JPCERT CC®

Japan Computer Emergency Response Team Coordination Center

JPCERT-IR-2016-01

発行日: 2016-04-14

JPCERT/CC インシデント報告対応レポート
[2016 年 1 月 1 日 ～ 2016 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、2016 年 1 月 1 日から 2016 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)	1176	1405	2006	4587	3440
インシデント件数 (注 3)	994	1410	1739	4143	3169
調整件数 (注 4)	678	1013	1264	2955	2053

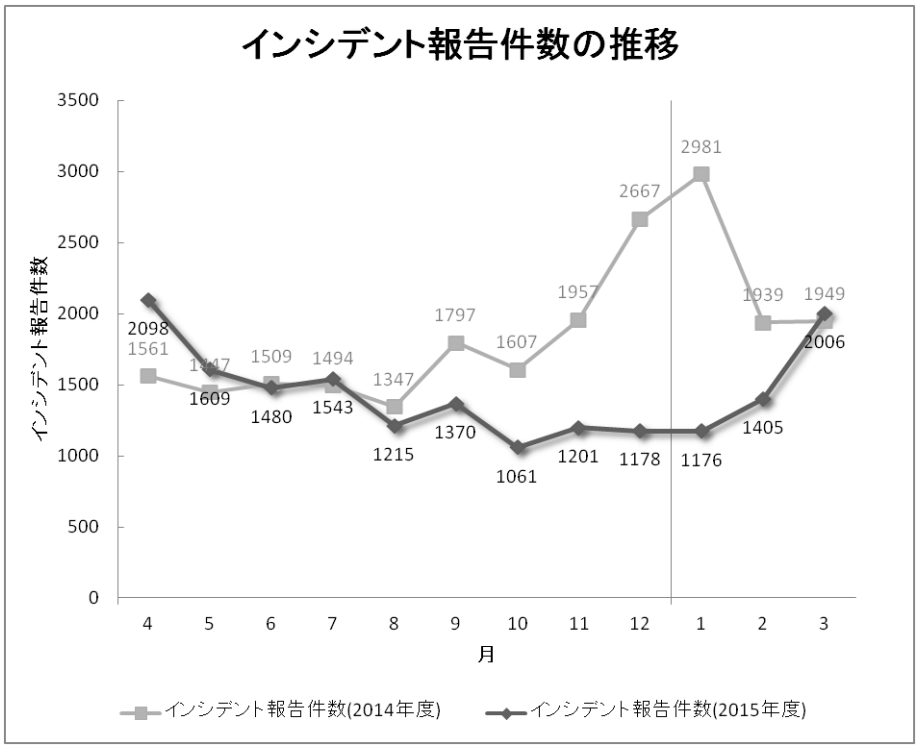
【注 2】「報告件数」は、報告者から寄せられた Web フォーム、メール、FAX による報告の総数を示します。

【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。

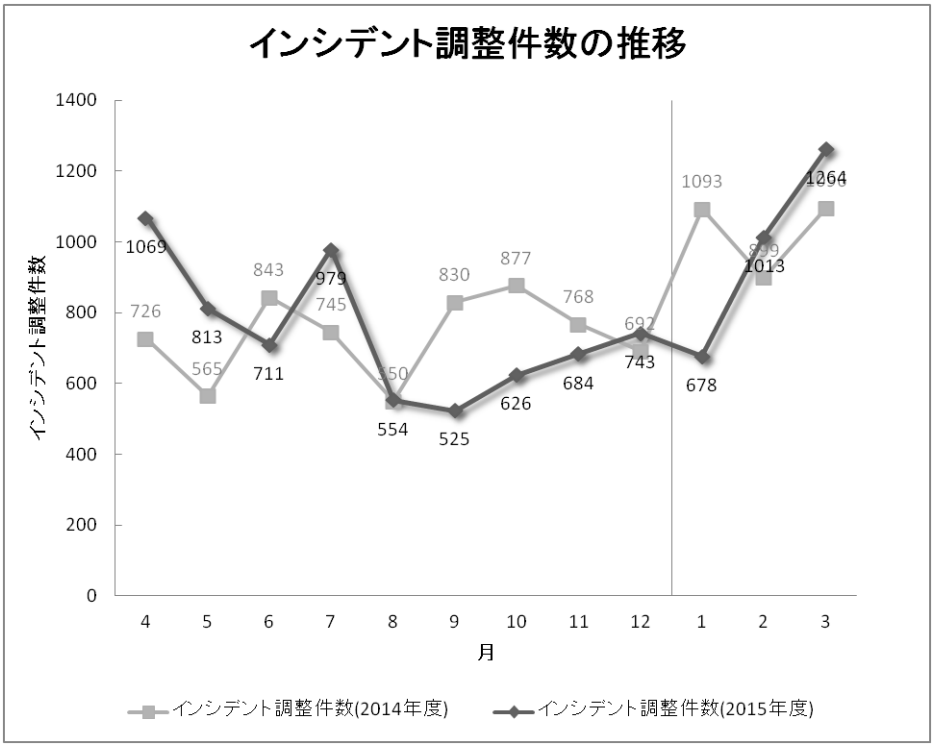
【注 4】「調整件数」は、インシデントの拡大防止のため、サイトの管理者等に対し、現状の調査と問題解決のための対応を依頼した件数を示します。

