JPCERT CC®

JPCERT/CC 四半期レポート

2025 年 10 月 1 日～2025 年 12 月 31 日

2026 年 1 月 22 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。

本資料では、 2025 年 10 月 1 日～2025 年 12 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

2025 年度の JPCERT/CC ベストレポーター賞を贈呈

インシデントや脆弱性といったサイバーセキュリティに関する問題をいち早く発見し正確な情報をご提供いただける皆さまは、JPCERT/CC が問題解決に向けて調整業務を的確に進めるための重要な情報源であり協力者です。インシデントや脆弱性の数が増加し、かつ問題が複雑化・高度化している現状においては、ご提供いただいた情報をもとに、より多くの問題を迅速に解決することがますます重要になってきています。このような状況を踏まえ、JPCERT/CC では、皆さまのお力添えに感謝の意をお伝えするとともに、特に優れた活動事例を広く知っていただく機会になればと考え、2021 年度に「ベストレポーター賞」を制定しました。インシデント報告と脆弱性報告の 2 つの部門を設け、インシデントまたは脆弱性情報の報告をいただいた方の中から、その件数や内容に基づき JPCERT/CC の活動に顕著な貢献をされた方に各賞を贈呈しています。

5 回目となる本年度は次の方々にベストレポーター賞をお贈りしました。

社会医療法人財団古宿会　齋藤 直哉 様（インシデント報告部門）

齋藤様は、医療機関や施設の情報システム運用管理者としてサイバーセキュリティ対策やインシデント対応を行う中で発見された、各施設や職員を標的とするフィッシングメールやフィッシングサイトに関する 500 件以上の報告をいただきました。それらの報告は JPCERT/CC によるサイトへの対応、分析、

注意喚起の発出等に生かされました。

GMO Flatt Security 株式会社　RyotaK 様（脆弱性報告部門）

RyotaK 様は、これまで数多くの製品の脆弱性を発見され、製品開発者や調整機関と連携して脆弱性情報の適切な情報流通に多大なご協力をいただき、CVD（Coordinated Vulnerability Disclosure）における報告者の模範となる対応を示されました。

今回の受賞者をはじめ、JPCERT/CC の活動に日々ご協力いただいている多くの方々にあらためて感謝申し上げます。

- JPCERT/CC ベストレポーター賞 2025
  https://www.jpcert.or.jp/award/best-reporter-award/2025.html

クライアントのリアルタイム監視ツール YAMAGoya の公開

JPCERT/CC では、Sigma および YARA ルールを活用して Windows 端末上での不正な挙動をリアルタイムに監視できる、オープンソースのスレットハンティングツール「YAMAGoya」を公開しました。

- GitHub：JPCERTCC/YAMAGoya
  https://github.com/JPCERTCC/YAMAGoya
- JPCERT/CC Eyes：Sigma および YARA ルールを活用したリアルタイムクライアント監視ツール YAMAGoya
  https://blogs.jpcert.or.jp/ja/2025/11/YAMAGoya.html

近年は、ファイルレスマルウェアやマルウェアの難読化等により、ファイル単体のスキャンだけではホスト上での不審なアクティビティの検知が難しくなっています。一方で、セキュリティコミュニティーでは Sigma や YARA などのルールが積極的に作成・公開され、その活用が進んでいるものの、既存のエンドポイント製品では独自の検知エンジンを利用している都合から、これらのルールを直接活用しづらい状況が見られます。 YAMAGoya は、こうした課題に対し、Sigma や YARA などの公開ルールの活用を前提とした監視・検知を支援することを目的としています。

YAMAGoya は、ETW（Event Tracing for Windows）によるイベント監視とメモリスキャンを組み合わせて検知を行うように設計されており、ファイル／プロセス／レジストリ／ネットワーク／ PowerShell ／ WMI 等を監視する機能を備えています。また、GUI および CLI の両方に対応しており、スレットハンティングやインシデント対応時の補助ツールとして活用することが可能です。

Windows 端末上でのスレットハンティングに、ぜひ本ツールをご活用ください。

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、2025 年 10 月 1 日から 2025 年 12 月 31 日まで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表 1.1[*2]に示します。

本四半期に寄せられた報告件数は 20,336 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 2,875 件でした。前四半期と比較して、報告件数は 15% 減少、調整件数は 12% 減少しました。また、前年同期（報告件数は 9,743 件、調整件数は 3,597 件）と比較すると、報告数は 109% 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 インシデント報告関連件数

	10 月	11 月	12 月	合計	前四半期合計
報告件数	6,852	7,039	6,445	20,336	23,857
インシデント件数	4,474	5,011	4,052	13,537	10,379
調整件数	1,011	799	1,065	2,875	3,257

[*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。 1 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。

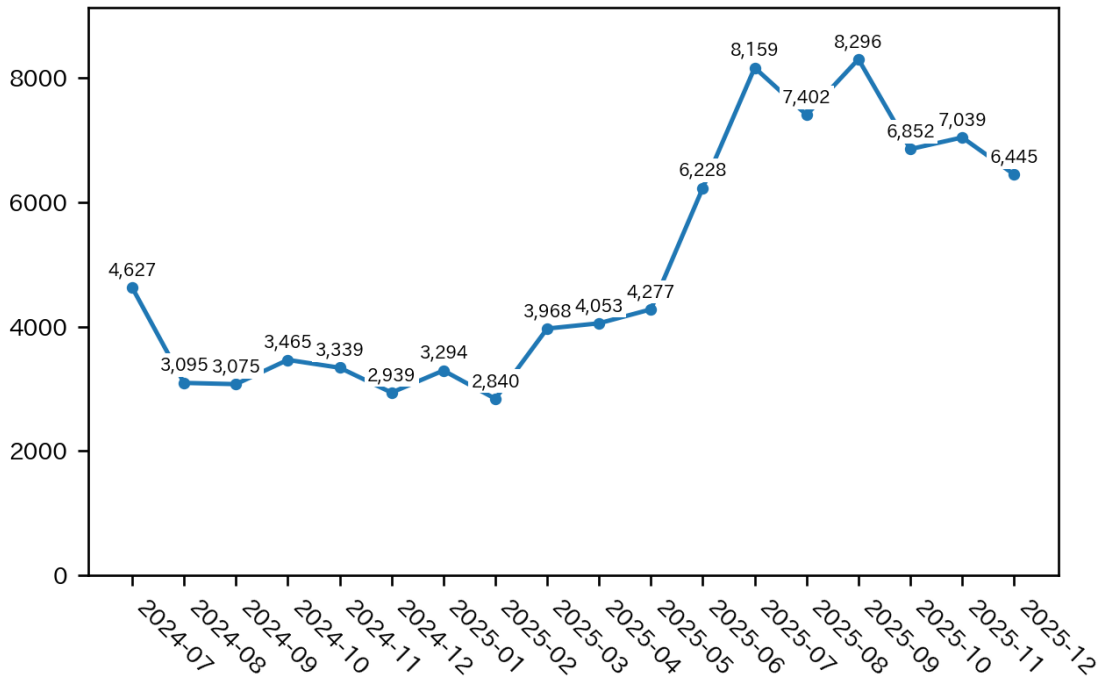

図 1.1 インシデント報告件数の推移

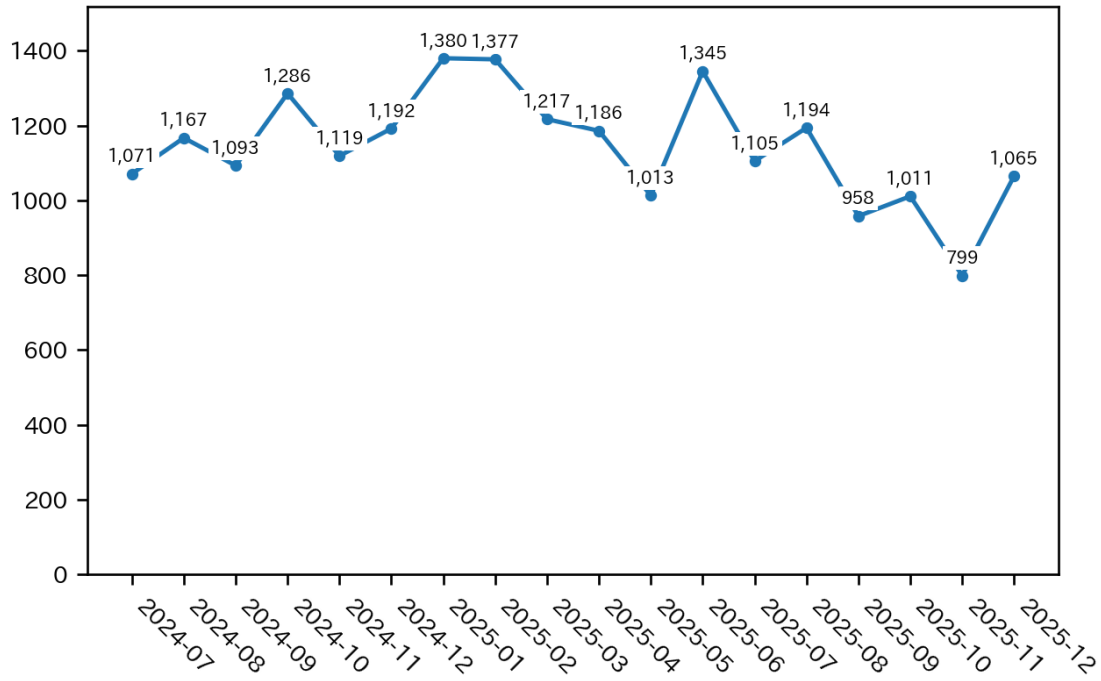

図 1.2 インシデント調整件数の推移

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	10 月	11 月	12 月	合計	前四半期合計
フィッシングサイト	4,073	4,624	3,700	12,397	9,063
Web サイト改ざん	23	65	17	105	319
マルウェアサイト	19	8	17	44	32
スキャン	216	156	97	469	452
DoS/DDoS	2	4	0	6	2
制御システム関連	0	0	0	0	0
標的型攻撃	1	0	2	3	3
その他	140	154	219	513	508

