JPCERT CC®

JPCERT-IR-2011-0003
発行日: 2011-07-11

# JPCERT/CC インシデント報告対応レポート
# [2011 年 4 月 1 日 ～ 2011 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、2011 年 4 月 1 日から 2011 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、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） | 532 | 564 | 471 | 1567 | 1936 |
| インシデント件数 （注 3） | 503 | 569 | 490 | 1562 | 1883 |
| 調整件数（注 4） | 182 | 270 | 202 | 654 | 596 |

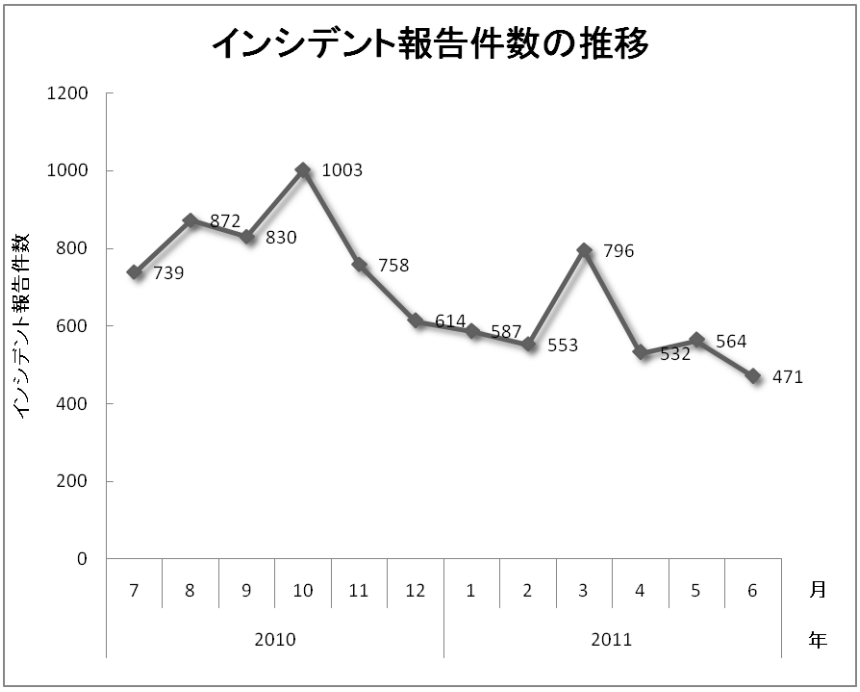
【注 2】「報告件数」は、報告者から寄せられた Web フォーム、メール、FAX による報告の総数を示します。

【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。

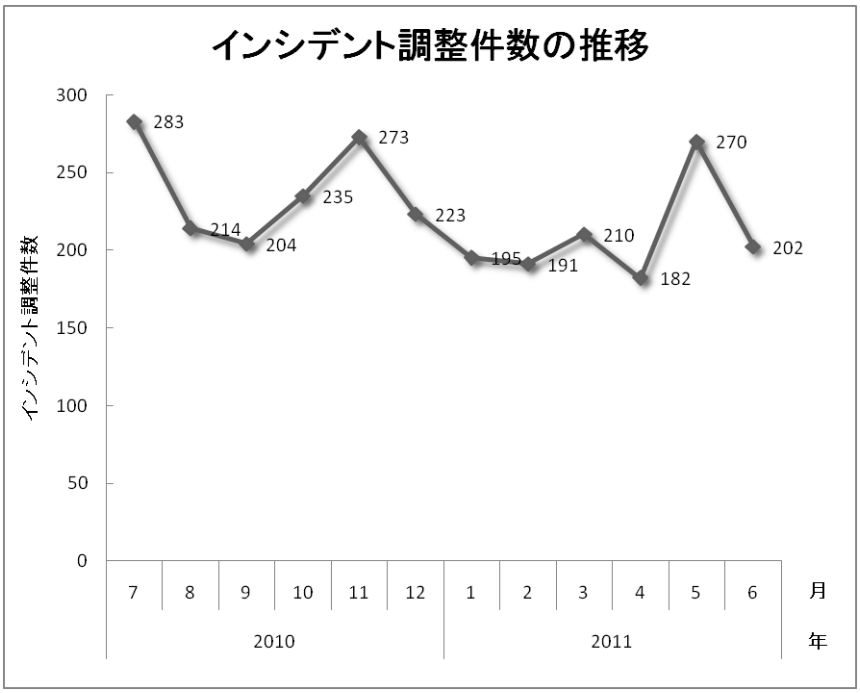
【注 4】「調整件数」とは、インシデントの拡大防止のため、サイトの管理者などに対し、現状の調査と問題解決のための対応を依頼した件数を示します。

