JPCERT CC®

JPCERT-IR-2011-0004
発行日: 2011-10-11

JPCERT/CC インシデント報告対応レポート
[2011 年 7 月 1 日 ～ 2011 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、2011 年 7 月 1 日から 2011 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、国際的な調整・支援が必要となるインシデントについて、日本の窓口組織として、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。この活動を通じて、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しています。

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）	574	687	457	1718	1567
インシデント件数 （注 3）	594	650	432	1676	1562
調整件数（注 4）	157	296	189	642	654

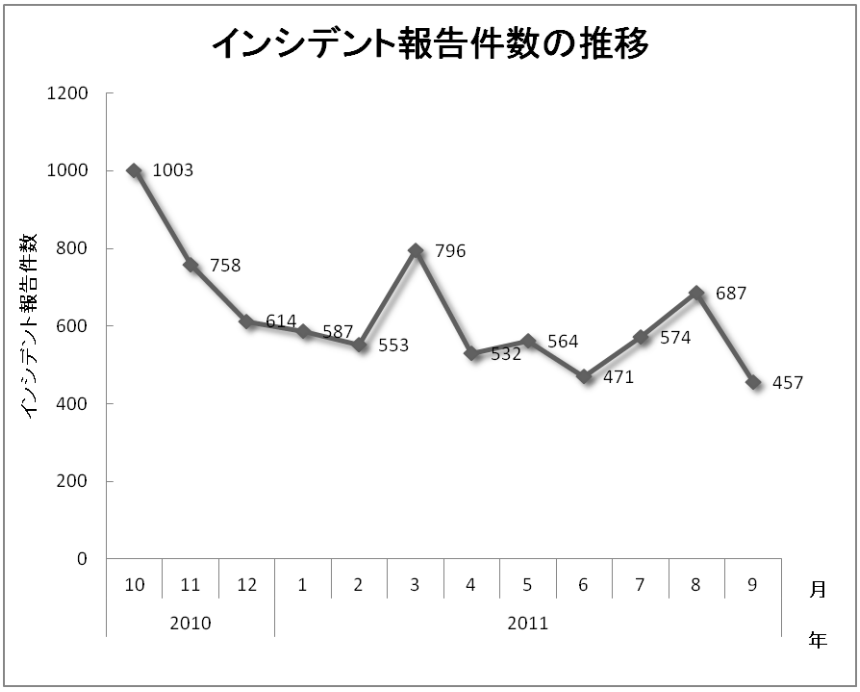
【注 2】「報告件数」は、報告者から寄せられた Web フォーム、メール、FAX による報告の総数を示します。

【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。ただし、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は、1 件のインシデントとして扱います。

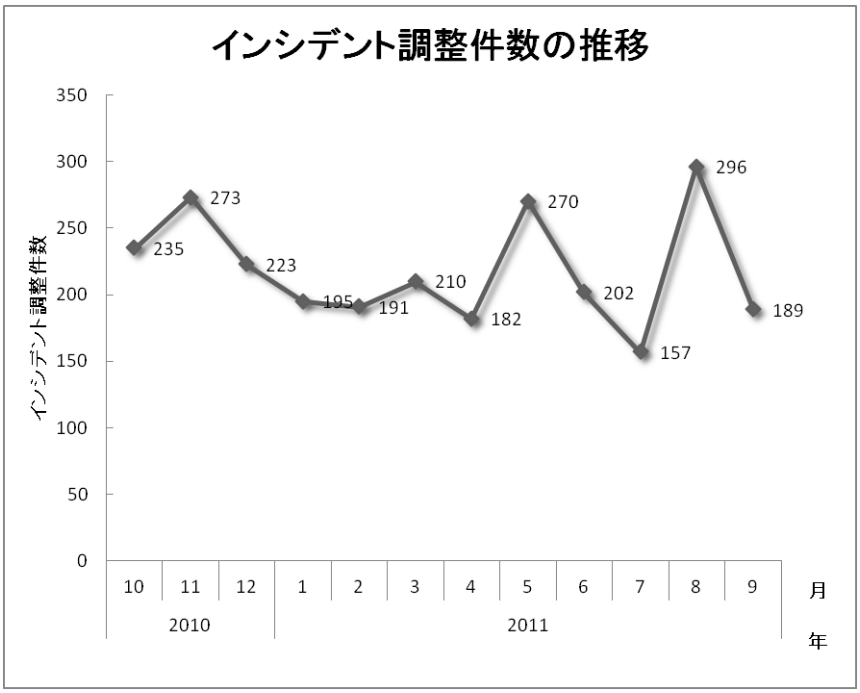
【注 4】「調整件数」とは、インシデントの拡大防止のため、サイトの管理者などに対し、現状の調査と問題解決のための対応を依頼した件数を示します。

