JPCERT CC®

JPCERT-IR-2014-02
発行日: 2014-04-15

JPCERT/CC インシデント報告対応レポート
[2014 年 1 月 1 日 ～ 2014 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、2014 年 1 月 1 日から 2014 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およ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、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することを目的として活動しています。国際的な調整・支援が必要となるインシデントについては、日本における窓口組織として、国内や国外(海外の CSIRT 等)の関係機関との調整活動を行っています。

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)	1606	1409	1883	4898	4812
インシデント件数 （注 3）	1643	1190	1696	4529	4788
調整件数（注 4）	739	614	636	1989	2135

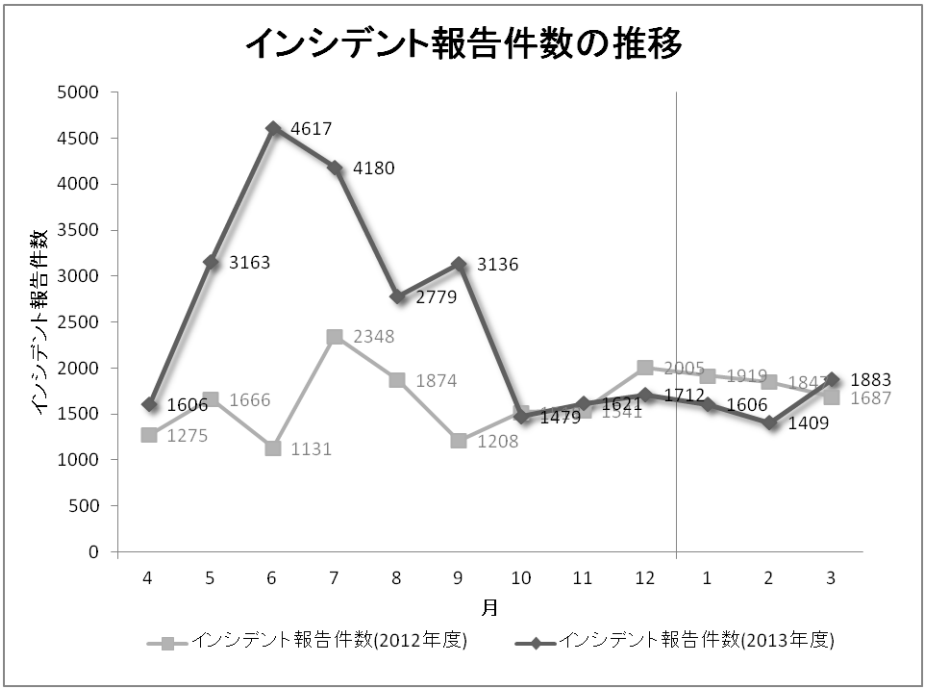
【注 2】「報告件数」は、報告者から寄せられた Web フォーム、メール、FAX による報告の総数を示します。

【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。

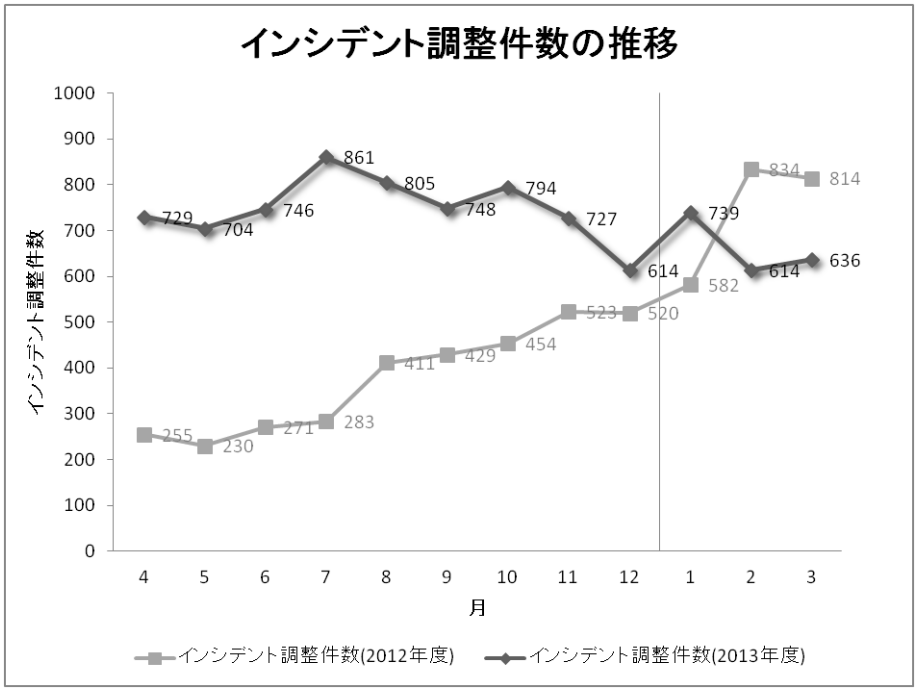
【注 4】「調整件数」は、インシデントの拡大防止のため、サイトの管理者等に対し、現状の調査と問題解決のための対応を依頼した件数を示します。

