JPCERT/CC インシデント報告対応レポート

2019 年 1 月 1 日 ～ 2019 年 3 月 31 日

一般社団法人 JPCERT コーディネーションセンター

2019 年 4 月 11 日

目次

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、2019 年 1 月 1 日から 2019 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、本レポートでは、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（前四半期より制御システム関連のインシデント報告関連件数の集計方法を変更しています）。

［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)	1,536	1,349	1,548	4,433	4,242
インシデント件数 (注 3)	1,649	1,562	1,761	4,972	4,488
調整件数 (注 4)	813	1,044	1,059	2,916	2,579

（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。

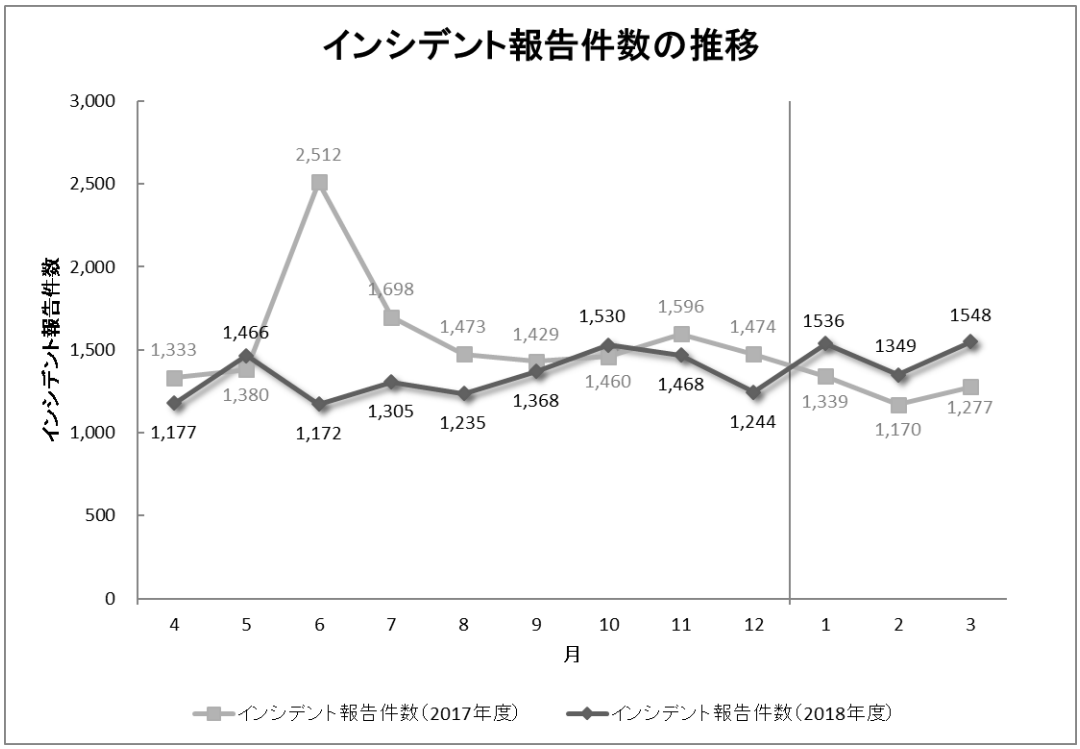
（注 3）「インシデント件数」は、各報告に含まれるインシデント件数の合計を示します。1 つのインシデントに関して複数件の報告が寄せられた場合にも、1 件として扱います。

