JPCERT/CC インシデント報告対応レポート

2020 年 10 月 1 日 ～ 2020 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

2021 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 3
2. 四半期の統計情報 3
3. インシデントの傾向 9
3.1. フィッシングサイトの傾向 9
3.2. Web サイト改ざんの傾向 11
3.3. 標的型攻撃の傾向 12
3.4. その他のインシデントの傾向 13
4. インシデント対応事例 14
付録-1. インシデントの分類 17

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ー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、2020 年 10 月 1 日から 2020 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、コンピューター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］

	10 月	11 月	12 月	合計	前四半期合計
報告件数 (注 2)	4,517	3,684	4,865	13,066	13,831
インシデント件数 (注 3)	2,883	2,087	2,459	7,429	8,386
調整件数 (注 4)	1,523	1,232	1,465	4,220	4,807

（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。

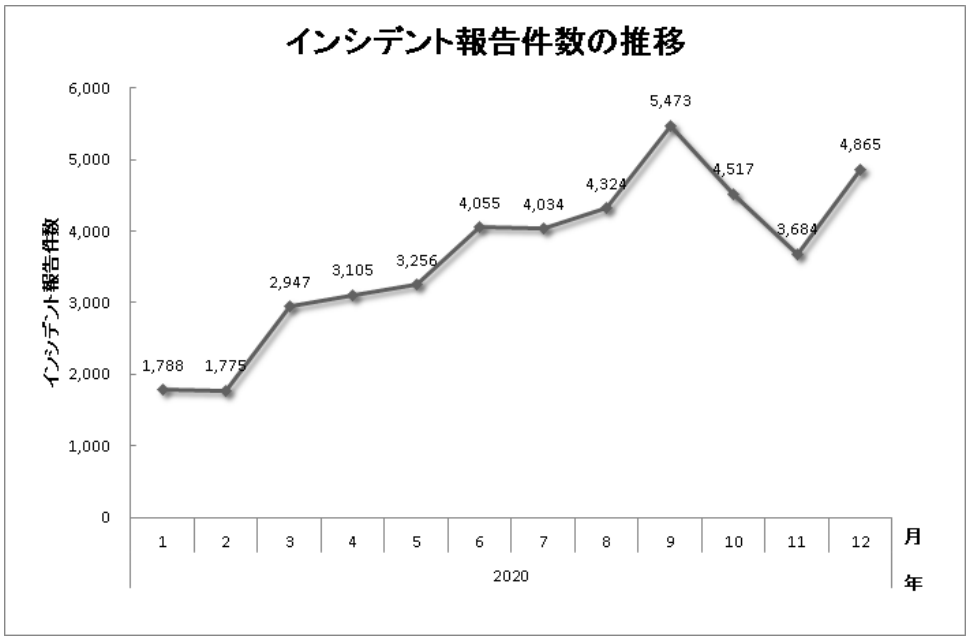
（注 3）「インシデント件数」は、各報告に含まれるインシデント件数の合計を示します。1 つのインシデントに関して複数件の報告が寄せられた場合にも、1 件として扱います。

