JPCERT CC®

JPCERT/CC 四半期レポート

2025 年 4 月 1 日～2025 年 6 月 30 日

2025 年 7 月 17 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 4

トピックス&ハイライト . . . 4

『JPCERT/CC 四半期レポート』リニューアル . . . 4

FIRST の理事に JPCERT/CC スタッフが再選 . . . 5

第 1 章　インシデント対応支援 6

1.1　四半期の統計情報 . . . 6

1.2　インシデントの傾向 . . . 12

1.2.1　フィッシングサイトの傾向 . . . 12

1.2.2　Web サイト改ざんの傾向 . . . 13

1.2.3　標的型攻撃の傾向 . . . 14

1.2.3.1　Ivanti Connect Secure の脆弱性（CVE-2025-22457）を悪用した攻撃 . . . 14

1.2.4　その他のインシデントの傾向 . . . 14

1.3　インシデント対応事例 . . . 14

1.3.1　侵入型ランサムウェア攻撃に関する国内組織への通知 . . . 15

第 2 章　脅威情報の分析と提供 16

2.1　情報収集・分析 . . . 16

2.1.1　Ivanti Connect Secure のスタックベースのバッファオーバーフローの脆弱性（CVE-2025-22457） . . . 16

2.1.2　Active! mail のスタックベースのバッファオーバーフローの脆弱性（CVE-2025-42599） . . . 17

2.1.3　Ivanti Endpoint Manager Mobile（EPMM）の脆弱性（CVE-2025-4427、CVE-2025-4428） . . . 18

2.2　Web サイトでの情報提供 . . . 18

2.2.1　注意喚起 . . . 18

2.2.2　CyberNewsFlash . . . 19

2.2.3　Weekly Report . . . 19

2.3　CISTA での情報提供 . . . 19

2.3.1　早期警戒情報 . . . 20

2.3.2　Analyst Note . . . 20

2.3.3　個別提供情報 . . . 20

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 21

3.1　インターネット定点観測システム「TSUBAME」を用いた観測 . . . 21

3.1.1　TSUBAME の観測データの活用 . . . 21

3.1.2　TSUBAME 観測動向 . . . 22

3.2 ハニーポットの運用とその分析 23

第 4 章 脆弱性関連情報の調整と流通 25
4.1 脆弱性関連情報の取り扱い状況 25
4.1.1 JPCERT/CC における脆弱性関連情報の取り扱い 25
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 26
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 . . . 27
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 27
4.1.3 共通脆弱性評価システム「CVSS v4.0」による評価の開始 28
4.1.4 連絡不能開発者対応 28
4.1.5 CNA および Root としての活動 29
4.2 日本国内の脆弱性情報流通体制の整備 29
4.2.1 日本国内製品開発者との連携 29

第 5 章 国内連携活動 31
5.1 業界団体やコミュニティー等との連携活動 31
5.1.1 SICE/JEITA/JEMIMA セキュリティ調査研究合同ワーキンググループ 31
5.1.2 セプターカウンシル運営委員会 31
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 32
5.2.1 早期警戒情報提供先との連携促進 32
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 32
5.3 情報・ツール等の提供 32
5.3.1 制御システムセキュリティ情報提供用メーリングリスト 32
5.3.2 JPCERT/CC ICS Security Notes 32
5.3.3 制御システム向けセキュリティ自己評価ツールの提供 33

第 6 章 国際連携活動 34
6.1 海外 CSIRT 構築支援および運用支援活動 34
6.2 国際 CSIRT 間連携 34
6.2.1 APCERT（Asia Pacific Computer Emergency Response Team） 34
6.2.1.1 APCERT Steering Committee 会議の実施 35
6.2.2 FIRST（Forum of Incident Response and Security Teams） 35
6.2.2.1 第 37 回 FIRST 年次会合への参加 35
6.2.2.2 FIRST の理事に再選 36
6.3 その他国際会議への参加 36
6.3.1 Locked Shields に参加 36
6.3.2 NatCSIRT 2025 への参加 37
6.4 国際標準化活動 37
6.5 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 37
6.5.1 CVE/FIRST VulnCon 2025 & Annual CNA Summit での講演 37

第 7 章 フィッシング対策協議会活動 38
7.1 フィッシング対策協議会事務局の運営 38
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 38

7.1.2 情報収集／配信 38
7.1.2.1 フィッシングの動向等に関する情報配信 38
7.1.2.2 定期報告 40
7.1.2.3 フィッシングサイト URL 情報の提供 41
7.1.2.4 フィッシング対策ガイドラインおよびフィッシングレポートの公開 41
7.2 フィッシング対策協議会の会員組織向け活動 42
7.2.1 運営委員会開催 42
7.2.2 ワーキンググループ会合等 開催支援 42

第 8 章 広報活動 43
8.1 講演 43
8.2 協力・後援 43
8.3 公開資料 44
8.3.1 インシデント報告対応レポート 44
8.3.2 インターネット定点観測レポート 44
8.3.3 脆弱性関連情報に関する活動報告 45
8.3.4 公式ブログ「JPCERT/CC Eyes」 45

付録 A インシデントの分類 47

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」という。）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」という。）の認知と対処、インシデントによる被害拡大の抑止に貢献することを目的として活動しています。国際的な調整・支援が必要となるインシデントについては、日本における窓口組織として国内外の関係機関との調整活動を行っています。

これらの活動のほとんどは、「 令和 7 年度サイバー攻撃等国際連携対応調整事業 」（経済産業省受託事業）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 」（内閣官房受託事業）として実施しています。

本資料では、 2025 年 4 月 1 日～2025 年 6 月 30 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

『JPCERT/CC 四半期レポート』リニューアル

JPCERT/CC の活動はインシデントの関係者間の調整を行うことから始まり、個々の調整で得られた知見をもとに緊急情報を公開することで広く注意を喚起していました。より多くの方に JPCERT/CC やその活動について知っていただけるよう、活動実績を定期的に取りまとめた活動概要を公開するようになりました。その後、脆弱性情報の調整やインターネット定点観測などに業務を拡大し、活動概要は JPCERT/CC のすべての業務を捉えた活動四半期レポートになっていきました。

「どのような情報をどのタイミングで誰が知るべきか」は、JPCERT/CC の業務の一つ一つで常に課題となります。この課題に対し各業務で最適解を求め、取り組み続けることによって JPCERT/CC の活動が形づくられてきました。今日の活動四半期レポートは、その全体像を示すものです。

JPCERT/CC が活動を開始した時代とは異なり、現在は世の中に多種多様なセキュリティ情報が存在しています。そのため、サイバーセキュリティに取り組む人たちは、自らの立場や置かれた状況に応じて適時適切な情報を選択・活用することが求められています。 JPCERT/CC では、そのような皆さんの取り組みに寄与できるよう活動を随時見直し、改善を重ねています。近年、インシデント報告対応は他の業務との関連性や一体性が高まってきました。こうした状況に鑑み、JPCERT/CC とその活動をより分かりやすくお伝えし、各種情報やサービスの一層の利活用につなげることを目的に、2025 年度から

『JPCERT/CC 活動四半期レポート』と『JPCERT/CC インシデント報告対応レポート』を統合することにいたしました。

JPCERT/CC は、「令和 7 年度サイバー攻撃等国際連携対応調整事業」（経済産業省受託事業）と「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」（内閣官房受託事業）を中核とする複数の受託業務や自主活動を、投入資源の適切な分離と管理をはかりつつ、一体的に実施することによって成果の最大化に努めています。個々の業務を通じて得られた有益な知見と JPCERT/CC としての活動の全体概況をバランスよく読者の皆さんにお伝えできるよう、今後も改善を続けていきます。

FIRST の理事に JPCERT/CC スタッフが再選

FIRST（Forum of Incident Response and Security Teams）の理事選挙に国際部マネージャーの内田有香子が立候補し、3 回目の当選を果たしました。FIRST は、2025 年 6 月現在、113 の国・地域にわたる 808 の CSIRT 組織を会員に擁する世界最大規模の CSIRT コミュニティーです。JPCERT/CC は、1998 年に日本で最初の会員となって以来、FIRST の活動に積極的に参加し海外の CSIRT との連携を深めてきました。

FIRST の活動は、Board of Directors を構成する 10 名の理事によって企画・立案されています。理事の任期は 2 年間で、毎年その半数が参加組織による選挙で選出されることになっています。2025 年 6 月にデンマークのコペンハーゲンで開催された年次総会で、事前に行われたオンライン投票の結果が発表され、内田を含む 5 名の理事が決定しました。今回の選挙結果は、JPCERT/CC の FIRST に対する継続的な貢献に対する認識と信頼感が寄与したものと受け止めています。なお、現在の理事の多くは欧米の出身で、アジアからの理事は引き続き内田のみです。

再選を受けて内田は「2024 年に福岡で FIRST カンファレンスが開催されたことを機に、日本国内でも FIRST への関心が高まっていると感じている。この勢いのまま、日本やアジアでのイベント実施等を含め、この地域での FIRST 関連活動をさらに推し進めていくとともに、国際連携の場として、多くの組織に FIRST を活用してもらえるよう、より一層努めたい。」と抱負を述べました。

Board of Directors の他のメンバーや歴任者については、次の Web ページをご参照ください。

- FIRST.Org,Inc., Board of Directors
  https://www.first.org/about/organization/directors

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 4 月 1 日から 2025 年 6 月 30 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示します（表 1.1）[*2]。

本四半期に寄せられた報告件数は 14,558 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 3,544 件でした。前四半期と比較して、報告件数は 44% 増加、調整件数は 11% 減少しました。また、前年同期（報告件数は 15,396 件、調整件数は 4,176 件）と比較すると、報告数は 5% 減少、調整件数は 15% 減少しました。

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（図 1.1, 1.2）。

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

表 1.1 インシデント報告関連件数

	4 月	5 月	6 月	合計	前四半期合計
報告件数	4,053	4,277	6,228	14,558	10,102
インシデント件数	2,532	2,574	3,242	8,348	6,081
調整件数	1,186	1,013	1,345	3,544	3,974

