JPCERT/CC インシデント報告対応レポート

2023 年 10 月 1 日 ～ 2023 年 12 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 1 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、2023 年 10 月 1 日から 2023 年 12 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 など）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

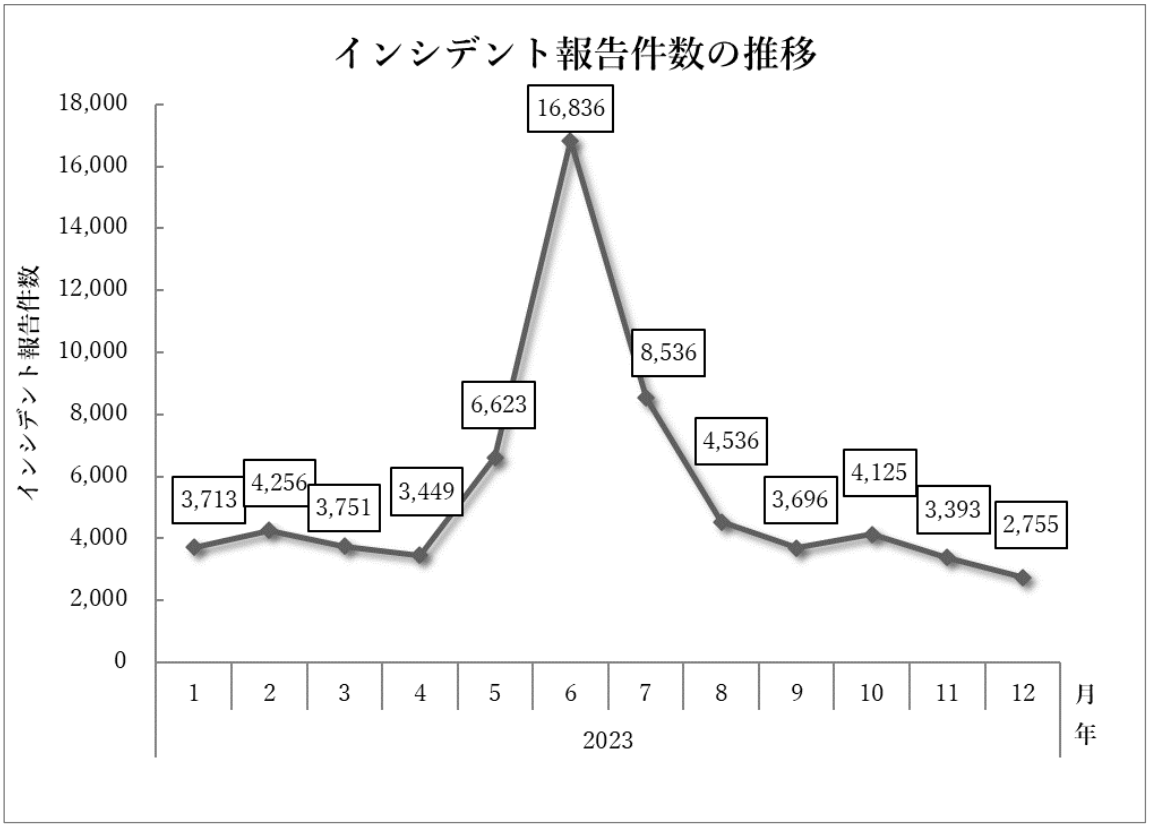
本四半期のインシデント報告の数、報告されたインシデントの総数、および、報告に対応して JPCERT/CC が行った調整の件数を［表 1］に示します。

