Japan Computer Emergency Response Team Coordination Center

JPCERT CC®

JPCERT-IR-2014-03
発行日: 2014-07-10

JPCERT/CC インシデント報告対応レポート
[2014 年 4 月 1 日 ～ 2014 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、2014 年 4 月 1 日から 2014 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)	1561	1447	1509	4517	4898
インシデント件数 (注 3)	1397	1401	1462	4260	4529
調整件数 (注 4)	726	565	843	2134	1989

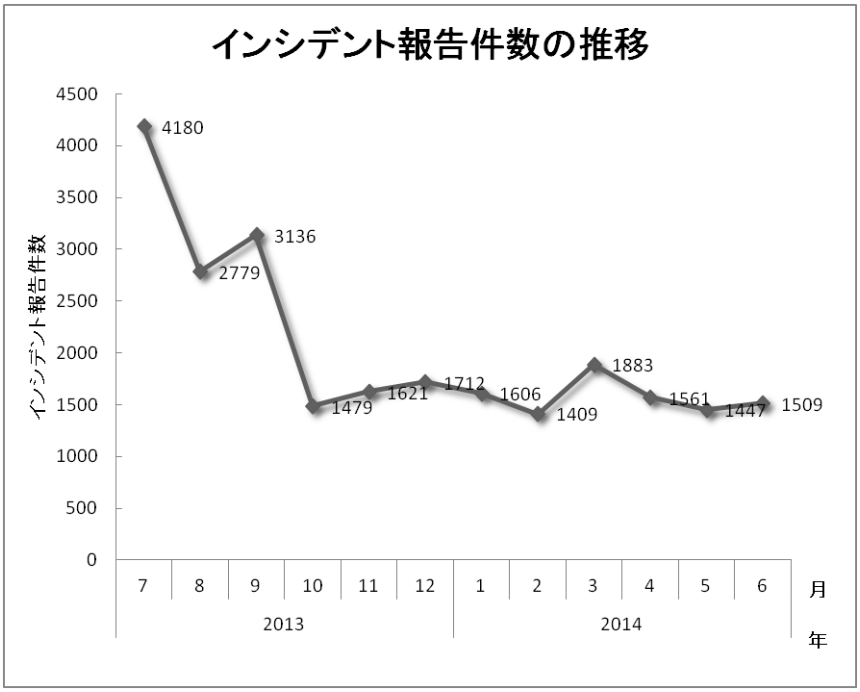
【注 2】「報告件数」は、報告者から寄せられた Web フォーム、メール、FAX による報告の総数を示します。

【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。

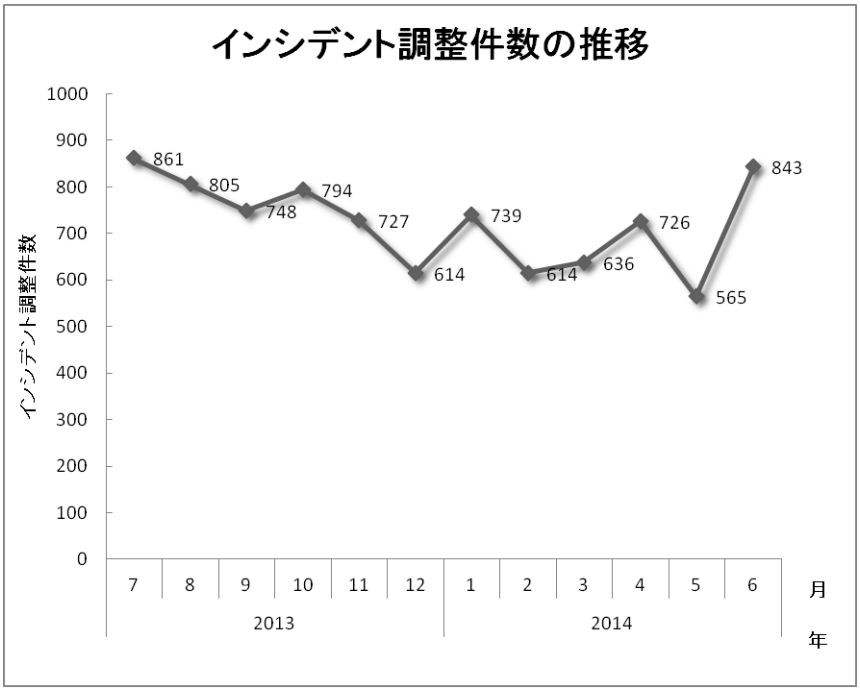
【注 4】「調整件数」は、インシデントの拡大防止のため、サイトの管理者等に対し、現状の調査と問題解決のための対応を依頼した件数を示します。

