JPCERT/CC 活動四半期レポート

2025 年 1 月 1 日～2025 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

2025 年 4 月 17 日

JPCERT CC®

目次

活動概要トピックス 4

セキュリティアナリスト向けカンファレンス JSAC2025 を開催 4

制御システムセキュリティカンファレンス 2025 を開催 5

第 1 章 早期警戒 6

1.1 インシデント対応支援 6

1.1.1 インシデントの傾向 6

1.1.1.1 フィッシングサイト 6

1.1.1.2 Web サイト改ざん 7

1.1.2 インシデント対応事例 8

1.1.2.1 Ivanti Connect Secure の脆弱性（CVE-2025-0282）により侵害された可能性がある国内組織への通知 8

1.1.3 インシデントに関する情報提供のお願い 8

1.2 情報収集・分析・提供 8

1.2.1 情報収集・分析 9

1.2.1.1 Ivanti Connect Secure などにおける脆弱性（CVE-2025-0282） . . . 9

1.2.1.2 Fortinet 製 FortiOS および FortiProxy における認証回避の脆弱性（CVE-2024-55591） 9

1.2.1.3 SonicWall 製 SMA1000 の AMC および CMC における脆弱性（CVE-2025-23006） 9

1.2.1.4 Palo Alto Networks 製 PAN-OS の認証回避の脆弱性（CVE-2025-0108） 10

1.2.2 Web サイトでの情報提供 10

1.2.2.1 注意喚起 10

1.2.2.2 CyberNewsFlash 11

1.2.2.3 Weekly Report 11

1.2.3 CISTA での情報提供 11

1.2.3.1 早期警戒情報 11

1.2.3.2 Analyst Note 11

1.2.3.3 個別提供情報 12

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 12

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 12

1.3.1.1 TSUBAME の観測データの活用 12

1.3.1.2 TSUBAME 観測動向 13

第 2 章 脆弱性関連情報流通促進活動 15

2.1 脆弱性関連情報の取り扱い状況 15

2.1.1 JPCERT/CC における脆弱性関連情報の取り扱い . . . 15
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 16
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 . . . 17
2.1.2.2 国際調整または独自調整で取り扱った脆弱性 . . . 17
2.1.3 連絡不能開発者対応 . . . 18
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 . . . 18
2.1.4.1 APCERT Coordinated Vulnerability Disclosure WG 第四回会合 . . . 18
2.1.5 CNA としての活動 . . . 19
2.2 日本国内の脆弱性情報流通体制の整備 . . . 19
2.2.1 日本国内製品開発者との連携 . . . 20
2.2.2 製品開発者との定期ミーティング等の実施 . . . 20
2.3 VRDA フィードによる脆弱性情報の配信 . . . 21

第 3 章 国内連携活動 23
3.1 業界団体やコミュニティー等との連携活動 . . . 23
3.1.1 SICE/JEITA/JEMIMA セキュリティ調査研究合同 WG . . . 23
3.1.2 セプターカウンシル運営委員会 . . . 23
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 . . . 24
3.2.1 早期警戒情報提供先との連携促進 . . . 24
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 . . . 24
3.3 情報・ツール等の提供 . . . 24
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 . . . 24
3.3.2 JPCERT/CC ICS Security Notes . . . 24
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 . . . 25

第 4 章 国際連携活動 26
4.1 海外 CSIRT 構築支援および運用支援活動 . . . 26
4.2 国際 CSIRT 間連携 . . . 26
4.2.1 APCERT（Asia Pacific Computer Emergency Response Team） . . . 26
4.2.1.1 APCERT Steering Committee 会議の実施 . . . 26
4.2.2 FIRST（Forum of Incident Response and Security Teams） . . . 27
4.3 海外 CSIRT 等の来訪および訪問 . . . 27
4.3.1 モンゴル MNCERT/CC の来訪（2 月 13 日） . . . 27
4.3.2 韓国 KrCERT/CC への訪問（3 月 12 日） . . . 27
4.4 その他国際会議への参加 . . . 27
4.4.1 RightsCon への参加（2 月 24 日〜27 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／配信 . . . 30
5.2.1 フィッシングの動向等に関する情報配信 . . . 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 32
5.2.4　フィッシング対策ガイドライン等の改定作業 32

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 37
8.1　講演 37
8.2　執筆 37
8.3　協力・後援 37

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

セキュリティアナリスト向けカンファレンス JSAC2025 を開催

2025 年 1 月 21 日、22 日に JSAC2025 を赤坂インターシティコンファレンスで開催しました。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。 8 回目の開催になる今回は、72 件の CFP 応募から採択されたワークショップ 3 件を含む 21 件の講演の他に、Lightning Talk セッションとして 2 件の発表が行われました。インシデント対応事例やマルウェア分析、フィッシング攻撃への対策といったインシデントの分析・対応および対策に関する技術や、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。また、今回は 38 名の講演者のうち 20 名が、台湾、韓国、シンガポール、カナダ、ポーランド、スウェーデンなどの海外から参加されました。

当日は、多く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、講演で発表されたインシデント対応に関するいくつもの具体的な事例はセキュリティアナリストのレベル向上につながるものである、と好評をいただいています。なお、講演資料は JSAC2025 の Web サイト上で公開しているほか、一部の講演動画は YouTube 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。

- JSAC2025
  https://jsac.jpcert.or.jp/
- JSAC2025 講演動画
  https://www.youtube.com/watch?v=QysGnVjXrfo&list=PLgEi6O-lWUIaz2-gaWWBjqHvtdIQtOwDE
- JSAC2025 開催レポート～DAY 1～
  https://blogs.jpcert.or.jp/ja/2025/02/jsac2025day1.html
- JSAC2025 開催レポート～DAY 2～
  https://blogs.jpcert.or.jp/ja/2025/03/jsac2025day2.html
- JSAC2025 開催レポート～Workshop & Lightning Talk～
  https://blogs.jpcert.or.jp/ja/2025/03/jsac2025-workshop-lightning-talk.html

制御システムセキュリティカンファレンス 2025 を開催

2025 年 2 月 5 日に「制御システムセキュリティカンファレンス 2025」を会場開催とオンライン配信のハイブリッドで開催し、会場 50 名、オンラインでは 511 名（参加申込数約 500 名、参加見込み 500 名規模、最大同時視聴者 250 名程度）の方々にご参加いただきました。共催の経済産業省から商務情報政策局 サイバーセキュリティ課長 武尾 伸隆氏に開会のごあいさつをいただき、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、IEC 62443 制御システムセキュリティ規格の現状、サイバーセキュリティを考慮したプロセス安全マネジメントフレームワークついて、CTEM を制御系システムのリスク低減策に応用 したケース、工場のインシデント対応訓練シナリオを使用した訓練で得られた気付き、SBOM 運用の課題とその対応策、脆弱性対応のための適切な資産管理手法へのチャレンジ等といったさまざまなトピックスに関する講演が行われました。前回に引き続き、制御システムユーザー企業が取り入れ可能な取り組みを複数紹介できたことは大きな成果であると考えます。また、複数の制御システムユーザー企業が連携して進める取り組みを紹介するトークセッションやパネルセッションを設け有意義な議論が行われた点、さらに、5 年ぶりに会場開催を再開したことで活発な質疑応答が行われた点は、本年度の大きな特徴となりました。

開催後のアンケート結果（有効回答数：281）によると、参加者の内訳は制御システムユーザーが 33.1%、制御システムベンダーが 11.0%、制御機器ベンダーが 15.1%、制御システムエンジニアリングが 11.0%、研究者が 7.8% で、前回と比べ制御システムベンダーや制御機器ベンダーが微増しています。また、オンライン配信では、前回同様に全国各地から多数の参加がありました。会場参加の事前登録者は予想を上回る早さで定員に達し、会場開催への期待の高さがうかがえました。また、98.3% 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。

