JPCERT-IR-2012-02
発行日: 2012-10-10

JPCERT/CC インシデント報告対応レポート
[2012 年 7 月 1 日 ～ 2012 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、2012 年 7 月 1 日から 2012 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、各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。

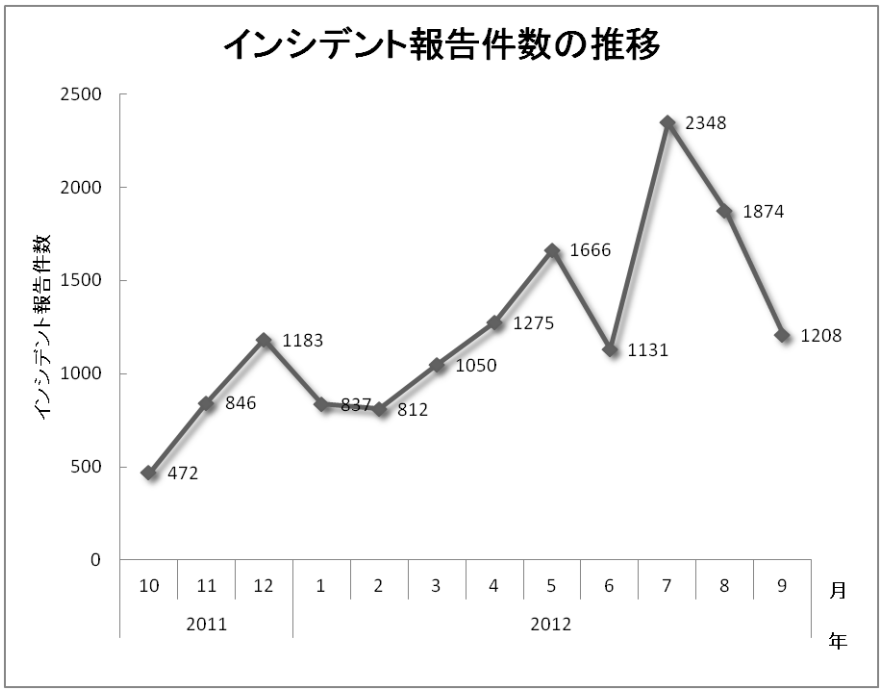
[表 1 インシデント報告関連件数]

	7 月	8 月	9 月	合計	前四半期合計
報告件数 (注 2)	2348	1874	1208	5430	4072
インシデント件数 （注 3）	2243	1835	1188	5266	3832
調整件数（注 4）	283	411	429	1123	756

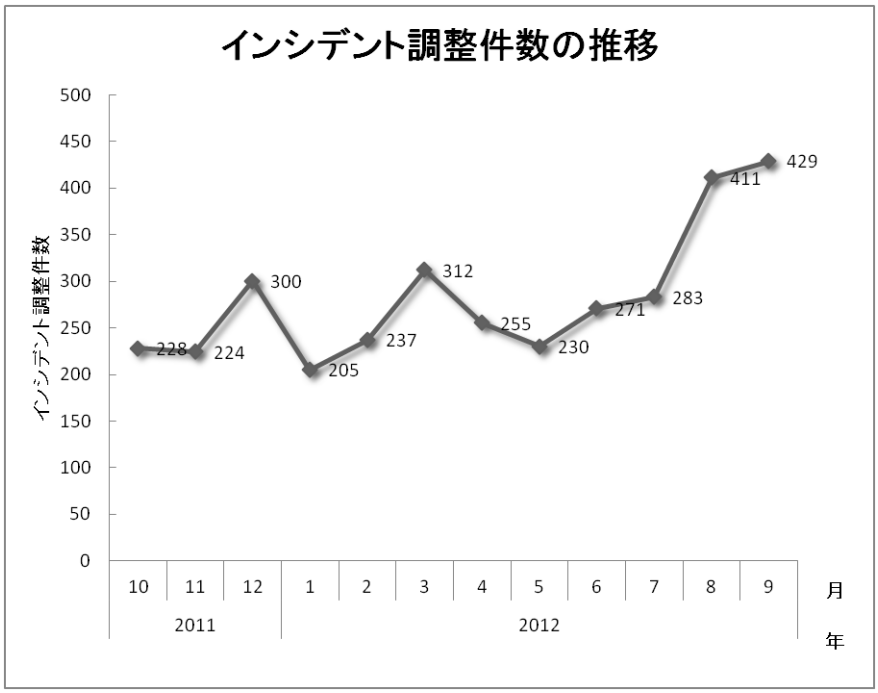
【注 2】「報告件数」は、報告者から寄せられた Web フォーム、メール、FAX による報告の総数を示します。
【注 3】「インシデント件数」は、各報告に含まれるインシデント件数の合計を示します。ただし、1 つのインシデントに関して複数件の報告が寄せられた場合は、1 件のインシデントとして扱います。
【注 4】「調整件数」とは、インシデントの拡大防止のため、サイトの管理者などに対し、現状の調査と問題解決のための対応を依頼した件数を示します。

