JPCERT-IR-2015-04
発行日: 2015-10-08

JPCERT/CC インシデント報告対応レポート
[2015 年 7 月 1 日 ～ 2015 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、2015 年 7 月 1 日から 2015 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)	1543	1215	1370	4128	5187
インシデント件数 (注 3)	1626	929	1193	3748	4188
調整件数 (注 4)	979	554	525	2058	2593

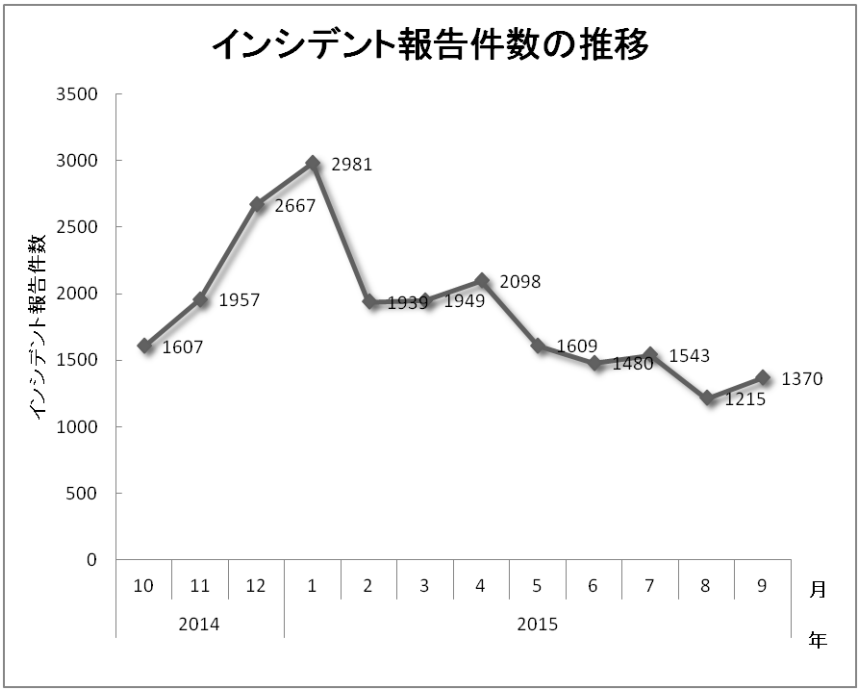
【注 2】「報告件数」は、報告者から寄せられた Web フォーム、メール、FAX による報告の総数を示します。

【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。

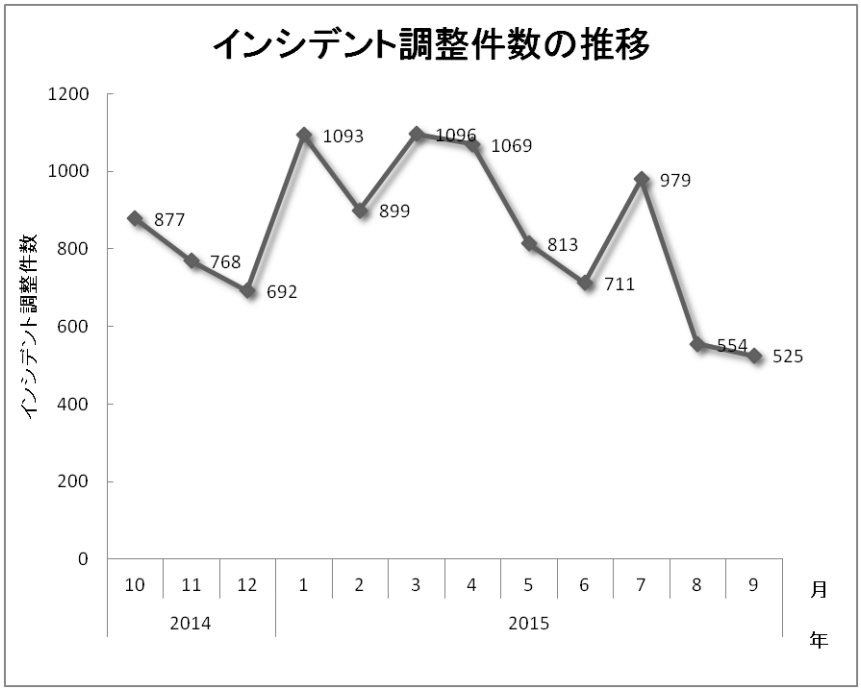
【注 4】「調整件数」は、インシデントの拡大防止のため、サイトの管理者等に対し、現状の調査と問題解決のための対応を依頼した件数を示します。

