JPCERT CC®

JPCERT/CC 四半期レポート

2026 年 4 月 1 日～2026 年 6 月 30 日

2026 年 7 月 16 日

一般社団法人 JPCERT コーディネーションセンター

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 8 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「 令和 8 年度サイバー対処能力の強化に向けたインシデント情報等に関する周知等の事務 」（内閣官房委託事業）として実施しています。

本レポートでは、 2026 年 4 月 1 日～2026 年 6 月 30 日　までの活動について報告しています。

なお、「第 4 章 国内連携活動」「第 5 章 国際連携活動」「第 6 章 フィッシング対策協議会活動」「第 7 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。

2026 年 10 月、JPCERT/CC は創立 30 周年の節目を迎えます。活動を支えてくださる皆さまに御礼申し上げます。

目次

トピックス＆ハイライト

2026 年度の JPCERT/CC 感謝状を贈呈

JPCERT/CC は、さまざまな国内のサイバー攻撃の被害を低減するために、インシデントへの対応支援活動、インシデントを未然に防ぐための早期警戒活動、マルウェア分析、ソフトウェア製品等の脆弱性に関する調整活動を行っています。これらの活動を進めるためには、皆さまからの情報提供やさまざまなご協力が必要です。JPCERT/CC では、そうした情報提供やご協力によってサイバーセキュリティ対策活動へ大きなご貢献をいただいた方へ感謝状を贈呈しています。

今年度は、オムロン株式会社 オムロン PSIRT 様へ感謝状をお贈りしました。

オムロン PSIRT 様は、製品セキュリティへの先進的な取り組みと豊富な脆弱性対応実績を通じて、他の製品開発者の模範となる活動をされてきました。また、JPCERT/CC の活動に対しても多方面にわたってご貢献いただきました。今年度の感謝状贈呈の詳細については次の Web ページで紹介しています。

- JPCERT/CC 感謝状 2026
  https://www.jpcert.or.jp/award/appreciation-award/2026.html

『インターネット定点観測レポート』を四半期レポートに統合

JPCERT/CC は、インターネット上に複数の観測用センサーを分散配置し、インターネット定点観測システム「TSUBAME」を構築、運営しています。TSUBAME で収集したデータは、脆弱性情報や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。TSUBAME の観測状況や分析結果は主に、『JPCERT/CC インターネット定点観測レポート』『JPCERT/CC 四半期レポート』「TSUBAME レポート Overflow（ブログ記事）」の形で、皆さまにお届けしてきました。これらのうち、『インターネット定点観測レポート』を本年度から『四半期レポート』に統合いたしました。この変更は、複数のレポートに内容が分散する、あるいは、内容や視点が曖昧になることを防ぎつつインターネット定点観測で得られた観測結果や知見を分かりやすくお伝えすることを目的としたものです。『インターネット定点観測レポート』をご覧いただいていた皆さまには、引き続きこの『JPCERT/CC 四半期レポート』を通じて知見をお伝えしていきます。また、これを契機に読者になられた皆さまには、インターネット定点観測やその結果の利活用について、新たな観点からのご意見ご感想をいただければ幸いです。

インターネット定点観測から得られた知見が、ご利用のシステムに内在する可能性がある不適切な設定や未対応の脆弱性などの問題点の発見とその対策行動に結び付くような、効果的な情報発信に引き続き努めます。

第 1 章

インシデント対応支援および脅威情報分析

1.1　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]。本節では、本四半期に受け付けたインシデント報告について、統計など定量的な観点と、特筆すべき事例を紹介します。

1.1.1　四半期の統計情報

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

本四半期に寄せられた報告件数は 14,056 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 3,398 件でした。前四半期と比較して、報告件数は 8% 減少、調整件数は 7% 増加しました。また、前年同期（報告件数は 14,558 件、調整件数は 3,544 件）と比較すると、報告数は 3% 減少、調整件数は 4% 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。

表 1.1 インシデント報告等の月別件数

	4 月	5 月	6 月	合計	前四半期合計
報告件数	5,432	4,770	3,854	14,056	15,345
インシデント件数	3,691	2,201	3,413	9,305	10,262
調整件数	1,296	799	1,303	3,398	3,168

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

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

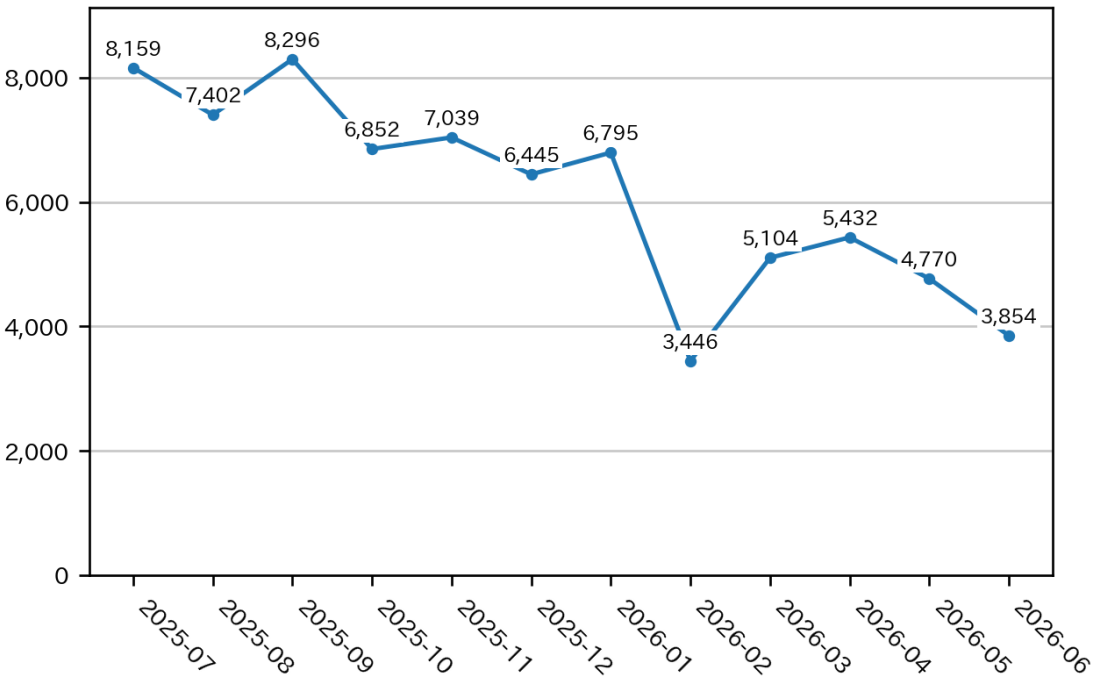


図 1.1 インシデント報告件数の推移

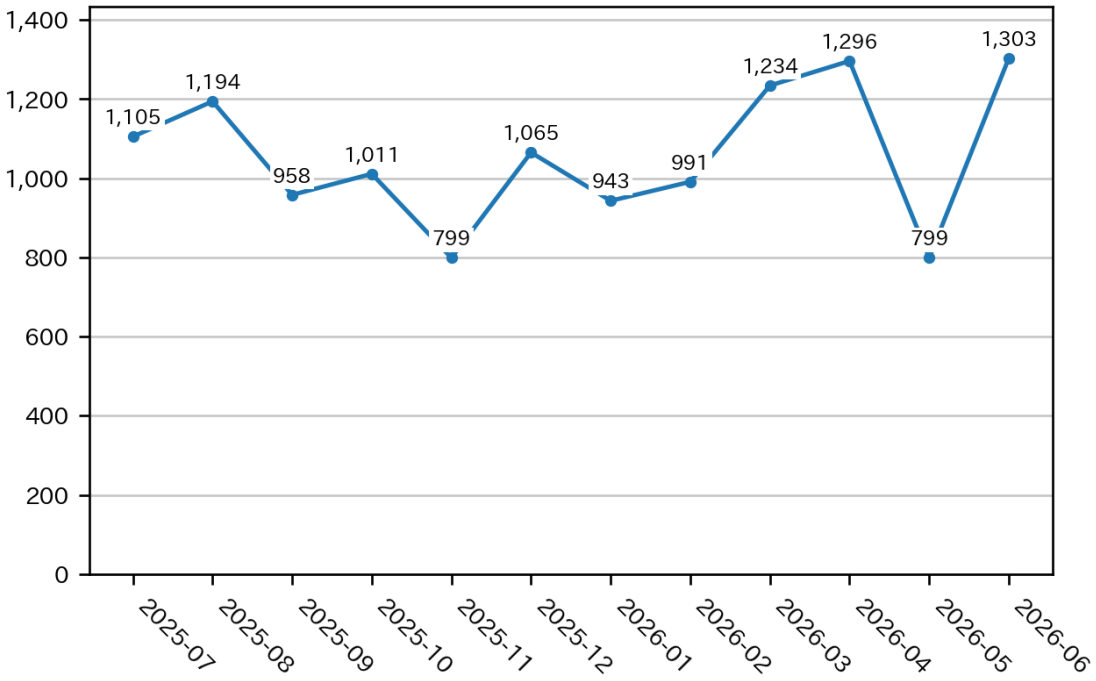


図 1.2 インシデント調整件数の推移

表 1.2 インシデント報告件数のカテゴリー別内訳

インシデント	4 月	5 月	6 月	合計	前四半期合計
フィッシングサイト	3,352	1,928	3,033	8,313	9,293
Web サイト改ざん	46	55	80	181	90
マルウェアサイト	3	13	5	21	32
スキャン	73	42	75	190	156
DoS/DDoS	1	0	0	1	4
ランサムウェア	3	3	2	8	0
制御システム関連	0	1	0	1	0
標的型攻撃	3	4	1	8	2
その他	210	155	217	582	685

