JPCERT-IR-2012-01
発行日: 2012-07-12

JPCERT/CC インシデント報告対応レポート
[2012 年 4 月 1 日 ～ 2012 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、2012 年 4 月 1 日から 2012 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、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。

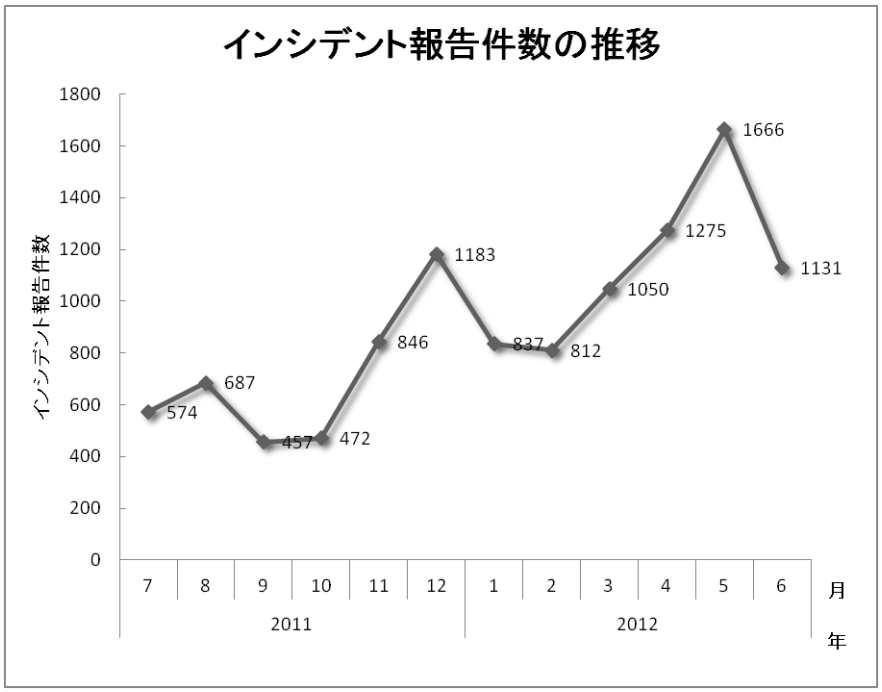
[表 1 インシデント報告関連件数]

	4 月	5 月	6 月	合計	前四半期合計
報告件数 (注 2)	1275	1666	1131	4072	2699
インシデント件数 （注 3）	1227	1505	1100	3832	2535
調整件数（注 4）	255	230	271	756	754

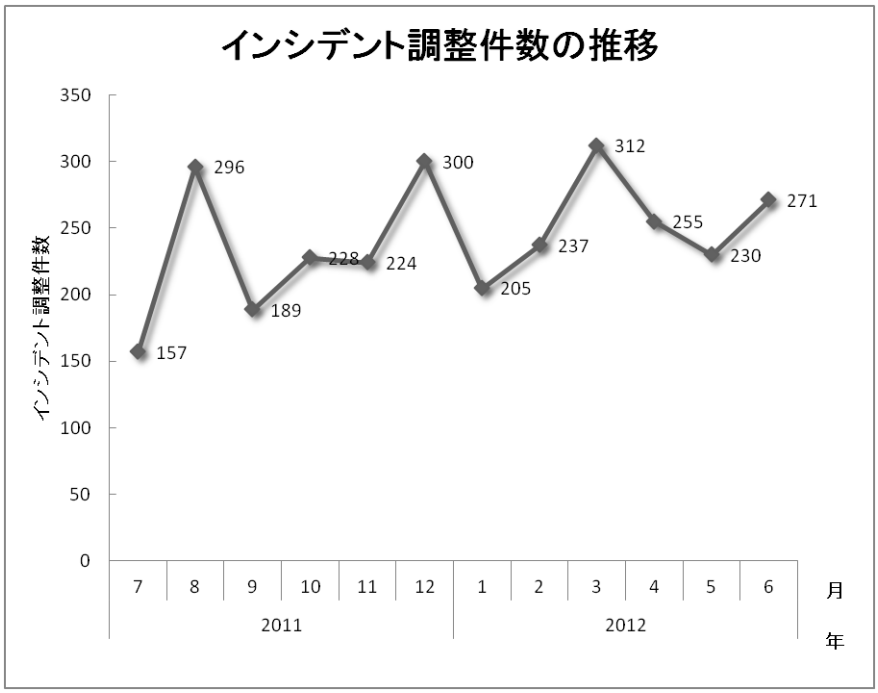
【注 2】「報告件数」は、報告者から寄せられた Web フォーム、メール、FAX による報告の総数を示します。
【注 3】「インシデント件数」は、各報告に含まれるインシデント件数の合計を示します。ただし、1 つのインシデントに関して複数件の報告が寄せられた場合は、1 件のインシデントとして扱います。
【注 4】「調整件数」とは、インシデントの拡大防止のため、サイトの管理者などに対し、現状の調査と問題解決のための対応を依頼した件数を示します。

