JPCERT Coordination Center

JPCERT/CC 活動四半期レポート

2024 年 1 月 1 日 ～ 2024 年 3 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 4 月 18 日

JPCERT CC®

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－　インシデント対応のファーストレスポンダー向け相談窓口を新たに開設

サイバー攻撃の高度化やランサムウェア攻撃の増加により、断片的な情報でインシデント初動対応の判断を速やかにしなければならない事案が増えており、被害組織やファーストレスポンダー（初動対応支援にあたるセキュリティベンダーや運用保守会社等）だけの知見では初動対応が困難なケースが増えています。こうした状況等を踏まえ、2024 年 3 月 11 日に経済産業省から被害組織のインシデント対応支援にあたる専門組織同士の情報共有のための「攻撃技術情報の取扱い・活用手引き」が公表されました。この手引きの検討において、JPCERT/CC は経済産業省とともに共同事務局を務め、草案作りも担当しました。

しかしながら、こうした手引きが整備されたからといって、ただちに専門組織同士の情報共有ができるわけではなく、また、現状でもそうした活動は限定的です。そこで JPCERT/CC では、専門組織やファーストレスポンダー同士の情報共有の橋渡しをするべく、サイバー攻撃の被害を受けた組織に加えて、セキュリティベンダーやシステム運用会社など被害の調査を支援する組織からの相談も受け付ける、新たな相談窓口を 3 月 25 日に開設しました。

JPCERT/CC インシデント相談・情報提供（被害組織／保守・調査ベンダー向け）
https://www.jpcert.or.jp/ir/consult.html

経済産業省「攻撃技術情報の取扱い・活用手引き」
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/cyber_attack/20231122_report.html

また、窓口の運用開始にあわせて、「ランサムウェア攻撃事案から見る、ファーストレスポンダー同士の情報共有が必要な理由」と題した分析レポートを公表しました。これは、直近のランサムウェア攻撃事案のインシデント対応における課題とあるべき姿を分析したものです。ランサムウェア攻撃事案の初動対応には他のインシデント対応以上に速やかな分析・判断が必要とされ、初動対応における不手際が業務復旧の遅れなど影響の拡大につながってしまいます。JPCERT/CC では、新たな窓口での実際の相談対応や情報共有活動への情報提供に加え、専門組織同士の情報共有の活性化のため、「攻撃技術情報の取扱い・活用手引き」の普及啓発活動として、公開レポートなどを通じてのケーススタディに関する情報発信も取り組んでいきます。

ランサムウェア攻撃事案から見る、ファーストレスポンダー同士の情報共有が必要な理由
https://blogs.jpcert.or.jp/ja/2024/03/ransom_incident_and_infosharing.html

－トピック2－　セキュリティアナリスト向けカンファレンス JSAC2024 を開催

2024 年 1 月 25 日、26 日に JSAC2024 を御茶ノ水ソラシティカンファレンスセンターで開催しました。本カンファレンスは、サイバー攻撃によるインシデントの分析・対応を行っているセキュリティアナリストの技術力向上に資するために、刻々と変化する攻撃の手口や新たな分析手法について情報を共有することを目的としています。

昨年はオンライン会議と対面会議とを組み合わせたハイブリット会議の形態で開催しましたが、7 回目となる今回は対面会議のみで開催。ワークショップ 3 件を含む 17 件の講演の他に、Lightning Talk セッションとして 6 件の発表が行われ、マルウェア分析やインシデント対応事例といったインシデント分析・対応に関する技術や、講演者独自の新しい技術的な知見、分析ツールなどが共有されました。

当日は、389 名（事前登録者数 471 名）の方にご来場いただき、活発な議論が行われました。参加者の方々からは、本カンファレンスがセキュリティアナリストのレベル向上につながっているとの好意的な意見をいただいております。今後も、さらに多くの方々にとって有意義なカンファレンスとなるように、ご意見をもとに工夫した企画を検討いたします。

なお、JSAC2024 の講演資料は JSAC2024 の Web サイト上で公開しています。また、カンファレンスの概要は JPCERT/CC Eyes でも紹介していますので、ご覧ください。

JSAC2024
https://jsac.jpcert.or.jp/

JSAC2024 開催レポート～DAY 1～
https://blogs.jpcert.or.jp/ja/2024/03/jsac2024day1.html

JSAC2024 開催レポート～DAY 2～
https://blogs.jpcert.or.jp/ja/2024/03/jsac2024day2.html

JSAC2024 開催レポート～Workshop & Lightning Talk～
https://blogs.jpcert.or.jp/ja/2024/03/jsac2024day2-workshop-lightning-talk.html

－トピック3－　制御システムセキュリティカンファレンス 2024 を開催

2024 年 2 月 7 日（水）に「制御システムセキュリティカンファレンス 2024」をオンライン開催し、419 名の方々にご参加いただきました。共催の経済産業省からサイバーセキュリティ・情報化審議官 上村昌博氏に開会のご挨拶をいただき、その後、講演募集（CFP）で採用された 3 件を含む計 7 件の講演が行われました。

はじめに JPCERT/CC からこの一年間を振り返りつつ制御システムセキュリティに関するさまざまな動きと現状を紹介し、その後、コンピューター数値制御の工作機械に潜むセキュリティリスクとその対策、制御システムユーザー組織で容易に取り組めるネットワークの監視手法、制御システム向けセキュリティポリシーを実装する際の課題とその対策、インシデント対応の備えの必要性とステークホルダー間の連携の重要性、製造業 10 社の制御システムセキュリティ担当者が取り組んだインシデント対応訓練のシナリオ作成等といったさまざまなトピックスを取り扱った講演が行われました。制御システムユーザー企業がステップバイステップで取り組むことのできる活動を複数紹介できたことや、プログラム後半のパネルディスカッションで複数の制御システムユーザー企業が連携して実施する取り組みについて紹介できたことは、今回のカンファレンスに特徴的なものでした。

開催後のアンケート結果（有効回答数：208）によると、参加者の内訳は制御システムユーザーが 38.5%、制御システムベンダーが 8.7%、制御機器ベンダーが 11.5%、制御システムエンジニアリングが 7.2%、研究者が 4.3%で、前回とほぼ同じでした。また、オンライン開催のため、前回同様に全国各地からご参加いただけました。事前登録者は例年よりも早いスピードで定員に達し、JPCERT/CC が実施する制御システムセキュリティに関するイベントへの関心の高さが伺えました。また、同じくアンケート結果から 97.6%の方から今後も参加したいイベントであるとの回答をいただきました。今回の実績を踏まえ今後も制御システムセキュリティに取り組む担当者の活動に資するイベントを企画していきます。

なお、講演資料は JPCERT/CC の Web サイト上で公開しています。また、カンファレンスの概要はブログ「JPCERT/CC Eyes」でレポートしていますので、ご覧ください。

制御システムセキュリティカンファレンス 2024
https://www.jpcert.or.jp/event/ics-conference2024.html

制御システムセキュリティカンファレンス 2024 講演資料
https://www.jpcert.or.jp/present/#year2024

制御システムセキュリティカンファレンス 2024 開催レポート
https://blogs.jpcert.or.jp/ja/2024/03/ics-conference2024.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 11,741 件、インシデント件数ベースでは 6,089 件でした（注 1）。

（注 1）「報告件数」は、報告者から寄せられた Web フォーム、メール、FAX による報告の総数を示します。また、「インシデント件数」は、各報告に含まれるインシデントの件数の合計を示し、1 つのインシデントに関して複数の報告が寄せられた場合にも 1 件のインシデントとして扱います。

JPCERT/CC が国内外のインシデントに関連するサイトとの調整を行った件数は 4,602 件でした。前四半期の 5,444 件と比較して 15%減少しています。「調整」とは、フィッシングサイトが設置されているサイトや、改ざんにより JavaScript が埋め込まれているサイト、ウイルス等のマルウェアが設置されたサイト、「scan」のアクセス元等の管理者等に対し、状況の調査や問題解決のための対応を依頼する活動です。

JPCERT/CC は、インターネット利用組織におけるインシデントの認知と対処、インシデントによる被害拡大の抑止に貢献することを目的として活動しています。国際的な調整・支援が必要となるインシデントについては、日本における窓口組織として、国内や国外（海外の CSIRT 等）の関係機関との調整活動を行っています。

インシデント報告対応活動の詳細については、別紙「JPCERT/CC インシデント報告対応レポート」をご参照ください。

JPCERT/CC インシデント報告対応レポート
https://www.jpcert.or.jp/pr/2023/IR_Report2023Q4.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 4,781 件で、前四半期の 4,473 件から 7%増加しました。また、前年度同期（5,553 件）との比較では、14%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	1 月	2 月	3 月	本四半期合計（割合）
国内ブランド	1,076	1,134	1,016	3,226 (67%)
国外ブランド	220	145	380	745 (16%)
ブランド不明 (注 2)	243	255	312	810 (17%)
全ブランド合計	1,539	1,534	1,708	4,781

（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。

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 76.8%、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 56.1%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、えきねっと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。

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 30%、国外が 70%であり、前四半期（国内が 21%、国外が 79%）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、57 件でした。前四半期の 72 件から 21%減少しています。

本四半期は、Web サイトを改ざんし、アクセスしたユーザーを偽物の EC サイトへ転送する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おり、アクセスした Web ブラウザーの JavaScript 設定に応じて異なる不審なサイトへ誘導する仕組みになっていました。

```
<html lang="jp">
<head>
    <meta content="text/html; charset=utf-8" http-equiv="Content-Type" />
    <meta http-equiv="refresh" content="0; url=https://[redacted]" />
</head>
<body>
  <noscript>
    <meta http-equiv="refresh" content="0; url=https://[redacted]" />
  </noscript>
  <script>
    document.location.href = "https://[redacted]";
  </script>
```

