JPCERT/CC インシデント報告対応レポート

2021 年 4 月 1 日 ～ 2021 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

2021 年 7 月 15 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、2021 年 4 月 1 日から 2021 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)	3,036	3,149	4,089	10,274	9,629
インシデント件数 (注 3)	2,399	2,299	2,279	6,977	7,108
調整件数 (注 4)	1,341	1,068	1,336	3,745	4,005

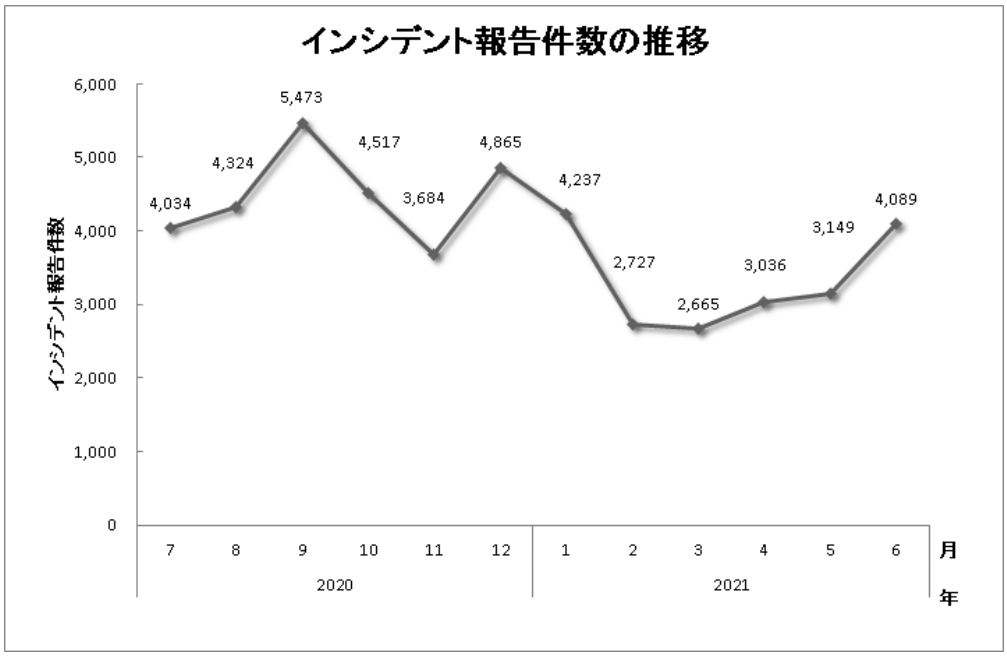
（注 2）「報告件数」は、報告者から寄せられた Web フォーム、メール、FAX による報告の総数を示します。

（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。

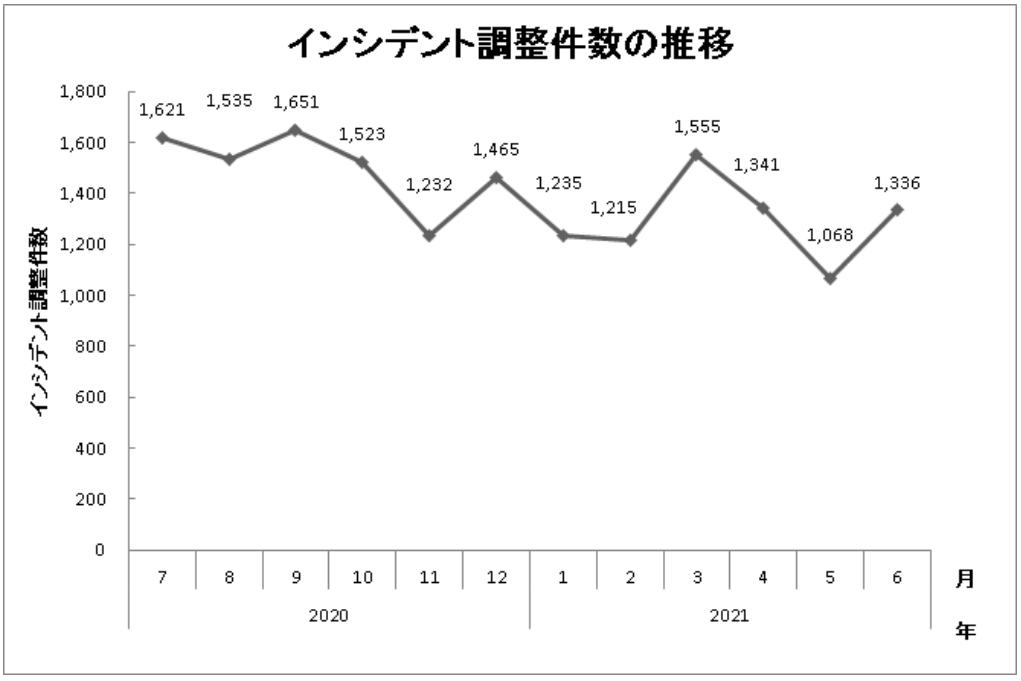
（注 4）「調整件数」は、インシデントの拡大防止のため、サイトの管理者等に対し、現状の調査と問題解決のための対応を依頼した件数を示します。