本四半期に寄せられた報告件数は、4072 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 756 件でした。前四半期と比較して、総報告件数は 51%増加し、調整件数は 0.3%増加しました。また、前年同期と比較すると、総報告数で 160%増加し、調整件数は 16%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]



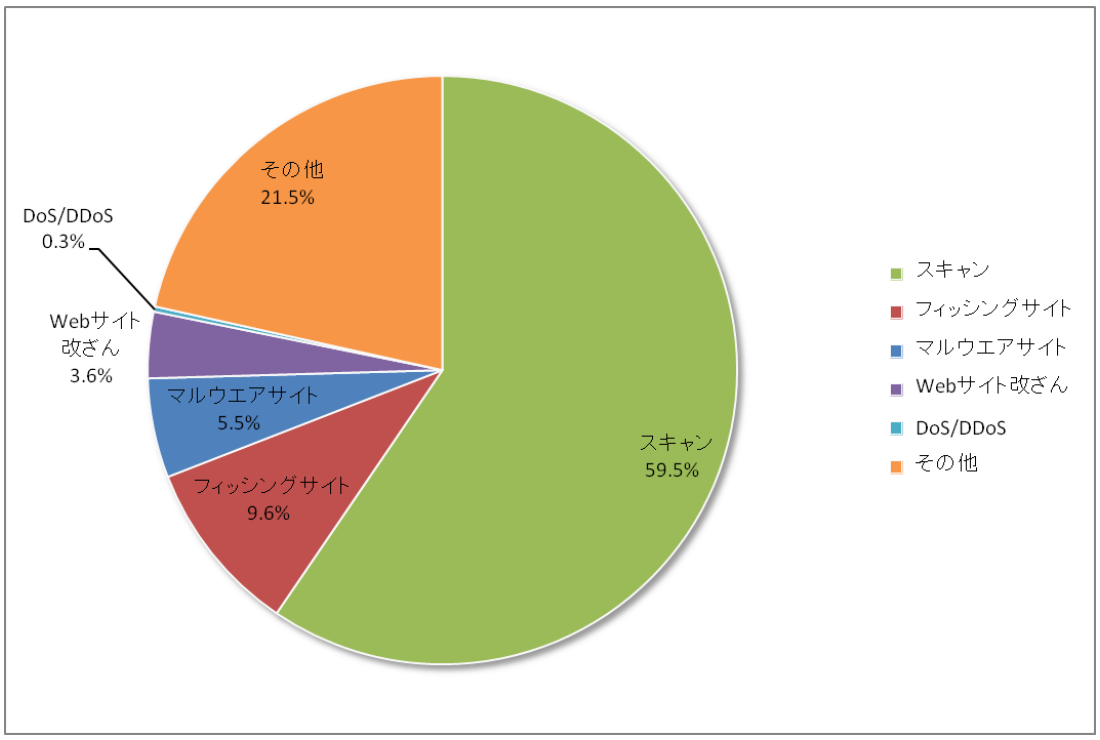
[図 2 インシデント調整件数の推移]

