JPCERT-IR-2015-05
発行日: 2016-01-14

JPCERT/CC インシデント報告対応レポート
[2015 年 10 月 1 日 ～ 2015 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、2015 年 10 月 1 日から 2015 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)	1061	1201	1178	3440	4128
インシデント件数 (注 3)	1029	1137	1003	3169	3748
調整件数 (注 4)	626	684	743	2053	2058

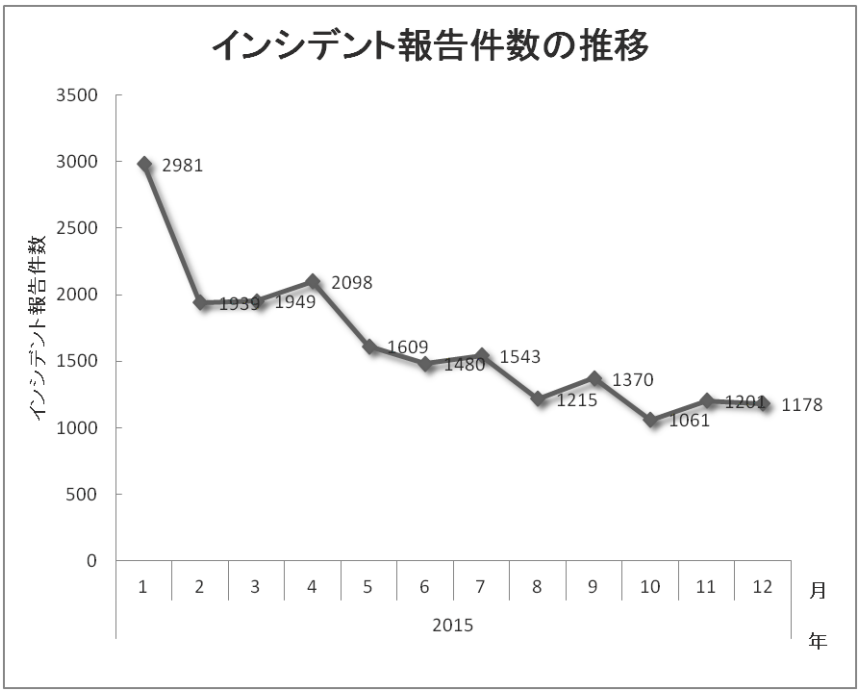
【注 2】「報告件数」は、報告者から寄せられた Web フォーム、メール、FAX による報告の総数を示します。

【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。

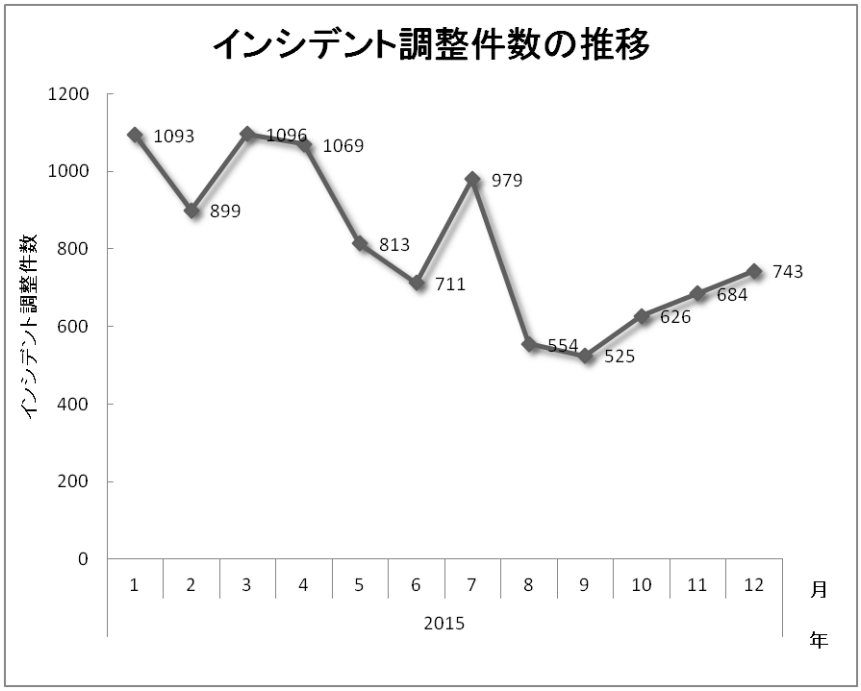
【注 4】「調整件数」は、インシデントの拡大防止のため、サイトの管理者等に対し、現状の調査と問題解決のための対応を依頼した件数を示します。

