

JPCERT/CC インシデント報告対応レポート

2024年4月1日～2024年6月30日



一般社団法人 JPCERT コーディネーションセンター

2024年7月18日

JPCERT **CC**®

目次

1	インシデント報告対応レポートについて	2
2	四半期の統計情報	3
3	インシデントの傾向	9
3.1	フィッシングサイトの傾向	9
3.2	Web サイト改ざんの傾向	10
3.3	標的型攻撃の傾向	10
3.4	その他のインシデントの傾向	11
4	インシデント対応事例	12
4.1	PAN-OS GlobalProtect の脆弱性への対応	12
	JPCERT/CC からのお願い	13
付録 A	インシデントの分類	14

改訂履歴：

2024年 7月18日 初版

2024年 9月 6日 P11. 誤植を修正

本活動は、経済産業省より委託を受け、「令和 6 年度サイバー攻撃等国際連携対応調整事業」として実施したものです。

1 インシデント報告対応レポートについて

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。）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（以下、「インシデント」という。）の報告を受け付けています*¹。本レポートでは、2024年4月1日から2024年6月30日までの間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。

JPCERT/CC は、インターネット利用組織におけるインシデントの認知と対処、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、国内や国外（海外の CSIRT 等）の関係機関との調整活動を行っています。

*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 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 2.1 に示します *1。

本四半期に寄せられた報告件数は 15,396 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 4,176 件でした。前四半期と比較して、報告件数は 31% 増加し、調整件数は 9% 減少しました。また、前年同期と比較すると、報告数は 43% 減少し、調整件数は 9% 減少しました。

図 2.1 と図 2.2 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 2.1 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	4,277	6,148	4,971	15,396	11,741
インシデント件数	2,280	2,398	1,926	6,604	6,089
調整件数	1,541	1,375	1,260	4,176	4,602

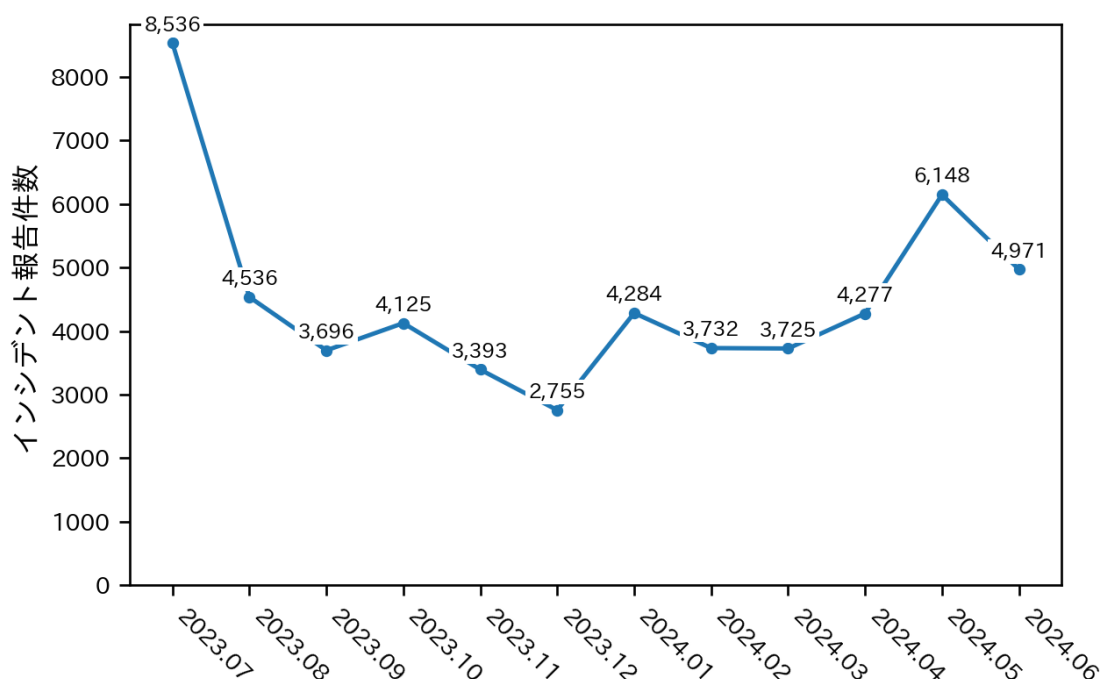


図 2.1 インシデント報告件数の推移

*1 報告件数は、報告者から寄せられた Web フォーム、メール、FAX 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。

