JPCERT CC®

Japan Computer Emergency Response Team Coordination Center

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 : 2016.07.13 17:34:43 +09'00'

JPCERT-IR-2016-02

発行日: 2016-07-14

JPCERT/CC インシデント報告対応レポート
[2016 年 4 月 1 日 ～ 2016 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」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 4 月 1 日から 2016 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)	1891	1488	1307	4686	4587
インシデント件数 (注 3)	1497	1168	1126	3791	4143
調整件数 (注 4)	984	820	755	2559	2955

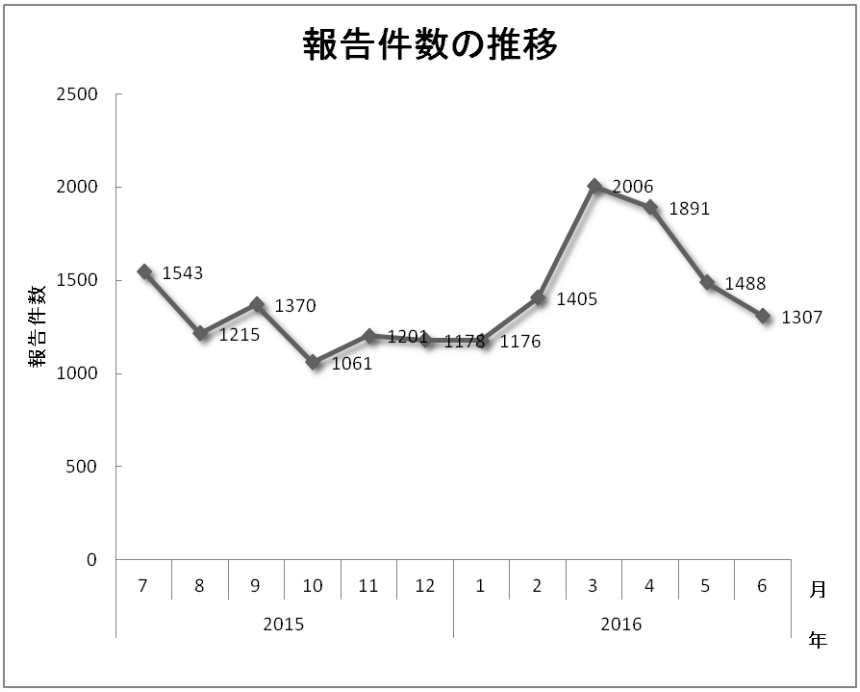
【注 2】「報告件数」は、報告者から寄せられた Web フォーム、メール、FAX による報告の総数を示します。

【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。

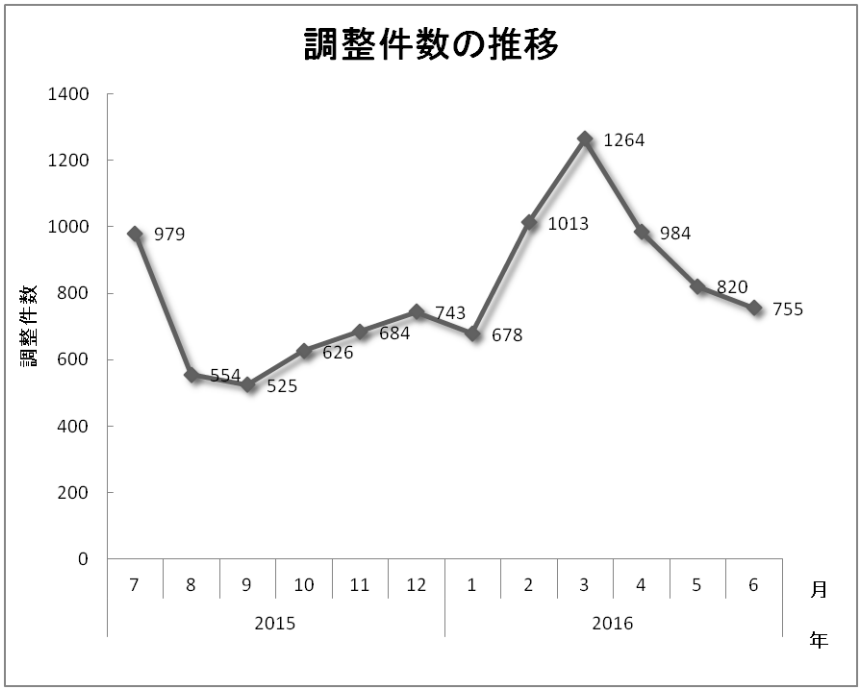
【注 4】「調整件数」は、インシデントの拡大防止のため、サイトの管理者等に対し、現状の調査と問題解決のための対応を依頼した件数を示します。