本四半期に寄せられた報告件数は、10,274 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 3,745 件でした。前四半期と比較して、報告件数は 7%増加し、調整件数は 6%減少しました。また、前年同期と比較すると、報告数は 1.4%減少し、調整件数は 11%減少しました。

［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］

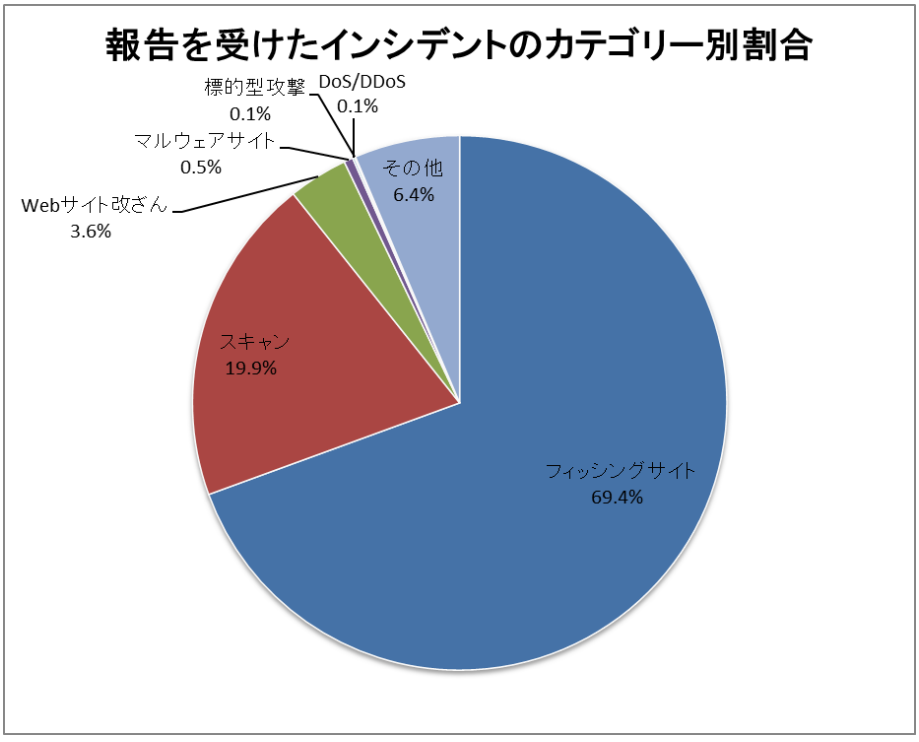


［図 2：インシデント調整件数の推移］

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］

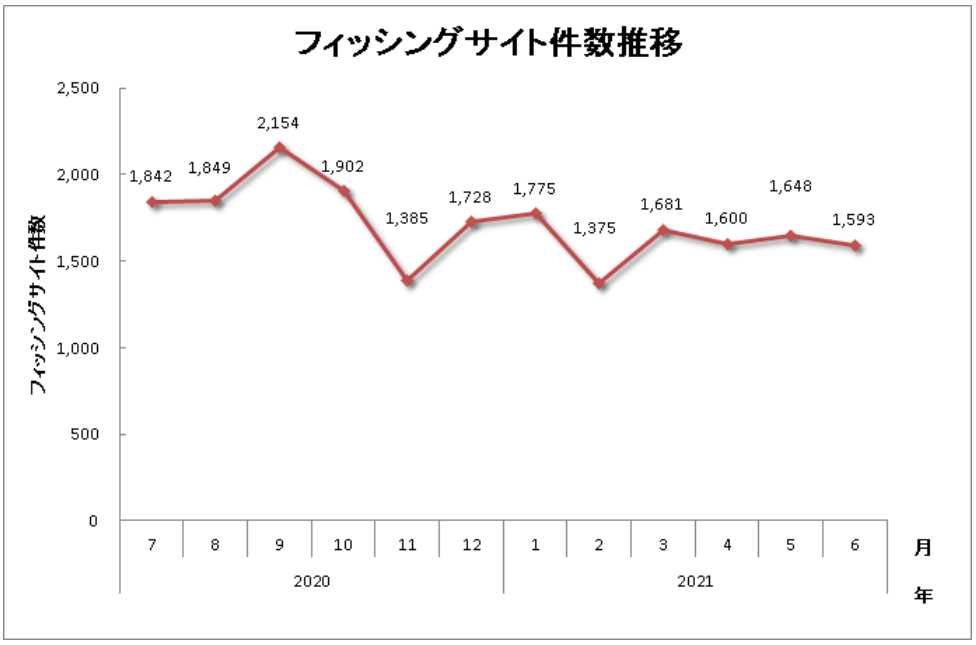
インシデント	4 月	5 月	6 月	合計	前四半期合計
フィッシングサイト	1,600	1,651	1,593	4,841	4,831
Web サイト改ざん	65	79	107	251	282
マルウェアサイト	12	8	18	38	138
スキャン	561	430	394	1,385	1,085
DoS/DDoS	3	4	1	8	2
制御システム関連	0	0	0	0	0
標的型攻撃	4	1	0	5	7
その他	154	126	166	449	763



