JPCERT-IR-2017-04
発行日: 2017-10-12

JPCERT/CC インシデント報告対応レポート
［2017 年 7 月 1 日 ～ 2017 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、2017 年 7 月 1 日から 2017 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］

	7 月	8 月	9 月	合計	前四半期合計
報告件数 (注 2)	1,698	1,473	1,429	4,600	5,225
インシデント件数 (注 3)	1,771	1,587	1,453	4,811	5,365
調整件数 (注 4)	725	759	750	2,234	2,553

（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。

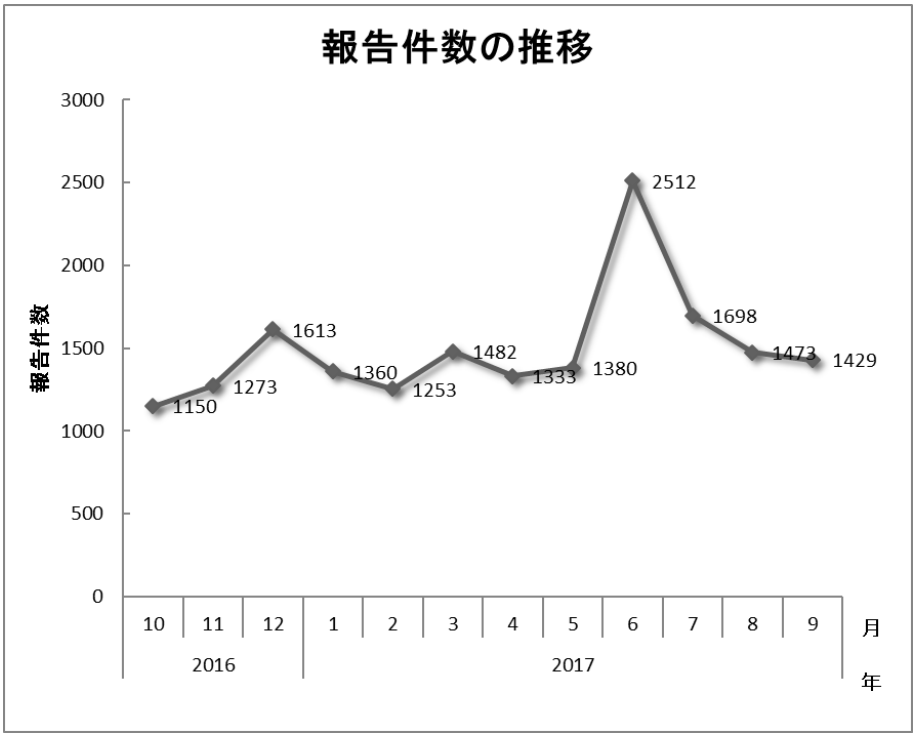
（注 3）「インシデント件数」は、各報告に含まれるインシデント件数の合計を示します。1 つのイン

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。

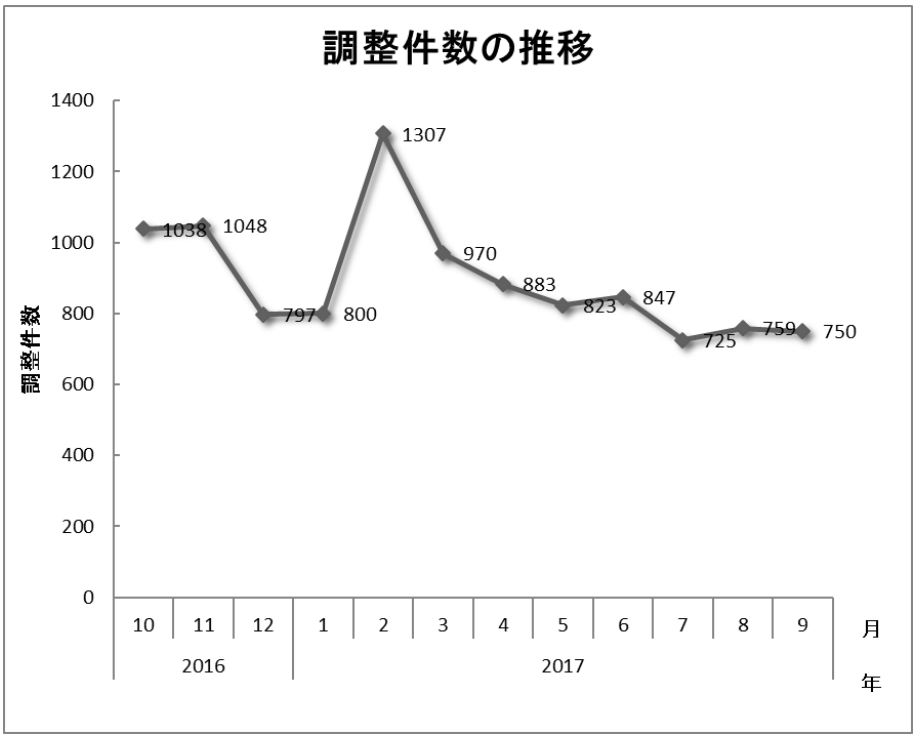
（注 4）「調整件数」は、インシデントの拡大防止のため、サイトの管理者等に対し、現状の調査と問題解決のための対応を依頼した件数を示します。

