JPCERT/CC®

JPCERT-IR-2014-01
発行日: 2014-01-16

JPCERT/CC インシデント報告対応レポート
[2013 年 10 月 1 日 ～ 2013 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、2013 年 10 月 1 日から 2013 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)	1479	1621	1712	4812	10095
インシデント件数 （注 3）	1456	1772	1560	4788	8284
調整件数（注 4）	794	727	614	2135	2414

【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。

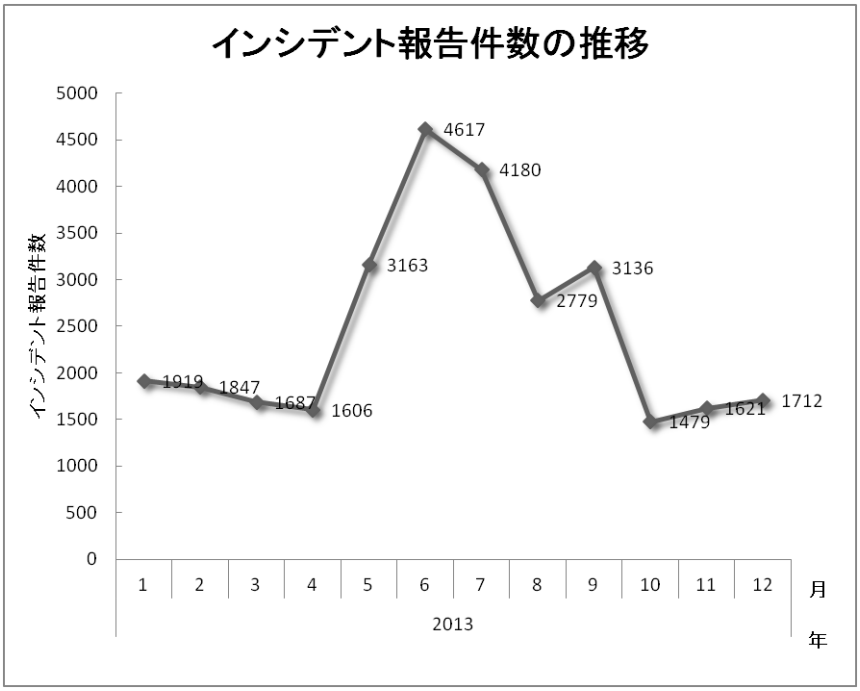
【注 3】「インシデント件数」は、各報告に含まれるインシデント件数の合計を示します。1 つのイン

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。

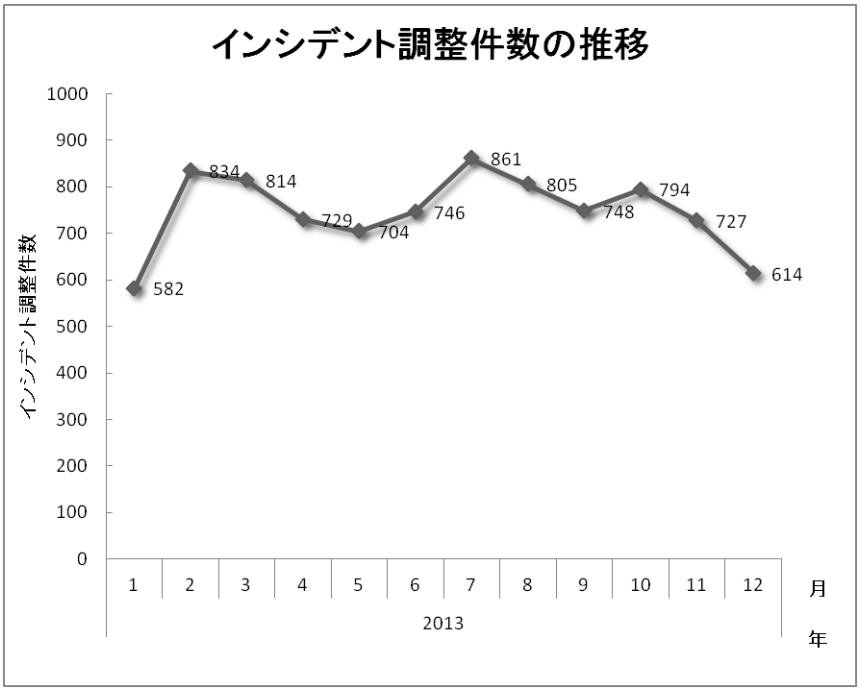
【注 4】「調整件数」は、インシデントの拡大防止のため、サイトの管理者等に対し、現状の調査と問題解決のための対応を依頼した件数を示します。

