Japan Computer Emergency Response Team Coordination Center

JPCERT/CC®

JPCERT-IR-2013-02
発行日: 2013-07-11

JPCERT/CC インシデント報告対応レポート
[2013 年 4 月 1 日 ～ 2013 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、2013 年 4 月 1 日から 2013 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]

	4 月	5 月	6 月	合計	前四半期合計
報告件数 (注 2)	1606	3163	4617	9386	5453
インシデント件数 （注 3）	1672	2951	4463	9086	5692
調整件数（注 4）	729	704	746	2179	2230

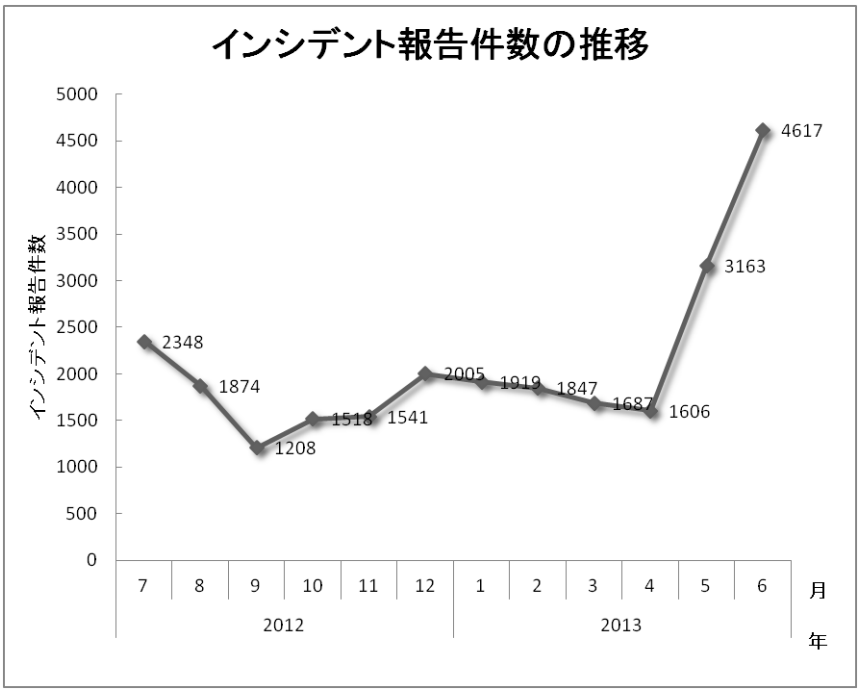
【注 2】「報告件数」は、報告者から寄せられた Web フォーム、メール、FAX による報告の総数を示します。

【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。

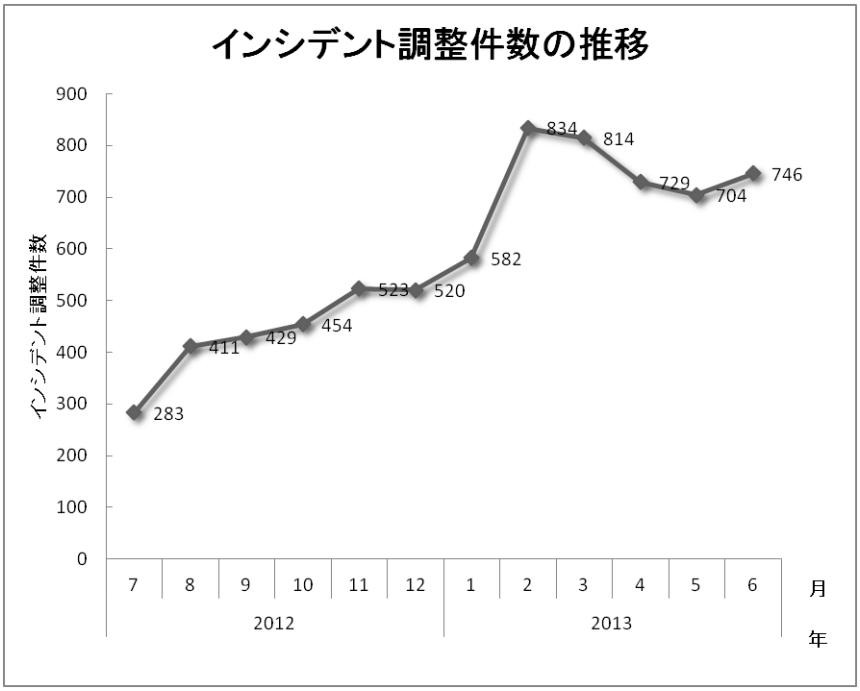
【注 4】「調整件数」とは、インシデントの拡大防止のため、サイトの管理者などに対し、現状の調査と問題解決のための対応を依頼した件数を示します。

