JPCERT/CC®

JPCERT-IR-2013-01
発行日: 2013-04-15

JPCERT/CC インシデント報告対応レポート
[2013 年 1 月 1 日 ～ 2013 年 3 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、2013 年 1 月 1 日から 2013 年 3 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]

	1 月	2 月	3 月	合計	前四半期合計
報告件数 (注 2)	1919	1847	1687	5453	5064
インシデント件数 （注 3）	1949	1836	1907	5692	5293
調整件数（注 4）	582	834	814	2230	1497

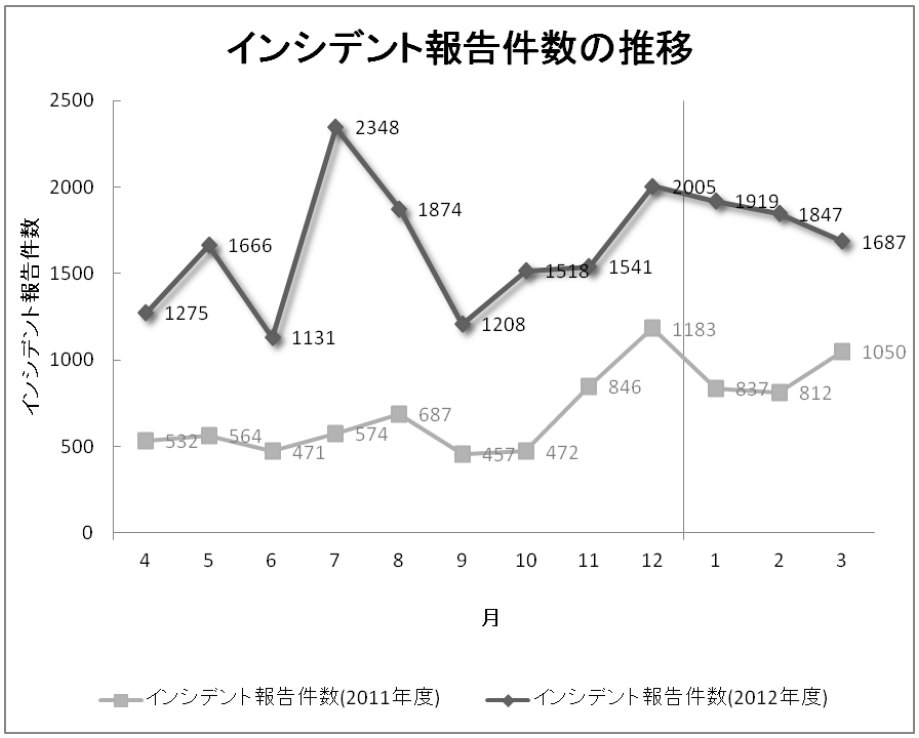
【注 2】「報告件数」は、報告者から寄せられた Web フォーム、メール、FAX による報告の総数を示します。

【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。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にも、1 件として扱います。

