電子署名者 : Japan Computer Emergency Response Team Coordination Center
DN : c=JP, st=Tokyo, l=Chiyoda-ku, email=office@jpcert.or.jp, o=Japan Computer Emergency Response Team Coordination Center, cn=Japan Computer Emergency Response Team Coordination Center
日付 : 2017.01.11 11:21:58 +09'00'

JPCERT-IR-2016-04
発行日: 2017-01-11

JPCERT/CC インシデント報告対応レポート
［2016 年 10 月 1 日 ～ 2016 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」といいます。）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」といいます。）の報告を受け付けています(注 1)。本レポートでは、2016 年 10 月 1 日から 2016 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)	1150	1273	1613	4036	3137
インシデント件数 (注 3)	1281	1409	1432	4122	2801
調整件数 (注 4)	1038	1048	797	2883	2122

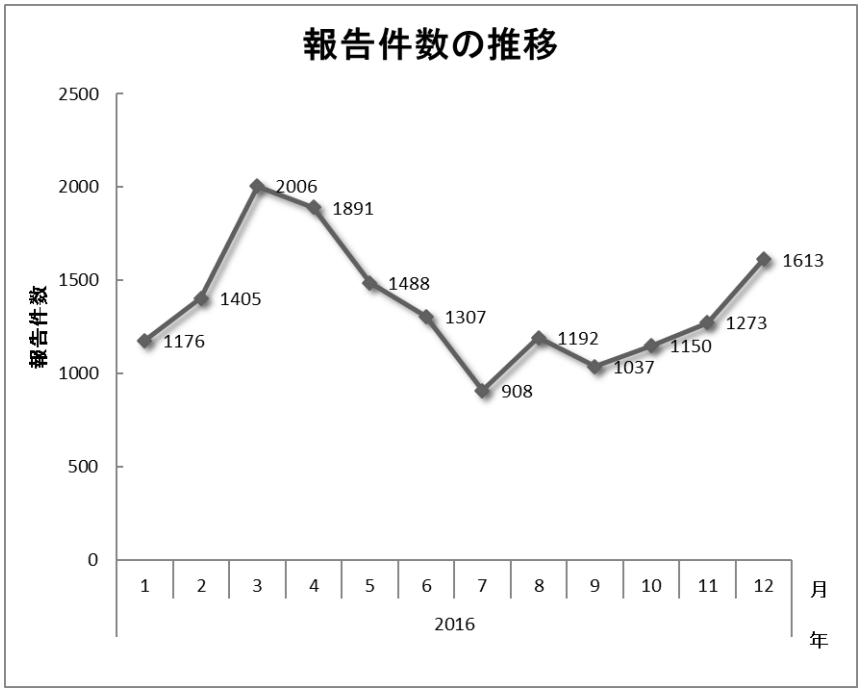
（注 2）「報告件数」は、報告者から寄せられた Web フォーム、メール、FAX による報告の総数を示します。

