JPCERT-IR-2018-04

発行日: 2018-10-16

JPCERT/CC インシデント報告対応レポート
［2018 年 7 月 1 日 ～ 2018 年 9 月 30 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 7 月 1 日から 2018 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（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］

	7 月	8 月	9 月	合計	前四半期合計
報告件数 (注 2)	1,305	1,235	1,368	3,908	3,815
インシデント件数 (注 3)	1,081	1,161	1,169	3,411	3,595
調整件数 (注 4)	687	846	683	2,216	2,124

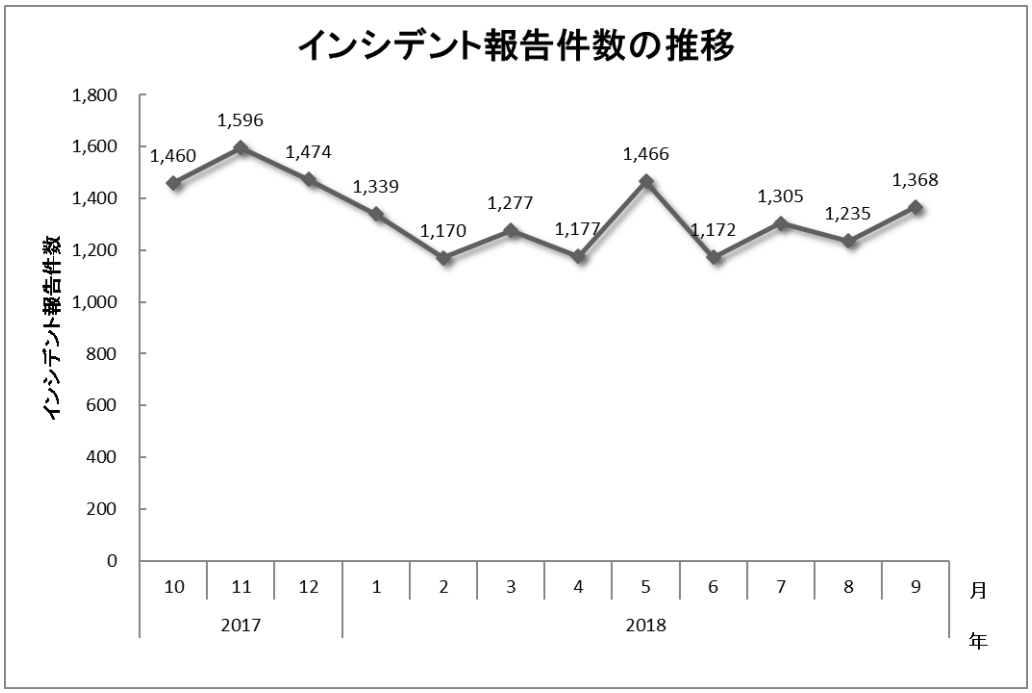
（注 2）「報告件数」は、報告者から寄せられた Web フォーム、メール、FAX による報告の総数を示します。

（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。

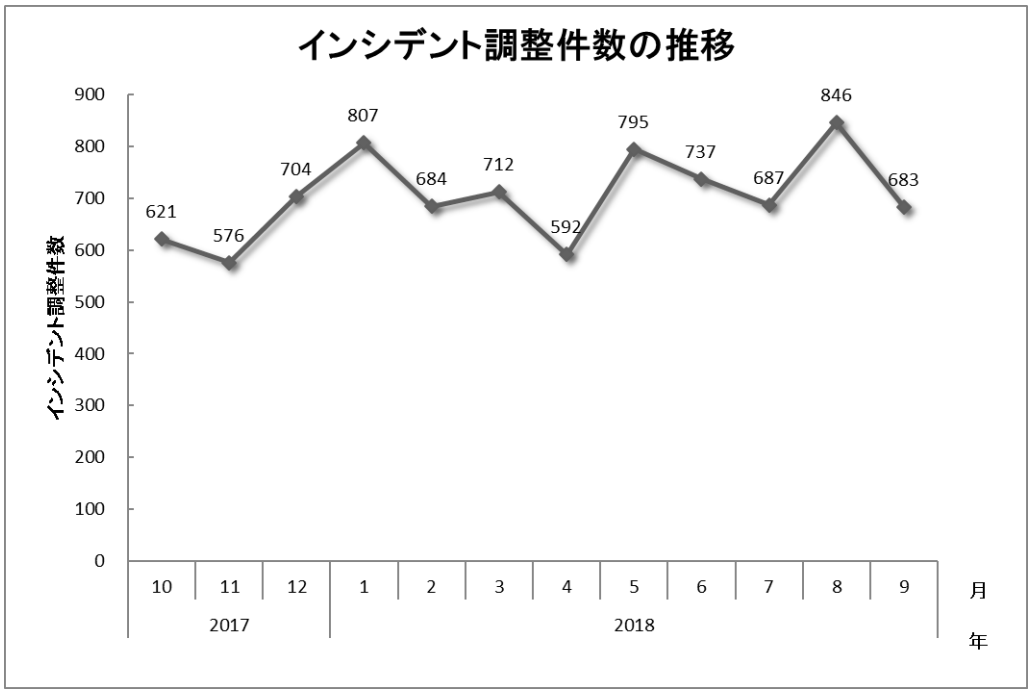
（注 4）「調整件数」は、インシデントの拡大防止のため、サイトの管理者等に対し、現状の調査と問題解決のための対応を依頼した件数を示します。

