JPCERT-IR-2018-02

発行日: 2018-04-12

JPCERT/CC インシデント報告対応レポート
[2018 年 1 月 1 日 ～ 2018 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」）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」）の報告を受け付けています(注 1)。本レポートでは、2018 年 1 月 1 日から 2018 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)	1,339	1,170	1,277	3,786	4,530
インシデント件数 (注 3)	1,424	1,223	1,210	3,857	4,735
調整件数 (注 4)	807	684	712	2,203	1,901

（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。

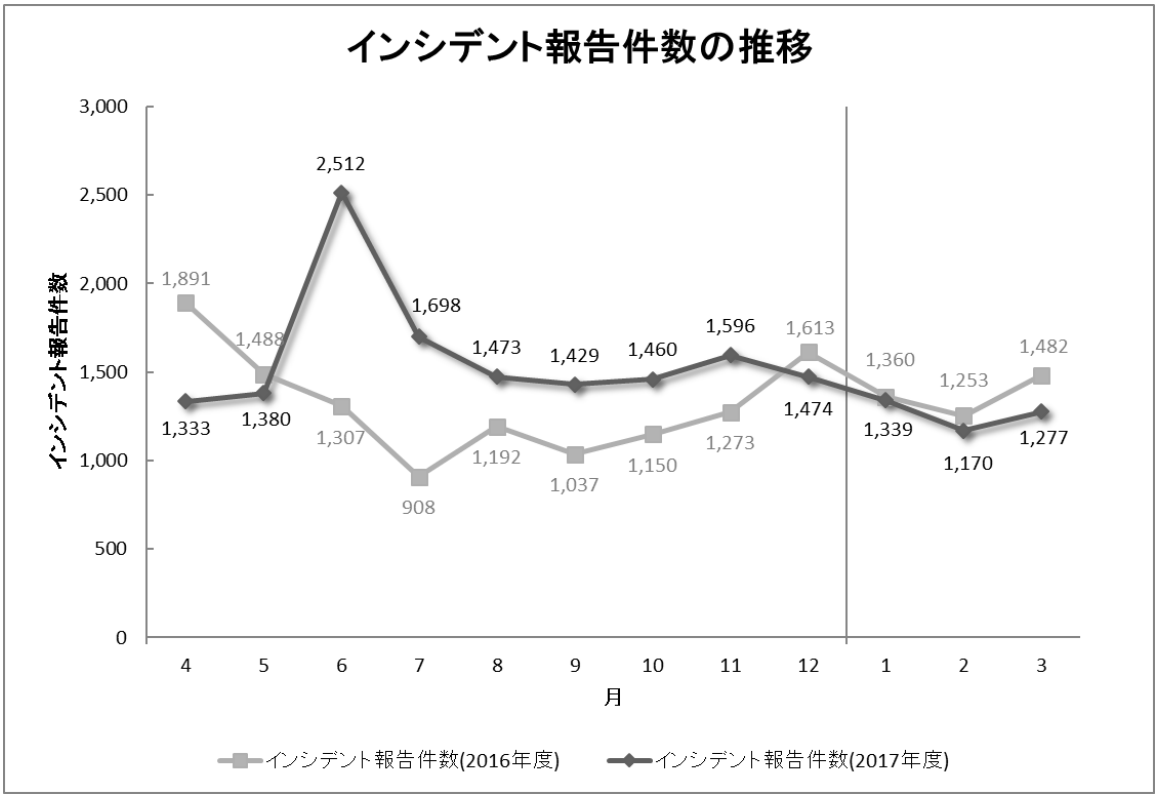
（注 3）「インシデント件数」は、各報告に含まれるインシデント件数の合計を示します。1 つのイン

