JPCERT CC®

Japan Computer Emergency Response Team Coordination Center

JPCERT-IR-2017-03

発行日: 2017-07-13

JPCERT/CC インシデント報告対応レポート
［2017 年 4 月 1 日 ～ 2017 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、2017 年 4 月 1 日から 2017 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。

［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)	1333	1380	2512	5225	4095
インシデント件数 (注 3)	1376	1388	2601	5365	4856
調整件数 (注 4)	883	823	847	2553	3077

（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。

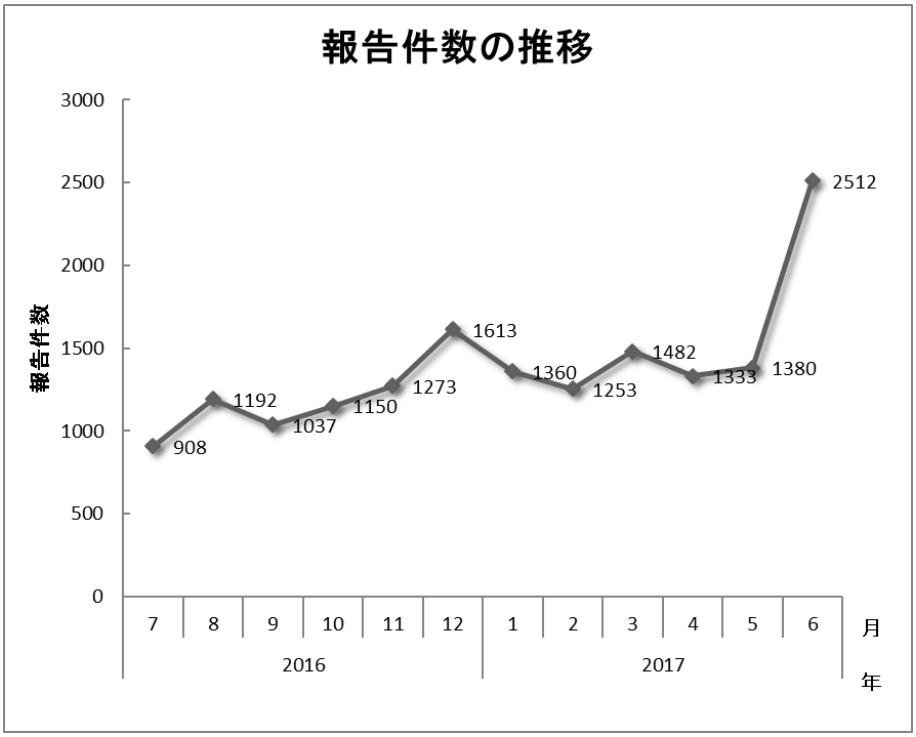
（注 3）「インシデント件数」は、各報告に含まれるインシデント件数の合計を示します。1 つのイン

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。

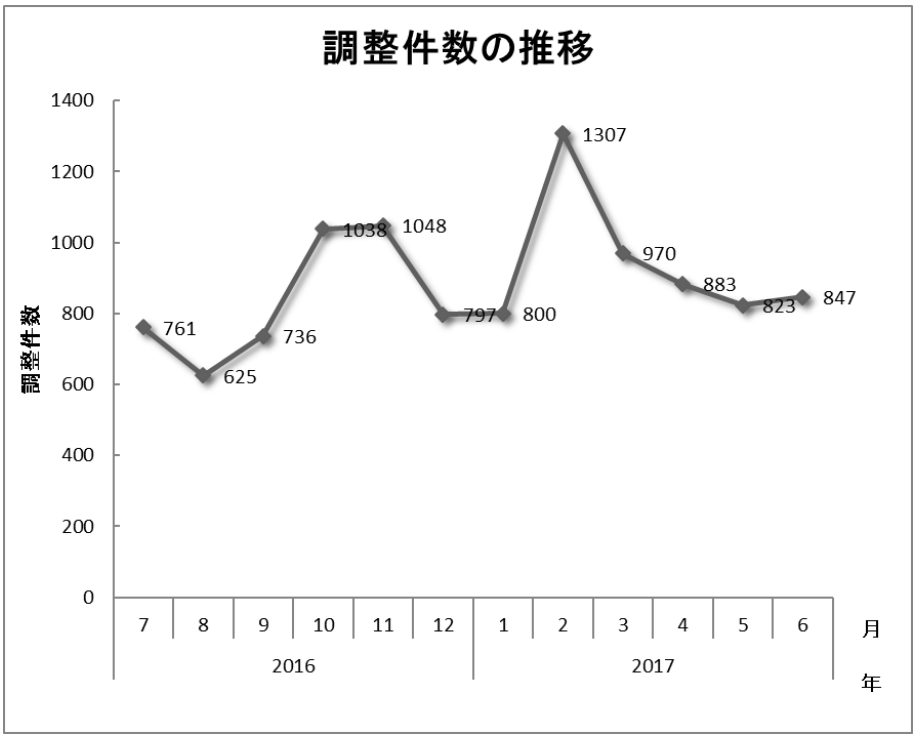
（注 4）「調整件数」は、インシデントの拡大防止のため、サイトの管理者等に対し、現状の調査と問題解決のための対応を依頼した件数を示します。

