JPCERT/CC インシデント報告対応レポート

2021 年 7 月 1 日 ～ 2021 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

2021 年 10 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、2021 年 7 月 1 日から 2021 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)	4,269	4,453	3,747	12,469	10,274
インシデント件数 (注 3)	2,490	3,319	2,977	8,786	6,977
調整件数 (注 4)	1,226	1,683	1,805	4,714	3,745

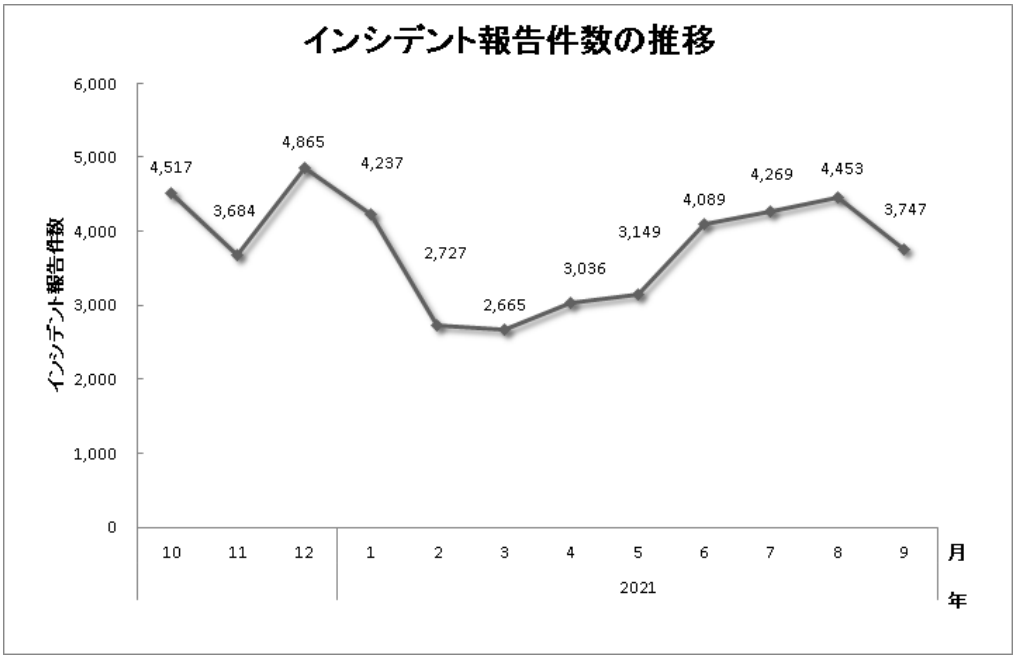
（注 2）「報告件数」は、報告者から寄せられた Web フォーム、メール、FAX による報告の総数を示します。

（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。

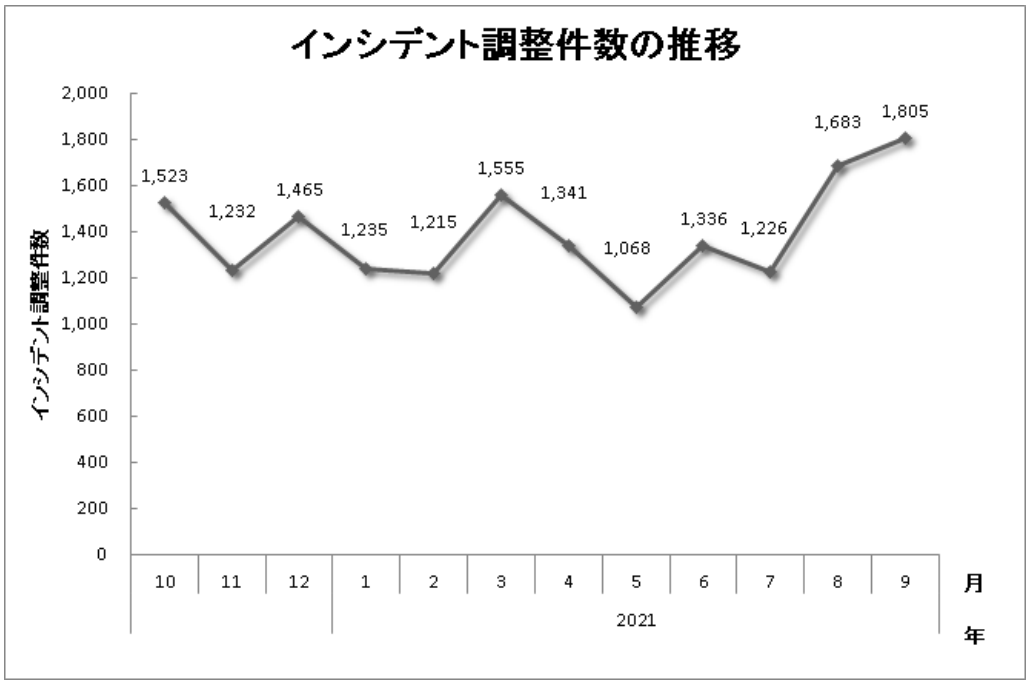
（注 4）「調整件数」は、インシデントの拡大防止のため、サイトの管理者等に対し、現状の調査と問題解決のための対応を依頼した件数を示します。