本四半期に寄せられた報告件数は、4587 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 2955 件でした。前四半期と比較して、報告件数は 33%増加し、調整件数は 44%増加しました。また、前年同期と比較すると、報告数で 33%減少し、調整件数は 4%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]

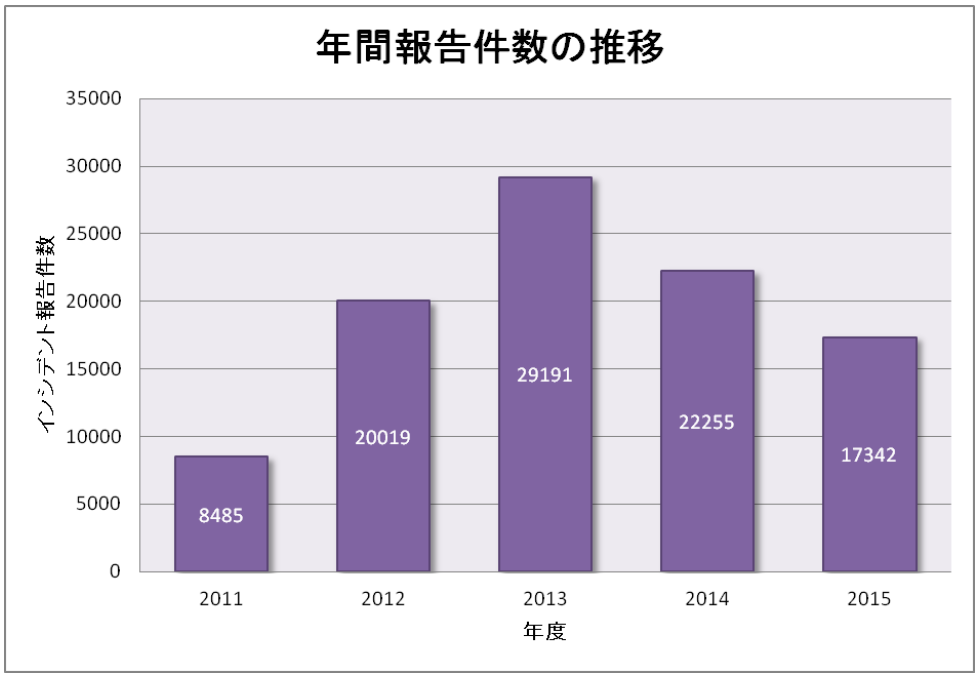
【参考】統計情報の年度比較

2015 年度を含む過去 5 年間の年度ごとの報告件数を[表 **2**]に示します。なお、各年度は 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	2011	2012	2013	2014	2015
報告件数	8485	20019	29191	22255	17342

2015 年度に寄せられた報告件数は 17342 件でした。前年度の 22255 件と比較して、22%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。



