JPCERT-IR-2015-03
発行日: 2015-07-14

JPCERT/CC インシデント報告対応レポート
[2015 年 4 月 1 日 ～ 2015 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、2015 年 4 月 1 日から 2015 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)	2098	1609	1480	5187	6869
インシデント件数 (注 3)	1621	1320	1247	4188	5485
調整件数 (注 4)	1069	813	711	2593	3088

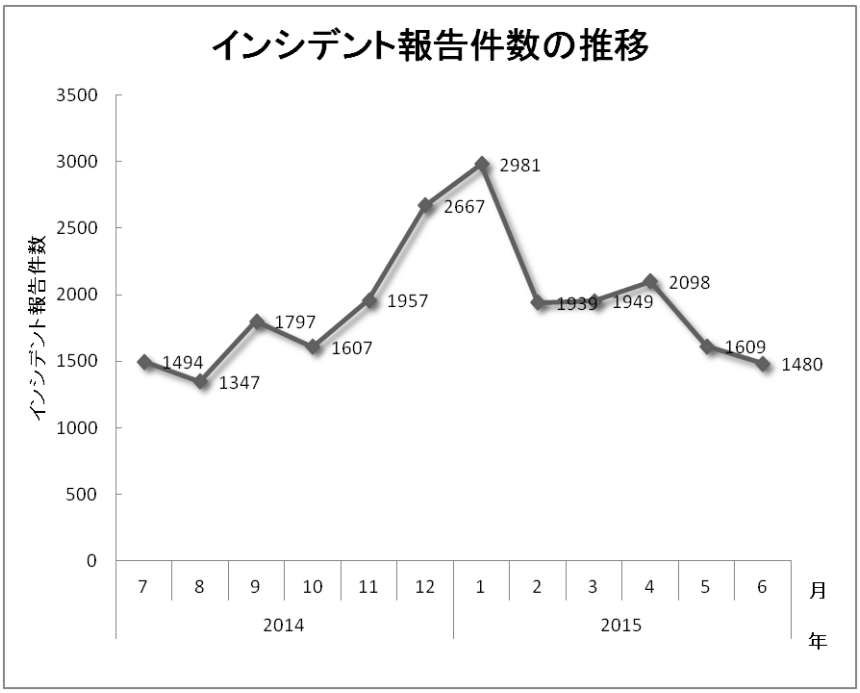
【注 2】「報告件数」は、報告者から寄せられた Web フォーム、メール、FAX による報告の総数を示します。

【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。

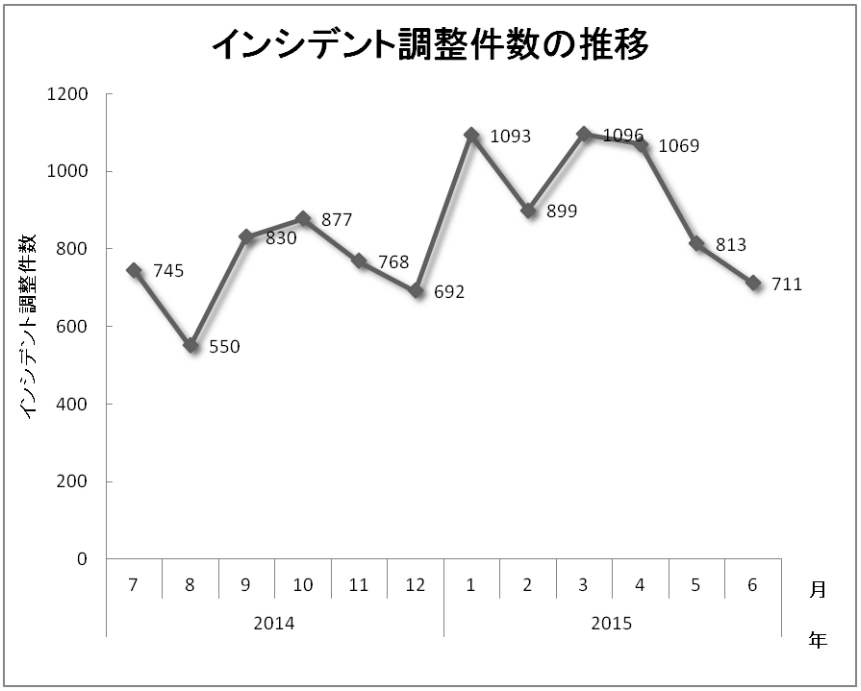
【注 4】「調整件数」は、インシデントの拡大防止のため、サイトの管理者等に対し、現状の調査と問題解決のための対応を依頼した件数を示します。