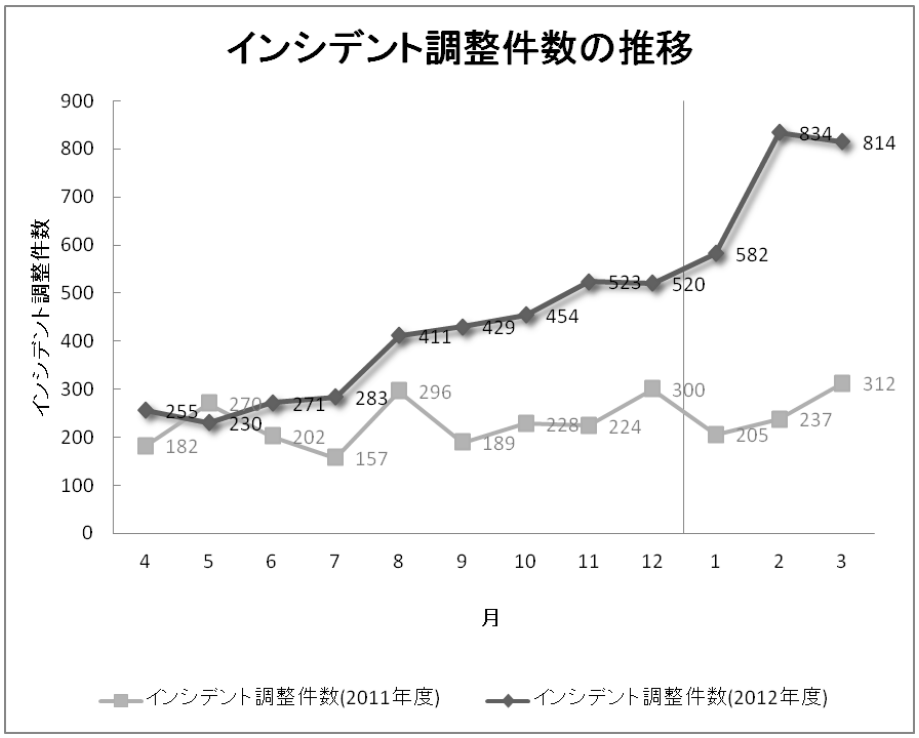
【注 4】「調整件数」とは、インシデントの拡大防止のため、サイトの管理者などに対し、現状の調査と問題解決のための対応を依頼した件数を示します。

本四半期に寄せられた報告件数は、5453 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 2230 件でした。前四半期と比較して、総報告件数は 8%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 102%増加し、調整件数は 196%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]

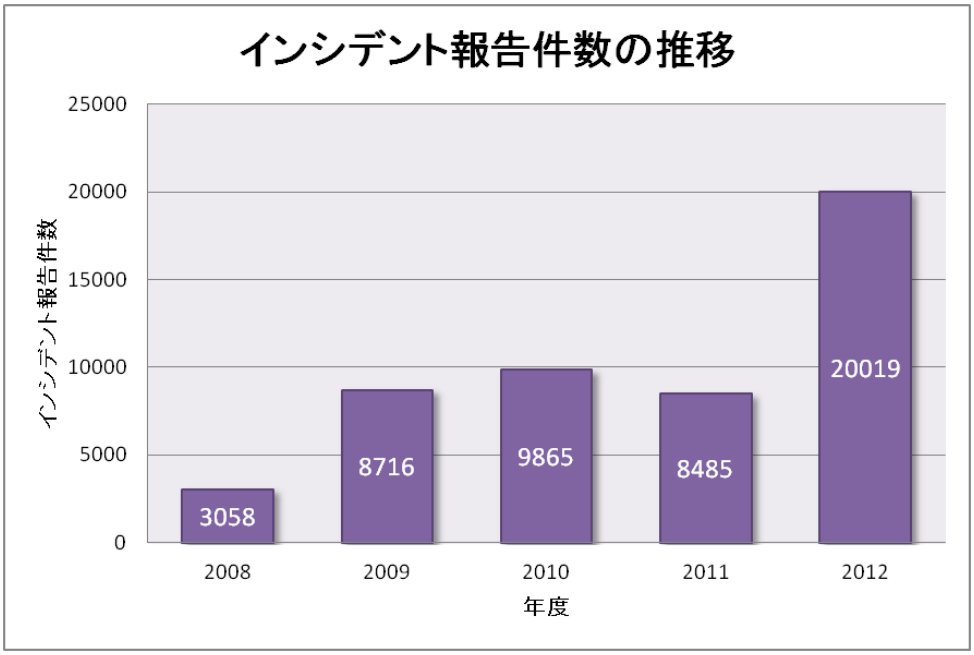
【参考】統計情報の年度比較

2012 年度を含む過去 5 年間の報告件数を表 2 に示します。なお、年度の期間は、当該年の 4 月 1 日から翌年の 3 月 31 日までとしています。

[表 2 年間報告件数の推移]

