Japan Computer Emergency Response Team Coordination Center

JPCERT CC®

JPCERT-IR-2012-03

発行日: 2013-01-17

JPCERT/CC インシデント報告対応レポート
[2012 年 10 月 1 日 ～ 2012 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、2012 年 10 月 1 日から 2012 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)	1518	1541	2005	5064	5430
インシデント件数 （注 3）	1569	1707	2017	5293	5266
調整件数（注 4）	454	523	520	1497	1123

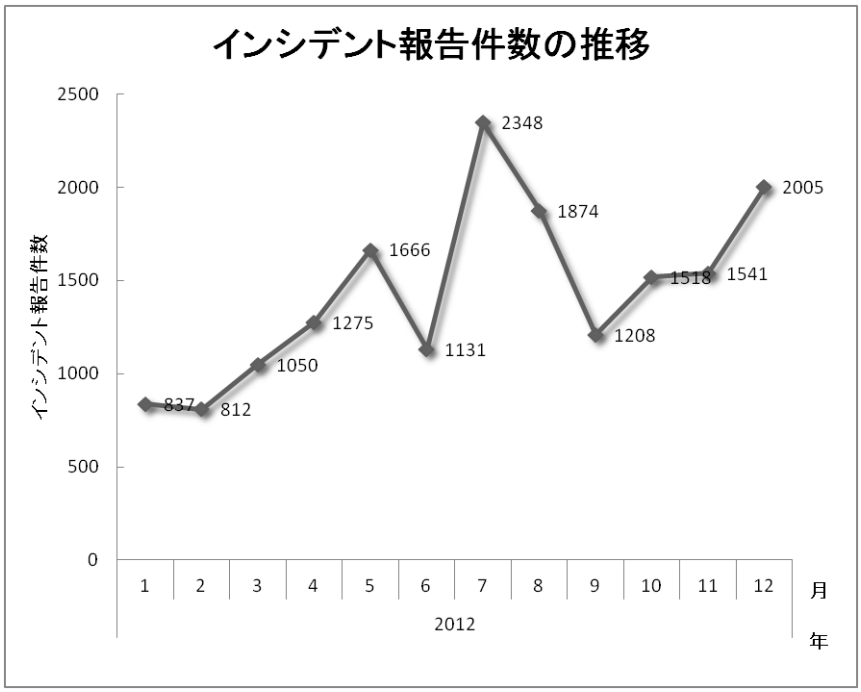
【注 2】「報告件数」は、報告者から寄せられた Web フォーム、メール、FAX による報告の総数を示します。

【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。

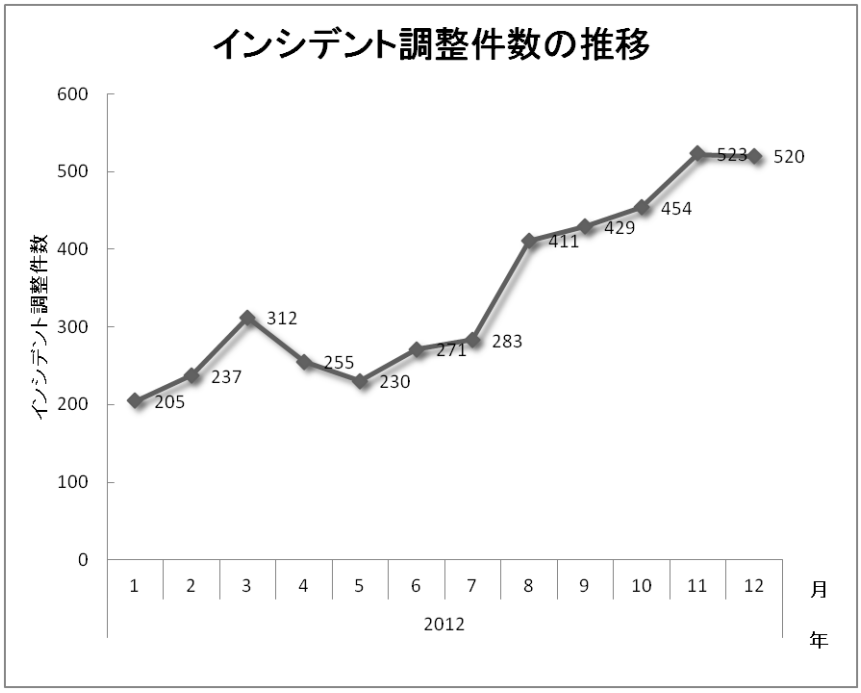
【注 4】「調整件数」とは、インシデントの拡大防止のため、サイトの管理者などに対し、現状の調査と問題解決のための対応を依頼した件数を示します。