本四半期に寄せられた報告件数は、5225 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 2553 件でした。前四半期と比較して、報告件数は 28%増加し、調整件数は 17%減少しました。また、前年同期と比較すると、報告数で 12%増加し、調整件数は 0.3%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］



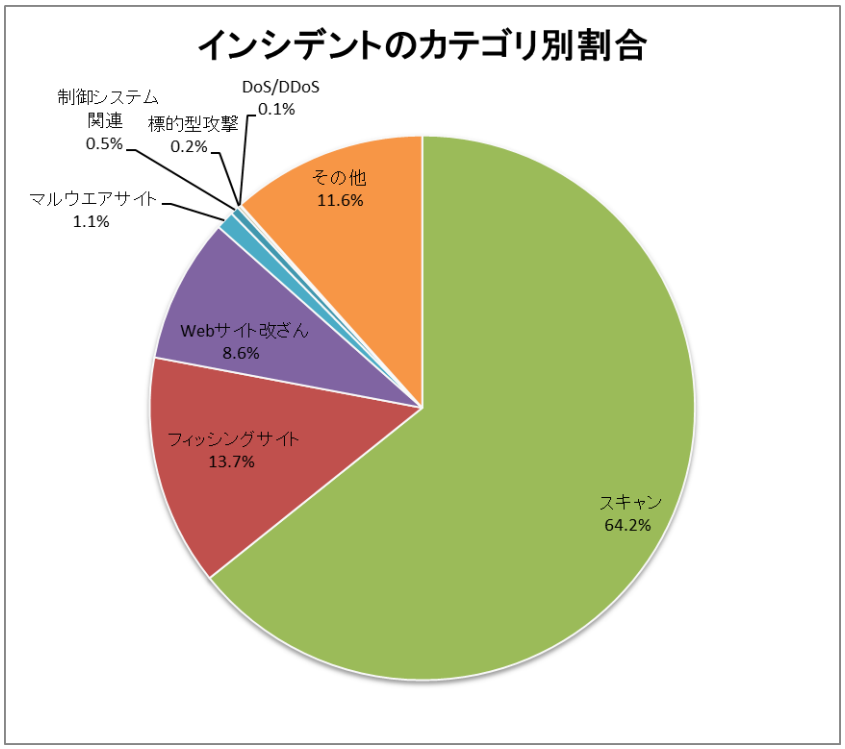
［図 2 インシデント調整件数の推移］

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。本四半期に報告を受けた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］

