Japan Computer Emergency Response Team Coordination Center

JPCERT CC®

JPCERT-IR-2013-03

発行日: 2013-10-10

JPCERT/CC インシデント報告対応レポート
[2013 年 7 月 1 日 ～ 2013 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」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、2013 年 7 月 1 日から 2013 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及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 など)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)	4180	2779	3136	10095	9386
インシデント件数 （注 3）	3210	2279	2795	8284	9086
調整件数（注 4）	861	805	748	2414	2179

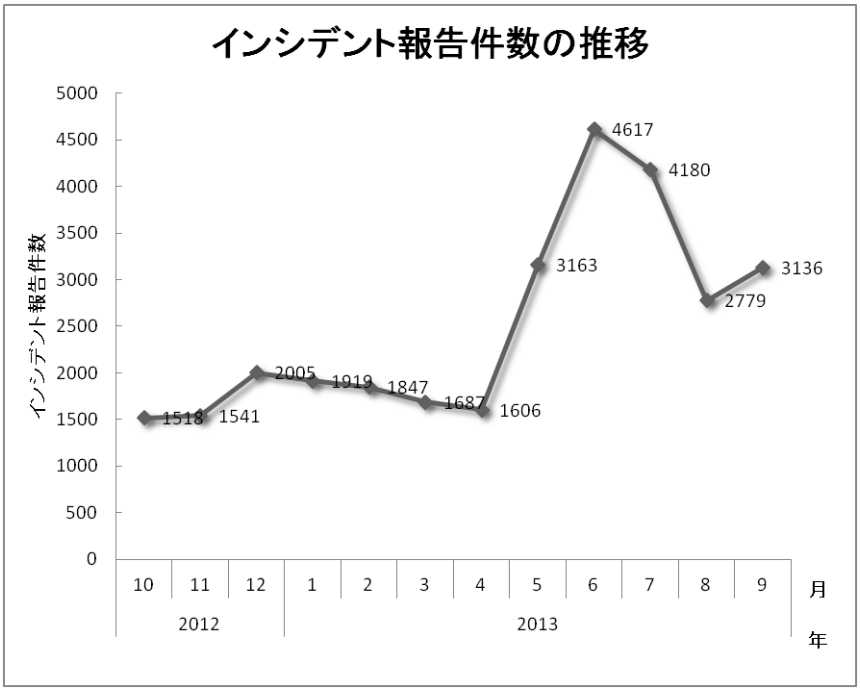
【注 2】「報告件数」は、報告者から寄せられた Web フォーム、メール、FAX による報告の総数を示します。

【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。

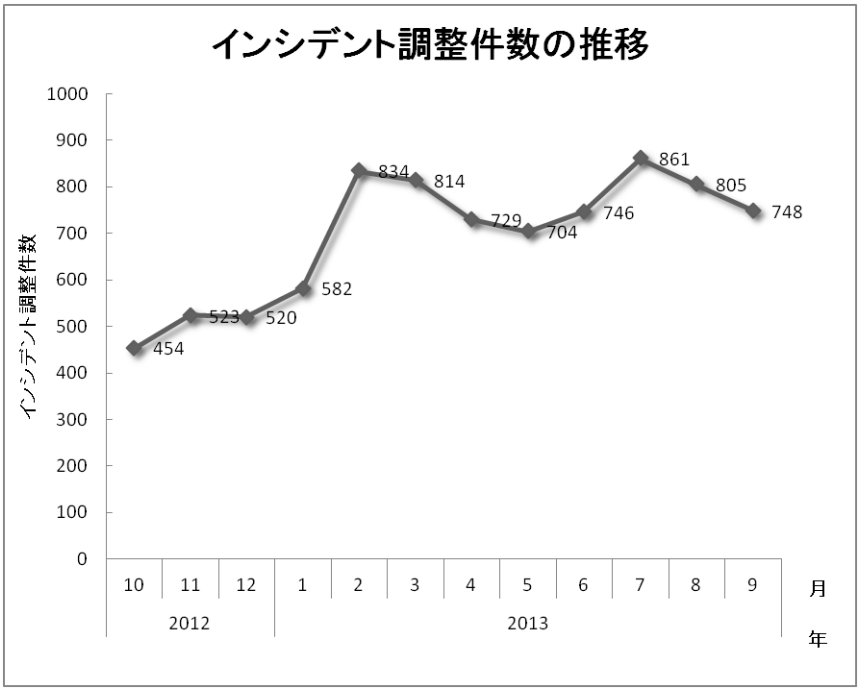
【注 4】「調整件数」とは、インシデントの拡大防止のため、サイトの管理者などに対し、現状の調査と問題解決のための対応を依頼した件数を示します。

