JPCERT/CC インシデント報告対応レポート

2020 年 7 月 1 日 ～ 2020 年 9 月 30 日

一般社団法人 JPCERT コーディネーションセンター

2020 年 10 月 15 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 7 月 1 日から 2020 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）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］

	7 月	8 月	9 月	合計	前四半期合計
報告件数 (注 2)	4,034	4,324	5,473	13,831	10,416
インシデント件数 (注 3)	2,640	2,600	3,146	8,386	7,123
調整件数 (注 4)	1,621	1,535	1,651	4,807	4,201

（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。

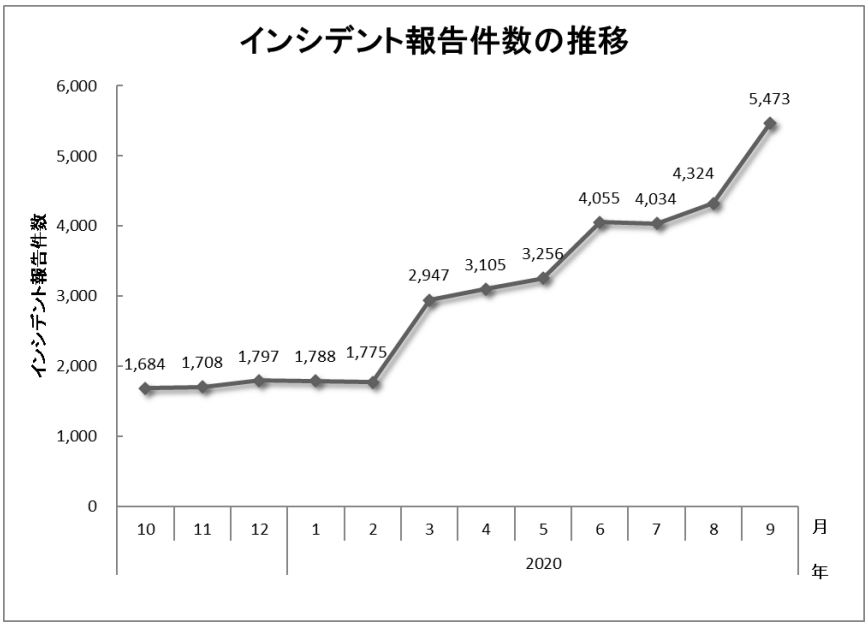
（注 3）「インシデント件数」は、各報告に含まれるインシデント件数の合計を示します。1 つのインシデントに関して複数件の報告が寄せられた場合にも、1 件として扱います。

（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。

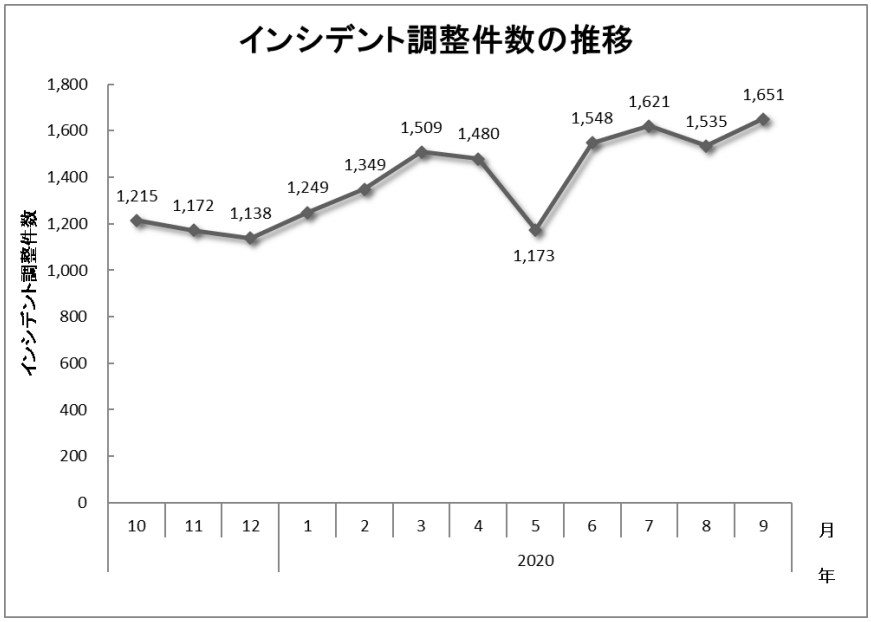
本四半期に寄せられた報告件数は、13,831 件でした。このうち、JPCERT/CC が国内外の関連するサイトとの調整を行った件数は 4,807 件でした。前四半期と比較して、報告件数は 33%増加し、調整件数は