本四半期に寄せられた報告件数は、4686 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 2559 件でした。前四半期と比較して、報告件数は 2%増加し、調整件数は 13%減少しました。また、前年同期と比較すると、報告数で 10%減少し、調整件数は 1%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 報告件数の推移］



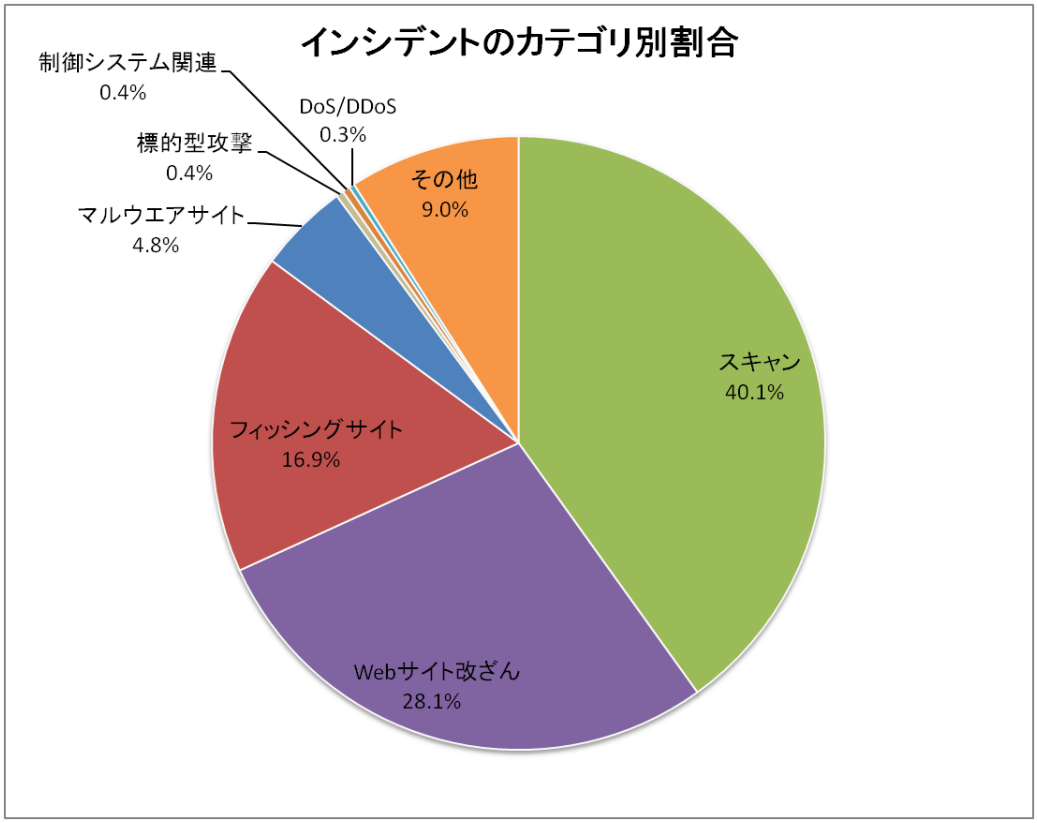
［図 2 インシデント調整件数の推移］

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］

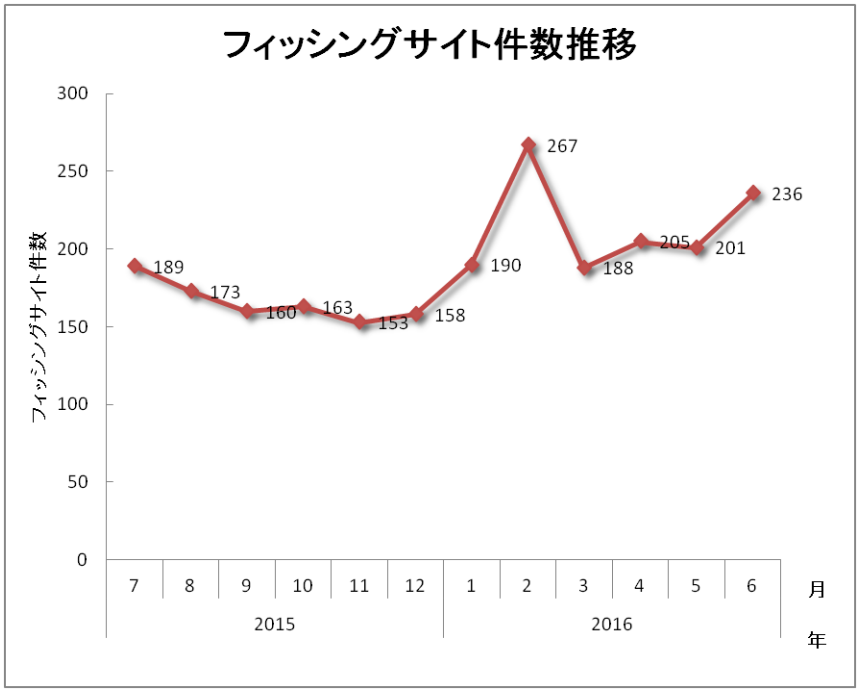
インシデント	4 月	5 月	6 月	合計	前四半期合計
フィッシングサイト	205	201	236	642	645
Web サイト改ざん	623	186	256	1065	1268
マルウエアサイト	71	43	67	181	100
スキャン	445	576	499	1520	1654
DoS/DDoS	5	1	5	11	86
制御システム関連	6	9	0	15	11
標的型攻撃	1	9	5	15	6
その他	141	143	58	342	373

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 40.1%、Web サイト改ざんに分類されるインシデントが 28.1%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 16.9%でした。