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]

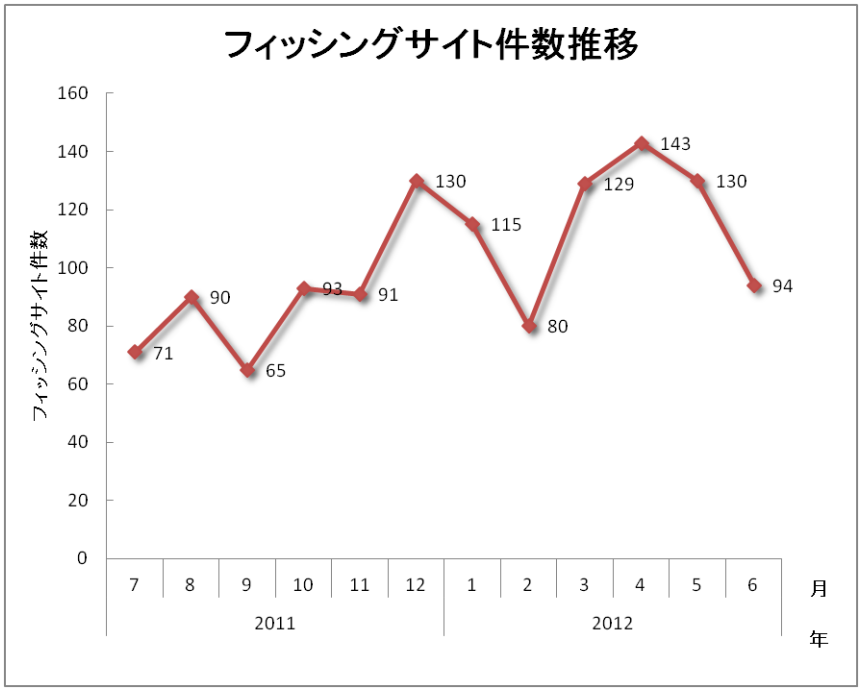
インシデントカテゴリ	4 月	5 月	6 月	合計	前四半期合計
フィッシングサイト	143	130	94	367	324
Web サイト改ざん	26	44	69	139	142
マルウエアサイト	70	82	57	209	162
スキャン	769	819	693	2281	1823
DoS/DDoS	4	5	2	11	7
その他	215	425	185	825	77

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 59.5%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 9.6%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 3.6%でした。

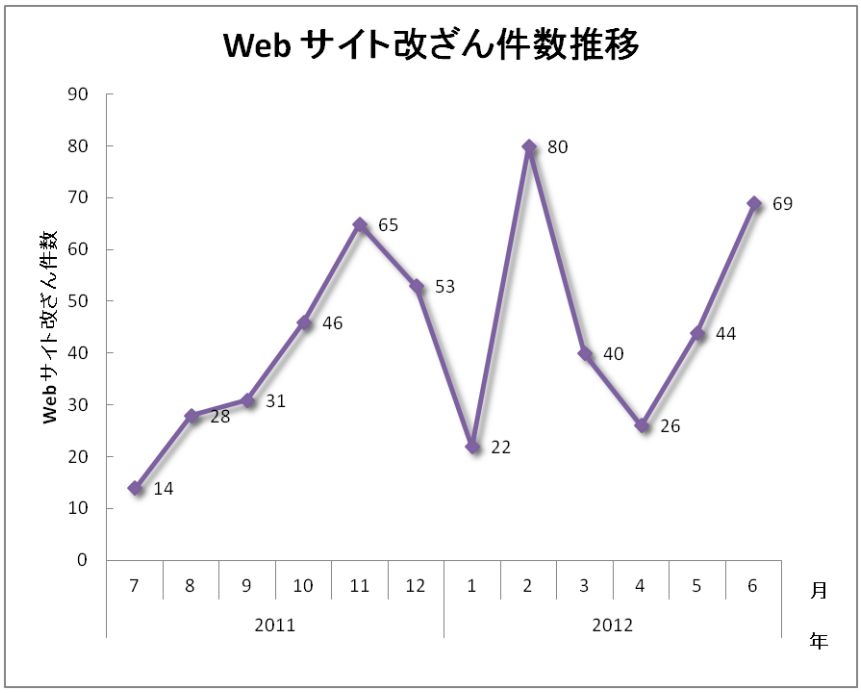


[図 4 インシデントのカテゴリ別割合]