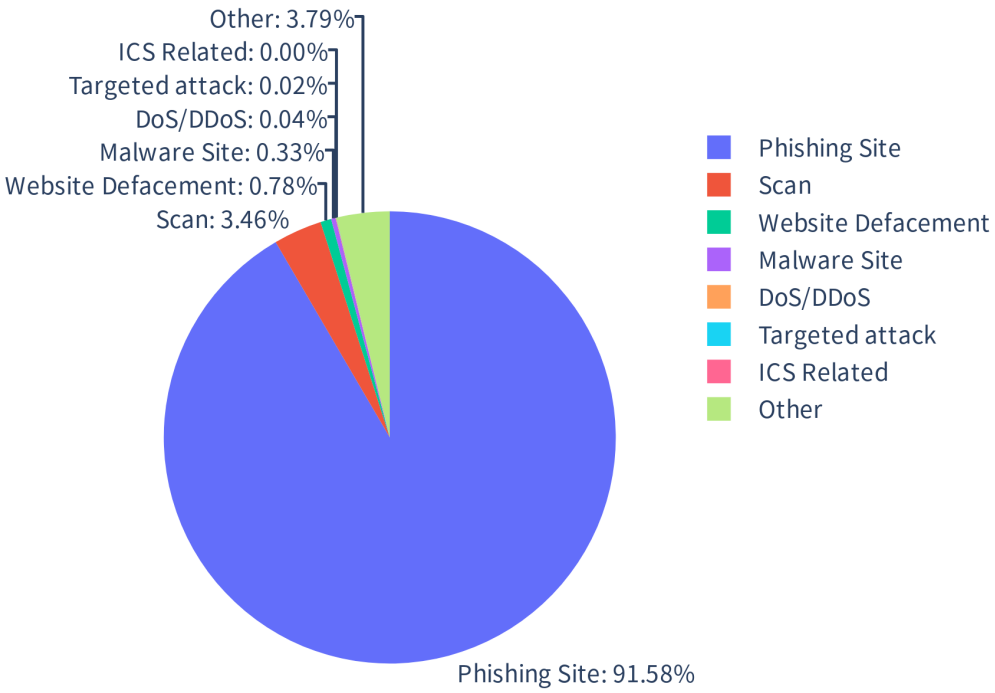

図 1.3 インシデント報告件数のカテゴリー別割合

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 91.58% 、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 3.46% 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。

