JPCERT-IR-2012-01

発行日: 2012-01-12

JPCERT/CC インシデント報告対応レポート
[2011 年 10 月 1 日 ～ 2011 年 12 月 31 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 10 月 1 日から 2011 年 12 月 31 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。

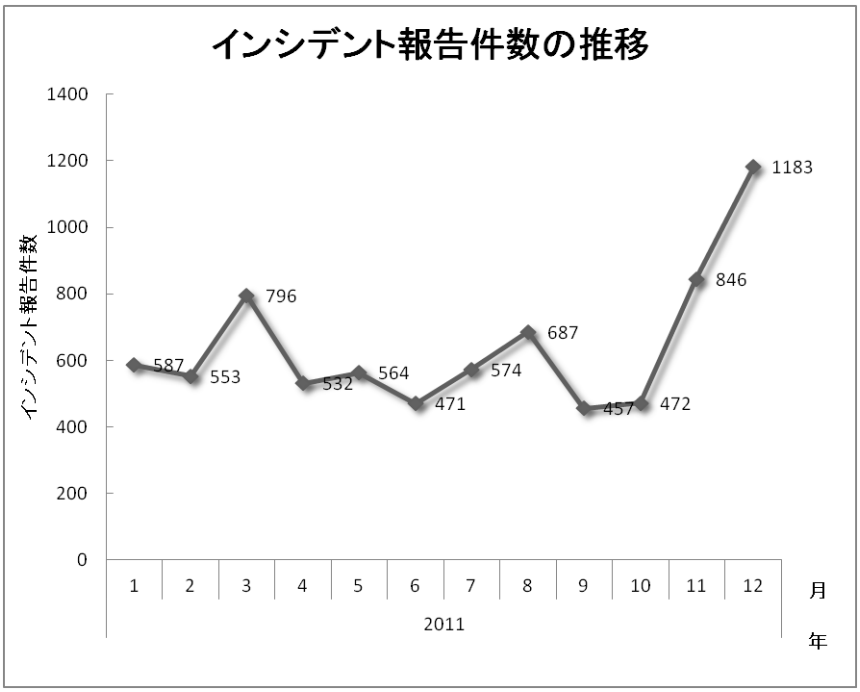
[表 1 インシデント報告関連件数]

	10 月	11 月	12 月	合計	前四半期合計
報告件数 (注 2)	472	846	1183	2501	1718
インシデント件数 （注 3）	452	799	1088	2339	1676
調整件数（注 4）	228	224	300	752	642

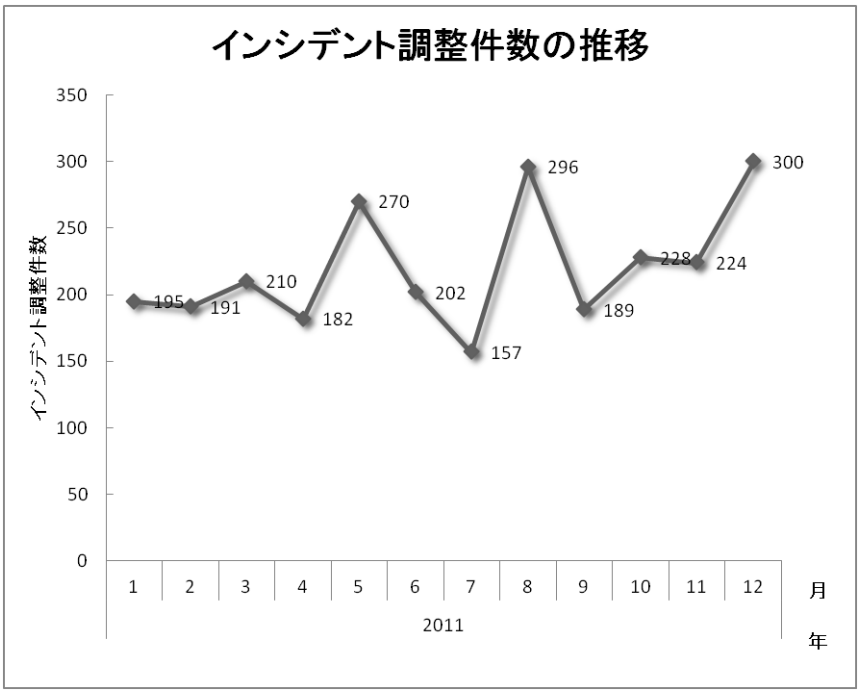
【注 2】「報告件数」は、報告者から寄せられた Web フォーム、メール、FAX による報告の総数を示します。
【注 3】「インシデント件数」は、各報告に含まれるインシデント件数の合計を示します。ただし、1 つのインシデントに関して複数件の報告が寄せられた場合は、1 件のインシデントとして扱います。
【注 4】「調整件数」とは、インシデントの拡大防止のため、サイトの管理者などに対し、現状の調査と問題解決のための対応を依頼した件数を示します。