本四半期に寄せられた報告件数は、1718 件でした。また、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 642 件で、前四半期の 654 件と比較して、2% 減少しています。

[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]



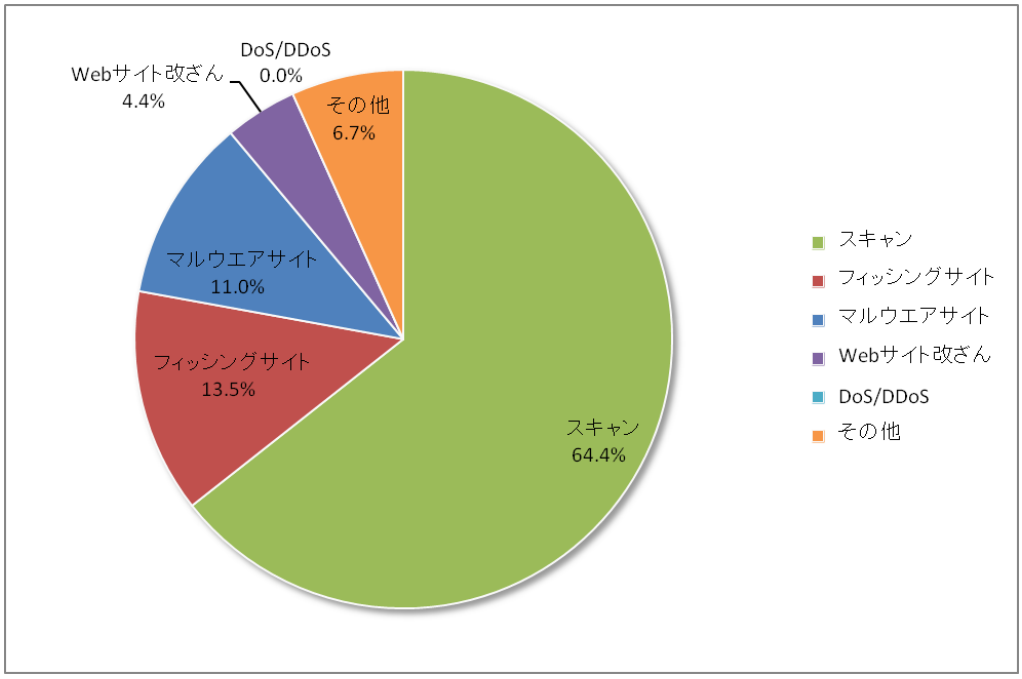
[図 2 インシデント調整件数の推移]

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。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]

