JPCERT-IR-2018-01
発行日: 2018-01-16

JPCERT/CC インシデント報告対応レポート
［2017 年 10 月 1 日 ～ 2017 年 12 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 10 月 1 日から 2017 年 12 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］

	10 月	11 月	12 月	合計	前四半期合計
報告件数 (注 2)	1,460	1,596	1,474	4,530	4,600
インシデント件数 (注 3)	1,522	1,710	1,503	4,735	4,811
調整件数 (注 4)	621	576	704	1,901	2,234

（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。

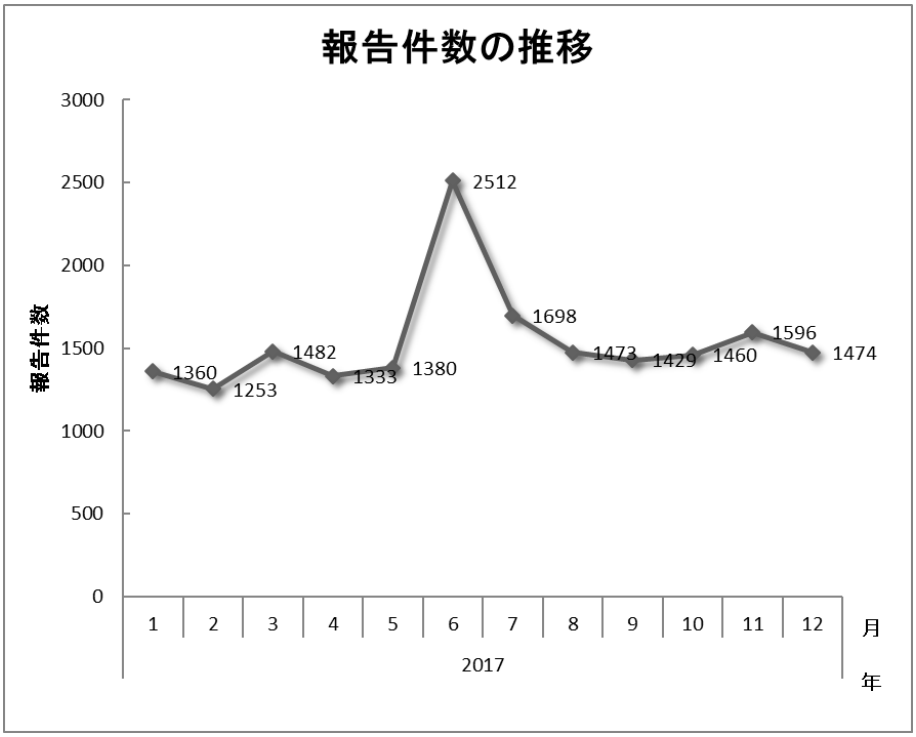
（注 3）「インシデント件数」は、各報告に含まれるインシデント件数の合計を示します。1 つのイン

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。

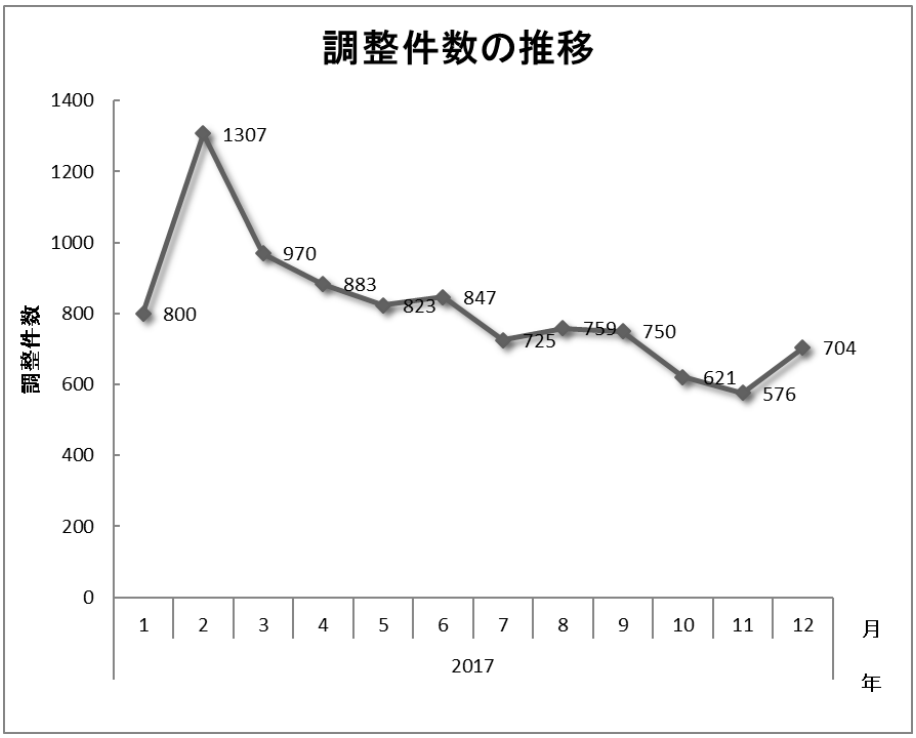
（注 4）「調整件数」は、インシデントの拡大防止のため、サイトの管理者等に対し、現状の調査と問題解決のための対応を依頼した件数を示します。

