JPCERT/CC インシデント報告対応レポート

2023 年 4 月 1 日 ～ 2023 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

2023 年 7 月 13 日

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 4 月 1 日から 2023 年 6 月 30 日までの間に受け付けたインシデント報告の統計および事例について紹介します。

（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

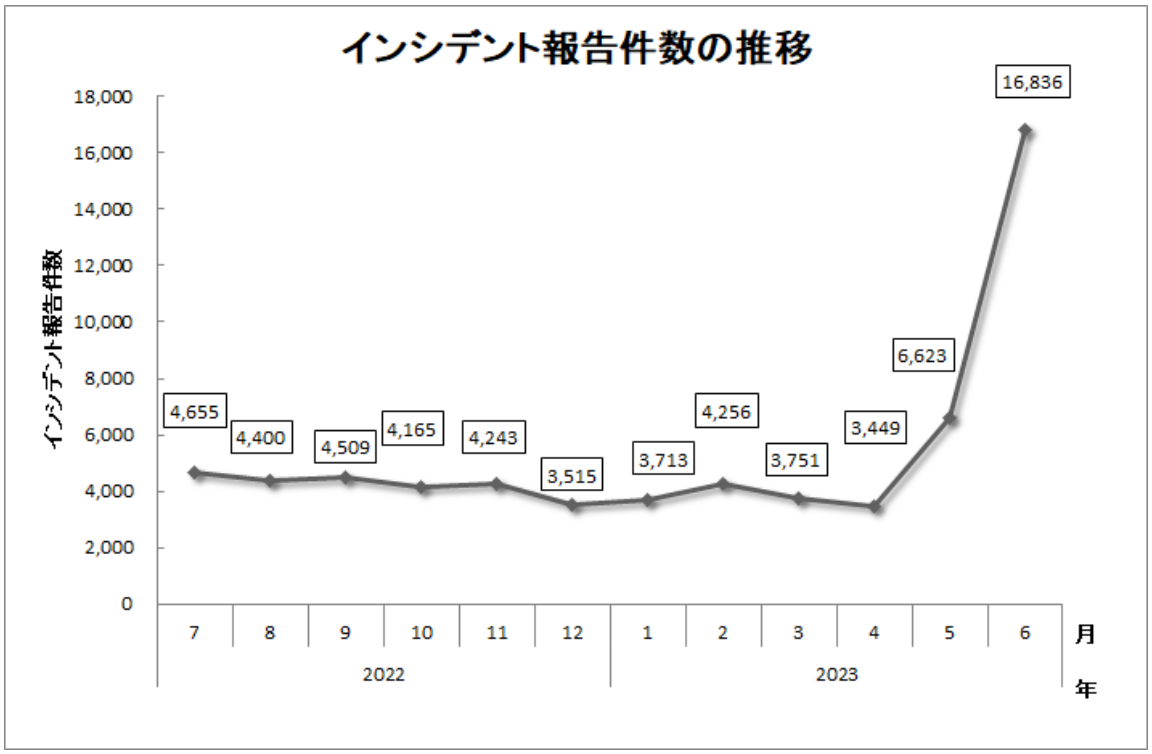
本四半期のインシデント報告の数、報告されたインシデントの総数、および、報告に対応して JPCERT/CC が行った調整の件数を［表 1］に示します。