[*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。

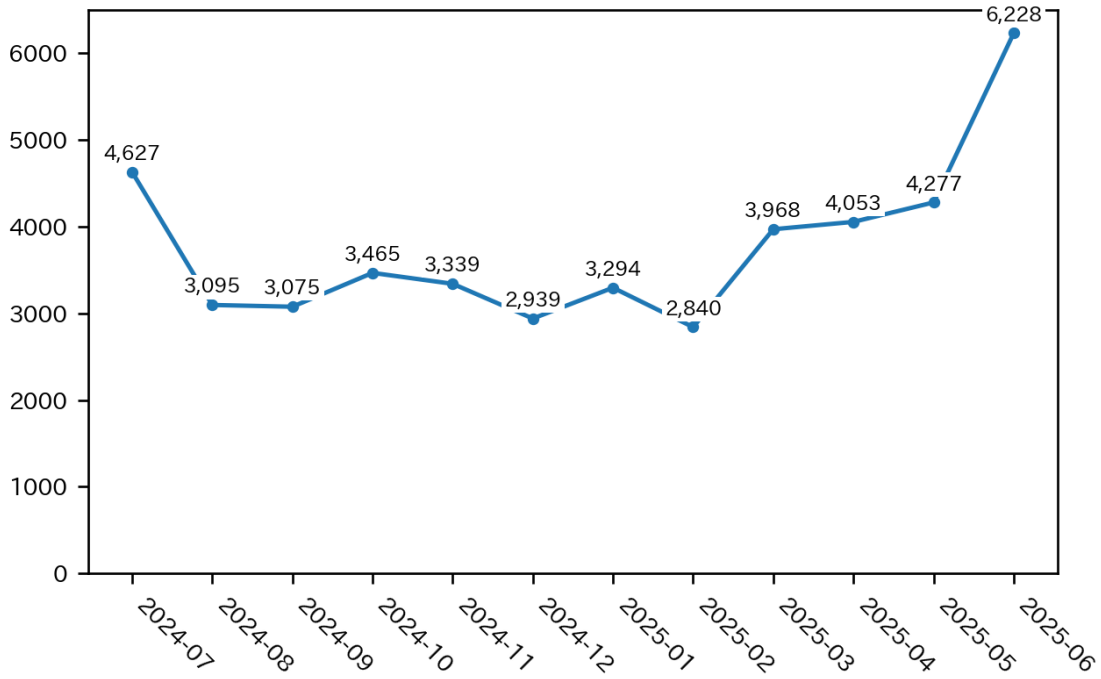

図 1.1 インシデント報告件数の推移

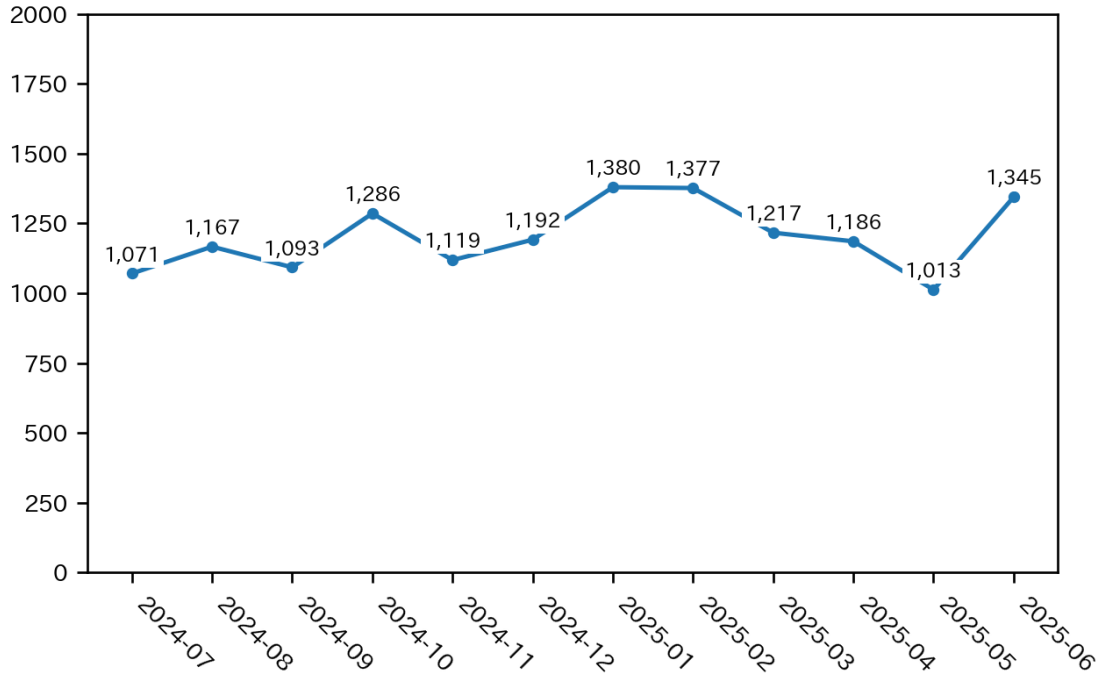

図 1.2 インシデント調整件数の推移

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	4 月	5 月	6 月	合計	前四半期合計
フィッシングサイト	2,222	2,256	2,880	7,358	5,267
Web サイト改ざん	26	64	141	231	95
マルウェアサイト	6	18	4	28	23
スキャン	90	88	62	240	256
DoS/DDoS	0	2	0	2	6
制御システム関連	0	0	0	0	0
標的型攻撃	1	2	2	5	1
その他	187	144	153	484	433

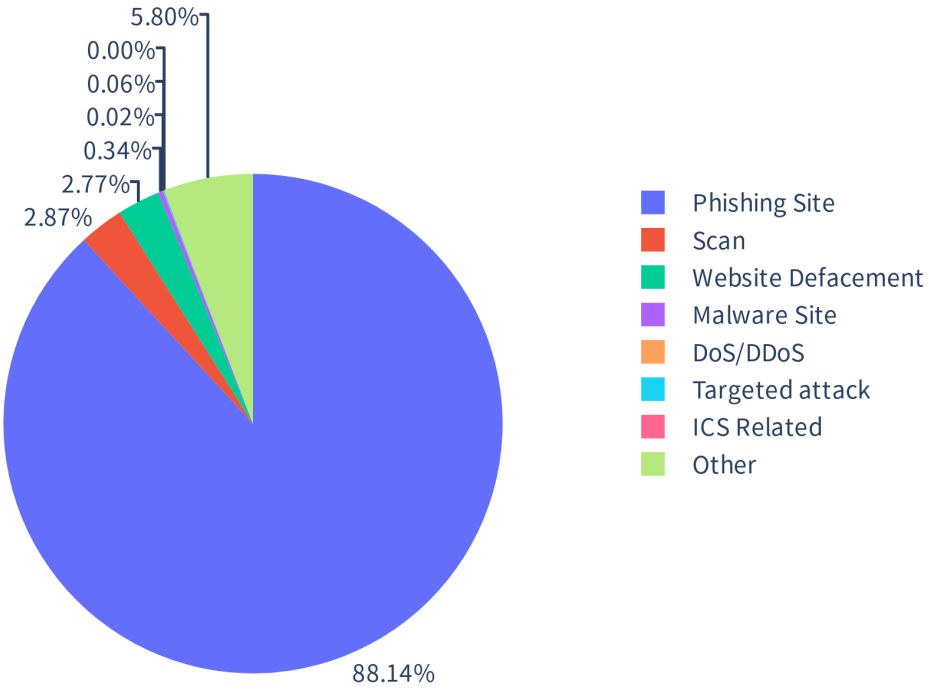

図 1.3 インシデント報告件数のカテゴリー別割合

い。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とカテゴリー別割合を示します（表 1.2, 図 1.3）。

フィッシングサイトに分類されるインシデントが 88% 、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% を占めています。