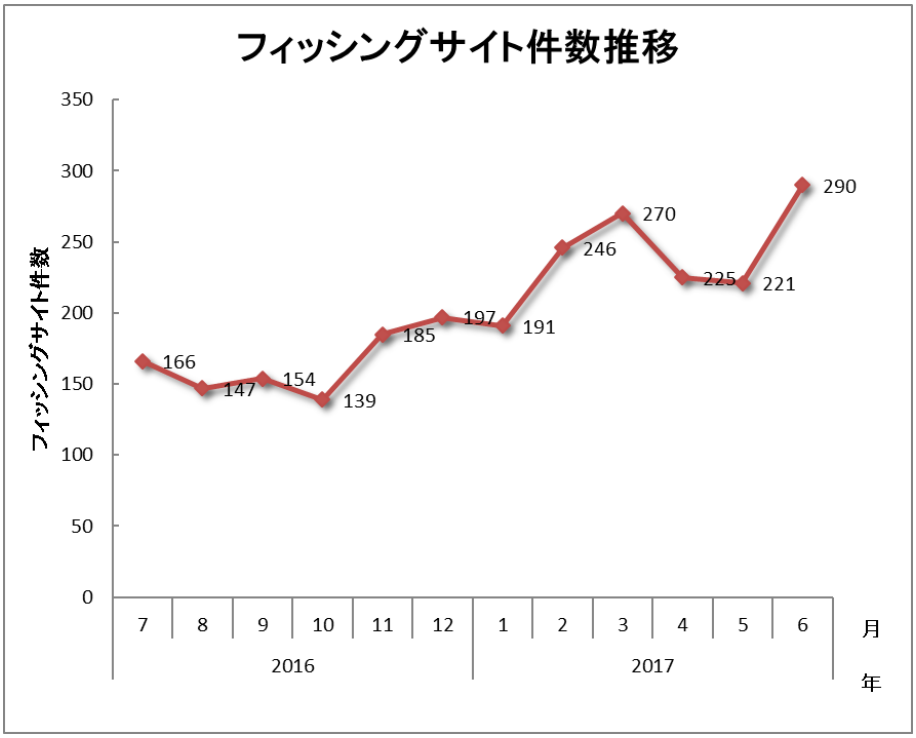
インシデント	4 月	5 月	6 月	合計	前四半期合計
フィッシングサイト	225	221	290	736	707
Web サイト改ざん	138	155	168	461	967
マルウエアサイト	24	15	20	59	91
スキャン	751	812	1884	3447	2391
DoS/DDoS	1	1	1	3	75
制御システム関連	25	2	0	27	4
標的型攻撃	6	1	2	9	11
その他	206	181	236	623	610

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 64.2%、フィッシングサイトに分類されるインシデントが 13.7%を占めています。