本四半期に寄せられた報告件数は、5064 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 1497 件でした。前四半期と比較して、総報告件数は 7%減少し、調整件数は 33%増加しました。また、前年同期と比較すると、総報告数で 102%増加し、調整件数は 99%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]



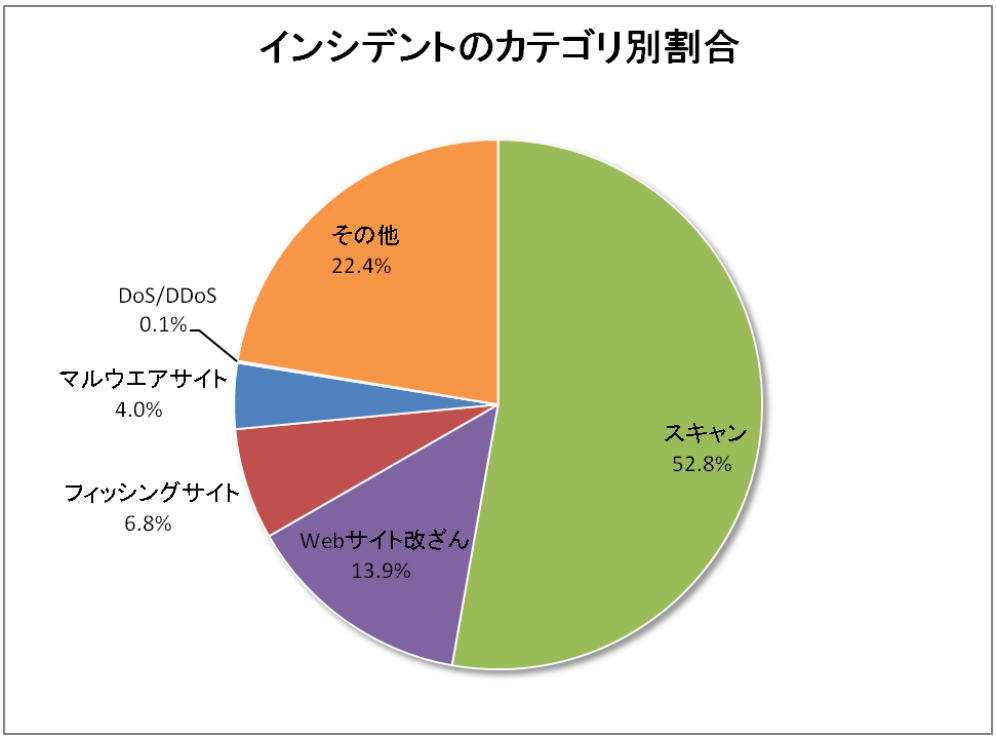
[図 2 インシデント調整件数の推移]

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]

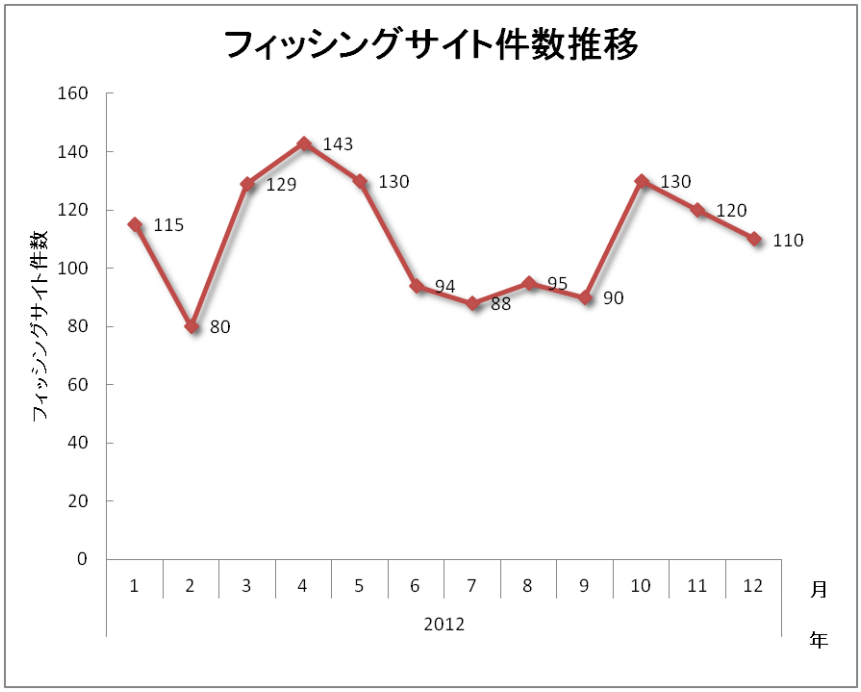
インシデントカテゴリ	10 月	11 月	12 月	合計	前四半期合計
フィッシングサイト	130	120	110	360	273
Web サイト改ざん	216	315	206	737	796
マルウエアサイト	86	69	58	213	202
スキャン	833	858	1103	2794	3391
DoS/DDoS	1	3	2	6	12
その他	303	342	538	1183	592