本四半期に寄せられた報告件数は、3,908 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 2,216 件でした。前四半期と比較して、報告件数は 2%増加し、調整件数は 4%増加しました。また、前年同期と比較すると、報告数で 15%減少し、調整件数は 1%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］



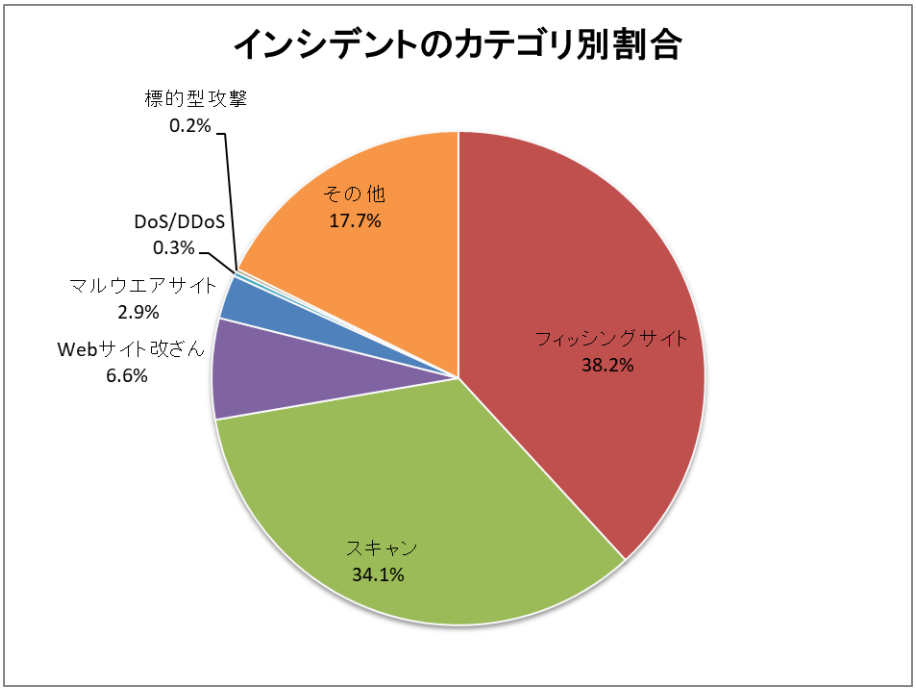
［図 2 インシデント調整件数の推移］

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］

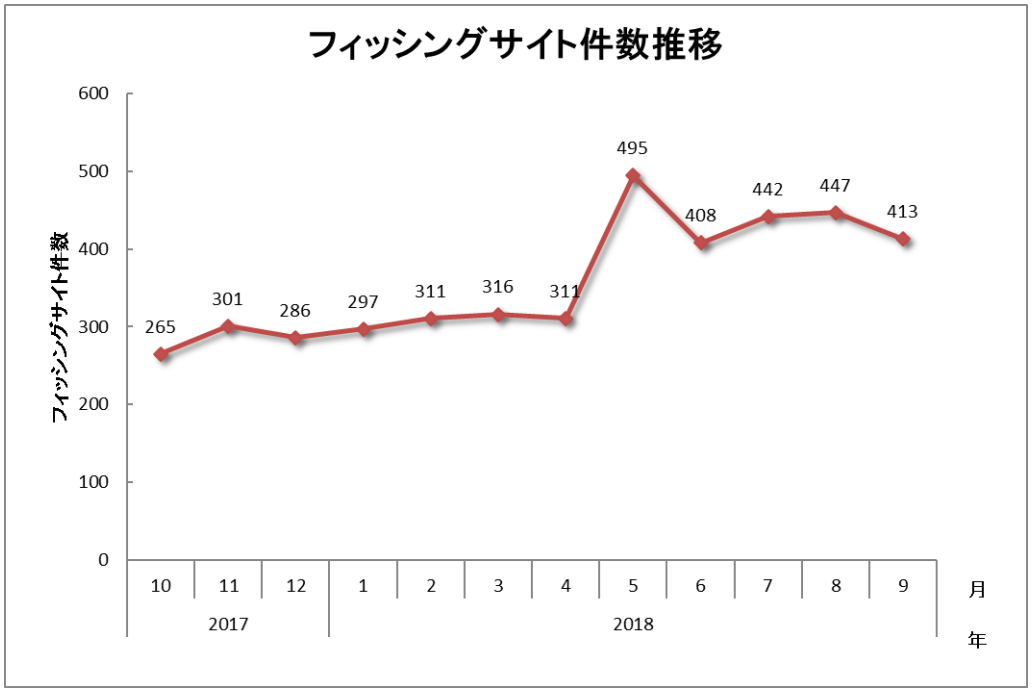
インシデント	7 月	8 月	9 月	合計	前四半期合計
フィッシングサイト	442	447	413	1,302	1,214
Web サイト改ざん	64	66	96	226	320
マルウエアサイト	28	45	25	98	89
スキャン	346	463	355	1,164	1,255
DoS/DDoS	9	0	1	10	0
制御システム関連	0	0	0	0	0
標的型攻撃	4	3	0	7	9
その他	188	137	279	604	708

