

JPCERT/CC 活動四半期レポート

2024年4月1日～2024年6月30日



一般社団法人 JPCERT コーディネーションセンター

2024年7月18日

JPCERT **CC**®

目次

活動概要トピックス	4
36th Annual FIRST Conference の開催にローカルホストとして協力（6月9日～14日）	4
第1章 早期警戒	5
1.1 インシデント対応支援	5
1.1.1 インシデントの傾向	5
1.1.1.1 フィッシングサイト	5
1.1.1.2 Web サイト改ざん	6
1.1.2 インシデント対応事例	6
1.1.2.1 PAN-OS GlobalProtect の脆弱性への対応	7
1.1.3 インシデントに関する情報提供のお願い	7
1.2 情報収集・分析	7
1.2.1 情報提供	8
1.2.1.1 注意喚起	8
1.2.1.2 Weekly Report	8
1.2.1.3 早期警戒情報	9
1.2.1.4 CyberNewsFlash	9
1.2.2 情報収集・分析・提供（早期警戒活動）事例	9
1.2.2.1 Palo Alto Networks 社製 PAN-OS GlobalProtect の OS コマンドインジェクションの脆弱性（CVE-2024-3400）に関する情報発信	9
1.2.2.2 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）に関する情報発信	10
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	10
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	10
1.3.1.1 TSUBAME の観測データの活用	11
1.3.1.2 TSUBAME 観測動向	11
第2章 脆弱性関連情報流通促進活動	14
2.1 脆弱性関連情報の取り扱い状況	14
2.1.1 JPCERT/CC における脆弱性関連情報の取り扱い	14
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	15
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	16
2.1.2.2 国際調整または独自調整で取り扱った脆弱性	16
2.1.3 連絡不能開発者対応	17
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	17
2.1.4.1 RSA Conference 2024 ならびに複数会合への参加	17

2.1.5	CNA としての活動	18
2.1.5.1	国内 CNA 会合第 4 回「CNA Talk」開催	18
2.2	日本国内の脆弱性情報流通体制の整備	18
2.2.1	日本国内製品開発者との連携	19
2.3	VRDA フィードによる脆弱性情報の配信	20
第 3 章	国内連携活動	22
3.1	業界団体やコミュニティー等との連携活動	22
3.1.1	貿易会 ISAC	22
3.1.2	SICE/JEITA/JEMIMA セキュリティ合同 WG	22
3.1.3	セプターカウンシル運営委員会	22
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	23
3.2.1	早期警戒情報提供先との連携促進	23
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	23
3.3	情報・ツール等の提供	23
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	23
3.3.2	JPCERT/CC ICS Security Notes	23
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	24
第 4 章	国際連携活動	25
4.1	海外 CSIRT 構築支援および運用支援活動	25
4.2	国際 CSIRT 間連携	25
4.2.1	APCERT (Asia Pacific Computer Emergency Response Team)	25
4.2.1.1	APCERT Steering Committee 会議の実施	25
4.2.2	FIRST (Forum of Incident Response and Security Teams)	26
4.2.3	36th Annual FIRST Conference への参加と開催支援 (6 月 9 日~14 日)	26
4.3	海外 CSIRT 等の来訪および訪問	27
4.3.1	フィンランド NCSC-FI の来訪 (4 月 16 日)	27
4.3.2	モンゴル Public CSIRT/CC および National CSIRT への訪問 (5 月 13 日、16 日)	27
4.4	その他国際会議への参加	27
4.4.1	Locked Shields に参加 (4 月 23 日~26 日)	27
4.4.2	NatCSIRT 2024 への参加 (6 月 14 日~15 日)	27
4.5	国際標準化活動	28
第 5 章	フィッシング対策協議会事務局の運営	29
5.1	フィッシングに関する報告・問い合わせの受け付け	29
5.2	情報収集/発信	30
5.2.1	フィッシングの動向等に関する情報発信	30
5.2.2	定期報告	30
5.2.3	フィッシングサイト URL 情報の提供	31
5.2.4	フィッシング対策ガイドライン等の改定作業	31
第 6 章	フィッシング対策協議会の会員組織向け活動	33
6.1	運営委員会開催	33

6.2	ワーキンググループ会合等 開催支援	33
第7章	公開資料	34
7.1	インシデント報告対応レポート	34
7.2	インターネット定点観測レポート	34
7.3	脆弱性関連情報に関する活動報告	35
7.4	公式ブログ「JPCERT/CC Eyes」	35
第8章	その他の活動	36
8.1	講演	36
8.2	執筆	36
8.3	協力・後援	36

本活動は、経済産業省より委託を受け、「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

36th Annual FIRST Conference の開催にローカルホストとして協力 (6月9日～14日)

FIRST (Forum of incident Response and Security Teams) は国際的な CSIRT のコミュニティーであり、2024年6月末現在、世界の111の国・地域から748チームが加盟しています。FIRSTでは、サイバーインシデントの予防、対応、技術分析等に関する最新動向の情報交換およびインシデント対応における連携強化を目的に年次会合を毎年開催しています。本年は6月9日から14日にかけて福岡で開催されました。

今回は“Bridging Security Response Gaps”をテーマに掲げて企画されました。6年ぶりのアジア地域での開催、さらに15年ぶりの日本での開催への関心も高く、講演募集に対して70あまりの発表枠に過去最多の294件の応募があり、参加者数も99の国・地域から997名に上りました。

JPCERT/CCは、本会合のローカルホストを務めました。海外からの参加者のビザ申請書類作成や国内関係者との調整などでFIRSTを支援するとともに、代表理事の歌代が開会セレモニーで歓迎のスピーチを行いました。展示エリアではローカルホストのブースを設置し、JPCERT/CCが提供しているインシデント調査ツールのデモ等を含めた活動全般の紹介も行いました。

本会合への支援を通じて、FIRSTに対するJPCERT/CCの長年の貢献をアピールするとともに、JPCERT/CCのプレゼンスを強化することができました。今後も、イベントやSIGなどFIRSTのさまざまな活動に積極的に携わり、CSIRT間の国際連携促進に寄与してまいります。

第36回FIRST年次会合についての詳細は、次のWebページをご参照ください。また、国際連携活動の章でも同会合について紹介しています(4.2.3)。

- 36th Annual FIRST Conference
<https://www.first.org/conference/2024/>

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 15,396 件、インシデント件数ベースでは 6,604 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 4,176 件でした。前四半期の 4,602 件と比較して 9% 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.jpccert.or.jp/pr/2024/IR_Report2024Q1.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 5,025 件で、前四半期の 4,781 件から 5% 増加しました。また、前年度同期（6,186 件）との比較では、19% の減少となりました。

*1 報告件数は、報告者から寄せられた Web フォーム、メール、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。

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	4月	5月	6月	本四半期合計	割合
国内ブランド	1,101	1,048	877	3,026	60%
国外ブランド	293	336	332	961	19%
ブランド不明	291	349	398	1,038	21%
全ブランド合計	1,685	1,733	1,607	5,025	

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 78%、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% で、それぞれ最も多くを占めました。

海外ブランドでは、Amazon や Apple を装ったフィッシングサイトが 8 割以上を占めました。

国内ブランドでは、メルカリや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。

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割合は、国内が 32%、国外が 68% であり、前四半期（国内が 30%、国外が 70%）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 43 件でした。前四半期の 57 件から 25% 減少しています。

本四半期は、ブラウザの通知機能を悪用して不審サイトに転送させる事例を確認しています。正規の Web サイトに不正な PHP のコードが挿入されており、アクセスしてきたユーザーのブラウザの通知機能で不審なサイトへ転送される仕組みになっていました。また、不正な PHP のコードは、攻撃者が用意したドメインに DNS クエリを送信し、レスポンスの TXT レコードに含まれるデータを転送先の URL として使用していました。また、攻撃者は不正な PHP コードを正規の Web サイトに挿入するために、改ざんサイトに WPCode と呼ばれるプラグインをインストールしていました。