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 52.8%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 6.8%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 13.9%でした。

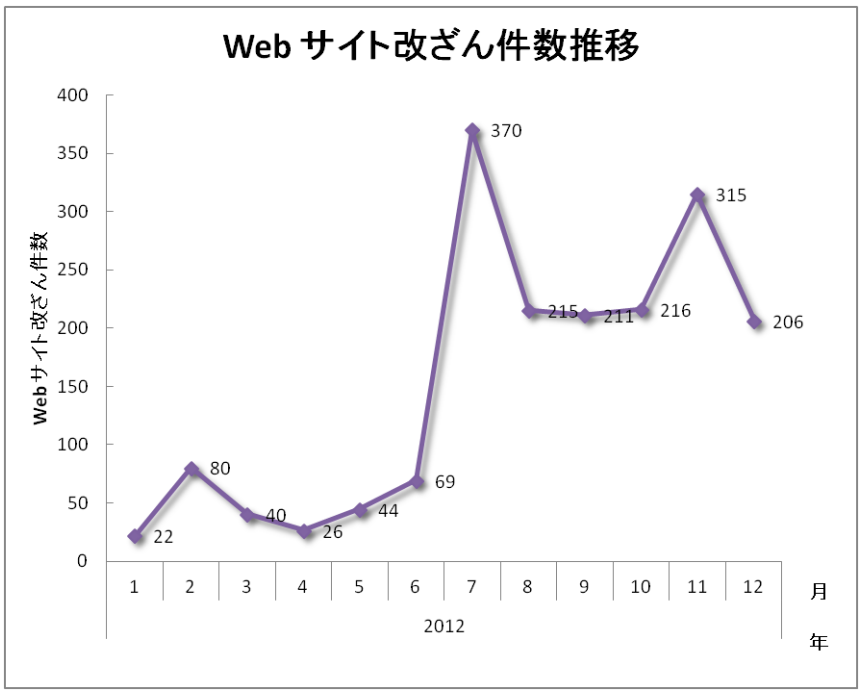


[図 4 インシデントのカテゴリ別割合]

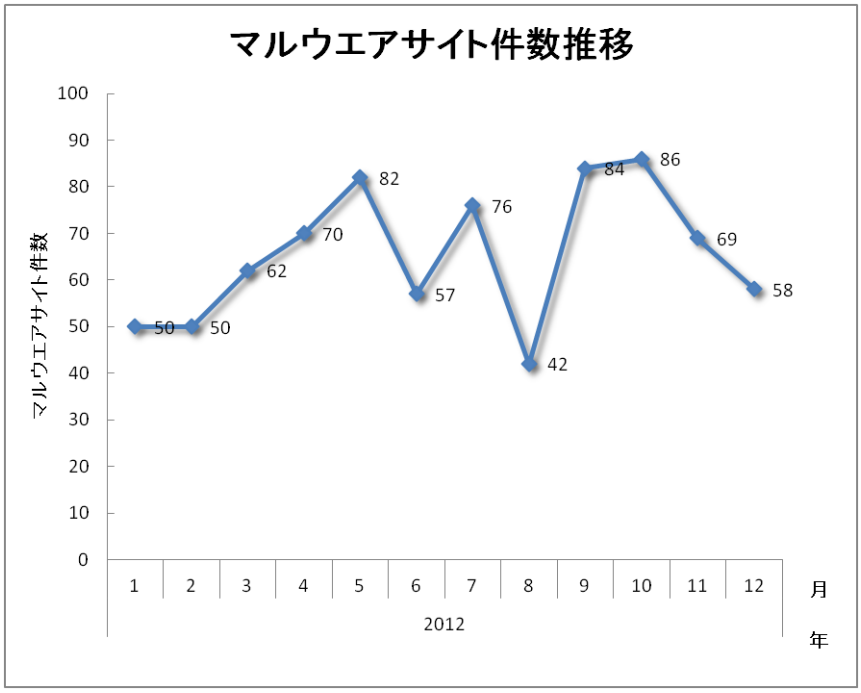
[図 5]から[図 8]に、フィッシングサイト、Web サイト改ざん、マルウエアサイト、スキャンのインシデントの過去 1 年間の月別推移を示します。