本四半期に寄せられた報告件数は、9386 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 2179 件でした。前四半期と比較して、総報告件数は 72%増加し、調整件数は 2%減少しました。また、前年同期と比較すると、総報告数で 131%増加し、調整件数は 188%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]



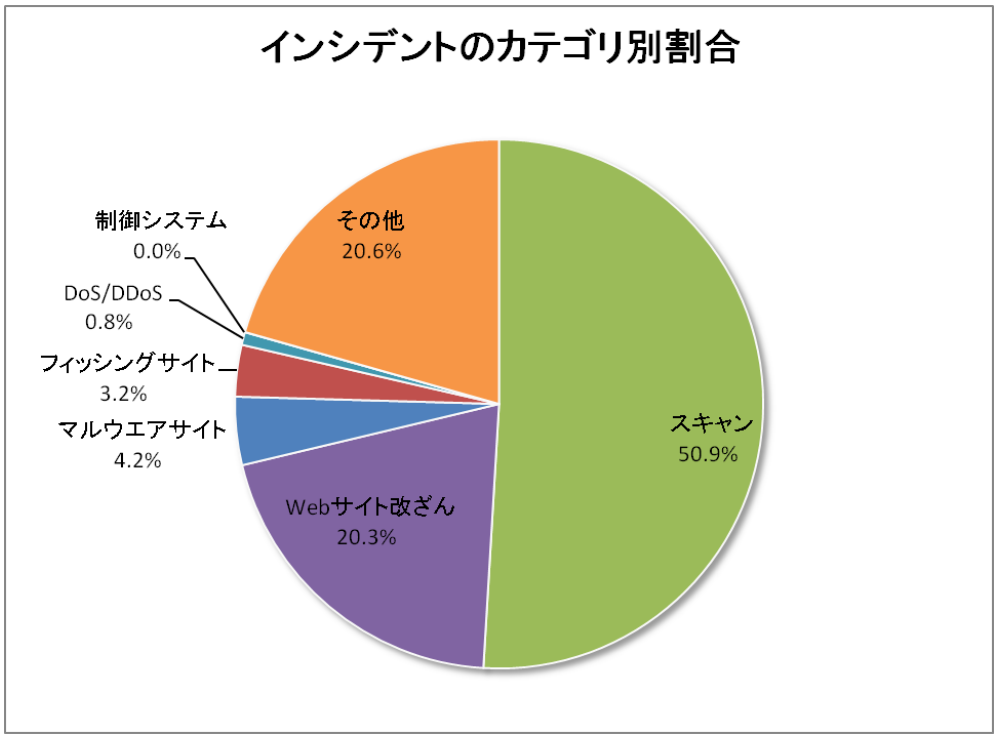
[図 2 インシデント調整件数の推移]

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 3 カテゴリ別インシデント件数]