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。

1.1.2.1 PAN-OS GlobalProtect の脆弱性への対応

2024年4月12日、Palo Alto Networks社はPAN-OSのGlobalProtect機能にOSコマンドインジェクションの脆弱性（CVE-2024-3400）があることを公表しました。GlobalProtectはリモートアクセス（VPN）などを提供する機能で、本脆弱性の悪用により、認証されていない遠隔の第三者に管理者権限で任意のコードを実行される可能性があります。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4月13日に注意喚起を行いました。

- Palo Alto Networks社製PAN-OS GlobalProtectのOSコマンドインジェクションの脆弱性（CVE-2024-3400）に関する注意喚起

<https://www.jpcert.or.jp/at/2024/at240009.html>

JPCERT/CCでは複数の組織から本脆弱性による被害があったとの報告を受けました。被害の多くは、脆弱性が発表されパッチが公表された4月14日以降に発生し、機器の構成ファイルが外部から閲覧可能な場所にコピーされ漏えいしていました。脆弱性の回避策であるデバイステレメトリを無効化していた組織では攻撃を阻止できていました。

また、JPCERT/CCでは、本脆弱性の悪用により侵害された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する通知を、外部組織から提供された情報をもとに行いました。4月20日時点では侵害された可能性のある機器が国内に252台ありましたが、それらすべての組織に通知し、6月11日時点で86台まで減少しています。通知を受けて初めて侵害に気付いた組織が多く、攻撃者によって改ざんされたコンテンツが機器の脅威防御機能により自動的に修正されたことに気付かないケースもありました。悪用が確認されている脆弱性が公表された場合には機器のアップデートをする前に侵害の有無を確認することを推奨します。

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

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.jpccert.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：12 件（うち更新情報が 6 件） <https://www.jpccert.or.jp/at/>

- 2024-04-10 2024 年 4 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)
- 2024-04-13 Palo Alto Networks 社製 PAN-OS GlobalProtect の OS コマンドインジェクションの脆弱性 (CVE-2024-3400) に関する注意喚起 (公開)
- 2024-04-15 Palo Alto Networks 社製 PAN-OS GlobalProtect の OS コマンドインジェクションの脆弱性 (CVE-2024-3400) に関する注意喚起 (更新)
- 2024-04-15 Palo Alto Networks 社製 PAN-OS GlobalProtect の OS コマンドインジェクションの脆弱性 (CVE-2024-3400) に関する注意喚起 (更新)
- 2024-04-17 Palo Alto Networks 社製 PAN-OS GlobalProtect の OS コマンドインジェクションの脆弱性 (CVE-2024-3400) に関する注意喚起 (更新)
- 2024-04-19 Palo Alto Networks 社製 PAN-OS GlobalProtect の OS コマンドインジェクションの脆弱性 (CVE-2024-3400) に関する注意喚起 (更新)
- 2024-04-22 Palo Alto Networks 社製 PAN-OS GlobalProtect の OS コマンドインジェクションの脆弱性 (CVE-2024-3400) に関する注意喚起 (更新)
- 2024-04-25 Palo Alto Networks 社製 PAN-OS GlobalProtect の OS コマンドインジェクションの脆弱性 (CVE-2024-3400) に関する注意喚起 (更新)
- 2024-05-15 2024 年 5 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)
- 2024-05-15 Adobe Acrobat および Reader の脆弱性 (APSB24-29) に関する注意喚起 (公開)
- 2024-06-12 2024 年 6 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)
- 2024-06-25 Operation Blotless 攻撃キャンペーンに関する注意喚起 (公開)

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.jpccert.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 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.jpccert.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：3 件（うち更新情報は 1 件） <https://www.jpccert.or.jp/newsflash/>

2024-04-01 XZ Utils に悪意のあるコードが挿入された問題（CVE-2024-3094）について

2024-04-09 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）

2024-05-30 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

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。

1.2.2.1 Palo Alto Networks 社製 PAN-OS GlobalProtect の OS コマンドインジェクションの脆弱性（CVE-2024-3400）に関する情報発信

2024 年 4 月 12 日（現地日付）、Palo Alto Networks は、PAN-OS の GlobalProtect 機能における OS コマンドインジェクションの脆弱性（CVE-2024-3400）に関するアドバイザリを公表しました。GlobalProtect はリモートアクセス（VPN）などを提供する機能です。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にルート権限で任意のコードを実行される可能性があります。アドバイザリの公表当時の同社の声明によれば、本脆弱性を悪用した攻撃が確認されているものの攻撃の発生は限定的であるとのことでしたが、今後本脆弱性を悪用する攻撃が増加する可能性を踏まえ、JPCERT/CC は同月 13 日（土）に注意喚起を発行し、緩和策の適用を推奨しました。

その後、同月 15 日（現地日付）に同社は本脆弱性を修正する Hotfix の提供を開始しました。そして、17 日（現地日付）には本脆弱性を実証するコード（Proof-of-Concept）が公開されました。JPCERT/CC

は注意喚起を随時更新し、日本語で最新の状況を発信し、必要な対策や調査の実施を推奨しました。

- Palo Alto Networks 社製 PAN-OS GlobalProtect の OS コマンドインジェクションの脆弱性 (CVE-2024-3400) に関する注意喚起

<https://www.jpccert.or.jp/at/2024/at240009.html>

1.2.2.2 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) に関する情報発信

2024 年 5 月 27 日 (現地日付) に Check Point Software Technologies がアドバイザリを公表し、同月 24 日 (現地日付) までに同社の一部の顧客に対する不正アクセスの試みを確認したことを明らかにしました。攻撃者は、パスワード認証のみに依存するローカルアカウントを使用し、同社の一部の顧客のネットワークに VPN 機能を用いたログインを試みていました。同社は、攻撃を防ぐための対策として、ローカルアカウントを使用していない場合は無効化することなどを推奨しました。

翌 28 日 (現地日付)、同社はアドバイザリを更新し、その後の調査で同社製品の VPN 機能における情報漏えいの脆弱性 (CVE-2024-24919) を発見したと公表しました。本脆弱性が悪用されると、遠隔の第三者によって同製品から機微な情報が窃取される可能性があり、同社は影響を受ける機能や製品の利用者に対策適用を呼びかけました。また、本脆弱性を悪用する攻撃が 2024 年 4 月から確認されていたと示す公開情報も確認されました。

本脆弱性を詳細に解説した情報も公表されており、今後本脆弱性を悪用する攻撃が増加する可能性があったことから、影響を受ける製品の利用者に対策を促すため、JPCERT/CC は同月 30 日に CyberNewsFlash を公開しました。

- 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

<https://www.jpccert.or.jp/newsflash/2024053001.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.jpccert.or.jp/tsubame/index.html>