本四半期に寄せられた報告件数は、5187 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 2593 件でした。前四半期と比較して、総報告件数は 24%減少し、調整件数は 16%減少しました。また、前年同期と比較すると、総報告数で 15%増加し、調整件数は 22%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]

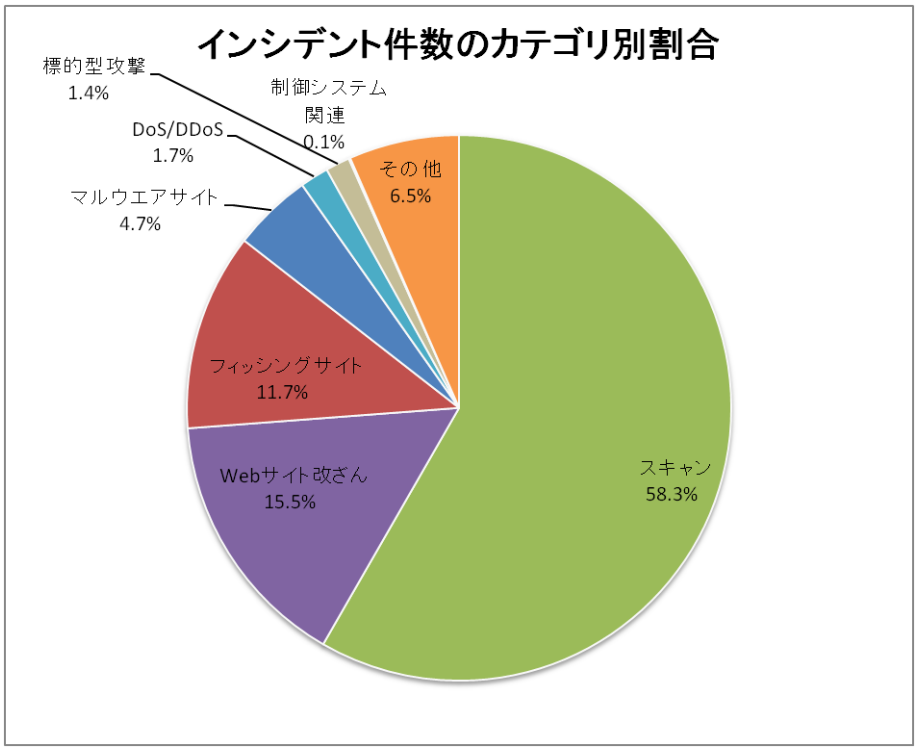
JPCERT/CC では、報告を受けたインシデントをカテゴリ別に分類し、各インシデントカテゴリに応じた調整、対応を実施しています。各インシデントの定義については、「付録-1. インシデントの分類」を参照してください。本四半期に報告を受けた各カテゴリのインシデント件数を[表 2]に示します。

[表 2 カテゴリ別インシデント件数]

インシデント	4 月	5 月	6 月	合計	前四半期合計
フィッシングサイト	191	144	156	491	466
Web サイト改ざん	209	175	265	649	792
マルウエアサイト	56	59	82	197	260
スキャン	976	823	643	2442	2980
DoS/DDoS	61	3	7	71	32
制御システム関連	0	4	0	4	5
標的型攻撃	12	21	27	60	-
その他	116	91	67	274	950