［表 1：インシデント報告関連件数］

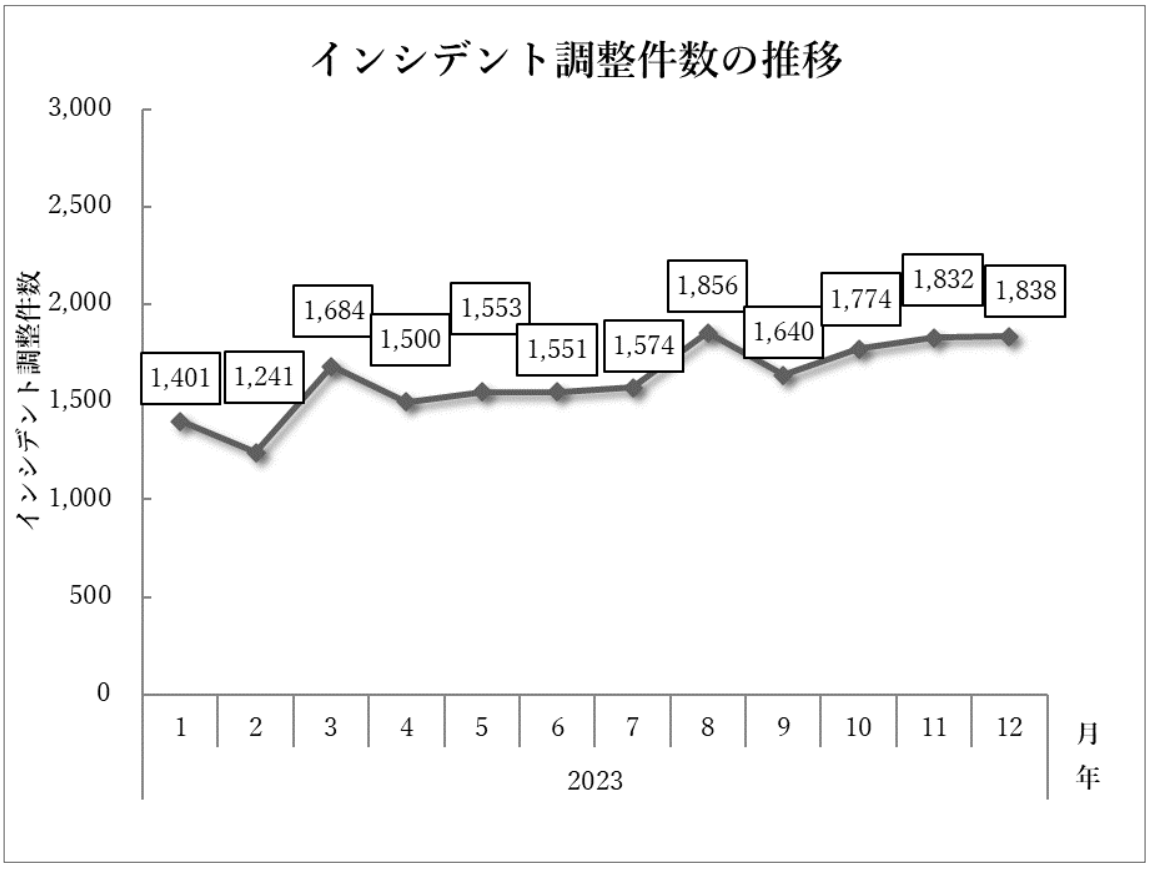
	10 月	11 月	12 月	合計	前四半期合計
報告件数 (注 2)	4,125	3,393	2,755	10,273	16,768
インシデント件数 (注 3)	2,386	2,164	1,898	6,448	5,903
調整件数 (注 4)	1,774	1,832	1,838	5,444	5,070

（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、サイトの管理者などに対し、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、10,273 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 5,444 件でした。前四半期と比較して、報告件数は 39%減少し、調整件数は 7%増加しました。また、前年同期と比較すると、報告数は 13.8%減少し、調整件数は 5%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］