本四半期に寄せられた報告件数は、10095 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 2414 件でした。前四半期と比較して、総報告件数は 8%増加し、調整件数は 11%増加しました。また、前年同期と比較すると、総報告数で 86%増加し、調整件数は 115%増加しました。

[図 1]～[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]



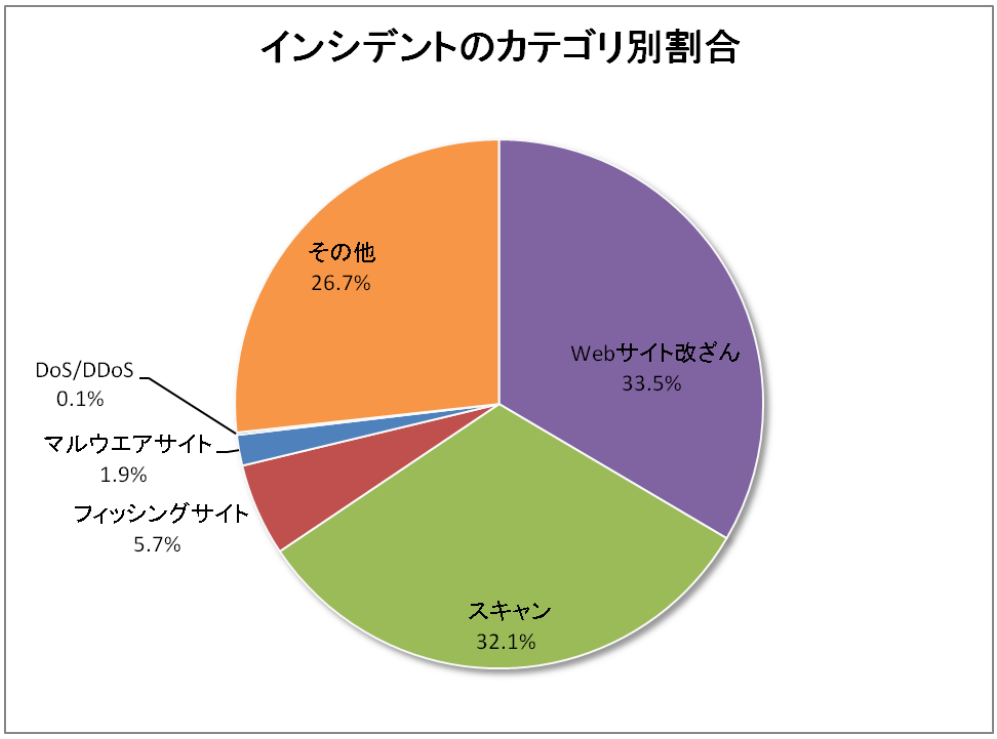
[図 2 インシデント調整件数の推移]

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、6.[付録]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 2 カテゴリ別インシデント件数]

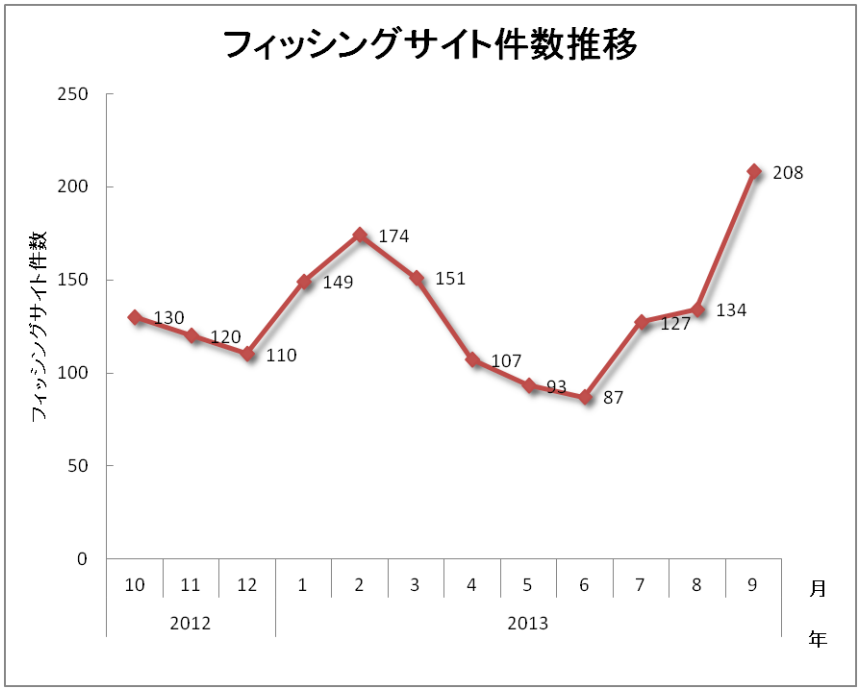
インシデントカテゴリ	7 月	8 月	9 月	合計	前四半期合計
フィッシングサイト	127	134	208	469	287
Web サイト改ざん	1106	687	981	2774	1847
マルウエアサイト	43	60	53	156	379
スキャン	1556	720	383	2659	4629
DoS/DDoS	12	0	0	12	71
制御システム	0	0	0	0	1
その他	366	678	1170	2214	1872