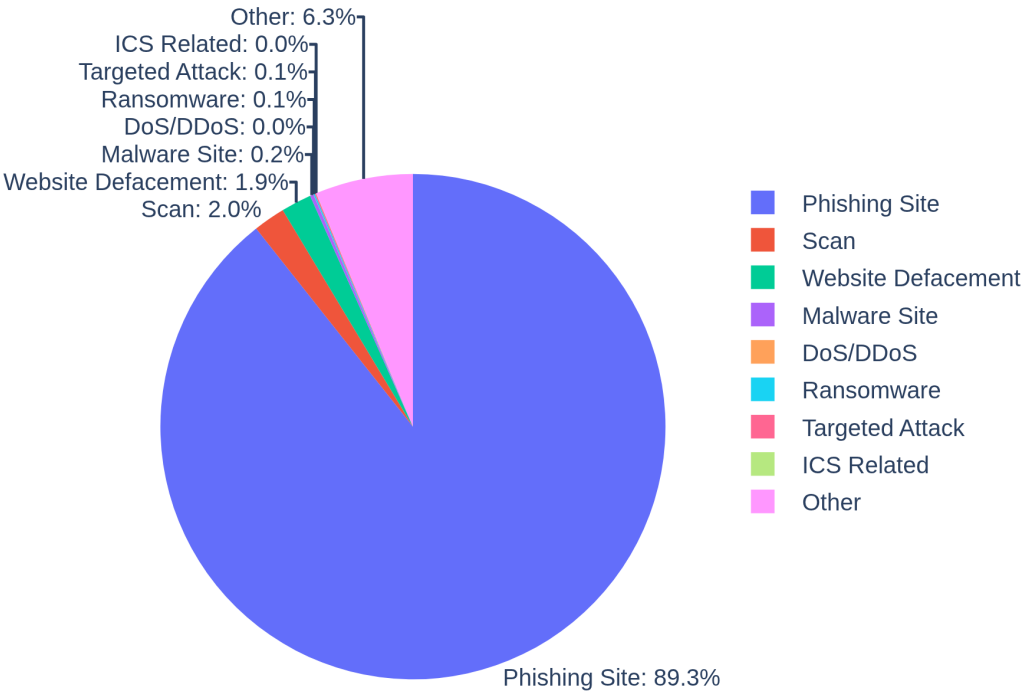


図 1.3 インシデント報告件数のカテゴリー別割合

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。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 89.3% 、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 2.0% 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。

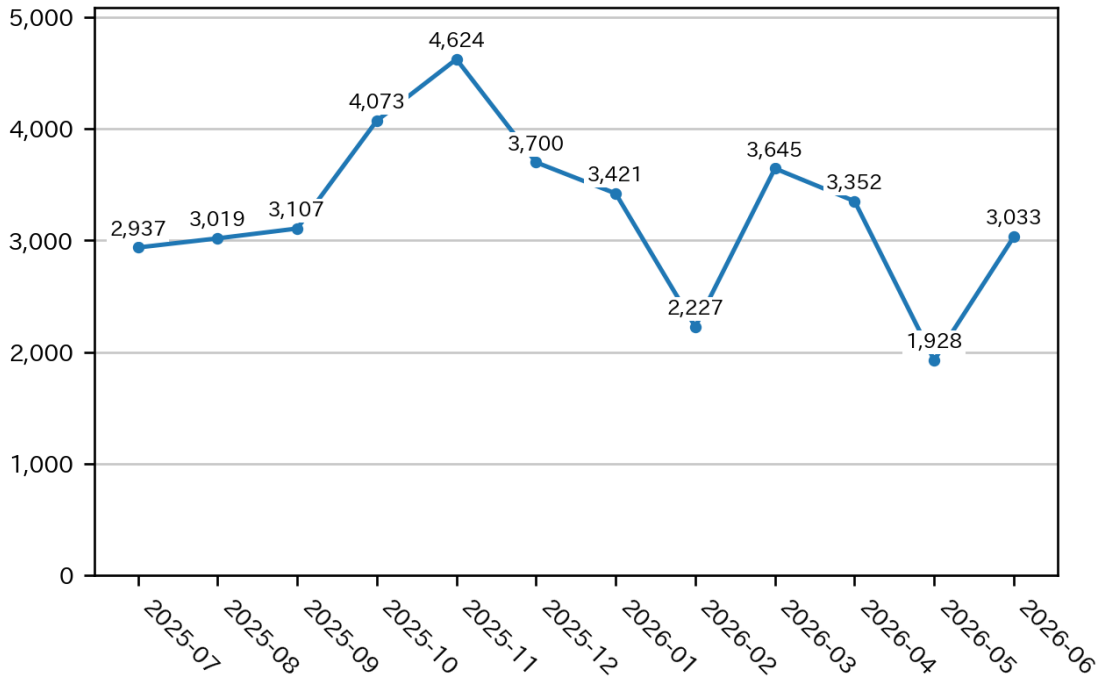


図 1.4 フィッシングサイト件数の推移

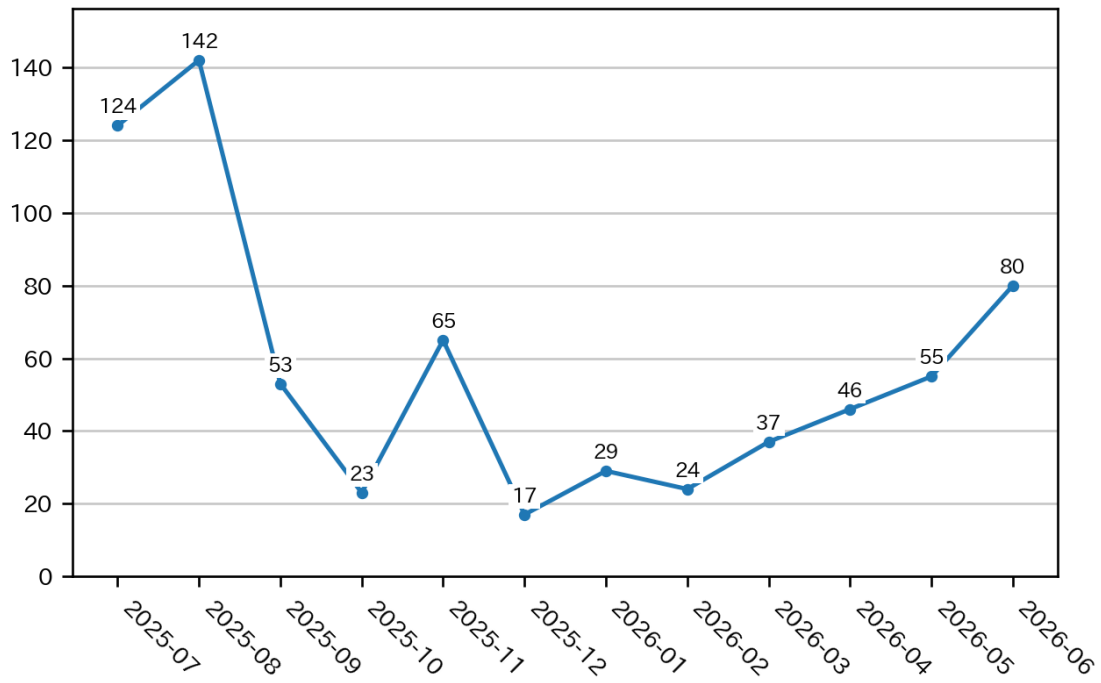


図 1.5 Web サイト改ざん件数の推移

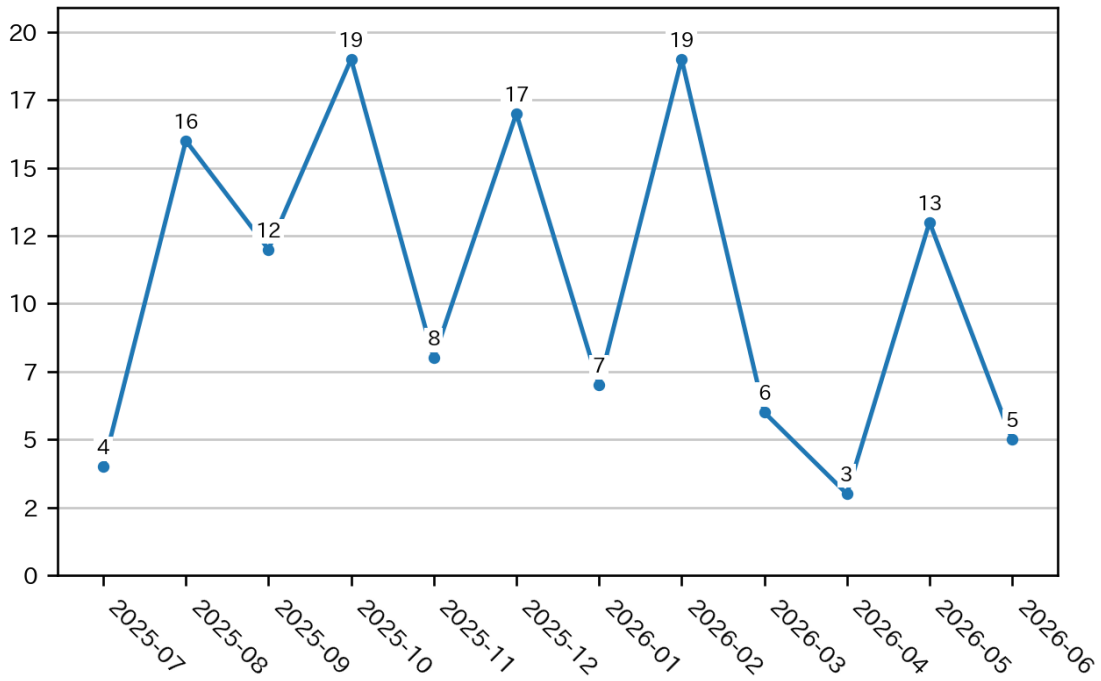


図 1.6 マルウェアサイト件数の推移

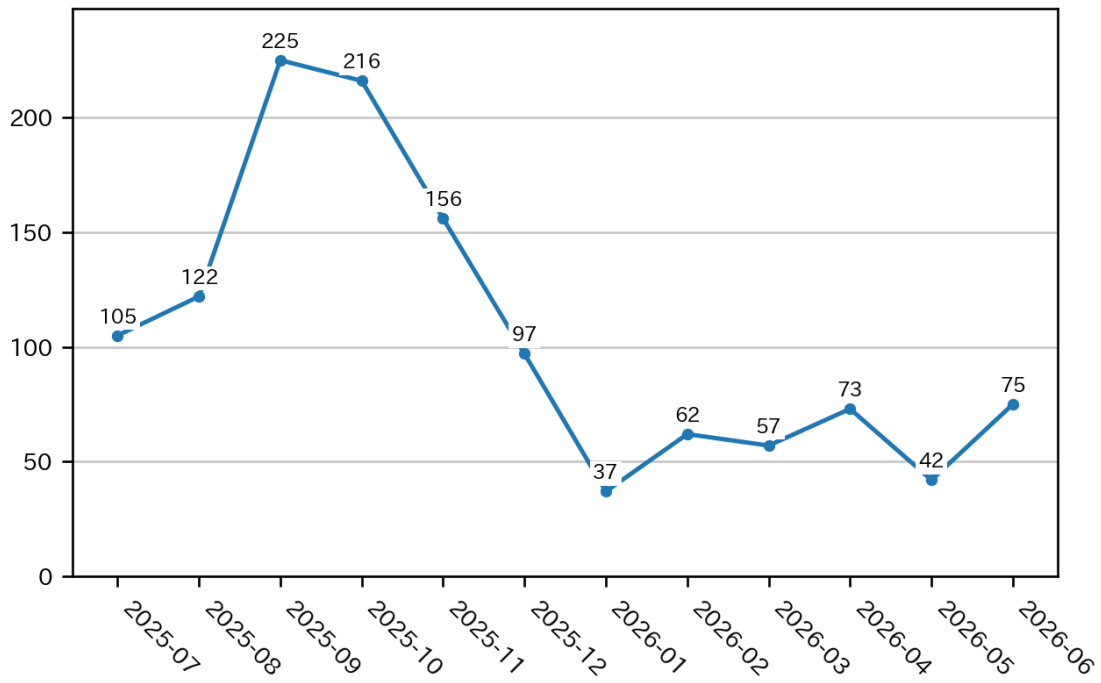


図 1.7 スキャン件数の推移

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	2,767	1,446	1,761	5,974	72%
国外ブランド	239	217	632	1,088	13%
ブランド不明	346	265	640	1,251	15%
全ブランド合計	3,352	1,928	3,033	8,313	