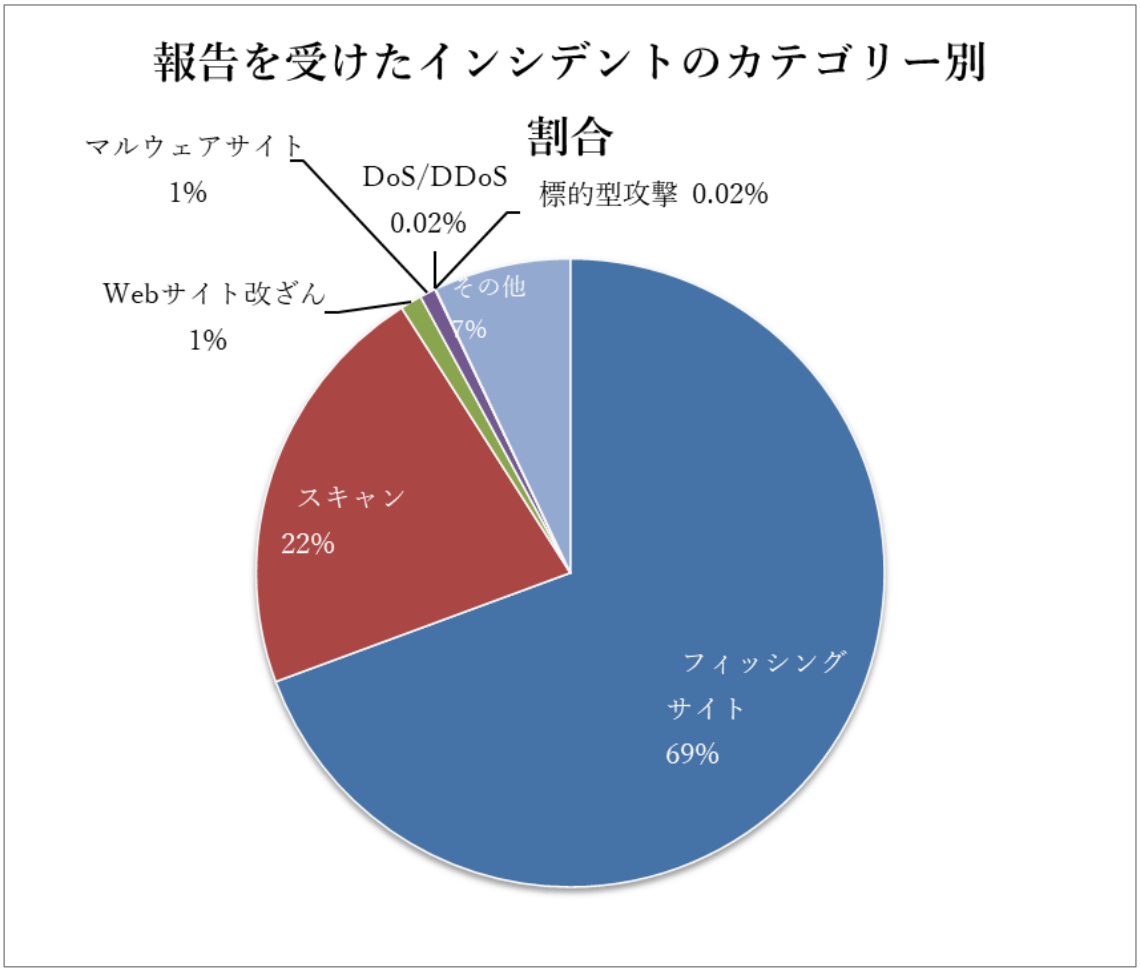


［図 2：インシデント調整件数の推移］

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。

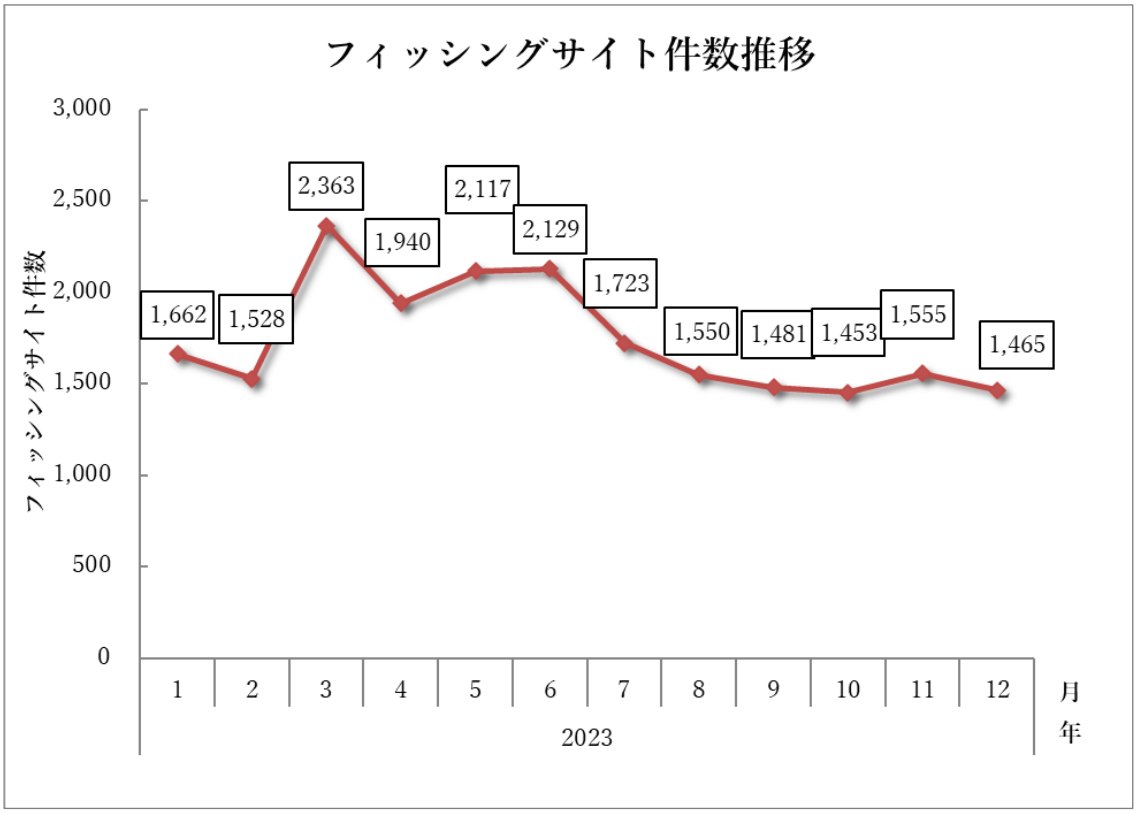
［表 2：報告を受けたインシデントのカテゴリーごとの数］

インシデント	10 月	11 月	12 月	合計	前四半期合計
フィッシングサイト	1,453	1,555	1,465	4,473	4,754
Web サイト改ざん	44	15	13	72	124
マルウェアサイト	19	19	15	53	89
スキャン	735	348	310	1,393	639
DoS/DDoS	1	0	0	1	3
制御システム関連	0	0	0	0	0
標的型攻撃	0	0	1	1	2
その他	134	227	94	455	292