（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。

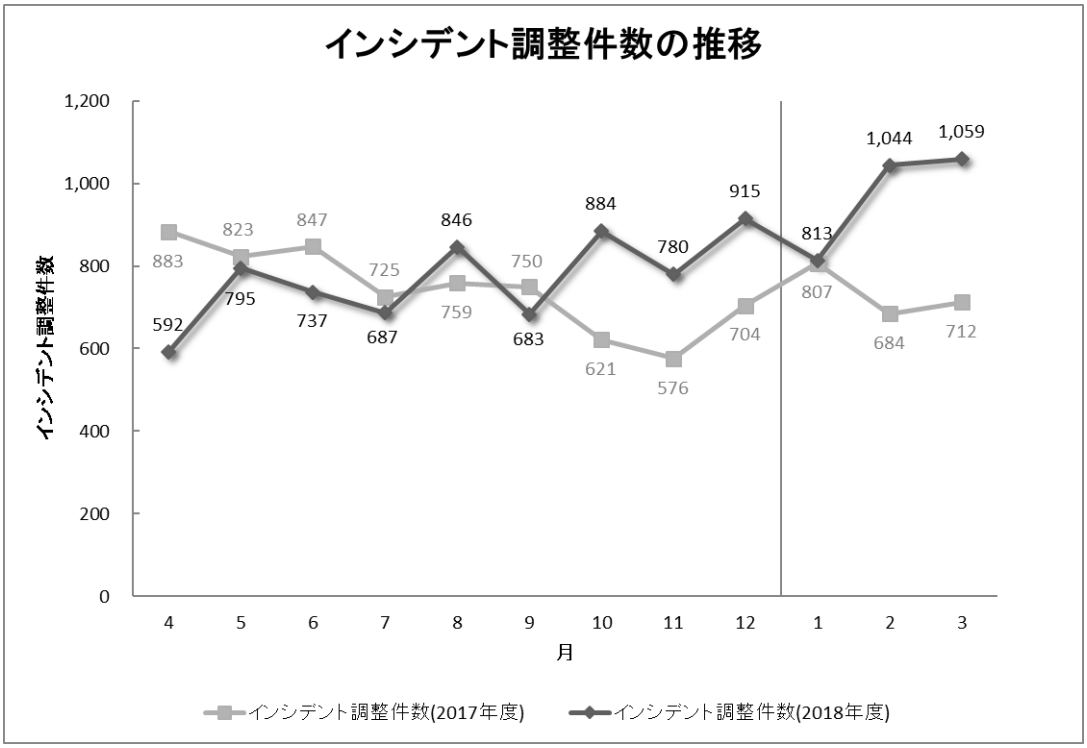
本四半期に寄せられた報告件数は、4,433 件でした。このうち、JPCERT/CC が国内外の関連するサイトとの調整を行った件数は 2,916 件でした。前四半期と比較して、報告件数は 5%増加し、調整件数は 13%

増加しました。また、前年同期と比較すると、報告数で 17%増加し、調整件数は 32%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］

【参考】統計情報の年度比較

2018 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	2014	2015	2016	2017	2018
報告件数	22,255	17,342	15,954	18,141	16,398

2018 年度に寄せられた報告件数は 16,398 件でした。前年度の 18,141 件と比較して、10%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。