本四半期に寄せられた報告件数は、4128 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 2058 件でした。前四半期と比較して、総報告件数は 20%減少し、調整件数は 21%減少しました。また、前年同期と比較すると、総報告数で 11%減少し、調整件数は 3%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]



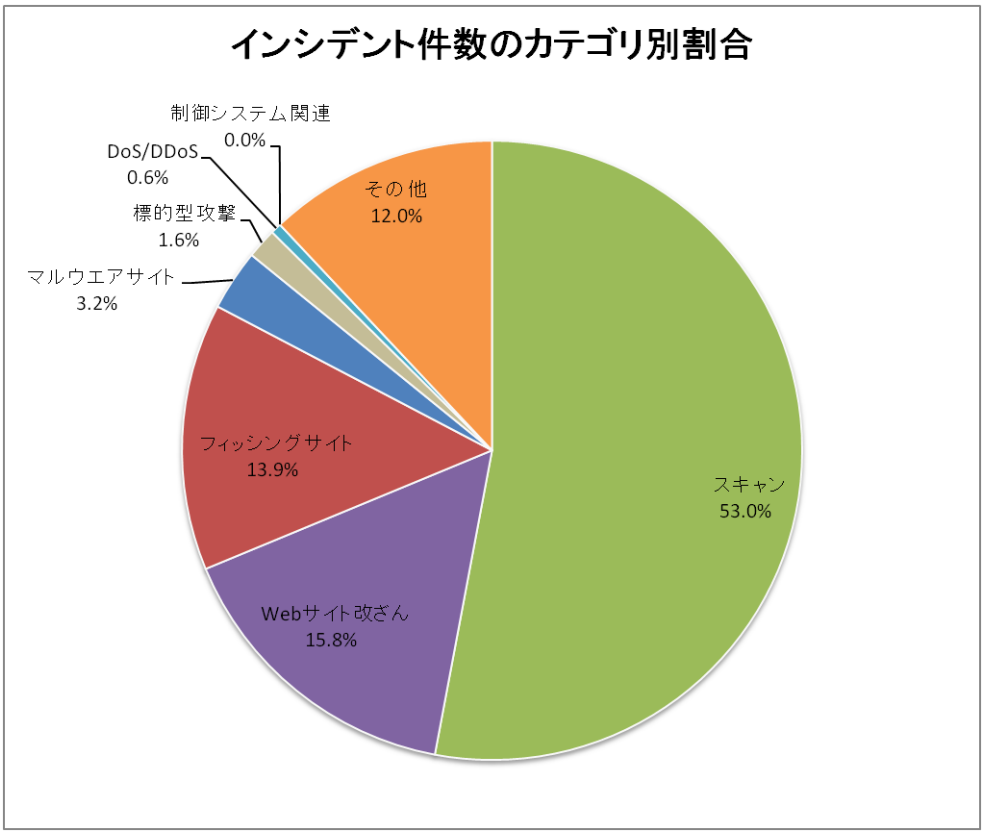
[図 2 インシデント調整件数の推移]

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]

