JPCERT CC®

JPCERT/CC 四半期レポート

2026 年 1 月 1 日～2026 年 3 月 31 日

2026 年 4 月 16 日

一般社団法人 JPCERT コーディネーションセンター

目次

はじめに

一般社団法人 JPCERT コーディネーションセンター（以下「JPCERT/CC」）は、インターネット利用組織における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」）の認知と対処および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外の関係機関と調整活動を行っています。

これらの活動のほとんどを、「 令和 7 年度サイバー攻撃等国際連携対応調整事業 」（経済産業省委託事業）および「 被害組織から円滑に攻撃技術情報を収集する手法に関する検証業務 」（内閣官房委託事業）として実施しています。

本レポートでは、 2026 年 1 月 1 日～2026 年 3 月 31 日 までの活動について報告しています。

なお、「第 5 章 国内連携活動」「第 6 章 国際連携活動」「第 7 章 フィッシング対策協議会活動」「第 8 章 広報活動」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。

トピックス＆ハイライト

セキュリティアナリスト向けカンファレンス「JSAC2026」を開催

2026 年 1 月 21 日～2026 年 1 月 23 日にかけて JSAC2026 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セキュリティ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。

9 回目の開催になる今回は、91 件の応募から採択された 20 件の講演（ワークショップ 3 件を含む）の他に、Lightning Talk セッションとして 6 件の発表、パネルディスカッションが行われました。インシデント対応事例や攻撃アクターの分析、近年のフィッシング攻撃の傾向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が共有されました。また、今回は初日に 3 つのアナリスト向け分析トレーニングを実施しました。トレーニング Day には 250 名の方にご参加いただき、アンケート結果では参加者の 98 %から次回のトレーニングにも参加したいという評価をいただきました。次年度も引き続きトレーニングを充実させていく予定です。

2 日目、3 日目のカンファレンス Day は、405 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、JSAC でしか聞くことができない講演がいくつもあり貴重なアナリスト同士の共有の場であると好評をいただいています。なお、講演資料は JSAC2026 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」でも紹介していますので、ご覧ください。

- JSAC2026
  https://jsac.jpcert.or.jp/
- JSAC2026 開催レポート～DAY 1～
  https://blogs.jpcert.or.jp/ja/2026/02/jsac2026day1.html
- JSAC2026 開催レポート～DAY 2～
  https://blogs.jpcert.or.jp/ja/2026/02/jsac2026day2.html
- JSAC2026 開催レポート～Workshop ／ Lightning Talk Session ／ Panel Discussion～
  https://blogs.jpcert.or.jp/ja/2026/03/jsac2026-ws-lt-pd.html

「制御システムセキュリティカンファレンス 2026」を開催

2026 年 2 月 10 日に制御システムセキュリティカンファレンス 2026 を開催しました。国内における制御システムのセキュリティ向上を目的に、2009 年に開始した催しです。コロナ禍のためオンライン開催ないしハイブリッド開催が続いていましたが、今回から完全な対面形式に復し、137 名の方々（事前登録者 216 名）にご参加いただきました。プログラムは公募による講演と JPCERT/CC の企画講演で構成し、経済産業省からの開会のあいさつに続き、JPCERT/CC からの発表 2 件、JPCERT/CC と外部講演者による共同発表 1 件、外部講演者による発表 3 件の計 6 件の講演が行われました。

JPCERT/CC からの 2 件の講演では、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について解説し、また、CVD に関連した脆弱性対応の枠組みに関する国際的な動向を紹介しました。JPCERT/CC と外部講演者による共同講演ではパネルディスカッション形式を取り入れ、JPCERT/CC が主催する制御システムユーザー組織のセキュリティ担当者コミュニティーの取り組み事例を紹介し、制御システムユーザーの実務に役立ててもらうための情報を提供しました。外部講演者による 3 件の講演では、工場で培われてきた「備え」をサイバーインシデント対応へ応用する考え方について、自動車産業においてデジタルツインの活用が進む背景やデジタルツインへの攻撃への防御手法について、さらには DFD（Data Flow Diagram）でシステム構造を整理し、Safety ／ Security 要件や SBOM や意思決定履歴を同一の台帳（JSON）に統合する手法の提案に関し発表していただきました。また、カンファレンス終了後には情報交換会を開催し、講演者・参加者の別なく、意見交換や情報共有を通じて交流を深めました。

アンケート結果によると、カンファレンスには制御機器／制御システムユーザーを中心として、制御システムエンジニアリング、制御システム／制御機器ベンダーおよび研究者の方々に幅広く参加していただきました。また、アンケート回答者の 3 人に 1 人は初参加であり、継続参加者と新規参加者の双方から貴重なご意見をいただきました。

なお、講演資料は JPCERT/CC の Web サイト、講演動画は JPCERT/CC の YouTube チャンネルで公開しています。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 2026
  https://www.jpcert.or.jp/event/ics-conference2026.html

- 制御システムセキュリティカンファレンス 2026 講演資料
  https://www.jpcert.or.jp/present/#year2026
- 制御システムセキュリティカンファレンス 2026 講演動画
  https://www.youtube.com/playlist?list=PLgEi6O-lWUIaE_ASwPJAjHVkOSYXjb3fY
- 制御システムセキュリティカンファレンス 2026 開催レポート
  https://blogs.jpcert.or.jp/ja/2026/03/ics-conference2026.html

第 1 章

インシデント対応支援

JPCERT/CC では、国内外で発生するインシデントの報告を受け付けています[*1]。本章では、本四半期に受け付けたインシデント報告について、統計など定量的な観点と、特筆すべき事例など定性的な観点から紹介します。

1.1 四半期の統計情報

本四半期のインシデント報告の数、報告されたインシデントの総数および報告に対応して JPCERT/CC が行った調整の件数を月別に表 1.1[*2]に示します。

本四半期に寄せられた報告件数は 15,345 件でした。このうち、JPCERT/CC が国内外の関連する組織との調整を行った件数は 3,168 件でした。前四半期と比較して、報告件数は 25% 減少、調整件数は 10% 増加しました。また、前年同期（報告件数は 10,102 件、調整件数は 3,974 件）と比較すると、報告数は 51% 増加、調整件数は 20% 減少しました。

図 1.1 と図 1.2 に報告件数および調整件数の過去 1 年間の月次の推移を示します。

JPCERT/CC では、報告を受けたインシデントをカテゴリー別に分類し、カテゴリーに応じた調整、対応を実施しています。各インシデントの定義については**付録 A インシデントの分類**をご参照ください。

表 1.1 インシデント報告等の月別件数

	1 月	2 月	3 月	合計	前四半期合計
報告件数	6,795	3,446	5,104	15,345	20,336
インシデント件数	3,677	2,536	4,049	10,262	13,537
調整件数	943	991	1,234	3,168	2,875

[*1] JPCERT/CC では、情報システムの運用におけるセキュリティ上の問題として捉えられる事象、コンピューターのセキュリティに関わる事件、できごとの全般を**インシデント**と呼んでいます。

[*2] **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。**インシデント件数**は、各報告に含まれるインシデント件数の合計を示します。一つのインシデントに関して複数件の報告が寄せられた場合にも、1 件として扱います。**調整件数**は、インシデントの拡大防止のため、サイトの管理者等に対し、現状の調査と問題解決のための対応を依頼した件数を示します。

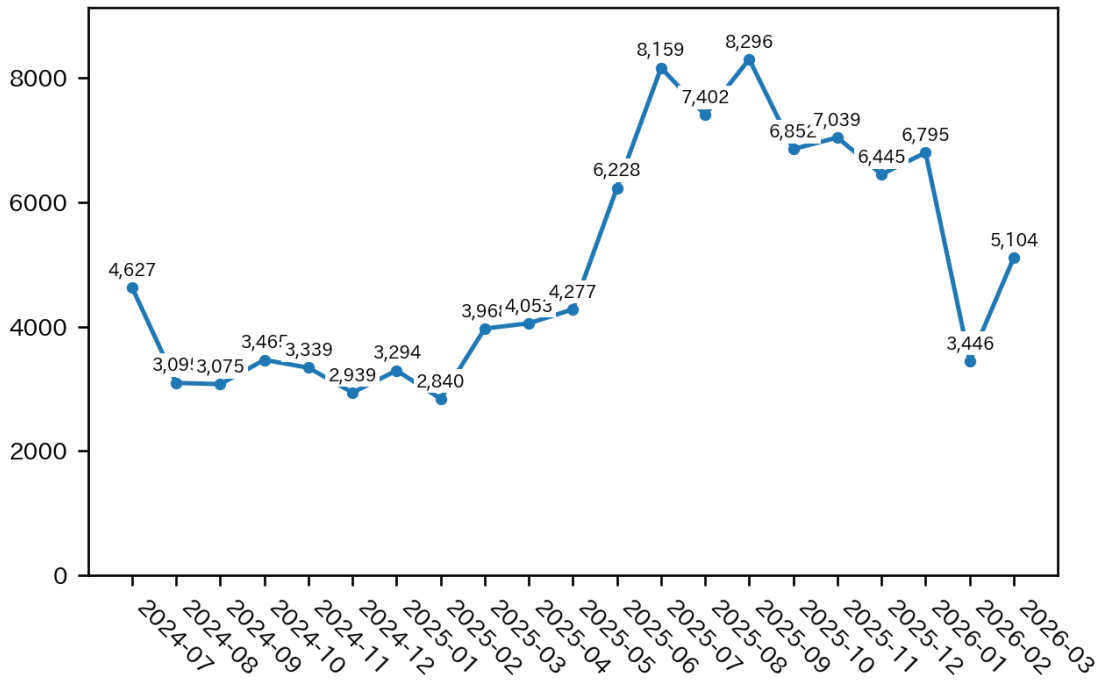

図 1.1 インシデント報告件数の推移

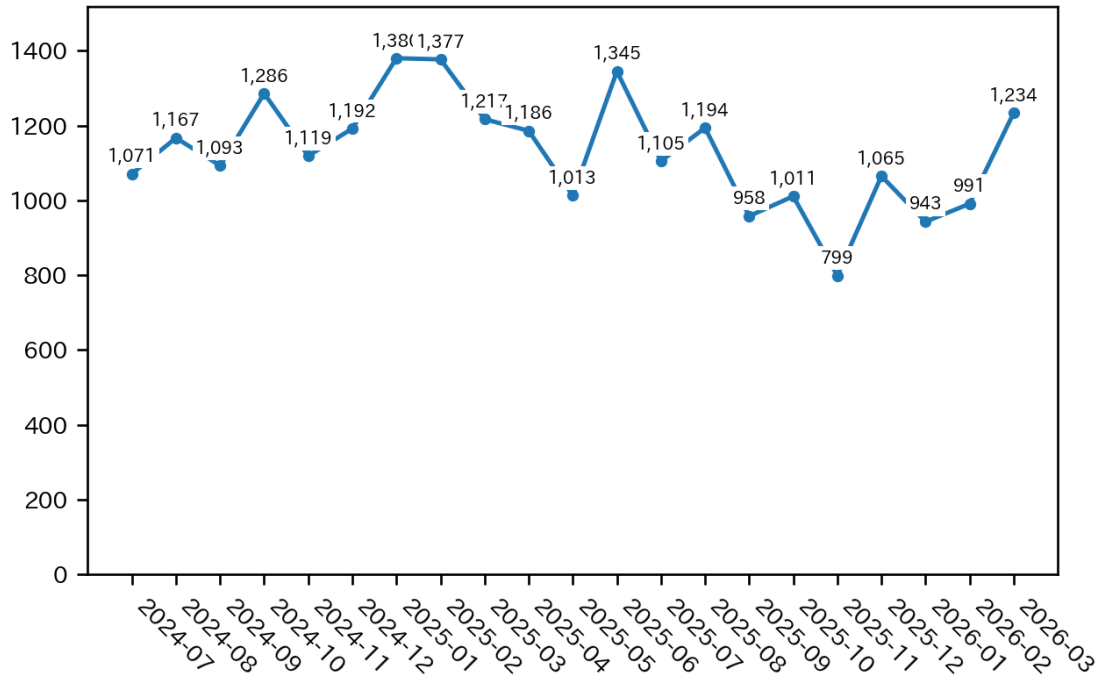

図 1.2 インシデント調整件数の推移

表 1.2 インシデント報告件数のカテゴリー別内訳

インシデント	1 月	2 月	3 月	合計	前四半期合計
フィッシングサイト	3,421	2,227	3,645	9,293	12,397
Web サイト改ざん	29	24	37	90	105
マルウェアサイト	7	19	6	32	44
スキャン	37	62	57	156	469
DoS/DDoS	0	1	3	4	6
制御システム関連	0	0	0	0	0
標的型攻撃	0	0	2	2	3
その他	183	203	299	685	513