本四半期に寄せられた報告件数は、12,469 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 4,714 件でした。前四半期と比較して、報告件数は 21%増加し、調整件数は 26%増加しました。また、前年同期と比較すると、報告数は 10%減少し、調整件数は 2%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］

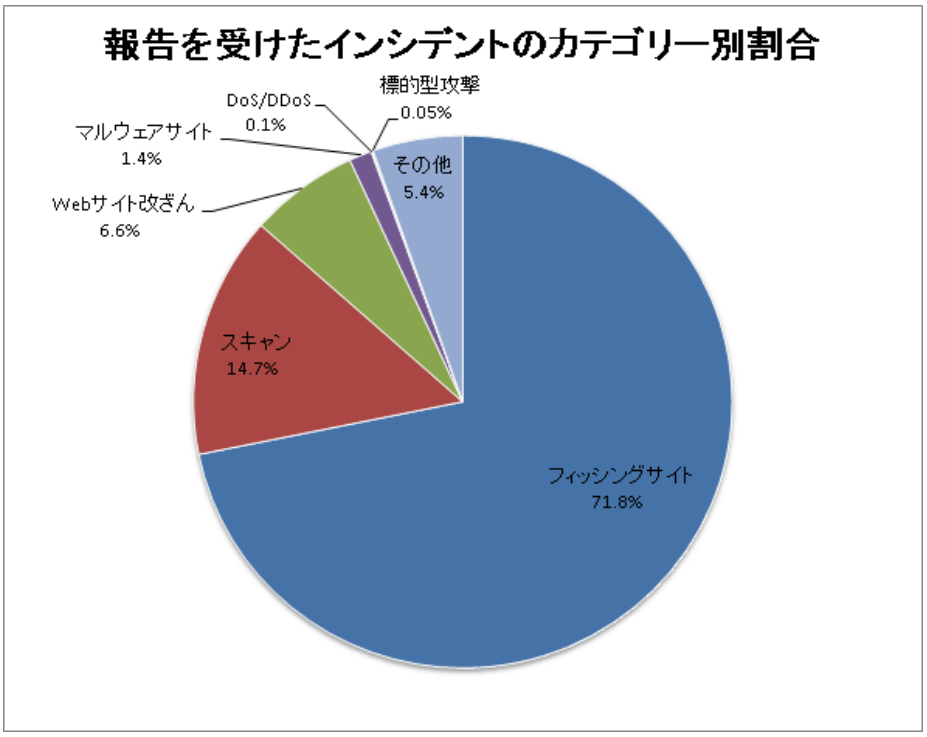


［図 2：インシデント調整件数の推移］

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］

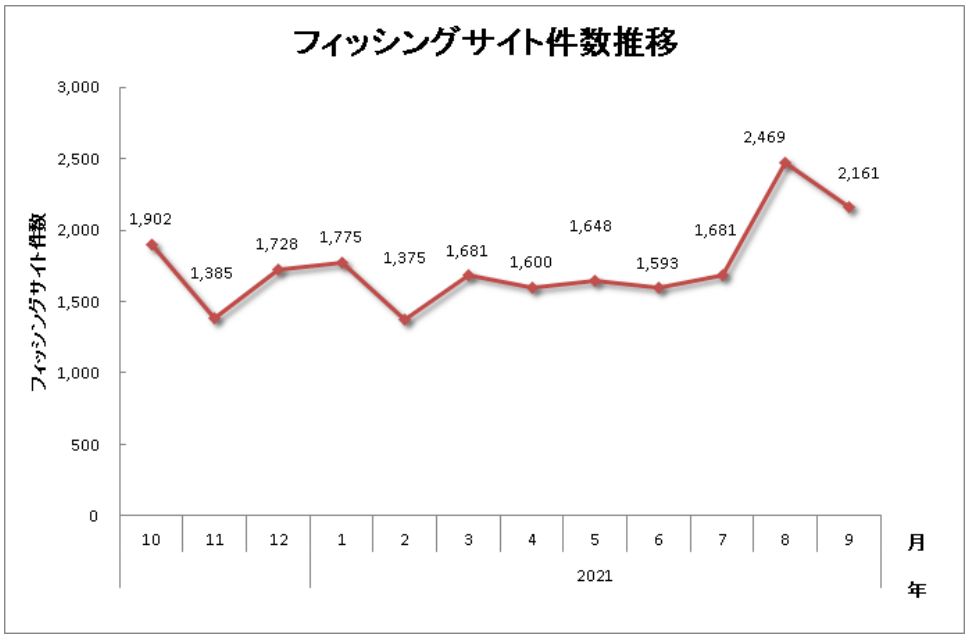
インシデント	7 月	8 月	9 月	合計	前四半期合計
フィッシングサイト	1,681	2,469	2,161	6,311	4,841
Web サイト改ざん	173	244	162	579	251
マルウェアサイト	10	26	83	119	38
スキャン	414	454	423	1,291	1,385
DoS/DDoS	1	0	6	7	8
制御システム関連	0	0	0	0	0
標的型攻撃	0	2	2	4	5
その他	211	124	140	475	449