本四半期に寄せられた報告件数は、4,530 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 1,901 件でした。前四半期と比較して、報告件数は 2%減少し、調整件数は 15%減少しました。また、前年同期と比較すると、報告件数で 12%増加し、調整件数は 34%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］



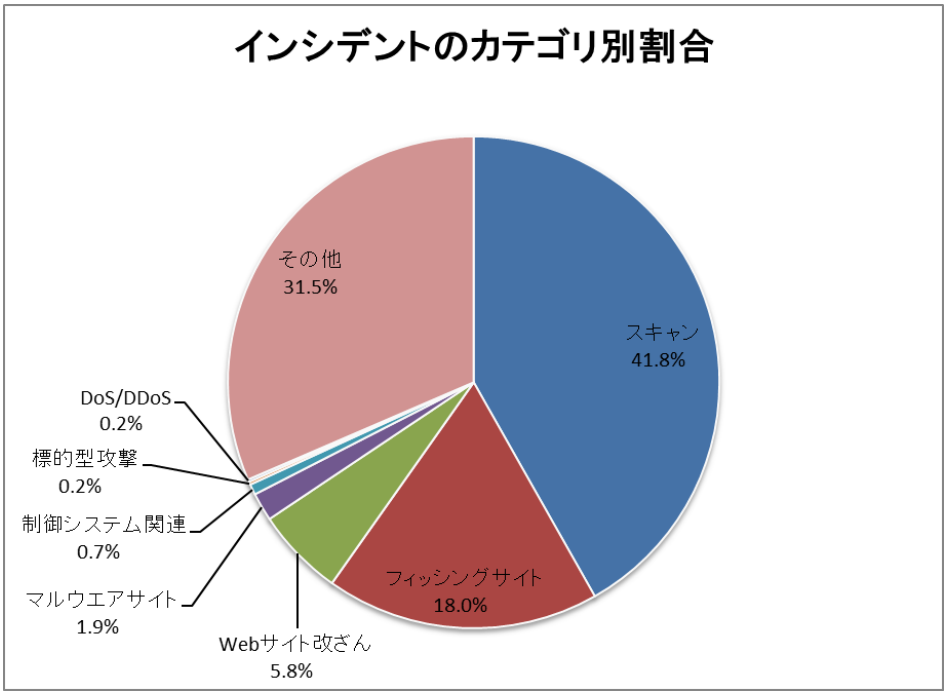
［図 2 インシデント調整件数の推移］

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］

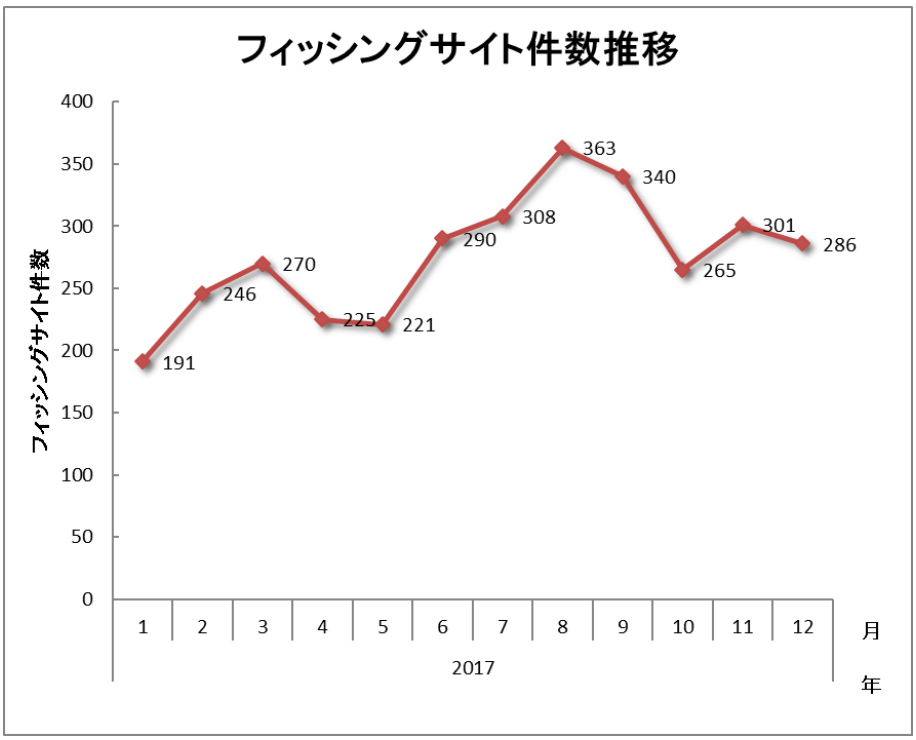
インシデント	10 月	11 月	12 月	合計	前四半期合計
フィッシングサイト	265	301	286	852	1,011
Web サイト改ざん	111	69	96	276	254
マルウエアサイト	26	28	34	88	98
スキャン	668	687	624	1,979	2,554
DoS/DDoS	6	2	0	8	7
制御システム関連	9	12	12	33	13
標的型攻撃	5	4	0	9	7
その他	432	607	451	1,490	867

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 41.8%、フィッシングサイトに分類されるインシデントが 18.0%を占めています。

