JPCERT CC®

Japan Computer Emergency Response Team Coordination Center

電子署名者 : Japan Computer Emergency Response Team Coordination Center
DN : c=JP, st=Tokyo, l=Chiyoda-ku, email=office@jpcert.or.jp, o=Japan Computer Emergency Response Team Coordination Center, cn=Japan Computer Emergency Response Team Coordination Center
日付 : 2016.10.11 17:46:57 +09'00'

JPCERT-IR-2016-03

発行日: 2016-10-12

JPCERT/CC インシデント報告対応レポート
[2016 年 7 月 1 日 ～ 2016 年 9 月 30 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 7 月 1 日から 2016 年 9 月 30 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］

	7 月	8 月	9 月	合計	前四半期合計
報告件数 (注 2)	908	1192	1037	3137	4686
インシデント件数 (注 3)	1012	873	916	2801	3791
調整件数 (注 4)	761	625	736	2122	2559

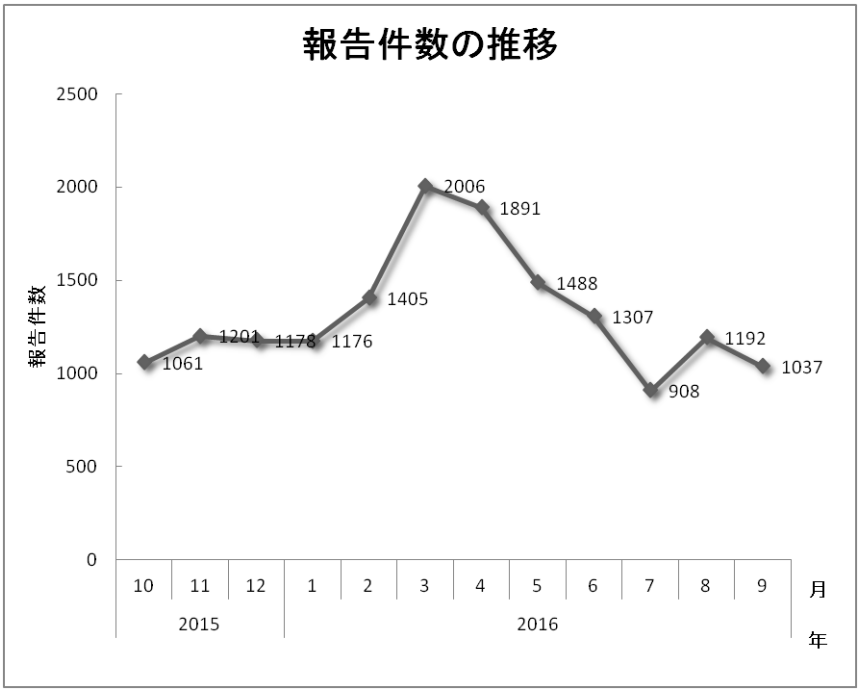
【注 2】「報告件数」は、報告者から寄せられた Web フォーム、メール、FAX による報告の総数を示します。