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 2025
  https://www.jpcert.or.jp/event/ics-conference2025.html
- 制御システムセキュリティカンファレンス 2025 講演資料
  https://www.jpcert.or.jp/present/#year2025
- 制御システムセキュリティカンファレンス 2025 開催レポート
  https://blogs.jpcert.or.jp/ja/2025/03/ics-conference2025.html

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 10,102 件、インシデント件数ベースでは 6,081 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 3,974 件でした。前四半期の 3,597 件と比較して 4% 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、「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/2025/IR_Report2024Q4.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 5,267 件で、前四半期の 4,780 件から 10% 増加しました。また、前年同期（4,781 件）との比較では、10% 増加しました。

[*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	1 月	2 月	3 月	合計	割合
国内ブランド	1,270	1,424	1,583	4,277	81%
国外ブランド	160	175	167	502	10%
ブランド不明	155	180	153	488	9%
全ブランド合計	1,585	1,779	1,903	5,267	

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 78.5%、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 73.3% 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、クレディセゾン、三井住友カード、JCB 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 53%、国外が 47% で、前四半期（国内が 36%、国外が 64%）より国内が増加しました。

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 95 件でした。前四半期の 53 件から 79% 増加しています。

本四半期は、次のような Web サイト改ざん事例を確認しています。

1. Web サイトへアクセス時に不審なショッピングサイトへリダイレクトさせる事例
   - .htaccess ファイルの改ざんおよび不正設置
   - PHP ファイルへのリダイレクトコード挿入
2. Web サイトに仮想通貨のマイニングを目的としたコードが挿入された事例
3. Web サイトに JavaScript で記載されたアドウェアが挿入されていた事例

事例 1 では、Web サーバー上のディレクトリに置かれる.htaccess ファイルが、改ざんされていたり、多数のディレクトリに不正に設置されたりしていました。不正に設置された.htaccess ファイルには、特定の拡張子を持つファイルへのアクセスを制限する、あるいは攻撃者が設置した PHP ファイルへリダイレクトする等の設定が含まれていました。

また、攻撃者が設置した PHP ファイルには、偽ショッピングサイトへリダイレクトするコードや C2 サーバーから取得した任意のコードを Web サーバー上で実行するコードが記載されていました。さらに、PHP で作成されたバックドアも設置されており、C2 サーバーへファイルを送信する機能がありま

[*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。

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。

1.1.2.1 Ivanti Connect Secure の脆弱性（CVE-2025-0282）により侵害された可能性がある国内組織への通知

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。被害を受けた組織の中には、Ivanti 社が提供する侵害を確認するための整合性チェックツールによる調査が正しく行えなくなるように改ざんされているケースもありました。これを受け、JPCERT/CC では、注意喚起と被害組織の一部で確認されたマルウェアの分析内容を公開しています。

- Ivanti Connect Secure などにおける脆弱性（CVE-2025-0282）に関する注意喚起
  https://www.jpcert.or.jp/at/2025/at250001.html
- Ivanti Connect Secure の脆弱性を利用して設置されたマルウェア SPAWNCHIMERA
  https://blogs.jpcert.or.jp/ja/2025/02/spawnchimera.html

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のアドレス情報の提供を外部組織から受け、それをもとに利用する国内のシステム管理者に自組織の機器の確認を要請しました。

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、注意喚起等の情報配信を行います。

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さら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、いただいたフィードバックまたは分析した情報のうち、特徴的なものを紹介します。

1.2.1.1 Ivanti Connect Secure などにおける脆弱性（CVE-2025-0282）

1 月 8 日（現地時間）、Ivanti が Ivanti Connect Secure（旧：Pulse Connect Secure）などにおける 2 件の脆弱性に関するアドバイザリを公表しました。このうち CVE-2025-0282 について、これを悪用した攻撃が一部の顧客に対して行われていることが言及されていました。また、Mandiant は同脆弱性を悪用する攻撃に関するレポートを公表しました。JPCERT/CC が確認したところ、同脆弱性を持つとみられるシステムが国内でも多数利用されていることが判明したため、同月 9 日に注意喚起を公開し、脆弱性の対処や調査に関する関連情報を提供しました。また、同脆弱性の情報公表以降、本脆弱性を悪用した攻撃の被害を受けたとみられるシステムに関する情報を海外機関などから入手できたため、これに基づいて関連する利用組織に情報提供を行いました。

1.2.1.2 Fortinet 製 FortiOS および FortiProxy における認証回避の脆弱性（CVE-2024-55591）

1 月 14 日（現地時間）、Fortinet が FortiOS と FortiProxy における認証バイパス脆弱性（CVE-2024-55591）に関するアドバイザリを公表しました。同社はすでにこの脆弱性が悪用されていることを確認していました。また、脆弱性情報が公表される前に、米セキュリティ組織 Arctic Wolf Networks がブログを公開し、2024 年 11 月 16 日から 12 月末までの間に Fortinet 製品を狙った攻撃が広く行われていたと述べていました。JPCERT/CC は、同脆弱性の影響を受ける FortiOS や FortiProxy が日本国内でも多数利用されている状況を確認したため、脆弱性への対策や調査を推奨すべく、1 月 15 日に注意喚起を公開しました。

1.2.1.3 SonicWall 製 SMA1000 の AMC および CMC における脆弱性（CVE-2025-23006）

1 月 23 日、SonicWall が SMA1000 アプライアンス管理コンソール（AMC）および中央管理コンソール（CMC）における認証前の信頼されていないデータのデシリアライゼーションの脆弱性（CVE-2025-23006）に関するアドバイザリを公表しました。このアドバイザリに、すでに脆弱性を悪用したとみられる攻撃に関する報告を受けているとの記載があり、JPCERT/CC は情報発信の方針を検討するため調査を行いました。同脆弱性の影響を受ける SMA1000 シリーズ製品のうち、管理コンソールが露出しているシステムを特定し、同システムを利用しているとみられる組織には 1 月中に情報提供を行いました。

また、JPCERT/CC から直接連絡することが難しい一部組織については、国内の専門機関と連携して通知を行いました。

1.2.1.4 Palo Alto Networks 製 PAN-OS の認証回避の脆弱性（CVE-2025-0108）

2 月 13 日（現地時間）、Palo Alto Networks が PAN-OS の管理 Web インタフェースにおける認証回避の脆弱性（CVE-2025-0108）に関するアドバイザリを公表しました。このアドバイザリに、すでに脆弱性を悪用したとみられる攻撃に関する報告を受けているとの記載があり、JPCERT/CC は情報発信の方針を検討するため調査を行いました。調査時点において、国内で管理 Web インタフェースの露出が確認できた PAN-OS の IP アドレスが約 20 件あり、インターネット側からの観測からいずれも同脆弱性の影響を受ける状態であると推定できたため、国内の専門機関と連携して通知を行いました。通知先の一部からは、脆弱性に対処した旨の連絡をフィードバックとあわせて受け取り、適切に対処されていることを外形的に確認するとともに、フィードバック内容は追加調査の参考にいたしました。

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」を公開し、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、7 件公開し、1 件の情報更新を行いました。

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

2025-01-09 Ivanti Connect Secure などにおける脆弱性（CVE-2025-0282）に関する注意喚起 (公開)

2025-01-15 2025 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 (公開)

2025-01-15 Fortinet 製 FortiOS および FortiProxy における認証回避の脆弱性（CVE-2024-55591）に関する注意喚起 (公開)

2025-02-12 2025 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 (公開)