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。Web サイト改ざんに分類されるインシデントは 33.5%、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は 32.1%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 5.7%でした。

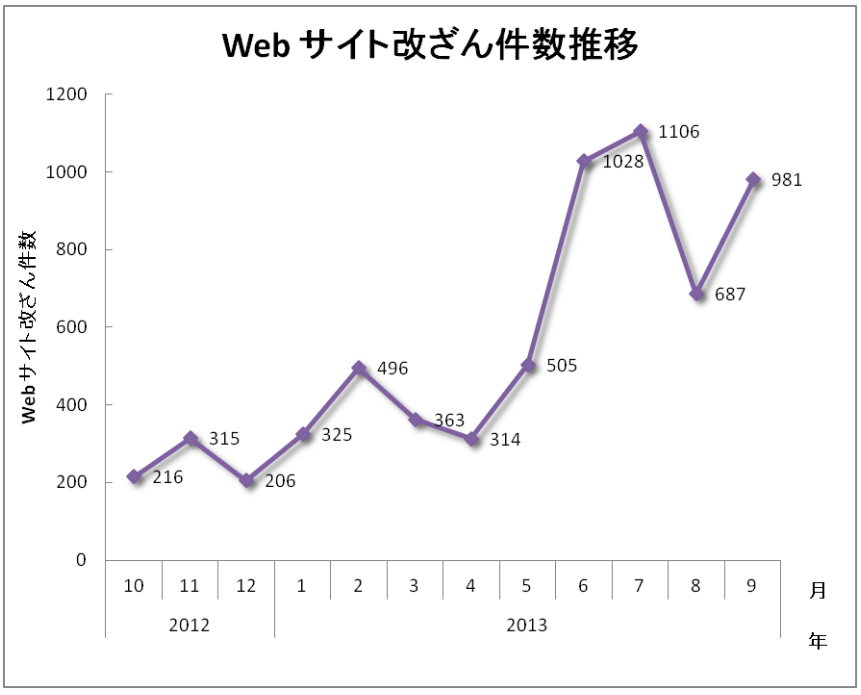


[図 4 インシデントのカテゴリ別割合]

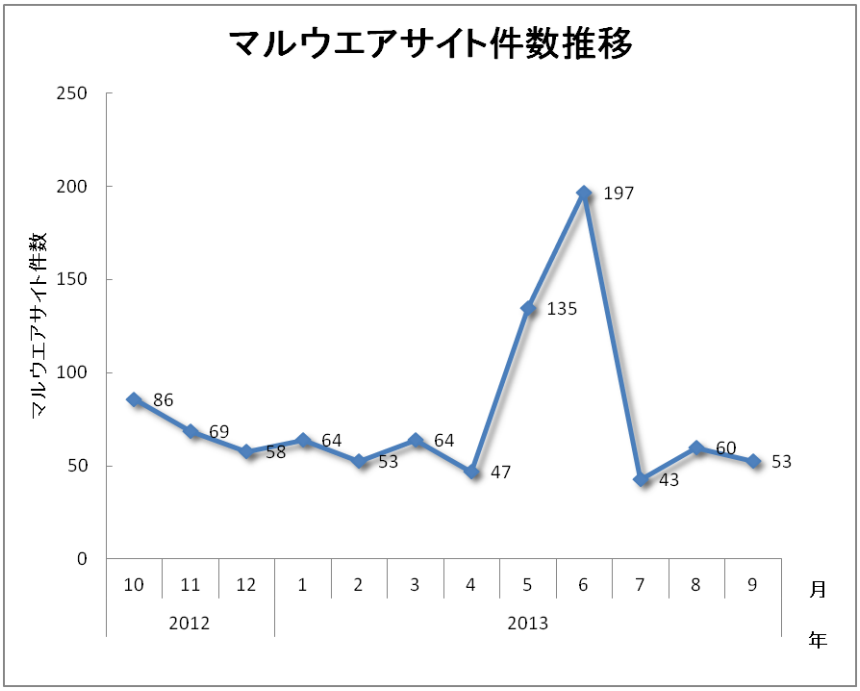
[図 5]から[図 8]に、フィッシングサイト、Web サイト改ざん、マルウエアサイト、スキャンのインシデントの過去 1 年間の月別推移を示します。