本四半期に寄せられた報告件数は、5430 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 1123 件でした。前四半期と比較して、総報告件数は 33%増加し、調整件数は 49%増加しました。また、前年同期と比較すると、総報告数で 216%増加し、調整件数は 75%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]



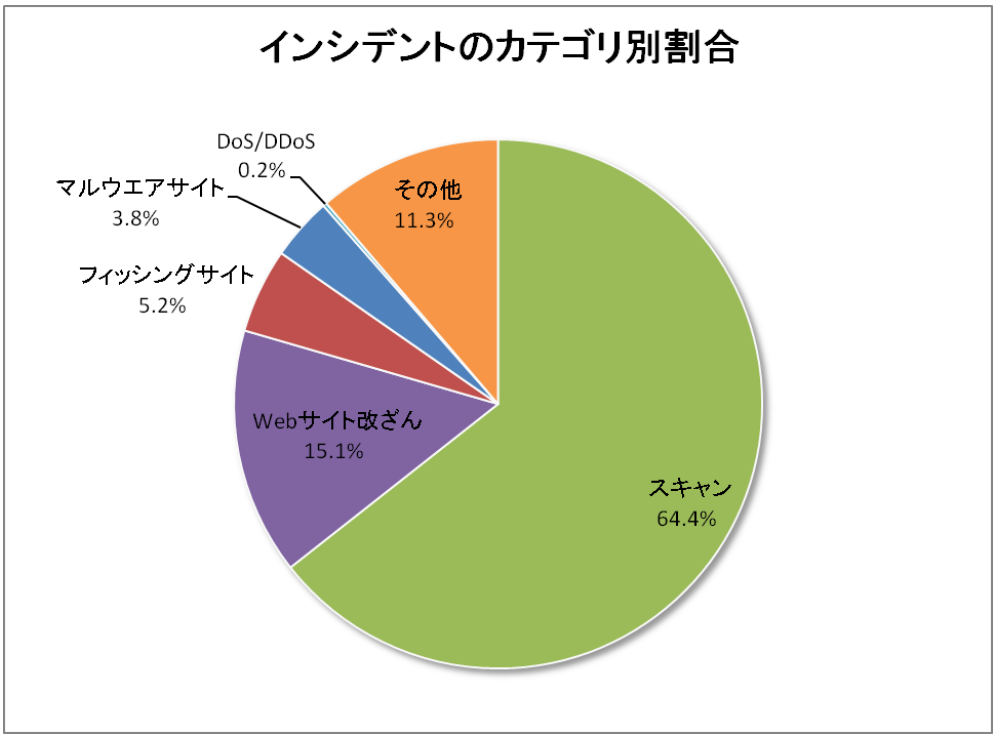
[図 2 インシデント調整件数の推移]

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]