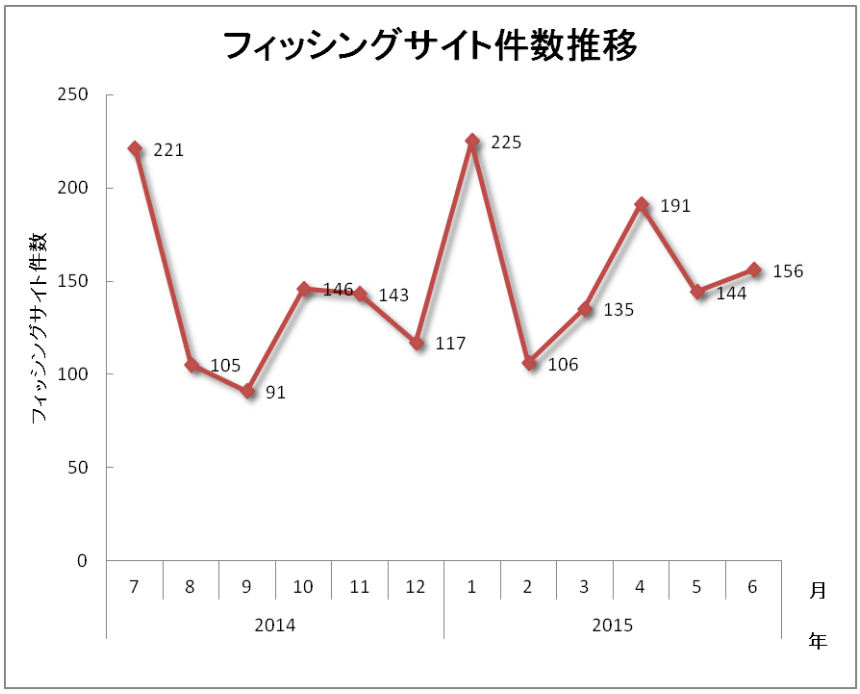
本四半期に発生したインシデントにおける各カテゴリの割合は、[図 3]のとおりです。スキャンに分類される、システムの弱点を探索するインシデントは 58.3%、Web サイト改ざんに分類されるインシデントは 15.5%を占めています。また、フィッシングサイトに分類されるインシデントは 11.7%でした。

JPCERT/CC では、本四半期からインシデントカテゴリに新たに「標的型攻撃」を追加しました。

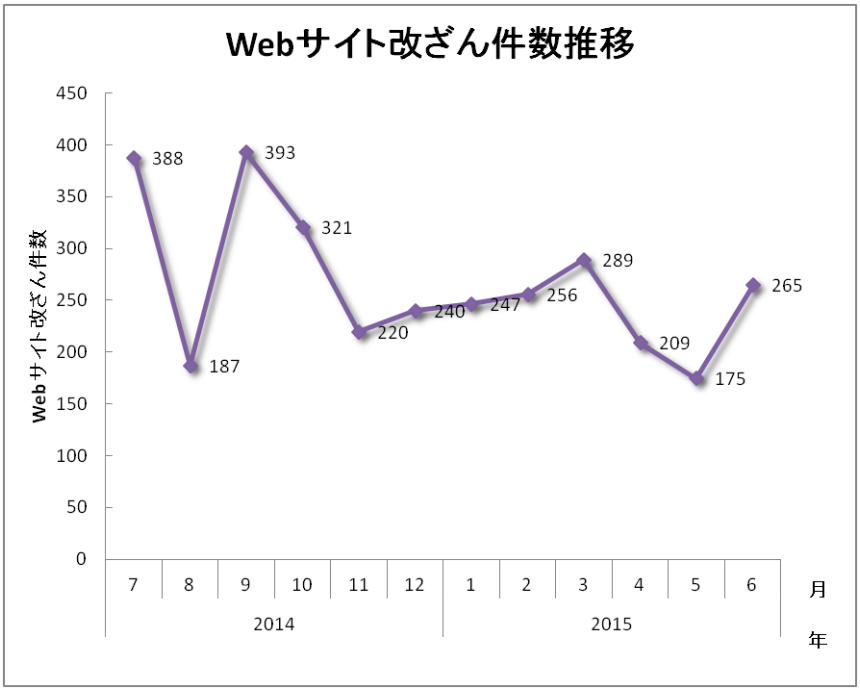


[図 3 インシデントのカテゴリ別割合]