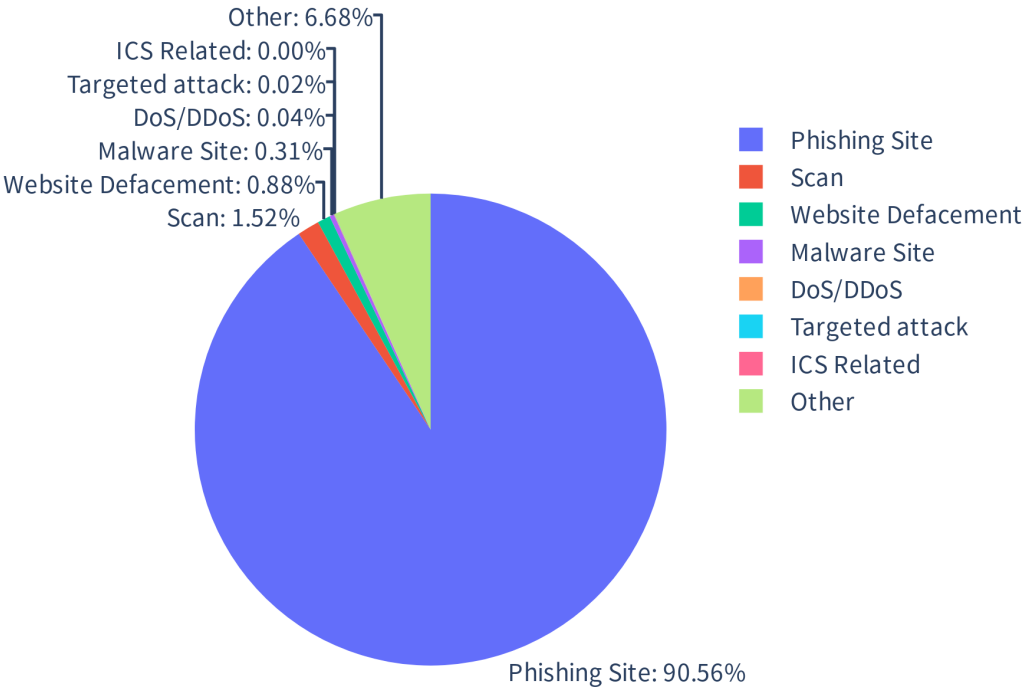

図 1.3 インシデント報告件数のカテゴリー別割合

本四半期に報告を受けたインシデント報告件数のカテゴリー別内訳を表 1.2、カテゴリー別割合を図 1.3 に示します。

フィッシングサイトに分類されるインシデントが 90.6% 、スキャンに分類される、システムの弱点を探索するインシデントが 1.5% を占めています。

図 1.4 から図 1.7 に、フィッシングサイト、Web サイト改ざん、マルウェアサイト、スキャンの各インシデントの過去 1 年間の月次の推移を示します。

また、図 1.8 にインシデントのカテゴリーごとの件数および調整・対応状況を示します。

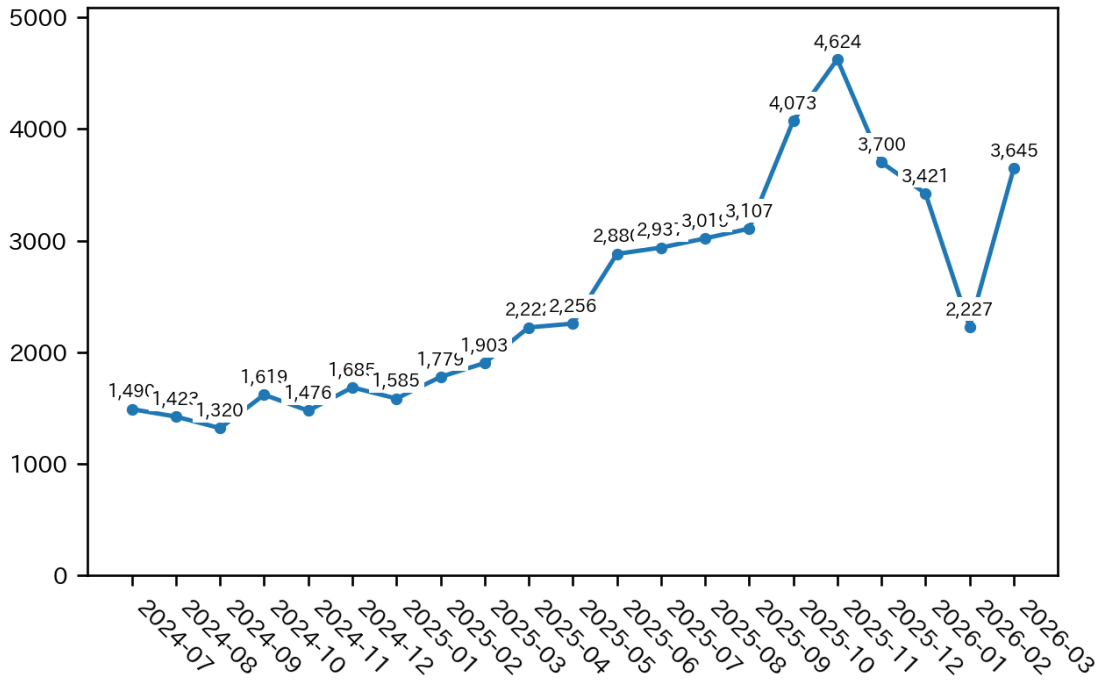

図 1.4 フィッシングサイト件数の推移

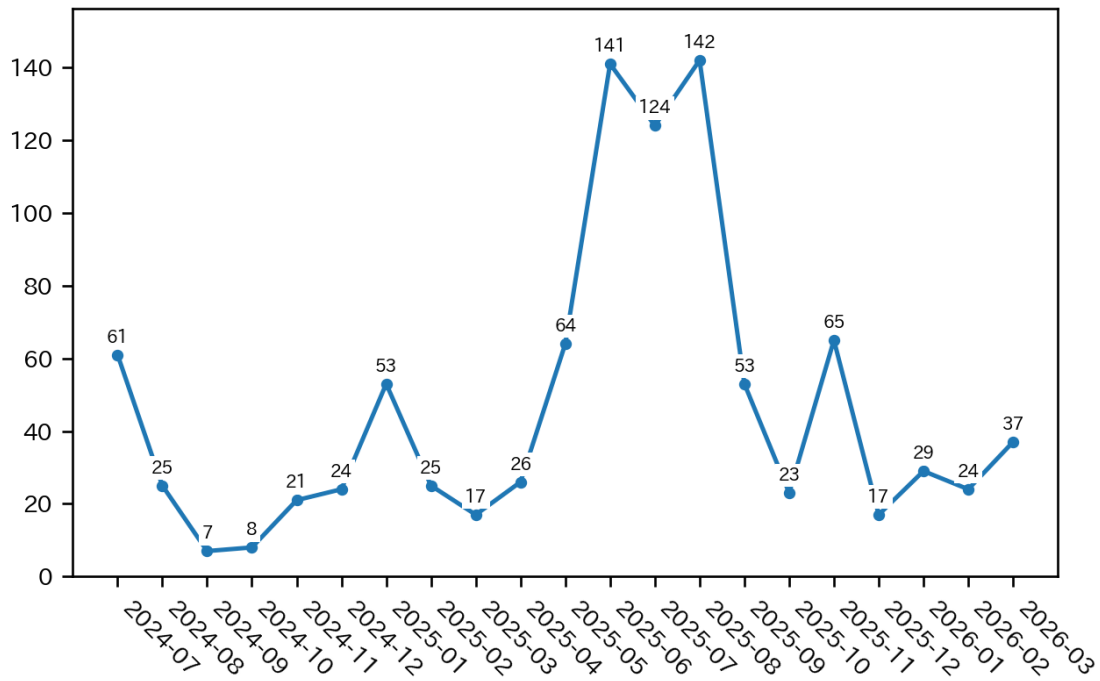

図 1.5 Web サイト改ざん件数の推移

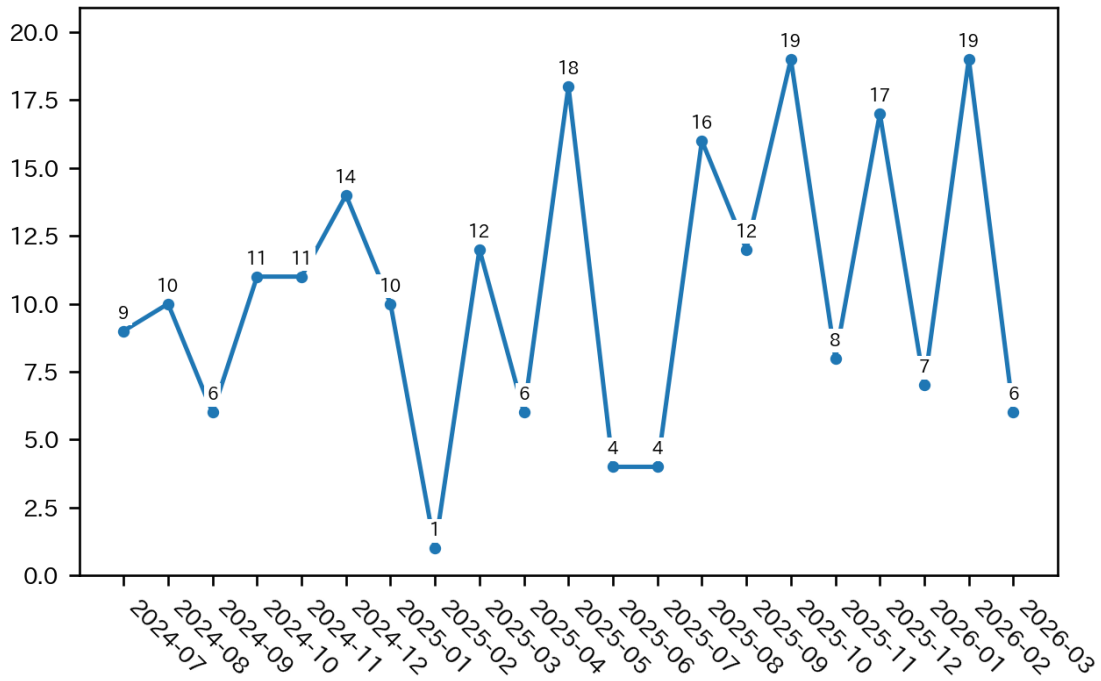

図 1.6 マルウェアサイト件数の推移

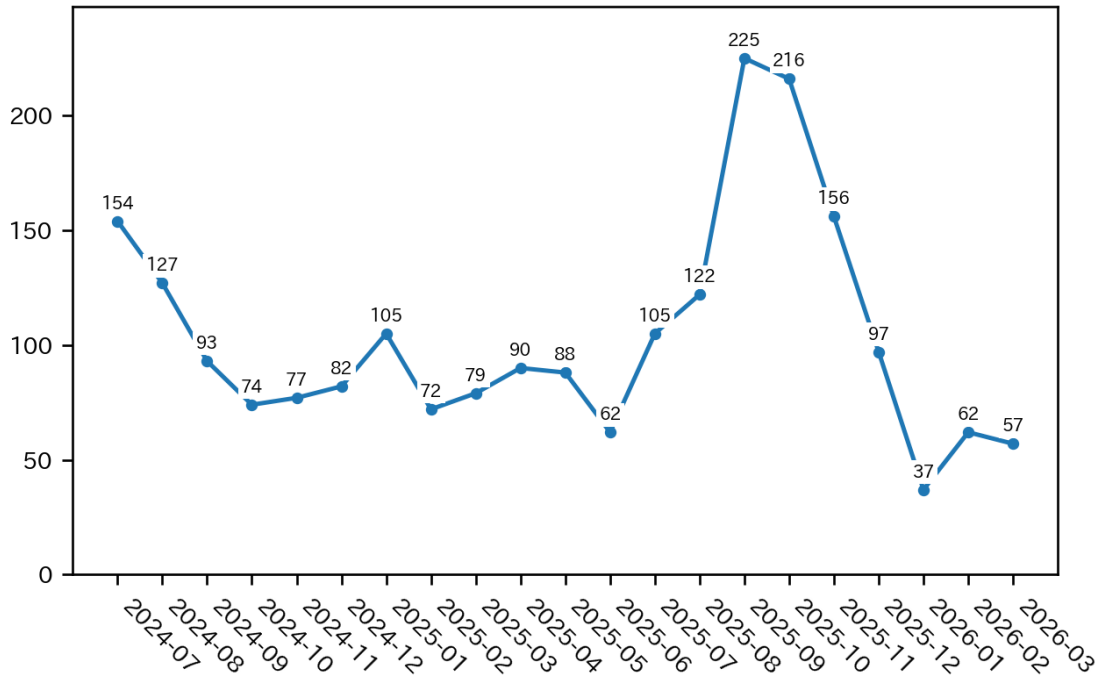

図 1.7 スキャン件数の推移

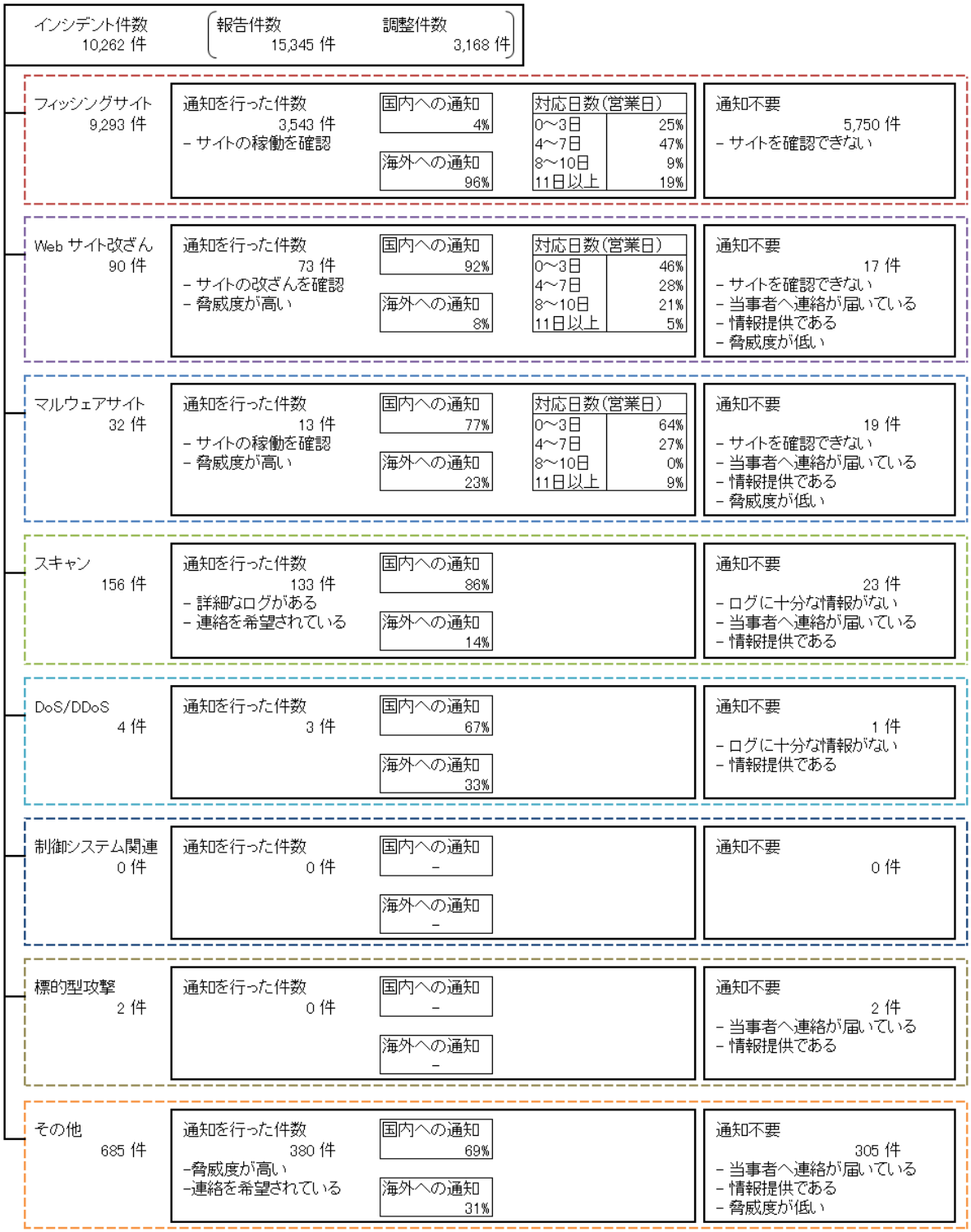

図 1.8 インシデントのカテゴリーごとの件数と調整・対応状況

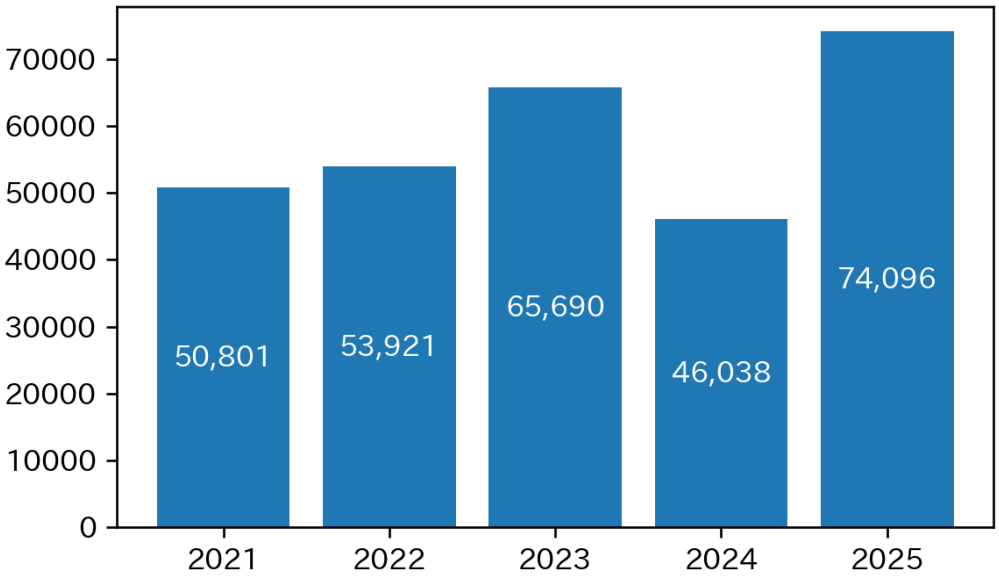

図 1.9 年度ごとの報告件数の推移

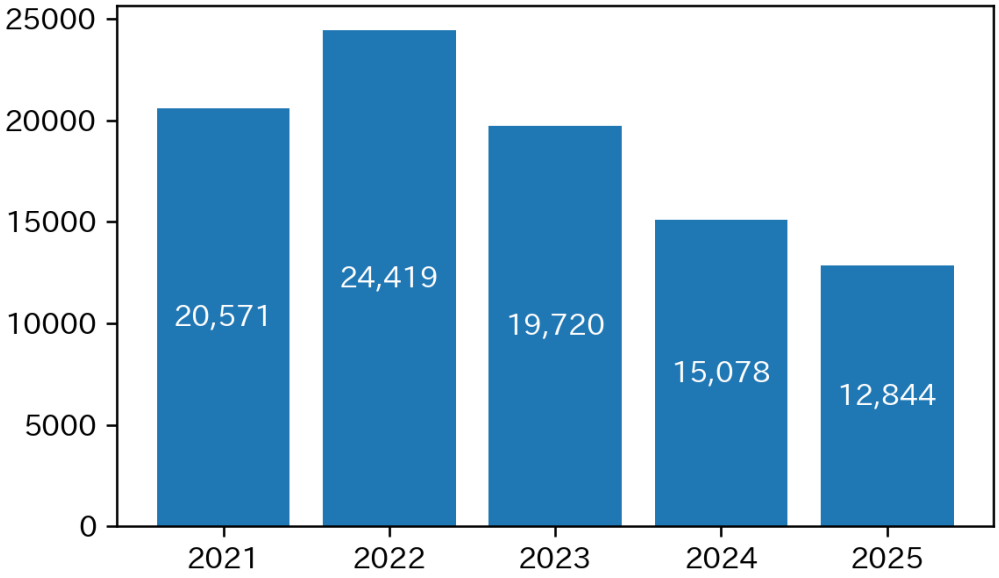

図 1.10 年度ごとの調整件数の推移

1.2　年次統計情報

本年度までの過去 5 年間の年度ごとの報告件数の推移を図 1.9 に、調整件数の推移を図 1.10 に示します。本年度に寄せられた報告件数は 74,096 件でした。前年度の 46,038 件と比較して 61% 増加しました。本年度に調整を行った件数は 12,844 件でした。前年度の 15,078 件と比較して 15% 減少しました。

表 1.3 ブランドの国内外別によるフィッシングサイト件数の内訳

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	2,644	1,448	3,020	7,112	76%
国外ブランド	199	377	323	899	10%
ブランド不明	578	402	302	1,282	14%
全ブランド合計	3,421	2,227	3,645	9,293	

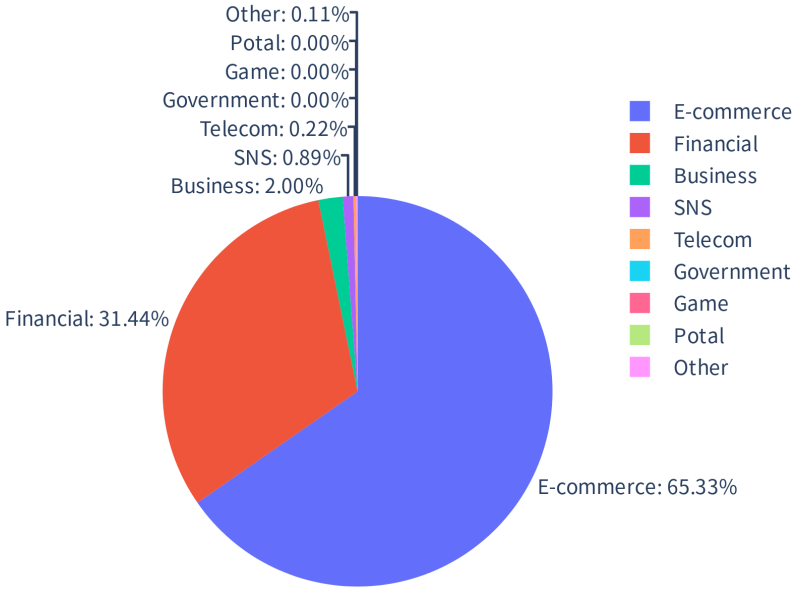

図 1.11 国外ブランドのフィッシングサイトの件数の業界別の割合

1.3 インシデントの傾向

1.3.1 フィッシングサイトの傾向

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 9,293 件で、前四半期の 12,397 件から 25% 減少しました。また、前年同期（5,267 件）との比較では、 76% 増加しました。

