフィッシング：1 件
- WESTER をかたるフィッシング：1 件
- レイク (新生フィナンシャル) をかたるフィッシング：1 件
- ORIX MONEY(オリックス・クレジット) をかたるフィッシング：1 件
- PayPay をかたるフィッシング：1 件
- au PAY 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

前述のとおり本四半期も前四半期から報告件数の増加が継続しており、引き続き注意が必要です。

本四半期に発生したフィッシングとしては、消費者金融をかたるフィッシング（図 5.2）や、以前から長期休暇前に発生している交通系をかたるフィッシングが発生しました（図 5.3）。フィッシングの誘導 URL については、サブドメインにランダムな文字列が使用された URL が大量に作成・使用されていることが、報告数の上昇に影響しています。

5.2.2 定期報告

報告されたフィッシングサイト数や毎月の活動報告等を協議会の Web サイトで次のとおり公開しています。

- フィッシング対策協議会 Web サイト
  https://www.antiphishing.jp/
- 2024/09 フィッシング報告状況
  https://www.antiphishing.jp/report/monthly/202409.html
- 2024/10 フィッシング報告状況

図 5.2 消費者金融をかたるフィッシングサイトの例

図 5.3 交通系をかたるフィッシングサイトの例

https://www.antiphishing.jp/report/monthly/202410.html

- 2024/11 フィッシング報告状況
  https://www.antiphishing.jp/report/monthly/202411.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。本四半期末時点で 52 組織に対し URL 情報を提供しており、今後も要望に応じて広く提供する予定です。

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の作成・改訂を行う作業部会です。本四半期は、2025 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や事業者および一般消費者が講ずべきフィッシング対策等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 1 回）
  日時：10 月 04 日（金）15：00〜18：00（みずほ R&T 会議室＋オンライン）
- 技術・制度検討ワーキンググループ会合（第 2 回）
  日時：11 月 01 日（金）15：30〜17：30（JPCERT/CC 会議室＋オンライン）
- 技術・制度検討ワーキンググループ会合（第 3 回）
  日時：11 月 25 日（月）16：30〜18：00（JPCERT/CC 会議室＋オンライン）
- 技術・制度検討ワーキンググループ会合（第 4 回）
  日時：12 月 23 日（月）15：30〜17：30（JPCERT/CC 会議室＋オンライン）

第 6 章

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 122 回運営委員会（オンライン）
  日時：10 月 17 日（木）16：00〜18：00
- 第 123 回運営委員会（オンライン）
  日時：11 月 21 日（木）16：00〜18：00
- 第 124 回運営委員会（JPCERT/CC 会議室＋オンライン）
  日時：12 月 19 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）
- フィッシング対策セミナー 2024
  日時：11 月 08 日（金）10：00〜16：00（オンライン）
- 第 4 回証明書普及促進ワーキンググループ会合
  日時：11 月 28 日（木）16：30〜18：00（オンライン）

第 7 章

公開資料

本章では JPCERT/CC が本四半期に公開した調査・研究の報告書やブログなど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について、報告の受け付けや、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。

- 2024-10-17
  JPCERT/CC インシデント報告対応レポート［2024 年 7 月 1 日〜2024 年 9 月 30 日］
  https://www.jpcert.or.jp/pr/2024/IR_Report2024Q2.pdf
- 2024-12-06
  JPCERT/CC Incident Handling Report [July 1, 2024 - September 30, 2024]
  https://www.jpcert.or.jp/english/doc/IR_Report2024Q2_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。センサーで観測されたパケットを分類し、脆弱性情報、マルウェアや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。

- 2024-11-12
  JPCERT/CC インターネット定点観測レポート［2024 年 7 月 1 日〜2024 年 9 月 30 日］

https://www.jpcert.or.jp/tsubame/report/report202407-09.html
https://www.jpcert.or.jp/tsubame/report/TSUBAME_Report2024Q2.pdf

- 2024-12-06
  JPCERT/CC Internet Threat Monitoring Report [July 1, 2024 - September 30, 2024]
  https://www.jpcert.or.jp/english/doc/TSUBAMEReport2024Q2_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、最終改正令和 6 年経済産業省告示第 93 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。

- 2024-10-17
  ソフトウェア等の脆弱性関連情報に関する届出状況［2024 年第 3 四半期（7 月〜9 月）］
  https://www.jpcert.or.jp/pr/2024/vulnREPORT_2024q3.pdf

7.4 公式ブログ「JPCERT/CC Eyes」

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 11 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/

2024-11-14 ETW Forensics - Event Tracing for Windows を活用したインシデントレスポンス -

2024-11-20 TSUBAME レポート Overflow（2024 年 7〜9 月）

2024-11-26 正規サービスを悪用した攻撃グループ APT-C-60 による攻撃

2024-12-19 近年の水飲み場攻撃事例 Part1

2024-12-25 サイバーセキュリティの「有事」に何が必要なのか 〜Locked Shields2024 演習参加からの考察〜

2024-12-26 近年の水飲み場攻撃事例 Part2

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

2024-11-14 ETW Forensics - Why use Event Tracing for Windows over EventLog? -

2024-12-11 Attack Exploiting Legitimate Service by APT-C-60

2024-12-17 TSUBAME Report Overflow (Oct-Dec 2024)

