JPCERT/CC®

Japan Computer Emergency Response Team Coordination Center

JPCERT-IR-2015-01
発行日: 2015-01-14

JPCERT/CC インシデント報告対応レポート
[2014 年 10 月 1 日 ～ 2014 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、2014 年 10 月 1 日から 2014 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]

	10 月	11 月	12 月	合計	前四半期合計
報告件数 (注 2)	1607	1957	2667	6231	4638
インシデント件数 (注 3)	1495	1707	2404	5606	4388
調整件数 (注 4)	877	768	692	2337	2125

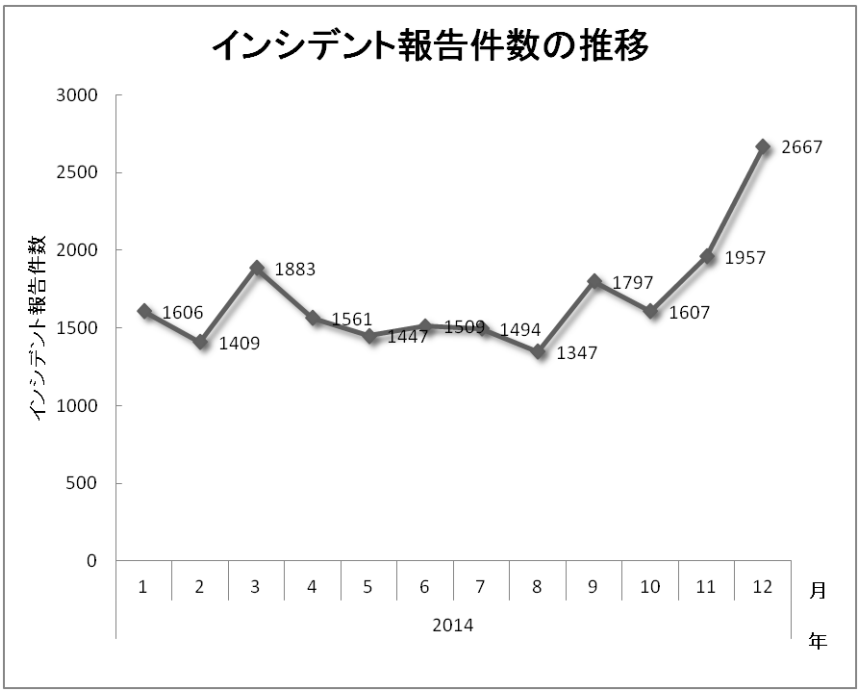
【注 2】「報告件数」は、報告者から寄せられた Web フォーム、メール、FAX による報告の総数を示します。

【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。

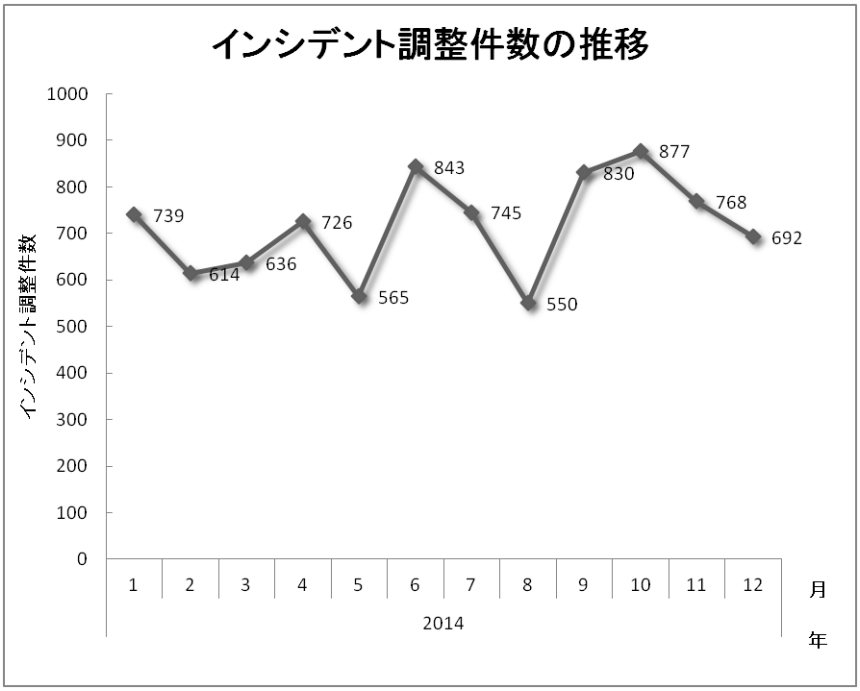
【注 4】「調整件数」は、インシデントの拡大防止のため、サイトの管理者等に対し、現状の調査と問題解決のための対応を依頼した件数を示します。