本四半期に寄せられた報告件数は、4812 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 2135 件でした。前四半期と比較して、総報告件数は 52%減少し、調整件数は 12%減少しました。また、前年同期と比較すると、総報告数で 5%減少し、調整件数は 43%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 インシデント報告件数の推移]



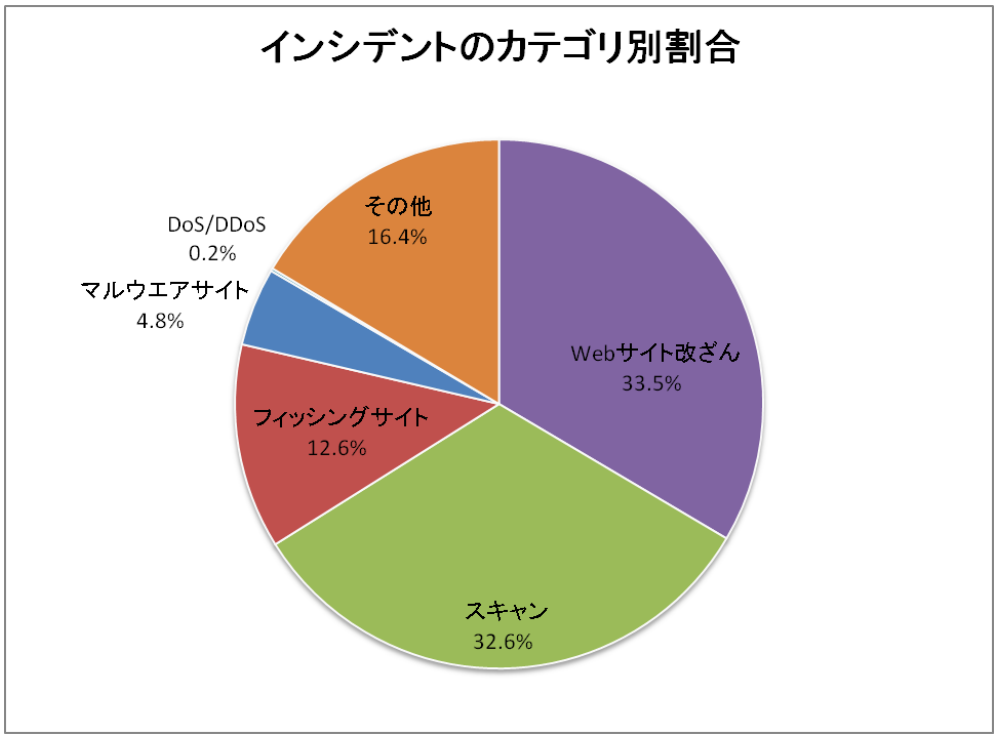
[図 2 インシデント調整件数の推移]

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]