（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。

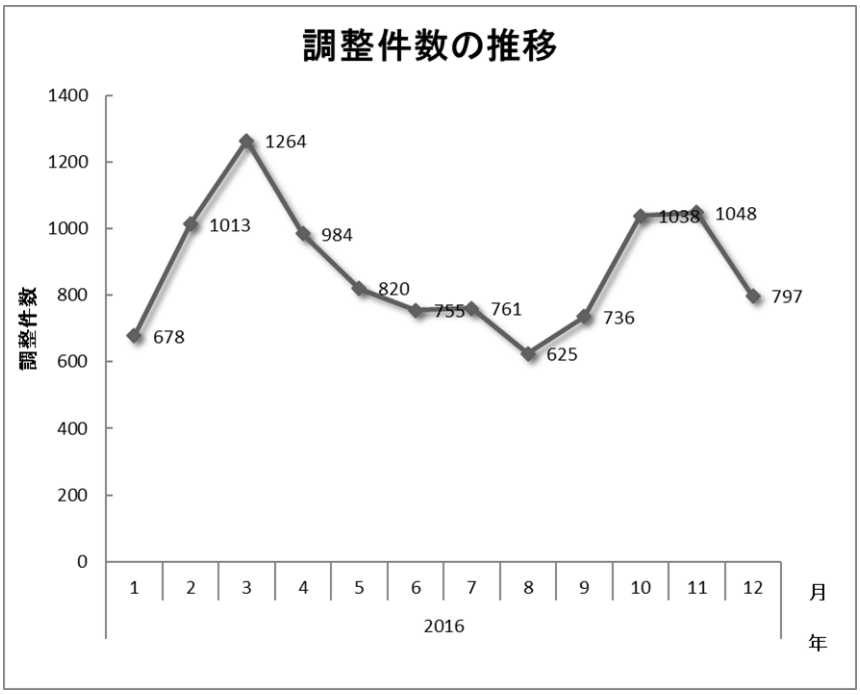
（注 4）「調整件数」は、インシデントの拡大防止のため、サイトの管理者等に対し、現状の調査と問題解決のための対応を依頼した件数を示します。

本四半期に寄せられた報告件数は、4036 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 2883 件でした。前四半期と比較して、報告件数は 29%増加し、調整件数は 36%増加しました。また、前年同期と比較すると、報告数で 17%増加し、調整件数は 40%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 報告件数の推移］