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。

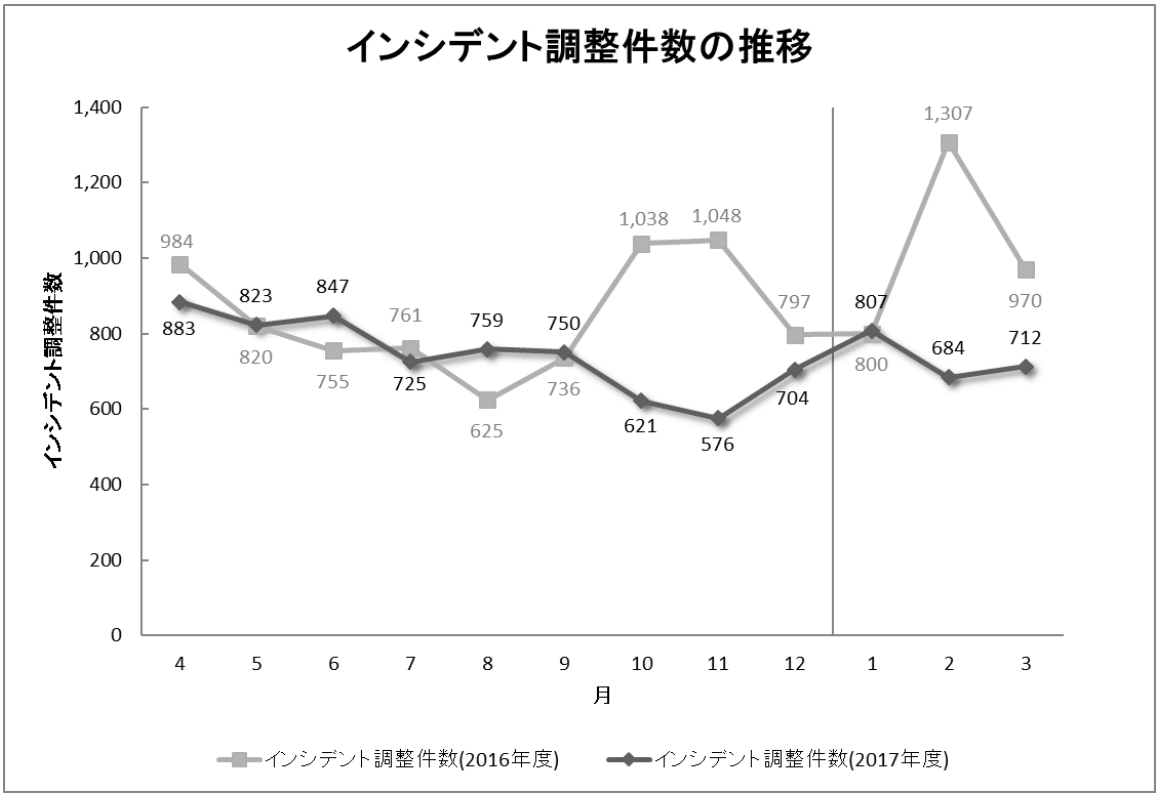
（注 4）「調整件数」は、インシデントの拡大防止のため、サイトの管理者等に対し、現状の調査と問題解決のための対応を依頼した件数を示します。

本四半期に寄せられた報告件数は、3,786 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 2,203 件でした。前四半期と比較して、報告件数は 16%減少し、調整件数は 16%増加しました。また、前年同期と比較すると、報告数で 8%減少し、調整件数は 28%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］

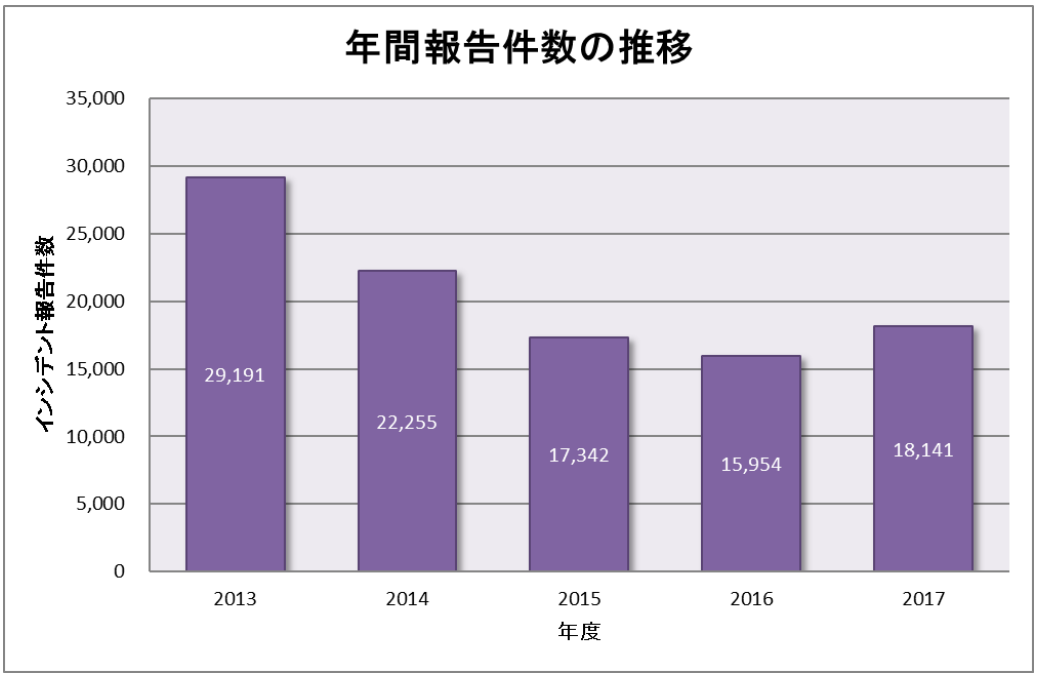
【参考】統計情報の年度比較

2017 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	2013	2014	2015	2016	2017
報告件数	29,191	22,255	17,342	15,954	18,141

2017 年度に寄せられた報告件数は 18,141 件でした。前年度の 15,954 件と比較して、14%増加しています。［図 3］に過去 5 年間の年間報告件数の推移を示します。