（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。

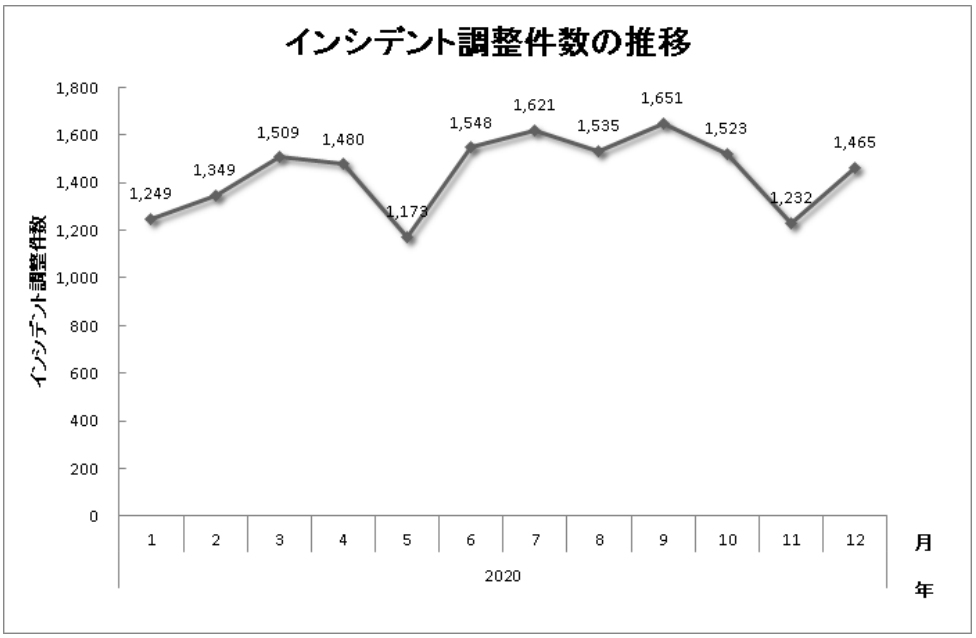
本四半期に寄せられた報告件数は、13,066 件でした。このうち、JPCERT/CC が国内外の関連するサイトとの調整を行った件数は 4,220 件でした。前四半期と比較して、報告件数は 6%減少し、調整件数は 11%減少しました。また、前年同期と比較すると、報告数は 152%増加し、調整件数は 20%増加しまし

た。

［図 1］と［図 2］に報告件数および調整件数の過去 1 年間の月次の推移を示します。



［図 1：インシデント報告件数の推移］

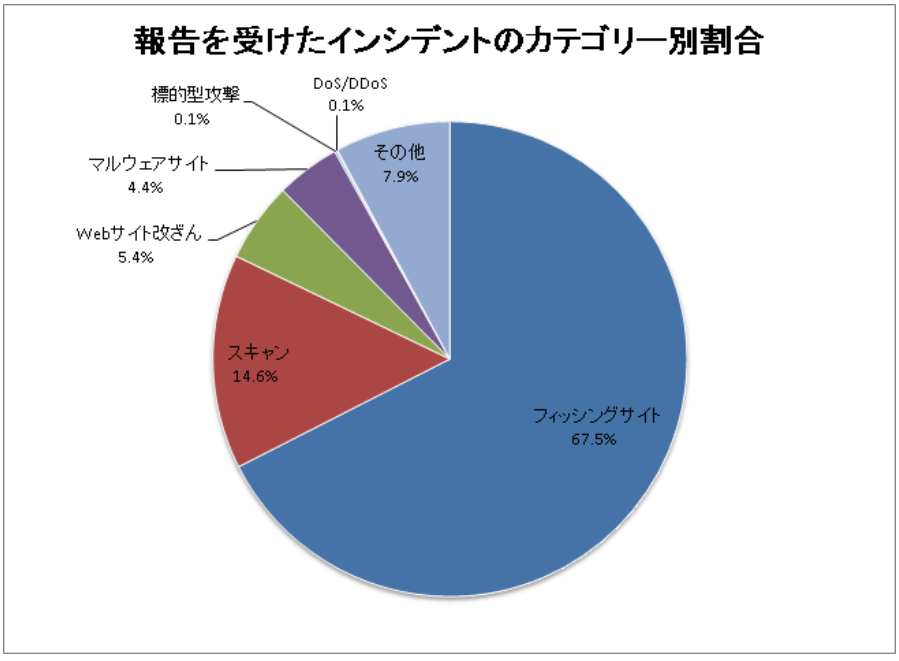


［図 2：インシデント調整件数の推移］

JPCERT/CC では、報告を受けたインシデントをカテゴリー別に分類し、各インシデントカテゴリーに応じた調整、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インシデントの件数のカテゴリーごとの内訳を［表 2］に示します。また、内訳を割合で示すと［図 3］のとおりです。