本四半期に寄せられた報告件数は、4898 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 1989 件でした。前四半期と比較して、総報告件数は 2%増加し、調整件数は 7%減少しました。また、前年同期と比較すると、総報告数で 10%減少し、調整件数は 11%減少しました。

[図 1]と[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]

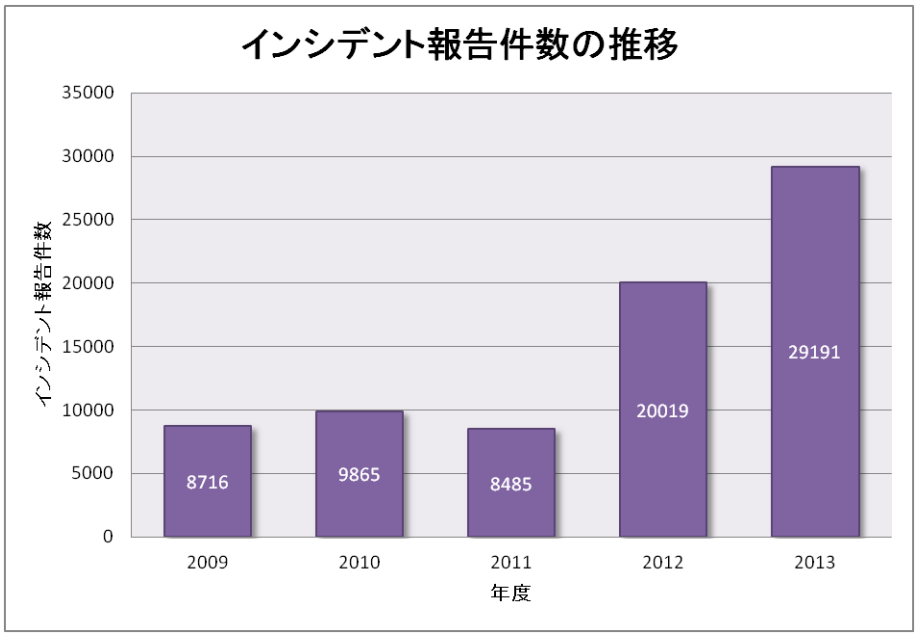
【参考】統計情報の年度比較

2013 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	2009	2010	2011	2012	2013
報告件数	8716	9865	8485	20019	29191

2013 年度に寄せられた報告件数は 29191 件でした。前年度の 20019 件と比較して、46%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。