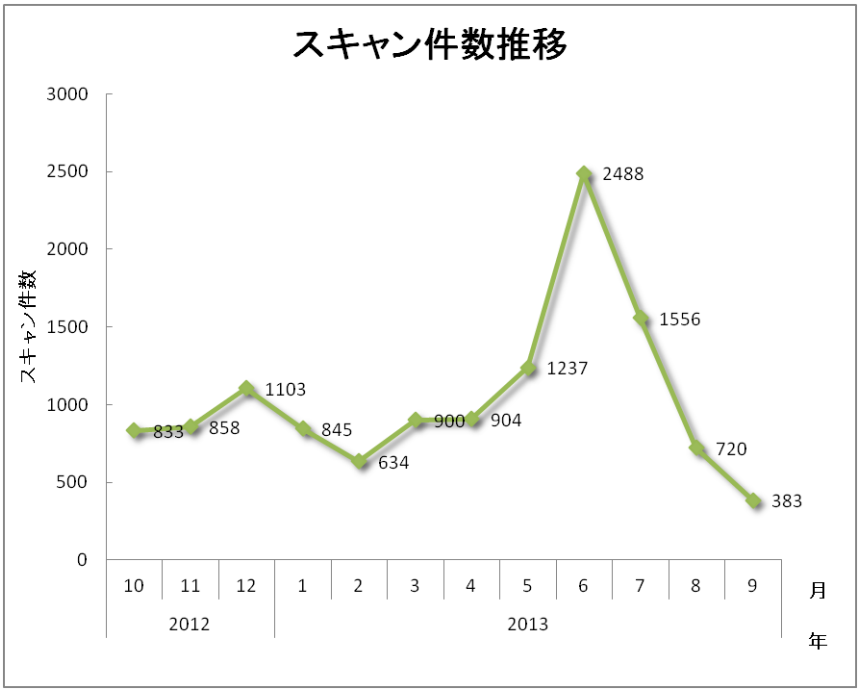
[図 5 フィッシングサイト件数推移]



[図 6 Web サイト改ざん件数推移]