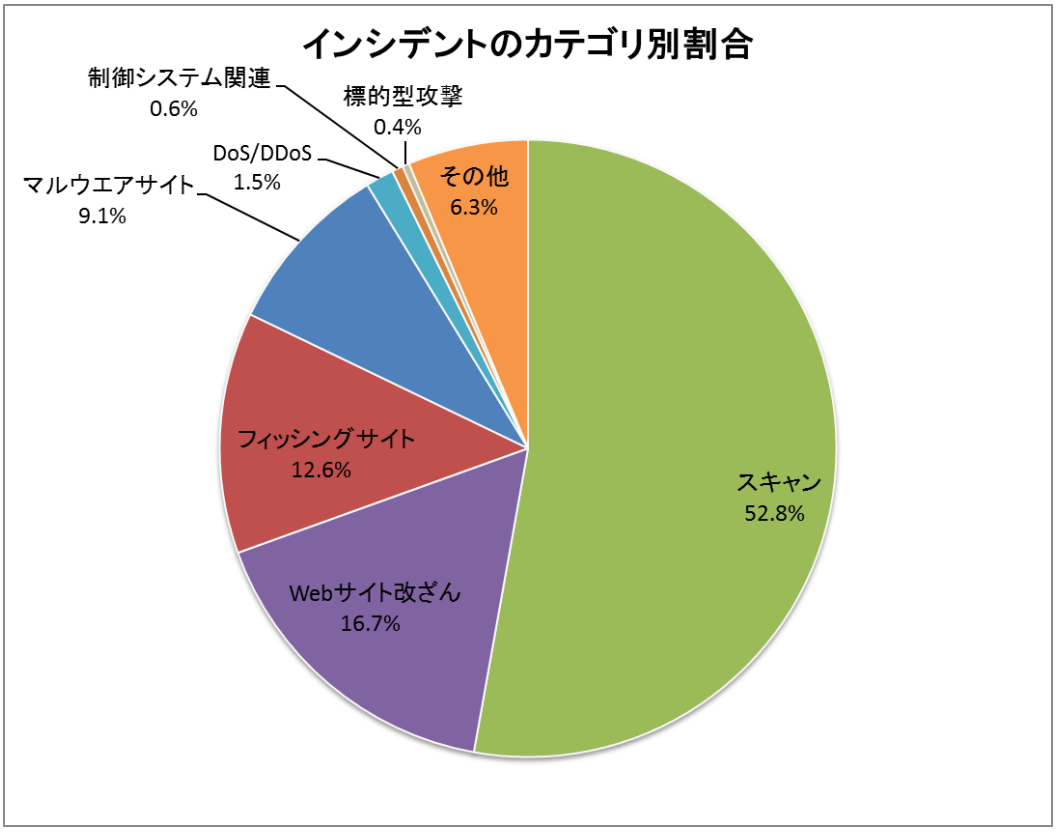
［図 2 インシデント調整件数の推移］

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］

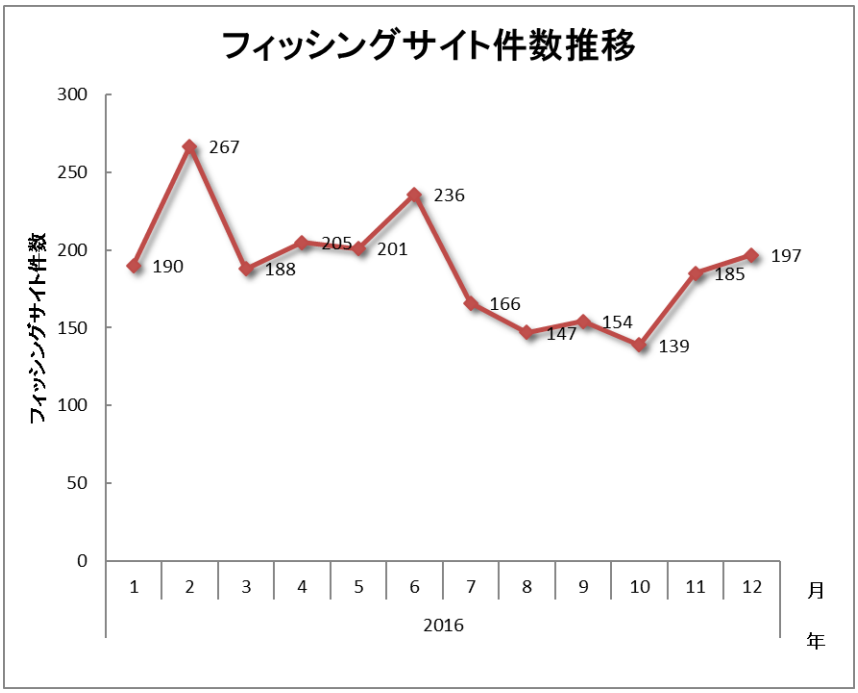
インシデント	10 月	11 月	12 月	合計	前四半期合計
フィッシングサイト	139	185	197	521	467
Web サイト改ざん	180	314	194	688	554
マルウエアサイト	110	116	150	376	337
スキャン	709	679	789	2177	1098
DoS/DDoS	59	2	0	61	54
制御システム関連	3	13	8	24	5
標的型攻撃	8	4	3	15	10
その他	73	96	91	260	276

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 52.8%、Web サイト改ざんに分類されるインシデントが 16.7%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 12.6%でした。

