JPCERT-IR-2014-04
発行日: 2014-10-09

JPCERT/CC インシデント報告対応レポート
[2014 年 7 月 1 日 ～ 2014 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、2014 年 7 月 1 日から 2014 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]

	7 月	8 月	9 月	合計	前四半期合計
報告件数 (注 2)	1494	1347	1797	4638	4517
インシデント件数 (注 3)	1474	1203	1711	4388	4260
調整件数 (注 4)	745	550	830	2125	2134

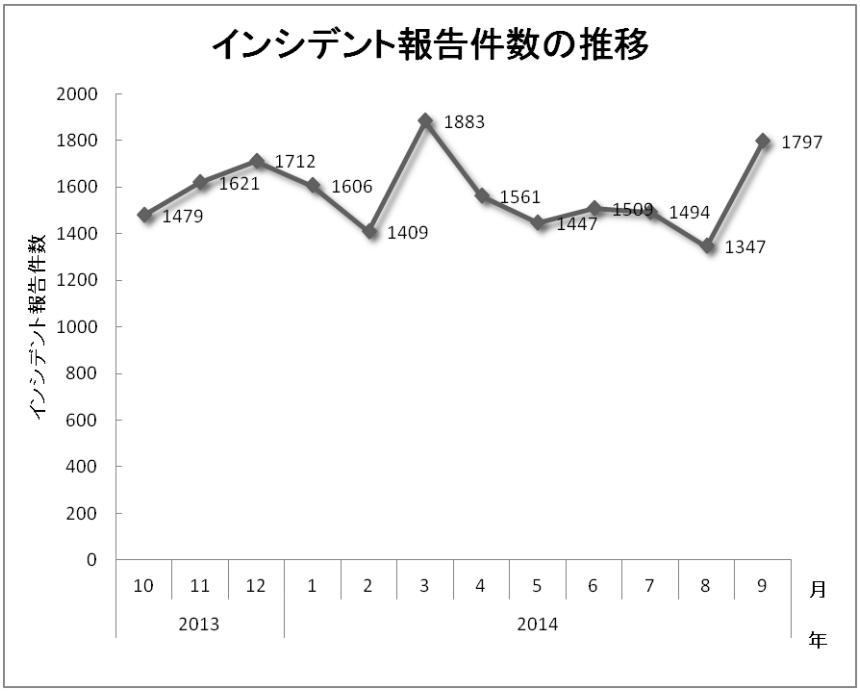
【注 2】「報告件数」は、報告者から寄せられた Web フォーム、メール、FAX による報告の総数を示します。

【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。

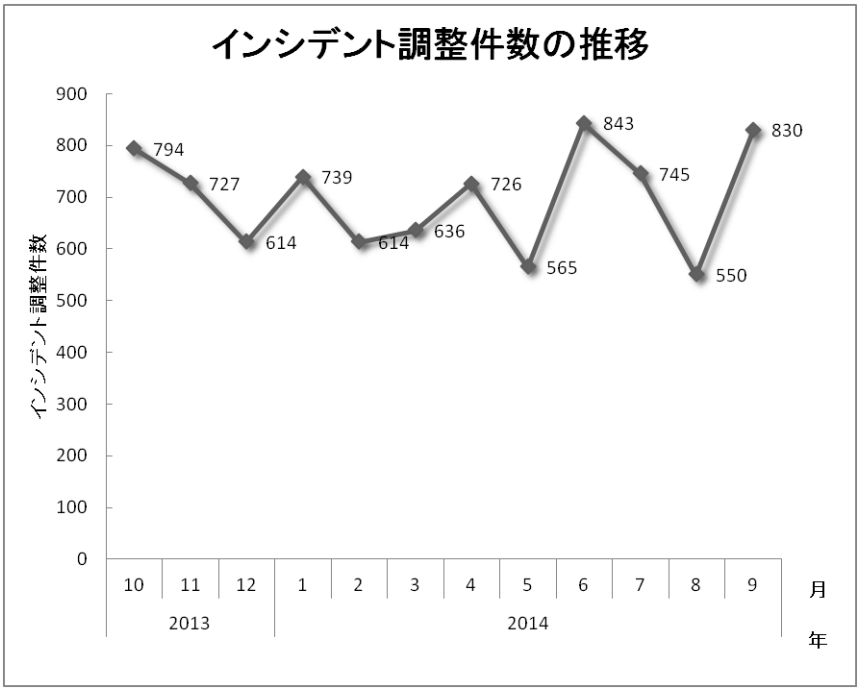
【注 4】「調整件数」は、インシデントの拡大防止のため、サイトの管理者等に対し、現状の調査と問題解決のための対応を依頼した件数を示します。