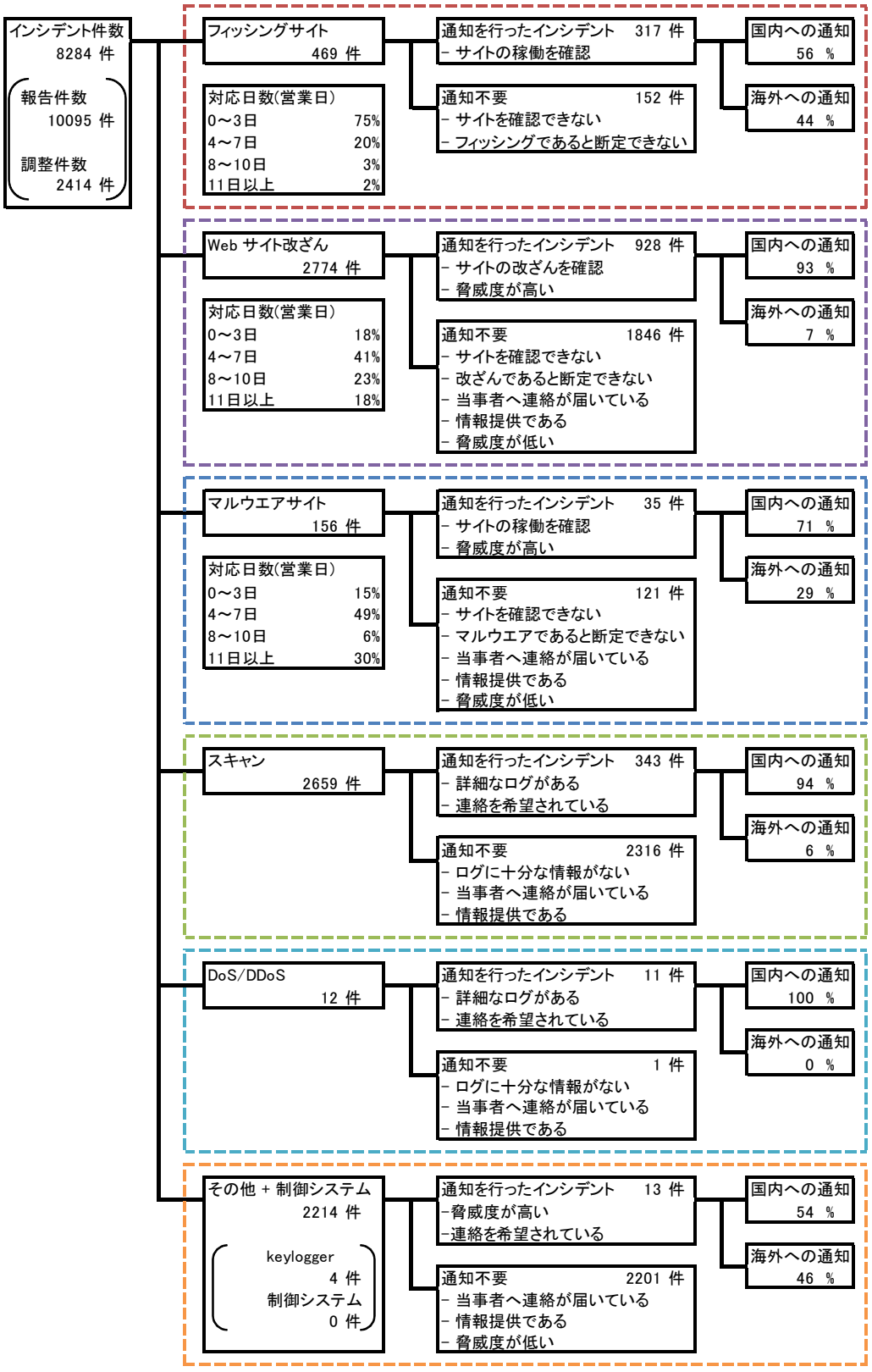


[図 7 マルウエアサイト件数推移]



[図 8 スキャン件数推移]