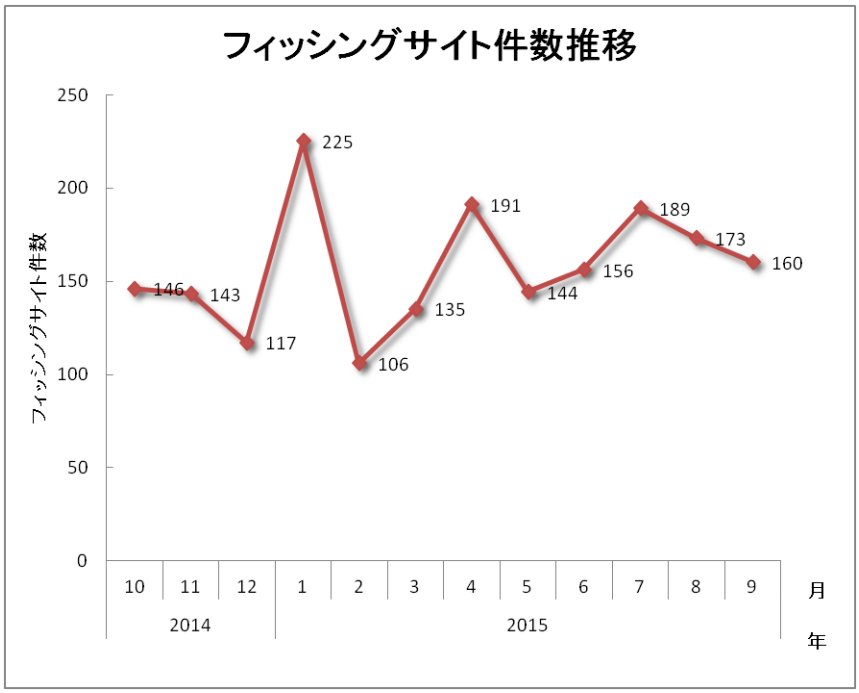
インシデント	7 月	8 月	9 月	合計	前四半期合計
フィッシングサイト	189	173	160	522	491
Web サイト改ざん	244	133	215	592	649
マルウエアサイト	51	30	38	119	197
スキャン	751	534	700	1985	2442
DoS/DDoS	13	1	7	21	71
制御システム関連	0	0	0	0	4
標的型攻撃	26	22	11	59	60
その他	352	36	62	450	274

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 53.0%、Web サイト改ざんに分類されるインシデントは 15.8%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 13.9%でした。

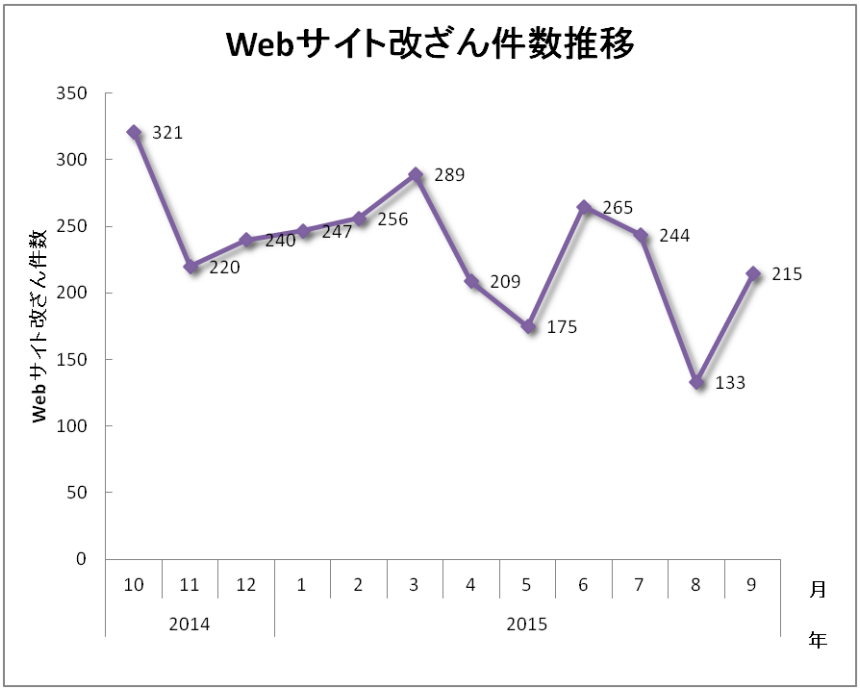


[図 3 インシデントのカテゴリ別割合]