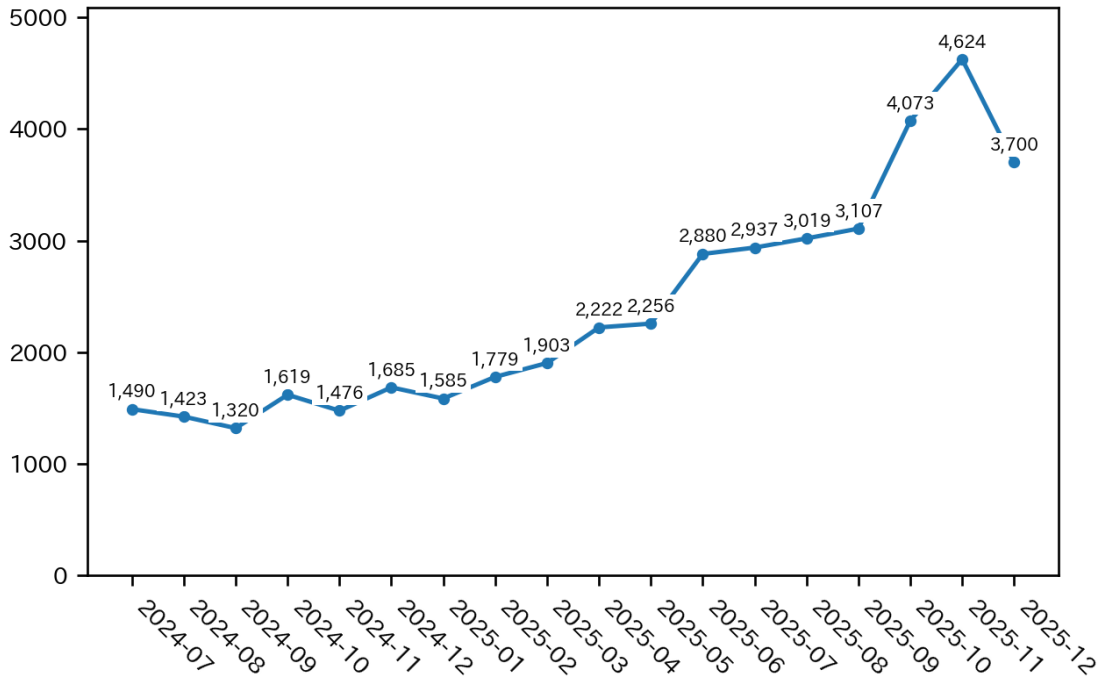

図 1.4 フィッシングサイト件数の推移

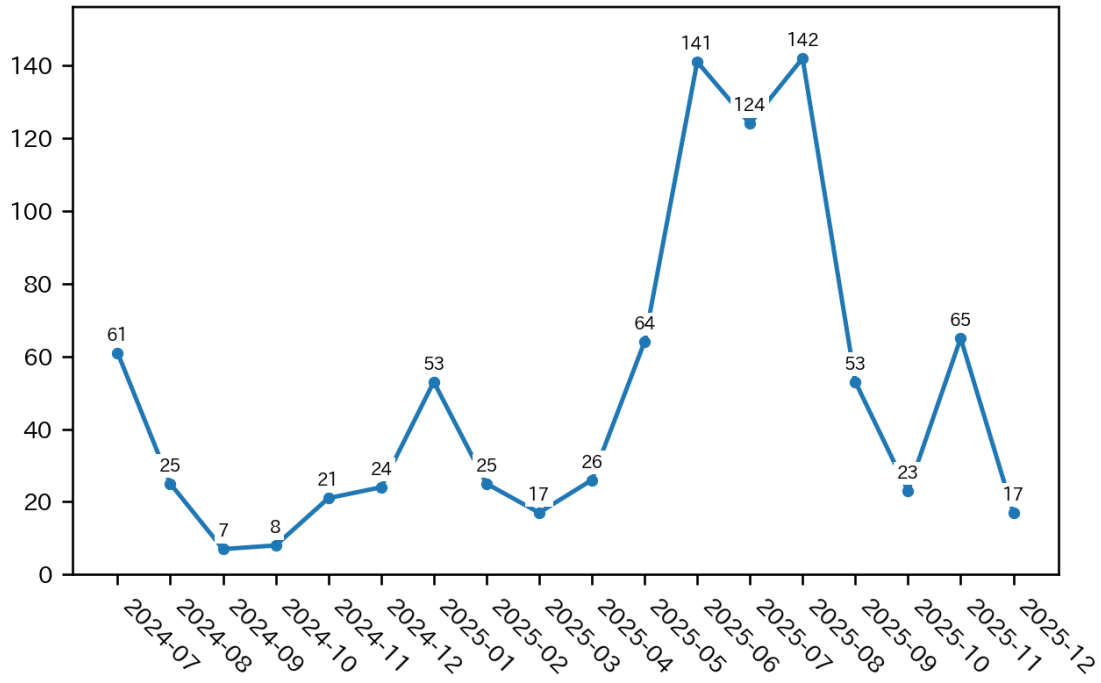

図 1.5 Web サイト改ざん件数の推移

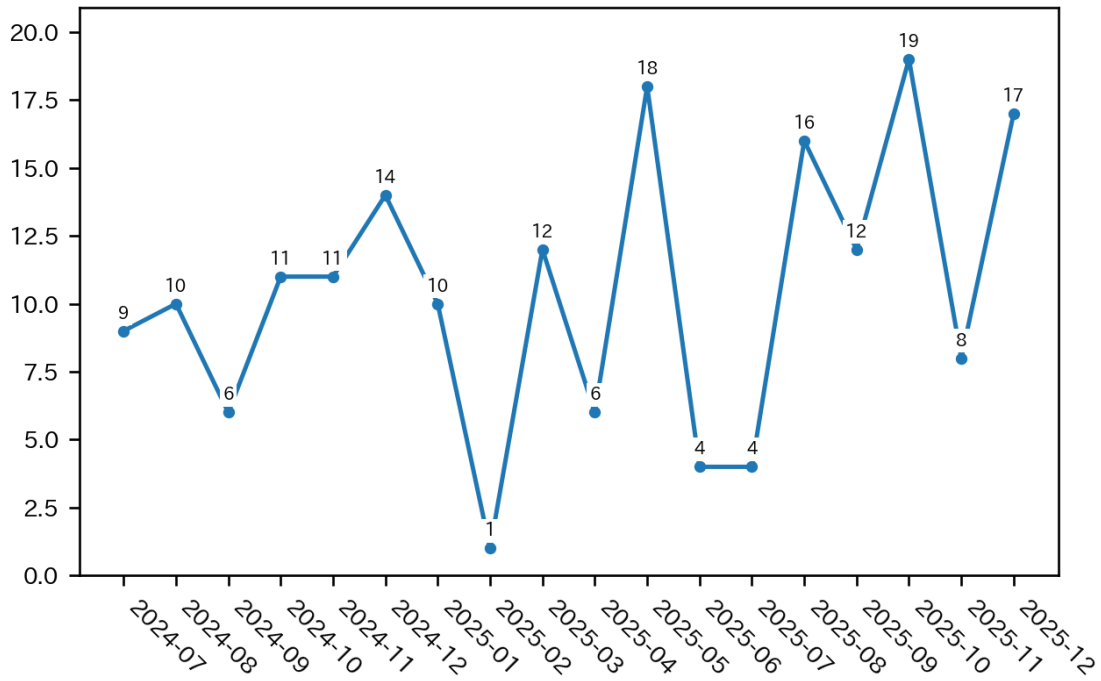

図 1.6 マルウェアサイト件数の推移

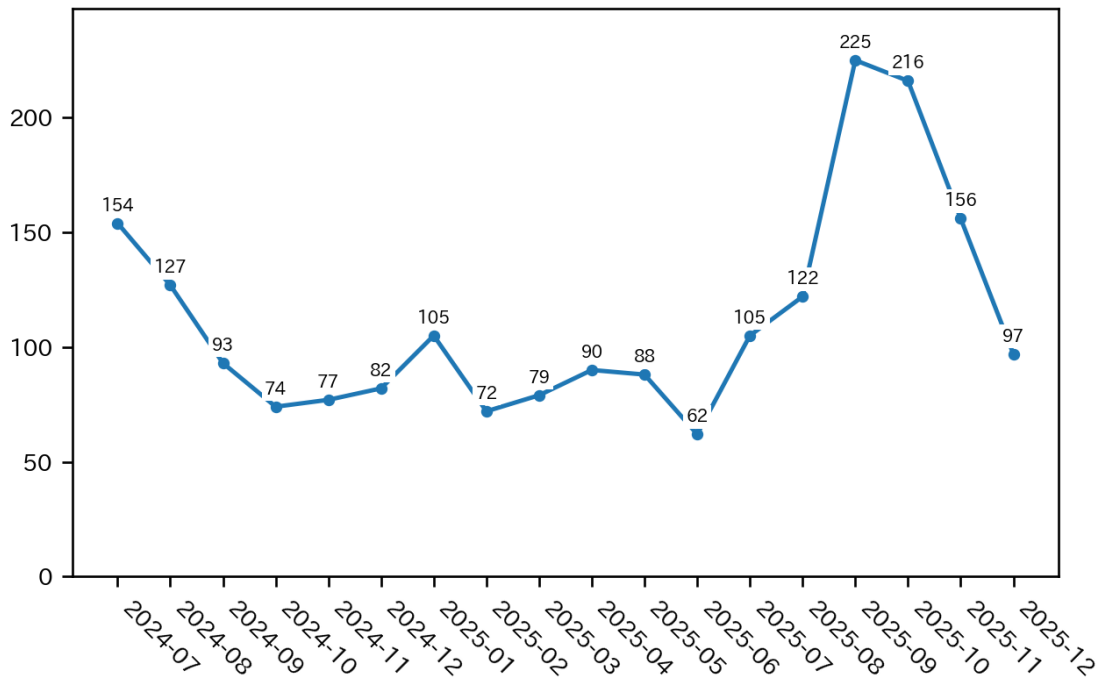

図 1.7 スキャン件数の推移

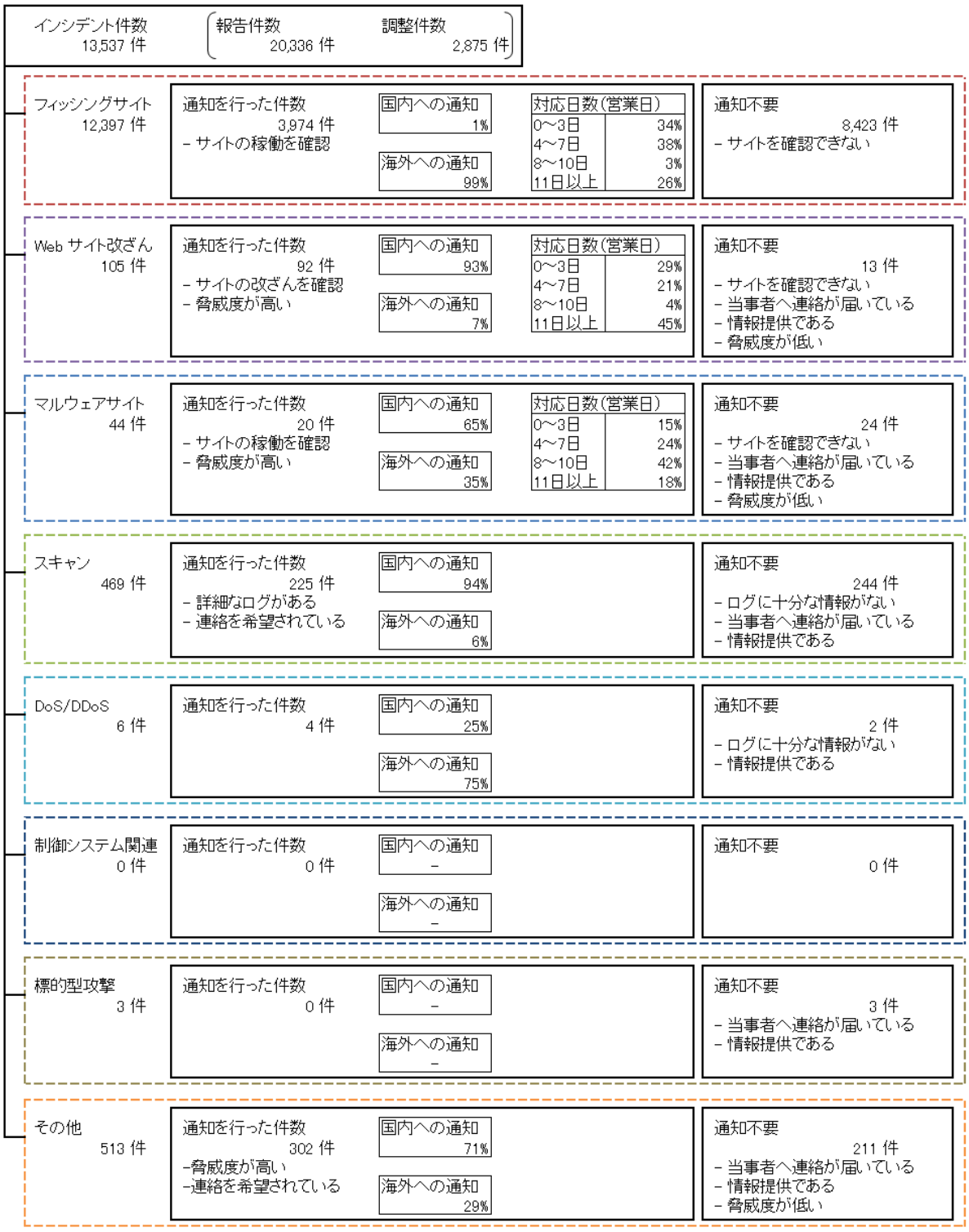

図 1.8 インシデントのカテゴリーごとの件数と調整・対応状況

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	10 月	11 月	12 月	合計	割合
国内ブランド	3,349	4,068	3,115	10,532	85%
国外ブランド	225	144	200	569	5%
ブランド不明	499	412	385	1,296	10%
全ブランド合計	4,073	4,624	3,700	12,397	

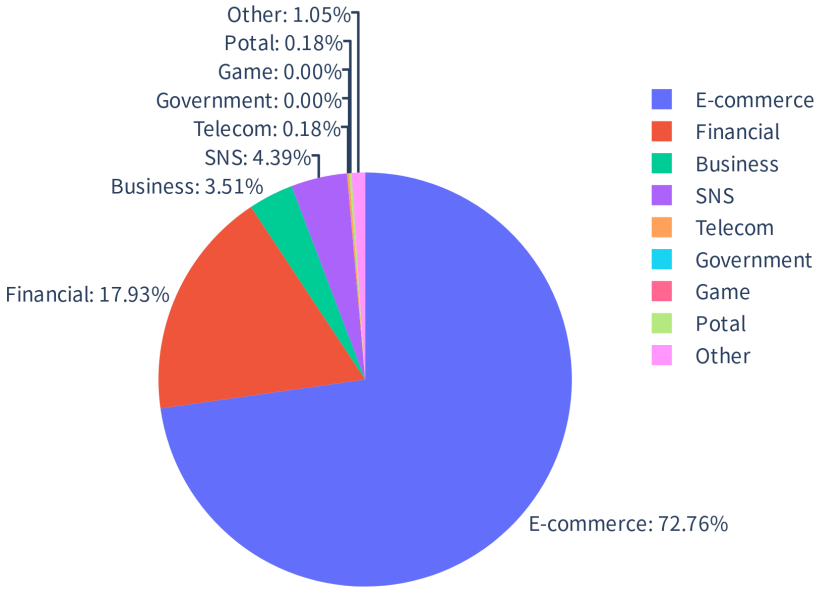

図 1.9 国外ブランドのフィッシングサイトの件数の業界別の割合

1.2 インシデントの傾向

1.2.1 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 12,397 件で、前四半期の 9,063 件から 37% 増加しました。また、前年同期（4,780 件）との比較では、 159% 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 569 件で、前四半期の 292 件から 95% 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 10,532 件で、前四半期の 7,235 件から 46% 増加しました。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 1.9 と図 1.10 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 72.76%、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 78.50% 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。

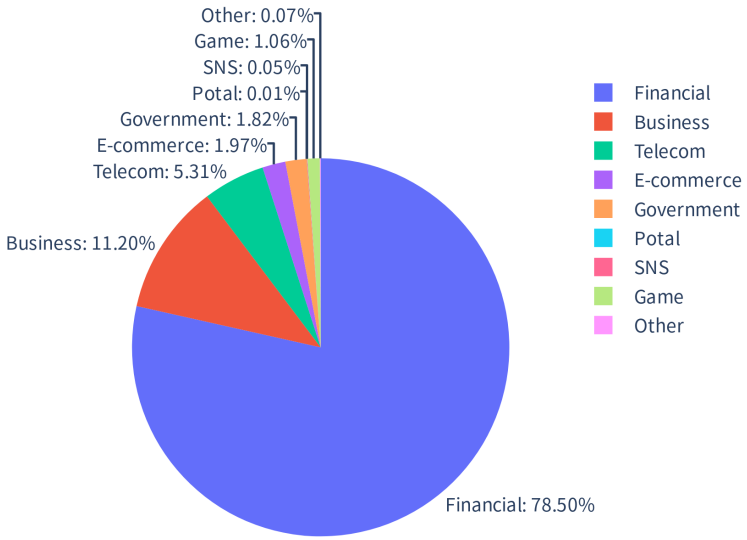

図 1.10 国内ブランドのフィッシングサイトの件数の業界別の割合

国外ブランドでは、Amazon と Apple ID 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 証券など証券会社の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、UC カードなどのクレジットカード会社のものも依然として多く報告されています。その他に本四半期は、PlayStation Store や任天堂のオンラインサービスといったゲーム関連会社の Web サイトを装ったフィッシングサイトの報告も寄せられるようになりました。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 99%、国内が 1% でした。

1.2.2 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 105 件でした。前四半期の 319 件から 67% 減少しています。

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。

- 事例 1：正規 Web サイトに個人情報を窃取するフォームが設置されていた事例（Telegram API の悪用）
- 事例 2：正規 Web サイトに Cloudflare の検証画面を表示するコードが設置されていた事例

事例 1 では、正規 Web サイトにアクセスしたユーザーに偽のログイン画面を表示し、個人情報を入力させるフォーム（図 1.11）が設置されていました。当該フォームには不正な JavaScript が埋め込まれており、入力フォームからフォーカスが外れたタイミング（blur イベント）で入力内容が Telegram の API を通じて攻撃者へ送信される仕組みになっていました。

事例 2 では、正規 Web サイトに Cloudflare の検証画面（Cloudflare Turnstile）に見せかけたチェックボックスを表示する不正なコードが設置されていました。ユーザーがチェックボックスをクリックすると、Windows キー＋ R で「ファイル名を指定して実行」ダイアログを開き、Ctrl ＋ V で貼り付けた後

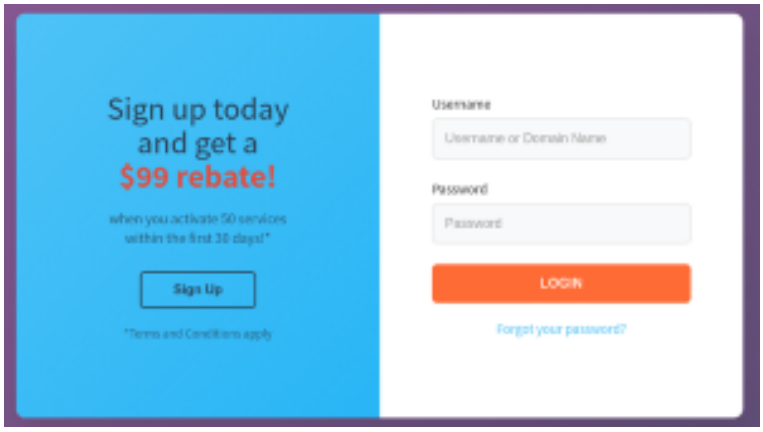

図 1.11 偽のログインフォーム

図 1.12 Cloudflare の検証画面に見せかけたチェックボックス

に Enter を押すよう促すメッセージ（図 1.12）が表示されます。このメッセージに従って操作すると、改ざんされた Web ページ上のスクリプトがあらかじめクリップボードに書き込んでいたコマンドが実行されます。クリップボードにコピーされるコマンドは、msiexec コマンドを実行し、外部から不正なコードのダウンロードおよび実行をするものでした。このように、ユーザーの操作を誘導して不正なコードを実行させようとする手法は、ClickFix と呼ばれています。

