JPCERT-IR-2018-03
発行日: 2018-07-12

JPCERT/CC インシデント報告対応レポート
［2018 年 4 月 1 日 ～ 2018 年 6 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 4 月 1 日から 2018 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、本稿では、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（本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)	1,177	1,466	1,172	3,815	3,786
インシデント件数 (注 3)	1,131	1,425	1,039	3,595	3,857
調整件数 (注 4)	592	795	737	2,124	2,203

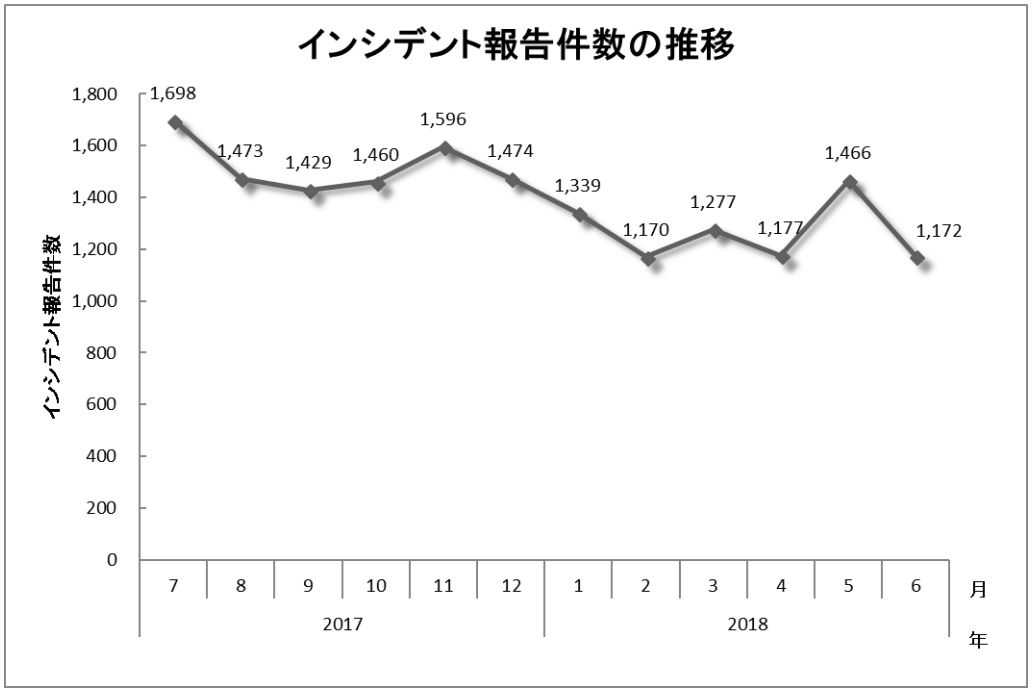
（注 2）「報告件数」は、報告者から寄せられた Web フォーム、メール、FAX による報告の総数を示します。