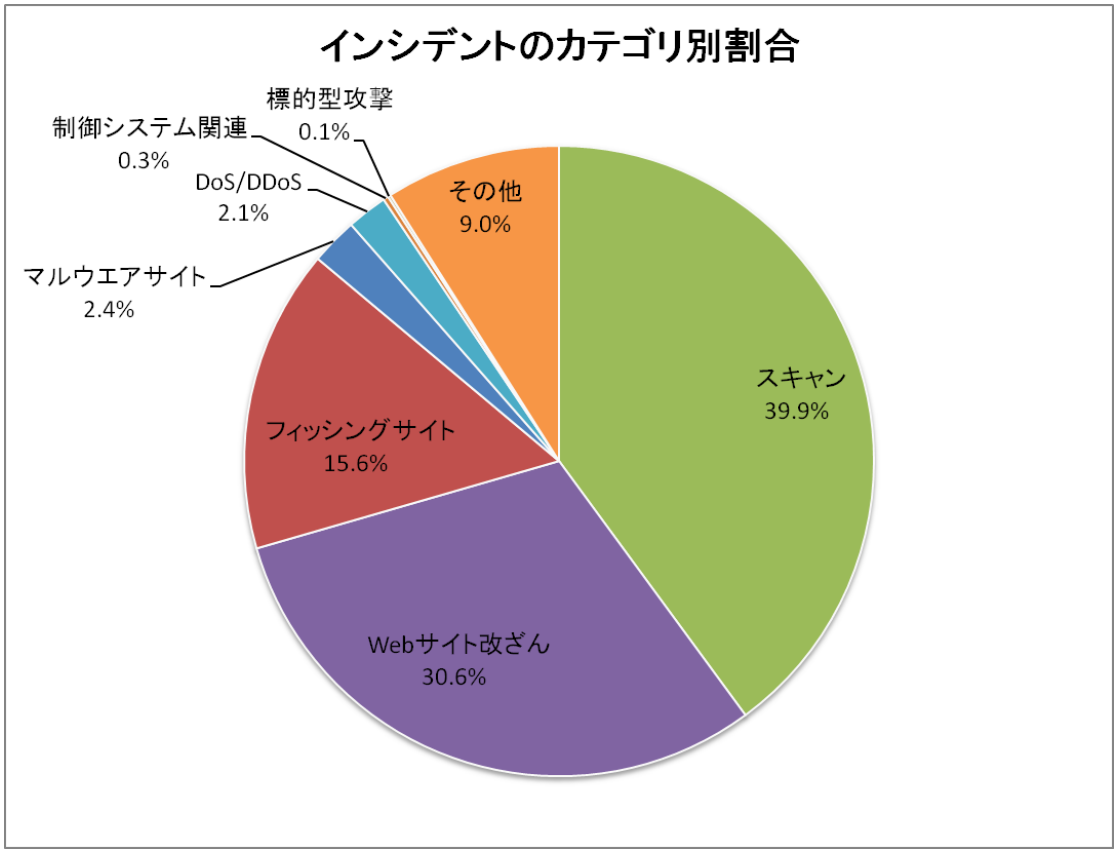
[図 3 年間報告件数の推移（年度比較）]

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]