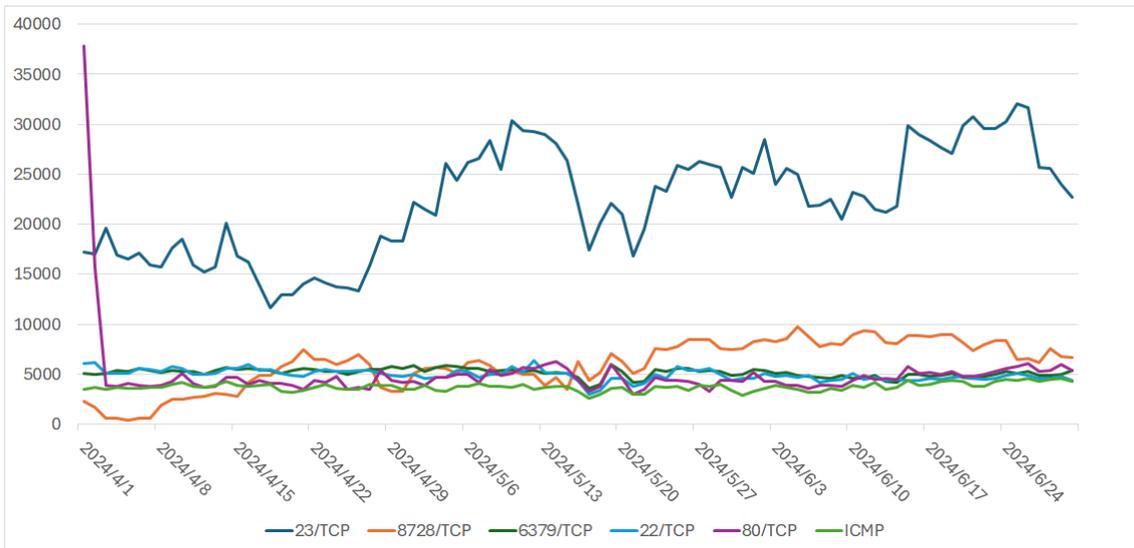


図 1.1 TSUBAME で観測された宛先ポートの上位 1 位から 5 位のパケット数
(2024 年 4 月 1 日～6 月 30 日)

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、2024 年 1 月から 3 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 (2024 年 1～3 月)
<https://www.jpcert.or.jp/tsubame/report/report202401-03.html>
- TSUBAME レポート Overflow (2024 年 1～3 月)
https://blogs.jpcert.or.jp/ja/2024/05/tsubame_overflow_2024-01-03.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。

また、過去 1 年間 (2023 年 7 月 1 日～2024 年 6 月 30 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。

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 番目に多かったのは 8728/TCP 宛の通信でした。これは Mikro Tik 社のルーターで API が使用するポート番号であるた

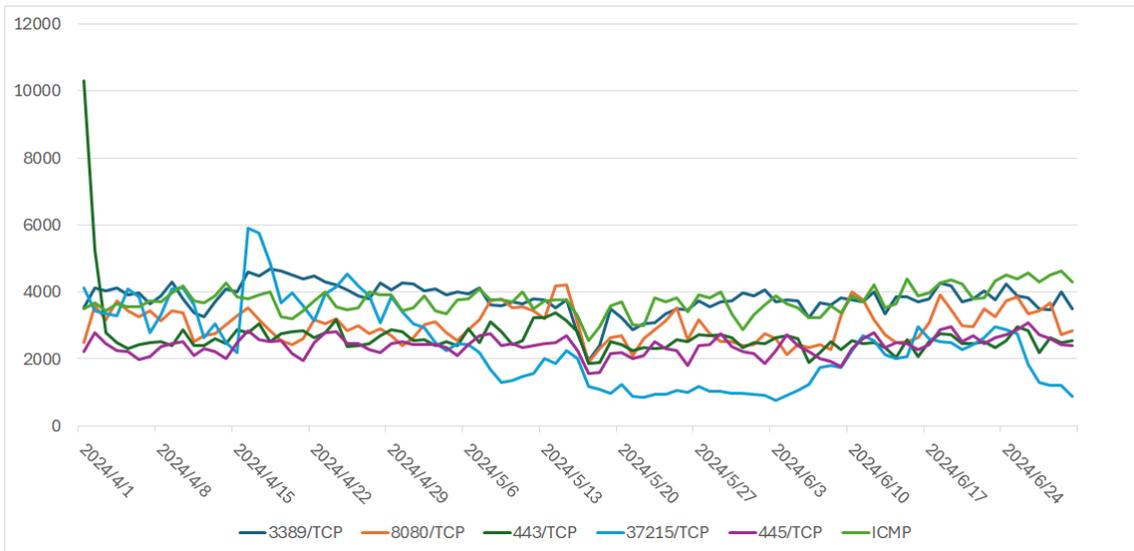


図 1.2 TSUBAME で観測された宛先ポートの上位 6 位から 10 位のパケット数
(2024 年 4 月 1 日～6 月 30 日)

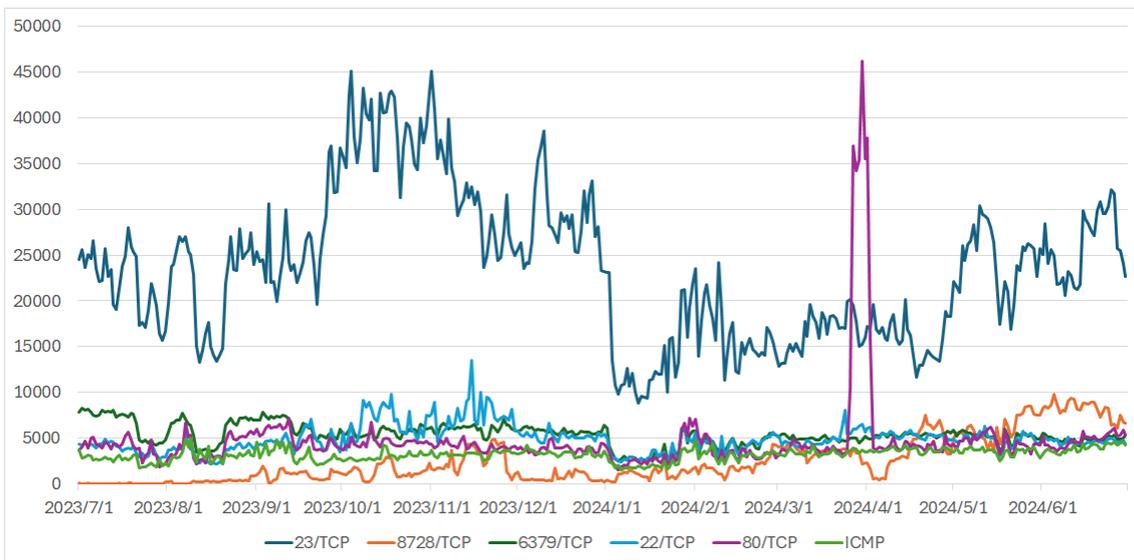


図 1.3 TSUBAME で観測された宛先ポートの上位 1 位から 5 位のパケット数
(2023 年 7 月 1 日～2024 年 6 月 30 日)

め、同ルーターの探索を目的としたパケットの可能性がります。2 位に 8728/TCP が入ったため、前四半期と比較し、第 3 位から第 5 位までの順位が一つずつ変動しました。6 位から 10 位に関しては、3389/TCP と 8080/TCP の順位が入れ替わりました。