（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。

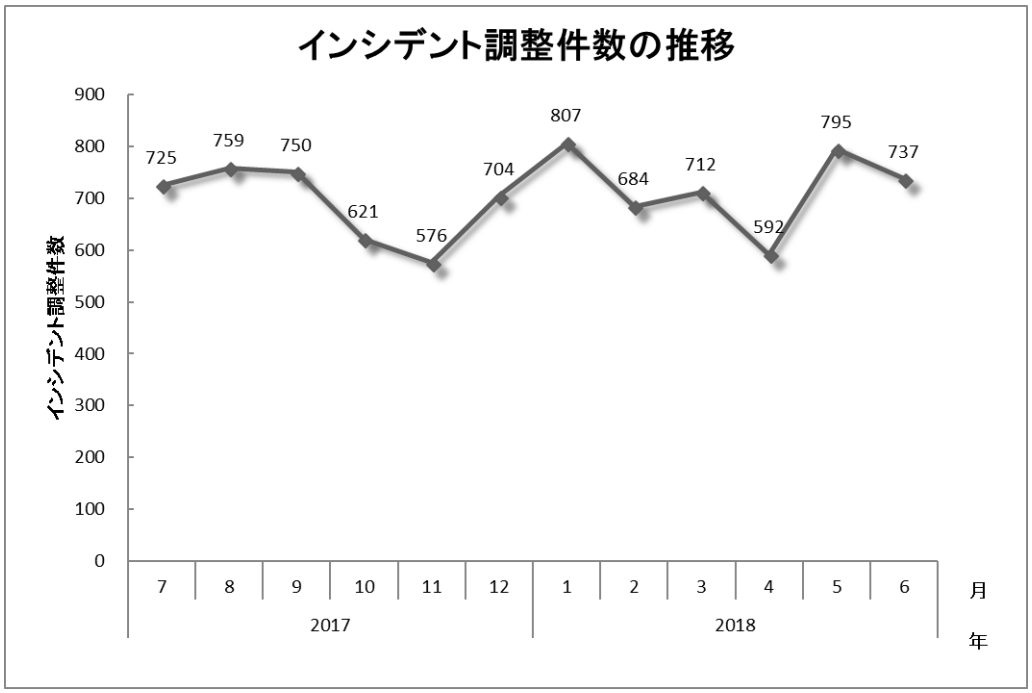
（注 4）「調整件数」は、インシデントの拡大防止のため、サイトの管理者等に対し、現状の調査と問題解決のための対応を依頼した件数を示します。

本四半期に寄せられた報告件数は、3,815 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 2,124 件でした。前四半期と比較して、報告件数は 1%増加し、調整件数は 4%減少しました。また、前年同期と比較すると、報告数で 27%減少し、調整件数は 17%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］