本四半期に寄せられた報告件数は、3440 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 2053 件でした。前四半期と比較して、総報告件数は 17%減少し、調整件数は 0.3%減少しました。また、前年同期と比較すると、総報告数で 45%減少し、調整件数は 12%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]



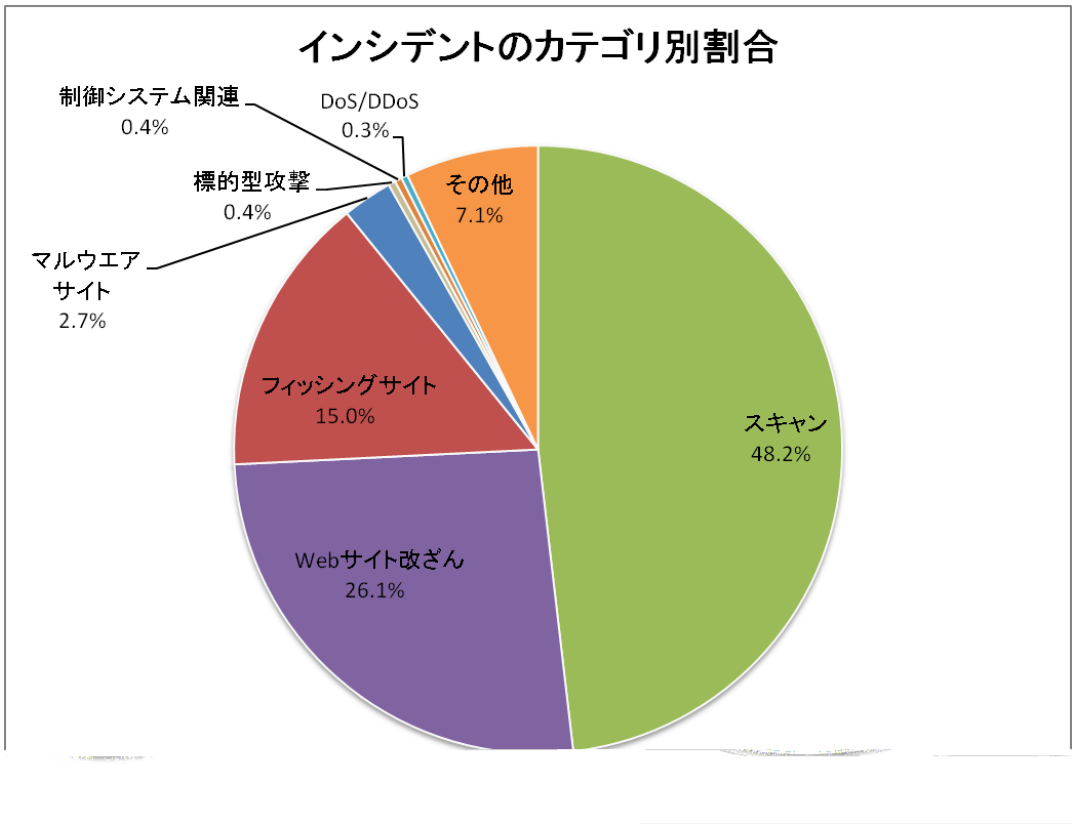
[図 2 インシデント調整件数の推移]