［表 2：報告を受けたインシデントのカテゴリーごとの内訳］

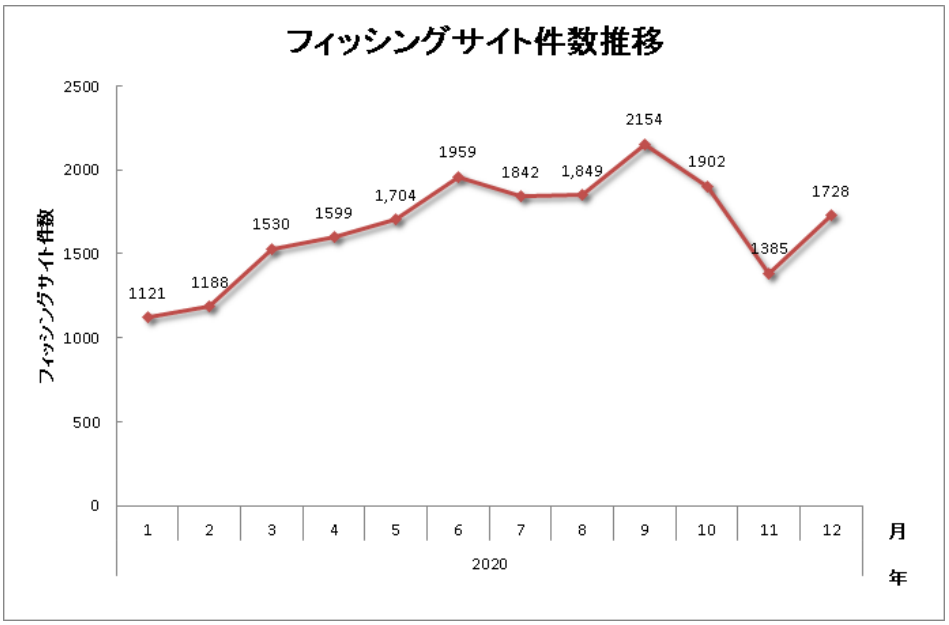
インシデント	10 月	11 月	12 月	合計	前四半期合計
フィッシングサイト	1,902	1,385	1,728	5,015	5,845
Web サイト改ざん	198	135	71	404	374
マルウェアサイト	82	143	99	324	158
スキャン	381	312	393	1,086	1,380
DoS/DDoS	5	0	0	5	8
制御システム関連	0	0	0	0	0
標的型攻撃	7	3	0	10	16
その他	308	109	168	585	605



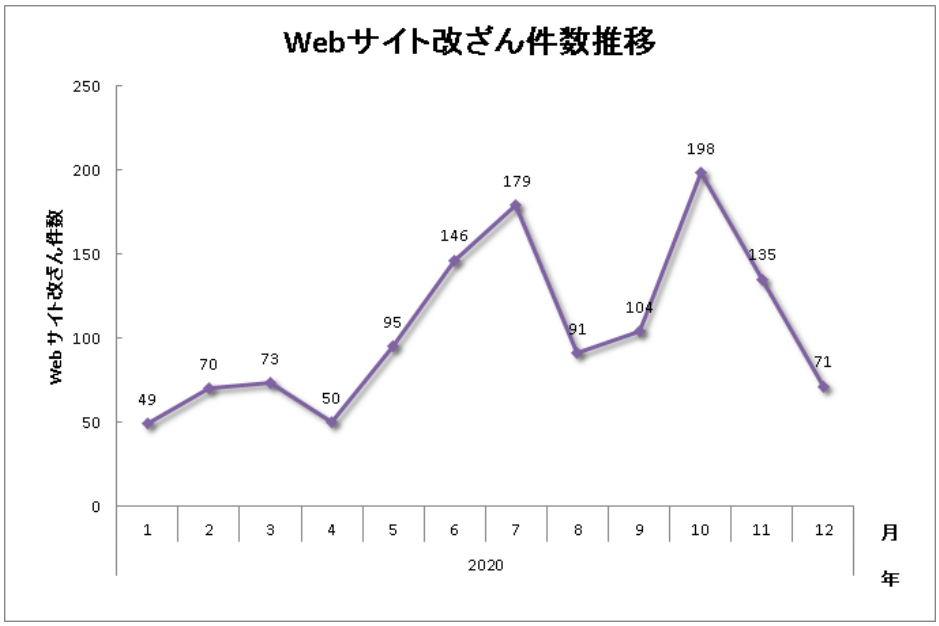
［図 3：報告を受けたインシデントのカテゴリー別割合］

フィッシングサイトに分類されるインシデントが 67.5%、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 14.6%を占めています。