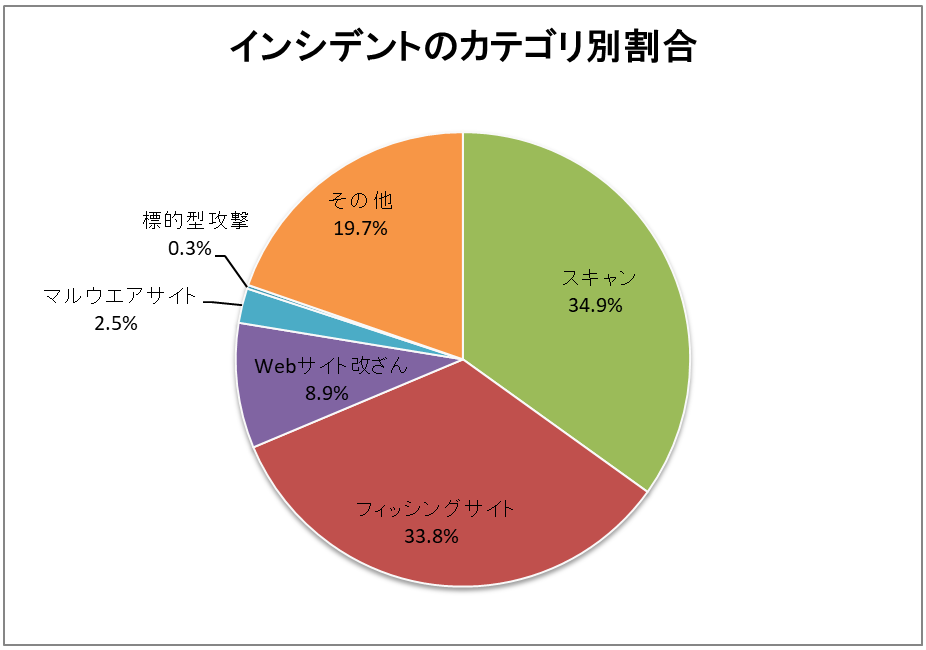
［図 2 インシデント調整件数の推移］

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］

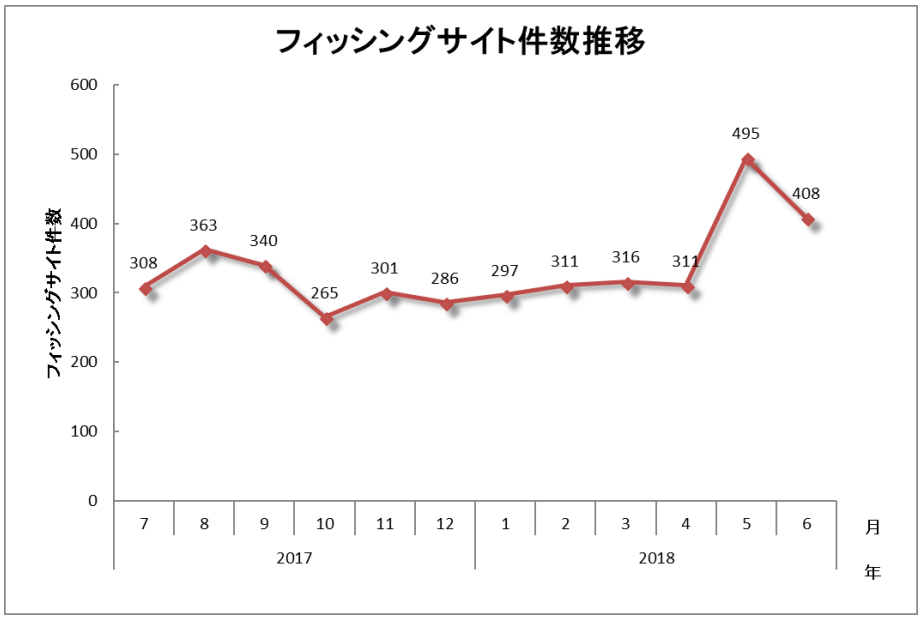
インシデント	4 月	5 月	6 月	合計	前四半期合計
フィッシングサイト	311	495	408	1,214	924
Web サイト改ざん	103	105	112	320	268
マルウエアサイト	29	28	32	89	63
スキャン	481	596	178	1,255	1,845
DoS/DDoS	0	0	0	0	1
制御システム関連	0	0	0	0	7
標的型攻撃	2	3	4	9	6
その他	205	198	305	708	743

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 34.9%、フィッシングサイトに分類されるインシデントが 33.8%を占めています。