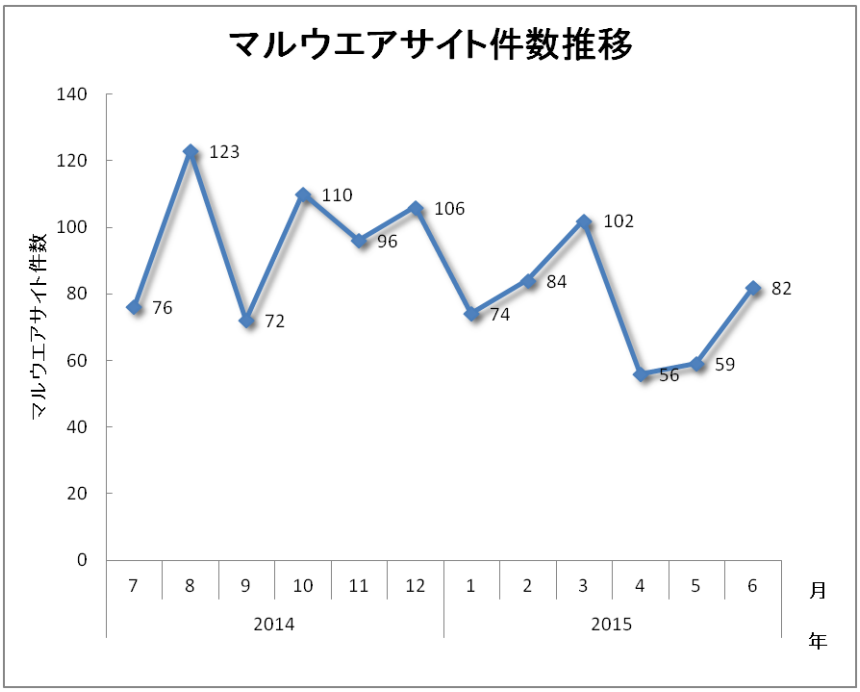
[図 4]から[図 7]に、フィッシングサイト、Web サイト改ざん、マルウエアサイト、スキャンのインシデントの過去 1 年間の月別推移を示します。



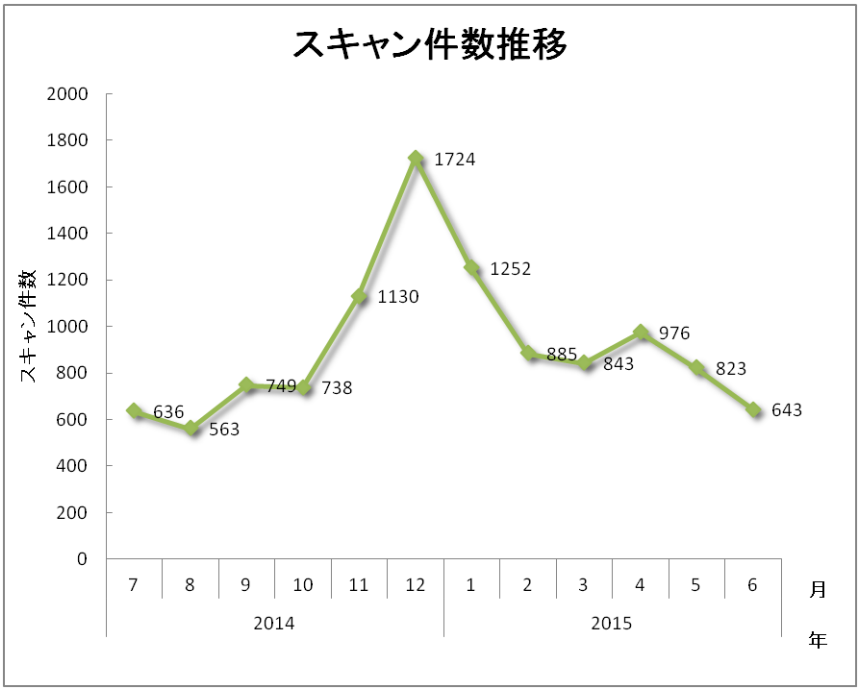
[図 4 フィッシングサイト件数推移]



[図 5 Web サイト改ざん件数推移]