[図 9]にインシデントにおける調整・対応状況の内訳を示します。



[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

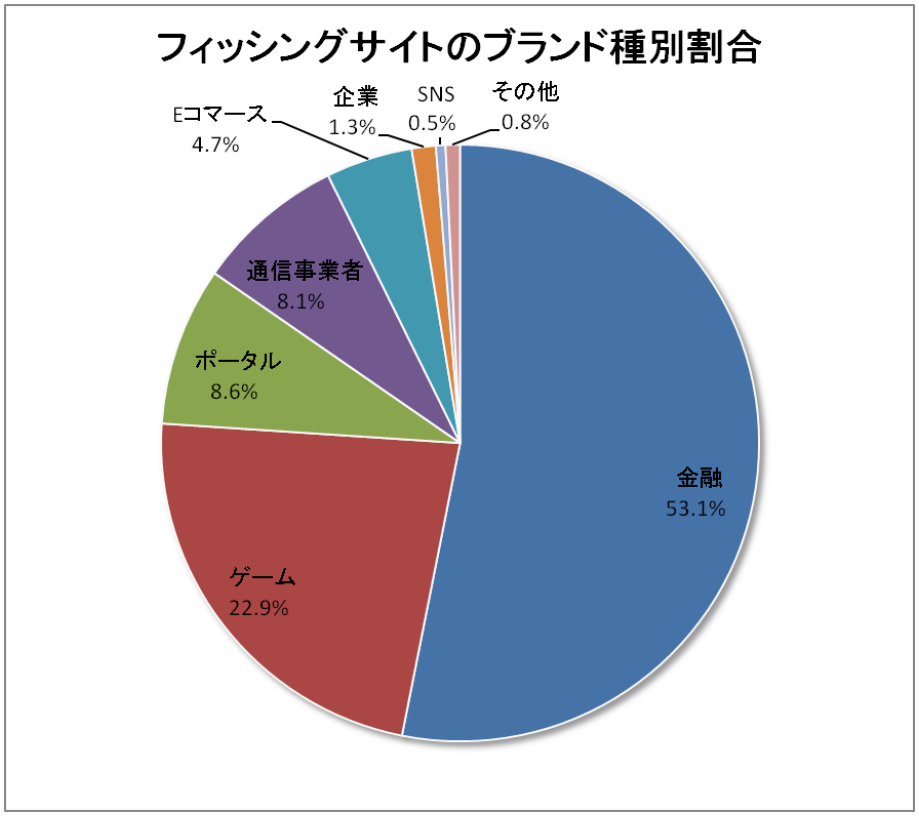
3.1. フィッシングサイトの傾向

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 469 件で、前四半期の 287 件から 63%増加しました。また、前年度同期(273 件)との比較では、72%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]、業界割合を[図 10]に示します。

[表 3 フィッシングサイトの国内・国外ブランド別の件数]

フィッシングサイト	7 月	8 月	9 月	合計 (割合)
国内ブランド	33	41	91	165(35%)
国外ブランド	73	68	78	219(47%)
ブランド不明(注 5)	21	25	39	85(18%)
月別合計	127	134	208	469(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などの理由により、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 165 件と、前四半期の 72 件から 129%増加しました。国外ブランドを装ったフィッシングサイトの件数は 219 件と、前四半期の 140 件から 56%増加しました。

JPCERT/CC で報告を受領したフィッシングサイト全体では、金融機関のサイトを装ったものが 53.1%、オンラインゲームサービスを装ったものが 22.9%を占めています。装われた国内ブランドの中ではオンラインゲームサービスが、また海外ブランドの中では金融機関が、それぞれ最も多数を占めました。

前四半期に引き続き、国内ゲーム会社のオンラインサービスを装ったフィッシングサイトの報告を多数受領しています。フィッシングサイトのドメイン名には、7 月から 8 月はブランド名を装った文字列やアルファベット 4 文字に.asia、 .pw、 .cc などのトップレベルドメインを組み合わせたものが多く使用され、9 月はアルファベット 1 文字か同じ文字 2 文字の後が kiki.com となっているものが多く使用されていました。国内ゲーム会社を装ったフィッシングサイトの中には、国内通信事業者が動的に割り当てる IP アドレスを持ち、しかも、IP アドレスを付与した通信事業者が複数あって時間とともに移動したものがありました。また、このような IP アドレスを持つ国内ゲーム会社を装ったフィッシングサイトと同じ IP アドレスで、海外のオンラインゲームサービスを装ったフィッシングサイトが存在していることも確認しています。

フィッシングサイトの調整先の割合は、国内が 56%、国外が 44%であり、前四半期(国内 54%、国外 46%)と比較して、国内への調整の割合が増えました。

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、2774 件でした。前四半期の 1847 件から 50%増加しています。

前四半期に引き続き、不審な iframe や難読化された JavaScript がページに挿入された Web サイトに関する報告が非常に多く寄せられています。改ざんされた Web サイトにアクセスすると、他の URL に誘導され、誘導先の php スクリプトによって、さらに複数のアプリケーションの脆弱性を使用した攻撃を行うサイトに誘導されることを確認しています。脆弱性が存在する古いバージョンの OS やアプリケーションがインストールされた PC が攻撃されると、マルウエアに感染して、PC に保存された様々な認証情報を窃取されたり、他のマルウエアをダウンロードされたりする可能性があります。改ざんの被害を受けた Web サイトの管理者から、不明な第三者による ftp の認証が記録されていたとの情報を複数いただいており、改ざんを許した一因として、Web サイトの管理に使用する PC が ftp などの認証情報を窃取するマルウエアに感染していたか、ftp のパスワードが容易に推測できるものであったなどの問題点が考えられます。

また、9 月中旬には、Web サイトに侵入したことを誇示することを目的とした、海外のハッカーグループによる改ざんの報告も多く寄せられました。

3.3.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、156 件でした。前四半期の 379 件から 59%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、2659 件でした。前四半期の 4629 件から 43%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 5]に示します。頻繁にスキャンの対象となったポートは、http(80/tcp)、smtp(25/tcp)、ssh(22/tcp)でした。前四半期の 6 月には WordPress のログイン画面に対するブルートフォース攻撃の報告が多数寄せられましたが、本四半期には同様の攻撃に関する報告の数が減少する傾向が見られました。