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]

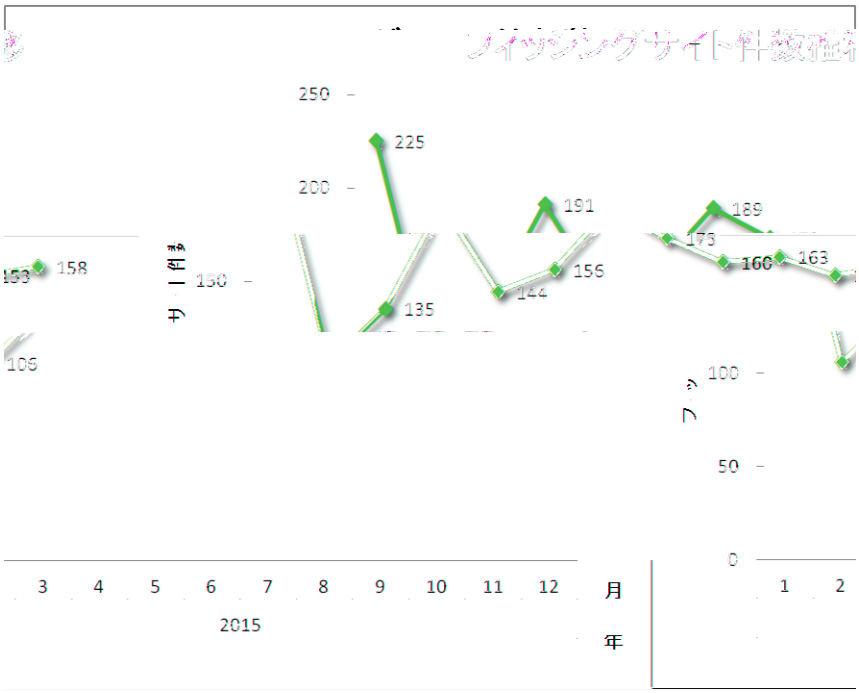
インシデント	10 月	11 月	12 月	合計	前四半期合計
フィッシングサイト	163	153	158	474	522
Web サイト改ざん	273	292	261	826	592
マルウエアサイト	25	32	27	84	119
スキャン	509	580	437	1526	1985
DoS/DDoS	5	3	3	11	21
制御システム関連	0	4	8	12	0
標的型攻撃	4	4	4	12	59
その他	50	69	105	224	450

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 48.2%、Web サイト改ざんに分類されるインシデントは 26.1%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 15.0%でした。