年度	2008	2009	2010	2011	2012
報告件数	3058	8716	9865	8485	20019

2012 年度に寄せられた報告件数は 20019 件でした。前年度の 8485 件と比較して、136 % 増加しています。 [図 3] に過去５年間の年間報告件数の推移を示します。



[図 3 インシデント報告件数の推移（年度比較）]

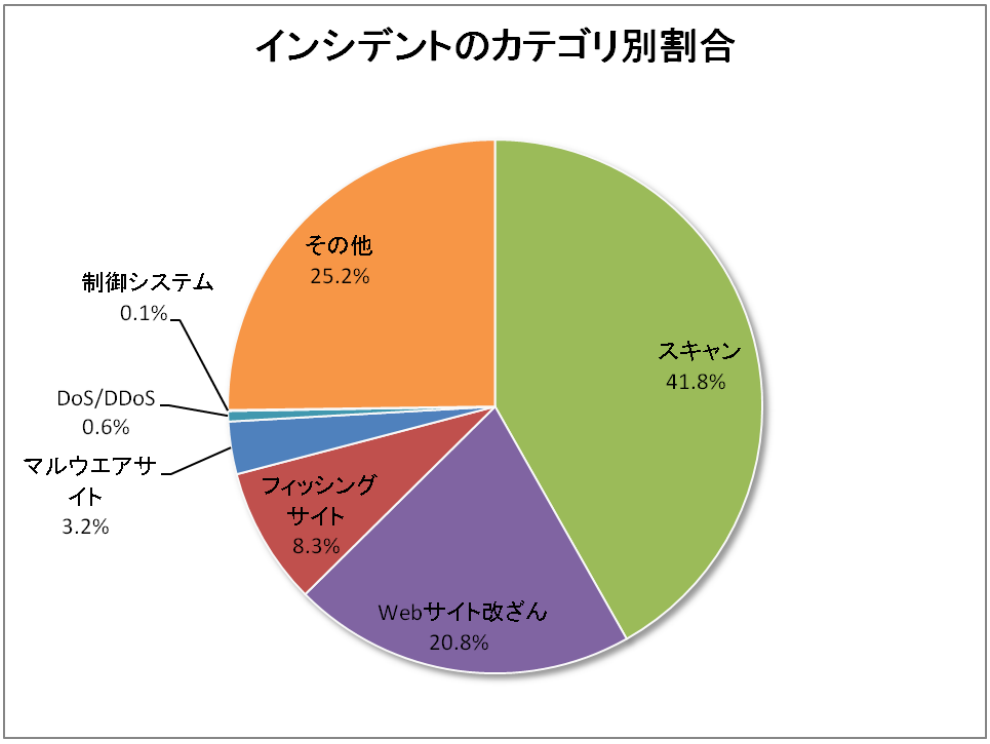
JPCERT/CC では、報告を受けたインシデントをカテゴリ別に分類し、各インシデントカテゴリに応じた調整、対応を実施しています。各インシデントの定義については、6.[付録]インシデントの分類を参照してください。本四半期に報告を受けた各カテゴリのインシデント件数を[表 3]に示します。

[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	1 月	2 月	3 月	合計	前四半期合計
フィッシングサイト	149	174	151	474	360
Web サイト改ざん	325	496	363	1184	737
マルウエアサイト	64	53	64	181	213
スキャン	845	634	900	2379	2794
DoS/DDoS	1	1	34	36	6
制御システム	3	0	0	3	-
その他	562	478	395	1435	1183

