JPCERT-IR-2015-02
発行日: 2015-04-16

JPCERT/CC インシデント報告対応レポート
[2015 年 1 月 1 日 ～ 2015 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、2015 年 1 月 1 日から 2015 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)	2981	1939	1949	6869	6231
インシデント件数 (注 3)	2127	1695	1663	5485	5606
調整件数 (注 4)	1093	899	1096	3088	2337

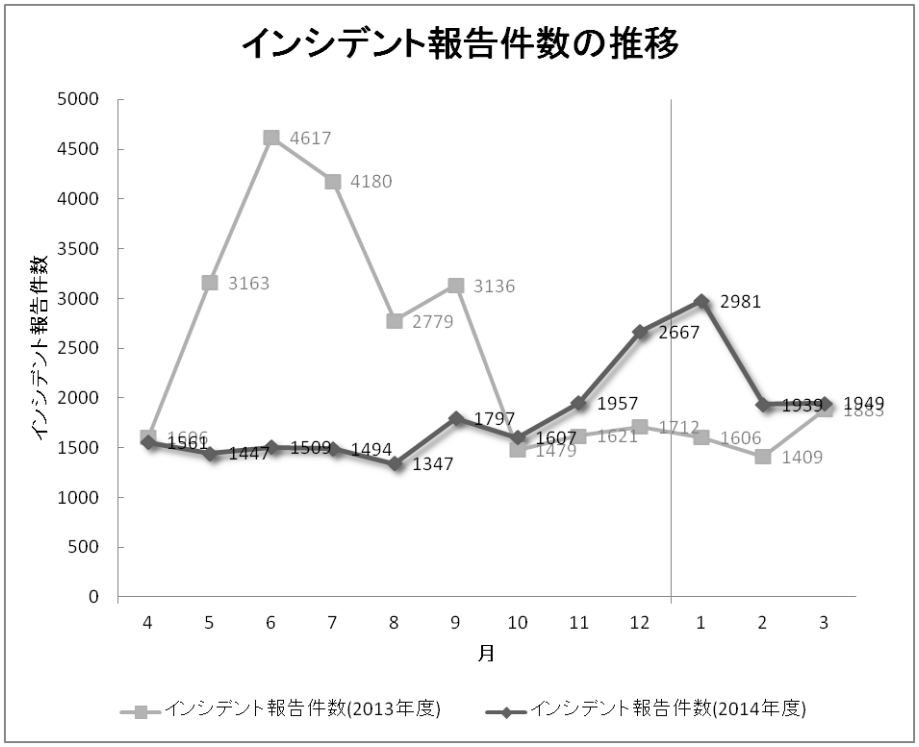
【注 2】「報告件数」は、報告者から寄せられた Web フォーム、メール、FAX による報告の総数を示します。

【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。

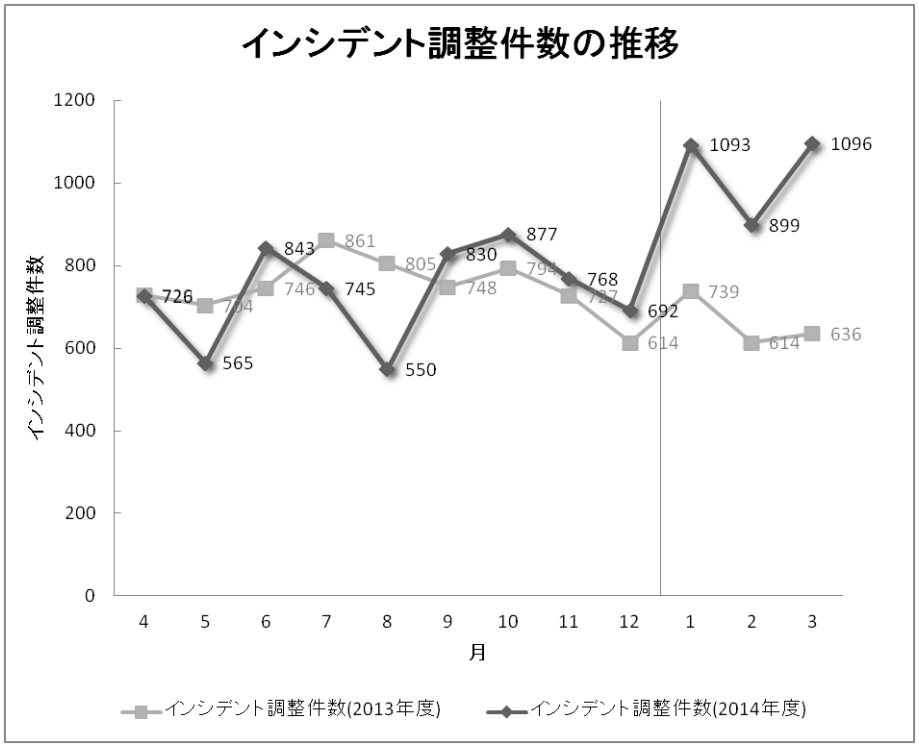
【注 4】「調整件数」は、インシデントの拡大防止のため、サイトの管理者等に対し、現状の調査と問題解決のための対応を依頼した件数を示します。