【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。

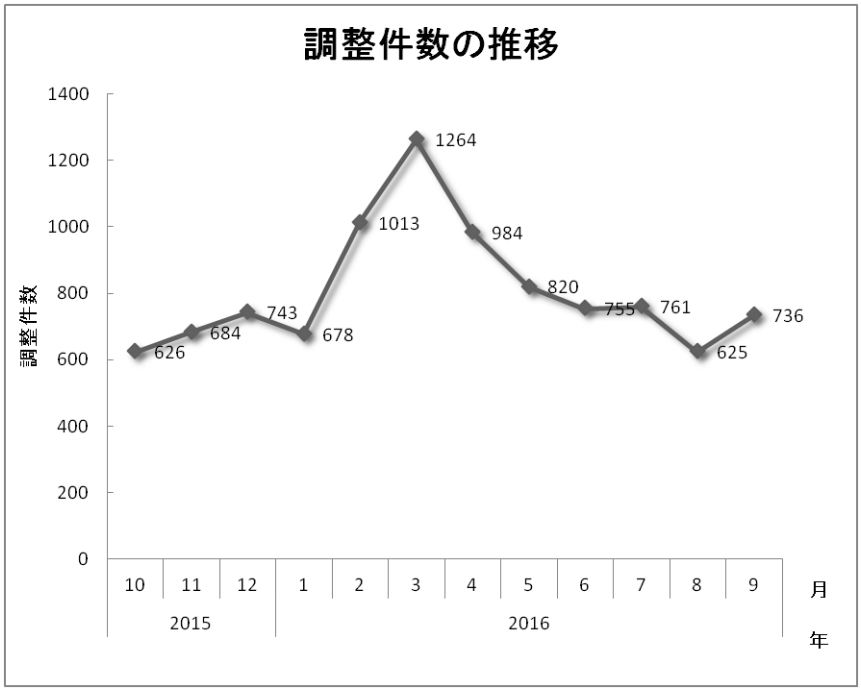
【注 4】「調整件数」は、インシデントの拡大防止のため、サイトの管理者等に対し、現状の調査と問題解決のための対応を依頼した件数を示します。

本四半期に寄せられた報告件数は、3137 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 2122 件でした。前四半期と比較して、報告件数は 33%減少し、調整件数は 17%減少しました。また、前年同期と比較すると、報告数で 24%減少し、調整件数は 3%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 報告件数の推移］



