JPCERT CC®

Japan Computer Emergency Response Team Coordination Center

JPCERT-IR-2017-01

発行日: 2017-04-13

JPCERT/CC インシデント報告対応レポート
［2017 年 1 月 1 日 ～ 2017 年 3 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、2017 年 1 月 1 日から 2017 年 3 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］

	1 月	2 月	3 月	合計	前四半期合計
報告件数 (注 2)	1360	1253	1482	4095	4036
インシデント件数 (注 3)	1405	1848	1603	4856	4122
調整件数 (注 4)	800	1307	970	3077	2883

（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。

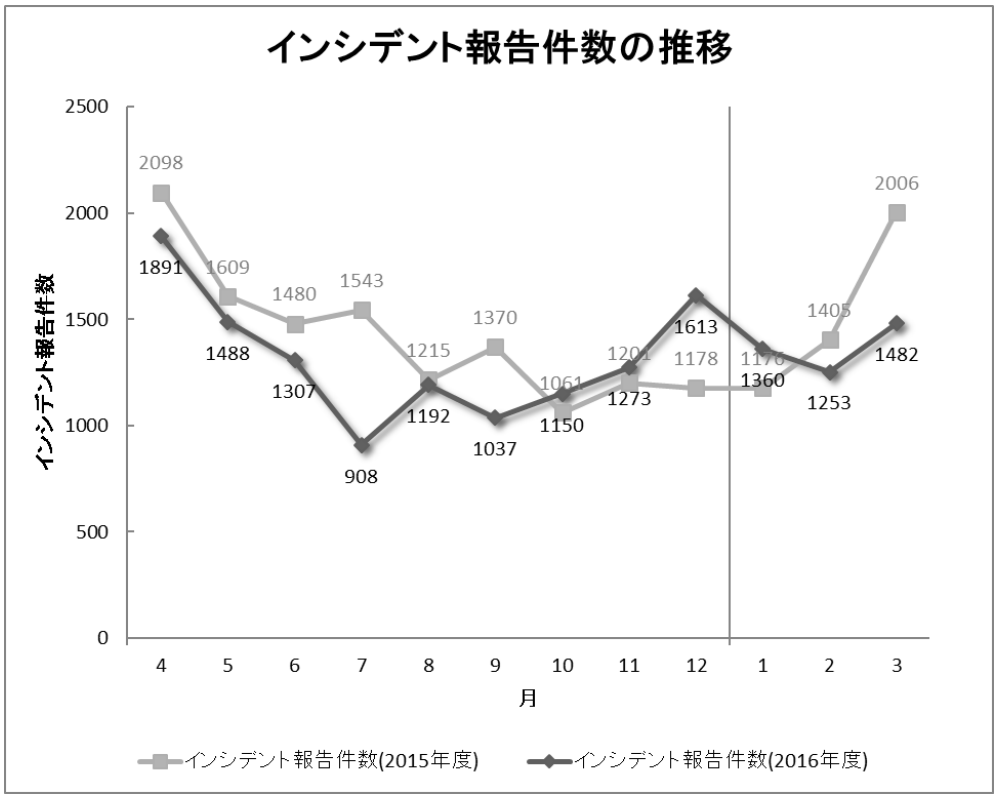
（注 3）「インシデント件数」は、各報告に含まれるインシデント件数の合計を示します。1 つのイン