本四半期に寄せられた報告件数は、4,600 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 2,234 件でした。前四半期と比較して、報告件数は 12%減少し、調整件数は 12%減少しました。また、前年同期と比較すると、報告件数で 47%増加し、調整件数は 5%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］



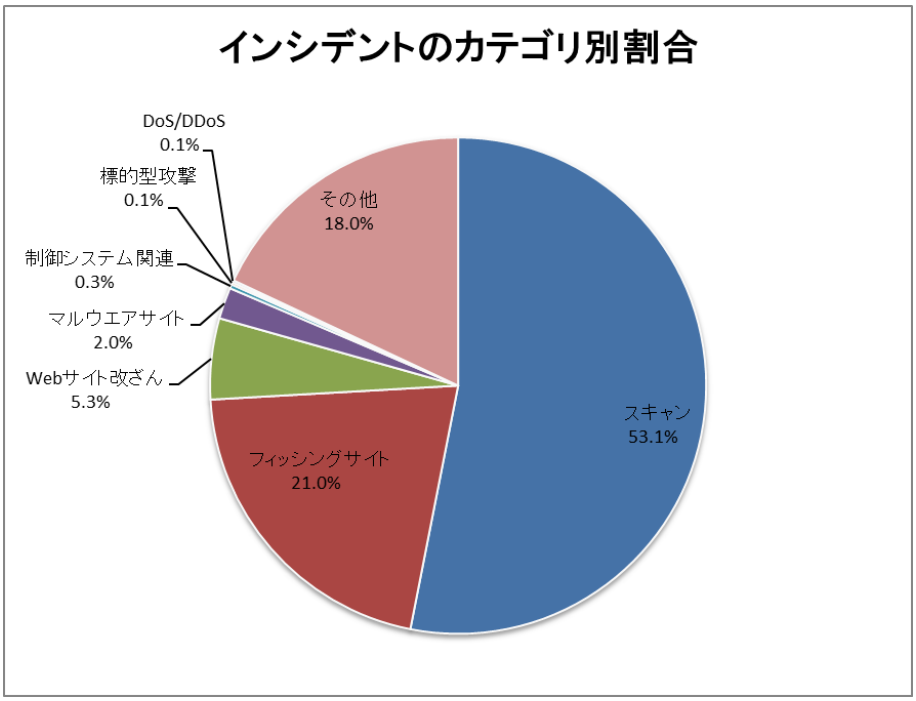
［図 2 インシデント調整件数の推移］

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］

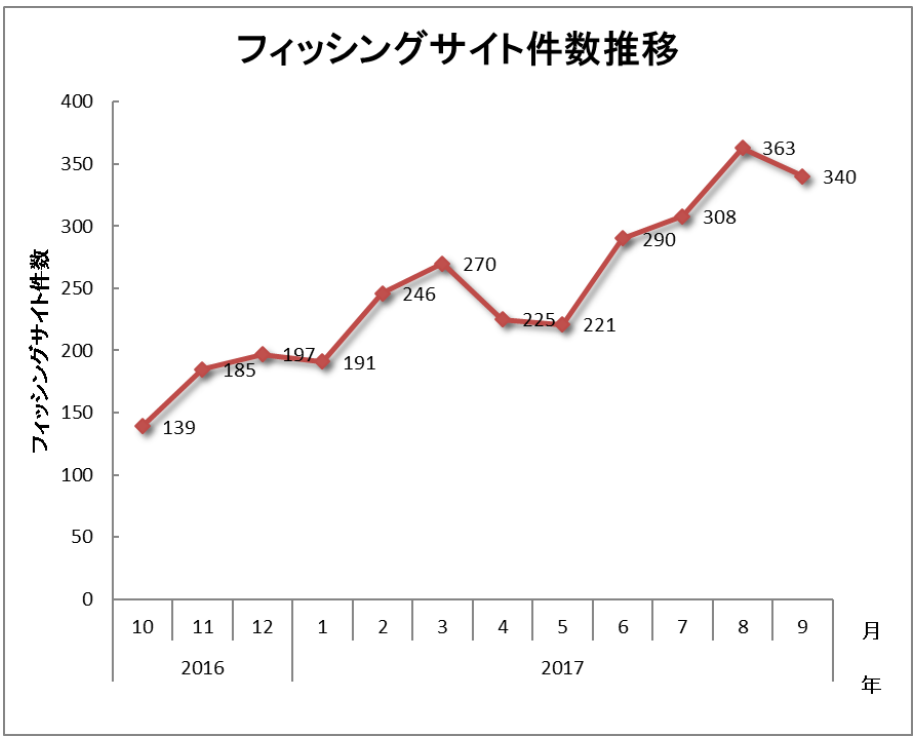
インシデント	7 月	8 月	9 月	合計	前四半期合計
フィッシングサイト	308	363	340	1,011	736
Web サイト改ざん	75	86	93	254	461
マルウエアサイト	25	42	31	98	59
スキャン	1,097	827	630	2,554	3,447
DoS/DDoS	1	0	6	7	3
制御システム関連	0	9	4	13	27
標的型攻撃	3	0	4	7	9
その他	262	260	345	867	623

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 53.1%、フィッシングサイトに分類されるインシデントが 21.0%を占めています。