［表 1：インシデント報告関連件数］

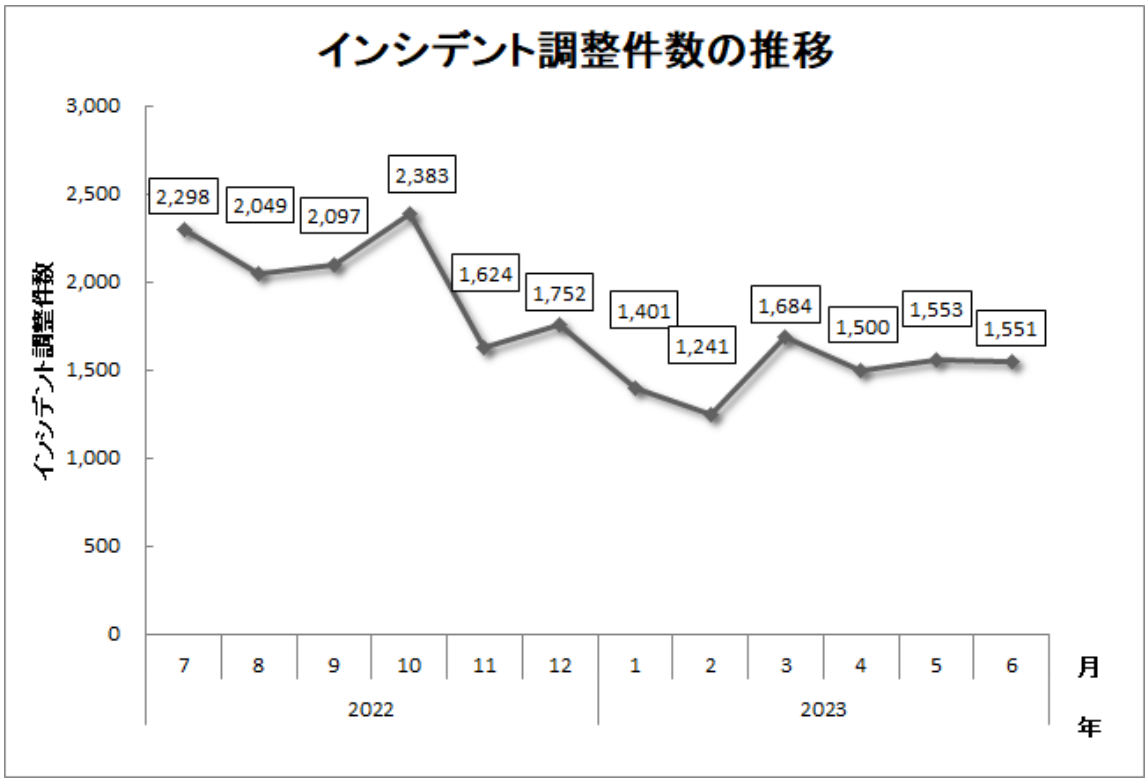
	4 月	5 月	6 月	合計	前四半期合計
報告件数 (注 2)	3,449	6,623	16,836	26,908	11,720
インシデント件数 (注 3)	2,416	2,867	2,642	7,925	8,459
調整件数 (注 4)	1,500	1,553	1,551	4,604	4,326

（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、26,908 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 4,604 件でした。前四半期と比較して、報告件数は 130%増加し、調整件数は 6%増加しました。また、前年同期と比較すると、報告数は 61%増加し、調整件数は 42%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］