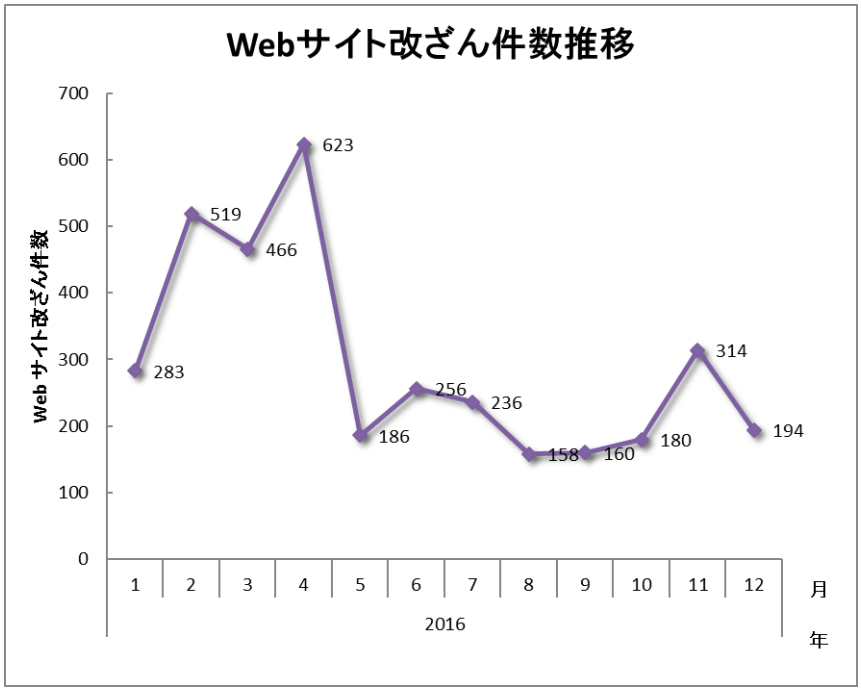


［図 3 インシデントのカテゴリ別割合］

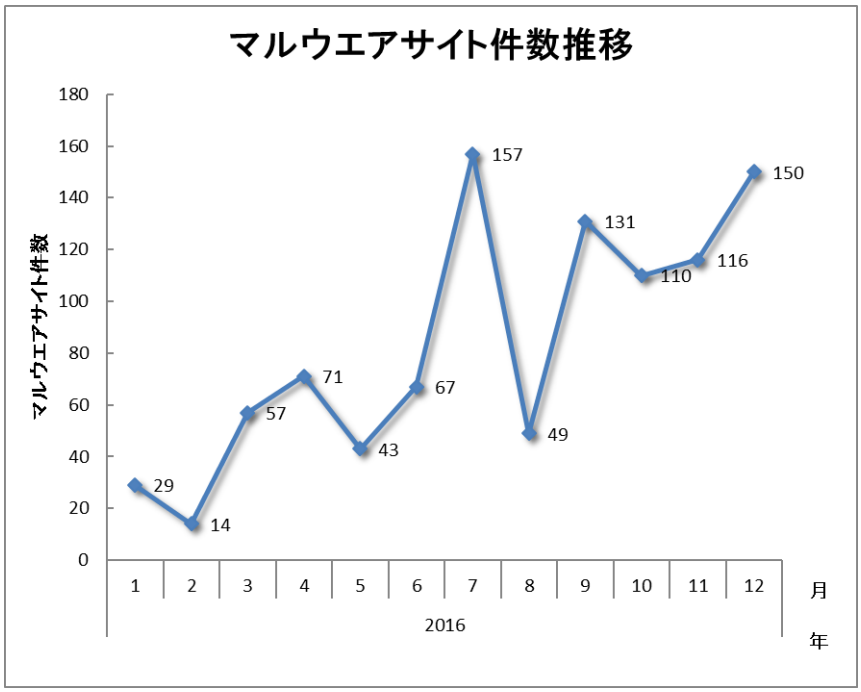
［図 4］から［図 7］に、フィッシングサイト、Web サイト改ざん、マルウエアサイト、スキャンのインシデントの過去 1 年間の月別推移を示します。



