JPCERT CC®

JPCERT Coordination Center

JPCERT/CC インシデント報告対応レポート

2024 年 1 月 1 日 ～ 2024 年 3 月 31 日

一般社団法人 JPCERT コーディネーションセンター

2024 年 4 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

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(注 1)。本レポートでは、2024 年 1 月 1 日から 2024 年 3 月 31 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。

（注 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。

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。

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 1］に示します。

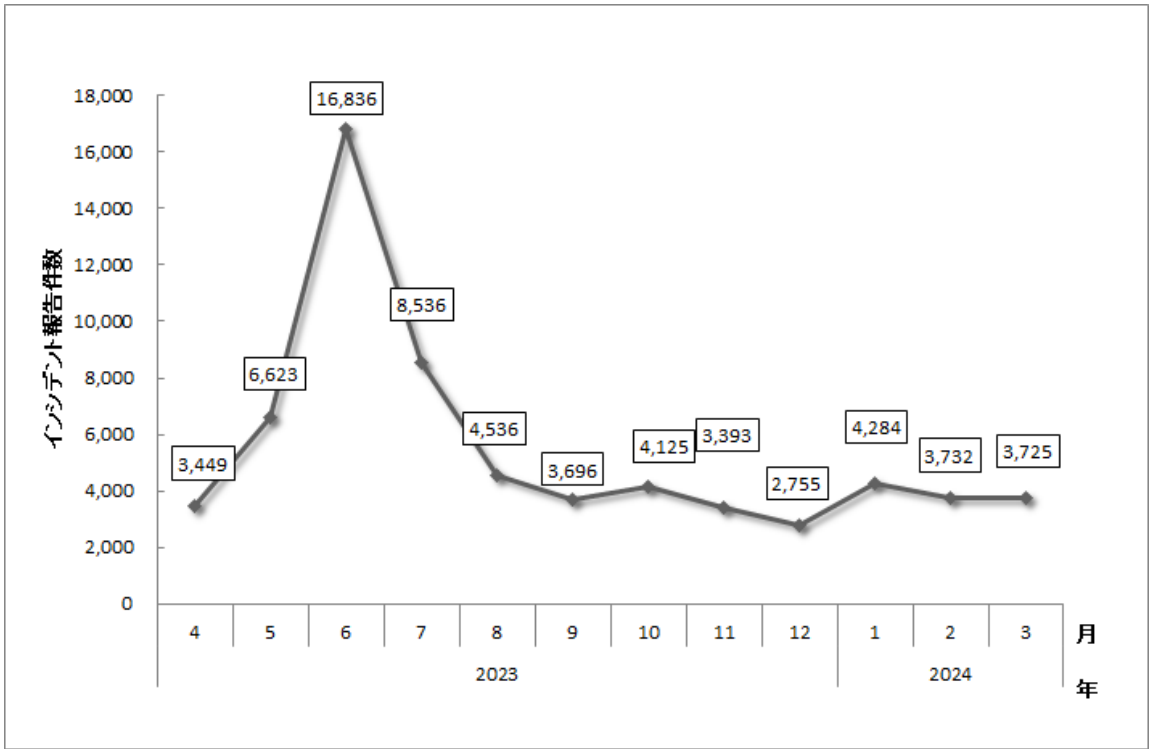
［表 1：インシデント報告関連件数］

	1 月	2 月	3 月	合計	前四半期合計
報告件数 (注 2)	4,284	3,732	3,725	11,741	10,273
インシデント件数 (注 3)	1,988	1,956	2,145	6,089	6,448
調整件数 (注 4)	1,719	1,596	1,287	4,602	5,444