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 38.2%、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 34.1%を占めています。

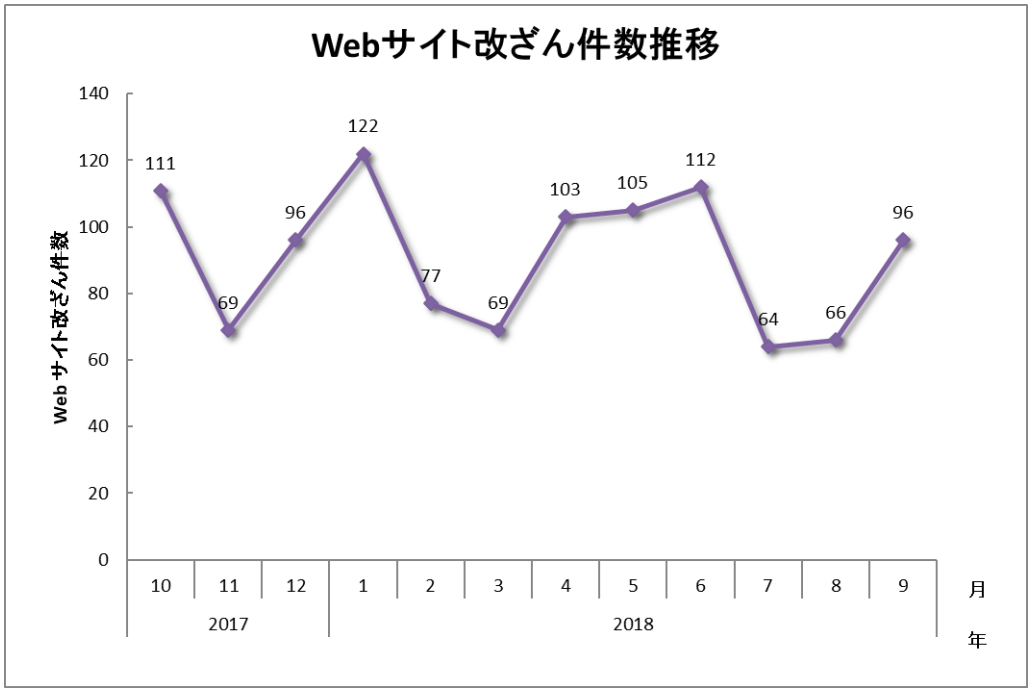


［図 3 インシデントのカテゴリ別割合］

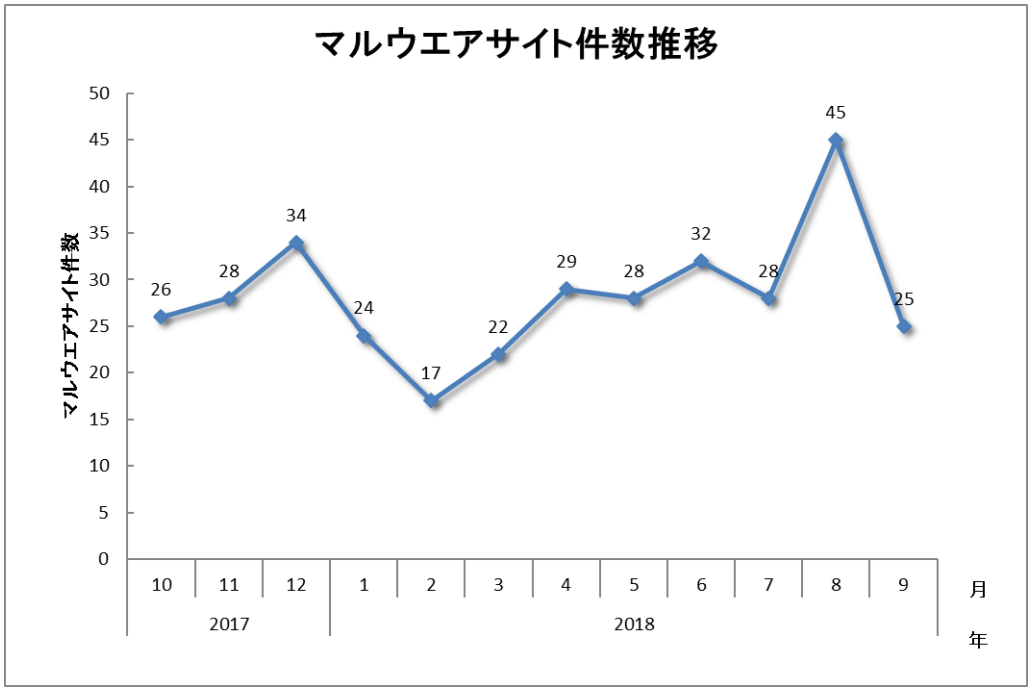
［図 4］から［図 7］に、フィッシングサイト、Web サイト改ざん、マルウエアサイト、スキャンのインシデントの過去 1 年間の月別推移を示します。