14%増加しました。また、前年同期と比較すると、報告数は 200%増加し、調整件数は 16%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］



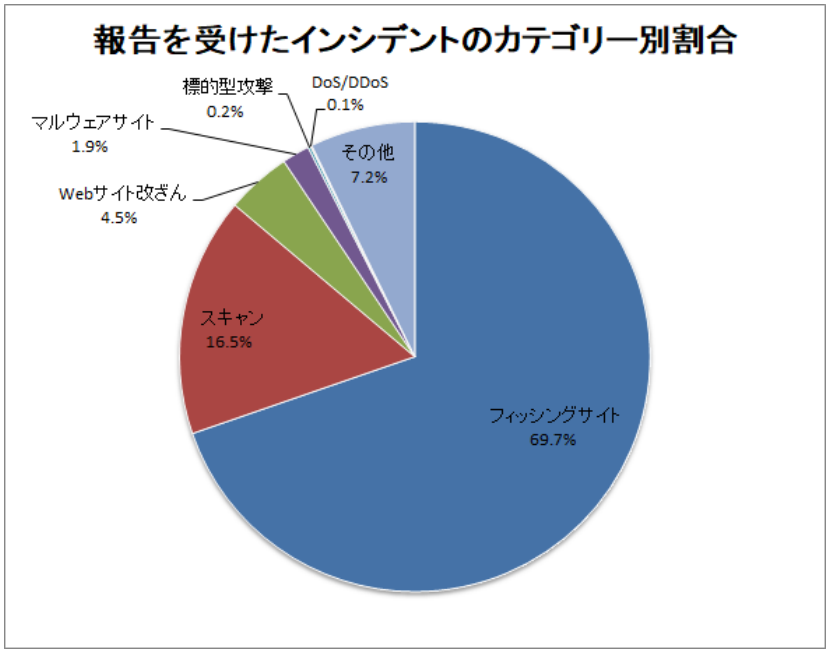
［図 2：インシデント調整件数の推移］

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］

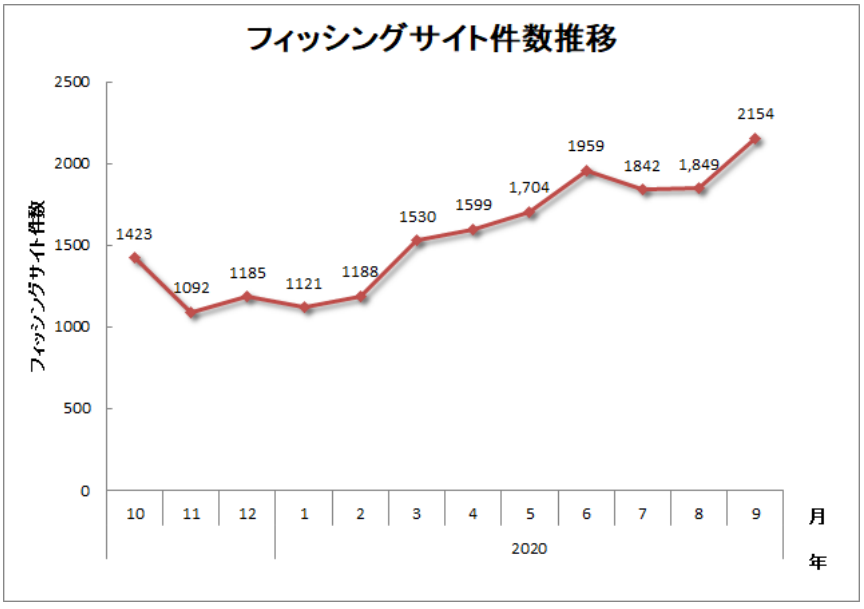
インシデント	7 月	8 月	9 月	合計	前四半期合計
フィッシングサイト	1,842	1,849	2,154	5,845	5,262
Web サイト改ざん	179	91	104	374	291
マルウェアサイト	67	38	53	158	133
スキャン	392	477	511	1,380	982
DoS/DDoS	4	4	0	8	70
制御システム関連	0	0	0	0	0
標的型攻撃	10	1	5	16	6
その他	146	140	319	605	379