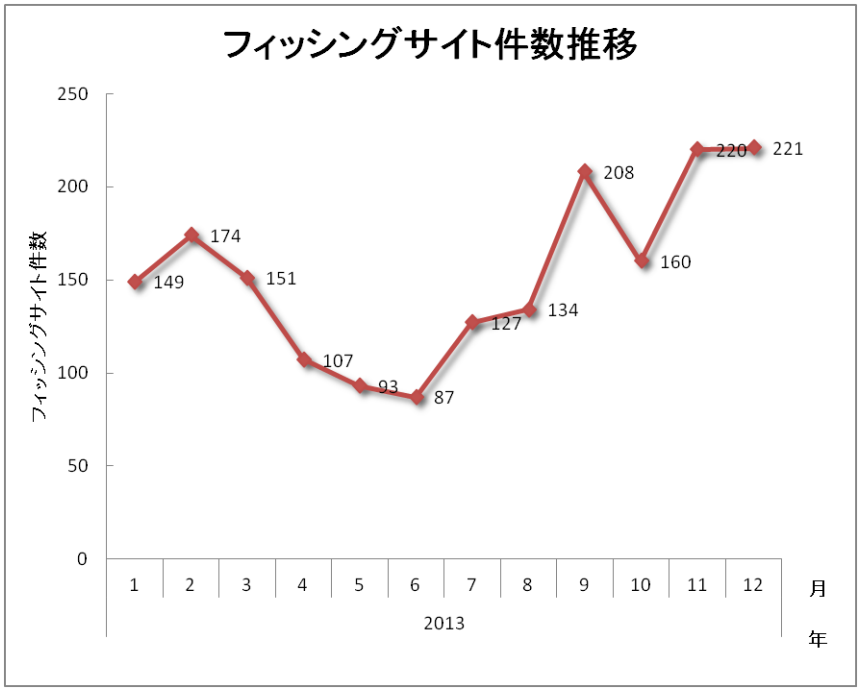
インシデントカテゴリ	10 月	11 月	12 月	合計	前四半期合計
フィッシングサイト	160	220	221	601	469
Web サイト改ざん	627	363	614	1604	2774
マルウエアサイト	70	110	49	229	156
スキャン	471	661	428	1560	2659
DoS/DDoS	5	2	1	8	12
制御システム関連	0	0	1	1	0
その他	123	416	246	785	2214

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。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 32.6%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。

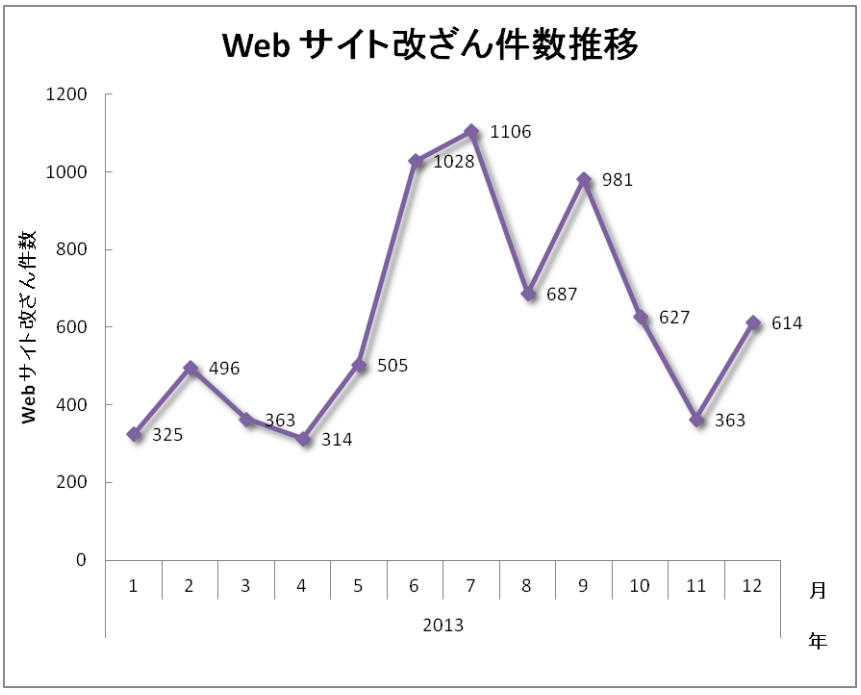


[図 3 インシデントのカテゴリ別割合]