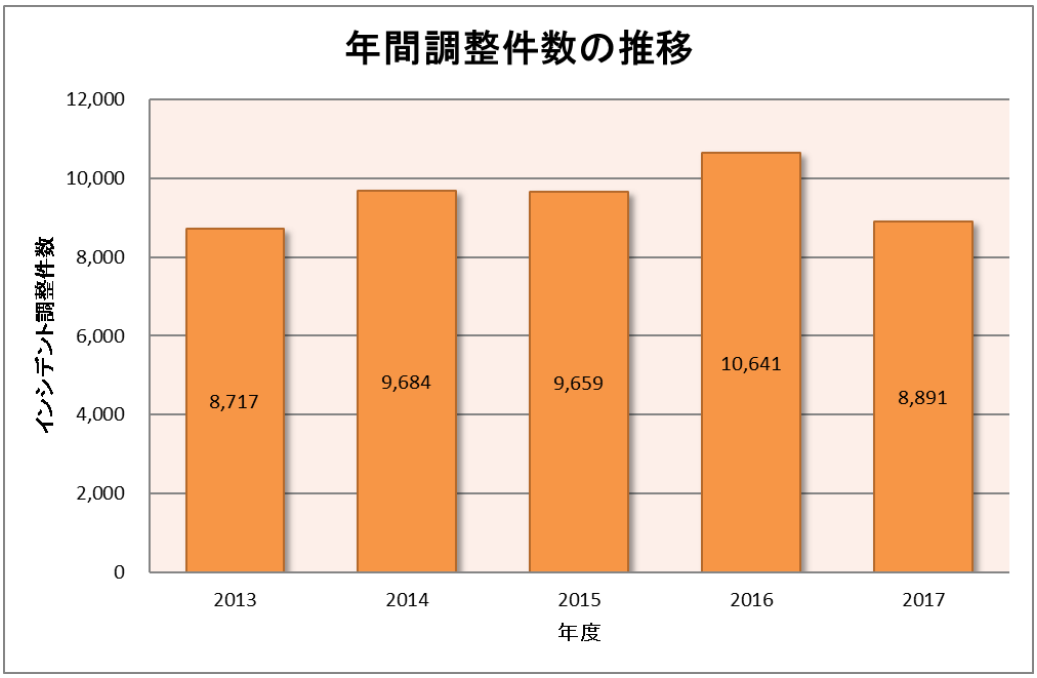
［図 3 年間報告件数の推移（年度比較)］

2017 年度を含む過去 5 年間の年度ごとの調整件数を［表 3］に示します。

［表 3: 調整報告件数の推移］

年度	2013	2014	2015	2016	2017
調整件数	8,717	9,684	9,659	10,641	8,891

2017 年度に調整を行った件数は 8,891 件でした。前年度の 10,641 件と比較して、16%減少しています。［図 4］に過去 5 年間の年間調整件数の推移を示します。