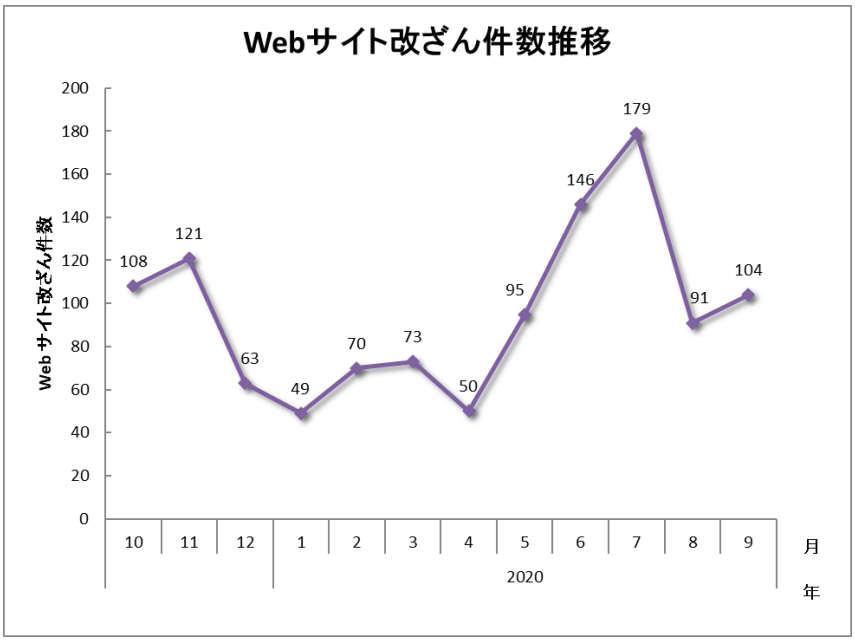
［図 3：報告を受けたインシデントのカテゴリー別割合］

フィッシングサイトに分類されるインシデントが 69.7%、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 16.5%を占めています。