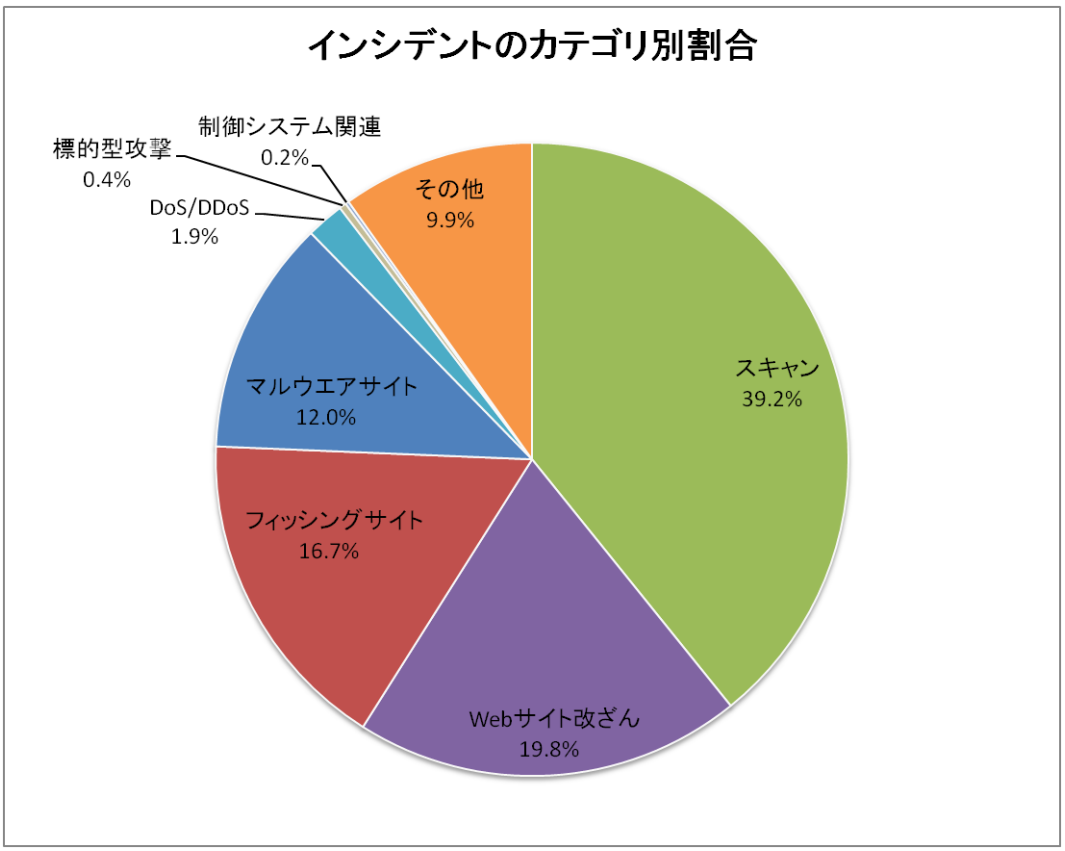
［図 2 インシデント調整件数の推移］

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］

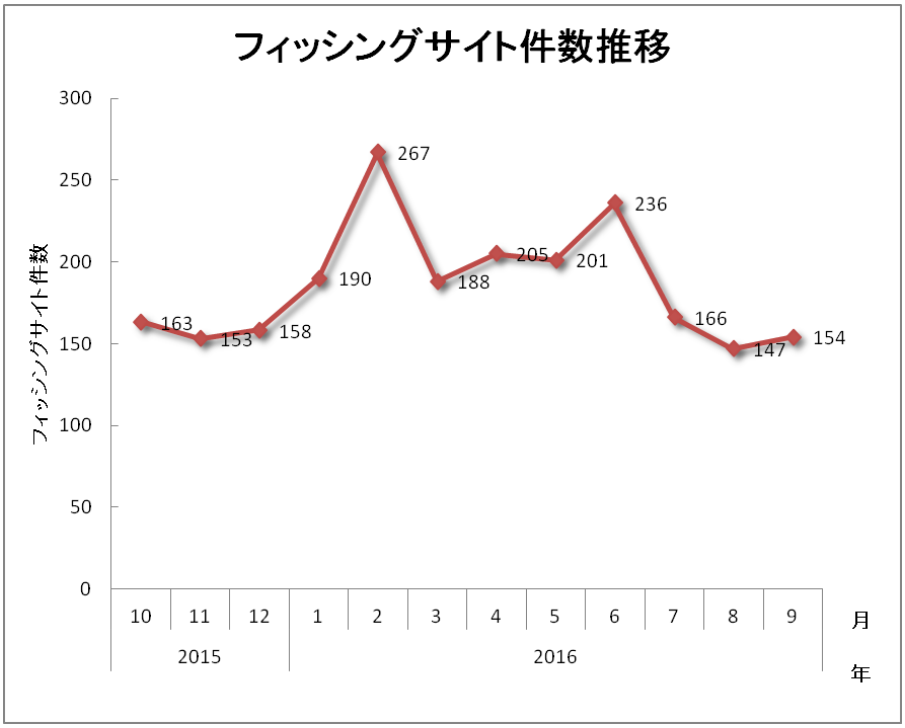
インシデント	7 月	8 月	9 月	合計	前四半期合計
フィッシングサイト	166	147	154	467	642
Web サイト改ざん	236	158	160	554	1065
マルウエアサイト	157	49	131	337	181
スキャン	371	412	315	1098	1520
DoS/DDoS	5	9	40	54	11
制御システム関連	2	2	1	5	15
標的型攻撃	1	6	3	10	15
その他	74	90	112	276	342

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が 39.2%、Web サイト改ざんに分類されるインシデントが 19.8%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 16.7%でした。