本四半期に寄せられた報告件数は、4517 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 2134 件でした。前四半期と比較して、総報告件数は 8%減少し、調整件数は 7%増加しました。また、前年同期と比較すると、総報告数で 52%減少し、調整件数は 2%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]



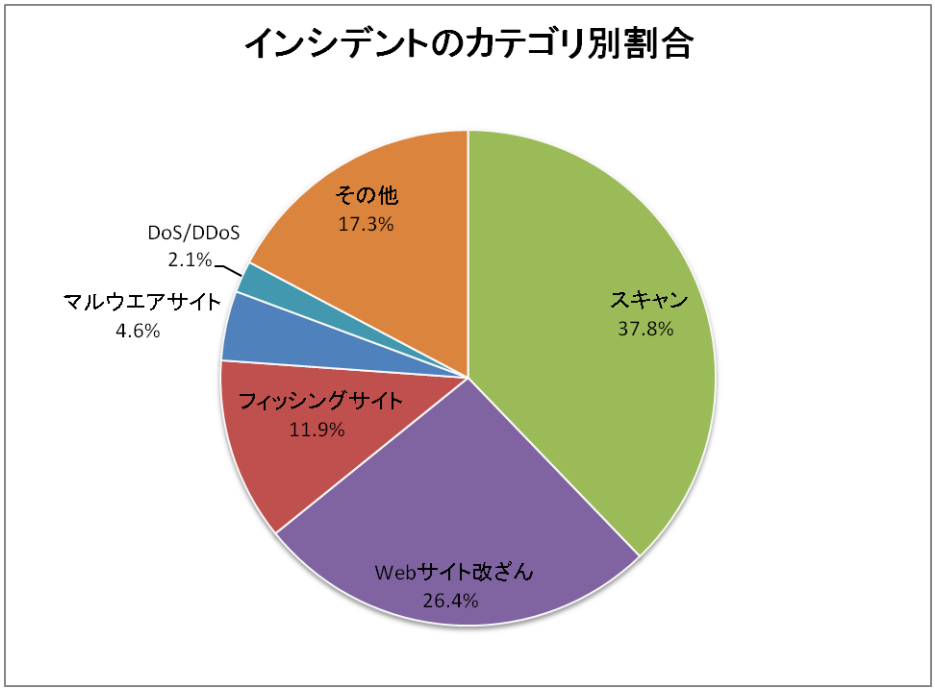
[図 2 インシデント調整件数の推移]

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]