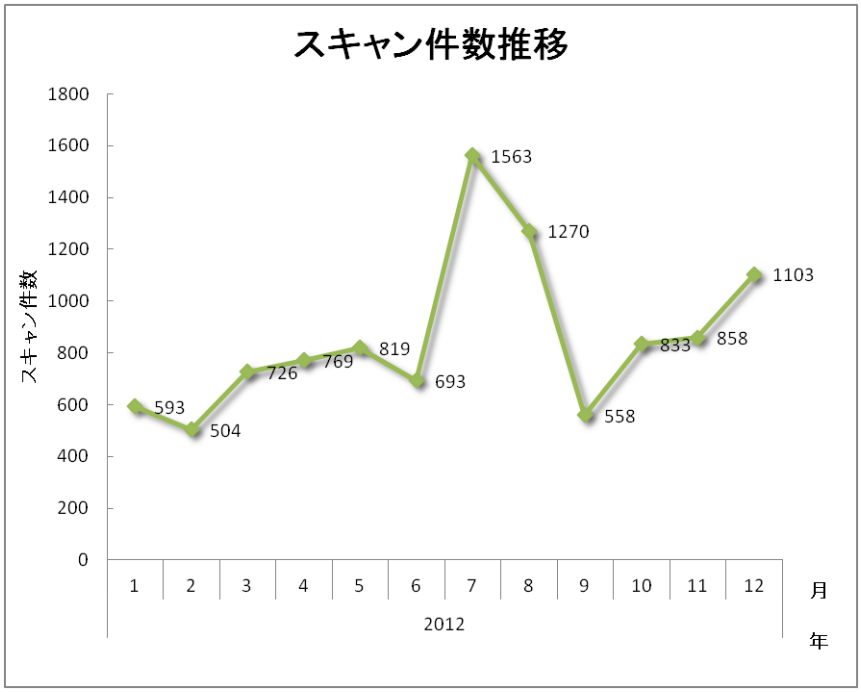
[図 5 フィッシングサイト件数推移]



[図 6 Web サイト改ざん件数推移]