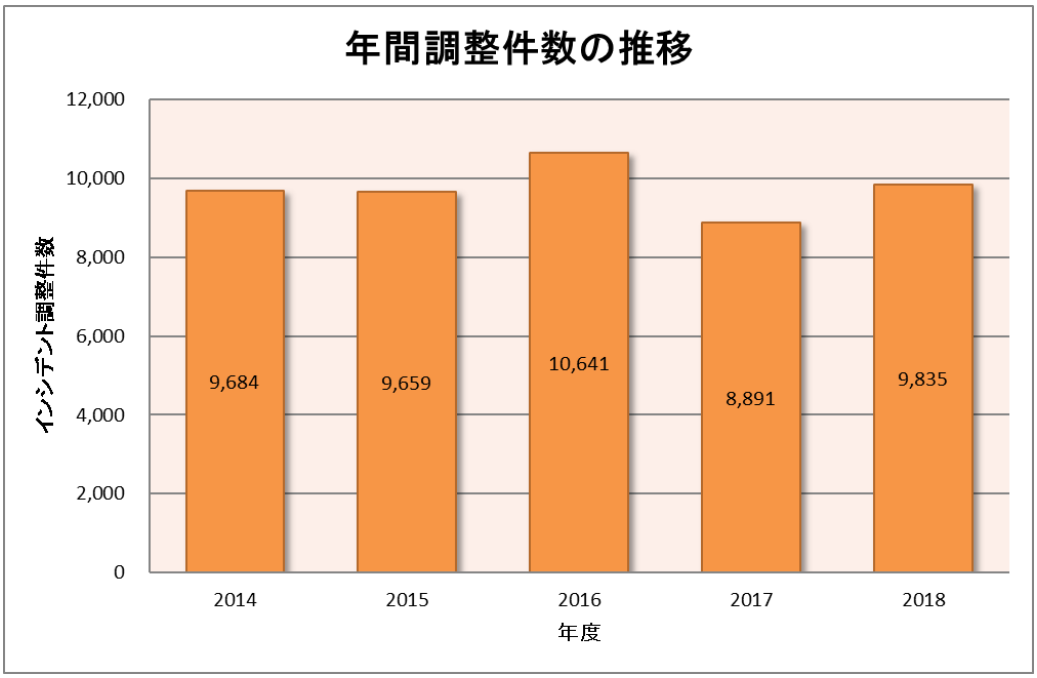
［図 3 年間報告件数の推移（年度比較)］

2018 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: 年間調整件数の推移］

年度	2014	2015	2016	2017	2018
調整件数	9,684	9,659	10,641	8,891	9,835

2018 年度に調整を行った件数は 9,835 件でした。前年度の 8,891 件と比較して、11%増加しています。［図 4］に過去 5 年間の年間調整件数の推移を示します。



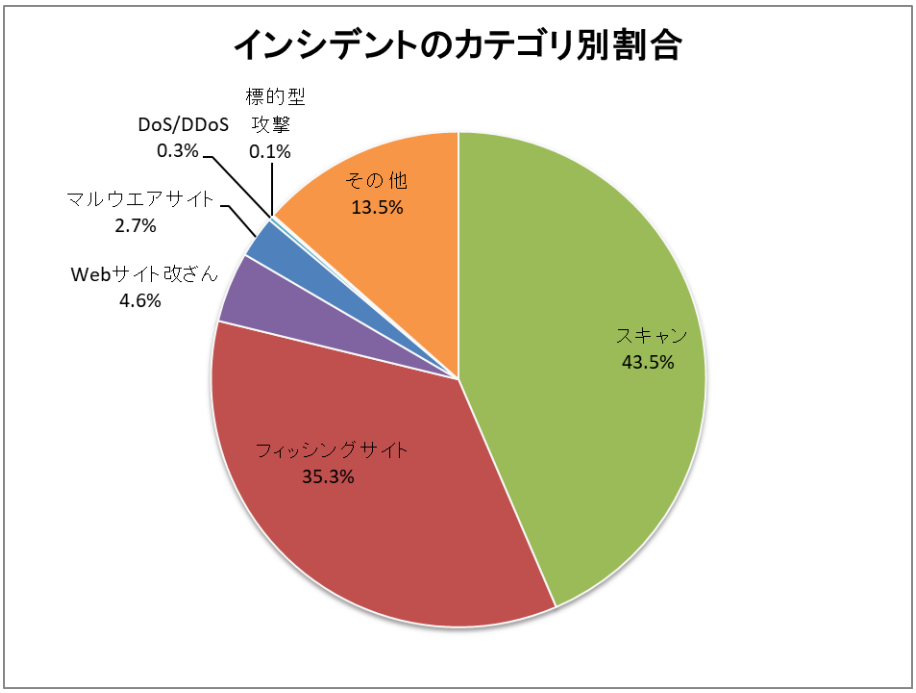
［図 4 年間調整件数の推移（年度比較）］

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。本四半期の報告に含まれる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］