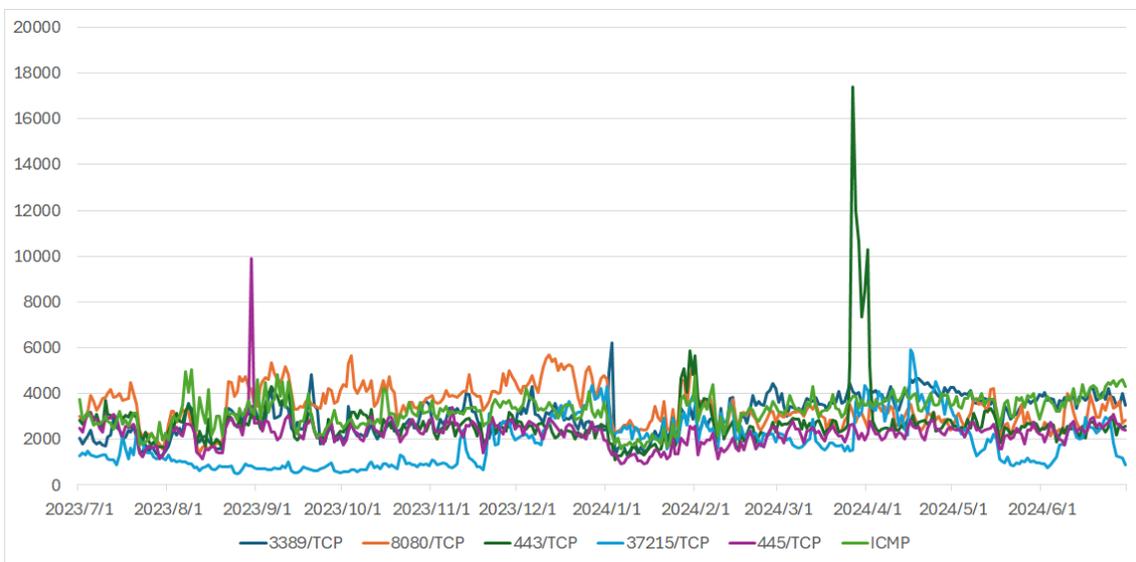


図 1.4 TSUBAME で観測された宛先ポートの上位 6 位から 10 位のパケット数
(2023 年 7 月 1 日～2024 年 6 月 30 日)

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、専門家コミュニティ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「ソフトウェア製品等の脆弱性関連情報に関する取扱規程」（平成 29 年経済産業省告示第 19 号）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。

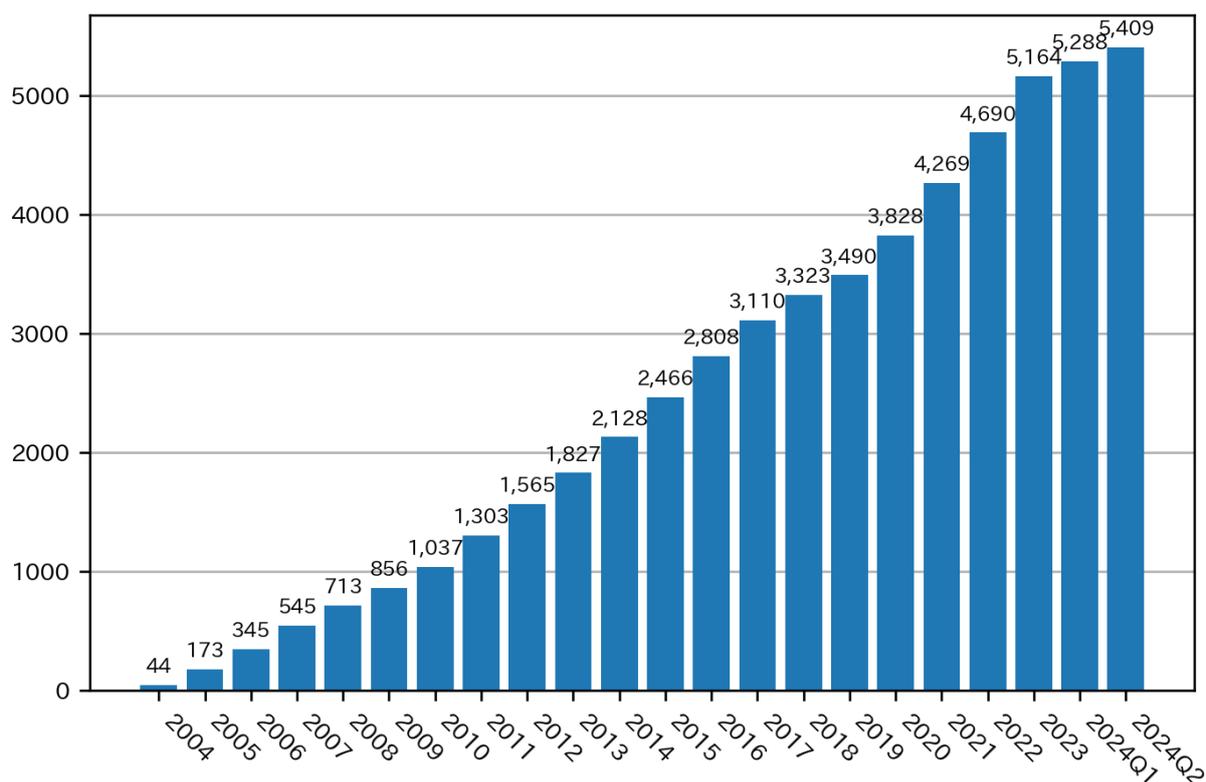


図 2.1 JVN 公表累積件数

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 121 件（累計 5,409 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：33 件（そのうち調整不能案件が 2 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：3 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。

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#43215077
 UNIVERSAL PASSPORT RX における複数の脆弱性
<https://jvn.jp/jp/JVN43215077/>

本件は、日本システム技術株式会社が提供する大学向けの統合管理ソフトウェア UNIVERSAL PASSPORT RX に影響する複数の脆弱性に関する情報です。調整を進める中で、製品開発者が同製品のすべての導入組織を把握・サポートしていることが分かりました。そこで、製品開発者から導入組織に個別に連絡していただき、一般公表までに確実に対策が適用できるように JVN での公表日程を調整しました。脆弱性情報を公表する最終的な目的は、ユーザーが対策を適用し、製品を安全に利用できる状況にすることです。そのために、JPCERT/CC では製品開発者とともに、より効果的な脆弱性情報流通のあり方を検討し、脆弱性情報を公表しています。

2.1.2.2 国際調整または独自調整で取り扱った脆弱性

- JVNTA#90371415
 Windows カーネルドライバの IOCTL 処理におけるアクセス制御不備の脆弱性
<https://jvn.jp/ta/JVNTA90371415/>

WDF（Windows Driver Framework）および WDM（Windows Driver Model）カーネルドライバの IOCTL（Input/Output Control：デバイス入出力制御）処理におけるアクセス制御不備の脆弱性の詳細と対処方法を示した、主にドライバー開発ベンダーに向けた注意喚起のためのアドバイザリです。本アドバイザリの共同執筆者である Broadcom 春山敬宏氏から複数ベンダーのドライバーに関する脆弱性の報告を受け取り、JPCERT/CC では各ベンダーと脆弱性調整を実施しました。これらの調整を通じて、特定ベンダーに限定せず、ドライバーの開発者や利用者に対して広く注意喚起を行うことが同種のドライバーの安全性を高める助けになると考え、本アドバイザリを公表しました。アドバイザリには、複数のベンダーとの調整を通じて知り得た効果的な修正方法を当該ベンダーの了解を得て掲載することができました。また、Windows ドライバーに関する注意喚起であるため、事前に Microsoft 社の了承を得ま

した。これら関係組織への調整にも、春山氏に協力いただきました。CVD (Coordinated Vulnerability Disclosure) の精神を理解しご協力いただいた春山氏および本件に関係する複数のベンダーに感謝します。

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、当該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」の新規公表は0件、「Japan Vulnerability Notes JP（連絡不能）一覧」の新規公表は2件となりました。

- 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 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 RSA Conference 2024 ならびに複数会合への参加

JPCERT/CCは5月6日から9日まで米国サンフランシスコにて開催されたサイバーセキュリティカンファレンス「RSA Conference 2024」に、主に脆弱性調整や関連するトピックについて国際的な最新動向の把握のため、聴講参加しました。現地では本カンファレンスと並行して開催された、米国CERT/CC主催の主に製品開発者を対象とした会合「CERT Vendor Meeting」ならびにSBOM関係者の集い「3rd Annual RSA SBOM Meetup」にも参加し、関係者との議論を通じた関係構築および情報収集に努めました。