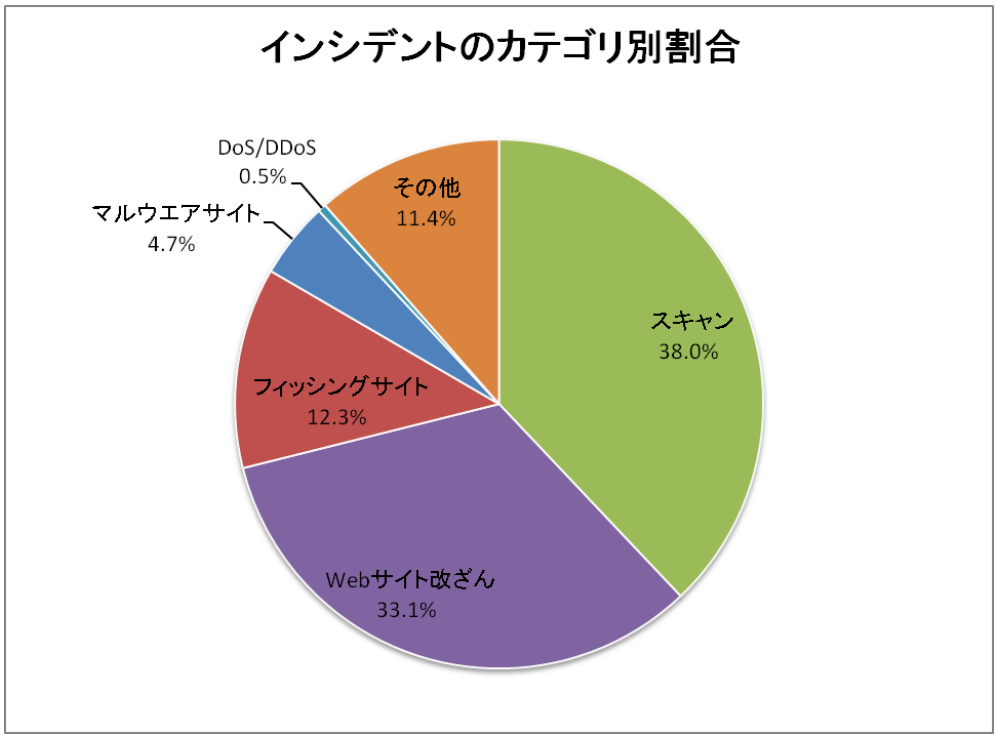
[図 3 インシデント報告件数の推移（年度比較）]

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、「付録-1. 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]

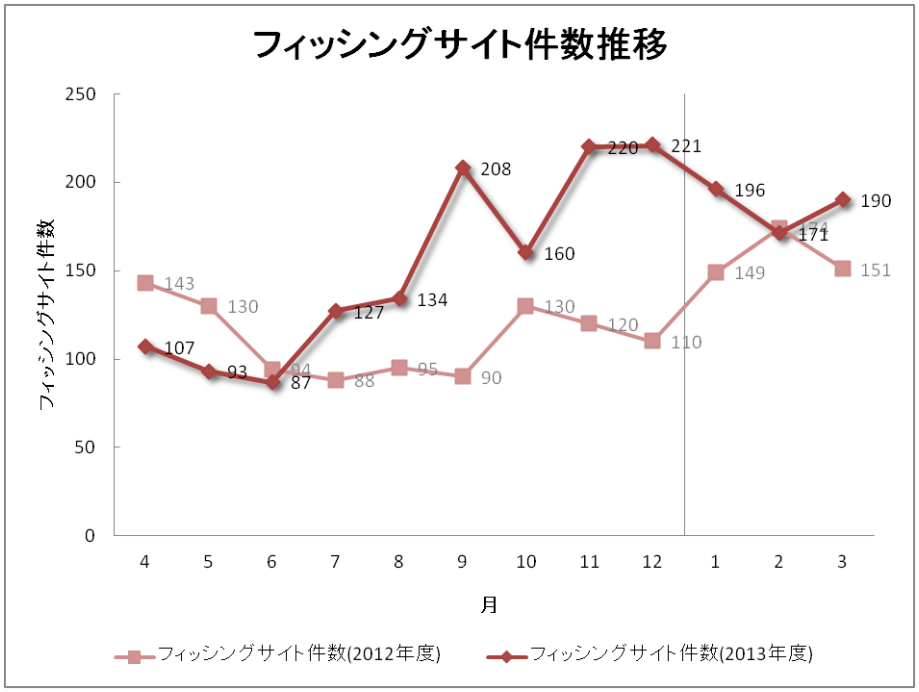
インシデントカテゴリ	1 月	2 月	3 月	合計	前四半期合計
フィッシングサイト	196	171	190	557	601
Web サイト改ざん	663	258	580	1501	1604
マルウエアサイト	110	46	55	211	229
スキャン	417	567	735	1719	1560
DoS/DDoS	3	0	20	23	8
制御システム関連	0	0	0	0	1
その他	254	148	116	518	785