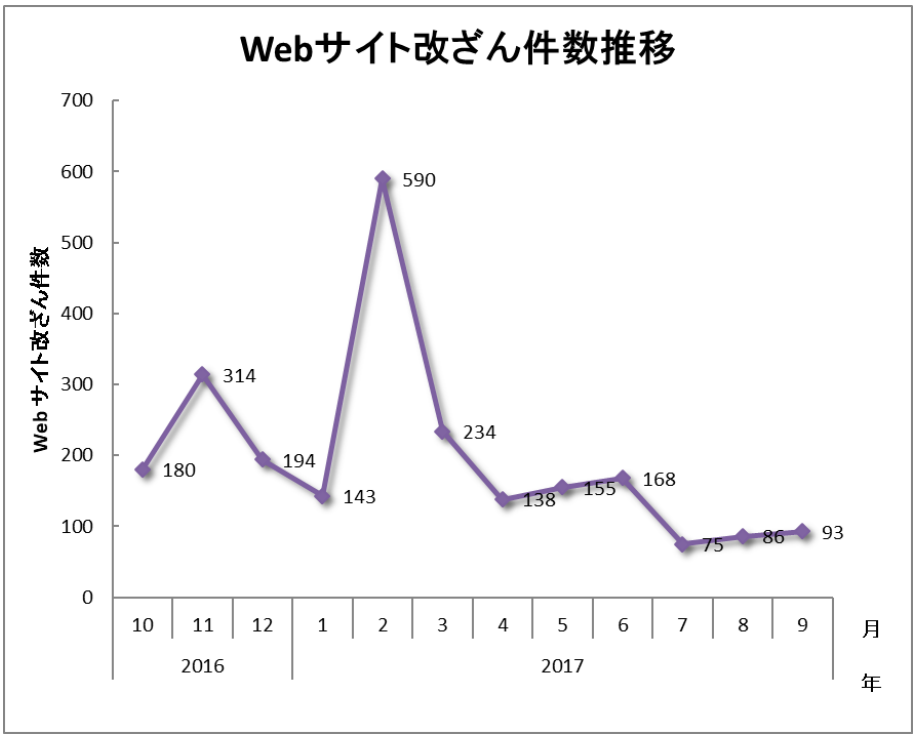


［図 3 インシデントのカテゴリ別割合］

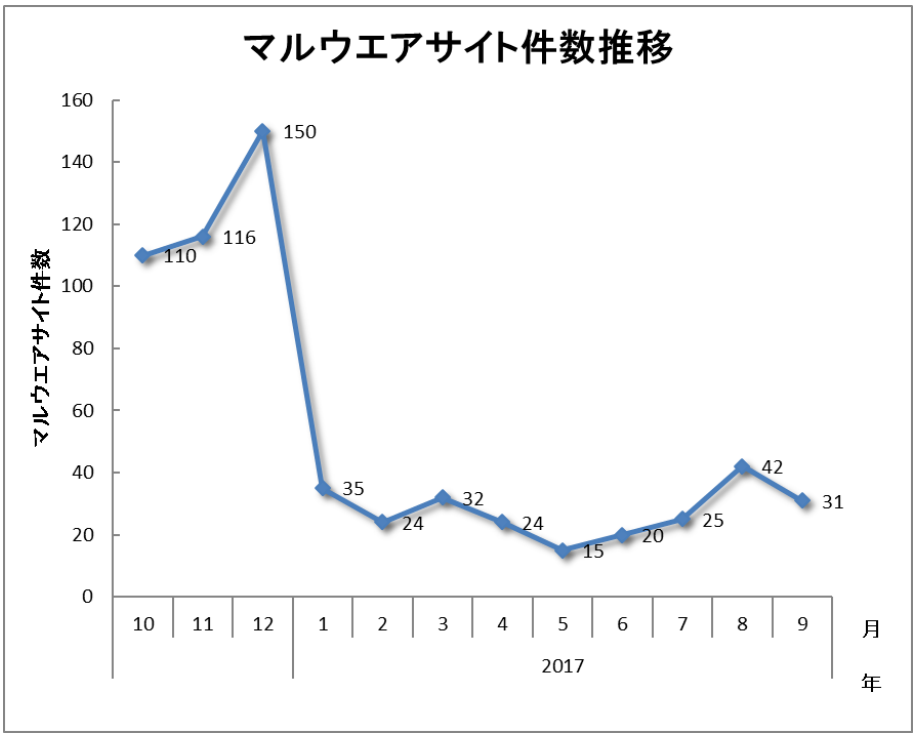
［図 4］から［図 7］に、フィッシングサイト、Web サイト改ざん、マルウエアサイト、スキャンのインシデントの過去 1 年間の月別推移を示します。