本四半期は、国外のブランドを装ったフィッシングサイトの件数が 899 件で、前四半期の 569 件から 58% 増加しました。また、国内のブランドを装ったフィッシングサイトの件数は 7,112 件で、前四半期の 10,532 件から 32% 減少しました。本四半期のブランドの国内外別によるフィッシングサイト件数の内訳[*3] を表 1.3 に、国外ブランドと国内ブランドそれぞれのフィッシングサイト件数の業界別の割合を図 1.11 と図 1.12 に示します。

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 65.3%、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 69.1% で、それぞれ最も多くを占めました。

[*3] **ブランド不明**は、報告されたフィッシングサイトが確認時に停止していた等の理由により、ブランドを確認することができなかったサイトの件数を示します。

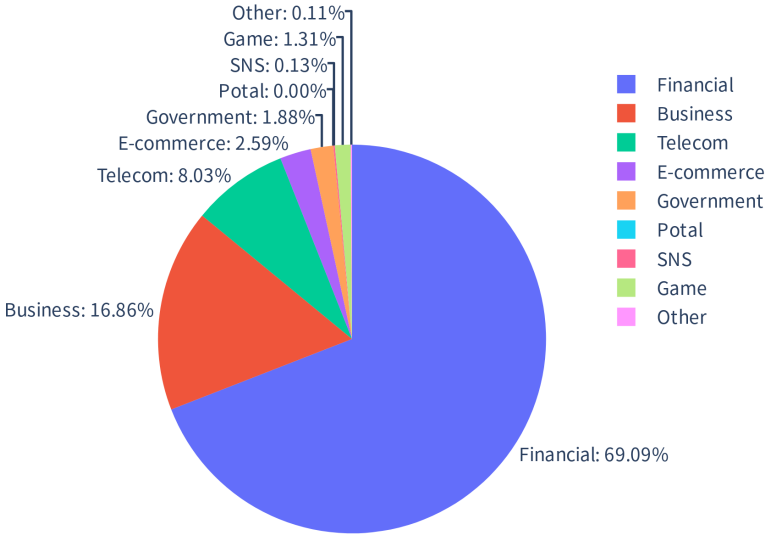

図 1.12 国内ブランドのフィッシングサイトの件数の業界別の割合

国外ブランドでは、Amazon と Apple Account を装ったフィッシングサイトが多くを占めました。国内ブランドでは、マネックス証券、SBI 証券、SMBC 日興証券など証券会社を装ったフィッシングサイトの報告が多く寄せられました。また、JCB、三井住友カード、セゾンカードなどのクレジットカード会社を装ったものも依然として多く報告されています。フィッシングサイトをテイクダウンするために調整したサイトの内訳は、国外が 96%、国内が 4% でした。

1.3.2 Web サイト改ざんの傾向

本四半期に報告が寄せられた Web サイト改ざんの件数は 90 件でした。前四半期の 105 件から 14% 減少しました。

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。

- 事例 1：正規 Web サイトに Web シェルが設置されていた事例
- 事例 2：正規 Web サイトに「Efimer」の拡散活動の一部の可能性のある改ざんが行われた事例

事例 1 では、国内の複数の正規 Web サイトにおいて、同じ Web シェル（図 1.13）が設置されていました。設置された Web シェルを使って攻撃者が任意のコマンドを実行したり、コンテンツを改ざんしたりした可能性があります。

事例 2 では、国内の WordPress で構築された複数の Web サイトが改ざんされ、「0x1c8c5b6a」という文字列を含むファイルが設置されていました。該当の文字列が含まれる Web サイトは攻撃者が不正な投稿や書き込みを行っている可能性が指摘されており、マルウェア「Efimer」の拡散活動によって改ざんされたものです。

- WordPress サイトの改ざんとトロイの木馬「Efimer」に関する注意喚起
  https://www.lac.co.jp/lacwatch/alert/20250826_004473.html

