JPCERT Coordination Center

JPCERT/CC インシデント報告対応レポート

2023 年 7 月 1 日 ～ 2023 年 9 月 30 日

一般社団法人 JPCERT コーディネーションセンター

2023 年 10 月 17 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、2023 年 7 月 1 日から 2023 年 9 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。

（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］

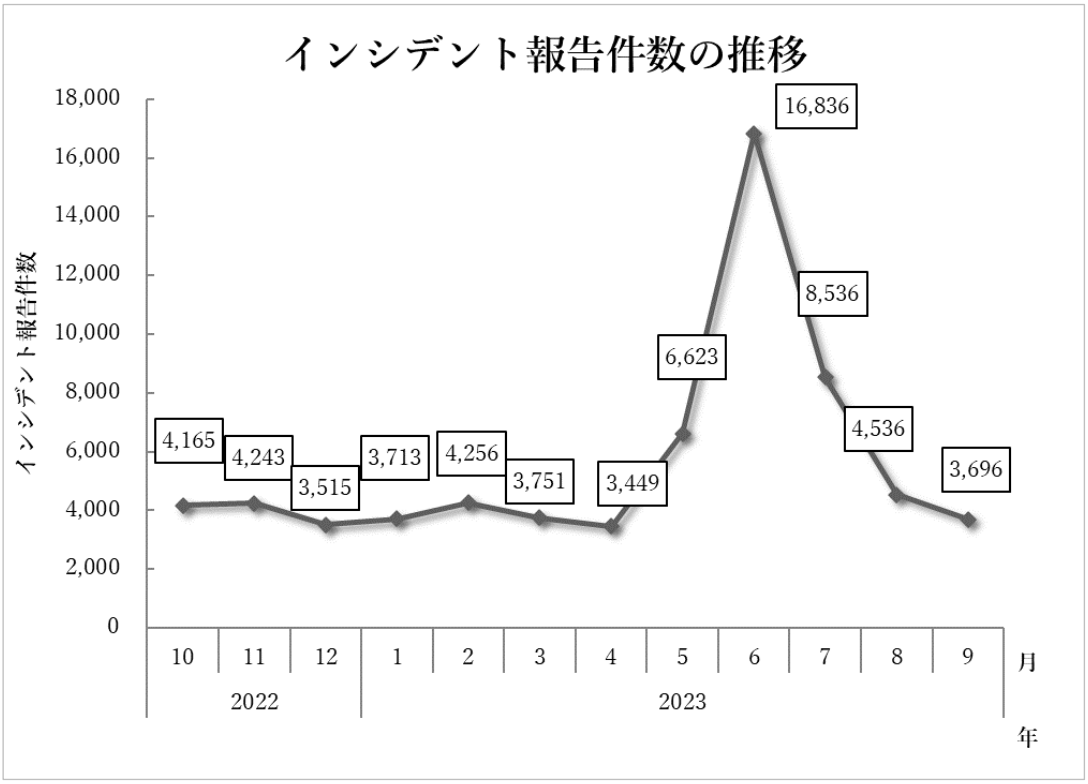
	7 月	8 月	9 月	合計	前四半期合計
報告件数（注 2）	8,536	4,536	3,696	16,768	26,908
インシデント件数（注 3）	2,157	1,952	1,794	5,903	7,925
調整件数（注 4）	1,574	1,856	1,640	5,070	4,604

（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。

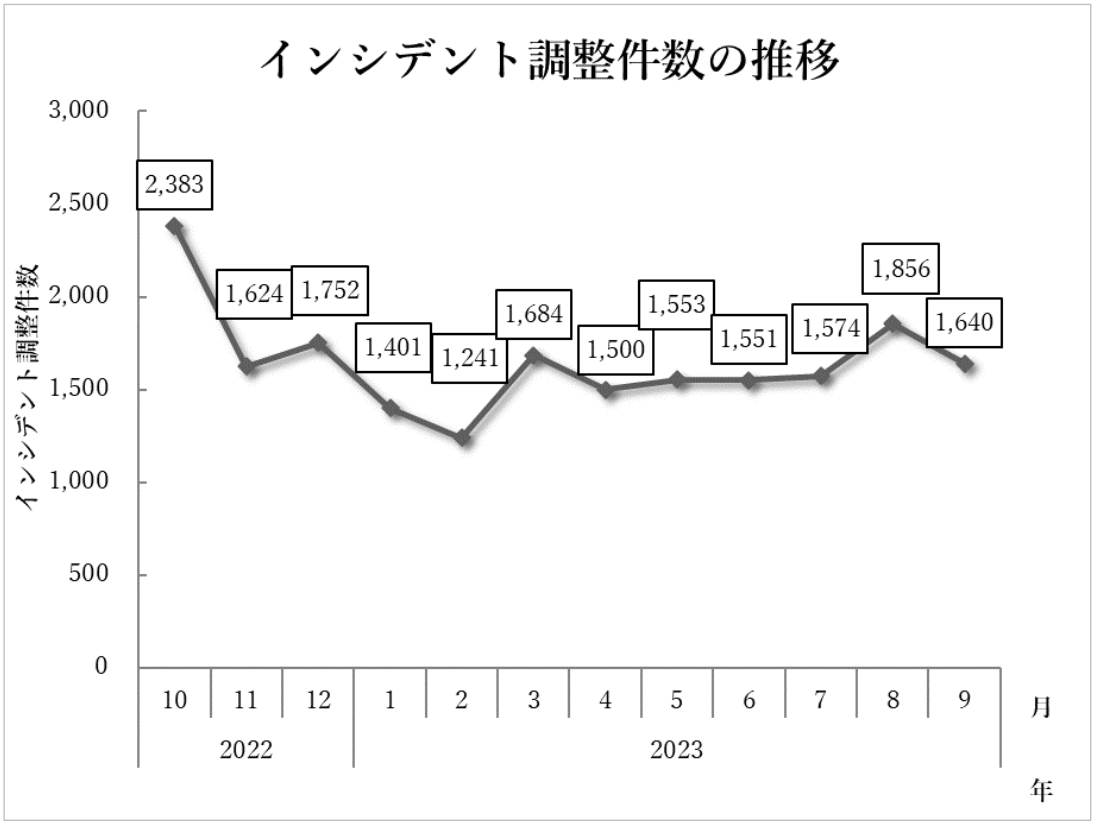
（注 3）「インシデント件数」は、各報告に含まれるインシデント件数の合計を示します。1 つのインシデントに関して複数件の報告が寄せられた場合にも、1 件として扱います。