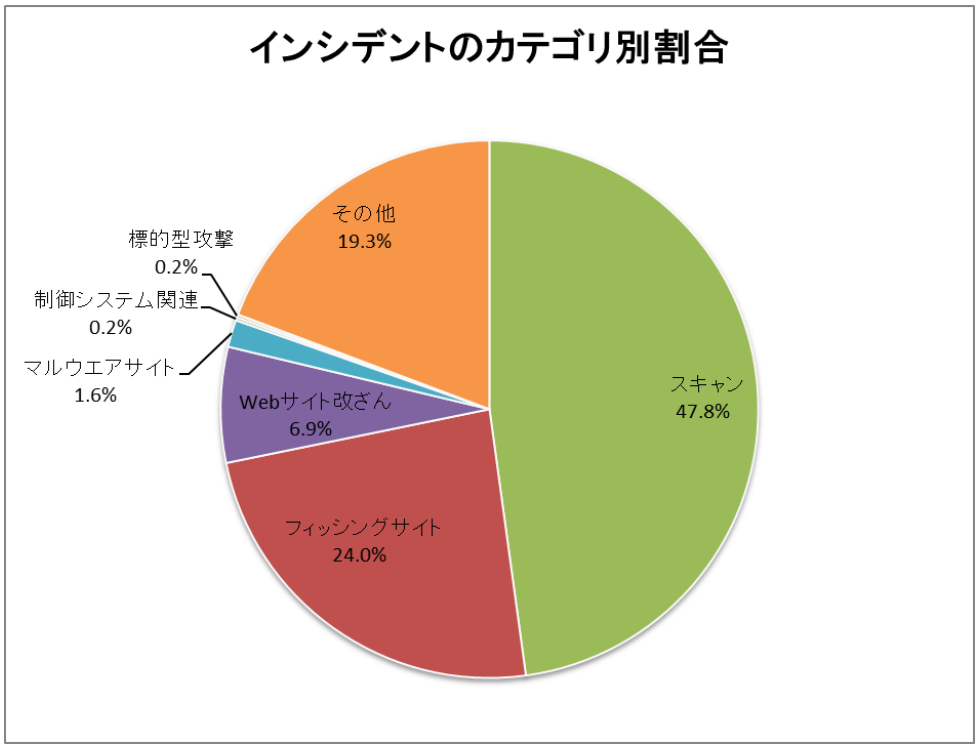
［図 4 年間調整件数の推移（年度比較）］

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 4］に示します。

［表 4 カテゴリ別インシデント件数］

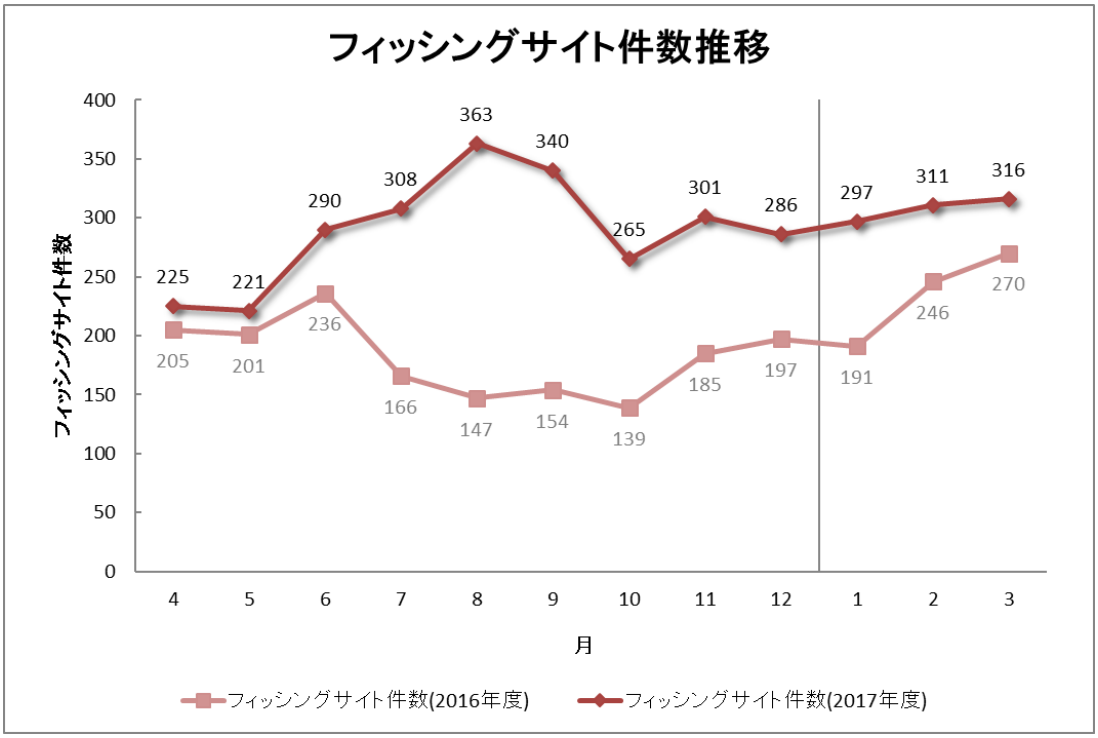
インシデント	1 月	2 月	3 月	合計	前四半期合計
フィッシングサイト	297	311	316	924	852
Web サイト改ざん	122	77	69	268	276
マルウエアサイト	24	17	22	63	88
スキャン	684	618	543	1,845	1,979
DoS/DDoS	0	1	0	1	8
制御システム関連	2	0	5	7	33
標的型攻撃	2	2	2	6	9
その他	293	197	253	743	1,490

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 5］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 47.8%、フィッシングサイトに分類されるインシデントが 24.0%を占めています。