本四半期に寄せられた報告件数は、1567 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 654 件でした。前四半期の 596 件と比較して、10%増加しています。

[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]



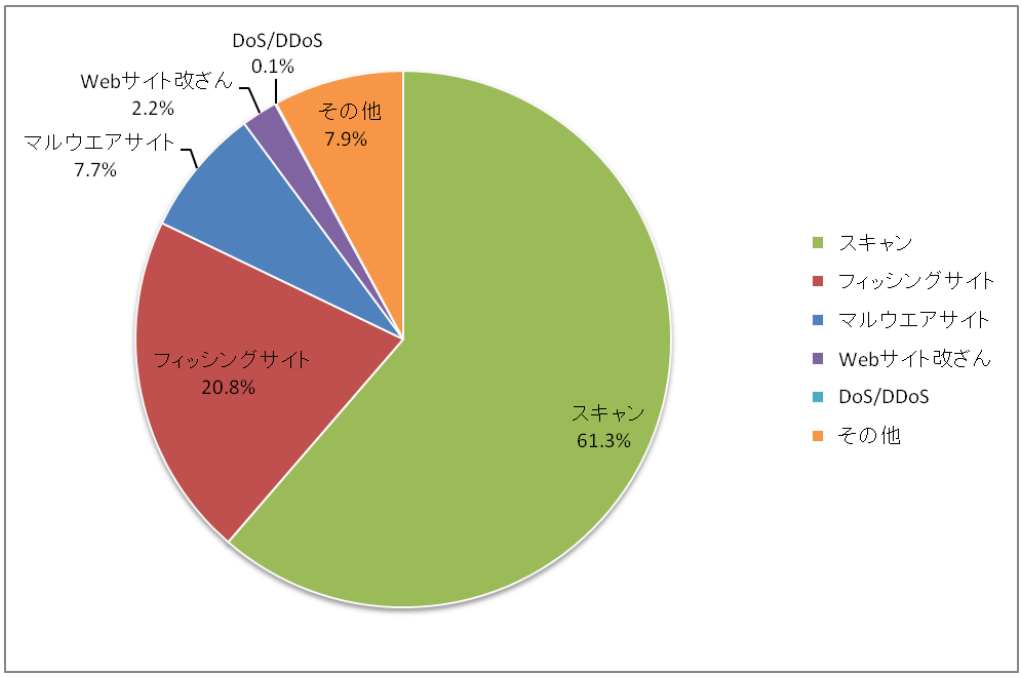

[図 2 インシデント調整件数の推移]

JPCERT/CC では報告を受けたインシデントをタイプ別に分類し、各インシデントタイプに応じた調整、対応を実施しています。本四半期に発生したインシデントのタイプ別件数を[表 3]に示します。

[表 3 タイプ別インシデント件数]