（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、16,768 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 5,070 件でした。前四半期と比較して、報告件数は 38%減少し、調整件数は 10%増加しました。また、前年同期と比較すると、報告数は 24%増加し、調整件数は 21%減少しました。［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］

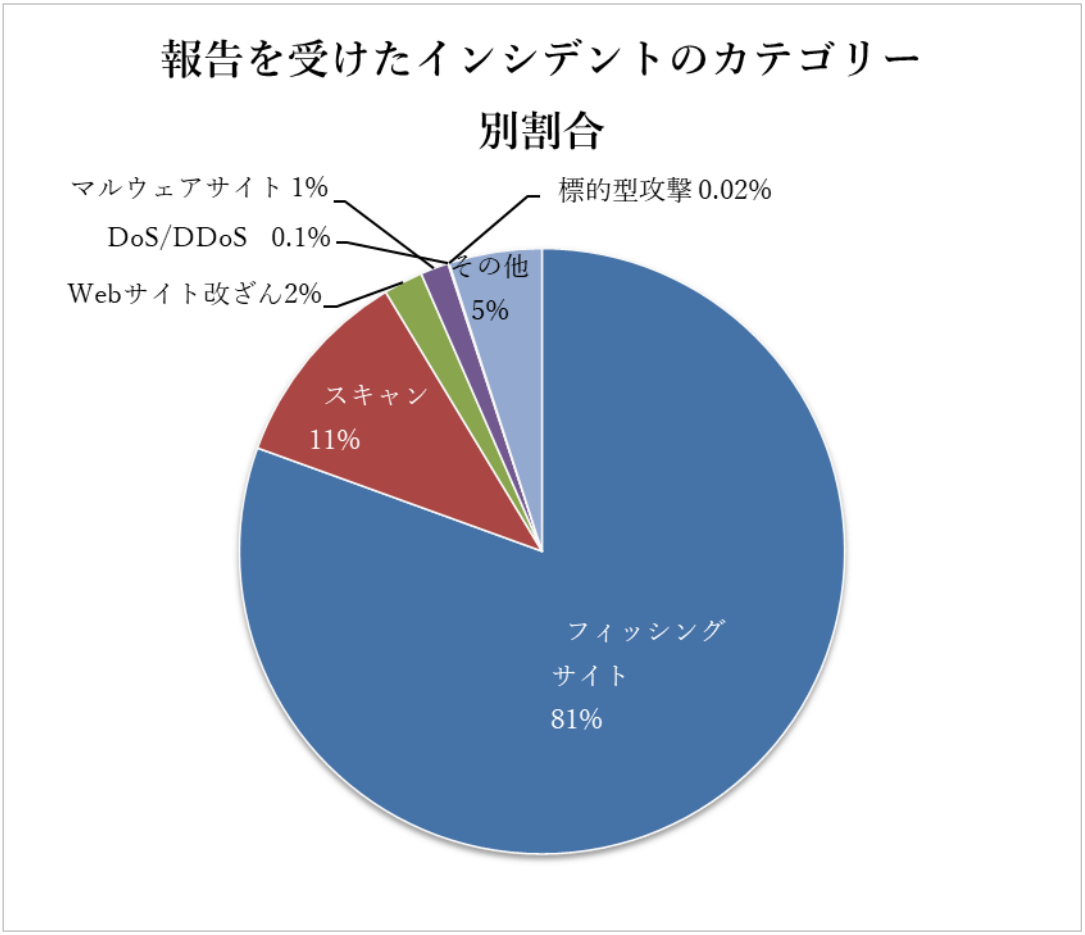


［図 2：インシデント調整件数の推移］

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。本四半期に報告を受けたインシデントの件数のカテゴリーごとの数を［表 2］に示します。また、カテゴリーの割合で示すと［図 3］のとおりです。