本四半期に寄せられた報告件数は、4638 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 2125 件でした。前四半期と比較して、総報告件数は 3%増加し、調整件数は 0.4%減少しました。また、前年同期と比較すると、総報告数で 54%減少し、調整件数は 12%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]



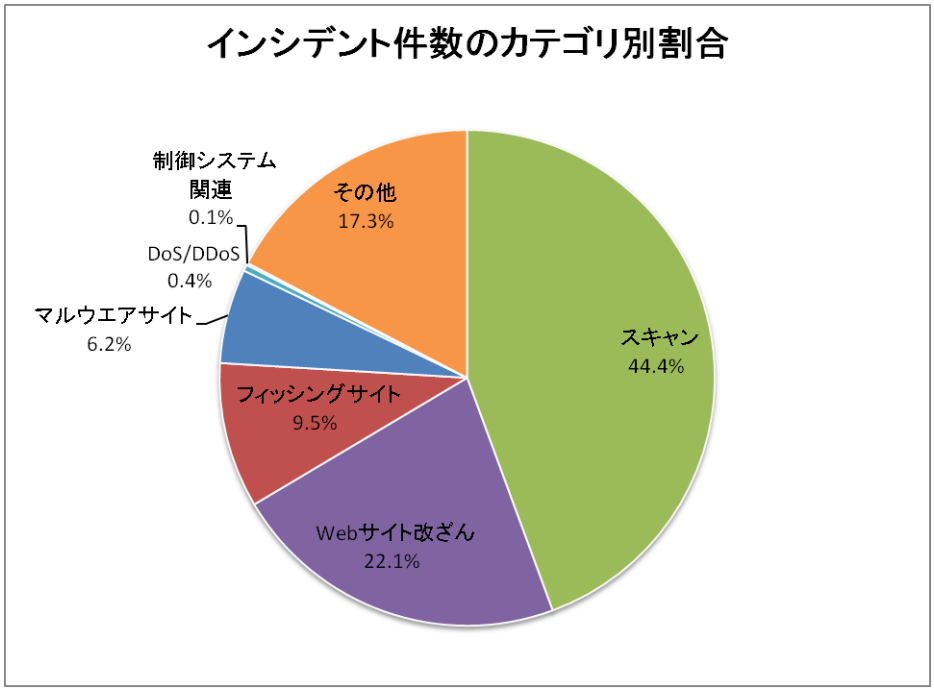
[図 2 インシデント調整件数の推移]

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]