［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) Ivanti Connect Secure の複数の脆弱性への対応

2024 年 1 月 10 日、Ivanti 社は Ivanti Connect Secure（旧称：Pulse Connect Secure）および Ivanti Policy Secure ゲートウェイに脆弱性があることを公表しました。公表されたものに、認証バイパスの脆弱性（CVE-2023-46805）とコマンドインジェクションの脆弱性（CVE-2024-21887）が含まれており、これらを悪用することで遠隔の第三者が任意のコマンドを実行できます。本脆弱性はすでに悪用が確認されていたことから JPCERT/CC でも 1 月 11 日に注意喚起を行いました。その後さらに Ivanti 社から関連する複数の脆弱性が公表されました。その中に、権限昇格の脆弱性（CVE-2024-21888）、SSRF の脆弱性（CVE-2024-21893）および XML 外部実体参照の脆弱性（CVE-2024-22024）が含まれていたことから、JPCERT/CC では 2 月 21 日に対策と悪用事例を整理した資料を公開しました。

Ivanti Connect Secure および Ivanti Policy Secure の脆弱性（CVE-2023-46805 および CVE-2024-21887）に関する注意喚起
https://www.jpcert.or.jp/at/2024/at240002.html

2024 年 1 月以降の Ivanti Connect Secure などの脆弱性の状況について
https://www.jpcert.or.jp/newsflash/2024021601.html

JPCERT/CC では、外部組織から提供された情報をもとに、Web シェルやバックドアが設置されたと疑われる機器および脆弱性が未修正で侵害され可能性がある機器を利用している国内のシステム管理者に対して通知を行いました。
また、JPCERT/CC では複数の組織からこれらの脆弱性によって被害を受けたとの相談を受けており、脆弱性が公開された直後の 1 月 11 日から WIREFIRE と呼ばれる Web シェルや ZIPLINE と呼ばれるバックドアが設置された事例を複数確認しています。本脆弱性を攻撃する PoC が公開された 1 月 16

日以降には、機器に仮想通貨マイニングツールを設置するような攻撃も確認されています。一部の組織では Ivanti 製品の内部整合性チェックツールが改ざんされ、設置された Web シェルやバックドアを検知できなくなっていました。

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 36,000 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：16 件（うち更新情報が 9 件）　https://www.jpcert.or.jp/at/

2024-01-10　2024 年 1 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

2024-01-11　Ivanti Connect Secure および Ivanti Policy Secure の脆弱性（CVE-2023-46805 および CVE-2024-21887）に関する注意喚起
2024-01-15　Ivanti Connect Secure および Ivanti Policy Secure の脆弱性（CVE-2023-46805 および CVE-2024-21887）に関する注意喚起（更新）
2024-01-17　2024 年 1 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
2024-01-17　Ivanti Connect Secure および Ivanti Policy Secure の脆弱性（CVE-2023-46805 および CVE-2024-21887）に関する注意喚起（更新）
2024-01-31　Ivanti Connect Secure および Ivanti Policy Secure の脆弱性（CVE-2023-46805 および CVE-2024-21887）に関する注意喚起（更新）
2024-02-01　Ivanti Connect Secure および Ivanti Policy Secure の脆弱性（CVE-2023-46805 および CVE-2024-21887）に関する注意喚起（更新）
2024-02-09　Fortinet 製 FortiOS の境域外書き込みの脆弱性（CVE-2024-21762）に関する注意喚起
2024-02-09　Ivanti Connect Secure および Ivanti Policy Secure の脆弱性（CVE-2023-46805 および CVE-2024-21887）に関する注意喚起（更新）
2024-02-14　2024 年 2 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
2024-02-14　Adobe Acrobat および Reader の脆弱性（APSB24-07）に関する注意喚起
2024-02-14　Ivanti Connect Secure および Ivanti Policy Secure の脆弱性（CVE-2023-46805 および CVE-2024-21887）に関する注意喚起（更新）
2024-02-15　Fortinet 製 FortiOS の境域外書き込みの脆弱性（CVE-2024-21762）に関する注意喚起（更新）
2024-02-29　Fortinet 製 FortiOS の境域外書き込みの脆弱性（CVE-2024-21762）に関する注意喚起（更新）
2024-02-29　Ivanti Connect Secure および Ivanti Policy Secure の脆弱性（CVE-2023-46805 および CVE-2024-21887）に関する注意喚起（更新）
2024-03-13　2024 年 3 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：12 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 2 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：7 件（うち更新情報が 2 件）　https://www.jpcert.or.jp/newsflash/

2024-01-16	GitLab のパスワードリセット機能における脆弱性（CVE-2023-7028）について
2024-01-23	Apple 製品のアップデートについて（2024 年 1 月）
2024-02-14	ISC BIND 9 における複数の脆弱性について（2024 年 2 月）
2024-02-16	2024 年 1 月以降の Ivanti Connect Secure などの脆弱性の状況について
2024-02-21	2024 年 1 月以降の Ivanti Connect Secure などの脆弱性の状況について（更新）
2024-03-06	Apple 製品のアップデートについて（2024 年 3 月）
2024-03-08	Apple 製品のアップデートについて（2024 年 3 月）（更新）

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) Ivanti Connect Secure および Ivanti Policy Secure の脆弱性（CVE-2023-46805 および CVE-2024-21887）に関する情報発信

2024 年 1 月 10 日（現地時間）、Ivanti 社が Ivanti Connect Secure（旧: Pulse Connect Secure）および Ivanti Policy Secure ゲートウェイにおける脆弱性に関するアドバイザリを公表しました。本脆弱性を悪用した攻撃が行われていると書かれており、JPCERT/CC でも本脆弱性を悪用したとみられる攻撃が国内組織に対しても行われたことを確認したため、1 月 11 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、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高い機器のリストが、信頼できる情報筋から JPCERT/CC に提供されました。JPCERT/CC では、このリストを分析するとともに、インターネット上のスキャン・パケットの分析結果を突き合わせて、被害に気づいていない、または、対策を実施し

ておらず、いずれ攻撃を受ける可能性がある国内組織を多数特定しました。それらの組織に対して個別に通知を行い、状況確認と脆弱性への対処を呼びかけました。
その後に Ivanti 社はアドバイザリを複数回更新し、新たに確認された脆弱性情報や対策バージョン、新たな回避策などを公表しました。これに対応して JPCERT/CC 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。
また、脆弱性対応の参考にしていただくため、Ivanti 社が情報の更新を継続する中、公開された脆弱性情報の公開日やアドバイザリのリンク、回避策や対策（修正パッチ）情報の公開開始日、脆弱性の実証コード（PoC）の公開日、既知の悪用事例などに関する情報をまとめて CyberNewsFlash として公開しました。

Ivanti Connect Secure および Ivanti Policy Secure の脆弱性（CVE-2023-46805 および CVE-2024-21887）に関する注意喚起
https://www.jpcert.or.jp/at/2024/at240002.html

2024 年 1 月以降の Ivanti Connect Secure などの脆弱性の状況について
https://www.jpcert.or.jp/newsflash/2024021601.html

（2） Fortinet 製 FortiOS の境域外書き込みの脆弱性（CVE-2024-21762）に関する発信

2024 年 2 月 8 日（現地時間）、Fortinet 社は FortiOS および FortiProxy における境域外書き込みの脆弱性（CVE-2024-21762）に関するアドバイザリ（FG-IR-24-015）を公表しました。本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、細工した HTTP リクエストを送信し、結果として任意のコードまたはコマンドを実行する可能性があります。同社は、本脆弱性の悪用の可能性を示唆しており、JPCERT/CC は 2 月 11 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。

Fortinet 製 FortiOS の境域外書き込みの脆弱性（CVE-2024-21762）に関する注意喚起
https://www.jpcert.or.jp/at/2024/at240004.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、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等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 10 月から 12 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。

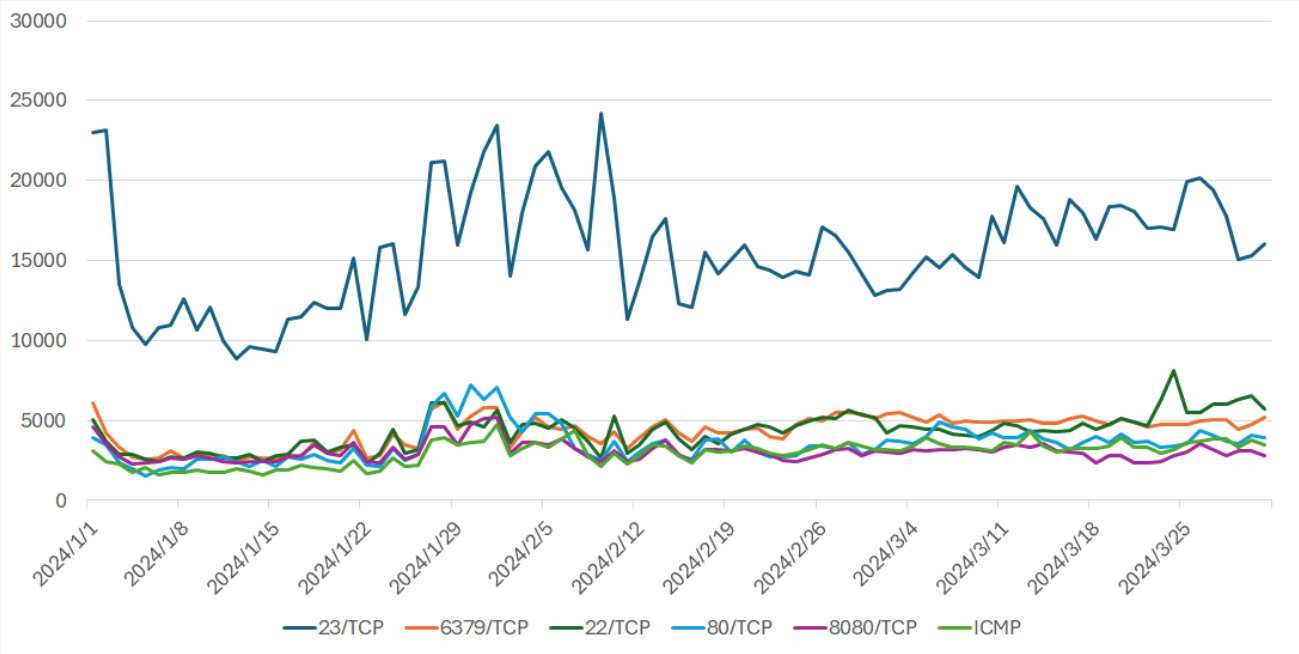
TSUBAME 観測グラフ
https://www.jpcert.or.jp/tsubame/index.html#examples