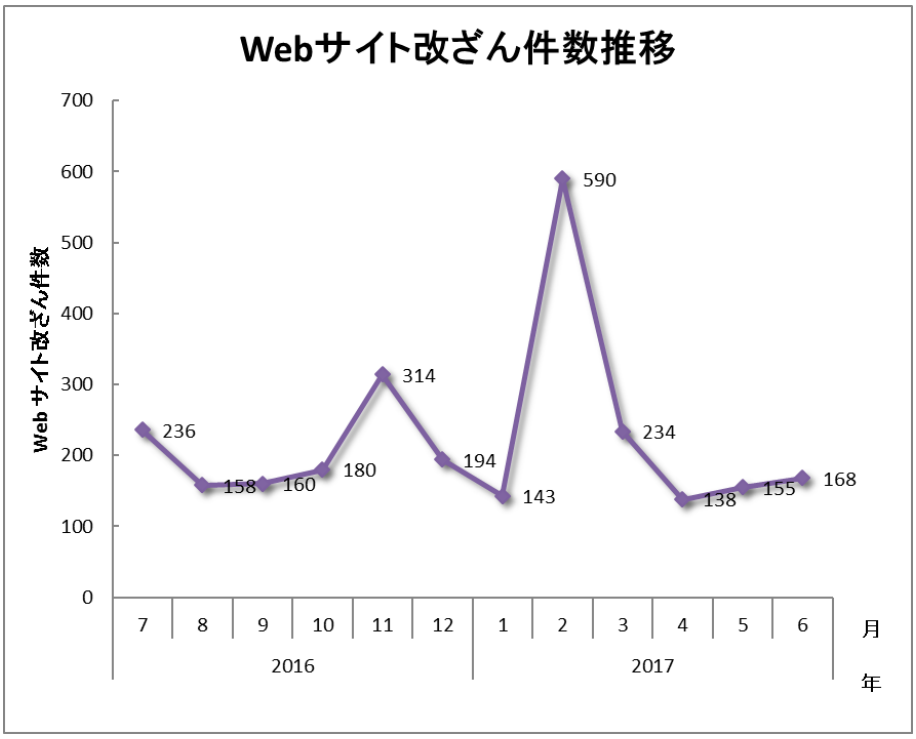


［図 3 インシデントのカテゴリ別割合］

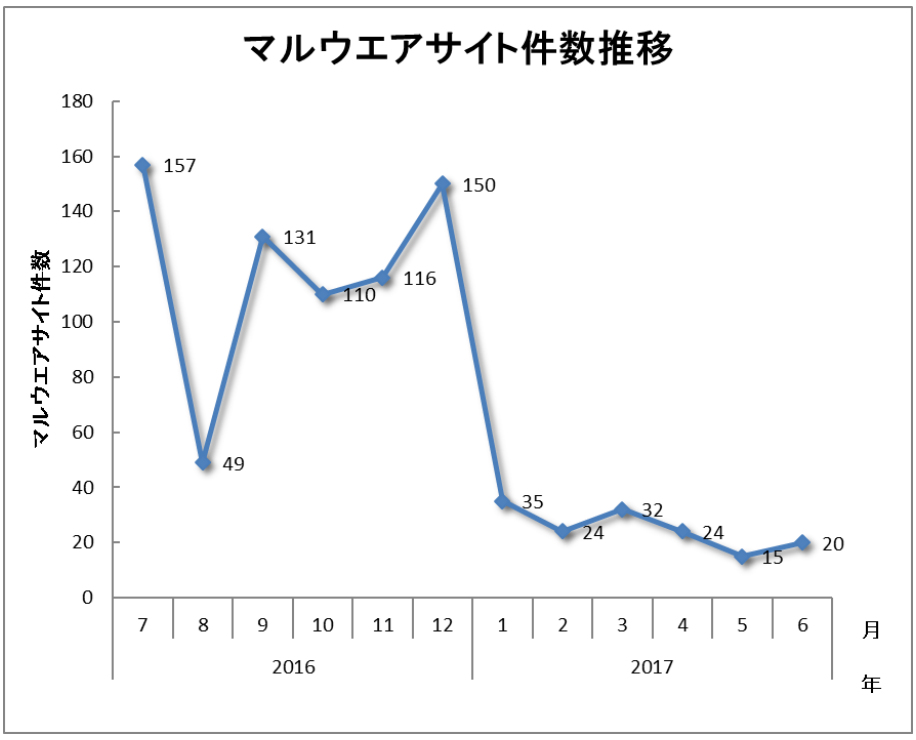
［図 4］から［図 7］に、フィッシングサイト、Web サイト改ざん、マルウエアサイト、スキャンのインシデントの過去 1 年間の月別推移を示します。