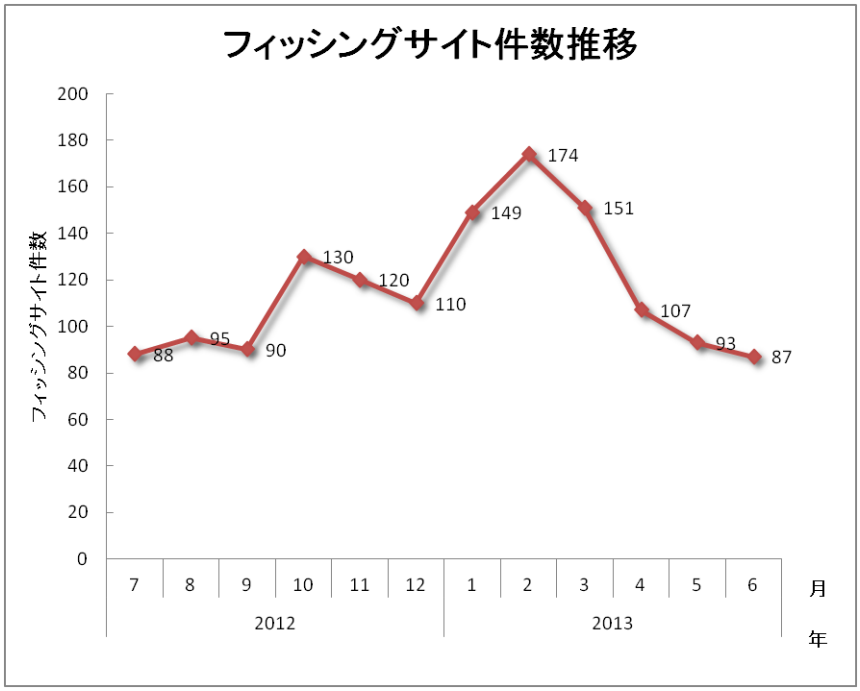
インシデントカテゴリ	4 月	5 月	6 月	合計	前四半期合計
フィッシングサイト	107	93	87	287	474
Web サイト改ざん	314	505	1028	1847	1184
マルウエアサイト	47	135	197	379	181
スキャン	904	1237	2488	4629	2379
DoS/DDoS	61	10	0	71	36
制御システム	0	1	0	1	3
その他	239	970	663	1872	1435

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。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 50.9%、Web サイト改ざんに分類されるインシデントは 20.3%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 3.2%でした。

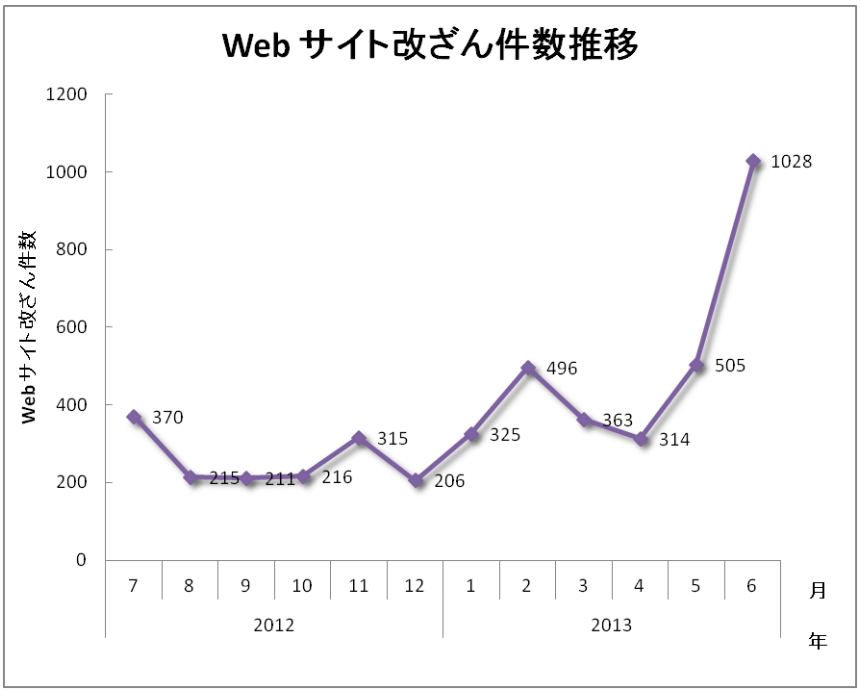


[図 4 インシデントのカテゴリ別割合]