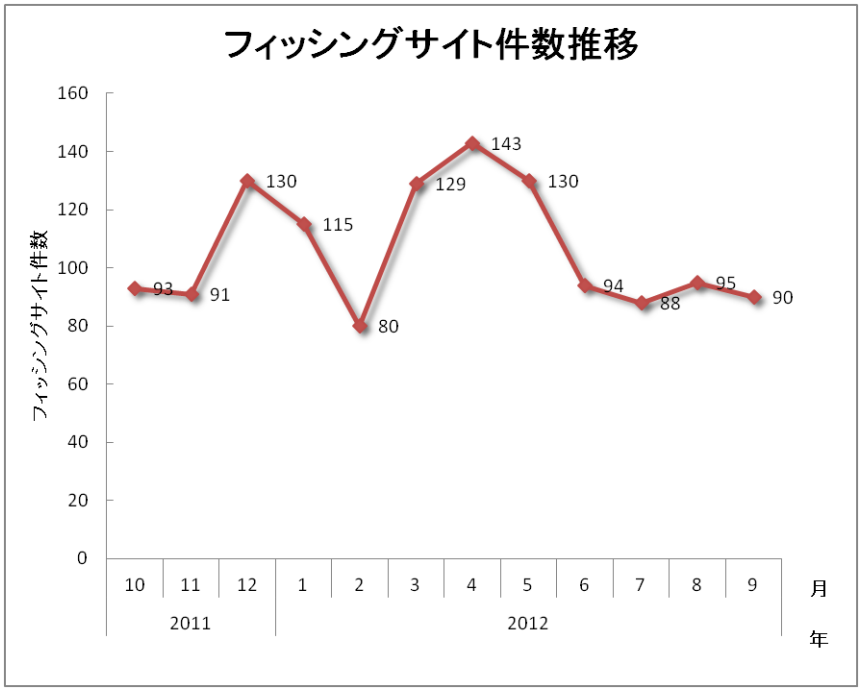
インシデントカテゴリ	7 月	8 月	9 月	合計	前四半期合計
フィッシングサイト	88	95	90	273	367
Web サイト改ざん	370	215	211	796	139
マルウエアサイト	76	42	84	202	209
スキャン	1563	1270	558	3391	2281
DoS/DDoS	3	2	7	12	11
その他	143	211	238	592	825

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 5.2%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 15.1%でした。

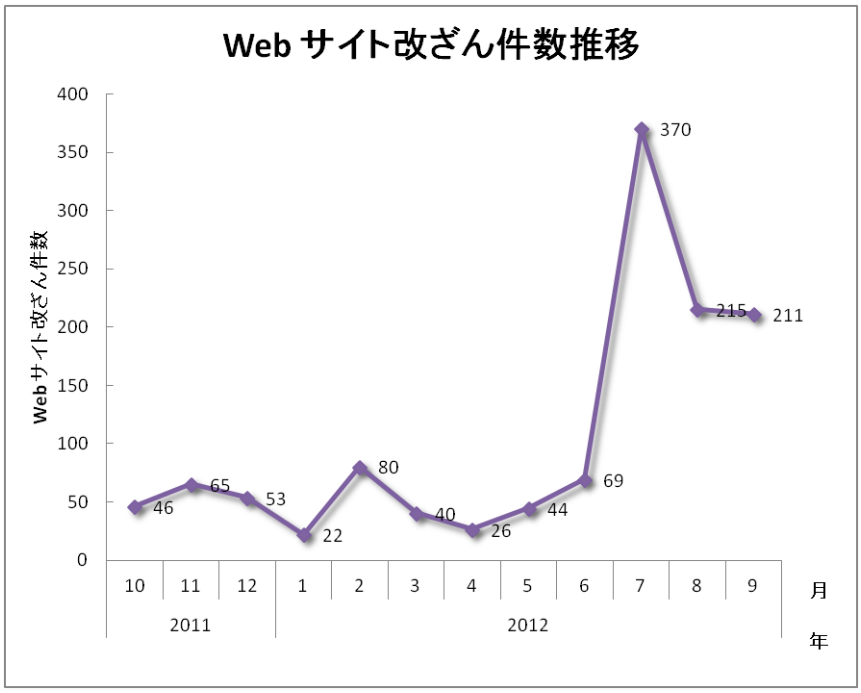


[図 4 インシデントのカテゴリ別割合]