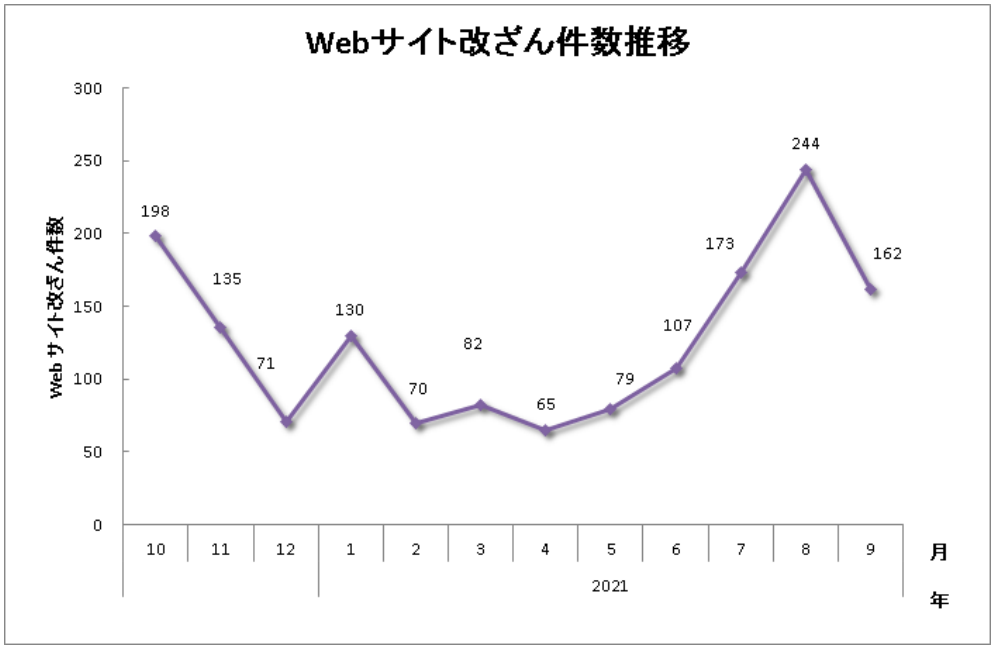
［図 3：報告を受けたインシデントのカテゴリー別割合］

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 14.7%を占めています。

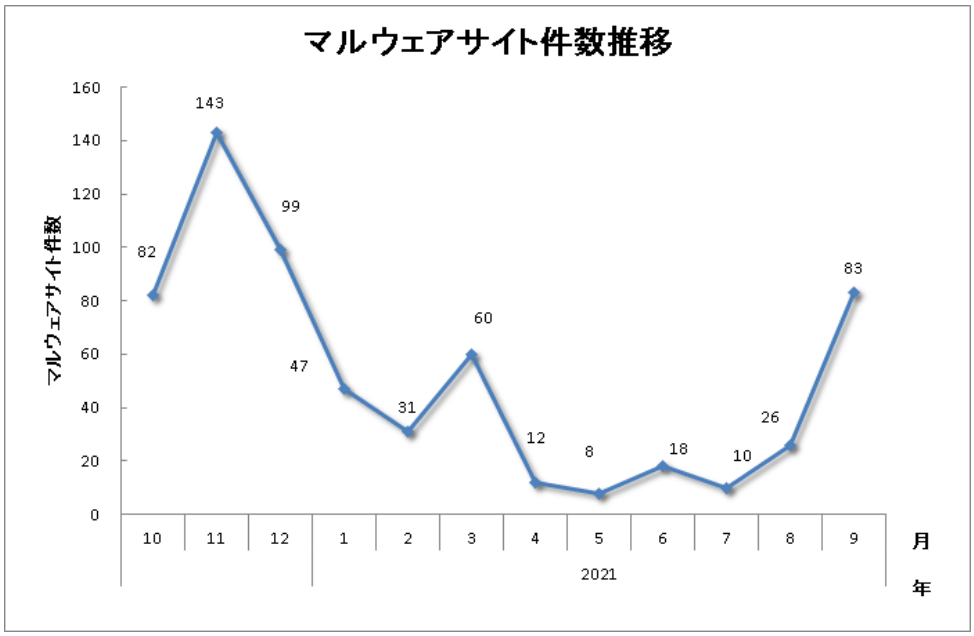
［図 4］から［図 7］に、フィッシングサイト、Web サイト改ざん、マルウェアサイト、スキャンのインシデントの過去 1 年間の月次の推移を示します。