本四半期に寄せられた報告件数は、2501 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 752 件でした。前四半期と比較して、総報告件数は 46% 増加し、調整件数は 17% 増加しました。また、前年同期と比較すると、総報告数で 5% 増加し、調整件数は 3% 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]



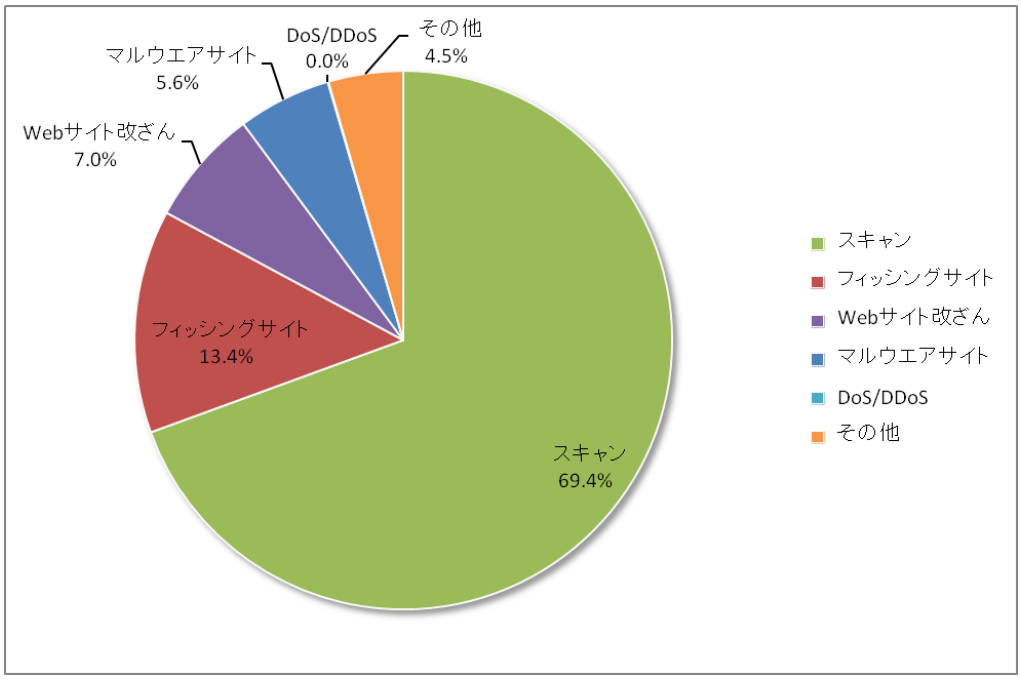
[図 2 インシデント調整件数の推移]

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。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]