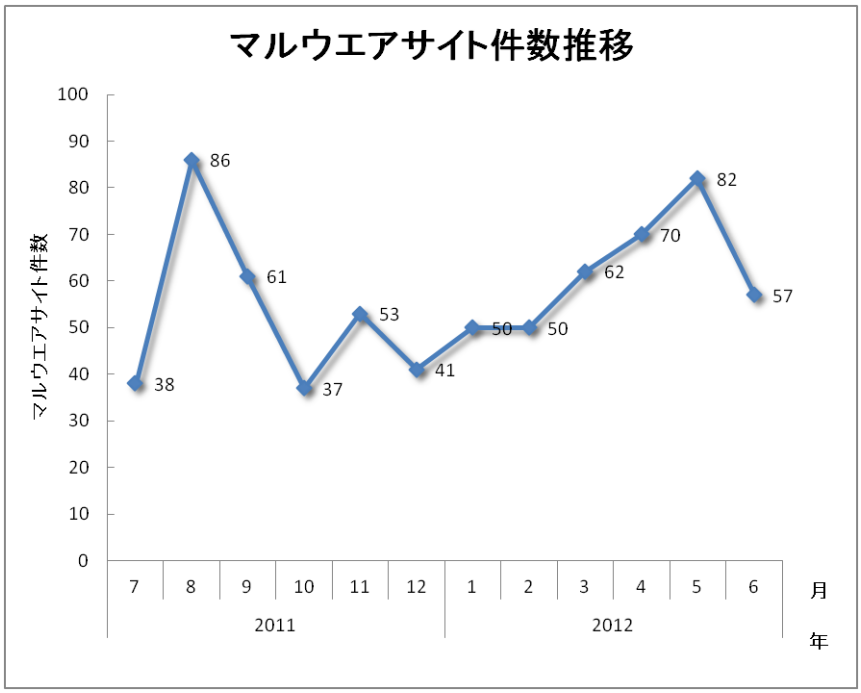
[図 5]から[図 8]に、フィッシングサイト、Web サイト改ざん、マルウエアサイト、スキャンのインシデントの過去 1 年間の月別推移を示します。



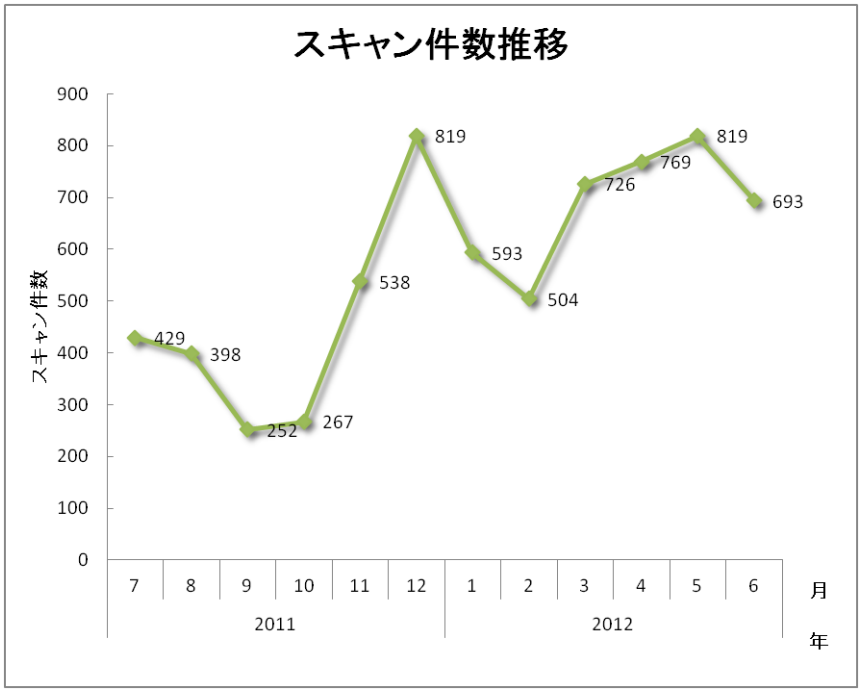
[図 5 フィッシングサイト件数推移]