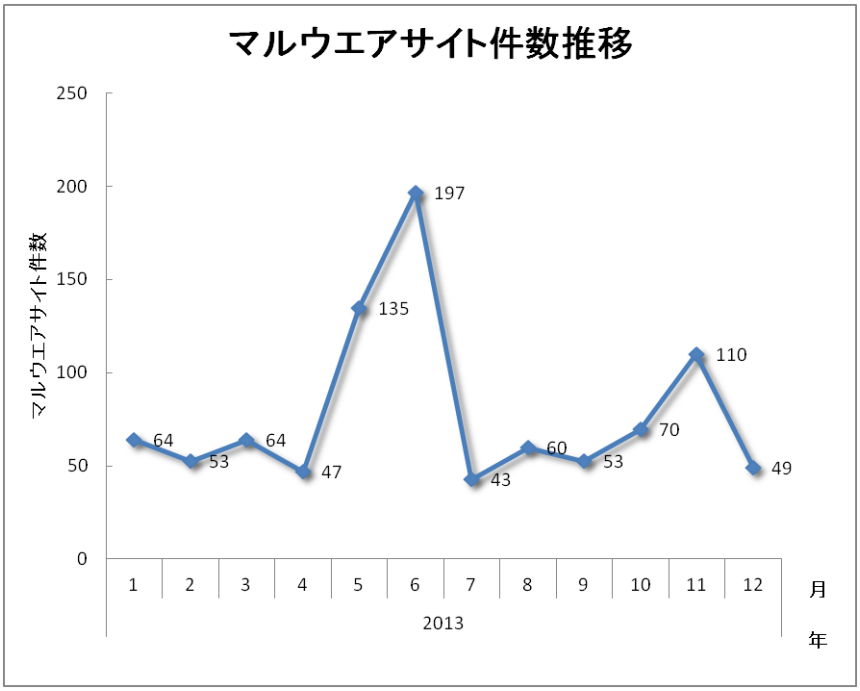
[図 4]から[図 7]に、フィッシングサイト、Web サイト改ざん、マルウエアサイト、スキャンのインシデントの過去 1 年間の月別推移を示します。



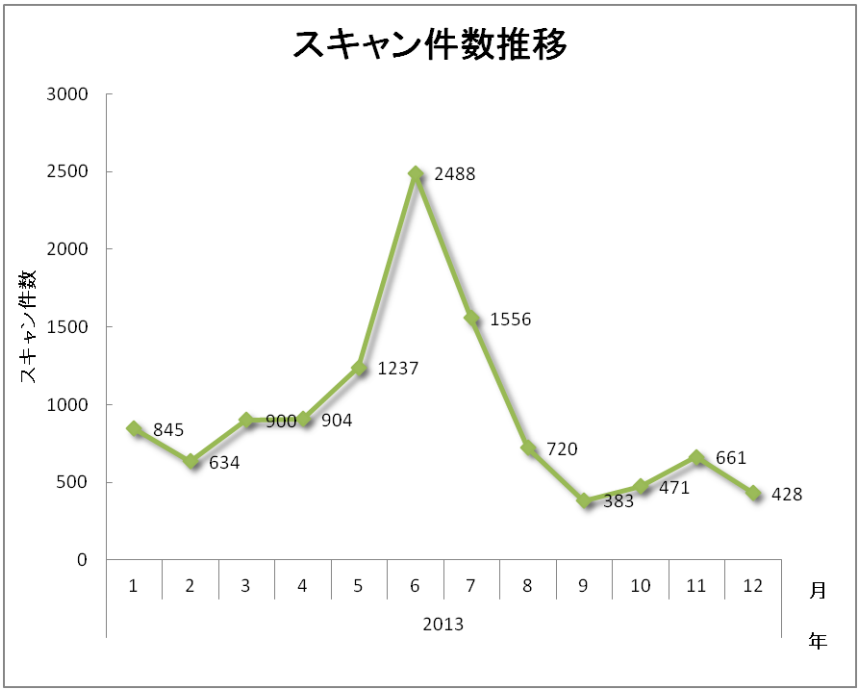
[図 4 フィッシングサイト件数推移]



[図 5 Web サイト改ざん件数推移]