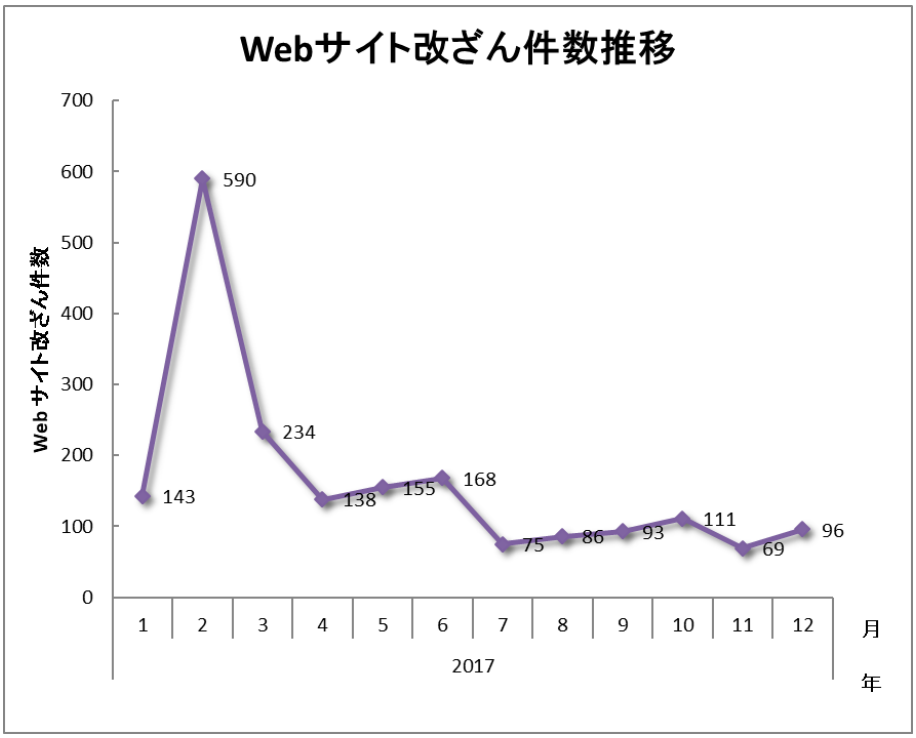


［図 3 インシデントのカテゴリ別割合］

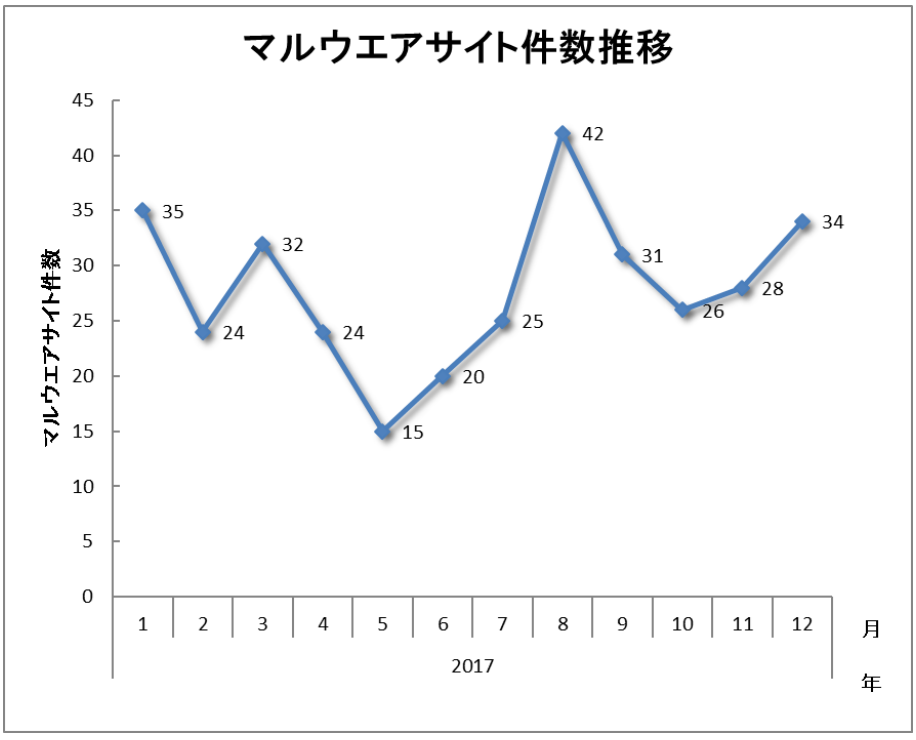
［図 4］から［図 7］に、フィッシングサイト、Web サイト改ざん、マルウエアサイト、スキャンのインシデントの過去 1 年間の月別推移を示します。