本四半期に寄せられた報告件数は、6869 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 3088 件でした。前四半期と比較して、総報告件数は 10%増加し、調整件数は 32%増加しました。また、前年同期と比較すると、総報告数で 40%増加し、調整件数は 55%増加しました。

[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]

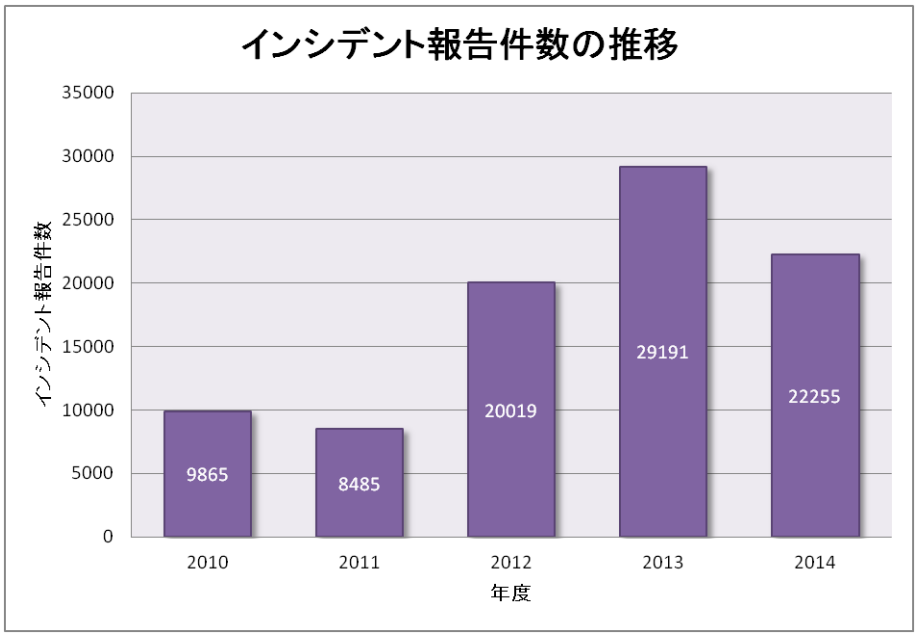
【参考】統計情報の年度比較

2014 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	2010	2011	2012	2013	2014
報告件数	9865	8485	20019	29191	22255

2014 年度に寄せられた報告件数は 22255 件でした。前年度の 29191 件と比較して、24%減少しています。[図 **3**]に過去 5 年間の年間報告件数の推移を示します。