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。

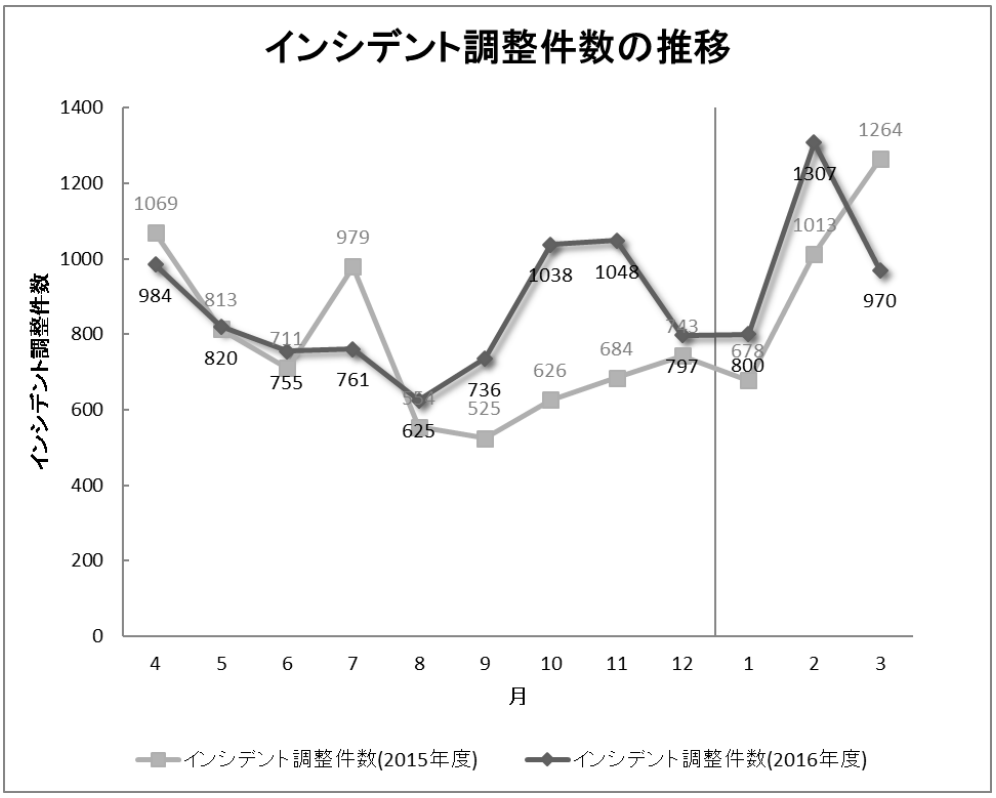
（注 4）「調整件数」は、インシデントの拡大防止のため、サイトの管理者等に対し、現状の調査と問題解決のための対応を依頼した件数を示します。

本四半期に寄せられた報告件数は、4095 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 3077 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 7%増加しました。また、前年同期と比較すると、報告数で 11%減少し、調整件数は 4%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］

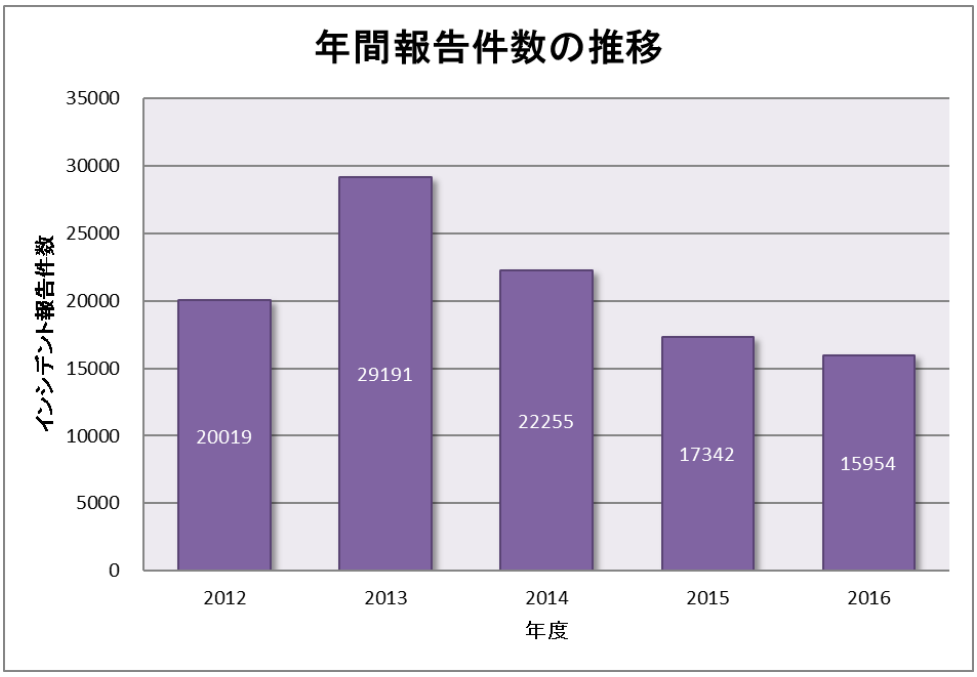
【参考】統計情報の年度比較

2016 年度を含む過去 5 年間の年度ごとの報告件数を［表 2］に示します。なお、各年度は 4 月 1 日から翌年の 3 月 31 日までとしています。

［表 2: 年間報告件数の推移］

年度	2012	2013	2014	2015	2016
報告件数	20019	29191	22255	17342	15954

2016 年度に寄せられた報告件数は 15954 件でした。前年度の 17342 件と比較して、8%減少しています。［図 3］に過去 5 年間の年間報告件数の推移を示します。