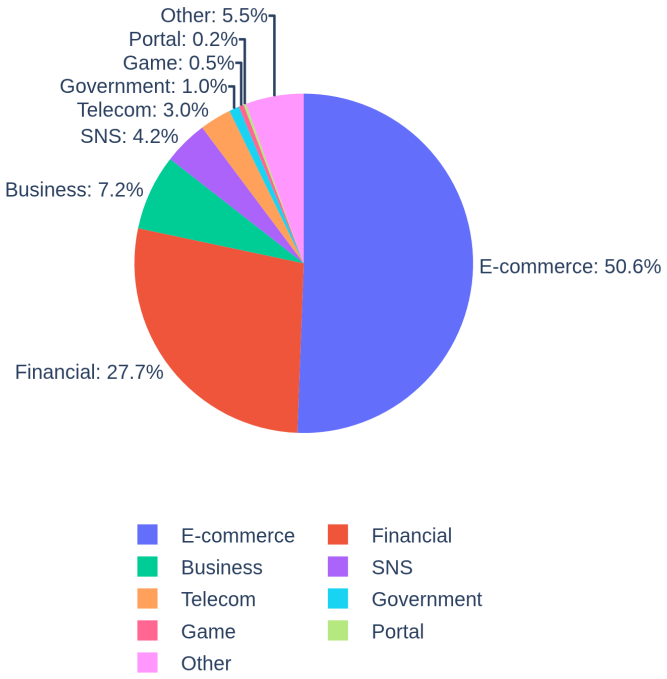


図 1.8 国外ブランドのフィッシングサイトの件数の業界別の割合

1.1.2 インシデントの傾向

1.1.2.1 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 8,313 件で、前四半期の 9,293 件から 11% 減少しました。また、前年同期（7,358 件）との比較では、13% 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は 1,088 件で、前四半期の 899 件から 21% 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 5,974 件で、前四半期の 7,112 件から 16% 減少しました。

本四半期のブランドの国内外別によるフィッシングサイト件数の内訳[*3] を表 1.3 に、国外ブランドと国内ブランドそれぞれのフィッシングサイト件数の業界別の割合を図 1.8 と図 1.9 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

[*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。

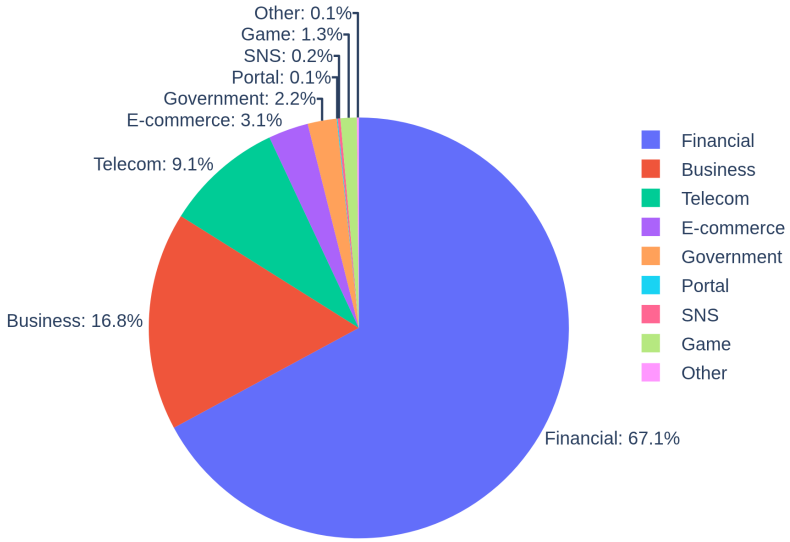


図 1.9 国内ブランドのフィッシングサイトの件数の業界別の割合

トを装ったものが 50.7%、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 67.1% で、それぞれ最も多くを占めました。

国外ブランドでは、Amazon、Apple Account、VISA 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、セゾンカード、マネックス証券、SBI 証券、三井住友カード、楽天を装ったフィッシングサイトの報告が多く寄せられました。

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 93%、国内が 7% でした。

1.1.2.2 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 181 件でした。前四半期の 90 件から 101% 大幅に増加しました。

本四半期は、次のような Web サイト改ざん事例を確認しています。

- 事例 1：正規 Web サイトで海外オンラインカジノのコンテンツが表示される事例
- 事例 2：正規 Web サイトに不審なログインページと遠隔操作ツールが設置された事例

事例 1 では、国内の複数の正規 Web サイトが改ざんされ、検索エンジンが利用するユーザーエージェント（Googlebot）でアクセスした場合に、海外のオンラインカジノのコンテンツが表示される状態になっていました。これは、海外のオンラインカジノサイトを検索結果の上位に表示させることを目的とした、SEO ポイズニングであると考えられます。

事例 2 では、国内の正規 Web サイトが改ざんされ、不審なログインページが設置されていました。当該サイトはボイスフィッシングの誘導先として報告されていましたが、それは攻撃者がインターネットバンキングの認証情報の窃取を目的として設置したログインページによるものと考えられます。また、改ざんされた Web サイトには遠隔操作ツールも設置されており、認証情報の窃取とは別にユーザーを遠隔

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

操作しようとしていた可能性があります。

1.1.2.3 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 8 件でした。

正規クラウドサービスを悪用した標的型攻撃メール

本四半期は、攻撃グループ APT-C-60 が関与した可能性がある標的型攻撃メールの報告が複数寄せられました。標的型攻撃メールに記載された Proton Drive のリンクにアクセスすると RAR ファイルをダウンロードさせられます。RAR ファイル内に含まれる LNK ファイルを開くと、GitHub や GitLab などの正規クラウドサービスからマルウェアがダウンロードされて、感染します。

1.1.2.4 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 21 件でした。前四半期の 32 件から 34% 減少しています。

本四半期に報告が寄せられたスキャン件数は 190 件でした。前四半期の 156 件から 22% 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)、HTTP（80/TCP)、HTTPS（443/TCP)、81/TCP でした。

その他に分類されるインシデントの件数は 582 件でした。前四半期の 685 件から 15% 減少しました。

1.2　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。

1.2.1　情報収集・分析

JPCERT/CC が収集・分析する情報には、自ら収集した情報に加え、ご報告いただいた国内外で発生するインシデントの情報や、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、情報共有プラットフォーム「CISTA（Collective Intelligence Station for Trusted Advocates)」（1.2.3 参照）を介した各組織からのフィードバックは、他組織へも展開するなど有効活用しています。

1.2.2　Web サイトでの情報提供

JPCERT/CC は、Web サイトで「注意喚起」や「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、JPCERT/CC が運用する情報配信用メーリングリストの登録者（本四半期末時点で約 43,000 名）には、一部の情報をメールでも配信しています。

1.2.2.1　注意喚起

深刻かつ影響範囲の広い脆弱性などが公表された場合には、「注意喚起」を公開し、利用者に対して広く対策を呼びかけています。

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

本四半期は、12 件公開または更新しました。
以下、期間中に公開または更新した情報を、最終更新日順に一覧で記載します。

- 2026-04-13
  Adobe Acrobat および Reader の脆弱性（APSB26-43）に関する注意喚起
- 2026-04-15
  2026 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
- 2026-04-15
  Adobe Acrobat および Reader の脆弱性（APSB26-44）に関する注意喚起

- 2026-04-27
  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
- 2026-05-13
  2026 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
- 2026-05-13
  GUARDIANWALL MailSuite 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
- 2026-05-21
  TrendAI Apex One などのトレンドマイクロ製品における複数の脆弱性に関する注意喚起
- 2026-05-22
  Palo Alto Networks 製 PAN-OS における認証回避の脆弱性（CVE-2026-0265）に関する注意喚起
- 2026-06-10
  Check Point Software Technologies 社製品における認証バイパスの脆弱性（CVE-2026-50751）に関する注意喚起
- 2026-06-10
  2026 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
- 2026-06-10
  Adobe Acrobat および Reader の脆弱性（APSB26-63）に関する注意喚起
- 2026-06-23
  Fortinet 製品に関連する認証情報の漏えいに関する注意喚起

1.2.2.2 Weekly Report

JPCERT/CC が収集したセキュリティ関連情報のうち重要と判断した情報の概要をまとめ、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 件公開しました。

- JPCERT/CC Weekly Report
  https://www.jpcert.or.jp/wr/

1.2.3 CISTA での情報提供

JPCERT/CC は、サイバーセキュリティに関する脅威情報や分析・対策情報を、各組織のサイバーセキュリティ関連部門や組織内 CSIRT などの方々が共有する場として、情報共有プラットフォーム「CISTA」を運営しています。CISTA は JPCERT/CC の取り組みにご賛同いただける組織を対象とした登録制としています。

CISTA については、次の Web ページをご参照ください。

- CISTA（シスタ）
  https://www.jpcert.or.jp/cista/

CISTA では、JPCERT/CC が提供した情報に対して、受信組織が JPCERT/CC 宛てにフィードバック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、許可された共有範囲などに応じて、他組織への情報提供などに活用、還元しています。