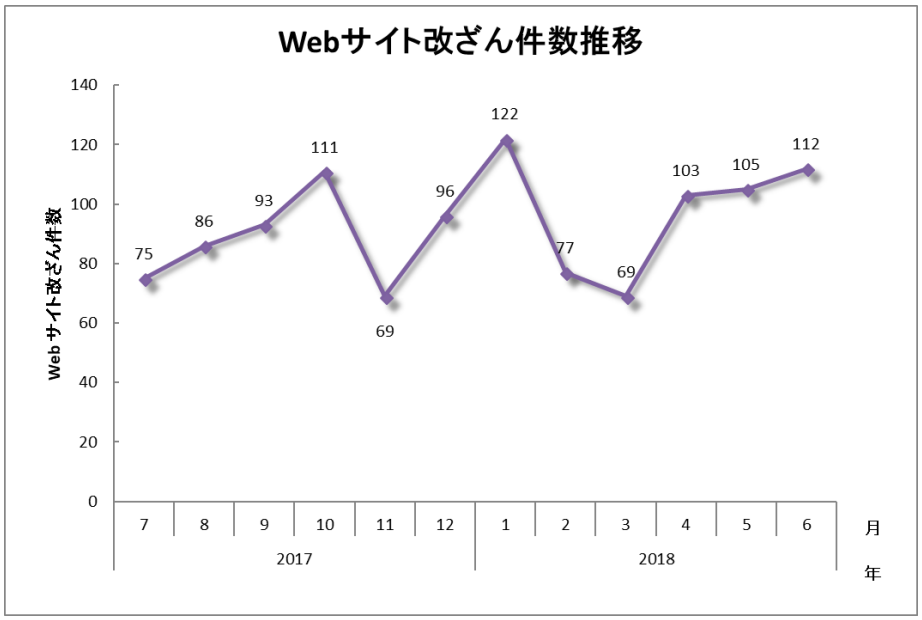


［図 3 インシデントのカテゴリ別割合］

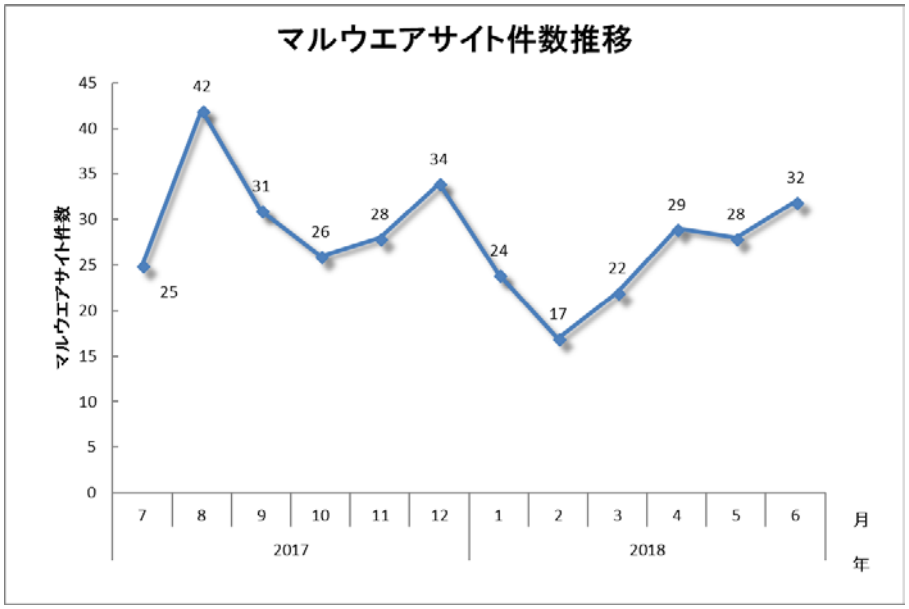
［図 4］から［図 7］に、フィッシングサイト、Web サイト改ざん、マルウエアサイト、スキャンのインシデントの過去 1 年間の月別推移を示します。