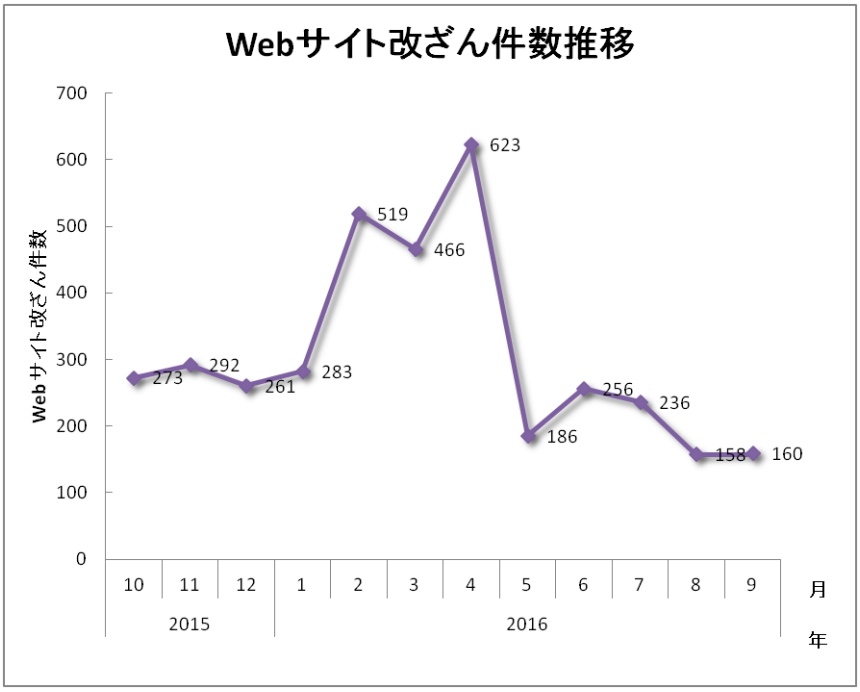


［図 3 インシデントのカテゴリ別割合］

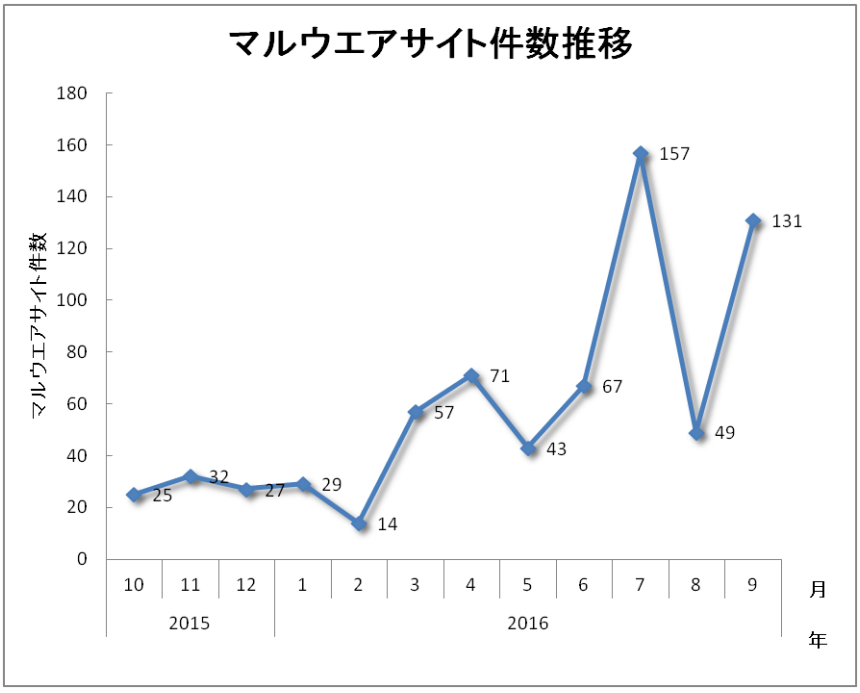
［図 4］から［図 7］に、フィッシングサイト、Web サイト改ざん、マルウエアサイト、スキャンのインシデントの過去 1 年間の月別推移を示します。