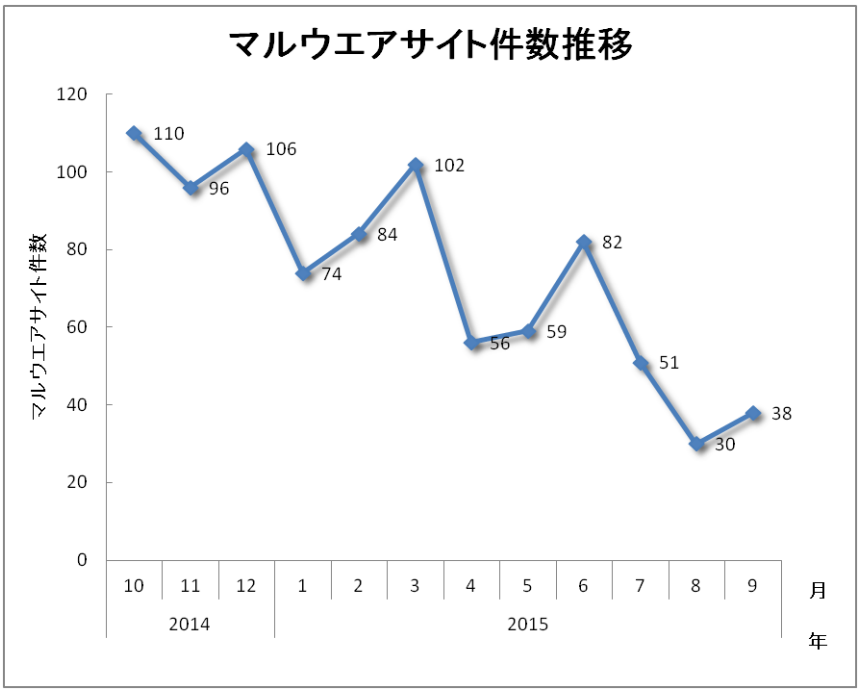
[図 4]から[図 7]に、フィッシングサイト、Web サイト改ざん、マルウエアサイト、スキャンのインシデントの過去 1 年間の月別推移を示します。



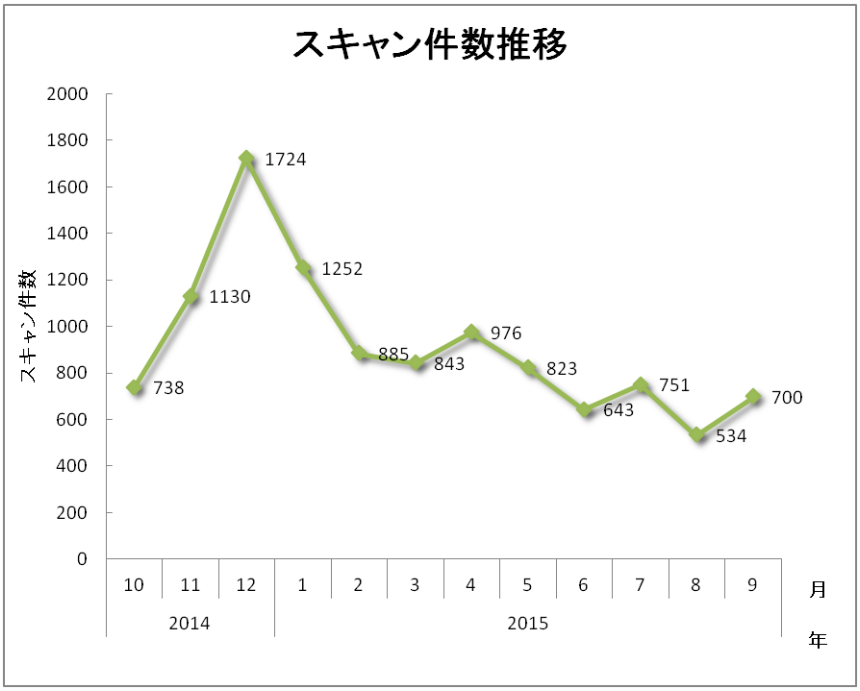
[図 4 フィッシングサイト件数推移]



[図 5 Web サイト改ざん件数推移]