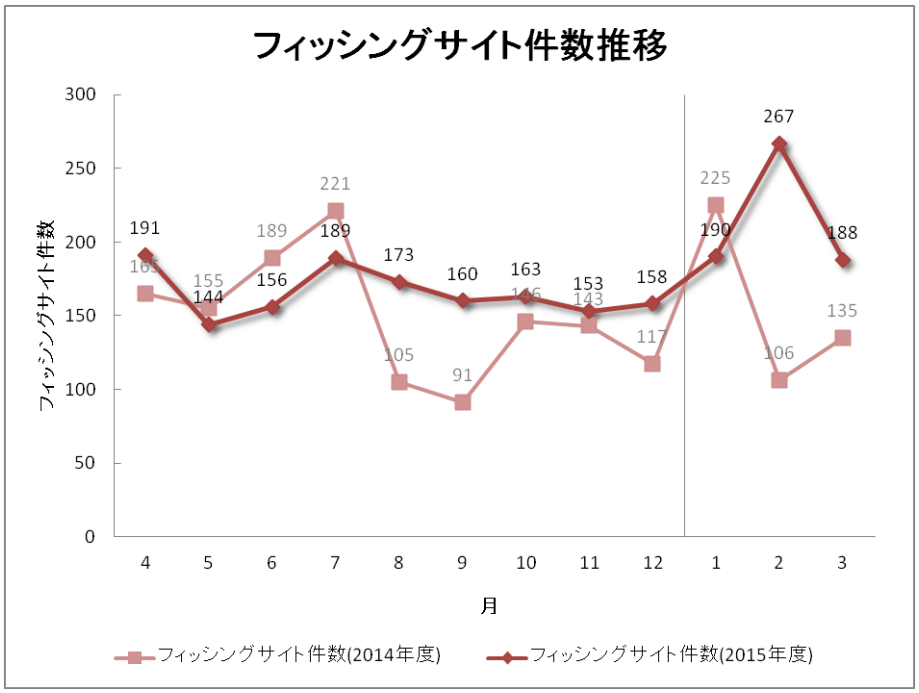
インシデント	1 月	2 月	3 月	合計	前四半期合計
フィッシングサイト	190	267	188	645	474
Web サイト改ざん	283	519	466	1268	826
マルウエアサイト	29	14	57	100	84
スキャン	374	457	823	1654	1526
DoS/DDoS	14	39	33	86	11
制御システム関連	8	3	0	11	12
標的型攻撃	2	4	0	6	12
その他	94	107	172	373	224

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が 39.9%、Web サイト改ざんに分類されるインシデントが 30.6%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 15.6%でした。

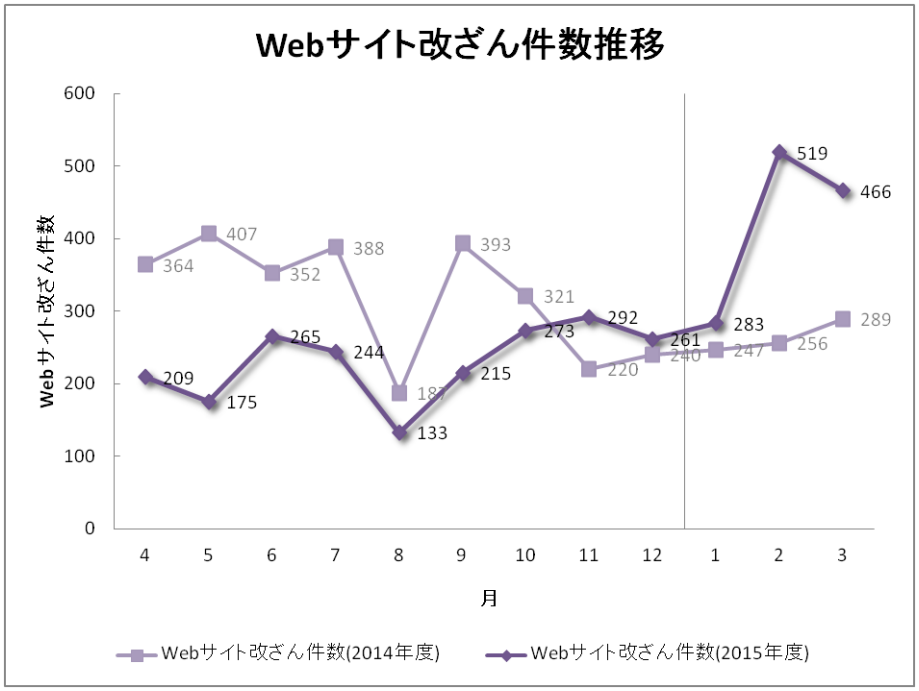


[図 4 インシデントのカテゴリ別内訳]