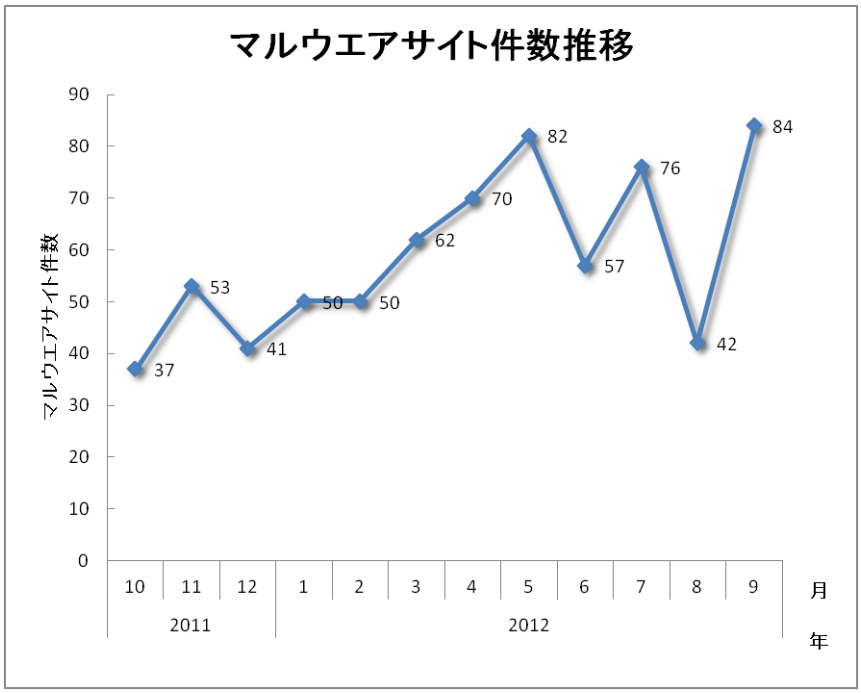
[図 5]から[図 8]に、フィッシングサイト、Web サイト改ざん、マルウエアサイト、スキャンのインシデントの過去 1 年間の月別推移を示します。



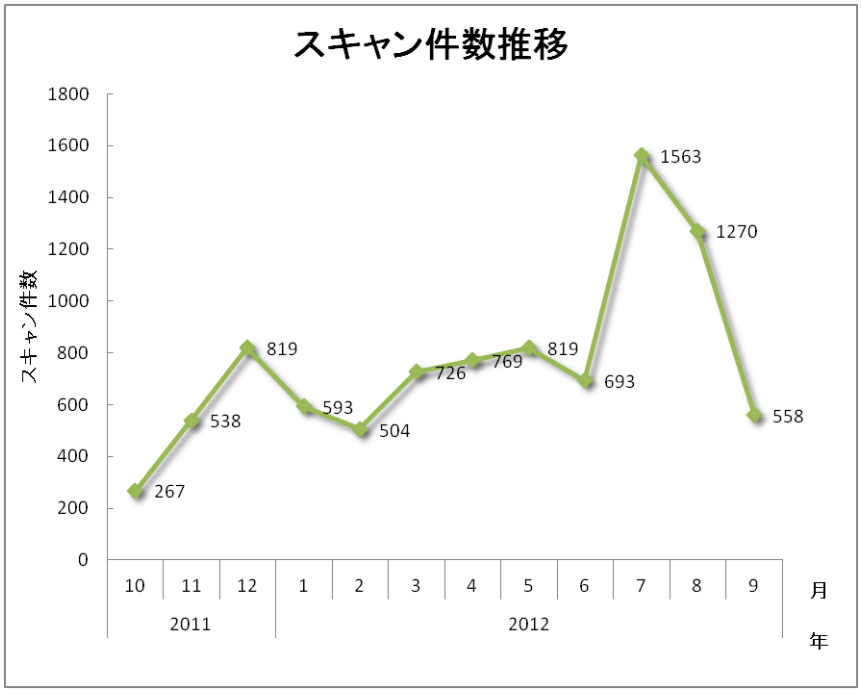
[図 5 フィッシングサイト件数推移]