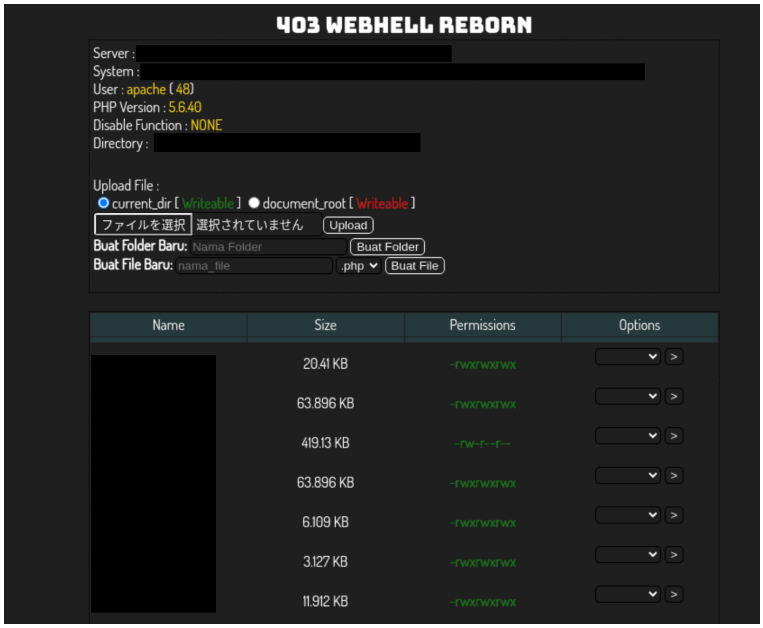

図 1.13 Web シェル

1.3.3 標的型攻撃の傾向

標的型攻撃に分類されるインシデントの件数は 2 件でした。

1.3.3.1 GitHub を悪用した標的型攻撃メール

本四半期は、GitHub を悪用した標的型攻撃メールの報告が寄せられました。メール本文中のリンクをクリックすると ZIP ファイルがダウンロードされ、ZIP ファイル内の LNK ファイルを実行すると、GitHub 上に保存されているおとり文書と PowerShell ファイルが実行される仕組みになっていました。PowerShell ファイルは、端末情報をテキストファイルとして GitHub にアップロードするようになっており、アップロードされた情報から標的と判断された場合、さらなる攻撃活動が行われると考えられます。
なお、本攻撃は 2025 年 8 月に Trellix が報告した攻撃キャンペーンと類似点が見られることから同種の攻撃キャンペーンの可能性があります。

- The Coordinated Embassy Hunt: Unmasking the DPRK-linked GitHub C2 Espionage Campaign
  https://www.trellix.com/blogs/research/dprk-linked-github-c2-espionage-campaign/

1.3.4 その他のインシデントの傾向

本四半期に報告が寄せられたマルウェアサイトの数は 32 件でした。前四半期の 44 件から 27% 減少しています。

本四半期に報告が寄せられたスキャン件数は 156 件でした。前四半期の 469 件から 66% 減少しています。スキャンの対象となったポートの上位 10 位を表 1.4 に示します。頻繁にスキャンの対象となった

表 1.4 ポート別のスキャン件数の上位 10 位

ポート	1 月	2 月	3 月	合計
23/tcp	25	26	7	58
80/tcp	2	4	14	20
443/tcp	1	7	4	12
81/tcp	1	2	2	5
8000/tcp	0	2	3	5
8080/tcp	0	1	4	5
5555/tcp	2	2	0	4
82/tcp	0	1	3	4
9000/tcp	0	0	4	4
85/tcp	0	3	0	3

ポートは、 Telnet（23/TCP)、HTTP（80/TCP)、HTTPS（443/TCP)、81/TCP でした。

その他に分類されるインシデントの件数は 685 件でした。前四半期の 513 件から 34% 増加しました。

1.4 インシデント対応事例

本四半期に行った対応の事例を紹介します。

1.4.1 侵害された海外 Web サイトを踏み台としたフィッシング事案

攻撃者に改ざんされ、SEO スパム化された上でフィッシングサイトへの誘導に悪用された正規 Web サイトの報告を多数受けました。報告された多数のドメインを調査した結果、対象の多くが国外のホスティング環境で運用されていることが確認されました。このため、各国の National CSIRT に関連情報を共有し、サイト管理者やホスティング事業者への注意喚起および対応が行われるよう調整を実施しました。

1.4.2 偽の警告画面を表示するサポート詐欺事案への対応

正規 Web サイトを閲覧中に偽のセキュリティ警告画面を表示し、ユーザーにサポート窓口への連絡を促す事案に関する報告を多数受けました。これらの報告はフィッシングとして寄せられていましたが、調査の結果、偽の警告画面が表示されるなど、いわゆるサポート詐欺である可能性が高い挙動が確認されました。 JPCERT/CC では、セキュリティ警告画面が表示される正規 Web サイトの管理者に対して調整を実施しました。

第 2 章

脅威情報の分析と提供

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、脆弱性情報や脅威情報、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・対策のための情報を提供しています。

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などを収集し、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ポータルサイト「CISTA（Collective Intelligence Station for Trusted Advocates）」（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および分析した情報のうち、特徴的なものを紹介します。

2.1.1 React Server Components の脆弱性（CVE-2025-55182）

2025 年 12 月 3 日（現地時間）、The React Team は React Server Components の脆弱性（CVE-2025-55182）に関するアドバイザリ[*1]を公表しました。React Server Components は、React のレンダリングの一部をサーバー側で行い、その結果をクライアントに送信する仕組みです。本脆弱性により、攻撃者が細工した HTTP リクエスト（HTTP 経由の不正な Flight ペイロード）を、React Server Components（RSC）を利用するサーバーに送信することで、認証を経ずに任意のコードが実行される可能性があります。JPCERT/CC は、本脆弱性の悪用観測などの情報は未確認であったものの、本脆弱性は認証を経ず

[*1] “Critical Security Vulnerability in React Server Components”. The React Team. https://react.dev/blog/2025/12/03/critical-security-vulnerability-in-react-server-components, (2025-12-03)

に任意のコード実行が可能であること、また、React Server Components を利用する Next.js などの主要フレームワークは国内でも広く採用されており影響を受けるシステムが多岐にわたると想定されたことから、対策の早期実施を広く呼びかける目的で、2025 年 12 月 5 日に CyberNewsFlash[*2]を公開しました。

その後、JPCERT/CC に本脆弱性の悪用に関する複数の報告が寄せられました。その中には、本脆弱性が公開後比較的短期間で悪用され、複数の攻撃者が広範囲に攻撃を行った可能性を示唆する事案が含まれていました。この事例のように、遠隔から任意のコード実行によってシステムへ深刻な影響を与える攻撃が、脆弱性の公表から間を置かず広範囲に発生するケースが増加傾向にあるため、パッチの迅速な適用が重要度を増しています。確認した攻撃活動の実態に鑑みて、JPCERT/CC では、攻撃のタイムラインや使用されたマルウェアの分析をまとめたブログ記事[*3]を公開しました。

また、本脆弱性を悪用して Web サイトを改ざんし、本脆弱性への対応を促すメッセージを表示させていた事例もありました。改ざんされた Web サイトにアクセスすると、4 カ国語で「CVE-2025-55182 の脆弱性があるため、早急にパッチの適用が必要」といった警告が表示されていました。調査の結果、約 50 件の Web サイトで改ざんが行われていることが判明し、当該サイトの管理者などに対して個別通知を実施しました。

2.1.2 MongoDB における情報漏えいの脆弱性（CVE-2025-14847）

2025 年 12 月 19 日（現地時間）、MongoDB は MongoDB における初期化されていないヒープメモリからの情報漏えいの脆弱性（CVE-2025-14847）に関するアドバイザリ[*4]を公表しました。本脆弱性は、認証されていない遠隔の第三者が細工した通信を送信することで、初期化されていないヒープメモリ内に残っている情報を読み取る脆弱性で、結果的に MongoDB 内の機密情報（API キー、認証情報など）の漏えいにつながる可能性がありました。

複数のセキュリティ企業から、本脆弱性の実証コード（Proof-of-Concept）の解説を含むブログ記事[*5]が公開されたほか、海外において本脆弱性の悪用が示唆される情報[*6]も確認しました。本脆弱性に類する、メモリ内の情報を読み取られる過去の脆弱性は複数ありますが、このうち CitrixBleed（CVE-2023-4966）は、ランサムグループ LockBit が初期侵入に悪用したことが確認されている事例[*7]もあり、社会的に大きな影響を与えました。このような背景から、JPCERT/CC は本脆弱性を悪用した攻撃活動が国内にも

[*2] “React Server Components の脆弱性（CVE-2025-55182）について”. JPCERT/CC. https://www.jpcert.or.jp/newsflash/2025120501.html, (2025-12-05)

[*3] “React2Shell を悪用する複数の攻撃アクターによる侵害事例”. JPCERT/CC. https://blogs.jpcert.or.jp/ja/2026/02/react2shell.html, (2026-02-13)

[*4] “Make minimally sized buffers for uncompressed Messages”. MongoDB. https://jira.mongodb.org/browse/SERVER-115508, (2025-12-19)

[*5] “MongoBleed (CVE-2025-14847): MongoDB Memory Leak Flaw”. Rapid7. https://www.rapid7.com/blog/post/etr-mongobleed-cve-2025-1484-critical-memory-leak-in-mongodb-allowing-attackers-to-extract-sensitive-data/, (2025-12-29)

[*6] “MongoBleed CVE-2025-14847: Critical Memory Leak in MongoDB Allowing Attackers to Extract Sensitive Data”. Resecurity. https://www.resecurity.com/blog/article/mongobleed-cve-2025-14847-mongodb-memory-leak-flaw, (2025-12-30)

[*7] “CVE-2023-4966: LockBit Exploits Citrix Bleed in Ransomware Attacks”. Picus Security. https://www.picussecurity.com/resource/blog/cve-2023-4966-lockbit-exploits-citrix-bleed-in-ransomware-attacks, (2024-05-09)

広がる可能性を懸念し、2026 年 1 月 6 日に CyberNewsFlash[*8]を公開しました。

Shadowserver Foundation は、本脆弱性の影響を受ける可能性のある国内ホストとして、約 120 件の情報を JPCERT/CC へ共有しました。このホスト数はさらに増え、2026 年 1 月中旬の時点で約 600 件に上ったことを受け、内訳の大半を占めるホスティング事業者向けに、契約ユーザーへ対応の周知を依頼する個別通知を実施しました。また、本脆弱性の対応が進んでいない企業に対しては JPCERT/CC からも個別に通知して対応を促しました。

2.1.3 Cisco Secure Email Gateway および Cisco Secure Email and Web Manager の脆弱性（CVE-2025-20393）

2025 年 12 月 17 日（現地時間）、Cisco は Cisco Secure Email Gateway および Cisco Secure Email and Web Manager の脆弱性を標的とした攻撃活動に関するアドバイザリ[*9]を公表しました。これは「Spam Quarantine」機能を有効にし、インターネットに公開して稼働させている場合に、root 権限で任意のコマンド実行が可能となる脆弱性（CVE-2025-20393、CVSS 基本値 10.0）です。遅くとも、脆弱性が公表される前の 2025 年 11 月下旬には悪用されていたことが報告されています。

JPCERT/CC は、本脆弱性の公表以前から当該製品の侵害に関する報告を受けており、それ以外にも国内で約 10 件、脆弱性の悪用が可能になるホストの稼働が確認されたため、脆弱性公表直後から利用組織に対して個別通知を行いました。また、開発元および販売代理店とも連携して、脆弱性情報の流通状況や対処の進展状況の観察を継続していたところ、侵害後の横展開を被った際の調査に関する知見が関係組織へ行き渡っていない状況がみられたため、個別通知を通じて得られた調査知見や攻撃に関する情報について、関係者の許可を得た上で共有し、他の組織における調査にも活用してもらうことができました。

2.1.4 0apt ランサムウェアグループのリークサイト掲載

2026 年 1 月下旬から 2 月上旬にかけて、ランサムウェアグループ「0apt」が、同グループが管理するとみられるリークサイト上に日本企業を含む、およそ 200 件の侵害主張を一挙に掲載しました。JPCERT/CC が投稿された組織名などを分析する限り、実在しない組織名が混在しており、侵害を裏付けるデータサンプルや技術的証拠が欠如していることから、本件の侵害主張の信憑性は低いと評価しました。同時期には同グループが使用するとみられるランサムウェアの検体が確認されていますが、当該検体では AES-256 や RSA に加え「Speck」暗号が利用されており、コードの一部に AI 生成とみられる特徴があるとの指摘[*10]もありました。JPCERT/CC は、掲載対象された組織のうち連絡可能な 4 組織に対して個別に通知し、事態に関する JPCERT/CC の見解を伝えながら、各組織の対応方針などに関し情報交換を行いました。

[*8] “MongoDB における情報漏えいの脆弱性（CVE-2025-14847）について”. JPCERT/CC. https://www.jpcert.or.jp/newsflash/2026010601.html, (2026-01-06)

[*9] “Reports About Cyberattacks Against Cisco Secure Email Gateway And Cisco Secure Email and Web Manager”. Cisco. https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sma-attack-N9bf4, (2025-12-17)

[*10] “0APT Ransomware – The Real Fake?”. The Raven File. https://theravenfile.com/2026/02/14/0apt-ransomware-the-real-fake/, (2026-02-14)

2.1.5 Ivanti Endpoint Manager Mobile (EPMM) の脆弱性 (CVE-2026-1281、CVE-2026-1340)

2026 年 1 月 29 日（現地時間）、Ivanti は Ivanti Endpoint Manager Mobile（EPMM）におけるリモートコード実行の脆弱性（CVE-2026-1281、CVE-2026-1340）に関するアドバイザリを公表しました。本脆弱性を悪用された場合、認証されていない攻撃者によって任意のコードが実行される可能性があります。公表当時、Ivanti はごく少数の顧客環境において本脆弱性の悪用を確認していると公表していました。JPCERT/CC では、本脆弱性の影響を受ける可能性がある製品の国内における利用を確認しており、今後、脆弱性の概念実証が公開される事態を想定し、日和見的な攻撃者による活動をけん制する狙いで、翌 2026 年 1 月 30 日に注意喚起[*11]を公開しました。