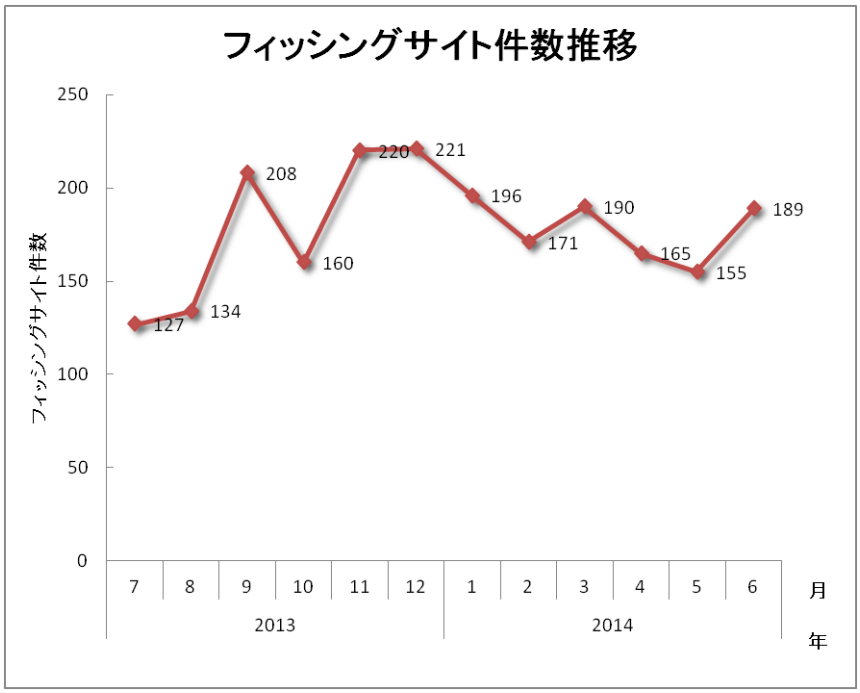
インシデントカテゴリ	4 月	5 月	6 月	合計	前四半期合計
フィッシングサイト	165	155	189	509	557
Web サイト改ざん	364	407	352	1123	1501
マルウエアサイト	63	72	59	194	211
スキャン	558	534	519	1611	1719
DoS/DDoS	50	33	5	88	23
制御システム関連	0	0	0	0	0
その他	197	200	338	735	518

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は 37.8%、Web サイト改ざんに分類されるインシデントは 26.4%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 11.9%でした。

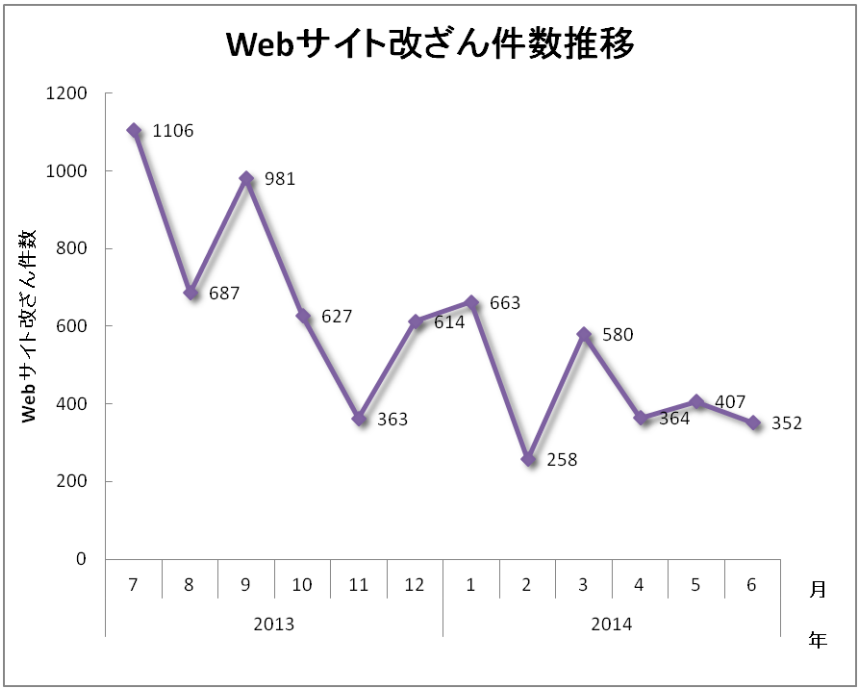


[図 3 インシデントのカテゴリ別割合]