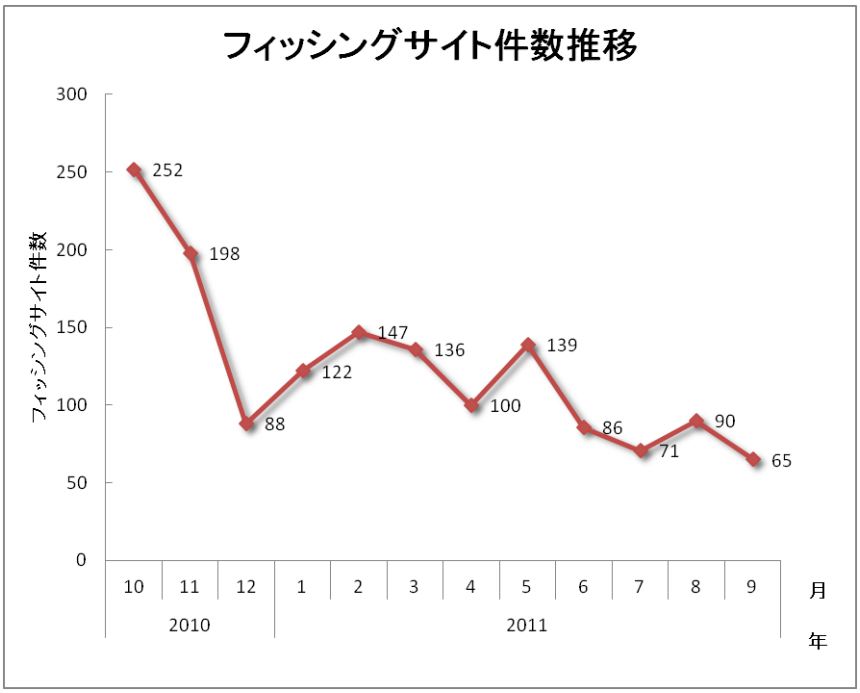
インシデントカテゴリ	7 月	8 月	9 月	合計	前四半期合計
フィッシングサイト	71	90	65	226	325
Web サイト改ざん	14	28	31	73	34
マルウエアサイト	38	86	61	185	121
スキャン	429	398	252	1079	958
DoS/DDoS	0	0	0	0	1
その他	42	48	23	113	123

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 64.4% と大きな割合を占めています。フィッシングサイトに分類されるインシデントが 13.5% を占めています。また、Web サイト改ざんに分類されるインシデントは 4.4% でした。

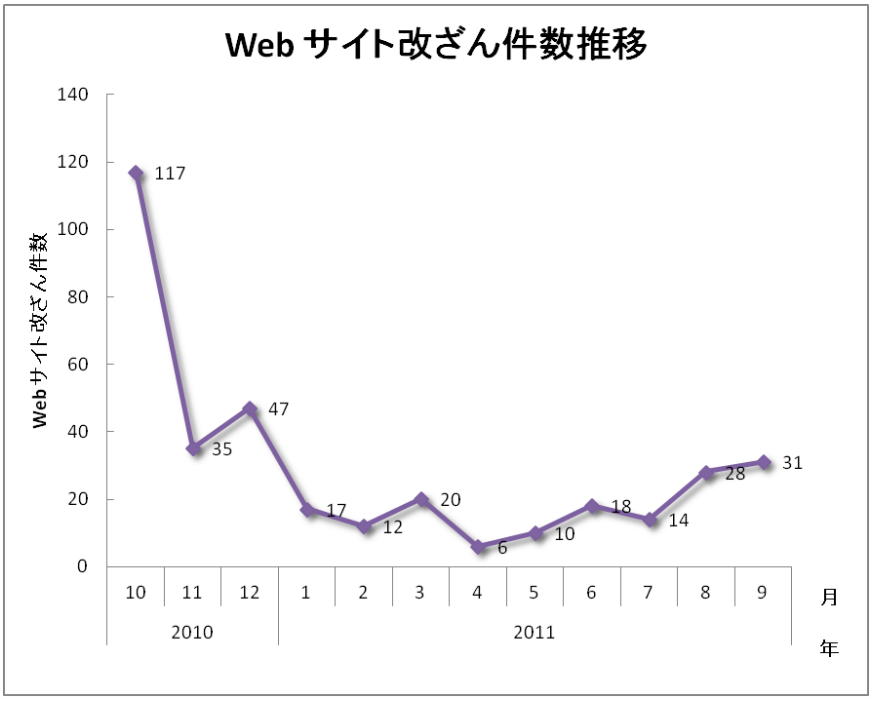


[図 4 インシデントのカテゴリ別割合]