[図 6 Web サイト改ざん件数推移]

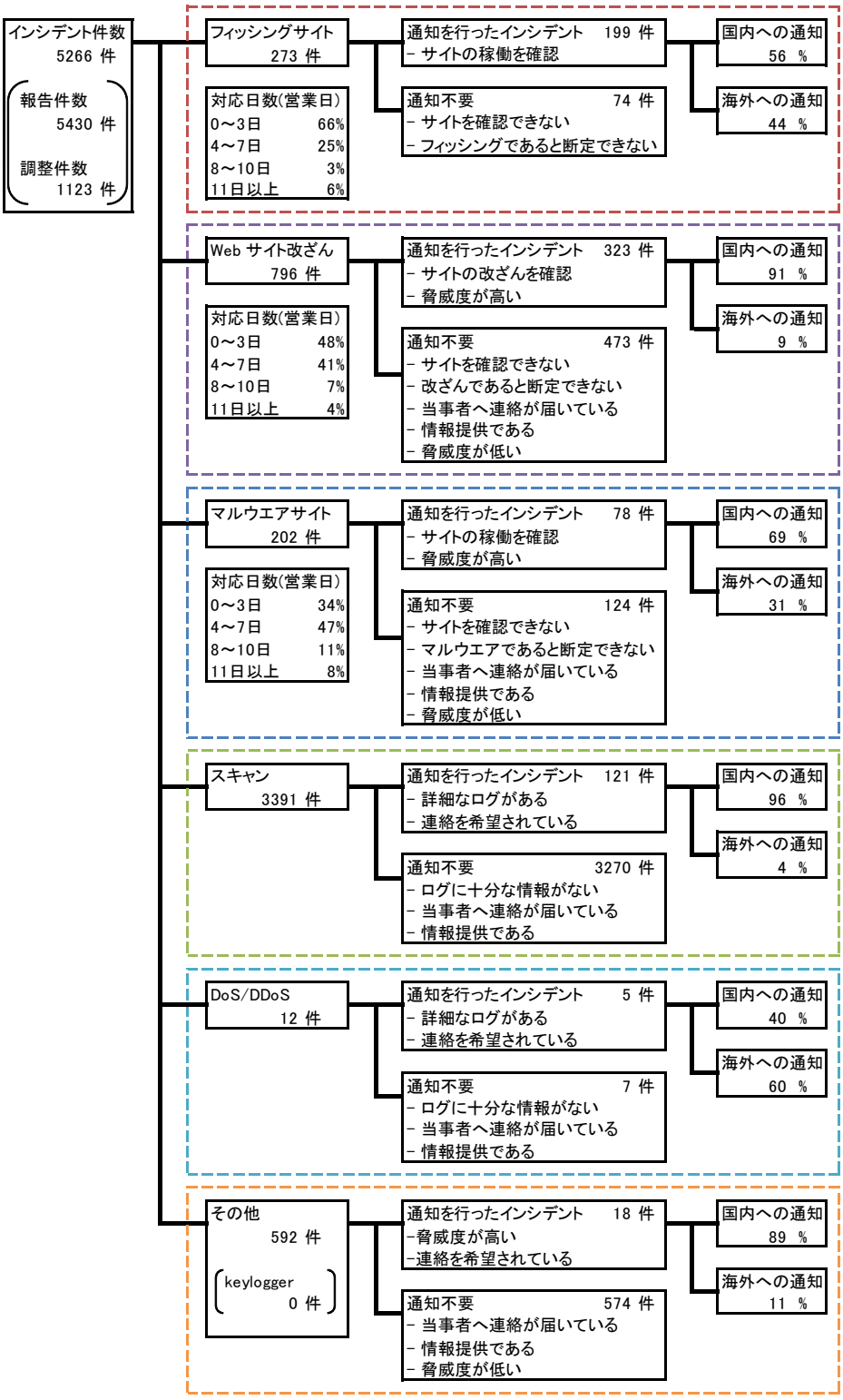


[図 7 マルウエアサイト件数推移]