[表 4　ポート別のスキャン件数]

ポート	7 月	8 月	9 月	合計
80/tcp	1339	531	192	2062
25/tcp	169	158	170	497
22/tcp	26	34	28	88
3389/tcp	9	10	5	24
1433/tcp	4	5	3	12
5900/tcp	4	4	3	11
21/tcp	5	1	4	10
udp	4	1	1	6
445/tcp	4	0	1	5
143/tcp	3	0	1	4
23/tcp	2	1	1	4
8443/tcp	1	1	1	3
3306/tcp	0	0	2	2
icmp	1	0	0	1
135/tcp	0	1	0	1
443/tcp	0	0	1	1
4899/tcp	0	1	0	1
5901/tcp	0	0	1	1
65500/tcp	0	1	0	1
7822/tcp	1	0	0	1
8080/tcp	1	0	0	1
8880/tcp	0	0	1	1
不明	0	3	3	6
月別合計	1573	752	418	2743

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。

【金融系マルウエアが通信を行う国内サーバに関する対応】

2013 年 7 月はじめ、Citadel とよばれる金融系マルウエアの通信先となっている日本国内のサーバに関する報告が寄せられました。マルウエアは、侵入されたと見られる Web サーバ上の php スクリプトに対してリクエストを送信していました。Web サーバの管理者に連絡したところ、攻撃者によりサーバ上に設置されていた複数のファイルをご提供いただくことができました。設置されていたファイルには、マルウエアに感染したホストからのリクエストを受け取る php スクリプトのファイル、暗号化されているリクエストを復号する鍵などの情報を含む設定ファイル、リクエストに対して返されるバイナリのデータなどがありました。php スクリプトは、リクエストのサイズなどをチェックして、マルウエアからの通信である場合には暗号化されているリクエストを復号した後にデータを返し、マルウエアからの通信でなかった場合には 404 Not found と表示する仕組みになっていました。

【海外鉄道会社への DDoS 攻撃に使用された国内オープンリゾルバに関する対応】

2013 年 7 月末、海外のセキュリティ組織から、日本国内の複数の DNS サーバを悪用した DNS アンプ攻撃を鉄道会社が受けているという報告を受領しました。報告で指摘された DNS サーバを調査したところ、外部からの再帰問合せに対して返答するいわゆる「オープンリゾルバ」になっており、JPCERT/CC は DNS サーバを管理する組織に対応を依頼し、多くのサーバで外部からの問合せを受け付けないようにする対策が行われたことを確認しました。

【Web 広告の改ざんによるマルウエア配布に関する対応】

2013 年 8 月、国内サイトに掲載されている Web 広告のソースコードに、不正なスクリプトが埋め込まれているという報告を受領しました。報告された Web 広告を調査したところ、外部のサイトに誘導する JavaScript が埋め込まれており、アクセス元の IP アドレスが特定の国のものである場合には Java などの複数の脆弱性を使用した攻撃を行うサイトに誘導し、PC を情報の窃取を目的とするマルウエアに感染させる仕組みになっていました。JPCERT/CC から広告サービスを配信する海外の事業者に対応を依頼したところ、サーバに問題が発生していたことを確認し、対策を行ったとの返信を受領しました。

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 URL 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 URL 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おります。購読をご希望の方は、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、以下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など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など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などのサイトに似せた 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などにより悪意のあるスクリプトや iframe など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 など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など) 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無いもの) を指します。また、マルウエアなど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など)
- 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、ワームなど）による感染の試み (未遂に終わったもの)
- ssh,ftp,telnet など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など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。

- 大量の通信などにより、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 メールなど) を受信させることによるサービス妨害

○ 制御システム

「制御システム」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」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などを発生させる攻撃

○ その他

「その他」とは、上記に含まれないインシデントを指します。

JPCERT/CC では、たとえば、以下を「その他」に分類しています。

- 脆弱性などをついたシステムへの不正侵入
- ssh,ftp,telnet など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、ワームなど）の感染

本活動は、経済産業省より委託を受け、「平成２５年度情報セキュリティ対策推進事業」として実施したものです。