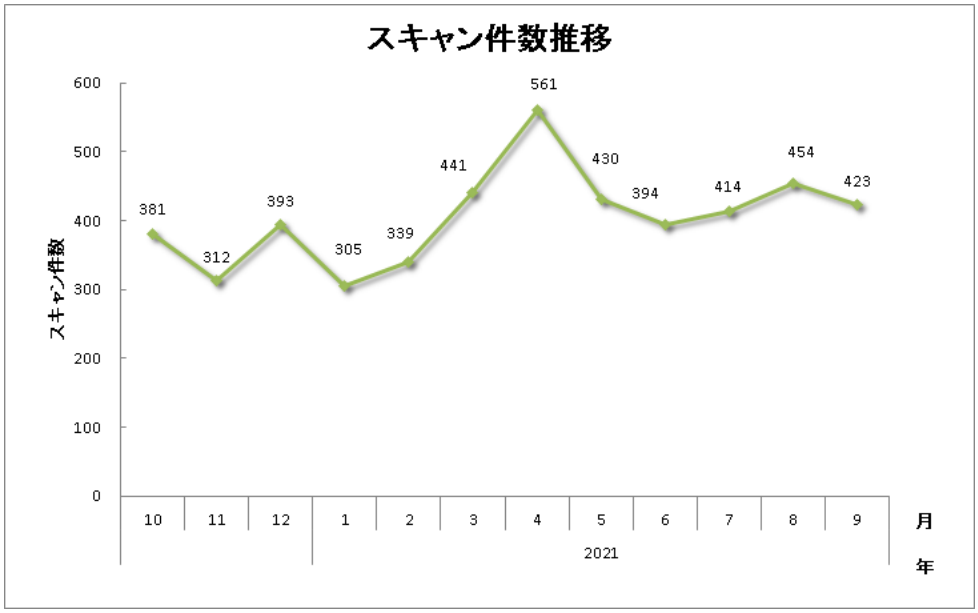
［図 4：フィッシングサイト件数の推移］



［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

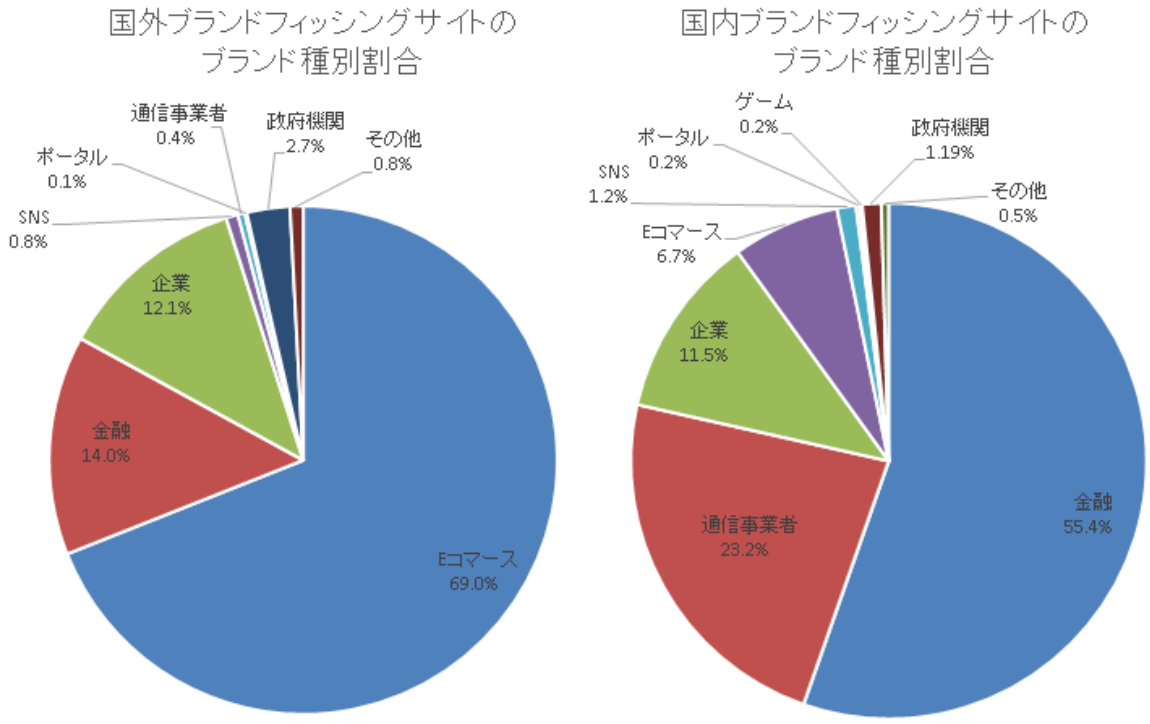
本四半期に報告が寄せられたフィッシングサイトの件数は 6,311 件で、前四半期の 4,841 件から 30%増加しました。また、前年度同期（5,845 件）との比較では、8%の増加となりました。

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 3,533 件となり、前四半期の 2,732 件から 29%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 1,570 件となり、前四半期の 1,134 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	1,032	1,389	1,112	3,533（56%）
国外ブランド	263	516	791	1,570（25%）
ブランド不明 (注 5)	386	564	258	1,208（19%）
全ブランド合計	1,681	2,469	2,161	6,311

（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、国外ブランドでは E コマースサイトを装ったものが 69%、国内ブランドでは金融機関のサイトを装ったものが 55.4%で，それぞれ最も多くを占めました。