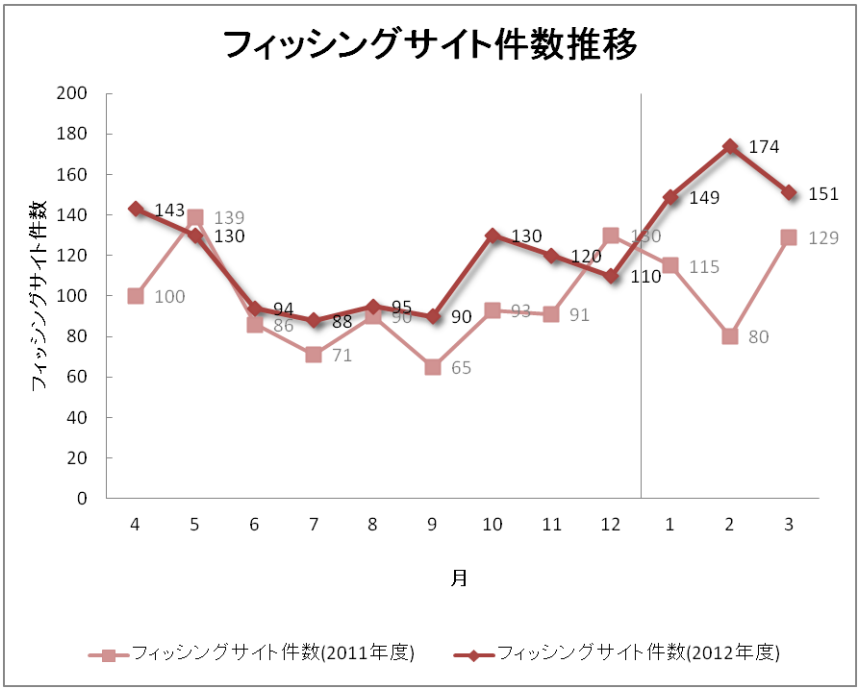
本四半期に発生したインシデントにおける各カテゴリの割合は、[図 4]のとおりです。スキャンに分類される、システムの弱点を探索するインシデントは 41.8%、Web サイト改ざんに分類されるインシデントは 20.8%を占めています。また、フィッシングサイトに分類されるインシデントは 8.3%でした。

JPCERT/CC では、本四半期から制御システムに関わるインシデント報告の受付を開始しました。これにあわせ、インシデントカテゴリに、新たに「制御システム」を追加しました。

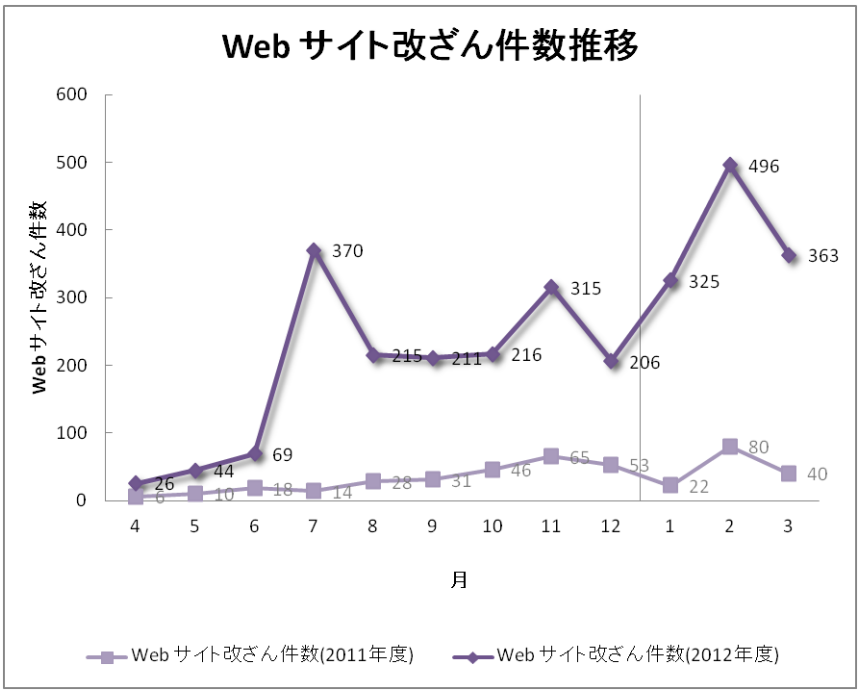


[図 4 インシデントのカテゴリ別割合]