2025-03-12 2025 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 (公開)

2025-03-12 Adobe Acrobat および Reader の脆弱性（APSB25-14）に関する注意喚起 (公開)

2025-03-28 a-blog cms における信頼できないデータのデシリアライゼーションの脆弱性に関する注意喚起 (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 として公開することがあります。本四半期は 1 件公開しました。

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

2025-01-30　ISC BIND 9 における複数の脆弱性について（2025 年 1 月）

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 として公開しています。本四半期は 12 件公開し、計 101 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」の受け取りを希望する方々に提供する登録制の 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 1,260 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」として提供しています。本四半期は 57 件配信しました。

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。本四半期は 15 件提供しました。先述の Ivanti Connect Secure などにおける脆弱性（CVE-2025-0282）、SonicWall 製 SMA1000 の AMC および CMC における脆弱性（CVE-2025-23006）、PAN-OS の認証回避の脆弱性（CVE-2025-0108）などの影響を受けるホストを管理する組織に対して情報提供を行いました。

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、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「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 10〜12 月）
  https://www.jpcert.or.jp/tsubame/report/report202410-12.html
- TSUBAME レポート Overflow（2024 年 10〜12 月）
  https://blogs.jpcert.or.jp/ja/2025/02/tsubame-overflow20241012.html

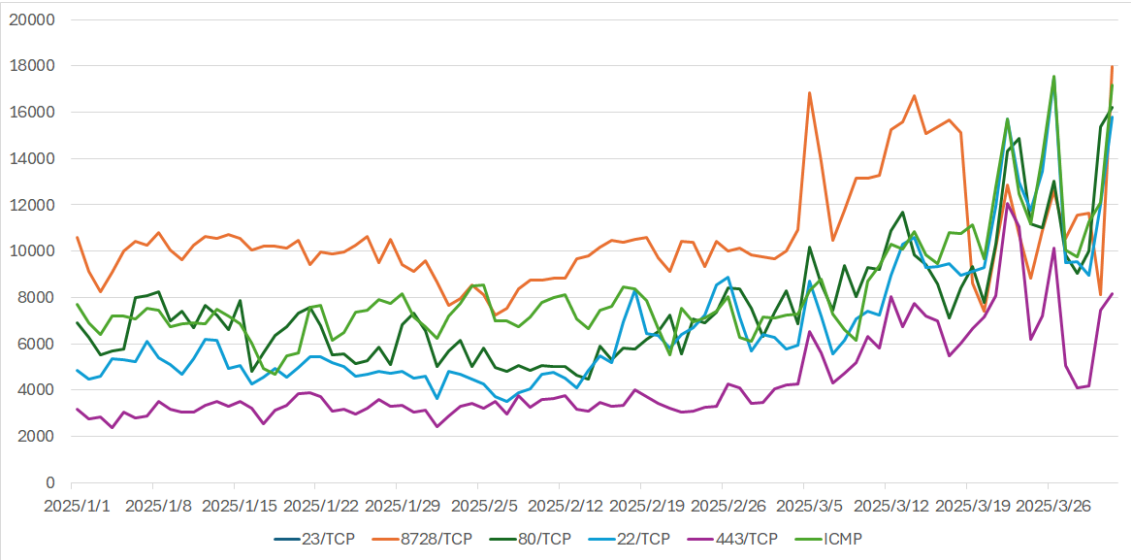


図 1.1 TSUBAME で観測された宛先ポートの上位 1 位〜5 位のパケット数
（2025 年 1 月 1 日〜3 月 31 日）

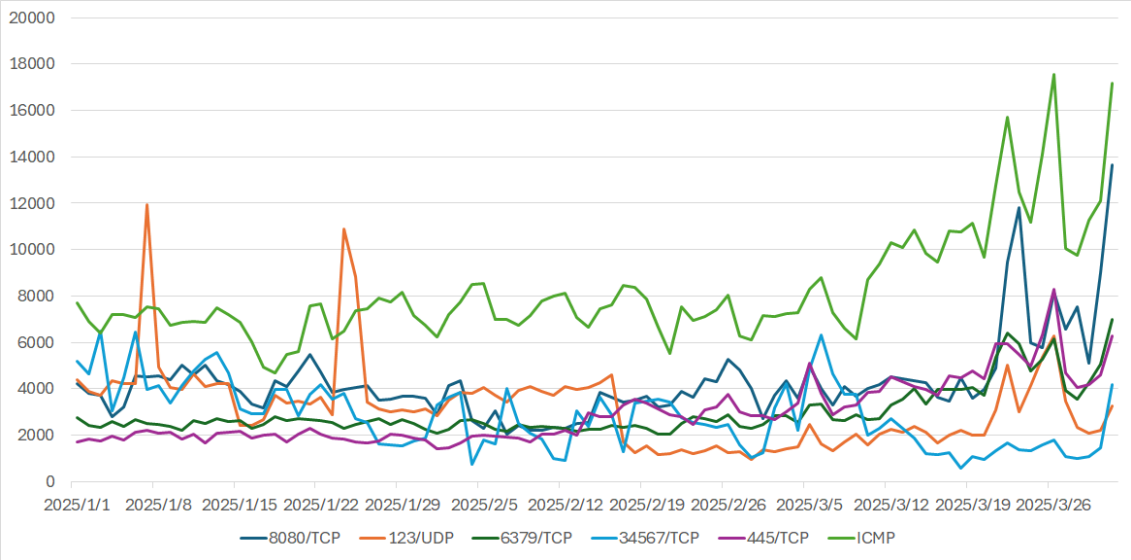


図 1.2 TSUBAME で観測された宛先ポートの上位 6 位〜10 位のパケット数
（2025 年 1 月 1 日〜3 月 31 日）

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 1.1 と図 1.2 に示します。

また、過去 1 年間（2024 年 4 月 1 日〜2025 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。

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。増減の波はありますが、徐々に増加してきています。2 位の 8728/TCP、3 位の 80/TCP、5 位の 443/TCP については一時