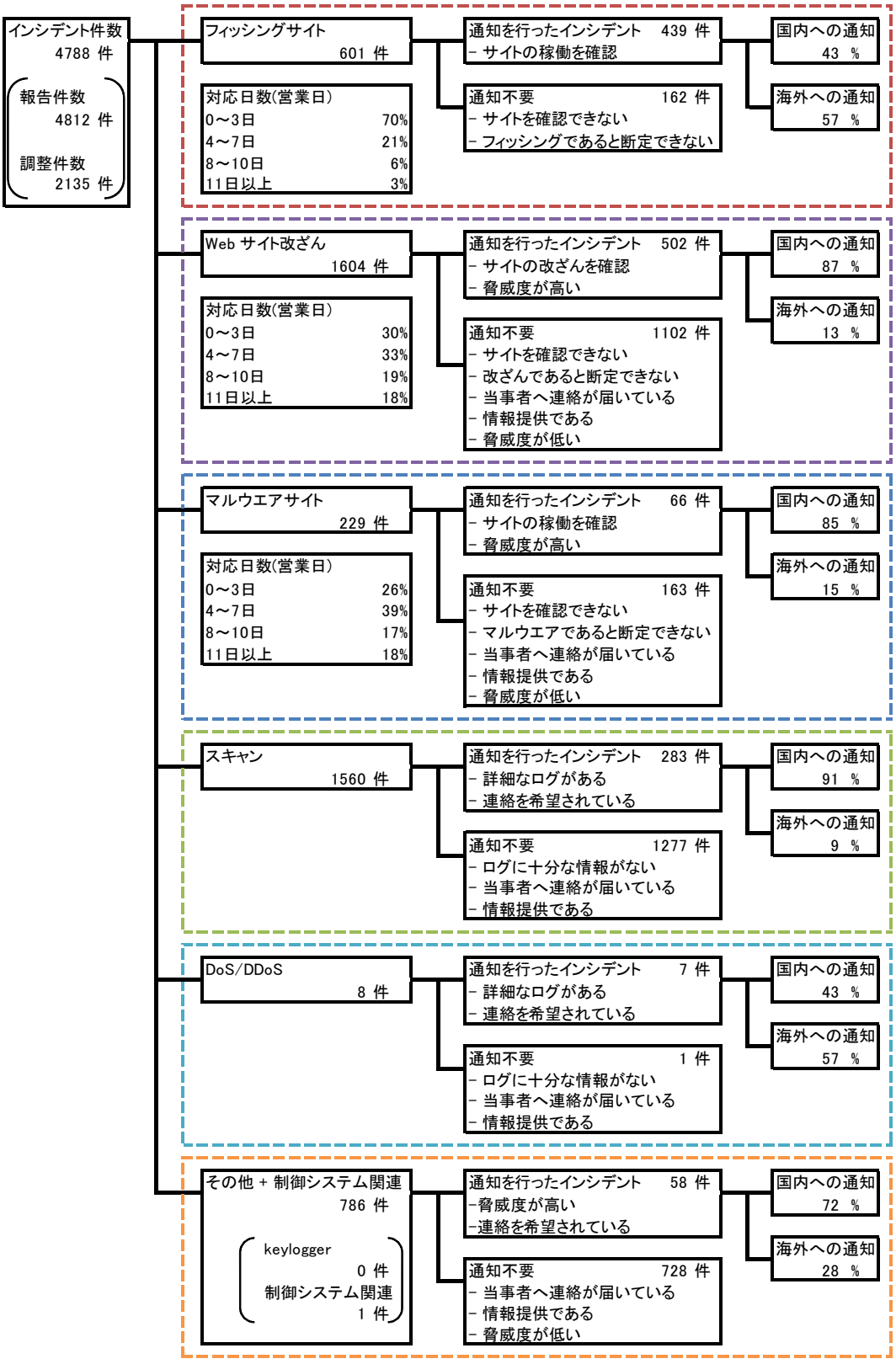


[図 6 マルウエアサイト件数推移]