また、日本国内においても約 40 件のホストで同製品の稼働が確認されたため、一部の利用組織に対して個別に通知し、早期の対策適用および調査の実施を推奨しました。2026 年 1 月 30 日（現地時間）には脆弱性の概念実証の解説記事が公開[*12]され、その後、本脆弱性を悪用する攻撃の拡大が確認されました。JPCERT/CC では、国内外のパートナー組織および通知先から得られた情報、公開情報などを総合的に分析し、調査に資する攻撃の痕跡に関する情報を対象組織に提供しました。

2.1.6 FileZen における OS コマンドインジェクションの脆弱性（CVE-2026-25108）

ソリトンシステムズは、2026 年 2 月 13 日、FileZen における OS コマンドインジェクションの脆弱性（CVE-2026-25108）に関する情報[*13]を公表しました。当該製品にログオンしたユーザーが、本脆弱性を悪用して任意の OS コマンドを実行する可能性があり、ソリトンシステムズは公表の時点で本脆弱性の悪用を確認していると言及しています。なお、同社は公表前に JPCERT/CC へ本脆弱性に関する報告を行っており、JPCERT/CC ではこれを受けて調整を進め、同社の公表と同日に JVN で脆弱性情報（JVN#84622767 FileZen における OS コマンドインジェクションの脆弱性）[*14]を公表しています。詳しくは 4.1.2.1 をご参照ください。

同社は、本脆弱性の対策を 2026 年 1 月 13 日にリリースしていますが、JPCERT/CC では、その時点でも、本脆弱性の影響を受ける可能性がある製品が国内において相当数利用されている状況を確認していました。そのため、2026 年 2 月 13 日に、注意喚起[*15]を公開し、本脆弱性への対策実施を広く呼びかけました。また、同製品は政府省庁や自治体などでも使用されていたため、関係する組織に対しても個別に通知し、情報提供を行いました。

[*11] “Ivanti Endpoint Manager Mobile（EPMM）の脆弱性（CVE-2026-1281、CVE-2026-1340）に関する注意喚起”. JPCERT/CC. https://www.jpcert.or.jp/at/2026/at260002.html, (2026-01-30)

[*12] “Someone Knows Bash Far Too Well, And We Love It (Ivanti EPMM Pre-Auth RCEs CVE-2026-1281 & CVE-2026-1340)”. watchTowr. https://labs.watchtowr.com/someone-knows-bash-far-too-well-and-we-love-it-ivanti-epmm-pre-auth-rces-cve-2026-1281-cve-2026-1340/, (2026-01-30)

[*13] “ 【重要】FileZen ログオン後画面でのコマンドインジェクション脆弱性について”. 株式会社ソリトンシステムズ. https://www.soliton.co.jp/support/2026/006657.html, (2026-02-13)

[*14] “JVN#84622767 FileZen における OS コマンドインジェクションの脆弱性”. JVN. https://jvn.jp/jp/JVN84622767/, (2026-02-13)

[*15] “FileZen における OS コマンドインジェクションの脆弱性（CVE-2026-25108）に関する注意喚起”. JPCERT/CC. https://www.jpcert.or.jp/at/2026/at260004.html, (2026-02-13)

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 42,000 名）には一部の情報をメールでも配信しています。

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。

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

本四半期は、8 件公開しました。

- 2026-01-14
  2026 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)
- 2026-01-30
  Ivanti Endpoint Manager Mobile（EPMM）の脆弱性（CVE-2026-1281、CVE-2026-1340）に関する注意喚起 (公開)
- 2026-02-12
  2026 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)
- 2026-02-13
  FileZen における OS コマンドインジェクションの脆弱性（CVE-2026-25108）に関する注意喚起 (公開)
- 2026-03-11
  2026 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)
- 2026-03-11
  Adobe Acrobat および Reader の脆弱性（APSB26-26）に関する注意喚起 (公開)
- 2026-03-30
  F5 BIG-IP Access Policy Manager の脆弱性（CVE-2025-53521）に関する注意喚起 (公開)
- 2026-03-31
  NetScaler ADC および NetScaler Gateway における境界外読み取りの脆弱性（CVE-2026-3055）に関する注意喚起 (公開)

2.2.2 CyberNewsFlash

JPCERT/CC は、公開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。

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

本四半期は、1 件公開し、1 件の情報を更新しました。

- 2026-01-06
  MongoDB における情報漏えいの脆弱性（CVE-2025-14847）について
- 2026-01-07
  React Server Components の脆弱性（CVE-2025-55182）について（更新）

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 120 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/

2.3 CISTA での情報提供

JPCERT/CC は、登録制の情報共有プラットフォーム「CISTA」を運営しています。「早期警戒情報」の受け取りを希望する方々にご登録いただいていて、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 1,300 組織との間で情報共有を行っています。

「早期警戒情報」の枠組みについては、次の Web ページをご参照ください。

- 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、他組織への情報提供などで活用、還元しています。

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 4 件発信しました。

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 58 件発信しました。

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って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ホストの利用組織などに対して情報を提供しています。なお、対象の組織へ CISTA で個別に情報を提供できない場合は、JPNIC WHOIS を利用して登録されている連絡先に通知する、あるいは ISP や保守ベンダーに通知を依頼する場合もあります。本四半期は 30 件提供しました。先述の脆弱性情報や脅威情報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。

第 3 章

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

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、これをホスティングサービス等を利用することで国内外に複数分散配置して、インターネット定点観測システム「TSUBAME」を構築し運用しています。センサーによって受信されるパケットは、特定の機器や特定のサービス機能を探索するために行われていると考えられます。 JPCERT/CC では、センサーで観測されたパケットを継続的に収集し、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あわせて分析しています。その分析から、インターネットを介した攻撃活動や、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。

3.1　インターネット定点観測システム「TSUBAME」を用いた観測

「TSUBAME」では、インターネットからセンサーに到達するパケットのうち TCP、UDP および ICMP パケットを記録しています。なお、センサーはハニーポットとは異なり、到達したパケットに対して応答はしません。ワームの感染活動や弱点探索のためのスキャンなど、セキュリティ上の脅威となるトラフィックの観測を行っています。

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

3.1.1　TSUBAME の観測データの活用

JPCERT/CC では、組織のシステム管理者の方々がインシデント対応や対策などに活用いただけるよう、「TSUBAME」で得た観測データを提供しています。四半期ごとに観測データに基づいた個別の情報提供の他、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』やブログ「TSUBAME レポート Overflow」を公開しています。ブログでは、レポートに書ききれなかった分析内容や、期間中に発生した特徴的な事象を取り上げています。

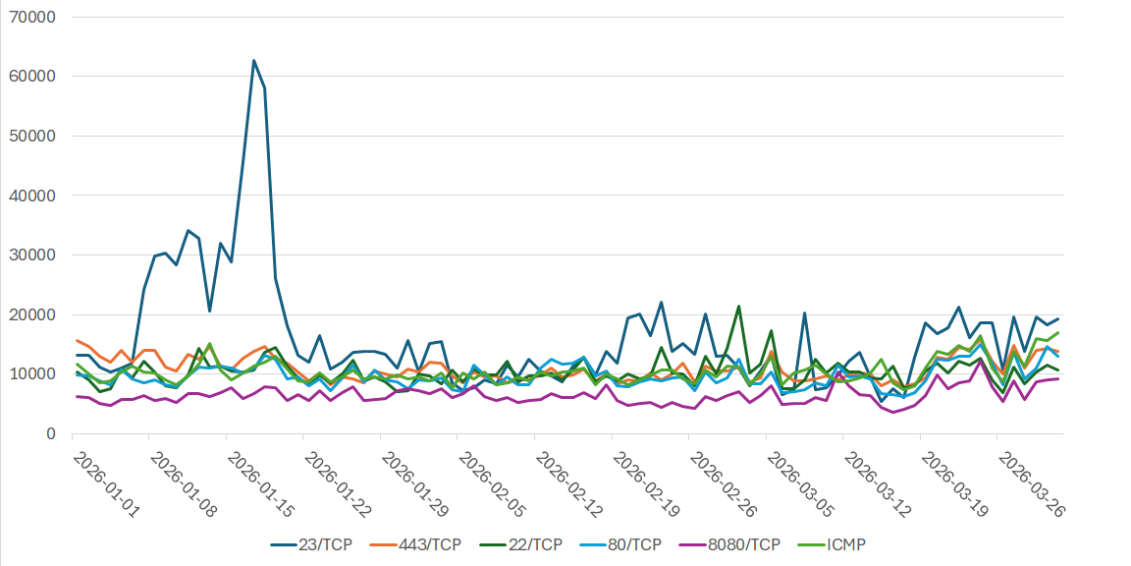

図 3.1 TSUBAME で観測された宛先ポートの上位 1 位〜5 位のパケット数（2026 年 1 月 1 日〜2026 年 3 月 31 日）

- JPCERT/CC インターネット定点観測レポート
  https://www.jpcert.or.jp/tsubame/report/
- TSUBAME レポート Overflow
  https://blogs.jpcert.or.jp/ja/tags/tsubame/

3.1.2 TSUBAME 観測動向

本四半期に日本国内の 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[*1]したものを図に示します。自組織のネットワークに届くパケットの傾向を分析する際に参考にしてください。

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 3.1 と図 3.2 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、2026 年 1 月上旬ごろから 2 週間ほど一時的な増加が見られました。 2 位は 443/TCP でした。3 位は 22/TCP、4 位は 80/TCP で、前四半期の順位と入れ替わりました。5 位には 8080/TCP が入りました。

過去 1 年間（2025 年 4 月 1 日〜2026 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 3.3 と図 3.4 に示します。

[*1] DDoS 攻撃等、特定のセンサーでのみ一時的に観測したパケット等については、上述の趣旨から外れるため集計から除外しています。

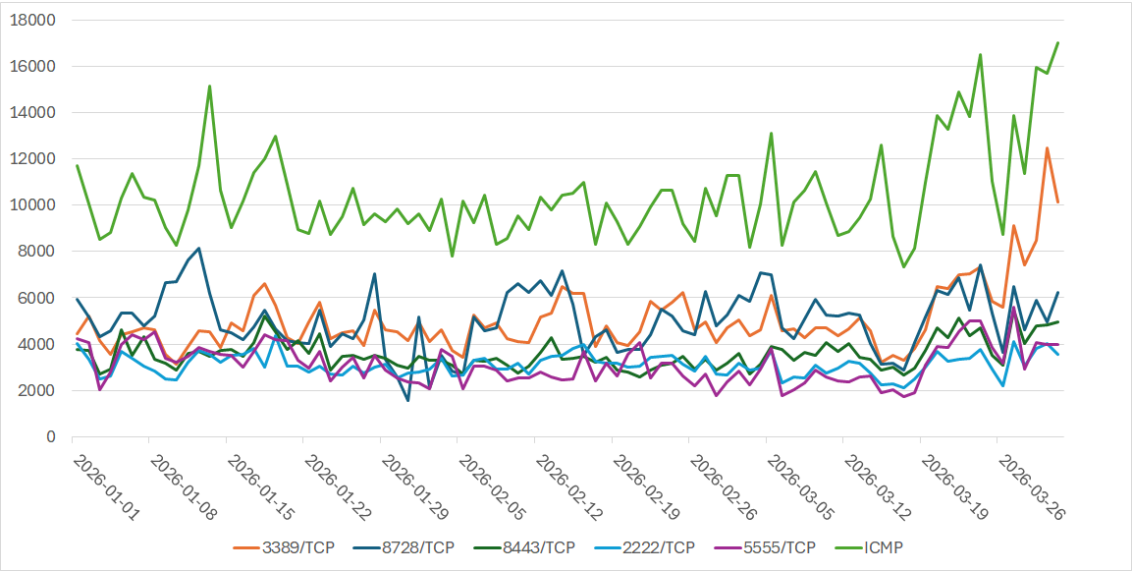

図 3.2 TSUBAME で観測された宛先ポートの上位 6 位〜10 位のパケット数
（2026 年 1 月 1 日〜2026 年 3 月 31 日）

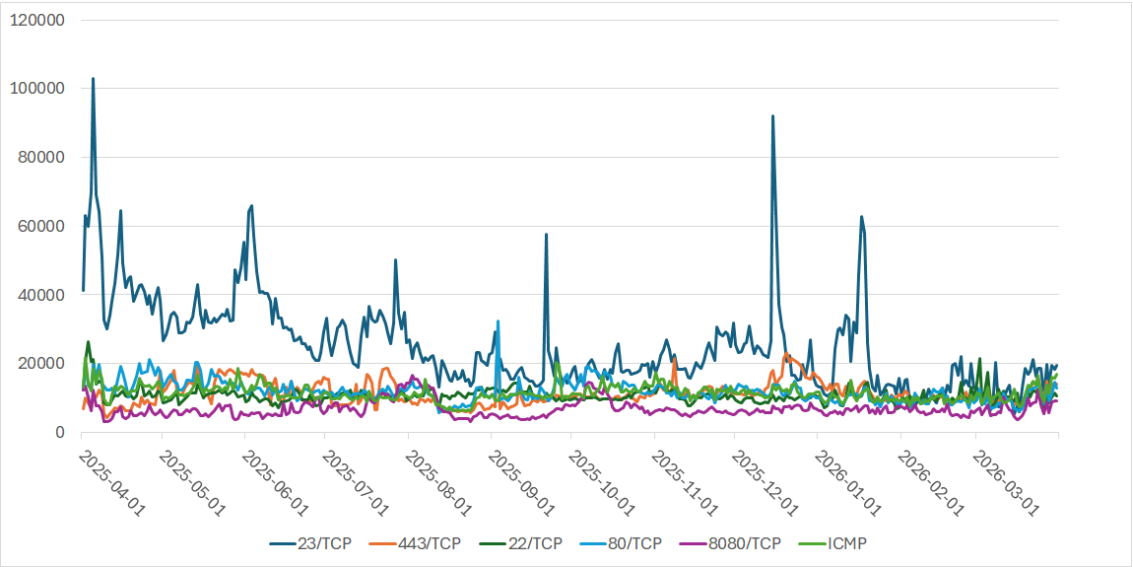

図 3.3 TSUBAME で観測された宛先ポートの上位 1 位〜5 位のパケット数
（2025 年 4 月 1 日〜2026 年 3 月 31 日）

3.2　ハニーポットの運用とその分析

JPCERT/CC では、HTTP や HTTPS などのサービスに対する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、「TSUBAME」の観測結果とあわせて、攻撃活動を分析しています。