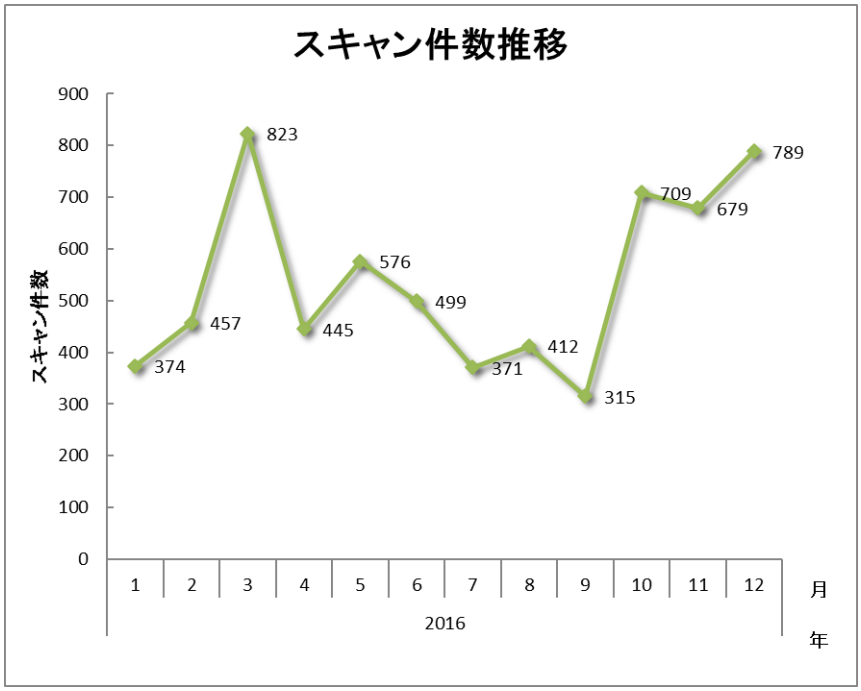
［図 4 フィッシングサイト件数の推移］



［図 5 Web サイト改ざん件数の推移］

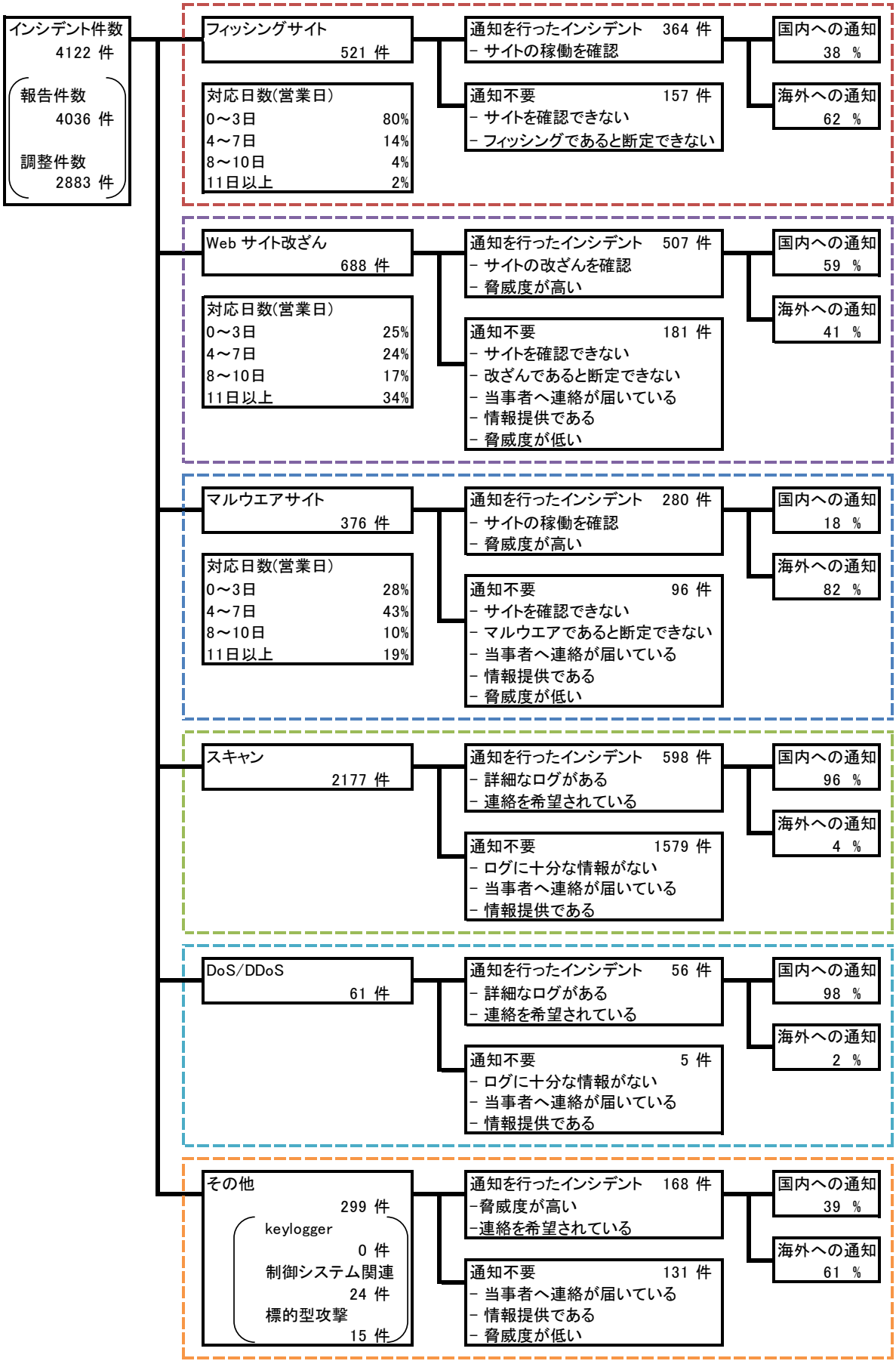


［図 6 マルウエアサイト件数の推移］



［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

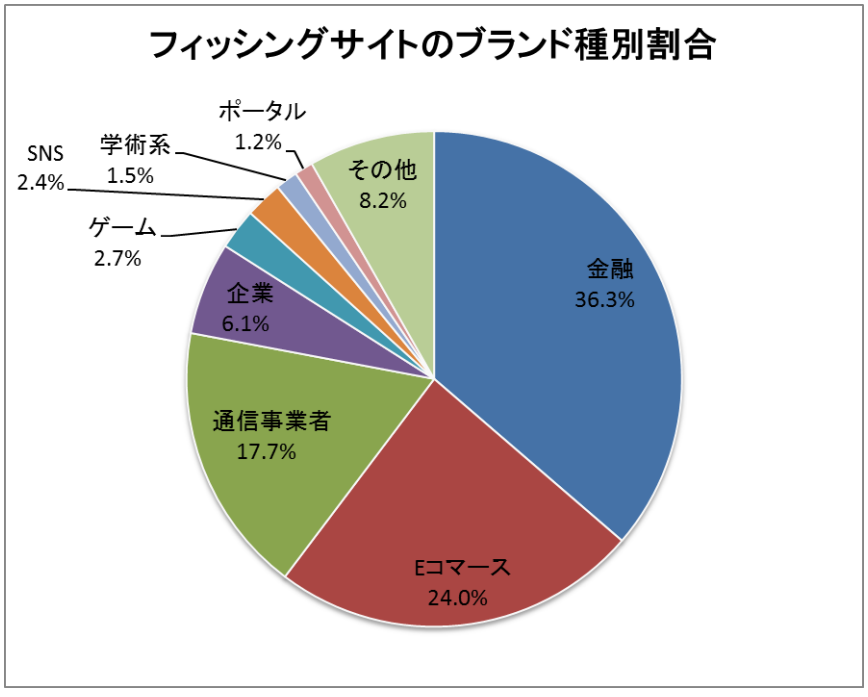
3.1. フィッシングサイトの傾向

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 521 件で、前四半期の 467 件から 12%増加しました。また、前年度同期（474 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 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	24	47	63	134(26%)
国外ブランド	88	106	85	279(54%)
ブランド不明 (注 5)	27	32	49	108(21%)
月別合計	139	185	197	521(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 134 件となり、前四半期の 106 件から 26%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 279 件となり、前四半期の 243 件から 15%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、金融機関のサイトを装ったものが 36.3%、E コマースサイトを装ったものが 24.0%でした。