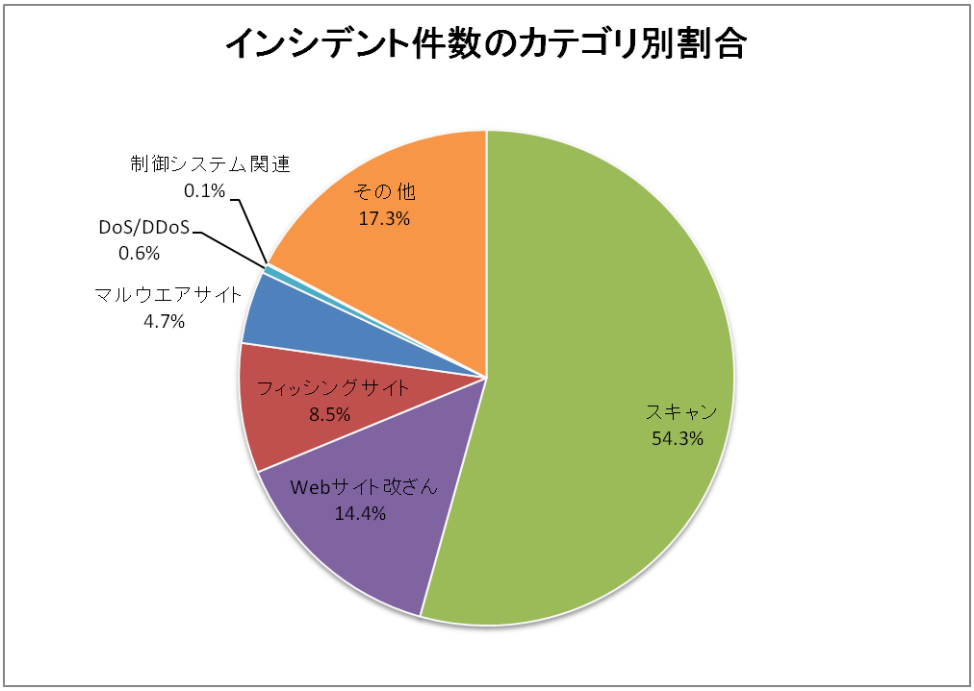
[図 3 インシデント報告件数の推移（年度比較）]

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]

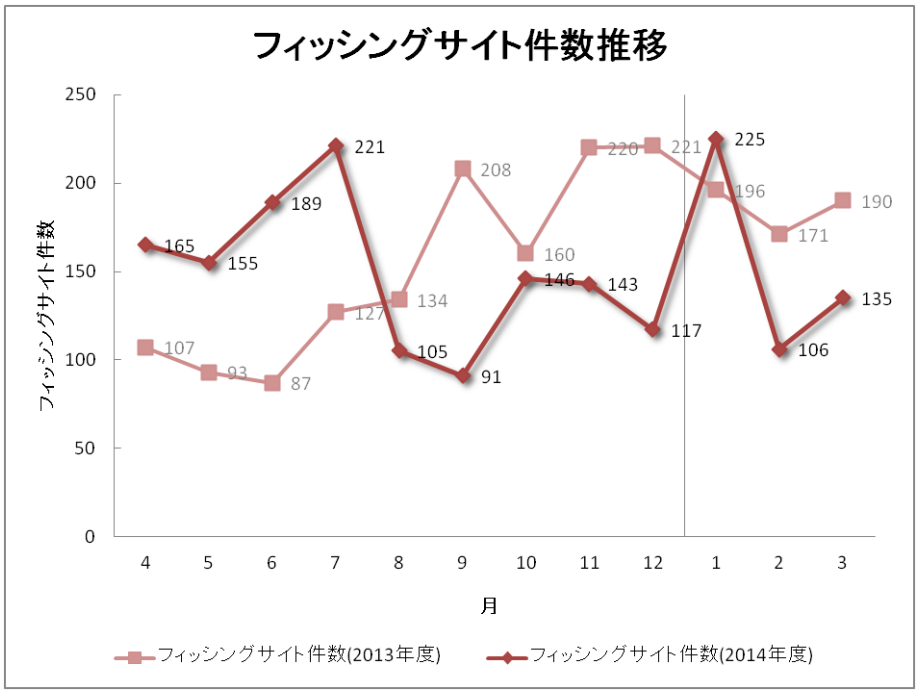
インシデントカテゴリ	1 月	2 月	3 月	合計	前四半期合計
フィッシングサイト	225	106	135	466	406
Web サイト改ざん	247	256	289	792	781
マルウエアサイト	74	84	102	260	312
スキャン	1252	885	843	2980	3592
DoS/DDoS	23	1	8	32	14
制御システム関連	0	4	1	5	3
その他	306	359	285	950	498