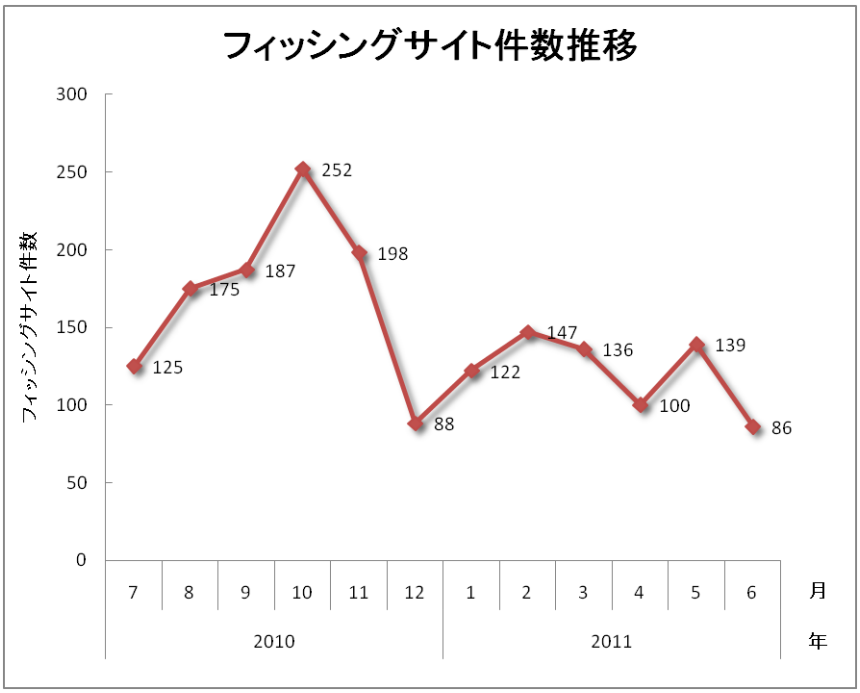
| インシデント | 4 月 | 5 月 | 6 月 | 合計 | 前四半期合計 |
|---|---|---|---|---|---|
| フィッシングサイト | 100 | 139 | 86 | 325 | 405 |
| Web サイト改ざん | 6 | 10 | 18 | 34 | 49 |
| マルウエアサイト | 42 | 54 | 25 | 121 | 352 |
| スキャン | 325 | 320 | 313 | 958 | 919 |
| DoS/DDoS | 1 | 0 | 0 | 1 | 3 |
| その他 | 29 | 46 | 48 | 123 | 155 |

本四半期に発生したインシデントのタイプ別割合は、[図 4]のとおりです。システムの弱点を探索するスキャンに分類されるインシデントは 61.3%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 20.8%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 2.2%でした。

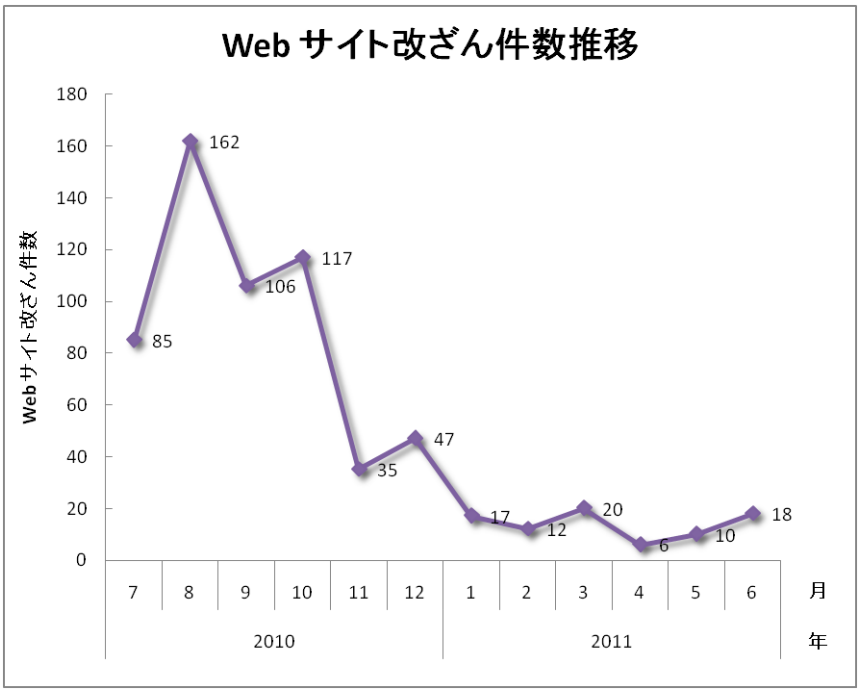



[図 4 インシデントのタイプ別割合]