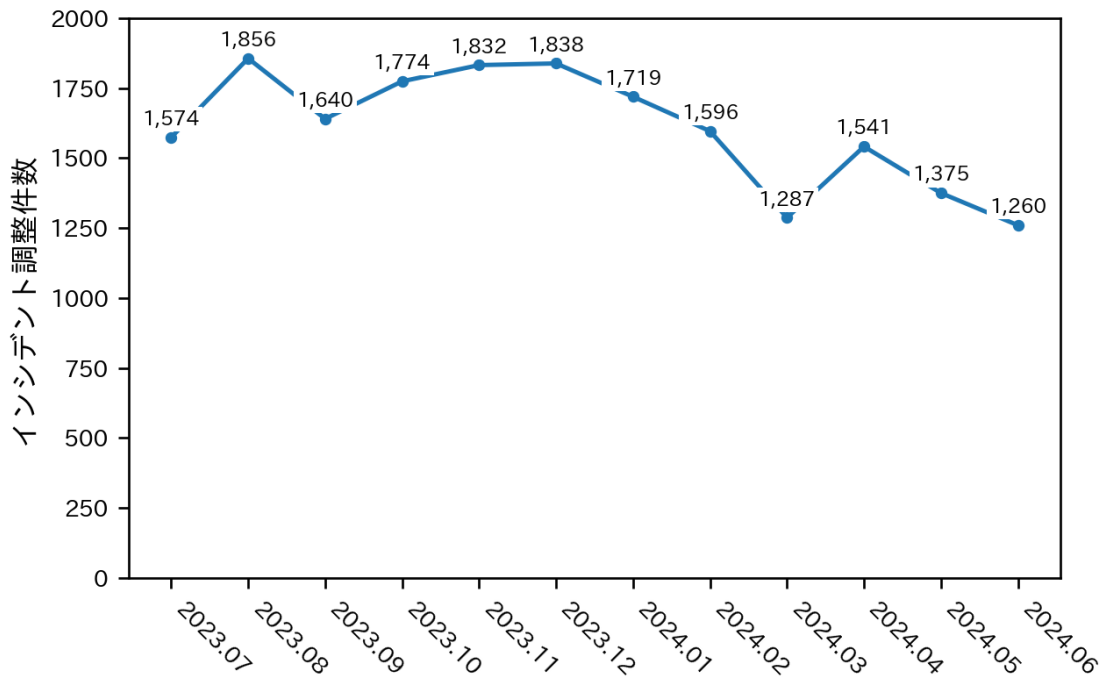


図 2.2 インシデント調整件数の推移

表 2.2 インシデント報告件数のカテゴリ別内訳

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	1,685	1,733	1,607	5,025	4,781
Web サイト改ざん	8	20	15	43	57
マルウェアサイト	28	12	5	45	45
スキャン	252	285	152	689	697
DoS/DDoS	0	1	2	3	2
制御システム関連	0	0	0	0	0
標的型攻撃	2	0	0	2	4
その他	305	347	145	797	503

JPCERT/CC では、報告を受けたインシデントをカテゴリ別に分類し、各インシデントカテゴリに応じた調整、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参照してください。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別内訳を表 2.2 に示します。また、カテゴリ別割合は図 2.3 のとおりです。

フィッシングサイトに分類されるインシデントが 76%、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 10% を占めています。

図 2.4 から図 2.7 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 2.8 にインシデントのカテゴリごとの件数および調整・対応状況を示します。