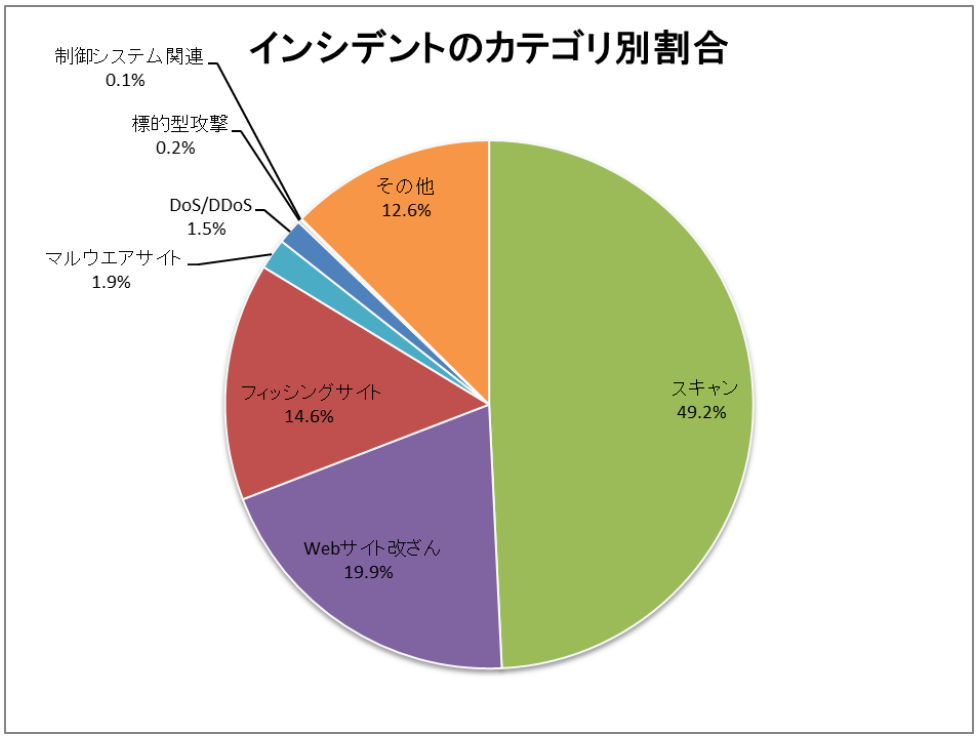
［図 3 年間報告件数の推移（年度比較）］

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 3］に示します。

［表 3 カテゴリ別インシデント件数］

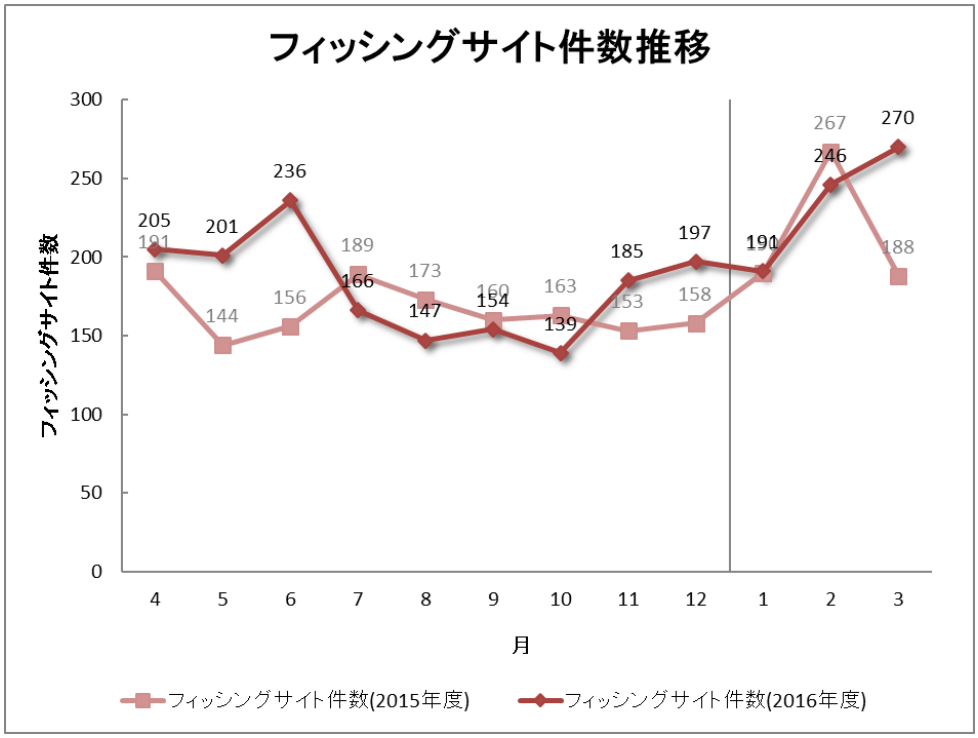
インシデント	1 月	2 月	3 月	合計	前四半期合計
フィッシングサイト	191	246	270	707	521
Web サイト改ざん	143	590	234	967	688
マルウエアサイト	35	24	32	91	376
スキャン	869	682	840	2391	2177
DoS/DDoS	16	58	1	75	61
制御システム関連	3	0	1	4	24
標的型攻撃	4	6	1	11	15
その他	144	242	224	610	260