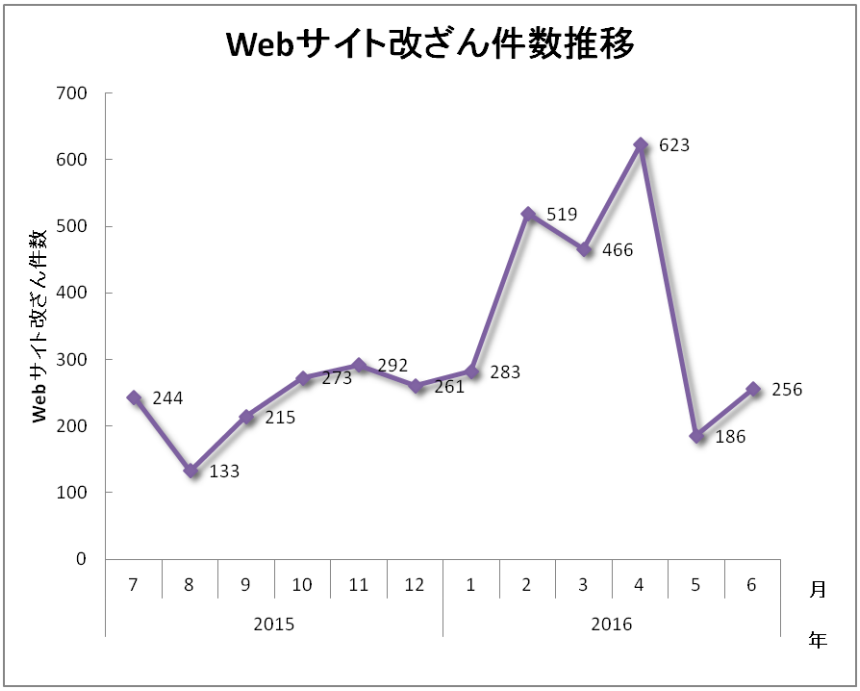


［図 3 インシデントのカテゴリ別内訳］

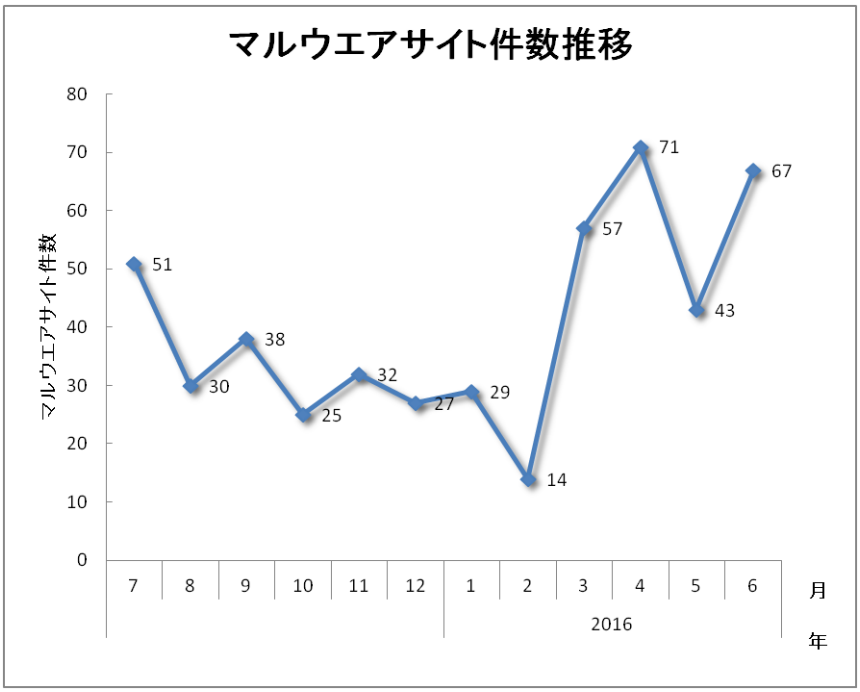
［図 4］から［図 7］に、フィッシングサイト、Web サイト改ざん、マルウエアサイト、スキャンのインシデントの過去 1 年間の月別推移を示します。