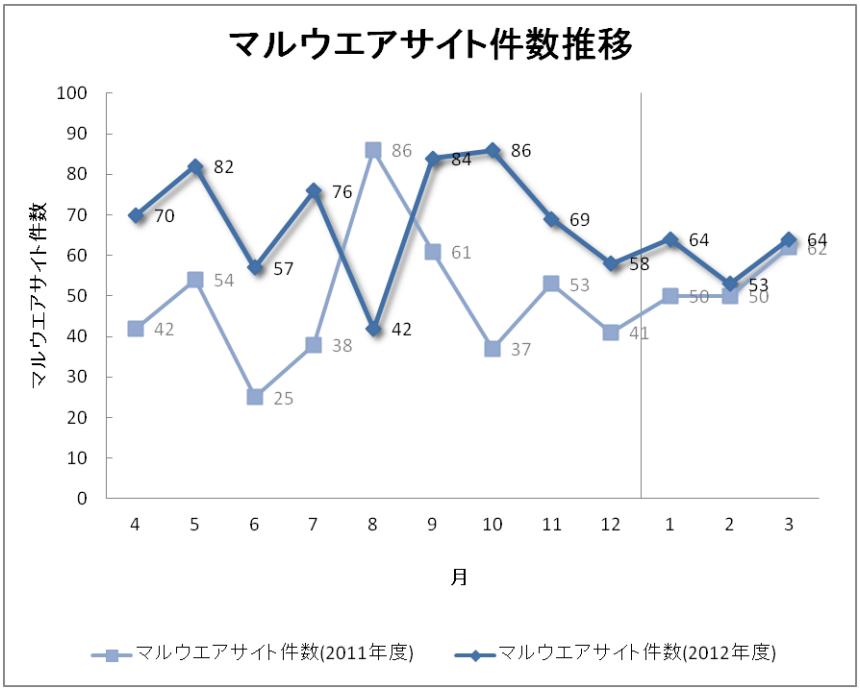
[図 5]から[図 8]に、フィッシングサイト、Web サイト改ざん、マルウエアサイト、スキャンのインシデントの過去 1 年間の月別推移を示します。



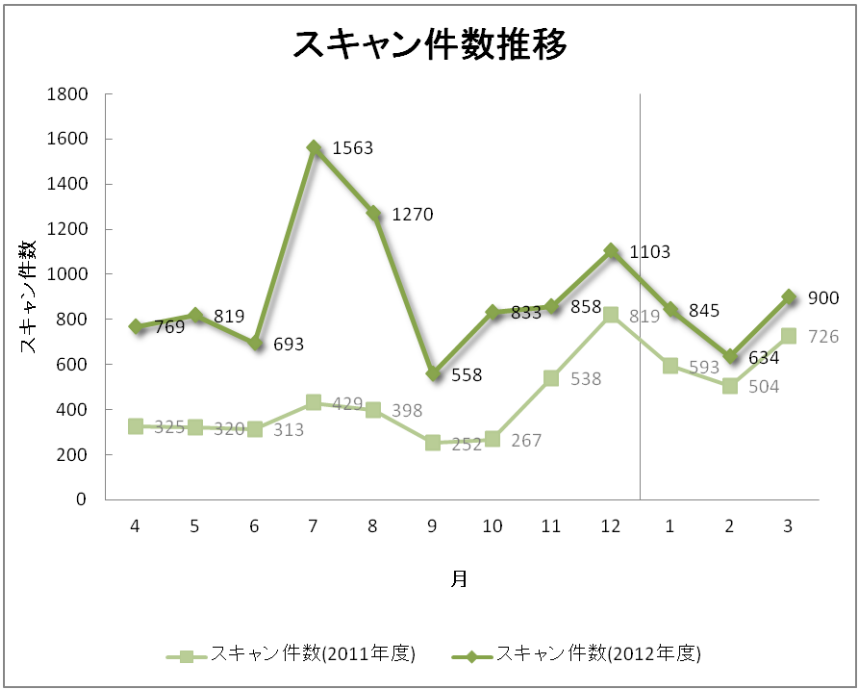
[図 5 フィッシングサイト件数推移]