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 38.0%、Web サイト改ざんに分類されるインシデントは 33.1%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 12.3%でした。

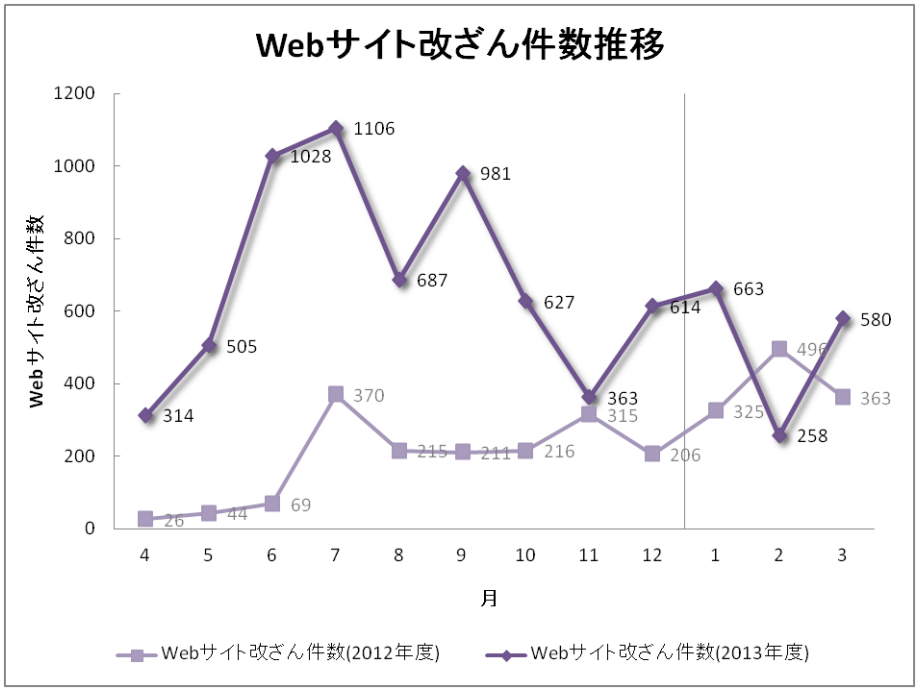


[図 4 インシデントのカテゴリ別割合]

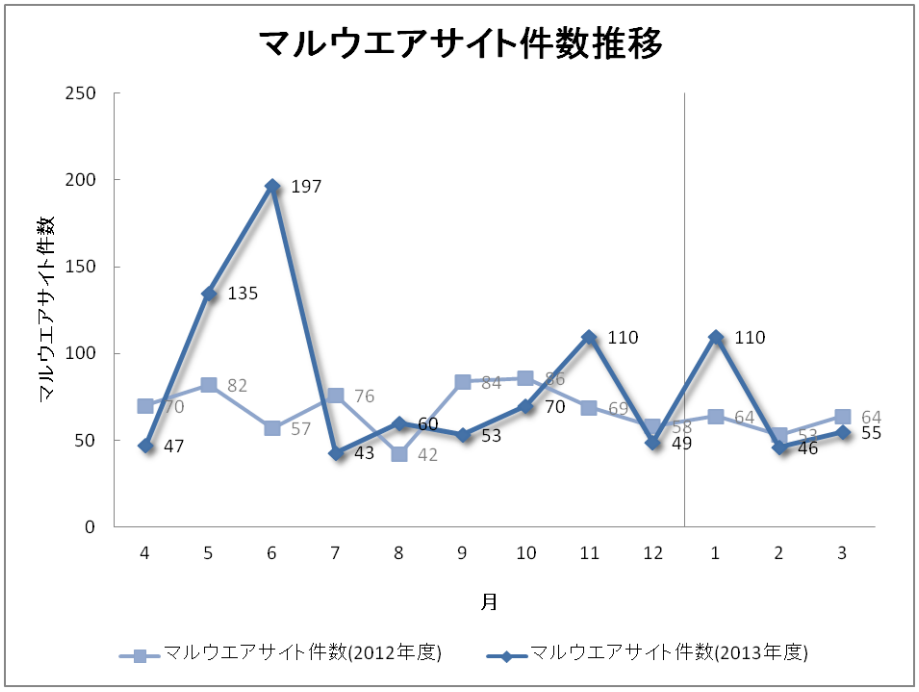
[図 5]から[図 8]に、フィッシングサイト、Web サイト改ざん、マルウエアサイト、スキャンのインシデントの過去 1 年間の月別推移を示します。