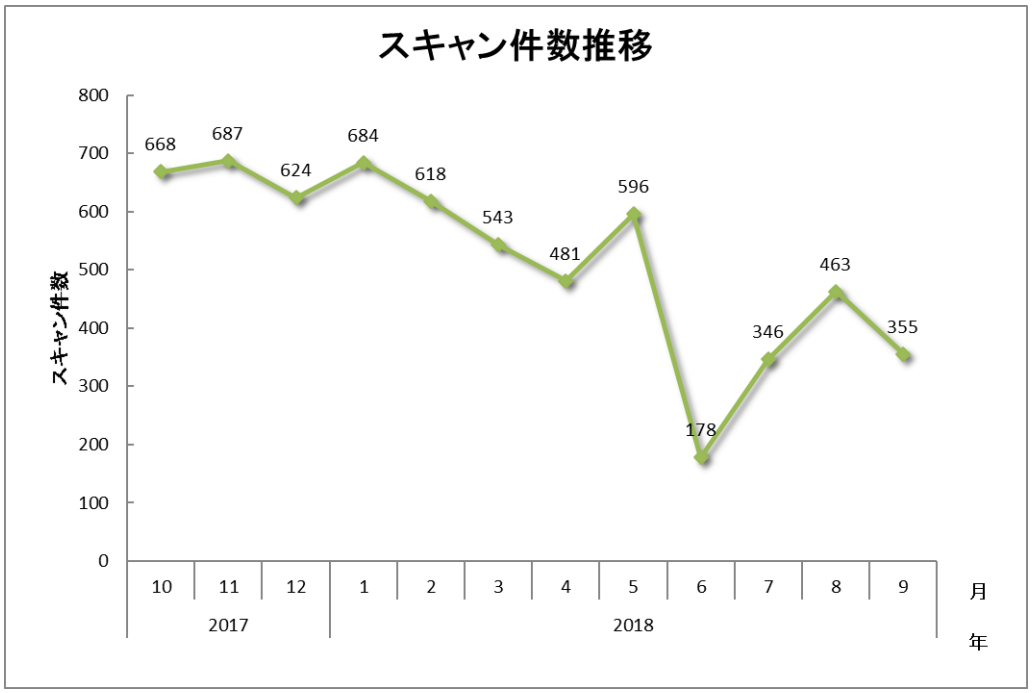
［図 4 フィッシングサイト件数の推移］



［図 5 Web サイト改ざん件数の推移］

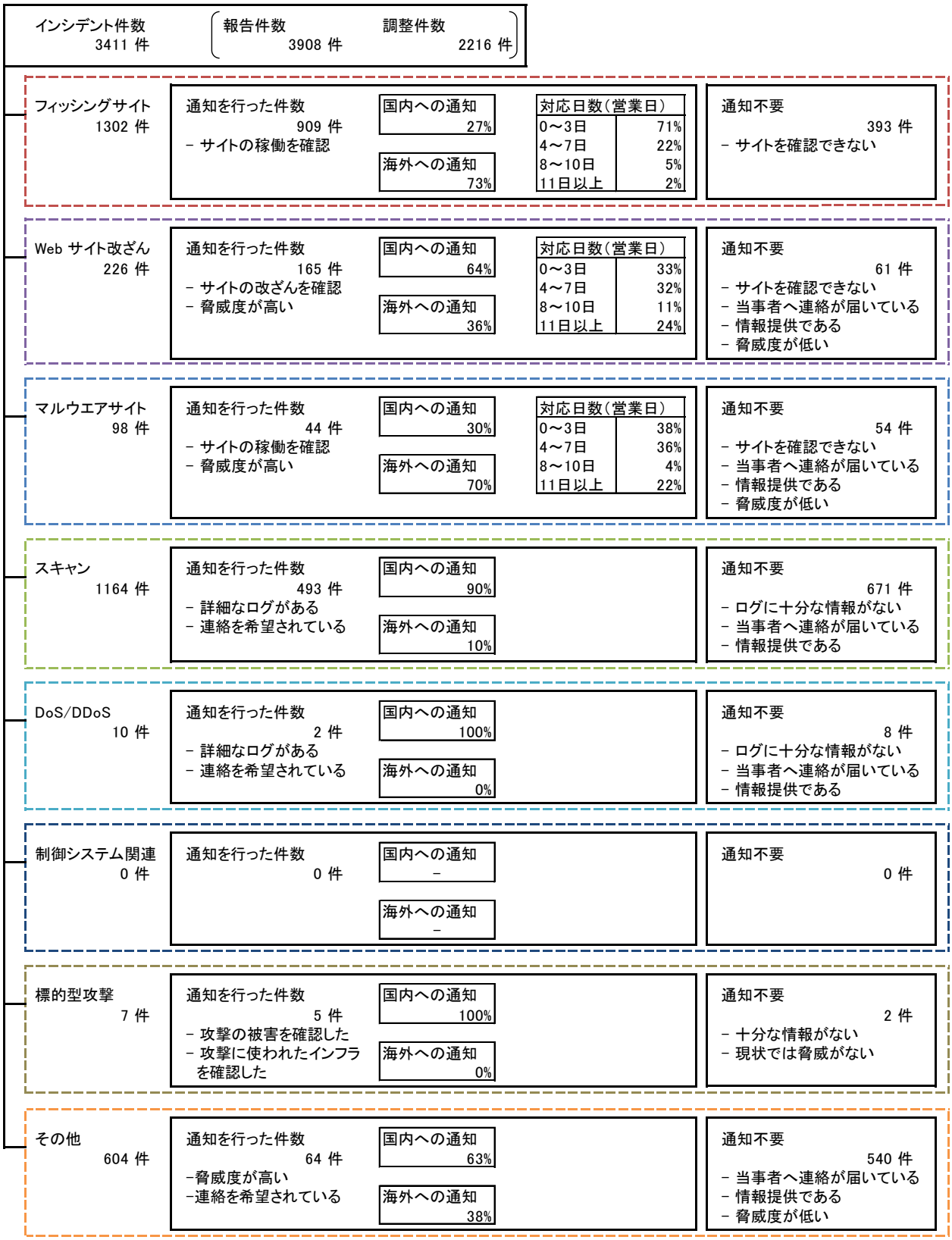


［図 6 マルウエアサイト件数の推移］



［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（前四半期より図の構成を変更しています）。