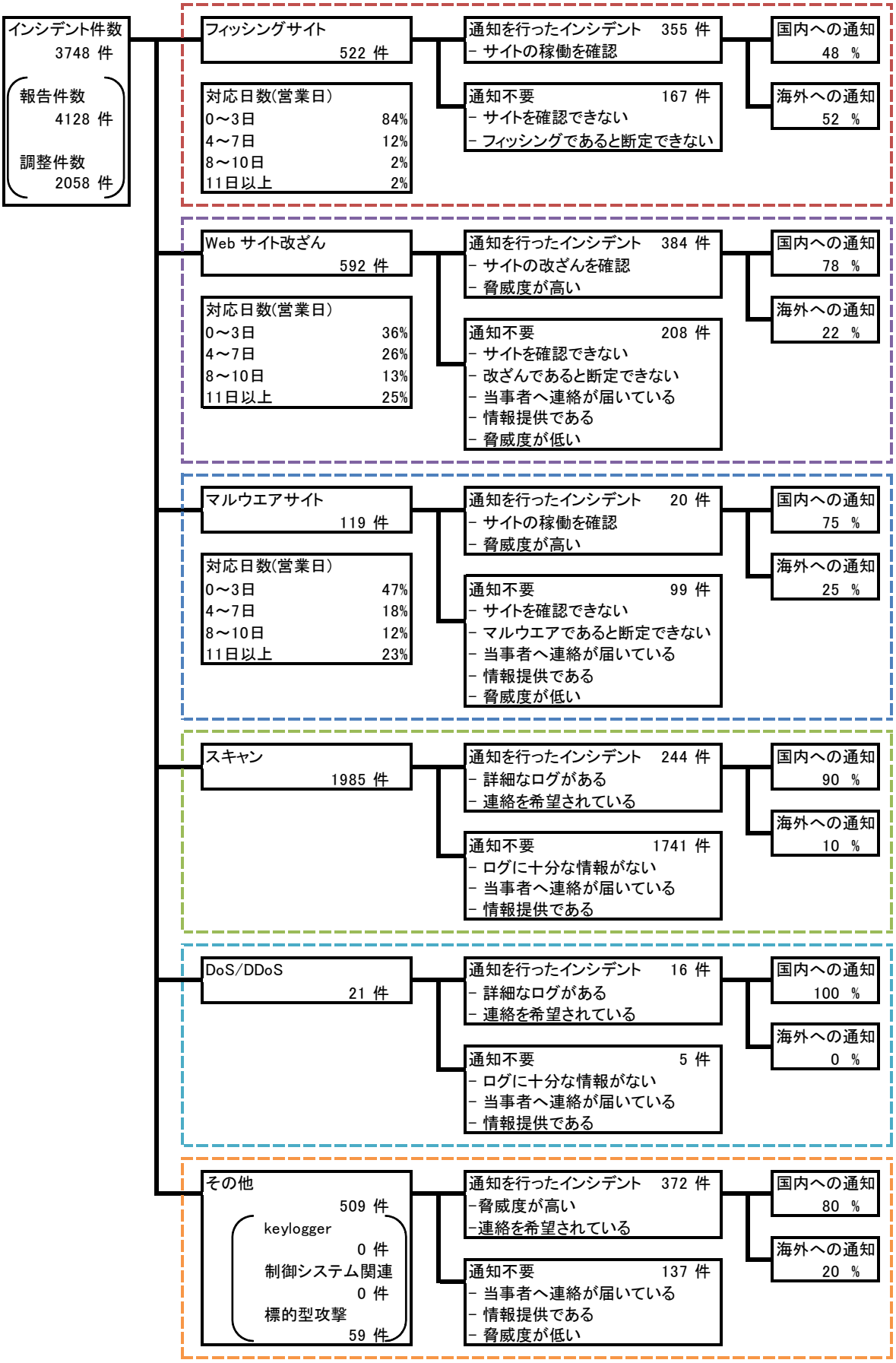


[図 6 マルウエアサイト件数推移]