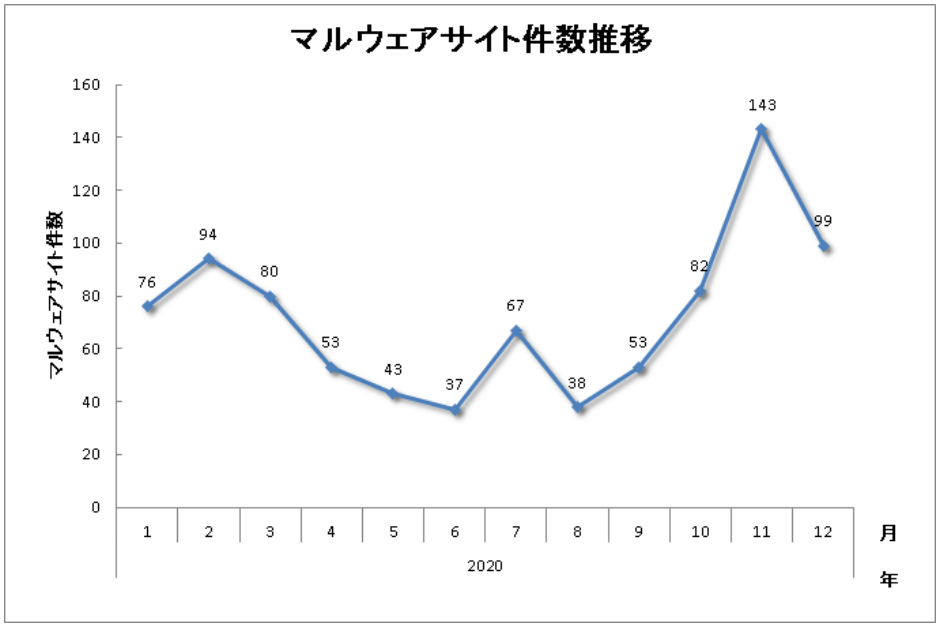
［図 4］から［図 7］に、フィッシングサイト、Web サイト改ざん、マルウェアサイト、スキャンのインシデントの過去 1 年間の月次の推移を示します。