- 2024 USA | RSA Conference
<https://www.rsaconference.com/usa>
- CERT Vendor Meeting 2024
<https://cert-vendor-meeting-2024.eventbrite.com>
- 3rd Annual RSA SBOM Meetup - (2024)

<https://lu.ma/rsa-sbom-meetup>

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、国内の製品開発者をスコープとする Root として活動しています。

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、85 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 国内 CNA 会合第 4 回「CNA Talk」開催

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しています。4 月 26 日には、JPCERT/CC を Root としている国内 CNA9 組織を招いた会合「CNA Talk」を開催し、各組織の状況や課題、また改定されたルール等、CNA としての活動に関する複数の議題について議論ならびに情報共有し、国内 CNA コミュニティーにおける連携体制の強化を図りました。

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）

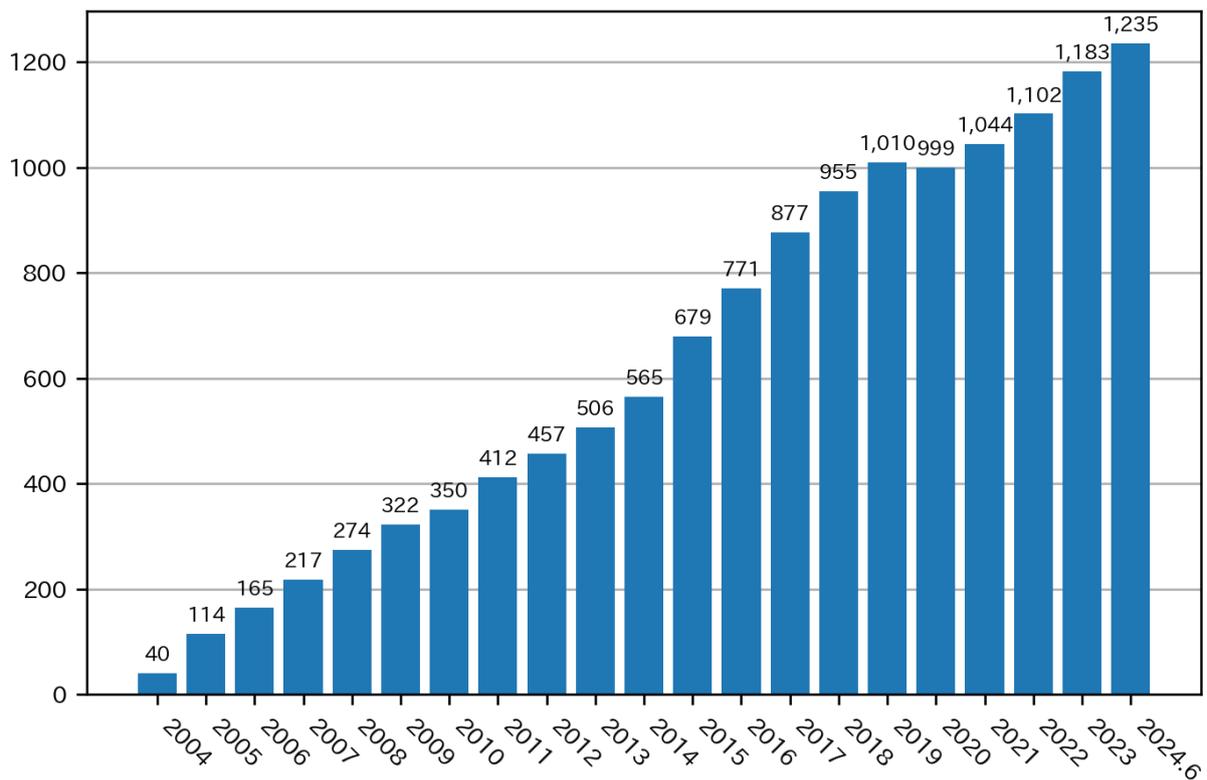


図 2.2 製品開発者登録数

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>

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 6 月 30 日現在で 1,235 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>

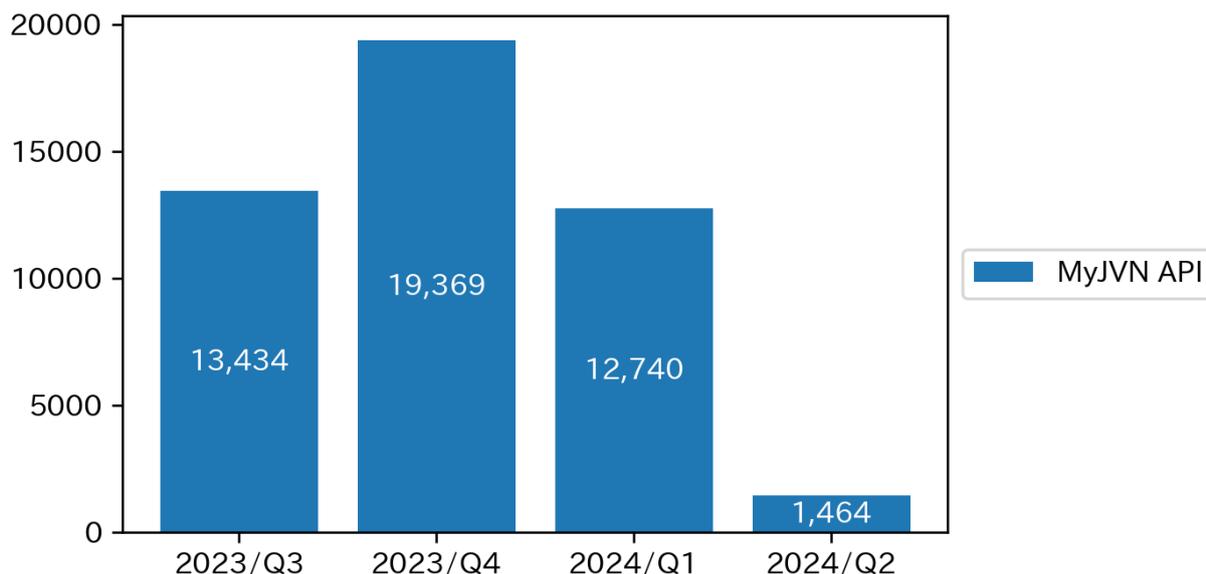


図 2.3 VRDA フィード配信件数

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 12% 増加しました。脆弱性情報の利用数については、約 4% 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。