本四半期に寄せられた報告件数は、6231 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 2337 件でした。前四半期と比較して、総報告件数は 34%増加し、調整件数は 10%増加しました。また、前年同期と比較すると、総報告数で 29%増加し、調整件数は 9%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]



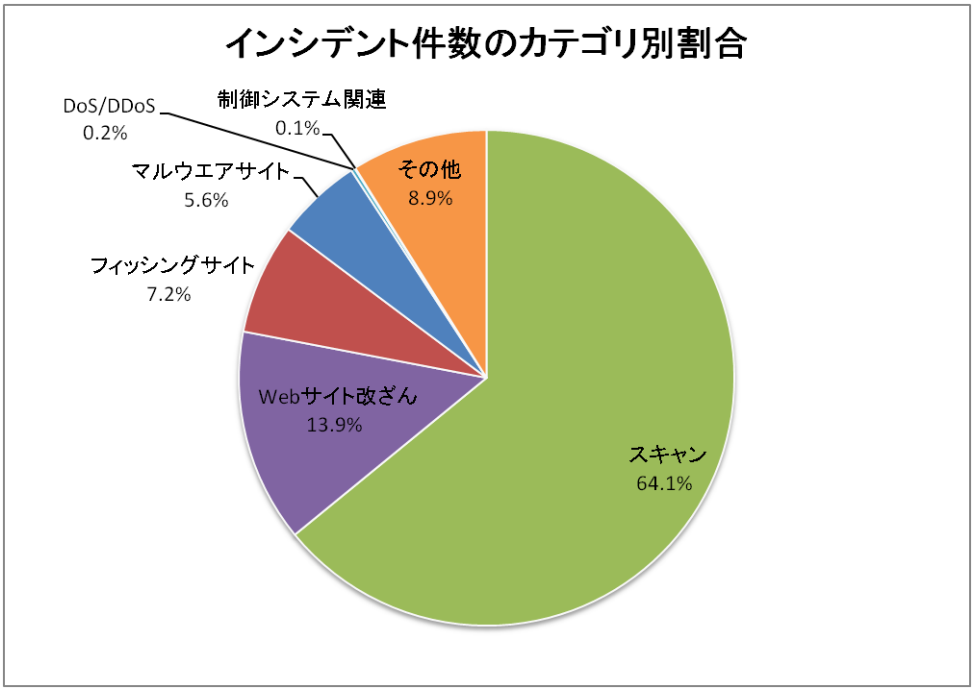
[図 2 インシデント調整件数の推移]

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 2]に示します。

[表 2 カテゴリ別インシデント件数]