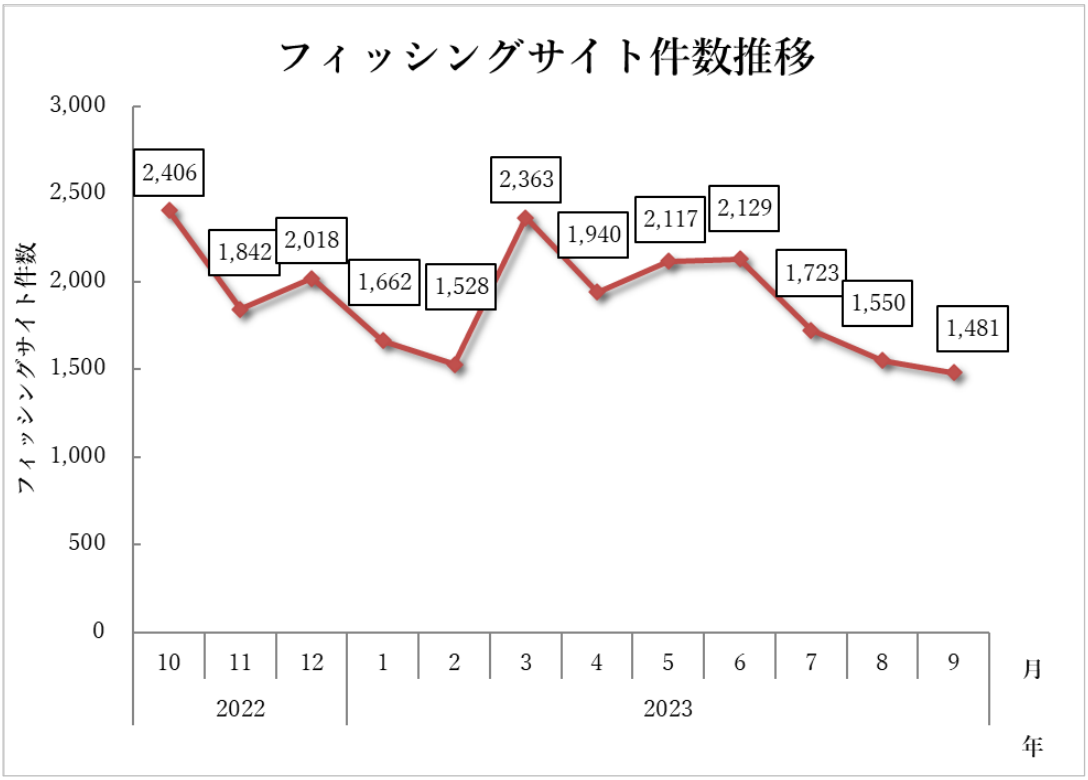
［表 2：報告を受けたインシデントのカテゴリーごとの数］

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	1,723	1,550	1,481	4,754	6,186
Web サイト改ざん	71	32	21	124	311
マルウェアサイト	13	38	38	89	97
スキャン	229	238	172	639	998
DoS/DDoS	0	0	3	3	8
制御システム関連	0	0	0	0	1
標的型攻撃	1	1	0	2	4
その他	120	93	79	292	320