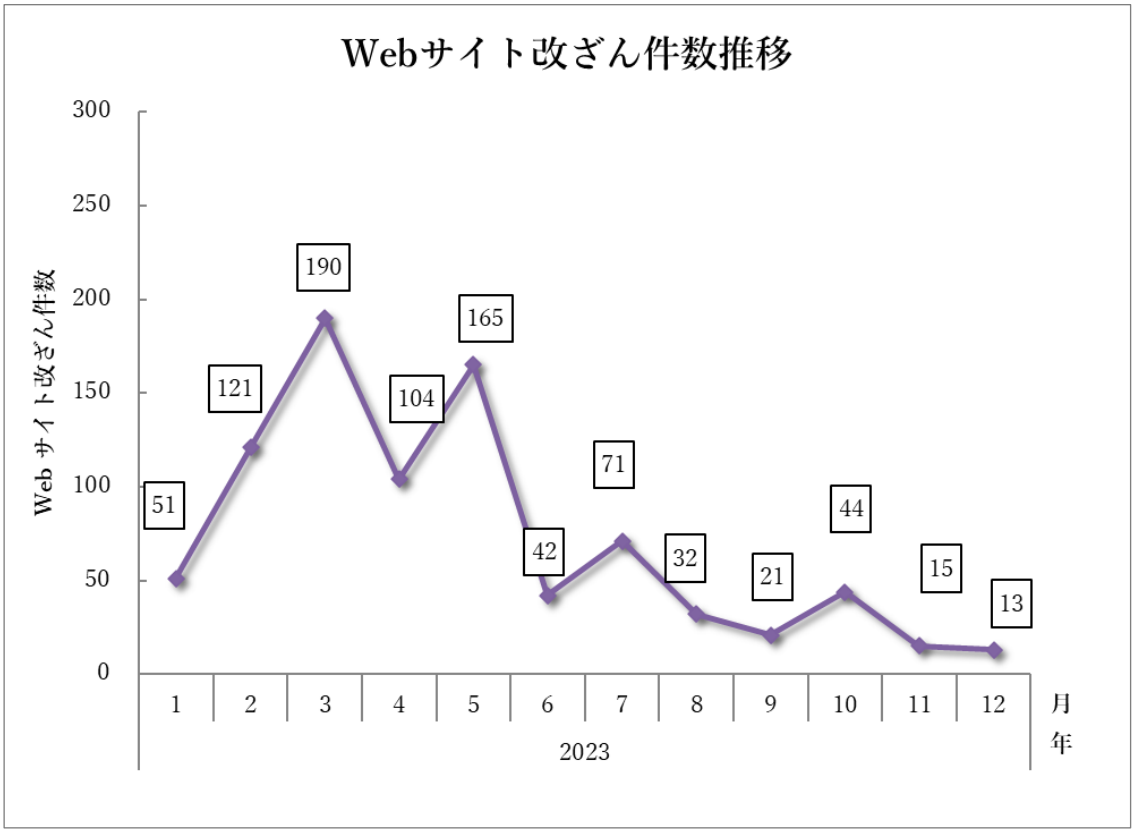


［図 3：報告を受けたインシデントのカテゴリー別割合］

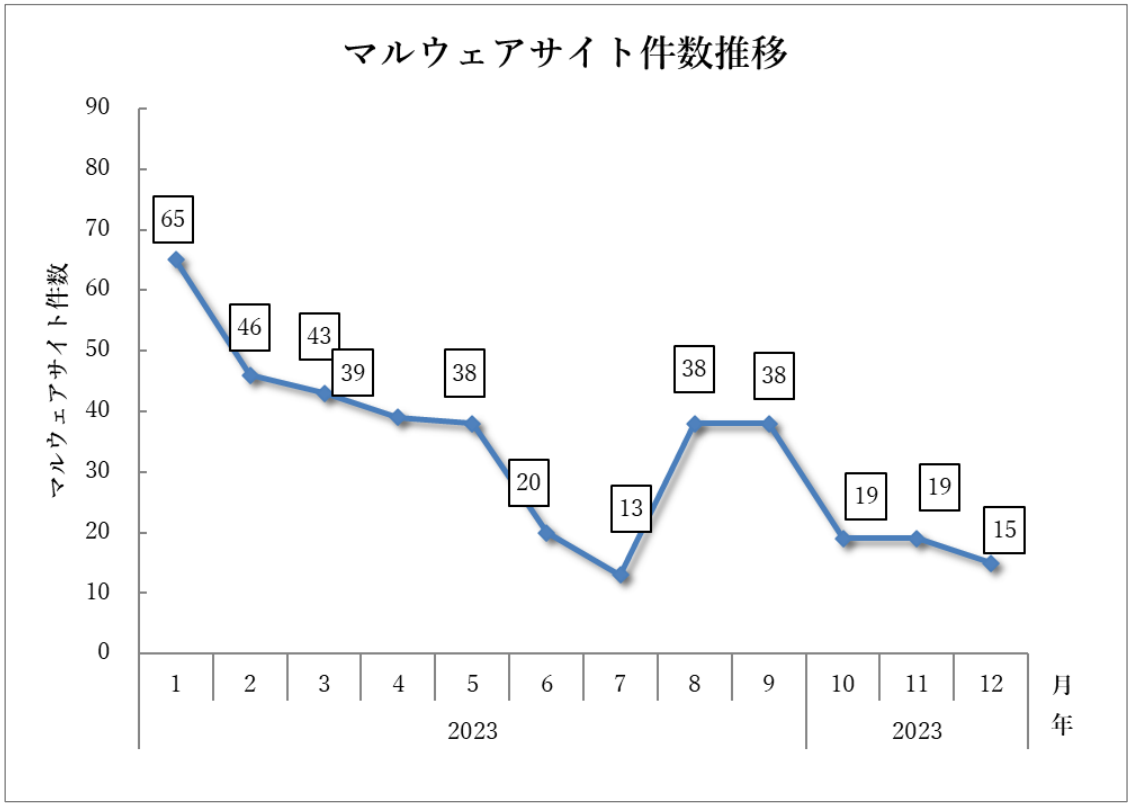
フィッシングサイトに分類されるインシデントが 69%、スキャンに分類される、システムの弱点を探索するインシデントが 22%を占めています。
［図 4］から［図 7］に、フィッシングサイト、Web サイト改ざん、マルウェアサイト、スキャンのインシデントの過去 1 年間の月次の推移を示します。