[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

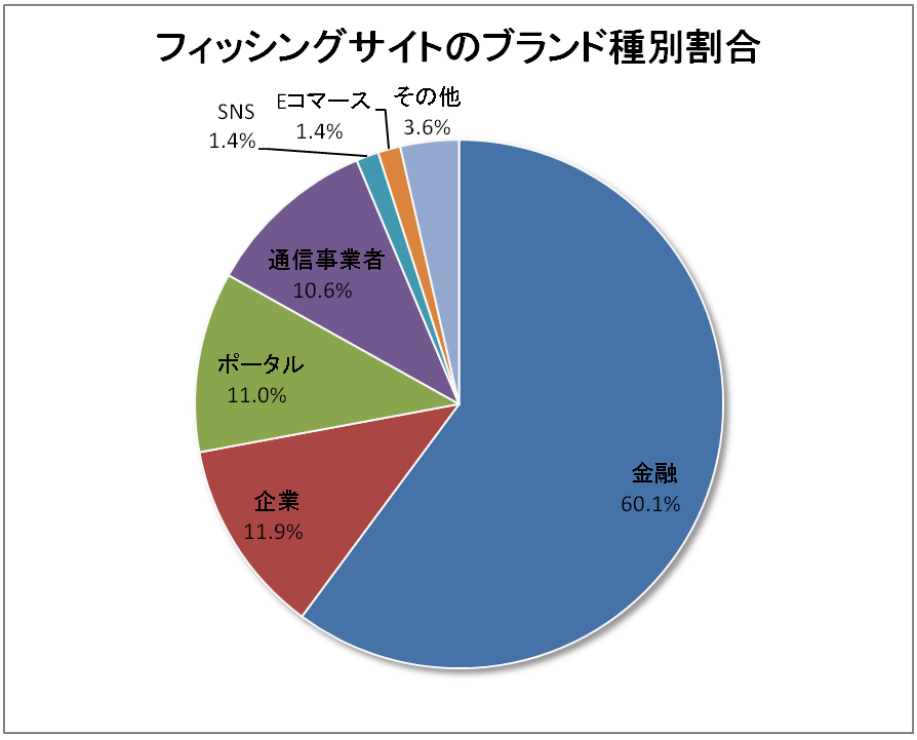
3.1. フィッシングサイトの傾向

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 273 件で、前四半期の 367 件から 26%減少しました。また、前年度同期（226 件）との比較では、21%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 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	7 月	8 月	9 月	国内外別合計（割合）
国内ブランド	17	26	14	57(21%)
国外ブランド	56	54	51	161(59%)
ブランド不明（注 5）	15	15	25	55(20%)
月別合計	88	95	90	273(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 57 件と、前四半期の 68 件から 16%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 161 件と、前四半期の 225 件から 28%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については、金融機関のサイトを装ったものが 60.1%を占めています。

本四半期は、国内通信事業者を装ったフィッシングサイトの報告が複数寄せられました。複数の異なるブランドのフィッシングサイトを確認しましたが、ブランドが異なっていても同じドメインを使用しているものや、サブディレクトリ名が類似しているものがありました。その背景としては、横断的に日本の通信事業者のアカウントの窃取を狙っている攻撃者か、日本の通信事業者を装うフィッシングサイトを構築するためのツールが存在するといった可能性が考えられます。

フィッシングサイトの調整先の割合は、国内が 56%、国外が 44%と、前四半期の割合（国内 50%、国外 50%）と比較して、国内への調整が増えました。

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、796 件でした。前四半期の 139 件から 473%増加しています。

本四半期は、Web サイトが使用する JavaScript ファイルが改ざんされているという報告が非常に多く寄せられたため、Web サイト改ざんの件数が大きく増加しています。この改ざんは、ホスティング・サービス業者などが利用している、あるサーバ管理ツールの脆弱性を使用して大規模に行われた可能性があります。