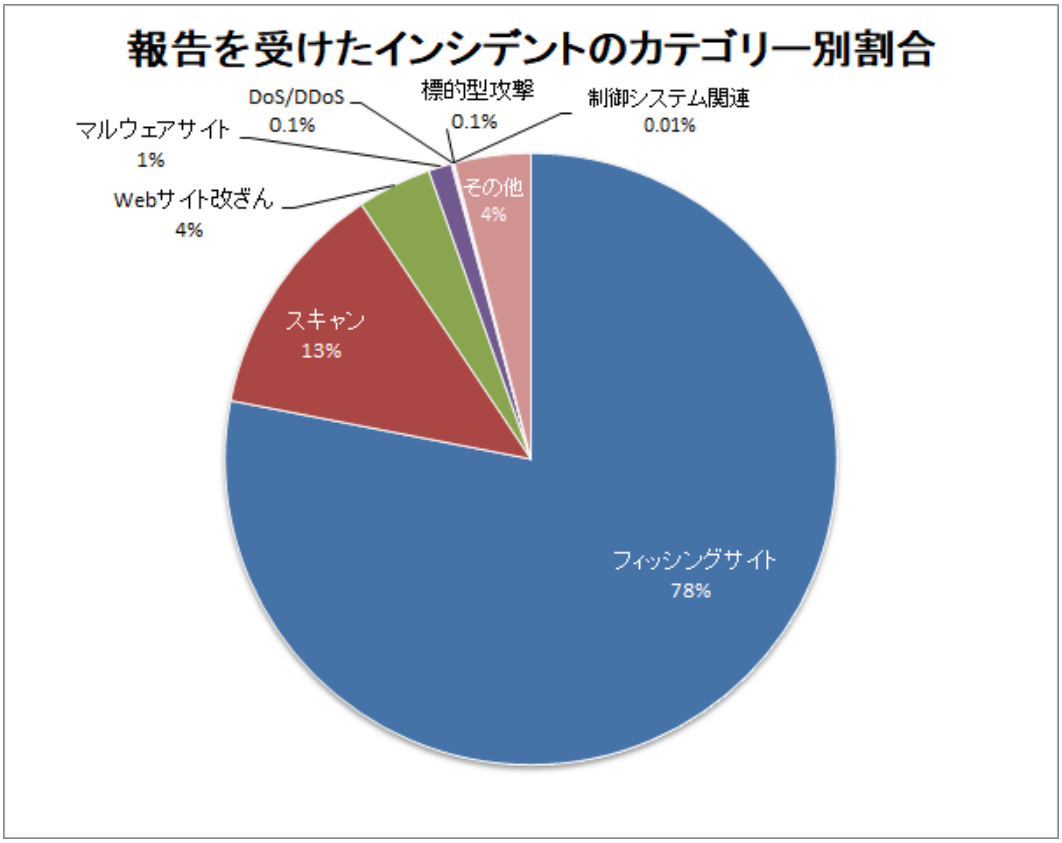


［図 2：インシデント調整件数の推移］

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］

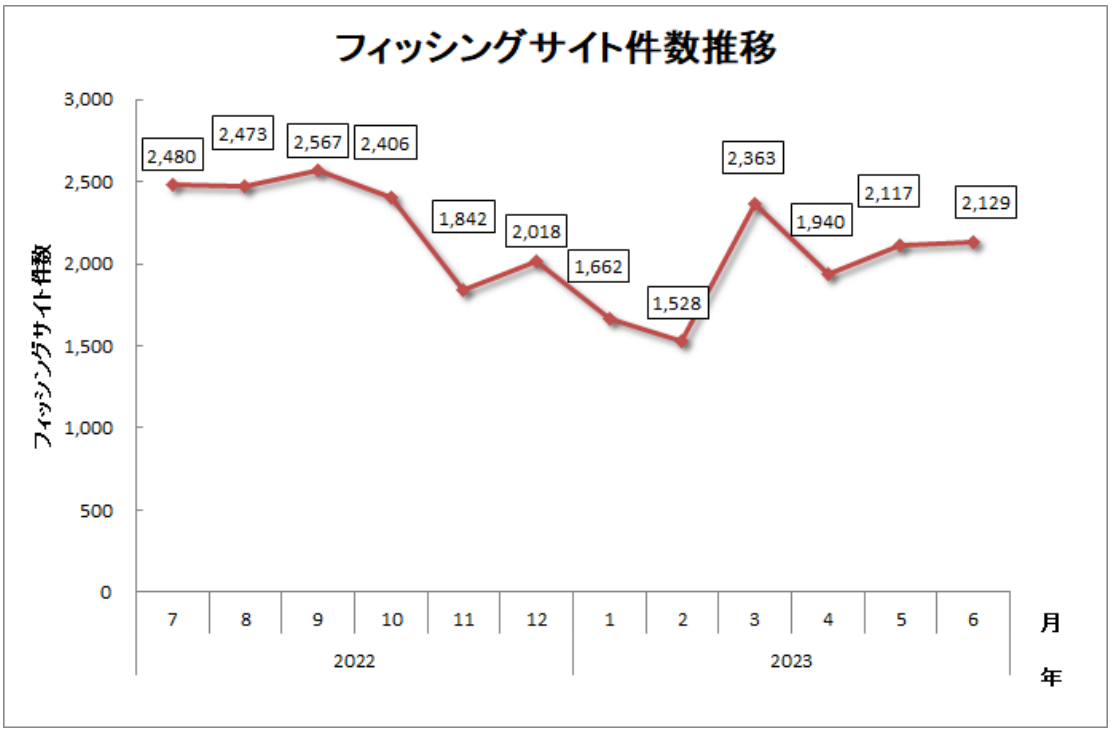
インシデント	4 月	5 月	6 月	合計	前四半期合計
フィッシングサイト	1,940	2,117	2,129	6,186	5,553
Web サイト改ざん	104	165	42	311	362
マルウェアサイト	39	38	20	97	154
スキャン	251	418	329	998	2,059
DoS/DDoS	0	7	1	8	9
制御システム関連	0	0	1	1	0
標的型攻撃	1	1	2	4	3
その他	81	121	118	320	319