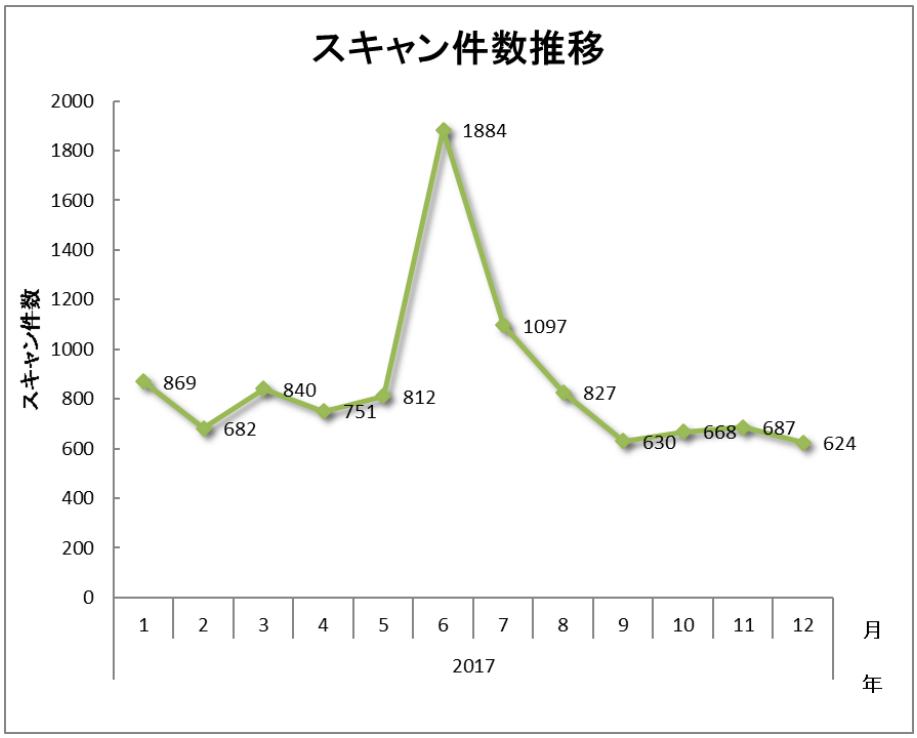
［図 4 フィッシングサイト件数の推移］



［図 5 Web サイト改ざん件数の推移］

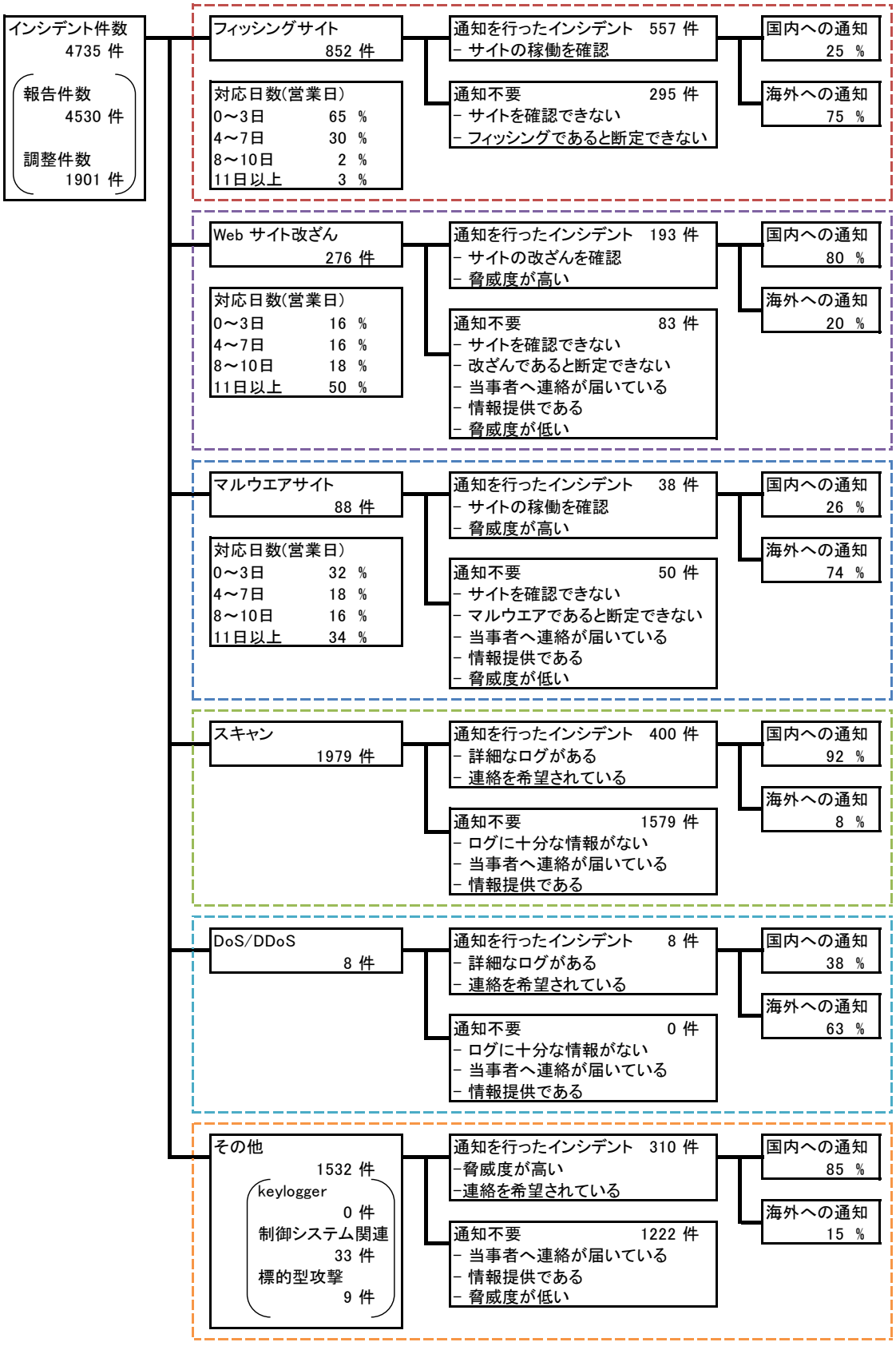


［図 6 マルウエアサイト件数の推移］



［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

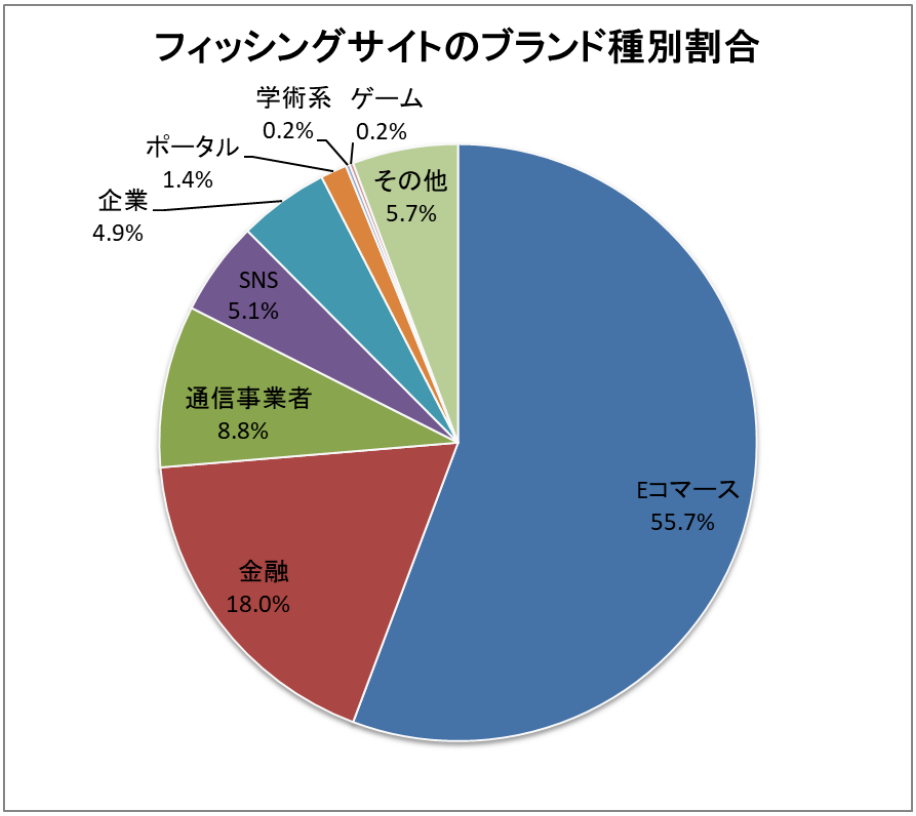
3.1. フィッシングサイトの傾向

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 852 件で、前四半期の 1,011 件から 16%減少しました。また、前年度同期（521 件）との比較では、64%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	10 月	11 月	12 月	国内外別合計（割合）
国内ブランド	42	32	43	117(14%)
国外ブランド	192	216	191	599(70%)
ブランド不明 (注 5)	31	53	52	136(16%)
全ブランド合計	265	301	286	852(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 117 件となり、前四半期の 173 件から 32%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 599 件となり、前四半期の 686 件から 13%減少しました。

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 55.7%、金融機関のサイトを装ったものが 18.0%、通信事業者のサイトを装ったものが 8.8%でした。