2012 年 8 月には、同月にゼロデイ脆弱性として公開された Java の脆弱性(CVE-2012-4681)が、改ざんされた Web サイトから誘導されるマルウエア配布サイトの攻撃に組み込まれたことを確認しました。この脆弱性を使用した攻撃により、古いバージョンの Java を使用していると、マルウエアに感染する危険性があります。

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、202 件でした。前四半期の 209 件から 3%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、3391 件でした。前四半期の 2281 件から 49%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	1361	1018	299	2678
25/tcp	105	83	128	316
22/tcp	63	56	69	188
udp	29	99	54	182
3389/tcp	1	36	2	39
143/tcp	1	0	8	9
icmp	1	1	3	5
21/tcp	0	0	4	4
23/tcp	0	2	1	3
110/tcp	1	0	1	2
5900/tcp	0	1	1	2
139/tcp	0	1	0	1
8080/tcp	0	1	0	1
不明	1	0	11	12
月別合計	1563	1298	581	3442

スキャンの対象となったポートは、http(80/tcp)、smtp(25/tcp)、ssh(22/tcp)の順でした。udp については、SIP(5060/udp) などへのスキャンを確認しています。

4. 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。

【サーバ管理ツールの脆弱性を使用した Web サイト改ざん】
2012 年 7 月以降、Web サイトが使用する JavaScript ファイルが改ざんされているという報告を多数受領しています。改ざんされたサイトは、特定のサーバ管理ツールを使ったホスティング事業者のサーバ上に構築されているという共通点がありました。この管理ツールの脆弱性を悪用した攻撃によって、ホスティング・サービスを利用しているユーザのアカウントが窃取され、JavaScript ファイルが改ざんされた可能性があります。改ざんされた JavaScript ファイルには、末尾に難読化されたコードが挿入されたり、末尾にコードを挿入した後にファイル全体が難読化されたりしていました。挿入されたコードの動作は、アクセスした日時から動的に誘導先サイトのドメインの文字列を生成し、サイトに誘導するための iframe タグをページに追加するものでした。誘導先となるサイトのドメインは 12 時間ごとに変化する仕組みになっており、使用されるドメインはあらかじめ登録されていました。最終的に誘導されるサイトでは、複数の脆弱性を使用した攻撃により、偽ウイルス対策ソフトが PC にインストールされることを確認しました。
JPCERT/CC では、改ざんされたサイトの管理者に対応を逐次依頼しております。

【国内金融機関を装ったマルウエア配布サイト】
2012 年 7 月、国内金融機関を装ったフィッシングメールの報告を受領しました。メール内のリンクから誘導されるサイトは国内金融機関を装ったものでしたが、アカウント情報を入力するフォームなどはなく、サイトの末尾には不審な Java アプレットが埋め込まれていました。分析の結果、Java アプレットは Java の脆弱性(CVE-2012-1723)を使用した攻撃によって PC にマルウエアをインストールし、その結果 PC は海外のサーバに https で通信を行うことが分かりました。
JPCERT/CC は、国内金融機関を装ったサイトと、マルウエアが接続する先のサーバの管理者に対応を依頼し、これらが停止したことを確認しました。

【国内の多数の Web サイト改ざん】
2012 年 9 月中旬、国内の Web サイトが改ざんされているという報告を短期間に集中して受領しました。これらの一連の Web サイト改ざんでは、尖閣諸島に関する中国側の意見を主張する画像が挿入されていましたが、改ざんの対象となったサイトについては、業種や規模などに共通性は見いだせませんでした。日本のサイトを対象に検索ツールを使って脆弱性を探しまわり、発見した脆弱点をついてサイトに不正に侵入し、用意した画像を設置する手法がとられたと考えられます。

JPCERT/CC は、Web サイト管理者に対応を依頼し、順次 Web サイトが修正されていることを確認しました。

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 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

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。

- 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２４年度情報セキュリティ対策推進事業（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。