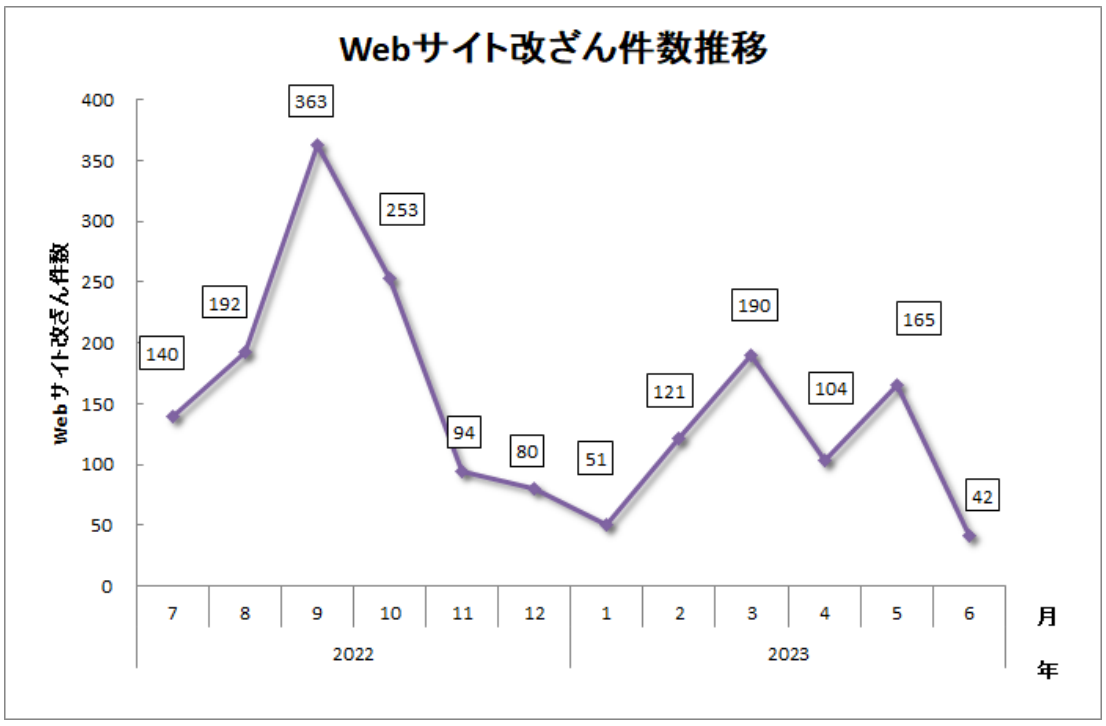
［図 3：報告を受けたインシデントのカテゴリー別割合］

フィッシングサイトに分類されるインシデントが 78%、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 13%を占めています。

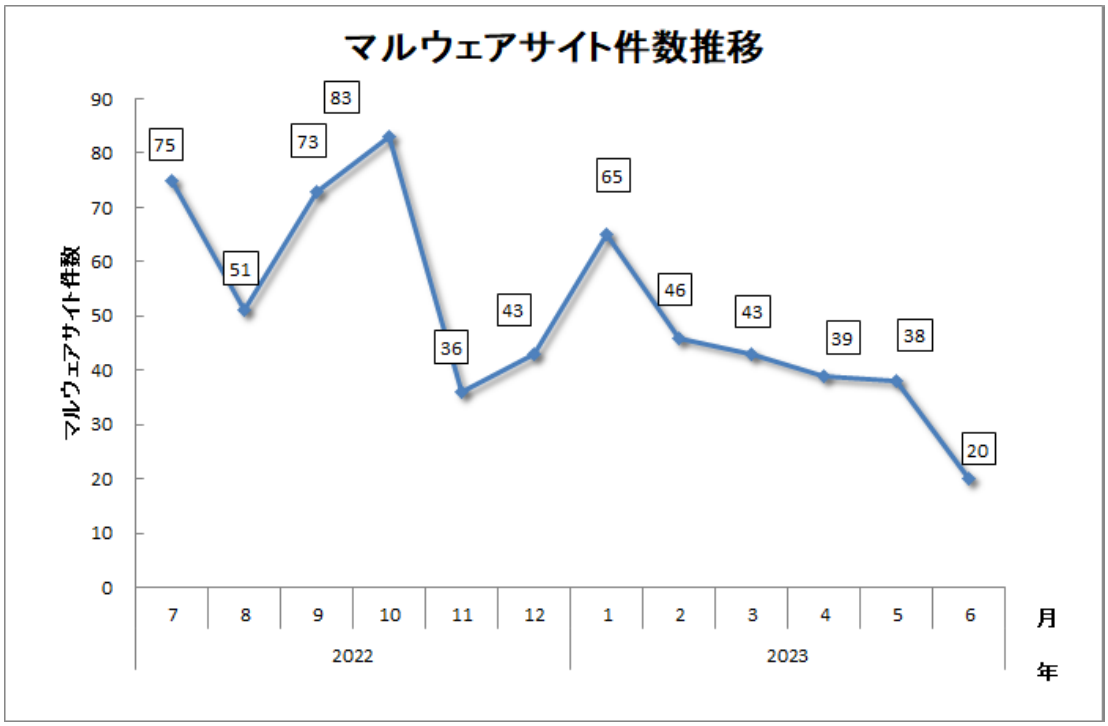
［図 4］から［図 7］に、フィッシングサイト、Web サイト改ざん、マルウェアサイト、スキャンのインシデントの過去 1 年間の月次の推移を示します。