2024-12-19 Recent Cases of Watering Hole Attacks, Part 1

2024-12-26 Recent Cases of Watering Hole Attacks, Part 2

第 8 章

その他の活動

8.1 講演

1. 堀 充孝（早期警戒グループ 脅威情報アナリスト）
   「サイバーセキュリティにおける脅威動向と JPCERT/CC の取り組み」
   A10 Connect 2024（主催：A10 ネットワークス株式会社、講演日：10 月 2 日）
2. 洞田 慎一（早期警戒グループ 部門長）
   「サイバーインシデント解決への向き合い方」
   日本医用画像専門技術会主催セミナー（主催：日本医用画像専門技術会、講演日：10 月 13 日）
3. 洞田 慎一（早期警戒グループ 部門長）
   「防犯カメラ・レコーダー等の防犯設備に対するインシデントから考える対策」
   第 26 回 日本防犯設備協会 特別セミナー（主催：公益社団法人日本防犯設備協会、講演日：10 月 18 日）
4. 洞田 慎一（早期警戒グループ 部門長）
   「サイバーインシデント解決への向き合い方」
   日本医用画像専門技術会主催セミナー（主催：日本医用画像専門技術会、講演日：10 月 19 日）
5. 洞田 慎一（早期警戒グループ 部門長）
   「サイバーインシデント解決への向き合い方」
   日本医用画像専門技術会主催セミナー（主催：日本医用画像専門技術会、講演日：11 月 16 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）
   「セキュリティアナリストの仕事とは ～JPCERT/CC の情報発信から見る脅威インテリジェンスの仕組み～」
   セキュリティフォーラム（主催：株式会社テプコシステムズ、講演日：11 月 18 日）
7. 宮地 利雄（技術顧問）
   「ICS Security in Japan: Retrospect & Prospects」
   産業応用部門 2024 年度大会（主催：公益社団法人計測自動制御学会 産業応用部門、講演日：11 月 20 日）
8. 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）
   「最近のサイバー攻撃事例から考える、「境界」から見たゼロトラストとサイバーハイジーンの捉

え方」
第 4 回 経済安全保障セミナー（主催：日本製薬工業協会 産業政策委員会、講演日：11 月 25 日）

9. 衛藤 亮介（早期警戒グループ 脅威アナリスト）、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）
「サイバー攻撃に対する個人・組織の初動対応ポイント～研究者／研究機関を狙う攻撃のケーススタディから～」
情報セキュリティセミナー（主催：国立大学法人東京大学、講演日：12 月 13 日）
10. 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）
パネルディスカッション参加
我が国における能動的サイバー防御実現に向けたシンポジウム（主催：紀尾井町戦略研究所株式会社、講演日：12 月 16 日）
11. 洞田 慎一（早期警戒グループ 部門長）
「サイバーインシデント解決への向き合い方」
日本医用画像専門技術会主催セミナー（主催：日本医用画像専門技術会、講演日：12 月 21 日）

8.2 協力・後援

本四半期は次の行事の開催に協力または後援等を行いました。

1. 重要インフラサイバーセキュリティコンファレンス&産業サイバーセキュリティコンファレンス
（主催：株式会社インプレス、重要インフラサイバーセキュリティコンファレンス実行委員会、開催日：10 月 8 日）
2. 情報セキュリティワークショップ in 越後湯沢 2024
（主催：NPO 法人新潟情報セキュリティ協会、情報セキュリティワークショップ in 越後湯沢 実行委員会、開催日：10 月 10 日、11 日）
3. Hardening 2024 Convolutions
（主催：Hardening Project、開催日：10 月 16 日～18 日）
4. Security Days Fall 2024
（主催：株式会社ナノオプト・メディア、開催日：10 月 16 日、22～25 日、29 日）
5. 第 24 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、開催日：11 月 11 日、12 日）
6. Internet Week 2024
（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、開催日：11 月 19 日～21 日）
7. デジタル・フォレンジック・コミュニティ 2024 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 2024 実行委員会、開催日：12 月 9 日、10 日）
8. 日本セキュリティ・マネジメント学会 第 36 回学術講演会
（主催：一般社団法人日本セキュリティ・マネジメント学会、開催日：12 月 21 日）

最新情報については JPCERT/CC の Web サイトを参照してください。

- JPCERT コーディネーションセンター（JPCERT/CC）：https://www.jpcert.or.jp/
- インシデント情報の提供および対応依頼：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：dc-info@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
- 公開資料の引用、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

JPCERT/CC 活動四半期レポート ［ 2024 年 10 月 1 日～2024 年 12 月 31 日 ］

- 発行履歴
  - 2025 年 1 月 23 日　初版
- 発行者
  一般社団法人 JPCERT コーディネーションセンター
  〒103-0023
  東京都中央区日本橋本町 4-4-2 東山ビルディング 8 階
  TEL 03-6271-8901 FAX 03-6271-8908
  URL https://www.jpcert.or.jp/