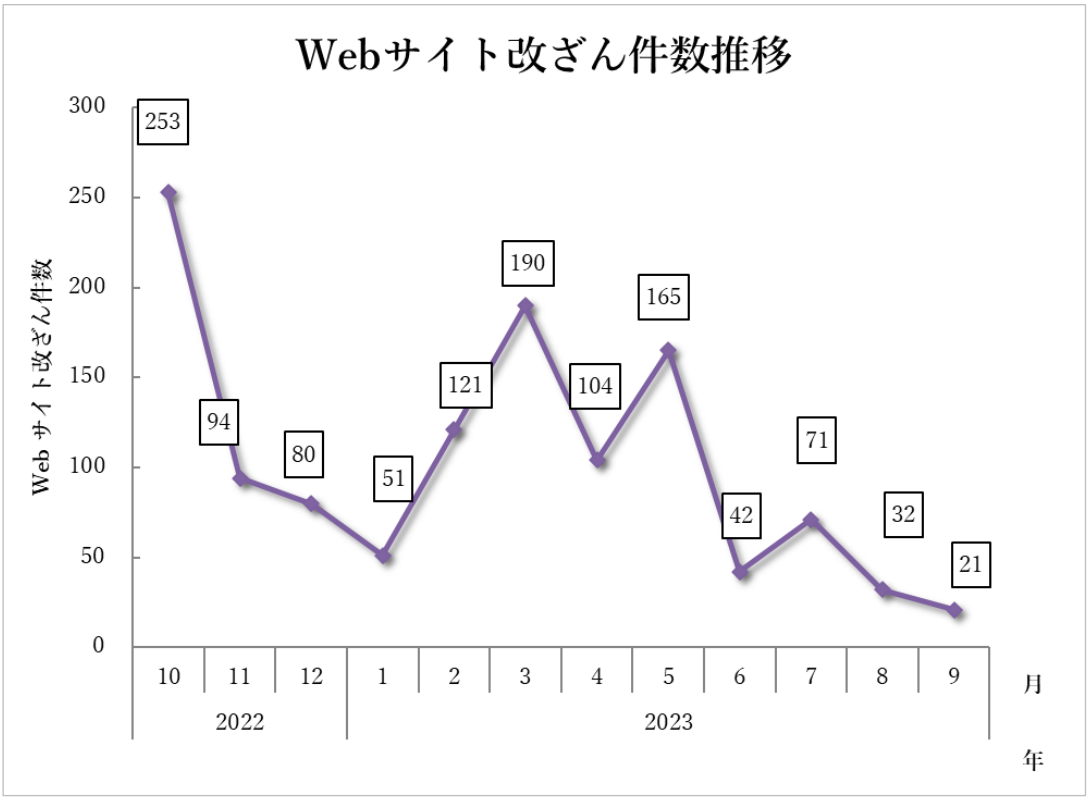


［図 3：報告を受けたインシデントのカテゴリー別割合］

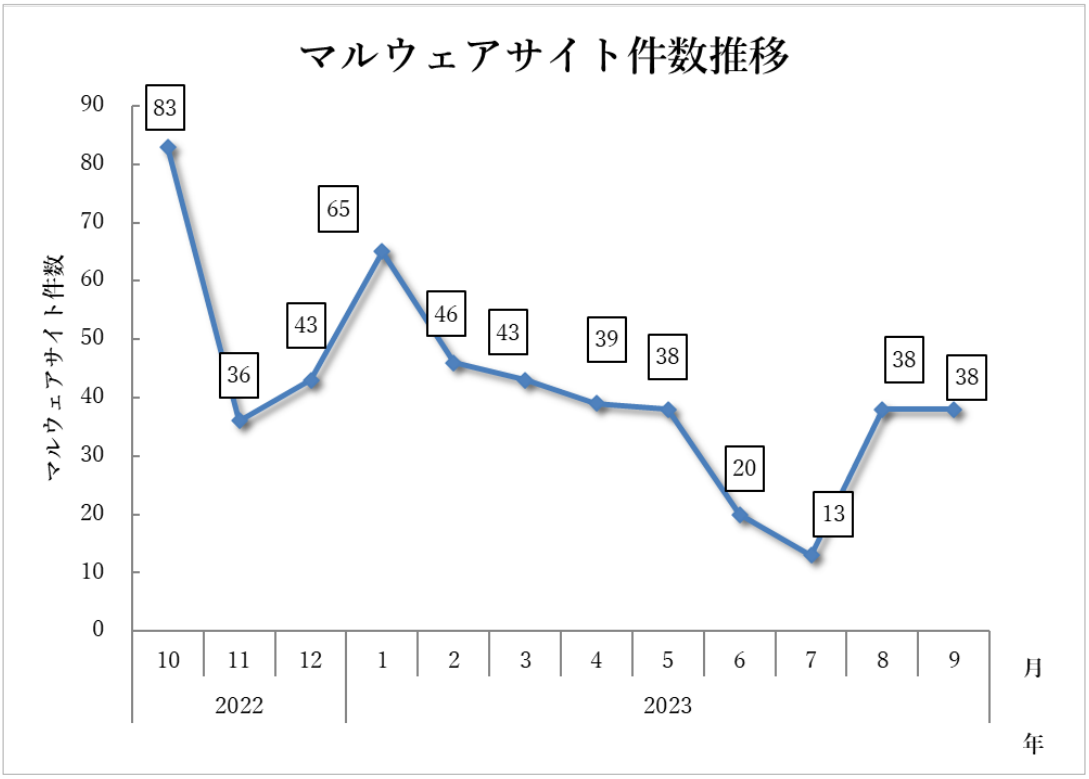
フィッシングサイトに分類されるインシデントが 81%、スキャンに分類される、システムの弱点を探索するインシデントが 11%を占めています。
［図 4］から［図 7］に、フィッシングサイト、Web サイト改ざん、マルウェアサイト、スキャンのインシデントの過去 1 年間の月次の推移を示します。