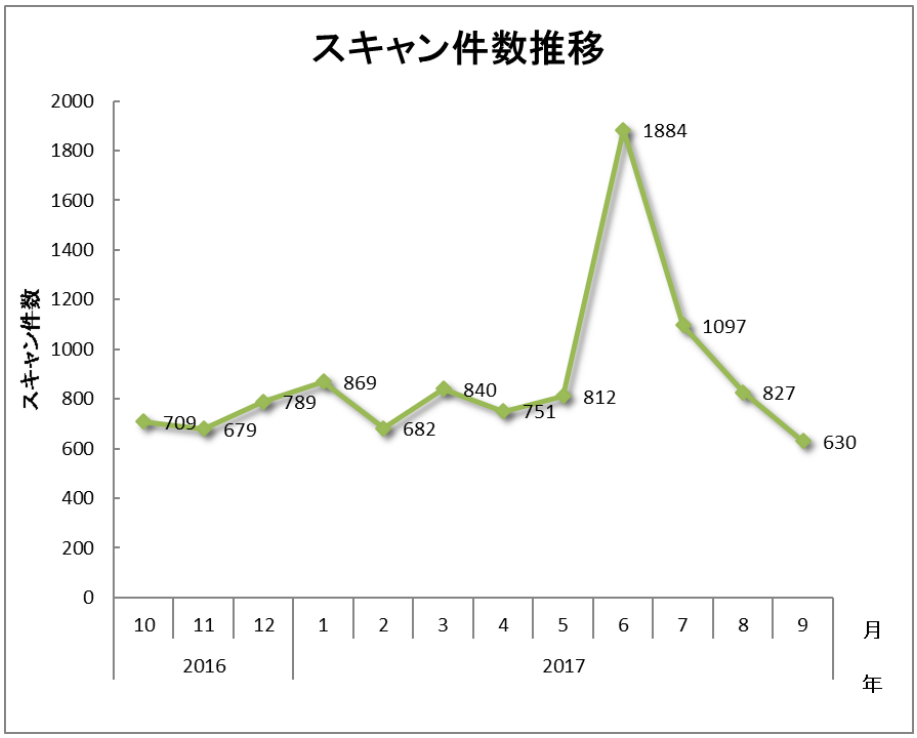
［図 4 フィッシングサイト件数の推移］



［図 5 Web サイト改ざん件数の推移］

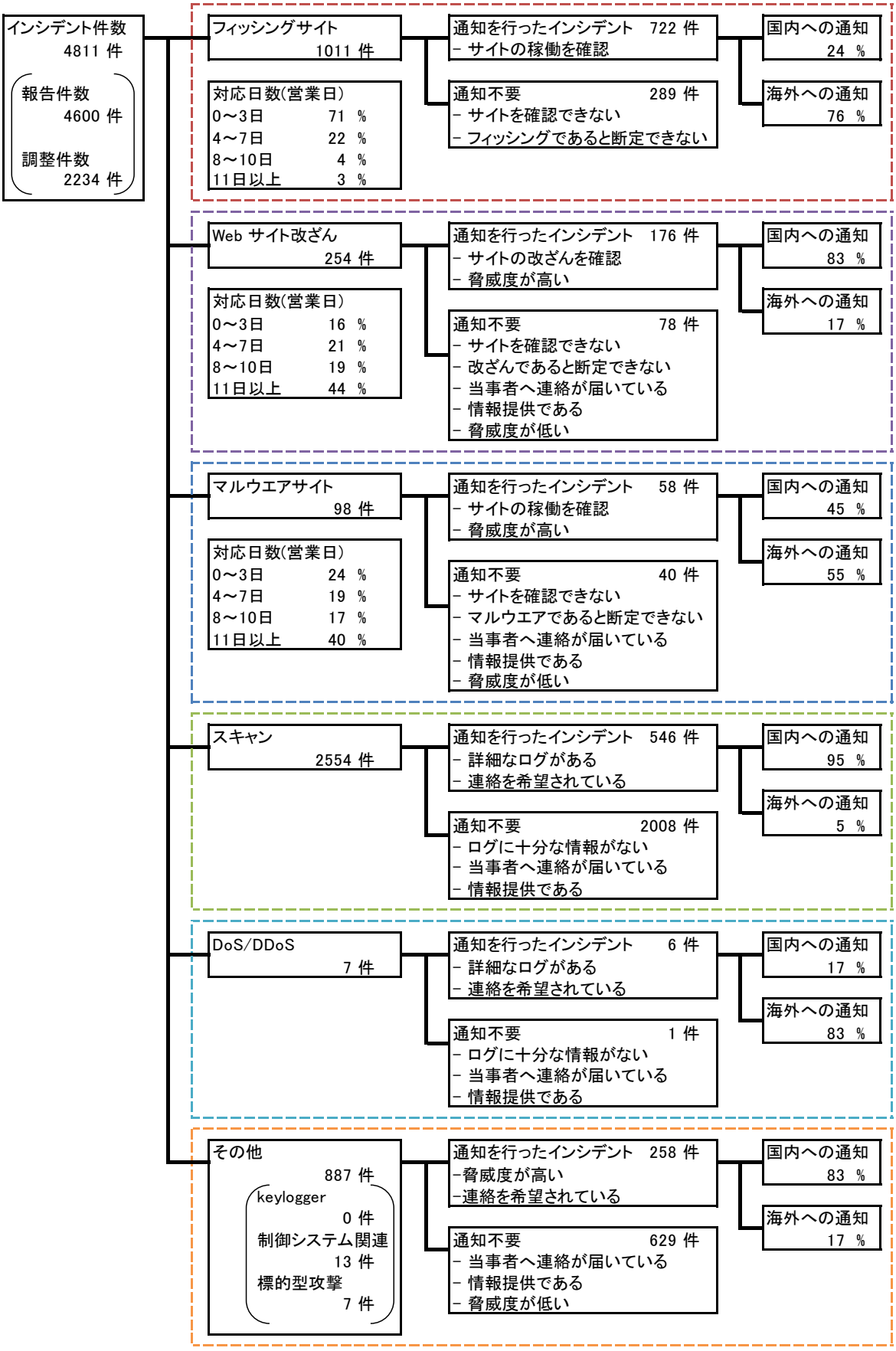


［図 6 マルウエアサイト件数の推移］



［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

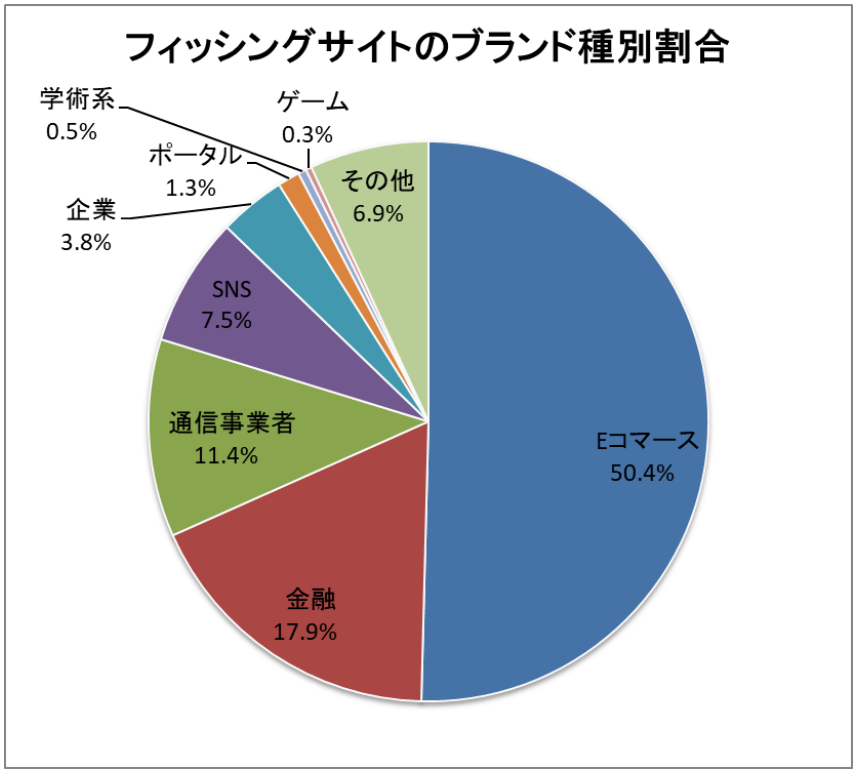
3.1. フィッシングサイトの傾向

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 1,011 件で、前四半期の 736 件から 37%増加しました。また、前年度同期（467 件）との比較では、116%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	7 月	8 月	9 月	国内外別合計（割合）
国内ブランド	69	58	46	173(17%)
国外ブランド	196	253	237	686(68%)
ブランド不明 (注 5)	43	52	57	152(15%)
全ブランド合計	308	363	340	1,011(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 173 件となり、前四半期の 209 件から 17%減少しました。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 686 件となり、前四半期の 586 件から 17%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 50.4%、金融機関のサイトを装ったものが 17.9%、通信事業者のサイトを装ったものが 11.4%でした。

本四半期は、攻撃者がフィッシング目的で新規にドメインの取得やサーバの利用契約をしたと見られるフィッシングサイトが多く確認され、その中には無料の SSL サーバ証明書を使用して HTTPS に対応しているフィッシングサイトも多くありました。