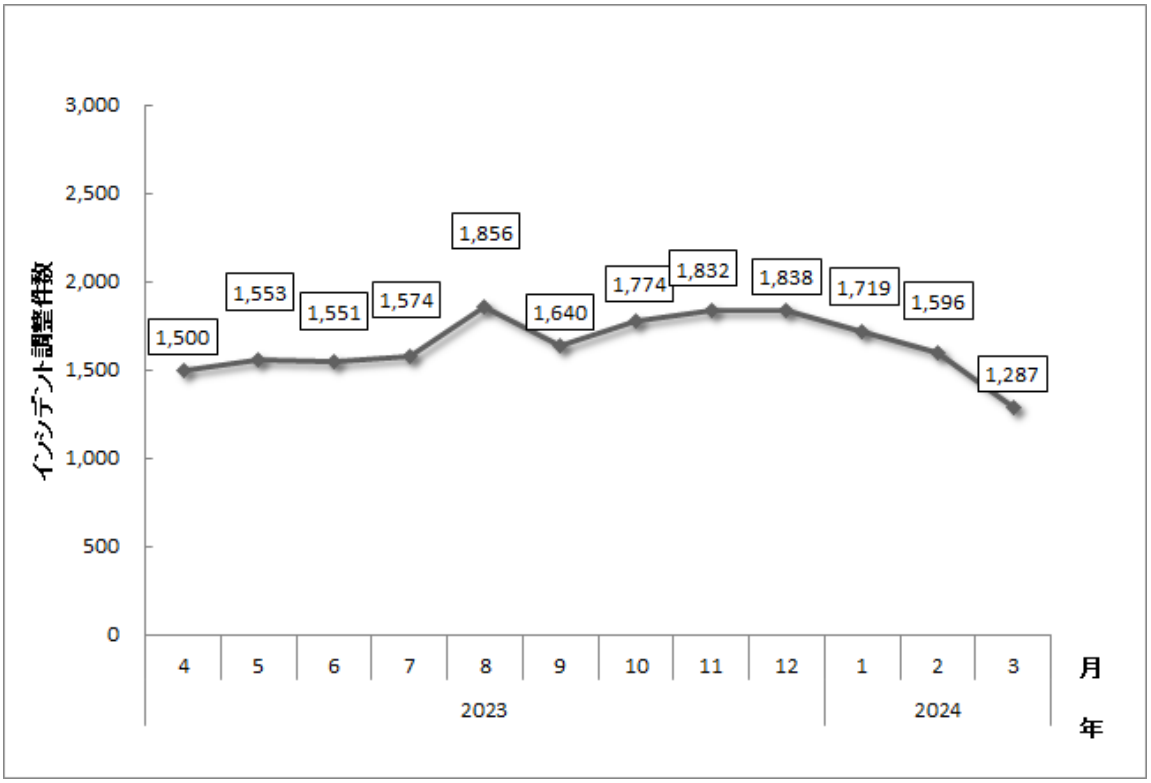
（注 2）「報告件数」は、報告者から寄せられた Web フォーム、メール、FAX による報告の総数を示します。
（注 3）「インシデント件数」は、各報告に含まれるインシデント件数の合計を示します。1 つのインシデントに関して複数件の報告が寄せられた場合にも、1 件として扱います。
（注 4）「調整件数」は、インシデントの拡大防止のため、サイトの管理者等に対し、現状の調査と問題解決のための対応を依頼した件数を示します。

本四半期に寄せられた報告件数は 11,741 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 4,602 件でした。前四半期と比較して、報告件数は 14%増加し、調整件数は 15%減少しました。また、前年同期と比較すると、報告数は 0.2%増加し、調整件数は 6%増加しました。

［図 1］と［図 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。



［図 1：インシデント報告件数の推移］



［図 2：インシデント調整件数の推移］

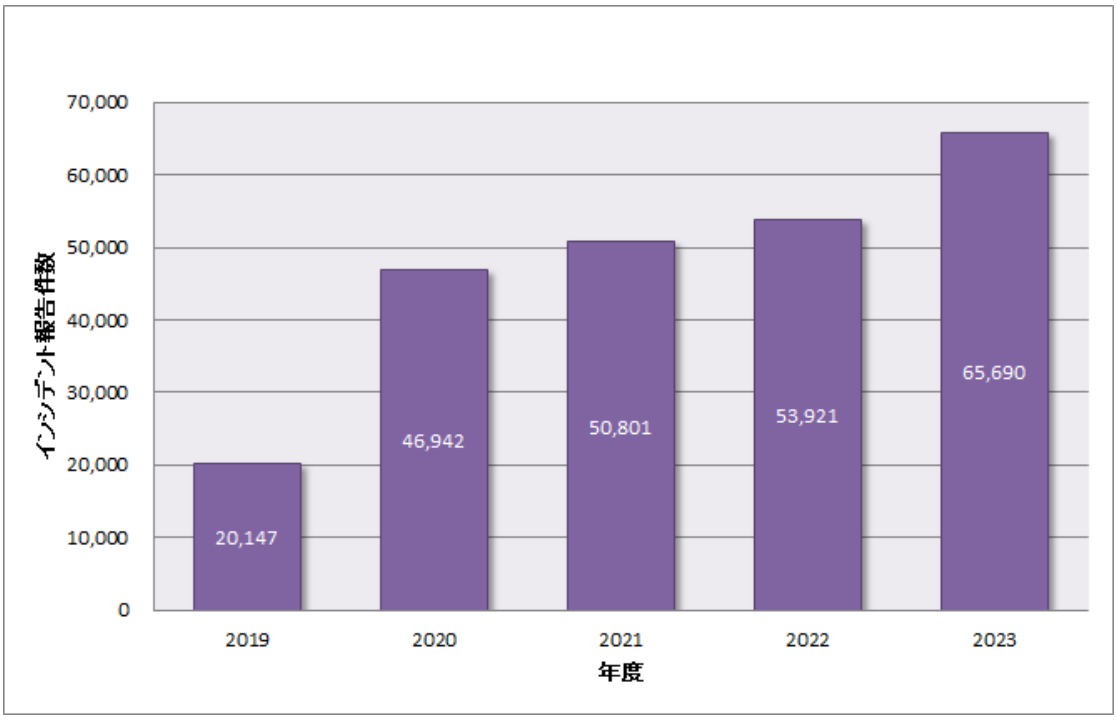
【参考】統計情報の年度比較

2023 年度を含む過去 5 年間の年度ごとの報告件数を［表 2］に示します。なお、各年度は 4 月 1 日から翌年の 3 月 31 日までとしています。

［表 2：年間報告件数の推移］

年度	2019	2020	2021	2022	2023
報告件数	20,147	46,942	50,801	53,921	65,690

2023 年度に寄せられた報告件数は 65,690 件でした。前年度の 53,921 件と比較して、22%増加しています。［図 3］に過去 5 年間の年間報告件数の推移を示します。