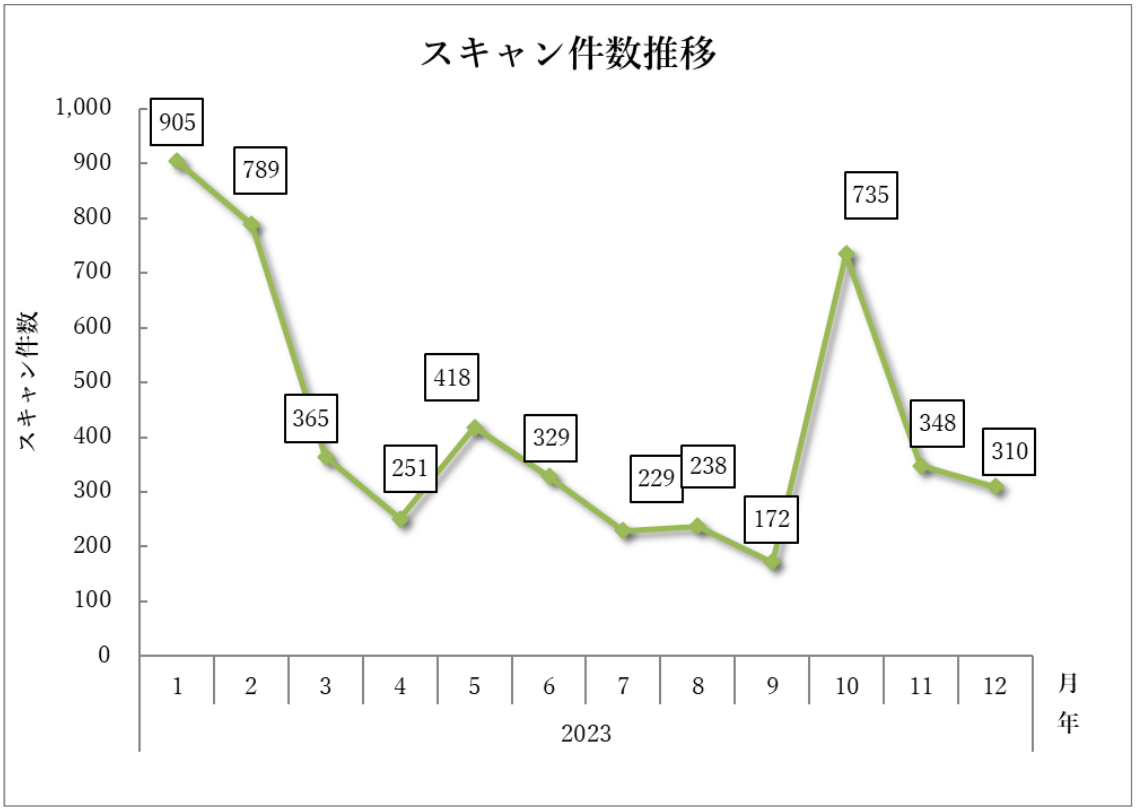
［図 4：フィッシングサイト件数の推移］



［図 5：Web サイト改ざん件数の推移］

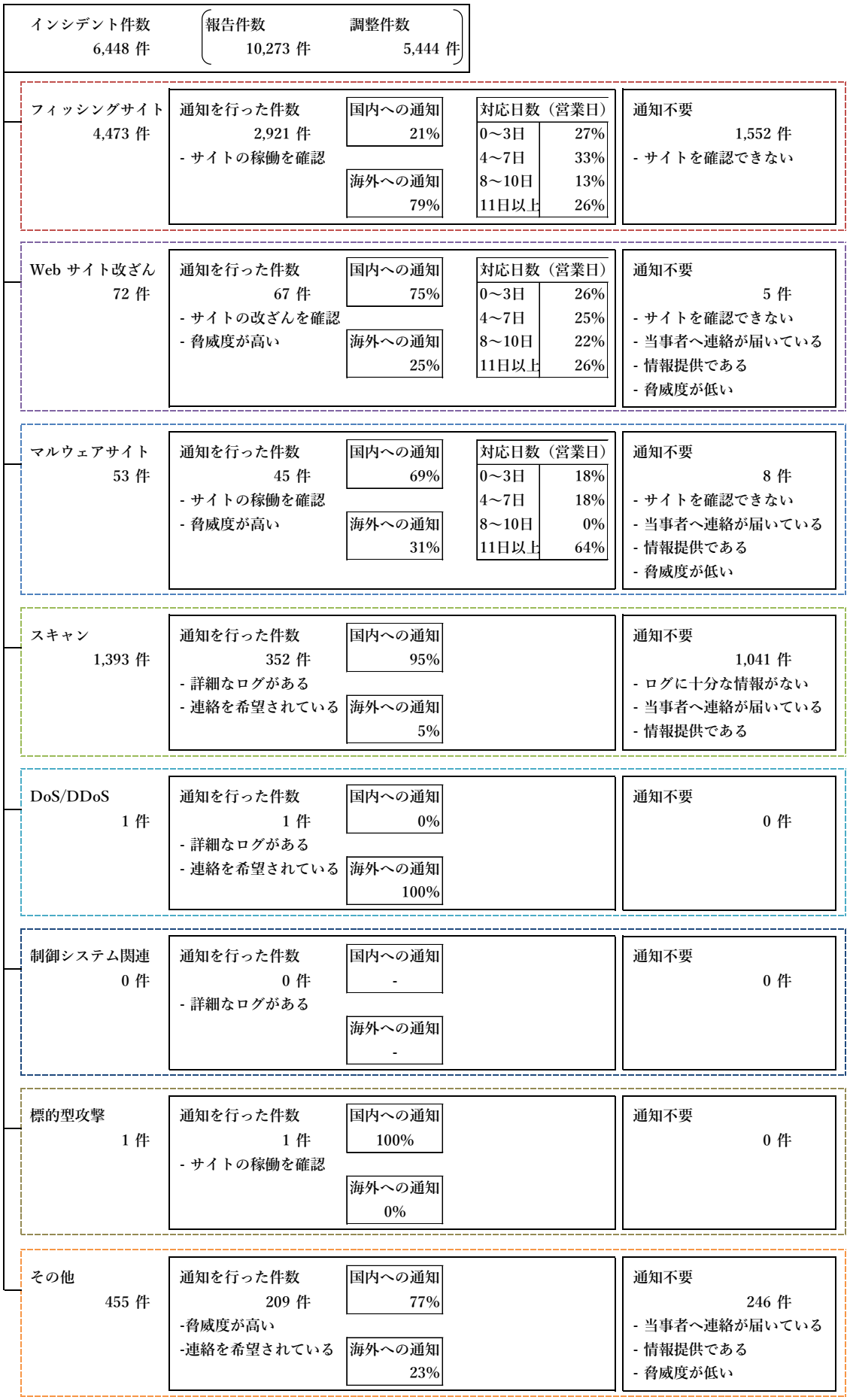


［図 6：マルウェアサイト件数の推移］