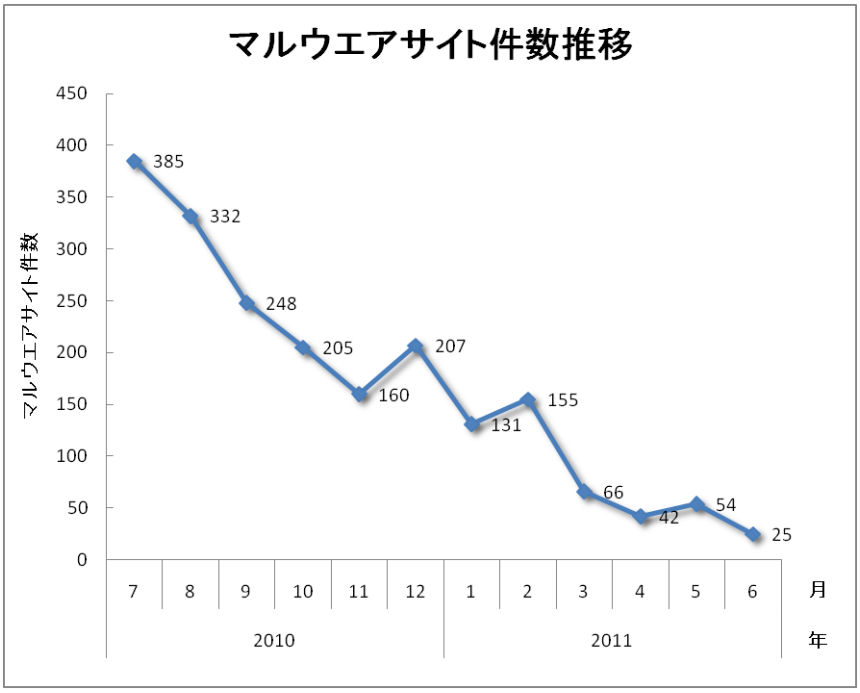
[図 5]から[図 8]に、フィッシングサイト、Web サイト改ざん、マルウエアサイト、スキャンのインシデントの過去 1 年間の月別推移を示します。



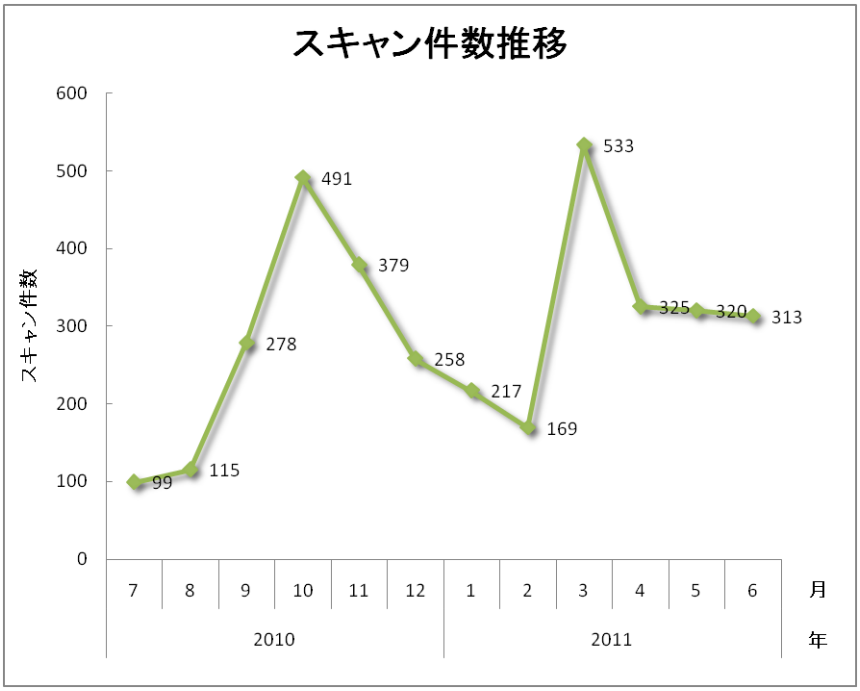

[図 5 フィッシングサイト件数推移]