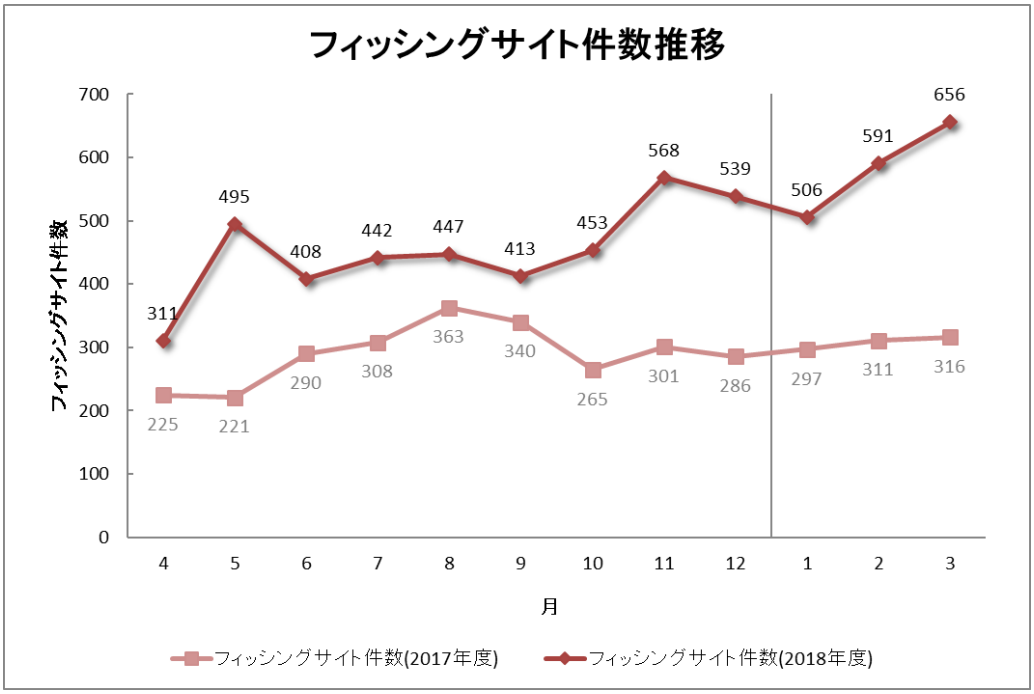
インシデント	1 月	2 月	3 月	合計	前四半期合計
フィッシングサイト	506	591	656	1,753	1,560
Web サイト改ざん	43	126	60	229	242
マルウエアサイト	25	33	78	136	75
スキャン	838	587	740	2,165	1,677
DoS/DDoS	9	4	0	13	7
制御システム関連	0	0	0	0	0
標的型攻撃	1	3	2	6	4
その他	227	218	225	670	923

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 43.5%、フィッシングサイトに分類されるインシデントが 35.3%を占めています。