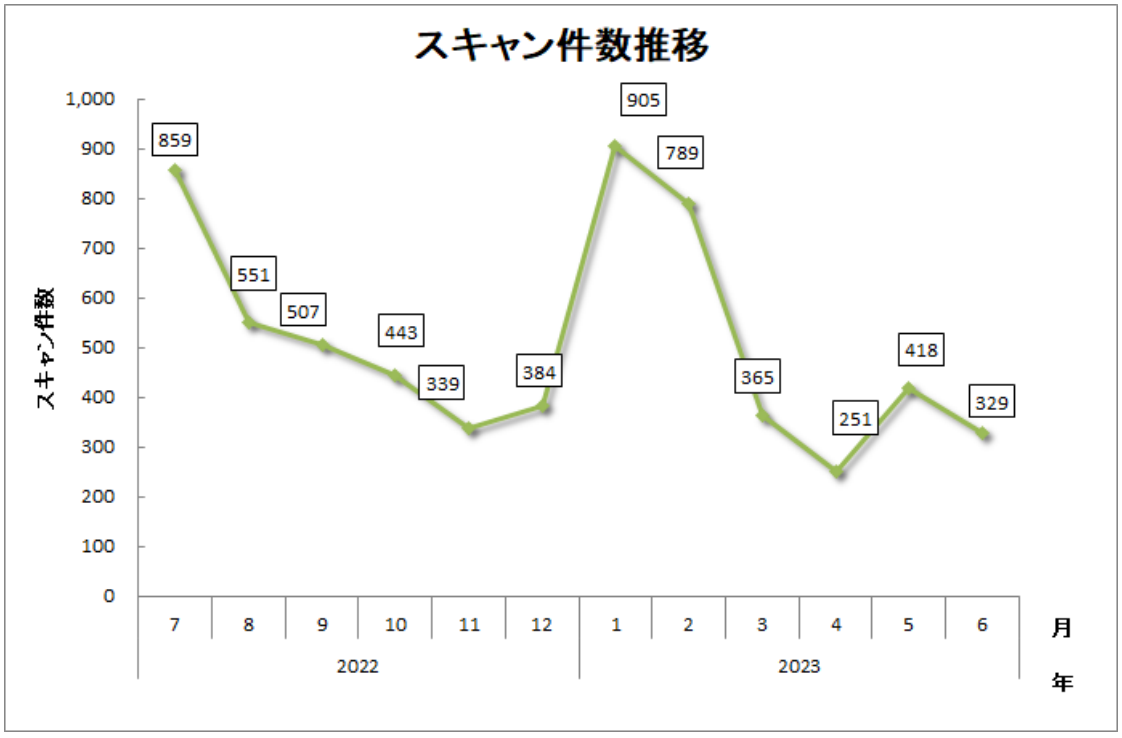
［図 4：フィッシングサイト件数の推移］



［図 5：Web サイト改ざん件数の推移］

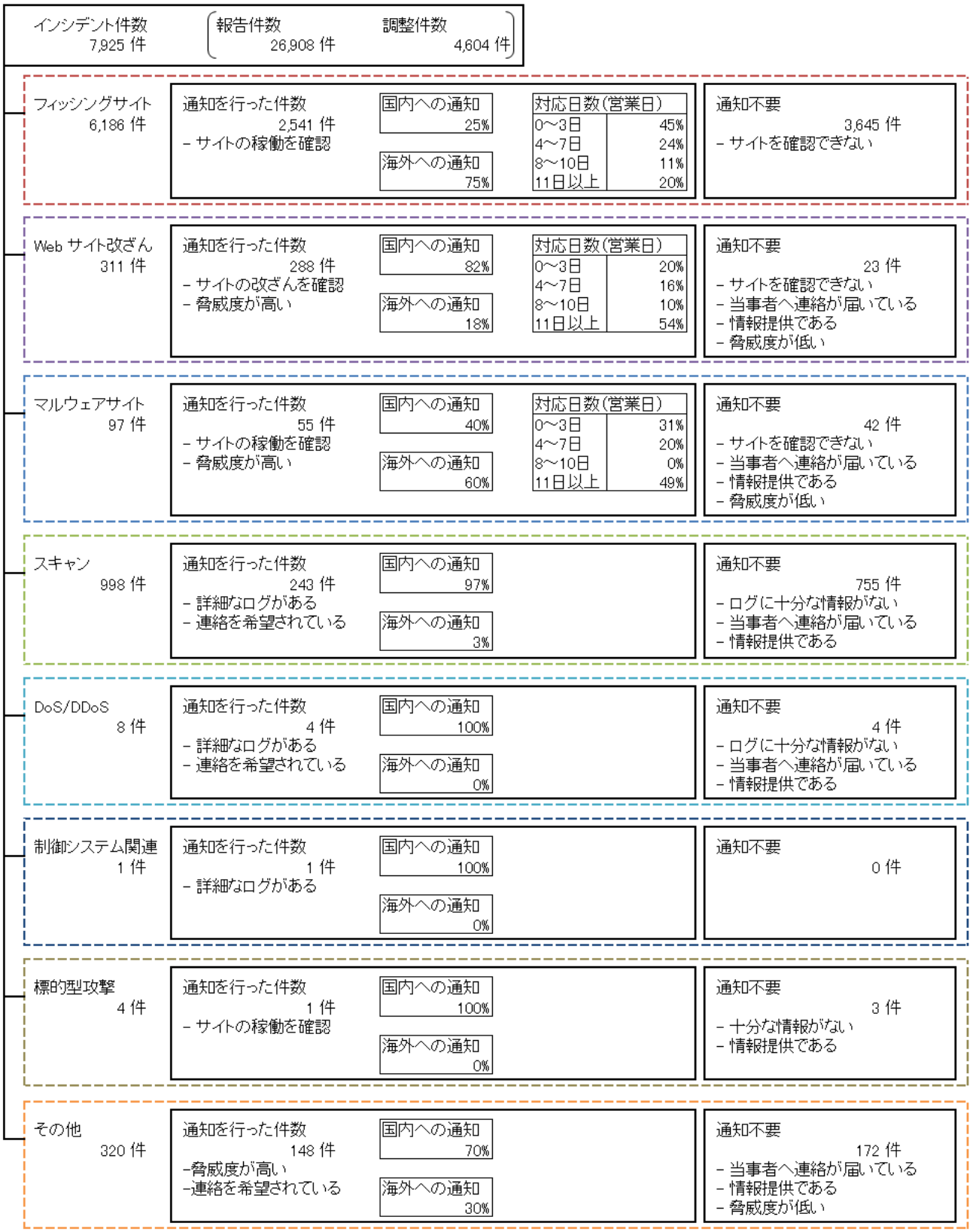


［図 6：マルウェアサイト件数の推移］



［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

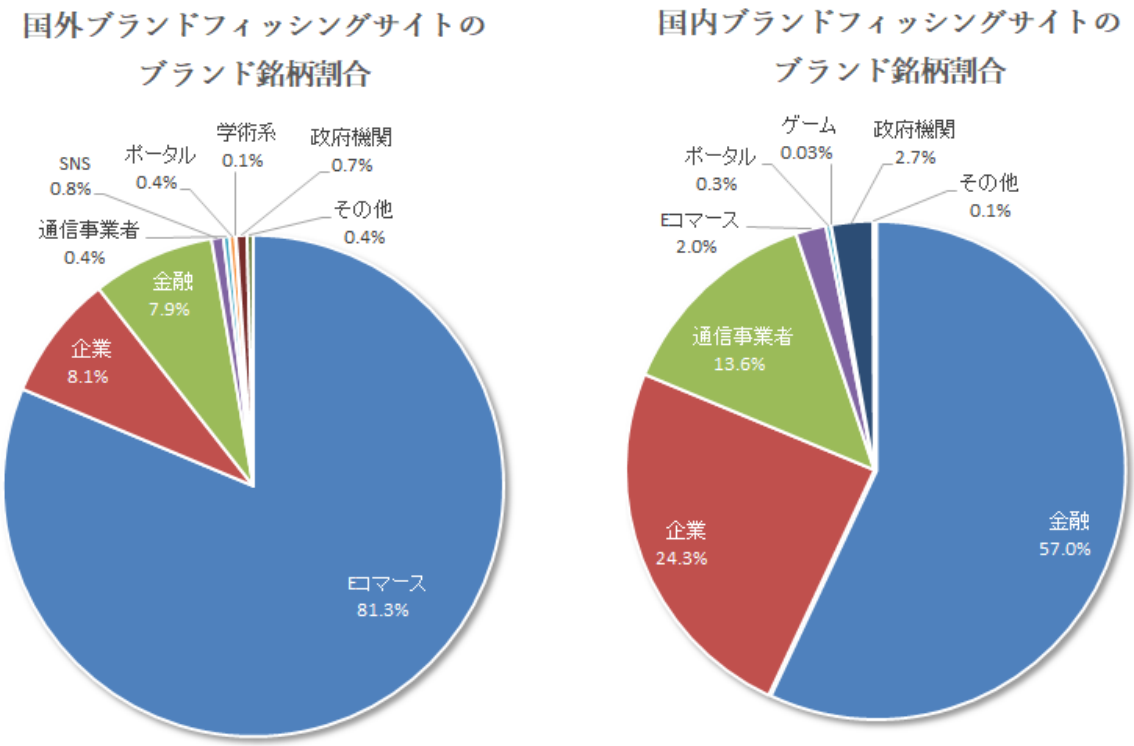
本四半期に報告が寄せられたフィッシングサイトの件数は 6,186 件で、前四半期の 5,553 件から 11%増加しました。また、前年度同期（8,088 件）との比較では、24%の減少となりました。

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 3,700 件となり、前四半期の 3,170 件から 17%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 1,568 件となり、前四半期の 1,730 件から 9%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	4 月	5 月	6 月	本四半期合計（割合）
国内ブランド	1,127	1,351	1,222	3,700(60%)
国外ブランド	587	482	499	1,568(25%)
ブランド不明 (注 5)	226	284	408	918(15%)
全ブランド合計	1,940	2,117	2,129	6,186