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 54.3%、Web サイト改ざんに分類されるインシデントは 14.4%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 8.5%でした。

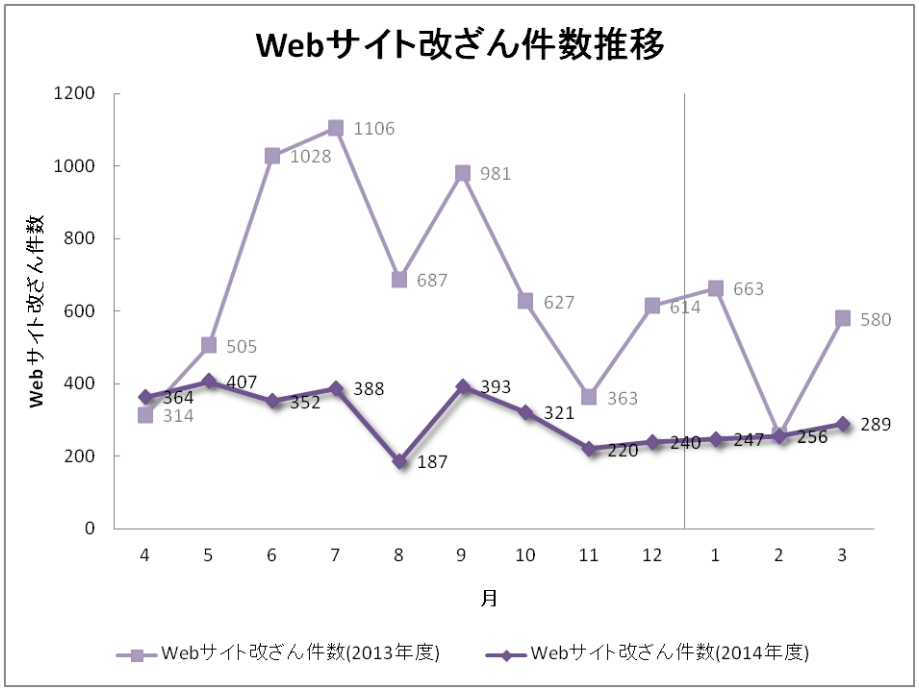


[図 4 インシデントのカテゴリ別割合]

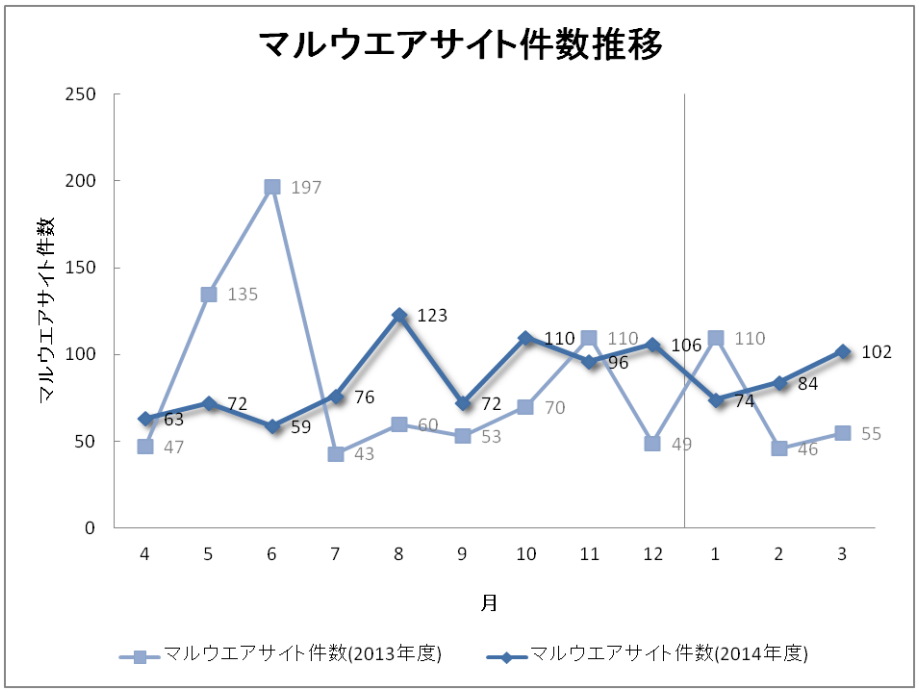
[図 5]から[図 8]に、フィッシングサイト、Web サイト改ざん、マルウエアサイト、スキャンのインシデントの過去 1 年間の月別推移を示します。