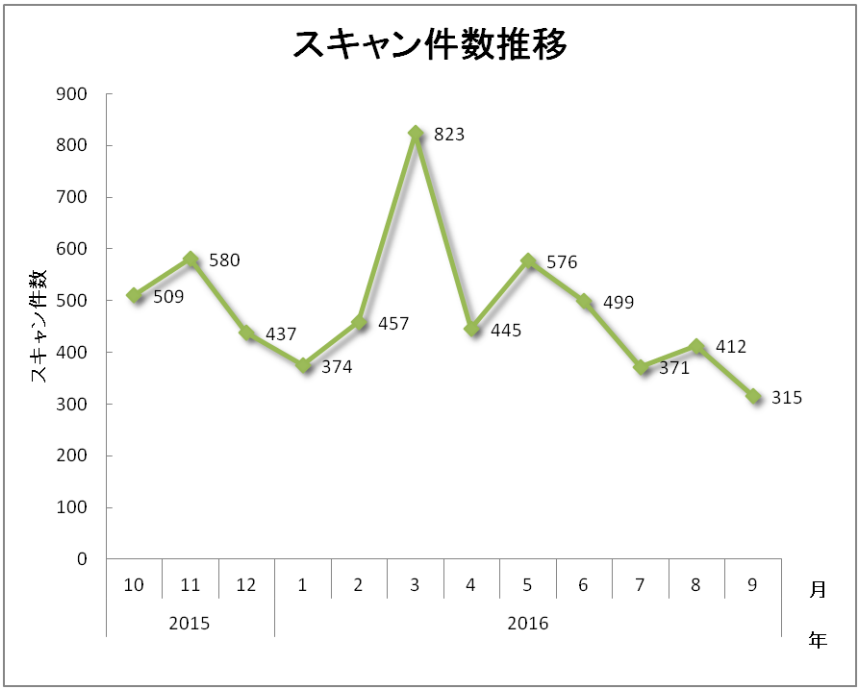
［図 4 フィッシングサイト件数の推移］



［図 5 Web サイト改ざん件数の推移］

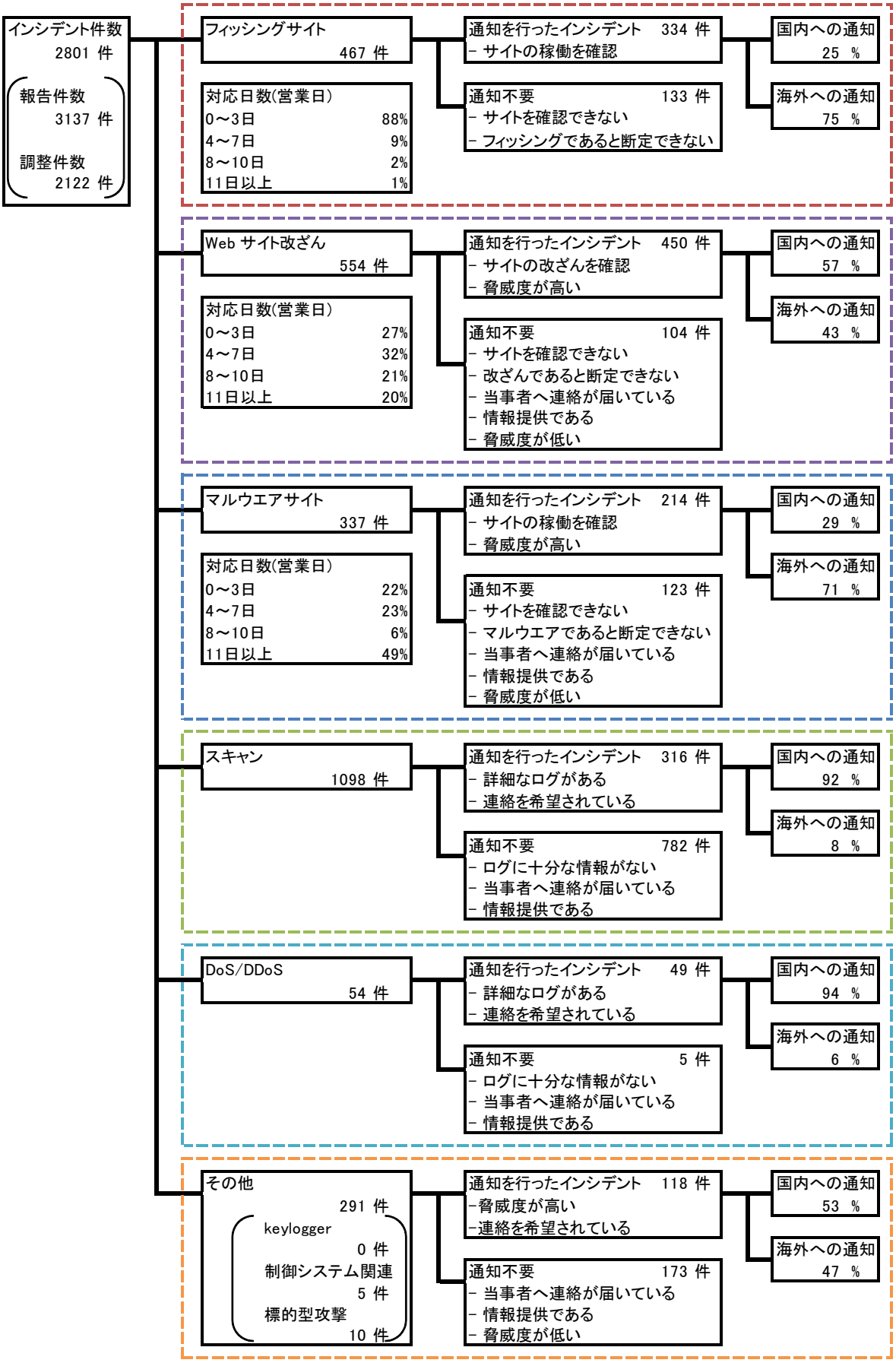


［図 6 マルウエアサイト件数の推移］



［図 7 スキャン件数の推移］

［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

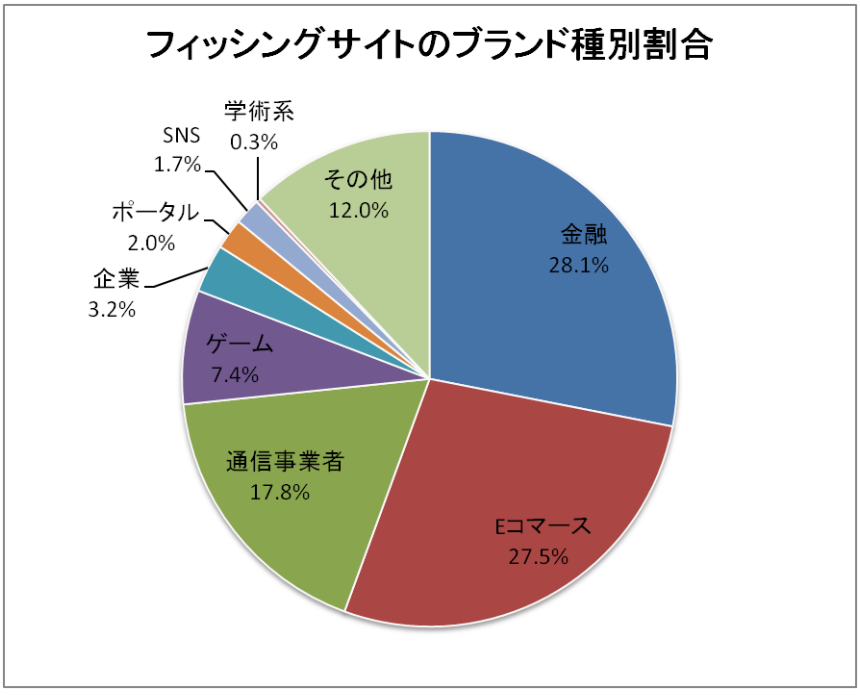
3.1. フィッシングサイトの傾向

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 467 件で、前四半期の 642 件から 27%減少しました。また、前年度同期（522 件）との比較では、11%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］、業界別の内訳を［図 9］に示します。

［表 3 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	7 月	8 月	9 月	国内外別合計（割合）
国内ブランド	30	43	33	106(23%)
国外ブランド	94	73	76	243(52%)
ブランド不明 (注 5)	42	31	45	118(25%)
月別合計	166	147	154	467(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 106 件となり、前四半期の 126 件から 16%減少しました。また、国外のブランドを装ったフィッシングサイトの件数は 243 件となり、前四半期の 312 件から 22%減少しました。