(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 81.3%、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 57%で，それぞれ最も多くを占めました。

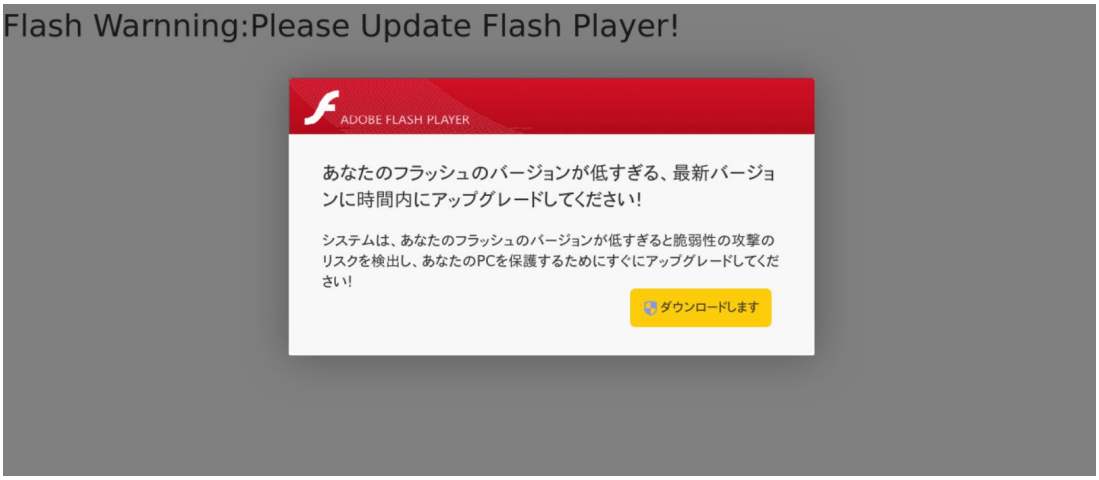
海外ブランドでは、Amazon を装ったフィッシングサイトが全体の半数以上を占めていました。
国内ブランドでは、JR 東日本が提供する Web サイト「えきねっと」や ETC の利用照会サービスを装ったフィッシングサイトが多く報告されました。
国内金融機関では、前四半期に引き続きエポスカード、セゾンカード、イオンカード、そして、三井住友カードを装ったフィッシングサイトが引き続き多く報告されました。

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 25%、国外が 75%であり、前四半期（国内が 24%、国外が 76%）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、311 件でした。前四半期の 362 件から 14%減少しています。

本四半期は、Web サイトの閲覧時に［図 10］のような偽の Adobe Flash Player のアップグレード表示することで、マルウェアに感染させる Web サイトを改ざん事例が寄せられました。表示された偽のアップグレード画面の指示にしたがってファイルをダウンロードし、インストールすると Cobalt Strike と呼ばれる攻撃ツールがホスト上にインストールされます。



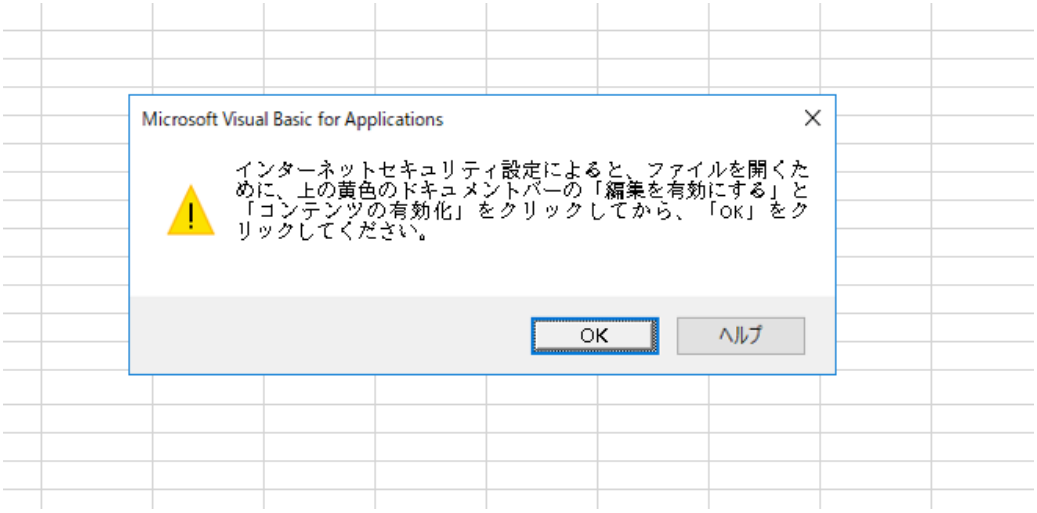
［図 10：改ざんされたサイトへアクセス時の表示画面］

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。次に、確認されたインシデントを紹介します。

(1) マルウェア LODEINFO を用いた攻撃

本四半期は、マルウェア LODEINFO を感染させようとする標的型攻撃の報告が寄せられました。本攻撃では、過去にメールでやり取りのあった人物に詐称してターゲットに対してメールを送信し、何回かのメールのやり取りを経て、不正な Excel ファイルが送られてきます。不正な Excel ファイルは［図 11］のように、マクロの実行を促す内容が記載されており、マクロを実行すると PEM ファイルを装った LODEINFO（［図 12］）がダウンロード・実行されます。