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 4］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 49.2%、Web サイト改ざんに分類されるインシデントが 19.9%を占めています。また、フィッシングサイトに分類されるインシデントは 14.6%でした。

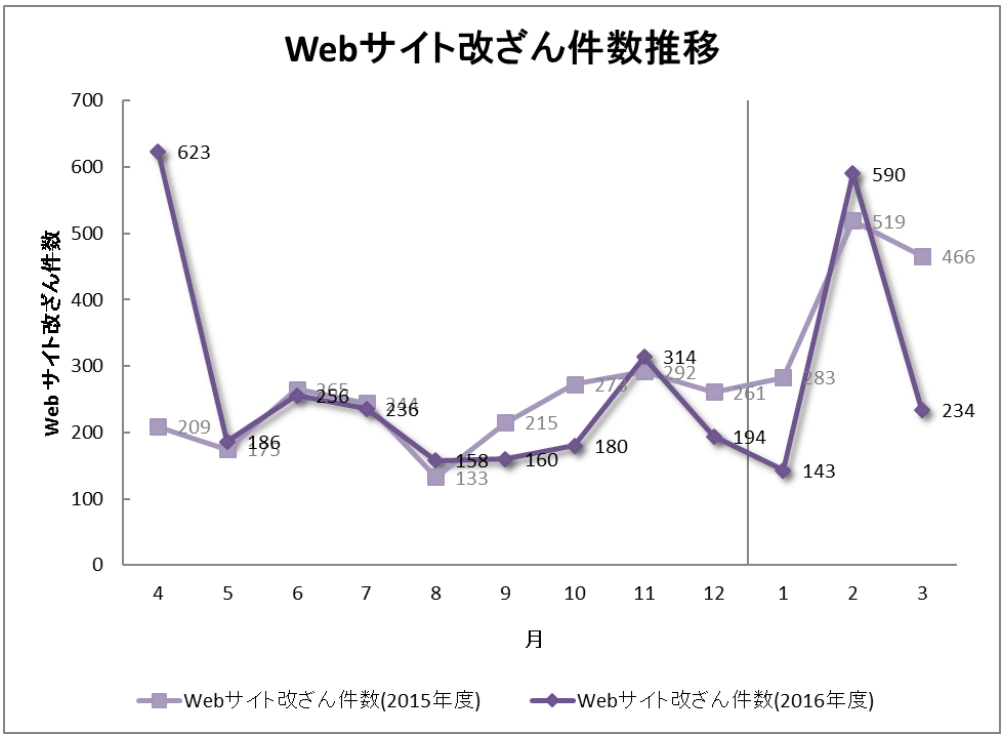


［図 4 インシデントのカテゴリ別割合］

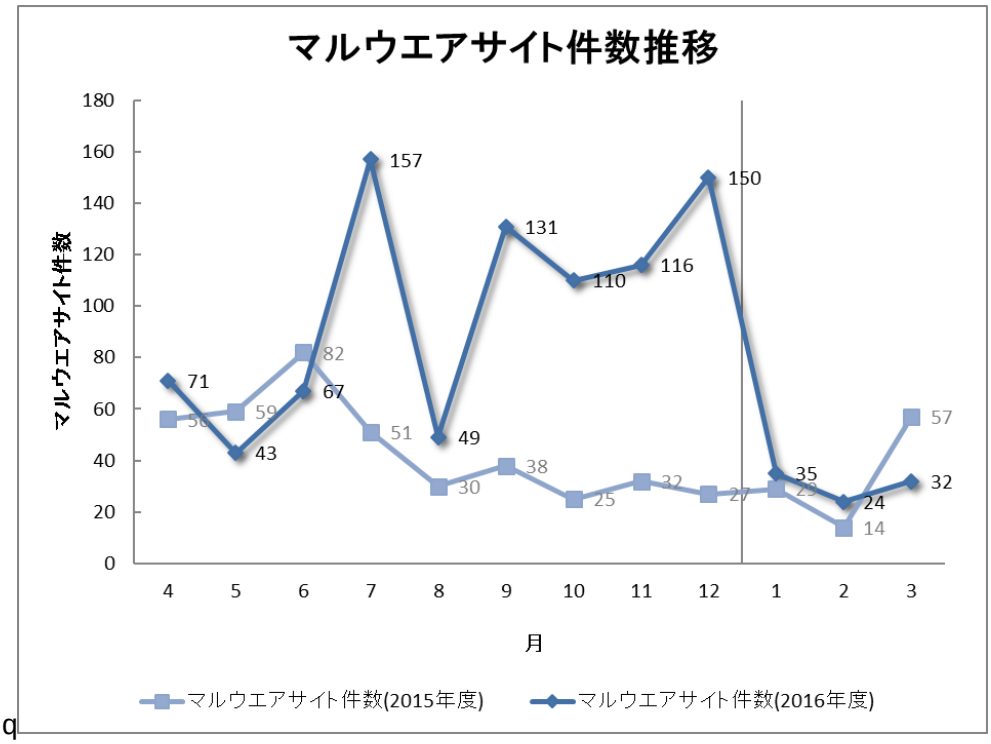
［図 5］から［図 8］に、フィッシングサイト、Web サイト改ざん、マルウエアサイト、スキャンのインシデントの過去 1 年間の月別推移を示します。