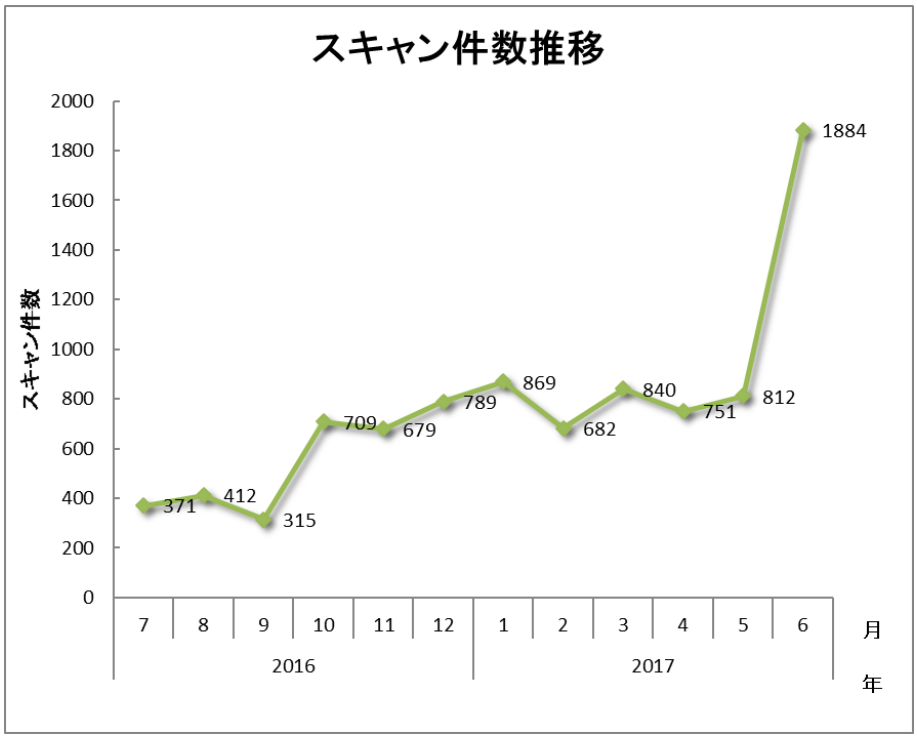
［図 4 フィッシングサイト件数の推移］



［図 5 Web サイト改ざん件数の推移］

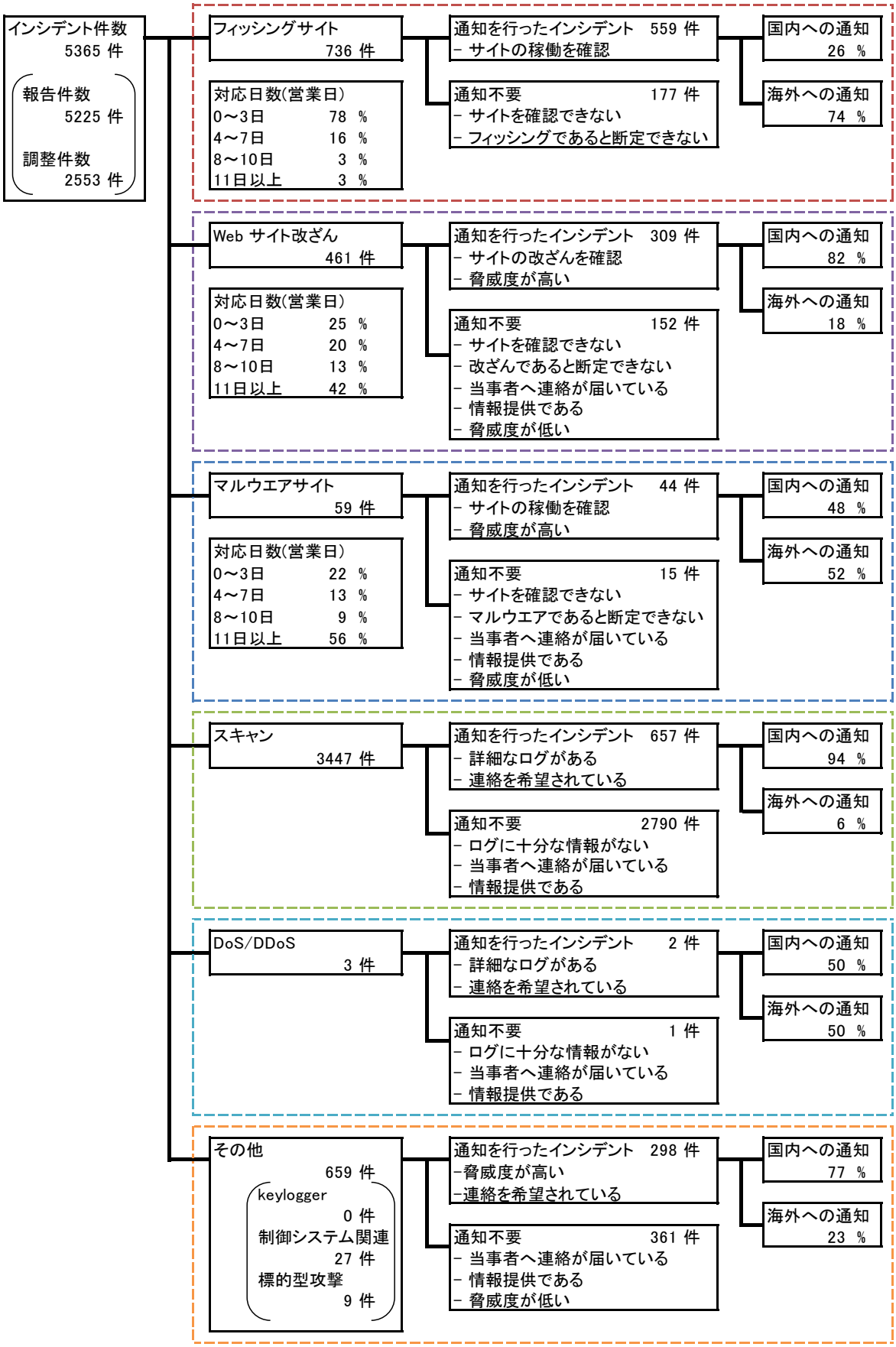


［図 6 マルウエアサイト件数の推移］



［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。



［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

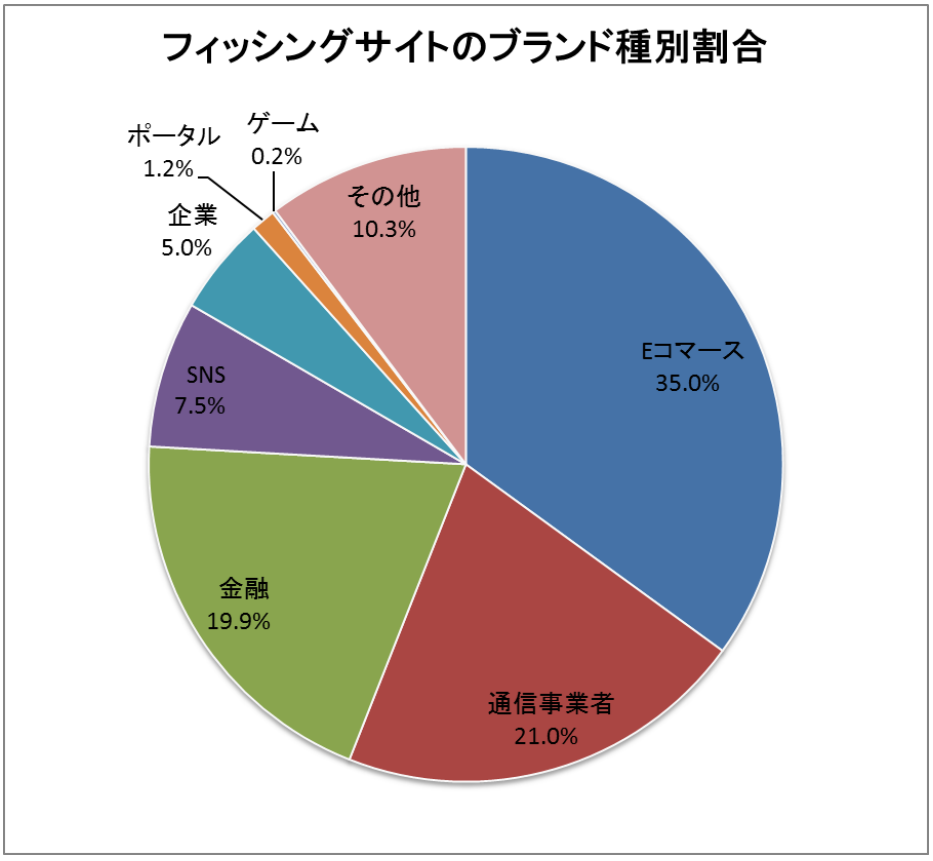
3.1. フィッシングサイトの傾向

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 736 件で、前四半期の 707 件から 4%増加しました。また、前年度同期（642 件）との比較では、15%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	52	69	88	209(28%)
国外ブランド	143	115	176	434(59%)
ブランド不明 (注 5)	30	37	26	93(13%)
全ブランド合計	225	221	290	736(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 209 件となり、前四半期の 183 件から 14%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 586 件となり、前四半期の 424 件から 38%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 35.0%、通信事業者のサイトを装ったものが 21.0%、金融機関のサイトを装ったものが 19.9%でした。