[図 6　Web サイト改ざん件数推移]

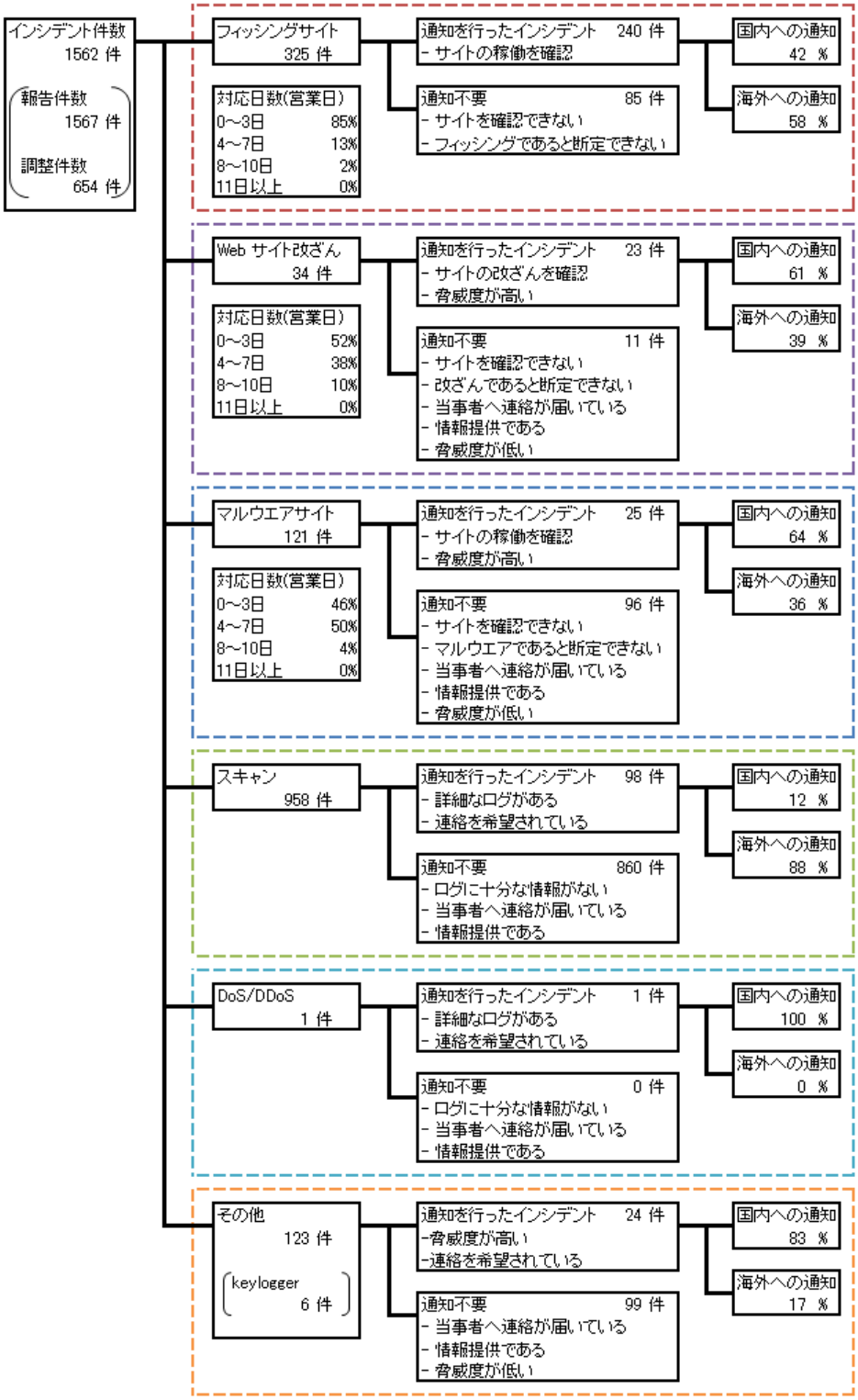



[図 **7** マルウエアサイト件数推移]