1.2.3.1 早期警戒情報

収集した脆弱性情報や脅威情報などのうち、重要な情報インフラなどに重大な影響を及ぼす可能性があり、重要インフラなどを提供する組織に迅速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 3 件発信しました。

1.2.3.2 Analyst Note

収集した脆弱性情報や脅威情報などのうち、JPCERT/CC が注目すべきと考えたものを、毎日まとめて「Analyst Note」として提供しています。

本四半期は 61 件発信しました。

1.2.3.3 インディケータ情報

国内の組織に対して行われた攻撃活動のうち、特定の組織や業界を標的としたと考えられるものについては、関係組織の許可を得た上で、把握していない被害の発見や被害防止を目的として、「インディケータ情報」として攻撃を検知するための情報を提供しています。

本四半期は 8 件提供しました。

1.2.3.4 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などの「脆弱なホスト」や、すでに脆弱性の悪用によって不正プログラム設置や改ざん、認証情報の窃取がな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 38 件提供しました。先述の脆弱性情報や脅威情報などの影響を受けるホストを管理する組織に対して情報提供を行いました。

1.2.4 対応事例

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、調整・対応した脆弱性や脅威情報のうち、特徴的なものを紹介します。

1.2.4.1 cPanel、WHM における認証バイパスの脆弱性（CVE-2026-41940）

WebPros International が、2026 年 4 月 28 日に cPanel および WHM における認証バイパスの脆弱性（CVE-2026-41940）に関するアドバイザリ[*4]を公表しました。本脆弱性は、cPanel および WHM において認証を回避される脆弱性であり、悪用された場合、攻撃者が当該製品の root 権限を取得します。当該製品の稼働状況を調査したところ、国内で約 2,000 台が稼働しており 、ホスティング事業者の管理下にあるホストの割合が高いことを確認しました。当該製品は、ホスティング事業者がサーバーなどを管理するために利用しているケースが多く、共有ホスティング環境で採用されている場合、侵害の範囲によっては同居する全テナントが影響を受ける可能性が高いため、JPCERT/CC が参加する、ホスティング事業者などで構成されたコミュニティーに対し対処状況を確認するようお願いしました。

アドバイザリ公表の翌日には本脆弱性の実証コード（Proof-of-Concept）を含む技術詳細[*5]をセキュリティ企業が公開し、翌々日以降から本脆弱性の悪用によって Sorry ランサムウェアを展開する攻撃や、Mirai マルウェアの亜種を配布するために悪用されているとの観測情報などが相次ぎました[*6][*7]。さらに、2026 年 2 月以降、本脆弱性がゼロデイとして悪用されていたことも報告されており、公開された実証コードから悪用の難易度も低いと考えられ、さらに広く悪用されることが懸念されました。また、Sorry ランサムウェアによる被害に関して国内組織から報告を受領しました。被害組織は、ホスティング事業者のテナントとして、同事業者が提供するサービスを通じて当該製品を利用していました。被害組織は、同事業者に対して痕跡調査への協力を求めましたが、利用契約上の制約を理由に協力を得られず、十分な痕跡調査を実施するには至りませんでした。加えて、連携する海外組織から当該製品を利用している国内ホスト約 80 台が不審な通信を行っているとの情報[*8]を受領しました。これらのホストについて、本脆弱性の影響を受けている可能性を踏まえ、対象組織に対して個別に通知し、本脆弱性への対処を促しました。

[*4] “WebPros International Security: CVE-2026-41940 - cPanel & WHM / WP2 Security Update 04/28/2026”. cPanel. https://support.cpanel.net/hc/en-us/articles/40073787579671-Security-CVE-2026-41940-cPanel-WHM-WP2-Security-Update-04-28-2026, (2026-04-28)

[*5] “watchtowr The Internet Is Falling Down, Falling Down, Falling Down (cPanel & WHM Authentication Bypass CVE-2026-41940)”. watchTowr. https://labs.watchtowr.com/the-internet-is-falling-down-falling-down-falling-down-cpanel-whm-authentication-bypass-cve-2026-41940/, (2026-04-29)

[*6] “The cPanel Situation Is. . . ”. Censys. https://censys.com/blog/the-cpanel-situation-is/, (2026-05-01)

[*7] “Critrical cPanel flaw mass-exploited in”Sorry” ransomware attacks”. Bleeping Computer. https://www.bleepingcomputer.com/news/security/critrical-cpanel-flaw-mass-exploited-in-sorry-ransomware-attacks/, (2026-05-02)

[*8] “ShadowServer HIGH: Darknet Events Report”. https://www.shadowserver.org/what-we-do/network-reporting/honeypot-darknet-events-report/

1.2.4.2 GUARDIANWALL MailSuite 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-2026-32661）

JPCERT/CC は、キヤノンマーケティングジャパンが提供する企業向け統合メールセキュリティソリューション「GUARDIANWALL MailSuite」の脆弱性に関する報告を受けました。同製品利用者の環境でインシデントが発生し、その調査の過程で脆弱性を発見したとして報告されたものでした。本脆弱性は当該製品の Web サービスに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るもので、インターネット経由で外部からの侵害につながる可能性があり、本脆弱性を悪用する攻撃の被害を受ける組織の拡大が懸念されました。そのため、被害拡大を防止するための対策情報や攻撃に関する情報の流通のため、JPCERT/CC は報告者および製品開発者との調整を行いました。脆弱性の調整に関する詳細については 3.1.2.1 をご参照ください。製品開発者が脆弱性情報（CVE-2026-32661）[*9]を公表した 2026 年 5 月 13 日に、JPCERT/CC は JVN アドバイザリ[*10]を公表し、注意喚起[*11]を公開しました。注意喚起では、影響を受ける製品の利用組織に対し、修正パッチの適用に加え、すでに侵害を受けている可能性も考慮して侵害有無の確認、必要なログの保全および回避策の実施を呼びかけました。また、報告者から提供を受けた攻撃に関する情報については、利用組織による調査や被害把握を支援することを目的に、インディケータ情報として CISTA 利用組織へ共有しました。

1.2.4.3 Cisco Catalyst SD-WAN コントローラにおける認証バイパスの脆弱性（CVE-2026-20182）

Cisco が、2026 年 5 月 14 日、Cisco Catalyst SD-WAN コントローラにおける不適切な認証の脆弱性（CVE-2026-20182）に関するアドバイザリ[*12]を公表しました。本脆弱性は、Cisco Catalyst SD-WAN Controller おいて認証を回避される脆弱性であり、公表時点ですでに本脆弱性の悪用を観測していることに言及されていました。 攻撃者は本脆弱性を悪用することで、Cisco Catalyst SD-WAN コントローラにおいて内部での高い権限を持つ非ルートユーザーアカウントとしてログインする可能性があります。

また、攻撃者が認証を回避して接続を確立した際の認証完了を示すログが、正規のピアによるものと同一の形式で記録されるため、ログの確認のみでは侵害の検知が困難であることが考えられます。攻撃者は、確立した非ルートユーザーアカウントを用い NETCONF にアクセスし、結果として SD-WAN ファブリックのネットワーク構成を操作する可能性があります。

本製品に関しては、2026 年 2 月にも認証バイパスの脆弱性（CVE-2026-20127）が公開されており、かつ 2023 年からゼロデイ悪用が続いていたことが Cisco Talos の調査によって推定されています。JPCERT/CC は、攻撃者が引き続き本製品を標的にすることを想定し、国内において本脆弱性の影響を受ける状態でインターネットへ露出しているホストを把握するための調査を実施しました。しかし、本脆弱性の対象となるサービスは SD-WAN 機器間の制御接続に用いられるものであり、Web 応答やバナー

[*9] “GUARDIANWALL MailSuite 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ついて”. キヤノン IT ソリューションズ株式会社. https://security-support.canon-its.jp/info_and_news/show/804?site_domain=GUARDIANWALL, (2026-05-13)

[*10] “JVN#35567473: GUARDIANWALL MailSuite 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”. Japan Vulnerability Notes. https://jvn.jp/jp/JVN35567473/, (2026-05-13)

[*11] “GUARDIANWALL MailSuite 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 コーディネーションセンター（JPCERT/CC）. https://www.jpcert.or.jp/at/2026/at260013.html, (2026-05-13)

[*12] “Cisco Catalyst SD-WAN Controller Authentication Bypass Vulnerability”. Cisco. https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-rpa2-v69WY2SW, (2026-05-14)

のような特徴的な応答が得られにくいため、本製品の稼働状態はスキャンサービスでは網羅的に捕捉できず、実態の把握には限界があることから、Cisco と連携して国内の利用状況を把握することで調査結果を補いました。

また、Cisco は 2026 年 6 月 4 日に Cisco Catalyst SD-WAN Manager の認証済み特権昇格の脆弱性（CVE-2026-20245）のアドバイザリ[*13]を公表し、CVE-2026-20182 を含む他の脆弱性などとの悪用の連鎖によって、未認証の攻撃者が同製品上で特権を得る攻撃シナリオを示唆しています。

JPCERT/CC は、国内組織から同製品の侵害が関わる事案の報告を受け、調査を支援していました。当該組織から受領した情報や侵害された機器のログなどの分析を行った結果、攻撃者により CVE-2026-20245 を悪用した可能性がうかがわれる痕跡が 2026 年 4 月時点のログに確認され、管理者権限アカウントの追加、作成した管理者権限を利用した内部ネットワークのルーターの WebUI へのログインおよび設定変更操作を実施した痕跡も確認しました。分析から得られたインディケータ情報は当該組織へ還元するとともに、JPCERT/CC が連携する国際的なコミュニティーなどへ情報を共有しました。

[*13] “Cisco Catalyst SD-WAN Manager Authenticated Privilege Escalation Vulnerability”. Cisco. https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-privesc-4uxFrdzx, (2026-06-04)

第 2 章

インターネット上の探索活動や攻撃活動に関する観測と分析

JPCERT/CC では、不特定多数に向けて発信されるパケットを収集する観測用センサーを開発し、これをホスティングサービス等を利用することで国内外に複数分散配置して、インターネット定点観測システム「TSUBAME」を構築し運用しています。センサーによって受信されるパケットは、特定の機器や特定のサービス機能を探索するために行われていると考えられます。 JPCERT/CC では、センサーで観測されたパケットを継続的に収集し、脆弱性情報、マルウェアや攻撃ツールの情報などと照らしあわせて分析しています。その分析から、インターネットを介した攻撃活動や、攻撃の準備活動等を把握できる場合があり、グローバルな攻撃活動等の迅速な把握に努めています。