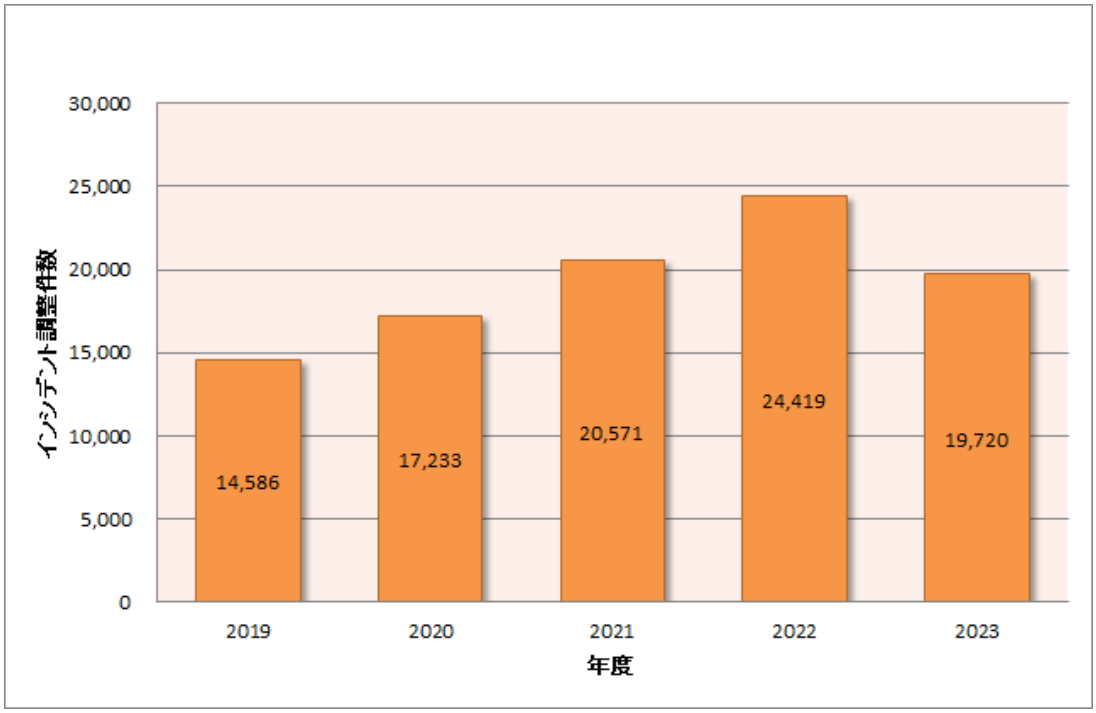
［図 3：年間報告件数の推移（年度比較）］

2023 年度を含む過去 5 年間の年度ごとの調整件数を［表 3］に示します。

［表 3：調整報告件数の推移］

年度	2019	2020	2021	2022	2023
調整件数	14,586	17,233	20,571	24,419	19,720

2023 年度に調整を行った件数は 19,720 件でした。前年度の 24,419 件と比較して、19%減少しています。［図 4］に過去 5 年間の年間調整件数の推移を示します。