1.2.3 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 3 件でした。

1.2.3.1 Microsoft の認証情報を狙った AiTM 攻撃

本四半期は、Microsoft の認証情報を狙っ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 OneDrive を模倣したページが表示され、そのページ上に表示されたファイルをクリックすると偽の Microsoft のログインポップアップが生成されるというものです。そこに入力し

表 1.4 ポート別のスキャン件数の上位 10 位

ポート	10 月	11 月	12 月	合計
23/tcp	79	60	41	180
22/tcp	70	38	20	128
80/tcp	33	29	16	78
25/tcp	16	14	6	36
143/tcp	6	11	2	19
443/tcp	0	11	0	11
21/tcp	5	0	0	5
85/tcp	3	0	0	3
8080/tcp	0	0	3	3
5001/tcp	1	0	1	2

た認証情報は攻撃者のリバースプロキシによって窃取されます。

1.2.4 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 44 件でした。前四半期の 32 件から 38% 増加しています。

本四半期に報告が寄せられたスキャン件数は 469 件でした。前四半期の 452 件から 3% 増加しています。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ポートは、 Telnet（23/TCP)、SSH（22/TCP)、HTTP（80/TCP)、SMTP（25/TCP）でした。

その他に分類されるインシデントの件数は 513 件でした。前四半期の 508 件から 1% 増加しました。

1.3 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。

1.3.1 Operation Endgame で判明した Rhadamanthys に感染している国内組織への通知

JPCERT/CC では、Operation Endgame 3.0 に関連して、国内で Rhadamanthys への感染が疑われるホストに関する情報を外部組織から受領しました。

- Operation Endgame
  https://www.operation-endgame.com/

Operation Endgame は、Europol を中心に複数国の法執行機関が協力して実施している国際的なオペ

レーションです。フェーズ 3 では、Rhadamanthys を含む複数のマルウェアのインフラ差し押さえに成功し、多くの被害組織の特定につながりました。これを受けて JPCERT/CC では、該当ホストを管理する組織に対し、感染ホストの特定および（感染が確認された場合の）対処の実施を依頼しています。また、応答のあった組織には必要に応じて助言を行い、封じ込めを支援しています。

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 Web フレームワークで使われる「Badsecrets」問題

2025 年 10 月 29 日、JPCERT/CC は CyberNewsFlash「既知または弱いシークレットを設定した Web アプリケーションの改ざんリスクについて」[*1]を公開しました。Web フレームワーク等を利用して Web アプリケーションを構築する際に、推測可能な弱いシークレットやインターネット上のサンプルコード等に含まれるデフォルト／既知のシークレットを設定したまま本番運用している場合、環境や条件次第で署名・暗号化処理を偽装され、任意のコード実行に至る可能性がある懸念から、対処および調査に関する関連情報を提供しました。本件に類する問題については、10 年ほど前から複数の組織が指摘しています。

[*1] “既知または弱いシークレットを設定した Web アプリケーションの改ざんリスクについて”. JPCERT/CC. https://www.jpcert.or.jp/newsflash/2025102901.html, (2025-10-29)

2023 年、海外のセキュリティ企業である Black Lantern Security がこの問題を持つ Web フレームワークで構築された Web アプリケーションを横断的にチェックするツールを公開[*2]しました。2025 年 9 月に Shadowserver Foundation が JPCERT/CC に共有[*3]した当ツールによる検出結果には、国内のホストが約 2,500 件含まれていました。また、同年 10 月、Elastic から本問題の悪用により TOLLBOOTH バックドアへの感染が疑われる国内のホスト情報[*4]が提供されました。これを受けて感染疑義のあるホストの管理組織へ個別通知したところ実際に TOLLBOOTH 感染の痕跡が確認されたため、国内においても潜在的に侵害を受けている組織へ注意を促す必要性が高いと判断しました。そこで、当該フレームワーク別の悪用の容易性や任意のコード実行が可能か否か、起き得る被害の深刻さなど、いくつかの観点から通知対応の優先順位を付け、脆弱な状態で公開されていると検出された国内のホストのうち約 400 ホストの利用組織に対し、潜在的リスクの低減を目的とする状況の確認および必要な対処を促す情報提供を実施しました。

2.1.2 LANSCOPE エンドポイントマネージャー オンプレミス版における通信チャネルの送信元検証不備の脆弱性（CVE-2025-61932）

2025 年 10 月 20 日、エムオーテックスは LANSCOPE エンドポイントマネージャー オンプレミス版における通信チャネルの送信元検証不備の脆弱性（CVE-2025-61932）に関するアドバイザリ[*5]を公表しました。本脆弱性は、製品開発者から自社製品届け出として報告され、パートナーシップガイドラインに基づいた公表が行われました。本件の調整の詳細については 4.1.2.1 をご参照ください。

JPCERT/CC は本脆弱性を悪用した攻撃活動が水面下でなされている可能性があると判断し、開発者とも調整の上、同日に CyberNewsFlash を公開[*6]しました。攻撃を受ける可能性が高まると想定される利用ケースや、悪用の可能性がうかがわれる攻撃活動に関する情報を紹介し、製品利用者へ対策や調査の実施を呼びかけました。

2.1.3 WSUS における認証なしの RCE の脆弱性（CVE-2025-59287）

2025 年 10 月 14 日（現地時間）、Microsoft の定例アップデートの中で、Windows Server Update Services（WSUS）における信頼できないデータのデシリアライズの脆弱性（CVE-2025-59287）に対する修正パッチが提供[*7]されました。本脆弱性によって、攻撃者が WSUS で使用するポート番号（8530、8531）に対して細工した HTTP リクエストを送信することで任意のコードを実行できます。2025 年

[*2] “Introducing Badsecrets”. Black Lantern Security. https://blog.blacklanternsecurity.com/p/introducing-badsecrets, (2023-03-20)

[*3] “HIGH: Badsecrets Report”. The Shadowserver Foundation. https://www.shadowserver.org/what-we-do/network-reporting/badsecrets-report/, (2025-09-08)

[*4] “TOLLBOOTH: What’s yours, IIS mine”. Elastic. https://www.elastic.co/security-labs/tollbooth, (2025-10-22)

[*5] “【重要なお知らせ】LANSCOPE エンドポイントマネージャー オンプレミス版におけるリモートでコードが実行される脆弱性について （CVE-2025-61932）”. エムオーテックス株式会社. https://www.motex.co.jp/news/notice/2025/release251020/, (2025-10-20)

[*6] “LANSCOPE エンドポイントマネージャー オンプレミス版における通信チャネルの送信元検証不備の脆弱性（CVE-2025-61932）について”. JPCERT/CC. https://www.jpcert.or.jp/newsflash/2025102001.html, (2025-10-20)

[*7] “Windows Server Update Service (WSUS) のリモートでコードが実行される脆弱性”. マイクロソフト株式会社. https://msrc.microsoft.com/update-guide/ja-jp/vulnerability/CVE-2025-59287, (2025-10-14)

10 月 22 日（現地時間）に HawkTrace が本脆弱性に関する詳細解説および PoC を公開[*8]しましたが、Microsoft は本脆弱性の修正が不十分だったとして 2025 年 10 月 23 日（現地時間）、緊急の更新プログラムを公開するに至りました。

複数のセキュリティ企業が 2025 年 10 月 24 日（現地時間）以降に、本脆弱性を悪用した攻撃を観測したとの情報[*9][*10]を公表しました。さらに、2025 年 10 月 27 日には WSUS が稼働している国内ホスト約 10 件の情報が海外組織から提供されました。こうした状況を踏まえ、JPCERT/CC では攻撃が見られるものの限定的と判断し、2025 年 10 月 28 日から当該ホストに対する個別通知を開始しました。その後、通知先の組織から「リモート勤務者や出張者に対して Windows Update を提供するために当該ポートをオープンにしている」との情報を受領したため、本脆弱性の影響を受ける可能性があるホストを継続的に調査し、最終的に約 60 件のホストに対して個別通知を実施、製品利用者へ JPCERT/CC が確認している脆弱性悪用に関する情報や侵害調査に関する情報を提供し、対策や調査の実施を呼びかけました。

2.1.4 FortiWeb のパストラバーサルの脆弱性（CVE-2025-64446）

2025 年 11 月 13 日（現地時間）、watchTowr Labs が Fortinet 製 FortiWeb におけるパストラバーサルの脆弱性（2025 年 11 月 13 日時点で CVE 未採番）に関する PoC を公表[*11]しました。本脆弱性が悪用されると、管理画面にアクセスした攻撃者が管理者権限で任意のコマンドを実行することができ、深刻な影響を及ぼす可能性があります。2025 年 10 月 6 日（現地時間）には Defused が Fortinet 製品に関連する不審な攻撃通信を観測したと先んじて公表[*12]しており、watchTowr の PoC 公表を受けて、この攻撃が本脆弱性を悪用したものである可能性が高いことが明らかになりました。また、2025 年 11 月 13 日（現地時間）には Rapid7 が本脆弱性の PoC 検証結果を公開[*13]し、FortiWeb の最新バージョン（8.0.2）では対策が確認された一方、8.0.1 など旧バージョンでは悪用が成立することを公表しました。

PoC の公表によって本脆弱性の悪用拡大が懸念されるものの、JPCERT/CC が国内の利用状況を調査したところ、FortiWeb を使用しているホストは十数件程度にとどまり、影響を受けるホストは少数であることが確認されました。このため、広く注意喚起を行うのではなく、すでに悪用が観測されている状況を踏まえ、該当ホストに対して 2025 年 11 月 14 日に個別通知を実施しました。その後、同日（2025 年 11 月 14 日、現地時間）に Fortinet が本脆弱性（CVE-2025-64446）に関するアドバイザリ[*14]を公表

[*8] “CVE-2025-59287 WSUS Unauthenticated RCE”. HawkTrace Security. https://hawktrace.com/blog/CVE-2025-59287-UNAUTH, (2025-10-22)

[*9] “Exploitation of Windows Server Update Services Remote Code Execution Vulnerability (CVE-2025-59287)”. Huntress. https://www.huntress.com/blog/exploitation-of-windows-server-update-services-remote-code-execution-vulnerability, (2025-10-24)

[*10] “Windows Server Update Services (WSUS) vulnerability abused to harvest sensitive data”. Sophos. https://news.sophos.com/en-us/2025/10/29/windows-server-update-services-wsus-vulnerability-abused-to-harvest-sensitive-data/, (2025-10-29)

[*11] “When The Impersonation Function Gets Used To Impersonate Users (Fortinet FortiWeb Auth. Bypass CVE-2025-64446)”. watchTowr. https://labs.watchtowr.com/when-the-impersonation-function-gets-used-to-impersonate-users-fortinet-fortiweb-auth-bypass/, (2025-11-14)

[*12] “Unknown Fortinet exploit (possibly a CVE-2022-40684 variant)”. “X - Defused@DefusedCyber” . https://x.com/DefusedCyber/status/1975242250373517373, (2025-10-06)