[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

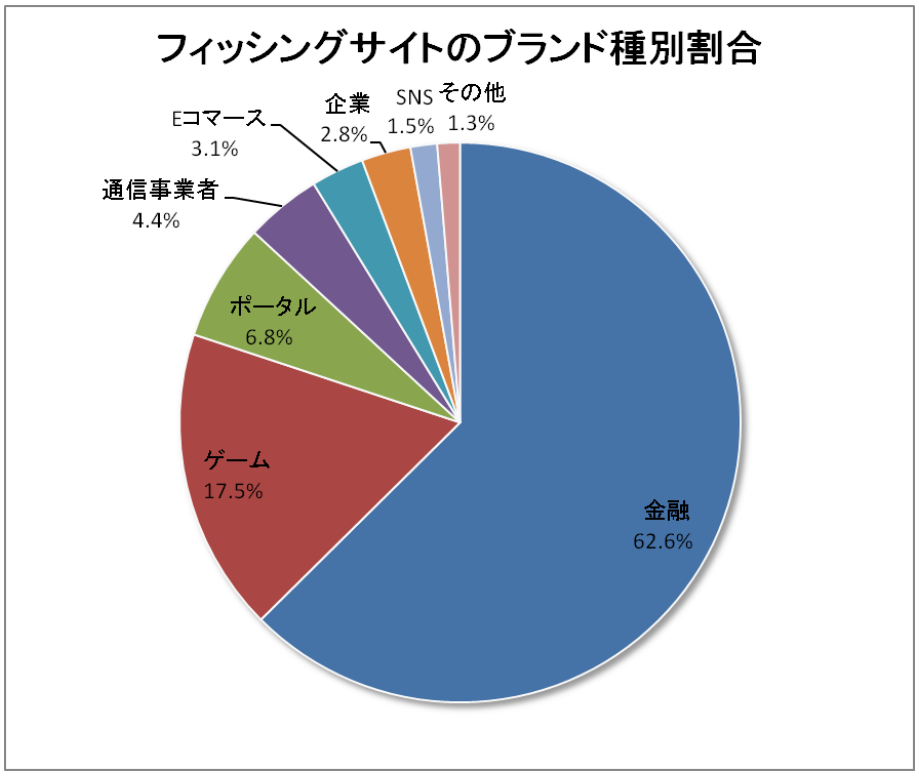
3.1. フィッシングサイトの傾向

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 601 件で、前四半期の 469 件から 28%増加しました。また、前年度同期(360 件)との比較では、67%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	10 月	11 月	12 月	合計 (割合)
国内ブランド	34	99	120	253(42%)
国外ブランド	78	74	52	204(34%)
ブランド不明(注 5)	48	47	49	144(24%)
月別合計	160	220	221	601(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 253 件と、前四半期の 165 件から 53%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 204 件と、前四半期の 219 件から 7%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 62.6%、オンラインゲームサービスを装ったものが 17.5%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。

前四半期に引き続き、国内通信事業者が動的に割り当てる IP アドレスを持ち、国内および海外の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ました。11 月に入ってからは、このようなフィッシングサイトに誘導するためのページが設置された海外の Web サイトを多数確認しました。誘導元となるサイトは特定の CMS を使用している傾向が見られたことから、CMS の脆弱性を悪用され、誘導するためのページを不正に設置された可能性があると考えられます。11 月半ばには、ゲーム会社を装ったフィッシングサイトが稼働しているサーバ上で、国内金融機関を装ったフィッシングサイトが同時に稼働していることを確認しており、それ以降は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。

また、国内通信事業者の Web メールサービスや、国内大学等で導入されている Web メール製品を装ったフィッシングサイトの報告を複数受領しており、これらについては海外の特定の無料ホスティングサービスを使用している傾向が見られました。

フィッシングサイトの調整先の割合は、国内が 43%、国外が 57%であり、前四半期(国内 56%、国外 44%)と比較して、国外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、1604 件でした。前四半期の 2774 件から 42%減少しています。

不正な iframe や JavaScript がページに挿入された Web サイトに関する報告が、依然として多く寄せられています。改ざんによって挿入されるコードには前四半期から大きな変化は見られませんが、改ざんされたサイトを閲覧することでマルウエアに感染し、PC に保存されている認証に使用する情報等が窃取される可能性があります。サイトの管理に使用する PC がマルウエアに感染し、ftp のパスワードが盗まれた結果、不正な ftp 認証によって Web サイトの改ざんが行われるという循環が多くなっている可能性があります。マルウエアに感染することを防ぐためには、まずは、OS やアプリケーションのアップデートや、ウイルス対策ソフトの定義ファイルを最新の状態にする等の最低限の基本的な対策が重要となります。