JPCERT/CC が報告を受けたフィッシングサイトの内訳は、金融機関のサイトを装ったものが 28.1%、E コマースサイトを装ったものが 27.5%でした。

前四半期に引き続き、国内通信事業者の Web メールを装ったフィッシングサイトに関する報告が多数寄せられています。これらのフィッシングサイトでは、海外の Web サイトに不正に侵入して設置されたものや、無料 Web サイトサービスを使用して設置されたものがありました。無料 Web サイトサービスは、大学の Web メールを装ったフィッシングサイトでも使用されており、メールの認証情報を窃取しようとする攻撃者に悪用される傾向があります。

金融機関を装ったフィッシングでは、複数のクレジットカードのブランドを装ったフィッシングサイトの報告が寄せられています。これらのフィッシングサイトでは、無料で登録できる.cc ドメインや.online ドメインを使用しているという特徴が見られました。

国内オンラインゲームを装ったフィッシングサイトでは、無料で登録できる.cc ドメインのサブドメインを正規サイトに似せた多数の URL が作成されており、香港、中国の特定のホスティング事業者の IP アドレスが割り当てられていました。

フィッシングサイトの調整先の割合は、国内が 25%、国外が 75%であり、前四半期（国内 30%、国外 70%）に比べ、国外と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、554 件でした。前四半期の 1065 件から 48%減少しています。

前四半期に引き続き、”jquery.min.php”という文字列を含む URL に誘導する、不正な JavaScript が埋め込まれる改ざんが多く確認されました。改ざんの被害を受けたサイトとの調整において、サイト管理者の方から、改ざんされた PHP ファイルや、改ざんされた原因の調査結果を提供していただいた事例があり、この事例では、CMS への攻撃によって、攻撃者がコードの実行に使用するバックドアの設置や、PHP ファイルの改ざんが行われたことが分かりました。

改ざんの被害を受けたサイトは CMS を使用している Web サイトが多く、CMS およびそのテーマやプラグインを対象としたスキャンが広範囲に行われていることから推測すると、JPCERT/CC が認知している以上に多数の Web サイトで改ざんが発生している可能性があります。Web サイトの管理に CMS を使用している場合は、最新のバージョンにアップデートし、不要なテーマやプラグインを削除するなどの対策を実施することが推奨されます。

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、10 件でした。前四半期の 15 件から 33%減少しています。本四半期は、延べ 2 組織に対応を依頼しました。

7 月下旬以降、複数の国内組織から、特定の攻撃グループの標的型攻撃によるものと見られるマルウエア感染の報告が寄せられました。

これらの被害組織から、マルウエア感染端末で発見されたファイルの提供を受け分析したところ、HTTP を使用して攻撃者のサーバと通信し遠隔操作を行う HTTP ボットに分類されるマルウエアや、攻撃者が情報収集に使用したと見られるツールなどが確認されました。また、被害組織から提供されたプロキシサーバのログを調査したところ、HTTP ボットに感染した端末と攻撃者のサーバとの通信には、暗号化された文字列が含まれており、復号すると、攻撃者が感染端末を遠隔操作して情報を収集するためのコマンドを実行した結果などが含まれていることが分かりました。

この一連の攻撃では、被害組織のネットワーク上で、一台の感染端末を踏み台にして多数の端末にマルウエア感染を広げていました。これらのマルウエアは、ひとつの被害組織のなかでも感染端末ごとに通信先が設定されており、攻撃者からの指令を伝達する C2 サーバが多数確認されました。また、マルウエアの通信先には、不正に侵入された国内の Web サーバが多く使用されていました。通信先として悪用されたサーバ上には、攻撃者とボットとのやり取りを仲介する PHP スクリプトが設置されており、この PHP スクリプトによって、攻撃者からボットへの命令の送信やボットから送信されたデータの保存、サーバ上に保存されたデータの取得・削除といった操作ができるようになっていました。