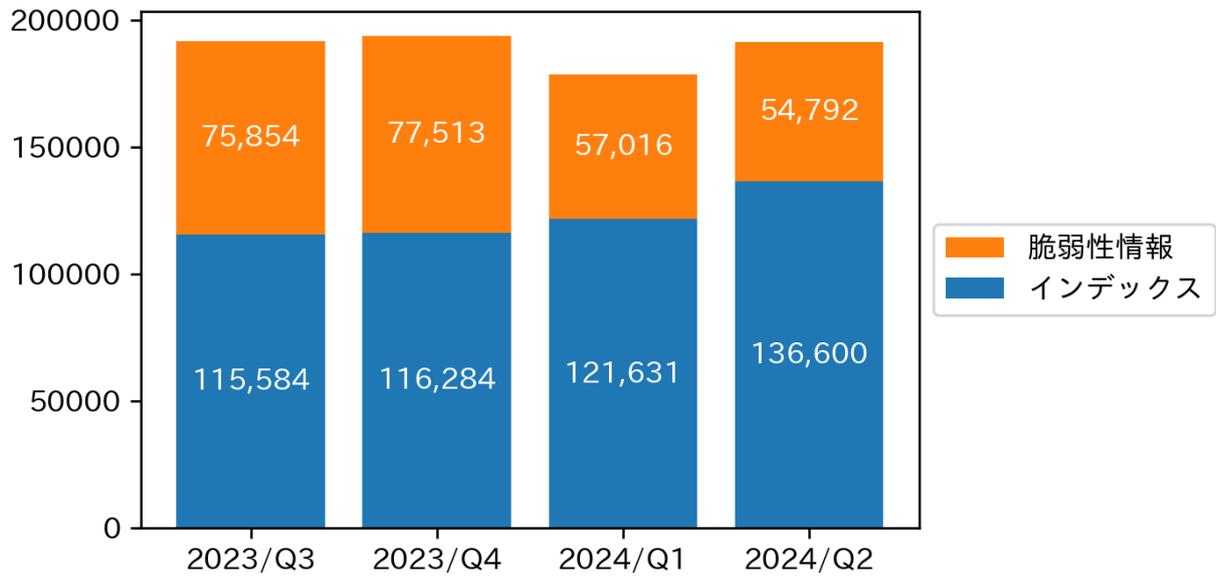


図 2.4 VRDA フィード利用件数

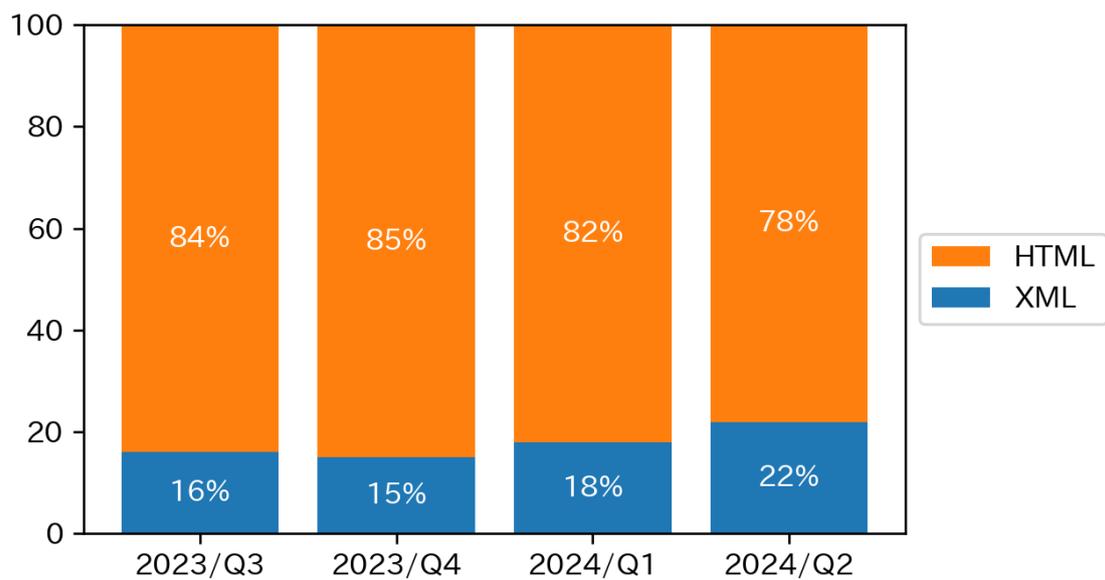


図 2.5 脆弱性情報のデータ形式別利用割合

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は、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。本四半期では次のような活動を行いました。

3.1.1 貿易会 ISAC

2024 年 5 月 17 日に開催された第 33 回技術部会に参加し、「ゼロデイ脆弱性に対する JPCERT/CC のインシデント対応支援」について講演を行いました。

3.1.2 SICE/JEITA/JEMIMA セキュリティ合同 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）が定期的で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。

3.1.3 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。本四半期は、6 月 10 日に開催された第 76 回セプターカウンシル運営委員会にて「Palo Alto Networks 社製 PAN-OS GlobalProtect の OS コマンドインジェクション脆弱性 (CVE-2024-3400)

に関する注意喚起」について情報を提供し、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 の登録組織に対して、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。オフラインでの会合を開催するなどして組織間の交流も図っており、参加組織にはご講演等のご協力をいただいております。なお、本四半期において新たに 20 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向け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。

本四半期で新たに参加した組織を含め、2024 年 6 月末時点においてこのグループには 30 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、2024 年 6 月末時点において 1,441 名に登録していただいております。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、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以下の 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.jpccert.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。

- 2024-04-12 JPCERT/CC ICS Security Notes FY2023_#Q4

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.jpccert.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.jpccert.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.jpccert.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

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 は 5 月 8 日に電話会議を行い、今後の APCERT の運営方針等について議論しました。JPCERT/CC は Steering Committee メンバーとして会議に参加すると同時に、事務局として会議運営をサポートしました。

4.2.2 FIRST (Forum of Incident Response and Security Teams)

JPCERT/CC は、1998 年の加盟以来、FIRST の活動に積極的に参加しています。2021 年 6 月からは、JPCERT/CC の国際部マネージャー 内田有香子が FIRST の理事を務めています。本四半期は、毎月のオンラインによる理事会に加えて、下記の年次会合に先立って福岡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>

4.2.3 36th Annual FIRST Conference への参加と開催支援 (6 月 9 日～14 日)

第 36 回 FIRST 年次会合が 6 月 9 日から 14 日にかけて福岡で開催されました。本会合は、サイバーインシデントの予防、対応、技術分析等に関する最新動向の情報交換およびインシデント対応チームの連携強化を目的に毎年開催されています。今回は、昨年と同様に現地開催を主体とし、一部セッションをオンラインで同時配信する形で行われました。今年は“Bridging Security Response Gaps”のテーマの下に多種多様なトピックが取り上げられ、99 の国・地域から 997 名が参加しました。

JPCERT/CC は本会合のローカルホストとして、会合開催前から海外からの参加者のビザ申請書類作成や国内関係者との調整などで FIRST を支援してきました。また、代表理事の歌代がローカルホストとして開会式で歓迎のスピーチを行いました。

今回は、JPCERT/CC から 2 件の講演が採択されました。“Are You Lazarus? - Cryptocurrency Hackers Targeting Japanese Organizations”と題した講演では、近年観測されている日本の仮想通貨関連事業者を狙った攻撃動向やその特徴を解説しました。また、“Pushing Coordinated Vulnerability Disclosure Forward in Asia Pacific”と題した講演では、日本国内やアジア太平洋地域で JPCERT/CC が推進している脆弱性コーディネーションに関する関係組織間の連携促進を目的とした活動を紹介しました。

また、この機会を利用し、世界各国の National CSIRT や製品ベンダーの CSIRT 等と個別に意見を交換しました。各地域間の情報共有の促進や信頼関係の醸成によって、国際間でのインシデント対応調整がより円滑に進められるよう、今後もこのような会合に積極的に参加してまいります。

第 36 回 FIRST 年次会合についての詳細は、次の Web ページをご参照ください。

- 36th Annual FIRST Conference
<https://www.first.org/conference/2024/>

4.3 海外 CSIRT 等の来訪および訪問

4.3.1 フィンランド NCSC-FI の来訪 (4 月 16 日)

フィンランドの National CSIRT である NCSC-FI 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 モンゴル Public CSIRT/CC および National CSIRT への訪問 (5 月 13 日、16 日)

モンゴルで新設された Public CSIRT/CC および National CSIRT をそれぞれ訪問し、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。

4.4 その他国際会議への参加

4.4.1 Locked Shields に参加 (4 月 23 日～26 日)

4 月 23 日から 26 日にかけて、NATO サイバー防衛協力センター (Cooperative Cyber Defence Centre of Excellence : CCDCOE) が主催する国際的なサイバー演習 Locked Shields 2024 にオンライン参加しました。JPCERT/CC の職員 5 名は日本の政府や重要インフラ事業者の参加者とともにブルーチームの一員として、インシデントの対応および法務・広報の課題に取り組みました。