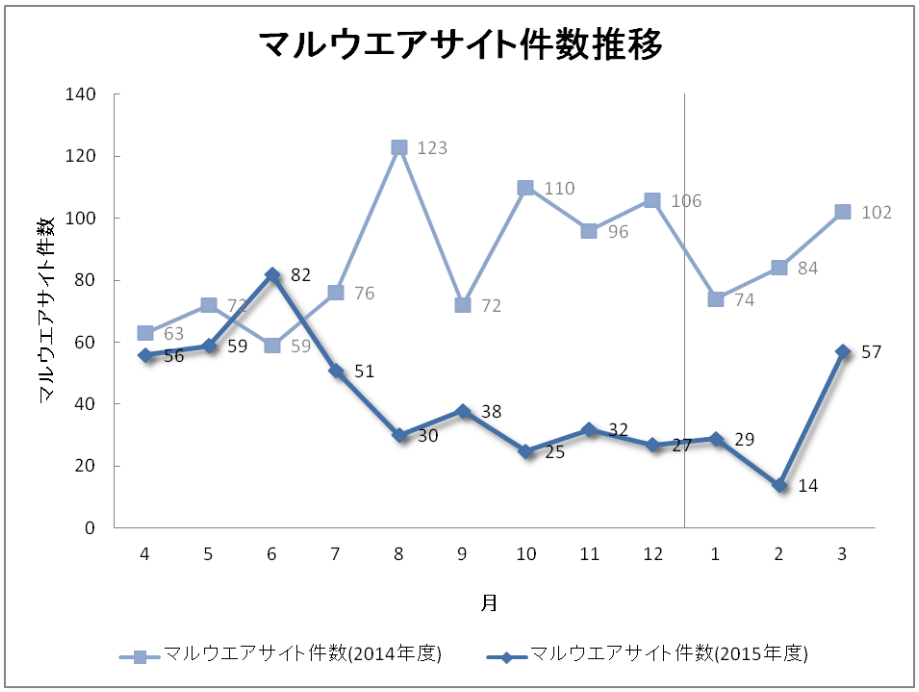
[図 5]から[図 8]に、フィッシングサイト、Web サイト改ざん、マルウエアサイト、スキャンのインシデントの過去 1 年間の月別推移を示します。



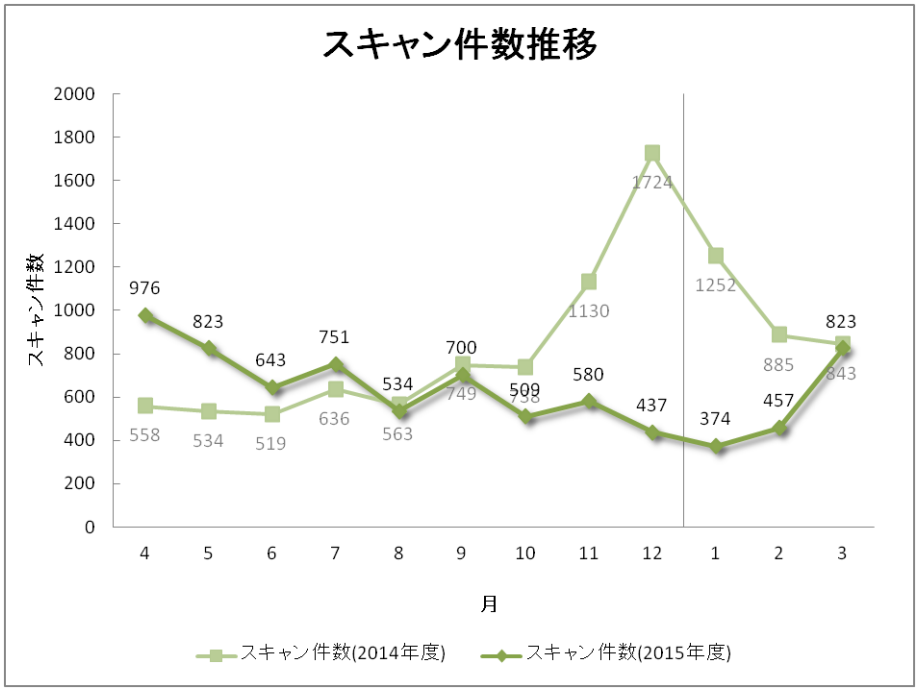
[図 5 フィッシングサイト件数の推移]



[図 6 Web サイト改ざん件数の推移]