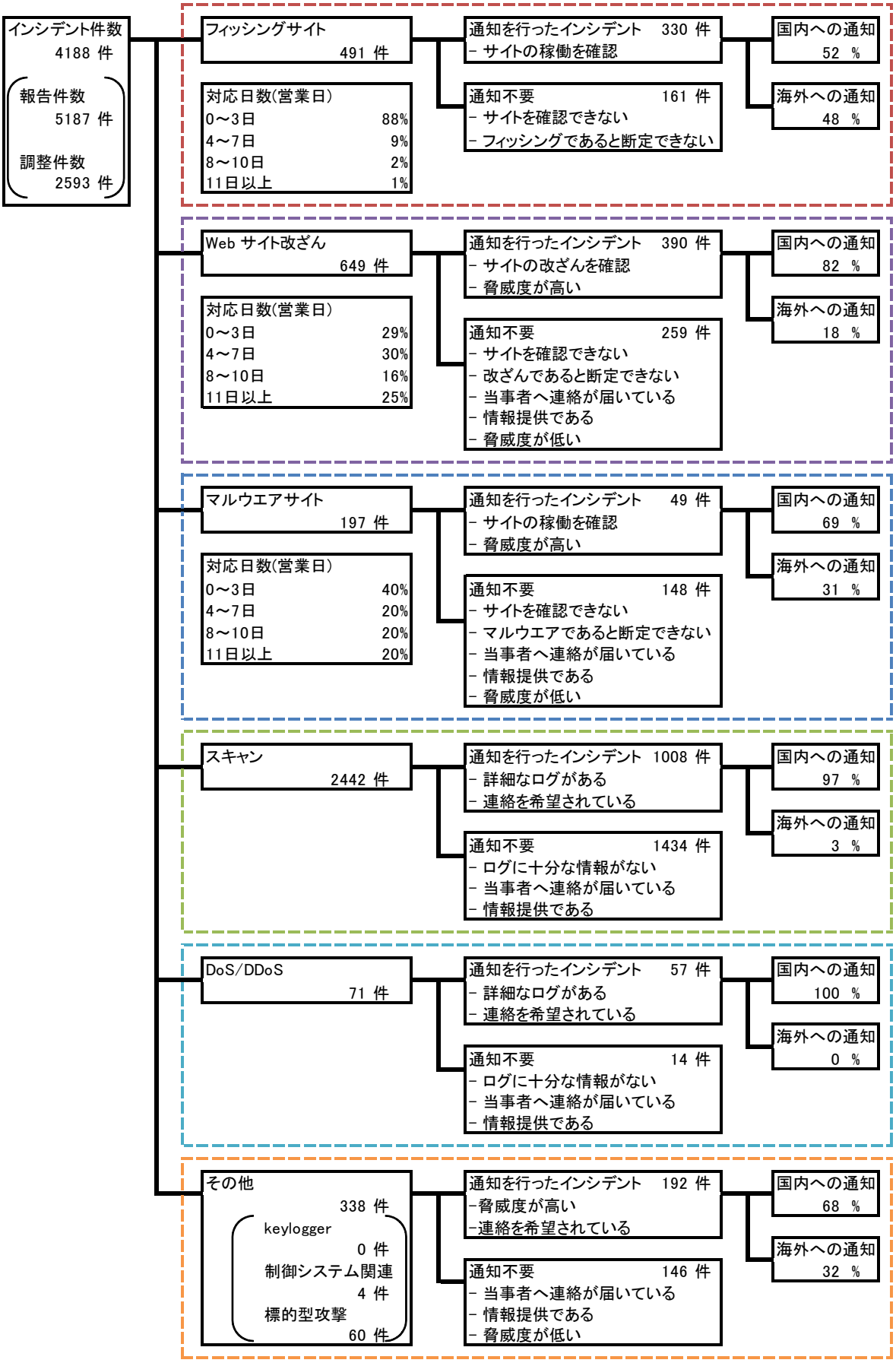


[図 6 マルウエアサイト件数推移]