本四半期の国内ブランドのフィッシングサイトのうち、国内通信事業者または SNS のフィッシングサイトが 8 割以上を占めました。国内金融機関を装ったフィッシングサイトでは、クレジットカード番号の ID 登録サイトを装ったフィッシングサイトのみが確認され、その他の国内インターネットバンキングなどを装ったものはありませんでした。

国内通信事業者の Web メールのログイン画面を装ったサイトの多くは、侵入されたと見られる海外の Web サイトに設置されていました。特定のブランドを装ったフィッシングでは、Web フォームを作成する正規のサービスを使用して立ち上げられたフィッシングサイトに、短縮 URL から誘導するといった手法が共通して使用されていました。

SNS を装ったフィッシングサイトのほとんどは.cn ドメインを使用しており、ドメイン名は 4 月から 5 月初めにかけてはランダムな英字 5～6 文字、5 月半ば以降は被害ブランド名の後ろに英字 2～4 文字がついたドメイン名が使用されていました。また、多くのサイトで、香港の IP アドレスが使用されていました。

フィッシングサイトの調整先の割合は、国内が 26%、国外が 74%であり、前四半期（国内 27%、国外 73%）に比べ、国外への調整の割合が増加しています。

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、461 件でした。前四半期の 967 件から 52%減少しています。

前四半期に引き続き、初回アクセス時にのみページ末尾に不正なスクリプトが埋め込まれる改ざんが観測されました。改ざんされたサイトに埋め込まれるスクリプトとして、フォントのアップデートのポップアップを表示するものや、Adobe Flash Player の脆弱性を使用した攻撃を行うサイトに誘導するものを確認しており、いずれも最終的にランサムウエアがダウンロードされる仕組みになっていました。

初回アクセス時にのみ不正なスクリプトが埋め込まれる改ざんは、CMS を使用した Web サイトで多く確認されています。また、6 月初めごろから、WordPress 用プラグイン WP Job Manager の脆弱性によって画像ファイルを不正に設置されたとみられる国内サイトが多く確認されました。CMS およびそのプ

ラグインの脆弱性は、改ざんなどの攻撃に悪用される可能性があるため、常に最新のバージョンのものを使用し、不要であれば削除するといった対策を行っておくことが重要です。

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 11 件から 18%減少しています。本四半期は、対応を依頼した組織は 2 件でした。

本四半期には、Daserf とよばれる HTTP ボットや wali とよばれるダウンローダなどを使用した標的型攻撃に関する報告が複数寄せられました。同種の標的型攻撃に関する報告は、昨年の 8 月ごろから寄せられています。

攻撃に使用されるマルウエアの感染経路の一つとして、資産管理ソフトの脆弱性が悪用されていることを確認しています。攻撃者はこの脆弱性を悪用した攻撃を、昨年の 6 月ごろから継続して行っている可能性があります。グローバル IP アドレスが割り当てられている PC 上で、脆弱性をもつバージョンの資産管理ソフトが攻撃パケットを受信すると、当該 PC がダウンローダに感染し、その後ダウンローダによって、HTTP ボットをダウンロードして実行します。

HTTP ボットは、攻撃者の C&C サーバから命令を受信し、PC から収集した情報を送信します。HTTP ボットの通信相手である C&C サーバに、国内の侵入された Web サーバが悪用されている例を多く確認しています。HTTP ボットは、感染 PC から収集した情報を C&C サーバに送信する際に、暗号化してはいますが HTTP リクエストのパラメータに埋め込むため、HTTP リクエストから暗号化された情報を取り出して復号することで、攻撃者が情報収集のために PC 上で行った操作などを確認できることがあります。