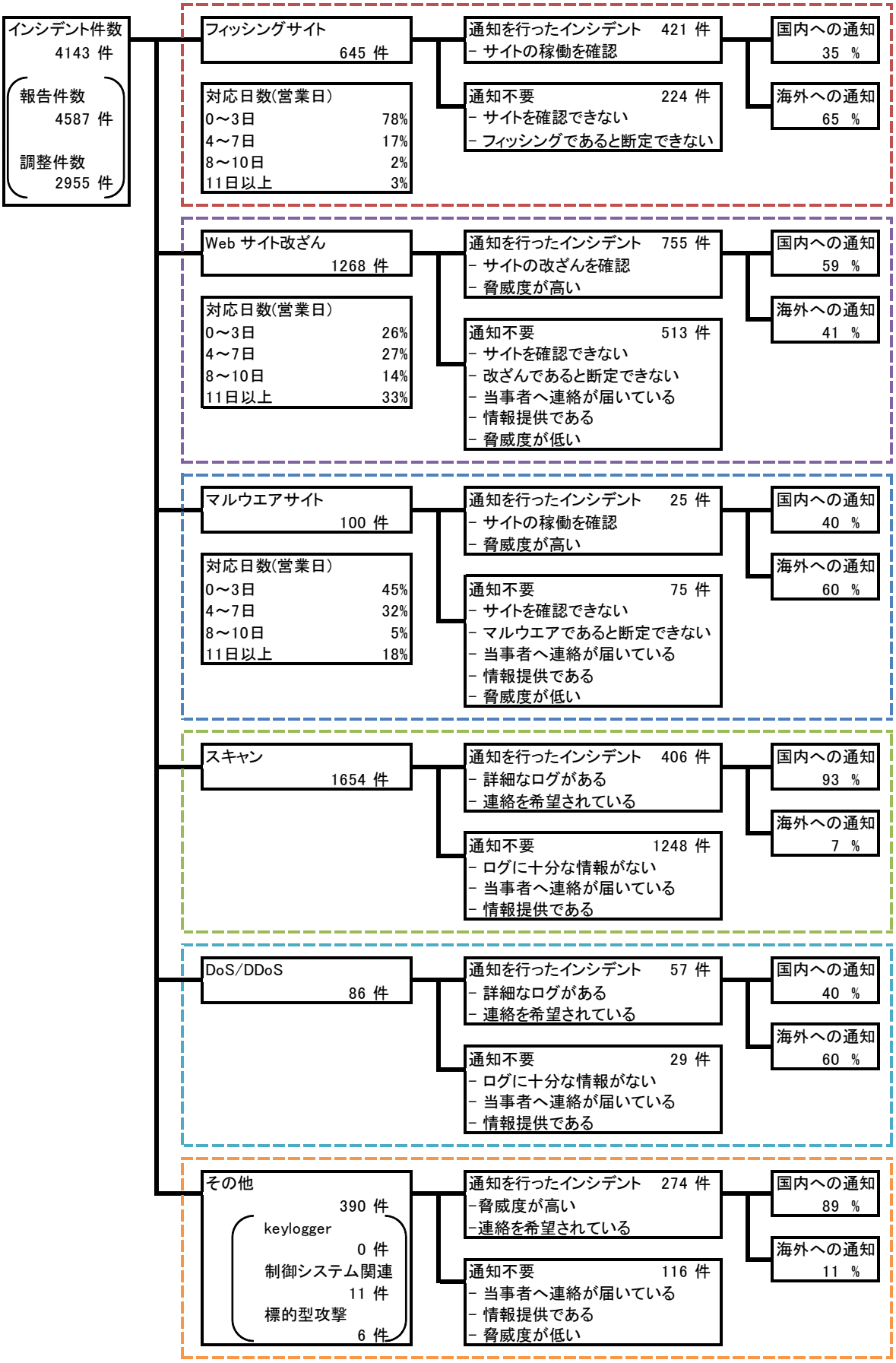


[図 7 マルウエアサイト件数の推移]



[図 8 スキャン件数の推移]