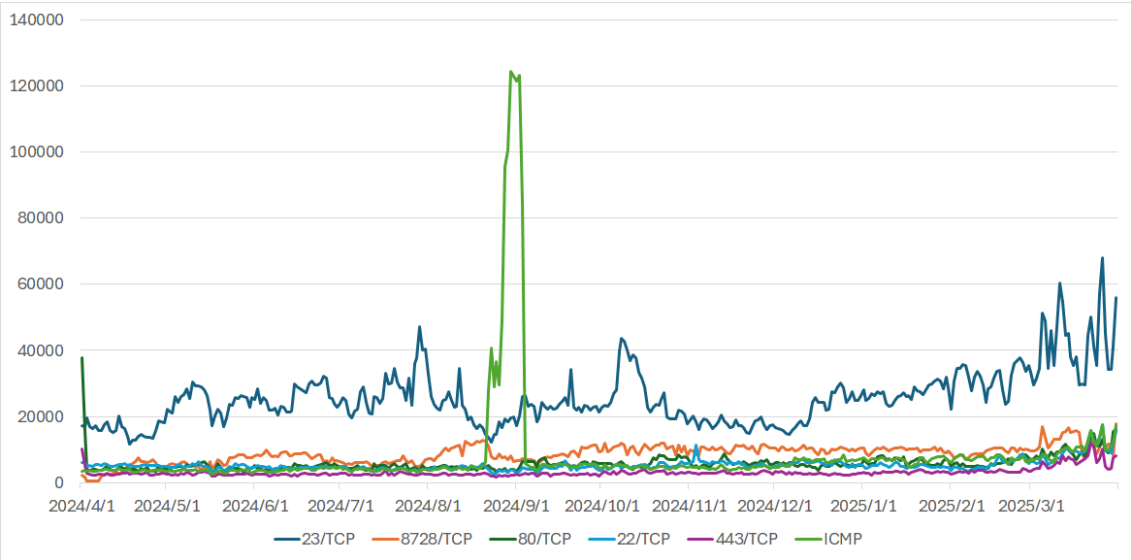


図 1.3 TSUBAME で観測された宛先ポートの上位 1 位～5 位のパケット数
（2024 年 4 月 1 日～2025 年 3 月 31 日）

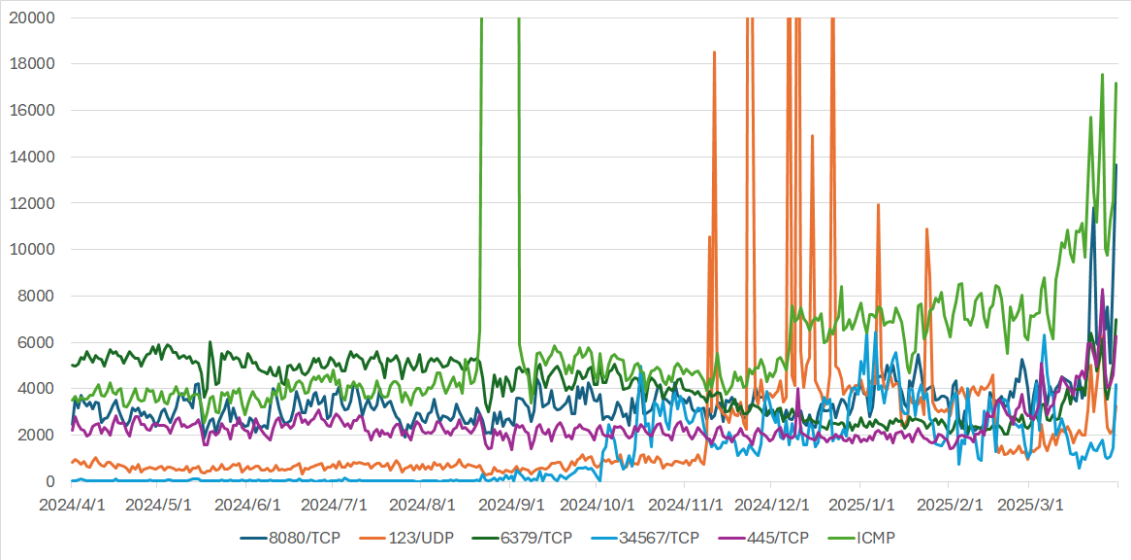


図 1.4 TSUBAME で観測された宛先ポートの上位 6 位～10 位のパケット数
（2024 年 4 月 1 日～2025 年 3 月 31 日）

的な増減はありますが、大きな変化はありません。4 位の 22/TCP（ssh）は 2 月 13 日ごろからパケット数が増加してきています。

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。

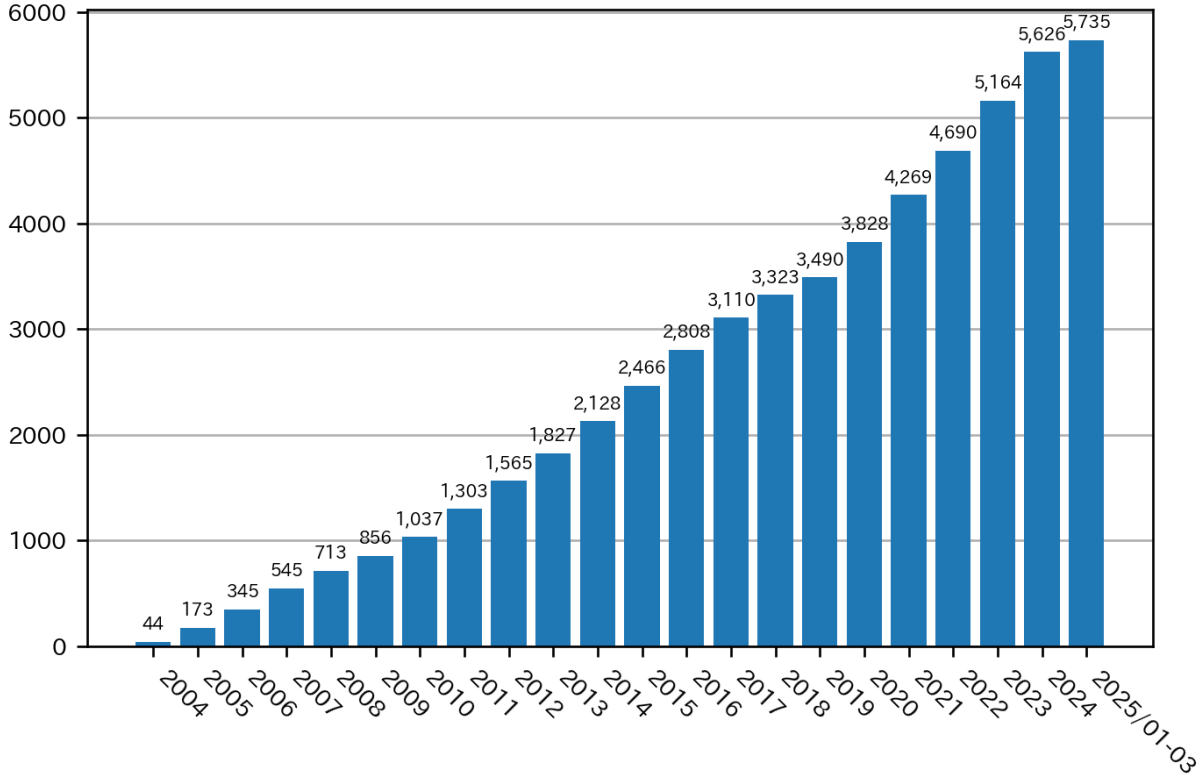


図 2.1 JVN 公表累積件数

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 109 件（累計 5,735 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：22 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：86 件
- 脆弱性情報に関連する技術情報等に関するもの：1 件

なお、パートナーシップガイドラインに基づく脆弱性関連情報に関する四半期ごとの届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#05508012
  EXIF Viewer Classic におけるクロスサイトスクリプティングの脆弱性
  https://jvn.jp/jp/JVN05508012/

個人開発者の Rodrigue（以前の呼称は Kakera）が提供する EXIF Viewer Classic の脆弱性情報に関するアドバイザリです。本件の脆弱性報告を受けて製品開発者へ複数回連絡をしたものの応答が得らなかったため、2012 年に JVN サイトの「連絡不能開発者一覧」に製品情報を掲載し広く情報を募っていました。それでも情報が得られなかったことから、2023 年、製品ユーザーに本脆弱性が存在し開発者による修正が期待できないためリスクがあることを知らせる手続きに移行しました。この手続きを進めるにあたって製品開発者に再度連絡したところ応答があり調整を再開、本アドバイザリを公表しました。これによって、脆弱性の情報だけでなく、それを修正するための対策方法を含むアドバイザリを製品ユーザーに提供することができました。製品開発者と連絡が取れなかったり、途中で連絡が途切れてしまったりといった案件は他にもあります。このような案件に対処するため「情報セキュリティ早期警戒パートナーシップ」では開発者と調整が成立しない場合でも対象製品のユーザーにリスクを知らせるための手続きが定められています。このように、時間が経過しても粘り強く連絡を試みることで公表に至る場合もあります。寄せられた報告に真摯に向き合い、手続きに沿って丁寧に対応することで、1 件でも多くユーザーに有益な対策情報を提供できるように努めています。