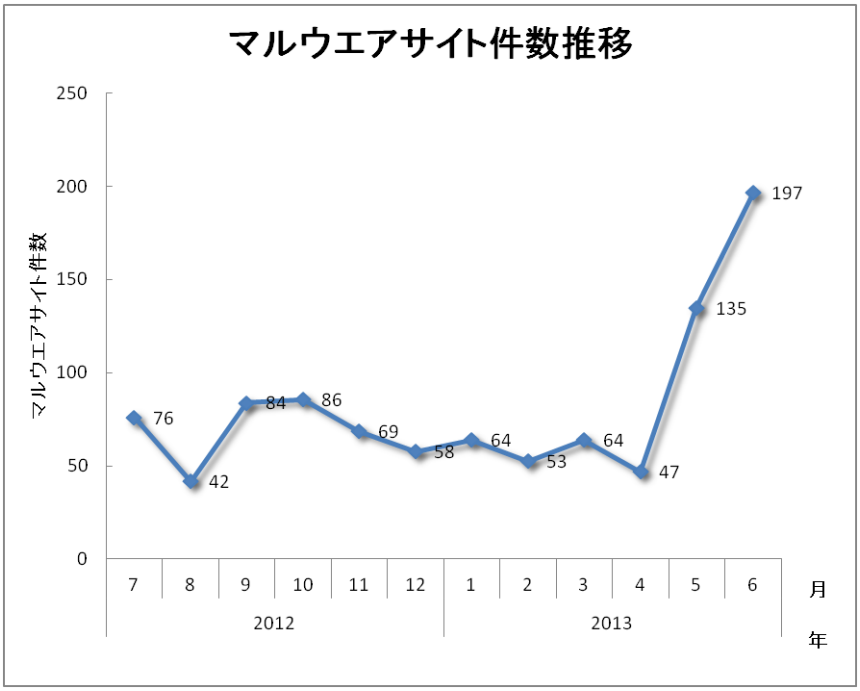
[図 5]から[図 8]に、フィッシングサイト、Web サイト改ざん、マルウエアサイト、スキャンのインシデントの過去 1 年間の月別推移を示します。



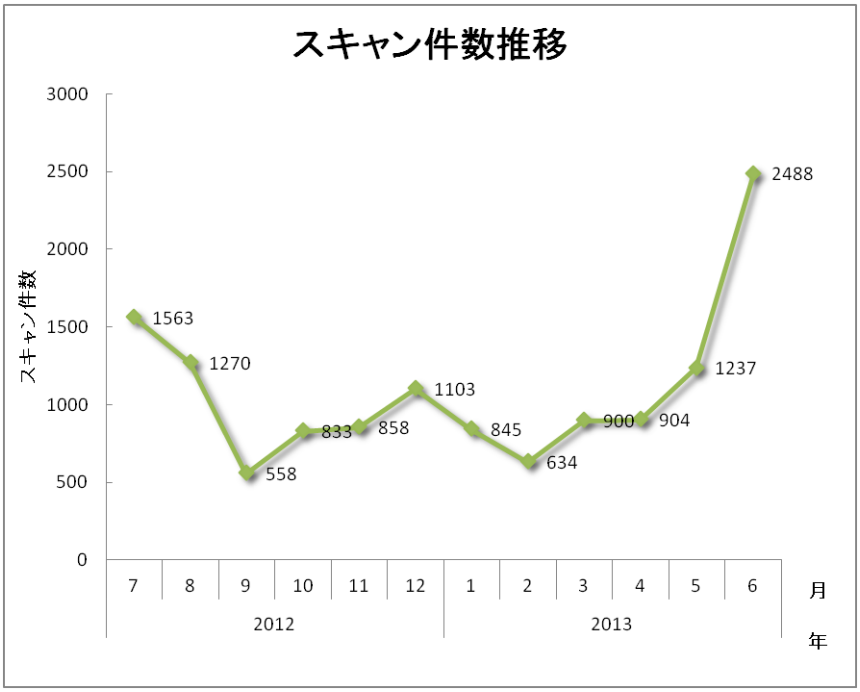
[図 5 フィッシングサイト件数推移]



[図 6 Web サイト改ざん件数推移]