2.1　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、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 TCP、UDP および ICMP パケットを収集しています。なお、センサーはハニーポットとは異なり、到達したパケットに対して応答しません。

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

2.1.1　TSUBAME の観測データの活用

JPCERT/CC では、組織のシステム管理者の方々がインシデント対応や対策などに活用できるよう、「TSUBAME」で得た観測データを提供しています。観測データに基づいた個別の情報提供の他、四半期ごとに『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」を公開してきました。従来『インターネット定点観測レポート』で提供してきた内容は、本四半期分から本レポート第 2 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」に掲載しています。また、ブロ

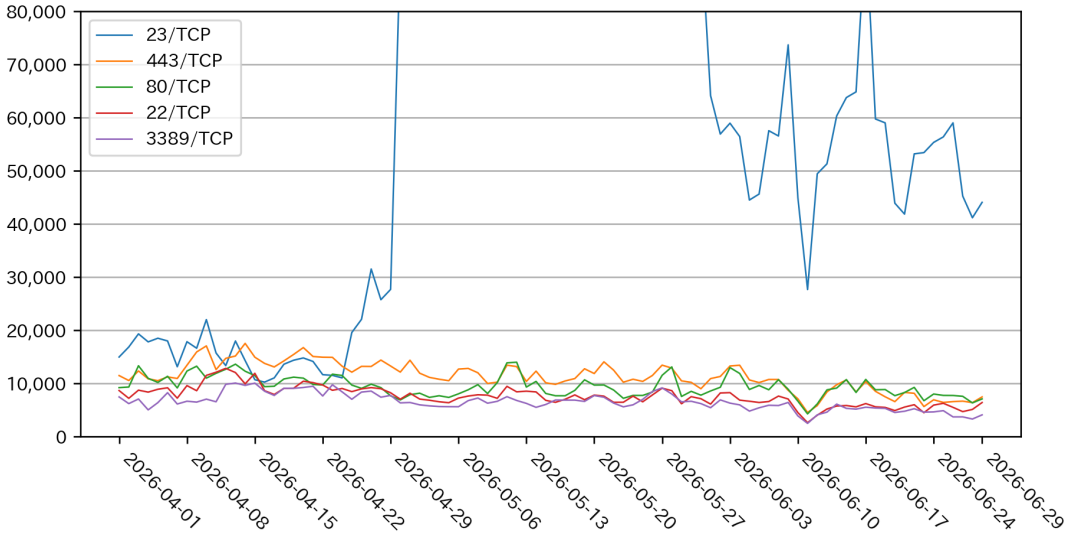


図 2.1 TSUBAME で観測された宛先ポートの上位 1 位〜5 位のパケット数

グ「TSUBAME レポート Overflow」では、引き続き、本レポートに掲載しきれない分析内容や期間中に発生した特徴的な事象を取り上げます。

- JPCERT/CC インターネット定点観測レポート
  - インターネット定点観測レポート（2026 年 1〜3 月）
    https://www.jpcert.or.jp/tsubame/report/report202601-03.html
- TSUBAME レポート Overflow
  - TSUBAME レポート Overflow（2025 年 10〜12 月）
    https://blogs.jpcert.or.jp/ja/2026/05/tsubame-overflow20251012.html
  - TSUBAME レポート Overflow（2026 年 1〜3 月）
    https://blogs.jpcert.or.jp/ja/2026/06/tsubame-overflow20260103.html

2.1.2 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の件数を宛先ポート別に集計[*1]したものを図 2.1 に示します。自組織のネットワークに届くパケットの傾向を分析する際に参考にしてください。

本四半期に最も多く観測されたパケットは 23/TCP（Telnet）宛てで、2026 年 5 月上旬に Mirai の特徴を持つパケットの突発的な増加が見られましたが、その後は少しずつ減少しています。2 位は 443/TCP でした。3 位は 80/TCP、4 位は 22/TCP で、前四半期から順位が入れ替わりました。5 位には 3389/TCP が入りました。頻繁に探索された国内のサービス（宛先ポート番号）のトップ 5 を表 2.1 に、探索元地域のトップ 5 を表 2.2 に示します。

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

表 2.1 頻繁に探索された国内のサービス（宛先ポート番号）のトップ 5

順位	宛先ポート番号	前四半期の順位
1	Telnet（23/TCP）	1
2	https（443/TCP）	3
3	http（80/TCP）	2
4	ssh（22/TCP）	5
5	rdp（3389/TCP）	6

表 2.2 探索元地域トップ 5

順位	探索元地域	前四半期の順位
1	米国（US）	1
2	オランダ（NL）	4
3	英国（GB）	8
4	ドイツ（DE）	6
5	ルーマニア（RO）	7

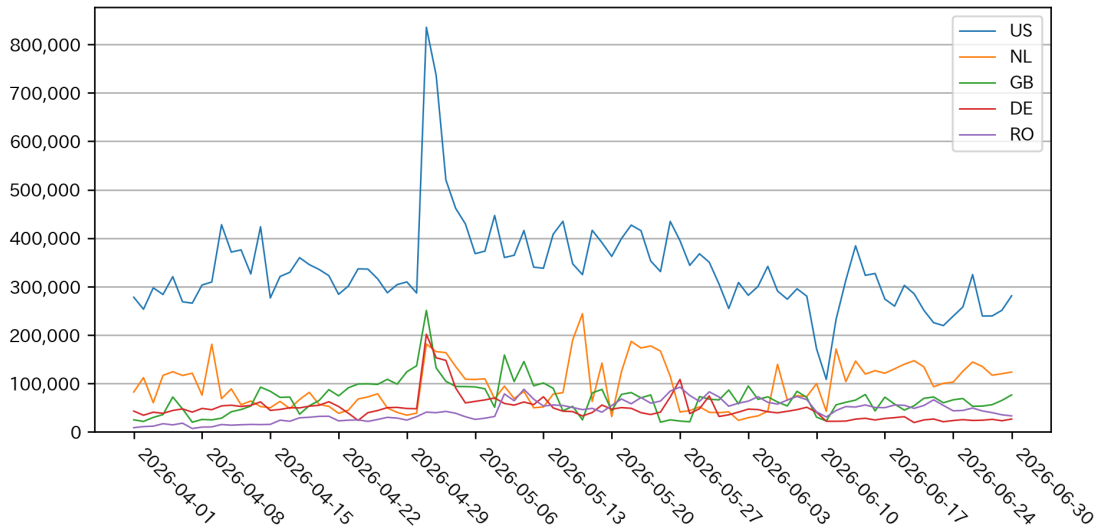


図 2.2 探索元地域からのパケット数の推移

表 2.1 に示したサービスを探索するパケット観測数の推移を図 2.1 に示します。

国内を対象とした探索活動の探索元地域を、本四半期において活動が活発だった順に並べたトップ 5 を表 2.2 に示します。

トップは米国、オランダが 2 番目に入りました。3 番目以降は、英国、ドイツ、ルーマニアといずれも前四半期では TOP5 以降だった地域が入りました。なお、TSUBAME では RIR（Regional Internet Registry）による割り当て情報を用いて個々の IP アドレスの地域を判断しています。

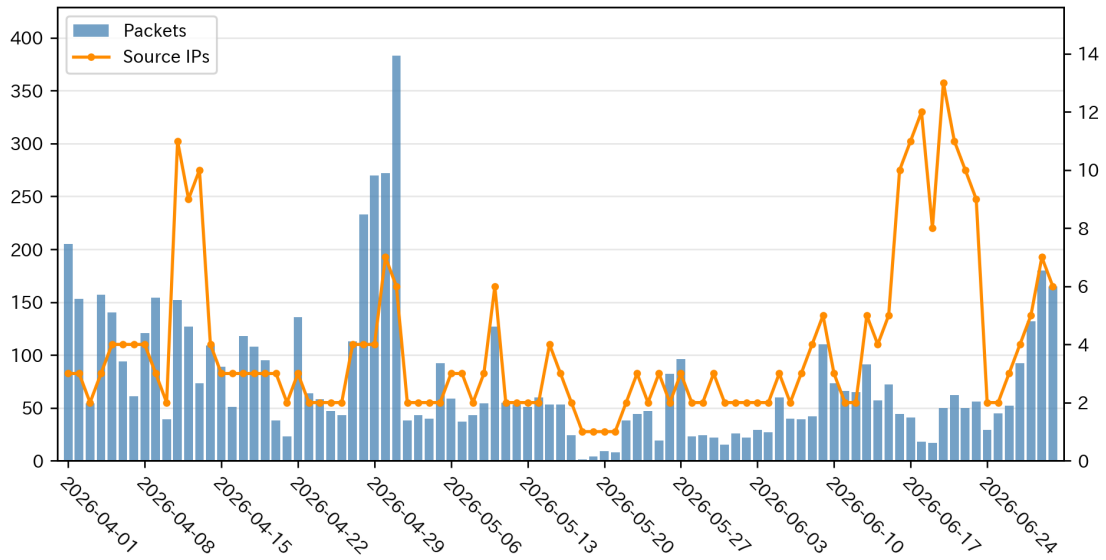


図 2.3 CVE-2025-55182 を狙った攻撃活動の観測数

2.2 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。

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

前四半期に引き続き、React Server Components の脆弱性（CVE-2025-55182）を標的とする攻撃パケットが継続的に観測されています（図 2.3）。

ペイロードに含まれる攻撃コードには複数のバリエーションが見られ、攻撃者による改良が続けられている状況がうかがえます。本脆弱性を悪用した攻撃活動は今後も継続する可能性が高く、引き続き注意が必要です。

2.2.2 LLM 関連フレームワークの脆弱性を狙う通信

n8n におけるコード実行の脆弱性（CVE-2026-21858）や llama-cpp-python / SGLang におけるコード実行の脆弱性（CVE-2024-34359 / CVE-2026-5760）といった、LLM と連携するフレームワークやライブラリの脆弱性を標的とした攻撃パケットやスキャンパケットが、2026 年 4 月下旬ごろから散発的に観測されています。

LLM と連携する開発基盤はインターネットとの通信経路を持つことが比較的多いと考えられます。脆弱性の修正を適用するだけでなく、通信を適切に制御するなど、多層的な防御を意識した対策が重要です。