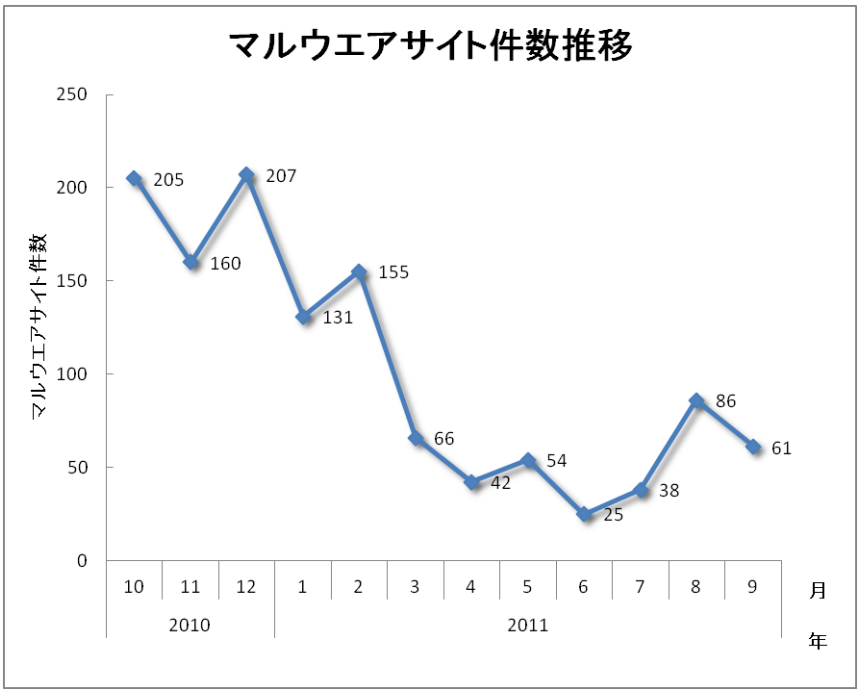
[図 5]から[図 8]に、フィッシングサイト、Web サイト改ざん、マルウエアサイト、スキャンのインシデントの過去 1 年間の月別推移を示します。



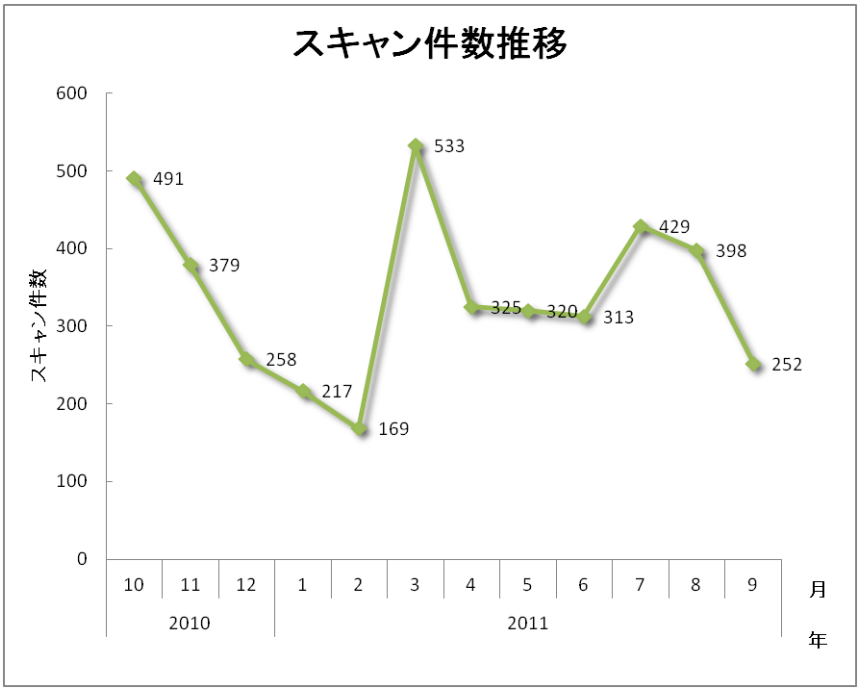
[図 5 フィッシングサイト件数推移]



[図 6　Web サイト改ざん件数推移]