その他にも、なりすましメールによって、遠隔操作を行うマルウエア PlugX や、複数の機能を持つボットのダウンロードおよび実行を行う拡張子を偽装したマルウエアが送りつけられるといった報告が寄せられました。

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、337 件でした。前四半期の 181 件から 86%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、1098 件でした。前四半期の 1520 件から 28%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、SMTP（25/TCP）、SSH（22/TCP）、HTTP（80/TCP）でした。

［表 4 ポート別のスキャン件数］

ポート	7 月	8 月	9 月	合計
25/tcp	167	198	123	488
22/tcp	60	114	73	247
80/tcp	48	40	43	131
23/tcp	43	10	10	63
21/tcp	11	3	6	20
443/tcp	4	4	0	8
3389/tcp	3	1	3	7
6667/tcp	0	5	1	6
53/udp	0	0	6	6
33442/udp	2	2	2	6
4752/udp	3	2	0	5
53413/udp	1	3	0	4
445/tcp	0	2	2	4
1433/tcp	1	0	3	4
8473/udp	0	1	2	3
62374/udp	0	0	3	3
51331/udp	2	1	0	3
5060/udp	1	1	1	3
23887/udp	1	1	1	3
222/tcp	0	3	0	3
143/tcp	0	1	2	3
137/udp	0	0	3	3
8443/tcp	0	2	0	2
8080/tcp	1	0	1	2
5050/tcp	0	1	1	2
441/tcp	2	0	0	2
20472/udp	0	2	0	2
1723/tcp	1	1	0	2
その他	294	104	106	504
月別合計	645	502	392	1539

その他に分類されるインシデントの件数は、276 件でした。前四半期の 342 件から 19%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。

【国内インターネットバンキングの認証情報を窃取するファーミング】
8 月初頭以降、Web ブラウザから正規のインターネットバンキングの URL を指定してアクセスしても、実際には攻撃者が用意したサーバ上の偽のサイトに誘導され、入力した認証情報が窃取される、ファーミングとよばれる攻撃手法が使われたサイトに関する報告が多数寄せられています。

攻撃者が使用するサーバには、国内インターネットバンキングを装ったコンテンツや、攻撃者が使用する管理画面と見られるコンテンツが設置されていることがあり、JPCERT/CC では、悪用されているサーバを確認次第、管理する事業者に適切な対応を取るよう依頼し、サーバの停止に向けた調整を進めています。

また、本件に関連すると見られるマルウエアが確認されたため分析したところ、感染した PC から国内金融機関などの特定のサイトにアクセスすると、マルウエアに組み込まれたプロキシを経由し、HTTP リクエストに特定の情報を付加して攻撃者のサーバにアクセスする仕組みになっていました。

【マルウエアが添付された日本語メールに関する対応】
本四半期は、マルウエアを含む ZIP ファイルが添付された日本語のメールが多く確認されました。メールの送信元アドレスや件名、文面は運送会社を装ったものが多く、宅配物の発送に関する書類の送付に見せかけて、添付ファイルを開かせることを狙ったものと見られます。また、その他にも、短い件名や文面で写真や請求書の送付を装い、添付ファイルを開くよう促すメールなども確認されました。

添付された ZIP ファイルには、Shiotob や Bebloh、URLZone などの名前でウイルス対策ソフトによって検知されるマルウエアが含まれていました。マルウエアを分析したところ、C&C サーバと通信を行い、Ursnif や Gozi などの名前で検知される、インターネットバンキングなどの認証情報を窃取する金融系マルウエアをダウンロードして実行することが分かりました。

JPCERT/CC では、報告された複数のマルウエア添付メールの送信元であった国内の IP アドレスを管理する通信事業者に、メールの配送について事実関係を確認するよう依頼しました。また、ダウンロードされる金融系マルウエアが、侵入されたと見られる国内 IP アドレスの Web サーバに設置されているとの報告に関しては、ホスティング事業者に調査・対応を行うよう依頼し、マルウエアが削除されたことを確認しました。

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 28 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。