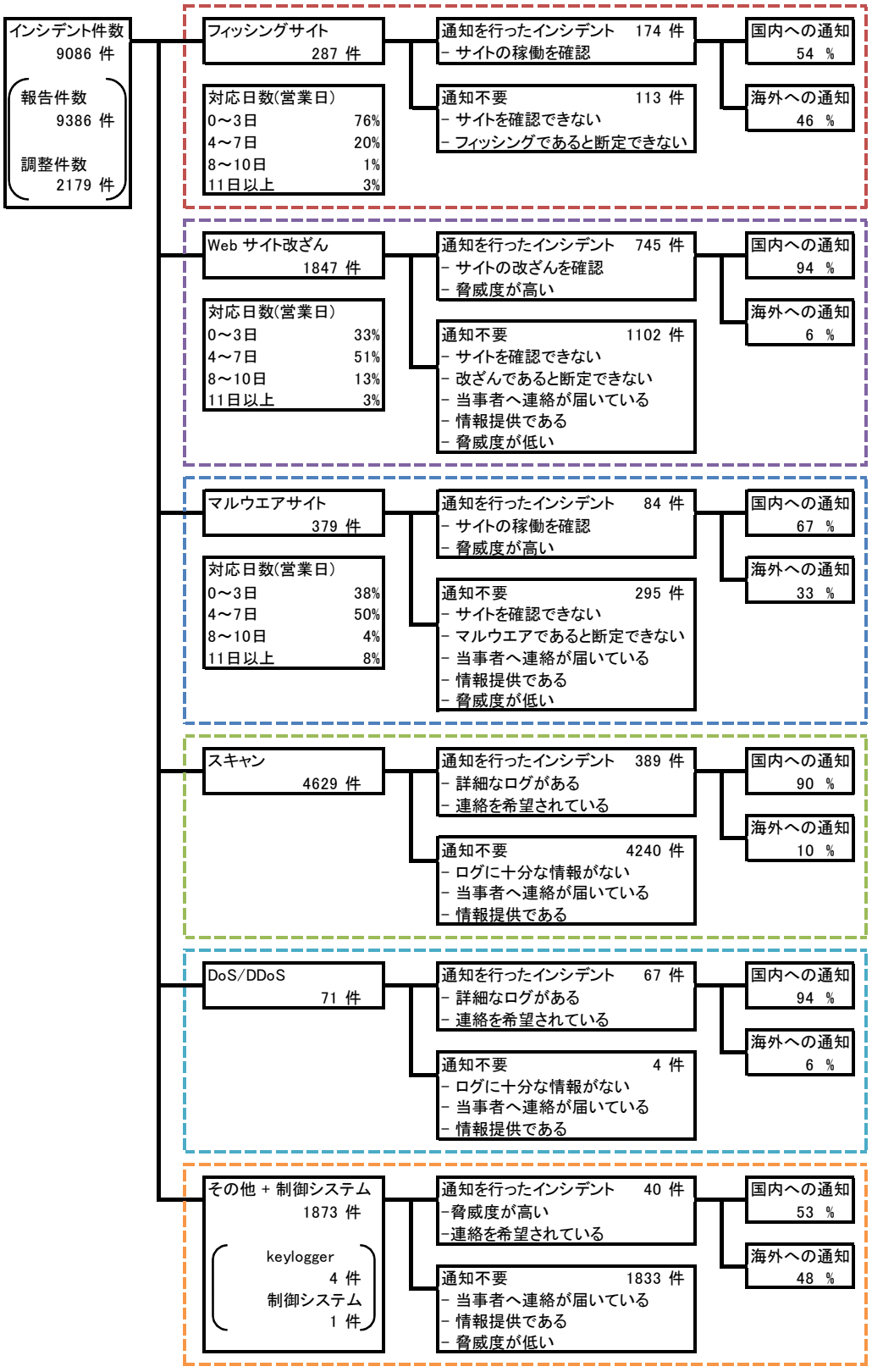


[図 7 マルウエアサイト件数推移]