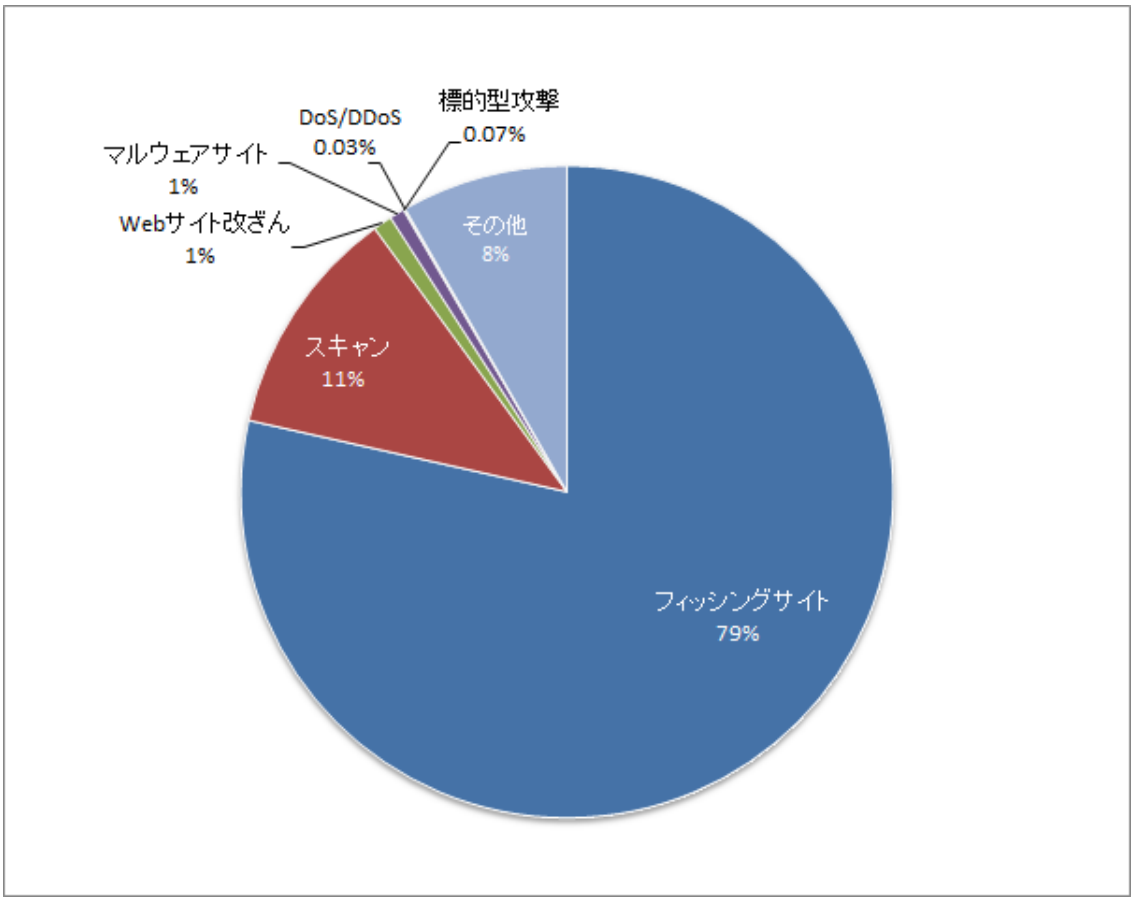


［図 4：年間調整件数の推移（年度比較）］

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、各インシデント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-1. インシデントの分類」を参照してください。本四半期にインシデント報告件数のカテゴリー別内訳を［表 4］に示します。また、カテゴリー別割合は［図 5］のとおりです。

［表 4：インシデント報告件数のカテゴリー別内訳］

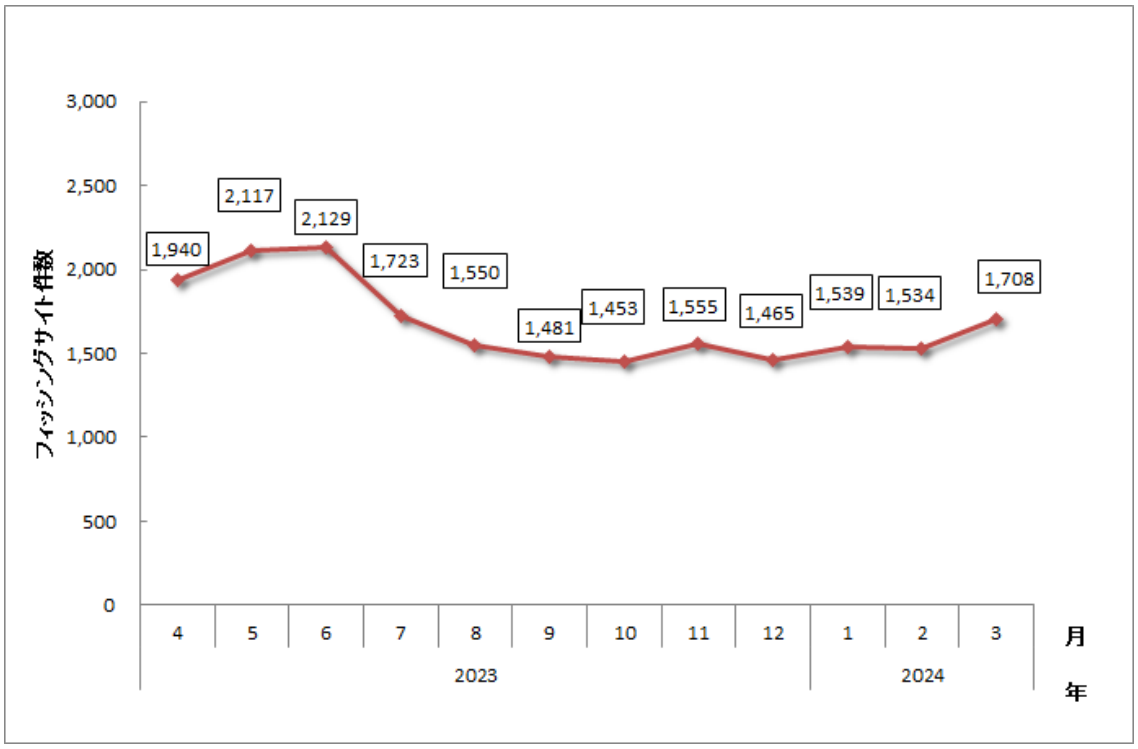
インシデント	1 月	2 月	3 月	合計	前四半期合計
フィッシングサイト	1,539	1,534	1,708	4,781	4,473
Web サイト改ざん	20	18	19	57	72
マルウェアサイト	11	14	20	45	53
スキャン	280	240	177	697	1,393
DoS/DDoS	0	1	1	2	1
制御システム関連	0	0	0	0	0
標的型攻撃	2	0	2	4	1
その他	136	149	218	503	455