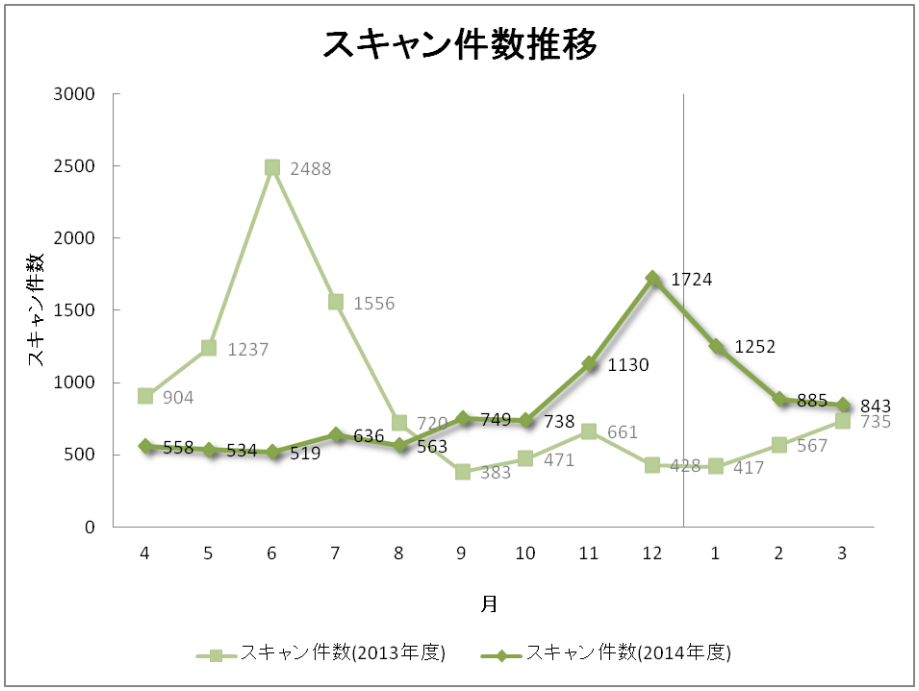
[図 5 フィッシングサイト件数推移]



[図 6 Web サイト改ざん件数推移]