- Locked Shields
<https://ccdcoe.org/exercises/locked-shields/>

4.4.2 NatCSIRT 2024 への参加 (6 月 14 日～15 日)

第 36 回 FIRST 年次会合に連続した日程で、米国 CERT/CC が主催する National CSIRT Meeting (NatCSIRT) 2024 が福岡で開催されました。本会合は、世界各国の National CSIRT が一堂に会し、国を代表するインシデント対応チームとしての活動計画や課題を共有し、開発ツールや共同プロジェクト、調査研究等に関して発表し議論することを目的に毎年開催されています。JPCERT/CC は、国内でのランサムウェア感染事例や、攻撃者グループおよび手口の変化、また被害組織に関連する法制度等の環境について発表を行いました。

NatCSIRT についての詳細は、次の Web ページをご参照ください。

- NatCSIRT 2024
<https://resources.sei.cmu.edu/news-events/events/natcsirt/index.cfm>

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。

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、5月は2023年10月以来久しぶりに14万件を超えました。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。

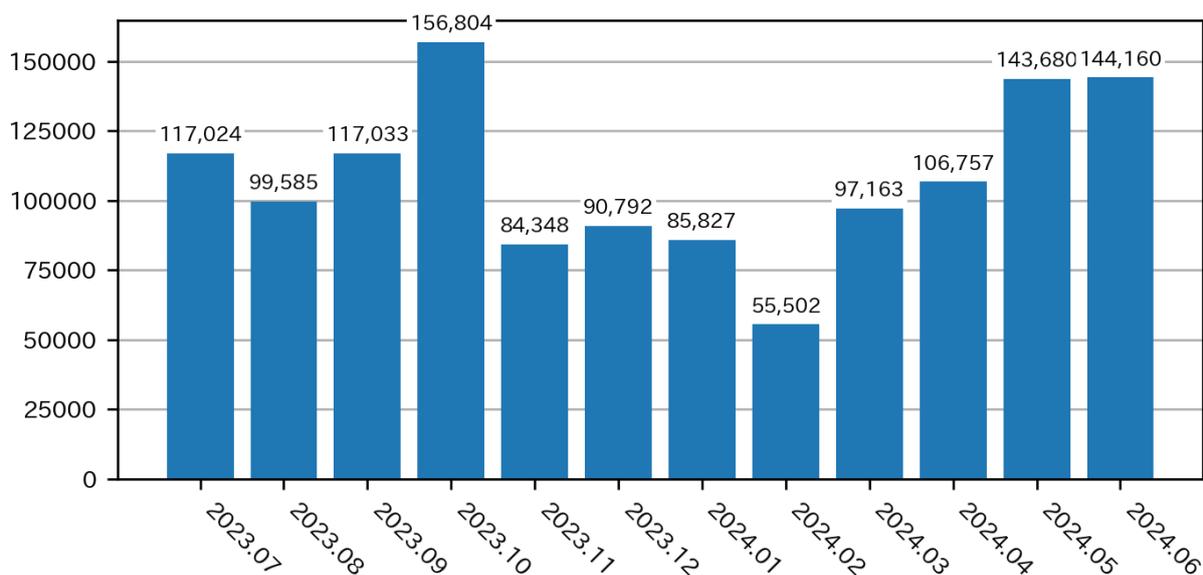


図 5.1 フィッシング報告件数

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 23.5% を占めました。次いで、「三井住友カード」をかたるフィッシングの報告も多く、全体の約 15.3 %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計 4 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。

- 東京ガスをかたるフィッシング：1 件
- Mastercard をかたるフィッシング：1 件
- イオンカードをかたるフィッシング：1 件
- 国税庁をかたるフィッシング：1 件

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、新生活を開始するタイミングで誤認しやすいと考えられる電力会社やガス会社をかたるフィッシング（図 5.2）や、確定申告時期にあたり e-Tax（国税電子申告・納税システム）をかたるフィッシング^{*1}（図 5.3）などが発生しました。フィッシングの誘導 URL についても、セキュリティ検知機構を回避する試みとして、Unicode を使用した飾り文字を混ぜたり、短縮 URL サービスを利用したり、クラウドサービスで発行可能なドメインを使用したり、メール文面に複数の URL を埋め込んだりすることが引き続き行われています。

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。

- 協議会 Web ページ
<https://www.antiphishing.jp/>
- 2024/03 フィッシング報告状況
<https://www.antiphishing.jp/report/monthly/202403.html>
- 2024/04 フィッシング報告状況
<https://www.antiphishing.jp/report/monthly/202404.html>
- 2024/05 フィッシング報告状況

^{*1} https://www.antiphishing.jp/news/alert/nta_20240522.html

【myTOKYOGAS】ご請求料金確定のお知らせ

日頃より、myTOKYOGASをご利用いただきありがとうございます。

今月のご請求金額が確定いたしました、期限内にお支払いを完了してください。万一、支払期日を過ぎると、サービスのご供給を【停止】致します。

お支払い期限: 2024/04/24

下記URLよりログインしてお支払いください。

▼ 支払いの詳細リンクエント

の部分のリンク
<https://bit.ly/m-●●●●> など

※更新の有効期限は、24時間です。

お支払い前に、添付の請求書をご確認いただき、お支払い金額が正確であることをご確認ください。

既にお支払いいただいた場合は、このお知らせを無視していただいて結構です。ご不明な点やご質問がある場合は、お気軽にお問い合わせください。お客様サポートチームがお手伝いいたします。

ご協力とご理解に感謝いたします。早期のお支払いをお待ちしております。

*本メールはセキュリティ確保のため送信専用のメールアドレスから自動配信しています。

ご返信いただいてもご対応いたしかねますので、あらかじめご了承ください。発行元：東京ガス株式会社 〒105—8527 東京都港区海洋1—5—20

Copyright(c) TOKYO GAS Co.,Ltd. All Rights Reserved. twin edition

【myTOKYOGAS】ご請求料金確定のお知らせ（自動配信メール）

メール文面の例

図 5.2 東京ガスをかたるフィッシングの例

<https://www.antiphishing.jp/report/monthly/202405.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 54 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。

2023 年度に技術・制度検討ワーキンググループにおいて作成と改定を進めた、「フィッシング対策ガイドライン 2024 年度版」（事業者と利用者向け）および「フィッシングレポート 2024」を 2024 年 6 月 4 日に公開しました。それぞれの文書については、次の Web ページをご参照ください。