[図 6 Web サイト改ざん件数推移]

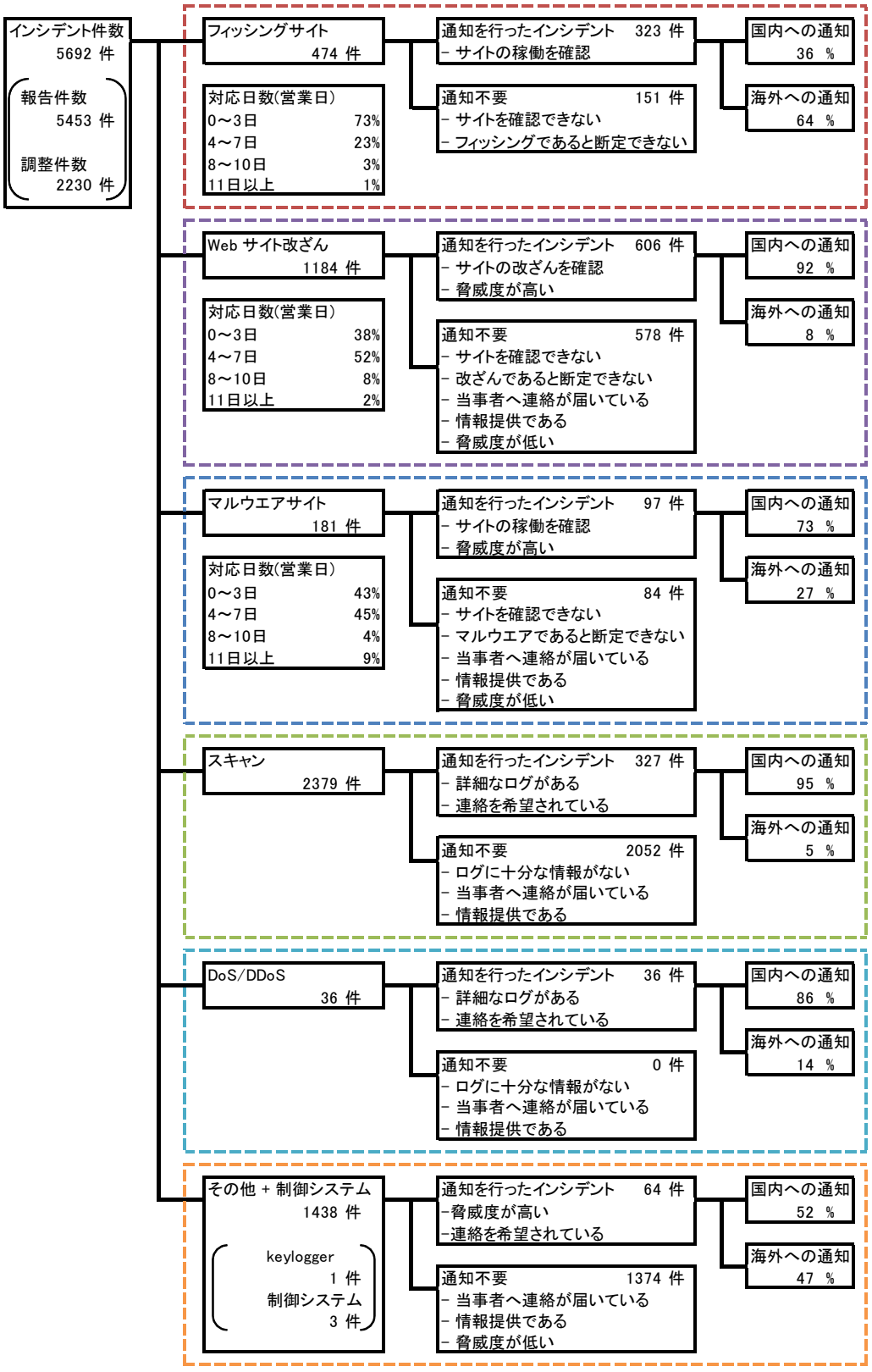


[図 7 マルウエアサイト件数推移]