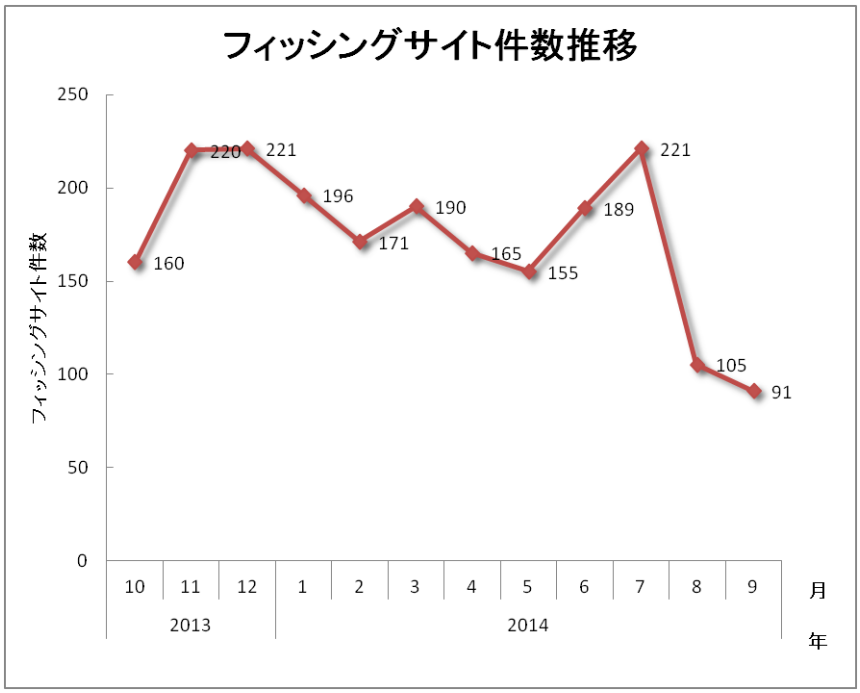
インシデントカテゴリ	7 月	8 月	9 月	合計	前四半期合計
フィッシングサイト	221	105	91	417	509
Web サイト改ざん	388	187	393	968	1123
マルウエアサイト	76	123	72	271	194
スキャン	636	563	749	1948	1611
DoS/DDoS	7	0	11	18	88
制御システム関連	0	0	6	6	0
その他	146	225	389	760	735

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 44.4%、Web サイト改ざんに分類されるインシデントは 22.1%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 9.5%でした。

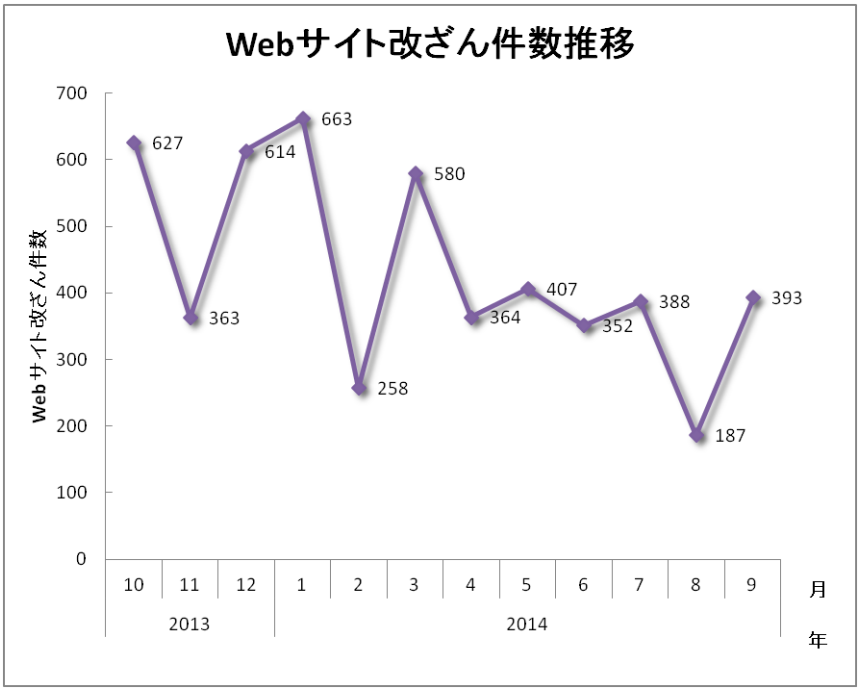


[図 3 インシデントのカテゴリ別割合]