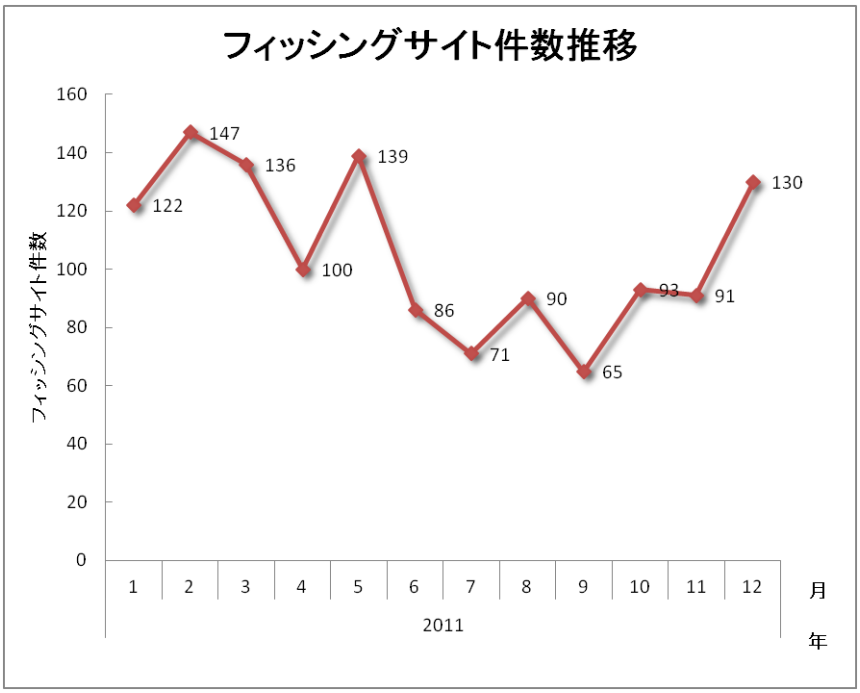
インシデントカテゴリ	10 月	11 月	12 月	合計	前四半期合計
フィッシングサイト	93	91	130	314	226
Web サイト改ざん	46	65	53	164	73
マルウエアサイト	37	53	41	131	185
スキャン	267	538	819	1624	1079
DoS/DDoS	1	0	0	1	0
その他	8	52	45	105	113

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 69.4% 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 13.4% 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 7.0% でした。

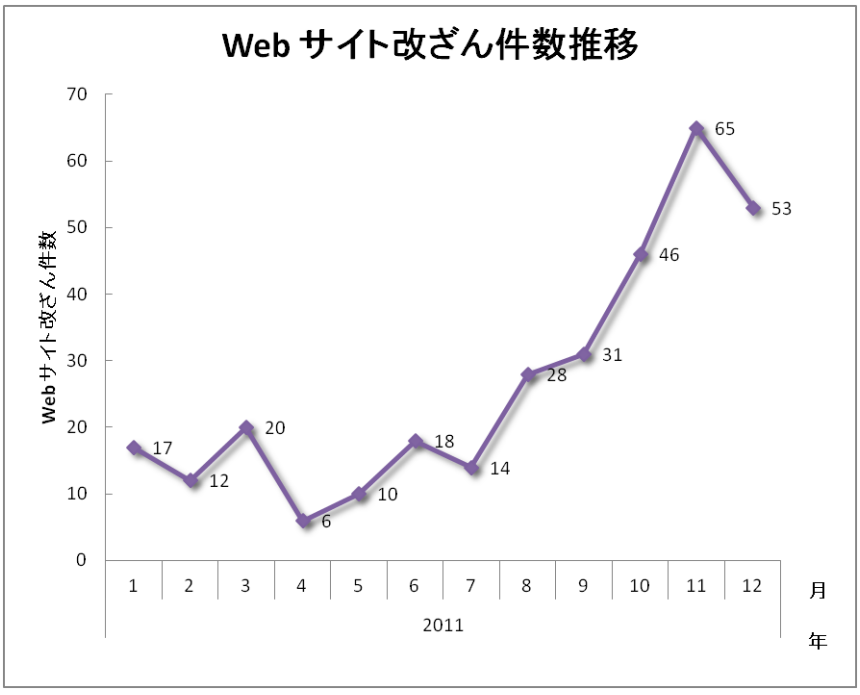


[図 3 インシデントのカテゴリ別割合]