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（図 1.4〜1.7）。

また、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 1.8）。

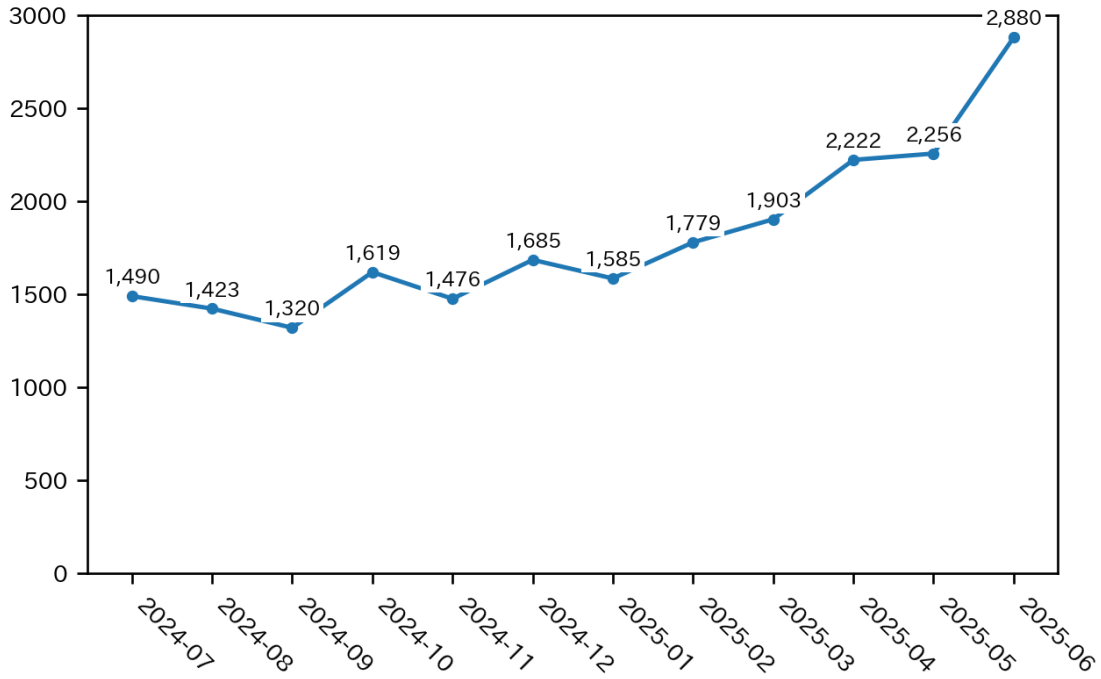

図 1.4 フィッシングサイト件数の推移

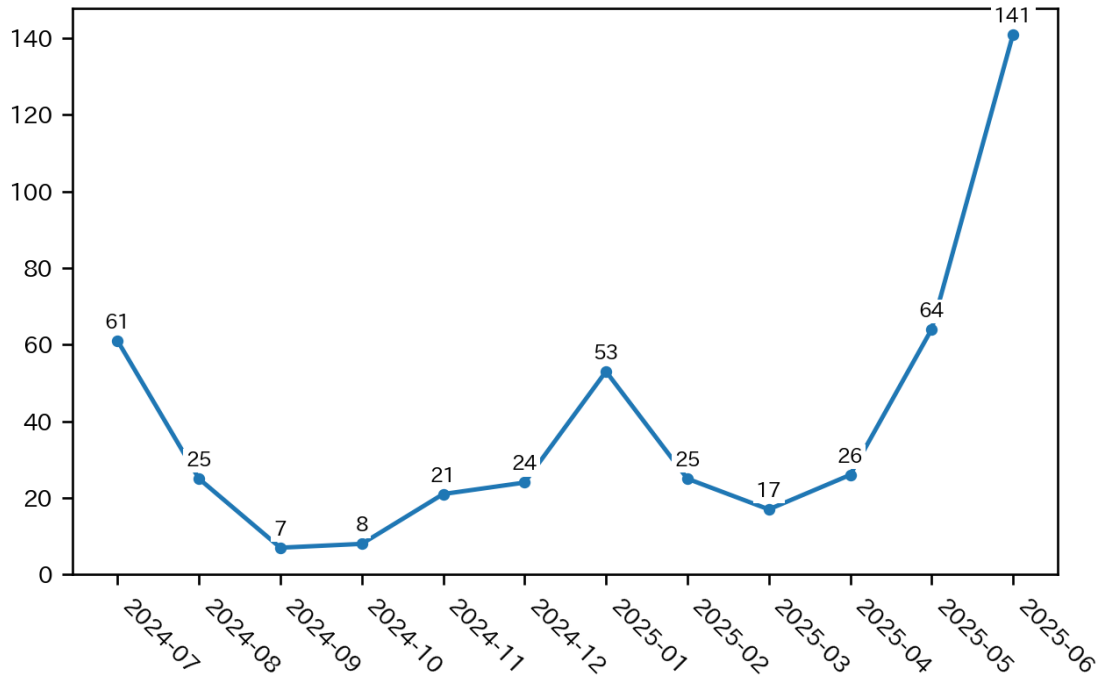

図 1.5 Web サイト改ざん件数の推移

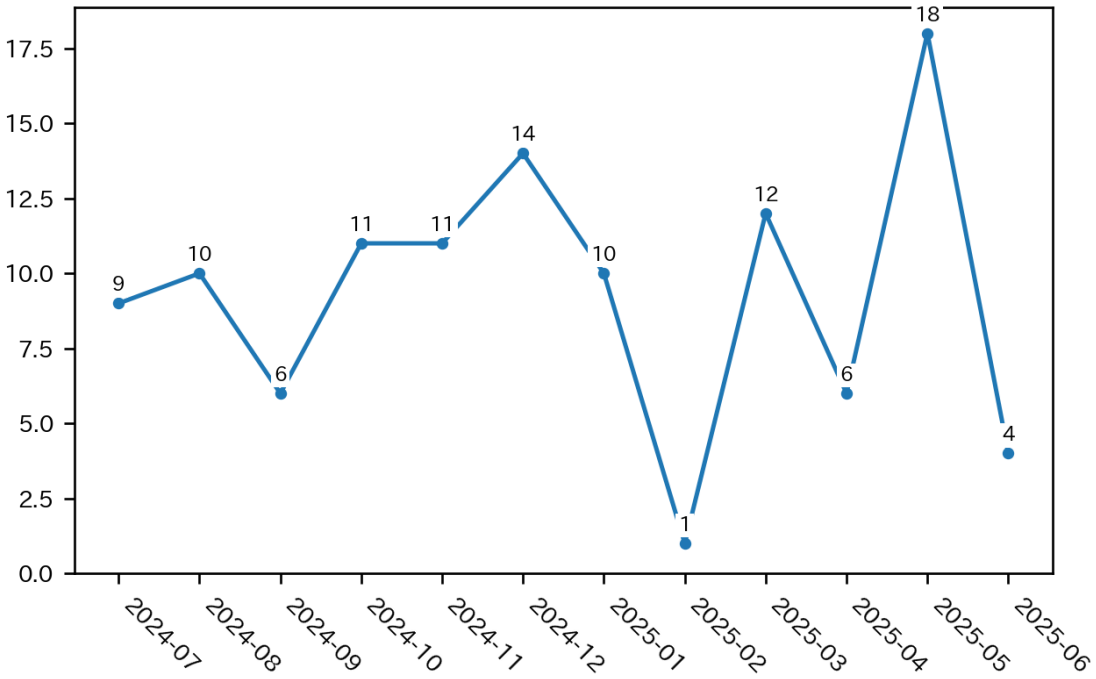

図 1.6 マルウェアサイト件数の推移

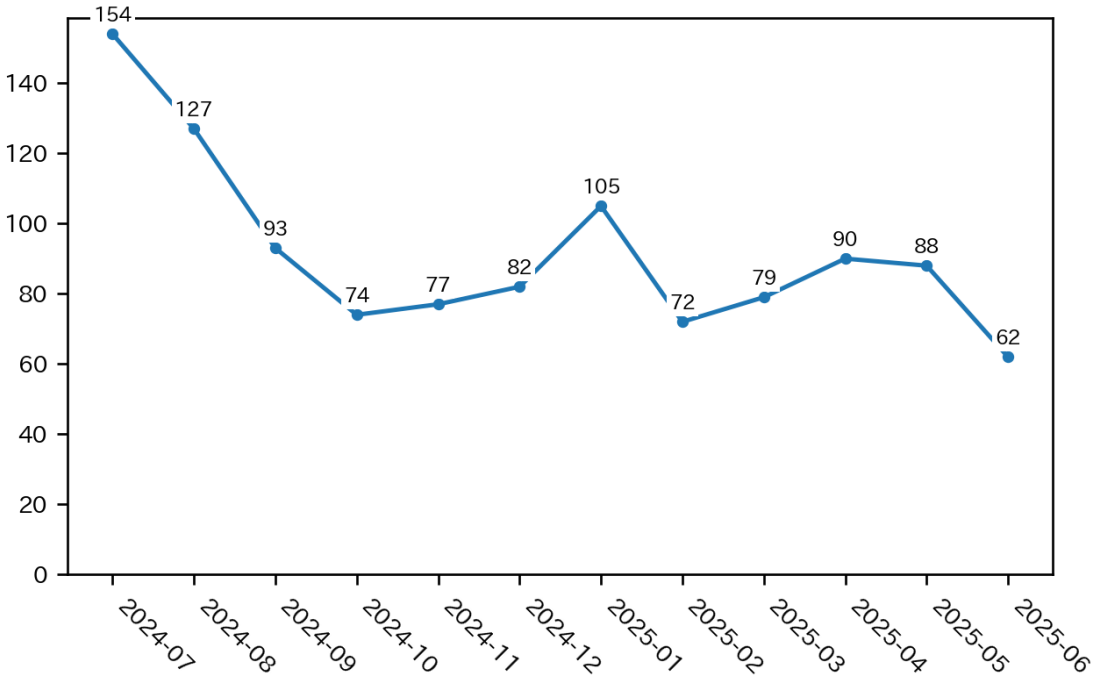

図 1.7 スキャン件数の推移

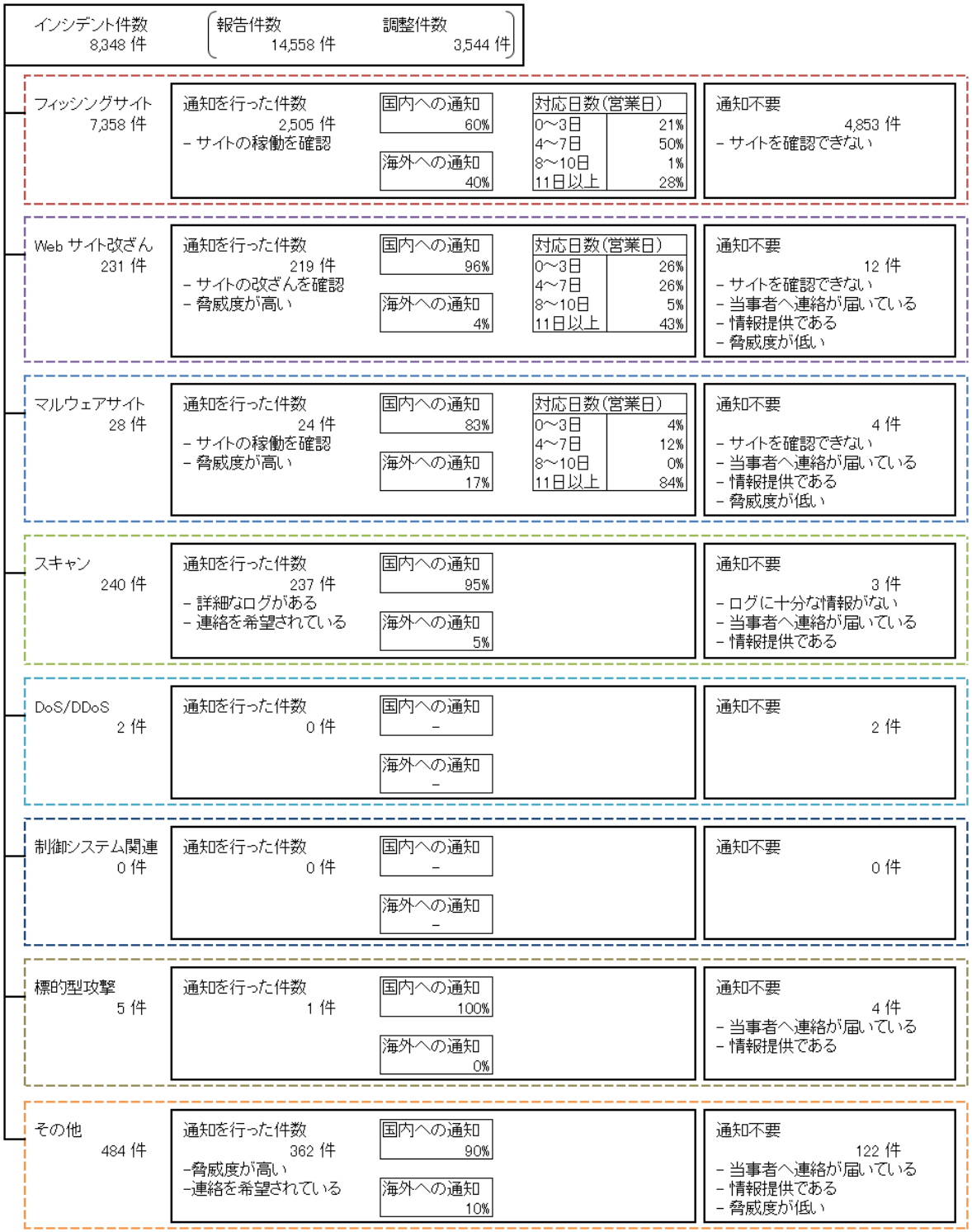

図 1.8 インシデントのカテゴリーごとの件数と調整・対応状況

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	4 月	5 月	6 月	合計	割合
国内ブランド	1,880	1,731	2,339	5,950	81%
国外ブランド	109	194	282	585	8%
ブランド不明	233	331	259	823	11%
全ブランド合計	2,222	2,256	2,880	7,358	

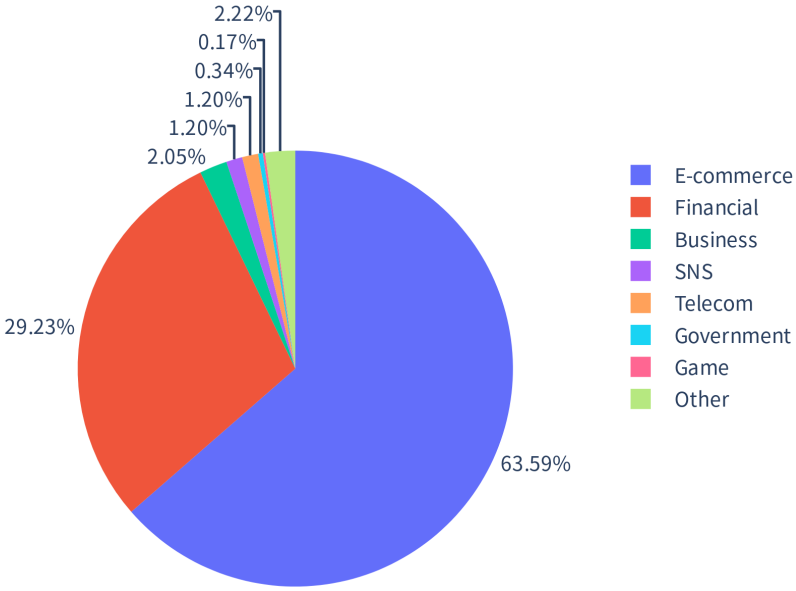

図 1.9 国外ブランドのフィッシングサイトの件数の業界別の割合

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 7,358 件で、前四半期の 5,267 件から 40% 増加しました。また、前年同期（5,025 件）との比較では、 46% 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 585 件で、前四半期の 502 件から 17% 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 5,950 件で、前四半期の 4,277 件から 39% 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] （表 1.3）と、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（図 1.9, 1.10）を示します。

JPCERT/CC が報告を受けたフィッシングサイトのうち、国外ブランド関連の報告では E コマースサイトを装ったものが 63.6%、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 70.2% 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。