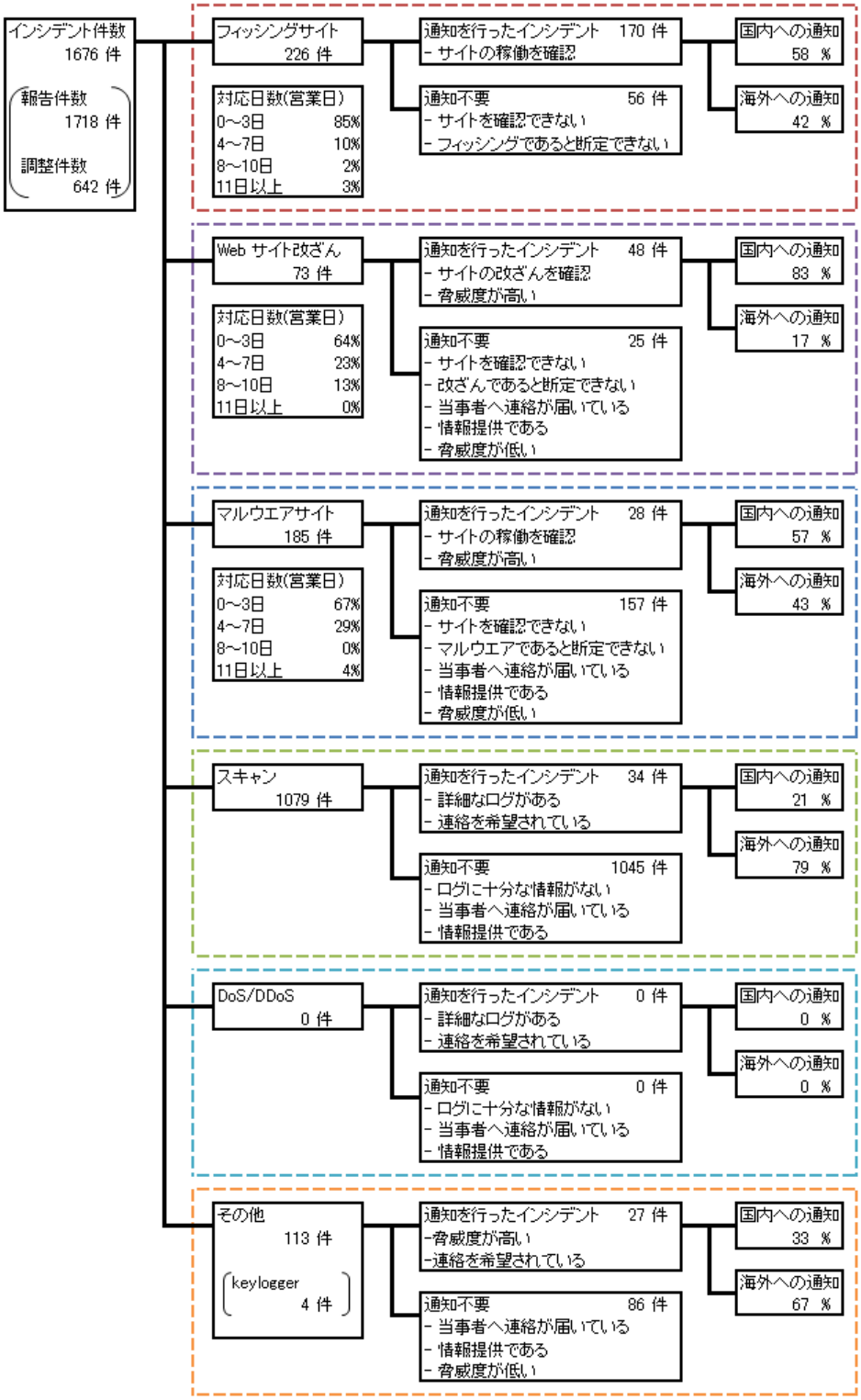


[図 **7** マルウエアサイト件数推移]



[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]