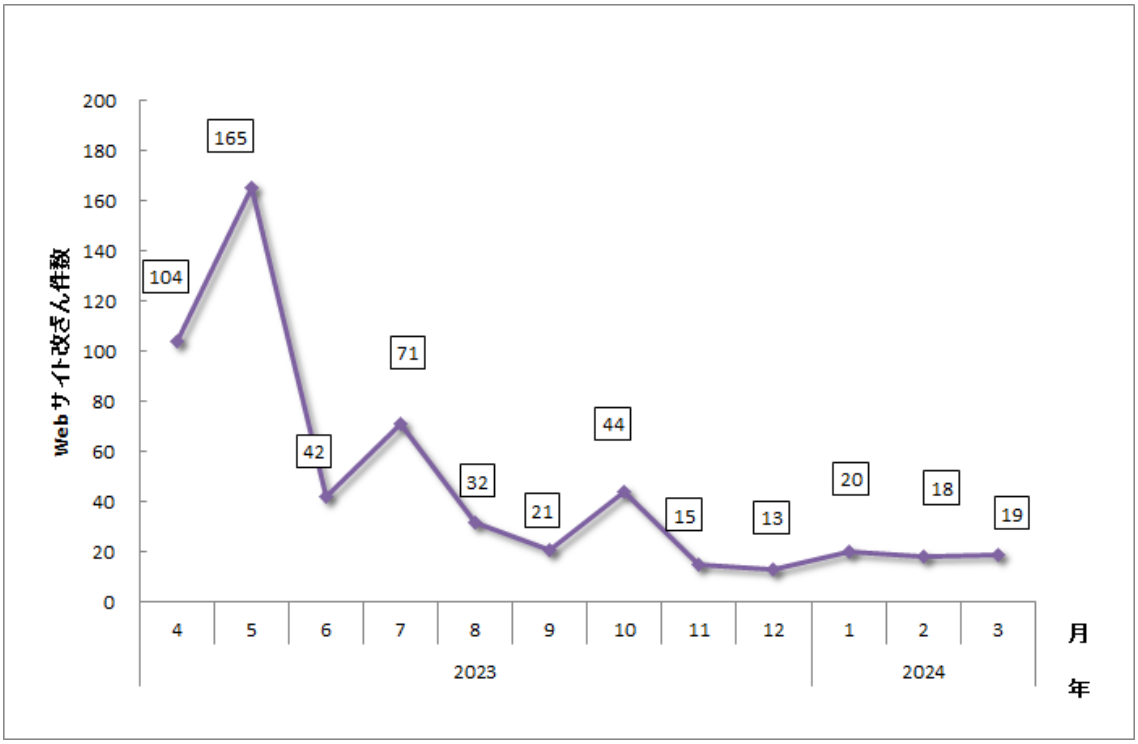
［図 5：インシデント報告件数のカテゴリー別割合］

フィッシングサイトに分類されるインシデントが 79%、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 11%を占めています。

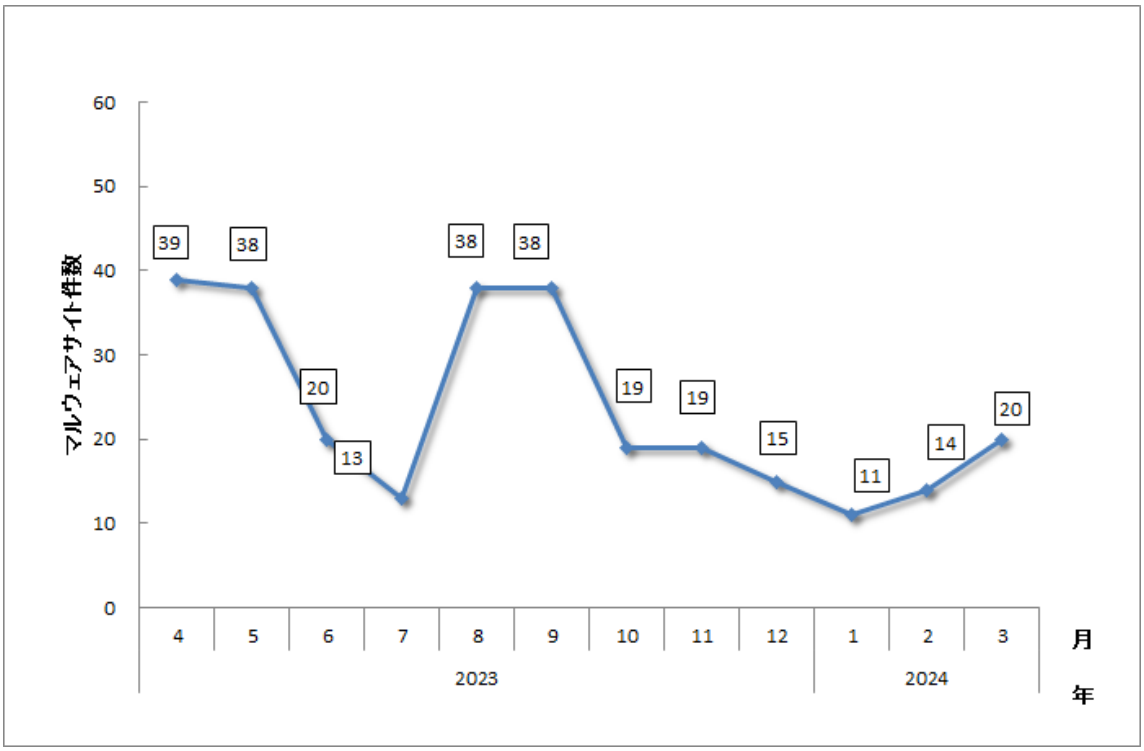
［図 6］から［図 9］に、フィッシングサイト、Web サイト改ざん、マルウェアサイト、スキャンのインシデントの過去 1 年間の月次の推移を示します。