[*13] “CVE-2025-64446: Critical Vulnerability in Fortinet FortiWeb Exploited in the Wild”. Rapid7. https://www.rapid7.com/blog/post/etr-critical-vulnerability-in-fortinet-fortiweb-exploited-in-the-wild/, (2025-11-13)

[*14] “Path confusion vulnerability in GUI”. Fortinet. https://fortiguard.fortinet.com/psirt/FG-IR-25-910, (2025-11-14)

したことを受け、JPCERT/CC では FortiWeb を用いた PoC 検証を実施し、悪用時に確認されるログの特徴を整理した上で、アドバイザリ情報および調査すべき観点を追記し再び対象組織へ通知しました。

2.1.5 ArrayAG の DesktopDirect 機能の脆弱性

2025 年 12 月 3 日、JPCERT/CC は、Array Networks 製 Array AG シリーズにおけるコマンドインジェクションの脆弱性に関する注意喚起を公開[*15]しました。同社は、2025 年 5 月に本脆弱性を修正するバージョンをリリース[*16]していましたが、JPCERT/CC では 2025 年 8 月以降に本脆弱性を悪用する攻撃が国内で発生し当該製品に Webshell が設置されたことなどを確認していました。本脆弱性情報は開発元や販売代理店経由で利用者に通知済みと想定されましたが、国内で攻撃が発生している状況下において、本脆弱性情報を認識しておらず、被害の確認や対策の実施ができていない利用者が他にもいる可能性を懸念し、開発元と調整の上で注意喚起を発行しました。注意喚起の公開時点で本脆弱性に関する情報は公表されていませんでしたが、脆弱性の影響を受ける対象や対策などの情報を開発元とも確認し、JPCERT/CC が確認していた攻撃に関する情報も紹介して製品利用者に対策や調査の実施を呼びかけました。

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、6 件公開し、2 件の情報を更新しました。

- 2025-10-01 Cisco ASA および FTD における複数の脆弱性（CVE-2025-20333、CVE-2025-20362）に関する注意喚起 (更新)
- 2025-10-15 2025 年 10 月マイクロソフトセキュリティ更新プログラムに関する注意喚起 (公開)
- 2025-11-12 2025 年 11 月マイクロソフトセキュリティ更新プログラムに関する注意喚起 (公開)

[*15] “Array Networks Array AG シリーズにおけるコマンドインジェクションの脆弱性に関する注意喚起”. JPCERT/CC. https://www.jpcert.or.jp/at/2025/at250024.html, (2025-12-03)

[*16] “Array OS release 9.4.5.9 for the Array AG 1000 series is now available for download.”. “X - Array Support@ArraySupport”. https://x.com/ArraySupport/status/1921373397533032590, (2025-05-11)

- 2025-12-03 Array Networks Array AG シリーズにおけるコマンドインジェクションの脆弱性に関する注意喚起 (公開)
- 2025-12-05 Array Networks Array AG シリーズにおけるコマンドインジェクションの脆弱性に関する注意喚起 (更新)
- 2025-12-10 Adobe Acrobat および Reader の脆弱性（APSB25-119）に関する注意喚起 (公開)
- 2025-12-10 2025 年 12 月マイクロソフトセキュリティ更新プログラムに関する注意喚起 (公開)
- 2025-12-22 WatchGuard 製 Firebox の iked における境界外書き込みの脆弱性（CVE-2025-14733）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、5 件公開し、2 件の情報を更新しました。

- 2025-10-20 LANSCOPE エンドポイントマネージャー オンプレミス版における通信チャネルの送信元検証不備の脆弱性（CVE-2025-61932）について
- 2025-10-21 WatchGuard 製ファイアウォール「Firebox」の iked における境界外書込みの脆弱性（CVE-2025-9242）について
- 2025-10-22 LANSCOPE エンドポイントマネージャー オンプレミス版における通信チャネルの送信元検証不備の脆弱性（CVE-2025-61932）について（更新）
- 2025-10-24 ISC BIND 9 における複数の脆弱性について（2025 年 10 月）
- 2025-10-29 既知または弱いシークレットを設定した Web アプリケーションの改ざんリスクについて
- 2025-12-05 React Server Components の脆弱性（CVE-2025-55182）について
- 2025-12-10 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 13 件公開し、計 99 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」の枠組みに関する詳細は、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 60 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 79 件提供しました。先述の Web フレームワークで使われる「Badsecrets」問題、WSUS における認証なしの RCE の脆弱性（CVE-2025-59287）、FortiWeb のパストラバーサルの脆弱性（CVE-2025-64446）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。センサーに向けて発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対比して分析しています。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。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、各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。

- JPCERT/CC インターネット定点観測レポート

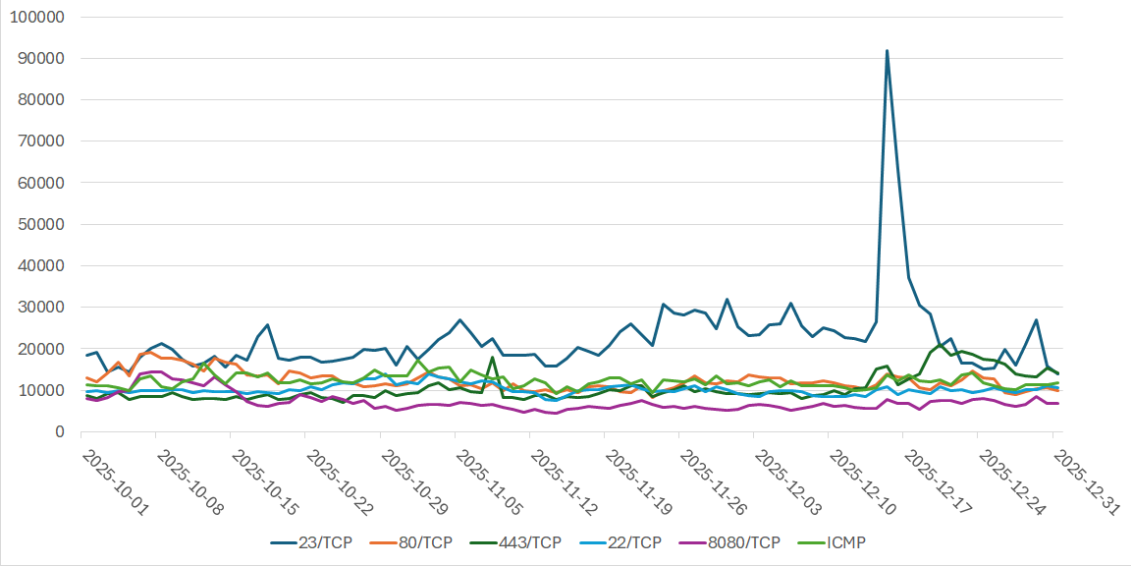

図 3.1 TSUBAME で観測された宛先ポートの上位 1 位〜5 位のパケット数（2025 年 10 月 1 日〜2025 年 12 月 31 日）

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、2025 年 11 月 19 日ごろと、2025 年 12 月 15 日ごろに一時的な増加が見られました。 2 位は 80/TCP でした。3 位は 443/TCP、4 位は 22/TCP で、前四半期の順位と入れ替わりました。8080/TCP は 5 位に入りました。

過去 1 年間（2025 年 1 月 1 日〜2025 年 12 月 31 日）の宛先ポート別パケット数の上位 1〜5 位および 6〜10 位の観測数の推移を図 3.3 と図 3.4 に示します。

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

[*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。

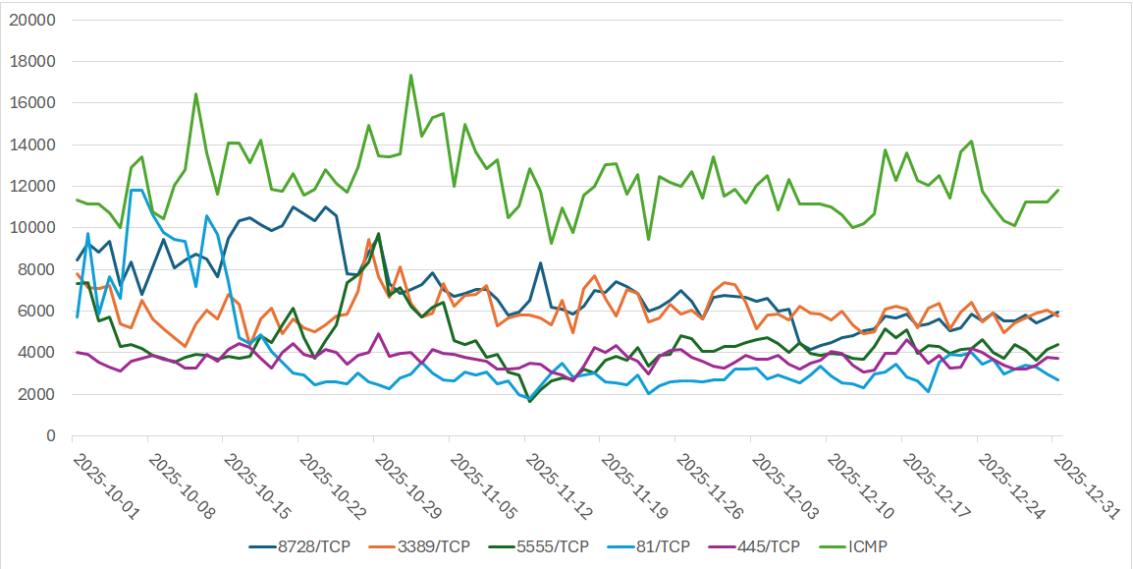

図 3.2 TSUBAME で観測された宛先ポートの上位 6 位～10 位のパケット数
（2025 年 10 月 1 日～2025 年 12 月 31 日）

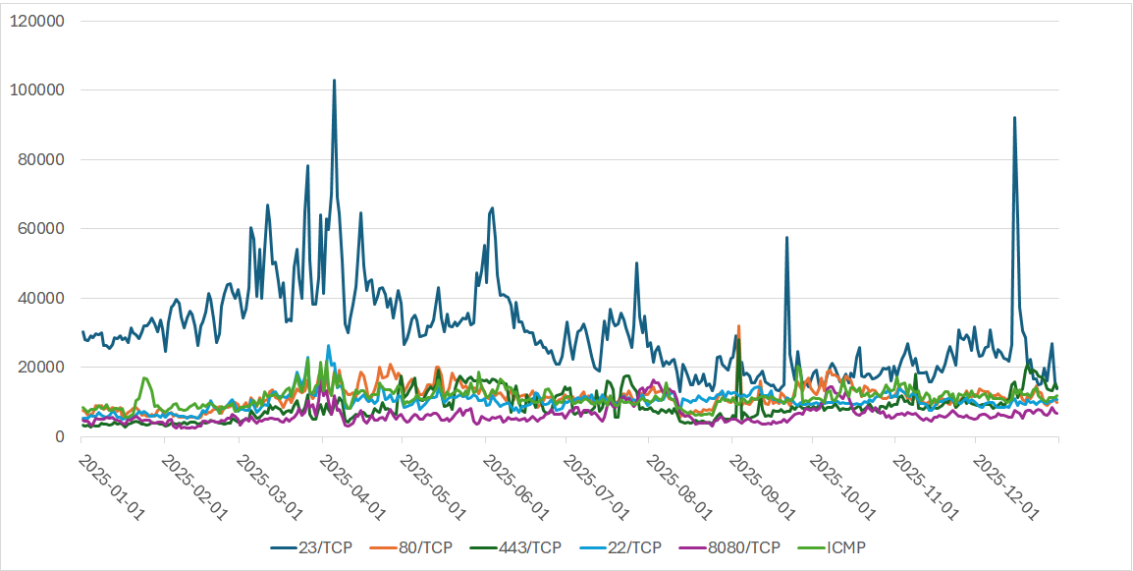

図 3.3 TSUBAME で観測された宛先ポートの上位 1 位～5 位のパケット数
（2025 年 1 月 1 日～2025 年 12 月 31 日）

観測結果とあわせて、攻撃活動を分析しています。本四半期は、React Server Components の脆弱性（CVE-2025-55182）に関する通信を確認しています。