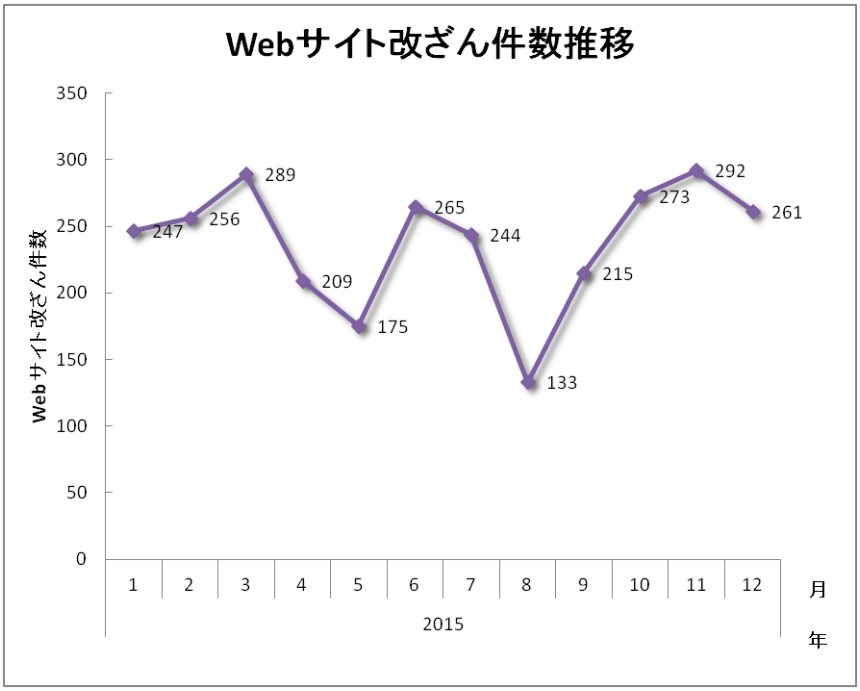


[図 3 インシデントのカテゴリ別割合]

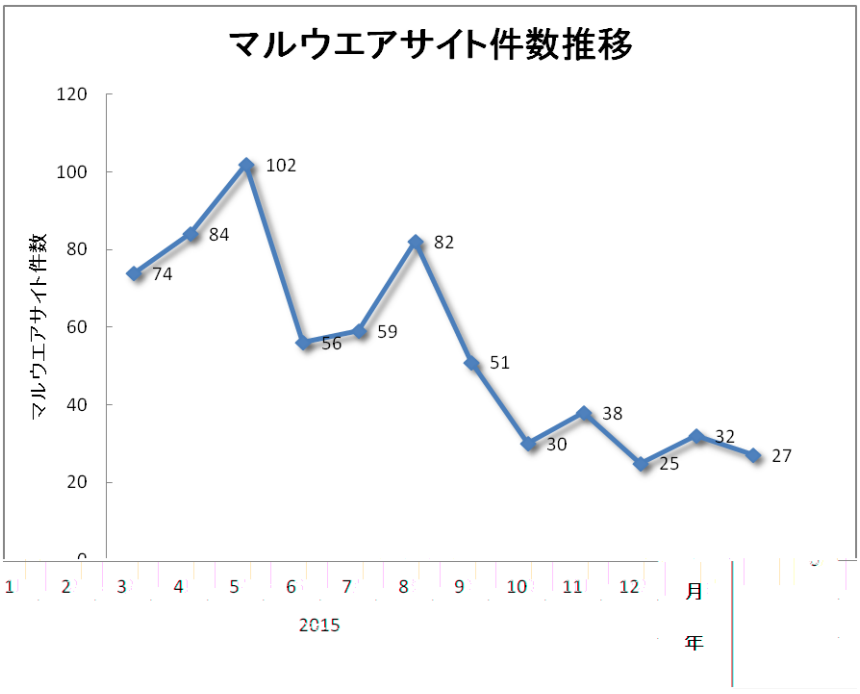
[図 4]から[図 7]に、フィッシングサイト、Web サイト改ざん、マルウエアサイト、スキャンのインシデントの過去 1 年間の月別推移を示します。



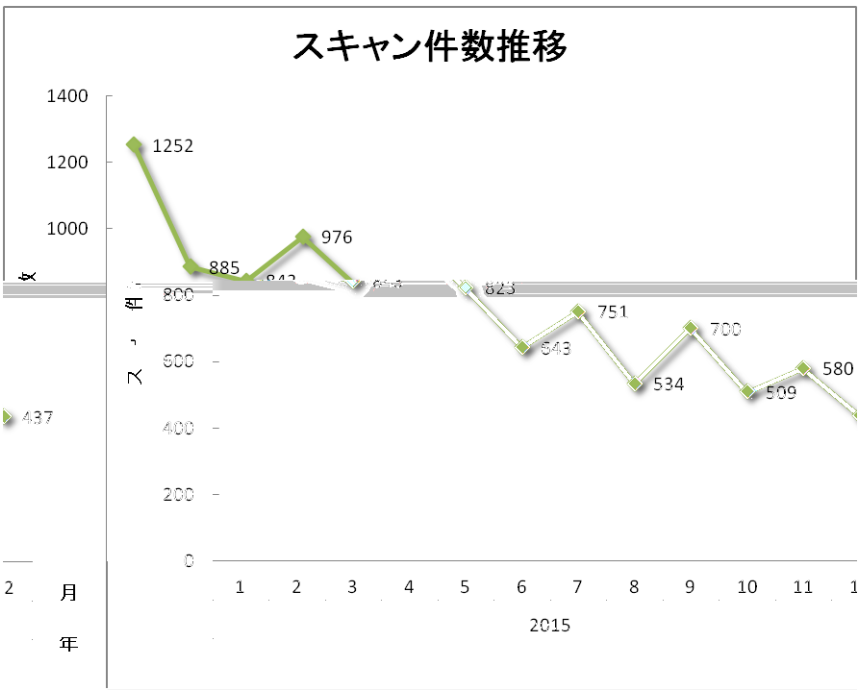
[図 4 フィッシングサイト件数推移]