これまでのフィッシングサイトは、サーバ証明書を使用していないような一般の Web サイトにフィッシングのコンテンツが置かれたものが多く、HTTPS を使用するフィッシングサイトはあまり多くはありませんでした。最近では、無料で証明書を作成できるサービスや、証明書が用意される Web サイト作成サービス、CDN サービスなどがあるため、攻撃者にとっても、これらのサービスを悪用したり、サービスを利用しているサイトに侵入したりすることで、HTTPS のフィッシングサイトを立ち上げやすくなってきていると考えられます。したがって、これまではフィッシングサイトを見分ける手段の一つとして、URL が HTTPS であるか否かを Web ブラウザのアドレスバーで確認する方法がありましたが、今や HTTPS のサイトであっても注意が必要です。

国内ブランドのフィッシングサイトは、前四半期に引き続き、通信事業者の Web メールを装ったフィッシングサイトと、SNS 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。国内通信事業者を装ったフィッシングでは、海外の無料 Web サイト作成サービスでサイトを立ち上げ、短縮 URL で誘導する手法が多く見られました。また、SNS を装ったフィッシングのほとんどは、.cn の下で正規サイトを装ったドメイン名を使用していました。

フィッシングサイトの調整先の割合は、国内が 24%、国外が 76%であり、前四半期（国内 26%、国外 74%）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、254 件でした。前四半期の 461 件から 45%減少しています。

前四半期に比べて、改ざんされた Web サイトに関する報告が大幅に減少しました。原因としては、Web サイトの改ざんを容易にするような新しい脆弱性が確認されなかったことや、マルウエアを配布する手段として、Web サイト改ざんによるドライブバイダウンロード攻撃よりも、ファイルを添付してメールで送る方法が主流になってきていることなどが考えられます。

8 月後半から、CMS を使用した Web サイトのページ末尾に埋め込まれた不正なスクリプトによってサポート詐欺サイトに誘導される事例を確認しています。サポート詐欺サイトは、PC がマルウエアに感染しているという偽の警告を表示し、マルウエアの削除手順について案内するため、表示されている電話番号に電話をかけるよう促すものでした。

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、7 件でした。前四半期の 9 件から 22%減少しています。本四半期は、対応を依頼した組織は 7 件でした。

7 月後半ごろ、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、複数の組織から寄せられました。これらの報告では、攻撃に使われた手口やファイルの名前に共通点が見られました。

報告を受けたなりすましメールの一つには ZIP ファイルが添付されており、展開すると、TXT ファイルに偽装したショートカットファイル（LNK ファイル）と、RTF 形式の文書ファイルが含まれていました。これらのファイルを開くと、海外のサーバから Powershell スクリプトをダウンロードして実行する仕組みになっていました。RTF ファイルには、2017 年 4 月に修正された Microsoft 製品の脆弱性（CVE-2017-0199）を悪用して、スクリプトをダウンロードし実行するコードが含まれていました。最終的にダウンロードされるスクリプトは、攻撃によって侵害した PC を操作するためのもので、そのコードは脆弱性診断などの目的で使用されるツールに類似していました。

また、報告された別のなりすましメールには、ファイルをダウンロードするためのリンクが記載されており、ダウンロードされる ZIP ファイルを展開すると、先に述べた事例と同様に RTF ファイルと LNK ファイルが含まれていました。こちらの RTF ファイルは無害なものでしたが、LNK ファイルをたどると、LNK ファイルで指定されたホストから Powershell スクリプトをダウンロードし、実行する仕組みになっていました。

これらのなりすましメールは、いずれも国内のメールサーバが配送元になっていました。JPCERT/CC から、なりすましメールの配送元サーバを管理していた組織に連絡したところ、アカウントが不正に使用されていたとの返信をいただきました。

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 59 件から 66%増加しています。本四半期は、不審なメールに添付されたスクリプトファイルからダウンロードされるランサムウエアや、マクロ付き文書ファイルの実行またはメール本文に記載されたリンクにアクセスすることでダウンロードされる金融系マルウエアに関する報告が多く寄せられました。