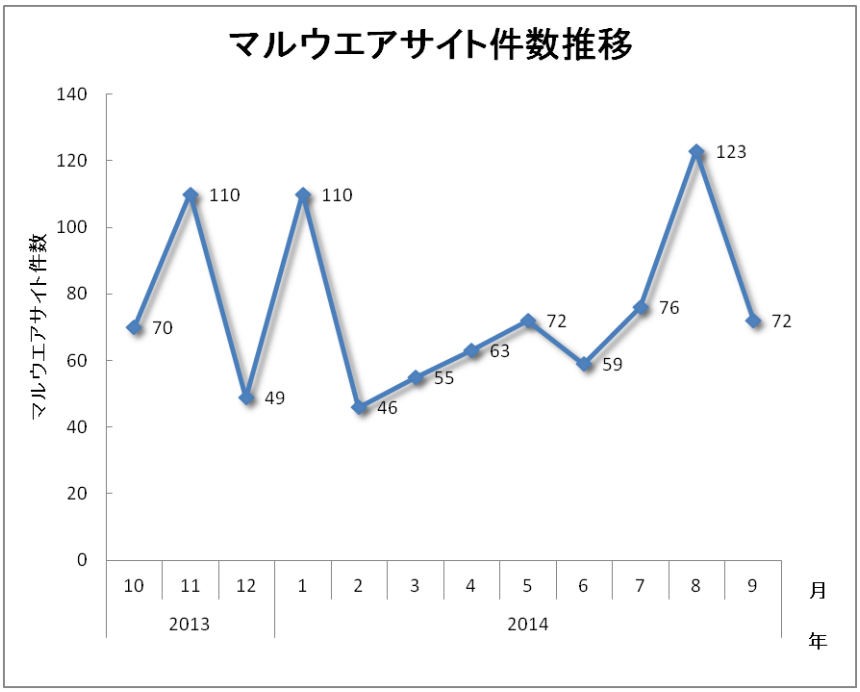
[図 4]から[図 7]に、フィッシングサイト、Web サイト改ざん、マルウエアサイト、スキャンのインシデントの過去 1 年間の月別推移を示します。



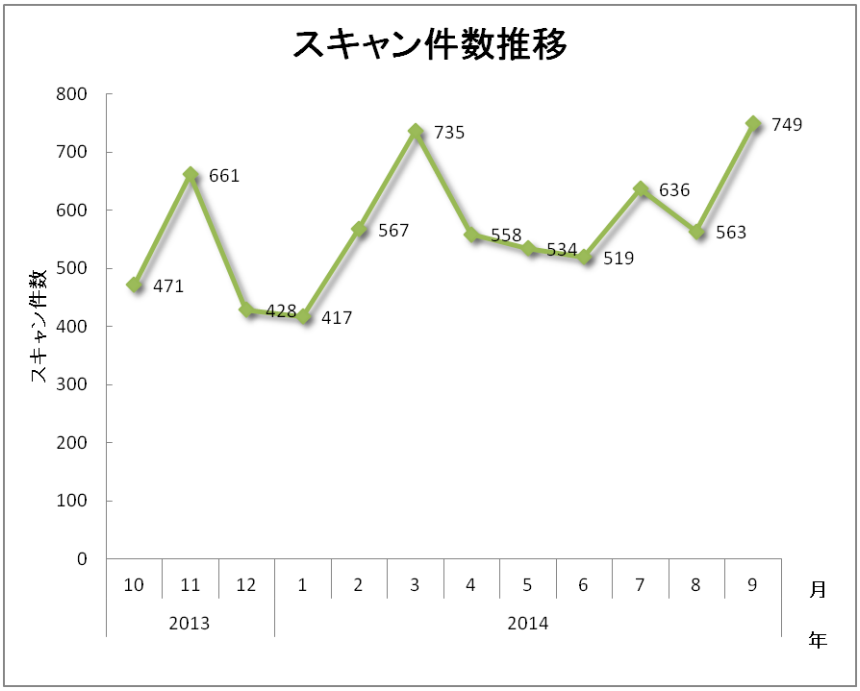
[図 4 フィッシングサイト件数推移]



[図 5 Web サイト改ざん件数推移]