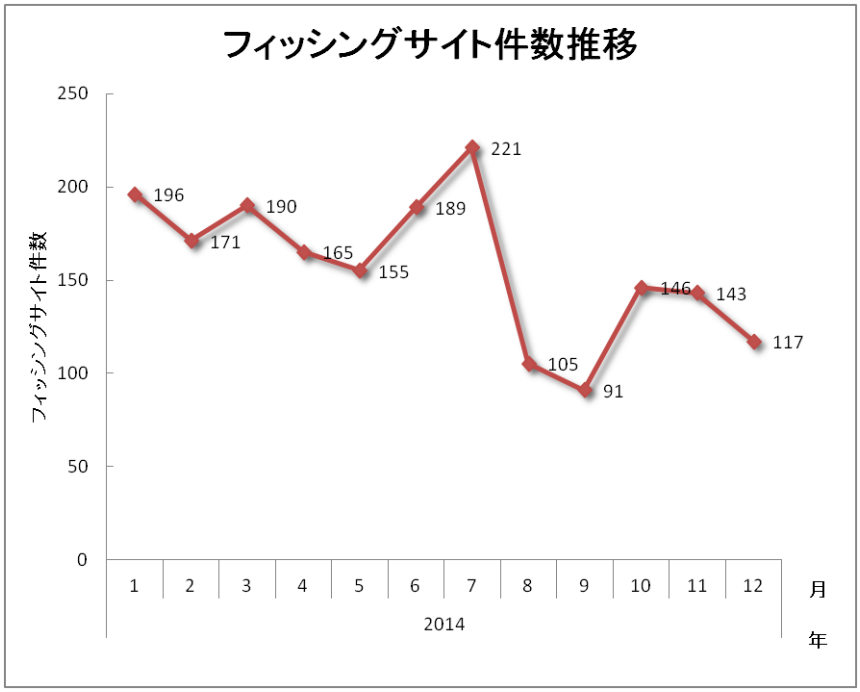
インシデントカテゴリ	10 月	11 月	12 月	合計	前四半期合計
フィッシングサイト	146	143	117	406	417
Web サイト改ざん	321	220	240	781	968
マルウエアサイト	110	96	106	312	271
スキャン	738	1130	1724	3592	1948
DoS/DDoS	1	0	13	14	18
制御システム関連	0	3	0	3	6
その他	179	115	204	498	760

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 64.1%、Web サイト改ざんに分類されるインシデントは 13.9%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 7.2%でした。

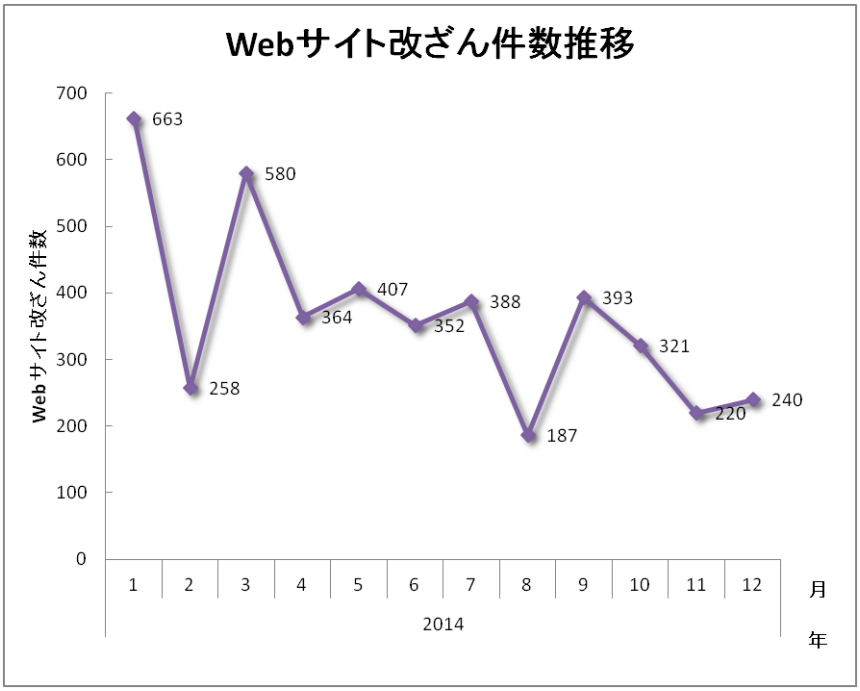


[図 3 インシデントのカテゴリ別割合]