2.1.2.2 国際調整または独自調整で取り扱った脆弱性

- JVNVU#94903505
  rsync における複数の脆弱性
  https://jvn.jp/vu/JVNVU94903505/

rsync はリモートコンピューター、ローカルコンピューターおよびストレージデバイス間でファイルを同期するために用いられるオープンソースソフトウェアです。Rsync Project および米国 CERT/CC から rsync の 6 つの脆弱性が公開されたことを契機に、JVN でも国内向けに本アドバイザリを公表しました。本件は、CERT/CC が研究者から脆弱性報告を受けて複数の開発者や各国の調整機関と公開前に詳細情

報を共有し、公開日時やその内容を調整しました。JPCERT/CC も日本の調整機関としてこの調整に参加し、情報公開前から国内の Linux 系ディストリビューターらと連携しました。その後、本アドバイザリの公表によって、Linux ディストリビューターだけでなく国内で rsync を利用するユーザーに広く脆弱性の存在とアップデートの必要性を知らせました。 JPCERT/CC では、本件のように、脆弱性情報の公表時までに脆弱性対策とその対策のユーザーへの提供準備が必要な関係者と、脆弱性の公表後に提供された対策を適用すればいい関係者を切り分け、前者には対策準備を進められるよう公開前に詳細情報を提供し、後者には情報公開時に JVN アドバイザリ公表やメールでの公表通知で対策情報を提供しています。こうすることで、前者が情報を知らず対策準備ができないため情報公開時にユーザーからの問い合わせへの対応などで混乱したり、短期間での対策を迫られたりすることを防げます。また、脆弱性情報が公表前に流出するリスクを減らし、後者が対策のないうちから無用な騒ぎに巻き込まれることを避けることができます。

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、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 Coordinated Vulnerability Disclosure WG 第四回会合

JPCERT/CC は、アジア太平洋地域における CSIRT コミュニティーである APCERT（Asia Pacific Computer Emergency Response Team）に、同組織の複数組織と協力しワーキンググループ「Coordinated Vulnerability Disclosure WG」を設立し、脆弱性調整や CVE Program 活動についての情報共有や、課題への取り組みを進めています。本四半期におけるワーキンググループ会合では、参加組織によ

る脆弱性調整に関する発表が行われたほか、ワーキンググループの今後の活動に関して議論が行われました。

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。

2008 年 5 月以降、JVN で公表する脆弱性情報には他の CNA が採番したケースを除き、JPCERT/CC が採番した CVE ID を付与しています。本四半期は、56 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

2.2　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

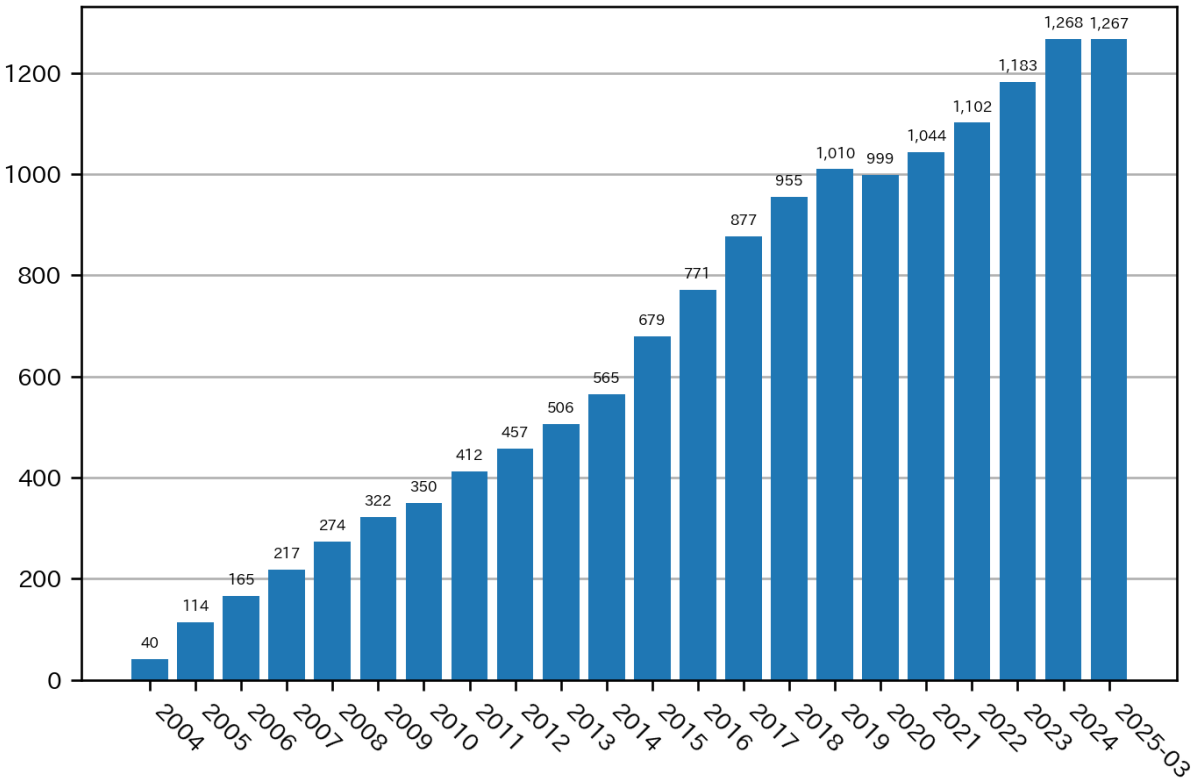


図 2.2 製品開発者登録数

2.2.1 日本国内製品開発者との連携

本規程において、調整機関である JPCERT/CC に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 1,267 となっています。本四半期は製品開発者リストに登録されている製品開発者の活動状況などを精査し、廃業や活動終了などのため今後の脆弱性対応を期待できない製品開発者の登録を抹消しました。上記の登録数にはこの登録抹消に伴う減少分が反映されています。登録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

本四半期は 3 月 19 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開催しました。ミーティングでは、VINCE（脆弱性調整の関係者間コミュニケーションツール）の利用における課題、製品開発者の脆弱性対応における法律上・契約上の課題、脆弱性を悪用する攻撃活動の観測状況の報告と今後の調査・分析の提案、PSIRT 活動のベストプラクティスガイド改定版の紹介といったテーマで、参