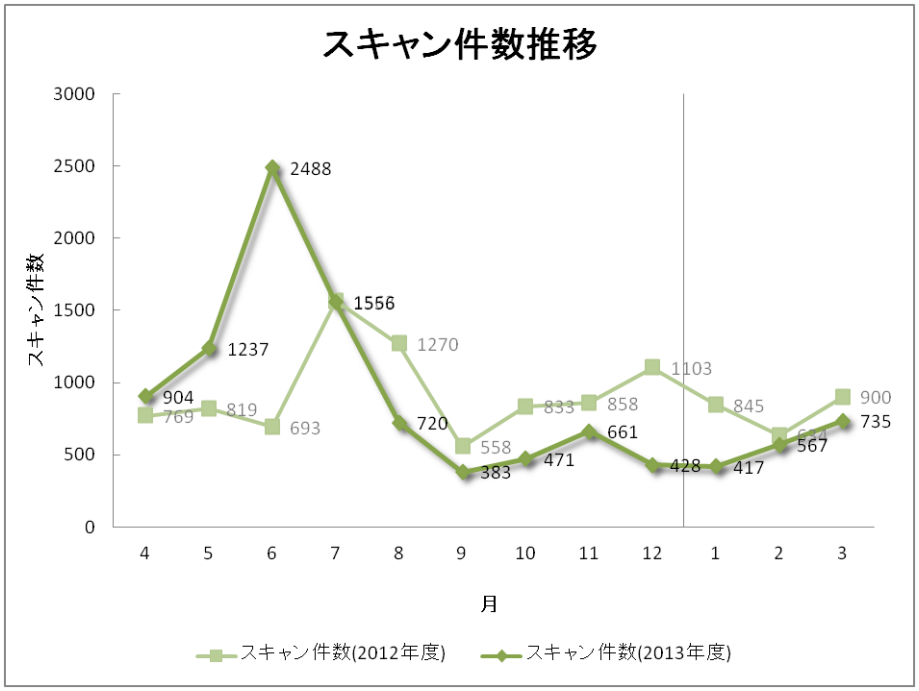
[図 5 フィッシングサイト件数推移]



[図 6 Web サイト改ざん件数推移]