インターネット定点観測レポート（2023 年 10～12 月）
https://www.jpcert.or.jp/tsubame/report/report202310-12.html

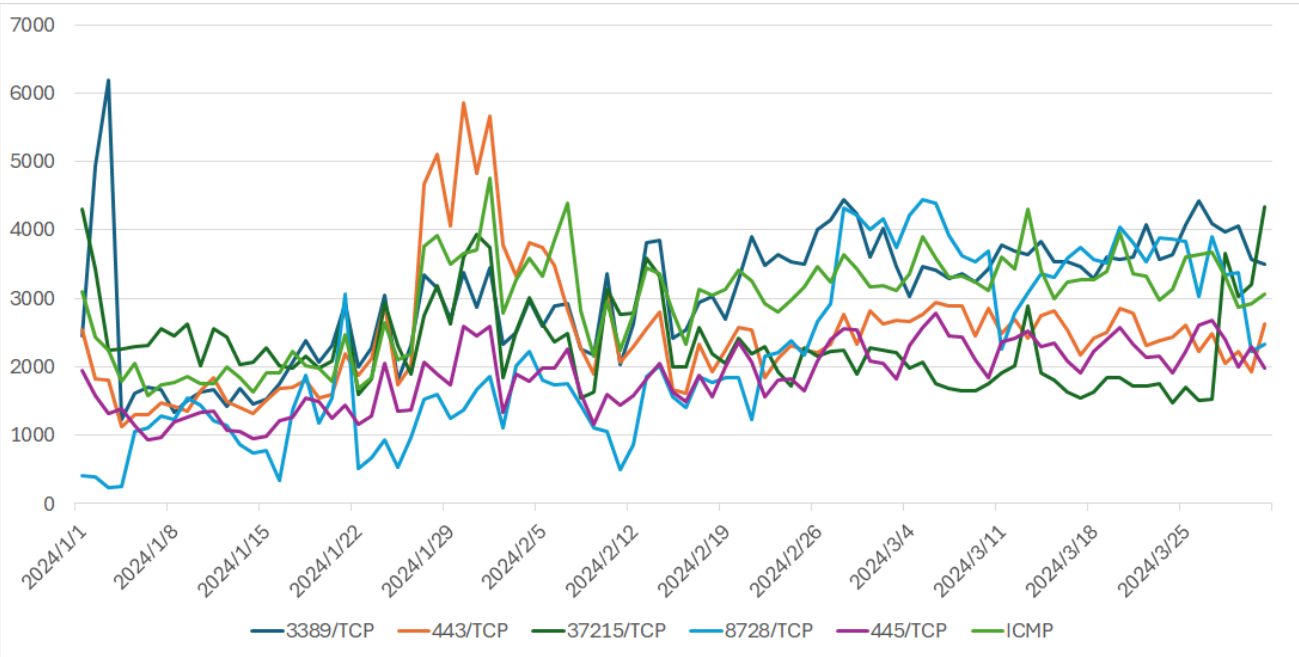
TSUBAME レポート Overflow（2023 年 10～12 月）
https://blogs.jpcert.or.jp/ja/2024/02/tsubame_overflow_2023-10-12.html

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、本四半期における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 1-1］と［図 1-2］に示します。

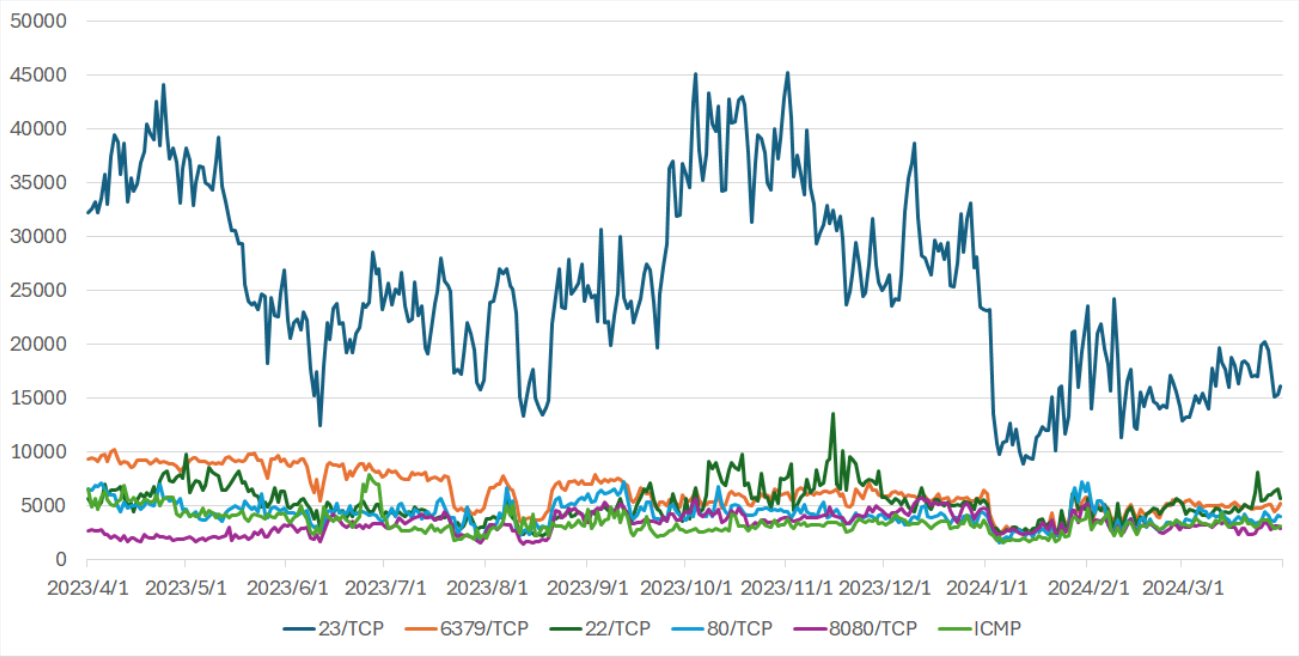


［図 1-2：TSUBAME で観測された宛先ポートの上位 1 位から 5 位のパケット数（2024 年 1 月 1 日～3 月 31 日)］

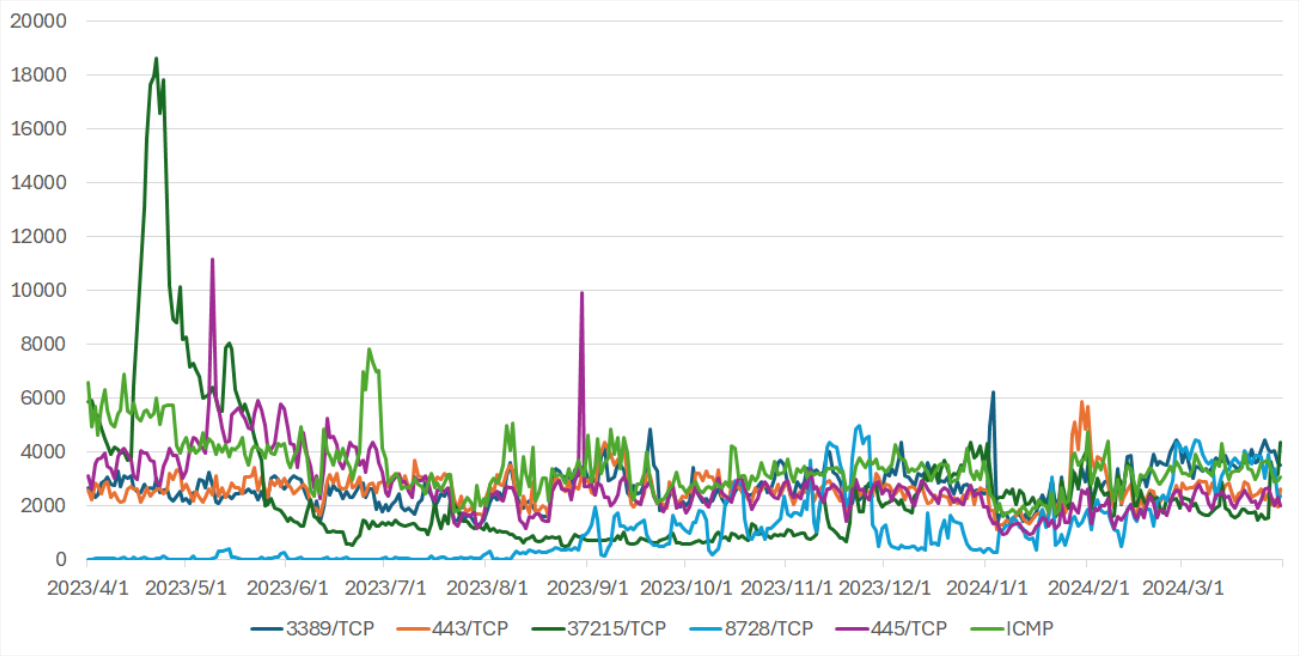


［図 1-3：TSUBAME で観測された宛先ポートの上位 6 位から 10 位のパケット数（2024 年 1 月 1 日～3 月 31 日)］

また、過去 1 年間（2023 年 4 月 1 日～2024 年 3 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 1-3］と［図 1-4］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 4 月 1 日～2024 年 3 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 4 月 1 日～2024 年 3 月 31 日)］