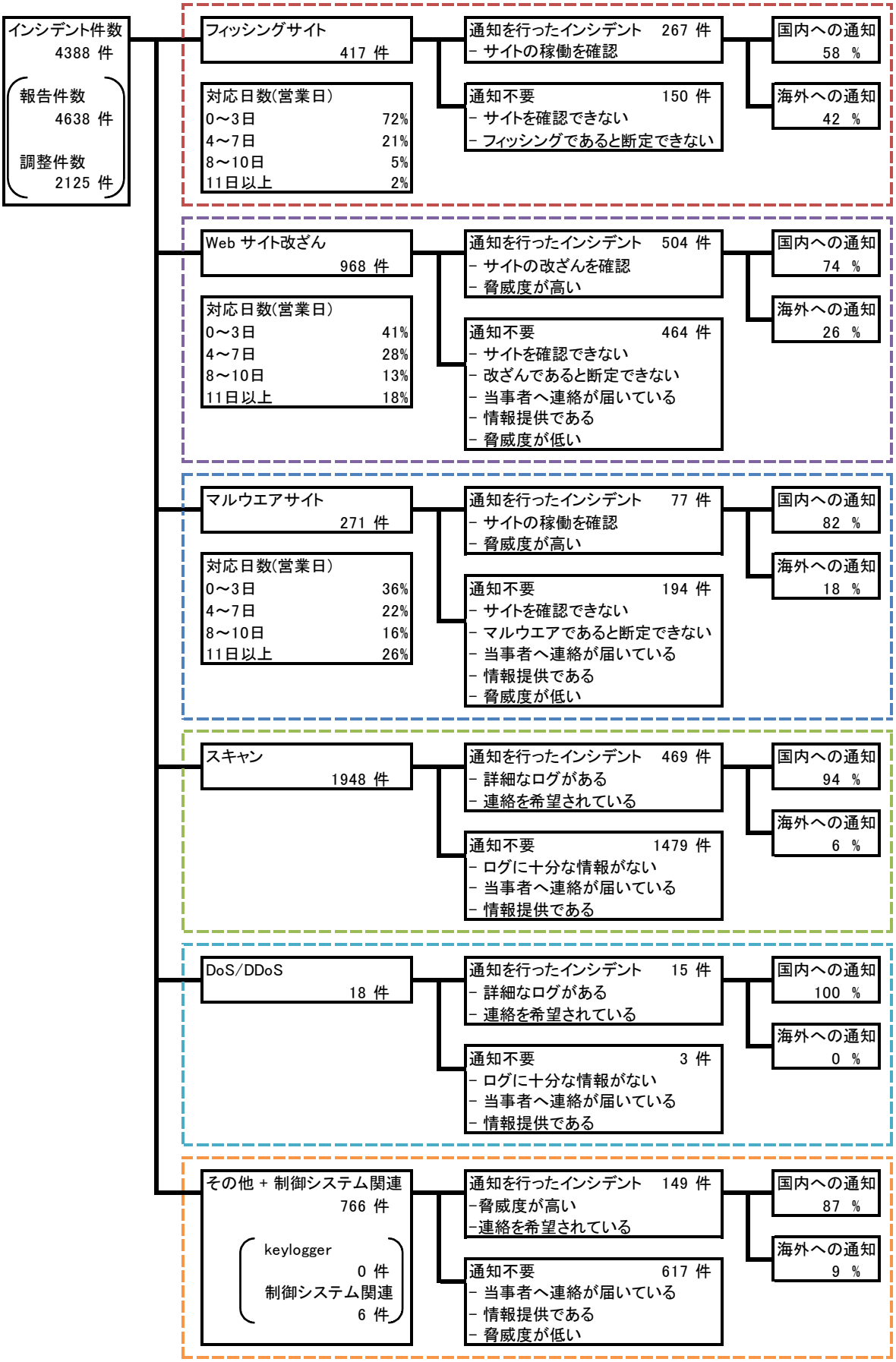


[図 6 マルウエアサイト件数推移]