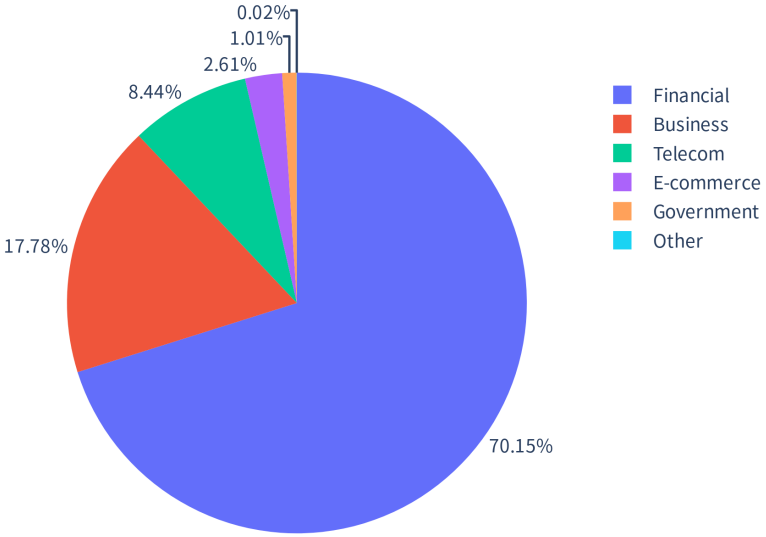

図 1.10 国内ブランドのフィッシングサイトの件数の業界別の割合

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全体の 6 割近くを占めました。国内ブランドでは、SBI 証券、JCB、三井住友カード、楽天を装ったフィッシングサイトが多く報告されました。サイトテイクダウンのために調整したフィッシングサイトの内訳は、国内が 60%、国外が 40% で、前四半期（国内が 53%、国外が 47%）より国内の割合が増えました。

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 231 件でした。前四半期の 95 件から 143% 増加しています。

本四半期は、次のような Web サイト改ざん事例を確認しています。

1. Web サイトに偽の CAPTCHA を表示するコードが挿入されていた事例
2. Web サイトに不正な WordPress プラグインなどが設置されていた事例

事例 1 では、改ざんされた Web サイトにアクセスすると、その操作が人間によるものかを判定する CAPTCHA を装ったチェックボックス（図 1.11）が表示され、チェックすると Windows キー＋ R で開いたウィンドウで Ctrl ＋ V を押し、最後に Enter を押すように促すメッセージが表示されます。このメッセージに従って操作すると、スクリプトによってクリップボードにコピーされたコマンドが実行されます。実行されるコマンドは、mshta コマンドの引数に不審な URL を指定したもので、不正なコードのダウンロードおよび実行が目的と見られるものでした。このような、ユーザーの操作によっ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。

事例 2 では、不正な WordPress プラグイン（SocGholish と呼ばれるマルウェア）が Web サイトに設置されており、Web サイトにアクセスすると不正なコードが挿入された Web ページを応答する改ざんが施されていました。同じ Web サイトには、不正な WordPress プラグインの他に、偽ショッピングサイトに誘導するための PHP ファイル、ファイルの操作やコマンドの実行が可能な Web シェルなども設置

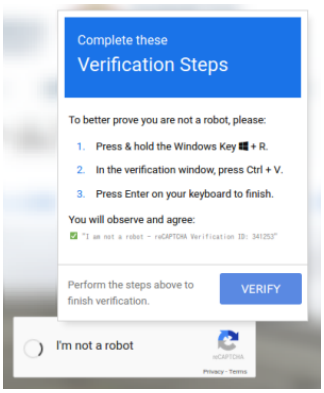

図 1.11 ClickFix のポップアップ画面

されていました。

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 5 件でした。そのうち 1 件を紹介します。

1.2.3.1 Ivanti Connect Secure の脆弱性（CVE-2025-22457）を悪用した攻撃

本四半期は、Ivanti Connect Secure の脆弱性（CVE-2025-22457）を悪用した攻撃の被害報告が複数寄せられました。いずれの事案においても Ivanti Connect Secure に SPAWNSLOTH や SPAWNSNARE、SPAWNCHIMERA と呼ばれるバックドアが設置されており、中国関連とされる攻撃グループ UNC5221 による攻撃であると考えられます。本事例の一部では AD への侵害や Cobalt Strike を使って複数の端末に横展開が行われるなど、ネットワーク内部への侵入も確認されています。

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 28 件でした。前四半期の 23 件から 22% 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 240 件でした。前四半期の 256 件から 6% 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 位を示します（表 1.4）。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）、88/TCP でした。

その他に分類されるインシデントの件数は 484 件でした。前四半期の 433 件から 12% 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例を紹介します。

表 1.4 ポート別のスキャン件数の上位 10 位

ポート	4 月	5 月	6 月	合計
23/tcp	29	55	49	133
22/tcp	9	4	10	23
80/tcp	7	1	1	9
88/tcp	6	1	1	8
8080/tcp	5	0	3	8
79/tcp	4	2	2	8
9001/tcp	3	0	3	6
9000/tcp	4	0	1	5
81/tcp	4	0	1	5
8081/tcp	4	0	1	5

1.3.1 侵入型ランサムウェア攻撃に関する国内組織への通知

本四半期も、複数の被害組織から侵入型ランサムウェア攻撃（SafePay、BlackLock など）による被害報告を受けています。

また、海外のセキュリティ組織から、日本企業の海外グループ会社の環境が、ランサムウェアによる攻撃を受けている可能性があるとの報告を複数受けました。 JPCERT/CC では、日本企業のセキュリティ担当者に情報を共有し、事実確認と対処を依頼しました。これにより、通知先の企業では、ランサムウェア攻撃の被害が発生する前にバックドアが削除され、被害が拡大する前に対処することができました。

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、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または分析した情報のうち、特徴的なものを紹介します。

2.1.1 Ivanti Connect Secure のスタックベースのバッファオーバーフローの脆弱性（CVE-2025-22457）

2025 年 4 月 4 日、Ivanti が Ivanti Connect Secure、Policy Secure、ZTA ゲートウェイにおけるスタックベースのバッファオーバーフローの脆弱性（CVE-2025-22457）に関するアドバイザリを公表[*1]しまし

[*1] “April Security Advisory Ivanti Connect Secure, Policy Secure & ZTA Gateways (CVE-2025-22457)”. Ivanti. https://forums.ivanti.com/s/article/April-Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-22457, (2025-04-03).

た。同日、Mandiant からは本脆弱性を悪用する攻撃に関するレポートが公表[*2]されました。本脆弱性の影響を受けるとみられるシステムが国内でも多数利用されている事実と、本脆弱性を悪用する攻撃が国内で発生する可能性が判明したため、JPCERT/CC は直ちに注意喚起を公開[*3]し、脆弱性の対処や侵害有無の調査に関する情報を提供しました。さらに、JPCERT/CC は国内外の組織と連携し、本脆弱性の影響を受ける可能性があるシステムや、すでに本脆弱性を悪用する攻撃を受けた可能性があるシステムの管理組織に対して被害の未然防止や最小化のための個別通知をしました。その後、攻撃を受けた可能性のある組織とのやり取りの中で、Ivanti が提供する整合性チェックツールの出力結果が改ざんされる事例や、利用組織において整合性チェックツールの仕様に対する理解が不十分なため、適切な対応に至らなかった事例などを確認しました。これらを踏まえて 2025 年 4 月 30 日に注意喚起を更新し、あらためて注意を呼びかけました。

2.1.2 Active! mail のスタックベースのバッファオーバーフローの脆弱性（CVE-2025-42599）

2025 年 4 月 18 日、クオリティアが Active! mail におけるスタックベースのバッファオーバーフローの脆弱性に関するお知らせを公表[*4]しました。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 2025 年 4 月 18 日に JVN で脆弱性情報 （JVN#22348866 Active! mail におけるスタックベースのバッファオーバーフローの脆弱性）を公表[*5]しています。詳しくは「第 4 章 脆弱性関連情報の調整と流通 脆弱性関連情報の取り扱い状況」をご参照ください。また、本脆弱性を悪用した攻撃がすでに確認されていたため、同日、JPCERT/CC は注意喚起を公開[*6]しました。脆弱性の発見者からの報告に基づき、本脆弱性の影響を軽減するための方法として、Web アプリケーションファイアウォール（WAF）を運用している場合の検査および防御方法の例示などをしながら、本脆弱性の影響を受ける製品やサービスを利用している方向けに、対策の適用および侵害有無の調査などを実施するよう呼びかけました。さらに、本脆弱性を悪用する攻撃を受けた組織から共有された攻撃の痕跡に関する情報を、インディケータ情報として CISTA サービスの利用者へ同月内に配信しました。

[*2] “Suspected China-Nexus Threat Actor Actively Exploiting Critical Ivanti Connect Secure Vulnerability (CVE-2025-22457)”. Mandiant. https://cloud.google.com/blog/topics/threat-intelligence/china-nexus-exploiting-critical-ivanti-vulnerability, (2025-04-04).

[*3] “Ivanti Connect Secure などにおける脆弱性（CVE-2025-22457）に関する注意喚起”. JPCERT/CC. https://www.jpcert.or.jp/at/2025/at250008.html, (2025-04-04).

[*4] “Active! mail 6 の脆弱性に関する重要なお知らせ”. 株式会社クオリティア. https://www.qualitia.com/jp/news/2025/04/18_1030.html, (2025-04-18).

[*5] “JVN#22348866 Active! mail におけるスタックベースのバッファオーバーフローの脆弱性”. JVN. https://jvn.jp/jp/JVN22348866/, (2025-04-18).

[*6] “Active! mail におけるスタックベースのバッファオーバーフローの脆弱性に関する注意喚起”. JPCERT/CC. https://www.jpcert.or.jp/at/2025/at250010.html, (2025-04-18).

2.1.3 Ivanti Endpoint Manager Mobile (EPMM) の脆弱性 (CVE-2025-4427、CVE-2025-4428)

2025 年 5 月 13 日、Ivanti が Ivanti Endpoint Manager Mobile（EPMM）の脆弱性に関するセキュリティアドバイザリを公表[*7]しました。同製品には認証回避の脆弱性（CVE-2025-4427）と任意のコード実行の脆弱性（CVE-2025-4428）が存在し、これらの脆弱性を組み合わせることによって、認証なしで任意のコードを実行される可能性があります。Ivanti によれば、ごく少数の利用組織で本脆弱性の悪用が確認されています。JPCERT/CC では、本脆弱性の影響を受ける可能性がある製品が国内で稼働していることを確認していたため、2025 年 5 月 14 日に注意喚起を公表[*8]し、以降、同製品を利用しているとみられる組織に情報提供を行いました。

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、7 件公開し、2 件の情報更新を行いました。

- 2025-04-04 Ivanti Connect Secure などにおける脆弱性（CVE-2025-22457）に関する注意喚起 (公開)
- 2025-04-09 2025 年 4 月マイクロソフトセキュリティ更新プログラムに関する注意喚起 (公開)
- 2025-04-18 Active! mail におけるスタックベースのバッファオーバーフローの脆弱性に関する注意喚起 (公開)
- 2025-04-30 Ivanti Connect Secure などにおける脆弱性（CVE-2025-22457）に関する注意喚起 (更新)
- 2025-05-09 Fortinet 製 FortiOS および FortiProxy における認証回避の脆弱性（CVE-2024-55591）に関する注意喚起 (更新)

[*7] “Security Advisory Ivanti Endpoint Manager Mobile (EPMM) May 2025 (CVE-2025-4427 and CVE-2025-4428)”. Ivanti. https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Endpoint-Manager-Mobile-EPMM, (2025-05-13).

[*8] “Ivanti Endpoint Manager Mobile（EPMM）の脆弱性（CVE-2025-4427、CVE-2025-4428）に関する注意喚起”. JPCERT/CC. https://www.jpcert.or.jp/at/2025/at250011.html, (2025-05-14).