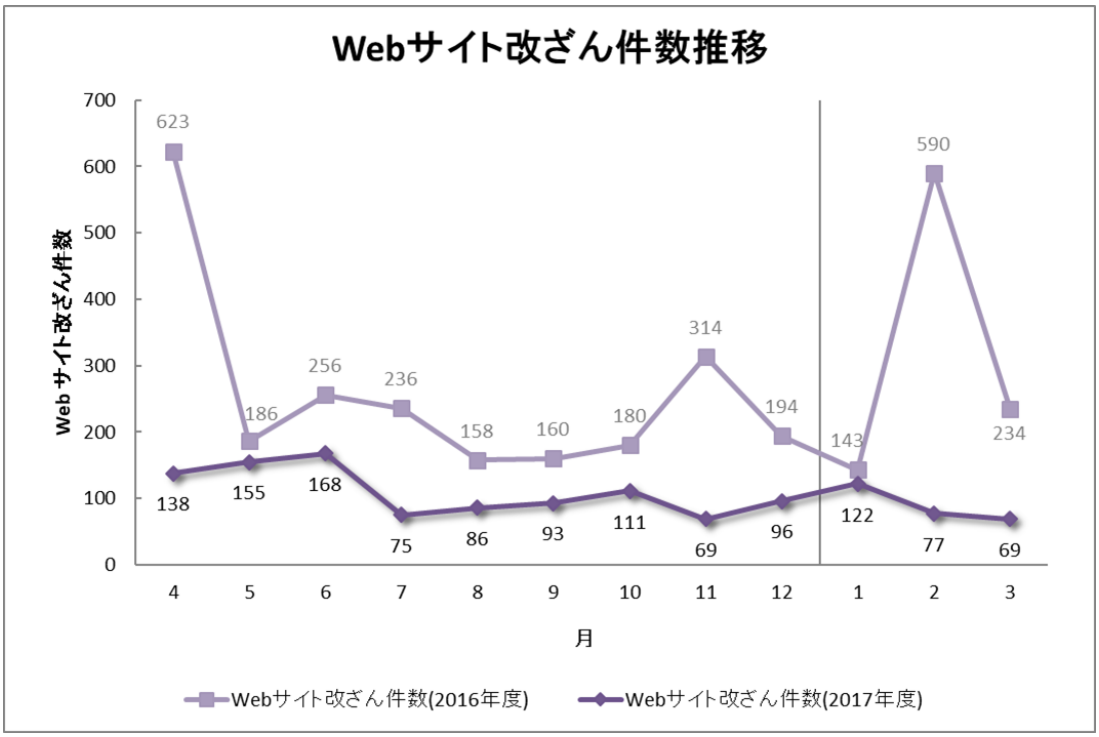


［図 5 インシデントのカテゴリ別割合］

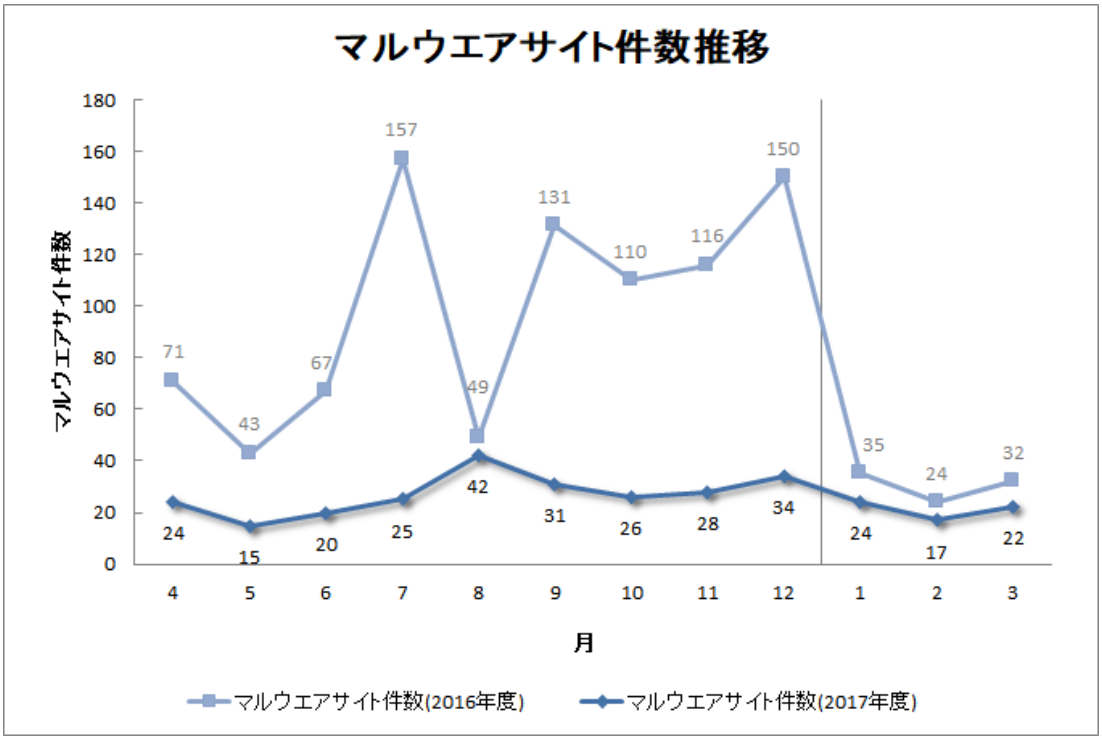
［図 6］から［図 9］に、フィッシングサイト、Web サイト改ざん、マルウエアサイト、スキャンのインシデントの過去 1 年間の月別推移を示します。