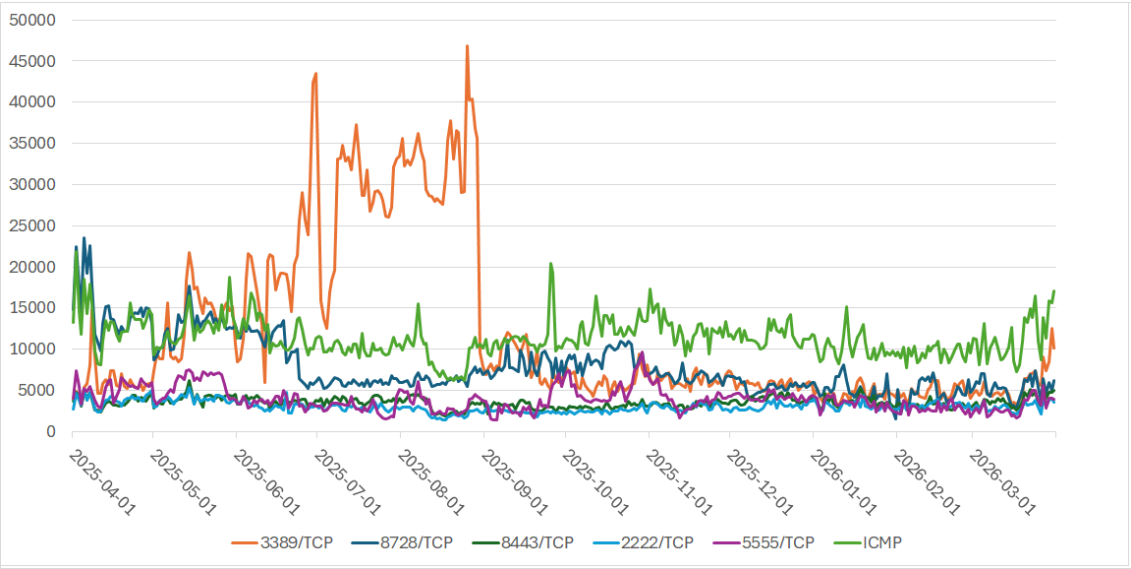

図 3.4 TSUBAME で観測された宛先ポートの上位 6 位〜10 位のパケット数
（2025 年 4 月 1 日〜2026 年 3 月 31 日）

3.2.1 React Server Components の脆弱性（CVE-2025-55182）を狙った攻撃活動の観測

2025 年 12 月 3 日に公表された React Server Components の脆弱性（CVE-2025-55182）を標的とした攻撃パケットが、公表直後から継続的に観測されています（図 3.5）。

当初観測された通信のペイロードに含まれる攻撃コードは、wget コマンドによるマルウェアのダウンロードを目的とした比較的単純なものでした。しかし、2026 年 1 月中旬ごろからは、他のプロセスを停止させるコードや永続化処理を含む、より複雑な攻撃コードが見られるようになっています。本脆弱性を悪用した攻撃活動は今後も継続する可能性が高く、引き続き注意が必要です。

なお、2026 年 2 月 16 日から 2026 年 3 月 19 日にかけて観測されたパケット数の急激な増加については、特定の送信元から既存の PoC コードを利用した大量のスキャンパケットが送信されたことが原因であり、実質的な攻撃活動の増加を示すものではないと分析しています。

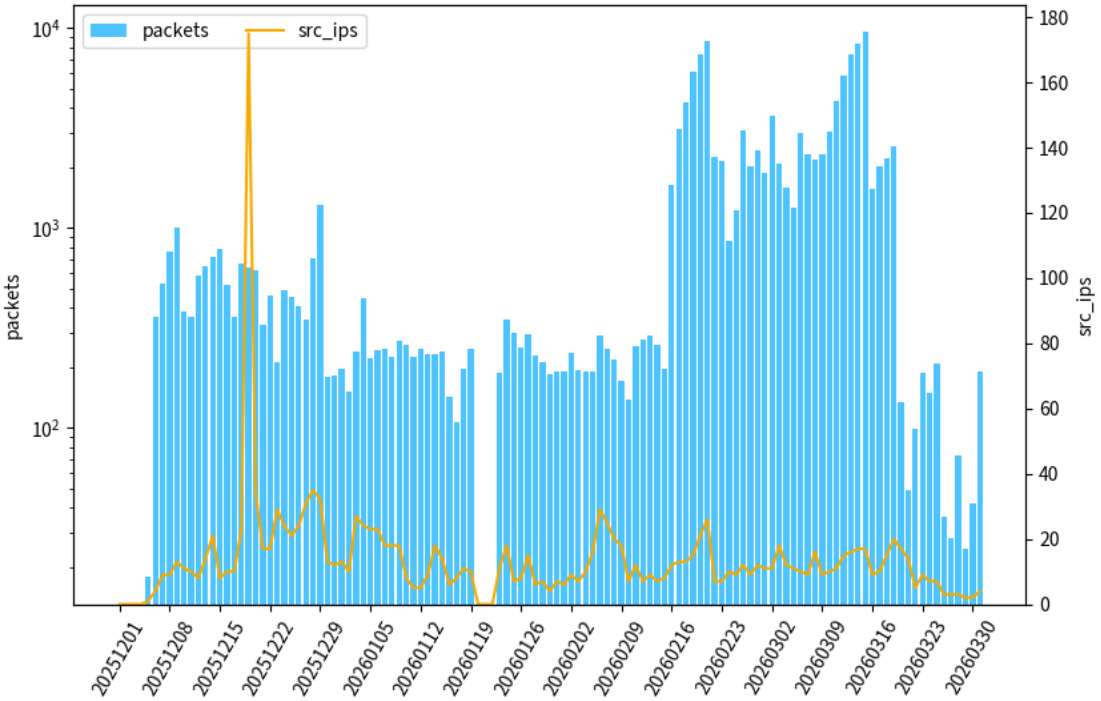

図 3.5 CVE-2025-55182 を狙った攻撃活動の観測数（2025 年 12 月 1 日〜2026 年 3 月 31 日）

第 4 章

脆弱性関連情報の調整と流通

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、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。

4.1 脆弱性関連情報の取り扱い状況

4.1.1 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、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 に参加しています。CVE Program は、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って進められてきた国際的な活動です。米国の MITRE が事務局を務めています。 JPCERT/CC は、CVE Program 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）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、この規程の細目を定めた「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」）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。

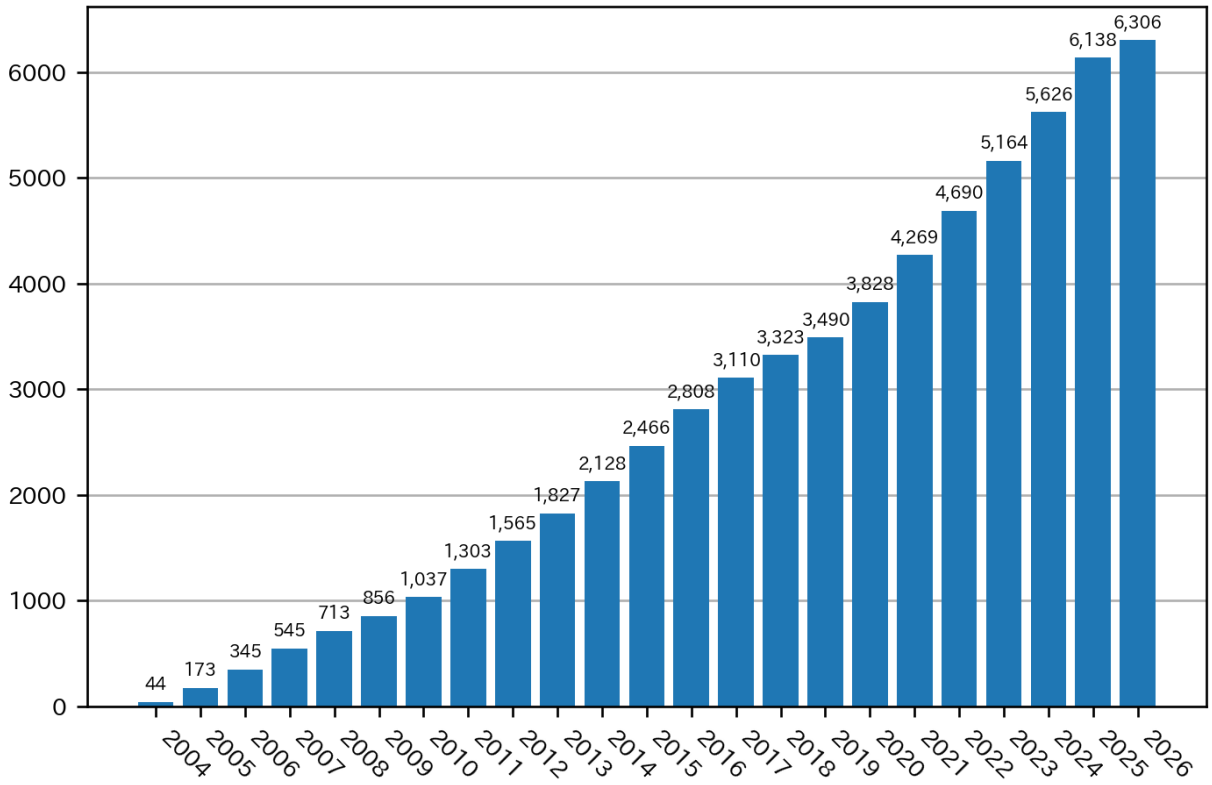

図 4.1 JVN 公表累積件数

4.1.2 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 168 件、累積 6,306 件で、累積の推移は図 4.1 のとおりです。

本四半期に公表された個々の脆弱性情報については、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：47 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：119 件
- 脆弱性情報に関連する技術情報等に関するもの：2 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。

- 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

4.1.2.1 特筆すべき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

本四半期に公表に至った脆弱性のうち、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について、特筆すべきものを紹介します。

- JVN#84622767
  FileZen における OS コマンドインジェクションの脆弱性
  https://jvn.jp/jp/JVN84622767/

ソリトンシステムズが提供するファイル受け渡し専用アプライアンス「FileZen」の脆弱性です。本製品は、公的機関や重要インフラなどを含む、国内の組織で利用されています。この脆弱性は製品開発者から自社製品の脆弱性を発見したとして報告されました。脆弱性の内容は、攻撃者によって細工した HTTP リクエストを送信された場合、製品が稼働する OS 上で任意のコマンドが実行される可能性があるというものです。脆弱性を悪用された場合、機密性・完全性・可用性すべてに深刻な影響が及ぶ恐れがあることから、利用者の混乱のみならずより大きな被害につながる可能性は否定できません。なお、製品開発者との調整の過程で、製品利用者の環境ですでにこの脆弱性が悪用されていたことが判明しました。そのため、JVN アドバイザリ公表に際しては、表題に「緊急」と表示し、悪用が確認されたことを詳細情報に記載して、利用組織に迅速な対応を促しました。また、本アドバイザリ公表後、本件に関する警戒情報として注意喚起を公開し、利用者にさらなる注意を呼び掛けました。本件に関する詳細については 2.1.6 をご参照ください。

4.1.2.2 特筆すべき国際調整または独自調整で取り扱った脆弱性

- JVNVU#95177764
  PRIMERGY が搭載する「iRMC S5/S6」における不適切な権限設定の脆弱性
  https://jvn.jp/vu/JVNVU95177764/

エフサステクノロジーズが提供するサーバー製品 PRIMERGY（プライマジー）に搭載されたリモート管理モジュール「iRMC S5/S6」の脆弱性です。大多数の脆弱性調整は、脆弱性を発見した研究者や製品開発者自身からの通知を受けて始まります。しかしながら、この脆弱性の場合は、MITRE 発行の「CVE ID：CVE-2025-65002」が日本のベンダーの製品に影響する可能性があることを JPCERT/CC が認識したことが発端となっています。この脆弱性情報について当該製品開発者であるエフサステクノロジーズ