[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

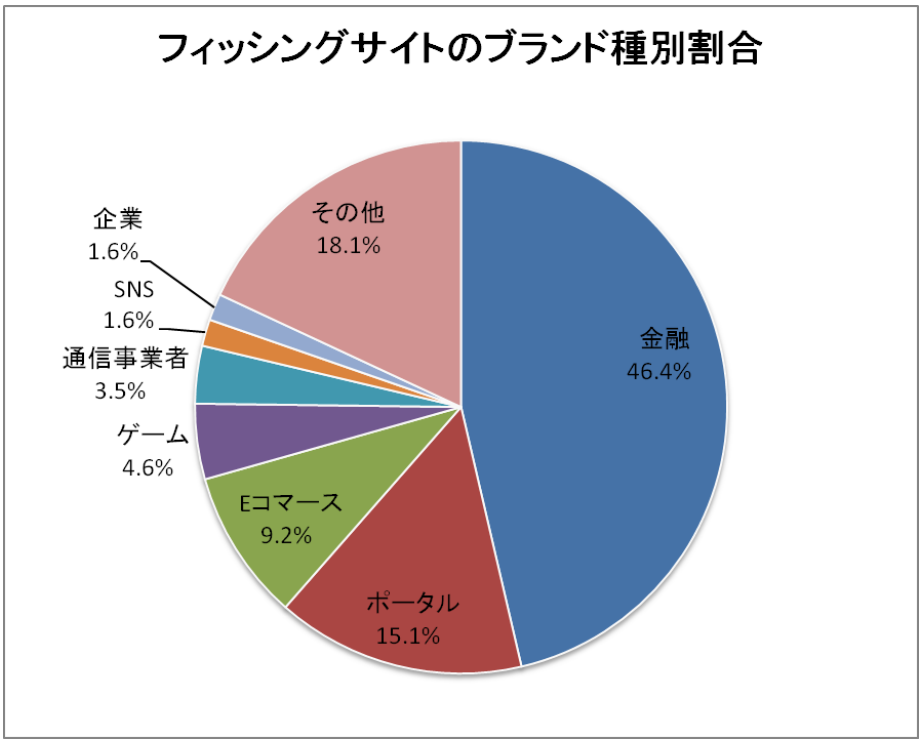
3.1. フィッシングサイトの傾向

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 491 件で、前四半期の 466 件から 5%増加しました。また、前年度同期(509 件)との比較では、4%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	4 月	5 月	6 月	国内外別合計(割合)
国内ブランド	53	35	44	132(27%)
国外ブランド	92	74	73	239(49%)
ブランド不明(注 5)	46	35	39	120(24%)
月別合計	191	144	156	491(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 132 件と、前四半期の 54 件から 144%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 239 件と、前四半期の 281 件から 15%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 46.4%、ポータルサイトを装ったものが 15.1%を占めています。装われたブランドは、国内、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の件数が、前四半期に比べて大きく増加しました。国内金融機関を装ったフィッシングサイトのドメインには 5 月後半までは cn.com 配下のものが多く使用されていましたが、それ以降は.pw、.ml、.gq、.ga などの ccTLD 配下のものが多く見られました。フィッシングサイトのほとんどは海外の IP アドレスを使用しており、日本の IP アドレスは 4 月の半ばに少数確認されたのみでした。

また、以前は国内金融機関を装ったフィッシングサイトが、国内 ISP によって割り当てられた動的な IP アドレスを使うケースが多くありましたが、そうしたケースが現在は韓国の省庁を装ったフィッシングサイトで継続的に確認されています。

フィッシングサイトの調整先の割合は、国内が 52%、国外が 48%であり、前四半期(国内 73%、国外 27%)に比べ、国外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、649 件でした。前四半期の 792 件から 18%減少しています。

本四半期は、改ざんされた Web サイトにアクセスして不正なサイトに誘導され、いわゆるランサムウエアに感染したという報告が多く寄せられました。改ざんされた Web サイトを確認したところ、埋め込まれる不正なコードには、body タグの直後に cookie を送信する JavaScript と、攻撃サイトに誘導する iframe が埋め込まれているという特徴がありました。また、誘導先の攻撃サイトでは、マルウエアに感染させるために、Internet Explorer や Adobe Flash Player の脆弱性が使用されていました。