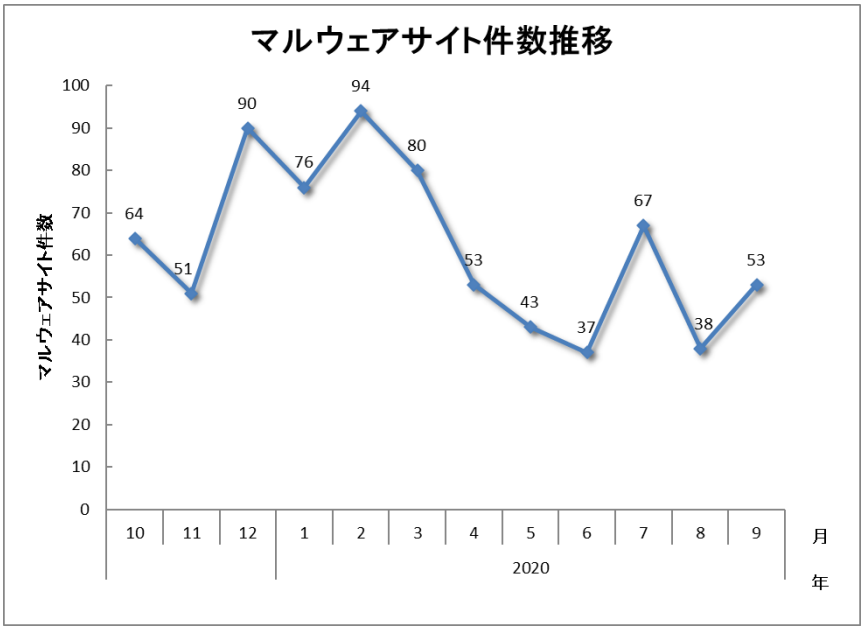
［図 4］から［図 7］に、フィッシングサイト、Web サイト改ざん、マルウェアサイト、スキャンのインシデントの過去 1 年間の月次の推移を示します。