[図 6 Web サイト改ざん件数推移]

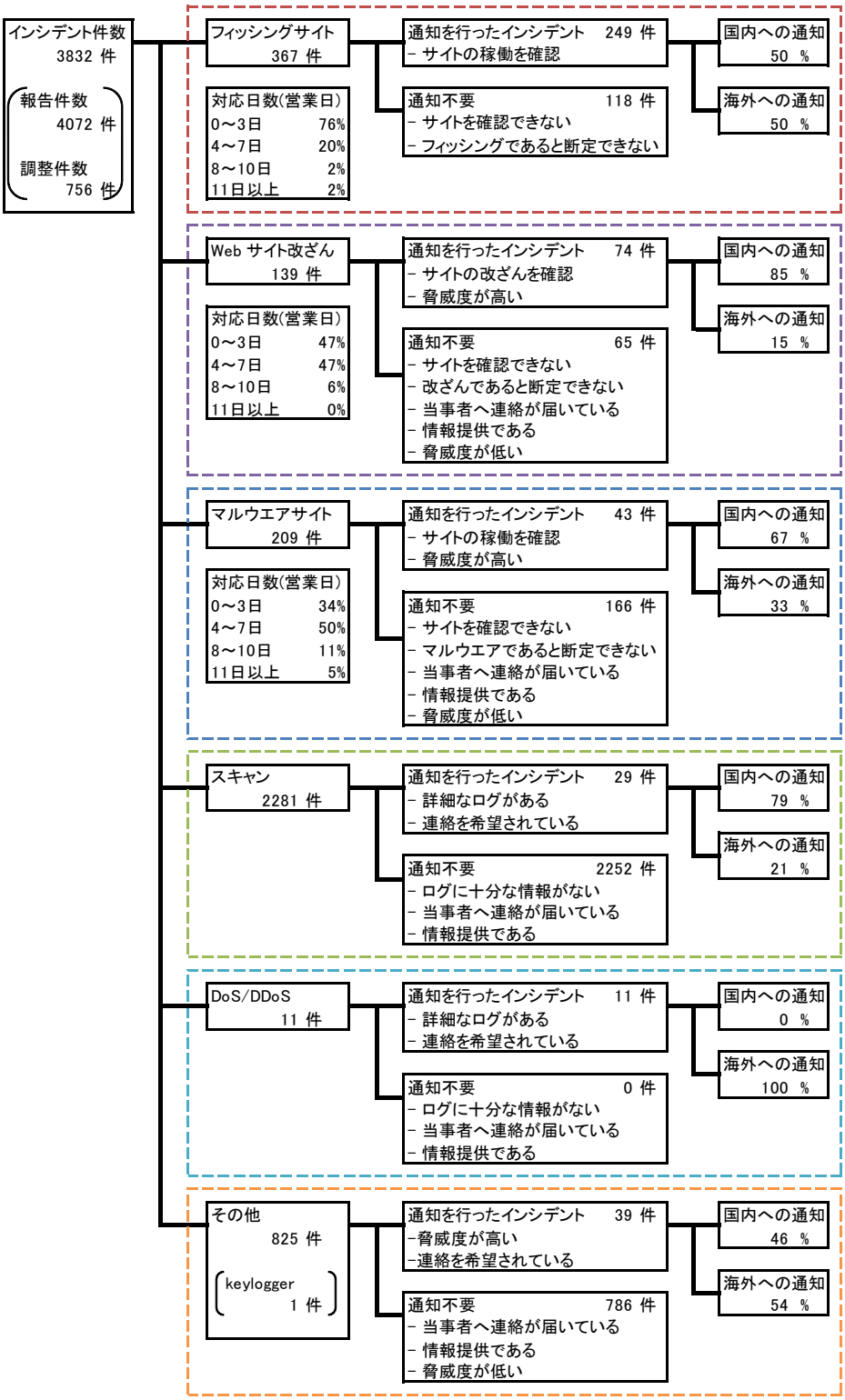


[図 7 マルウエアサイト件数推移]



[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

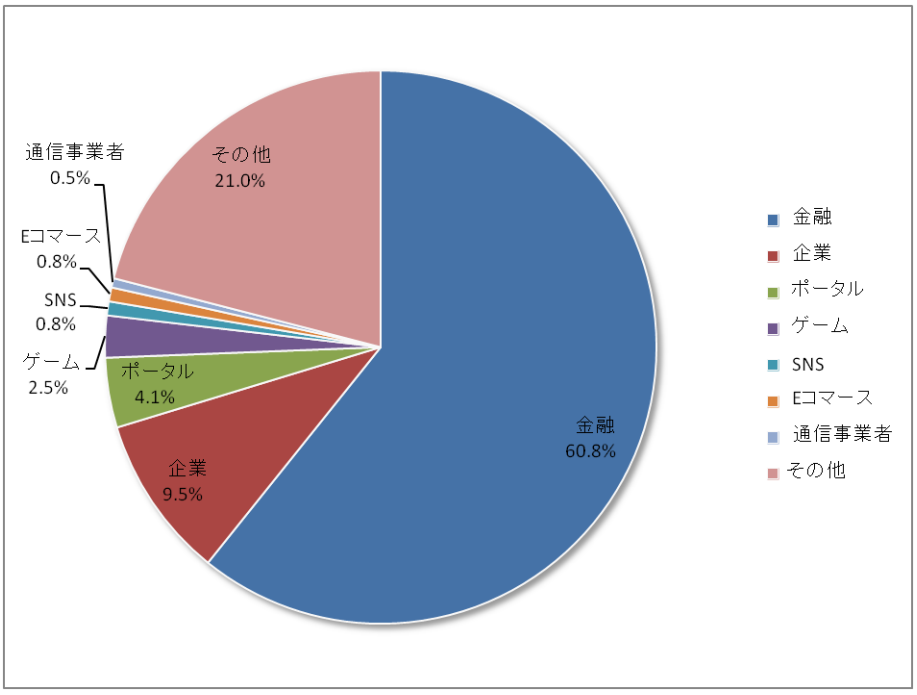
3.1. フィッシングサイトの傾向

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 367 件で、前四半期の 324 件から 13%増加しました。また、前年度同期（325 件）との比較では、13%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	4 月	5 月	6 月	国内外別合計（割合）
国内ブランド	29	19	20	68(19%)
国外ブランド	83	87	55	225(61%)
ブランド不明（注 5）	31	24	19	74(20%)
月別合計	143	130	94	367(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 68 件と、前四半期の 58 件から 17%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 225 件と、前四半期の 221 件から 2%増加しました。
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 60.8%を占めています。

本四半期の国内金融機関を装ったフィッシングサイトは、前四半期と同様にダイナミック DNS サービスのドメインを使用したものが大半であり、それ以外に短縮 URL や CDN などのサービスを使用した事例の報告も受けています。フィッシングサイトの標的となるブランドは、大手の銀行に限らず、様々なブランドのインターネットバンキングを装ったサイトを確認しています。

フィッシングサイトの調整先の割合は、国内が 50%、国外が 50%と、前四半期の割合（国内 65%、国外 35%）と比較して、国外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、139 件でした。前四半期の 142 件から 2%減少しています。