［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

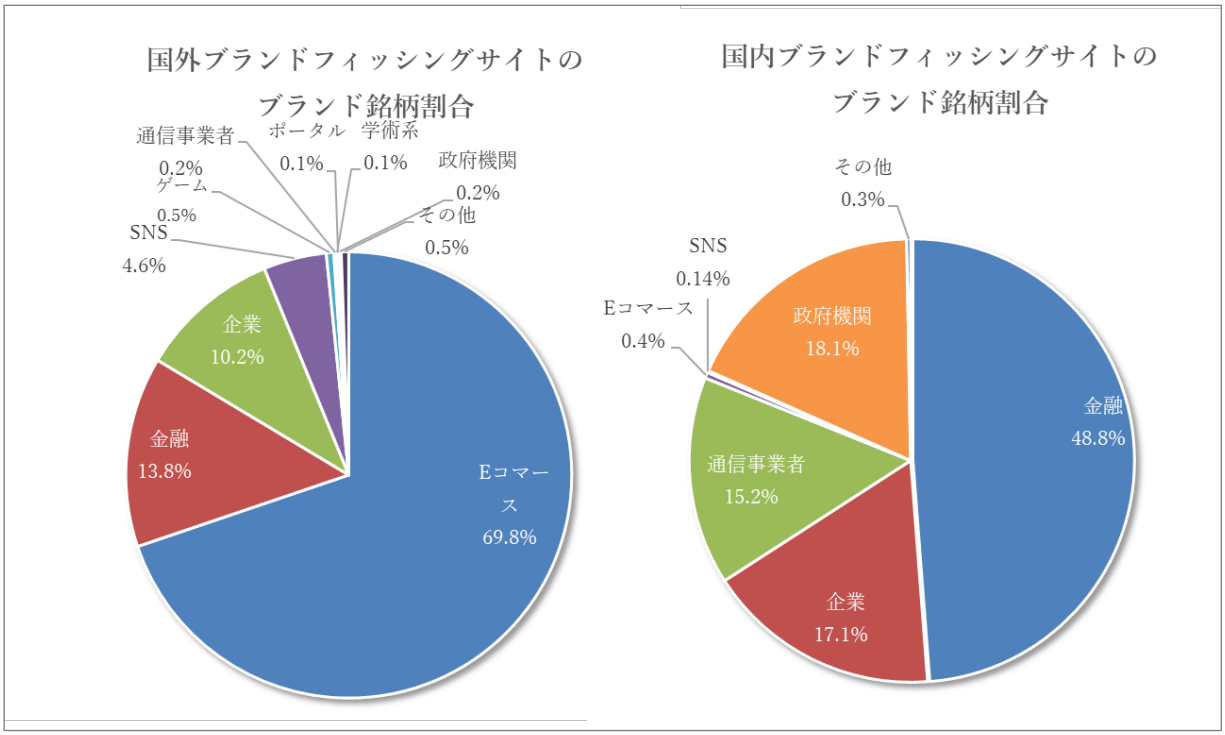
本四半期に報告が寄せられたフィッシングサイトの件数は 4,473 件で、前四半期の 4,754 件から 6%減少しました。また、前年度同期（6,266 件）との比較では、29%の減少となりました。