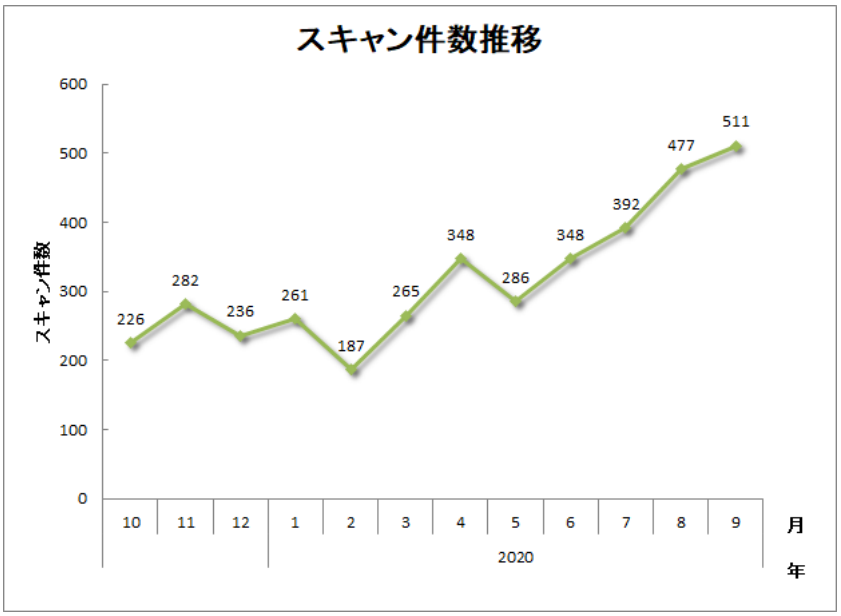
［図 4：フィッシングサイト件数の推移］



［図 5：Web サイト改ざん件数の推移］

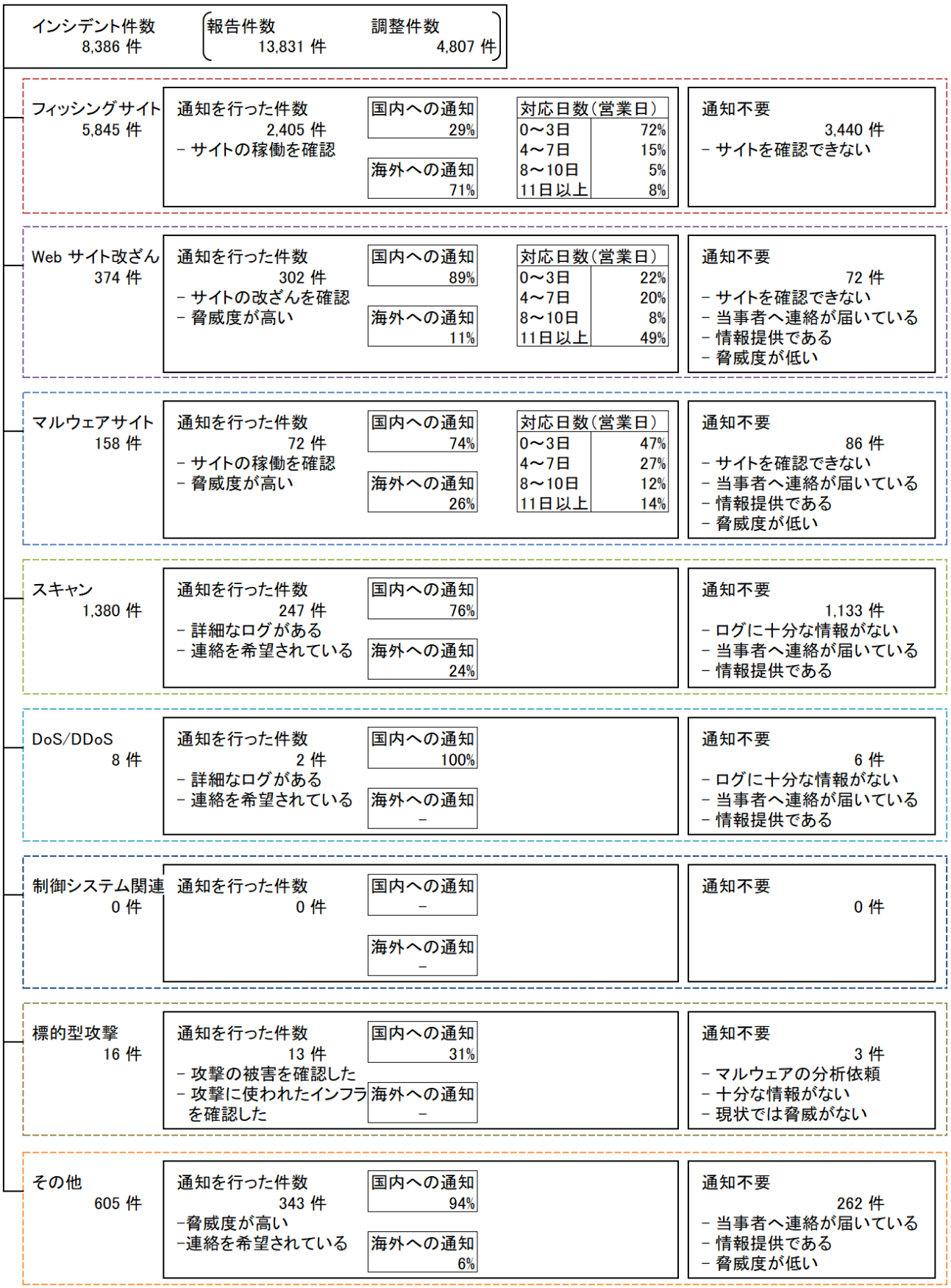


［図 6：マルウェアサイト件数の推移］



［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

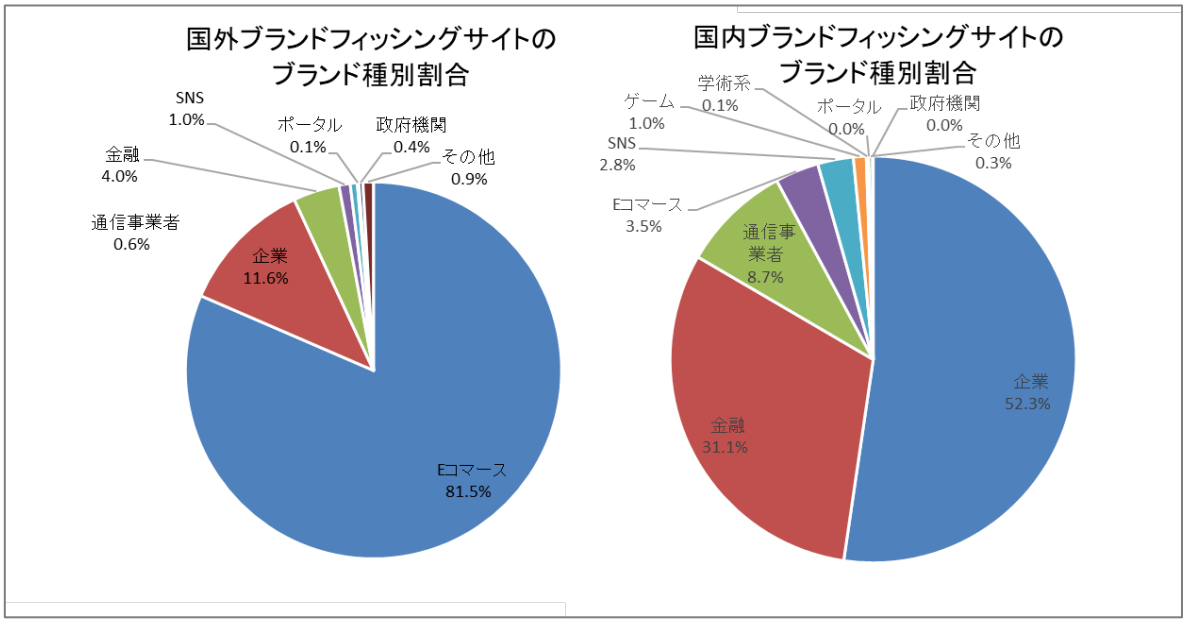
本四半期に報告が寄せられたフィッシングサイトの件数は 5,845 件で、前四半期の 5,262 件から 11%増加しました。また、前年度同期（3,457 件）との比較では、69%の増加となりました。

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 2,043 件となり、前四半期の 1,489 件から 37%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 3,122 件となり、前四半期の 3,265 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	7 月	8 月	9 月	本四半期合計（割合）
国内ブランド	590	607	846	2,043(35%)
国外ブランド	1,089	1,047	986	3,122(53%)
ブランド不明 (注 5)	163	195	322	680(12%)
全ブランド合計	1,842	1,849	2,154	5,845