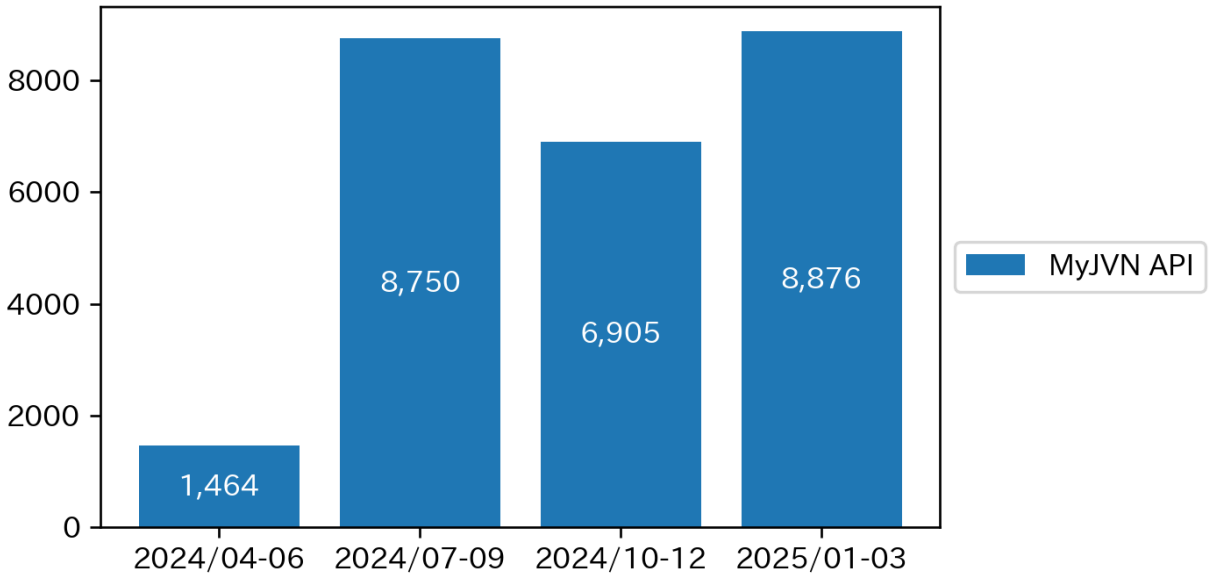


図 2.3 VRDA フィード配信件数

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。

図 2.4 に示したように、インデックスの利用数は、前四半期と比較し約 41% 減少しました。脆弱性情報の利用数は約 30% 減少しました。

図 2.5 に示したように、データ形式別利用傾向は、前四半期と比較し大きな変化は見られませんでした。

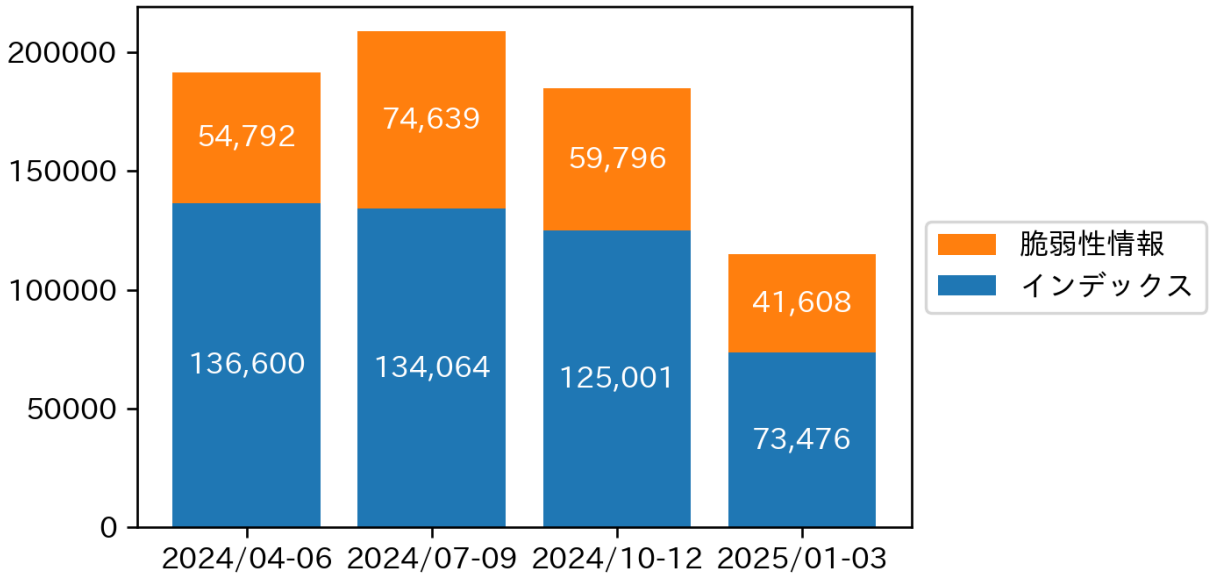


図 2.4 VRDA フィード利用件数

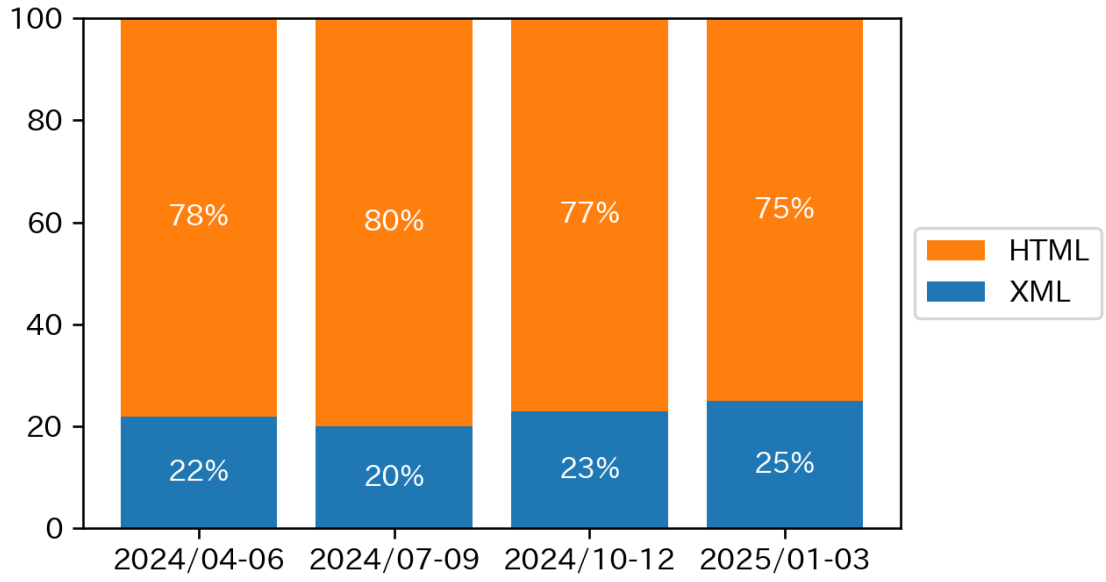


図 2.5 脆弱性情報のデータ形式別利用割合

第 3 章

国内連携活動

前章まで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、平時から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 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。

3.1.2 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を支援しています。本四半期においては、3 月 6 日に開催された第 79 回セプターカウンシル運営委員会で、「Ivanti Connect Secure などにおける脆弱性（CVE-2025-0282）に関する注意喚起」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いただくなど、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 17 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 33 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 1,700 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、ご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。

なお、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は 4 月末をもってサービスを終了する予定です。

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。

- 2025-01-17 JPCERT/CC ICS Security Notes FY2024_#Q3

なお、ICS Security Notes は 4 月末をもってサービスを終了する予定です。

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 1 月 15 日に電話会議を、3 月 10 日と 11 日には韓国のソウルで対面の会議を行い、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。

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加え、1 月にモナコ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

4.3 海外 CSIRT 等の来訪および訪問

4.3.1 モンゴル MNCERT/CC の来訪（2 月 13 日）

モンゴルの MNCERT/CC および同国のサイバーセキュリティ関係者が 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もに、今後の協力について意見交換を行いました。

4.3.2 韓国 KrCERT/CC への訪問（3 月 12 日）

韓国の KrCERT/CC のオフィスを訪問しました。活動の状況について紹介を受けるとともに、施設を見学し、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 RightsCon への参加（2 月 24 日〜27 日）

デジタル空間における人権をテーマにした世界最大規模の国際会議である RightsCon が、2 月 24 日から 27 日にかけて台北市で開催されました。世界の多くの国・地域から、この分野の研究者、ジャーナリスト、人権擁護団体関係者、政府関係者、テクノロジー企業担当者などが幅広く参加しました。（図 4.1）JPCERT/CC は初めて現地で参加し、特にサイバーセキュリティや、スパイウェア、グローバルガバナンス等に関する国際的な議論の動向を把握し、JPCERT/CC の国際連携活動に活かすことを目的として発表を聴講するなど、情報収集に努めました。RightsCon については次の Web ページをご参照ください。