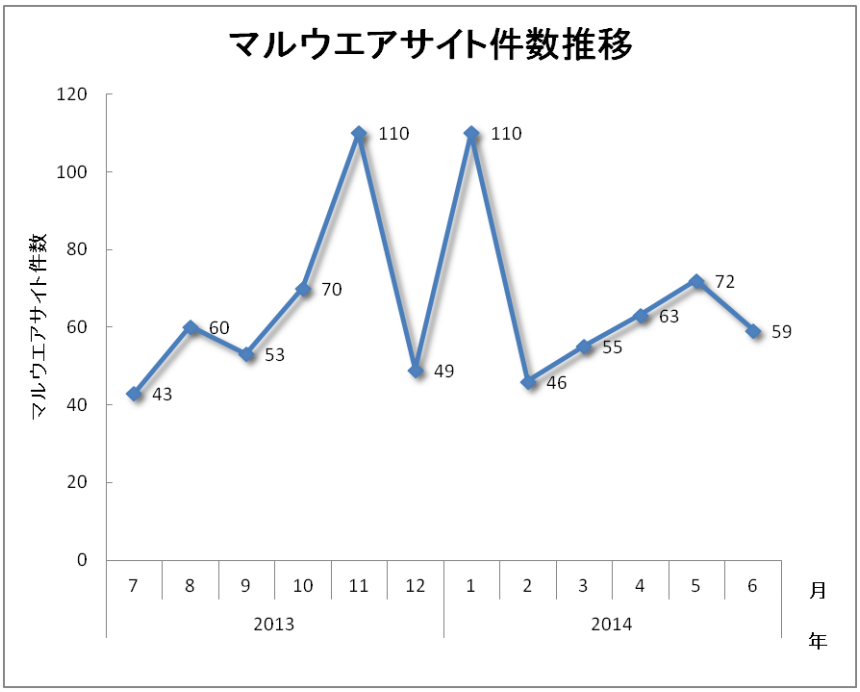
[図 4]から[図 7]に、フィッシングサイト、Web サイト改ざん、マルウエアサイト、スキャンのインシデントの過去 1 年間の月別推移を示します。



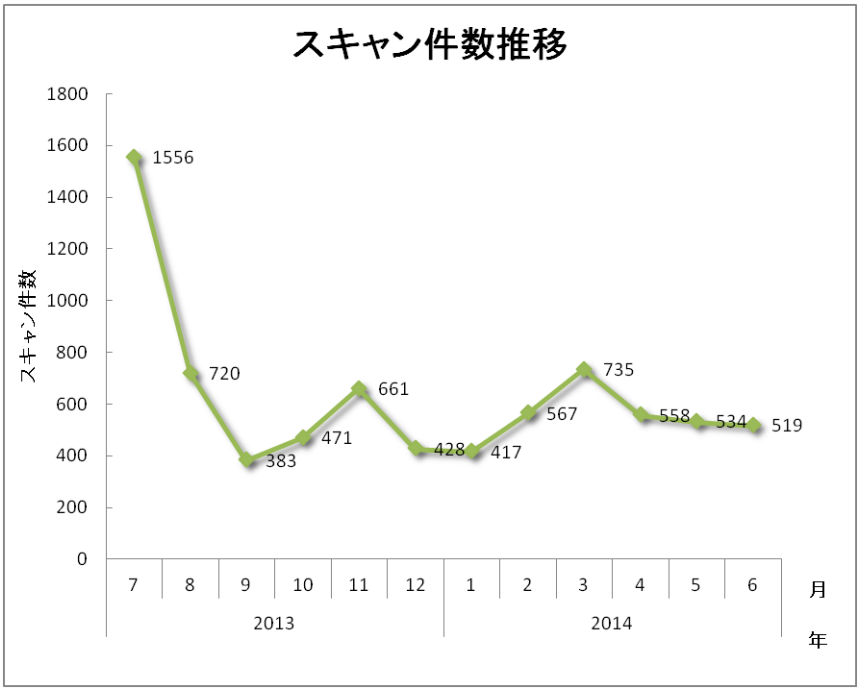
[図 4 フィッシングサイト件数推移]



[図 5 Web サイト改ざん件数推移]