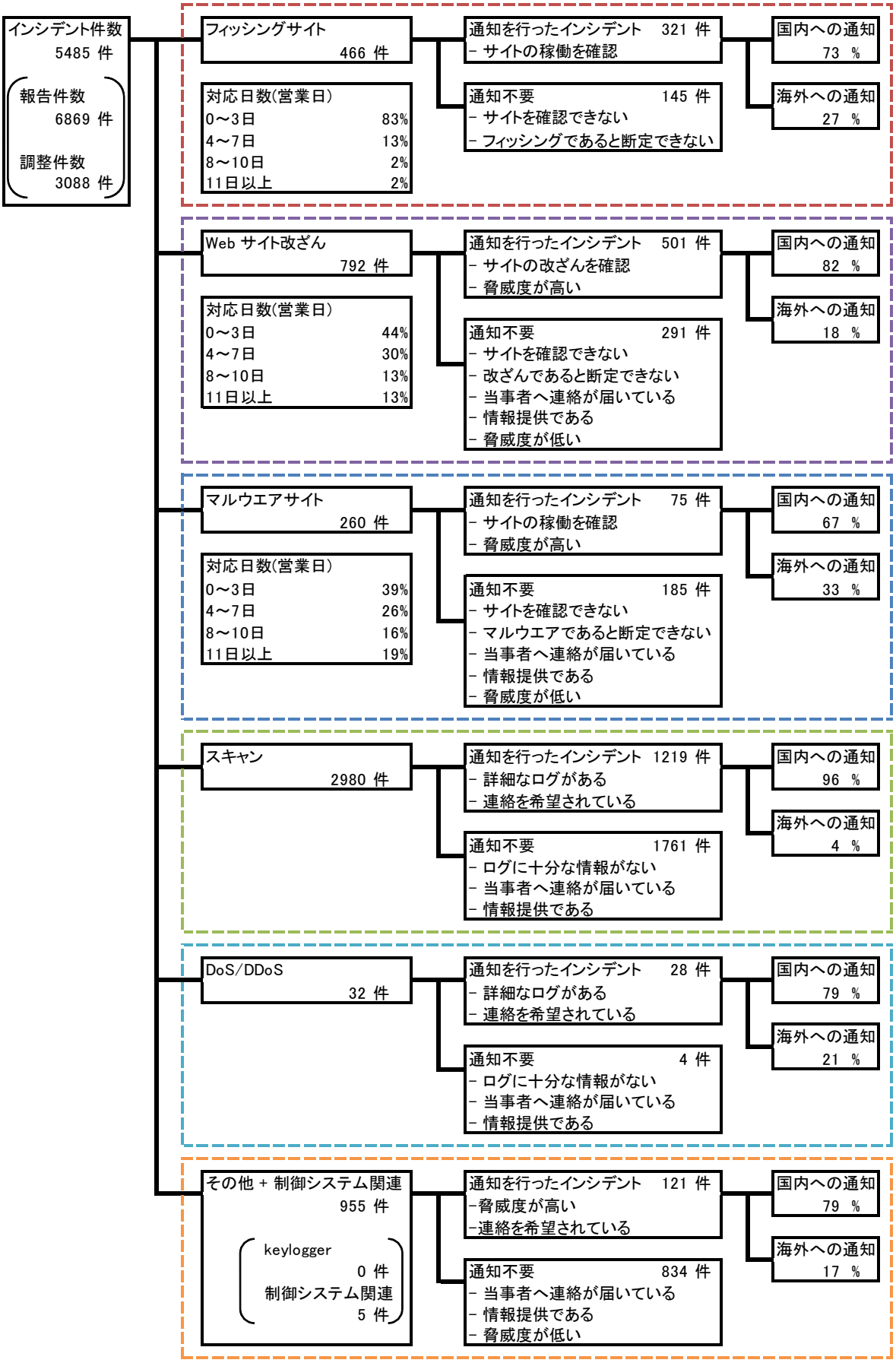


[図 7 マルウエアサイト件数推移]



[図 8 スキャン件数推移]