[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

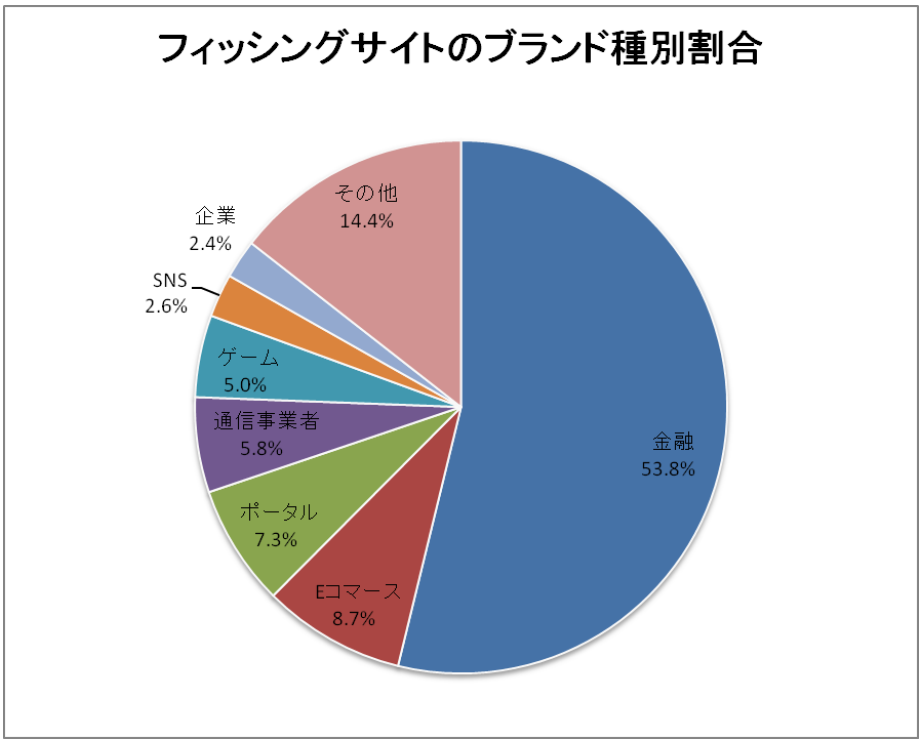
3.1. フィッシングサイトの傾向

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 522 件で、前四半期の 491 件から 6%増加しました。また、前年度同期(417 件)との比較では、25%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	7 月	8 月	9 月	国内外別合計(割合)
国内ブランド	51	32	30	113(22%)
国外ブランド	96	97	75	268(51%)
ブランド不明 (注 5)	42	44	55	141(27%)
月別合計	189	173	160	522(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 113 件となり、前四半期の 132 件から 14 %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 268 件となり、前四半期の 239 件から 12%増加しました。

JPCERT/CC が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 53.8%、E コマースサイトを装ったものが 8.7%で、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。

国内金融機関および国内オンラインゲームを装ったフィッシングサイトを調べると、大量に作成された.com ドメインが使用されており、大半のドメインに香港の IP アドレスが割り当てられていました。金融機関のフィッシングでは標的のブランド名に似せた文字列を含むドメイン名が、オンラインゲームのフィッシングでは無作為に作られた文字列のドメイン名が多く使用されていました。また、xyz、top、space のような比較的新しい gTLD を使用したフィッシングサイトを確認しています。

国内ブランドを装ったフィッシングサイトが使用していた IP アドレスの国別内訳を見ると、43.1%が香港、28.5%がアメリカの IP アドレスであり、あわせて 7 割以上を占めていました。

フィッシングサイトの調整先の割合は、国内が 48%、国外が 52%であり、前四半期(国内 52%、国外 48%)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、592 件でした。前四半期の 649 件から 9%減少しています。

7 月に Adobe Flash Player の脆弱性が複数公開されました。それから間もなくして、国内 Web サイトが改ざんされ、それらの脆弱性を悪用した攻撃サイトに誘導していた事例を JPCERT/CC でも確認しました。その後も、同じ攻撃目的で改ざんされた国内 Web サイトの報告を多数受領し、複数の改ざんパターンがあることを特定しています。