本四半期に報告が寄せられたスキャンの件数は、2,554 件でした。前四半期の 3,447 件から 26%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。

［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	892	438	348	1,678
25/tcp	122	185	132	439
80/tcp	63	76	28	167
53/udp	29	51	5	85
23/tcp	24	12	23	59
21/tcp	12	10	14	36
445/tcp	9	5	8	22
2222/tcp	8	10	4	22
3389/tcp	4	5	9	18
2323/tcp	3	3	4	10
9000/tcp	3	0	5	8
443/tcp	1	0	7	8
1433/tcp	2	3	3	8
993/tcp	1	1	4	6
81/tcp	3	1	2	6
4752/udp	1	1	4	6
123/udp	0	1	3	4
8080/tcp	0	2	1	3
7547/tcp	2	0	1	3
5060/udp	1	1	1	3
2375/tcp	0	0	3	3
143/tcp	1	2	0	3
50681/udp	1	0	1	2
3544/udp	2	0	0	2
110/tcp	0	1	1	2
その他	548	693	583	1,824
月別合計	1,732	1,501	1,194	4,427

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。6 月半ばから 7 月半ばにかけて、国内 IP アドレスから行われた SSH のスキャンに関する報告が多数寄せられました。国内 ISP と協力してスキャン元のホストについて調査した結果、スキャンを行って

いたホストは無線 LAN ルータの脆弱性を悪用され、攻撃の踏み台となっていた可能性があることが分かりました。JPCERT/CC は当該ルータ製品を販売する企業と調整し、ルータ製品の脆弱性に関する注意喚起を公開しました。

その他に分類されるインシデントの件数は、867 件でした。前四半期の 623 件から 39%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。

(1) マルウエアが埋め込まれたサーバ管理ツールに関する対応
8 月半ばごろ、韓国の National CSIRT である KrCERT/CC から「サーバ管理ツールを配布している韓国の企業が攻撃によって侵害され、7 月後半から 8 月の初めにかけて、マルウエアが不正に埋め込まれた状態でツールが公開されていた」という情報提供がありました。また、KrCERT/CC からは、マルウエアが埋め込まれた状態でツールが公開されていた期間に、ツールをダウンロードするリンクにアクセスした日本の IP アドレスのリストが提供されました。

JPCERT/CC は、ツールをダウンロードした可能性がある国内組織に、マルウエアが埋め込まれたバージョンのツールをダウンロードしていないか確認し、もしツールを使用している場合には最新バージョンへのアップデートを検討するように連絡しました。その結果、複数の通知先から、実際にツールをダウンロードし使用していたという返信がありました。一方で、JPCERT/CC から通知先に提供した情報では、実際にツールがダウンロードされ使用されたのかどうかを確認できなかったという返信も多くありました。

(2) ランサムウエア WannaCry の亜種に関する対応
8 月半ばごろ、国内の複数の組織から、ランサムウエア WannaCry の亜種が、組織内部のネットワーク上で検知されたという情報が寄せられました。WannaCry は、5 月半ばごろに感染端末上のファイルを暗号化し復号に金銭の支払いを要求するランサムウエアとして確認され、その後、6 月の後半ごろにファイルの暗号化を行わない亜種が確認されました。

被害組織から提供された情報によると、ファイルを暗号化される被害は確認されなかったものの、マルウエアに感染した PC が SMBv1 プロトコルの脆弱性（MS17-010）を悪用したスキャンを内部ネットワークに対して行うことで感染が拡大し、新たに感染した端末がスキャンを行うことによる通信の増大や、スキャンを受けた一部のホストの OS が異常終了するなどの被害が発生したとのことでした。被害組織から提供された検体を分析したところ、暗号化を実行するコードに不備がありファイルの暗号化が行われない、WannaCry の亜種であることを確認できました。

JPCERT/CC は、海外のセキュリティ組織から継続して提供される WannaCry の通信先ドメインにアクセスした国内 IP アドレスの情報をもとに、感染端末が存在している可能性がある国内組織に連絡する活動を行っています。

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 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。