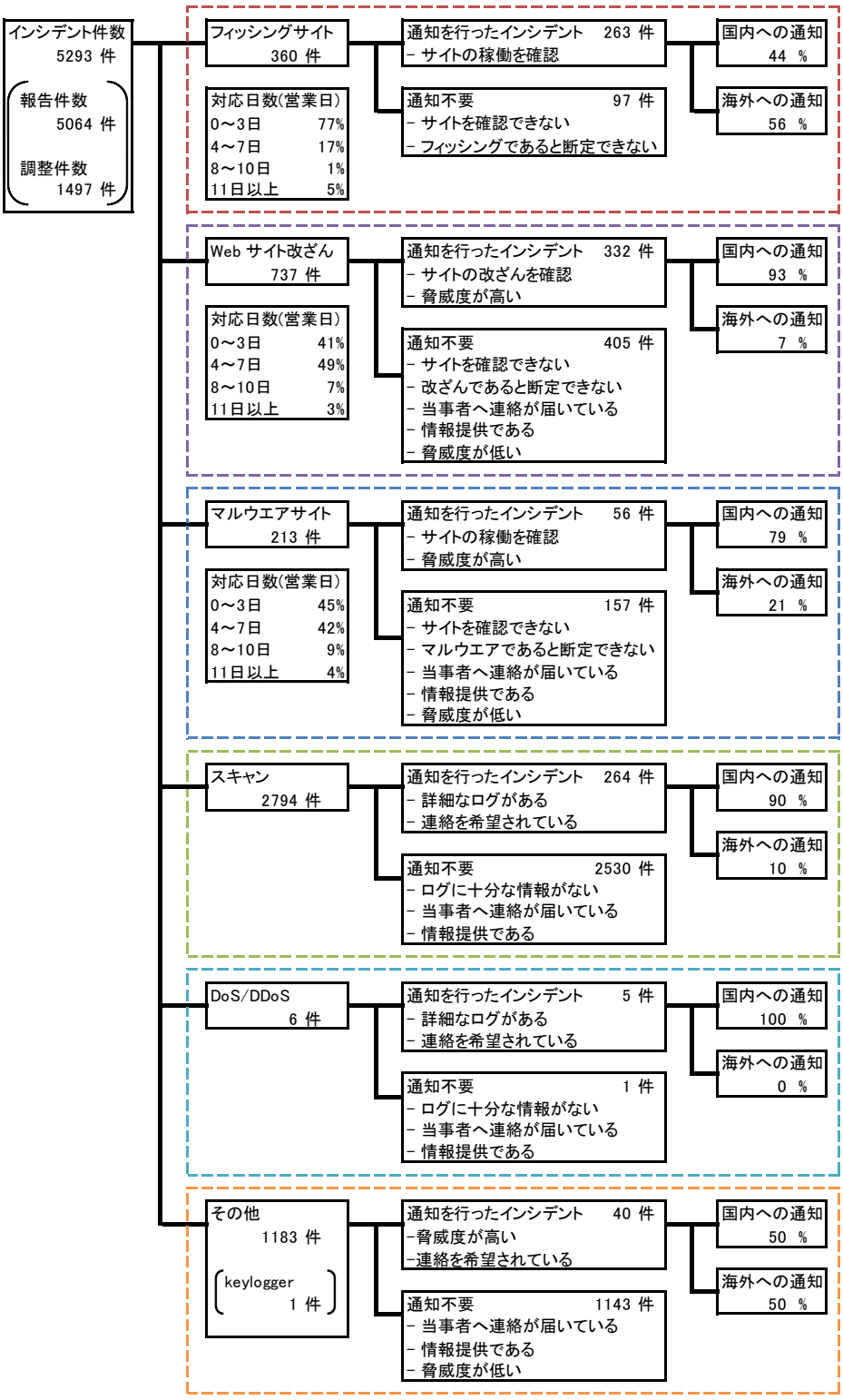


[図 7 マルウエアサイト件数推移]



[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

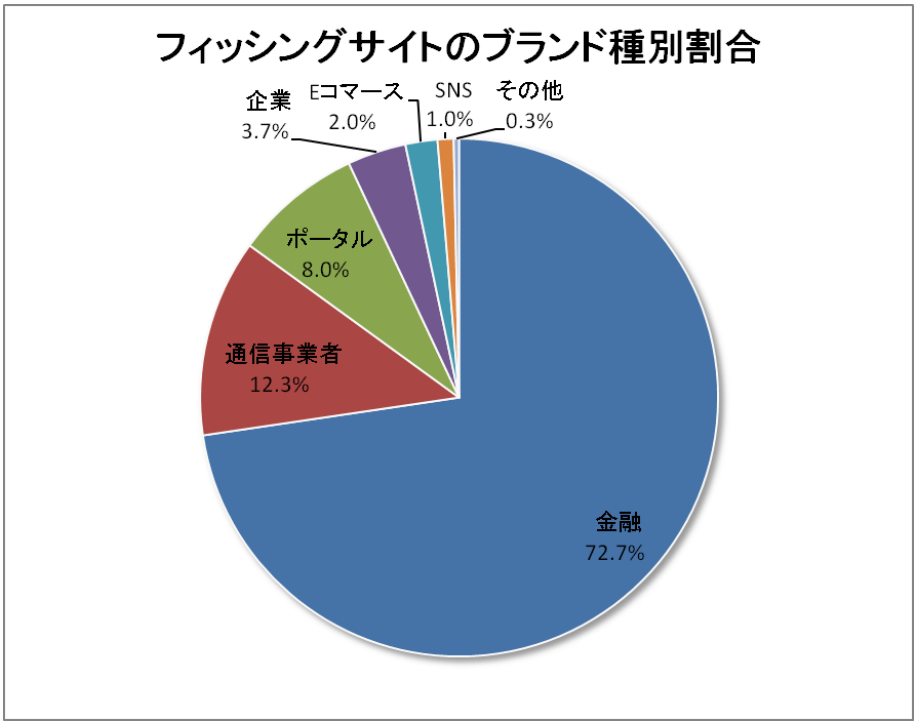
3.1. フィッシングサイトの傾向

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 360 件で、前四半期の 273 件から 32%増加しました。また、前年度同期（314 件）との比較では、15%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	10 月	11 月	12 月	合計（割合）
国内ブランド	25	25	24	74(21%)
国外ブランド	87	71	69	227(63%)
ブランド不明（注 5）	18	24	17	59(16%)
月別合計	130	120	110	360(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 74 件と、前四半期の 57 件から 30%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 227 件と、前四半期の 161 件から 41%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 72.7%を占めています。