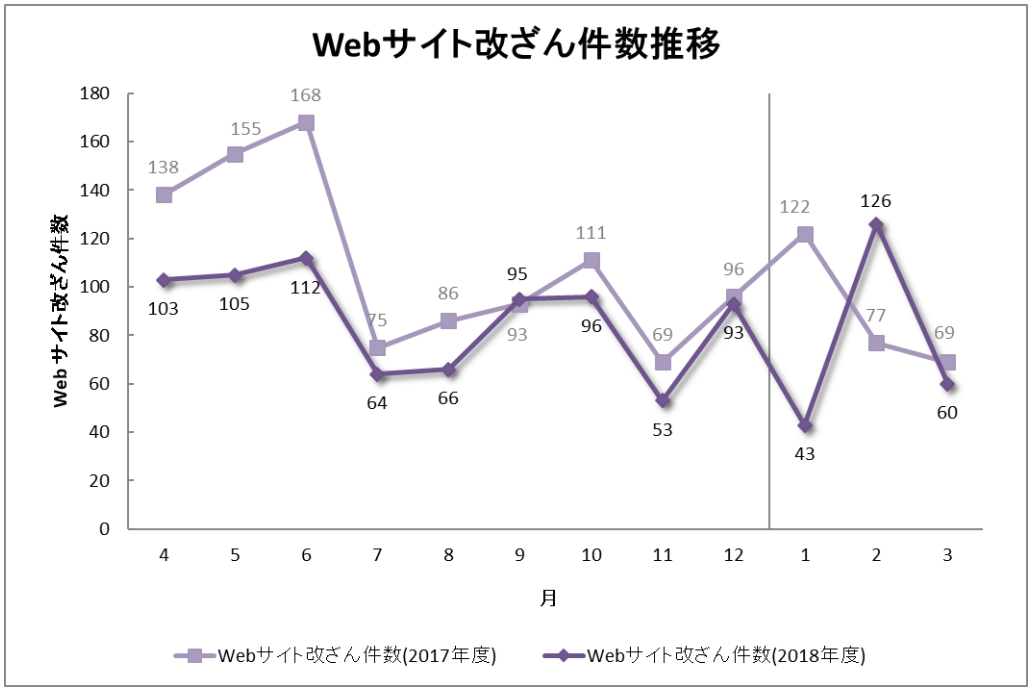


［図 5 インシデントのカテゴリ別割合］

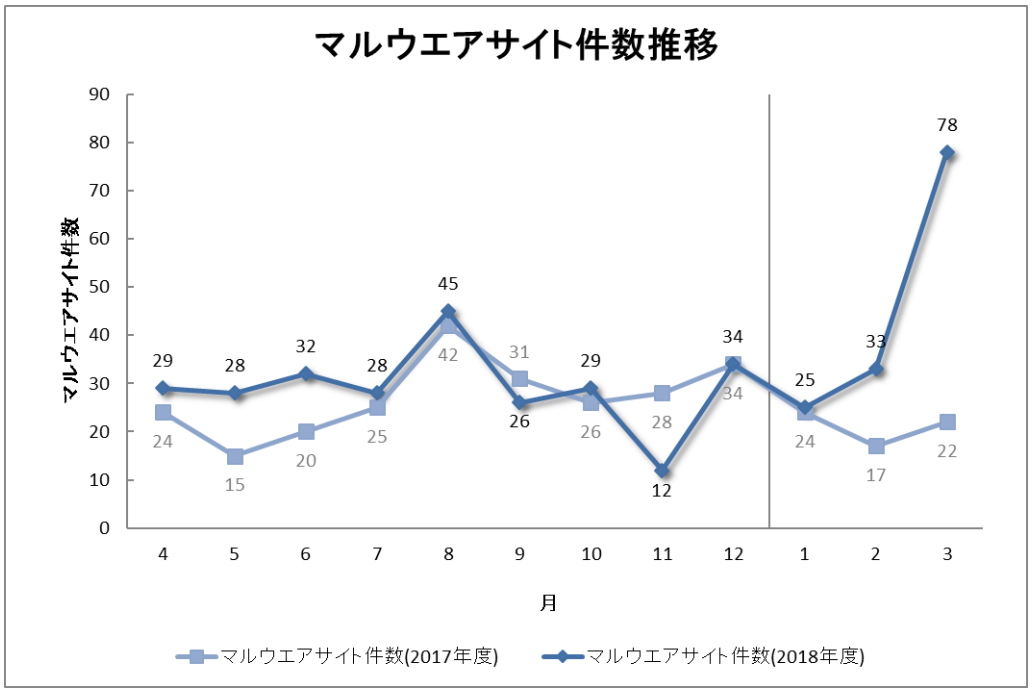
［図 6］から［図 9］に、フィッシングサイト、Web サイト改ざん、マルウエアサイト、スキャンのインシデントの過去 1 年間の月別推移を示します。