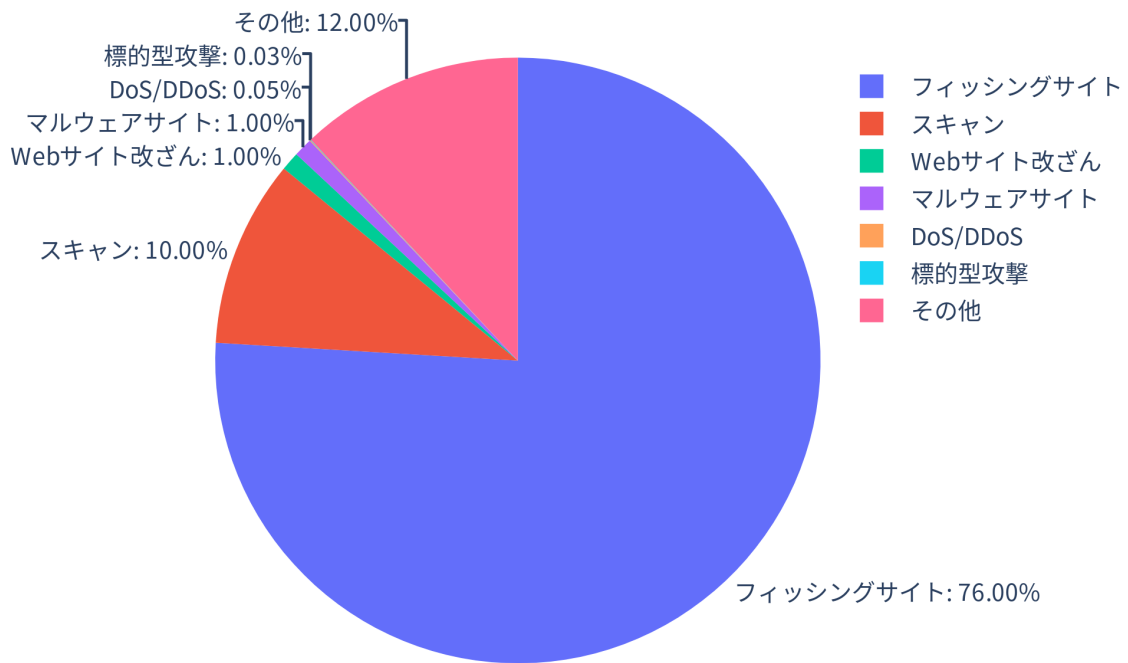


図 2.3 インシデント報告件数のカテゴリー別内訳

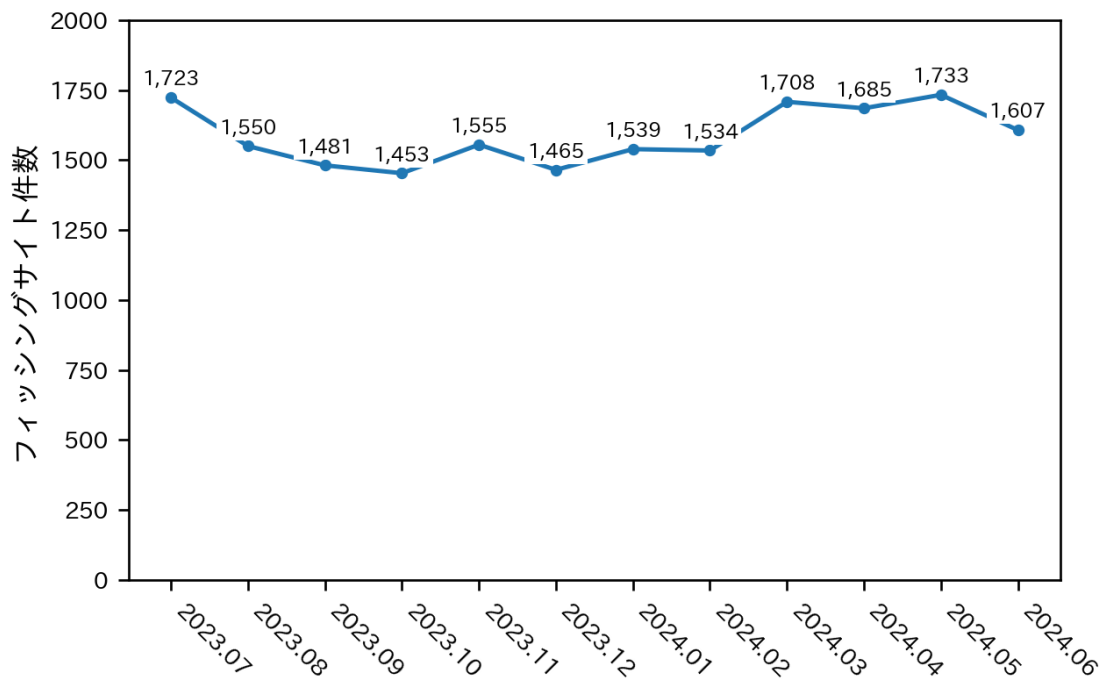


図 2.4 フィッシングサイト件数の推移

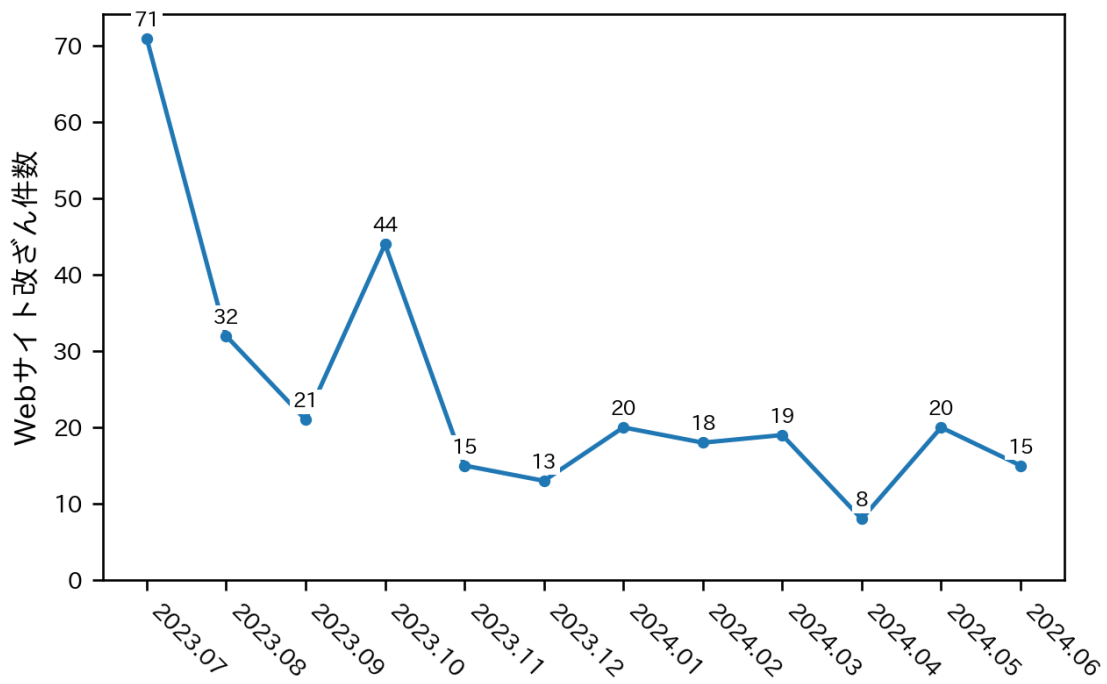


図 2.5 Web サイト改ざん件数の推移

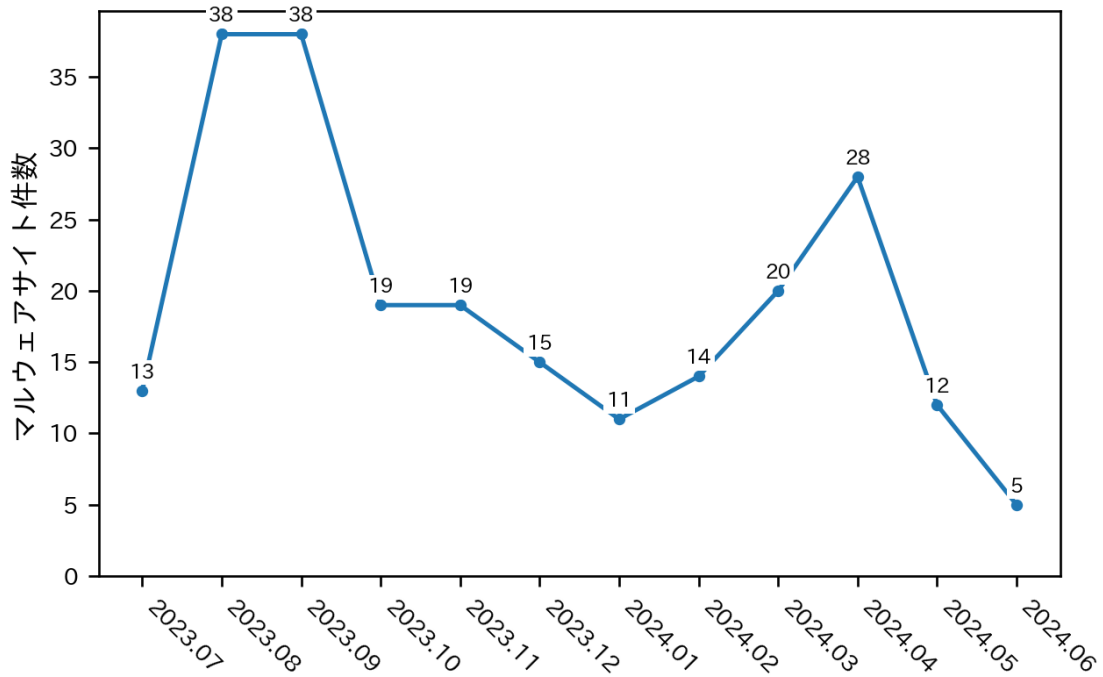


図 2.6 マルウェアサイト件数の推移

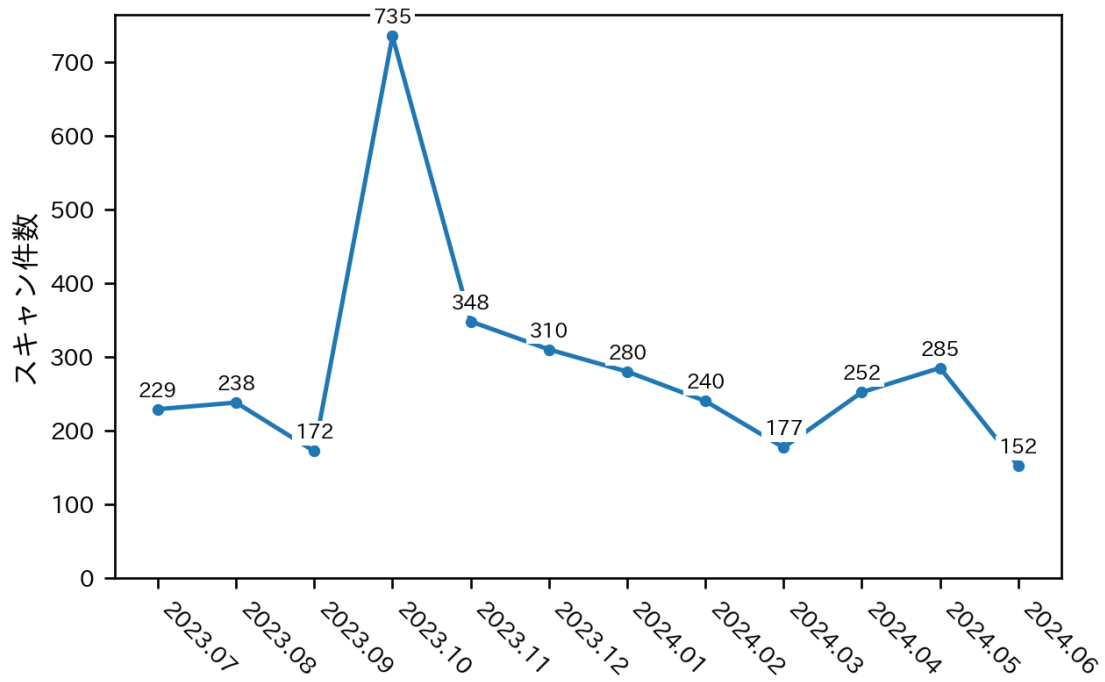


図 2.7 スキャン件数の推移

インシデント件数 6,604 件	報告件数 15,396 件	調整件数 4,176 件		
フィッシングサイト 5,025 件	通知を行った件数 2,347 件 - サイトの稼働を確認	国内への通知 32% 海外への通知 68%	対応日数(営業日) 0~3日 34% 4~7日 38% 8~10日 10% 11日以上 19%	通知不要 2,678 件 - サイトを確認できない