[図 9]に内訳を含むインシデントにおける調整・対応状況を示します。



[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

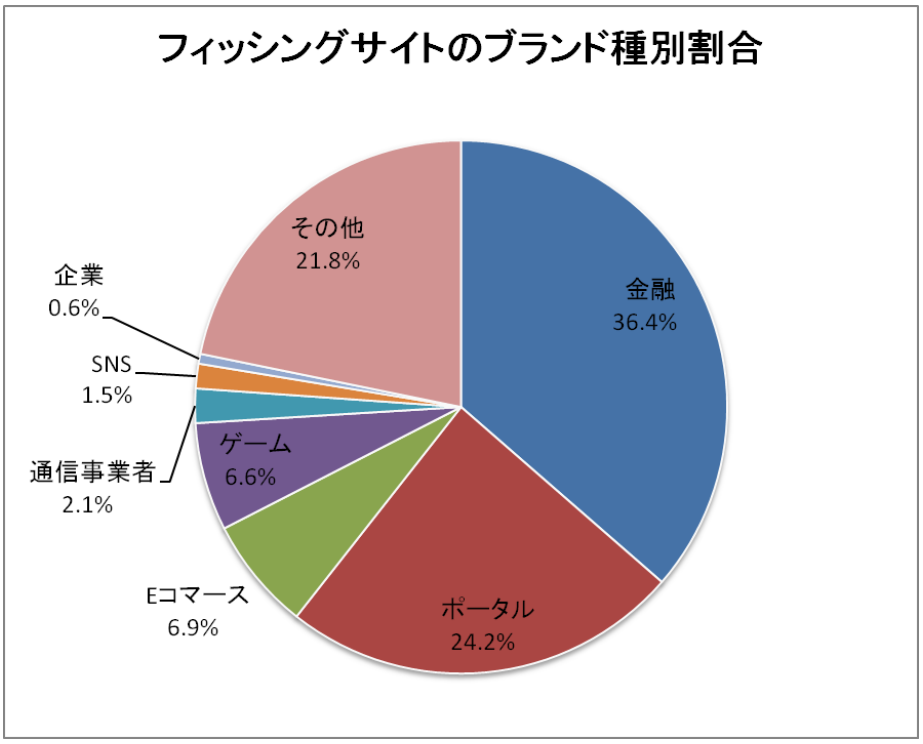
3.1. フィッシングサイトの傾向

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 466 件で、前四半期の 406 件から 15%増加しました。また、前年度同期(557 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]、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	22	18	14	54(12%)
国外ブランド	136	52	93	281(60%)
ブランド不明(注 5)	67	36	28	131(28%)
月別合計	225	106	135	466(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 54 件と、前四半期の 75 件から 28%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 281 件と、前四半期の 236 件から 19%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全体では、金融機関のサイトを装ったものが 36.4 %、ポータルサイトを装ったものが 24.2%を占めています。装われたブランドは、国内ブランドではゲーム、海外ブランドでは金融機関が最も多数を占めました。

前四半期の 11 月から確認されていなかった国内金融機関を装ったフィッシングサイトが、1 月の後半に短期間ながら確認されました。最初に確認した時点でのフィッシングサイトの IP アドレスは、以前にも使用されていた国内 ISP のネットワークのものでしたが、その後複数回にわたり別の国内 ISP のものに変化し、最終的に香港の IP アドレスになった後でサイトが停止しました。複数の国内 ISP の IP アドレスに切り替わったことから、フィッシングサイトとして使用されたホストは、攻撃者の管理下にあるボットまたはプロキシであると考えられます。

また、前四半期に引き続き、国内オンラインゲームサービスを装ったフィッシングサイトについての報告が継続的に寄せられています。オンラインゲームサービスを装ったフィッシングサイトでは、ランダムに付与されたと考えられるアルファベット 5 文字の.com ドメインの URL が大量に確認されていますが、ドメインが異なるサイトでも IP アドレスは共通しており、ホストとしては単一であると見られます。また、複数の異なるゲームのフィッシングサイトが同一の IP アドレスを使用していた例も確認しており、同一の攻撃者が複数ブランドのフィッシングを行っている可能性があります。

フィッシングサイトの調整先の割合は、国内が 73%、国外が 27%であり、前四半期(国内 70%、国外 30%)に比べ、国内への調整が増加しています。

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、792 件でした。前四半期の 781 件から 1%増加しています。

本四半期は、Web の検索エンジンでブランド製品の名称などを検索すると、検索結果に大量の不審なショッピングサイトが表示されるという報告を複数受領しました。これらの Web サイトは、検索結果の表示では日本語のショッピングサイトのように見えますが、Web サイトのトップディレクトリにアクセスするとショッピングサイトとは無関係な Web サイトであり、外部から不正にコンテンツを設置された可能性があります。

それらの Web サイトには、大量のブランド製品名などの文字列や難読化された JavaScript が埋め込まれており、JavaScript の難読化を解除すると、不審なショッピングサイトを参照する iframe や、アクセス解析に使用する JavaScript を確認できました。このような改ざんの目的は、検索結果を不正に操作することにあると推測されます。