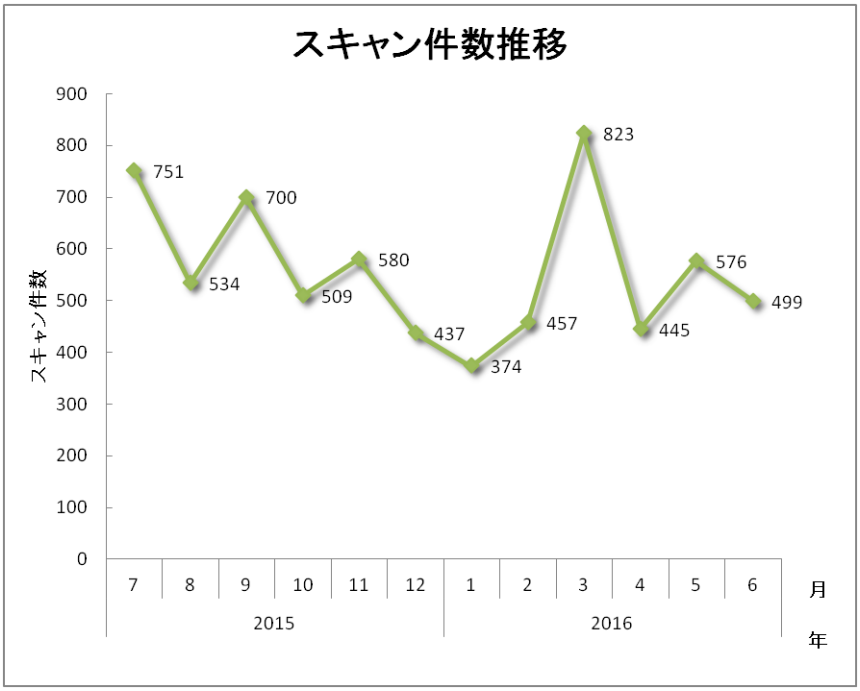
［図 4 フィッシングサイト件数の推移］



［図 5 Web サイト改ざん件数の推移］

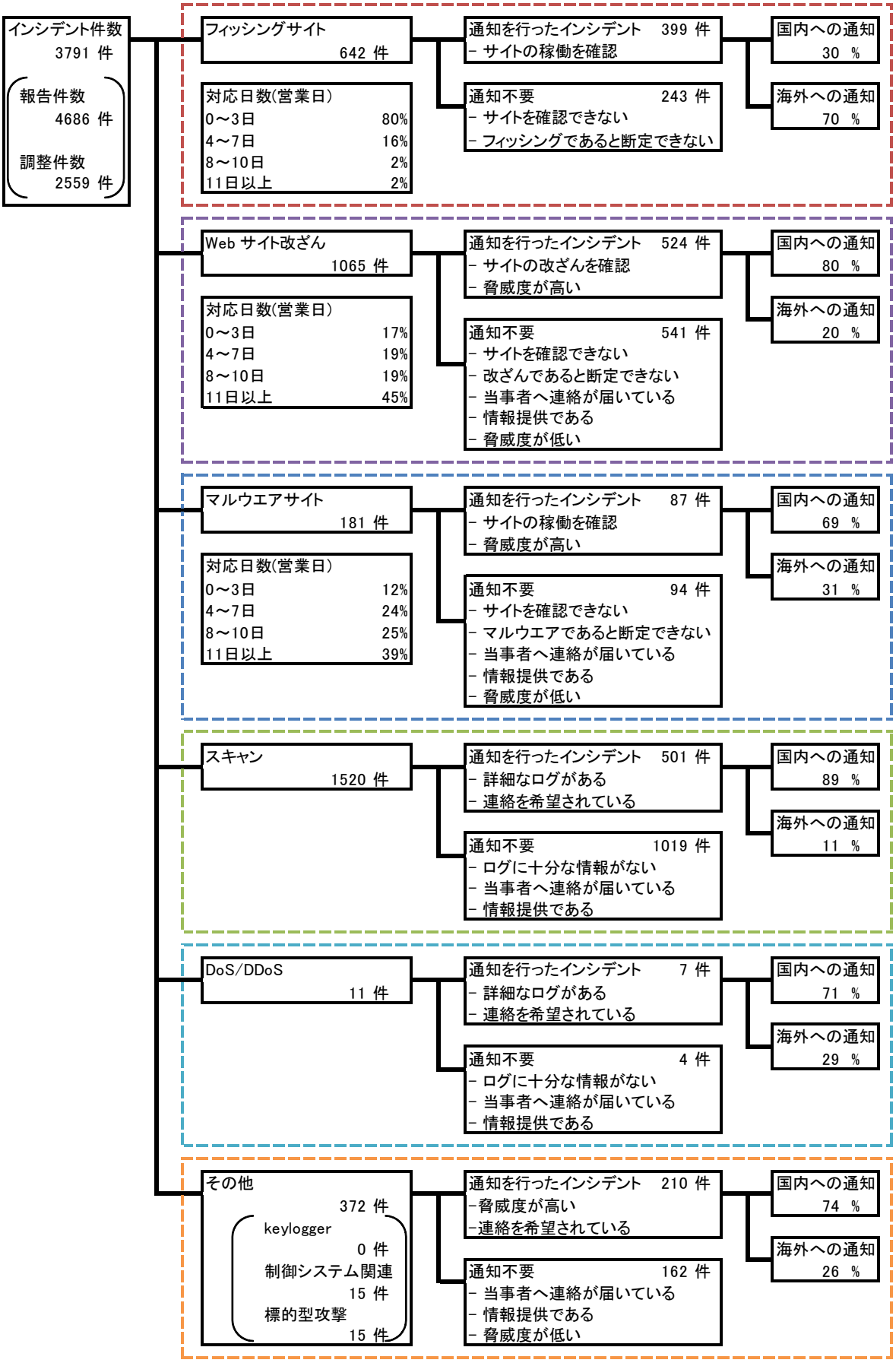


［図 6 マルウエアサイト件数の推移］



［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

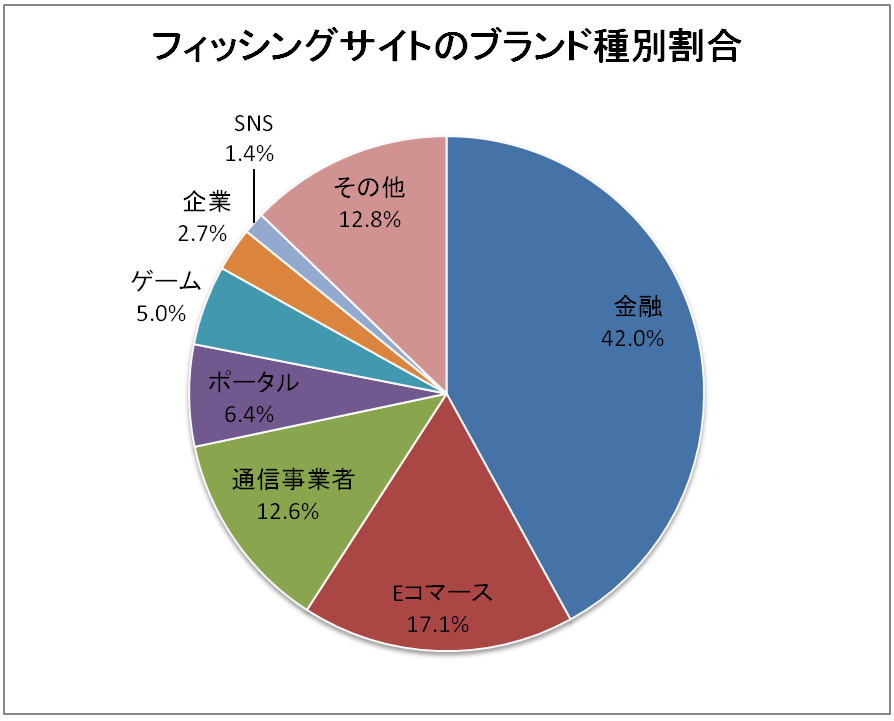
3.1. フィッシングサイトの傾向

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 642 件で、前四半期の 645 件から 0.5%減少しました。また、前年度同期（491 件）との比較では、31%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	国内外別合計（割合）
国内ブランド	44	38	44	126(20%)
国外ブランド	115	108	89	312(49%)
ブランド不明 (注 5)	46	55	103	204(32%)
月別合計	205	201	236	642(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内訳］