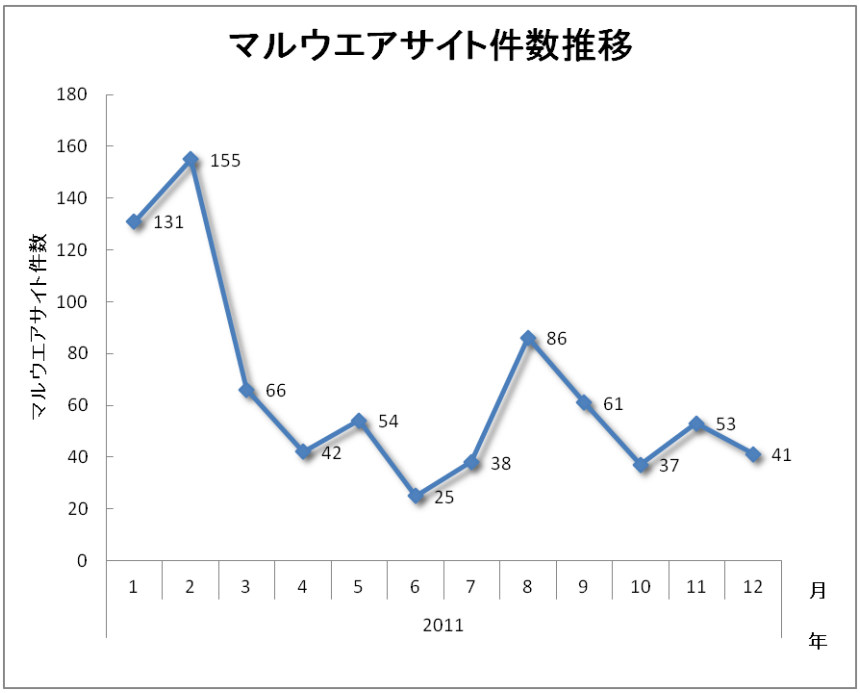
[図 4]から[図 7]に、フィッシングサイト、Web サイト改ざん、マルウエアサイト、スキャンのインシデントの過去 1 年間の月別推移を示します。



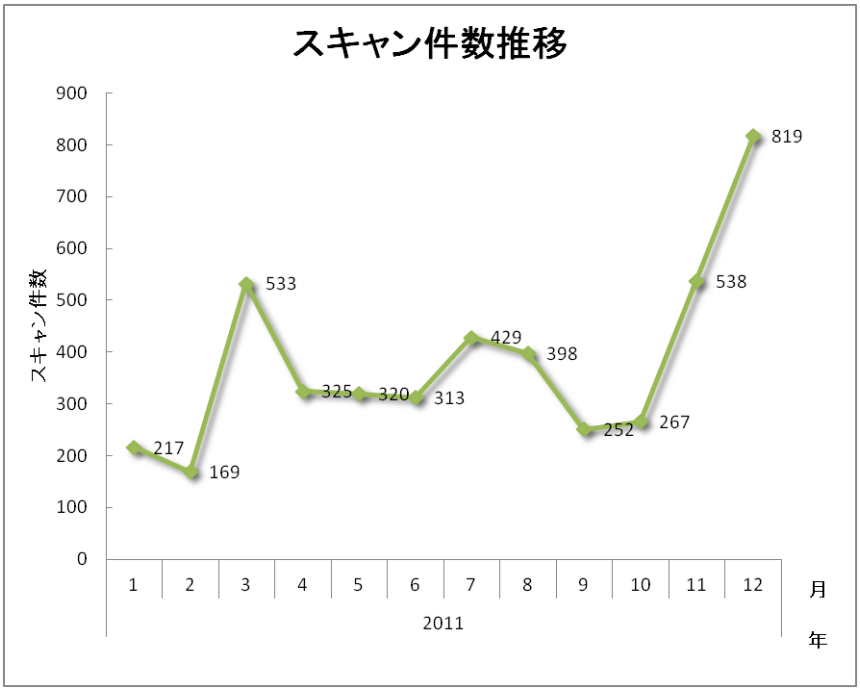
[図 4 フィッシングサイト件数推移]