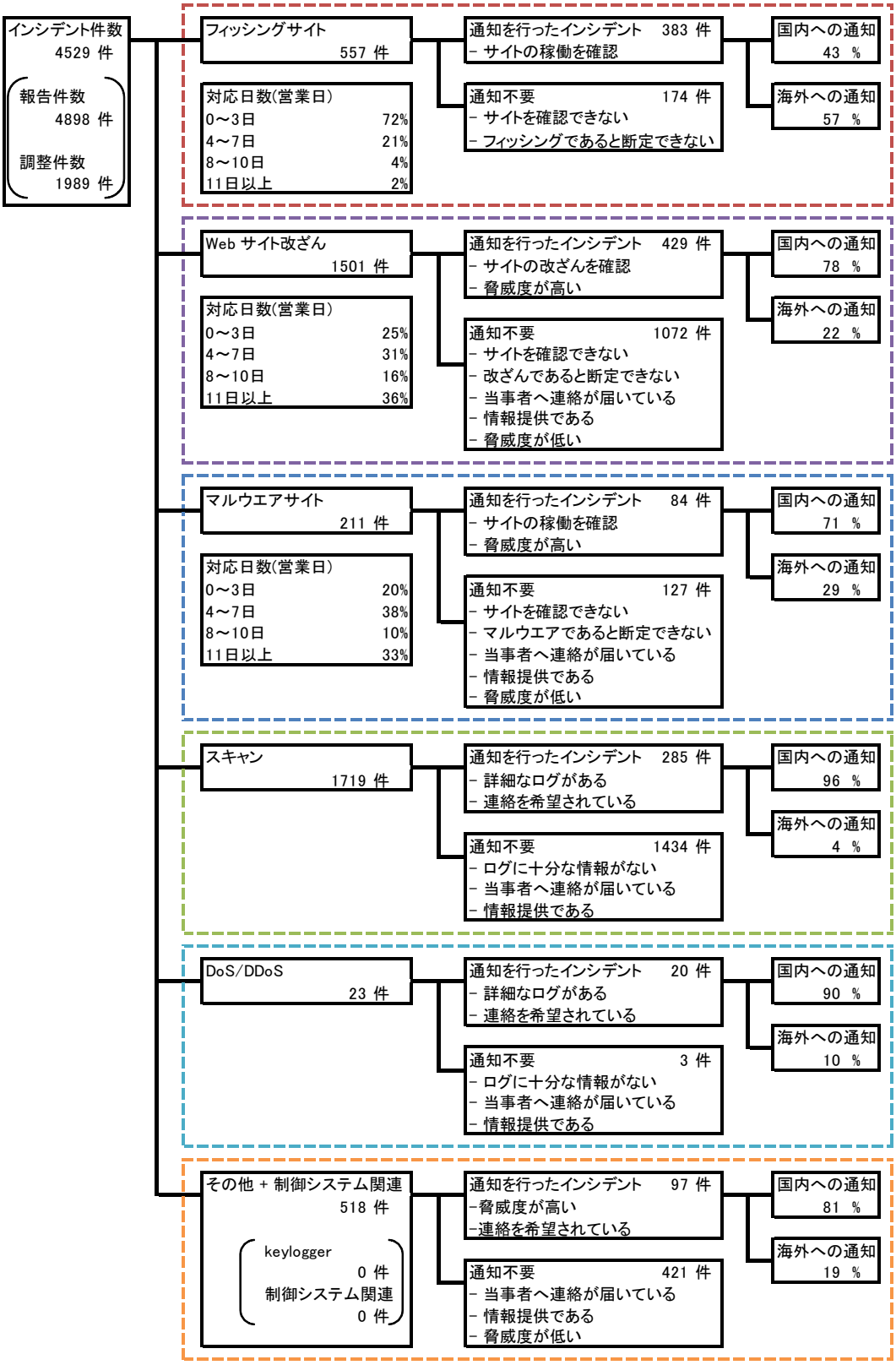


[図 7 マルウエアサイト件数推移]