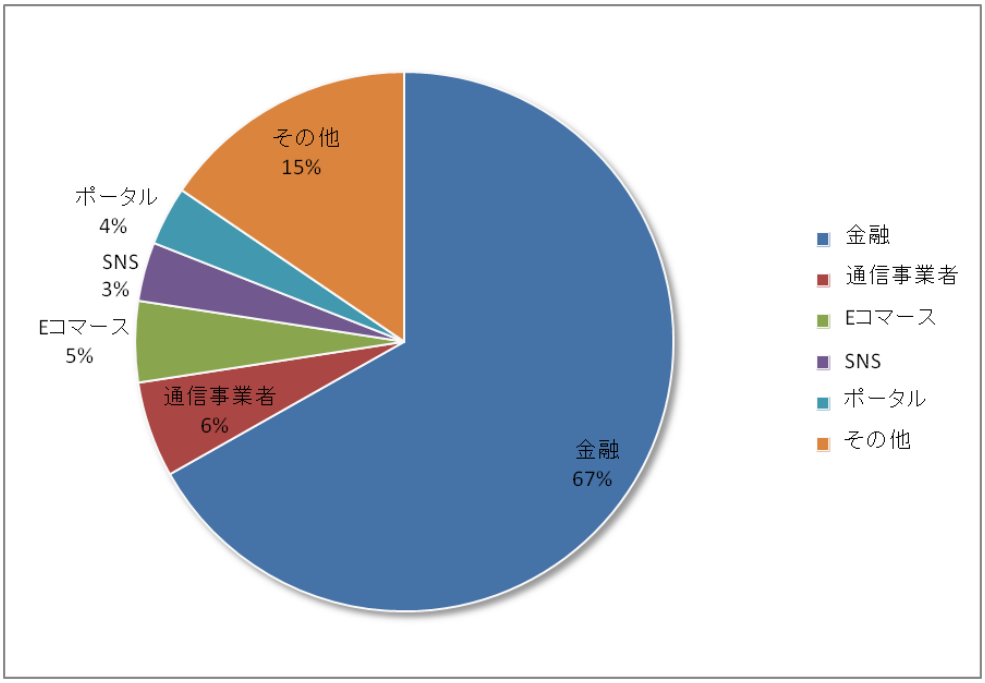
3. インシデントの傾向

本章で説明する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。

本四半期に報告が寄せられたフィッシングサイトの件数は 226 件で、前四半期の 325 件から 30% 減少しました。また、前年度同四半期（487 件）との比較では、54% 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] 、フィッシングサイトのブランド種別割合を [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	7 月	8 月	9 月	国内外別合計（割合）
国内ブランド	9	4	18	31(14%)
国外ブランド	53	77	35	165(73%)
ブランド不明	9	9	12	30(13%)
月別合計	71	90	65	226(100%)



[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 31 件と、前四半期の 118 件から 74% 減少しました。これは、前四半期まで多数報告されていた国内ポータルサイトを装ったフィッシングサイトが大幅に減少したためです。
国内ポータルサイトを装ったフィッシングサイトは、2009 年 6 月以降、大量に確認されていました。これらのフィッシングサイトの特徴は、攻撃者が第三者のサーバに侵入してフィッシングサイトを設置する宿借り型ではなく、レンタルサーバや、動的 DNS サービスを使用してモバイルネットワーク上の PC に設置した持ち家型だったことです。
2011 年 6 月末に国内ポータルサイトを装ったフィッシング詐欺を行っていたグループが逮捕され、このグループの活動が停止したことにより、本四半期における国内ポータルサイトを装うフィッシングサイトの報告は大幅に減少しました。
一方、国外ブランドを装ったフィッシングサイトの件数も 165 件と、前四半期の 173 件から 5% 減少しました。

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% と、前四半期の割合（国内 42%、国外 58%）と比較して、国内への調整が増えました。
前四半期の国内ポータルサイトを装ったフィッシングサイトの多くは海外レンタルサーバを使用していましたが、このタイプのフィッシングサイトが減少したことによって海外への通知が減ったためです。

また、フィッシングサイトのうち、金融関連のサイトを装ったものが 67% を占めました。前四半期のブランド種別割合では、金融関連サイトが 45%、ポータルサイトが 35 % を占めていましたが、本四半期は国内ポータルサイトを装ったフィッシングサイトの減少により、フィッシングサイトのブランド種別においてポータルサイトが占める割合が 4 % まで減少し、相対的に金融関連サイトが占める割合が 45%から 67%に増加しました。

本四半期に報告が寄せられた Web サイト改ざんの件数は、73 件でした。前四半期の 34 件から 115% 増加しています。
7 月から 8 月にかけて、検索サイトの画像検索結果を悪用した攻撃に組み込まれたサイトと、オープンソースの E コマースサイト構築アプリケーションである osCommerce を使用したサイトに対する改ざんが多数報告されました。