[図 5　Web サイト改ざん件数推移]

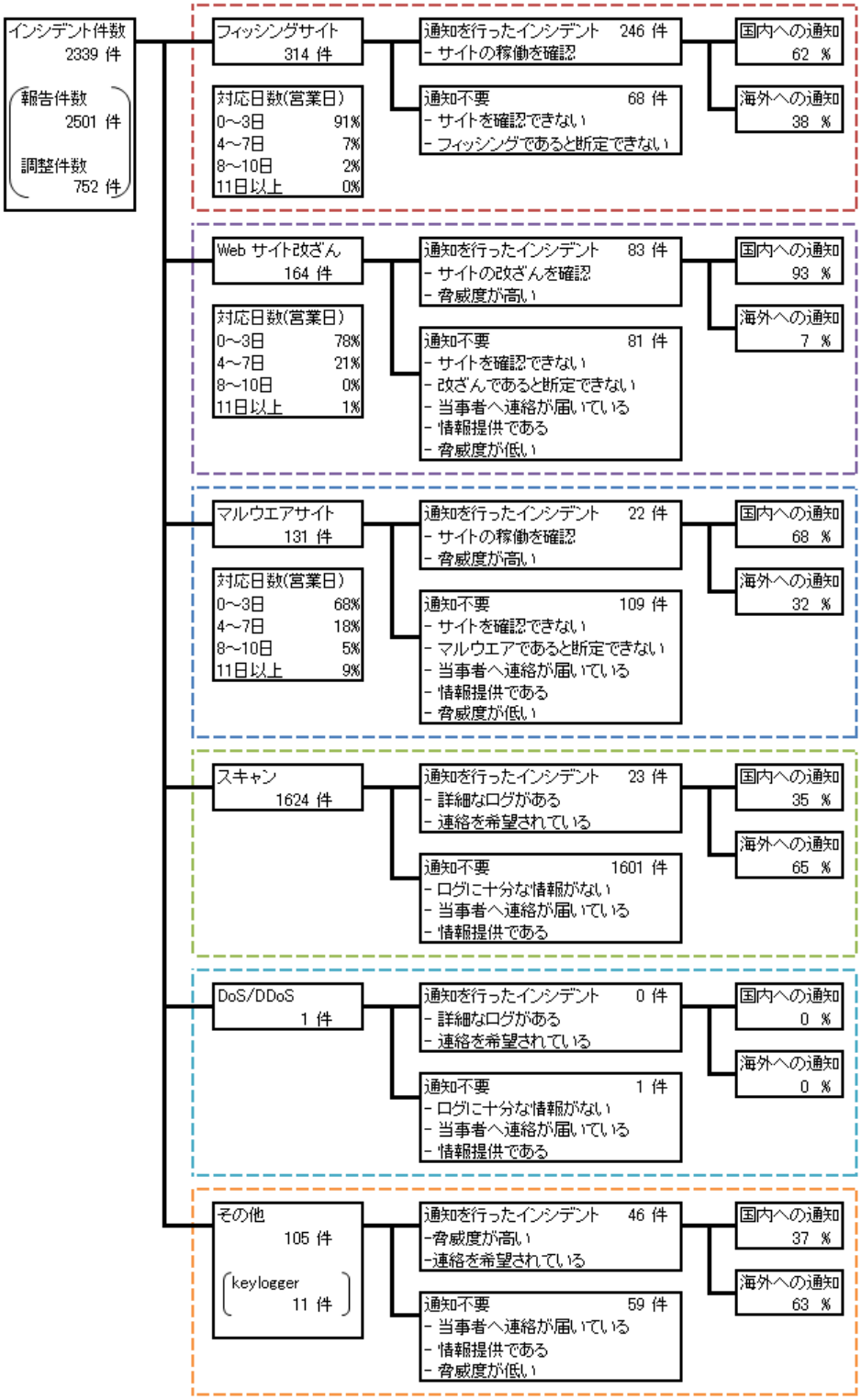


[図 6 マルウエアサイト件数推移]