[図 5 Web サイト改ざん件数推移]

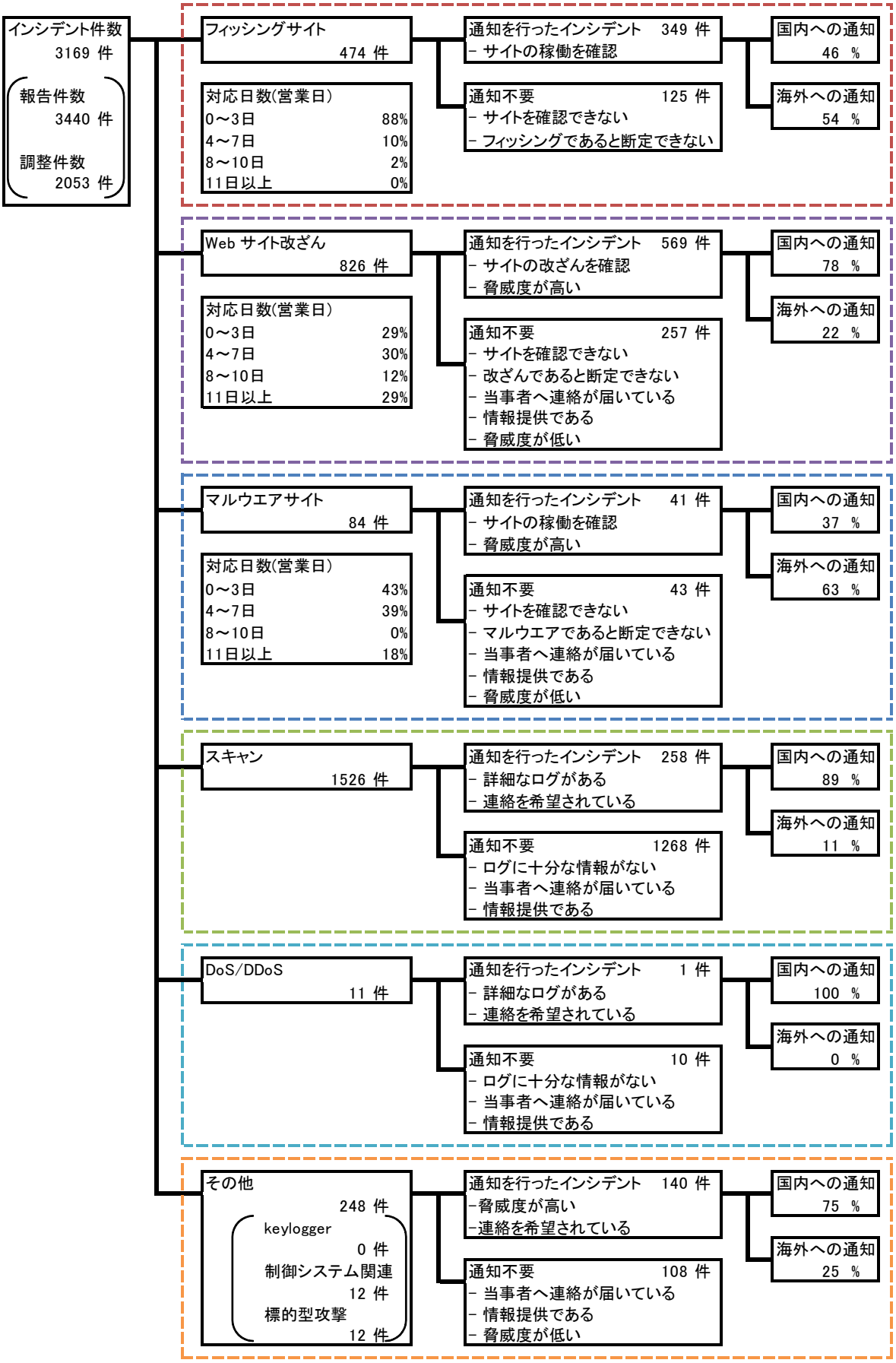


[図 6 マルウエアサイト件数推移]



[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

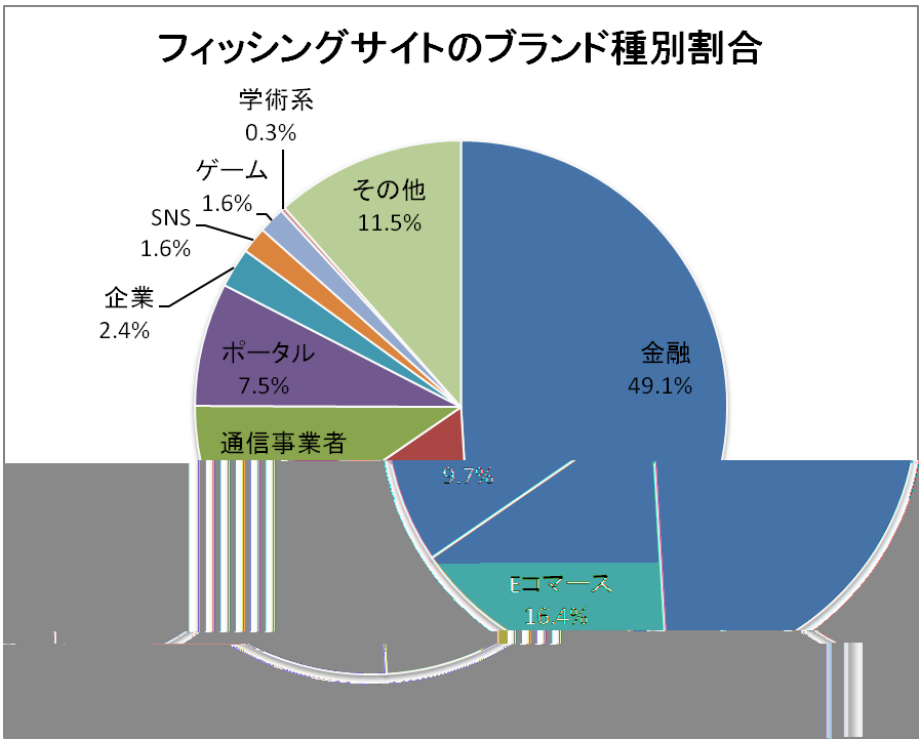
3.1. フィッシングサイトの傾向

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 474 件で、前四半期の 522 件から 9%減少しました。また、前年度同期(406 件)との比較では、17%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 3]、業界別の内訳を[図 9]に示します。

[表 3 報告されたフィッシングサイト件数の国内・国外ブランド別内訳]

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	30	35	59	124(26%)
国外ブランド	93	88	69	250(53%)
ブランド不明 (注 5)	40	30	30	100(21%)
月別合計	163	153	158	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 報告されたフィッシングサイトのブランド種別内訳]