本四半期には、マルウエア配布サイトへの誘導ページを作りこまれたとの報告を多数受領しました。これらの誘導サイトの多くは、ルートディレクトリ下にランダムな英数字 6～8 文字の名前を持つディレクトリが作成され、そのディレクトリ下にマルウエア配布サイトへ誘導する JavaScript を含んだ html ファイルが設置されていました。
誘導先のマルウエア配布サイトは、2012 年 2 月に公開された Java の脆弱性(CVE-2012-0507)など、複数の脆弱性を使用して誘導した PC をマルウエアに感染させます。古い Java を使用している場合には危険性があります。

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、209 件でした。前四半期の 162 件から 29%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、2281 件でした。前四半期の 1823 件から 25%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	4 月	5 月	6 月	合計
80/tcp	618	588	482	1688
25/tcp	110	125	120	355
22/tcp	26	83	62	171
143/tcp	9	9	2	20
8080/tcp	0	6	5	11
23/tcp	0	7	3	10
110/tcp	2	2	3	7
3389/tcp	2	3	1	6
5900/tcp	0	0	3	3
5060/udp	0	0	2	2
8266/udp	0	0	1	1
8081/tcp	0	0	1	1
49939/udp	0	0	1	1
445/tcp	0	0	1	1
443/tcp	1	0	0	1
25537/udp	0	0	1	1
24504/udp	0	0	1	1
/icmp	0	0	1	1
不明	1	1	4	6
月別合計	769	824	694	2287

スキャンの対象となったポートは、上位から http(80/tcp)、smtp(25/tcp)、ssh(22/tcp)の順でした。

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。

【韓国の金融機関を装ったフィッシングサイト】
2012 年 4 月より、韓国の金融機関を装ったフィッシングサイトが国内に多数稼働していることを確認しています。韓国の金融機関を装ったフィッシングサイトを国内で確認したのは、本四半期が初となります。フィッシングサイトは正規サイトに類似したドメイン名を使用しており、フィッシング目的でドメイン名を取得したと考えられます。また、フィッシングサイトは国内通信事業者の接続サービスの IP アドレスが割り当てられており、レンタルサーバ事業者のサーバなどにフィッシングのコンテンツを設置したものではないことを確認しています。
JPCERT/CC では、IP アドレスを管理する国内通信事業者に対応を依頼し、これらのサイトが停止したことを確認しました。また、韓国の National CSIRT である KrCERT/CC に情報を共有しました。

【2012 年 4 月に公開された Windows の脆弱性(MS12-027)を使用した標的型攻撃の対応】
2012 年 5 月に、国内のある組織から当該組織を装って送信された標的型攻撃メールの報告を受領しました。標的型攻撃メールは、当該組織から実際に送信されたメールの再送を装っており、2012 年 4 月に公開された Windows の脆弱性(MS12-027)を使用するマルウエアが添付されていました。この標的型攻撃メールは、実際には海外の IP アドレスから送信されており、メール配送の中継には国内のレンタルサーバが使用されていました。
JPCERT/CC では、標的型攻撃メールの中継に使用されたレンタルサーバのホスティング事業者に、サーバが不正なメールの中継に使用されていることを連絡し、対応を行っていただきました。

【海外通信事業者から提供されたマルウエア感染情報への対処】
2012 年 5 月に、海外通信事業者から国内重要インフラ事業者組織のマルウエア感染に関する情報提供を受けました。提供された情報には、マルウエア感染したホストの IP アドレス（国内組織）と、感染ホストが通信した海外サーバの情報が含まれており、このうち海外サーバのドメインは、過去に対応した標的型攻撃の C&C サーバと同一のものでした。
JPCERT/CC より国内組織に対して、組織内 PC のマルウエア確認、および不審な通信の確認を依頼した結果、国内組織においてマルウエア感染 PC が特定され、当該 PC から不審な通信が発生していた事実が確認されました。その後、被害範囲の特定やウイルス駆除などの対応および再発防止の実施について報告をいただきました。

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。