その他に、標的型攻撃と見られる、マルウエアが添付されたメールに関する報告が複数寄せられました。4 月後半に報告された標的型攻撃メールには、2017 年 4 月のアップデートで修正された Microsoft 製品の脆弱性（CVE-2017-0199）を悪用した攻撃を行うファイルが添付されていました。また、ダミーの文書ファイルとショートカットファイルが添付されており、ショートカットファイルを実行すると、最終的にボットの機能を持つマルウエアが実行され、PowerShell スクリプトによって追加のマルウエアがダウンロード、実行される攻撃手法も確認されています。この手法は、以前に見られた Asruex や ChChes といった HTTP ボットに感染させる標的型攻撃メールと類似しています。

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、59 件でした。前四半期の 91 件から 35%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、3447 件でした。前四半期の 2391 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。

［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	340	288	1471	2099
25/tcp	198	302	232	732
53/udp	104	35	82	221
80/tcp	34	53	24	111
23/tcp	19	28	10	57
1433/tcp	4	25	3	32
445/tcp	3	23	5	31
21/tcp	5	11	14	30
143/tcp	2	25	0	27
81/tcp	18	3	1	22
110/tcp	4	8	3	15
2222/tcp	3	8	0	11
3389/tcp	2	4	4	10
2323/tcp	4	1	1	6
5060/udp	1	0	3	4
9000/tcp	0	0	3	3
51331/udp	0	1	2	3
4752/udp	2	0	1	3
33442/udp	2	0	1	3
その他	144	294	435	873
月別合計	889	1109	2295	4293

頻繁にスキャンの対象となったポートは、SSH（22/TCP）、SMTP（25/TCP）、DNS（53/UDP）でした。6 月半ばごろから、国内 IP アドレスが攻撃元となっている、SSH を対象としたスキャンの報告が増加しています。スキャンが増加した原因として、ネットワーク機器の脆弱性を悪用した攻撃が行われており、マルウエアに感染した機器が増加しているなどの可能性が考えられるため、JPCERT/CC は攻撃元となっているホストに関する情報を収集しています。

その他に分類されるインシデントの件数は、623 件でした。前四半期の 610 件から 2%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。

【IIS 6.0 WebDAV サービスの脆弱性の影響を受ける国内サイトに関する対応】
4 月初めごろ、海外のセキュリティ研究者から、Microsoft IIS 6.0 の WebDAV の脆弱性（CVE-2017-7269）が内在する国内 Web サイトのリストを受け取りました。CVE-2017-7269 は、すでにサポート期間が終了している Windows Server 2003 R2 の、IIS 6.0 の WebDAV サービスにおける脆弱性で、2017 年 3 月 27 日に公表されました。脆弱なサーバでは、細工したリクエストを受信すると、任意のコードが実行される可能性があります。

JPCERT/CC は、提供されたリストをもとに特定されたサイト管理者に、サーバ上で WebDAV サービスが稼働しているか確認を依頼したところ、複数から、サーバの WebDAV を無効にするなどの対応を行った旨の返信を受け取りました。

【金融系マルウエアに感染させることを目的とした日本語メールに関する対応】
本四半期は、マルウエアに感染させることが目的と見られる、実行ファイルや文書ファイルを含む ZIP ファイルが添付された日本語のメールが送付されるケースを多数確認しています。6 月には、4 月に修正された Microsoft 製品の脆弱性（CVE-2017-0199）を使用した攻撃を行う文書ファイルが添付されたケースも確認されています。添付されたファイルを開くと、最終的に Ursnif や DreamBot とよばれる、インターネットバンキングの情報を窃取するマルウエアがダウンロード、実行されます。マルウエアは、匿名通信技術である Tor で通信を行うためのモジュールをダウンロードし、Tor ネットワーク上にある C&C サーバと通信して、設定やコマンドの取得を行います。

Ursnif の実行ファイルが設置された国内 Web サイトが複数確認されており、JPCERT/CC はサーバを管理する事業者に、サーバの悪用について事実関係を確認するよう依頼しました。また、マルウエア添付メールの送信元として、国内 IP アドレスが使用されている事例を複数確認しており、メール送信元の IP アドレスを管理する通信事業者に対応を依頼しました。

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 29 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。