Web サイト改ざん 43 件	通知を行った件数 38 件 - サイトの改ざんを確認 - 脅威度が高い	国内への通知 97% 海外への通知 3%	対応日数(営業日) 0~3日 44% 4~7日 25% 8~10日 9% 11日以上 22%	通知不要 5 件 - サイトを確認できない - 当事者へ連絡が届いている - 情報提供である - 脅威度が低い
マルウェアサイト 45 件	通知を行った件数 24 件 - サイトの稼働を確認 - 脅威度が高い	国内への通知 29% 海外への通知 71%	対応日数(営業日) 0~3日 47% 4~7日 35% 8~10日 0% 11日以上 18%	通知不要 21 件 - サイトを確認できない - 当事者へ連絡が届いている - 情報提供である - 脅威度が低い
スキャン 689 件	通知を行った件数 429 件 - 詳細なログがある - 連絡を希望されている	国内への通知 96% 海外への通知 4%		通知不要 260 件 - ログに十分な情報が無い - 当事者へ連絡が届いている - 情報提供である
DoS/DDoS 3 件	通知を行った件数 3 件 - 詳細なログがある - 連絡を希望されている	国内への通知 33% 海外への通知 67%		通知不要 0 件 - ログに十分な情報が無い - 情報提供である
制御システム関連 0 件	通知を行った件数 0 件	国内への通知 - 海外への通知 -		通知不要 0 件
標的型攻撃 2 件	通知を行った件数 0 件 - サイトの稼働を確認	国内への通知 - 海外への通知 -		通知不要 2 件 - 当事者へ連絡が届いている - 情報提供である
その他 797 件	通知を行った件数 190 件 - 脅威度が高い - 連絡を希望されている	国内への通知 77% 海外への通知 23%		通知不要 607 件 - 当事者へ連絡が届いている - 情報提供である - 脅威度が低い

図 2.8 インシデントのカテゴリごとの件数と調整・対応状況

3 インシデントの傾向

3.1 フィッシングサイトの傾向

本四半期に報告が寄せられたフィッシングサイトの件数は 5,025 件で、前四半期の 4,781 件から 5% 増加しました。また、前年度同期 (6,186 件) との比較では、19% の減少となりました。

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 961 件となり、前四半期の 745 件から 29% 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 3,026 件となり、前四半期の 3,226 件から 6% 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*1 を表 3.1、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 3.1 と図 3.2 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 78%、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 48% で、それぞ

表 3.1 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	本四半期合計	割合
国内ブランド	1,101	1,048	877	3,026	60%
国外ブランド	293	336	332	961	19%
ブランド不明	291	349	398	1,038	21%
全ブランド合計	1,685	1,733	1,607	5,025	