[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

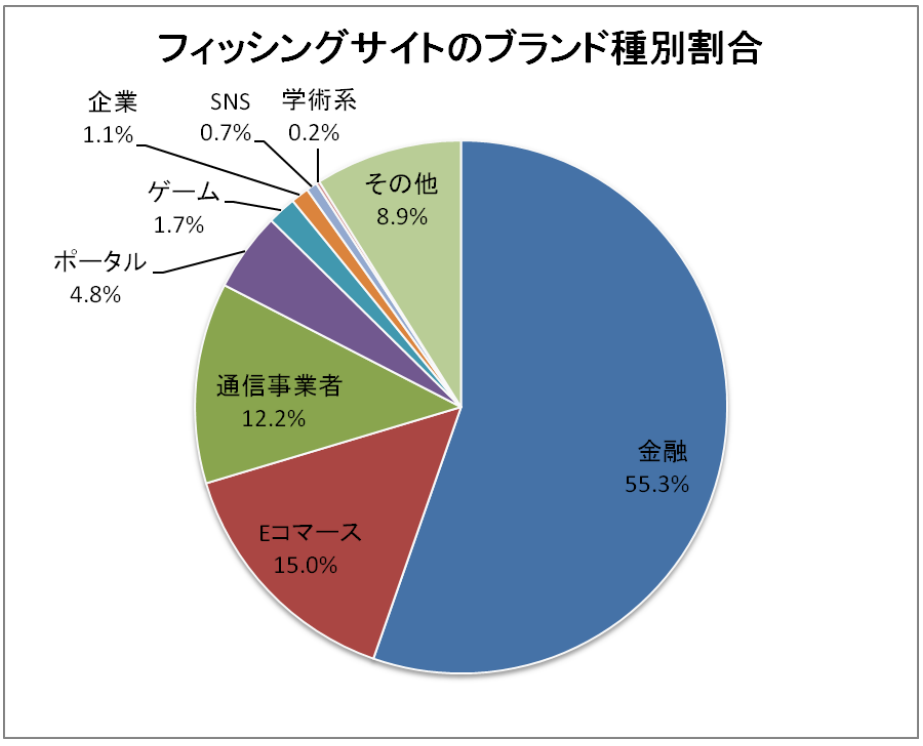
3.1. フィッシングサイトの傾向

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 645 件で、前四半期の 474 件から 36%増加しました。また、前年度同期(466 件)との比較では、38%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]、業界別の内訳を[図 10]に示します。

[表 4 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	1 月	2 月	3 月	国内外別合計(割合)
国内ブランド	48	96	45	189(29%)
国外ブランド	75	95	100	270(42%)
ブランド不明 (注 5)	67	76	43	186(29%)
月別合計	190	267	188	645(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 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 189 件となり、前四半期の 124 件から 52%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 270 件となり、前四半期の 250 件から 8%増加しました。

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 55.3%、E コマースサイトを装ったものが 15.0%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。

1 月末から 3 月前半にかけて、特定の国内金融機関を装ったフィッシングサイトが多く確認されました。この事例のフィッシングメールには、中国の複数の Web サイトの "/images"ディレクトリに不正に設置されたページが記載されており、このページから転送されるフィッシングサイトは香港や中国の IP アドレスのホストが使用されていました。

また同時期に、別の国内金融機関の類似ドメインを使用したフィッシングサイトも多数確認しています。これらのフィッシングサイトでは、正規サイトを装った.com ドメインを使用し、韓国の IP アドレスのホストが使用されていました。

オンラインゲームを装ったフィッシングサイトは、3 月半ば以降は多くの報告が寄せられています。特定のゲームを装ったフィッシングサイトが約 60URL 確認されましたが、ユニークな IP アドレスの数は 6 つのみで、すべて香港の通信事業者のものでした。また、これらのフィッシングサイトでは、無料で登録できる.cc のドメインを使用しているという特徴が見られました。

フィッシングサイトの調整先の割合は、国内が 35%、国外が 65%であり、前四半期(国内 46%、国外 54%)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、1268 件でした。前四半期の 826 件から 54%増加しています。

前四半期に引き続き、CMS を使用した Web サイトが改ざんされている例が非常に多く確認されました。

改ざんされた Web サイトに仕掛けられた不正な JavaScript によって誘導されたサイトで、Internet Explorer、Adobe Flash Player、Silverlight などのアプリケーションの脆弱性が攻撃され、その攻撃によってマルウエアがダウンロード、実行されます。攻撃される Silverlight の脆弱性は、2016 年 1 月に修正された比較的新しい脆弱性(CVE-2016-0034)であることを確認しています。