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 2,796 件となり、前四半期の 3,029 件から 8%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 1,116 件となり、前四半期の 997 件から 12%増加しました。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	10 月	11 月	12 月	本四半期合計（割合）
国内ブランド	894	1,047	855	2,796 (63%)
国外ブランド	371	278	467	1,116 (25%)
ブランド不明 (注 5)	188	230	143	561 (13%)
全ブランド合計	1,453	1,555	1,465	4,473

（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などの理由により、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 69.8%、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 48.8%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ました。
国内ブランドでは、総務省のマイナポイント事業や、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、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、セゾンカードや PayPay 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 21%、国外が 79%であり、前四半期（国内が 25%、国外が 75%）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、72 件でした。前四半期の 124 件から 42%減少しています。

本四半期は、不審なサイトへの転送させる Web サイトの改ざん事例を複数確認しました。改ざんされた Web サイトには［図 10］のようなスクリプトが設置されていて、初めてのアクセスだった場合にだけ不審なサイトに誘導する仕組みになっていました。なお、不審サイトは、ラッキービジター詐欺やブラウザーの通知機能を悪用するサイトであることを確認しています。

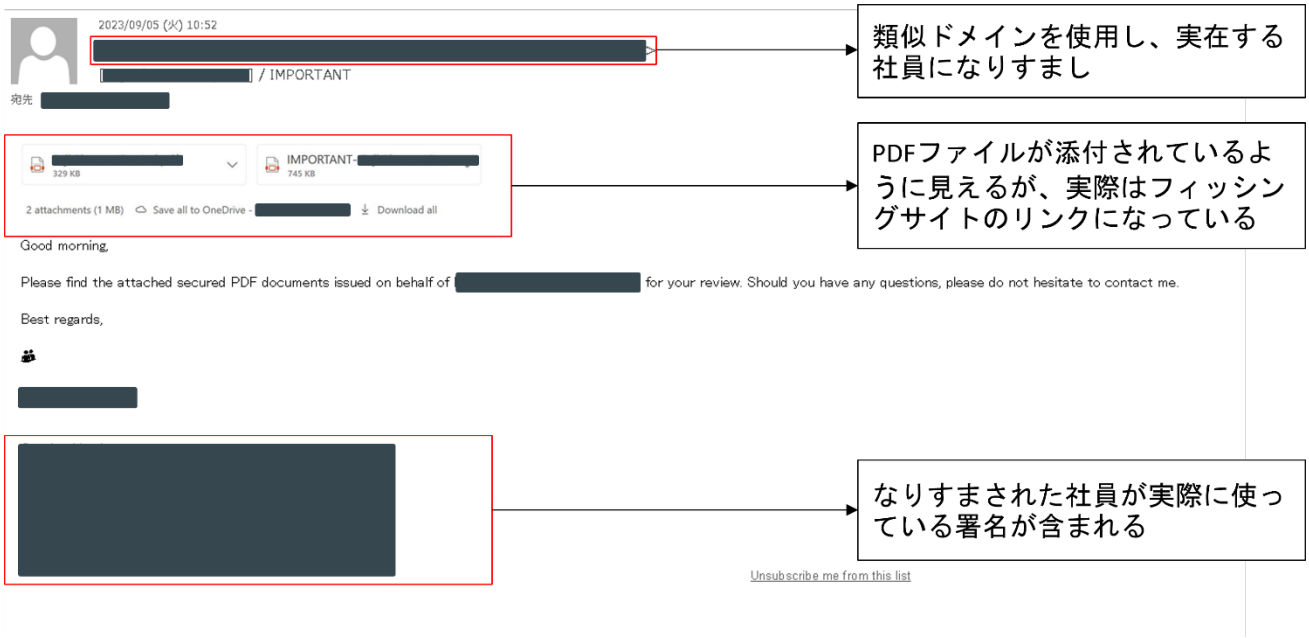
```
localStorage.setItem('test', 'testValue');

if ((localStorage.getItem('test') !== null) &&  (localStorage.getItem('click3') == null)){

    var click_r = false;
    document.addEventListener("click", function(){

    if(click_r == false){
    localStorage.setItem('click3', 'click3');
    window.open("[redacted]");
    click_r = true;
    }
    });
}
```