第 3 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。

3.1 脆弱性関連情報の取り扱い状況

3.1.1 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 番号を付与しています。

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。

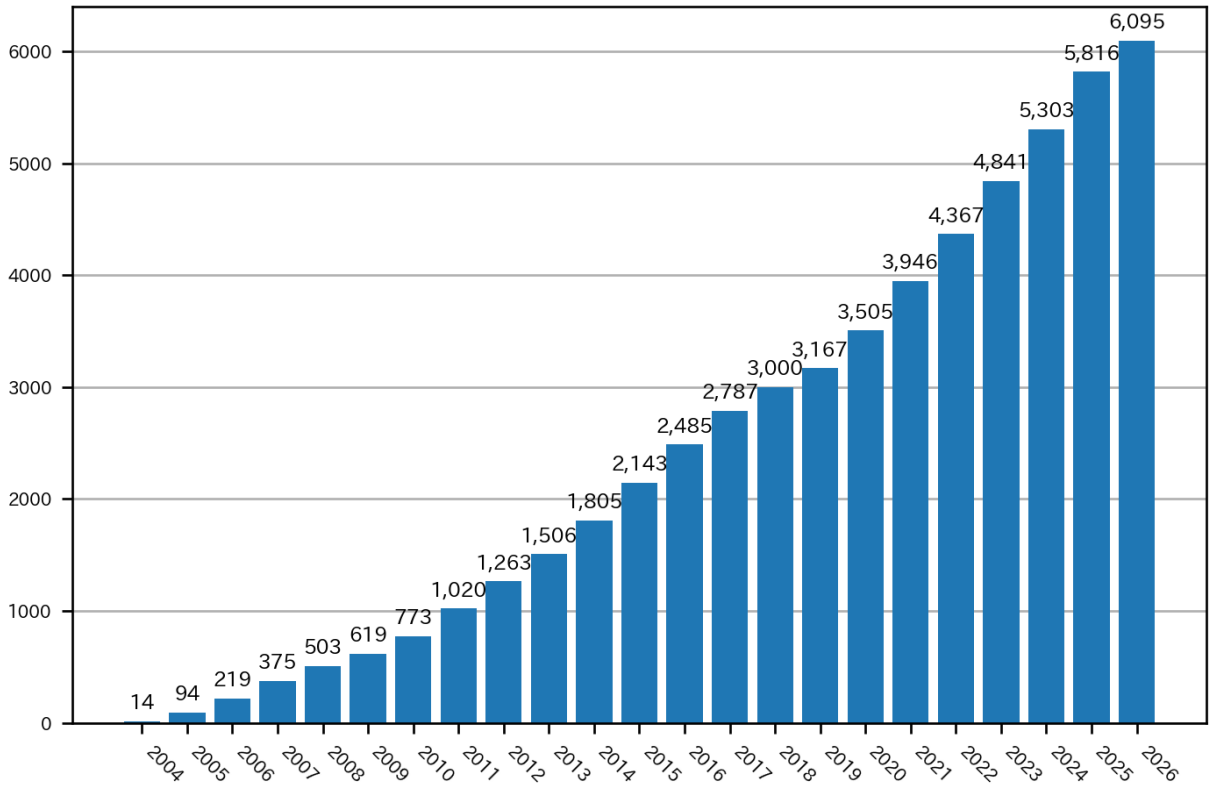


図 3.1 JVN 公表累積件数

3.1.2 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 111 件、累積 6,095 件で、累積の推移は図 3.1 のとおりです。

本四半期に公表された個々の脆弱性情報については、次の Web サイトをご参照ください。

- 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：44 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：67 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

3.1.2.1 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#35567473 GUARDIANWALL MailSuite 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#35567473 GUARDIANWALL MailSuite 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/JVN35567473/

キヤノンマーケティングジャパンが提供する企業向け統合メールセキュリティソリューション「GUARDIANWALL MailSuite」の脆弱性です。本製品は、公的機関や重要インフラの運用を担う企業などを含む、国内の多くの組織で利用されています。

この脆弱性は、製品利用者の環境で発生したインシデントを調査する過程で発見したとして製品開発者から報告されました。攻撃者によって細工されたリクエストが送信されるとスタックベースのバッファーオーバーフローが引き起こされ、認証なしで任意のコードが実行される可能性があるというものです。悪用された場合、機密性・完全性・可用性すべてに深刻な影響が及ぶ恐れがあり、利用者の混乱のみならずより大きな被害につながる可能性があります。なお、製品利用者の環境でこの脆弱性の悪用が確認されていたため、JVN アドバイザリ公表に際しては、表題に「緊急」と表示し、悪用が確認されたことを詳細情報に記載して、利用組織に迅速な対応を促しました。また、本アドバイザリ公表後、本件に関する警戒情報として注意喚起を公開し、利用者にさらなる注意を呼び掛けました。注意喚起については 1.2.4.2 をご参照ください。

JVN#00263243、JVN#57877356 JPCERT/CC が提供するツール（EmoCheck、LogonTracer）の脆弱性対応

- JVN#00263243 EmoCheck における DLL 読み込みに関する脆弱性
  https://jvn.jp/jp/JVN00263243/
- JVN#57877356 LogonTracer における複数の脆弱性

https://jvn.jp/jp/JVN57877356/

両件は、JPCERT/CC が提供するツールの脆弱性に関する情報です。情報セキュリティ早期警戒パートナーシップを通じて報告を受け、JPCERT/CC が製品開発者として脆弱性の修正と関連情報の流通を実施しました。DLL 読み込みに関する脆弱性が存在するとの報告を受けた EmoCheck は、2019 年ごろに発生した Emotet の感染拡大に対抗するために 2020 年 2 月に公開した感染チェックを行うためのツールです。Emotet の脅威がなくなったため、脆弱性報告を機に配布を終了するとともに、利用停止を呼び掛けました。イベントログの分析をサポートするツールである LogonTracer は、脆弱性への対策を行った v2.0 をリリースしました。

JPCERT/CC では、この度の対応を今後の活動に生かし、製品開発者の皆さまに寄り添いながらより質の高い調整を目指してまいります。

3.1.2.2 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。

3.1.2.3 脆弱性調整に関連するその他の特筆すべき事項

海外のベンダーや CERT 組織が公表するセキュリティアドバイザリに基づき JVN で公表する日本語アドバイザリの形式変更について、紹介します。

JVNVU#96777324 Intel 製品に対するアップデート（2026 年 5 月）

- JVNVU#96777324 Intel 製品に対するアップデート（2026 年 5 月）
  https://jvn.jp/vu/JVNVU96777324/

JPCERT/CC はこれまで、Intel、Siemens、Apache などの OSS プロジェクトや、米国 CERT/CC、CISA ICS が発行する情報を邦訳し、識別子「JVNVU#8 桁の番号」を付けたアドバイザリとして JVN で公表してきました。しかし、自動翻訳サービスが普及したことから、JVN ではアドバイザリの詳細に関する邦訳記載を止め、アドバイザリが公開または更新された際の通知に重点を置く簡略形式に変更しました。2026 年 3 月から順次適用を開始し、本四半期ではその範囲を拡大、2026 年 5 月公表の Intel のアドバイザリはこの簡略形式を採用しています。JVN では、読者の利用環境の変化等に応じてアドバイザリ形式を柔軟に見直すことによって、有益な情報をより迅速にお届けしたいと考えております。

3.1.3 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/

3.1.4 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、65 件の脆弱性に CVE ID を付与しました。

CNA および CVE については、次の Web ページをご参照ください。

- CNA（CVE Numbering Authority）
  https://www.jpcert.or.jp/vh/cna.html
- Overview About the CVE Program
  https://www.cve.org/About/Overview

3.2 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。

- 国内における脆弱性関連情報を取り扱う全ての皆様へ – 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に則した対応に関するお願い –
  https://www.meti.go.jp/policy/netsecurity/vul_request.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

3.2.1 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 3.2 に示すとおり 1,364 です。

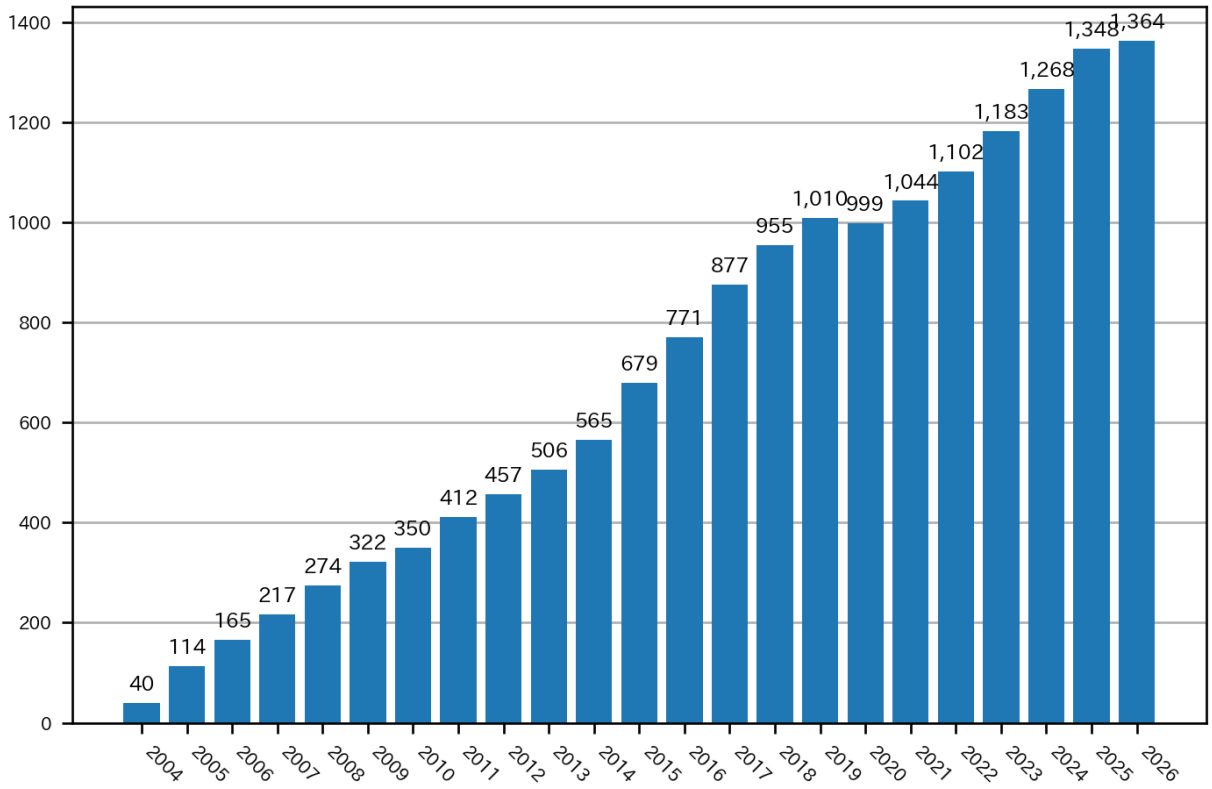


図 3.2 製品開発者登録数

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

第 4 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。

4.1 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。

4.1.1 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。

4.1.2 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、国家サイバー統括室（NCO）と共同でセプターカウンシルの事務局を支援しています。本四半期は、2026 年 6 月 8 日に開催された第 84 回セプターカウンシル運営委員会で、最近のソフトウェアサプライチェーン攻撃事案の状況と対策について情報を共有しました。