- 2025-05-14 2025 年 5 月マイクロソフトセキュリティ更新プログラムに関する注意喚起 (公開)
- 2025-05-14 Ivanti Endpoint Manager Mobile（EPMM）の脆弱性（CVE-2025-4427、CVE-2025-4428）に関する注意喚起 (公開)
- 2025-06-11 2025 年 6 月マイクロソフトセキュリティ更新プログラムに関する注意喚起 (公開)
- 2025-06-11 Adobe Acrobat および Reader の脆弱性（APSB25-57）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、3 件公開しました。

- 2025-04-17 AiCloud が稼働する ASUS 製 WiFi ルーターからの通信の観測
- 2025-05-12 SonicWall 製 SMA100 シリーズにおける複数の脆弱性（CVE-2023-44221、CVE-2024-38475）を組み合わせた攻撃について
- 2025-05-22 ISC BIND 9 における脆弱性について（2025 年 5 月）

2.2.3 Weekly Report

JPCERT/CC が収集したセキュリティ関連情報のうち重要と判断した情報の概要をレポートにまとめ、原則として毎週水曜日（各週の第 3 営業日）に Weekly Report として公開しています。本四半期は 12 件公開し、計 94 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 1,260 組織との間で情報共有を行っています。「早期警戒情報」の枠組みに関する詳細は、次の Web ページをご参照ください。

- 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 1 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 62 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 65 件提供しました。先述の Ivanti Connect Secure の脆弱性（CVE-2025-22457）、Active! mail の脆弱性（CVE-2025-42599）、Ivanti Endpoint Manager Mobile（EPMM）の脆弱性（CVE-2025-4427、CVE-2025-4428）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。本四半期は、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」を公開しました。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。「TSUBAME レポート Overflow（2025 年 1〜3 月）」では、前年度の観測結果から日本国内に関連するインシデント例を振り返り、特に Mirai の特徴を持った探索パケットの観測状況や送信元の特徴に関する調査結果を示しました。

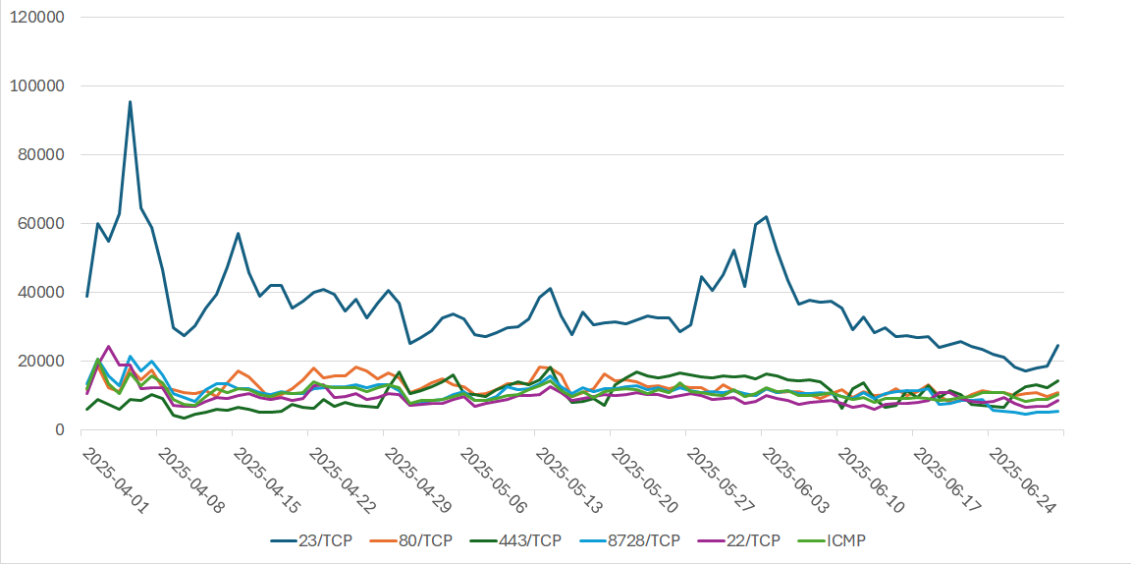

図 3.1 TSUBAME で観測された宛先ポートの上位 1 位〜5 位のパケット数（2025 年 4 月 1 日〜2025 年 6 月 30 日）

- JPCERT/CC インターネット定点観測レポート［2025 年 1 月 1 日〜2025 年 3 月 31 日］
  https://www.jpcert.or.jp/tsubame/report/report202501-03.html
- TSUBAME レポート Overflow（2025 年 1〜3 月）
  https://blogs.jpcert.or.jp/ja/2025/06/tsubame-overflow20250103.html

また、「TSUBAME」で観測される探索パケットの送信元がネットワークカメラである事例が複数見られることから、日本防犯設備協会に観測データなどの提供を行い、『防犯カメラシステムネットワーク構築ガイドⅡ別冊』の作成に協力しました。

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 位とに分けて示します（図 3.1, 3.2）。

また、過去 1 年間（2024 年 7 月 1 日〜2025 年 6 月 30 日）の、宛先ポート別パケット数の上位 1〜5 位および 6〜10 位の観測数の推移を示します（図 3.3, 3.4）。

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 4 月 5 日ごろに急激な増加が見られました。2 位に 80/TCP、3 位に 443/TCP が入り、8728/TCP は 4 位と前四半期から順位が入れ替わりました。Web 上で使用するポートに対する探索パケットが増加しています。5 位の 22/TCP については一時的な増減はあるものの、大きな変化はありません。

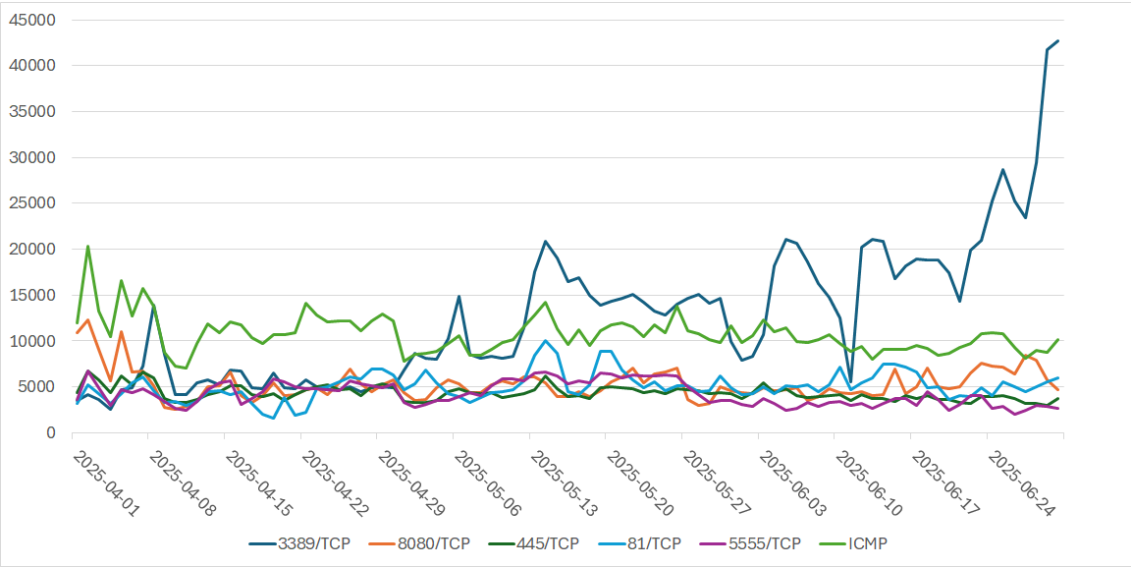

図 3.2 TSUBAME で観測された宛先ポートの上位 6 位〜10 位のパケット数
（2025 年 4 月 1 日〜2025 年 6 月 30 日）

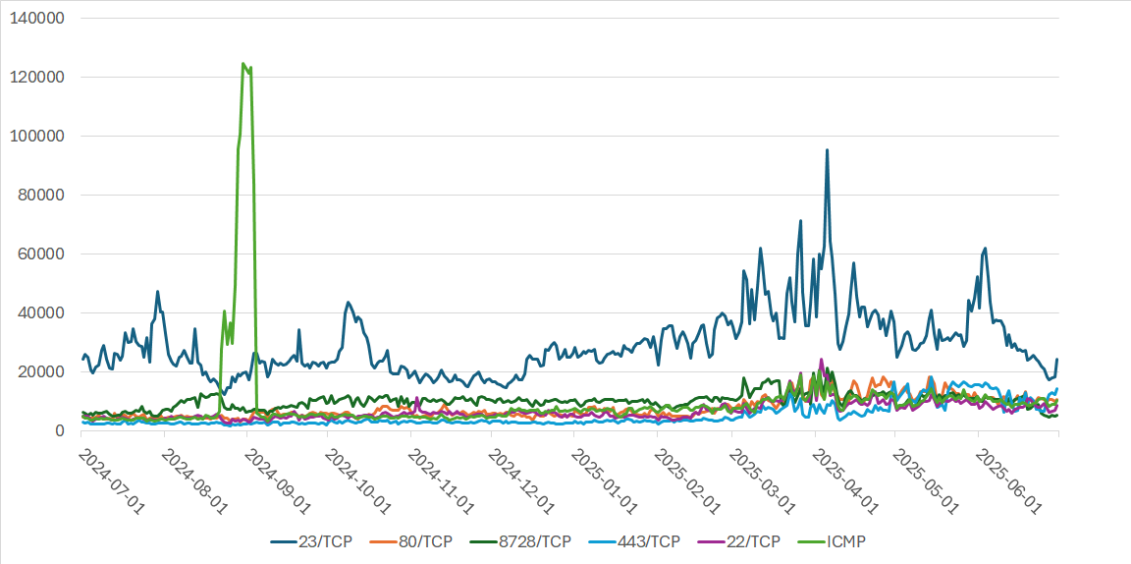

図 3.3 TSUBAME で観測された宛先ポートの上位 1 位〜5 位のパケット数
（2024 年 7 月 1 日〜2025 年 6 月 30 日）

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。

2025 年 6 月 2 日から 2025 年 6 月 4 日にかけて開催された、ハニーポットの開発者や運用者らが集うワークショップ（Honeynet Project Annual Workshop 2025）に参加し、情報収集や意見交換を行いました。Honeynet Project Annual Workshop 2025 の詳細は、次の Web ページをご参照ください。

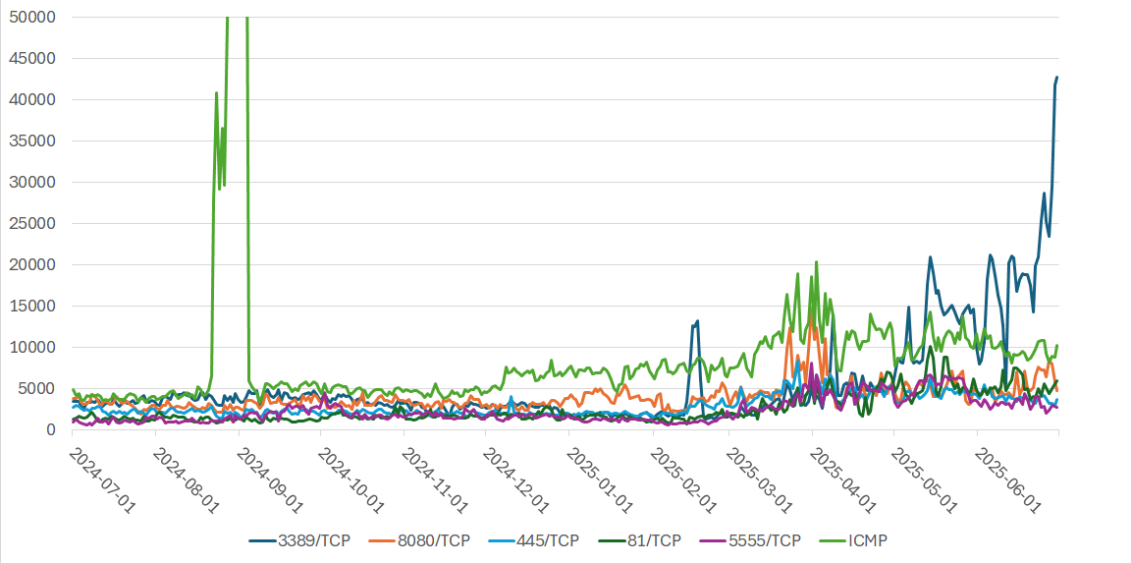

図 3.4 TSUBAME で観測された宛先ポートの上位 6 位〜10 位のパケット数
（2024 年 7 月 1 日〜2025 年 6 月 30 日）

- The Honeynet Project Annual Workshop 2025
  https://prague2025.honeynet.org/

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、独立行政法人情報処理推進機構（IPA）と共同運営している脆弱性情報ポータル JVN（Japan Vulnerability Notes）を通じて公表することで広く注意を促す活動を行っています。さらに、脆弱性の作り込みを防ぐためのセキュアコーディングの普及や、制御システムの脆弱性の問題にも取り組んでいます。