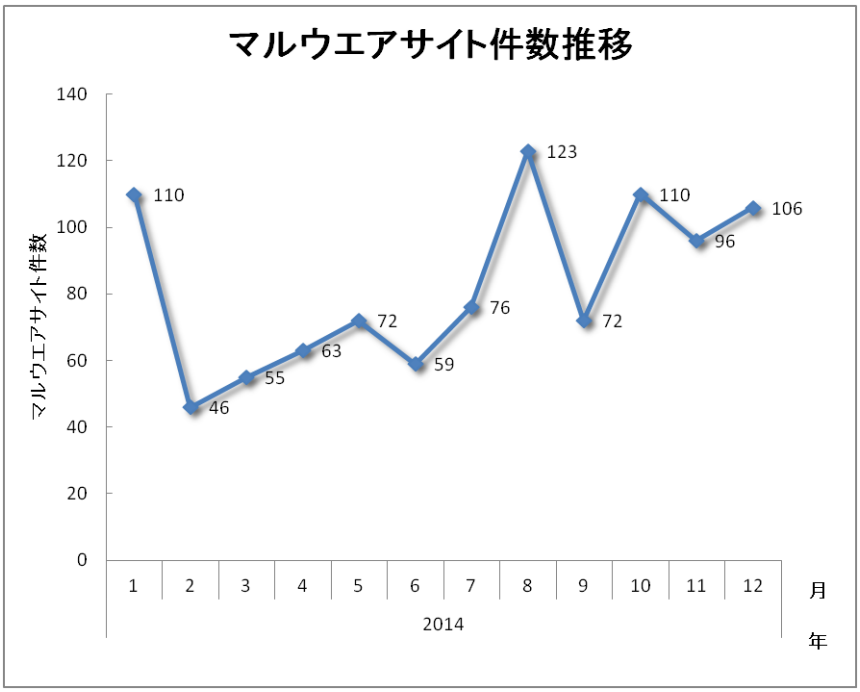
[図 4]から[図 7]に、フィッシングサイト、Web サイト改ざん、マルウエアサイト、スキャンのインシデントの過去 1 年間の月別推移を示します。



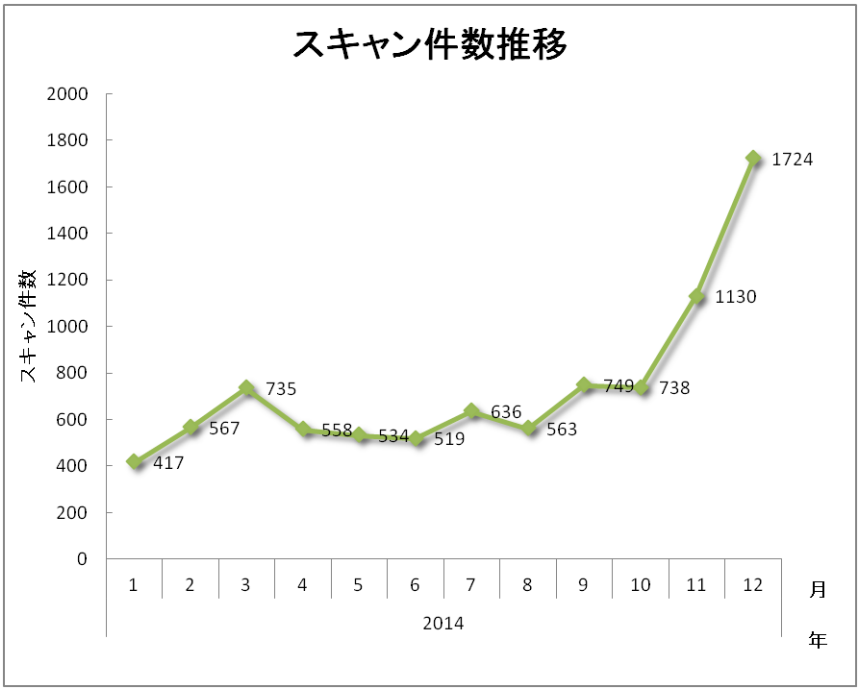
[図 4 フィッシングサイト件数推移]



[図 5 Web サイト改ざん件数推移]