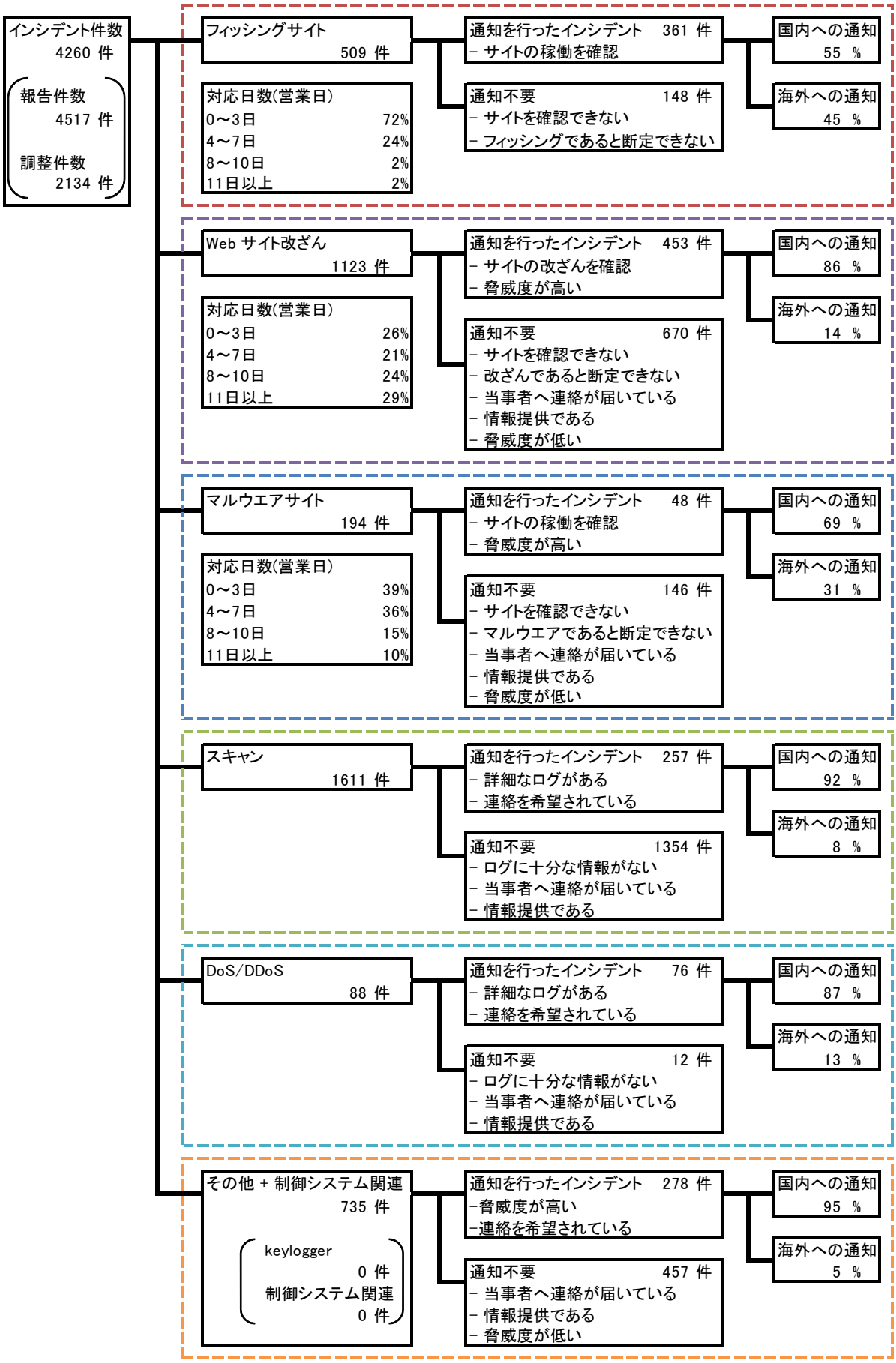


[図 6 マルウエアサイト件数推移]



[図 7 スキャン件数推移]

[図 8]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 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