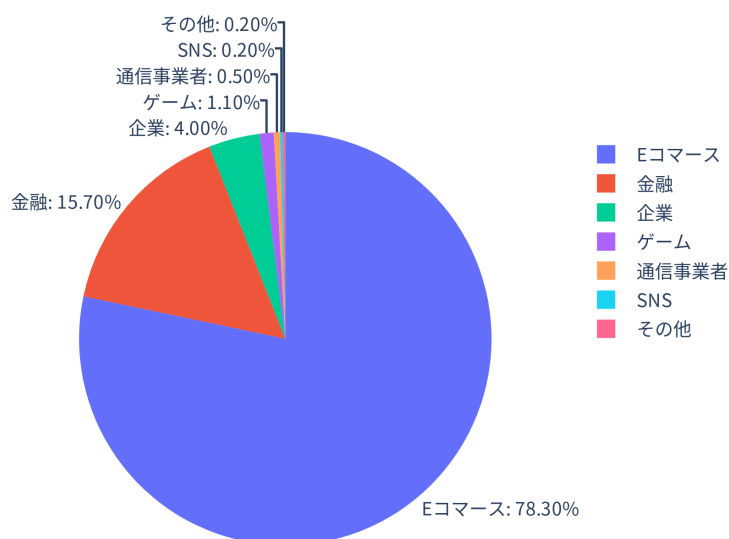


図 3.1 国外ブランドのフィッシングサイトの件数の業界別の割合

*1 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。

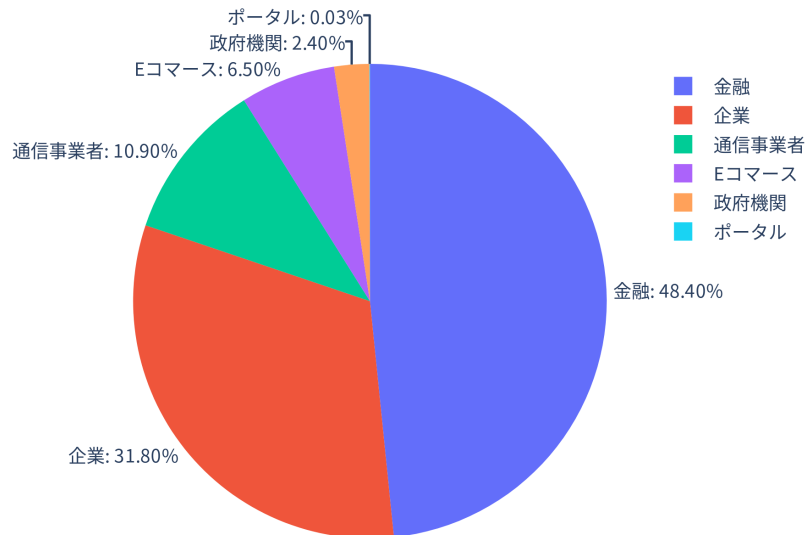


図 3.2 国内ブランドのフィッシングサイトの件数の業界別の割合

れ最も多くを占めました。

海外ブランドでは、Amazon や Apple を装ったフィッシングサイトが 8 割以上を占めました。

国内ブランドでは、メルカリやえきねっとを装ったフィッシングサイトが多く報告されました。国内金融機関では、前四半期に引き続きエポスカード、イオンカード、そして三井住友カードを装ったフィッシングサイトが引き続き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割合は、国内が 32%、国外が 68% であり、前四半期（国内が 30%、国外が 70%）と比較し国内の割合が増加しました。

3.2 Web サイト改ざんの傾向

本四半期に報告が寄せられた Web サイト改ざんの件数は 43 件でした。前四半期の 57 件から 25% 減少しています。

本四半期は、ブラウザの通知機能を悪用して不審サイトに転送させる事例を確認しています。正規の Web サイトに不正な PHP のコードが挿入されており、アクセスしてきたユーザーのブラウザの通知機能で不審なサイトへ転送される仕組みになっていました。また、不正な PHP のコードは、攻撃者が用意したドメインに DNS クエリを送信し、レスポンスの TXT レコードに含まれるデータを転送先の URL として使用していました。また、攻撃者は不正な PHP コードを正規の Web サイトに挿入するために、改ざんサイトに WPCode と呼ばれるプラグインをインストールしていました。

3.3 標的型攻撃の傾向

標的型攻撃に分類されるインシデントの件数は 2 件でした。

本四半期は、標的型攻撃メールの報告が寄せられました。標的型攻撃メールに添付されていたファイルは

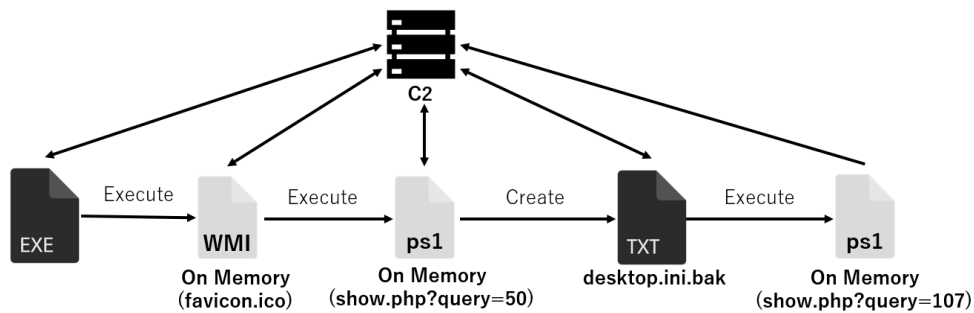


図 3.3 添付ファイル実行からマルウェアに感染するまでの流れ

表 3.2 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	106	117	122	345
22/tcp	90	64	19	173
25/tcp	29	52	7	88
443/tcp	10	34	2	46
80/tcp	13	9	2	24
37215/tcp	3	2	0	5
2323/tcp	1	2	0	3
143/tcp	1	2	0	3
110/tcp	1	1	0	2
9530/tcp	1	0	0	1

拡張子 exe の前に大量の空白を入れることで、ファイルの種別をわかりづらくしていました。添付ファイルを実行すると、C2 サーバーへシステム情報やキーボードの入力情報等を送信するマルウェアがダウンロードされます。ダウンロードされるマルウェアは PowerShell で記述されていて、ハードディスク上にファイルとして保存されず、メモリ上で実行されます。図 3.3 は、マルウェアに感染するまでの流れです。