国内ブランドを装ったフィッシングサイトについては、前四半期に引き続き、Web メールのアカウント情報を狙った事例が多く報告されました。国内通信事業者の Web メールのログイン画面を装ったフィッシングサイトが、10 月末から継続して確認されており、これらのフィッシングでは、メールに記載された短縮 URL から実際のフィッシングサイトへ誘導する傾向が見られました。また、10 月末と 11 月後半には、国内の複数の大学の Web メールのログイン画面を装ったフィッシングサイトの報告が寄せられました。この中には、異なる大学で、同じ海外の無料 Web サイト作成サービスが使用されているものもあることから、これらは同一の攻撃者によるフィッシングである可能性が考えられます。

オンラインゲームを装ったフィッシングサイトは、10 月と 11 月以降とで、被害ブランドやサイトが設置されるホスティングサービスに変化が見られましたが、前四半期に引き続き、フィッシングサイトで使用されていたほとんどのドメインは、無料で取得できる.cc ドメインでした。

金融関係の国内ブランドのフィッシングサイトでは、クレジットカード情報を窃取しようとするものが多く確認された一方、銀行を装ったフィッシングサイトはごく少数にとどまりました。

フィッシングサイトの調整先の割合は、国内が 38%、国外が 62%であり、前四半期（国内 25%、国外 75%）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、688 件でした。前四半期の 554 件から 24%増加しています。

Web サイトのトップページに、index_old.php という名の不正な PHP ファイルを読み込むスクリプトが埋め込まれる改ざんについて情報提供があり、11 月 14 日に、”Web サイト改ざんに関する注意喚起”を公開しました。不正な PHP ファイルが読み込まれると、Web サイトにアクセスした IP アドレスやブラウザのユーザエージェント、アクセス時刻などをログとして記録するようになるため、攻撃のための情報を収集される可能性があります。

前四半期に引き続き、Web サイト改ざんについて多数の報告が寄せられており、改ざんされた Web サイトの多くは WordPress などの CMS が使用されていました。また、Magento という CMS を使用した国内の多数の E コマースサイトに、クレジットカード番号などを窃取するスクリプトが埋め込まれているという報告が寄せられました。各サイトを調査したところ、複数のサイトに不正なスクリプトが埋め込

まれていることを確認したため、改ざんされたサイトの管理者へ対応を依頼しました。

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、15 件でした。前四半期の 10 件から 50%増加しています。本四半期は、延べ 7 組織に対応を依頼しました。

前四半期のインシデント報告対応レポートで紹介した、多数の C2 サーバを使用する高度な標的型攻撃について対応を進めています。この一連の攻撃で使用されたマルウエアの、C2 サーバとして使われた機器の管理者に対して、機器を調査し、攻撃者が設置したファイル・プログラムなどを採取して提供してもらえるよう依頼しました。

提供いただいた事例には、攻撃者が侵入した痕跡が残っているにも関わらず、マルウエアの通信先に指定された URL に該当するプログラムファイルが存在しない例や、既存のプログラムファイルに不審な変更の痕跡がない例がありました。これは、攻撃者が C2 サーバとして悪用できるように準備はしたが、実際には一度も使用されなかった事例の可能性があります。

その他に、本四半期は、マルウエアが添付されたなりすましメールに関する報告が複数寄せられました。10 月後半に報告されたなりすましメールに添付されていたのは、ダウンローダと呼ばれる種類のマルウエアであり、PlugX と呼ばれる遠隔操作マルウエアの通信先として 8 月末に確認されていた IP アドレスのホストから、別のマルウエアをダウンロードすることが確認されました。

11 月後半には、PDF ファイルと実行ファイルを含む ZIP ファイルが添付されたなりすましメールの報告が寄せられました。この実行ファイルは、外部から命令を受信して動作する遠隔操作型のマルウエアであることが分析により分かりました。このマルウエアの通信先サーバは、同時期に別の国内組織に送付された、なりすましメールに添付されていたマルウエアの通信先とも一致していることから、ほぼ同時期に複数の国内組織が同じような攻撃を受けていた可能性があります。