に照会したところ、この時点で、JPCERT/CC との連携窓口である日本側の PSIRT では本脆弱性が公表されていたことを認知していませんでした。その後、製品開発者内部（国内の製品開発部門と本 CVE ID の発行を MITRE に依頼した海外関係会社）での確認を経て、本脆弱性が日本国内で使用されている製品に影響することが判明したため、本アドバイザリを公表しました。本件のように、国内で利用されている製品の脆弱性が、国内の製品開発者が把握していない状態で公開され、国内ユーザー向けに情報が提供できていないケースが時々あります。こうした事態を防ぐため、製品開発者は日本国内だけでなく海外支社、関係会社等と連携して脆弱性開示プロセスを共通化し、公開情報の内容や公開のタイミングを全社的にコントロールする必要があります。JPCERT/CC でも、新規発行される CVE ID を独自に監視して国内の製品開発者と連携することで、JVN でのアドバイザリ公表を通じて製品ユーザーへ必要な情報が届くように努めています。

4.1.3 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ことがあります。このような場合は、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）に沿って対応します。この手順では、公表判定委員会での諮問等を経て公表の可否を判断します。 JPCERT/CC はこの手順に基づき、JVN 上で「連絡不能開発者一覧」「Japan Vulnerability Notes JP（連絡不能）一覧」を公表しています。本四半期においては、いずれも新規公表は 0 件です。

- 連絡不能開発者一覧：該当する製品開発者名の連絡先情報を広く求めるための一覧
  https://jvn.jp/reply/
- Japan Vulnerability Notes JP（連絡不能）一覧：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周知するための一覧
  https://jvn.jp/adj/

4.1.4 CNA および Root としての活動

JPCERT/CC では、CVE Program の活動に参加し、CNA として CVE ID の採番や、Root として国内の製品開発者をスコープとする活動をしています。

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、63 件の脆弱性に CVE ID を付与しました。

CNA および CVE については、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
- Overview About the CVE Program
  https://www.cve.org/About/Overview

4.2 日本国内の脆弱性情報流通体制の整備

JPCERT/CC では、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

4.2.1 日本国内製品開発者との連携

JPCERT/CC は調整機関として脆弱性情報の提供先となる製品開発者のリストを整備しています。製品開発者に登録をお願いしており、本四半期末時点での登録数は図 4.2 に示すとおり 1,348 です。

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

4.2.2 製品開発者との定期ミーティング等の実施

本四半期は、2026 年 3 月 13 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。会場とオンライン配信のハイブリッド形式で、参加者はあわせて 90 名を超えました。内容は、脆弱性報告の受理・不受理に関する PSIRT 向けガイド、製品開発者による PSIRT 活動事例、制御システムセキュリティ担当者コミュニティーにおける脆弱性対応の取り組み、CISA ICS アドバイザリに関する JVN での掲載スタイル変更と多岐にわたり、意見交換を行いました。

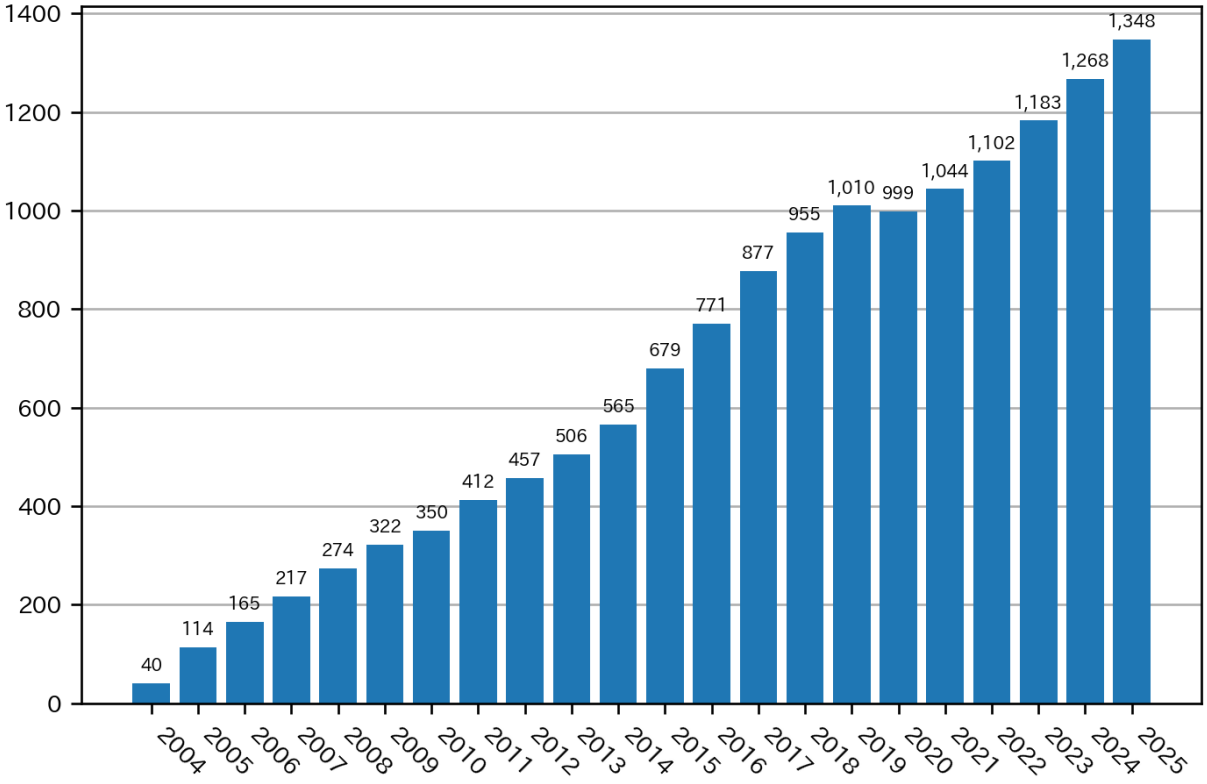

図 4.2 製品開発者登録数

第 5 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の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、平時からこれらの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。

5.1 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実施しました。

5.1.1 交通 ISAC

2026 年 1 月 19 日に開催された第 3 回交通 ISAC カンファレンスに参加し、「サイバー脅威への取り組みと情報共有」というタイトルで講演を行いました。

5.1.2 日本貿易会 ISAC

2026 年 2 月 20 日に開催された合同部会に参加し、「サプライチェーン全体のサイバーセキュリティ向上に向けた取り組みと法的課題」というタイトルで講演を行いました。

5.1.3 SICE/JEITA/JEMIMA セキュリティ調査研究合同ワーキンググループ

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、制御システムセキュリティに関して専門家の方々と意見を交換しました。

5.1.4 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、国家サイバー統括室（NCO）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。本四半期は、2026 年 3 月 9 日に開催された第 83 回セプターカウンシル運営委員会で、Cisco Catalyst SD-WAN Controller/Manager の脆弱性を悪用する攻撃活動の状況について情報を共有しました。

5.2 国内関係機関との連携強化および情報交換の環境整備

5.2.1 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。対面での会合を開催するなどして組織間の交流を促すとともに、登録組織の方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、本四半期は、新たに 4 組織が CISTA の利用組織として登録されました。

5.2.2 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運営しています。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 と登録組織の実務者とが協働し、実践的な検討を行っています。

なお、本四半期末時点で 37 組織が登録されています。

5.3 情報・ツール等の提供

5.3.1 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 6 章

国際連携活動

JPCERT/CC が対応するインシデントの多くが、諸外国の CSIRT や ISP、政府機関との情報共有や協力を必要とします。そのため、JPCERT/CC では、インシデントが発生する前から各国における信頼できるカウンターパートを特定し、いざというときに相互に協力するための信頼関係を築いています。本章では、そのような国際連携活動について、特筆すべき成果を記します。

6.1 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。

6.2 国際 CSIRT 間連携

APCERT や FIRST 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。

6.2.1 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 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/

6.2.1.1 APCERT Steering Committee 会議の実施

APCERT の Steering Committee は 2026 年 2 月 5 日に電話会議を行い、APCERT の運営方針等について議論しました。 JPCERT/CC は Steering Committee メンバーとして会議に参加すると同時に、事務局として会議運営をサポートしました。

6.2.2 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おり、 2021 年 6 月からは国際部の内田が理事を務めています。本四半期は、毎月のオンライン理事会に加え、2026 年 1 月にドミニカ共和国で開催された対面での理事会にも参加しました。

FIRST 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

6.3 海外 CSIRT 等の来訪および訪問

JPCERT/CC は海外 CSIRT への訪問や、海外 CSIRT から JPCERT/CC への来訪を通じて、活動の状況をヒアリングするとともに今後の協力について意見交換を行っています。本四半期は、次の組織を訪問しました。（図 6.1、 図 6.2 を参照）

- CERT-EU への訪問（2026 年 1 月 29 日）
- アゼルバイジャン CERT.AZ への訪問（2026 年 3 月 2 日）
- アゼルバイジャン CERT.GOV.AZ への訪問（2026 年 3 月 3 日）

6.4 その他国際会議への参加

6.4.1 Tallinn Cyber Diplomacy Winter School 2026 でのパネル登壇

JPCERT/CC は、2026 年 3 月 2 日にタイのバンコクで開催された Tallinn Cyber Diplomacy Winter School 2026 に参加しました。この会議は、サイバー外交や国際連携の協力・推進を目的とし、主に各国の外交官や政策担当者などが参加して毎年開催されているものです。サイバー脅威に関するパネルセッションに登壇し、最新の攻撃事例やインシデント対応における CERT の役割、CERT 間の国際連携などについて発言しました。

- Tallinn Cyber Diplomacy Winter School 2026
  https://cyberdiplomacy.ee/wp-content/uploads/2026/03/winter-school-2026-agenda.pdf

図 6.1 CERT.AZ 訪問時の写真

図 6.2 CERT.GOV.AZ 訪問時の写真

6.5　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訂に、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、2026 年 3 月にドイツのニュルンベルクで WG3 に関連する会議が開催されました。改訂作業中の ISO/IEC 29147（脆弱性情報公開）ならびに 30111（脆弱性取り扱い手順）両標準についての作業原案（Working Draft）に関し、脆弱性の定義や他文書との整合性に加えて、脆弱性対応における要求事項と推奨事項の判断等が大きな論点になりました。JPCERT/CC はメインエディターとして参加し、各国のエキスパートからのコメントの取り扱いについて議論しました。その結果、Working Draft を改版し、6 月までに第 2 版を作成することが決定しました。今回の大きな論点としては、脆弱性の定義や他

文書との整合性に加えて、脆弱性対応における要求事項と推奨事項の判断等がありました。

第 7 章

フィッシング対策協議会活動

フィッシング対策協議会（本章において、以下「協議会」）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って、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、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。

協議会では、経済産業省から委託された活動のほかに、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についても支援しています。具体的には「 7.2 フィッシング対策協議会の会員組織向け活動」に記載した活動が該当します。

本章では本四半期におけるこれら活動について記載します。

7.1 フィッシング対策協議会事務局の運営

7.1.1 フィッシングに関する報告・問い合わせの受け付け

本四半期分の件数はまだ確定していないものの、フィッシングの報告件数は大幅に減少しています。例年、旧正月の時期には cn ドメインを発信源とするフィッシングメールの報告が減少する傾向が確認されていますが、本四半期は例年を上回る減少幅となりました。この要因の一つとして、1 月末ごろに Google が実施した世界最大規模のレジデンシャルプロキシ[*1]ネットワークの無力化[*2]が影響している可能性があります。

過去 1 年間のフィッシング報告件数の推移を図 7.1 に示します。

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 16.2% を占めまし

[*1] 家庭の回線に接続されたスマートフォン、PC、IoT 機器などを中継点として住宅用 IP アドレス経由で通信を行うプロキシ。一般ユーザーの通信に見えるため検知されにくく、不正アクセスや詐欺など犯罪者に悪用されることがある。

[*2] 「No Place Like Home Network: Disrupting the World's Largest Residential Proxy Network」 https://cloud.google.com/blog/topics/threat-intelligence/disrupting-largest-residential-proxy-network?hl=en