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、対象となる脆弱性に関係する製品開発者の特定、脆弱性関連情報の適切な窓口への連絡、製品開発者による脆弱性の検証や対処に向けた調整を行い、JVN を通じて脆弱性情報等を一般に公表しています。また、公表した脆弱性情報の国際的かつ効果的な情報流通のために、CVE（Common Vulnerabilities and Exposures）Program（個々の脆弱性を特定、記述、公表されたものをカタログ化することを使命として、1999 年から専門家コミュニティーにより進められてきた国際的な活動。米国の MITRE が事務局を務めている）において、配下の CNA（CVE Numbering Authority、CVE 採番機関）を統括する Root の役割を担うとともに、自ら CNA として CVE 番号の付与を行っています。

JPCERT/CC は、経済産業省告示「ソフトウエア製品等の脆弱性関連情報に関する取扱規程」（平成 29 年経済産業省告示第 19 号、最終改正令和 6 年経済産業省告示第 93 号）に基づく「調整機関」として、製品開発者とのコーディネーションを行っています。調整機関としての活動は、この規程に基づく「情報セキュリティ早期警戒パートナーシップガイドライン（以下、「パートナーシップガイドライン」という。）に沿って、脆弱性情報の「受付機関」である IPA と緊密に連携して進めています。

また、CERT/CC や CISA、NCSC-NL、NCSC-FI といった海外の調整組織との国際調整、国内外から寄せられる報告や調整依頼にも対応しています。

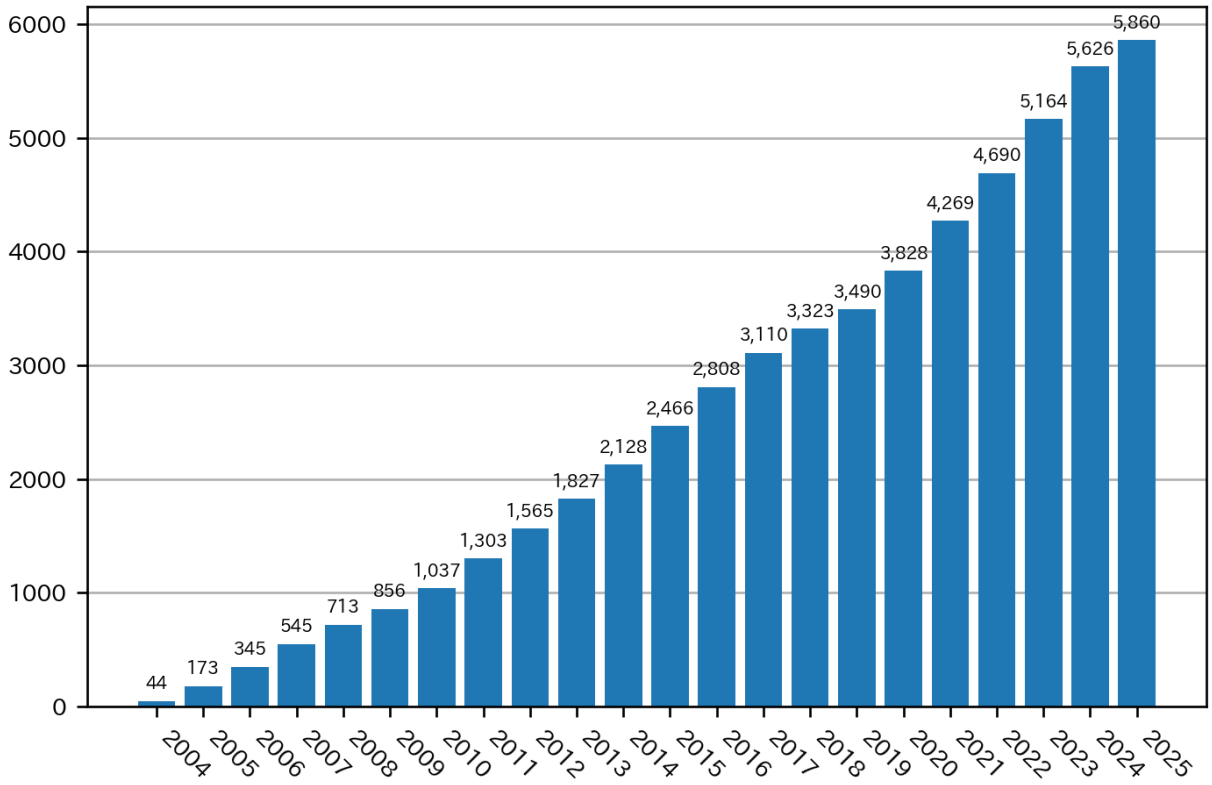

図 4.1 JVN 公表累積件数

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 125 件、累計 5,860 件です（図 4.1）。

本四半期に公表された個々の脆弱性情報に関しては、次の Web ページをご参照ください。

- JVN（Japan Vulnerability Notes）
  https://jvn.jp/

本四半期において公表に至った脆弱性情報件数の内訳は次のとおりです。

- パートナーシップガイドラインに基づき報告された脆弱性情報に関するもの：23 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：102 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。

- 独立行政法人情報処理推進機構（IPA）ソフトウェア等の脆弱性関連情報に関する届出状況
  https://www.ipa.go.jp/security/reports/vuln/software/index.html

本四半期に公表に至った脆弱性のうち、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と国際調整または独自調整で取り扱った脆弱性について、それぞれ特筆すべきものを紹介します。

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

- JVN#22348866
  Active! mail におけるスタックベースのバッファオーバーフローの脆弱性
  https://jvn.jp/jp/JVN22348866/

本件は、クオリティアが提供するビジネス Web メール製品「Active! mail」の脆弱性に関するアドバイザリです。この脆弱性は、遠隔の第三者によって細工されたリクエストが送信された場合、認証なしで任意のコードを実行される可能性があり、脆弱性を悪用されると、製品利用者に深刻な影響を及ぼします。製品開発者からは、脆弱性情報とともに脆弱性を悪用した攻撃を確認したとする情報が JPCERT/CC に報告されました。脆弱性の悪用を示す情報がある場合、JPCERT/CC では JVN でのアドバイザリ公表に向けた調整に加え、警戒情報の公開やインシデントへの対処・対策のための情報提供など、幅広く対応にあたります。本アドバイザリでは、製品利用者に注意を促すため、表題に「緊急」と表示するとともに、攻撃が観測されていることを本文中に書き添えています。また、本アドバイザリ公表後、警戒情報の公開も行い、製品利用者に対し速やかな対応を進めるよう呼びかけました。本件に関する警戒情報公開の詳細については 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

- JVNVU#93701955
  キヤノン製プロダクション/オフィス/スモールオフィス向け複合機およびレーザービームプリンターの一部のプリンタドライバにおける複数の境界外書き込みの脆弱性
  https://jvn.jp/vu/JVNVU93701955/

本件は、LIPSLX や LIPS4、PS3、PCL6、CARPS2 など、キヤノン製プリンタードライバーの脆弱性に関するアドバイザリであり、これらのドライバーは国内向け製品にも海外向け製品にも組み込まれています。この脆弱性に関する情報は、まずキヤノンが Common Vulnerabilities and Exposures サイトで公表し、これを確認した JPCERT/CC は同社と協力して JVN アドバイザリを作成し、脆弱性情報流通を進めました。この脆弱性の影響を受ける製品は、地域によって異なる製品名や型番が付与されている

ため、同社は日米欧の関係会社と連携して、各地域向けにアドバイザリを作成し公表しました。広く海外展開を行っている製品では、地域によって製品名や型番が異なることがあります。このような製品の脆弱性に対しては、地域ごとにアドバイザリを出せるよう各地域の関係会社との間で連携や調整を行うことがあります。また、一つの脆弱性に対し複数のアドバイザリを出す場合は、対策など内容に違いが生じないようにする、公表のタイミングを合わせるといった調整も必要です。 JPCERT/CC では地域や関係者が多岐にわたるような場合でも、緊密かつ友好的に連携することで協調的脆弱性開示（Coordinated Vulnerability Disclosure：CVD）を実施し、公表のタイミングや内容について注意を払い、製品利用者のセキュリティを確保できるよう努めています。

4.1.3 共通脆弱性評価システム「CVSS v4.0」による評価の開始

2023 年 11 月、FIRST が CVSS v4.0 をリリースしました。CVSS v4.0 は CVSS v3.1 からのメジャーアップデートとして、基本評価基準（Base Metrics）の細分化や、評価項目の曖昧さの改善などがなされています。JVN では、2014 年 4 月 1 日から CVSS v2.0（2024 年 3 月 31 日に掲載終了）、2015 年 12 月 1 日から CVSS v3.0 ／ v3.1 を掲載しています。JPCERT/CC では、JVN アドバイザリへの CVSS v4.0 の掲載方法の検討、CVSS v4.0 の評価スキル習得を目的とした勉強会の実施など、JVN での CVSS v4.0 掲載に向けた準備を進めてきました。そして、2025 年 4 月 21 日から、新規公表する JVN アドバイザリへの CVSS v4.0 掲載を開始しました。

- 共通脆弱性評価システム CVSS v4 による評価採用のお知らせ（2025-04-14）
  https://jvn.jp/nav/info2025041471.html

4.1.4 連絡不能開発者対応

パートナーシップガイドラインに基づいて報告された脆弱性について、製品開発者と連絡が取れない場合、公表判定委員会での諮問等による連絡不能開発者案件を公表するための手順（2014 年 5 月告示・ガイドライン改正）に沿って対応を行うケースがあります。 JPCERT/CC ではこの手順に基づき、該当する製品開発者名の連絡の手掛かりを広く求めるための「連絡不能開発者一覧」と、公表判定委員会で公表が妥当と判定された脆弱性を、製品利用者に向けて周知するための「Japan Vulnerability Notes JP（連絡不能）一覧」を JVN 上で公表しています。本四半期においては、「連絡不能開発者一覧」および「Japan Vulnerability Notes JP（連絡不能）一覧」の新規公表は 0 件です。

- 連絡不能開発者一覧
  https://jvn.jp/reply/
- Japan Vulnerability Notes JP（連絡不能）一覧
  https://jvn.jp/adj/

4.1.5　CNA および Root としての活動

JPCERT/CC では、CVE Program の活動に参加し、国際的な脆弱性情報流通を円滑に進めるために、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、64 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。製品開発者には製品開発者リストへの登録をお願いしています。製品開発者の登録数は本四半期末時点で 1,287 です（図 4.2）。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