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、376 件でした。前四半期の 337 件から 12%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、2177 件でした。前四半期の 1098 件から 98%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。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	10 月	11 月	12 月	合計
22/tcp	255	186	260	701
25/tcp	156	161	286	603
80/tcp	70	205	161	436
53/udp	128	61	24	213
23/tcp	28	31	33	92
21/tcp	35	33	0	68
2323/tcp	9	16	6	31
5358/tcp	0	0	11	11
3389/tcp	2	4	2	8
5060/udp	0	0	6	6
33442/udp	2	0	3	5
23887/udp	0	2	3	5
4752/udp	2	1	1	4
81/tcp	0	2	1	3
554/tcp	0	2	1	3
2222/tcp	0	0	3	3
143/tcp	1	1	1	3
51331/udp	2	0	0	2
445/tcp	0	2	0	2
30586/udp	1	1	0	2
137/udp	2	0	0	2
その他	242	161	197	600
月別合計	935	869	999	2803

その他に分類されるインシデントの件数は、260 件でした。前四半期の 276 件から 6%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。

【WordPress などの CMS を使用した Web サイトの改ざん】
本四半期に確認された Web サイトの改ざんには、初回アクセス時には正規の Web ページの末尾に難読化された不正な JavaScript が埋め込まれるが、その後は同じ IP アドレスからアクセスしても正規の Web ページだけを返すものが複数ありました。改ざんされたサイトの管理者の一部によれば、使用している CMS のほとんどの PHP ファイルの先頭部分に不審なコードが埋め込まれていました。この不審なコードは、サイトにアクセスしてきた IP アドレスの情報を C2 サーバに送信し、C2 サーバからの返答によって、不正な JavaScript を埋め込むか正規の Web ページを返すかを制御する仕組みになっていました。任意の PHP コードを実行するバックドアが設置されている事例もありました。

11 月末ごろには、CMS のテンプレートファイルとして使用される PHP ファイル header.php に、jquery.min.php 等の文字列を含むスクリプトが埋め込まれ、何度修正しても埋め込みが繰り返されるという報告が寄せられました。攻撃者が Web からサーバの操作を行うために使用する WebShell や CMS の正規のプラグインを装ったもの、メール送信機能を持つものなど、複数の不審な PHP ファイルも置かれていました。

こうした改ざんやファイル設置をするために攻撃者は、FTP や SSH のパスワードを破ってサーバに侵入した、あるいは、脆弱性を悪用してファイルをアップロードした、CMS の管理画面のパスワードを破った、プラグインに偽装した悪意のあるファイルを遠隔操作してアップロードしたなどの手口が考えられます。

対策としては、サーバの管理画面や FTP、SSH サーバにおいて、アクセス元を特定の IP アドレスだけに制限すること、推測されにくい十分長い文字列のパスワードを設定すること、CMS およびテーマ、プラグインを最新のバージョンに保つこと、不要なテーマやプラグインを無効化するだけでなくシステムから完全に削除することなどが挙げられます。

【Magento を使用した E コマースサイトの改ざん】
11 月末ごろ、イタリアの CERT Nazionale Italia から、Magento という CMS を使用して構築された複数 E コマースサイトに、クレジットカード情報や認証情報を窃取するコードが埋め込まれているとの情報が寄せられました。提供された被害サイトのリストをもとに個々の国内 E コマースサイトを確認したところ、複数のトップページや、クレジットカード番号の入力値に問題がないかチェックするための JavaScript に、不審なスクリプトが埋め込まれていました。

不審なスクリプトが埋め込まれていた E コマースサイトを管理する、複数のホスティング事業者に対して、当該コードが意図したものであるか確認するよう JPCERT/CC から依頼しました。

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。

本文書を引用、転載する際には JPCERT/CC 広報 (pr@jpcert.or.jp) まで確認のご連絡をお願いします。最新情報については JPCERT/CC の Web サイトを参照してください。

JPCERT コーディネーションセンター(JPCERT/CC)
https://www.jpcert.or.jp/