本四半期は、前四半期と比較して約 1.3 倍のフィッシングサイトの報告がありました。

国内ブランドのフィッシングサイトでは、銀行やクレジットカード会社の会員用ログインページを装ったものや携帯通信キャリアのユーザー用ログインページを装ったものが多数報告されました。また、家電量販店のオンラインサイトや ISP が提供する Web メールを装ったものの報告が今まで以上に多く寄せられました。さらに、ETC の利用照会サービスや厚生労働省が提供するコロナワクチンナビを装ったフィッシングサイトの報告も寄せられました。
一方で、国外ブランドのフィッシングサイトの報告数には前四半期からほとんど変化がなく、通販サイトのログインページを装ったものが半数以上占めていました。

フィッシングサイトに利用されるドメインについては、5～7 文字の英字と数字の組み合わせで使った文字列に .com, .cn, .xyz, .shop, .top などの TLD と組み合わせたものが特に多く、これらのドメインのサブドメインに正規のブランド名に似せた文字列を使うドメイン名が多く見られました。

フィッシングサイトの調整先の割合は、国内が 23%、国外が 77%であり、前四半期（国内が 19%、国外が 81%）と比べて国内の調整が増加しました。

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、579 件でした。前四半期の 251 件から 131%増加しています。

本四半期は、改ざんされた Web サイトから、偽 EC サイトへ転送される事例が複数寄せられています。Web サイトには［図 10］や［図 11］のような不正な JavaScript コードが挿入されていました。挿入された JavaScript コードは難読化されており, アクセスしてきたブラウザーの Referrer の値をチェックし、検索エンジン経由のアクセスと判断された場合のみ、転送する仕組みになっています。

```
<script>
    eval(('if(' + '/(g' + 'o' + 'ogle|' + 'yahoo' + '|bing' + '|ao' + 'l)/' + 'i' + '.t' + 'es' + 't(do' + 'c' + 'umen' + 't.r' + 'ef'
+ 'er' + 'rer))' + '{win' + 'dow' + '.se' + 'tTim' + 'eout(' + 'f' + 'unct' + 'ion' + '(){t' + 'o' + 'p.lo' + 'cat' + 'ion' + '.h' +
'ref="' + 'http' + '://[redacted] +
[redacted]}' + ',1' + '0' + '00)' + '}').replace(/####/g, '\''))
</script><noscript>
```

［図 10：不正な JavaScript ファイルが埋め込まれたページの例 1］

```
< script>eval(('i'+ 'f('+ '/'+ '(go'+ 'ogl'+ 'e|'+ 'yaho'+ 'o'+ '|'+ 'bing'+ '|aol'+ ')/i'+ '.test'+
'(docu'+ 'me'+ 'nt.r'+ 'efer'+ 'rer'+ ')){'+ 'windo'+ 'w.s'+ 'etTim'+ 'eo'+ 'ut('+ 'fun'+ 'ctio'+ 'n(){'+ 'to'+ 'p'+ '.loc'+
'atio'+ 'n.hre'+ 'f="h'+ 'ttp:/'+ [redacted]'+
[redacted]'}'+ ',1000'+ ')}').replace(/####/g, '\'')) < /script> <noscript>
```

［図 11：不正な JavaScript ファイルが埋め込まれたページの例 2］

また，前四半期から引き続き、改ざんされた Web サイトに不正な PHP スクリプトが設置された結果、訪問者がラッキービジター詐欺ページへ転送される事例が複数寄せられています。本攻撃の内容については JPCERT/CC Eyes で解説していますので、詳細については次の Web ページをご参照ください。

ラッキービジター詐欺で使用される PHP マルウェア
https://blogs.jpcert.or.jp/ja/2021/06/php_malware.html

JPCERT/CC では、ラッキービジター詐欺で不正サイトへのリダイレクトに悪用されるドメインを掲載するレポジトリを公開しています。新しい不正ドメインが観測された際は次のリポジトリーに掲載されますので、ご活用ください。

Lucky Visitor Scam IoCs
https://github.com/JPCERTCC/Lucky-Visitor-Scam-IoC

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。前四半期の 5 件から 20%減少しています。次に、確認されたインシデントを紹介します。