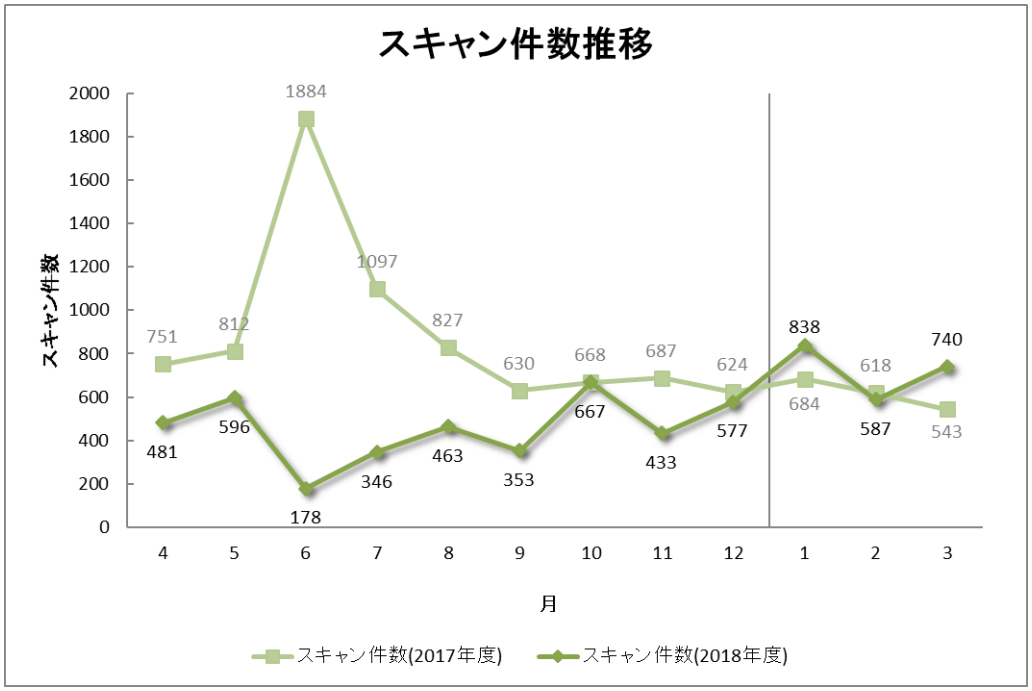
［図 6 フィッシングサイト件数の推移］



［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］にインシデントのカテゴリごとの件数および調整・対応状況を示します。

［図 10 インシデントのカテゴリごとの件数と調整・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

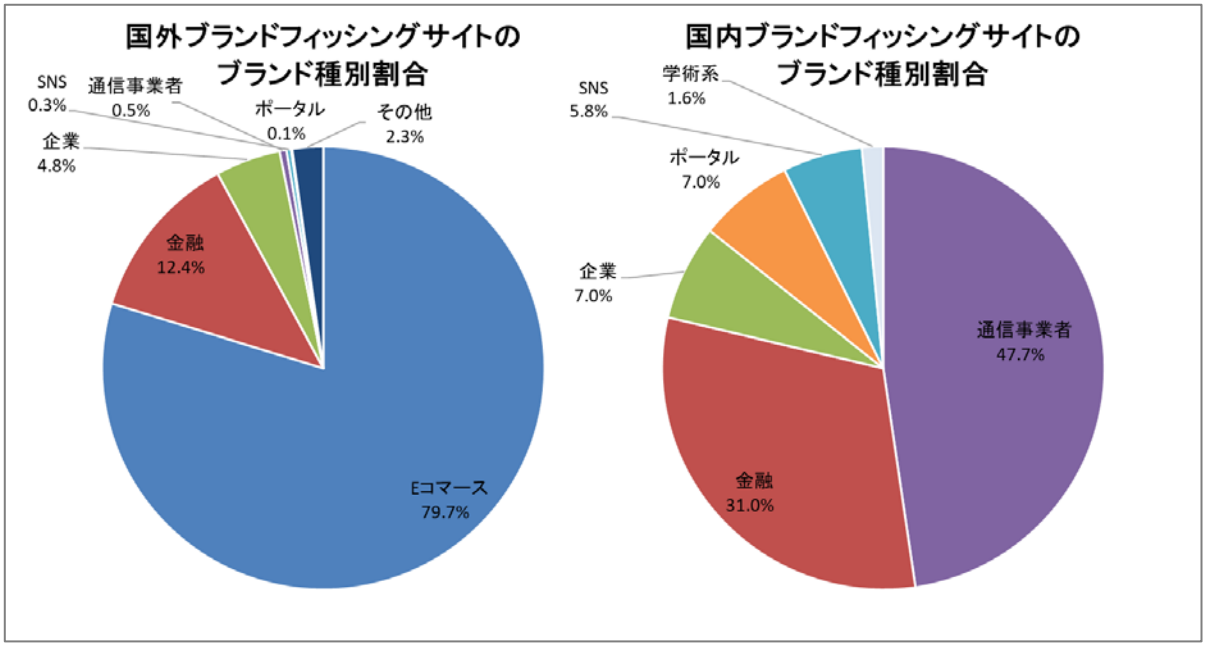
本四半期に報告が寄せられたフィッシングサイトの件数は 1,753 件で、前四半期の 1,560 件から 12%増加しました。また、前年度同期（924 件）との比較では、65%の増加となりました。