（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。



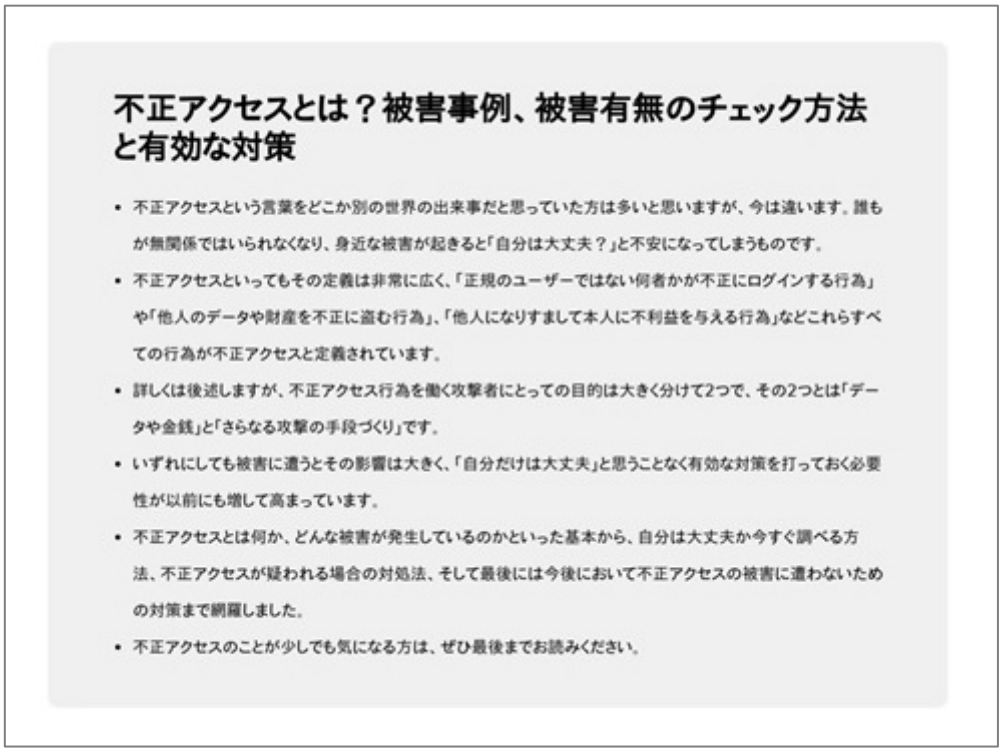
［図 9：フィッシングサイトのブランド種別割合（国内・国外別）］

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 81.5%、国内ブランドでは企業のサイトを装ったものが 52.3%で，それぞれ最も多くを占めました。

国外ブランドについても国内ブランドについても、それぞれ特定の通販サイトを装ったフィッシングサイトのログイン画面を装ったものが非常に多く、ともに過半数を占めています。

その他に国内ブランドでは、国内の銀行やクレジットカード会社のオンラインサービスや、インターネットサービスプロバイダーなどが提供する Web メールのログイン画面を装ったものが増加傾向にありました。
また、フィッシングサイトのドメインには、正規サイトのドメインやブランド名に英数字を加えた.com や.top、.cn、 .xyz ドメインが多く使われていました。

一部の国内の銀行を装ったフィッシングサイトの中には、PC 上のブラウザーからアクセスすると、スマートフォン等でアクセスした時とは異なる次のようなコンテンツを表示させるものもありました。



［図 10：PC 上のブラウザーからアクセスした際に表示されるコンテンツ］

フィッシングサイトの調整先の割合は、国内が 29%、国外が 71%であり、前四半期（国内が 50%、国外が 50%）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、374 件でした。前四半期の 291 件から 29%増加しています。

本四半期は、改ざんされた Web サイトから、次のような URL で示される Web サイトを経由し、不審なサイトに転送される報告が複数寄せられました。

```
https[:]//somelandingpage[.]live/?utm_campaign=<ランダムな英数字>&t=main7d
```

この転送は、検索エンジン経由でアクセスを行った場合にのみ発生し、Web ページに直接アクセスを行った場合には、無害なコンテンツが表示されるようになっていました。［図 11］は、改ざんされた Web ページを検索エンジン経由でアクセスした際に表示されるコンテンツの例です。

```
<html>
  <head>
    <META http-equiv="refresh" content="1;URL=https://thvedroisil6.live/?utm_campaign=[redacted]&t=main7d">
   <script>
   window.location = "https://thvedroisil6.live/?utm_campaign=[redacted]&t=main7d";
   </script>
  </head>
  <body>
  To the new location please <a href="https://thvedroisil6.live/?utm_campaign=[redacted]&t=main7d"><b>click here.</b></a>
  </body>
</html>
```

［図 11：転送コードの例］

今回報告のあった事例では、最終的に当選詐欺の Web サイトや、不審な商品販売サイトなどが表示されることを確認しています。

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、16 件でした。前四半期の 6 件から 167%増加しています。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

本四半期には、Lazarus（Hidden Cobra とも言われる）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寄せられました。攻撃には、ネットワーク侵入時には、侵入するために使われたマルウェアとは異なるものによって攻撃が行われていました。また、ネットワーク内で感染を広げるために、攻撃者は GitHub などで公開されているフリーのツールなどを使用していました。ネットワーク侵入後に使われ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

(2) マルウェア Winnti を利用した攻撃

8 月頃に報告が寄せられた標的型攻撃ではマルウェア Winnti が使用されていました。複数のクラウドサーバーがマルウェア感染の被害にあっており、攻撃者が社内に設置されサーバーだけではなく、外部のクラウドサービスを利用したサーバーもターゲットにしていることがわかりました。