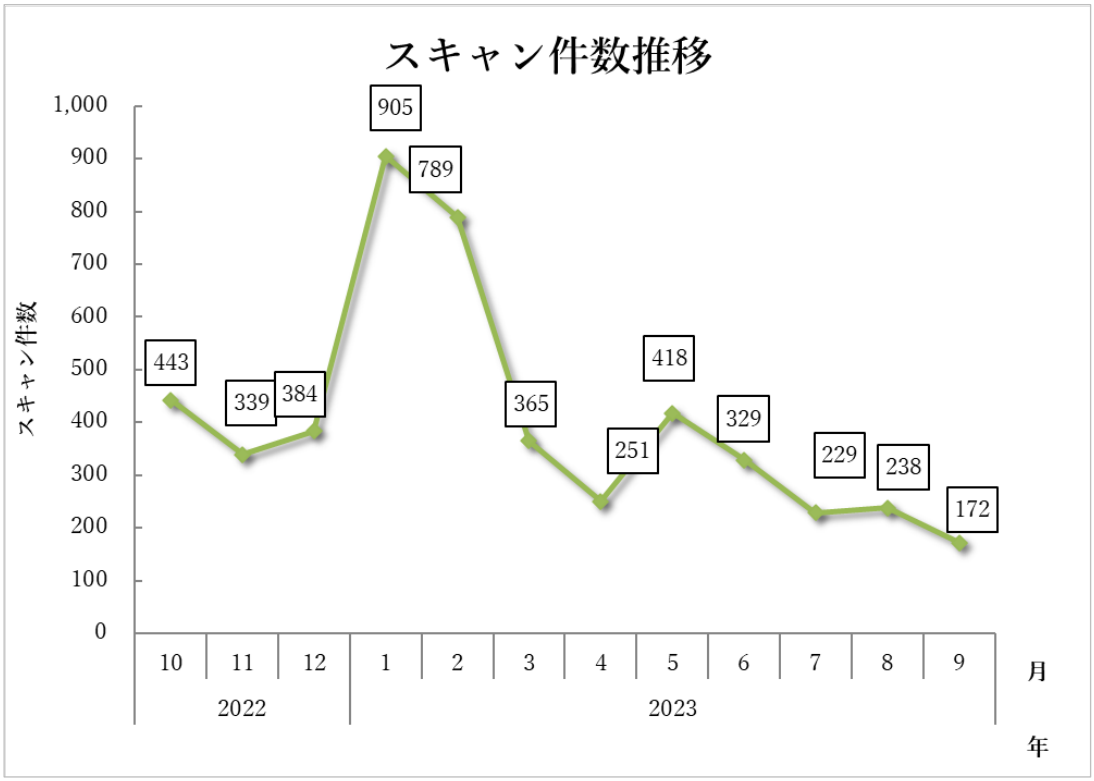
［図 4：フィッシングサイト件数の推移］



［図 5：Web サイト改ざん件数の推移］

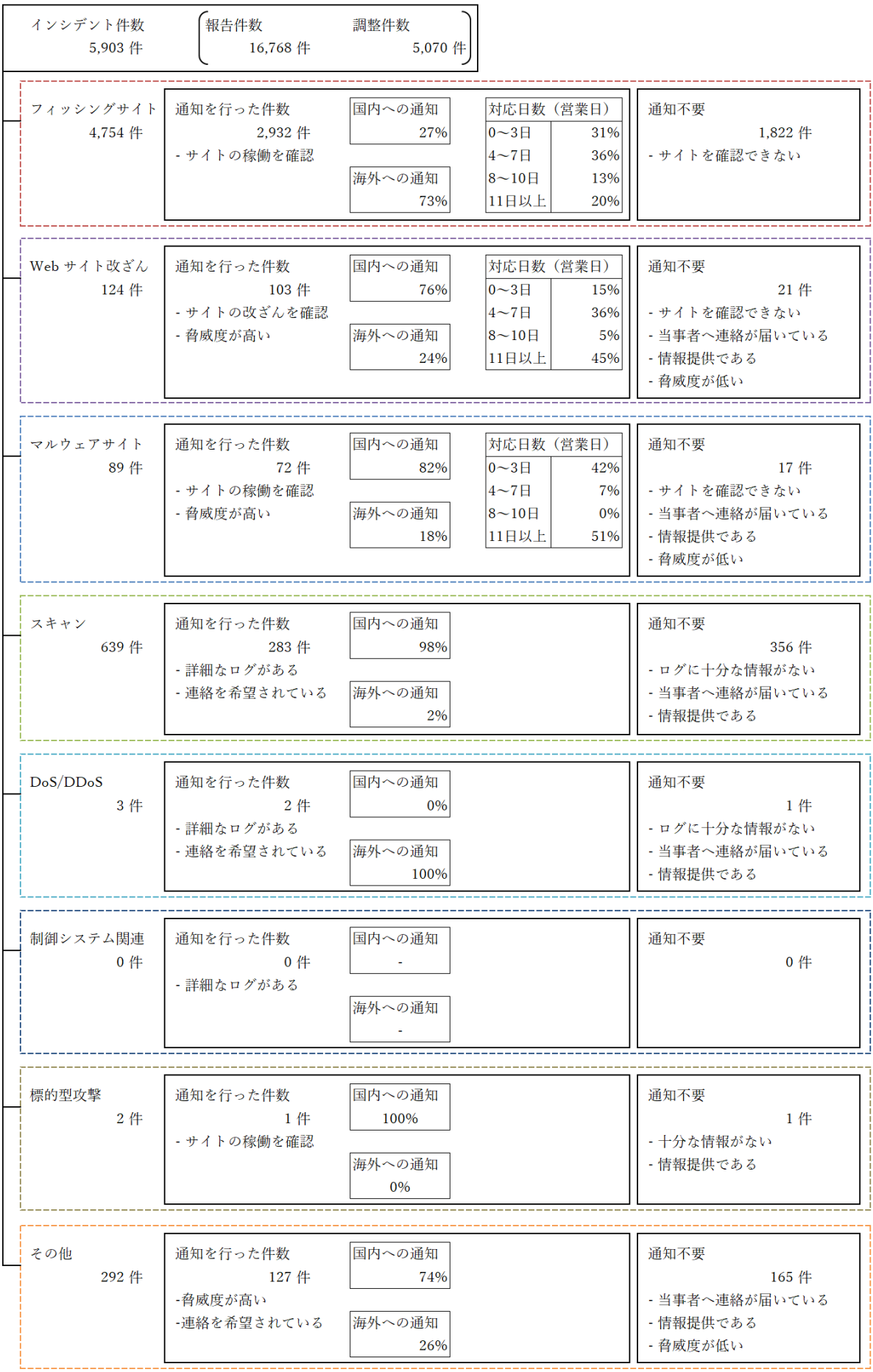


［図 6：マルウェアサイト件数の推移］



［図 7：スキャン件数の推移］

［図 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 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］