また、改ざんされた国内 Web サイトにアクセスすることにより、国内組織を標的とした攻撃に使用されたマルウエア Emdivi がダウンロードされる事例が本四半期には確認されました。改ざんされたサイトでは、正規の js ファイルに不正なコードが埋め込まれており、それによって、同サイト上に不正に設置された、上記の脆弱性を悪用する swf ファイルを読み込ませるページに誘導される仕組みになっていました。

9 月上旬ごろから、Web サイトに埋め込まれた広告によってマルウエア配布サイトに誘導されたと推測されるインシデントの報告を受領しています。報告をもとに Web サイト上の広告を定期的に取得して観測したところ、広告に埋め込まれる js ファイルが、不定期に不正なコードが混ざったものになっていることを確認しました。

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、119 件でした。前四半期の 197 件から 40%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、1985 件でした。前四半期の 2442 件から 19%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、HTTP(80/TCP)、SMTP(25/TCP) 、SSH(22/TCP)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	352	233	390	975
25/tcp	96	99	145	340
22/tcp	126	84	80	290
21/tcp	63	23	9	95
31385/udp	20	14	11	45
2632/udp	16	17	12	45
61222/udp	17	16	10	43
16358/udp	17	7	5	29
445/tcp	11	10	7	28
1433/tcp	3	10	13	26
3389/tcp	8	11	3	22
443/tcp	0	0	20	20
23/tcp	9	5	6	20
/udp	0	0	17	17
110/tcp	6	2	0	8
3306/tcp	1	1	3	5
8080/tcp	2	0	2	4
5900/tcp	0	0	3	3
8621/tcp	0	0	2	2
19/udp	2	0	0	2
その他	4	4	17	25
月別合計	753	536	755	2044

その他に分類されるインシデントの件数は、450 件でした。前四半期の 274 件から 64%増加しています。

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】
本四半期は、標的型攻撃に関する連絡を 67 組織に行っています。そのうち 52 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。また、Emdivi の対応の他に、PlugX とよばれる遠隔操作マルウエアや、アクセスした端末の情報を収集する ScanBox とよばれる JavaScript のツールなどに関連して、被害組織やインフラとして使用されていたサーバを管理する組織へ連絡を行いました。

7 月には、国内 Web サイトが改ざんされて、Emdivi の感染経路として使用された事例を複数確認しました。また、8 月以降も、Emdivi を添付して送りつけられる標的型攻撃メールの事例を確認しています。

攻撃者は Emdivi に感染した端末を踏み台として、組織内ネットワークの AD サーバや他の端末に侵入し、マルウエア感染の拡大や情報の窃取を試みます。攻撃は一般的に次のような手順で行われていました。

(1)なりすましメールや Web サイト改ざんによる攻撃で PC をマルウエアに感染させ、攻撃の踏み台とする端末を組織内に作り出す。
(2)感染端末上で ipconfig、netstat などの OS の標準コマンドを実行し、端末やネットワークの情報を収集する。収集した情報をマルウエアの C&C サーバに送信する。
(3)感染端末上で攻撃に使用する次のようなツールをダウンロードする。

- AD の情報を取得する Microsoft 製の正規のツール
- ログインアカウントのパスワードを窃取する不正なツール
- Kerberos KDC の脆弱性(MS14-068)を悪用し、権限昇格するツール
- 遠隔操作に使用するリモートシェルのクライアントおよびサーバ
- ファイル圧縮ツール

(4)何らかの方法で AD の管理者アカウントを窃取する。AD の管理者アカウントを窃取するために上記のようなツールを使用している可能性が高いと推測されるが、解明するための痕跡を発見できないことが多い。
(5) AD の管理者アカウントを使用して、AD サーバ上でマルウエアをインストールするタスクを登録し、AD サーバをマルウエアに感染させる。また、組織内ネットワーク上の端末をマルウエアに感染させる。
(6)組織内ネットワーク上の端末やサーバから文書ファイルなどを収集し、ファイル圧縮ツールでパスワード付きの圧縮ファイルにまとめて外部に送信する。ファイルの送信先としてオンラインストレージが使用されることがある。

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。

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 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２７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。