4.2 国内関係機関との連携強化および情報交換の環境整備

4.2.1 CISTA 利用組織との連携促進

CISTA 利用組織に対し、CISTA を介した情報共有活動に加えて、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、利用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 27 組織を CISTA の利用組織として登録しました。

4.2.2 製造業の制御システムセキュリティ担当者向け課題検討グループ

JPCERT/CC では、製造業を中心とした制御システムセキュリティ担当者による課題検討グループを運営しています。このグループでは、制御システムセキュリティに関する共通課題について、JPCERT/CC と登録組織の実務者とが協働し、実践的な検討を行っています。

なお、本四半期末時点で 37 組織が登録されています。

4.3 情報・ツール等の提供

4.3.1 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 5 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。

5.1 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。

5.2 国際 CSIRT 間連携

APCERT や FIRST で主導的な役割を担う等、国際的な CSIRT 連携の枠組みにも積極的に参加しています。

5.2.1 APCERT（Asia Pacific Computer Emergency Response Team）

APCERT は 2003 年 2 月に発足したアジア太平洋地域の CSIRT コミュニティーです。 JPCERT/CC は、発足時から継続して Steering Committee（運営委員会）のメンバーに選出されており、また、その事務局も担当しています。

APCERT および APCERT における JPCERT/CC の役割については、次の Web ページをご参照ください。

- JPCERT/CC within APCERT
  https://www.jpcert.or.jp/english/apcert/

5.2.1.1 APCERT Steering Committee 会議の実施

APCERT の Steering Committee は 2026 年 4 月 8 日にマレーシアのクアラルンプールで対面での会議を、また 2026 年 6 月 30 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。

5.2.2 FIRST（Forum of Incident Response and Security Teams）

JPCERT/CC は、1998 年の加盟以来、FIRST の活動に積極的に参加しており、 2021 年 6 月からは国際部の内田が理事を務めています。本四半期は、毎月のオンライン理事会に加え、2026 年 4 月にドイツのミュンヘン、2026 年 6 月にアメリカのデンバーでそれぞれ開催された対面での理事会にも参加しました。

FIRST については、次の Web ページをご参照ください。

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

5.2.2.1 第 38 回 FIRST 年次会合への参加

第 38 回 FIRST 年次会合が 2026 年 6 月 14 日から 2026 年 6 月 19 日にかけてアメリカのデンバーで開催されました。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 “Peak Defense: Building Adaptive Systems for Modern Threats” をテーマに多種多様なトピックが取り上げられ、各国から 700 名程度が現地参加しました。会期中、JPCERT/CC は世界各国の 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じて各地域の関係機関との情報共有や信頼関係構築を進め、国際的なインシデント対応調整をより円滑に進められるよう、今後も連携強化に努めます。第 38 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。

- 38th ANNUAL FIRST CONFERENCE
  https://www.first.org/conference/2026/

5.3 海外 CSIRT 等の来訪および訪問

JPCERT/CC は海外 CSIRT への訪問や海外 CSIRT から JPCERT/CC への来訪を通じて、活動の状況をヒアリングするとともに今後の協力について意見交換を行っています。本四半期は、次の訪問や来訪がありました。

- CyberSecurity Malaysia への訪問（2026 年 4 月 9 日）
- CERT-EU からの来訪（2026 年 5 月 26 日）

5.4 その他国際会議への参加

5.4.1 Locked Shields に参加

2026 年 4 月 20 日から 2026 年 4 月 24 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 2026 にオンライン参加しました。JPCERT/CC の職員 5 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/

5.4.2 NatCSIRT2026 への参加

第 38 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）2026 がアメリカのデンバーで開催されました。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。この会議で JPCERT/CC は、インシデント対応における AI の活用に関するパネルディスカッションに登壇し、AI を用いた業務効率化の事例などについて紹介しました。NatCSIRT についての詳細は、次の Web ページをご参照ください。

- NatCSIRT 2026
  https://resources.sei.cmu.edu/news-events/events/natcsirt/index.cfm

5.5 国際標準化活動

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

本四半期において、WG3 では、改訂作業中の ISO/IEC 29147（脆弱性情報公開）ならびに ISO/IEC 30111（脆弱性取り扱い手順）の両標準について、2026 年 3 月の国際会議での決定事項に基づき作業草案の第 2 版（WD2）の作成を進めました。その結果、WD2 を完成させ、SC27 事務局へ送付するとともに、参加国への配布を依頼しました。今後、各国のエキスパートから WD2 に対するコメントが寄せられ、今秋の国際会議において、それらのコメントの取り扱いが検討される予定です。

5.6 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、世界各地域で脆弱性調整を担う組織と協力関係を結び、国際的な活動の調整や情報共有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。

5.6.1 CVE/FIRST VulnCon 2026 & Annual CNA Summit への参加

2026 年 4 月 13 日から 2026 年 4 月 16 日にかけて、FIRST と CVE Program が合同で主催する CVE/FIRST VulnCon 2026 & Annual CNA Summit がアメリカのアリゾナ州スコッツデールで開催されました。JPCERT/CC は、Coordinated Vulnerability Disclosure (CVD) に関する手法の議論を交えた机上演習をファシリテーターとして企画・実施したほか、米 CISA が主導して 2024 年に設立し、JPCERT/CC も Co-chair として活動に協力している脆弱性コーディネーター組織による国際的なコミュニティー「Global Community of Practice on Coordinated Vulnerability Disclosure（CVD-COP）」の会合を運営しました。同会合では、活動状況や今後の課題等に関する発表や情報共有、意見交換が行われました。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 2026 & Annual CNA Summit
  https://www.first.org/conference/vulncon26/

第 6 章

フィッシング対策協議会活動

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

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

協議会では、経済産業省から委託された活動のほかに、会員組織向けの独自の活動を運営委員会の決定に基づいて行っており、JPCERT/CC は事務局としてこれらの活動の実施についても支援しています。具体的には「 6.2 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。

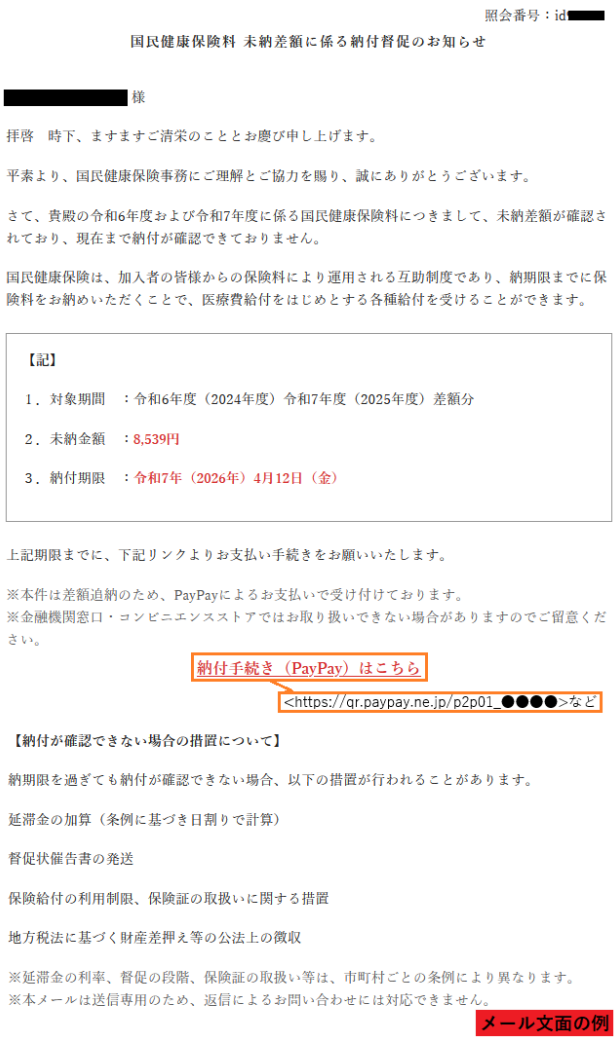
6.1 フィッシング対策協議会事務局の運営

6.1.1 フィッシングに関する報告・問い合わせの受け付け

本四半期分はまだ確定していないものの、フィッシングの報告件数は前四半期に引き続き減少する見通しです。2026 年 4 月に多く報告されていた証券系のフィッシングは 2026 年 5 月以降減少しました。一方、2026 年 3 月から報告が続いている、国民健康保険、住民税、国民年金などの納付依頼を装い、PayPay アプリを使って直接送金させる手口は増加しました（図 6.1）。

過去 1 年間のフィッシング報告件数の推移を図 6.2 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 13.9% を占めました。次いで、楽天カードをかたるフィッシングの報告が多く、全体の約 12.9% を占めました。



照会番号：id[redacted]

国民健康保険料 未納差額に係る納付督促のお知らせ

[redacted]様

拝啓　時下、ますますご清栄のこととお慶び申し上げます。

平素より、国民健康保険事務にご理解とご協力を賜り、誠にありがとうございます。

さて、貴殿の令和6年度および令和7年度に係る国民健康保険料につきまして、未納差額が確認されており、現在まで納付が確認できておりません。

国民健康保険は、加入者の皆様からの保険料により運用される互助制度であり、納期限までに保険料をお納めいただくことで、医療費給付をはじめとする各種給付を受けることができます。

【記】

1．対象期間　：令和6年度（2024年度）令和7年度（2025年度）差額分

2．未納金額　：8,539円

3．納付期限　：令和7年（2026年）4月12日（金）

上記期限までに、下記リンクよりお支払い手続きをお願いいたします。

※本件は差額追納のため、PayPayによるお支払いで受け付けております。
※金融機関窓口・コンビニエンスストアではお取り扱いできない場合がありますのでご留意ください。