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件数が 258 件となり、前四半期の 282 件から 9%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 1198 件となり、前四半期の 985 件から 22%増加しました。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］、国内・国外ブランドの業界別の内訳を［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	98	72	88	258(15%)
国外ブランド	301	430	467	1,198(68%)
ブランド不明 (注 5)	107	89	101	297(17%)
全ブランド合計	506	591	656	1,753(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（国内・国外別）］

JPCERT/CC が報告を受けたフィッシングサイトの内訳では、国外ブランドでは E コマースサイトを装ったものが 79.7%、国内ブランドでは通信事業者のサイトを装ったものが 47.7%で最多でした。

E コマースサイトを装ったフィッシングサイトに関する報告は前四半期よりも多く寄せられています。中でも特定の国外ブランドのフィッシングサイトの報告数が一年前と比較して倍増し、全体の半数以上を占めるに到りました。
国外ブランドのフィッシングサイトに使われるドメインは約半数が.com ドメインで中には日本語ドメインや日本語 TLD の「.コム」ドメインを使用したものもありました。
また、短縮 URL サービスを利用してフィッシングサイトへ転送されるケースも多く報告があり、中には複数の短縮 URL サービスを経由した後にフィッシングサイトへ転送されるケースもありました。

国内ブランドのフィッシングサイトでは SNS を装ったフィッシングサイトが前四半期に比べて減少しましたが、金融機関や通信事業者を装ったフィッシングサイトについては増加傾向にありました。

金融機関を装ったフィッシングサイトについてはブランド名の後ろに co や cojp などの文字列を加えたものに.com, .org.などの gTLD や.eu, .it, .za などの ccTLD など様々な TLD を組み合わせたドメインが使用されていました。
また、中には定期的にサイトの稼働と停止を繰り返すものもありました。

通信事業者を装ったフィッシングサイトについては大半が台湾の IP アドレス上で稼働しており、ドメイン名については正規サイトと似た紛らわしい.com ドメインを使用したものが多く、そのほとんどが中国のレジストラで取得されたものでした。

フィッシングサイトの調整先の割合は、国内が 21%、国外が 79%であり、前四半期（国内が 28%、国外が 72%）と比べて国外への通知の割合が増加しました。

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、229 件でした。前四半期の 242 件から 5%減少しています。

2 月頃から、改ざんされた Web サイトから次のような URL の Web ページを経由し、不審なサイトに転送されるといった報告が複数寄せられています。

```
https[:]//somelandingpage[.]com/3gGykjDJ?frm=script&#038;
```

上記 URL の Web ページへの転送は、改ざんされたページの至る所に埋め込まれた JavaScript によって行われ､約 50 もの同一の改ざんコードが挿入されているページも確認しました｡改ざんされていた HTML ソースの例を［図 12］に示します。

［図 12 改ざんされた Web ページの HTML ソースに埋め込まれた JavaScirpt］

改ざんされた Web サイトからの転送先として、不審なブログサイトや、不審なソフトウエアをダウンロードさせる Web サイトなどを確認しています。この不正な転送は、次のような.tk ドメインの URL をもつものを含む、複数の Web サイトを経由する特徴があります。

```
http://<ドメイン名>.tk/index/?<数字の列>
```

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 4 件から 50%増加しています。本四半期に対応を依頼した組織は 3 組織でした。次に、確認されたインシデントを紹介します。

(1) 資産管理ソフトウエアの脆弱性を悪用した新たなマルウエアの感染を試みる標的型攻撃

2018 年 3 月以前から、資産管理ソフトウエアの脆弱性を悪用して xxmm や Datper と呼ばれるマルウエアに感染させる攻撃がありましたが、2019 年 1 月に、JavaScript で作成された新たなマルウエアに感染させる攻撃の報告が寄せられました。このマルウエアは Node.js を使って動作し、HTTP で C&C サーバと通信します。C&C サーバから受信する命令により、任意のコマンドの実行や、ファイルのアップロード・ダウンロード、感染した端末の情報を送信する可能性があります。