［図 11：マクロの実行を誘導する Excel ファイル］

［図 12：PEM ファイルを装って暗号化された LODEINFO］

現在、LODEINFO のバージョンは v0.6.8、v0.6.9 などを確認しており、継続してマルウェアの開発が続けられていることが分かっています。

(2) DangerousPassword に関連すると考えられる暗号資産交換事業者への攻撃

本四半期は、攻撃キャンペーン DangerousPassword（CryptoMimic または、SnatchCrypto とも呼ばれる）に関連する暗号資産交換事業者への攻撃を確認しています。

ターゲットとなった組織のホスト上で、外部から Windows インストーラー（MSI ファイル）をダウンロードして、実行する不正な Python スクリプトが見つかっており、攻撃者は、何らかの方法で Python スクリプトをターゲットホスト上で実行させたと考えられます。ダウンロードされる MSI ファイルは、以前に弊センターのブログでも紹介したものと同種であり、感染ホストの情報を外部に送信する機能があります。DangerousPassword は、従来のショートカットファイルを用いた攻撃手法以外にさまざまな攻撃手法を用いてマルウェア感染を狙っていることが判明しており、活発な活動がうかがえます。

JPCERT/CC Eyes「攻撃キャンペーン DangerousPassword に関連する攻撃動向」
https://blogs.jpcert.or.jp/ja/2023/05/dangerouspassword.html

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 97 件でした。前四半期の 154 件から 37%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 998 件でした。前四半期の 2,059 件から 52%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）、SIP（5060/UDP）、Telnet（23/TCP）、37215/TCP、HTTP（80/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	4 月	5 月	6 月	合計
22/tcp	139	179	106	424
5060/udp	0	144	119	263
23/tcp	33	31	42	106
37215/tcp	34	33	11	78
80/tcp	24	12	10	46
25/tcp	11	6	8	25
52869/tcp	1	2	21	24
21/tcp	2	5	2	9
143/tcp	4	2	1	7
445/tcp	1	2	2	5
月別合計	255	423	329	1007

その他に分類されるインシデントの件数は、320 件でした。前四半期の 319 件とほぼ同数でした。

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) DNS の再帰的な問い合わせを使った DDoS 攻撃の報告への対応

本四半期は、存在しないサブドメインを含む FQDN を大量に権威 DNS サーバーへ問い合せする DDoS 攻撃（以下、「DNS 水責め攻撃」という。）が発生し、その攻撃において国内の IP アドレスが悪用されているとの報告を受けました。JPCERT/CC では当該 IP アドレスの管理者に対して状況の確認と対策の実施を依頼しました。

DNS 水責め攻撃が発生すると攻撃対象サイトの Web サイトや名前解決を必要とするサービスが利用できなくなる可能性があります。また、権威 DNS サーバーが複数のドメイン名を管理している場合、攻撃対象以外のドメイン名も影響をうける可能性があります。サービス提供者は、自身のドメイン名を管理する権威 DNS サーバーにおいて、これらの攻撃に対する備え（攻撃の監視や、対策、攻撃発生時の回避策の準備等が適切に行われているか）の確認をお願いします。

JPRS トピックス&コラム No.021
Bot 経由で DNS サーバーを広く薄く攻撃～DNS 水責め攻撃の概要と対策～
https://jprs.jp/related-info/guide/topics-column/no21.html

また、キャッシュ DNS サーバーやルーター（ISP などが提供するキャッシュ DNS サーバーに転送）がインターネットからの問い合わせを無制限に受け付けて応答してしまうオープンリゾルバー状態となっていると攻撃の踏み台として悪用される恐れがあることから、自身の管理するシステムがオープンリゾルバー状態となっていないか。また、オープンリゾルバー対策が取られているかの確認をお願いします。

オープンリゾルバー確認サイト
https://www.openresolver.jp/

(2) 侵入型ランサムウェア攻撃被害に関する報告への対応

本四半期は、ランサムウェア（BlackByte、LockBit、Blackcat、Akira など）の感染報告を複数受けています。JPCERT/CC では、報告者から被害範囲や調査状況、報告時点の対応状況などをヒアリングし、得られた情報もとに、関連するランサムウェア攻撃の特徴などの情報を提供し対応方針に関するアドバイスをしています。

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.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。