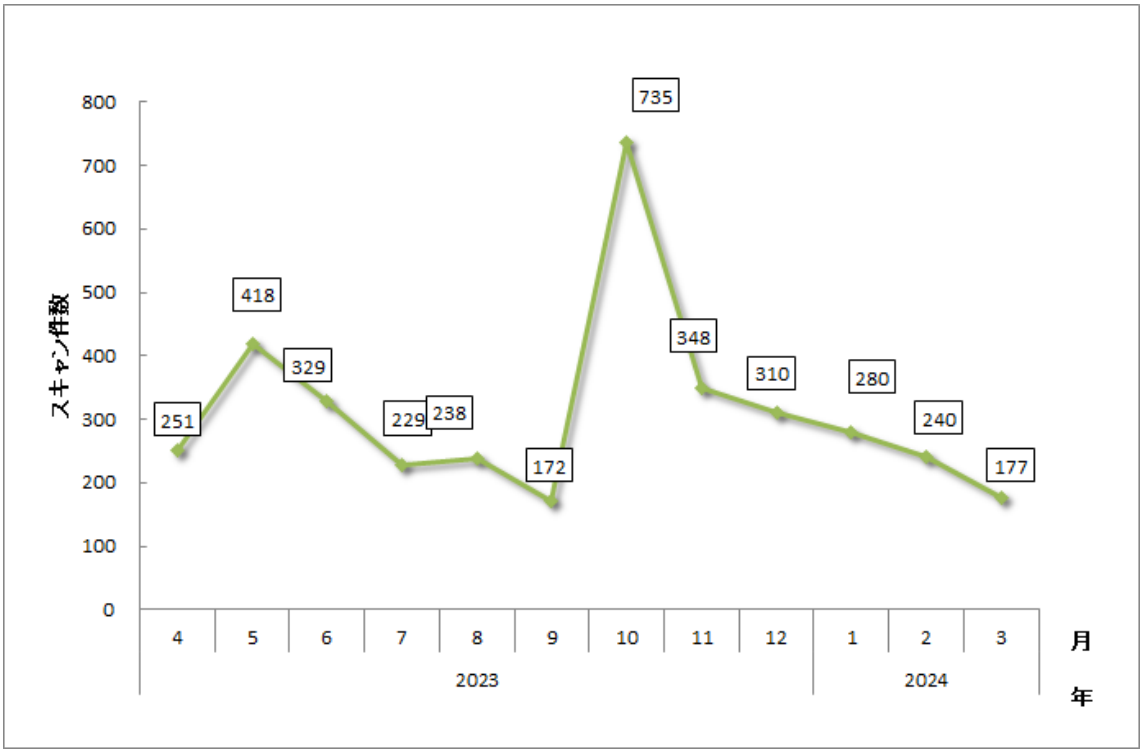
［図 6：フィッシングサイト件数の推移］



［図 7：Web サイト改ざん件数の推移］

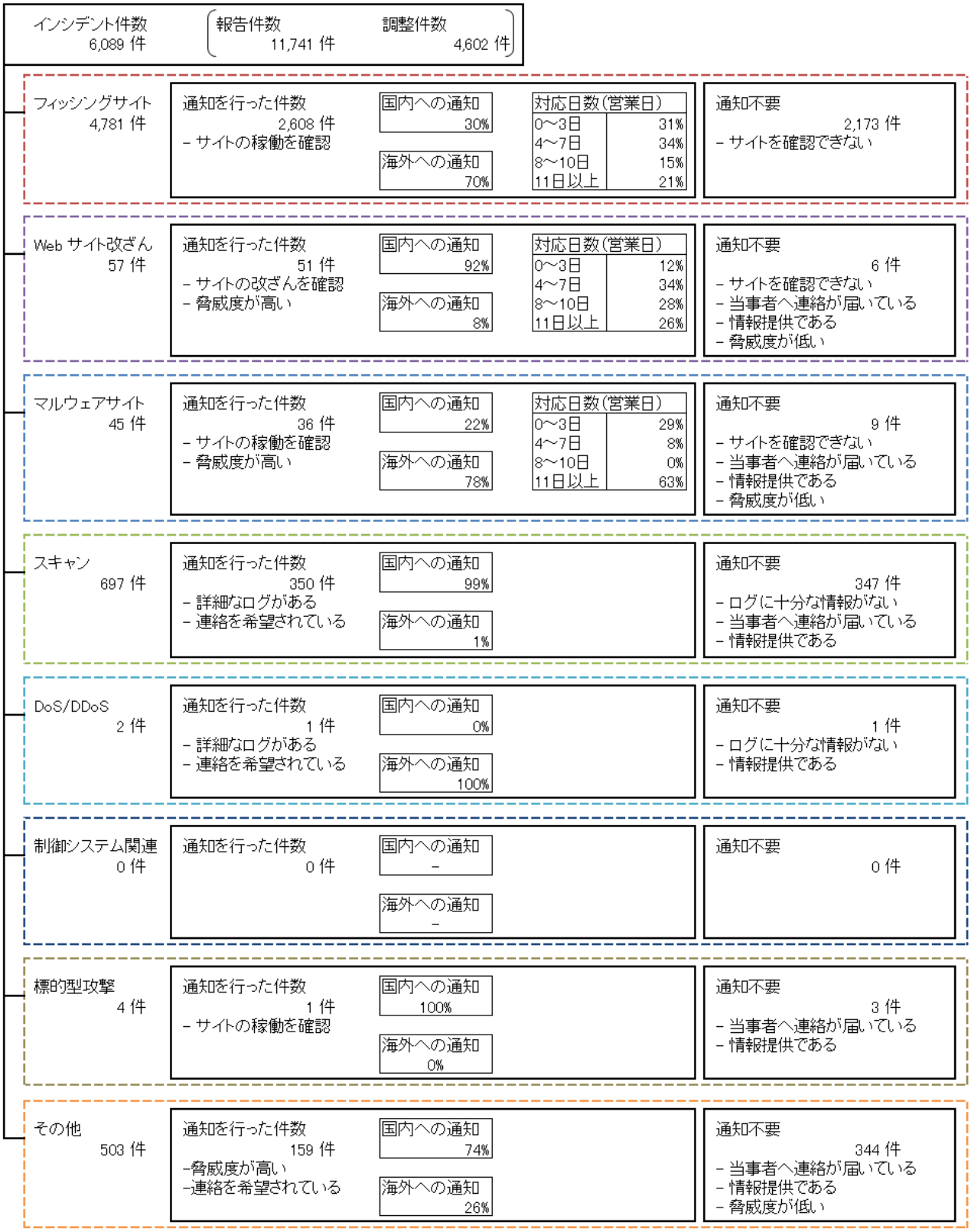


［図 8：マルウェアサイト件数の推移］



［図 9：スキャン件数の推移］

［図 10］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 10：インシデントのカテゴリーごとの件数と調整・対応状況］

3. インシデントの傾向

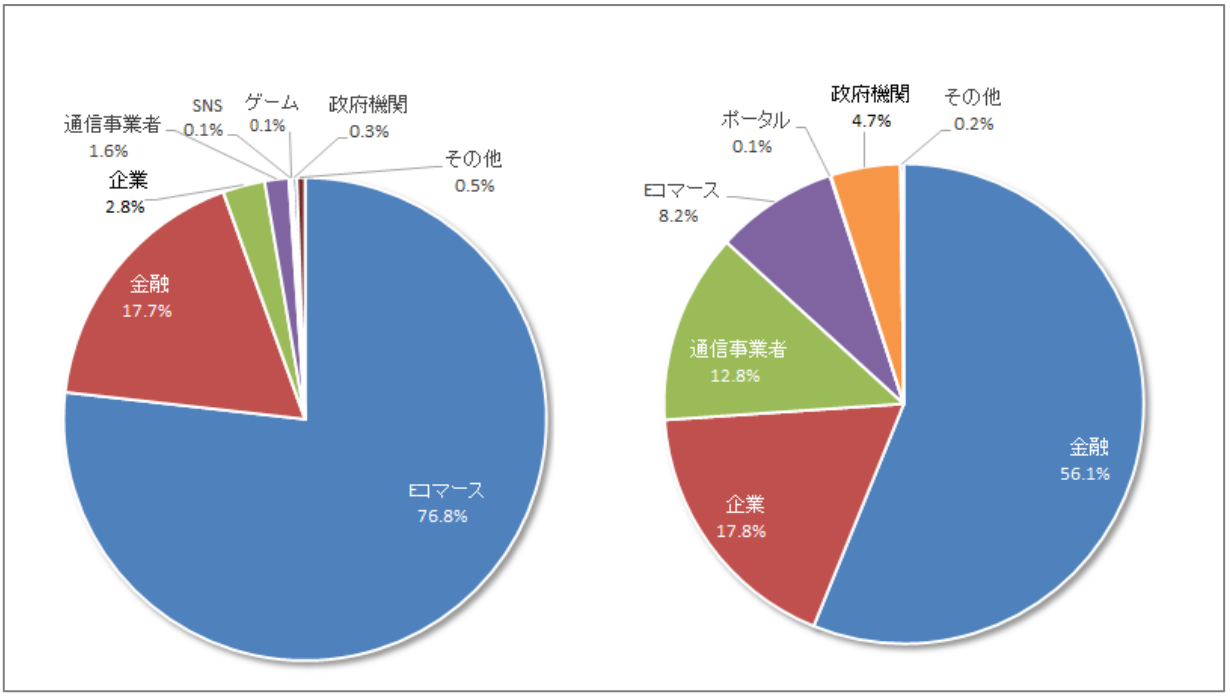
3.1. フィッシングサイトの傾向

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 4,781 件で、前四半期の 4,473 件から 7%増加しました。また、前年度同期（5,553 件）との比較では、14%の減少となりました。
本四半期は、国内のブランドを装ったフィッシングサイトの件数が 3,226 件となり、前四半期の 2,796 件から 15%増加しました。また、国外のブランドを装ったフィッシングサイトの件数は 745 件となり、前四半期の 1,116 件から 33%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を［表 5］、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の件数の業界別の割合を［図 11］に示します。