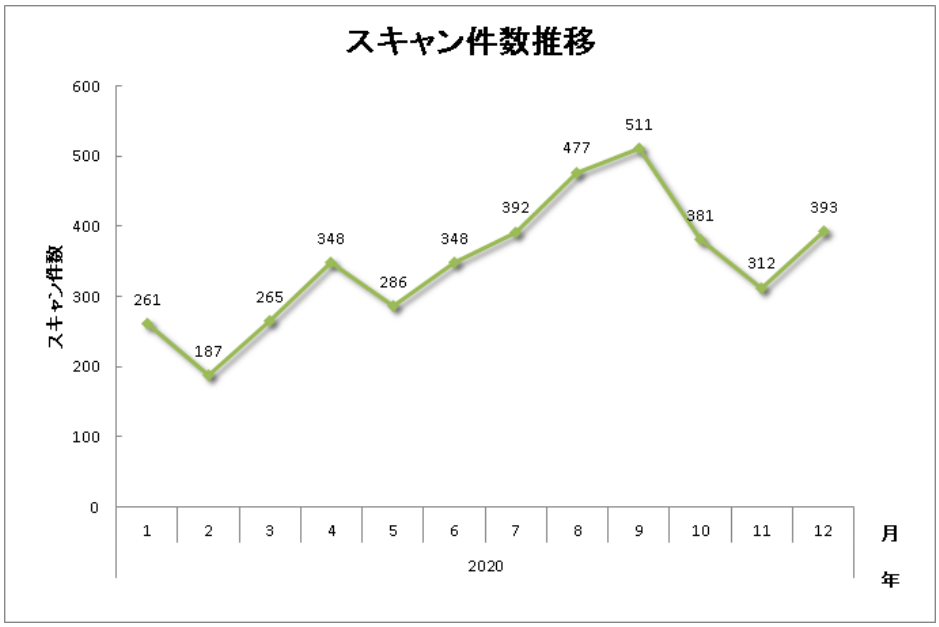
［図 4：フィッシングサイト件数の推移］



［図 5：Web サイト改ざん件数の推移］

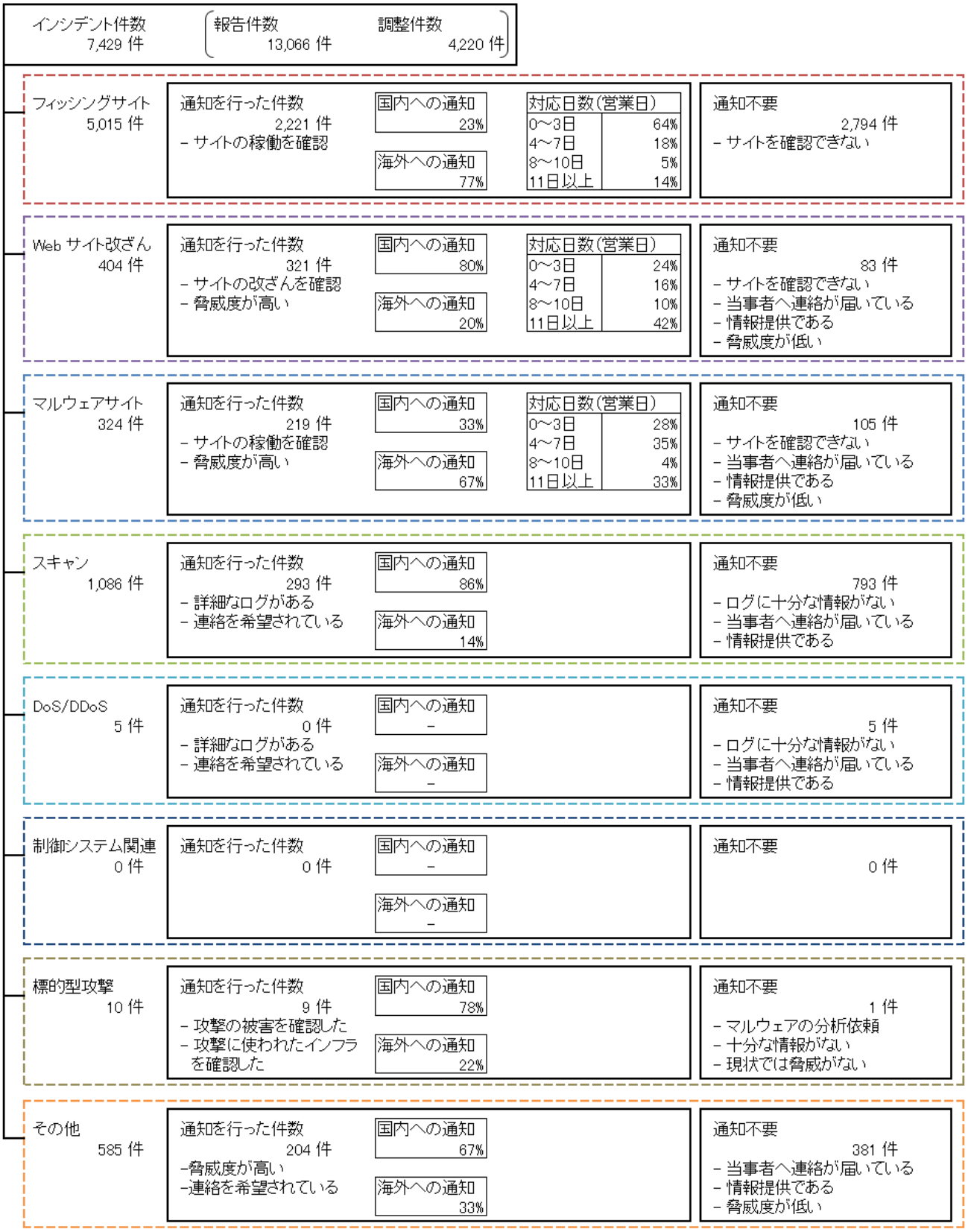


［図 6：マルウェアサイト件数の推移］



［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ー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ーごとの件数と調整・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