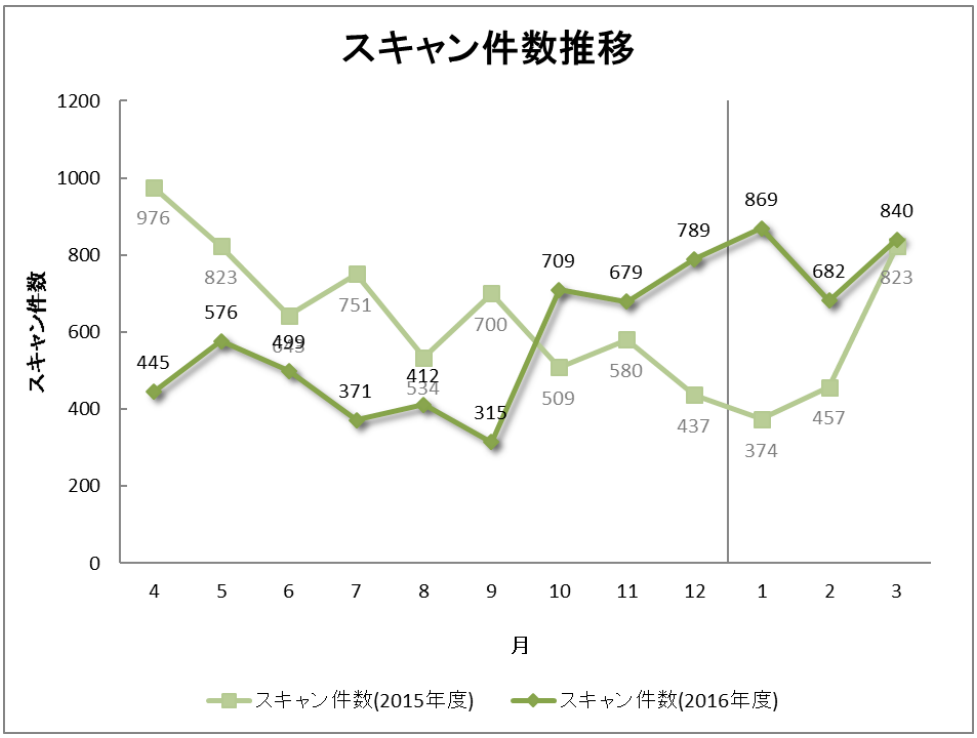
［図 5 フィッシングサイト件数の推移］



［図 6 Web サイト改ざん件数の推移］

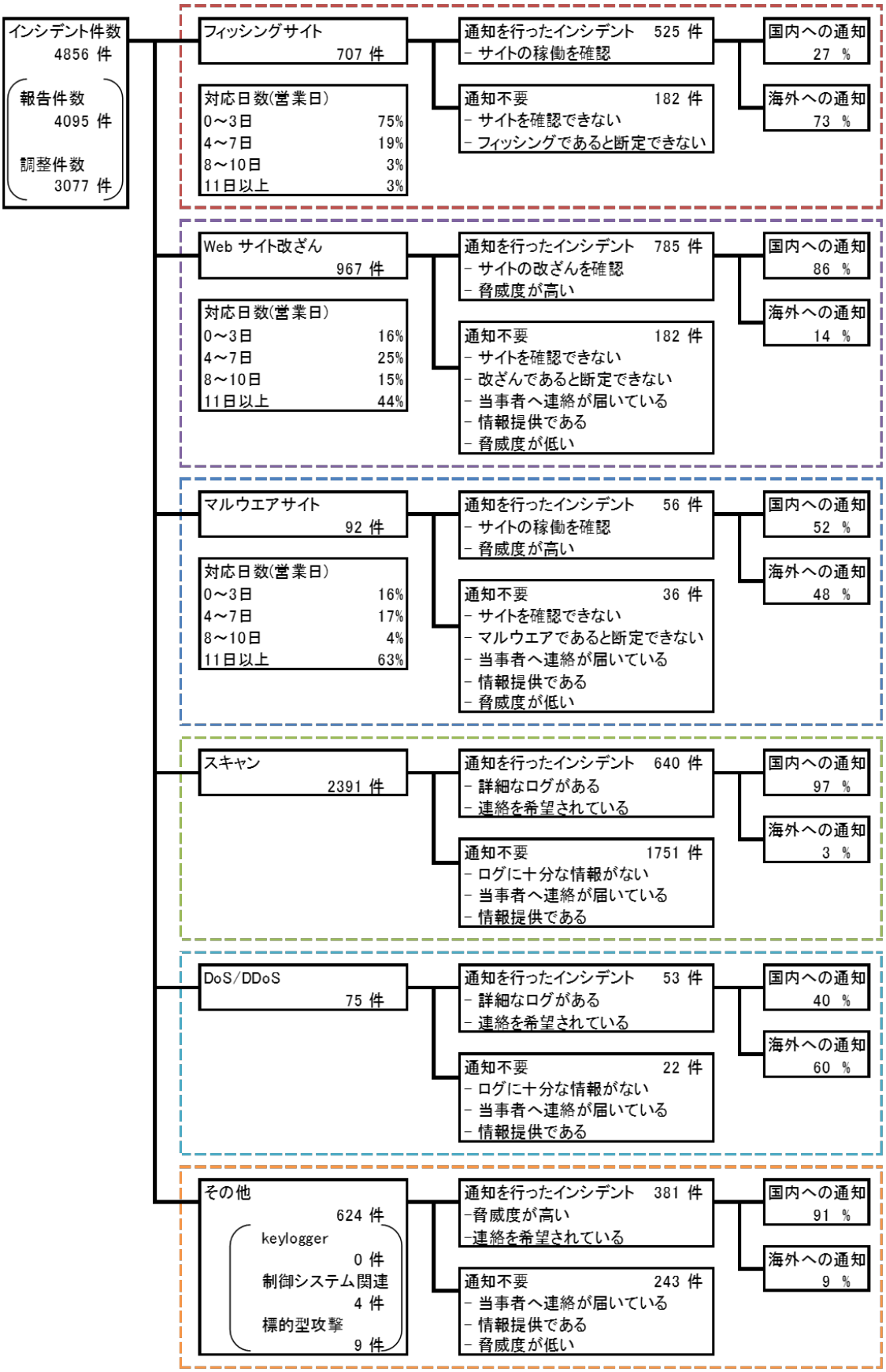


［図 7 マルウエアサイト件数の推移］



［図 8 スキャン件数の推移］

［図 9］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 9 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