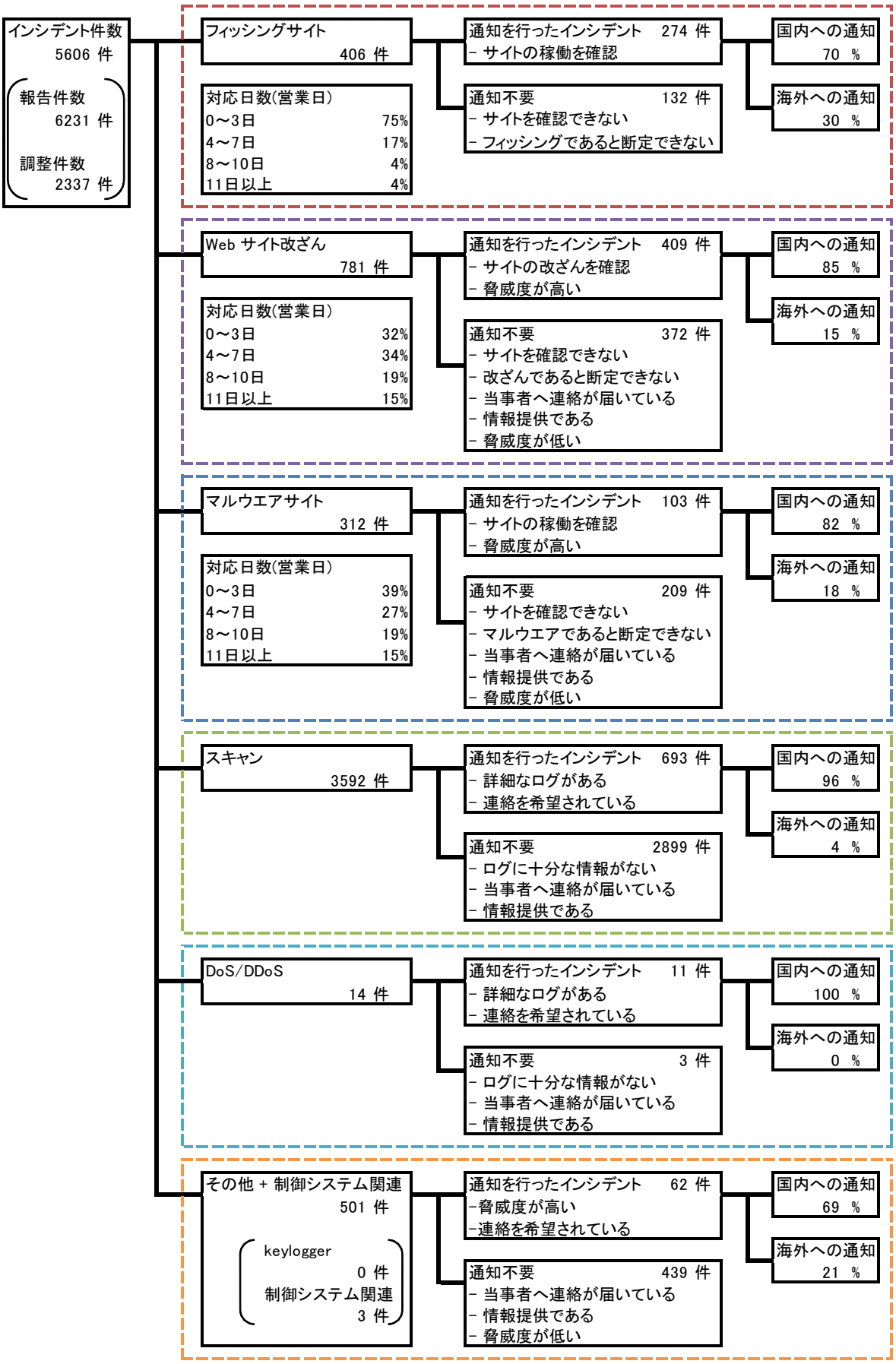


[図 6 マルウエアサイト件数推移]



[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 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