[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

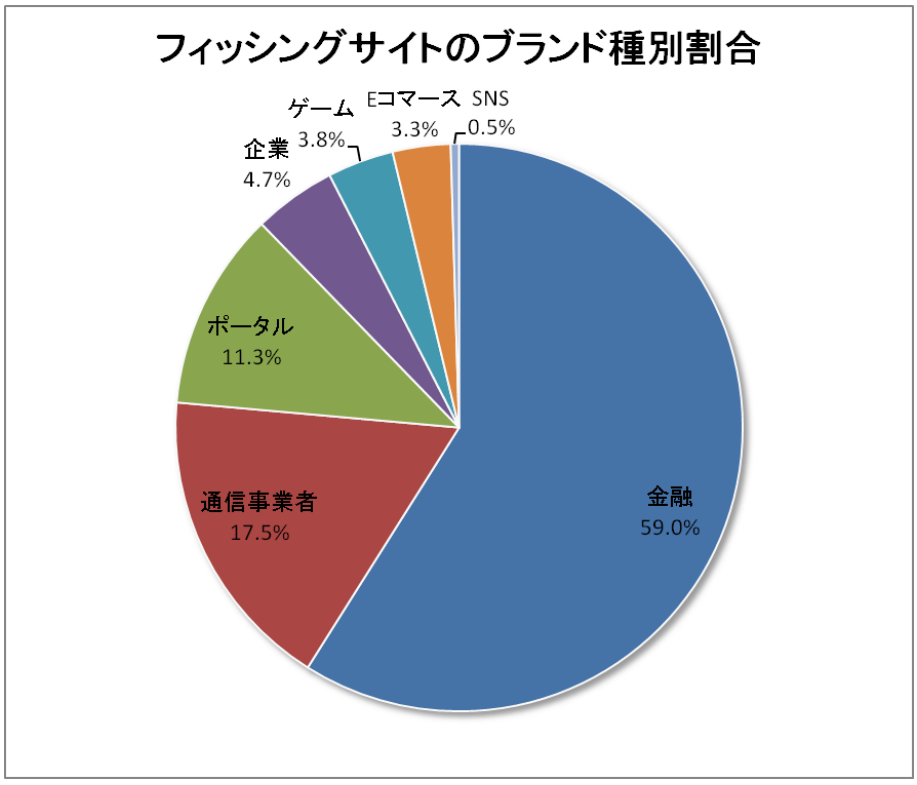
3.1. フィッシングサイトの傾向

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 287 件で、前四半期の 474 件から 39%減少しました。また、前年度同期(367 件)との比較では、22%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 4]、業界割合を[図 10]に示します。

[表 4 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	合計 (割合)
国内ブランド	20	27	25	72(25%)
国外ブランド	62	37	41	140(49%)
ブランド不明(注 5)	25	29	21	75(26%)
月別合計	107	93	87	287(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 72 件と、前四半期の 112 件から 36%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 140 件と、前四半期の 285 件から 51%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では、金融機関のサイトを装ったものが 59.0%、通信事業者を装ったものが 17.5%を占めています。国内ブランドでは通信事業者を装ったサイトが、海外ブランドでは金融機関を装ったサイトが占める割合がそれぞれ最多でした。

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の報告を多数受領しています。以前は、特定の海外無料ホスティングサービスを利用して多くのフィッシングサイトが構築されていましたが、本四半期は WordPress などの CMS(Contents Management System) を使用している海外のサーバに侵入して設置したと見られるものが多く確認されました。

5 月から 6 月にかけて、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複数受領しています。これらのフィッシングサイトのドメイン名は、正規サイトに似せたものになっており、フィッシングサイトを確認した日から遡って数日から 2 カ月以内に新しく登録されたものでした。確認したサイトの内の一つは IP アドレスが不定期に変化しており、これらの IP アドレスはいずれも国内通信事業者が割り当てる動的な IP アドレスでした。

フィッシングサイトの調整先の割合は、国内が 54%、国外が 46%であり、前四半期(国内 36%、国外 64%)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、1847 件でした。前四半期の 1184 件から 56%増加しています。