[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 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

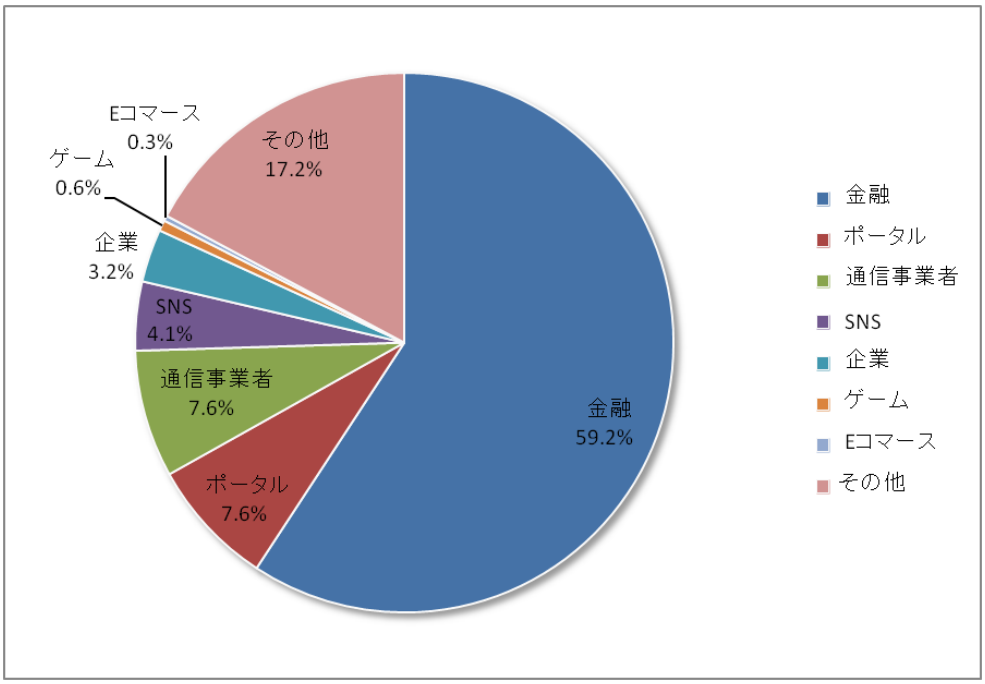
本章で説明する各インシデントの定義については、6.[付録]インシデントの分類を参照してください。

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 314 件で、前四半期の 226 件から 39% 増加しました。また、前年度同期（538 件）との比較では、42% 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 3] 、フィッシングサイトのブランド種別割合を [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	10 月	11 月	12 月	国内外別合計（割合）
国内ブランド	22	19	24	65(21%)
国外ブランド	54	58	86	198(63%)
ブランド不明（注 5）	17	14	20	51(16%)
月別合計	93	91	130	314(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 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 65 件と、前四半期の 31 件から 110% 増加しました。一方、国外ブランドを装ったフィッシングサイトの件数は 198 件と、前四半期の 165 件から 20% 増加しました。

前四半期に引き続き、国内金融機関を装ったフィッシングの報告を多数受領しています。この国内金融機関を装ったフィッシングでは、以下のようにフィッシングの手法を変えてアカウント情報を詐取しようとしていることを確認しています。8 月には、メールに実行ファイル形式のマルウエアを添付し、金融機関のアカウント情報を詐取しようとする手法、9 月には、第三者の Web サイトを改ざんしてフィッシングサイトを設置し、そこにユーザを誘導する手法が使用されました。また本四半期に入り、海外のレンタルサーバ上にフィッシングサイトを設置し、ダイナミック DNS サービスを組み合わせる手法が増加していることを確認しています。

JPCERT/CC で報告を受領したフィッシングサイトのうち、金融機関のサイトを装ったものが 59%、通信事業者のサイトを装ったものが 8% を占め、通信事業者を標的としたフィッシングも増加しています。