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ェアサイトの数は 158 件でした。前四半期の 133 件から 19%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 1,380 件でした。前四半期の 982 件から 41%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 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	7 月	8 月	9 月	合計
22/tcp	208	179	178	565
25/tcp	50	135	188	373
80/tcp	92	89	76	257
143/tcp	10	10	18	38
445/tcp	4	13	19	36
23/tcp	5	15	14	34
443/tcp	14	10	8	32
62223/tcp	8	9	8	25
1433/tcp	1	7	6	14
8080/tcp	1	4	3	8
9530/tcp	5	2	0	7
81/tcp	5	2	0	7
3306/tcp	1	4	1	6
8081/tcp	0	2	3	5
37215/tcp	0	1	4	5
3389/tcp	2	2	1	5
7547/tcp	0	2	2	4
60001/tcp	0	3	1	4
26/tcp	1	2	1	4
その他	11	9	11	31
月別合計	418	500	542	1460

その他に分類されるインシデントの件数は、605 件でした。前四半期の 379 件から 60%増加しています。

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) ランサムウェアに関する報告への対応

本四半期は国内の複数組織より、国内や海外の事業所内の端末がランサムウェアに感染し、ファイルが暗号化されたとの報告が寄せられました。JPCERT/CC では、暗号化されたファイルの拡張子などの特徴をもとに感染したマルウェアの種類を判断して、攻撃の特徴や手法などの情報を提供しました。
被害を受けた組織の中には、攻撃の際に窃取された情報を攻撃者の Web サイトに公開される事例も確認されました。

(2) マルウェア Emotet に関する報告への対応

活動を止めたと見られていたマルウェア Emotet が、2020 年 7 月中旬から活発化しました。JPCERT/CC には、Emotet により認証情報が窃取されたメールアカウントがスパムメールの送信に使用されているという報告や、国内の Web サイトが改ざんされ、Emotet が設置されているという報告が多数寄せられました。JPCERT/CC では、メールサーバーの管理者に対して、メールアカウントの不正使用の確認依頼や、Web サーバーの管理者に対して、改ざん箇所の調査と対応依頼を行いました。

また、確認した直近の事例をもとに「マルウエア Emotet への対応 FAQ」のコンテンツの更新と、変化した Emotet を検知するための EmoCheck V1.0 を 2020 年 8 月 11 日に公開しました。

マルウエア Emotet への対応 FAQ
https://blogs.jpcert.or.jp/ja/2019/12/emotetfaq.html

JPCERTCC/EmoCheck: Emotet detection tool for Windows OS
https://github.com/JPCERTCC/EmoCheck/releases

(3) サブドメイン乗っ取りに関する報告への対応

本四半期には、Subdomain Takeover と呼ばれる攻撃法により、サブドメインを乗っ取って不正なコンテンツを掲載した事案が興味深い事例として見られました。この攻撃法は、[図 12]に示したように CNAME レコードを利用して、サブドメイン（図の例では test.example.co.jp）の参照を CDN サービスのドメイン（図の例では test.example.net）に転送するように設定して運用していたものの、後になって CDN サービスの契約を解除したまま放置されているような状況で行われます。

```
;; QUESTION SECTION:
;test.example.co.jp.            IN      ANY

;; ANSWER SECTION:
test.example.co.jp.    3600    IN      CNAME   test.examle.net.
```

［図 12：悪用された CNAME レコード例］

攻撃者が同じドメインで CDN サービスの契約を結べば、放置されていたドメインが乗っ取られてしまいます。本四半期には、正規のサブドメインに見えるようなサイトで当選詐欺のページが最終的に表示されるとの報告が複数ありました。JPCERT/CC では、対象となったドメイン管理者に対して、CNAME レコードの修正などを依頼しました。

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。