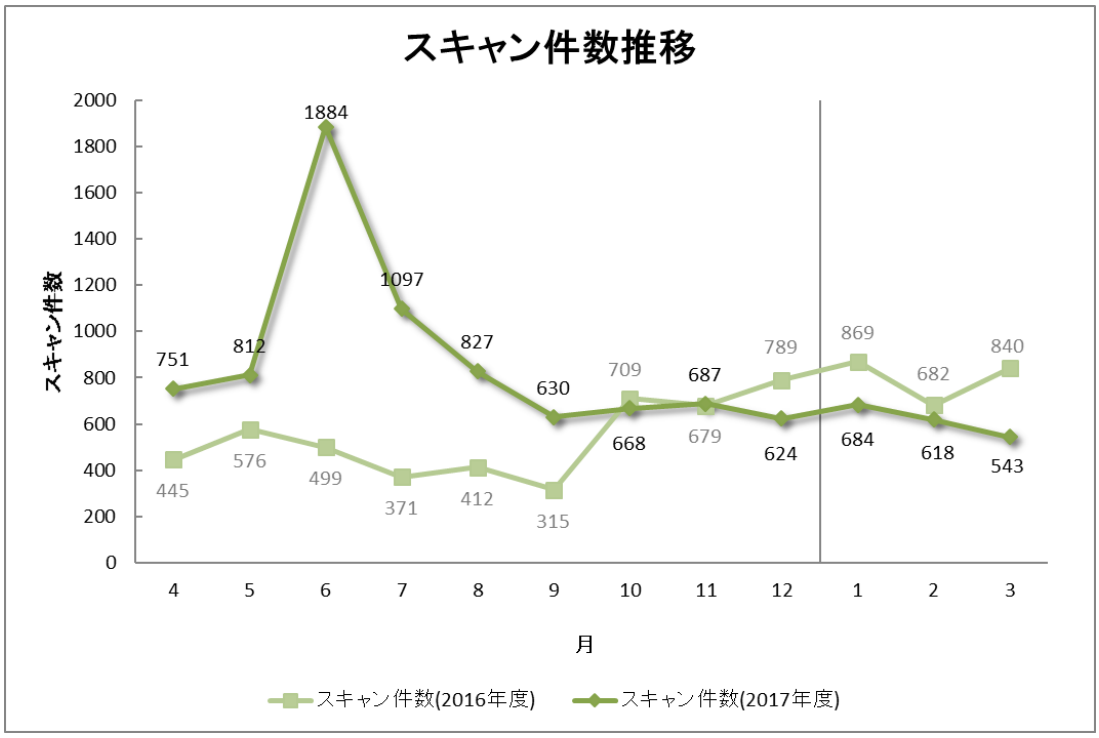
［図 6 フィッシングサイト件数の推移］



［図 7 Web サイト改ざん件数の推移］

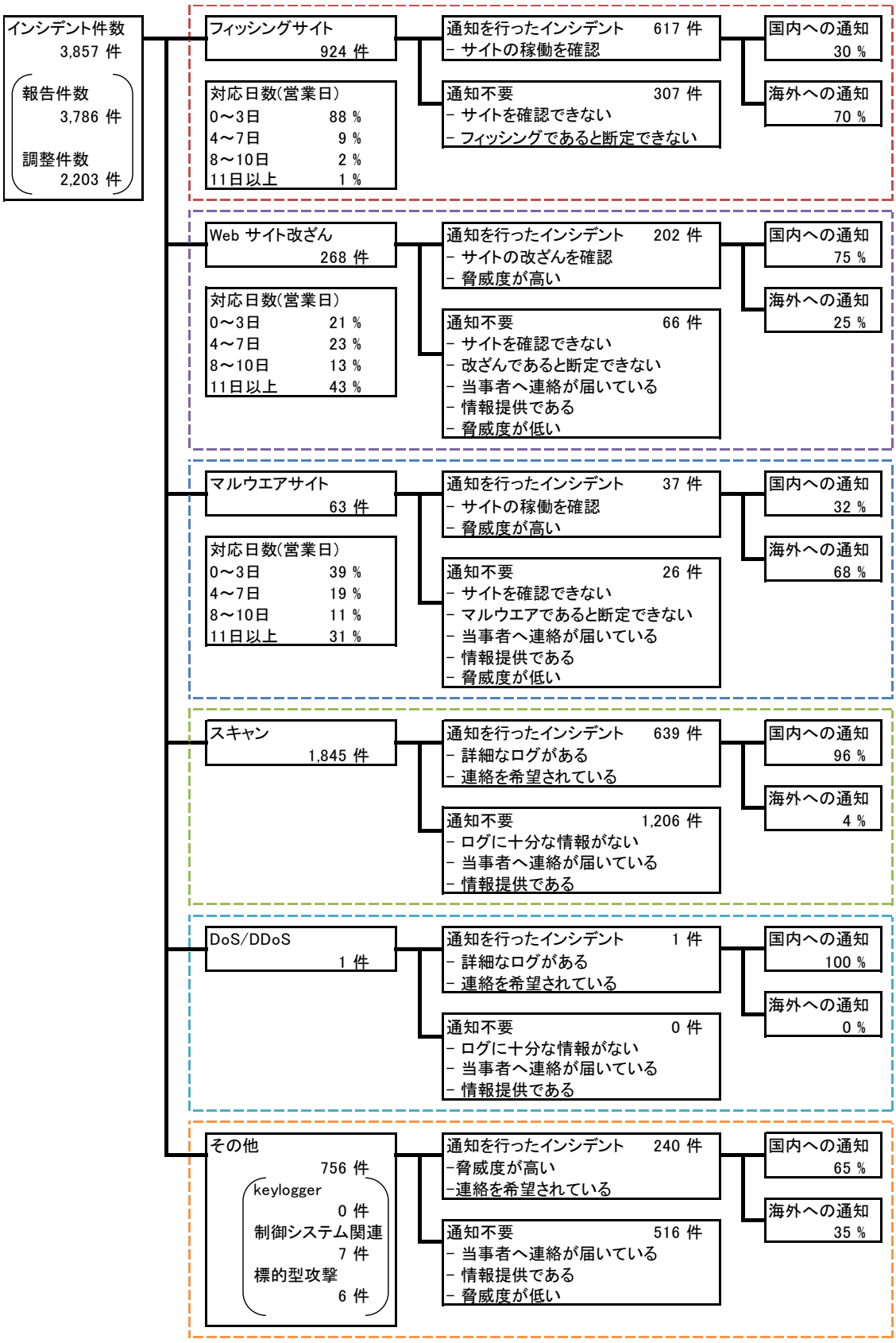


［図 8 マルウエアサイト件数の推移］



［図 9 スキャン件数の推移］

［図 10］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 10 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