フィッシングサイトの調整先の割合は、国内が 62%、国外が 38% と、前四半期の割合（国内 58%、国外 42%）と比較して、国内への調整が増えました。

本四半期に報告が寄せられた Web サイト改ざんの件数は、164 件でした。前四半期の 73 件から 125% 増加しています。

本四半期は、WordPress で構築されたサイトの改ざんの報告を多数受領しました。この改ざんでは、WordPress の Timthumb プラグインの脆弱性を使用したとみられる攻撃により、Web ページに難読化された JavaScript が挿入されます。この JavaScript が挿入されたサイトを閲覧した PC は、アプリケーションの脆弱性を攻撃するサイトに転送され、その結果マルウエアがインストールされることを確認しています。

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、131 件でした。前四半期の 185 件から 29% 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、1624 件でした。前四半期の 1079 件から 51%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 4]に示します。

[表 4　ポート別のスキャン件数]

ポート	10 月	11 月	12 月	合計
80/tcp	124	312	505	941
25/tcp	50	125	182	357
22/tcp	76	82	117	275
143/tcp	2	9	4	15
/udp	10	0	0	10
23/tcp	0	0	4	4
110/tcp	2	2	0	4
5900/tcp	0	1	1	2
89/tcp	0	1	0	1
80/udp	0	0	1	1
5060/udp	0	0	1	1
445/tcp	1	0	0	1
3389/tcp	0	1	0	1
139/tcp	1	0	0	1
不明	2	6	4	12
月別合計	268	539	819	1626

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。ssh に対するスキャンについては、不正侵入することを目的としたブルートフォース攻撃が多くを占めています。

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。

【 複数の金融機関が狙われたフィッシング】

2011 年 10 月には、前四半期に引き続き、国内金融機関を装ったフィッシングサイトの報告を多数受領しました。この一連のフィッシングでは、数週間ごとに標的とする国内金融機関が移り変わっていく現象が見られ、同一の攻撃者ないしグループの関与がうかがえました。

また、フィッシングサイトを、乗っ取った他者のサーバ上でなく、海外のレンタルサーバ上に設置し、ダイナミック DNS サービスを使用して、ホスト名に金融機関のブランド名を使った事例が目立ちました。JPCERT/CC では、フィッシングサイトが設置されているサーバを管理する組織やサーバが設置された地域の National CSIRT に対応を依頼するとともに、ドメインのレジストラにも対応を依頼することでこれらのフィッシングサイトを平均 1.8 日でテイクダウンすることができました。

【WordPress で構築された Web サイトの改ざん増加】

2011 年 11 月頃、WordPress で構築された Web サイトが改ざんされたという報告を多数受領しました。改ざんされた Web ページには難読化された JavaScript が挿入されており、この JavaScript が挿入されたサイトを閲覧した PC は、アプリケーションの脆弱性を攻撃するサイトに転送され、その結果 PC にマルウエアがインストールされる場合があることを確認しました。12 月上旬には、10 月に公開された Java の新しい脆弱性を使用してマルウエアをインストールさせようとする攻撃サイトが出現したことを確認しました。

JPCERT/CC では改ざんされた Web サイトの IP アドレスを管理する ISP に連絡し、対応を依頼しました。また 12 月上旬には、Java SE を対象とした既知の脆弱性を狙う攻撃に関する注意喚起を行いました。(JPCERT/CC Alert 2011-12-05 Java SE を対象とした既知の脆弱性を狙う攻撃に関する注意喚起)

【ISP サービスのアカウントを詐取するフィッシング】

本四半期は、複数の ISP 事業者のサービスを騙るフィッシングの報告を多数受領しました。ISP のアカウント情報のような一見したところでは金銭利益に結び付かないように見えるサービスに対するフィッシングも増加していることを確認しています。

JPCERT/CC では、フィッシングサイト停止の対応を行うとともに、ISP 事業者とも協力し、被害の分析を行っています。

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

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。