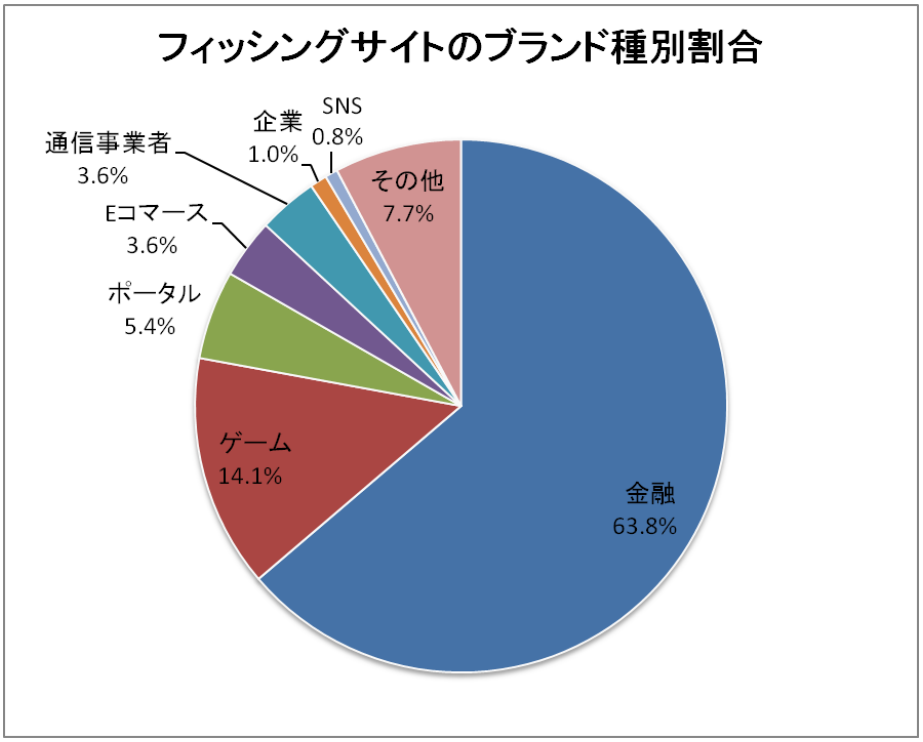
3.1. フィッシングサイトの傾向

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 509 件で、前四半期の 557 件から 9%減少しました。また、前年度同期(287 件)との比較では、77%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]、業界割合を[図 9]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	4 月	5 月	6 月	国内外別合計（割合）
国内ブランド	50	36	81	167(33%)
国外ブランド	71	79	76	226(44%)
ブランド不明(注 5)	44	40	32	116(23%)
月別合計	165	155	189	509(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 167 件と、前四半期の 229 件から 27%減少しました。国外ブランドを装ったフィッシングサイトの件数は 226 件と、前四半期の 187 件から 21%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 63.8%、オンラインゲームサービスを装ったものが 14%を占めています。装われたブランドは、国内ブランド、海外ブランドともに金融機関が最も多数を占めました。

6 月半ば頃から、国内金融機関を装ったフィッシングサイトが増加しています。フィッシングの仕組みは以前から確認されているものと同様に、転送設定が埋め込まれたページを不正に設置されたと見られる海外の Web サイトから、国内通信事業者が動的に割り当てる IP アドレスを持ったフィッシングサイトに誘導されるようになっていました。フィッシングサイトは”英字 3 文字.co.in”というドメインを持っており、ドメイン登録者のメールアドレスなどの情報が一致しているという共通性がありました。また、一つの IP アドレスのホストに、3 種類の国内金融機関のフィッシングサイトが併存している事例を確認しました。

国内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の報告も、非常に多く受領しています。オンラインゲームのフィッシングサイトには、.tk、.co.vu といった無料のドメインや、.pw ドメインを使用しているという特徴がありました。.tk ドメインのフィッシングサイトは、他のドメインに置かれたフィッシングサイトの本体をフレームを使用して表示し、フィッシングメールには.tk ドメインの URL を記載していました。これは、本体となるサイトをブロックリストに登録され難くするための方策と考えられます。

フィッシングサイトの調整先の割合は、国内が 55%、国外が 45%であり、前四半期(国内 43%、国外 57%)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、1123 件でした。前四半期の 1501 件から 25%減少しています。