3. インシデントの傾向

3.1. フィッシングサイトの傾向

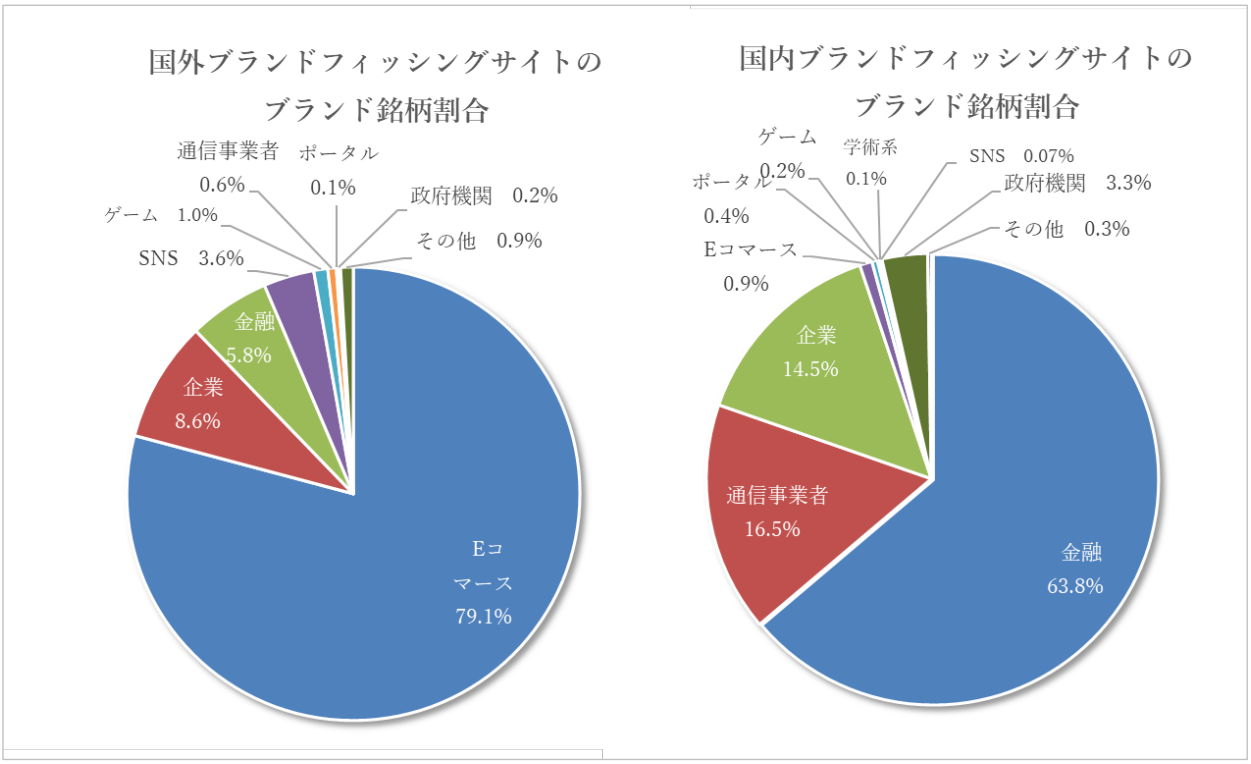
本四半期に報告が寄せられたフィッシングサイトの件数は 4,754 件で、前四半期の 6,186 件から 23%減少しました。また、前年度同期（7,520 件）との比較では、37%の減少となりました。

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 3,029 件となり、前四半期の 3,700 件から 18%減少しました。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 997 件となり、前四半期の 1,568 件から 36%減少しました。本四半期のフィッシングサイトが装ったブランドの国内・国外別数を［表 3］、国内・国外ブランドの業界別数を［図 9］に示します。

［表 3：フィッシングサイト件数の国内・国外ブランド別数］

フィッシングサイト	7 月	8 月	9 月	本四半期合計（割合）
国内ブランド	1,052	980	997	3,029 (64%)
国外ブランド	438	310	249	997 (21%)
ブランド不明 (注 5)	233	260	235	728 (15%)
全ブランド合計	1,723	1,550	1,481	4,754

(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 9：フィッシングサイトのブランド銘柄割合（国内・国外別）］

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 79.1%、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 63.8%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ていました。
国内ブランドでは、JR 東日本が提供する Web サイト「えきねっと」や、ETC の利用照会サービス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、セゾンカード、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。前四半期と比較すると、TEPCO、モバイル Suica、横浜銀行、厚生労働省、au じぶん銀行を装ったフィッシングサイト数の減少が目立ちました。

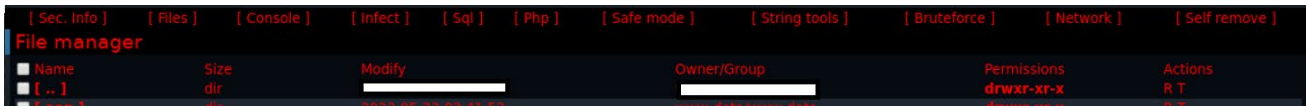
フィッシングサイトテイクダウンのために調整したサイトの割合は、国内が 27%、国外が 78%であり、前四半期（国内が 25%、国外が 75%）と比較しほぼ同じ割合となりました。

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、124 件でした。前四半期の 311 件から 60%減少しています。

本四半期は、不審なサイトへの転送スクリプト（［図 10］）を挿入する事例やフィッシングキットを設置事例、メール送信プログラムを設置する事例など、正規の Web サイトに対するさまざまな攻撃を確認しました。これらの Web サイトには［図 11］のような WebShell が設置され、外部からサーバー内のファイルの閲覧やファイルのアップロード・ダウンロード、任意のコマンドを実行することが可能になっていました。