[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

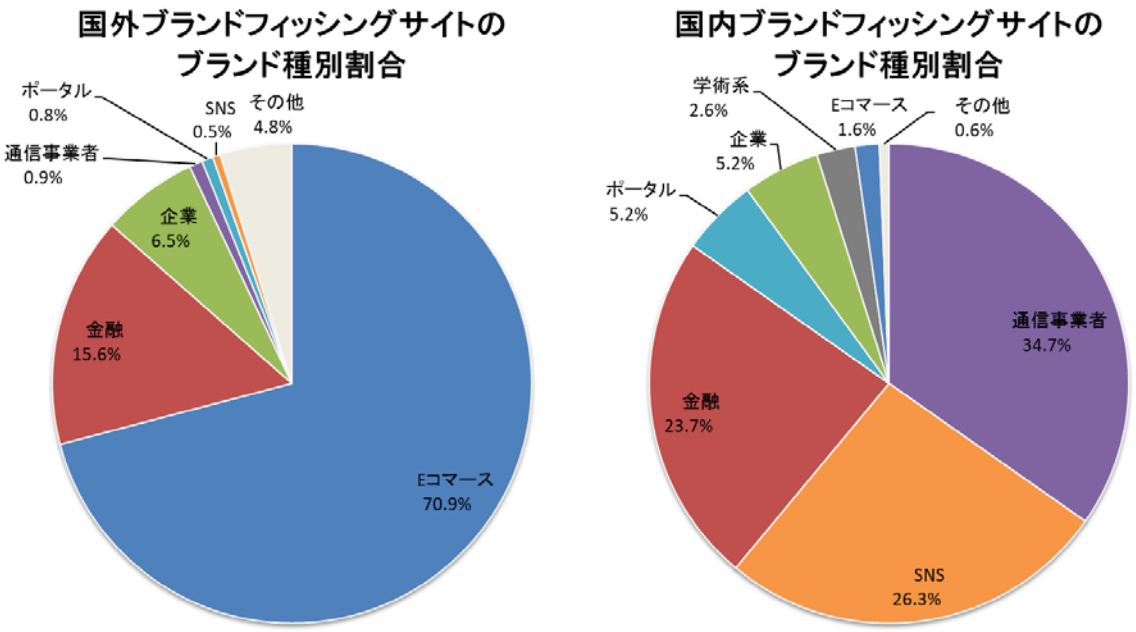
本四半期に報告が寄せられたフィッシングサイトの件数は 1,302 件で、前四半期の 1,214 件から 7%増加しました。また、前年度同期（1,011 件）との比較では、29%の増加となりました。