[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]

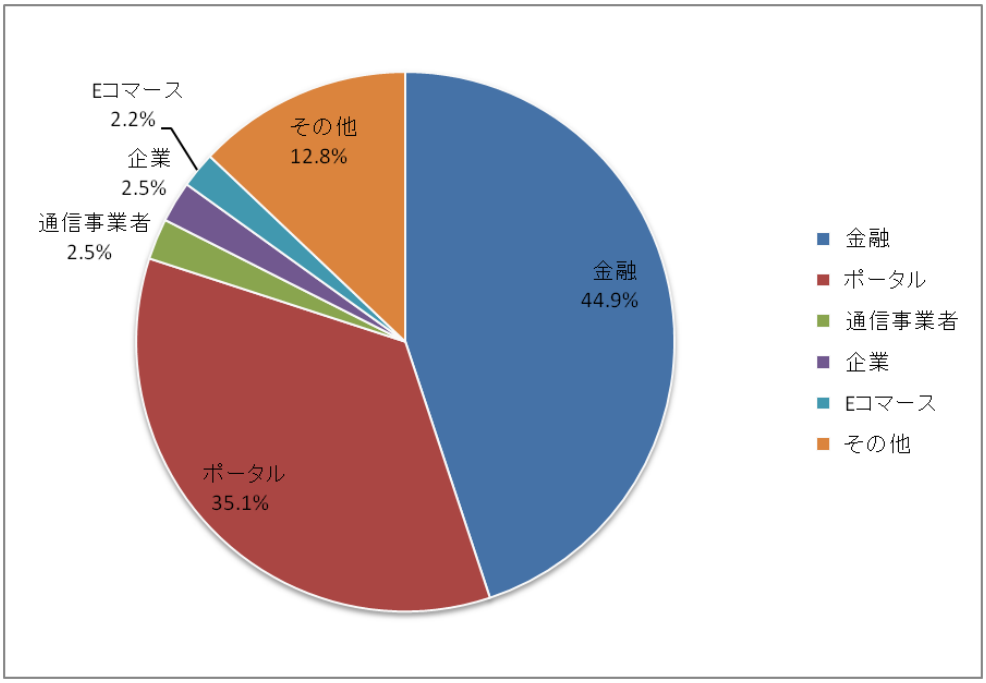
## 3. インシデントの傾向

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 325 件で、前四半期の 405 件から 20%減少しました。また、前年度同四半期（388 件）との比較では、16%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 | 4 月 | 5 月 | 6 月 | 国内外別合計（割合） |
|---|---|---|---|---|
| 国内ブランド | 43 | 32 | 43 | 118(36%) |
| 国外ブランド | 53 | 83 | 37 | 173(53%) |
| ブランド不明 | 4 | 24 | 6 | 34(10%) |
| 月別合計 | 100 | 139 | 86 | 325(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 118 件と、前四半期の 84 件から 40 % 増加しました。これは、国内ポータルサイトを装ったフィッシングサイトが多数確認されたためです。また、国外ブランドを装ったフィッシングサイトの件数は 173 件と、前四半期の 247 件から 30 % 減少しました。これは、前四半期に多く確認されていた、海外の電子決済サービスを装ったフィッシングサイトの件数が減少したためです。フィッシングサイトの内、金融関連のサイトを装ったものが 44.9 %、ポータルサイトを装ったものが 35.1%を占めました。

フィッシングサイトの調整先の割合は、国内が 42 %、国外が 58% と、前四半期の割合（国内 61%、国外 39%）と比較して、国外への調整が増えました。これは、国内のポータルサイトを装ったフィッシングサイトの多くが海外の無料ホスティングサービスを使用していたためです。その他、国内のポータルサイトを装ったフィッシングサイトでは、移動体通信ネットワークの IP アドレスとダイナミック DNS サービスのドメインを使用したサイトの稼働も確認しており、これら 2 種類のパターンが多くを占めています。