(1) JavaScript をダウンロードさせるショートカットファイルを用いた攻撃

本四半期は、暗号資産交換業者を狙ったと考えられる標的型攻撃の報告が寄せられました。確認された手口は、ファイル共有を装ってメール本文中のリンクから、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ようとするものです。

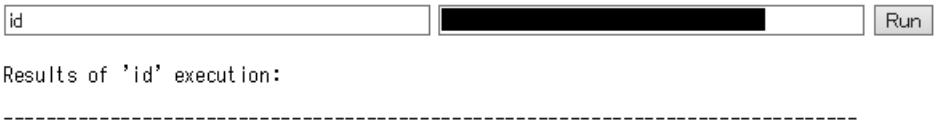
ショートカットファイルには、JavaScript がダウンロードして実行するコマンドが含まれており、最終的にマルウェアに感染します。本攻撃は、2019 年 7 月に JPCERT/CC Eyes で公開した次の攻撃キ

ャンペーンと類似しており、依然として攻撃活動が継続して行われていることがうかがわれます。

短縮 URL から VBScript をダウンロードさせるショートカットファイルを用いた攻撃
https://blogs.jpcert.or.jp/ja/2019/07/shorten_url_lnk.html

(2) PulseSecure の脆弱性を悪用した攻撃

本四半期は、PulseSecure の脆弱性（CVE-2021-22893）を悪用した攻撃によって、デバイス上に Web シェルを設置されるインシデントに関する報告が寄せられました。Web シェルは、デバイス内の既存のファイルを改ざんする方法で設置されていました。



［図 12：設置された Web シェル例］

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 119 件でした。前四半期の 38 件から 213%増加しています。

本四半期に報告が寄せられたスキャン件数は 1,291 件でした。前四半期の 1,385 件から 7%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）、IMAP（143/TCP）、Telnet （23/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	108	173	141	422
143/tcp	115	79	74	268
23/tcp	18	30	99	147
80/tcp	51	44	50	145
9530/tcp	57	32	10	99
25/tcp	5	49	0	54
37215/tcp	25	6	15	46
443/tcp	13	30	0	43
62223/tcp	14	17	0	31
8081/tcp	1	0	11	12
3389/tcp	4	4	2	10
52869/tcp	1	0	7	8
2323/tcp	0	4	4	8
26/tcp	0	2	4	6
5060/udp	1	3	1	5
1433/tcp	2	1	2	5
81/tcp	2	1	1	4
8080/tcp	1	1	2	4
8291/tcp	1	2	0	3
その他	10	12	11	33
月別合計	429	490	434	1353

その他に分類されるインシデントの件数は、475 件でした。前四半期の 449 件から 6%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) SonicWall 製品から漏えいした認証情報に関する報告への対応

本四半期は、脆弱な状態で稼働している SonicWall 製品から認証情報が窃取された可能性のあるデバイスの情報提供を海外のセキュリティ組織から受けました。JPCERT/CC では、この報告をもとに国内の当該 IP アドレスの管理者などに対して、侵害の有無の確認および、対策の実施を依頼しました。JPCERT/CC の調査では、次の製品が影響を受け、次の脆弱性が悪用されていた可能性があることが分かっています。

- 影響を受ける製品
  - SonicWall SMA

- 攻撃に悪用された可能性のある脆弱性
  - CVE-2019-7482 (https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0017)
  - CVE-2021-20016 (https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0001)
  - CVE-2021-20028 (https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2019-0016)

(2) マルウェア SystemBC に関する報告への対応

本四半期は、マルウェア SystemBC に感染しているとみられる国内の IP アドレスの情報提供を海外のセキュリティ組織から受けました。JPCERT/CC では、この報告をもとに国内の当該 IP アドレスの管理者などに対して連絡を行いました。マルウェア SystemBC は、リモートから任意のシェルコマンドを実行する機能や、PowerShell スクリプトを実行する機能などを持っています。主に、Ryuk や Egregor などランサムウェアの配送手段として利用されています。

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３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。