画像検索結果を悪用した攻撃では、攻撃者が脆弱なサーバに悪意のあるファイルを設置し、画像検索サイトで人気の高いキーワードで関連した画像を閲覧した際にウイルス対策ソフトを装ったマルウエアをダウンロードさせるサイトに誘導する仕組みになっていました。

osCommerce を使用したサイトに対する改ざんでは、title タグなどの後ろに iframe や JavaScript が埋め込まれており、ページの読み込み時に不審なサイトにアクセスさせる仕組みになっていました。

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、185 件でした。前四半期の 120 件から 53% 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、1079 件でした。前四半期の 958 件から 13% 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。

[表 5: ポート別のスキャン件数]

ポート	7 月	8 月	9 月	合計
80/tcp	285	233	127	645
22/tcp	69	79	75	223
25/tcp	62	44	48	154
/icmp	1	27	0	28
445/tcp	2	7	0	9
3389/tcp	0	4	0	4
21/tcp	1	3	0	4
110/tcp	1	2	0	3
5900/tcp	0	0	2	2
/udp	2	0	0	2
9415/	0	1	0	1
1433/tcp	0	1	0	1
143/tcp	0	1	0	1
不明	6	3	0	9
月別合計	429	405	252	1086

スキャンの対象となったポートは、http(80/tcp)、ssh(22/tcp)、smtp(25/tcp)の順に多く確認しています。ssh に対するスキャンは、不正侵入することを目的としたブルートフォース攻撃を多く確認しています。8 月後半には、RDP (3389/tcp) に対するスキャンを複数確認しています。

インシデント対応事例

以下に、本四半期に行った対応の例を紹介します。

【 国内金融機関を装ったフィッシング】

2011 年 8 月末から、複数の国内金融機関を装ったフィッシングメールが確認されています。フィッシングメールには実行ファイルが添付されており、これを実行すると、インターネットバンキングの ID 、パスワードなどの入力を促す画面が表示され、入力した情報は攻撃者の用意したサーバに送信されます。添付された実行ファイルによって送信先サーバが異なっており、国内、海外の複数のサーバが送信先として使用されています。JPCERT/CC では、実行ファイルを分析して情報送信先のサーバを特定し、サーバを管理する組織や National CSIRT に対応を依頼しています。海外の National CSIRT や、捜査機関などとも連携した対応により、送信先サーバの停止を順次確認していますが、現在も送信先サーバを変更した実行ファイルが報告され、JPCERT/CC は対応を継続しています。

【Remote Desktop (RDP) TCP 3389 番ポートに対するスキャン】

2011 年 8 月中旬より Remote Desktop (RDP) TCP 3389 番ポートへのスキャンが増加していることを、JPCERT/CC が運用するインターネット定点観測システム (ISDAS) において確認しました。これは、TCP 3389 番ポートにスキャンを行い、その後に脆弱なパスワードのクラックなどを通じ、感染活動を行うマルウエア (Morto) によるものと考えられます。観測データを分析した結果、国内の複数アドレスからスキャンが行われていたことが判明したため、当該ネットワークの管理者に連絡をおこない、マルウエア駆除等の対応を依頼しました。8 月下旬以降はスキャンが減少していますが、マルウエアの活動が一時的に停止している可能性も考えられるため、念のため注意喚起を発行しました。

【MasterCard を装ったフィッシング】

2011 年 8 月の初旬に、MasterCard を装ったフィッシングメールに関する報告を多数受領しました。フィッシングメールから誘導されるフィッシングサイトでは日本語が使用されているため、日本人を標的とした攻撃と推定されます。また、このフィッシングで使用されたフィッシングサイトの多くは海外に設置されていました。JPCERT/CC は、フィッシングサイトが設置されているネットワークの ISP へ依頼をするとともに、同地域の National CSIRT へ協力を要請し、サイトの停止を行っています。

4. 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/

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

5. [付録]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。

- Gumblar ウイルスによる不審なスクリプト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

○ 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２３年度コンピュータセキュリティ早期警戒体制の整備（不正アクセス行為等対策業務）」事業として実施したものです。