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、229 件でした。前四半期の 156 件から 47%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、1560 件でした。前四半期の 2659 件から 41%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	10 月	11 月	12 月	合計
25/tcp	317	475	236	1028
80/tcp	156	171	155	482
22/tcp	42	122	65	229
135/tcp	0	14	1	15
21/tcp	7	4	2	13
5900/tcp	3	2	5	10
udp	4	5	1	10
3389/tcp	4	1	3	8
445/tcp	0	5	1	6
1433/tcp	0	2	2	4
143/tcp	1	1	1	3
8080/tcp	0	0	2	2
6200/tcp	0	2	0	2
4899/tcp	0	1	1	2
443/tcp	1	0	1	2
110/tcp	0	1	1	2
その他/tcp	8	10	2	20
不明	2	1	1	4
月別合計	545	817	480	1842

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。

【オープンリゾルバ確認サイトの公開】

JPCERT/CC は、2013 年 10 月 31 日に、利用者の近辺の DNS サーバがオープンリゾルバになっていないかどうかを確認するための「オープンリゾルバ確認サイト」を公開しました。オープンリゾルバとは、外部からの再帰的な名前解決の問合せを許可している DNS サーバです。攻撃者が攻撃対象の IP アドレスになりすましてオープンリゾルバに名前解決の問合せを行うと、オープンリゾルバは名前解決の結果の応答パケットを攻撃対象に送信します。DoS 攻撃に使用されるこの手法は、パケットのサイズが小さい名前解決の問合せにより、サイズの大きい応答パケットを攻撃対象に送りつけることができるため、DNS アンプ攻撃と呼ばれます。このように悪用されるため、オープンリゾルバが問題視されているのです。

サイトの公開後、オープンリゾルバと判定された DNS サーバについて、多数の情報をご提供いただいています。ご提供いただいた情報によると、オープンリゾルバと判定された DNS サーバには、PPPoE や DHCP によってネットワーク接続の際に自動で設定されるものや、契約プロバイダから DNS サーバとして使用するよう指定されたものが多くありました。

【国内マルウエア配布ホストに関する対応】

2013 年 10 月末、海外セキュリティ研究組織から、マルウエアを配布している複数の国内ホストに関する情報を受領しました。これらのホストは国内通信事業者が動的に割り当てる IP アドレスを持っていました。ホスト上では Web サーバが稼働しており、ルートディレクトリ直下に“calc.exe”というファイル名のマルウエアが設置されていました。JPCERT/CC では、当該 IP アドレスを管理する通信事業者に調査を依頼し、結果として、マルウエアの配付が停止されたことを確認しました。

また、海外セキュリティ組織から、ボットネットが使用しているドメインに割り当てられていたとされる国内 IP アドレスのリストを受け取り、上記のケースと同様にマルウエアが設置されている IP アドレスを確認し対処を依頼しました。JPCERT/CC では、マルウエアが設置されているホストを確認し次第、当該 IP アドレスを管理する組織に対処を依頼しています。

【脆弱性検査ツールを使用したスキャン】

2013 年 10 月から 11 月にかけて、脆弱性検査ツールを使用したとみられるスキャンに関する報告を複数受け取りました。一般に、この種のスキャンでは、ディレクトリトラバーサル攻撃と見られる GET リクエストや、Web サイトのメールフォームに対する POST リクエスト等が短時間に大量に行われ、サーバの負荷の増大だけでなく、当該サーバへのメールの大量送信や不正なファイルのアップロード等の被害が発生します。

受け取った報告の中には国内 IP アドレスが攻撃元となっていたものがあり、JPCERT/CC は攻撃元 IP アドレスのネットワーク管理組織に調査を依頼し、対応を行ったとの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。