納付手続き（PayPay）はこちら
<https://qr.paypay.ne.jp/p2p01_●●●●>など

【納付が確認できない場合の措置について】

納期限を過ぎても納付が確認できない場合、以下の措置が行われることがあります。

延滞金の加算（条例に基づき日割りで計算）

督促状催告書の発送

保険給付の利用制限、保険証の取扱いに関する措置

地方税法に基づく財産差押え等の公法上の徴収

※延滞金の利率、督促の段階、保険証の取扱い等は、市町村ごとの条例により異なります。
※本メールは送信専用のため、返信によるお問い合わせには対応できません。

メール文面の例

図 6.1 PayPay へ誘導するフィッシングメールの例

6.1.2　情報収集／配信

6.1.2.1　定期報告

報告されたフィッシングサイト数や毎月の活動報告等を協議会の Web サイトで公開しました。

- フィッシング対策協議会 Web サイト
  https://www.antiphishing.jp/
- 2026/03 フィッシング報告状況
  https://www.antiphishing.jp/report/monthly/202603.html
- 2026/04 フィッシング報告状況
  https://www.antiphishing.jp/report/monthly/202604.html
- 2026/05 フィッシング報告状況
  https://www.antiphishing.jp/report/monthly/202605.html

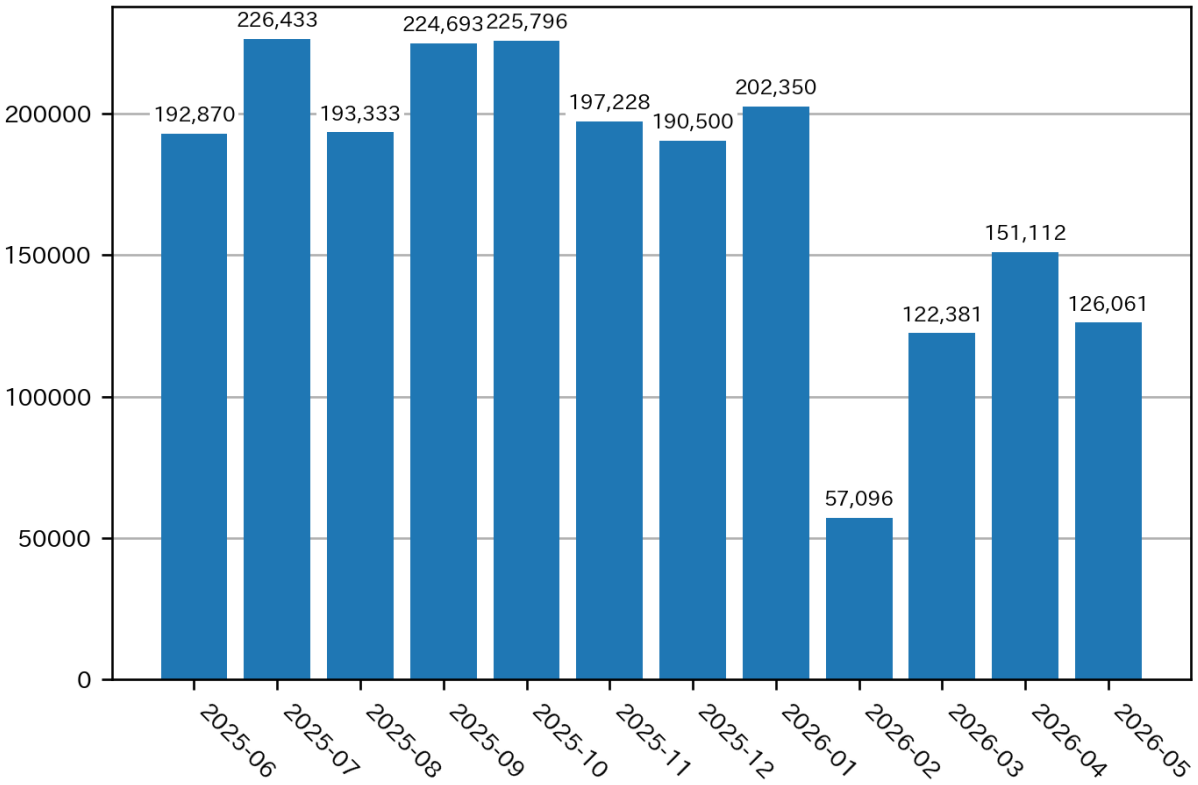


図 6.2 フィッシング報告件数

6.1.2.2 フィッシングサイト URL 情報の提供

フィッシング対策ツールバーやアンチウイルスソフトなどを提供している事業者やフィッシングに関する研究を行っている学術機関である協議会の会員等に対し、協議会に報告されたフィッシングサイトの URL を集めたリストを提供しています。これは、フィッシング対策製品の強化や、関連研究の促進を目的としたものです。本四半期末時点で 51 組織に情報を提供しており、今後も要望に応じて広く提供する予定です。

6.1.2.3 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。前年度に技術・制度検討ワーキンググループで改定・作成を進めた『フィッシング対策ガイドライン 2026 年度版』『利用者向けフィッシング詐欺対策ガイドライン 2026 年度版』および『フィッシングレポート 2026』を、2026 年 6 月 1 日に公開しました。これまでの PDF 版に加え、HTML 形式の Web ページでも掲載しています。

- 資料公開： フィッシング対策ガイドライン改定のお知らせ
  https://www.antiphishing.jp/news/info/guideline2026.html.html
- 資料公開： フィッシングレポート 2026 公開のお知らせ
  https://www.antiphishing.jp/news/info/press_phishing_report2026.html

6.2　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。

6.2.1　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 137 回運営委員会
  開催日：2026 年 4 月 23 日
- 第 138 回運営委員会
  開催日：2026 年 5 月 28 日
- 第 139 回運営委員会
  開催日：2026 年 6 月 25 日

6.2.2　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。

- リサーチワーキンググループ会合
  開催日：2026 年 4 月～2026 年 6 月 毎週火曜日
- 証明書普及促進ワーキンググループ会合
  開催日：2026 年 5 月 25 日
- フィッシング対策協議会　2026 年度総会
  開催日：2026 年 6 月 17 日

第 7 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。

7.1 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。

- be Connected Executive Roundtable ランサムウェア時代のサイバーレジリエンス ～体験型ディスカッションで深める、インシデント対応力の強化～
  タイトル：ランサムウェア攻撃被害を「当たり前」にしないための備え
  講演者：佐々木 勇人（サイバーセキュリティコーディネーショングループ 担当部門長 兼 政策担当部長 脅威アナリスト）
  主催：株式会社ビジネス・フォーラム事務局
  講演日：2026 年 5 月 20 日
- 令和 8 年度 自治体 CSIRT 協議会総会
  タイトル：侵入型ランサムウェアの初動対応
  講演者：矢野 雄紀（サイバーセキュリティコーディネーショングループ 脅威分析・インシデント対応チーム）
  主催：自治体 CSIRT 協議会事務局
  講演日：2026 年 5 月 27 日

7.2 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。

- 第 30 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：2026 年 5 月 21 日〜2026 年 5 月 23 日

- Interop Tokyo 2026
  主催：Interop Tokyo 実行委員会
  開催日：2026 年 6 月 10 日〜2026 年 6 月 12 日
- エッジ AI イニシアチブ 2026
  主催：アイティメディア株式会社
  開催日：2026 年 6 月 16 日〜2026 年 6 月 18 日

7.3 公開資料

本四半期は次の資料を公開しました。

7.3.1 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、『インターネット定点観測レポート』として邦文および英文で公表してきましたが、同レポートは下記の 2025 年度第 4 四半期分をもって終了し、本レポートに統合しました。今後は、本レポート**第 2 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**をご参照ください。

- 2026-05-15
  JPCERT/CC インターネット定点観測レポート［2026 年 1 月 1 日〜2026 年 3 月 31 日］
  https://www.jpcert.or.jp/tsubame/report/report202601-03.html
- 2026-06-17
  JPCERT/CC Internet Threat Monitoring Report [January 1, 2026 - March 31, 2026]
  https://www.jpcert.or.jp/english/tsubame/report/report202601-03.html

7.3.2 ソフトウェア等の脆弱性関連情報に関する届出状況

IPA と JPCERT/CC は、それぞれ受付機関および調整機関として、経済産業省告示「ソフトウエア製品等の脆弱性関連情報に関する取扱規程」（平成 29 年経済産業省告示第 19 号、最終改正令和 6 年経済産業省告示第 93 号）等に基づく脆弱性関連情報流通制度の運用の一端を 2004 年 7 月から担っています。この制度の運用に関連した前四半期の活動実績と、同期間中に公表された脆弱性に関する注目すべき動向をまとめてレポートとして公表しています。

- 2026-04-16
  ソフトウェア等の脆弱性関連情報に関する届出状況［2026 年第 1 四半期（1 月〜3 月）］
  https://www.jpcert.or.jp/pr/2026/vulnREPORT_2026q1.pdf

7.3.3 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 件の記事を公開しました。

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

- 2026-05-13
  TSUBAME レポート Overflow（2025 年 10〜12 月）
- 2026-06-02
  TSUBAME レポート Overflow（2026 年 1〜3 月）
- 2026-06-11
  ツール分析結果シートのアップデート

英語版発行件数：2 件 https://blogs.jpcert.or.jp/en/

- 2026-04-14
  ICS Security Conference 2026
- 2026-05-14
  TSUBAME Report Overflow (Oct-Dec 2025)

付録 A

インシデントの分類

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

フィッシングサイト

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

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

Web サイト改ざん

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

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

マルウェアサイト

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

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

スキャン

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

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

DoS/DDoS

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

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

制御システム関連インシデント

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

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

標的型攻撃

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

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

その他

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

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

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

- JPCERT コーディネーションセンター（JPCERT/CC）：https://www.jpcert.or.jp/
- インシデント情報の提供および対応依頼：info@jpcert.or.jp, https://www.jpcert.or.jp/form/
- 脆弱性情報ハンドリングに関するお問い合わせ：vultures@jpcert.or.jp
- 制御システムセキュリティに関するお問い合わせ：dc-info@jpcert.or.jp
- セキュアコーディングセミナーのお問い合わせ：secure-coding@jpcert.or.jp
- 公開資料の引用、講演依頼、その他のお問い合わせ：pr@jpcert.or.jp
- PGP 公開鍵について：https://www.jpcert.or.jp/jpcert-pgp.html

JPCERT/CC 四半期レポート ［ 2026 年 4 月 1 日〜2026 年 6 月 30 日 ］

- 発行履歴
  - 2026 年 7 月 16 日　初版
  - 2026 年 7 月 16 日　誤植修正
  - 2026 年 7 月 29 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/