(2) DNS の A レコードを利用して通信を行う Cobalt Strike

ペネトレーションテストツール Cobalt Strike を悪用した攻撃の報告が 2019 年 2 月に寄せられました。Cobalt Strike は HTTP,HTTPS の他、DNS プロトコルを利用して C&C サーバと通信する機能を持っており、今回の攻撃では DNS の A レコードの問合せと応答を用いて C&C サーバと通信を行っていました。

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、136 件でした。前四半期の 75 件から 81%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、2,165 件でした。前四半期の 1,677 件から 29%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 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)）、HTTP（80/TCP）、microsoft-ds（445/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	255	205	271	731
80/tcp	111	66	121	298
445/tcp	120	84	56	260
23/tcp	18	76	116	210
53/udp	188	0	0	188
25/tcp	47	71	48	166
1433/tcp	42	14	1	57
3306/tcp	0	0	47	47
222/tcp	0	13	30	43
2222/tcp	1	12	27	40
22222/tcp	0	9	27	36
5555/tcp	11	17	6	34
37215/tcp	12	9	9	30
443/tcp	14	12	1	27
81/tcp	10	9	3	22
8080/tcp	17	3	2	22
9000/tcp	11	6	0	17
8443/tcp	12	5	0	17
3389/tcp	6	4	4	14
2323/tcp	4	2	8	14
2004/tcp	0	14	0	14
8181/tcp	5	4	1	10
その他	39	25	20	84
月別合計	923	660	798	2381

その他に分類されるインシデントの件数は、670 件でした。前四半期の 923 件から 27%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。

(1) マルウエア「Ursnif」への感染を狙うメールに関する対応

本四半期も継続してマルウエア Ursnif への感染を狙うメールに関する報告が多く寄せられました。このメールには、悪意のあるマクロが含まれた Microsoft Office ドキュメントが添付されています。マクロは、最終的に Ursnif をダウンロードし、端末上で実行します。

添付ファイルに含まれるマクロには、実行端末の言語環境を検知するコードが含まれており、日本語環境の利用者を狙っていることが確認されています。また、このマクロがダウンロードする Ursnif は画像共有サイトにアップロードされていました。画像共有サイトにはステガノグラフィを用いて Ursnif などのファイルを埋め込んだ画像ファイルが設置されていました。

JPCERT/CC では、不審なコンテンツが設置された画像共有サイトのサービス管理者へ適切に対応するように依頼しました。また、マルウエアへの感染が疑われるホストの IP アドレスに関する情報を入手し、当該 IP アドレスの管理者へ適切に対応するように依頼しました。

(2) 通信事業者のサービスを装ったマルウエア配布サイトに関する対応

前四半期には、宅配事業社の Web サイト[2]を模倣して Android マルウエアを配布する Web サイトに関する報告が寄せられましたが、本四半期はそれに加えて通信事業者の Web サイトを模倣したものも 3 月初旬より確認しています。この Web サイトは Android マルウエアを配布するのに加えて、Apple 社のフィッシングサイトへの誘導も行っていました。これらの模倣サイトに利用されているドメインは前四半期と同様に継続的に同一レジストラから取得されていることを確認しております。

JPCERT/CC は、IP アドレスの管理者並びに当該国の National CSIRT に適切に対応を行うよう依頼しました。また、模倣サイトに利用されるドメインのレジストラにも適切に対応を行うように依頼しました。

5. 参考文献

(1) 気象庁｜報道発表資料
気象庁発表の警報等を装った迷惑メールにご注意下さい
https://www.jma.go.jp/jma/press/1811/08c/WARNmail.html

(2) IPA 安心相談窓口だより
宅配便業者をかたる偽ショートメッセージに関する相談が急増中
https://www.ipa.go.jp/security/anshin/mgdayori20180808.html

(3) ヤマト運輸
ヤマト運輸の名前を装った迷惑メールにご注意ください
http://www.kuronekoyamato.co.jp/ytc/info/info_181212.html

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 30 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。