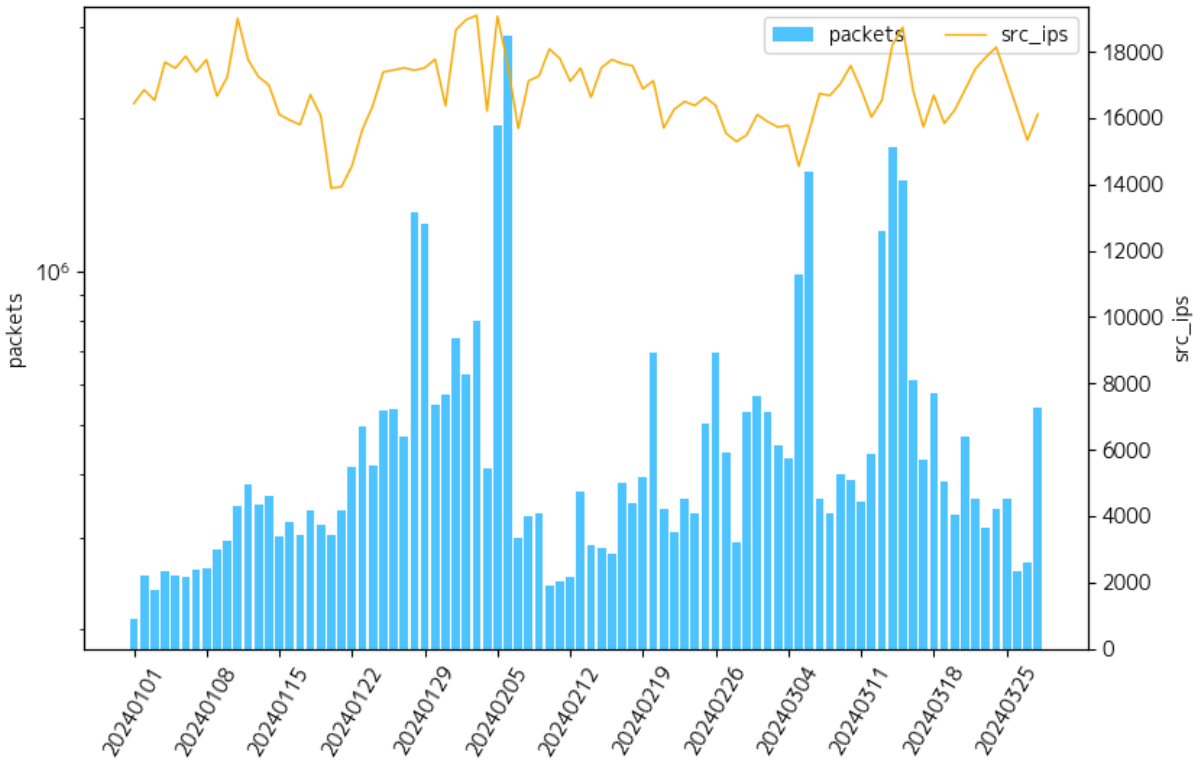
本四半期に最も多く観測されたパケットは 23/TCP (telnet) 宛の通信でした。2 番目と 3 番目は 22/TCP（SSH）宛と 6379/TCP 宛の通信で、前四半期と順序が入れ替わりました。4 番目と 5 番目に多く観測されたパケットは Port80/TCP(http) 、Port8080/TCP 宛の通信でした。9 位にはパケット数が増えた 8728/TCP 宛が入りました。

1.3.2. ハニーポットの運用とその分析

JPCERT/CC では、HTTP/HTTPS 通信を記録する低対話型のハニーポットをインターネット上に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 1-5］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）。