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、260 件でした。前四半期の 312 件から 17%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、2980 件でした。前四半期の 3592 件から 17%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、DNS(53/UDP)、HTTP(80/TCP)、SMTP(25/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
53/UDP	267	221	294	782
80/TCP	426	200	149	775
25/TCP	186	212	181	579
22/TCP	114	84	108	306
8080/TCP	134	46	9	189
10000/TCP	49	18	1	68
2632/UDP	23	17	12	52
31385/UDP	17	18	16	51
16358/UDP	27	15	9	51
21/TCP	7	4	35	46
61222/UDP	14	17	10	41
23/TCP	9	16	5	30
3389/TCP	4	2	3	9
445/TCP	2	5	0	7
1433/TCP	0	2	4	6
143/TCP	2	0	3	5
123/UDP	0	1	3	4
443/TCP	2	0	1	3
3306/TCP	0	1	2	3
110/TCP	1	1	1	3
その他	15	30	22	67
月別合計	1299	910	868	3077

DNS の通信の送信元として、オープンリゾルバとなっている国内ホストを非常に多く確認しています。オープンリゾルバは DDoS 攻撃に使用される可能性があるため、ホストを管理する組織やユーザに対して、サーバやルータ等の機器の設定を見直していただくよう、連絡を行っています。

その他に分類されるインシデントの件数は、950 件でした。前四半期の 498 件から 91%増加しています。本四半期に件数が大幅に増加した原因としては、ドメインに対して複数の IP アドレスを割り当て、さらに割り当てる IP アドレスを短期間で切り替えることにより、不正な目的で使用するホストの停止を難しくする fast-flux に関する報告が増加したことがあげられます。

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。

【.pw ドメインのサイトに誘導するように改ざんされた国内 Web サイトに関する対応】
3 月の前半に、複数の国内企業の Web サイトに.pw ドメインの URL に誘導する不審な iframe が埋め込まれているという報告を受領しました。.pw ドメインは、登録に利用者の住所(所在地)などによる制限が設けられておらず、個人による利用も可能なドメインです。改ざんされた Web サイトでは、HTML ファイルもしくは JavaScript ファイルに不正な iframe が埋め込まれていました。iframe の誘導先である.pw ドメインの URL にアクセスすると、さらに他のサイトに誘導され、誘導先のサイトで、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ました。攻撃に使用される脆弱性のうち、Adobe Flash Player の脆弱性(CVE-2015-0311)は、2015 年 1 月末に修正されたものでした。

JPCERT/CC は、改ざんされた Web サイトの管理者に調査・対応を行うよう依頼しました。

【金融系マルウエアが使用するファイルが設置された海外サーバに関する対応】
2 月の半ばに、金融系マルウエアに感染した PC にダウンロードされるファイルが設置された、複数の海外サーバに関する情報を受領しました。この金融系マルウエアは、日本の銀行の情報を含む設定ファイルを海外のサーバから取得し、さらに、感染した PC がインターネットバンキングのサイトにアクセスすると、設定ファイルの取得先とは別の海外サーバから JavaScript を取得して Web フォームを生成し、フォームに入力された情報を窃取することを確認しています。

JPCERT/CC は、設定ファイルおよび JavaScript が設置されていたサーバを管理する海外のホスティング事業者に連絡し、適切な措置を行うよう依頼しました。結果として、通知先の事業者から対応を行ったとの連絡を受け、実際にファイルが削除されたことを確認しました。

【外部からアクセス可能な状態になっているサーバアプリケーションに関する対応】
データベースアプリケーション MongoDB のアクセスコントロールを適切に行っておらず、外部から情報の閲覧や操作が可能な状態になっているサーバが大量に存在しているという情報を 2 月の半ばごろドイツの学術系組織が公開しました。同時期にドイツの学術系 CSIRT より、MongoDB などのサーバアプリケーションへのアクセスを制限していない日本国内のホストのリストを受領しました。

JPCERT/CC は、リストに記載されていたホストを管理するホスティング事業者に連絡し、ユーザに設定が意図したものであるか確認するよう依頼しました。

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 Web ページをご参照ください。

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 Web ページ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、次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、上記以外のインシデントを指します。

JPCERT/CC が「その他」に分類しているものの例を次に掲げます。

- 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２６年度サイバー攻撃等国際連携対応調整事業」として実施したものです。