[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

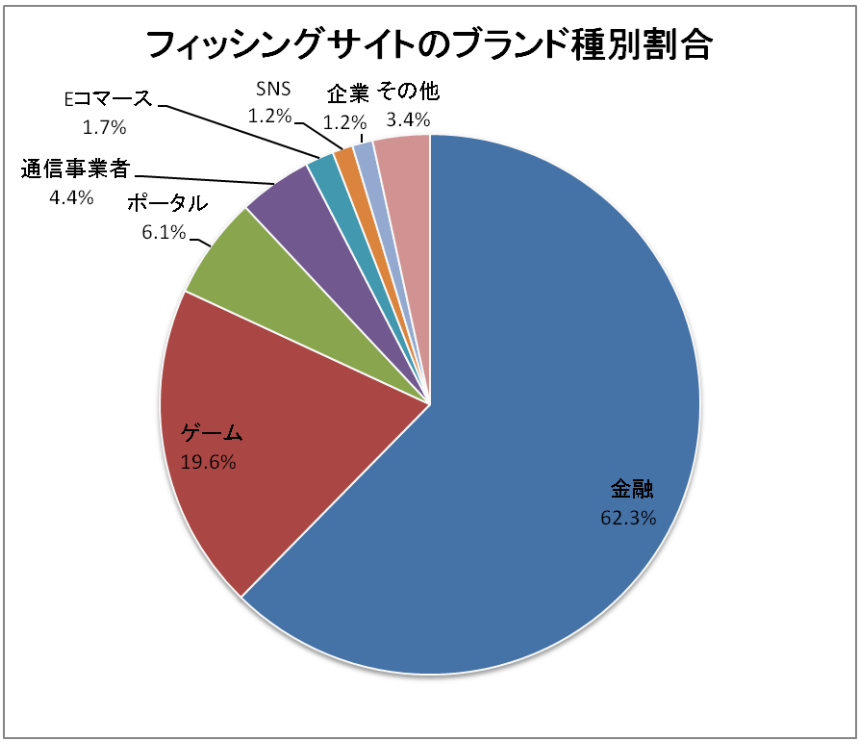
3.1. フィッシングサイトの傾向

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 557 件で、前四半期の 601 件から 7%減少しました。また、前年度同期(474 件)との比較では、18%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	国内外別合計(割合)
国内ブランド	75	70	84	229(41%)
国外ブランド	64	70	53	187(25%)
ブランド不明(注 5)	57	31	53	141(32%)
月別合計	196	171	190	557(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等の理由により、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 229 件と、前四半期の 253 件から 9%減少しました。国外ブランドを装ったフィッシングサイトの件数は 187 件と、前四半期の 204 件から 8%減少しました。

JPCERT/CC で報告を受領したフィッシングサイト全体では、金融機関のサイトを装ったものが 62.3%、オンラインゲームサービスを装ったものが 19.6%を占めています。装われたブランドは、国内ブランド、海外ブランドともに、金融機関が最も多数を占めました。

2014 年 2 月半ばに、検索エンジンの検索連動型広告を使用して国内金融機関を装ったフィッシングサイトに誘導する手法が確認されました。不正な広告は広告欄の最上位に表示され、金融機関の正規サイトの URL を記載しているため、画面上の表示を見ただけではフィッシングサイトへ誘導するものとは分からないようになっていました。フィッシングの被害を防ぐためには、パスワードなど機微な情報の入力に先立って URL が正規サイトのものであるか確認するなどの基本的な対策に加え、金融機関が提供している場合にはワンタイムパスワードサービスやフィッシング対策ソフトウェアを利用するなどの対策が重要です。

前四半期に引き続き、国内通信事業者が動的に割り当てる IP アドレスを持った、国内および海外のオンラインゲームサービスと国内金融機関を装ったフィッシングサイトに関する報告を非常に多く受領しました。国内金融機関を装ったフィッシングサイトは 1 月末から 2 月後半にかけて確認されない期間がありましたが、2 月末以降には、前四半期にも見られた海外の Web サイトから誘導されるフィッシング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 43%、国外が 57%であり、前四半期(国内 43%、国外 57%)と同じ割合になっています。

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、1501 件でした。前四半期の 1604 件から 6%減少しています。

2014 年 2 月後半に国内の複数の Web サイトが改ざんされ、Internet Explorer の当時未修正だった脆弱性(CVE-2014-0322)を攻撃する不正なファイルが設置されていました。改ざんされた Web サイトは、埋め込まれた iframe や JavaScript によって、脆弱性を攻撃する swf ファイルや jar ファイルなどに利用者を誘導して、閲覧した PC をマルウエアに感染させる仕組みになっていました。攻撃によって感染するマルウエアを分析した結果、海外のサーバへの端末情報の送信や、攻撃者がマルウエアへの命令に使用していたと考えられる国内ブログサービスの特定のページにアクセスして、何らかの情報を取得するなどの挙動を確認することができました。

一方で、不正な iframe や JavaScript がページに挿入された Web サイトに関する報告も大量に受領しています。

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、211 件でした。前四半期の 229 件から 8%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、1719 件でした。前四半期の 1560 件から 10%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。頻繁にスキャンの対象となったポートは、smtp(25/tcp)、http(80/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
25/tcp	193	318	342	853
80/tcp	156	180	300	636
22/tcp	79	54	50	183
udp	4	40	29	73
21/tcp	3	2	16	21
23/tcp	0	2	10	12
3389/tcp	1	5	5	11
143/tcp	1	5	2	8
5900/tcp	3	2	1	6
5000/tcp	0	0	5	5
1433/tcp	4	1	0	5
8080/tcp	1	0	1	2
443/tcp	2	0	0	2
3306/tcp	0	0	2	2
135/tcp	0	2	0	2
9090/tcp	0	0	1	1
7822/tcp	1	0	0	1
6000/tcp	0	0	1	1
5631/tcp	1	0	0	1
50000/tcp	0	0	1	1
500/tcp	1	0	0	1
25724/tcp	0	1	0	1
不明	13	12	8	33
月別合計	463	624	774	1861