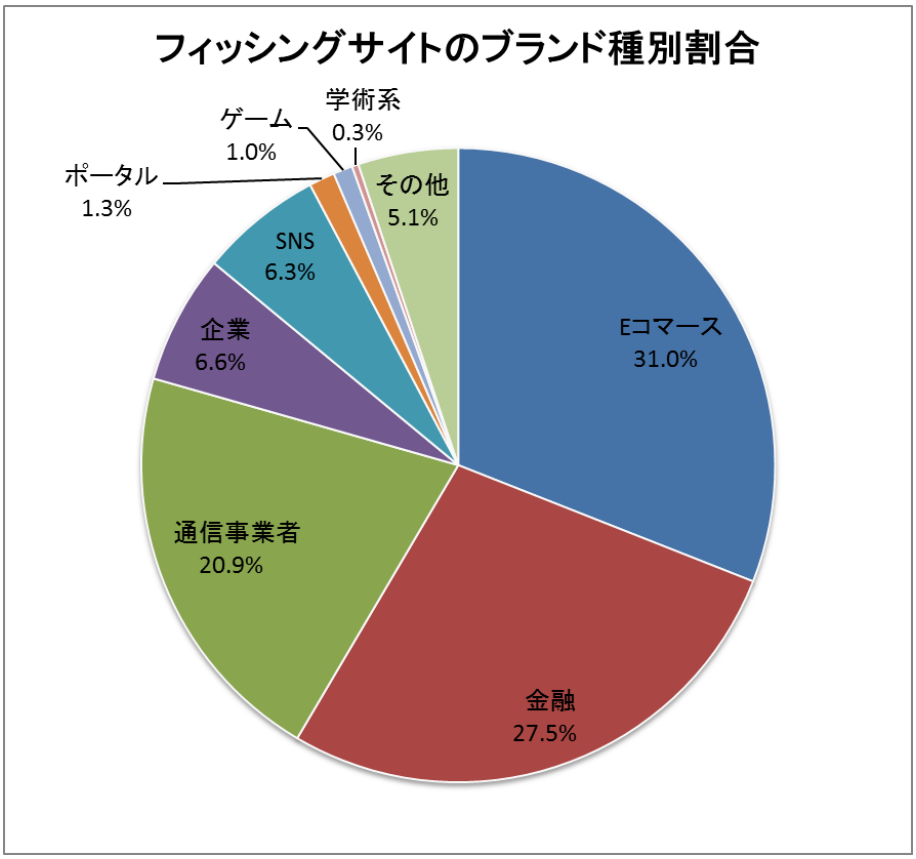
3.1. フィッシングサイトの傾向

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 707 件で、前四半期の 521 件から 36%増加しました。また、前年度同期（645 件）との比較では、10%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 4］、業界別の内訳を［図 10］に示します。

［表 4 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	1 月	2 月	3 月	本四半期合計（割合）
国内ブランド	56	42	85	183(26%)
国外ブランド	111	161	152	424(64%)
ブランド不明 (注 5)	24	43	33	100(14%)
全ブランド合計	191	246	270	707(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 10 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 183 件となり、前四半期の 134 件から 37%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 424 件となり、前四半期の 279 件から 52%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 31.0%、金融機関のサイトを装ったものが 27.5%、通信事業者のサイトを装ったものが 20.9%でした。

国内ブランドのフィッシングサイトでは、国内通信事業者の Web メールのログイン画面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。これらのフィッシングサイトの大半は、海外の IP アドレスで稼働しており、侵入されたとみられる海外の Web サイトや、海外のホスティングサービス上に作成されていました。特に、ロシアの特定のホスティングサービスが継続して使用されていました。

1 月以降、日本マイクロソフトを装ったフィッシングメールが継続して確認されています。フィッシングメールの内容は、オフィスソフトのプロダクトキーが不正にコピーされているため検証作業を行う必要があるとして、メール内のリンクから認証を行うよう誘導するものでした。リンクの誘導先は、Microsoft アカウントの情報を窃取するフィッシングサイトで、ホスト名には共通して support、security、microsoft などの文字列が含まれていました。

フィッシングサイトの調整先の割合は、国内が 27%、国外が 73%であり、前四半期（国内 38%、国外 62%）に比べ、国内での調整が増加しています。

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、967 件でした。前四半期の 688 件から 41%増加しています。

アクセスするとフォントのアップデートを促すポップアップが表示されるように改ざんされたとみられる Web サイトに関する報告が 1 月ごろから複数寄せられています。ポップアップ上のボタンを押すと EXE ファイルがダウンロードされ、EXE ファイルを実行するとランサムウエアに感染することを確認しています。ポップアップを表示する不正なスクリプトは、アクセス元のリファラ、ユーザエージェントが特定のものであり、且つアクセス元 IP アドレスからの初回のアクセス時にのみ、ページに埋め込まれるようになっていました。

2 月初めごろ、WordPress の REST API の脆弱性を悪用した攻撃が大規模に行われ、攻撃によって改ざんされたと見られる国内サイトが非常に多く確認されました。改ざんの内容は、海外のハッカーグループがページ上にメッセージを埋め込むものでした。

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、11 件でした。前四半期の 15 件から 27%減少しています。本四半期は、対応を依頼した組織はありませんでした。

2 月から 3 月にかけて、標的型攻撃と見られるなりすましメールに関する報告が複数寄せられています。確認したメールには、ZIP ファイルが添付されているか、ZIP ファイルをダウンロードするリンクが存在し、いずれの場合も ZIP ファイルには拡張子が.lnk のショートカットファイルが含まれていました。このショートカットファイルが開かれると、PowerShell コマンドで追加のファイルがダウンロード、実行される仕組みになっていました。ダウンロードされるファイルは攻撃によって異なり、PowerShell スクリプトや EXE ファイルなどが見られました。

PowerShell スクリプトがダウンロードされる事例では、.lnk ファイルを実行すると、最初に短縮 URL へのアクセスが行われ、リダイレクト先から画像ファイルに偽装した PowerShell スクリプトがダウンロードされるようになっていました。ダウンロードされた PowerShell スクリプトを実行すると、ダミーの文書が表示される裏でマルウエアが実行され、ChChes と呼ばれる、HTTP で C&C サーバと通信を行うマルウエア（HTTP ボット）に感染することを確認しました。同様の攻撃に関与した複数の C&C サーバが確認されており、さまざまなドメイン名が使われていましたが、それらのドメインの登録情報には類似性が見られました。