［表 5：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	1 月	2 月	3 月	本四半期合計（割合）
国内ブランド	1,076	1,134	1,016	3,226 (67%)
国外ブランド	220	145	380	745 (16%)
ブランド不明 (注 5)	243	255	312	810 (17%)
全ブランド合計	1,539	1,534	1,708	4,781

(注 5)「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 11：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の件数の業界別の割合］

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 76.8%、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 56.1%で、それぞれ最も多くを占めました。

海外ブランドでは、Amazon を装ったフィッシングサイトが全体の半数以上を占めました。
国内ブランドでは、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。

フィッシングサイトテイクダウンのために調整したサイトの割合は、国内が 30%、国外が 70%であり、前四半期（国内が 21%、国外が 79%）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 57 件でした。前四半期の 72 件から 21%減少しています。

本四半期は、Web サイトを改ざんし、アクセスしたユーザーを偽物の EC サイトへ転送する事例を複数確認しました。改ざんされた Web サイトには［図 12］のようなスクリプトが設置されており、アクセスした Web ブラウザーの JavaScript 設定に応じて異なる不審なサイトへ誘導する仕組みになっていました。

```
<html lang="jp">
<head>
    <meta content="text/html; charset=utf-8" http-equiv="Content-Type" />
    <meta http-equiv="refresh" content="0; url=https://[redacted]" />
</head>
<body>
  <noscript>
    <meta http-equiv="refresh" content="0; url=https://[redacted]" />
  </noscript>
  <script>
    document.location.href = "https://[redacted]";
  </script>
```

［図 12：不審なサイトを表示するスクリプト］

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 4 件でした。

本四半期は、NOOPDOOR と呼ばれるマルウェアを用いた標的型攻撃の報告が複数寄せられました。初期侵入経路としては VPN の脆弱性などが悪用された可能性が疑われています。攻撃者は、侵入後に複数

の端末に横展開し、NOOPDOOR を設置した。また、攻撃者は設置したマルウェアを最終的に端末から削除しているという特徴も見られます。

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 53 件から 15%減少しました。

本四半期に報告が寄せられたスキャン件数は 697 件でした。前四半期の 1,393 件から 50%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 6］に示します。頻繁にスキャンの対象となったポートは、SSH（22/TCP）、Telnet（23/TCP）、SMTP（25/TCP）、HTTP（80/TCP）でした。

［表 6：ポート別のスキャン件数の上位 10 位］

ポート	1 月	2 月	3 月	合計
22/tcp	107	118	68	293
23/tcp	106	78	80	264
25/tcp	36	23	17	76
80/tcp	14	10	8	32
37215/tcp	9	3	1	13
5888/tcp	5	2	0	7
445/tcp	2	2	0	4
2323/tcp	2	1	1	4
143/tcp	1	2	1	4
443/tcp	1	1	1	3

その他に分類されるインシデントの件数は 503 件でした。前四半期の 455 件から 11%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。

(1) Ivanti Connect Secure の複数の脆弱性への対応

2024 年 1 月 10 日、Ivanti 社は Ivanti Connect Secure（旧称：Pulse Connect Secure）および Ivanti Policy Secure ゲートウェイに脆弱性があることを公表しました。公表されたものに、認証バイパスの脆弱性（CVE-2023-46805）とコマンドインジェクションの脆弱性（CVE-2024-21887）が含まれており、これらを悪用することで遠隔の第三者が任意のコマンドを実行できます。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 1 月 11 日に注意喚起を行いました。その後さらに Ivanti

社から関連する複数の脆弱性が公表されました。その中に、権限昇格の脆弱性（CVE-2024-21888）、SSRF の脆弱性（CVE-2024-21893）および XML 外部実体参照の脆弱性（CVE-2024-22024）が含まれていたことから、JPCERT/CC では 2 月 21 日に対策と悪用事例を整理した資料を公開しました。

Ivanti Connect Secure および Ivanti Policy Secure の脆弱性（CVE-2023-46805 および CVE-2024-21887）に関する注意喚起
https://www.jpcert.or.jp/at/2024/at240002.html

2024 年 1 月以降の Ivanti Connect Secure などの脆弱性の状況について
https://www.jpcert.or.jp/newsflash/2024021601.html

JPCERT/CC では、外部組織から提供された情報をもとに、Web シェルやバックドアが設置されたと疑われる機器および脆弱性が未修正で侵害され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して通知を行いました。
また、JPCERT/CC では複数の組織からこれらの脆弱性によって被害を受けたとの相談を受けており、脆弱性が公開された直後の 1 月 11 日から WIREFIRE と呼ばれる Web シェルや ZIPLINE と呼ばれるバックドアが設置された事例を複数確認しています。本脆弱性を攻撃する PoC が公開された 1 月 16 日以降には、機器に仮想通貨マイニングツールを設置するような攻撃も確認されています。一部の組織では Ivanti 製品の内部整合性チェックツールが改ざんされ、設置された Web シェルやバックドアを検知できなくなっていました。

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.jpcert.or.jp/form/

インシデントの報告（Web フォーム）
https://form.jpcert.or.jp/

制御システムインシデントの報告
https://www.jpcert.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.jpcert.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.jpcert.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.jpcert.or.jp/announce.html

付録-1. 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

本活動は、経済産業省より委託を受け、「令和 5 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。