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 126 件となり、前四半期の 189 件から 33%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 312 件となり、前四半期の 270 件から 16%増加しました。

JPCERT/CC が報告を受領し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 42.0%、E コマースサイトを装ったものが 17.1%で、装われたブランド別内訳では、国内ブランドは通信事業者、海外ブランドは金融機関が最も多数を占めました。

本四半期は、国内通信事業者の 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サイトの多くは、侵入されたとみられる海外の Web サイトに設置されていました。異なる通信事業者のブランドを装った複数の Web ページを収容したフィッシングサイトを確認しており、国内通信事業者が提供する Web メールのアカウント窃取を目的とした攻撃が活発になっている可能性があります。

国内金融機関を装ったフィッシングサイトは、4 月から 5 月後半にかけては継続的に確認していましたが、6 月後半までのおよそ 1 か月間は、新規の IP アドレスのフィッシングサイトが確認されておらず、攻撃が減少してきている傾向が見られました。

国内オンラインゲームを装ったフィッシングサイトは、4 月から 6 月前半までは 1 つのブランドのみ確認されていましたが、6 月半ばに別のブランドが複数確認されるようになりました。いずれのフィッシングサイトも、前四半期にも確認された、無料で登録できる.cc のドメイン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 30%、国外が 70%であり、前四半期（国内 35%、国外 65%）に比べ、国外へ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、1065 件でした。前四半期の 1268 件から 16%減少しています。

前四半期に多く確認された、特定のブラウザでアクセスした場合のみ、不正な JavaScript を表示する仕組みの改ざんも見られましたが、その他に、”jquery.min.php”という文字列を含む URL に誘導する JavaScript が、head タグ内の末尾に埋め込まれる改ざんが多く確認されました。改ざんされたサイトの多くは CMS を使用しており、CMS のテーマやプラグインの脆弱性を使用した攻撃や、管理画面の認証を破られたことによって侵入され、改ざんされた可能性があります。

また、通信販売を利用して商品を購入する際に、検索エンジンサイトで商品を検索すると不審な通信販売サイトが表示される事例が数多く確認されました。この不審な通信販売サイトは、第三者の正規 Web サイトを改ざんして作成されており、その正規サイトを調査すると正規サイトと関係のない様々な商品を販売する通信販売のページを模したサイトが大量に表示されることを確認しました。対象サイトの