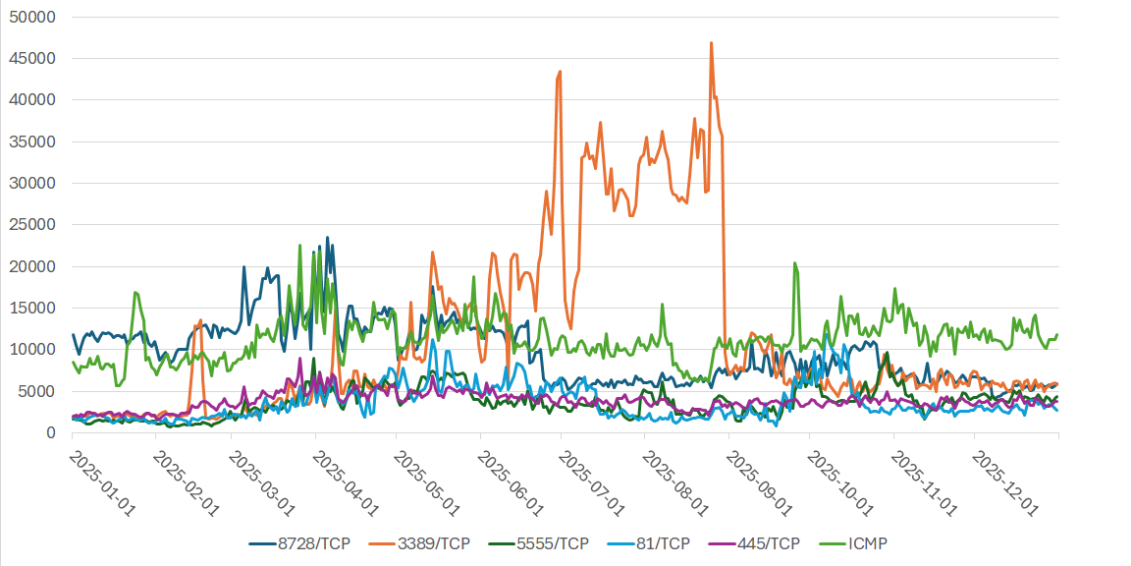

図 3.4 TSUBAME で観測された宛先ポートの上位 6 位～10 位のパケット数
（2025 年 1 月 1 日～2025 年 12 月 31 日）

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。

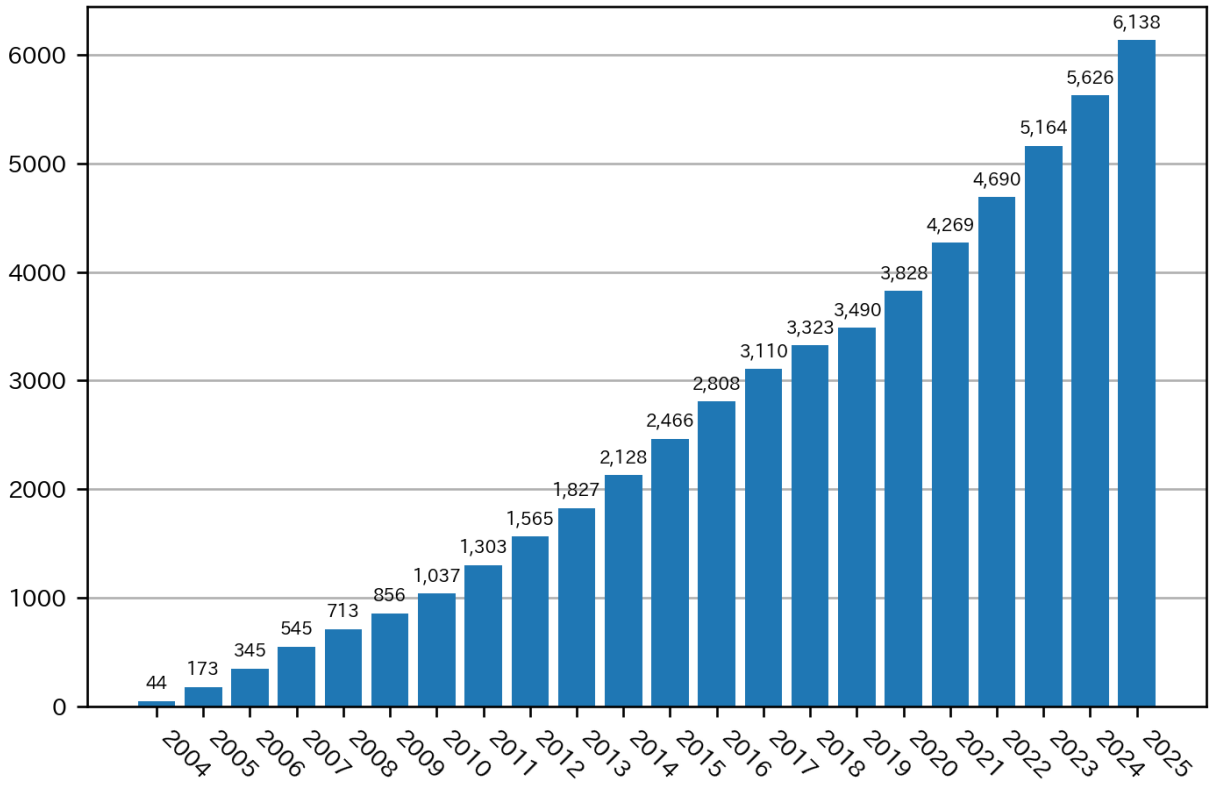

図 4.1 JVN 公表累積件数

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 142 件、累積 6,138 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：39 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：103 件
- 脆弱性情報に関連する技術情報等に関するもの：0 件

なお、パートナーシップガイドラインに基づく脆弱性関連情報に関する四半期ごとの届け出状況については、次の Web ページをご参照ください。

- 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#86318557
  LANSCOPE エンドポイントマネージャー オンプレミス版における通信チャネルの送信元検証不備の脆弱性
  https://jvn.jp/jp/JVN86318557/

エムオーテックスが提供する IT 資産管理ツール「LANSCOPE エンドポイントマネージャー オンプレミス版」の脆弱性です。この脆弱性は製品開発者からの自社製品届け出として報告され、調整の過程で製品利用者の環境で脆弱性を悪用しようとしている可能性がある不正なパケットが確認されていることが判明しました。JPCERT/CC では、脆弱性を悪用した攻撃活動を断定する情報までは得られなかったものの、水面下で攻撃活動が行われている可能性があると判断しました。 IT 資産管理ツールは、主に企業など組織で利用されており、脆弱性が悪用された場合は組織の活動そのものに影響を与えかねません。JVN アドバイザリ公表に際しては、表題に「緊急」と表示し、詳細情報に「開発者によると、顧客環境において外部より不正なパケットを受信する事例が確認されているとのことです。」と記載して、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 CyberNewsFlash を公開し、攻撃を受けるリスクが高いと考えられる製品動作環境を示すことで、さらなる注意を呼びかけました。本件に関する警戒情報の公表の詳細については 2.1.2 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

本四半期において特筆すべき脆弱性はありませんでした。

4.1.2.3 脆弱性調整に関連するその他の特筆すべき事項

協調された脆弱性開示（CVD：Coordinated Vulnerability Disclosure）におけるセキュリティ研究者と調整機関との協力関係について、本四半期に公表した富士電機の作画ソフトウェア V-SFT の脆弱性を例にとって紹介します。

- JVNVU#90008453

富士電機製 V-SFT における複数の脆弱性
https://jvn.jp/vu/JVNVU90008453/

富士電機の作画ソフトウェア V-SFT は同社製プログラマブル表示器のアプリケーションの設計などに用いられるもので、本アドバイザリでは 9 件の脆弱性について指摘しています。本年度、この他に 3 件のアドバイザリ（JVNVU#97228144、JVNVU#94011267、JVNVU#93984110）が JVN で公表されています。計 4 件のアドバイザリのうち 3 件は、セキュリティ研究者の Michael Heinzl 氏から報告された 22 件の脆弱性に関連しています。同氏は、これまでも産業用／制御システムや機器の脆弱性を多く報告しており、JPCERT/CC では 2022 年にベストレポーター賞を贈呈しています。以後も日本製品に含まれる脆弱性の分析を熱心に続けるとともに、責任ある情報開示（Responsible Disclosure）を行っています。同氏以外にも、スマートフォンアプリ、ネットワーク機器、製品インストーラーなど、得意とする分野の製品の脆弱性を発見し、継続的に報告してくださる方々は多数存在します。JPCERT/CC の CVD 活動は、このような理解ある報告者と自らが提供する製品のセキュリティ品質を高めることに積極的な開発者の協力によって成立していますが、状況によっては両者の利害が対立することもあります。研究者として脆弱性を探索している報告者からは、検出した脆弱性を研究成果あるいはその裏付けとして学会の開催タイミングに合わせて公表を望まれる場合があります。一方、開発者は調査や修正プログラム作成・提供のために必要な時間を確保した上での公表を希望します。このように調整がつかず、修正プログラム提供前に脆弱性情報が公開されると、製品ユーザーが攻撃のリスクにさらされてしまう可能性もあります。このような事態を防ぐため、JPCERT/CC は報告者がその能力を正当に評価され、開発者は製品ユーザーを守ることができるように、円滑な情報共有を実施して互いの状況を理解し合えるように努めています。本件のような JVN アドバイザリ公表は、関係者すべての CVD 活動の成果です。こうした調整活動を積み重ね、より多くの関係者と信頼関係を構築し、協力関係を保つことによって、CVD を推進したいと考えております。

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、87 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
- 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 1,325 です。本四半期において、登録者の活動状況などを精査し、廃業や活動終了などのため脆弱性対応が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