［図 10：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 1 件でした。

本四半期は、組織を詐称して不正なメールを送信するなりすましメールの報告が寄せられました。攻撃者は事前に詐称する組織のものと紛らわしいドメインを取得した上で、そのドメインを使用して当該組織に実在する社員を名乗ってメールを送信していました。［図 11］のようにメールの本文中には、なりすまされた社員が実際に使っている署名が含まれています。また、本メールは不特定多数にではなく、詐称した組織の取引先に対してのみ送信されており、事前に関係者のメール情報を窃取した上で攻撃を行っている可能性があります。



［図 11：詐称メールの例］

本攻撃は、2022 年 3 月頃から行われていることを確認しています。今回報告のあった組織以外にも複数の組織が被害を受けており、いずれの例でも、本文中に正規と思われる署名が記載されており、紛らわしいドメイン（［表 4］）から送信されたメールが見つかっています。

［表 4：紛らわしいドメインの選び方の例］

正規ドメイン	正規のものに対応する紛らわしいドメイン
example[.]jp	example-jp[.]com
example[.]com	example[.]co
example[.]com	exmple[.]com

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 53 件でした。前四半期の 89 件から 40%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 1,393 件でした。前四半期の 639 件から 118%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 5］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 5：ポート別のスキャン件数の上位 10 位］

ポート	10 月	11 月	12 月	合計
22/tcp	604	257	172	1,033
23/tcp	79	70	77	226
25/tcp	1	4	38	43
80/tcp	12	5	2	19
445/tcp	9	5	3	17
443/tcp	7	1	7	15
8080/tcp	5	3	3	11
56575/tcp	10	0	1	11
37215/tcp	1	0	4	5
143/tcp	0	3	2	5

その他に分類されるインシデントの件数は、455 件でした。前四半期の 292 件から 56%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) Proself の脆弱性（CVE-2023-45727）への対応

2023 年 10 月 10 日に、ノースグリッド社はオンラインストレージ構築パッケージ製品「Proself」における XML 外部実体参照（XXE）に関する脆弱性があることを公開しました。本脆弱性を悪用して、システム内の任意のファイルを外部へ送信する攻撃が確認されたことから JPCERT/CC でも 10 月 10 日に注意喚起を行いました。

Proself の XML 外部実体参照（XXE）に関する脆弱性を悪用する攻撃の注意喚起
https://www.jpcert.or.jp/at/2023/at230022.html

JPCERT/CC では、パッチ未適用と思われる国内の Proself を利用しているシステム管理者に対して通知を行いました。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、すでに攻撃を受けている可能性もありますので、JPCERT/CC が公開しているインディケータ情報を参考に、不審な通信がないことを確認することを推奨します。

日本の組織を標的にした外部からアクセス可能な IT 資産を狙う複数の標的型サイバー攻撃活動に関する注意喚起
https://www.jpcert.or.jp/at/2023/at230029.html

(2) Cisco IOS XE の脆弱性（CVE-2023-20198）への対応

Cisco 社は、2023 年 10 月 16 日に Cisco IOS XE ソフトウェアの Web UI 機能に権限昇格の脆弱性があることを公開しました。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最上位の特権アカウントを作成し当該システムを制御する可能性があることから、JPCERT/CC でも 10 月 18 日に注意喚起を行いました。

Cisco IOS XE の Web UI の脆弱性(CVE-2023-20198)に関する注意喚起
https://www.jpcert.or.jp/at/2023/at230025.html

JPCERT/CC には、本脆弱性を悪用してバックドアが設置された被害報告が国内外の組織から寄せられています。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。影響を受ける製品を利用している場合には速やかなアップデートをお願いします。

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などに対する停止・閉鎖を目的とした調整や、利用者向けの注意喚起など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など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など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などのサイトに似せた 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などにより悪意のあるスクリプトや iframe など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 など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など）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、マルウェアなど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など）
- 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、ワームなど）による感染の試み（未遂に終わったもの）
- ssh,ftp,telnet など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など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。

- 大量の通信などにより、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 メールなど）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などを発生させる攻撃

○ 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。

- 脆弱性などを突いたシステムへの不正侵入
- ssh、ftp、telnet など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、ワームなど）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。