URL に直接アクセスした場合は、関連するキーワードが埋め込まれた正規のページが表示されるのに対し、検索エンジンサイトの URL をリファラに指定してアクセスした場合には、iframe タグによって不審な通信販売サイトのページを読み込ませるようになっていました。

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 6 件から 150%増加しています。本四半期は、延べ 2 組織に対応を依頼しました。

Web ページにアクセスした PC の環境情報を収集する、Scanbox とよばれる攻撃フレームワークの情報送信先に対して、国内組織の IP アドレスから通信が行われていることを 5 月初めごろ確認しました。調査したところ、アクセスのリファラ情報から、組織内部で使用するネットワーク装置の Web UI が改ざんされ、Scanbox のコードが埋め込まれた可能性があることが分かりました。

また、5 月半ばには、海外のセキュリティ組織から、マルウエアが感染端末から収集した情報を送信する先となっている、海外の C&C サーバと通信を行っていた国内 IP アドレスの情報を受領しました。

JPCERT/CC は、入手した情報をもとに、関連する国内組織に対して、該当する通信が発生していないか、事実関係を調査するよう依頼しました。

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、181 件でした。前四半期の 100 件から 81%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、1520 件でした。前四半期の 1654 件から 8%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。頻繁にスキャンの対象となったポートは、SMTP（25/TCP）、HTTP（80/TCP）、SSH（22/TCP）でした。

［表 4 ポート別のスキャン件数］

ポート	4 月	5 月	6 月	合計
25/tcp	219	289	270	778
80/tcp	107	82	76	265
22/tcp	47	58	58	163
23/tcp	34	29	51	114
53/udp	16	76	0	92
21/tcp	11	11	13	35
123/tcp	0	0	20	20
445/tcp	7	4	6	17
53413/udp	2	2	7	11
8080/tcp	4	2	2	8
443/tcp	2	6	0	8
3389/tcp	1	4	2	7
143/tcp	6	1	0	7
1433/tcp	3	3	0	6
51331/udp	1	2	2	5
81/tcp	1	0	3	4
53/tcp	0	4	0	4
3306/tcp	3	0	1	4
82/tcp	0	2	1	3
50943/udp	0	2	1	3
5060/udp	1	2	0	3
5001/tcp	0	0	3	3
その他	18	139	144	301

その他に分類されるインシデントの件数は、342 件でした。前四半期の 373 件から 8%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。

【個人利用のネットワーク接続ストレージとみられる匿名 FTP サーバ】
本四半期は、国内 ISP の回線で稼働している匿名 FTP サーバに関する報告を多数受領しました。通常の匿名 FTP サーバは公開を目的としていますが、報告が寄せられた FTP サーバは、IP アドレスの逆引き名やディレクトリ名の特徴などから、個人や企業が NAS（ネットワーク接続ストレージ）を意図せずに公開し、運用しているものと推測されました。また、これらの多くに、特定のファイル名が付けられた、不審な SCR ファイルや HTML ファイルなどが設置されており、マルウエアの設置場所として悪用されている可能性が考えられました。

JPCERT/CC は、念のため FTP サーバの状態が意図したものであるか、顧客に連絡していただくよう複数の通信事業者に依頼しました。その結果、FTP に接続できなくなったり、アクセスに認証がかけられたりするなど、対策が取られたと考えられる例が少数ながら確認されましたが、多くは状態に変化が見られませんでした。

【情報窃取マルウエア Pony によって窃取された認証情報】
4 月後半に、海外のセキュリティ組織から、マルウエア Pony によって窃取されたとみられる認証情報のデータを受領しました。Pony は、多くのツールやブラウザなどから認証情報を窃取する機能を持ったマルウエアであり、マルウエアが添付されたメールや改ざんされた Web サイトから、脆弱性を攻撃するサイトに誘導するドライブバイダウンロード攻撃によって感染する可能性があります。受領したデータには、Pony に感染したユーザの端末から窃取したと推測される、Web サービスや、メールサーバなどの認証情報が含まれていました。

JPCERT/CC は、受領したデータから国内の Web サービスやユーザが関連する認証情報を抽出し、各サービスを運用する企業に対して、マルウエアに感染したユーザの端末からサービスの認証情報が窃取された可能性がある旨を連絡しました。

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。