ショートカットファイルが添付される標的型攻撃メールは、以前から継続して確認されていますが、ショートカットファイルを実行することでダウンロードされるファイルや感染するマルウエアの種類は、時期によって違いが見られます。2015 年 11 月から 2016 年 6 月にかけて確認された標的型攻撃メールでは、添付ファイルに含まれる.lnk ファイルを実行すると、マルウエア（ダウンローダ）に感染し、このマルウエアが画像に見せかけたファイルをダウンロードした後にデコードし実行することで、Asruex と呼ばれる HTTP ボットに感染させる仕組みになっていました。

マルウエア ChChes と PowerShell を悪用して感染を広げる事例の詳細については、下記をご参照ください。

Cookie ヘッダーを用いて C&C サーバとやりとりするマルウエア ChChes(2017-01-26)
https://www.jpcert.or.jp/magazine/acreport-ChChes.html

PowerSploit を悪用して感染するマルウエア(2017-02-10)
https://www.jpcert.or.jp/magazine/acreport-ChChes_ps1.html

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、91 件でした。前四半期の 376 件から 76%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、2391 件でした。前四半期の 2177 件から 10%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 5］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）、DNS（53/UDP）でした。

［表 5 ポート別のスキャン件数］

ポート	1 月	2 月	3 月	合計
22/tcp	469	272	520	1261
25/tcp	147	110	127	384
53/udp	53	124	85	262
80/tcp	69	58	43	170
23/tcp	58	34	17	109
2323/tcp	16	9	4	29
2222/tcp	11	6	4	21
5358/tcp	13	6	1	20
21/tcp	5	1	9	15
3389/tcp	9	4	1	14
7547/tcp	7	4	1	12
23231/tcp	7	1	0	8
5555/tcp	6	0	0	6
53413/udp	1	5	0	6
4752/udp	2	2	2	6
23887/udp	4	1	1	6
123/udp	6	0	0	6
51331/udp	3	1	1	5
33442/udp	4	1	0	5
443/tcp	1	3	0	4
5432/tcp	1	1	1	3
1433/tcp	1	2	0	3
その他	199	165	159	523
月別合計	1092	810	976	2878

その他に分類されるインシデントの件数は、610 件でした。前四半期の 260 件から 135%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。

【Apache Struts 2 の脆弱性を使用した攻撃】
2017 年 3 月に Apache Struts 2 の脆弱性(S2-045、CVE-2017-5638)が公開され、当該脆弱性を悪用したと見られる攻撃に関する報告が、複数寄せられました。攻撃の実証コードは脆弱性公開の翌日には公開されており、被害組織からの報告によると、実証コード公開の同日には攻撃と見られるアクセスが発生していた可能性があります。すなわち、脆弱性情報が公開された直後に対策を行わなければ、攻撃を防げなかったと考えられる状況でした。

この攻撃によって、サーバアプリケーションを実行しているユーザの権限で、任意のコマンドを実行される可能性があり、実際に、攻撃によって、ファイルの設置や削除といった被害が発生した事例を確認しています。複数の報告元から提供されたログから攻撃者が実行を試みたコマンドを調査したところ、ユーザ名やサーバ OS のバージョンなどの情報収集を行うコマンドやバックドアとみられる jsp ファイルを外部からダウンロードするコマンド、仮想通貨のマイニングを行うツールのダウンロードおよび実行を行うコマンドなどが確認されました

国内 ISP が管理する動的な IP アドレスが攻撃元であったと報告されていますが、これらは攻撃の踏み台として使用されたホストである可能性があります。

【ボットネットの C&C サーバと通信している国内 IP アドレスに関する対応】
金融系のマルウエアや情報を窃取するマルウエアといったさまざまなボットネットが使用していた Avalanche と呼ばれる大規模な通信基盤が、2016 年 12 月にヨーロッパの法執行機関によって停止されました。Avalanche に属していた C&C サーバが使用していたドメインは、現在は無害化されており、マルウエアに感染した PC からの通信を確認するシンクホールとして運用されています。

シンクホールへ通信を行っている国内 IP アドレスのリストを JPCERT/CC はドイツの National CSIRT である CERT-Bund から継続して受け取っています。Avalanche は金融系トロイや情報窃取系のマルウエアの通信先として使用されており、リストによると、シンクホールに通信しているホストのおよそ半数は Rovnix と呼ばれるマルウエアに感染していることが分かりました。Rovnix は国内インターネットバンキングのアカウント情報を狙ったマルウエアで、2016 年 3 月前後に確認された日本郵政を装ったメールにも、添付ファイルとして同じマルウエアが使われていました。JPCERT/CC は、IP アドレスを管理する通信事業者への連絡や、国内の関連組織へのリストの共有を行っています。

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 28 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。