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 124 件となり、前四半期の 113 件から 10%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 250 件となり、前四半期の 268 件から 7%減少しました。

JPCERT/CC が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 49.1%、E コマースサイトを装ったものが 16.4%で、装われたブランド別内訳では、国内、海外ブランドともに金融機関が最も多数を占めました。

国内金融機関を装ったフィッシングでは、異なるブランドを装っていてもドメインや IP アドレスに共通点が見られるものがあり、特定の攻撃者グループが複数のブランドを標的としてフィッシングを行っている可能性が考えられます。10 月から継続的に確認されている複数ブランドのフィッシングは、TLD が.com であり、香港のホスティングサービスが多く使用されていました。また、11 月末以降に確認された別の複数ブランドのフィッシングでは、韓国やアメリカのホスティングサービスが多く使用され、URL には.help、.ren、.link などの gTLD 配下で、正規サイトを装ったサブドメインを取得して使用されていました。

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も多く寄せられており、フィッシングサイトの多くは侵入されたと見られる海外の Web サイト上に設置されていました。一方で、本四半期の国内オンラインゲームを装ったフィッシングサイトは、10 月の後半と 12 月の半ばに確認されたのみで、非常に少数でした。

フィッシングサイトの調整先の割合は、国内が 46%、国外が 54%であり、前四半期(国内 48%、国外 52%)に比べ、海外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、826 件でした。前四半期の 592 件から 40%増加しています。

本四半期は、改ざんされた Web サイトにアクセスした際に、セキュリティ製品がランサムウエアのダウンロードを検知したという報告が複数寄せられました。body タグの直後やページの最上部に難読化されたコードが埋め込まれた Web サイトの改ざんが特に多く、WordPress、Joomla、Drupal などの CMS を使用して構築されたサイトが改ざんされている傾向が見られました。改ざんされたサイトにアクセスすると、不正なコードによって攻撃サイトに誘導され、Adobe Flash Player や Internet Explorer などの脆弱性を悪用した攻撃によって、マルウエアのダウンロード、実行が行われることを確認しています。

改ざんされた Web サイトの管理者からサイトのコンテンツを提供していただき調査したところ、CMS のデフォルトのファイルに//istart や//iend などの文字列を含む不正なコードが埋め込まれていました。改ざんされた原因としては、CMS および CMS のテーマ、プラグインの脆弱性を悪用する攻撃や、管理用のパスワードの窃取などが考えられます。

3.3.標的型攻撃の傾向

標的型攻撃に分類されるインシデントの件数は、12 件でした。前四半期の 59 件から 80%減少しています。本四半期には、11 組織（延べ数）に対して連絡を行いました。

標的型攻撃が本年度の前半には非常に多く確認されましたが、本四半期はわずかが確認されたのみでした。攻撃者の活動が停止している可能性もありますが、攻撃されている組織が気づいていない可能性も考えられます。警戒を怠ることなく、標的型攻撃に備えて十分に対策ができているか、次の点を中心とした点検を推奨します。

- PC がマルウエアに感染し、攻撃者の侵入を招くことを防ぐために、PC の OS、アプリケーションを常に最新の状態にアップデートしているか。
- 攻撃者がネットワークへの侵入後に Active Directory サーバの脆弱性を攻撃しても耐えられるよう、サーバのセキュリティアップデートを確実に適用しているか。
- ネットワーク内で横断的に侵害が行われることを防ぐため、Active Directory のドメインに参加している PC で管理者権限が適切に運用され、パスワードの共有や使いまわしが行われていないか。
- 文書ファイルに偽装したマルウエアを添付した、なりすましメールに対抗するため、不審な送信元からのメールをブロックし、添付ファイルの種類を制限する等しているか。

さらに、攻撃の早期発見や、原因の調査ができるように、PC およびサーバのイベントログや、プロキシ、ファイアウォール、DNS クエリなどのログが適切に取得できているかについても、ご確認ください。