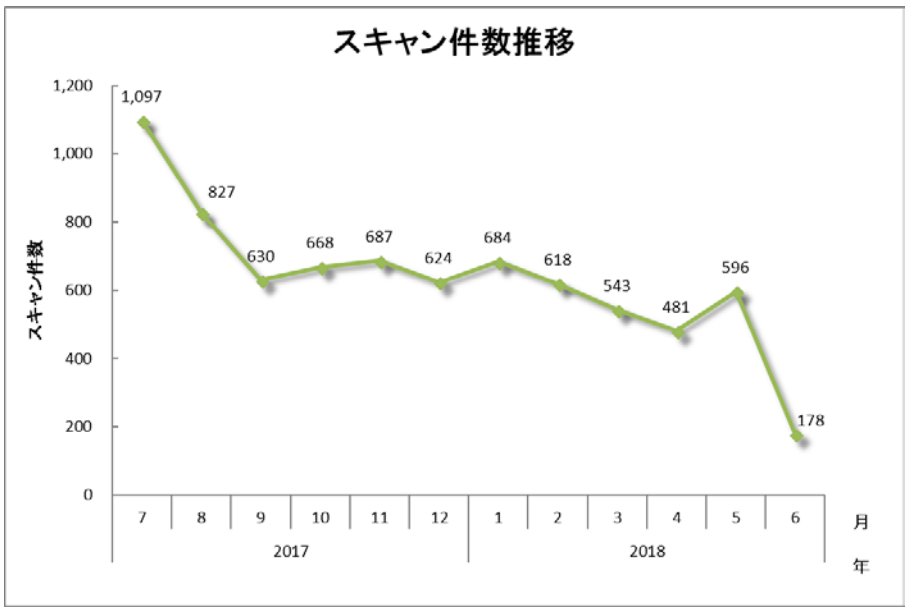
［図 4 フィッシングサイト件数の推移］



［図 5 Web サイト改ざん件数の推移］

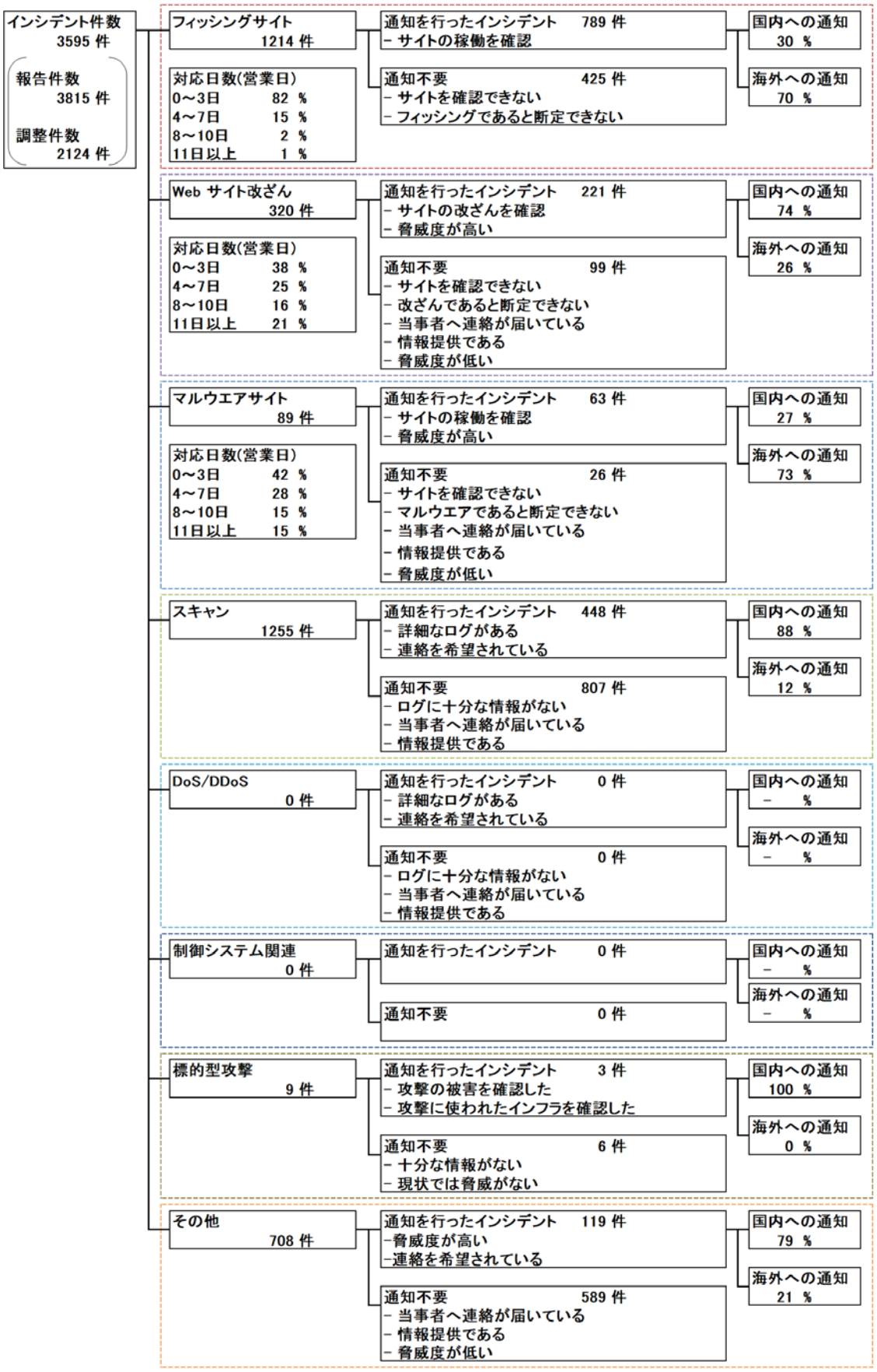


［図 6 マルウエアサイト件数の推移］



［図 7 スキャン件数の推移］

［図 8］に内訳を含むインシデントにおける調整・対応状況を示します（本四半期より図の構成を変更しています)。



［図 8 インシデントにおける調整・対応状況］

3. インシデントの傾向

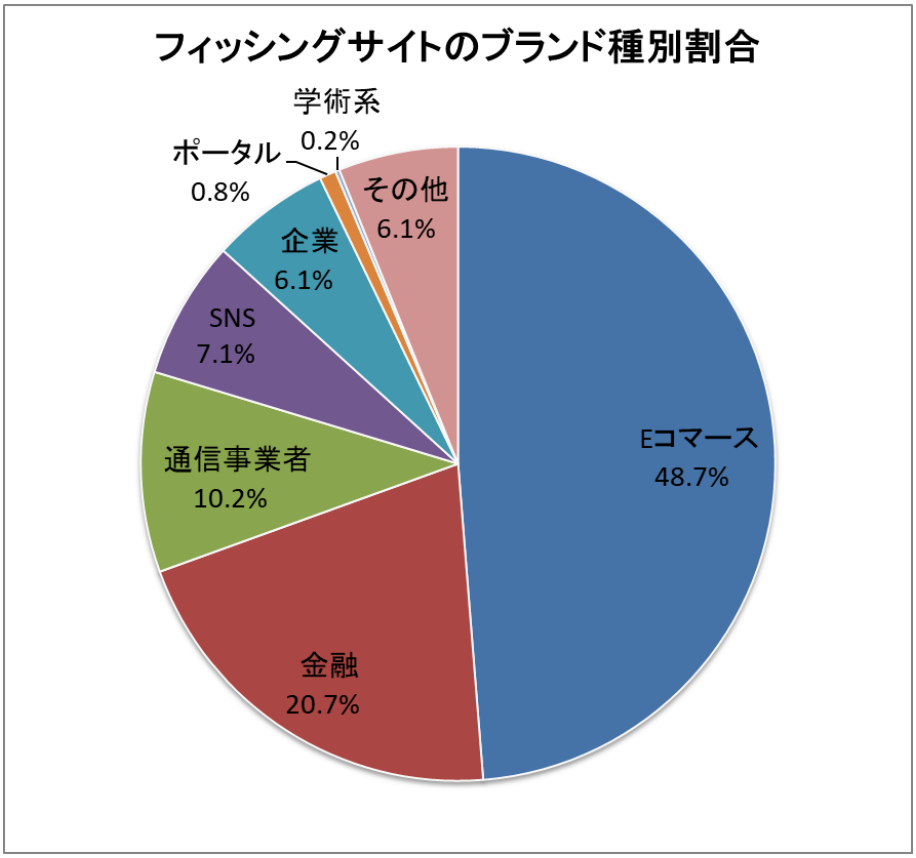
3.1. フィッシングサイトの傾向

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 1,214 件で、前四半期の 924 件から 31%増加しました。また、前年度同期（736 件）との比較では、65%の増加となりました。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］、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	67	85	76	228(19%)
国外ブランド	166	298	258	722(59%)
ブランド不明 (注 5)	78	112	74	264(22%)
全ブランド合計	311	495	408	1,214(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］