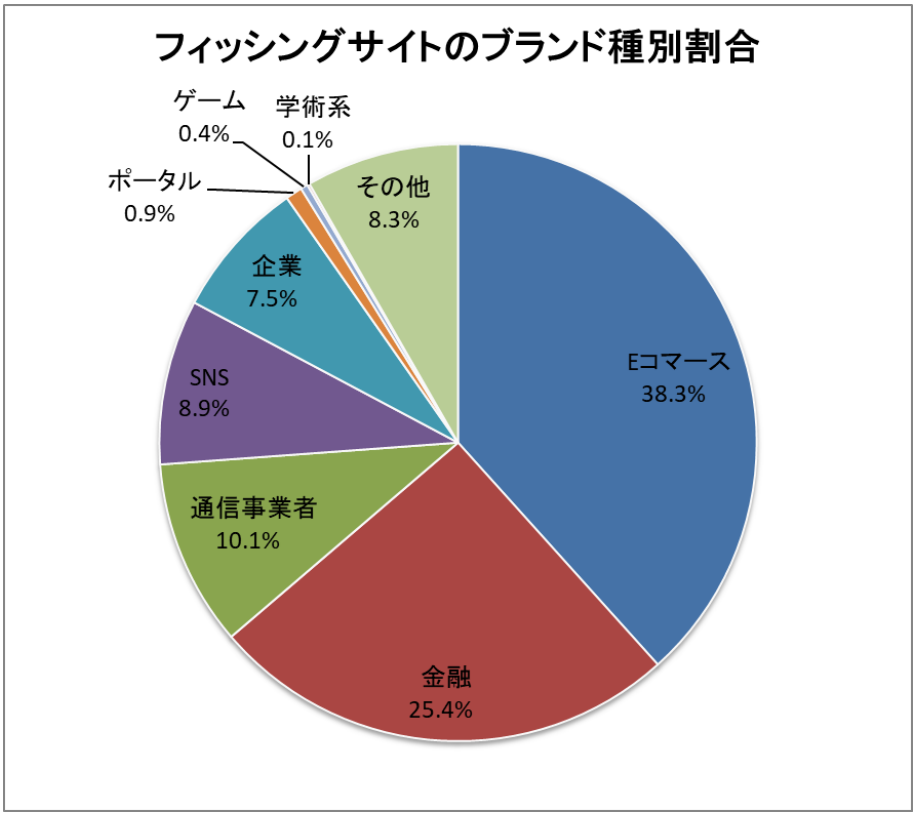
3.1. フィッシングサイトの傾向

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 924 件で、前四半期の 852 件から 18%増加しました。また、前年度同期（707 件）との比較では、31%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 5］、業界別の内訳を［図 11］に示します。

［表 5 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	本四半期合計（割合）
国内ブランド	78	58	72	208(23%)
国外ブランド	174	212	178	564(61%)
ブランド不明 (注 5)	45	41	66	152(16%)
全ブランド合計	297	311	316	924(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 11 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 208 件となり、前四半期の 117 件から 78%増加しました。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 564 件となり、前四半期の 599 件から 6%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、E コマースサイトを装ったものが 38.3%、金融機関のサイトを装ったものが 25.4%、通信事業者のサイトを装ったものが 10.1%でした。

前四半期と同様に、特定の海外ブランドのアカウント窃取を目的としたフィッシングサイトに関する報告が多く寄せられています。異なる見た目でありながら、同じサービスのアカウントを窃取するフィッシングサイトが複数確認されています。一つのフィッシングサイトが停止した後、同じサーバ上で新たに異なる見た目のフィッシングサイトが確認されるなど、攻撃者が共通していると見られるものもありました。

国内ブランドのフィッシングサイトでは、通信事業者、SNS、金融機関を装ったフィッシングサイトに関する報告が多く寄せられました。国内通信事業者を装ったフィッシングサイトでは、ある 2 つのブランドに関する報告が多く、一方は海外の Web サイト作成サービスに設置され、もう一方は WordPress を使ったサイトに設置されるといった傾向が見られました。SNS を装ったフィッシングサイトは、ブランド名に 2、3 文字の英小文字を連結した.cn ドメインを使用したものが、本年度は継続して確認されています。金融機関を装ったフィッシングサイトでは、クレジットカード情報の窃取を目的としたものが大半を占めました。

フィッシングサイトの調整先の割合は、国内が 30%、国外が 70%であり、前四半期（国内 25%、国外 75%）に比べ、国内で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、268 件でした。前四半期の 276 件から 3%減少しています。

本四半期は、Google Chrome からアクセスしてきたユーザに不審なサイトへの誘導やポップアップの表示を行う、不正な JavaScript が埋め込まれる改ざんを確認しました。不審なポップアップが表示される改ざんとしては、Chrome のフォントパックのアップデートを装ってランサムウエアをダウンロードさせ、実行させるものが 2 月に確認されました。同様の手法は 2017 年 1 月ごろにも確認されていましたが、本四半期には以前とは異なる種類のランサムウエアがダウンロードされるようになっていました。3 月に複数の国内サイトに埋め込まれていた JavaScript は、ページ上をクリックするとロシア語の国際化ドメイン名を使用した URL に誘導する仕組みになっていましたが、確認した時点では誘導先が名前解決できない状態になっており、どのような脅威があるかは分かりませんでした。改ざんされたサイトは CMS を使用しているものが多く、脆弱性を悪用した攻撃や、管理画面から不正にログインされてファイルを設

置されることによって、不正なスクリプトを埋め込まれた可能性が考えられます。

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、6 件でした。前四半期の 9 件から 23%減少しています。本四半期は、対応を依頼した組織はありませんでした。