4 月初め頃、古いバージョンの Movable Type を使用している国内企業の Web サイトが改ざんされたという報告を複数受領しました。これらのサイトでは、Web ページが読み込む JavaScript ファイルが改ざんされ、外部の Web サイトに誘導する iframe を挿入するコードが埋め込まれていました。誘導先の Web サイトでは、攻撃者によって設置されたと見られる php スクリプトによって、複数のアプリケーションの脆弱性を攻撃するサイトに転送される仕組みになっていました。JPCERT/CC は、被害拡大の防止を目的として、5 月 15 日に旧バージョンの Movable Type の利用に関する注意喚起を公開しました。

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、194 件でした。前四半期の 211 件から 8%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、1611 件でした。前四半期の 1719 件から 6%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	264	301	162	727
80/tcp	256	168	268	692
22/tcp	57	52	34	143
123/udp	0	10	27	37
53/udp	0	1	32	33
21/tcp	2	9	8	19
443/tcp	11	3	2	16
5000/tcp	15	0	0	15
3389/tcp	3	5	5	13
1433/tcp	0	9	3	12
5060/udp	2	3	5	10
23/tcp	3	4	1	8
5900/tcp	1	1	1	3
445/tcp	0	2	1	3
143/tcp	2	1	0	3
7778/tcp	1	0	1	2
3306/tcp	1	1	0	2
110/tcp	1	1	0	2
icmp	0	0	1	1
19/udp	0	1	0	1
137/udp	0	0	1	1
その他/tcp	3	5	1	9
不明	28	4	4	36
月別合計	650	581	557	1788

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。

【Chargen プロトコルを使用した DDoS 攻撃の踏み台にされた国内ホストに関する対応】
2014 年 3 月末に、海外組織より、日本国内の複数のホストが Chargen プロトコルを使用した DDoS 攻撃の踏み台になっていたという報告を受領しました。Chargen はポート(通常 19/udp)への接続に対して文字列を出力する、通信の確認などの目的で使用されるプロトコルですが、UDP は通信のセッションが確立されないため、IP アドレスを偽装して攻撃対象にパケットを送りつける反射攻撃に悪用されることがあります。

JPCERT/CC は、攻撃元となっていた IP アドレスを管理する通信事業者に事実関係の確認を依頼したところ、攻撃元となっていた端末は Windows XP を使用しており、簡易 TCP/IP サービスがインストールされていたために意図せず Chargen が有効になっていた可能性があることが分かり、無効化する対策を講じていただきました。

【金融系ボットネットの国内ノードに関する対応】
2014 年 4 月初めに、海外のセキュリティ組織から、金融系マルウエア Gameover Zeus のボットネットにおいて C&C サーバの役割を持つ国内ノードの情報を受領しました。C&C サーバとボットで形成される一般的なボットネットと異なり、Gameover Zeus のボットネットは、相互に P2P 接続する複数のボットから形成されており、P2P ネットワークの中でスーパーノードとも呼ばれる一部のボットが C&C サーバの役割を持つ、テイクダウンされにくい仕組みで管理されています。

JPCERT/CC は、ノードとなっていた国内ホストの IP アドレスを管理する通信事業者に対応を依頼し、結果として、報告元より国内ホストがボットネットから切り離されたことを確認したとの連絡を受けました。

【4 月末に修正された Adobe Flash Player の脆弱性を攻撃するサイトに関する対応】
2014 年 5 月末に、特定の国内サイトに見せかけたドメインを持つ不審な Web サイトの情報を受領しました。Web サイトを分析したところ、サイトにアクセスすると、PC にインストールされた Adobe Flash Player のバージョンが古い場合、2014 年 4 月末に修正された脆弱性(APSB14-13)を使用した攻撃が実行され、外部のサイトからマルウエアがダウンロードされることを確認しました。

JPCERT/CC は、脆弱性を攻撃するサイトおよびマルウエアを配布するサイトのネットワーク管理組織に対応を依頼し、これらのサイトが停止したことを確認しました。

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、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

○ 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、例えば、以下を「その他」に分類しています。

- 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２６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。