- RightsCon
  https://www.rightscon.org/

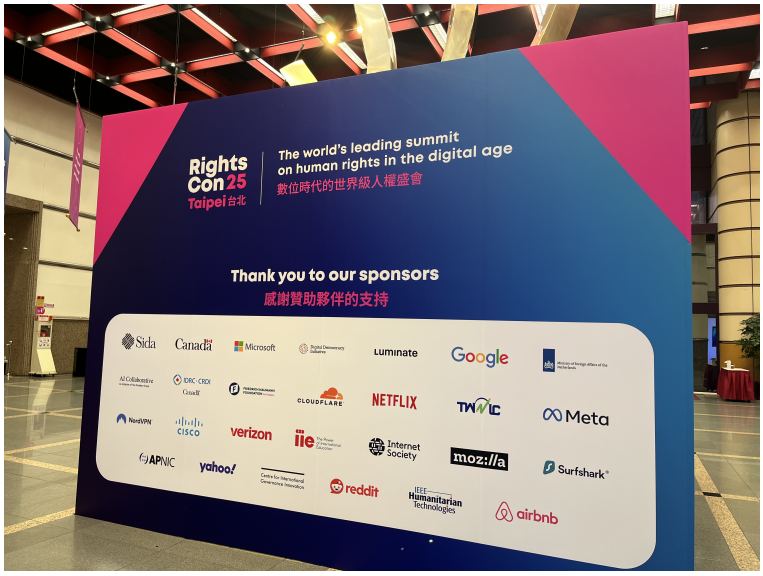


図 4.1 RightsCon の会場の様子

4.5 国際標準化活動

IT セキュリティ分野の標準化を行うための組織 ISO/IEC JTC-1/SC27 で進められている標準化活動のうち、作業部会 WG3（セキュリティの評価・試験・仕様に関する標準化を担当）で検討されている標準化作業の一部と、WG4（セキュリティコントロールとサービスに関する標準化を担当）で検討されているインシデント管理に関する標準の改定に、情報処理学会の情報規格調査会を通じて参加しています。

本四半期について WG3 では、国際会議において脆弱性情報公開ならびに脆弱性取り扱いの手法に関する文書の改訂が提案されたことを受け、関連する情報の収集ならびに対応の検討を開始しました。

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、ここ数年の傾向と同様に旧正月前後の期間に減少しました。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。

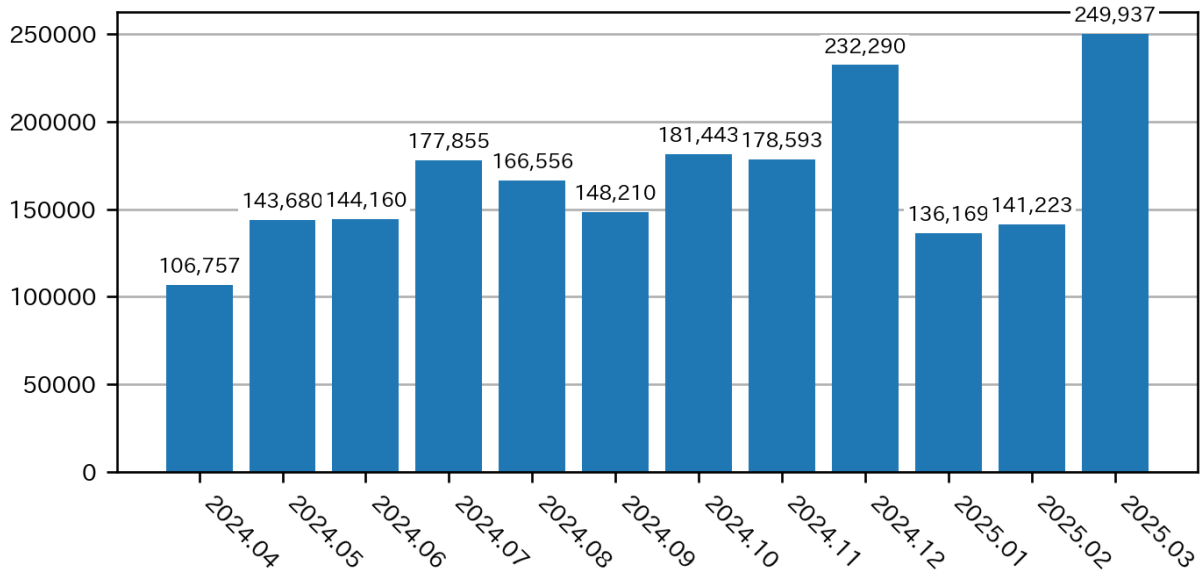


図 5.1 フィッシング報告件数

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 24.0% を占めました。次いで、「Apple」をかたるフィッシングの報告も多く、全体の約 9.2% を占めました。

5.2 情報収集／配信

5.2.1 フィッシングの動向等に関する情報配信

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 2 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。

- Apple をかたるフィッシング：1 件
- マネックス証券をかたるフィッシング：1 件

前述のとおり前四半期と比較して報告件数は減少していますが、引き続きフィッシングには注意が必要です。

本四半期に発生したフィッシングでは、抽選、支払い利用、新規契約、サイトへのログイン等によるポイントプレゼント、キャッシュバックなど、さまざまなキャンペーンを装って誘導する文面が多く報告されました（図 5.2）。利用者は毎日のように届く本物のメールを見慣れているため、それを模倣したフィッシングメールには違和感を覚えにくく、注意が必要です。また、利用都度通知、月額請求、本人確認、契約更新、退会、税金未納、宅配便配達不能通知などが件名に含まれるメールも引き続き報告されています（図 5.3）。2 月からは証券会社をかたるフィッシングも増加しています。フィッシングの誘導 URL については、メールごとに違うランダム文字列のサブドメインを付加した「使い捨て」URL や、同じホスト名で違うパラメーターを付加した使いまわしパターンが増加しました。

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/
- 2025/01 フィッシング報告状況
  https://www.antiphishing.jp/report/monthly/202501.html
- 2025/02 フィッシング報告状況
  https://www.antiphishing.jp/report/monthly/202502.html

週末限定！PayPayポイントキャッシュバック

週末にお買い物でチャンスを掴もう！

キャンペーン概要

2025年2月1日～2月28日の間、毎週末（毎週土・日）にPayPayでお買い物をするだけで、自動で抽選に参加できます。抽選で最大30,000円分のPayPayポイントがキャッシュバックされます。

詳細情報

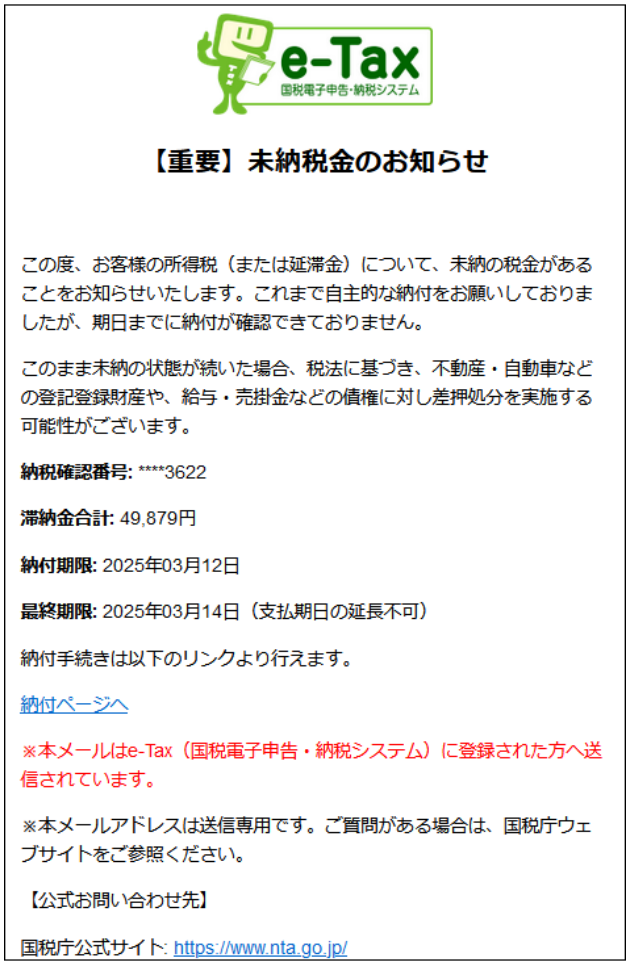
- **開催期間：**2025年2月1日～2月28日（週末限定）
- **参加方法：**週末に1回以上PayPayでお買い物するだけ
- **賞品：**最大30,000円分のPayPayポイント（毎週抽選）
- **当選発表：**翌週の平日にPayPayアプリ内で通知