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 309 件となり、前四半期の 228 件から 36%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 784 件となり、前四半期の 722 件から 9%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	110	97	102	309(24%)
国外ブランド	255	287	242	784(60%)
ブランド不明 (注 5)	77	63	69	209(16%)
全ブランド合計	442	447	413	1,302(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は、国外ブランドでは E コマースサイトを装ったものが 70.9%、国内ブランドでは通信事業者のサイトを装ったものが 34.7%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多く寄せられています。フィッシングサイトのドメインは、正規サイトと紛らわしい名前で新規に登録されたものが多く、.com ドメインが特に多く使われていましたが、.jp ドメインの悪用も多数確認されています。

国内ブランドのフィッシングサイトでは、通信事業者、SNS、金融機関を装ったものが多く確認されており、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としては、国内 ISP の Web メールのログイン画面を装ったものや、携帯キャリアのアカウントを狙ったものを確認している。携帯キャリアのフィッシングサイトは、正規サイトを装った.com ドメインのものが多く、異なるブランドのフィッシングサイトに同じ IP アドレスが割り当てられている場合があった
- SNS を装ったフィッシングサイトは、以前は.cn ドメインが継続的に使用されていたが、8 月半ば以降、.top ドメインも多く使用されている。その他に、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も 8 月末以降確認されている
- 国内金融機関を装ったフィッシングサイトでは、インターネットバンキングを装ったものがなく、すべてクレジットカード会社を装ったものだった。正規サイトと紛らわしい.com ドメインを使用したサイトが多く、特定のブランドのフィッシングサイトでは携帯キャリアのフィッシングサイトでも確認された IP アドレスが割り当てられている場合があった

フィッシングサイトの調整先の割合は、国内が 27%、国外が 73%であり、前四半期（国内が 30%、国外が 70%）と比べて国外への通知の割合が増加しました。

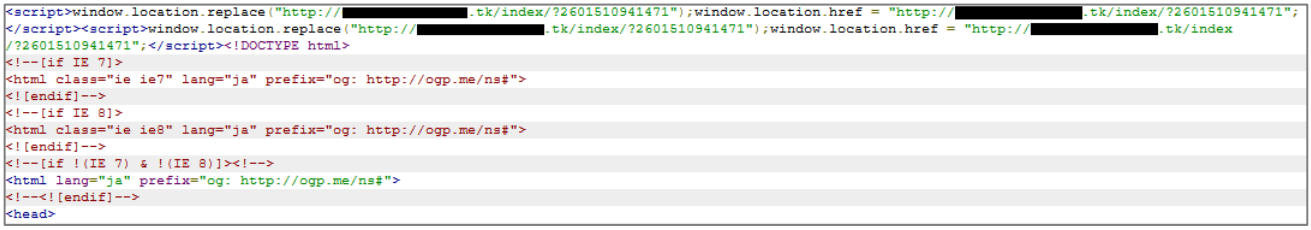
3.2. Web サイト改ざんの傾向

本四半期に報告が寄せられた Web サイト改ざんの件数は、226 件でした。前四半期の 320 件から 29%減少しています。

前四半期に引き続き、改ざんされた Web サイトから、次のような URL で示される Web ページを経由し、不審なサイトに転送されるといった報告が多く寄せられました。