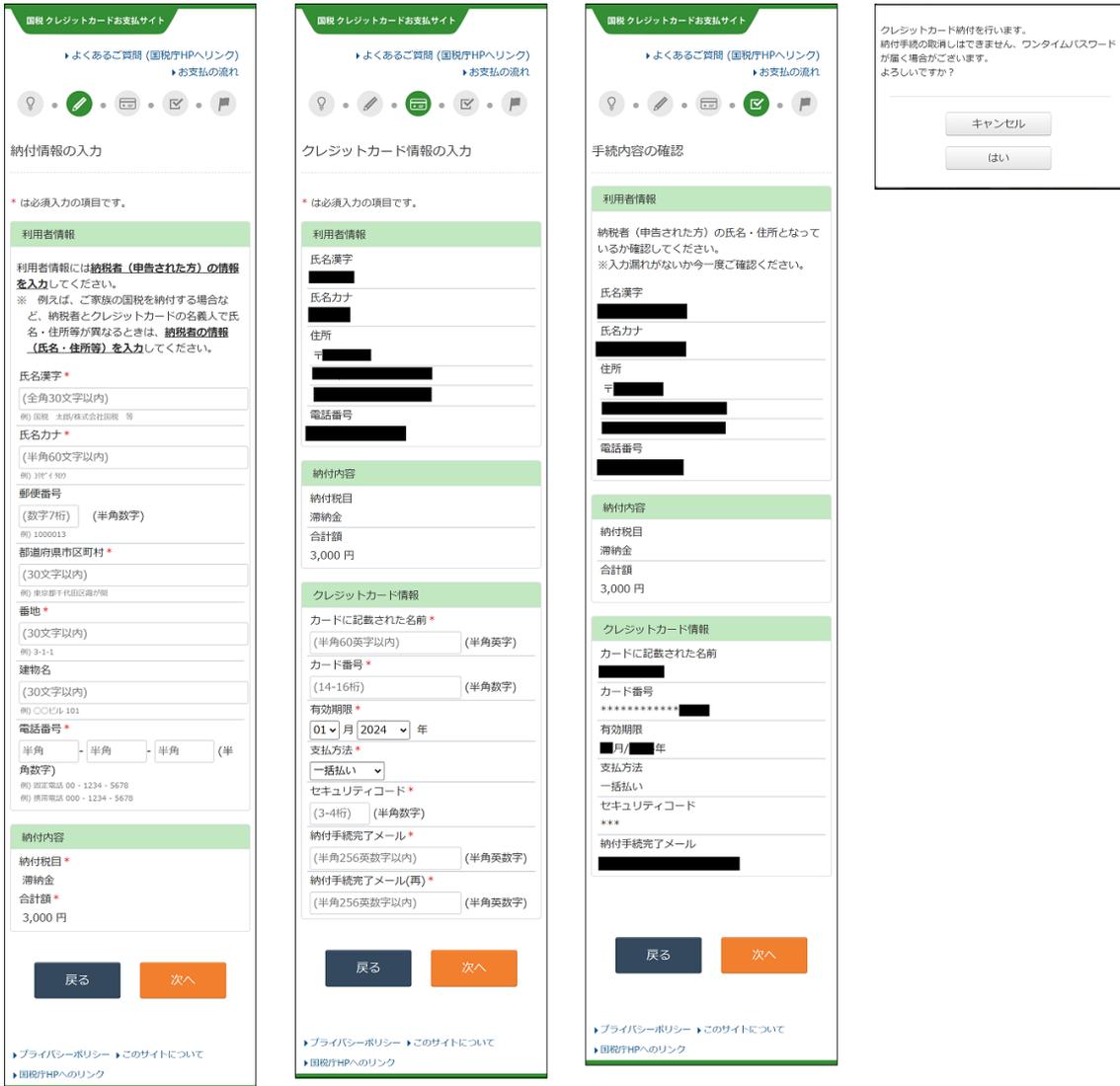


図 5.3 国税庁をかたるフィッシングの例

- フィッシング対策ガイドライン 2024 年度版
https://www.antiphishing.jp/report/guideline/antiphishing_guideline2024.html
- 利用者向けフィッシング詐欺対策ガイドライン 2024 年度版
https://www.antiphishing.jp/report/guideline/consumer_guideline2024.html
- フィッシングレポート 2024
https://www.antiphishing.jp/report/wg/phishing_report2024.html

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117回運営委員会（リクルート会議室+オンライン）
日時：4月25日（木）15：00～18：00
- 第118回運営委員会（オンライン）
日時：5月16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：4月～6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：5月14日（火）16：30～18：00（JPCERT/CC 会議室+オンライン）
- フィッシング対策ワークショップ
日時：4月26日（金）13：00～17：00（マクニカ会議室）
- フィッシング対策協議会 2024年度総会
日時：6月21日（金）15：00～17：15（エッサム神田ホール2号館）

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け付け、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。

- 2024-04-18
JPCERT/CC インシデント報告対応レポート [2024 年 1 月 1 日～2024 年 3 月 31 日]
https://www.jpcert.or.jp/pr/2024/IR_Report2023Q4.pdf
- 2024-06-06
JPCERT/CC Incident Handling Report [January 1, 2024 - March 31, 2024]
https://www.jpcert.or.jp/english/doc/IR_Report2023Q4.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。

- 2024-05-02
JPCERT/CC インターネット定点観測レポート [2024 年 1 月 1 日～2024 年 3 月 31 日]

<https://www.jpccert.or.jp/tsubame/report/report202401-03.html>

https://www.jpccert.or.jp/tsubame/report/TSUBAME_Report2023Q4.pdf

- 2024-06-06

JPCERT/CC Internet Threat Monitoring Report [January 1, 2024 - March 31, 2024]

https://www.jpccert.or.jp/english/doc/TSUBAMEReport2023Q4_en.pdf

7.3 脆弱性関連情報に関する活動報告

IPA と JPCERT/CC は、それぞれ受付機関および調整機関として、ソフトウェア製品等の脆弱性関連情報に関する取扱規程（平成 29 年経済産業省告示 第 19 号）等に基づく脆弱性関連情報流通制度の運用の一端を 2004 年 7 月から担っています。この制度の運用に関連した前四半期の活動実績と、同期間中に公表された脆弱性に関する注目すべき動向をまとめてレポートとして公表しています。

- 2024-04-18

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 1 四半期 (1 月～3 月)]

https://www.jpccert.or.jp/pr/2024/vulnREPORT_2024q1.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 7 件の記事を公表しました。

日本語版発行件数：3 件 <https://blogs.jpccert.or.jp/ja/>

2024-04-04 世界の CSIRT から ～タイ、インドネシア～

2024-05-09 TSUBAME レポート Overflow (2024 年 1～3 月)

2024-06-26 Volt Typhoon の攻撃キャンペーンにどう備えていくべきなのか
～将来の攻撃に備える Threat Hunting のアプローチについて考える～

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

2024-04-11 JSAC2024 -Workshop & Lightning talk-

2024-04-11 JSAC2024 -Day 2-

2024-04-24 ICS Security Conference 2024

2024-06-21 TSUBAME Report Overflow (Apr-Jun 2024)

第 8 章

その他の活動

8.1 講演

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）
「情報セキュリティ 10 大脅威 2024」から考える 攻撃者を“先回り”する対策
個人情報保護セミナー 2024（主催：一般財団法人日本データ通信協会、講演日：2024 年 5 月 24 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）
「情報セキュリティ 10 大脅威 2024」から考える 攻撃者を“先回り”する対策
個人情報保護セミナー 2024（主催：一般財団法人日本データ通信協会、視聴可能期間：2024 年 6 月 3 日～24 日）
3. 朝長 秀誠（技術統括 兼 インシデントレスポンスグループ マネージャー）
トークセッション「マルウェアを知り尽くした達人に聞く脅威の展望 2024」
Macnica Security Forum 2024（主催：株式会社マクニカ、視聴可能期間：2024 年 6 月 17 日～7 月 15 日）

8.2 執筆

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）
「サイバー攻撃、被害公表のあり方に「正解」の道筋 被害組織の批判ではなく対応の適切な評価へ」
（掲載媒体名：東洋経済オンライン、発行：株式会社東洋経済新報社、公開日：2024 年 4 月 5 日）
2. 宮地 利雄（技術顧問）
「制御システムセキュリティの動向」
（掲載書籍名：計測技術 2024 年 6 月号、発行：日本工業出版株式会社、発行日：2024 年 5 月 24 日）

8.3 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. Interop Tokyo 2024

(主催：Interop Tokyo 実行委員会、開催日：2024 年 6 月 12 日～14 日)

2. エッジ AI イニシアチブ 2024

(主催：EE Times Japan、開催日：2024 年 6 月 19 日～21 日)

本文書を引用、転載する際には JPCERT/CC 広報 (pr@jpcert.or.jp) まで確認のご連絡をお願いします。

本文書に記載の社名、製品名は各社の商標または登録商標です。

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 : 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>

JPCERT/CC 活動四半期レポート [2024 年 4 月 1 日 ~ 2024 年 6 月 30 日]

- 2024 年 7 月 18 日 初版発行
- 発行
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/>