[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

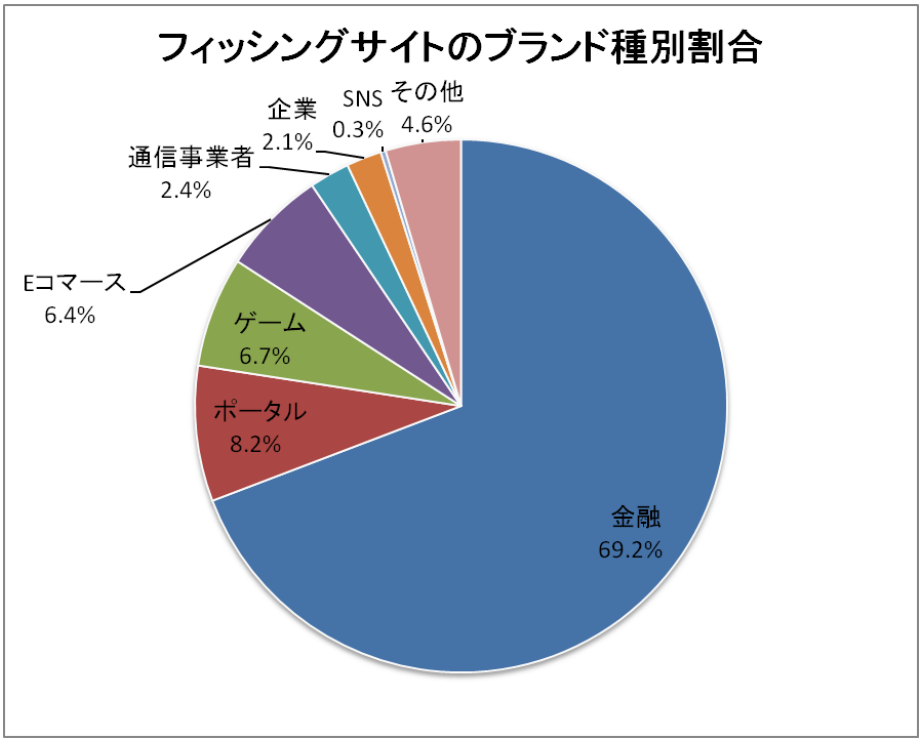
3.1. フィッシングサイトの傾向

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 417 件で、前四半期の 509 件から 18%減少しました。また、前年度同期(469 件)との比較では、11%の減少となりました。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	7 月	8 月	9 月	国内外別合計（割合）
国内ブランド	99	26	14	139(33%)
国外ブランド	73	63	53	189(45%)
ブランド不明(注 5)	49	16	24	89(21%)
月別合計	221	105	91	417(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 139 件と、前四半期の 167 件から 17%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 189 件と、前四半期の 226 件から 16%減少しました。

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 69.2 %、オンラインゲームサービスを装ったものが 6.7%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。

国内金融機関を装ったフィッシングサイトは、発生時期にかたよりがあり、7 月と 9 月後半には、不正にファイルを設置されたと見られる海外のサイトから、国内通信事業者の IP アドレスが割り当てられたフィッシングサイトに誘導される例を多数確認しましたが、8 月から 9 月前半にかけては、わずかな報告があるのみでした。

7 月から 8 月にかけて、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が多く寄せられていましたが、9 月以降は報告が大幅に減少しました。

また、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の報告を複数受領しています。このようなフィッシングサイトは、Web メールの認証情報を窃取し、スパムメールやフィッシングメールを送信することを目的としていると考えられます。

フィッシングサイトの調整先の割合は、国内が 58%、国外が 42%であり、前四半期(国内 55%、国外 45%)に比べ、国内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、968 件でした。前四半期の 1123 件から 14%減少しています。