上記のような改ざんが行われた Web サイトでは、WordPress を使用しているという共通点が見られました。WordPress のような CMS を使用している Web サイトは、CMS やそのプラグインのバージョンが古い場合、脆弱性をつかれて改ざんされてしまう恐れがあります。Web サイトの管理者は、CMS を常に最新のバージョンに維持し、不要なプラグインを削除するなどの対策を取ることが重要です。

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、197 件でした。前四半期の 260 件から 24%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、2442 件でした。前四半期の 2980 件から 18%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、DNS(53/UDP)、SMTP(25/TCP) 、HTTP(80/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
53/udp	354	261	159	774
25/tcp	149	208	167	524
80/tcp	213	167	135	515
22/tcp	142	86	78	306
31385/udp	23	18	22	63
61222/udp	15	23	11	49
2632/udp	16	16	15	47
16358/udp	15	17	14	46
21/tcp	16	12	9	37
445/tcp	10	2	7	19
3389/tcp	4	2	13	19
8080/tcp	10	4	2	16
23/tcp	4	1	8	13
1433/tcp	2	1	7	10
3544/udp	4	1	1	6
143/tcp	1	3	2	6
110/tcp	0	1	4	5
その他	22	10	21	53
月別合計	1000	833	675	2508

DNS の通信の送信元として、オープンリゾルバとなっている国内ホストを非常に多く確認しています。オープンリゾルバは DDoS 攻撃に使用される可能性があるため、ホストを管理する組織やユーザに対して、サーバやルータ等の機器の設定を見直していただくよう、連絡を行っています。

その他に分類されるインシデントの件数は、274 件でした。前四半期の 950 件から 71%減少しています。

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。

【国内組織を標的とした高度な攻撃に関する対応】
JPCERT/CC では、国内組織を標的とした高度な攻撃に関して、使用されたマルウエア、C&C サーバなどの調査、被害組織への調査協力を行うなどの活動に取り組んでいます。

本四半期は、標的型攻撃に関する連絡を 66 組織に行っており、そのうち 44 組織への連絡は Emdivi と呼ばれる遠隔操作マルウエアに関連したものでした。Emdivi に感染した組織では、社内のアクティブディレクトリやファイルサーバなどにも侵入され、様々な機密情報や個人情報が漏えいするなどの被害が発生しています。

JPCERT/CC では、引き続き、被害組織への対応支援、調査協力を行うとともに、被害の可能性のある組織への連絡、調査協力などの活動を通じて被害拡大防止の活動に取り組んで参ります。

【ランサムウエアの国内 C&C サーバに関する対応】
本四半期は、PC 内のファイルを暗号化し、復号のために金銭等を要求する、いわゆるランサムウエアに感染したという報告が多く寄せられました。

4 月末にカナダの National CSIRT から、ランサムウエアの C&C サーバとなっている国内 Web サイトの URL の情報が提供されました。提供された情報から、国内にある複数の正規の Web サイトに、マルウエア感染端末からの POST リクエストを受信するための php ファイルが設置されていることが分かりました。また、関連するマルウエア検体を分析したところ、実際に国内 Web サイトの URL に対して通信が行われることを確認しました。JPCERT/CC では、当該 Web サイト管理者に URL が意図したものであるか確認するよう依頼し、通知先から対応した旨について返信をいただきました。

その後は国内からもランサムウエアに感染したという被害の情報が多く寄せられるようになったため、JPCERT/CC では被害の拡大を防止するため、ランサムウエア感染に関する注意喚起を公開しました。

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 Web ページをご参照ください。

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 Web ページ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、次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

○ 標的型攻撃

「標的型攻撃」とは、特定の組織、企業、業種などを標的として、マルウエア感染や情報の窃取などを試みる攻撃を指します。

JPCERT/CC では、以下を「標的型攻撃」と分類しています。

- 特定の組織に送付された、マルウエアが添付されたなりすましメール
- 閲覧する組織が限定的である Web サイトの改ざん
- 閲覧する組織が限定的である Web サイトになりすまし、マルウエアに感染させようとするサイト
- 特定の組織を標的としたマルウエアが通信を行うサーバ

○ その他

「その他」とは、上記以外のインシデントを指します。

JPCERT/CC が「その他」に分類しているものの例を次に掲げます。

- 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。