[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

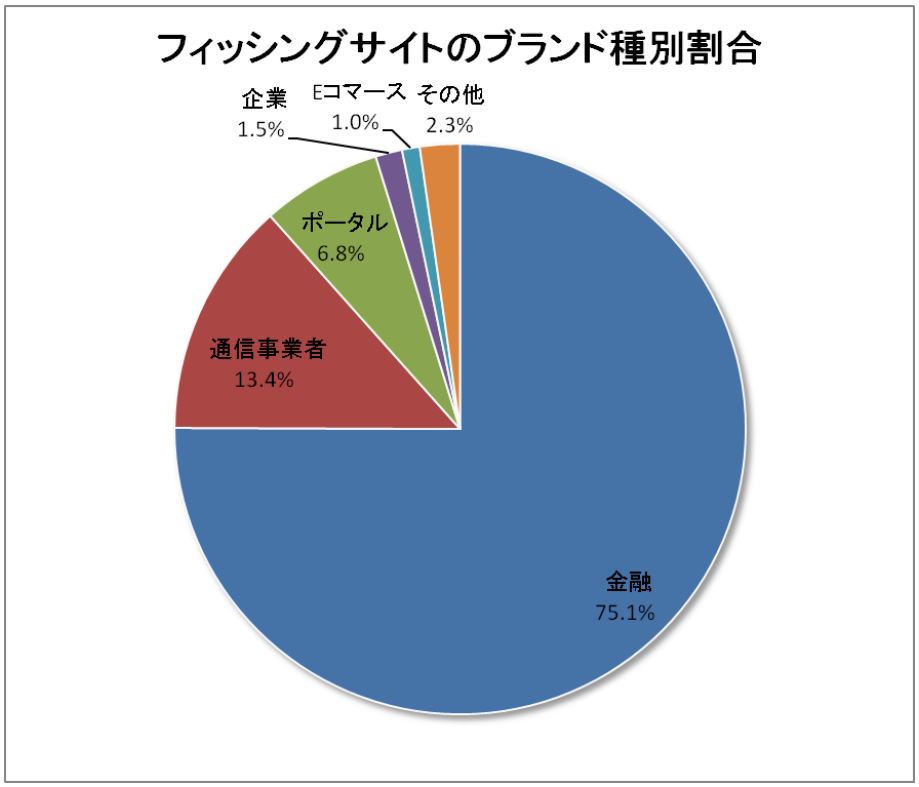
3.1. フィッシングサイトの傾向

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 474 件で、前四半期の 360 件から 32%増加しました。また、前年度同期（324 件）との比較では、46%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	1 月	2 月	3 月	合計 (割合)
国内ブランド	42	40	30	112(24%)
国外ブランド	84	103	98	285(60%)
ブランド不明（注 5）	23	31	23	77(16%)
月別合計	149	174	151	474(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 112 件と、前四半期の 74 件から 51%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 285 件と、前四半期の 227 件から 26%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 75.1%を占めています。

本四半期は、国内金融機関を装ったフィッシングサイトと、国内通信事業者の Web メールサービスを装ったフィッシングサイトの報告を多数受領しています。これらのフィッシングサイトは、海外の特定の無料ホスティングサービスを使って構築される傾向があることを確認しています。国内金融機関を装ったフィッシングサイトでは、見た目はインターネットバンキングのログイン画面を装っていながら、クレジットカードの情報を入力させることを目的としたものが多くありました。

フィッシングサイトの調整先の割合は、国内が 36%、国外が 64%であり、前四半期（国内 44%、国外 56%）と比較して、国外への調整の割合が増えました。

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、1184 件でした。前四半期の 737 件から 61%増加しています。