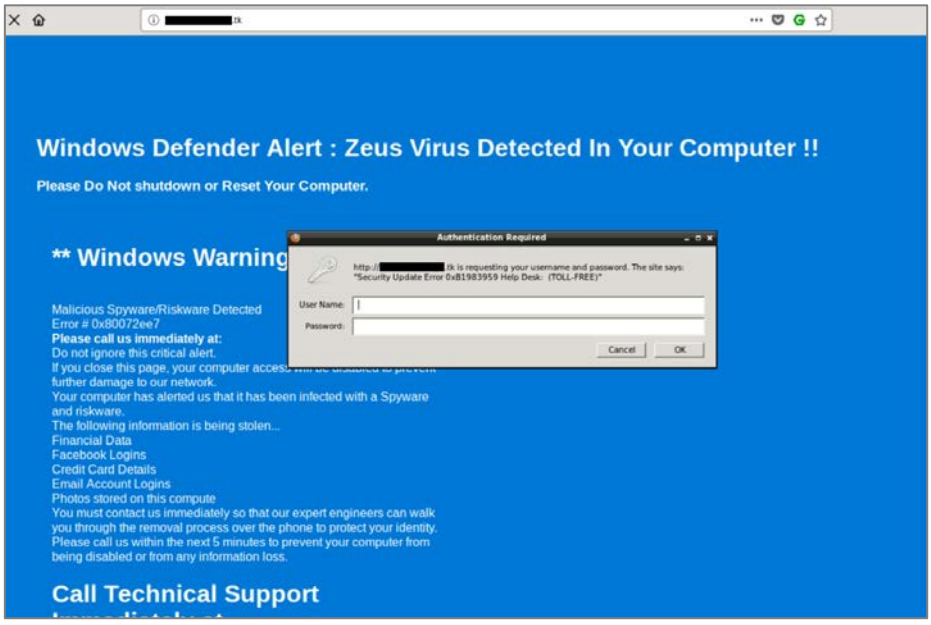
```
http://<ドメイン名>.tk/index/?<数字の列>
```

.tk ドメインの URL への転送は、ページの最上部に埋め込まれた JavaScript（[図 10] 参照）や、ページが読み込む JavaScript ファイル内に埋め込まれた難読化されたスクリプトなどによって行われることを確認しています。



[図 10 .tk ドメインの URL に転送する JavaScript]

改ざんされたサイトからの転送先として、偽のマルウエア感染の警告を表示するサイトや、広告を表示するサイト、「アンケートに回答すると賞品が入手できる」と書かれた不審なサイトなどを確認しています。また、.tk ドメインのサイトのドキュメントルートにアクセスすると、アクセスしたブラウザによっては、偽のマルウエア感染の警告が表示される場合がありました。（[図 11] 参照）



［図 11 偽のマルウエア感染の警告表示］

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、7 件でした。前四半期の 9 件から 22%減少しています。このうち対応を依頼した組織は 3 組織でした。

本四半期は、マクロ付きのファイルが添付された標的型攻撃メールに関する報告が複数寄せられましたが、最終的に実行されるマルウエアの種類はさまざまでした。次に、確認された 3 つの例を紹介します。

(1) マルウエア ANEL に感染させるマクロ付きの Word ファイル

2018 年 7 月から 8 月にかけて、ANEL と呼ばれる HTTP ボットに感染させることを目的とした標的型攻撃メールに関する報告が複数寄せられました。いずれの報告でも、攻撃者は無料の国内 Web メールサービスを使用し、パスワードがかかったマクロ付きの Word ファイルを添付したメールと、添付ファイルのパスワードが書かれたメールを送付していました。Word ファイルのマクロを実行すると、マルウエアが展開、実行され、ユーザのログオン時にマルウエアを自動実行する設定がレジストリに追加されるようになっていました。

(2) Cobalt Strike Beacon に感染させるマクロ付きの Word ファイル

7 月後半に複数の組織で確認された標的型攻撃メールでは、添付ファイルを実行することで、最終的にペネトレーションテストツール Cobalt Strike のペイロード（Cobalt Strike Beacon）が実行されることを確認しました。メールにはマクロ付きの Word ファイルが添付されており、マクロを実行すると、国内サイトから画像ファイルを装った不正なファイルをダウンロードするとともに、ファイルから展開した実行ファイルを実行するタスクを登録する仕組みになっていました。タスクに登録される

実行ファイルはダウンローダであり、HTTP で C&C サーバと通信を行う Cobalt Strike Beacon をダウンロードし、メモリ上に展開して実行するものでした。