フィッシングサイトが装ったブランドの国内、海外の内訳では、海外ブランドが 70%を占め、国内ブランドの割合は 14%でした。海外ブランドの割合が多いのは、特定の海外ブランドを装ったフィッシングメールが広く出回っており、多数の報告が寄せられていることが原因です。それらのフィッシングメールから誘導される特定ブランドを装ったサイトの一部を JPCERT/CC が確認したところ、ブラウザの言語設定が日本語の場合にだけフィッシングサイトとして機能し、それ以外の場合には「サイトが停止している」と表示されました。これらは日本語を使うユーザだけを標的にしていると見られます。

国内ブランドを装ったフィッシングサイトについては、通信事業者の Web メールサービスを装ったフィッシングサイトと、SNS を装った.cn ドメインの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。国内通信事業者の複数のブランドや国内の大学の Web メールサービスを装ったフィッシングサイト等、Web メールサービスのアカウントを窃取するフィッシングサイトの構築に、Web サイトを簡易に開設できる海外の無料サービスがしばしば使用されていることを確認しています。

フィッシングサイトの調整先の割合は、国内が 25%、国外が 75%であり、前四半期（国内 24%、国外 76%）に比べ、国内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、276 件でした。前四半期の 254 件から 9%増加しています。

Web サイトに不正に埋め込まれたスクリプトによって、マルウエア感染の警告を表示して偽のサポートへの電話を促す詐欺サイトや、不審なツールのダウンロードを促すサイトなどに転送される事例を多く確認しています。また、ブログページや、現在使用されていないドメインへのアクセスがあった場合に広告が表示されるドメインパーキングからも、サポート詐欺サイトなどに転送される事例を確認しています。不審なサイトへの転送は、正規のブログパーツや広告から呼び出されるページの転送設定やスクリプトによって行われており、広告配信ネットワークが悪用されている可能性があります。

10 月初めごろから、仮想通貨に関連した演算処理（マイニング）をサイト閲覧者の端末上で実行させるスクリプトが埋め込まれた Web サイトに関する報告が寄せられています。このようなサイトには、改

ざんされてスクリプトを埋め込まれたと見られるサイトがある一方で、サイト管理者が意図してスクリプトを使用していると見られる例もありました。

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、9 件でした。前四半期の 7 件から 29%増加しています。本四半期は、対応を依頼した組織は 7 件でした。

10 月末から 11 月初めにかけて、標的型攻撃と見られるなりすましメールで、Microsoft Office ドキュメントの DDE（Dynamic Data Exchange）プロトコルを悪用するファイルが添付された事例を確認しました。10 月末に報告が寄せられたなりすましメールには、DDE フィールドが埋め込まれた docx 形式の文書ファイルが添付されており、この文書ファイルを開いた際に表示されるダイアログでアプリケーションの起動を許可すると、C&C サーバへの通信が発生する仕組みになっていました。また、11 月初めに寄せられた報告では、なりすましメールに DDE を悪用する msg ファイルが添付されていました。ファイルを開いた際に表示されるダイアログで許可を意味する応答を返すと、C&C サーバから HTTP ボットが取得され、実行されます。これにより、攻撃者は HTTP ボットに感染した端末で任意の機能を実行することができる仕組みとなっていました。DDE を悪用してマルウエアに感染させる攻撃手法は、標的型攻撃に限らず確認されており、11 月上旬には、Microsoft 社が「DDE フィールドを含む Microsoft Office ドキュメントを安全に開く方法」のセキュリティアドバイザリ(*1)を公開しています。

前四半期に引き続き、添付ファイル内のショートカットファイル（LNK ファイル）を実行させてマルウエアに感染させる攻撃手法を確認しています。10 月後半に寄せられた報告では、なりすましメールに添付された ZIP ファイル内に LNK ファイルが含まれていました。LNK ファイルを実行すると、Powershell スクリプトなどがダウンロードされた後、実行され、最終的に遠隔操作型のマルウエア PlugX に感染することを確認しました。

また、11 月半ばに報告が寄せられたなりすましメールでは、標的組織が受け取った正規のメールについての情報を入手した攻撃者が、その再送を装い、攻撃用のファイルをダウンロードさせるリンクを含むメールを標的組織に送信していました。リンクをクリックするとダウンロードされる ZIP ファイルは、Powershell スクリプトを実行する LNK ファイルを含んでおり、この LNK ファイルを実行すると、遠隔からの指令に従ってファイルのアップロード・ダウンロードや、コマンドの実行を行うマルウエアに感染することが確認されました。