3.4 その他のインシデントの傾向

本四半期に報告が寄せられたマルウェアサイトの数は 45 件でした。前四半期の 45 件から増減はありませんでした。

本四半期に報告が寄せられたスキャン件数は 689 件でした。前四半期の 697 件から 1% 減少しています。スキャンの対象となったポートの上位 10 位を表 3.2 に示します。頻繁にスキャンの対象となったポートは、Telnet (23/TCP)、SSH (22/TCP)、SMTP (25/TCP)、HTTPS (443/TCP) でした。

その他に分類されるインシデントの件数は 797 件でした。前四半期の 503 件から 58% 増加しました。

4 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。

4.1 PAN-OS GlobalProtect の脆弱性への対応

2024年4月12日、Palo Alto Networks社はPAN-OSのGlobalProtect機能にOSコマンドインジェクションの脆弱性（CVE-2024-3400）があることを公表しました。GlobalProtectはリモートアクセス（VPN）などを提供する機能で、本脆弱性の悪用により、認証されていない遠隔の第三者に管理者権限で任意のコードを実行される可能性があります。本脆弱性はすでに悪用が確認されていたことからJPCERT/CCでも4月13日に注意喚起を行いました。

- Palo Alto Networks社製PAN-OS GlobalProtectのOSコマンドインジェクションの脆弱性（CVE-2024-3400）に関する注意喚起

<https://www.jpcert.or.jp/at/2024/at240009.html>

JPCERT/CCでは複数の組織から本脆弱性による被害があったとの報告を受けました。被害の多くは、脆弱性が発表されパッチが公表された4月14日以降に発生し、機器の構成ファイルが外部から閲覧可能な場所にコピーされ漏えいしていました。脆弱性の回避策であるデバイステレメトリを無効化していた組織では攻撃を阻止できていました。

また、JPCERT/CCでは、本脆弱性の悪用により侵害された可能性がある機器を利用している国内のシステム管理者に対する通知を、外部組織から提供された情報をもとに行いました。4月20日時点では侵害された可能性のある機器が国内に252台ありましたが、それらすべての組織に通知し、6月11日時点で86台まで減少しています。通知を受けて初めて侵害に気付いた組織が多く、攻撃者によって改ざんされたコンテンツが機器の脅威防御機能により自動的に修正されたことに気付かないケースもありました。悪用が確認されている脆弱性が公表された場合には機器のアップデートをする前に侵害の有無を確認することを推奨します。

JPCERT/CC からのお願い

JPCERT/CC では、インシデントの発生状況や傾向を把握し、状況に応じて、攻撃元や情報発信先等に対する停止・閉鎖を目的とした調整や、利用者向けの注意喚起等の発行により対策実施の必要性の周知を図る活動を通じて、インシデント被害の拡大・再発防止を目指しています。

今後とも JPCERT/CC への情報提供にご協力をお願いします。なお、インシデントの報告方法については、次の Web ページをご参照ください。

- インシデントの報告
<https://www.jpccert.or.jp/form/>
- インシデントの報告 (Web フォーム)
<https://form.jpccert.or.jp/>
- 制御システムインシデントの報告
<https://www.jpccert.or.jp/ics/ics-form.html>
- 制御システムインシデントの報告 (Web フォーム)
<https://form.jpccert.or.jp/ics.html>

報告の暗号化を希望される場合は、JPCERT/CC の PGP 公開鍵をご使用ください。次の Web ページから入手することができます。

- 公開鍵
<https://www.jpccert.or.jp/keys/info-0x69ECE048.asc>
- PGP Fingerprint :
FC89 53BB DC65 BD97 4BDA D1BD 317D 97A4 69EC E048

JPCERT/CC では、発行する情報を迅速にお届けするためのメーリングリストを開設しています。利用をご希望の方は、次の情報をご参照ください。

- メーリングリストについて
<https://www.jpccert.or.jp/announce.html>

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

本文書を引用、転載する際には JPCERT/CC 広報 (pr@jpcert.or.jp) まで確認のご連絡をお願いします。

本文書に記載の社名、製品名は各社の商標または登録商標です。

最新情報については JPCERT/CC の Web サイトを参照してください。

- 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 : icsr@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 インシデント報告対応レポート [2024 年 4 月 1 日 ~ 2024 年 6 月 30 日]

- 2024 年 7 月 18 日 初版発行
2024 年 9 月 6 日 誤植修正
- 発行
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/>