今すぐ参加する

PayPay株式会社 | お問い合わせ

このメールは送信専用です。返信は受け付けておりません。

図 5.2 キャッシュバックをかたるフィッシングメールの例



e-Tax 国税電子申告・納税システム

【重要】未納税金のお知らせ

この度、お客様の所得税（または延滞金）について、未納の税金があることをお知らせいたします。これまで自主的な納付をお願いしておりましたが、期日までに納付が確認できておりません。

このまま未納の状態が続いた場合、税法に基づき、不動産・自動車などの登記登録財産や、給与・売掛金などの債権に対し差押処分を実施する可能性がございます。

納税確認番号: ****3622

滞納金合計: 49,879円

納付期限: 2025年03月12日

最終期限: 2025年03月14日（支払期日の延長不可）

納付手続きは以下のリンクより行えます。

納付ページへ

※本メールはe-Tax（国税電子申告・納税システム）に登録された方へ送信されています。

※本メールアドレスは送信専用です。ご質問がある場合は、国税庁ウェブサイトをご参照ください。

【公式お問い合わせ先】

国税庁公式サイト: https://www.nta.go.jp/

図 5.3 税金未納をかたるフィッシングメールの例

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。また、本年度の成果として、ガイドラインおよびレポートの改定概要を発表する活動報告会を実施しました。

- 技術・制度検討ワーキンググループ会合（第 5 回）
  日時：2 月 3 日（月）17：00〜19：00（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 6 回兼活動報告会）
  日時：2 月 25 日（火）15：00〜17：15（TKP 秋葉原カンファレンスセンター＋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 125 回運営委員会（オンライン）
  日時：2 月 20 日（木）16：00〜18：00
- 第 126 回運営委員会（JPCERT/CC 会議室 + オンライン）
  日時：3 月 21 日（金）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〜2 月　毎週火曜日 9：00〜9：30（オンライン）
- 第 5 回証明書普及促進ワーキンググループ会合
  日時：1 月 30 日（木）16：30〜18：00（オンライン）
- 第 11 回フィッシング対策勉強会
  日時：2 月 6 日（木）13：00〜15：00（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。

- 2025-01-23
  JPCERT/CC インシデント報告対応レポート［2024 年 10 月 1 日～2024 年 12 月 31 日］
  https://www.jpcert.or.jp/pr/2025/IR_Report2024Q3.pdf
- 2025-03-13
  JPCERT/CC Incident Handling Report [October 1, 2024 - December 31, 2024]
  https://www.jpcert.or.jp/english/doc/IR_Report2024Q3_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。

- 2025-02-28
  JPCERT/CC インターネット定点観測レポート［2024 年 10 月 1 日～2024 年 12 月 31 日］

https://www.jpcert.or.jp/tsubame/report/report202410-12.html
https://www.jpcert.or.jp/tsubame/report/TSUBAME_Report2024Q3.pdf

- 2025-03-13
  JPCERT/CC Internet Threat Monitoring Report [October 1, 2024 - December 31, 2024]
  https://www.jpcert.or.jp/english/doc/TSUBAMEReport2024Q3_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。

- 2025-01-23
  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 4 四半期（10 月～12 月）］
  https://www.jpcert.or.jp/pr/2025/vulnREPORT_2024q4.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 14 件の記事を公表しました。

日本語版発行件数：8 件 https://blogs.jpcert.or.jp/ja/

2025-01-10 あなたではなく組織の財産を狙う LinkedIn 経由のコンタクトにご用心

2025-01-20 APT アクターの分類 “中毒” ―Lazarus のサブグループ分類に見るアトリビューションの実務的課題―

2025-02-12 Ivanti Connect Secure の脆弱性を利用して設置されたマルウェア SPAWNCHIMERA

2025-02-26 JSAC2025 開催レポート～DAY 1～

2025-02-28 TSUBAME レポート Overflow（2024 年 10～12 月）

2025-03-05 JSAC2025 開催レポート～DAY 2～

2025-03-12 JSAC2025 開催レポート～Workshop & Lightning Talk～

2025-03-24 制御システムセキュリティカンファレンス 2025 開催レポート

英語版発行件数：6 件 https://blogs.jpcert.or.jp/en/

2025-01-20 Beware of Contacts through LinkedIn: They Target Your Organization’s Property, Not

Yours

2025-02-20 SPAWNCHIMERA Malware: The Chimera Spawning from Ivanti Connect Secure Vulnerability

2025-03-05 JSAC2025 -Day 1-

2025-03-19 JSAC2025 -Day 2-

2025-03-21 TSUBAME Report Overflow (Oct-Dec 2024)

2025-03-25 Tempted to Classifying APT Actors: Practical Challenges of Attribution in the Case of Lazarus's Subgroup

第 8 章

その他の活動

8.1　講演

1. 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：1 月 25 日）
2. 堀 充孝（早期警戒グループ 脅威情報アナリスト）
   「【KIIS セキュリティ人材育成プログラム】CSIRT 構築・運営」
   KIIS サイバーセキュリティ研究会 セキュリティ人材育成プログラム（主催：一般財団法人関西情報センター、講演日：1 月 28 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）
   「『能動的サイバー防御』導入に備えた “傾向と対策”」
   第 19 回セキュリティセミナー（主催：特定非営利活動法人新潟情報通信研究所、講演日：2 月 7 日）
4. 衛藤 亮介（早期警戒グループ 脅威アナリスト）
   「最近のサイバー攻撃の動向と対策について」
   第 35 回クレジット CEPTOAR 運営会議（主催：一般社団法人日本クレジット協会、講演日：2 月 14 日）

8.2　執筆

1. 藤堂 伸勝（早期警戒グループ 脅威情報アナリスト）
   「2024 年の情報セキュリティの動向」
   （掲載媒体名：インターネット白書 2025、発行：株式会社インプレス、発行日：2 月 14 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. 第 2 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：1 月 23 日）
2. 日本セキュリティ・マネジメント学会 第 16 回公開討論会
   （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：2 月 1 日）
3. 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：2 月 19 日〜20 日、3 月 14 日）
4. Security Days Spring 2025
   （主催：株式会社ナノオプト・メディア、開催日：3 月 5 日、11 日〜14 日、19 日）
5. Data Center Japan 2025
   （主催：特定非営利活動法人日本データセンター協会、開催日：3 月 18 日〜19 日）
6. サイバーセキュリティシンポジウム 2025
   （主催：株式会社経済産業新報社、開催日：3 月 25 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 ［ 2025 年 1 月 1 日～2025 年 3 月 31 日 ］

- 発行履歴
  - 2025 年 4 月 17 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/