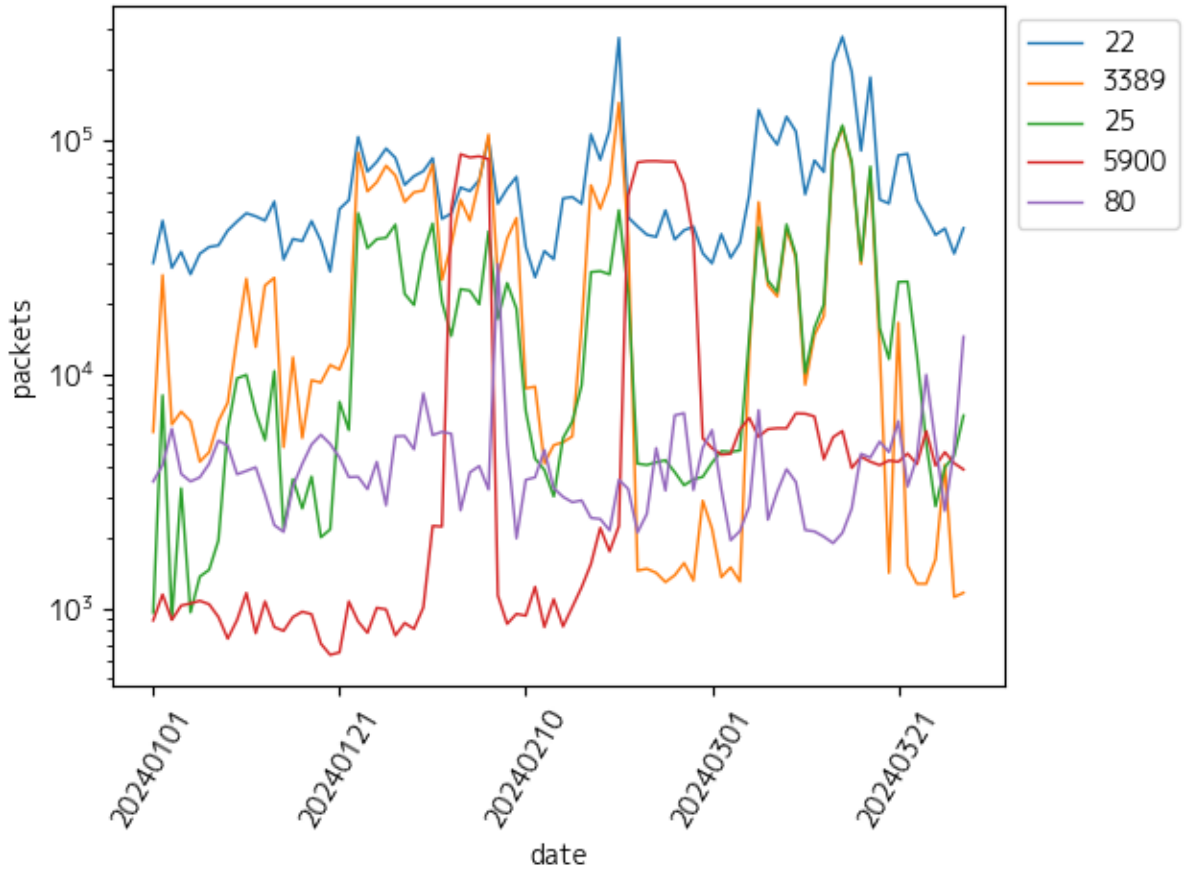


［図 1-6：ハニーポットに対するアクセス数の推移（2024 年 1 月 1 日～3 月 28 日）］

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 1-1］および［図 1-6］に示します。

［表 1-2：宛先ポート別アクセス数 トップ 5（2024 年 1 月 1 日～3 月 28 日）］

#	宛先ポート	アクセス数
1	22/TCP	5,890,356
2	3389/TCP	2,403,933
3	25/TCP	1,593,375
4	5900/TCP	1,152,610
5	80/TCP	696,155

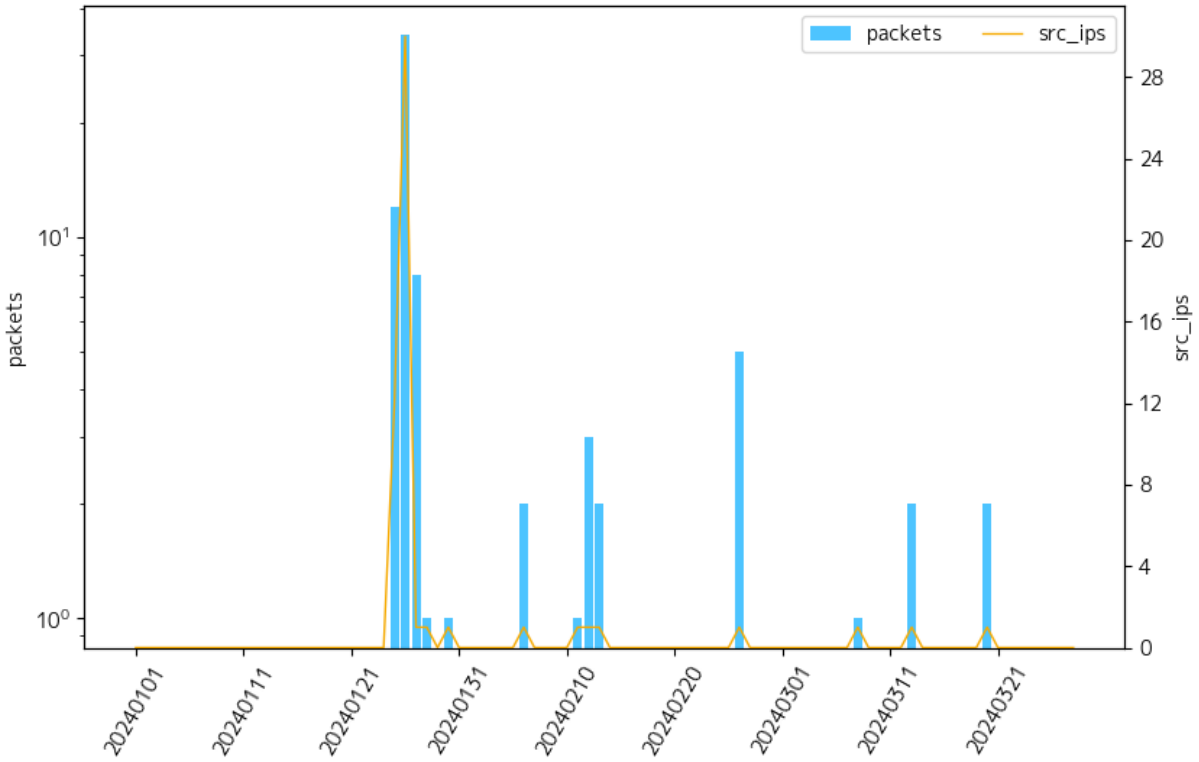


［図 1-7：宛先ポート別アクセス数 トップ 5（2024 年 1 月 1 日～3 月 28 日）］

前四半期と同様、本四半期においても、5900/TCP ポートに対するアクセスが多く観測されています。これらのアクセス元ホストの多くが、Graynoise などのデータベースによると、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。現時点では単なる調査研究なのか攻撃のための悪意ある探索なのかまでは判別することができません。

1.3.2.2. Atlassian Confluence Data Center および Server の脆弱性（CVE-2023-22527）に対する攻撃試行の観測

Atlassian Confluence Data Center および Server のテンプレートインジェクションの脆弱性（CVE-2023-22527）が、2024 年 1 月 16 日（米国時間）に公表されました。その 1 週間後に概念実証（PoC）コードが公開されたことから悪用が始まり、JPCERT/CC のハニーポットでも攻撃が観測されました［図 1-7］。攻撃の試行は、PoC コードの公開直後の 3 日間ほどは多くの送信元ホストからありましたが、その後は少なくなっています。



［図 1-8：Atlassian Confluence Data Center および Server の脆弱性（CVE-2023-22527）に対する攻撃試行の推移（2024 年 1 月 1 日～3 月 28 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、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。米国の MITRE 社が事務局を務めている）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 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。

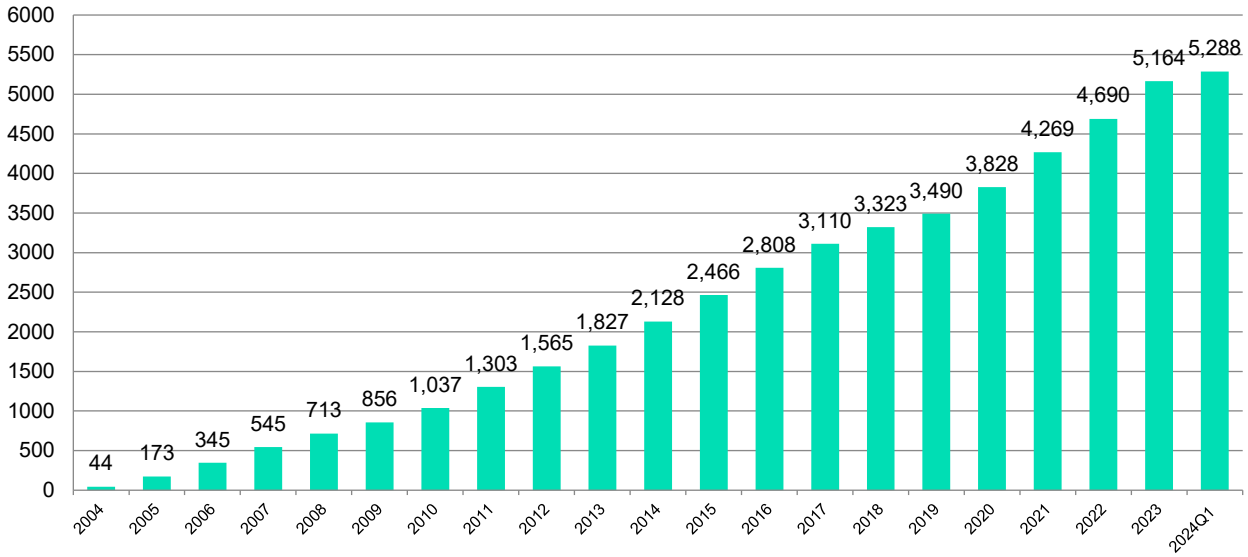
2.1.2. Japan Vulnerability Notes（JVN）において公表した脆弱性情報および対応状況

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（「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 124 件（累計 5,288 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：41 件（そのうち調整不能案件が 6 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：83 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。

(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#54451757
  SKYSEA Client View における複数の脆弱性
  https://jvn.jp/jp/JVN54451757/

このアドバイザリは、Ｓｋｙ株式会社製の IT 資産管理用ツール SKYSEA Client View のクライアントソ

フトウェアに影響する 2 件の脆弱性を含んでいます。この 2 件の脆弱性は報告者も報告時期も異なっていました。早く対応できたものから順に単独のアドバイザリとして公表することも検討しましたが、2 件のアドバイザリを短期間に連続して公表すればユーザーの対応負荷が増大することが懸念されました。そこで、ユーザーの対応が 1 回ですむよう、2 件の脆弱性を 1 つのパッチで修正対策し、アドバイザリも 1 つに集約するよう製品開発者と調整しました。脆弱性情報流通は必要なところに迅速に情報を届けることに加え、製品利用者のコスト抑えて効率を高めつつ、対策の適用を促進することも重要です。JPCERT/CC では、常に情報の受け手を意識した情報発信を心掛けています。

(2) 国際調整または独自調整で取り扱った脆弱性

- JVNVU#92420039
  Ivanti 製 Connect Secure および Policy Secure における複数の脆弱性
  https://jvn.jp/vu/JVNVU92420039/

Ivanti 社が VPN ソフトウェア Ivanti Connect Secure および NAC ソフトウェア Ivanti Policy Secure における複数の脆弱性を悪用したゼロデイ攻撃のアドバイザリを公表しました。JPCERT/CC は国内組織への同様の攻撃の可能性を認識し、国内ユーザーの注意を喚起するため本アドバイザリを公表しました。この時点では、修正パッチが未提供、またサポート終了製品への影響が未評価であり、対応検討には情報不足でした。JPCERT/CC は情報不足を補うため、その後の Ivanti 社の対応を注視しつつ、本アドバイザリと同時に発行した次の注意喚起で補足的な情報を提供しました。脆弱性の悪用や実証コードの公開が先行し、これを Ivanti 社による脆弱性対策が後追いした経緯を振り返ると、脆弱性発見者と開発者が連携し、脆弱性対応可能な情報を整えた上で情報公開する、協調的な脆弱性情報開示の重要性を改めて認識する案件となりました。なお、VPN 関連製品の脆弱性の報告の頻度が高まっており、JPCERT/CC としても幅広く情報を収集し利用者に必要な情報をタイムリーかつ適切に提供することに努めています。

> Ivanti Connect Secure および Ivanti Policy Secure の脆弱性（CVE-2023-46805 および CVE-2024-21887）に関する注意喚起
> https://www.jpcert.or.jp/at/2024/at240002.html

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。本四半期においては、2023 年度公表判定委員会が開催され、そこでの審議を経て、8 件（製品開発者数で 6 件）の公表が妥当と判定されました。公表前の最終確認が必要な 2 件を除き、6 件（製品開発者数で 6 件）を 3 月 25 日に「Japan Vulnerability Notes JP（連絡不能）一覧」に公表しました。最終確認中の 2 件に関しては、4 月中に公表する予定です。

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。

(1) CVE/FIRST VulnCon 2024 & Annual CNA Summit への参加

CVE Program が FIRST の SIG の一つである「PSIRT SIG」と合同で CVE/FIRST VulnCon 2024 & Annual CNA Summit を 3 月 25 日から 27 日の期間、米国ノースカロライナ州ラーレイにて開催しました。JPCERT/CC は本イベントで、アジアパシフィック地域における脆弱性調整の状況や課題点について講演しました。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。

CVE/FIRST VulnCon 2024 & Annual CNA Summit
https://www.first.org/conference/vulncon2024/

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 として活動を行っています。
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、76 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

（1）OpenAM Consortium 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、3 月 26 日（米国時間）に、OpenAM Consortium が JPCERT/CC を Root とした CNA として、あらたに 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 9 組織となります。

（2）CVE Program が提供するポッドキャストエピソードへの参加

CVE Program はポッドキャストシリーズ「We Speak CVE」を提供しています。本四半期に JPCERT/CC は、CVE Program の Root 組織である MITRE や CISA、INCIBE、Google、Red Hat とともに、本シリーズ中のエピソード「The Council of Roots（Root 組織協議会）」を収録しました。本エピソードでは、CVE Program における Root 組織の役割や CNA の勧誘手法、また存在する課題やその対処法、そして Root 組織がどのように協力しながら CVE Program におけるミッションを進めているか、といった Root 組織に関連するさまざまな話題をカバーしています。