誘導先サイトからダウンロードされるマルウエアには、金銭を要求して復号するために PC 上のファイルを暗号化するランサムウエアや、アカウントなどの情報を窃取するものなどがあることを確認しています。

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、6 件でした。前四半期の 12 件から 50%減少しています。本四半期は、4 組織（延べ数）に対応を依頼しました。

本四半期は、標的型攻撃のインフラとして使用された国内 IP アドレスや、特定の国内組織を標的とした攻撃に使用された可能性があるマルウエアの情報などを複数の海外セキュリティ組織から受領しました。JPCERT/CC は、提供された情報をもとに、関連する国内組織に事実関係の調査を依頼しました。

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、100 件でした。前四半期の 84 件から 19%増加しています。

本四半期に報告が寄せられたスキャンの件数は、1654 件でした。前四半期の 1526 件から 8%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、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	137	144	338	619
25/tcp	141	172	170	483
22/tcp	45	67	82	194
53/udp	0	1	109	110
23/tcp	12	16	43	71
445/tcp	23	18	17	58
21/tcp	3	7	37	47
123/udp	2	19	2	23
3389/tcp	5	3	5	13
143/tcp	7	1	4	12
53413/udp	4	2	5	11
8080/tcp	2	1	4	7
1433/tcp	0	1	2	3
110/tcp	2	1	0	3
10000/tcp	1	1	1	3
7001/tcp	1	1	0	2
5631/tcp	0	0	2	2
55849/udp	0	0	2	2
53413/tcp	0	1	1	2
139/tcp	0	1	1	2
10686/tcp	0	0	2	2
その他	5	74	17	96
月別合計	390	531	844	1765

その他に分類されるインシデントの件数は、373 件でした。前四半期の 224 件から 67%増加しています。

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。

【インターネット広告を使用したマルウエア配布に関する対応】
本四半期は、表示された広告が原因で国内 Web サイトから悪意のあるサイトへ誘導され、マルウエアがダウンロードされたという報告を複数受領しました。不正な広告は、正規の広告配信プラットフォームを経由して読み込まれており、マルウエアの配布を目的とした攻撃者が、なんらかの方法を使って正式な手順で広告の登録を行っています。不正な広告バナーに含まれる URL に、国内 Web サイトのドメインが使用されている例を複数確認しました。このようなドメインは登録情報を不正に書き変えてサブドメインが追加されたとみられ、海外の IP アドレスに対応付けられていました。また、不正広告のサーバは、無料で取得可能な SSL 証明書を使用しているという特徴が見られました。不正な広告からは、3.2 で述べた改ざんされた Web サイトと同様に、複数の脆弱性を攻撃するサイトに誘導され、マルウエアがダウンロードされることを確認しています。

不正な広告に使用されたホスト名および IP アドレスが意図したものであるか否かを確認するよう、悪用された可能性があるドメインの管理者に JPCERT/CC が依頼したところ、意図したものではなく、DNS 情報が不正に変更された可能性があることが分かりました。

【マルウエアが添付された、国内企業を騙るメールに関する対応】
3 月の初めごろ、国内企業を装った不審なファイルが添付されたメールを大量に受信したという報告が複数寄せられました。提供されたファイルを調査したところ、添付ファイルには JavaScript が含まれており、添付ファイルを開くとマルウエアを取得、実行し、最終的に、国内インターネットバンキングのユーザを標的としたマルウエアに感染することを確認しました。このマルウエアは、特定のインターネットバンキングにアクセスした際に、情報を窃取するために偽のフォームをページに埋め込む Web インジェクションの機能を持っており、この機能に使われる JavaScript を海外のサーバから取得するなどの挙動をすることが分かりました。

JPCERT/CC は、マルウエアを配布するサーバや、マルウエアが取得する設定ファイルを配布するサーバを管理する海外の通信事業者と、それらサーバが設置された地域に対応する海外の CSIRT に対応を依頼しました。

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

○ 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。