前四半期に引き続き、国内通信事業者を装ったフィッシングの報告が寄せられています。10 月半ばには、ケーブルネットワークなど複数通信事業者の Web メールサービスを装ったフィッシングサイトが確認されました。また、異なるブランドに関するフィッシングメールに、共通の文面が使用されている事例も確認されました。

10 月末には、国内金融機関のインターネットバンキングのページに利用者がアクセスした際に、第二認証情報などを入力させるための不正なポップアップ画面を表示し、入力された情報を窃取するマルウエアが確認されました。また、国内金融機関を装った一般的な手法のフィッシングサイトも継続して確認されています。

フィッシングサイトの調整先の割合は、国内が 44%、国外が 56%と、前四半期の割合（国内 56%、国外 44%）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、737 件でした。前四半期の 796 件から 7%減少しています。

Web サイト改ざんでは、ページに不正に挿入された JavaScript や iframe によってサイト閲覧者を攻撃サイトに誘導し、複数の脆弱性を使用した攻撃により PC をマルウエアに感染させるものが多く確認されています。

2012 年 11 月には、2012 年 10 月に修正された Java の脆弱性(CVE-2012-5076)を悪用してマルウエアに感染させる手法が、誘導先の攻撃サイトで使用されていることを確認しました。古いバージョンの Java を使用していると、その脆弱性を使用した攻撃により、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、213 件でした。前四半期の 202 件から 5%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、2794 件でした。前四半期の 3391 件から 18%減少しています。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	10 月	11 月	12 月	合計
80/tcp	409	430	391	1230
25/tcp	182	188	559	929
22/tcp	183	187	117	487
udp	57	58	60	175
5900/tcp	3	4	1	8
3389/tcp	2	2	1	5
21/tcp	1	1	2	4
143/tcp	1	3	0	4
110/tcp	2	2	0	4
8080/tcp	2	0	0	2
3306/tcp	1	1	0	2
8088/tcp	0	1	0	1
5901/tcp	0	1	0	1
135/tcp	1	0	0	1
不明	7	4	0	11
月別合計	851	882	1131	2864

頻繁にスキャンの対象となったポートは、http(80/tcp)、smtp(25/tcp)、ssh(22/tcp)でした。udp については、DNS(53/udp)や 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。

【国内大学からのデータベース情報流出】

2012 年 10 月の初めに、海外ハッカーグループが、世界各国の大学から窃取したデータベース情報をアップロードした URL のリストを、テキスト共有サイト Pastebin に投稿しました。内容を調査したところ、日本の複数の大学から漏えいしたように見受けられる情報が、複数のテキスト共有サイトにアップロードされていました。

JPCERT/CC は、データベース情報が流出した可能性がある大学に確認を依頼し、大学が調査した結果、実際にデータベースに対して不正なアクセスが発生していたことが分かりました。当該大学から流出した情報の削除依頼を受け、該当するすべてのテキスト共有サイトの管理者に投稿された情報の削除を要請し、データベース情報がサイトから削除されたことを確認しました。

【政府関係者を騙るマルウエア添付メール】

2012 年 10 月、JPCERT/CC 宛に、政府関係者を名乗る発信者から、ファイルが添付されたメールが届きました。このメールは、イタリアの IP アドレスのメールサーバから送信されたものでした。メールに添付されていたファイルを分析したところ、ファイルは RAT(Remote Access Trojan:リモートアクセス型トロイの木馬)に分類されるマルウエアであり、クラウドサービス上のサーバに接続を行うことが分かりました。

JPCERT/CC は、マルウエアが接続する先のクラウドサービスのネットワーク管理者に対して、サービスが何らかの攻撃に悪用されている可能性があることを連絡し、先方から調査、対応を行うとの返信を受領しました。

【国内金融機関のアカウント情報を窃取するマルウエアに関する対応】

2012 年 11 月、国内金融機関より、インターネットバンキングのアカウント情報を窃取するマルウエアに関する報告が寄せられました。報告によると、マルウエアはロシアの IP アドレスが割り当てられた「.cc」ドメインの Web サーバにアクセスものであったことから、JPCERT/CC では、マルウエアが接続する Web サーバのネットワーク管理者とドメイン管理者に状況を伝えて対処を依頼し、その結果、当該ドメインが停止されたことを確認しました。

JPCERT/CC®

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

JPCERT CC®

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

JPCERT CC®

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。