［図 10：不正に挿入された転送スクリプトの例］

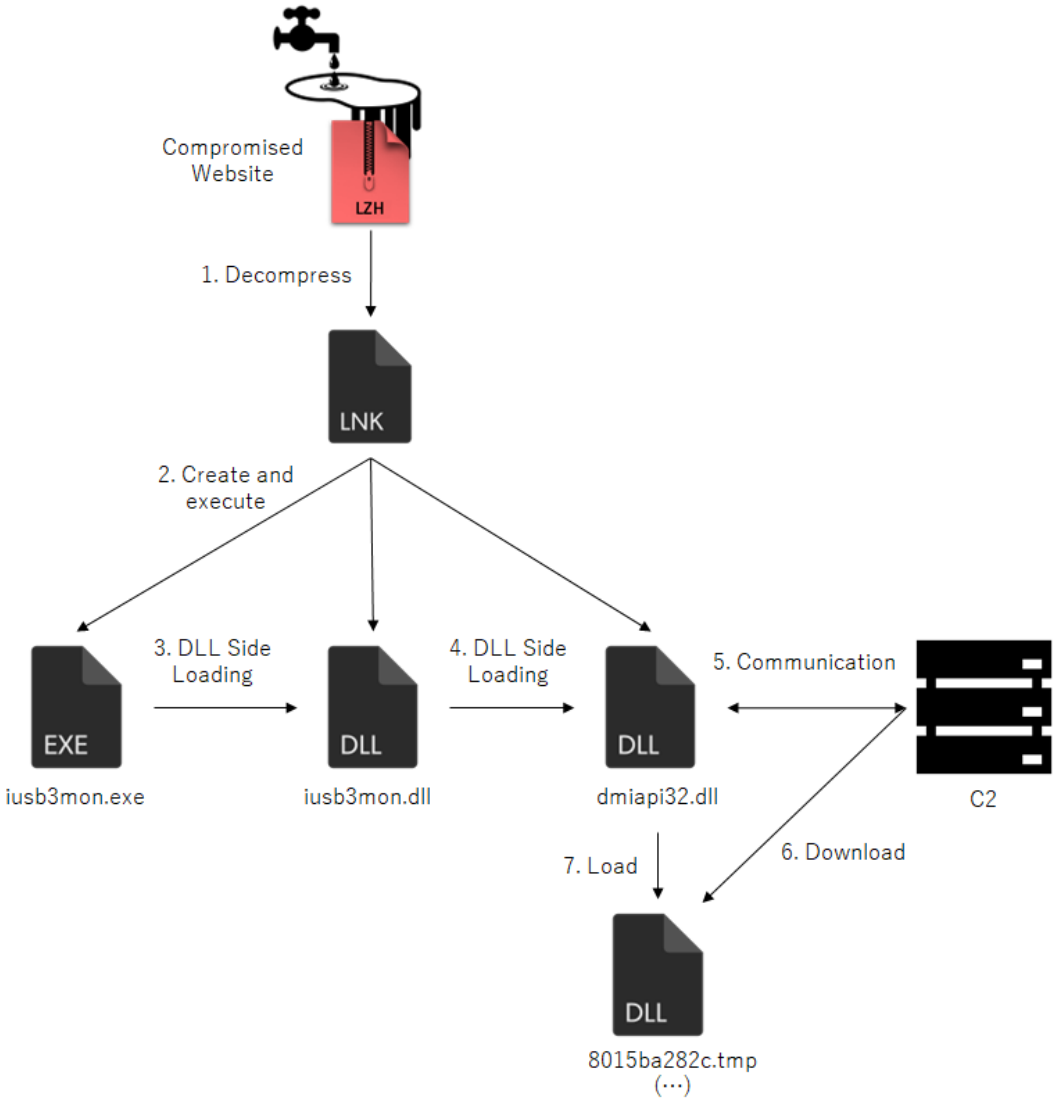


［図 11：不正に設置された WebShell の例］

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。そのうちの確認されたインシデントの例を紹介します。

本四半期は、有料会員向け購読サービスを提供している Web サイトが改ざんされ、有料コンテンツにアクセスしたユーザーが不正に設置されたマルウェアをダウンロードさせられる報告が寄せられました。ユーザーが改ざんされた Web サイトにアクセスすると LZH 形式の圧縮ファイルがダウンロードされ、その中のファイルを実行するとマルウェアに感染します。圧縮ファイルの中にはショートカットファイルが格納されており、ショートカットファイルを実行すると、端末内に複数のファイルが生成され、最終的に攻撃者のサーバーと通信し、追加のマルウェアがダウンロードされます。LZH 形式の圧縮ファイルを実行後、マルウェアに感染するまでの流れを［図 12］に示します。



［図 12：改ざんされた Web サイトからマルウェアが感染するまでの流れ］

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 89 件でした。前四半期の 97 件から 8%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639件でした。前四半期の998件から36%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 4］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）、HTTP（80/TCP）、37215/TCP、52869/TCP でした。

［表 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
22/tcp	112	125	85	322
23/tcp	50	66	55	171
80/tcp	21	12	7	40
37215/tcp	13	20	2	35
52869/tcp	12	5	0	17
445/tcp	1	2	8	11
443/tcp	9	1	1	11
25/tcp	5	1	4	10
8080/tcp	6	0	0	6
5555/tcp	2	0	1	3

その他に分類されるインシデントの件数は、292件でした。前四半期の320件から9%減少しました。

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) Citrix ADC および Citrix Gateway の脆弱性（CVE-2023-3519）への対応