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 228 件となり、前四半期の 208 件から 10%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 722 件となり、前四半期の 564 件から 28%増加しました。

JPCERT/CC が報告を受けたフィッシングサイトの内訳は、E コマースサイトを装ったものが 48.7%、金融機関のサイトを装ったものが 20.7%、通信事業者のサイトを装ったものが 10.2%でした。

前四半期に引き続き、特定の国外ブランドのアカウント窃取を目的としたフィッシングサイトに関する報告が非常に多く寄せられており、本四半期における国外ブランドのフィッシング件数の半数以上を占めました。

国内ブランドのフィッシングサイトでは、前四半期と同様に、通信事業者、SNS、金融機関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ました。通信事業者を装ったフィッシングでは、大手携帯キャリアの複数ブランドを装ったサイトを確認していますが、これらのサイトのドメインを登録したメールアドレスが共通していました。SNS を装ったフィッシングサイトでは.cn ドメインが使用され、金融機関を装ったフィッシングサイトでは、異なる 2 つのブランドで、.club、.top、.xyz のドメインが共通して使用されているという特徴が見られました。

これらの国外、国内ブランドのフィッシングサイトの多くが、正規のブランド名に類似したドメイン名の一部を少しずつ置き換えて、特定のレジストラから次々に取得して利用していました。このようなドメイン登録は、フィッシング目的であろうことを容易に判断できるため、ドメインの登録申請を受けたレジストラが検知し、却下するような運用が望まれます。

フィッシングサイトの調整先の割合は、国内が 30%、国外が 70%であり、前四半期と同じ割合でした。

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、320 件でした。前四半期の 268 件から 19%増加しています。

本四半期は、正規の Web サイトが改ざんされていて、それにアクセスすると、商品の当選を装ってクレジットカード番号などを入力させる、あるいは「マルウエアを検知した」との偽のメッセージを表示するサイトなどに最終的に転送される事例を多数確認しました。こうした不正な転送では、.tk ドメインの URL を経由する事例を多く確認しています。転送の手法として、ページの最上部に埋め込まれた JavaScript や、ページ内に埋め込まれた難読化された JavaScript など、異なる複数の手口を確認しましたが、転送先 URL のパスには共通のパターンが見られました。また、検索サービスの検索結果から初めて Web サイトにアクセスした時にのみ、.loan ドメインの偽のアンケートサイトに転送が行われるような改ざん事

例も多く確認しています。

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、9 件でした。前四半期の 6 件から 50%増加しています。本四半期に対応を依頼した組織は 3 組織でした。

2018 年 4 月初めに、Word 文書を含む zip ファイルが添付された不審なメールに関する報告が寄せられました。Word 文書には、vbs ファイルを作成、実行するマクロが組み込まれており、マクロの実行によってマルウエアがダウンロードされ、最終的にリモートデスクトップツール Ammyy Admin と、通信先からファイルをダウンロードするマルウエアがインストールされることを確認しました。不審メールは、悪用されたメールアカウントから国内のメールサーバを介し送信された可能性がありました。また、vbs ファイルおよび最終的に感染するマルウエアがアクセスする URL のホスト部は、いずれも侵入されて悪用されたと見られる国内 IP アドレスを持つ Web サイトを示していました。不審メールに添付された Word 文書を開くことで Ammyy Admin がインストールされる事例は、2017 年 4 月にも確認されており、今回攻撃に使用された Word 文書のファイル名や、マクロで作成した vbs ファイルを実行する手法などは、以前のものと共通していました。

5 月後半に、標的型攻撃と見られるなりすましメールの報告が寄せられました。メールに添付された zip ファイルにはパスワードがかけられており、展開用のパスワードが別のメールに記載されていました。zip ファイルに含まれている Word 文書を開くと、Windows の VBScript エンジンの脆弱性（CVE-2018-8174）を悪用する攻撃コードがダウンロードされ、マルウエアが実行される仕組みになっていました。CVE-2018-8174 の脆弱性は、2018 年 5 月の Microsoft のセキュリティ更新プログラムで修正されたもので、攻撃者が脆弱性の公表から時を置かずに攻撃に悪用した事例と言えます。攻撃の最終段階で実行されるマルウエアは、C&C サーバから HTTP で命令を受信して動作するボットでした。