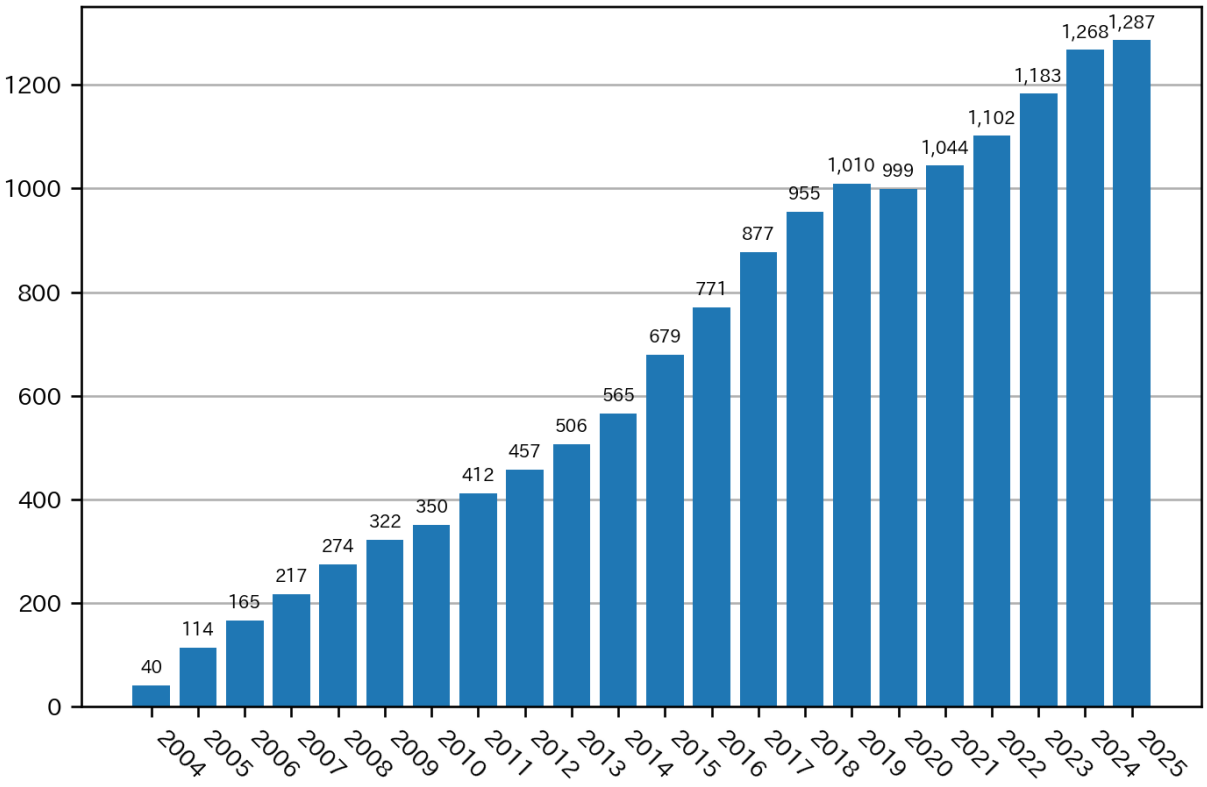

図 4.2 製品開発者登録数

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、平時からそうした組織とセキュリティ状況に関する情報や認識の共有に努め、緊急時の連携が円滑にできるようにするための環境づくりに取り組んでいます。

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行いました。

5.1.1 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、制御システムの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。

5.1.2 セプターカウンシル運営委員会

JPCERT/CC は、セプターカウンシルの活動に参加しワーキンググループ活動の支援や情報提供等を行うとともに、内閣サイバーセキュリティセンター（NISC）[*1]と共同でセプターカウンシルの事務局を支援しています。本四半期においては、2025 年 6 月 2 日に開催された第 80 回セプターカウンシル運営委員会で、Ivanti Connect Secure や Active! mail 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。

[*1] 2025 年 7 月 1 日 国家サイバー統括室（NCO）に改組

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、本四半期において新たに 10 組織が CISTA に登録されました。

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 34 組織が参加しています。

5.3 情報・ツール等の提供

5.3.1 制御システムセキュリティ情報提供用メーリングリスト

これまで制御システムセキュリティ情報提供用メーリングリストを用いて ICS Security Notes を配信していましたが、後述する同サービス終了に伴い、メーリングリストを 2025 年 4 月末をもって廃止しました。

制御システムセキュリティに関する情報提供については、今後は JPCERT/CC の Web 等を活用した取り組みに注力します。

5.3.2 JPCERT/CC ICS Security Notes

「JPCERT/CC ICS Security Notes」は、海外での事例や標準化動向などを JPCERT/CC からのお知らせとともに四半期ごとに配信するもので、JPCERT/CC が収集した制御システムセキュリティ関連の公開情報のうち特に着目していただきたい情報を選び、対象期間にどのような動きがあったのかがわかるよう、コンパクトにまとめたものです。

本四半期に提供した ICS Security Notes は次のとおりです。

- 2025-04-15 JPCERT/CC ICS Security Notes FY2024_#Q4

なお、ICS Security Notes は、国内各組織における制御システムセキュリティ関連の公開情報収集の取り組みが一定程度進んできたことからその役目を終えたと判断し、上記の提供をもってサービスを終了しました。今後は「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」や「制御システムセキュリティカンファレンス」等を通じて、より実践的な課題解決につながる取り組みに注力していき

ます。

5.3.3 制御システム向けセキュリティ自己評価ツールの提供

JPCERT/CC では、制御システムの構築と運用に関するセキュリティ上の問題項目を抽出し、バランスの良いセキュリティ対策を行っていただくことを目的として、簡便なセキュリティ自己評価ツールである日本版 SSAT（SCADA Self Assessment Tool：申し込み制）や J-CLICS（制御システムセキュリティ自己評価ツール）を無償で提供しています。

- 日本版 SSAT（SCADA Self Assessment Tool）
  https://www.jpcert.or.jp/ics/ssat.html
- J-CLICS STEP1 ／ STEP2（ICS セキュリティ自己評価ツール）
  https://www.jpcert.or.jp/ics/jclics.html
- J-CLICS 攻撃経路対策編（ICS セキュリティ自己評価ツール）
  https://www.jpcert.or.jp/ics/jclics-attack-path-countermeasures.html

第 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 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 5 月 22 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います。2021 年 6 月からは、国際部マネージャーの内田有香子が FIRST の理事を務めています。本四半期は、毎月のオンラインによる理事会に加え、2025 年 6 月にコペンハーゲンで開催された対面での理事会にも参加しました。 FIRST の詳細については、次の Web ページをご参照ください。

- FIRST
  https://www.first.org/
- FIRST.Org, Inc., Board of Directors
  https://www.first.org/about/organization/directors

6.2.2.1 第 37 回 FIRST 年次会合への参加

第 37 回 FIRST 年次会合が 2025 年 6 月 22 日から 2025 年 6 月 27 日にかけてデンマークのコペンハーゲンで開催されました。本会合は、サイバーインシデントの予防、対応、技術分析等に関する最新動向の情報交換およびインシデント対応チームの連携強化を目的に毎年開催されています。今年は “Fortresses of the Future: Building Bridges not Walls” をテーマに多種多様なトピックが取り上げられ、103 の国から 1,055 名が現地参加しました。今回 JPCERT/CC は “Establishing a Global Community of Practice on Coordinated Vulnerability Disclosure (CVD)” と題した講演を行い（図 6.1）、米国 CISA が主導して立ち上げた脆弱性情報流通に関わる国際的なコミュニティーにおける取り組みについて、CISA 担当者と共同で発表しました。

さらに、この機会を利用して世界各国の National CSIRT や製品ベンダーの CSIRT 等と個別に意見交換を行いました。このような会合への参加を通した各地域間の情報共有の促進や信頼関係の醸成によって、国際間でのインシデント対応調整がより円滑に進められるよう今後も活動してまいります。

第 37 回 FIRST 年次会合についての詳細は、次の Web ページをご参照ください。

- 37th Annual FIRST Conference
  https://www.first.org/conference/2025/
- FIRSTCON25 Delivers Global Collaboration and Groundbreaking Cybersecurity Initiatives
  https://www.first.org/newsroom/releases/20250627

図 6.1 JPCERT/CC の発表の模様

6.2.2.2　FIRST の理事に再選

FIRST の活動の企画・立案等を行う Board of Directors を構成する 10 名の理事は、加盟組織による選挙によって選出されます。理事の任期は 2 年間で、毎年半数が改選の対象となります。選挙はオンライン投票により行われ、2025 年 6 月 23 日の総会で内田を含む 5 名の当選が発表されました。これにより内田は 3 期目を務めることになりました。他の Board of Directors のメンバーについては、次の Web ページをご参照ください。

- FIRST.Org,Inc., Board of Directors
  https://www.first.org/about/organization/directors

6.3　その他国際会議への参加

6.3.1　Locked Shields に参加

2025 年 5 月 6 日から 2025 年 5 月 9 日にかけて、NATO サイバー防衛協力センター（Cooperative Cyber Defence Centre of Excellence：CCDCOE）が主催する国際的なサイバー演習 Locked Shields 2025 にオンライン参加しました。JPCERT/CC の職員 4 名が日本の政府や重要インフラ事業者の参加者とともにブルーチームの一員として、インシデントの対応および法務・広報の課題に取り組みました。

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

6.3.2 NatCSIRT 2025 への参加

第 37 回 FIRST 年次会合に連続した日程で、米国 CERT/CC が主催する National CSIRT Meeting（NatCSIRT）2025 がデンマークのコペンハーゲンで開催されました。本会合は、世界各国の National CSIRT が一堂に会し、国を代表するインシデント対応チームとしての活動計画や課題を共有し、開発ツールや共同プロジェクト、調査研究等に関して発表し議論することを目的に毎年開催されています。

NatCSIRT についての詳細は、次の Web ページをご参照ください。

- NatCSIRT 2025
  https://resources.sei.cmu.edu/news-events/events/natcsirt/index.cfm

6.4 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、国際会議で改訂が提案された脆弱性情報公開ならびに脆弱性取り扱いの手法に関する文書について、引き続き情報収集など対応の準備を進めました。

6.5 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。本四半期の活動を次に紹介します。

6.5.1 CVE/FIRST VulnCon 2025 & Annual CNA Summit での講演

2025 年 4 月 7 日から 2025 年 4 月 10 日にかけて、CVE Program と FIRST の SIG の一つである「PSIRT SIG」が合同で主催する CVE/FIRST VulnCon 2025 & Annual CNA Summit が米国ノースカロライナ州ローリーにて開催されました。 JPCERT/CC は、2024 年に設立され JPCERT/CC も参加している国際的な脆弱性コーディネーター組織によるコミュニティー「Global Community of Practice on Coordinated Vulnerability Disclosure（CVD-COP）」について、米国関係者とともに、その設立目的や、この活動で現在特定されている課題点等に関する講演を行いました。イベントの詳細については、次の Web ページをご参照ください。

- CVE/FIRST VulnCon 2025 & Annual CNA Summit
  https://www.first.org/conference/vulncon2025/

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」という。）は、フィッシングに関する情報収集・提供と動向分析、技術・制度的対応の検討等を行う会員組織です。 JPCERT/CC は、経済産業省からの委託により、協議会の活動のうち、一般消費者からのフィッシングに関する報告・問い合わせの受け付け、フィッシングサイトに関する注意喚起等、一部のワーキンググループの運営等を行っています。

また、協議会は報告を受けたフィッシングサイトについて JPCERT/CC に報告しており、これを受けて JPCERT/CC がインシデント対応支援活動の一環としてフィッシングサイトを停止するための調整等を行っています。

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、前四半期と比較し増加しました。過去 1 年間のフィッシング報告件数の推移を示します（図 7.1）。