本四半期に報告が寄せられた Web サイト改ざんの件数は、34 件でした。前四半期の 49 件から 31%減少しています。これは、2009 年度から多発していたいわゆる Gumblar による Web 改ざんへの対策が各サイトで進んだことにより大幅に減少したためです。報告件数は減少傾向にありますが、 4 月の初めには大規模な SQL インジェクション攻撃の発生が確認されており、新たな攻撃に備えて JPCERT/CC では引き続き攻撃の分析や動向調査を行っています。

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、121 件でした。前四半期の 352 件から 66 % 減少しています。これは、海外のセキュリティ対応機関から定常的に寄せられていたマルウエアの報告が減少したためです。また、いわゆる Gumblar による Web 改ざんに関連したマルウエアサイトも減少しています。

本四半期に報告が寄せられたスキャンの件数は、958 件でした。前四半期の 919 件から 4% 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 | 204 | 230 | 201 | 635 |
| 22/tcp | 69 | 64 | 68 | 201 |
| 25/tcp | 19 | 20 | 29 | 68 |
| /icmp | 22 | 0 | 0 | 22 |
| 110/tcp | 4 | 4 | 1 | 9 |
| /udp | 0 | 0 | 9 | 9 |
| 445/tcp | 7 | 0 | 1 | 8 |
| 21/tcp | 1 | 2 | 4 | 7 |
| 143/tcp | 2 | 0 | 4 | 6 |
| 9415/ | 0 | 0 | 1 | 1 |
| 80/udp | 0 | 0 | 1 | 1 |
| 5900/tcp | 1 | 0 | 0 | 1 |
| 5060/udp | 0 | 1 | 0 | 1 |
| 3389/tcp | 0 | 1 | 0 | 1 |
| 139/tcp | 0 | 0 | 1 | 1 |
| 不明 | 3 | 9 | 7 | 19 |
| 月別合計 | 332 | 331 | 327 | 990 |

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。http に対するスキャンでは、Web アプリケーションの脆弱性への攻撃を試みる RFI(リモート・ファイル・インクルード)攻撃を多く確認しています。また、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。

## 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。

【 金融機関のアカウント詐取を目的としたマルウエア】
2011 年 5 月と 6 月には、オンラインバンキングサービスのユーザを標的とするマルウエアの報告を国内の複数の金融機関から受領しました。本マルウエアは、ユーザがオンラインバンキングの Web ページを閲覧した際に、HTML フォームに第二認証情報などの入力項目を追加し、それを送信させることによってアカウント情報を詐取します。
JPCERT/CC では、マルウエアを解析し、マルウエアの通信先サーバとそれを制御していたサーバを停止するためのコーディネーションを実施し、両サーバの停止を確認しました。

【 Web メールサービスを装ったフィッシングサイト】
2011 年 6 月に、日本の政府関係者を騙って送信されたフィッシングメールを受け取ったという報告が寄せられました。このメールに記載された URL は、 Web メールサービスのログイン画面を装ったフィッシングサイトのものでした。
JPCERT/CC は、当該サイトの IP アドレスを管理する米国の ISP 及び関係する CSIRT と、ドメインのレジストラにフィッシングサイトの停止を依頼し、翌日に当該サイトの停止を確認しました。

【 IPv6 アドレスにおけるスキャン】
World IPv6 Day が実施された 2011 年 6 月 8 日に、 IPv6 アドレスからスキャンと思われる大量のアクセスを短時間の内に受けたという報告が寄せられました。JPCERT/CC は、アクセス元のネットワークを管理するドイツの ISP に対し連絡を行いました。

【Web アプリケーションサービスにて作成されたフィッシングサイト】
大手クラウドサービス事業者が提供する Web アプリケーションサービスを使用したフィッシングサイトが立ち上がっているという報告を受領しました。
JPCERT/CC では、当該サイトがフィッシングサイトである事を確認し Web アプリケーションサービス事業者へ調整を行っています。本フィッシングサイトは 2011 年 6 月 30 日現在も動作しており、対応を継続しています。

## 5. 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

## 6. [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。