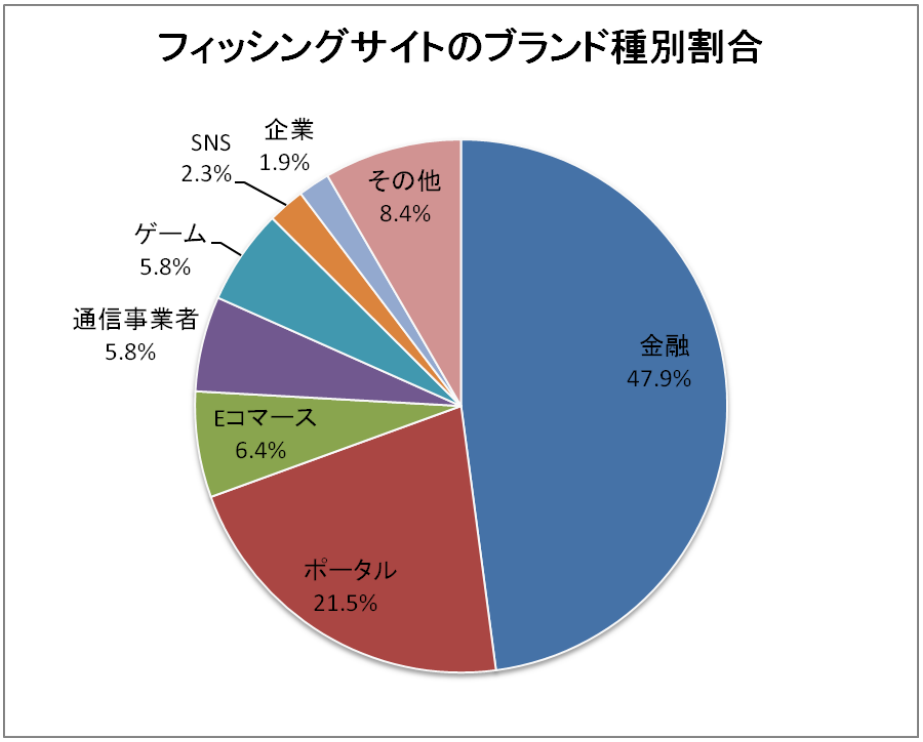
3.1. フィッシングサイトの傾向

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 406 件で、前四半期の 417 件から 3%減少しました。また、前年度同期(601 件)との比較では、32%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]、業界割合を[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	41	23	11	75(18%)
国外ブランド	78	91	67	236(58%)
ブランド不明(注 5)	27	29	39	95(23%)
月別合計	146	143	117	406(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 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 75 件と、前四半期の 139 件から 46%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 236 件と、前四半期の 189 件から 25%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 47.9 %、ポータルサイトを装ったものが 21.5%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。

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数が前四半期に比べて大幅に減少しました。これは、前四半期に非常に多く確認されていた国内金融機関を装ったフィッシングサイトが、10 月には減少し、11 月以降には確認されなかったことが原因となっています。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の数も前四半期に比べて減少していますが、10 月末以降、継続的に報告が寄せられています。

フィッシングサイトの調整先の割合は、国内が 70%、国外が 30%であり、前四半期(国内 58%、国外 42%)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、781 件でした。前四半期の 968 件から 19%減少しています。

Web サイトが改ざんされていて、そこから誘導される先のページに埋め込まれている Microsoft の脆弱性(MS14-064)を悪用するコードによって、マルウエアに感染させられる事例を 11 月後半から 12 月半ばに複数確認しました。

この脆弱性は 11 月のセキュリティアップデートで公表され、限定的な範囲で標的型攻撃に使用されていたとされたものです。前述の事例では、攻撃者が、11 月の公表から非常に短期間のうちに、修正プログラムを分析して脆弱性の情報を入手し、それを悪用するコードを開発して Web サイトに組み込んだものと推測されます。この事例からも、セキュリティアップデートの公開後は、攻撃の被害を防ぐために、できる限り早く適用することが推奨されます。

また、12 月初めごろから、難読化された JavaScript がページの末尾に埋め込まれた改ざんで、tag[数字 1,2 文字].php のような URL の不審なサイトに誘導するものを多数確認しています。その他にも、難読化された JavaScript と外部サイトのリンクが埋め込まれた改ざんで、Web の検索結果で特定のサイトを上位に表示させるための SEO ポイズニングを目的としたと見られるものや、薬の販売や宣伝を目的としたとみられるサイトへの転送設定のみが記述されたページなどが不正に設置される事例を多数確認しています。

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、312 件でした。前四半期の 271 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、3592 件でした。前四半期の 1948 件から 84%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。頻繁にスキャンの対象となったポートは、http(80/tcp)、smtp(25/tcp)、dns(53/udp)でした。

本四半期は、GNU bash の脆弱性を使用した攻撃の被害や、攻撃元になっていた国内 IP アドレスに関する報告が複数寄せられました。また、12 月には、NAS(ネットワーク接続ストレージ)が攻撃元になっている、8080/tcp を対象としたスキャンに関する報告が多く寄せられました。