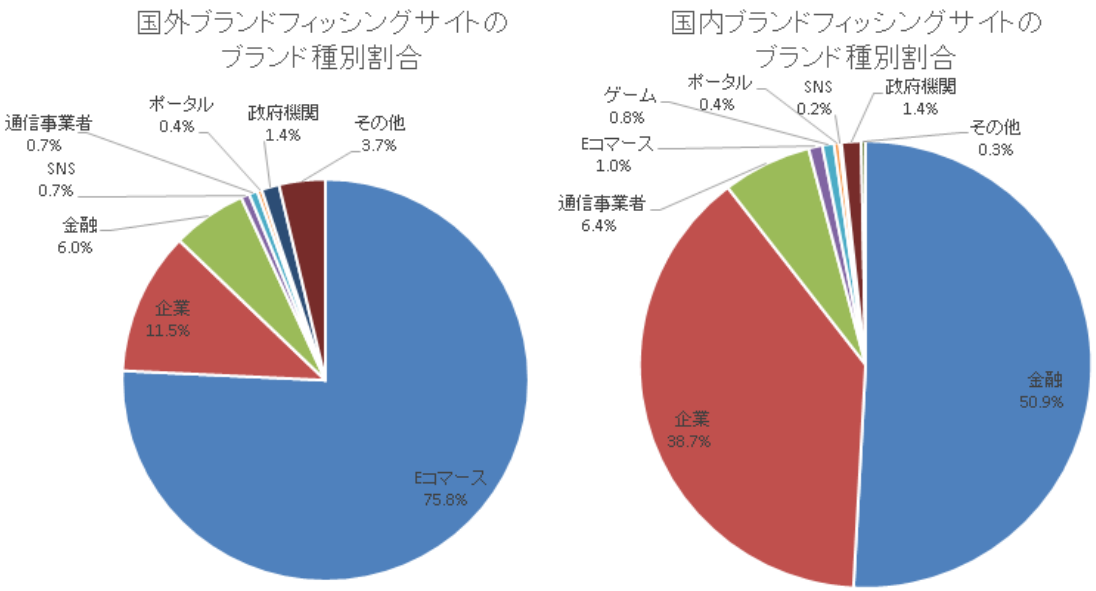
本四半期に報告が寄せられたフィッシングサイトの件数は 5,015 件で、前四半期の 5,845 件から 14%減少しました。また、前年度同期（3,700 件）との比較では、36%の増加となりました。

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 2,635 件となり、前四半期の 2,043 件から 29%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 1,629 件となり、前四半期の 3,122 件から 48%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	931	777	927	2,635(53%)
国外ブランド	697	385	547	1,629(32%)
ブランド不明 (注 5)	274	223	254	751(15%)
全ブランド合計	1,902	1,385	1,728	5,015

（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 75.8%、国内ブランドでは金融機関のサイトを装ったものが 50.9%で，それぞれ最も多くを占めました。

国外ブランドは特定の通販サイトを装ったフィッシングサイトが多い状況は前四半期と同じですが、国内ブランドは金融機関のサイトを装ったフィッシングサイトが急増しています。

また、本四半期には新型コロナウイルス感染症対策における特別定額給付金の給付を騙ったフィッシングサイトの報告が多数寄せられました。これは特別給付金に関する特別サイトが開設されたという内容のメールでフィッシングサイトへ誘導し、個人情報やクレジットカード情報を入力させるだけではなく、運転免許証やパスポートなどの本人確認書類のコピーをアップロードさせようとするものでした。

このフィッシングサイトの URL には総務省の Web サイトに似せた kyufukin.soumu.go.jp や soumu-go-jp などの文字列が使われ、一見しただけでは偽物かどうかの判断に迷うようなものが多く見受けられました。

［図 10：特別定額給付金の給付を騙ったフィッシングサイト］

フィッシングサイトの調整先の割合は、国内が 23%、国外が 77%であり、前四半期（国内が 29%、国外が 71%）と比べて国外への調整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、404 件でした。前四半期の 374 件から 8%増加しています。

本四半期は、改ざんされた Web サイトから、特定ブランドを扱う E コマースサイトに誘導される事例が複数寄せられました。改ざんされた Web サイトには不正な JavaScript ファイルが設置されており、［図 11］のようなスクリプトタグでブラウザーに読み込まれるようになっていました。

```
<html>
<script type="text/javascript" src="promk.js"></script>
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8" />
<title>[redacted]</title>
<meta name="keywords" content="[redacted]" />
<meta name="description" content="[redacted]
<meta name="viewport" content="width=device-width, user-scalable=yes, initial-scale=1, minimum-scale=1, maximum-scale=3">
<meta property="og:title" content="[redacted]
<meta property="og:type" content="website">
<meta property="og:url" content="#">
<meta property="og:image" content="[redacted]" />
<meta property="og:description" content="[redacted]
<meta property="fb:app_id" content="[redacted]">
<base href="[redacted]" />
<script type="text/javascript" src="http://[redacted]/jss/promk1.js"></script>
<link href="/common/css/base.css" rel="stylesheet" type="text/css" media="screen, print" />
```