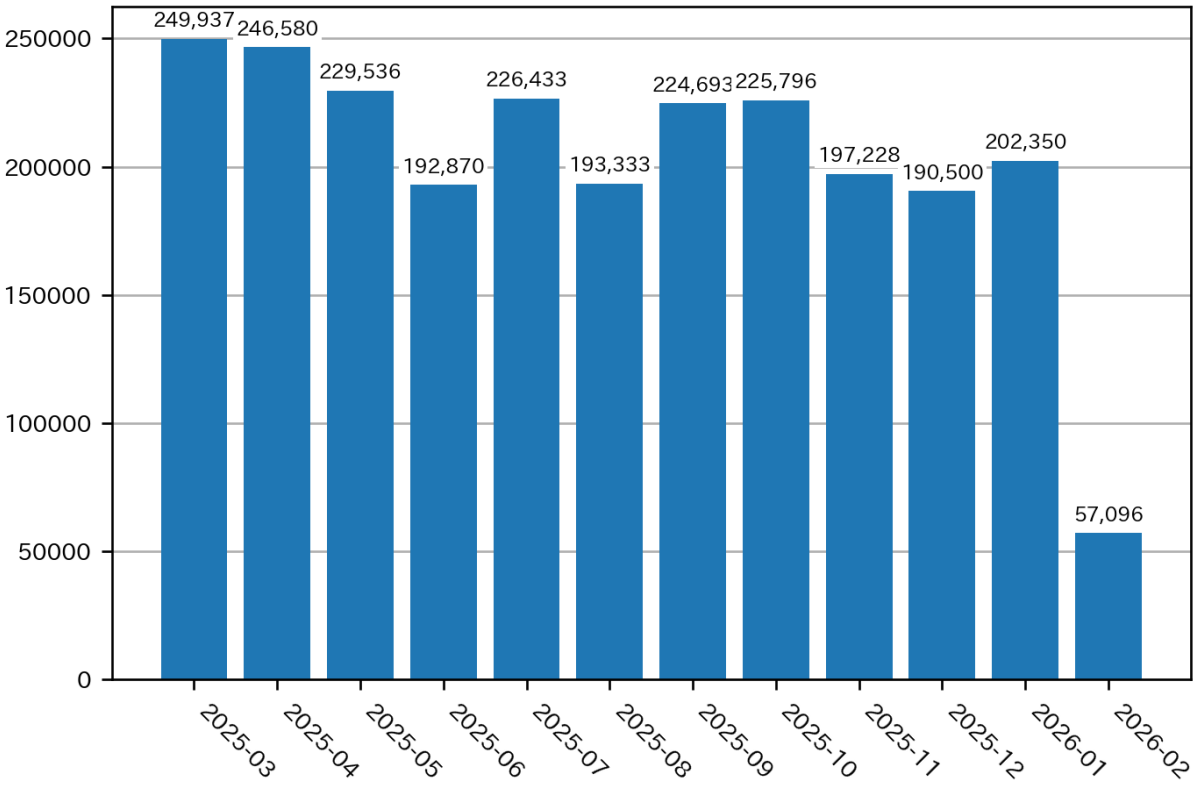

図 7.1 フィッシング報告件数

た。次いで、マネックス証券をかたるフィッシングの報告が多く、全体の約 7.9% を占めました。

7.1.2 情報収集／配信

7.1.2.1 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 サイトで公開しました。

- フィッシング対策協議会 Web サイト
  https://www.antiphishing.jp/
- 2025/12 フィッシング報告状況
  https://www.antiphishing.jp/report/monthly/202512.html
- 2026/01 フィッシング報告状況
  https://www.antiphishing.jp/report/monthly/202601.html
- 2026/02 フィッシング報告状況
  https://www.antiphishing.jp/report/monthly/202602.html

7.1.2.2 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 51 組織に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。

7.2 フィッシング対策協議会の会員組織向け活動

運営委員会の決定に基づいて行っている会員組織向けの独自の活動について、JPCERT/CC は事務局として次の活動を支援しました。

7.2.1 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 135 回運営委員会（オンライン）
  日時：2026 年 2 月 26 日 16:00〜18:00
- 第 136 回運営委員会（JPCERT/CC 会議室＋オンライン）
  日時：2026 年 3 月 26 日 16:00〜18:00

7.2.2 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：2026 年 1 月〜2026 年 3 月 毎週火曜日 9:00〜9:30（オンライン）
- 技術・制度検討ワーキンググループ会合
  日時：2026 年 1 月 29 日 16:00〜18:00（JPCERT/CC 会議室＋オンライン）
  同 成果報告会
  日時：2026 年 2 月 25 日 17:00〜19:00 成果報告会（TKP 秋葉原カンファレンスセンター カンファレンスルーム 2A ＋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：2026 年 2 月 16 日 16:00〜17:30 （オンライン）
- 偽サイト対応自動化タスクフォース会合
  日時：2026 年 1 月 30 日 11:00〜11:30 （オンライン）
  日時：2026 年 2 月 20 日 11:30〜12:00 （オンライン）
  日時：2026 年 3 月 17 日 10:30〜11:00 （オンライン）

- 第 12 回フィッシング対策勉強会
  日時：2026 年 1 月 28 日 17:00〜20:00（日本サイバー犯罪対策センター会議室）

第 8 章

広報活動

JPCERT/CC では事業成果について幅広く広報を行い、成果の普及と周知に努めています。情報の配信は、JPCERT/CC Web サイトや X（旧 Twitter）のほか、Web 媒体、放送媒体、出版媒体などの各種媒体を通じて実施しています。また、セミナーやイベントでの登壇などによる情報発信も行っています。

8.1 講演

本四半期は次のセミナーやイベント等で講演しました。

- サイバーテックトーク
  タイトル：繰り返されるエッジデバイス侵害の構造
  講演者：塚田 裕介（早期警戒グループ 脅威情報アナリスト）
  主催：ＳＯＭＰＯホールディングス
  講演日：2026 年 1 月 19 日
- ISAJ 技術フォーラム - OT サイバーセキュリティとプラント AI 応用
  タイトル：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〜
  講演者：宮地 利雄（技術顧問）
  主催：ISA 日本支部
  講演日：2026 年 2 月 19 日
- 令和 7 年度ボイラー・タービン主任技術者会議
  タイトル：電力業界におけるサイバー攻撃の脅威と JPCERT/CC の取り組み
  講演者：藤堂 伸勝（早期警戒グループ 脅威情報アナリスト）
  主催：経済産業省 中国四国産業保安監督部
  講演日：2026 年 2 月 27 日
- 【JPCERT/CC 講演】組み込み・制御システムのためのセキュア開発入門
  タイトル：組み込み・制御システムにおけるセキュア開発の基本
  講演者：木下 広海（早期警戒グループ 脆弱性アナリスト）
  主催：テクマトリックス
  講演日：2026 年 3 月 10 日

- セキュリティ・キャンプ 2026 コネクト
  タイトル：サイバー空間の脅威を知る
  講演者：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）
  主催：情報処理推進機構
  講演日：2026 年 3 月 27 日

8.2 執筆

本四半期は次の刊行物や Web サイト等に寄稿しました。

- インターネット白書 2026
  タイトル：2025 年の情報セキュリティ動向
  執筆者：白石 龍亮（早期警戒グループ 脅威アナリスト）
  発行：インプレス
  発行日：2026 年 2 月 27 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。

- 保守切れルータの取り換え促進キャンペーン
  主催：内閣官房内閣サイバーセキュリティセンター
  開催日：2026 年 2 月 1 日〜2026 年 3 月 18 日
- Security Days Spring 2026
  主催：ナノオプト・メディア
  開催日：2026 年 3 月 10 日〜2026 年 3 月 27 日
- Security Management Conference 2026 春
  主催：SB クリエイティブ
  開催日：2026 年 3 月 11 日〜2026 年 3 月 12 日
- Data Center Japan 2026
  主催：ナノオプト・メディア
  開催日：2026 年 3 月 24 日〜2026 年 3 月 25 日

8.4 公開資料

本四半期は次の資料を公開しました。

8.4.1 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。

- 2026-03-09
  JPCERT/CC インターネット定点観測レポート［2025 年 7 月 1 日～2025 年 9 月 30 日］
  https://www.jpcert.or.jp/tsubame/report/report202507-09.html
- 2026-03-25
  JPCERT/CC Internet Threat Monitoring Report [July 1, 2025 - September 30, 2025]
  https://www.jpcert.or.jp/english/tsubame/report/report202507-09.html
- 2026-03-09
  JPCERT/CC インターネット定点観測レポート［2025 年 10 月 1 日～2025 年 12 月 31 日］
  https://www.jpcert.or.jp/tsubame/report/report202510-12.html
- 2026-03-25
  JPCERT/CC Internet Threat Monitoring Report [October 1, 2025 - December 31, 2025]
  https://www.jpcert.or.jp/english/tsubame/report/report202510-12.html

8.4.2 ソフトウェア等の脆弱性関連情報に関する届出状況

IPA と JPCERT/CC は、それぞれ受付機関および調整機関として、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）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。

- 2026-01-22
  ソフトウェア等の脆弱性関連情報に関する届出状況［2025 年第 4 四半期（10 月～12 月）］
  https://www.jpcert.or.jp/pr/2026/vulnREPORT_2025q4.pdf

8.4.3 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 15 件の記事を公開しました。

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

- 2026-02-10
  Windows のイベントログ分析トレーニング用コンテンツの公開
- 2026-02-13
  React2Shell を悪用する複数の攻撃アクターによる侵害事例
- 2026-02-20
  JSAC2026 開催レポート〜DAY 1〜
- 2026-02-27
  JSAC2026 開催レポート〜DAY 2〜
- 2026-03-06
  JSAC2026 開催レポート〜Workshop ／ Lightning Talk Session ／ Panel Discussion〜
- 2026-03-24
  制御システムセキュリティカンファレンス 2026 開催レポート
- 2026-03-25
  世界の CSIRT から 〜アゼルバイジャン〜
- 2026-03-30
  TSUBAME レポート Overflow（2025 年 7〜9 月）

英語版発行件数：7 件 https://blogs.jpcert.or.jp/en/

- 2026-02-13
  Multiple Threat Actors Rapidly Exploit React2Shell: A Case Study of Active Compromise
- 2026-02-20
  JSAC2026 -Day 1-
- 2026-02-27
  JSAC2026 -Day 2-
- 2026-03-06
  JSAC2026 -Workshop/Lightning Talk Session/Panel Discussion-
- 2026-03-12
  Study of Binaries Created with Rust through Reverse Engineering
- 2026-03-25
  CSIRTs Around the World – Azerbaijan
- 2026-03-30
  TSUBAME Report Overflow (Jul-Sep 2025)

付録 A

インシデントの分類

JPCERT/CC では、寄せられた報告に含まれるインシデントを次の定義に従って分類しています。

フィッシングサイト

フィッシングサイトとは、銀行やオークション等のサービス事業者の正規サイトを装い、利用者の ID やパスワード、クレジットカード番号等の情報をだまし取る「フィッシング詐欺」に使用されるサイトを指します。
JPCERT/CC では、以下を**フィッシングサイト**に分類しています。

- 金融機関やクレジットカード会社等のサイトに似せた Web サイト
- フィッシングサイトに誘導するために設置された Web サイト

Web サイト改ざん

Web サイト改ざんとは、攻撃者もしくはマルウェアによって、Web サイトのコンテンツが書き換えられた（管理者が意図したものではないスクリプトの埋め込みを含む）サイトを指します。
JPCERT/CC では、以下を **Web サイト改ざん**に分類しています。

- 攻撃者やマルウェア等により悪意のあるスクリプトや iframe 等が埋め込まれたサイト
- SQL インジェクション攻撃により情報が改ざんされたサイト

マルウェアサイト

マルウェアサイトとは、閲覧することで PC がマルウェアに感染してしまう攻撃用サイトや、攻撃に使用するマルウェアを公開しているサイトを指します。
JPCERT/CC では、以下を**マルウェアサイト**に分類しています。

- 閲覧者の PC をマルウェアに感染させようとするサイト
- 攻撃者によりマルウェアが公開されているサイト

スキャン

スキャンとは、サーバーや PC 等の攻撃対象となるシステムの存在確認やシステムに不正に侵入するための弱点（セキュリティホール等）探索を行うために、攻撃者によって行われるアクセス（システムへの影響がないもの）を指します。また、マルウェア等による感染活動も含まれます。
JPCERT/CC では、以下を**スキャン**と分類しています。

- 弱点探索（プログラムのバージョンやサービスの稼働状況の確認等）
- 侵入行為の試み（未遂に終わったもの）
- マルウェア（ウイルス、ボット、ワーム等）による感染の試み（未遂に終わったもの）
- ssh、ftp、telnet 等に対するブルートフォース攻撃（未遂に終わったもの）

DoS/DDoS

DoS/DDoS とは、ネットワーク上に配置されたサーバーや PC、ネットワークを構成する機器や回線等のネットワークリソースに対して、サービスを提供できないようにする攻撃を指します。
JPCERT/CC では、以下を **DoS/DDoS** と分類しています。

- 大量の通信等により、ネットワークリソースを枯渇させる攻撃
- 大量のアクセスによるサーバープログラムの応答の低下、もしくは停止
- 大量のメール（エラーメール、SPAM メール等）を受信させることによるサービス妨害

制御システム関連インシデント

制御システム関連インシデントとは、制御システムや各種プラントが関連するインシデントを指します。
JPCERT/CC では、以下を**制御システム関連インシデント**と分類しています。

- インターネット経由で攻撃が可能な制御システム
- 制御システムを対象としたマルウェアが通信を行うサーバー
- 制御システムに動作異常等を発生させる攻撃

標的型攻撃

標的型攻撃とは、特定の組織、企業、業種などを標的として、マルウェア感染や情報の窃取などを試みる攻撃を指します。
JPCERT/CC では、以下を**標的型攻撃**と分類しています。

- 特定の組織に送付された、マルウェアが添付されたなりすましメール
- 閲覧する組織が限定的である Web サイトの改ざん
- 閲覧する組織が限定的である Web サイトになりすまし、マルウェアに感染させようとするサイト
- 特定の組織を標的としたマルウェアが通信を行うサーバー

その他

その他とは、上記以外のインシデントを指します。
JPCERT/CC が**その他**に分類しているものの例を次に掲げます。

- 脆弱性等を突いたシステムへの不正侵入
- ssh、ftp、telnet 等に対するブルートフォース攻撃の成功による不正侵入
- キーロガー機能を持つマルウェアによる情報の窃取
- マルウェア（ウイルス、ボット、ワーム等）の感染

最新情報については JPCERT/CC の Web サイトをご参照ください。

- 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 四半期レポート ［ 2026 年 1 月 1 日〜2026 年 3 月 31 日 ］

- 発行履歴
  - 2026 年 4 月 16 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/