8 月末ごろから、不正な JavaScript が埋め込まれた Web ページに関する報告が多く寄せられています。不正な JavaScript には、以前から確認されている改ざんと同様に、script タグに 6 桁の 16 進数を含むコメントタグがついているという特徴がありました。JavaScript から誘導される先の URL には複数のパターンがあるため、異なる種類の改ざんが複数発生している可能性が考えられます。最終的に誘導される先のサイトでは、PC のアプリケーションの脆弱性を攻撃されて、マルウエアのダウンロードおよび実行が行われることを確認しています。

JPCERT/CC では、Web サイト改ざんが継続的に発生している現状を受けて、8 月に注意喚起「ウェブサイトの改ざん回避のために早急な対策を」を発行しました。

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、271 件でした。前四半期の 194 件から 40%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、1948 件でした。前四半期の 1611 件から 21%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、http(80/tcp)、smtp(25/tcp)、dns(53/udp)でした。

[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	265	322	323	910
25/tcp	281	137	210	628
53/udp	62	52	172	286
22/tcp	57	47	38	142
16358/udp	0	7	18	25
61222/udp	0	5	16	21
21/tcp	7	6	7	20
2632/udp	0	7	11	18
31385/udp	0	6	11	17
3389/tcp	4	5	4	13
445/tcp	3	4	2	9
23/tcp	3	3	2	8
1433/tcp	1	0	2	3
143/tcp	1	0	2	3
icmp	2	0	0	2
7778/tcp	2	0	0	2
5900/tcp	2	0	0	2
5000/tcp	1	1	0	2
443/tcp	2	0	0	2
110/tcp	1	0	1	2
その他/tcp	0	1	4	5
その他/udp	1	0	6	7
不明	1	3	27	31
月別合計	696	606	856	2158

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。

【海外 HTTP プロキシサイトに関する対応】
2014 年 7 月上旬ごろ、複数の国内組織から、自組織の Web サイトを模倣したサイトが公開されており、認証情報を窃取しようとしている可能性があるとの報告を受領しました。これらのサイトの FQDN は、いずれも正規サイトの FQDN に共通のサフィックス・ドメインを追加した形式で、Web プロキシによって実現されていると見られるものでした。

プロキシと見られる Web サイトの管理者に当該サイトの意図を確認したところ、当該サイトは Web フィルタリングの回避や閲覧元の秘匿を目的として運用されていてフィッシングサイトではなく、サイトの所有者から要請があればプロキシの対象から除外するとの回答をいただきました。JPCERT/CC は、報告元に対してサイト管理者の意図を伝え、要請すればプロキシ対象から除外される旨を案内しました。

【.co.vu ドメインのフィッシングサイトに関する対応】
2014 年 7 月前半、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において、無料で登録できる.co.vu ドメインが大量に使用されていました。.vu ドメインはバヌアツ共和国に割り当てられたトップレベルドメインであるため、JPCERT/CC は太平洋諸島を管轄する CSIRT である PacCERT に.vu ドメインが悪用されていることを連絡し対処を要請しました。その後、フィッシングサイトに使用されていた.co.vu ドメインがすべて停止したことを確認しました。

それ以後にも、8 月初頭には.cu.cc ドメイン、8 月中旬には.pw ドメインで同様のフィッシングサイトが見つかりましたが、8 月後半までに消滅したことを確認しています。

【ボットネットの C&C サーバから発見された日本国内のボットの情報】
2014 年 7 月下旬に、クロアチアの National CSIRT から、国内 IP アドレスのボットに関する報告を受領しました。報告元によると、ボットネットの C&C サーバから発見されたボットの情報を調査したところ、ボットの多くが日本に割り当てられた IP アドレス範囲のものであったとのことでした。

JPCERT/CC では、報告元から提供されたボットの通信ログをもとに、ボットとなっていたホストの IP アドレスを所有する組織に、当該ホストにおいて不審な通信やマルウエア感染などが発生していないか事実関係の確認を依頼しました。その結果、複数の通知先組織から、ログと一致する通信の発生や、既にマルウエア感染を確認していたという返信をいただきました。

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。