本四半期は、不審な iframe タグがページの末尾に挿入される改ざんを受けた Web サイトの報告を非常に多く受領しました。iframe によって誘導される先のサイトにアクセスすると、複数のアプリケーションの脆弱性を使用した攻撃が行われることを確認しています。そのため、古いバージョンのアプリケーションがインストールされている PC でサイトを閲覧すると、PC がマルウエアに感染する可能性があります。

2013 年 3 月半ばには、特定のブラウザのユーザエージェントを使用して Web サイトにアクセスしたときにだけ、iframe が埋め込まれた Web ページが返され、不審な別のサイトに誘導されるという改ざんに関する報告が寄せられました。この iframe は、攻撃によってサーバに不正に設置された apache モジュールが、html ファイルや JavaScript ファイルをブラウザに渡す際に動的に埋め込んでいるものであることが分かりました。この iframe は、直接ファイルに埋め込まれるものではないため、Web サーバ上のファイルを調査しても改ざんのコードを確認することはできません。原因を特定するためには、apache の設定ファイルが改ざんされていたり、インストールしていない apache モジュールが存在したりしていないかを確認する必要があります。

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、181 件でした。前四半期の 213 件から 15%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、2379 件でした。前四半期の 2794 件から 15%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。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。

[表 5　ポート別のスキャン件数]

ポート	1 月	2 月	3 月	合計
80/tcp	403	247	299	949
25/tcp	259	252	423	934
udp	95	69	101	265
22/tcp	94	78	77	249
3389/tcp	3	5	6	14
21/tcp	5	2	6	13
143/tcp	3	7	3	13
8080/tcp	1	2	7	10
5900/tcp	2	1	4	7
23/tcp	2	1	2	5
110/tcp	4	0	1	5
icmp	0	0	3	3
1433/tcp	0	2	1	3
8443/tcp	1	0	0	1
514/tcp	0	1	0	1
4899/tcp	1	0	0	1
不明	6	0	2	8
月別合計	879	667	935	2481

4. インシデント対応事例

本四半期に行った対応の例を紹介します。

【DoS 攻撃に使用されるツールが設置されたサーバ】
海外の金融機関などに対する DDoS 攻撃の踏み台になっている可能性がある国内サーバの情報を 2013 年 1 月に海外組織から受領しました。提供された情報には、攻撃者が踏み台に指令を与えるための URL が含まれていました。この URL は普通にアクセスすると、ファイルが存在しないという表示を返すなど、外部からの調査に対して巧妙な偽装を行っていました。

JPCERT/CC は当該サーバの管理者に調査を依頼し、設置されていた攻撃ツールを入手しました。提供を受けた攻撃ツールを分析したところ、DDoS 攻撃で使用するようなパケットの送信やファイルのアップロードなどの機能を持っていることがわかりました。

【金融系マルウエアが通信を行うサーバに関する対応】
2013 年 1 月に、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の検体を国内金融機関から提供していただきました。JPCERT/CC が検体を分析したところ、このマルウエアに感染した PC は、ロシアの IP アドレスが割り当てられたサーバに対して通信を行うことが分かりました。JPCERT/CC はマルウエアが通信を行うサーバのネットワーク管理者に対して、サーバが悪用されていないか調査を依頼し、結果としてサーバが停止し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/

制御システムインシデントの報告
https://www.jpcert.or.jp/ics/ics-form.html

制御システムインシデントの報告（Web フォーム）
https://form.jpcert.or.jp/ics.html

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

○ 制御システム

「制御システム」とは、制御システムや各種プラントが関連するインシデントを指します。

JPCERT/CC では、以下を「制御システム」と分類しています。

- インターネット経由で攻撃が可能な制御システム
- 制御システムを対象としたマルウエアが通信を行うサーバ
- 制御システムに動作異常などを発生させる攻撃

○ 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。