国内の複数の組織において、組織で利用しているクラウドサービスに不正にログインされ、サービスの悪用によるメールの送信や、クラウドストレージ上のファイルへのアクセスが行われたといった内容のインシデントが発生しており、本四半期に情報が寄せられました。

同様の被害を受けたいくつかの組織には、組織の認証ポータルを装ったフィッシングサイトに誘導するフィッシングメールが、他の国内組織から送り付けられていました。また、フィッシングメールの送信元になっていた組織も、以前に類似のフィッシングの被害を受けている場合がありました。クラウドサービスに不正にログインされた被害組織の調査では、攻撃者が一度の情報入力でログインに成功している形跡が確認されており、フィッシングなどで窃取したアカウント情報を使用して、不正アクセスを行った可能性があります。

不正アクセスは、海外のホスティングサービスや、匿名ネットワーク Tor のノードと見られる IP アドレスなどから行われていたことを確認しています。これらの IP アドレスの情報を国内の被害組織に共有したところ、いくつかの組織において、共通の海外 IP アドレスからのアクセスが見つかりました。

JPCERT/CC では、類似の被害を受けた複数の組織と連携し、攻撃の調査や、関連する組織への情報の展開を実施しています。

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、63 件でした。前四半期の 88 件から 28%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、1,845 件でした。前四半期の 1,979 件から 7%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 6］に示します。頻繁にスキャンの対象となったポートは、SSH（22/TCP）、SMTP（25/TCP）、Telnet（23/TCP）でした。

［表 6 ポート別のスキャン件数］

ポート	1 月	2 月	3 月	合計
22/tcp	419	385	300	1,104
25/tcp	74	87	84	245
23/tcp	107	57	80	244
2323/tcp	41	17	33	91
80/tcp	26	15	36	77
81/tcp	2	7	8	17
445/tcp	8	4	4	16
8080/tcp	0	5	9	14
52869/tcp	5	8	0	13
3389/tcp	5	6	1	12
5555/tcp	0	4	6	10
21/tcp	7	1	2	10
82/tcp	1	0	6	7
443/tcp	3	2	2	7
2222/tcp	2	3	2	7
9999/tcp	0	0	6	6
53/udp	1	2	2	5
9000/tcp	0	4	0	4
8000/tcp	3	0	0	3
12817/udp	1	2	0	3
5912/tcp	2	0	0	2
5060/udp	1	1	0	2
44818/tcp	0	0	2	2
3333/tcp	2	0	0	2
3306/tcp	1	1	0	2
その他	429	632	444	1,505
月別合計	1,140	1,243	1,027	3,410

その他に分類されるインシデントの件数は、743 件でした。前四半期の 1,490 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。

【SMS から誘導される国内企業を装ったサイトに関する対応】
2018 年 1 月上旬に、国内企業を装って不審な Android のアプリケーション（APK ファイル）をインストールさせるサイトに関する報告が複数寄せられました。報告によると、国内企業になりすましたスマートフォン用 SMS のメッセージが出回っており、短縮 URL によって偽のサイトに誘導しているとのことでした。短縮 URL の誘導先は、クレジットカードの発行状況を確認するサイトや、宅配便の配送状況を追跡するサイトを装って、アプリをインストールするように促すものでした。サイトは 1 月上旬から 2 月下旬にかけて複数確認されましたが、いずれも同じ.cc のドメインを使用しており、台湾の IP アドレスが割り当てられていました。また、アプリを配布するサイトと同じ IP アドレスで、国内通信事業者を装って ID とパスワードを詐取するフィッシングサイトも確認されました。

JPCERT/CC では、国内企業を装ったサイトが設置されていたサーバと、不審な APK ファイルの通信先となるサーバを管理するホスティング事業者に対応を依頼し、最終的にこれらのサーバが停止したことを確認しました。

【Oracle WebLogic Server の脆弱性を使用した攻撃に関する対応】
JPCERT/CC は 2018 年 1 月 17 日に、“Oracle WebLogic Server の脆弱性（CVE-2017-10271）を使用した攻撃に関する注意喚起”を公開しました。本四半期は、当該脆弱性を悪用した攻撃に関する報告が複数寄せられました。

2018 年 2 月半ばに、WebLogic の脆弱性を悪用した攻撃の通信内容に関する報告が寄せられました。報告元から提供された通信のログを確認したところ、攻撃元からは細工された XML のデータが送信されており、データ内にファイルをダウンロードして実行するコマンドが埋め込まれていました。また、2 月後半には、WebLogic の脆弱性を悪用した攻撃によってサーバ上に設置されたファイルに関する報告が寄せられました。報告元から提供されたファイルには、外部からのファイルの取得や実行などを行うスクリプトと、スクリプトが取得したと見られる実行ファイルが含まれていました。実行ファイルは仮想通貨 Monero のマイニングを行うアプリケーション XMRig で、攻撃者はマイニングによる報酬の獲得を目的としていたと見られます。

JPCERT/CC では、攻撃に使用されていたスクリプトや実行ファイルが設置されたサーバを管理するホスティング事業者に、サーバが攻撃に悪用されていることを連絡し、対応を依頼しました。

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 29 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。