［図 11：不正な JavaScript ファイルが埋め込まれたページ］

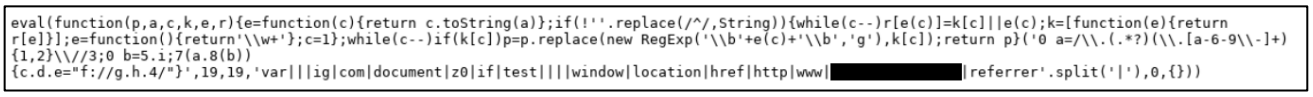
また、［図 12］、［図 13］および［図 14］は設置された不正な JavaScript ファイルの例です。JavaScript の難読化アルゴリズムの違いによって見かけは異なっていますが、いずれも Referrer の値をチェックし、検索エンジンからのアクセスの場合のみ、E コマースサイトに誘導するようになっています。

```
var s = document.referrer;
if (s.indexOf("google") > 0 || s.indexOf("bing") > 0 || s.indexOf("yahoo") > 0 || s.indexOf("aol") > 0) {
        window.location.href = 'http://[redacted]'
}
```

［図 12：不正な JavaScript ファイル例 1］

```
var PCeWEea$1$ = ['[redacted]',
"\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 n$E2$fXU2 = PCeWEea$1$[0];var JeZaGj3$msV3 = PCeWEea$1$[1];var b4 = window[PCeWEea$1$[2]]
[PCeWEea$1$[3]];if (b4) {       var orOebziI5 = JeZaGj3$msV3[PCeWEea$1$[4]](PCeWEea$1$[5]);     for (i = 0x0; i < orOebziI5[PCeWEea$1$[6]]; i++) {
if (b4[PCeWEea$1$[7]](orOebziI5[i]) > 0x0) {                    top[PCeWEea$1$[8]][PCeWEea$1$[9]] = n$E2$fXU2          }       }}
```

［図 13：不正な JavaScript ファイル例 2］



［図 14：不正な JavaScript ファイル例 3］

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 16 件から 38%減少しています。次に、確認されたインシデントを紹介します。

(1) Lazarus グループによる攻撃

本四半期も Lazarus（別名 Hidden Cobra）と呼ばれる攻撃グループによる国内組織を狙った標的型攻撃の報告が引き続き寄せられました。確認された攻撃は、SNS 経由で対象組織の個人を標的にマルウェアに感染させようとする不正なリンクを送信するものでした。組織のネットワーク内への直接的な攻撃ではなく、個人が使用する SNS から侵入することで、標的とする組織に気づかれないように組織内ネットワークに侵入しようとする意図が感じられます。

Lazarus が使用するマルウェアについては、JPCERT/CC Eyes で詳細を解説しています。

攻撃グループ Lazarus がネットワーク侵入後に使用するマルウェア
https://blogs.jpcert.or.jp/ja/2020/08/Lazarus_malware.html

攻撃グループ Lazarus が使用するマルウェア BLINDINGCAN
https://blogs.jpcert.or.jp/ja/2020/09/BLINDINGCAN.html

(2) SSL-VPN 製品の脆弱性を突いた攻撃

本四半期に報告された標的型攻撃の中には、SSL-VPN 製品の脆弱性を突いて侵入した事案が含まれていました。攻撃者は、国内組織の海外拠点に設置された SSL-VPN 製品の脆弱性を侵入経路とし、SigLoader(1)と呼ばれる新種のマルウェアを使用して、攻撃を行っていました。

2019 年より、さまざまな SSL-VPN 製品の脆弱性が公表されており、これらを狙った攻撃が引き続き活発に行われています。標的型攻撃だけでなく、金銭目的のランサムウェア攻撃にも悪用されており、この傾向は今後も続くと考えられます。パッチ管理の徹底とログの確認を推奨します。