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。

【海外への DDoS 攻撃に悪用された国内の NTP サーバに関する対応】
JPCERT/CC は、2014 年 1 月半ばに、ntpd の monlist 機能を使った DDoS 攻撃に関する注意喚起を発行しました。NTP は UDP を使用して通信するため、送信元 IP アドレスを詐称した問合せが可能です。また、ntpd の monlist 機能は、問合せパケットに比べてサイズの大きなパケットを返送します。そのため、攻撃者は、攻撃先の IP アドレスを送信元アドレスに設定して NTP サーバに monlist の問合せを行うことで、攻撃先に大きなサイズのデータを送りつけることができます。

2014 年 1 月から 2 月にかけて、複数の海外組織から、日本国内のネットワーク上に存在する NTP サーバから DDoS 攻撃を受けたという報告を受領しました。JPCERT/CC では、報告された IP アドレスのホストで ntpd の monlist 機能が有効になっているかどうかを調べ、有効になっていることが確認できたホストのネットワーク管理者には設定を変更するよう依頼しました。

【SSH ルートキットに感染した国内のホストに関する対応】
2014 年 1 月初め、海外の National CSIRT から、SSH ルートキットに感染した国内ホストの情報を受領しました。SSH ルートキットは、感染したホストにおける SSH 接続のアカウント情報や秘密鍵を窃取して外部のサーバに送信するマルウエアであり、報告元の組織からは、窃取した情報の送信先となっていたサーバと国内ホストが通信を行った記録が提供されました。また、SSH ルートキットは、すべてのユーザが読み書き可能なサイズの大きい内部メモリ領域を使用するという特徴があり、感染を確認するにはメモリ領域を調査する必要があるとのことでした。

JPCERT/CC は、提供された情報をもとに、該当するサーバのネットワーク管理者に対し、SSH ルートキットに感染している可能性および調査の方法等を通知しました。

【マイクロソフトと海外セキュリティ組織が行ったボットネット撲滅活動への対応】
マイクロソフトが中国の National CSIRT である CNCERT/CC と共同で行った、ボットネット「Nitol」を対象にした対策活動で差し押さえられた C&C(コマンドアンドコントロールサーバ)のログを、CNCERT/CC から受領しました。マルウエア Nitol に感染したコンピュータは、悪意ある第三者から遠隔操作され、保持している情報を窃取されます。

提供されたログをもとに、サーバのネットワーク管理者に、該当ログの日時に C&C へのアクセスが行われていないか、また該当ホストがマルウエアに感染していないか調査を依頼しました。依頼先の中には、Nitol 以外のマルウエアが検知された旨をご報告くださった組織もあり、検知されたマルウエアの情報を、報告組織の承諾を得て、CNCERT/CC に共有し、ボットネット対策活動に協力しました。

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/

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います。利用をご希望の方は、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等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等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等のサイトに似せた 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。

- 攻撃者やマルウエア等により悪意のあるスクリプトや iframe 等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 等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等)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ないもの)を指します。また、マルウエア等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等)
- 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、ワーム等)による感染の試み(未遂に終わったもの)
- ssh,ftp,telnet 等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等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。

- 大量の通信等により、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 メール等)を受信させることによるサービス妨害

○ 制御システム関連インシデント

「制御システム関連インシデント」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「制御システム関連インシデント」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等を発生させる攻撃

○ 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、例えば、以下を「その他」に分類しています。

- 脆弱性等を突いたシステムへの不正侵入
- ssh,ftp,telnet 等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、ワーム等)の感染

本活動は、経済産業省より委託を受け、「平成２５年度情報セキュリティ対策推進事業」として実施したものです。