2023年7月18日に、Citrix社はCitrix ADC および Citrix Gatewayにおける複数の脆弱性に関する情報を公開しました。これら脆弱性が悪用されると、認証されていない遠隔の第三者が任意のコードを実行するなどの可能性があることから JPCERT/CC でも7月19日に注意喚起を行っています。

Citrix ADC および Citrix Gateway の脆弱性（CVE-2023-3519）に関する注意喚起
https://www.jpcert.or.jp/at/2023/at230013.html

JPCERT/CC には、国内の組織から本脆弱性を悪用したと思われるアクセス試行があったとの報告が寄せられています。影響を受ける製品を利用している場合には速やかな対策をお願いします。

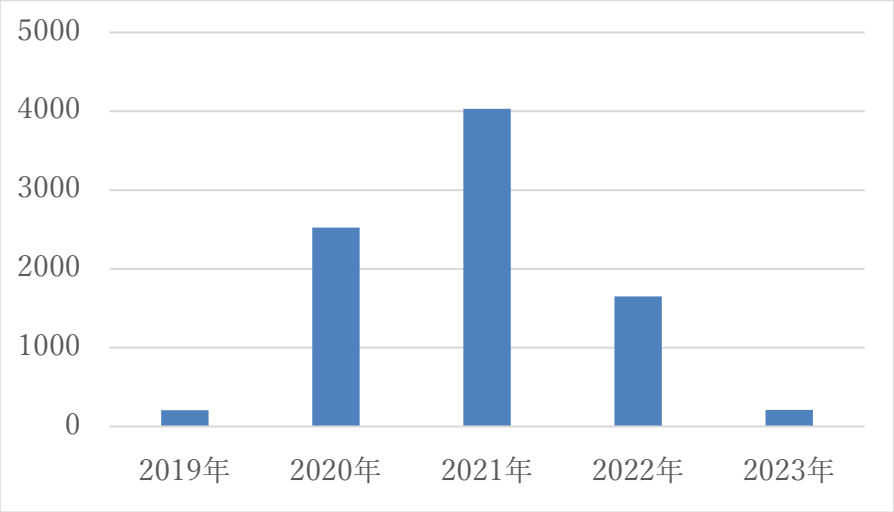
また、本脆弱性を修正するパッチを適用しても、パッチ適用前に攻撃者が設置したバックドアが残っている場合があります。JPCERT/CC ではバックドアが設置されていると思われる国内のデバイスの管理者に対して通知を行いました。

(2) Qakbot 感染端末への通知

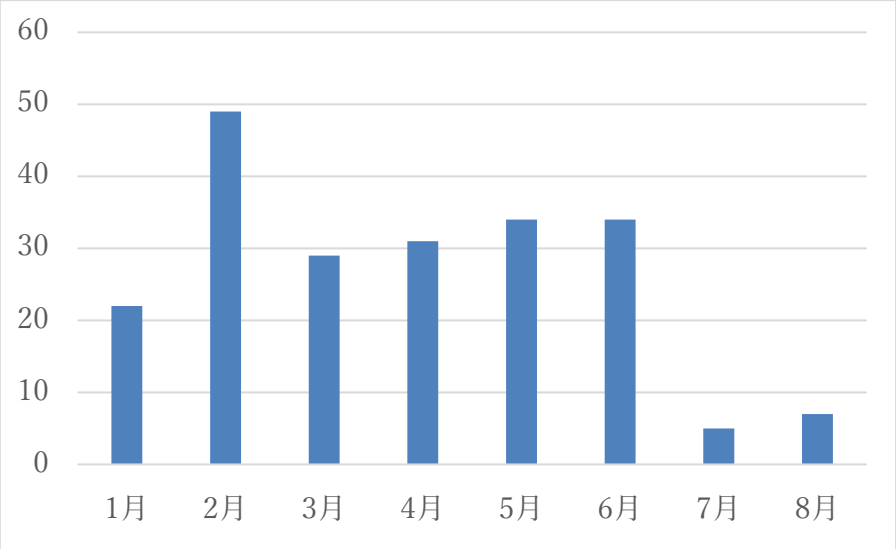
2023 年 8 月に、アメリカを中心とした 7 カ国の国際チームによってマルウェア Qakbot のテイクダウン作戦「Operation Duck Hunt」が実施されました。その結果、Qakbot の C2 サーバーが停止され、Qakbot の感染端末から Qakbot が削除されました。そして、Qakbot に感染した端末情報やアカウント情報が特定され、日本国内で感染した端末の情報（感染時期は、2019 年から 2023 年 8 月まで）が 9 月に JPCERT/CC に提供されました。

JPCERT/CC に提供された感染端末情報（4 万件）のうち約 80%は研究者の試験用端末に関するものと考えられます。そのような試験用端末の情報を除いた感染端末数をグラフにしたものが［図 13］です。ピークは 2021 年で、その後減少傾向にありました。さらに、2023 年の月毎の感染端末数をグラフにしたものが［図 14］です。現時点では、2021 年と比較すると感染端末が大幅に減少していることが分かります。

このデータをもとに JPCERT/CC では、現在でも Qakbot に感染している恐れがある端末のユーザーに対してネットワーク事業者を通じて通知を行っています。



［図 13：Qakbot 感染端末数の推移（年単位）］



［図 14：Qakbot 感染端末数の 2023 年の推移（月単位）］

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。