(3) マルウエア TSCookie に感染させるマクロ付きの Excel ファイル

8 月の後半に報告が寄せられた標的型攻撃メールには、マクロ付き Excel ファイル（xlsm ファイル）を含む RAR 形式の圧縮ファイルが添付されていました。Excel ファイルは暗号化されていましたが、開く際にパスワードを入力する必要がないように作成されていました。これは、Excel ファイルで使用可能な特別なパスワードが設定されていたためでした(1)。Excel ファイルのマクロを実行すると、スタートアップフォルダに実行ファイルが作成され、OS の起動時に自動実行されるようになっていました。実行ファイルは TSCookie と呼ばれるマルウエアで、2018 年 6 月末頃の標的型攻撃でも使用されていました。今回確認したマルウエアも、スタートアップフォルダにマルウエアが作成され、マルウエアを実行すると C&C サーバのポート 443/TCP に HTTP で接続するといった、以前のものと共通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、98 件でした。前四半期の 89 件から 10%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、1,164 件でした。前四半期の 1,255 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）、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	136	190	132	458
80/tcp	96	105	65	266
25/tcp	34	54	60	148
23/tcp	23	32	13	68
445/tcp	5	18	29	52
52869/tcp	0	21	3	24
3389/tcp	3	4	15	22
443/tcp	3	2	16	21
8080/tcp	5	5	8	18
5555/tcp	10	6	2	18
81/tcp	6	2	7	15
8000/tcp	10	2	2	14
37215/tcp	8	1	2	11
21/tcp	2	8	1	11
88/tcp	4	1	5	10
8181/tcp	0	0	9	9
8001/tcp	5	2	2	9
2323/tcp	3	3	2	8
84/tcp	4	0	2	6
82/tcp	4	1	0	5
8088/tcp	2	3	0	5
その他	505	338	29	872
月別合計	868	798	404	2,070

その他に分類されるインシデントの件数は、604 件でした。前四半期の 708 件から 15%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) 佐川急便を装って Android マルウエアを配布するサイトに関する対応

本四半期は佐川急便の Web サイトを模倣して Android のマルウエアを配布するサイト[(2)]に関する報告が継続して寄せられました。マルウエアは公式アプリを装った名前やアイコンを使用していましたが、必要な権限に SMS の送信やマイクの録音など、公式アプリと異なるものがありました。マルウエアを Android OS にインストールして起動すると、C&C サーバの情報を取得するためとみられる通信が確認できました。マルウエアの通信先は配布された時期によって変化があり、SNS の Web ページ上の文字列や、特定のメールアカウントの受信メールの件名から、次に通信する先の IP アドレスを抽出する仕組みになっていました。7 月下旬に入手したマルウエアの、メールの件名から通信先を取得するコードを［図 12］に示します。

```
Properties localProperties = new Properties();
localProperties.setProperty("mail.transport.protocol", "pop3");
localProperties.setProperty("mail.pop3.host", "[redacted]");
localProperties.setProperty("mail.pop3.port", "995");
localProperties.setProperty("mail.pop3.ssl.enable", "true");
localProperties.setProperty("mail.pop3.ssl.trust", "*");
Session localSession = Session.getDefaultInstance(localProperties);
d.e.b.h.a(localSession, "session");
localSession.setDebug(true);
Store localStore = localSession.getStore("pop3");
List localList = d.i.m.a((CharSequence)paramString, new char[] { ':' }, false, 0, 6, null);
localStore.connect((String)localList.get(0), (String)localList.get(1));
Folder localFolder = localStore.getFolder("INBOX");
localFolder.open(1);
d.e.b.h.a(localFolder, "folder");
Message[] arrayOfMessage = localFolder.getMessages();
int i1 = arrayOfMessage.length;
i2 = 0;
if (i2 < i1)
{
  Message localMessage = arrayOfMessage[i2];
  d.e.b.h.a(localMessage, "msg");
  String str2 = localMessage.getSubject();
  d.e.b.h.a(str2, "subject");
  if (!d.i.m.a(str2, "abcd", false, 2, null))
    break label293;
  String str3 = str2.substring(4);
  d.e.b.h.a(str3, "(this as java.lang.String).substring(startIndex)");
  Log.d("WS:", str3);
  str1 = p.a(str3);
}
```

メールサーバの接続の設定

メールの件名がabcdで始まる場合、後ろの文字列を抽出

抽出した文字列をデコードする処理を行う

［図 12 メールの件名から通信先を取得するマルウエアのコード］

マルウエアは端末から窃取した情報を送信する機能などを持っており、前四半期に確認された、DNS 設定を書き換えられたルータが、配下のネットワークに接続された端末にダウンロードさせる Android マルウエアと一致する箇所が見られました。

マルウエア配布サイトには、アクセス元の端末、ブラウザの環境をチェックする JavaScript が埋め込まれていました。さらに、8 月半ば以降は、Android 端末からのアクセスでない場合に、2 段階認

証の認証コードの窃取を目的としたフィッシングサイトに転送する仕組みになっていました。確認したすべてのサイトに、台湾の特定の ISP の動的な IP アドレスが割り当てられていたため、JPCERT/CC は、IP アドレスを管理する ISP と、台湾の National CSIRT である TWNCERT に、適切な対応を行うよう依頼しました。

5. 参考文献

(1) Cybozu Inside Out | サイボウズエンジニアのブログ
Excel の奇妙なパスワードとマクロウイルス
https://blog.cybozu.io/entry/2017/03/09/080000

(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

JPCERT CC®

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。