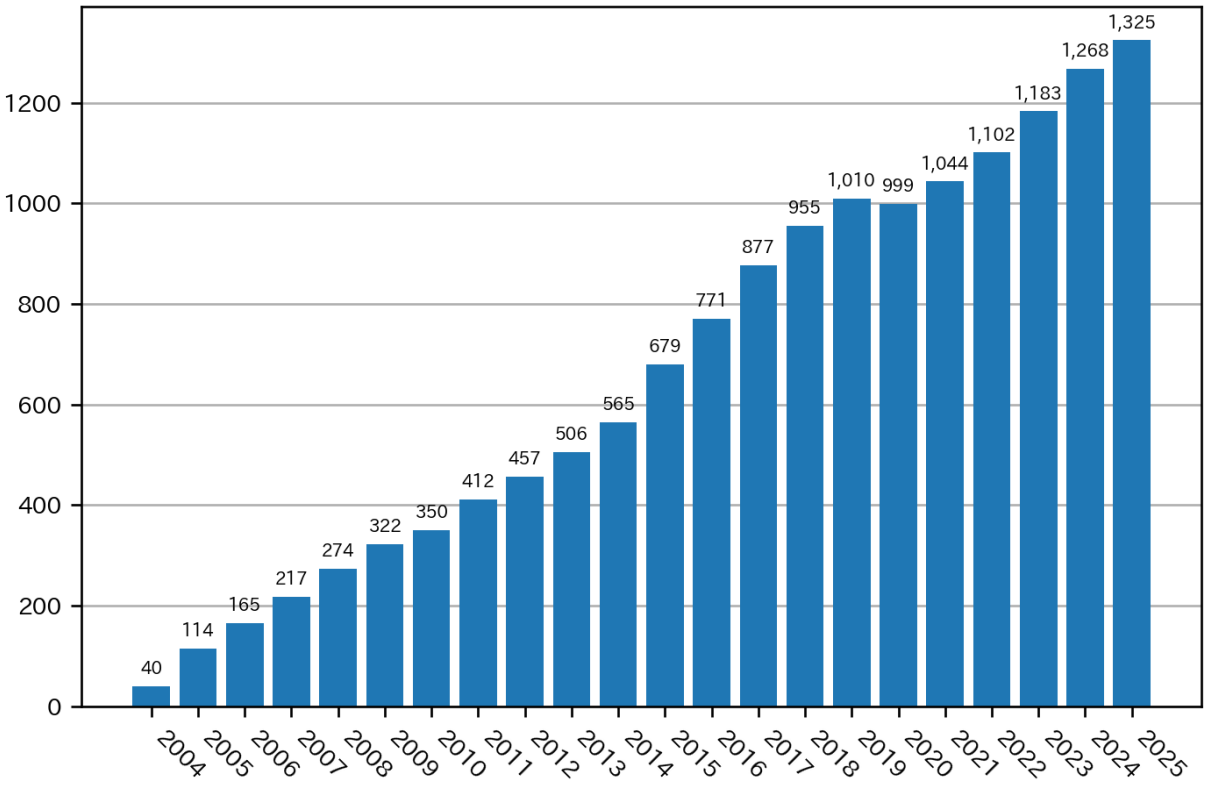

図 4.2 製品開発者登録数

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 日本貿易会 ISAC

2025 年 11 月 21 日に開催された実務部会に参加し、「脆弱性を悪用するインシデントへの対応〜Ivanti Connect Secure などの複数の脆弱性を悪用する攻撃〜」というタイトルで講演を行いました。

5.1.2 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。

5.1.3 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、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、2025 年 12 月 8 日に開催された第 82 回セプターカウンシル運営委員会で、Windows Server Update Services（WSUS）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 13 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 36 組織が参加しています。

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。

6.1.1 2025 FIRST & AfricaCERT Symposium: Africa and Arab Regions への参加

2025 年 12 月 2 日から 2025 年 12 月 5 日にかけて、FIRST と AfricaCERT が共催するアフリカ・アラブ地域向けのシンポジウムがモーリシャスで開催されました。JPCERT/CC はこのイベントに参加し、アフリカ諸国の CSIRT 担当者と意見交換を行いました。また、2025 年 12 月 4 日には国際部長の小宮山功一朗が “Sharing our CVD Journey: Insights and Lessons” と題した講演を行い、脆弱性ハンドリングにおける JPCERT/CC の知見や課題などを共有しました。イベントの詳細は下記 Web ページをご参照ください。

- 2025 FIRST & AfricaCERT Symposium: Africa and Arab Regions
  https://www.first.org/events/symposium/africa-arab-regions2025/

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 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/

6.2.1.1 APCERT Steering Committee 会議の実施

APCERT の Steering Committee は 2025 年 10 月 9 日と 2025 年 11 月 18 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。

6.2.1.2 APCERT 年次総会およびカンファレンス 2025 への参加

2025 年 11 月 25 日から 2025 年 11 月 28 日にかけて、APCERT の年次総会およびカンファレンスがオーストラリアのシドニーで開催されました。今年は “Cyber Horizons: Strengthening Regional Resilience - Together” というテーマのもと、APCERT のメンバー・パートナー組織やオーストラリアのサイバーセキュリティコミュニティーの代表者ら 100 名程度が参加しました。年次総会には APCERT の主要メンバーであるオペレーショナルメンバー（34 チーム）のうち JPCERT/CC を含む 21 チームが参加しました。Steering Committee メンバーのうち任期が満了する 3 チームの改選選挙では、JPCERT/CC に加え、CyberSecurity Malaysia（マレーシア）と Sri LankaCERT|CC（スリランカ）が再選しました。また、JPCERT/CC は事務局の再選も果たしました。議長チームおよび副議長チームの改選では、ACSC（オーストラリア）が議長チームに、KrCERT/CC（韓国）が副議長チームに選出されました。JPCERT/CC は引き続き APCERT の事務局および Steering Committee メンバーとしてさまざまな活動をリードしてまいります。また、2025 年 11 月 28 日に行われた Open Conference では、FIRST 理事を務める国際部マネージャーの内田有香子が FIRST の展開するグローバルなコミュニティー活動について講演を行いました。

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

6.3 海外 CSIRT 等の来訪および訪問

6.3.1 フィリピン CERT-PH への訪問

2025 年 11 月 19 日にフィリピンの CERT-PH の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。

6.3.2 韓国 KISA の来訪

2025 年 11 月 26 日に韓国の Korea Internet & Security Agency（KISA）が JPCERT/CC の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。

6.3.3 シンガポール CSA の来訪

2025 年 12 月 3 日にシンガポールの Cyber Security Agengy（CSA）が JPCERT/CC の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。

6.3.4 モーリシャス CERT-MU への訪問

2025 年 12 月 5 日にモーリシャスの CERT-MU のオフィスを訪問しました。同組織のセキュリティオペレーションセンターを見学し、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。

6.3.5 モンゴル Public CSIRT/CC、MNCERT/CC、National CSIRT への訪問

2025 年 12 月 12 日にモンゴルの CSIRT 関連組織（Public CSIRT/CC、MNCERT/CC、National CSIRT）をそれぞれ訪問しました。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。

6.4 その他国際会議への参加

6.4.1 Enhancing Cyber Resilience: Approach, Responses, and Practical Actions でのパネル登壇

2025 年 11 月 25 日に国際部部長の小宮山功一朗が ADR Institute for Strategic and International Studies の主催するカンファレンス Enhancing Cyber Resilience: Approach, Responses, and Practical Actions に参加しました。サイバーレジリエンスに関するパネルセッションに登壇し、CERT の役割について発言しました。

- Stratbase Pilipinas Conference 2025: Enhancing Cyber Resilience: Approach, Responses, and Practical Actions
  https://adrinstitute.org/2025/11/20/stratbase-pilipinas-conference-2025-enhancing-cyber-resilience-approach-responses-and-practical-actions/

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定に、情報処理学会の情報規格調査会を通じて参加しています。

本四半期は WG3 において、ISO/IEC 29147（脆弱性情報公開）ならびに 30111（脆弱性取り扱い手順）両標準の改訂作業が実質的に開始され、更新内容に関する議論や作業原案（Working Draft）の作成が行われました。

6.6 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や情報流通などにおいて相互に連携しています。また、FIRST 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。

6.6.1 インド太平洋地域向け日米 EU 産業制御システムサイバーセキュリティウィークにおけるワークショップ登壇

2025 年 11 月 18 日から 2025 年 11 月 21 日にかけて、経済産業省と産業サイバーセキュリティセンター（ICSCoE）が米国政府や EU 政府と連携し「インド太平洋地域向け日米 EU 産業制御システムサイバーセキュリティウィーク」を開催しました。

本イベントにはインド太平洋地域の産業界・政府機関の実務者が参加し、各業界特有のシナリオを用い

たワークショップや産業制御分野におけるサイバー攻撃に対するハンズオン演習などが実施されました。JPCERT/CC は脆弱性管理や SBOM に関するワークショップに登壇し、脆弱性調整の基礎や国際的な課題についての発表を行ったほか、参加者を交えた議論をリードしました。イベントの詳細は次の Web ページをご参照ください。

- 経済産業省「インド太平洋地域向け日米 EU 産業制御システムサイバーセキュリティウィーク」を実施しました
  https://www.meti.go.jp/press/2025/11/20251125001/20251125001.html

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、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

フィッシング報告件数は、引き続き高い水準で推移しています。本四半期分の件数が確定していませんが、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 13.0% を占めました。次いで、「Apple」をかたるフィッシングの報告が多く、全体の約 6.1% を占めました。

7.1.2 情報収集／配信

7.1.2.1 フィッシングの動向等に関する情報配信

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、広く注意を喚起しています。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 5 件発信しました。

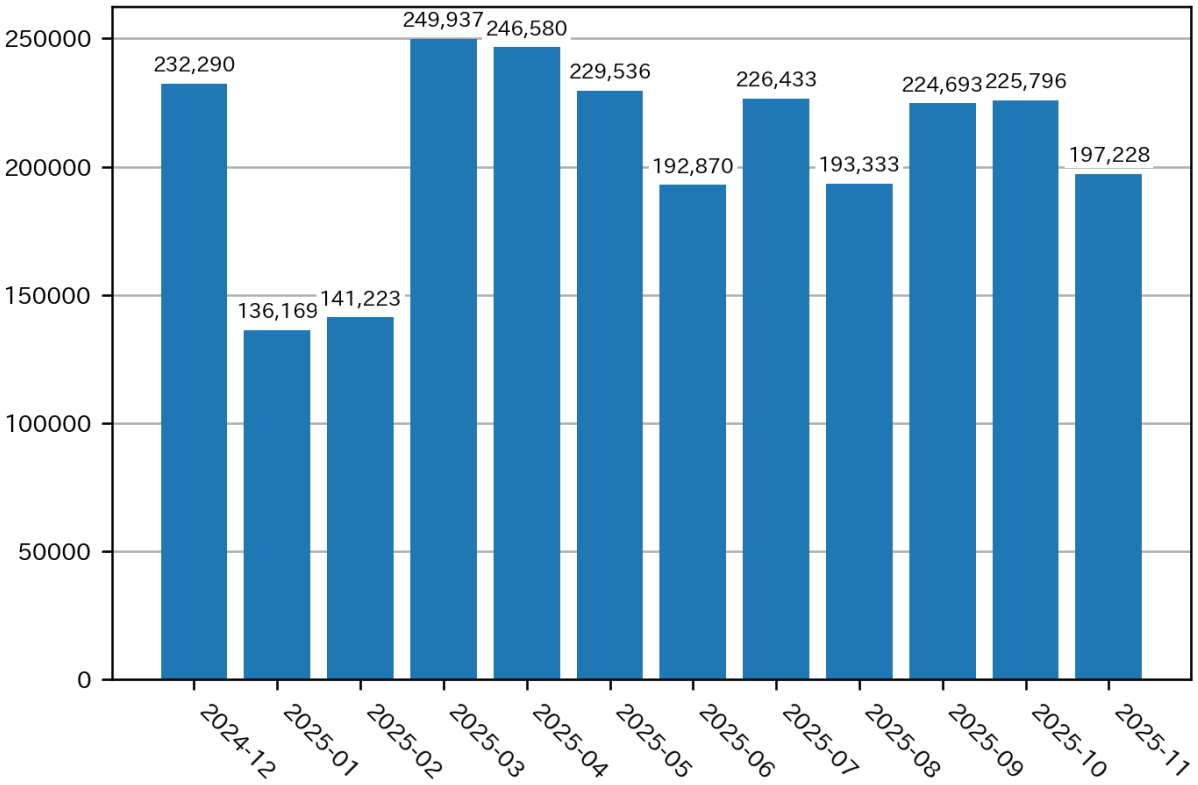

図 7.1 フィッシング報告件数

- 日本郵便をかたるフィッシング
- 宝くじ公式サイトをかたるフィッシング
- OpenAI (ChatGPT) をかたるフィッシング
- ローソンチケットをかたるフィッシング
- みずほ証券をかたるフィッシング