We Speak CVE: The Council of Roots
https://youtu.be/QIfU4mlPx_A

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/

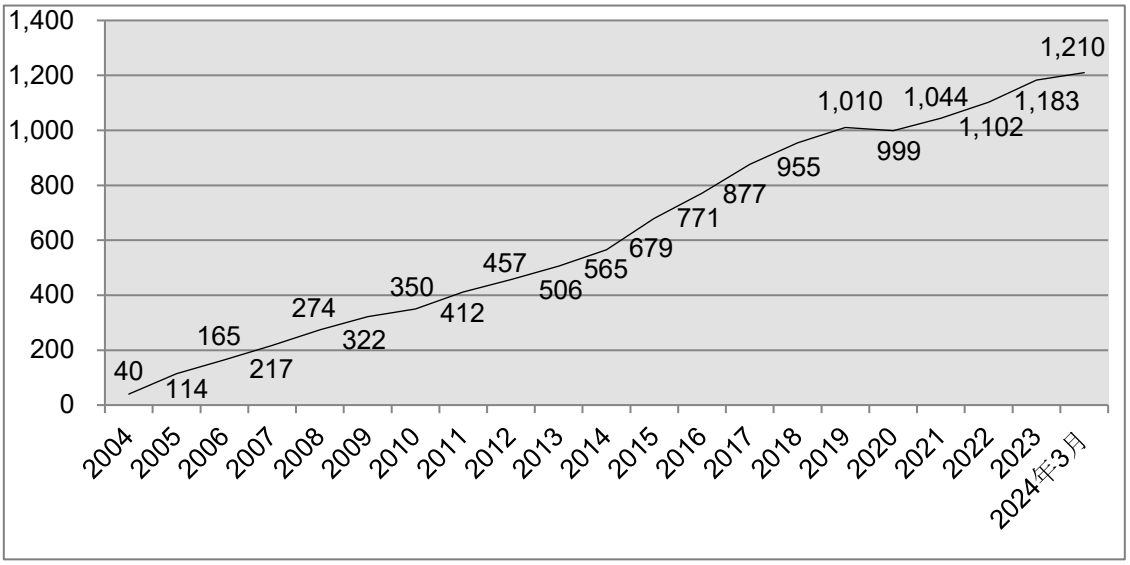
情報セキュリティ早期警戒パートナーシップガイドライン（2019 年版第 2 刷）
https://www.jpcert.or.jp/vh/partnership_guideline2019_r2.pdf

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、2024 年 3 月 31 日現在で 1,210 となっています。登録等の詳細については次の Web ページをご参照ください。

製品開発者登録
https://www.jpcert.or.jp/vh/register.html



［図 2-2：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 3 月 22 日に開催しました。当日は、脆弱性情報流通の制度運用に関する動向、PSIRT 活動のベストプラクティス調査結果、脆弱性対応演習の実施事例、製品開発者の PSIRT 活動事例、複数の製品開発者がサプライチェーンを通じて関連する脆弱性とそのコーディネーションにおける課題といったテーマについて参加者と情報を共有し意見を交換しました。

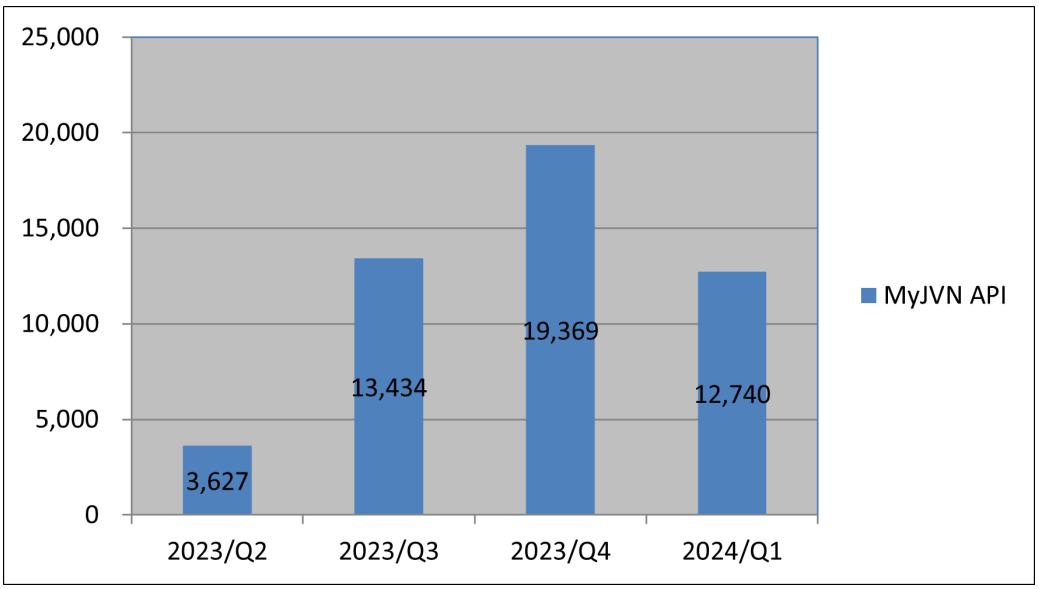
2.3. VRDA フィードによる脆弱性情報の配信

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。

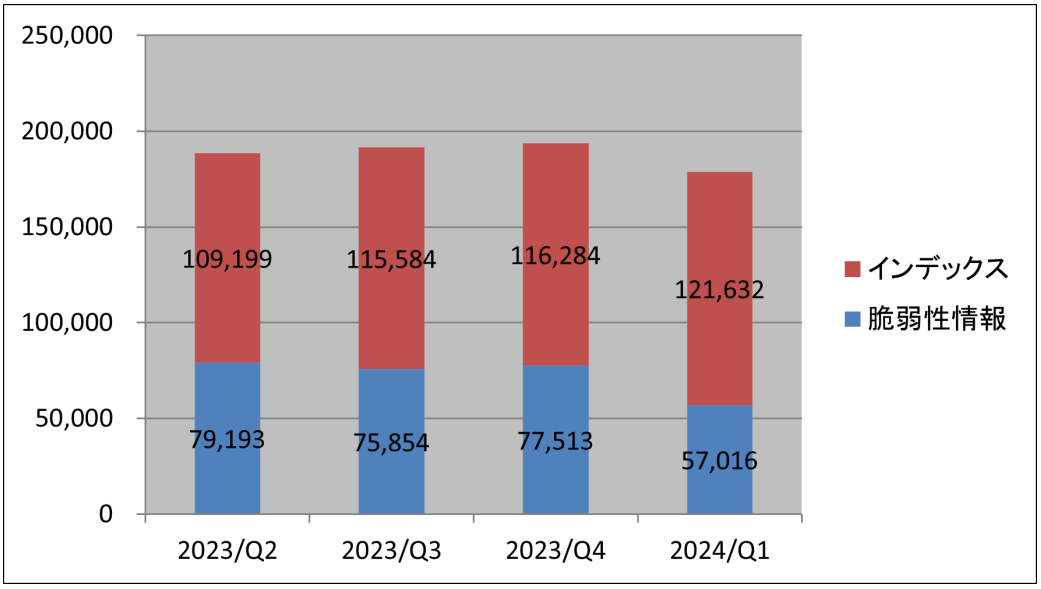
VRDA フィード 脆弱性脅威分析用情報の定型データ配信
https://www.jpcert.or.jp/vrdafeed/index.html

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。

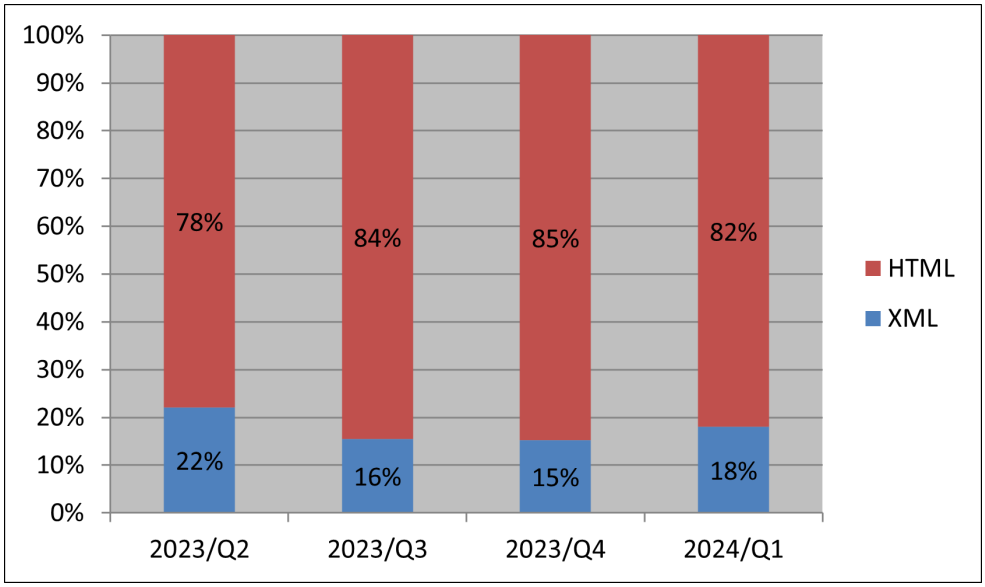


［図 2-3：VRDA フィード配信件数］



［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 5%増加しました。脆弱性情報の利用数については、約 26%減少しました。



［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 60 件でした。

3.2. 情報提供

3.2.1. 参考情報

JPCERT/CC では、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。

3.2.2. 情報提供用メーリングリストと「JPCERT/CC ICS Security Notes」

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、メーリングリ

ストには現在 1,389 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
https://www.jpcert.or.jp/ics/ics-community.html

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関係者には、「JPCERT/CC ICS Security Notes」を配信しています。「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、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）の調査やご相談等の連絡先、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。

2024-01-31　JPCERT/CC ICS Security Notes FY2023_#Q3

3.2.3. 注意喚起

JPCERT/CC では、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。

本四半期に発行した注意喚起は 0 件でした。

3.2.4. その他、特段の対策を呼びかけた脆弱性情報

JPCERT/CC では、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。

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。

3.3. 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 は、本四半期において新たな利用申し込みがなく、累計の提供数は 292 件です。