本四半期は、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ました。改ざんされたサイトに挿入されているコードは、種類によって誘導先の URL やコメントタグなどの特徴が異なっています。改ざんされたサイトにアクセスした場合、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、古いバージョンのアプリケーションを使用している PC はマルウエアに感染する可能性があります。
このような攻撃によって PC が感染するマルウエアとしては、PC 内に保存されている様々なアカウント情報を窃取するものや、PC をスパムメールの送信や DoS 攻撃の踏み台として使用するものなどを確認しています。Web サイトの管理に使用している PC が情報を窃取するマルウエアに感染すると、サーバへの接続に使用する FTP アカウント情報が窃取され、管理している Web サイトのコンテンツを改ざんされてしまい、さらに被害が拡大するおそれがあります。

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、379 件でした。前四半期の 181 件から 109%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、4629 件でした。前四半期の 2379 件から 95%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 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。http を対象としたスキャンでは、6 月上旬以降、WordPress を使用している Web サイトの管理画面に対する国内 IP アドレスからのブルートフォース攻撃の報告が多数寄せられました。

[表 5　ポート別のスキャン件数]

ポート	4 月	5 月	6 月	合計
80/tcp	509	885	2184	3578
25/tcp	290	332	278	900
22/tcp	79	71	29	179
udp	101	29	5	135
5900/tcp	0	4	16	20
3389/tcp	5	7	6	18
21/tcp	2	1	8	11
143/tcp	8	0	2	10
8080/tcp	2	2	0	4
23/tcp	1	1	2	4
5901/tcp	1	1	0	2
445/tcp	0	2	0	2
4275/tcp	0	0	2	2
1433/tcp	0	1	1	2
6675/tcp	0	1	0	1
4899/tcp	0	1	0	1
32771/tcp	1	0	0	1
2541/tcp	0	0	1	1
1521/tcp	1	0	0	1
135/tcp	0	0	1	1
110/tcp	1	0	0	1
不明	2	7	6	15
月別合計	1003	1345	2541	4889

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。

【国内金融機関のインターネットバンキングを標的としたマルウエアに関する対応】
2013 年 5 月初めごろ、金融系マルウエアの設定ファイル内に、国内金融機関のインターネットバンキングのアカウント情報を窃取するための設定があることを確認しました。設定ファイル内には、海外のサーバ上に置かれた JavaScript ファイルを参照する記述があり、この JavaScript ファイルは、利用者が標的となるインターネットバンキングのページにアクセスした際に、アカウントなどの情報を入力させるポップアップ画面を表示させ、入力された情報を窃取する仕組みになっていました。
JPCERT/CC では、JavaScript ファイルが設置されていたサーバを管理する海外ホスティング事業者に対応を依頼し、その結果、ファイルが取得できなくなったことを確認しました。

【マルウエア配布に使用するドメインに割り当てられる国内 IP アドレスに関する対応】
2013 年 5 月末頃、悪意のある実行ファイルが設置されている.us ドメインのサイトの報告を複数受領しました。これらのサイトは、名前解決を行う度に異なる IP アドレスが返される fast-flux の手法を使用しており、確認した IP アドレスの中には複数の国内ホストのものが含まれていました。3 章 1 節で紹介した国内ゲーム会社を装ったフィッシングサイトと、3 章 2 節で紹介した難読化された JavaScript が挿入される Web サイト改ざんの誘導先のサイトにも、同様に fast-flux が使用され、国内の IP アドレスが含まれていたことを確認しています。
これらの IP アドレスは国内通信事業者から割り当てられる動的なものであり、このような IP アドレスがマルウエア配布サイトに使用された原因としては、インターネットに直接接続している PC がマルウエアに感染したか、インターネット接続に使用するアカウント情報が窃取されたことにより、IP アドレスが攻撃者のリソースとして悪用されたためと考えられます。このような IP アドレスの 80/tcp にアクセスすると、ホストから返される一つの HTTP ヘッダに Apache と nginx の二つの Server ヘッダが存在するという特徴が見られました。
JPCERT/CC では、IP アドレスのネットワーク管理者に対応を依頼し、国内ホストが悪用される原因を調査しています。

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。