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、88 件でした。前四半期の 98 件から 10%減少しています。10 月半ば頃から、金融機関やクレジットカード会社などを騙るメールに記載されたリンク

からダウンロードしたファイルを実行すると、最終的に情報窃取系マルウエアに感染するという事例が継続的に確認されており、関連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、1,979 件でした。前四半期の 2,554 件から 23%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	10 月	11 月	12 月	合計
22/tcp	457	458	333	1248
25/tcp	91	101	109	301
80/tcp	32	54	30	116
23/tcp	12	19	54	85
21/tcp	9	10	26	45
2323/tcp	1	6	24	31
445/tcp	7	2	16	25
443/tcp	3	4	11	18
3389/tcp	6	2	5	13
53/udp	9	0	1	10
2222/tcp	7	0	1	8
9000/tcp	5	1	1	7
4752/udp	1	2	3	6
110/tcp	2	3	1	6
81/tcp	2	1	1	4
52869/tcp	0	0	4	4
143/tcp	1	1	2	4
123/udp	0	4	0	4
26551/udp	3	0	0	3
1433/tcp	1	1	1	3
その他	580	298	581	1459
月別合計	1229	967	1204	3400

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。

その他に分類されるインシデントの件数は、1,490 件でした。前四半期の 867 件から 72%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) 外部からリソースレコードを更新できる国内に設置された DNS サーバへの対応
外部からリソースレコードを更新できる設定になっている脆弱な国内 DNS サーバと、そのサーバの影響を受けるドメインの情報が、10 月半ばごろに海外のセキュリティ研究者から提供されました。それらの DNS サーバは、動的更新を許可しているが、更新者のアクセス制御や認証などが設定されておらず、任意のサブドメインを登録したり、既存のドメインの IP アドレスを書き換えたりできることから、悪意のあるサイトへの誘導や情報の窃取などに悪用される可能性がありました。悪用の防止のための対策としては、動的更新の無効化や、DNS の通信に署名することにより認証を可能にする TSIG を有効にすることなどが挙げられます。

JPCERT/CC は、提供された情報をもとに、DNS サーバを管理する複数の組織に連絡し、DNS の設定の見直しや、使用している DNS サーバの環境についての情報提供を依頼しました。その結果、「意図せず動的更新が有効になっていた」、「動的更新を実際に使用していたがセキュリティ保護をしていなかった」といった返信を、複数の通知先組織からいただきました。

(2) 23/TCP、2323/TCP に対するスキャンの増加に関する対応
JPCERT/CC が運用するインターネット定点観測システム TSUBAME において、日本の IP アドレスが送信元となっているパケットによる、ポート 23/TCP および 2323/TCP に対するスキャンの増加を 11 月上旬から観測しています。こうしたスキャン行為については、国内の通信事業者やセキュリティ組織からも、同様の情報が寄せられました。また、ほぼ同時期に日本の IP アドレス空間のポート 52869/TCP に対するスキャンの増加も確認しました。

調査の結果、ルータ製品が 52869/TCP に対するスキャンによってマルウエアに感染し、感染拡大のためのスキャンを行っていることが分かりました。ルータ製品が感染したマルウエアは、外部からの命令によってさまざまなプロトコルの通信を任意の対象に送り付ける機能を持ち、大規模な DDoS 攻撃に使用されたボットネットを構成する Mirai と呼ばれるマルウエアの亜種でした。感染した機器を放置することで、機器を踏み台として悪用した DDoS 攻撃が行われることが懸念されます。

JPCERT/CC では、本件について調査、対応を行っていた複数の国内組織と連携し、12 月 19 日に「Mirai 亜種の感染活動に関する注意喚起」(*2)を公開しました。

5. 参考文献

(1) マイクロソフト セキュリティ アドバイザリ 4053440
https://technet.microsoft.com/ja-jp/library/security/4053440.aspx

(2) Mirai 亜種の感染活動に関する注意喚起
https://www.jpcert.or.jp/at/2017/at170049.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 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。