3.4.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、84 件でした。前四半期の 119 件から 29%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、1526 件でした。前四半期の 1985 件から 23%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 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) 、SSH(22/TCP)でした。

[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	247	327	239	813
25/tcp	101	156	111	368
22/tcp	84	56	44	184
445/tcp	22	28	15	65
23/tcp	13	7	9	29
21/tcp	8	7	4	19
3389/tcp	3	4	9	16
1433/tcp	3	9	2	14
53/udp	0	0	9	9
61222/udp	5	3	0	8
8080/tcp	2	1	3	6
16358/udp	2	2	1	5
53/tcp	0	0	4	4
4899/tcp	3	0	1	4
31385/udp	3	1	0	4
2632/udp	2	2	0	4
5900/tcp	2	0	1	3
3306/tcp	2	1	0	3
139/tcp	1	2	0	3
6379/tcp	0	2	0	2
53413/udp	0	1	1	2
5060/udp	1	1	0	2
443/tcp	0	1	1	2
2048/udp	2	0	0	2
110/tcp	1	1	0	2
その他	21	35	9	65
月別合計	528	647	463	1638

その他に分類されるインシデントの件数は、224 件でした。前四半期の 450 件から 50%減少しています。

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。

【外部からのゾーン転送要求に応答する国内 DNS サーバに関する対応】
国内の約 1800 台のネームサーバで、本来はインターネットに公開すべきでない組織内のゾーン情報が合計約 8000 ドメインについて転送可能な状態となっているとの報告を 11 月半ばごろに海外の CSIRT から受領しました。ゾーン転送の機能は、DNS サーバ間でゾーン情報の更新を反映するために使用されますが、アクセス制御が適切に行われていない場合、隠すべき組織内ドメイン情報を意図せず第三者に取得され、攻撃のためのヒントを与える等、セキュリティの面で問題があるといわれています。

JPCERT/CC は、報告元から受領したリストをもとに、ネームサーバの管理者にゾーン転送の設定が意図したものであるか確認するよう、順次連絡を行っています。

【BGP 経路を不正に広報する海外 AS に関する対応】
自組織が管理しているグローバル IP アドレス範囲の BGP 経路情報が、海外の AS によって不正に広報されているという報告を 11 月初めごろ受領しました。BGP 経路情報を不正に広報されてグローバル IP アドレス範囲をハイジャックされたまま放置すると、スパムメールの送信などに悪用され、管理している IP アドレス範囲が不正なメール送信元のブラックリストなどに登録されてしまうおそれがあります。

JPCERT/CC は、不正に広報されていた BGP 経路情報を調査して、海外の ISP が当該グローバル IP アドレス範囲の広報を行っていることを確認し、不正に広報していた ISP および隣接する ISP に適切に対応するよう依頼しました。その結果、不正な広報をしていた ISP に隣接する ISP の管理者より、不正な BGP 経路情報を削除したとの返信を受領し、実際に BGP 経路情報が削除されたことを確認しました。本件は不正な BGP 経路情報の広報について JPCERT/CC が報告を受けた稀な事例でしたが、ある程度の頻度で類似事案が発生しており、BGP 経路情報が広報されていないグローバル IP アドレス範囲がハイジャックされる事例も多いことを確認しています。

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

○ 標的型攻撃

「標的型攻撃」とは、特定の組織、企業、業種などを標的として、マルウエア感染や情報の窃取などを試みる攻撃を指します。

JPCERT/CC では、以下を「標的型攻撃」と分類しています。

- 特定の組織に送付された、マルウエアが添付されたなりすましメール
- 閲覧する組織が限定的である Web サイトの改ざん
- 閲覧する組織が限定的である Web サイトになりすまし、マルウエアに感染させようとするサイト
- 特定の組織を標的としたマルウエアが通信を行うサーバ

○ 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２７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。