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

3.5. 制御システムセキュリティカンファレンス

2024 年 2 月 7 日（木）に「制御システムセキュリティカンファレンス 2024」をオンライン開催し、419

名の方々に参加いただきました。本カンファレンスは 2009 年 2 月から毎年開催しており、今回で 16 回目を迎えました。

昨年のアンケートでは、制御システムにおける脆弱性の管理、インシデントの検知や対応、サプライチェーンリスクへの対応などの課題を抱えているとの声を制御システムユーザーの方々からいただきました。これを踏まえ、今回のカンファレンスでは、制御システムセキュリティにおける脅威などの現状、関連業界や企業で行われているセキュリティに関する先進的な取り組み、制御システムユーザーのセキュリティに関する取り組み事例などを共有し、これらの課題解決の参考となるようなプログラム構成にしました。また、JPCERT/CC と制御システムユーザーによる共同発表や、JPCERT/CC が制御システムユーザーとのコミュニティー活動を通じて得た知見を共有する講演など、JPCERT/CC からの情報発信にも努めました。また、新たなオンライン配信の取り組みとして、制御システムユーザー3 組織によるパネルディスカッションを設けました。講演の一部については、公募を通じて広くご提案いただいたものから採択しました。

参加者の内訳は制御システムユーザーが約 4 割、制御システムベンダー等の制御システム関連組織が約 3 割、研究者やセキュリティベンダーを含めたその他組織が約 3 割でした。オンライン開催によって全国各地から視聴いただくことができました。オンライン講演のスナップショット画面を［図 3-1］に、プログラムを［表 3-1］に示します。詳細については次の Web ページをご参照ください。

制御システムセキュリティカンファレンス 2024
https://www.jpcert.or.jp/event/ics-conference2024.html
制御システムセキュリティカンファレン 2024 講演資料
https://www.jpcert.or.jp/present/#year2024

JPCERT/CC Eyes：制御システムセキュリティカンファレンス 2024 開催レポート
https://blogs.jpcert.or.jp/ja/2024/03/ics-conference2024.html

［図 3-1：制御システムセキュリティカンファレンス 2024 講演］

［表 3-1：制御システムセキュリティカンファレンス 2024 のプログラム］

「開会ご挨拶」 経済産業省 サイバーセキュリティ・情報化審議官　上村 昌博 氏
(1)「制御システムセキュリティの現在と展望～この 1 年間を振り返って～」 一般社団法人 JPCERT コーディネーションセンター 技術顧問 宮地 利雄
(2)「インダストリー4.0 時代の CNC 機械に潜むサイバーセキュリティリスク」 トレンドマイクロ株式会社 セキュリティエバンジェリスト　岡本 勝之 氏
(3)「攻撃者視点からみた OT 環境の通信監視　スモールスタートから始めてみよう」 株式会社サイバーディフェンス研究所 技術統括部 OT セキュリティグループ プリンシパルコンサルタント　安井 康二 氏
(4)「制御システムの脆弱性管理の課題とグローバルにおける事例」 Claroty Ltd. APJ Sales／Solution Engineer　加藤 俊介 氏
(5)「ICS セキュリティポリシーの現場への浸透および具体化に関する支援検討」 参天製薬株式会社 Digital＆IT 本部／Global Cybersecurity Manager　正木 文統 氏 一般社団法人 JPCERT コーディネーションセンター 制御システムセキュリティ対策グループ　堀 充孝
(6)「ICS 関連のセキュリティインシデント対応に備えて - 製造業を例に対応体制の整備上の課題と対策の第一歩を解説 -」 一般社団法人 JPCERT コーディネーションセンター 制御システムセキュリティ対策グループ マネージャー　河野 一之
(7)「製造業 10 社の実務者で議論した、制御系 SIRT が日常で取り組みたいインシデント対応訓練」 株式会社資生堂 情報セキュリティ部　大林 世昇 氏
「閉会挨拶」 一般社団法人 JPCERT コーディネーションセンター 理事　椎木 孝斉

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 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

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等を目的に、JPCERT/CC は海外 CSIRT との連携強化を進めています。また、APCERT（4.2.1 参照）や FIRST（4.2.2 参照）で主導的な役割を担う等、多国間の CSIRT 連携の枠組みにも積極的に参加しています。

4.2.1. APCERT（Asia Pacific Computer Emergency Response Team）

JPCERT/CC は、アジア太平洋地域の CSIRT コミュニティーである APCERT において、2003 年 2 月の発足時から継続して Steering Committee（運営委員会）のメンバーに選出されており、また、その事務局も担当しています。
APCERT の詳細および APCERT における JPCERT/CC の役割については次の Web ページをご参照ください。

JPCERT/CC within APCERT
https://www.jpcert.or.jp/english/apcert/

4.2.1.1. APCERT Steering Committee 会議の実施

APCERT の Steering Committee が、1 月 18 日に電話会議を、また 2 月 26 日にはタイのバンコクで対面会議を行い、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、毎月のオンラインによる理事会に加えて、1 月 23 日から 25 日にかけてアメリカのワシントンで開催された対面での理事会にも参加しました。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

4.2.2.1. CVE/FIRST VulnCon 2024 & Annual CNA Summit での講演（3 月 26 日）

脆弱性コーディネーションに関わる組織や PSIRT 担当者らを対象とした CVE/FIRST VulnCon 2024 & Annual CNA Summit がアメリカのノースカロライナ州・ローリーで 3 月 25 日から 27 日まで開催されました。JPCERT/CC は“Pushing Coordinated Vulnerability Disclosure forward in Asia Pacific”というタイトルで講演を行い、日本国内での CNA の取り組みに加えて、アジア地域の近隣国との脆弱性コーディネーションに関わる協力を促進する活動について紹介しました。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。

CVE/FIRST VulnCon 2024 & Annual CNA Summit
https://www.first.org/conference/vulncon2024/

4.3. 海外 CSIRT 等の来訪および訪問

4.3.1. 香港 HKCERT の来訪（1 月 24 日）

香港の HKCERT 職員 2 名が JPCERT/CC のオフィスに来訪し、双方の活動の状況について情報共有を図りました。

4.3.2. タイ ThaiCERT を訪問（2 月 27 日）

タイの ThaiCERT 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。

4.3.3. インドネシア IDSIRTII/CC を訪問（2 月 29 日）

インドネシアの IDSIRTII/CC 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。

4.3.4. ベルギー サイバーセキュリティセンター（CCB）の来訪（3 月 13 日）

ベルギーのサイバーセキュリティセンター長および 2 名の職員が JPCERT/CC のオフィスに来訪し、双方の活動の状況について情報共有を図りました。

4.4. その他国際会議への参加

4.4.1. ITU-T SG17 会議への参加（2 月 21～23 日）

スイスのジュネーブで開催された ITU-T SG17 会議の一部に参加しました。JPCERT/CC は X.1060 サイバーディフェンスセンターという標準の改定に関する情報を収集しました。この会議に参加した日本

国内の専門家と協力し、X.1060 の普及啓発にも努めています。

4.4.2. APRICOT での講演（2 月 29 日）

通信事業者などに所属する技術者向けのカンファレンスである APRICOT がタイのバンコクで 2 月 21 日から 3 月 1 日まで開催されました。JPCERT/CC はインターネットセキュリティに関するセッションで「IoT Devices Leveraged in Cyber Attacks and How Botnets are Created and Used: Findings through JPCERT/CC's Coordination」というタイトルの講演を行い、Mirai をはじめとした IoT 機器を標的とするマルウェアの傾向と、実際に対応したインシデント事例などを紹介しました。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。

APRICOT 2024
https://2024.apricot.net/

4.5. 国際標準化活動

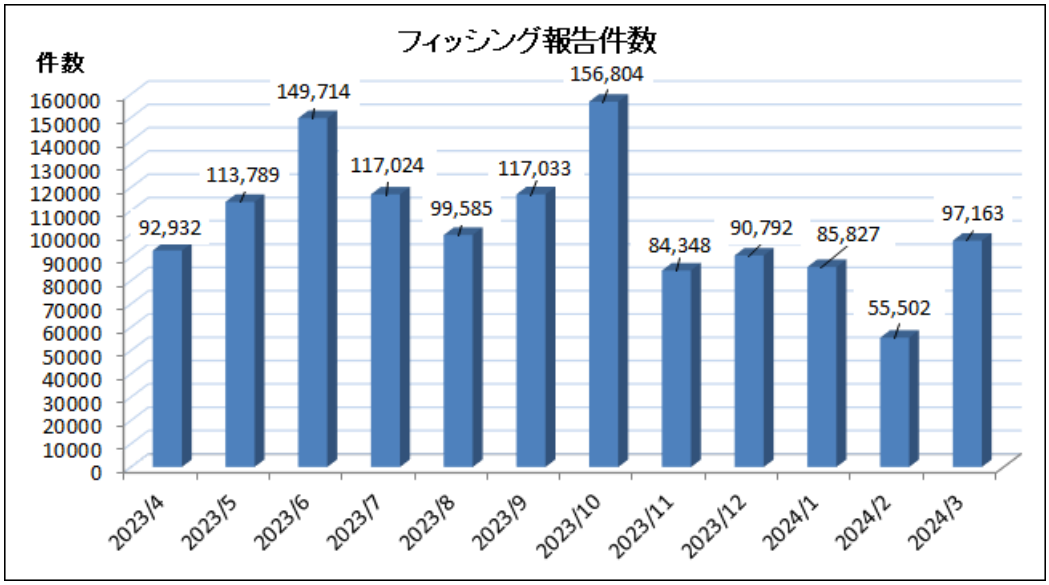
IT セキュリティ分野の標準化を行うための組織 ISO/IEC JTC-1/SC27 で進められている標準化活動のうち、作業部会 WG3（セキュリティの評価・試験・仕様に関する標準化を担当）で検討されている標準化作業の一部と、WG4（セキュリティコントロールとサービスに関する標準化を担当）で検討されているインシデント管理に関する標準の改定に、情報処理学会の情報規格調査会を通じて参加しています。
本四半期は、WG3 において、脆弱性情報公開手法に関する既存文書の更新についてコメントを提出しました。