報告件数の内訳では「SBI 証券」をかたるフィッシングの報告数が最も多く、全体の約 17.1% を占めました。次いで、「Apple」をかたるフィッシングの報告も多く、全体の約 9.6% 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 12 件発信しました。

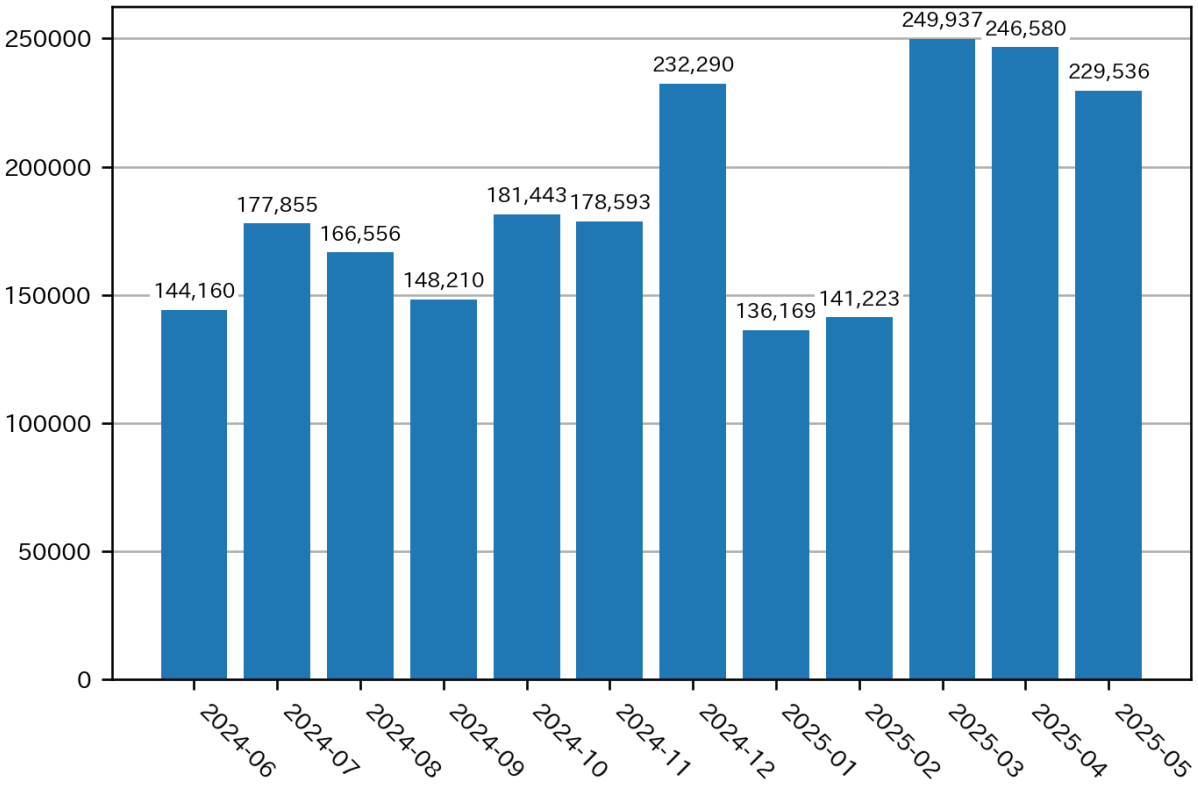

図 7.1 フィッシング報告件数

- SBI 証券をかたるフィッシング
- 楽天証券をかたるフィッシング
- 野村證券をかたるフィッシング
- 松井証券をかたるフィッシング
- LINE をかたるフィッシング
- ANA をかたるフィッシング
- 東京ガスをかたるフィッシング
- 三菱 UFJ モルガン・スタンレー証券をかたるフィッシング
- GMO クリック証券をかたるフィッシング
- PayPay カードをかたるフィッシング
- 大和証券をかたるフィッシング
- 岩井コスモ証券をかたるフィッシング

本四半期は、前四半期から続いている証券会社をかたるフィッシングが大幅に増加しました（図 7.2）。フィッシング攻撃により詐取されたアカウント情報で口座が乗っ取られ、不正に株の売買が行われて損失が出る等の被害が発生しており、注意が必要です。その他では前月に引き続き、移転や旅行シーズンを狙ったと思われる電気・ガス会社や宅配便業者、航空会社をかたるフィッシングが増加しました（図 7.3）。

図 7.2 証券会社をかたるフィッシングサイトの例

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/
- 2025/03 フィッシング報告状況
  https://www.antiphishing.jp/report/monthly/202503.html
- 2025/04 フィッシング報告状況
  https://www.antiphishing.jp/report/monthly/202504.html
- 2025/05 フィッシング報告状況
  https://www.antiphishing.jp/report/monthly/202505.html

図 7.3 航空会社をかたるフィッシングサイトの例

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。

7.1.2.4　フィッシング対策ガイドラインおよびフィッシングレポートの公開

「技術・制度検討ワーキンググループ」は、協議会の会員を中心とする有識者で構成される作業部会で、フィッシング対策に関するガイドラインや動向レポートの作成・改訂を行っています。 2024 年度に技術・制度検討ワーキンググループにおいて作成と改定を進めた『フィッシング対策ガイドライン 2025 年度版』『利用者向けフィッシング詐欺対策ガイドライン 2025 年度版』および『フィッシングレポート 2025』を 2025 年 6 月 3 日に公開しました。

- フィッシング対策ガイドライン 2025 年度版
  https://www.antiphishing.jp/report/guideline/antiphishing_guideline2025.html

- 利用者向けフィッシング詐欺対策ガイドライン 2025 年度版
  https://www.antiphishing.jp/report/guideline/consumer_guideline2025.html
- フィッシングレポート 2025
  https://www.antiphishing.jp/report/wg/phishing_report2025.html

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 は事務局として以下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 127 回運営委員会（オンライン）
  日時：2025 年 4 月 17 日（木）16：00〜18：00
- 第 128 回運営委員会（オンライン）
  日時：2025 年 5 月 21 日（水）16：00〜18：00
- 第 129 回運営委員会（オンライン）
  日時：2025 年 6 月 26 日（木）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 4 月〜2025 年 6 月　毎週火曜日 9：00〜9：30（オンライン）
- 被害状況共有ワーキンググループ会合
  日時：2025 年 4 月 18 日（金）16：00〜17：00（オンライン）
  日時：2025 年 5 月 9 日（金）16：00〜17：00（オンライン）
- 第 1 回証明書普及促進ワーキンググループ会合
  日時：2025 年 5 月 16 日（金）16：00〜17：30 （JPCERT/CC 会議室＋オンライン）
- フィッシング対策協議会　2025 年度総会
  日時：2025 年 6 月 17 日（火）15：00〜17：00（エッサム神田ホール 2 号館）

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へ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を行いました。

1. TECH+ セミナー 製造業× OT セキュリティ 2025 May. 工場・製造現場を守るセキュリティ事故の予防と対応策
   タイトル：事業継続のために必要なサイバー脅威への備え方～組織および工場関係者が行うべき事前準備と有事の相談先について～
   講演者：河野 一之（国内コーディネーショングループ 制御システムセキュリティ シニアアナリスト）
   主催：株式会社マイナビ TECH+ セミナー運営事務局
   講演日：2025 年 5 月 26 日
2. サイバーセキュリティ対策 2025 夏
   タイトル：サイバーセキュリティを「どこで」守るのか　－最近の攻撃事例から考えるゼロトラスト、サイバーハイジーン－
   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：SB クリエイティブ株式会社
   講演日：2025 年 6 月 6 日

8.2 協力・後援

本四半期は次の行事の開催に協力または後援等を行いました。

1. 第 29 回サイバー犯罪に関する白浜シンポジウム

主催：サイバー犯罪に関する白浜シンポジウム実行委員会
開催日：2025 年 5 月 22 日〜2025 年 5 月 24 日

2. Interop Tokyo 2025
   主催：Interop Tokyo 実行委員会
   開催日：2025 年 6 月 11 日〜2025 年 6 月 13 日
3. エッジ AI イニシアチブ 2025
   主催：アイティメディア株式会社
   開催日：2025 年 6 月 17 日〜2025 年 6 月 19 日

8.3 公開資料

JPCERT/CC が本四半期に公開した調査・研究の報告書やブログなどを記載しています。

8.3.1 インシデント報告対応レポート

JPCERT/CC では、国内外で発生するコンピューターセキュリティインシデントについて、報告の受け付けや、対応の支援、発生状況の把握、手口の分析、再発防止のための助言などを行っています。そうした活動の概要を紹介するために、インシデント報告数、報告されたインシデントの総数、報告に対応して JPCERT/CC が行った調整の件数などの統計情報、およびインシデントの傾向やインシデント対応事例を四半期ごとにまとめて、邦文および英文のレポートとして公表しています。なお、インシデント報告対応レポートによる公表は 2024 年度をもって終了しました。今後は本レポート「第 1 章 インシデント対応支援」をご参照ください。

- 2025-04-17
  JPCERT/CC インシデント報告対応レポート［2025 年 1 月 1 日〜2025 年 3 月 31 日］
  https://www.jpcert.or.jp/pr/2025/IR_Report2024Q4.pdf
- 2025-06-23
  JPCERT/CC Incident Handling Report [January 1, 2025 - March 31, 2025]
  https://www.jpcert.or.jp/english/doc/IR_Report2024Q4_en.pdf

8.3.2 インターネット定点観測レポート

JPCERT/CC では、インターネット上に複数のセンサーを分散配置し、不特定多数に向けて発信されるパケットを継続して収集するインターネット定点観測システム「TSUBAME」を構築・運用しています。センサーで観測されたパケットを分類し、脆弱性情報、マルウェアや攻撃ツールの情報などと対比して分析することで、攻撃活動やその準備活動の捕捉に努めています。こうしたインターネット定点観測の結果を四半期ごとにまとめて邦文および英文のレポートとして公表しています。

- 2025-06-06
  JPCERT/CC インターネット定点観測レポート［2025 年 1 月 1 日〜2025 年 3 月 31 日］

https://www.jpcert.or.jp/tsubame/report/report202501-03.html
https://www.jpcert.or.jp/tsubame/report/TSUBAME_Report2024Q4.pdf

- 2025-06-23
  JPCERT/CC Internet Threat Monitoring Report [January 1, 2025 - March 31, 2025]
  https://www.jpcert.or.jp/english/doc/TSUBAMEReport2024Q4_en.pdf

8.3.3 脆弱性関連情報に関する活動報告

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

- 2025-04-17
  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 1 四半期（1 月～3 月）］
  https://www.jpcert.or.jp/pr/2025/vulnREPORT_2025q1.pdf

8.3.4 公式ブログ「JPCERT/CC Eyes」

JPCERT コーディネーションセンター公式ブログ「JPCERT/CC Eyes」は、JPCERT/CC が分析・調査した内容、国内外のイベントやカンファレンスの様子などを JPCERT/CC のアナリストの眼を通して、いち早くお届けする読み物です。

本四半期においては次の 6 件の記事を公表しました。

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

- 2025-04-09
  RightsCon 2025 参加記
- 2025-04-24
  Ivanti Connect Secure に設置されたマルウェア DslogdRAT
- 2025-06-06
  TSUBAME レポート Overflow（2025 年 1～3 月）

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

- 2025-04-03
  JSAC2025 -Workshop & Lightning Talk-
- 2025-04-11
  ICS Security Conference 2025
- 2025-04-24

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 4 月 1 日〜2025 年 6 月 30 日 ］

- 発行履歴
  - 2025 年 7 月 17 日　初版
  - 2026 年 4 月 21 日　誤植修正
- 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/