[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	185	531	948	1664
25/tcp	129	172	234	535
53/udp	147	182	126	455
22/tcp	97	105	245	447
21/tcp	8	37	47	92
31385/udp	30	23	19	72
2632/udp	38	13	19	70
8080/tcp	4	3	54	61
61222/udp	17	17	25	59
16358/udp	24	12	20	56
10000/tcp	32	0	1	33
53/tcp	2	8	0	10
23/tcp	0	3	5	8
445/tcp	5	2	0	7
3389/tcp	2	4	0	6
1451/tcp	6	0	0	6
143/tcp	3	3	0	6
123/udp	0	6	0	6
80/udp	0	4	0	4
3544/udp	1	1	1	3
22/udp	2	0	0	2
その他	13	18	2	33
月別合計	745	1144	1746	3635

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。

【国内 Web サイトのドメイン名ハイジャックに関する対応】
ある国内企業の Web サイトが読み込むよう指定している JavaScript に不正なコードが埋め込まれていて、外部のサイトに誘導しているという情報を 10 月初めごろ海外のセキュリティ企業が公開しました。JPCERT/CC は、当該国内企業に事実関係の確認を依頼するとともに、海外セキュリティ企業に詳細な情報の提供を依頼しました。

その結果、海外セキュリティ企業から、過去の一定の期間に、当該国内企業のドメイン名に正規のものとは異なる IP アドレスが割り当てられていた可能性があるとの情報を受領しました。弊センターにて当該ドメイン名の登録情報と過去の名前解決の記録を調査したところ、不審なネームサーバが当該ドメイン名のネームサーバとして登録されていた期間が存在し、その期間には当該ドメイン名が正規のものとは異なる IP アドレスに名前解決されていたことが分かりました。

当該国内企業による調査においても、同サイト内の JavaScript が改ざんされた事実を確認できず、ドメイン名がハイジャックされて、不正な JavaScript が設置されたホストへの誘導が行われていた可能性が高いことが分かりました。

さらに調査した結果、同様の事象が複数の国内組織のドメイン名において発生していたことが判明したため、JPCERT/CC は該当する複数の組織に、ドメイン登録情報が不正に変更されていた可能性について、レジストラに調査を依頼するよう連絡しました。また、影響の深刻さを考慮し、注意喚起を 11 月 5 日に発行しました。

【国内組織のデータベース情報がアップロードされた文書共有サイトに関する対応】
国内複数組織のデータベースから脆弱な Web サイトを通じて流出したと見られる情報が、海外のテキスト共有サイト上で公開されているという報告を 11 月後半に受領しました。テキスト共有サイトの管理者に、国内組織から流出した可能性がある情報が公開されている旨を連絡したところ、不正なコンテンツについて通報があれば、削除するとの返信をいただきました。

JPCERT/CC は、データベース情報が流出した可能性がある国内組織に事実関係の確認を依頼し、削除が必要な場合、テキスト共有サイトの管理者に連絡するよう案内しました。また、希望した組織については、テキスト共有サイトの管理者への連絡を代行しました。

【12 月前半に発生した SSH ブルートフォース攻撃に関する対応】
12 月前半ごろ、「日本国内の IP アドレスから SSH ブルートフォース攻撃を受けた」という海外からの報告が多数寄せられました。報告元から提供されたログを JPCERT/CC が確認したところ、複数の攻撃で特定のユーザアカウントがログイン試行されているという共通性が見られました。また、同じ時期に、

国内および海外の数百の IP アドレスから、SSH のスキャンを受けたという報告が国内からも寄せられました。

JPCERT/CC は、報告元から提供されたスキャンのログをもとに、攻撃元の一部について、各 IP アドレスを管理する組織に事実関係の確認を依頼しました。その結果、GNU bash の脆弱性によってサーバに不正なファイルが設置され、SSH スキャンを行っていると見られる不正なプロセスが確認されたとの報告をいただいた組織があり、今年 9 月下旬に公表された同脆弱性の影響の一端であることが推測されました。

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、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。