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・問い合わせの受付

フィッシング報告件数は、例年低下傾向となる旧正月時期を含む 2 月に減少したものの、依然多くの報告を受けています。



［図 5-1：1 年間のフィッシング報告件数（月別）］

報告件数の内訳では、「Amazon」をかたるフィッシングの報告数が最も多く、全体の約 13.1%を占めていました。次いで、「イオンカード」をかたるフィッシングの報告も多く、全体の約 12.4%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 11 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。

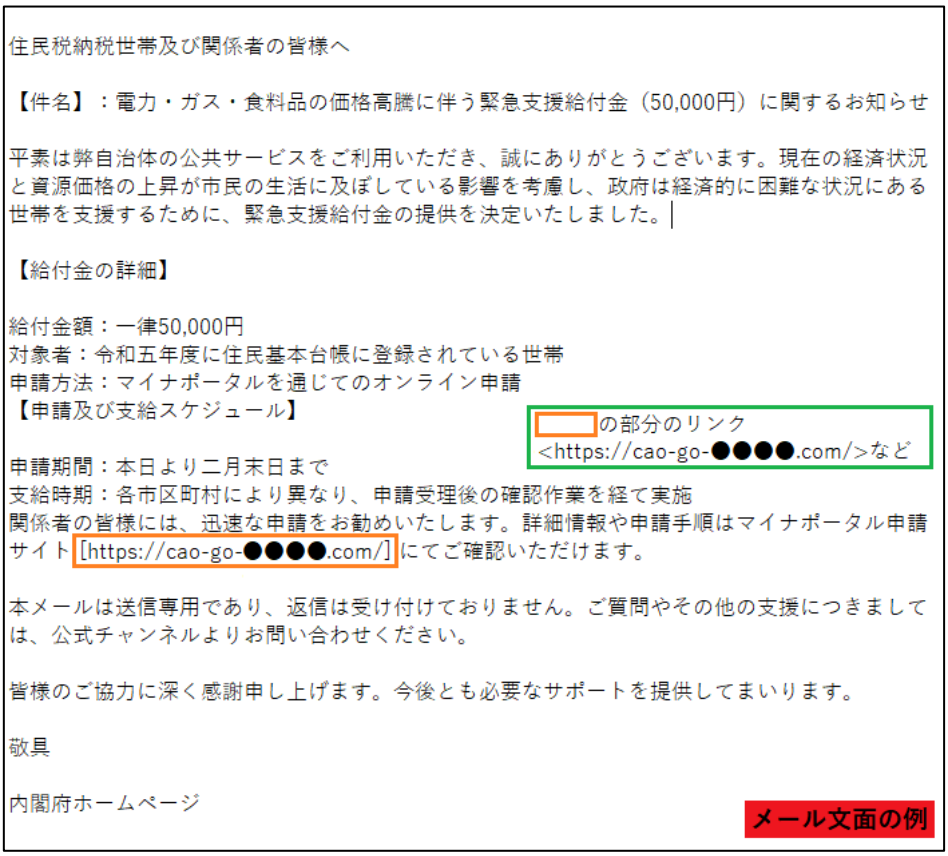
- 国税庁をかたるフィッシング：1 件
- Apple をかたるフィッシング：1 件
- メルカリをかたるフィッシング：1 件
- NTT ドコモをかたるフィッシング：1 件
- りそな銀行をかたるフィッシング：1 件
- ソニー銀行をかたるフィッシング：1 件
- イオンカードをかたるフィッシング：1 件
- ゆうちょ銀行をかたるフィッシング：1 件
- 内閣府を装うフィッシング：1 件
- ビックカメラをかたるフィッシング：1 件
- JR 西日本をかたるフィッシング：1 件

- 東京電力をかたるフィッシング：1 件

本四半期の報告件数は、旧正月にあたる 2 月に減少し、例年と同様の月次推移をたどりました。その後は報告件数の増加も考えられるため、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、他のブランドをかたり詐取した情報をリアルタイムで使用して、オンライン決済サービスのオンラインで行う本人確認機能(eKYC：electric Know Your Customer)を突破しようとしたフィッシング（[図 5-2]）や、内閣府をかたり電力・ガス・食料品等価格高騰緊急支援給付金を申請するために偽のマイナポータルへのアクセスを求めるフィッシング（[図 5-3]）などが発生しました。犯罪者が、詐取した情報をリアルタイムで悪用する事例も増加しており、利用者、事業者ともに引き続き注意が必要です。

［図 5-2：オンライン本人確認機能を突破しようとするフィッシングの例 ］

https://www.antiphishing.jp/news/alert/mercari_20240122.html



［図 5-3：内閣府をかたるフィッシングメールの例 ］
https://www.antiphishing.jp/news/alert/mynaportal_20240207.html

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。

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

2024/01 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/202401.html

2024/02 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/202402.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大する予定です。

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、法制度の整備状況等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等について議論し、取りまとめました。2 月には、今年度の活動報告会を兼ねた WG 会合を広く参加者を募るオープンな会として開催し、予定している改定内容の説明やフィッシング詐欺に係るトピックなどを報告しました。

- 技術・制度検討ワーキンググループ会合（第 5 回）
  日時：1 月 24 日（火）16：30～18：30
- 技術・制度検討ワーキンググループ会合（第 6 回兼報告会）
  日時：2 月 27 日（金）15：00～17：00

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 115 回運営委員会（オンライン）
  日時：2 月 15 日（木）16：00～18：00

- 第 116 回運営委員会（TOPPAN エッジ会議室＋オンライン）
  日時：3 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：1 月- 3 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：1 月 30 日（火）16：30～18：30（オンラインおよび JPCERT/CC 会議室）

- 第 9 回フィッシング対策勉強会（オンライン）
  日時：2 月 15 日（木）14：00～15：00

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。

2024-01-18
JPCERT/CC インシデント報告対応レポート［2023 年 10 月 1 日～2023 年 12 月 31 日］
https://www.jpcert.or.jp/pr/2024/IR_Report2023Q3.pdf

2024-03-27
JPCERT/CC Incident Handling Report [October 1, 2023 - December 31, 2023]
https://www.jpcert.or.jp/english/doc/IR_Report2023Q3_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。

2024-02-15
JPCERT/CC インターネット定点観測レポート［2023 年 10 月 1 日～2023 年 12 月 31 日］
https://www.jpcert.or.jp/tsubame/report/report202310-12.html
https://www.jpcert.or.jp/tsubame/report/TSUBAME_Report2023Q3.pdf

2024-03-27
JPCERT/CC Internet Threat Monitoring Report [October 1, 2032 - December 31, 2023]
https://www.jpcert.or.jp/english/doc/TSUBAMEReport2023Q3_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。

2024-01-18
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 4 四半期（10 月～12 月）］
https://www.jpcert.or.jp/pr/2023/vulnREPORT_2023q4.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 7 件の記事を公表しました。

日本語版発行件数：7 件　https://blogs.jpcert.or.jp/ja/

2024-03-26　ランサムウェア攻撃事案から見る、ファーストレスポンダー同士の情報共有が必要な理由

2024-03-18　JSAC2024 開催レポート～Workshop & Lightning Talk～
2024-03-14　制御システムセキュリティカンファレンス 2024 開催レポート
2024-03-11　JSAC2024 開催レポート～DAY 2～
2024-03-04　JSAC2024 開催レポート～DAY 1～
2024-02-21　PyPI を悪用した攻撃グループ Lazarus のマルウェア拡散活動
2024-02-20　TSUBAME レポート Overflow（2023 年 10～12 月）

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

2024-03-29　TSUBAME Report Overflow (Oct-Dec 2023)
2024-03-29　JSAC2024 -Day 1-
2024-02-28　New Malicious PyPI Packages used by Lazarus

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）：
「情報共有の不条理～なぜ共有の成果は見えにくいのか～」
SecureGRID アライアンス情報交換会（主催：ラック、講演日：2024 年 2 月 15 日）
(2) 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）：
「サイバー攻撃の被害公表を組織の『リスク』にしないためにできること」
「サイバー脅威インテリジェンスをめぐる内外動向と産官学連携」研究会（主催：防衛研究所、講演日：2024 年 3 月 1 日）
(3) 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）：
「業界を超えてどう情報共有していくことができるのか～サイバー攻撃情報の共有・公表ガイダンスのポイントから～」
第 15 回公開討論会（主催：日本セキュリティ・マネジメント学会、講演日：2024 年 3 月 2 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）：
「サイバー攻撃の被害公表を組織の『リスク』にしないためにできること」
情報セキュリティ戦略セミナー2024（主催：日経ビーピー、講演日：2024 年 3 月 19 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等を行いました。

(1) 第 8 回 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：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：2024 年 2 月 15 日～16 日）

(2) 第 1 回 交通 ISAC カンファレンス
（主催：一般社団法人交通 ISAC、開催日：2024 年 2 月 29 日）
(3) 第 14 回 TCG 日本支部（JRF）公開ワークショップ
（主催：Trusted Computing Group、開催日：2024 年 2 月 29 日）
(4) Security Days Spring 2024
（主催：株式会社ナノオプト・メディア、開催日：2024 年 3 月 5 日、7 日、12 日～15 日）
(5) セキュリティーフォーラム 2024
（主催：一般社団法人日本スマートフォンセキュリティ協会、開催日：2024 年 3 月 6 日）
(6) Cybersecurity Awards 2023
（主催：デジタル政策フォーラム、応募期間：2023 年 11 月 1 日～12 月 31 日、表彰：2024 年 3 月 15 日）

■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　：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