本四半期は、過去に狙われていたブランドをかたるフィッシングが多くなったほか、お歳暮時期や人が移動する時期を狙ったと推察される宅配サービスや交通サービスをかたるフィッシングが発生しました。それ以外にも、国勢調査への回答依頼を装って入力させた電話番号を悪用し、標的となるオンラインサービスの 2 段階認証を突破するために認証コードも入力させる試み（図 7.2）や、宝くじをプレゼントするとした文面で誘導するフィッシング（図 7.3）も発生しました。

7.1.2.2 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/
- 2025/09 フィッシング報告状況

図 7.2 国勢調査への回答依頼を装うフィッシングサイトの例

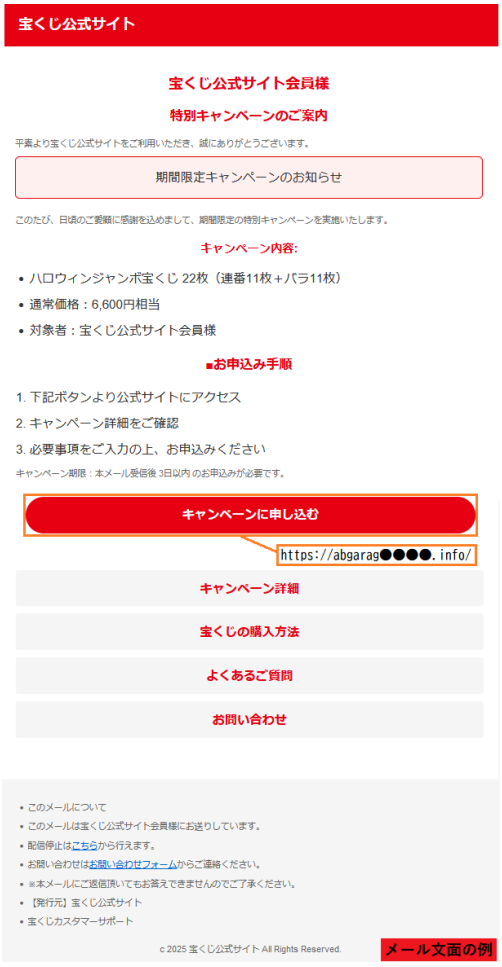

図 7.3 宝くじ公式サイトをかたるフィッシングメールの例

https://www.antiphishing.jp/report/monthly/202509.html

- 2025/10 フィッシング報告状況
  https://www.antiphishing.jp/report/monthly/202510.html
- 2025/11 フィッシング報告状況
  https://www.antiphishing.jp/report/monthly/202511.html

7.1.2.3 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 50 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。

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 132 回運営委員会（JPCERT/CC 会議室＋オンライン）
  日時：2025 年 10 月 23 日 16：00〜18：00
- 第 133 回運営委員会（JPCERT/CC 会議室＋オンライン）
  日時：2025 年 11 月 27 日 16：00〜18：00
- 第 134 回運営委員会（JPCERT/CC 会議室＋オンライン）
  日時：2025 年 12 月 25 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：2025 年 10 月〜2025 年 12 月 毎週火曜日 9：00〜9：30（オンライン）
- 第 2 回 技術・制度検討ワーキンググループ
  日時：2025 年 10 月 8 日 16：30〜18：00（JPCERT/CC 会議室＋オンライン）
- 第 3 回 技術・制度検討ワーキンググループ

日時：2025 年 11 月 6 日 15：30〜18：00（JPCERT/CC 会議室＋オンライン）

- フィッシング対策協議会 20 周年記念セミナー
  日時：2025 年 11 月 14 日 13：00〜19：30（赤坂インターシティコンファレンス the Air ＋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：2025 年 12 月 2 日 16：00〜17：30（JPCERT/CC 会議室＋オンライン）

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。

- ソフトウェア品質向上セミナー
  タイトル：組み込み・制御システムの脆弱性研究動向とセキュア開発の基本的な考え方
  講演者：福本 郁哉（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：2025 年 10 月 16 日
- Internet Week 2025
  タイトル：フィッシングの現状と対策の最新動向（2025 年版）
  講演者：平塚 伸世（国内コーディネーショングループ 情報セキュリティアナリスト）
  主催：日本ネットワークインフォメーションセンター
  講演日：2025 年 11 月 19 日
- Internet Week 2025
  タイトル：「サイバー安全保障」とは何を目指すものなのか ～防御側に求められる対策と思考とは？～
  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：日本ネットワークインフォメーションセンター
  講演日：2025 年 11 月 20 日
- Internet Week 2025
  タイトル：なりすましメールと DMARC を考える フィッシングメールの配信状況（2025 年版）
  講演者：平塚 伸世（国内コーディネーショングループ 情報セキュリティアナリスト）
  主催：日本ネットワークインフォメーションセンター

講演日：2025 年 11 月 20 日

- Internet Week 2025
  タイトル：狙われ続けるエッジデバイス ～JPCERT/CC 目線で見たサイバー攻撃～
  講演者：久下 達也（早期警戒グループ 脅威情報アナリスト）
  主催：日本ネットワークインフォメーションセンター
  講演日：2025 年 11 月 25 日
- セキュリティ人材育成プログラム
  タイトル：動ける CSIRT へ
  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：関西情報センター
  講演日：2025 年 12 月 4 日
- サイバーセキュリティ・セミナー
  タイトル：インシデントレスポンス概論 ～二次被害を最小限にするためのポイント～
  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：JTB ビジネスイノベーターズ
  講演日：2025 年 12 月 11 日
- Infoblox Exchange Tokyo 2025
  タイトル：事例から見る DNS Abuse の動向と国内への影響
  講演者：中井 尚子（インシデントレスポンスグループ シニアインシデントコーディネーター）
  主催：Infoblox
  講演日：2025 年 12 月 11 日
- ESET Cybersecurity Day in Tokyo
  タイトル：狙われ続けるエッジデバイス ～JPCERT/CC の活動からみるサイバー攻撃動向～
  講演者：堀 充孝（早期警戒グループ 脅威情報アナリスト）
  主催：イーセットジャパン
  講演日：2025 年 12 月 11 日
- 令和 7 年度土木部職員研修「サイバーセキュリティ研修」
  タイトル：サイバーセキュリティ研修
  講演者：白石 龍亮（早期警戒グループ 脅威情報アナリスト）
  主催：宮城県
  講演日：2025 年 12 月 19 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。

- 計測技術 2025 年 11 月号
  タイトル：日本国内における制御システムのセキュリティ：これまでと今後の展望
  宮地 利雄（技術顧問）

発行：日本工業出版
発行日：2025 年 11 月 5 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。

- 日本セキュリティ・マネジメント学会 第 37 回学術講演会
  主催：日本セキュリティ・マネジメント学会
  開催日：2025 年 10 月 4 日
- 第 3 回中部・東海版 重要インフラ&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：2025 年 10 月 7 日
- Hardening 2025 Invisible Divide
  主催：Hardening Project 実行委員会
  開催日：2025 年 10 月 8 日〜2025 年 10 月 10 日
- 情報セキュリティワークショップ in 越後湯沢 2025
  主催：新潟情報セキュリティ協会、情報セキュリティワークショップ in 越後湯沢実行委員会
  開催日：2025 年 10 月 10 日〜2025 年 10 月 11 日
- Security Days Fall 2025
  主催：ナノオプト・メディア
  開催日：2025 年 10 月 10 日〜2025 年 10 月 28 日
- 第 25 回迷惑メール対策カンファレンス
  主催：インターネット協会
  開催日：2025 年 11 月 4 日〜2025 年 11 月 5 日
- JAIPA Cloud Conference 2025
  主催：日本インターネットプロバイダー協会クラウド部会
  開催日：2025 年 11 月 4 日
- Internet Week 2025
  主催：日本ネットワークインフォメーションセンター
  開催日：2025 年 11 月 18 日〜2025 年 11 月 27 日
- デジタル・フォレンジック・コミュニティ 2025 in TOKYO
  主催：デジタル・フォレンジック研究会、デジタル・フォレンジック・コミュニティ 2025 実行委員会
  開催日：2025 年 12 月 8 日〜2025 年 12 月 9 日
- Security Management Conference 2025 Winter
  主催：SB クリエイティブ
  開催日：2025 年 12 月 10 日〜2025 年 12 月 11 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。

- 2025-10-24
  JPCERT/CC Internet Threat Monitoring Report [April 1, 2025 - June 30, 2025]
  https://www.jpcert.or.jp/english/doc/TSUBAMEReport2025Q1_en.pdf

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。

- 2025-10-16
  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 3 四半期（7 月〜9 月）］
  https://www.jpcert.or.jp/pr/2025/vulnREPORT_2025q3.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 5 件の記事を公表しました。

日本語版発行件数：2 件 https://blogs.jpcert.or.jp/ja/

- 2025-10-27
  攻撃グループ APT-C-60 による攻撃のアップデート
- 2025-11-18
  Sigma および YARA ルールを活用したリアルタイムクライアント監視ツール YAMAGoya

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

- 2025-10-28
  TSUBAME Report Overflow (Apr-Jun 2025)
- 2025-11-05
  Update on Attacks by Threat Group APT-C-60
- 2025-11-18
  YAMAGoya: A Real-time Client Monitoring Tool Using Sigma and YARA Rules

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 ［ 2025 年 10 月 1 日～2025 年 12 月 31 日 ］

- 発行履歴
  - 2026 年 1 月 22 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/