Pulse Connect Secure の脆弱性を狙った過去の攻撃事案については JPCERT/CC Eyes で詳細を解説しています。

Pulse Connect Secure の脆弱性を狙った攻撃事案
https://blogs.jpcert.or.jp/ja/2020/03/pulse-connect-secure.html

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ェアサイトの数は 324 件でした。前四半期の 158 件から 105%増加しています。

本四半期に報告が寄せられたスキャン件数は 1,086 件でした。前四半期の 1,380 件から 21%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	143	134	145	422
25/tcp	96	68	42	206
80/tcp	62	37	88	187
143/tcp	17	24	38	79
23/tcp	23	11	10	44
62223/tcp	16	15	12	43
445/tcp	8	13	20	41
443/tcp	1	10	29	40
5555/tcp	18	2	0	20
37215/tcp	2	6	6	14
3389/tcp	4	2	6	12
1433/tcp	2	2	8	12
8080/tcp	4	2	5	11
26/tcp	2	0	9	11
8081/tcp	1	1	4	6
2323/tcp	1	0	4	5
5500/tcp	0	2	2	4
81/tcp	1	2	0	3
3306/tcp	1	1	1	3
その他	8	13	18	39
月別合計	410	345	447	1202

その他に分類されるインシデントの件数は、585 件でした。前四半期の 605 件から 3%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) Fortinet 社製 FortiOS の SSL VPN 機能の脆弱性の影響を受けるホストについての対応

2020 年 11 月中旬、FortiOS の任意のファイル読み取りの脆弱性 (CVE-2018-13379) の影響を受けるホストの一覧がフォーラムなどで公開されていることを確認しました。この一覧にはホストの IP アドレスの他に、SSL-VPN 接続を利用するためのアカウント名や平文のパスワードの情報が含まれていました。

JPCERT/CC では、この情報をもとに国内の当該 IP アドレスの管理者に対して、アカウントのパスワードの変更、要素認証の導入、および利用している機器のバージョンの確認、さらに脆弱なバージョンを利用している場合は機器のバージョンアップなどをするよう連絡しました。

また、本件に関して注意喚起を発行しました。

Fortinet 社製 FortiOS の SSL VPN 機能の脆弱性 (CVE-2018-13379) の影響を受けるホストに関する情報の公開について
https://www.jpcert.or.jp/newsflash/2020112701.html

(2) マルウェア IcedID に関する報告への対応

本四半期には、マルウェア IcedID に感染させることを狙ったなりすましメールが複数報告されました。このなりすましメールの特徴は次のとおりで、Emotet の感染拡大手法と酷似しています。

- メールの本文が日本語で書かれている
- 過去にやり取りされたメールへの返信を装っている
- パスワード付き ZIP ファイルが添付されている
- ZIP ファイルの中身はマクロが含まれた Word 文書ファイル（マクロを有効にするとマルウェアに感染する）

JPCERT/CC では、SNS で注意喚起をするとともに、なりすまされたメールアカウントの持ち主に対し、メールアカウントが不正に使用されていないかの確認やパスワードの変更を依頼しました。

Twitter: Analysis Center (@jpcert_ac)
https://twitter.com/jpcert_ac/status/1324561915738091522

5. 参考文献

(1) 株式会社ラック
【緊急レポート】Microsoft 社のデジタル署名ファイルを悪用する「SigLoader」による標的型攻撃を確認
https://www.lac.co.jp/lacwatch/report/20201201_002363.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ェアによって、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。

- 攻撃者やマルウェ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

○ マルウェアサイト

「マルウェアサイト」とは、閲覧することで PC がマルウェ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ェアを公開しているサイトを指します。

JPCERT/CC では、以下を「マルウェアサイト」に分類しています。

- 閲覧者の PC をマルウェアに感染させようとするサイト
- 攻撃者によりマルウェアが公開されているサイト

○ スキャン

「スキャン」とは、サーバーや 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、マルウェ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）
- マルウェア（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ーや 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ー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ェアが通信を行うサーバー
- 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、マルウェ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、マルウェ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、マルウェ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ェアが通信を行うサーバー

○ 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ェアによる情報の窃取
- マルウェア（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、「令和２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。