JPCERT/CC では、感染拡大の防止や攻撃範囲の特定を目的として、報告元から提供されたマルウエアの分析によって判明した通信先 URL などの情報を関連する組織に共有する取り組みを、報告元の許可を得て行っています。

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、89 件でした。前四半期の 63 件から 41%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、1,255 件でした。前四半期の 1,845 件から 32%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）、SMTP（25/TCP）、HTTP（80/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	244	256	63	563
25/tcp	88	142	2	232
80/tcp	22	77	52	151
23/tcp	51	16	14	81
21/tcp	1	42	0	43
443/tcp	0	3	29	32
2323/tcp	9	6	6	21
81/tcp	5	6	8	19
8080/tcp	8	5	3	16
7001/tcp	13	2	0	15
445/tcp	8	5	2	15
5555/tcp	3	4	6	13
3389/tcp	5	4	4	13
82/tcp	4	4	3	11
8000/tcp	0	3	8	11
8888/tcp	0	5	3	8
85/tcp	0	5	3	8
84/tcp	0	5	3	8
8081/tcp	0	3	5	8
53/udp	7	0	1	8
6379/tcp	2	3	1	6
9000/tcp	1	3	1	5
その他	787	730	22	1,539
月別合計	1,258	1,329	239	2,826

その他に分類されるインシデントの件数は、708 件でした。前四半期の 743 件から 5%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。

【Cisco Smart Install Client の脆弱性に関する対応】
2018 年 3 月末に、Cisco Smart Install Client の脆弱性（CVE-2018-0171）の情報が公開され、セキュリティ企業が当該脆弱性の実証コードを公開しました。脆弱性情報と実証コードが公開された直後のタイミングで、JPCERT/CC のインターネット定点観測システム（TSUBAME）で、Cisco Smart Install Client が使用するポート（4786/tcp）に対するスキャンの増加を確認しました。

4 月半ばに、Cisco Smart Install Client の脆弱性を使用した攻撃について、国内から複数の情報が寄せられました。攻撃を受けた組織では、ネットワーク機器の再起動や設定の書き換えなどの被害が確認されました。攻撃が広範囲に行われている可能性があったため、JPCERT/CC は、海外セキュリティ組織から提供された、ポート 4786/tcp がインターネットからアクセス可能になっている国内 IP アドレスの情報をもとに、IP アドレスを管理している組織にネットワーク機器の設定について確認するよう依頼しました。

【ネットワーク機器の DNS 設定の不正な書き換えおよび関連するマルウエアに関する対応】
2018 年 3 月半ばに、ルータの DNS 設定が不正に書き換えられ、ルータ配下の端末が Web サイトにアクセスすると、不審な apk ファイルのダウンロードが行われるといった事象が発生していることが、公開情報から確認されました。

4 月半ばに、同様の事象で不正に設定される DNS サーバとして日本の IP アドレスのものが確認され、当該 DNS サーバを設定して特定の Web サイトへのアクセスを行ったところ、apk ファイルがダウンロードされることを確認できました。apk ファイルを分析したところ、3 月に確認された apk ファイルと類似していましたが、特定のメールアドレスにメールを送信する新たな機能があることが分かりました。送信されるメールは、件名に接続エラーを意味する簡体字中国語と端末の言語設定、本文に電話番号や ping コマンドの実行結果などが埋め込まれており、感染端末の把握を目的としたものと推測されます。JPCERT/CC は、不正な DNS サーバの IP アドレスを管理するホスティング事業者に連絡し、サーバを停止した旨の返信を受領しました。

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。