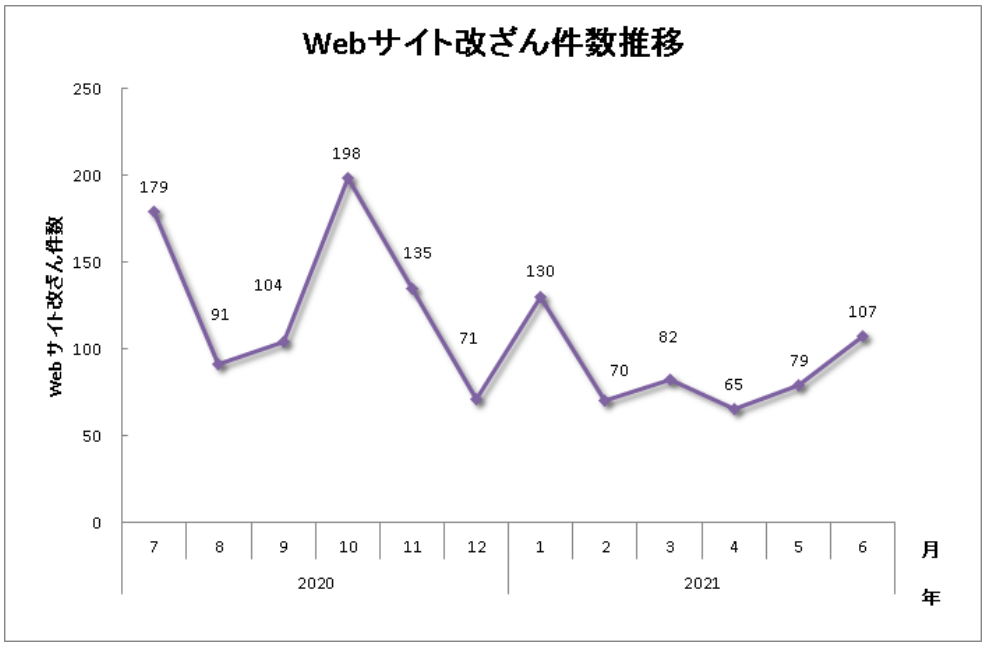
［図 3：報告を受けたインシデントのカテゴリー別割合］

フィッシングサイトに分類されるインシデントが 69.4%、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 19.9%を占めています。

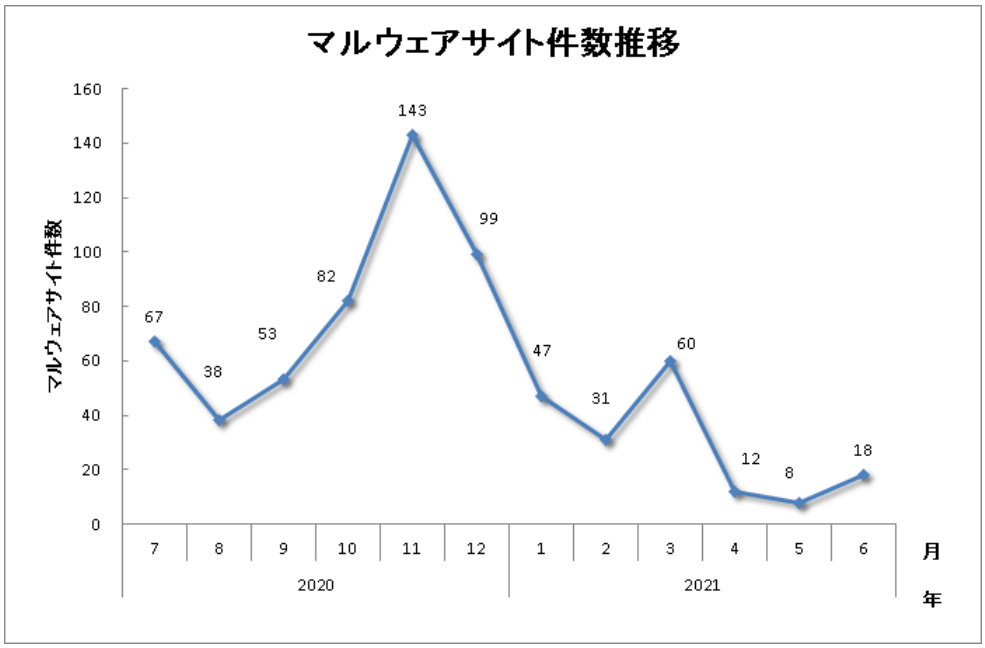
［図 4］から［図 7］に、フィッシングサイト、Web サイト改ざん、マルウェアサイト、スキャンのインシデントの過去 1 年間の月次の推移を示します。



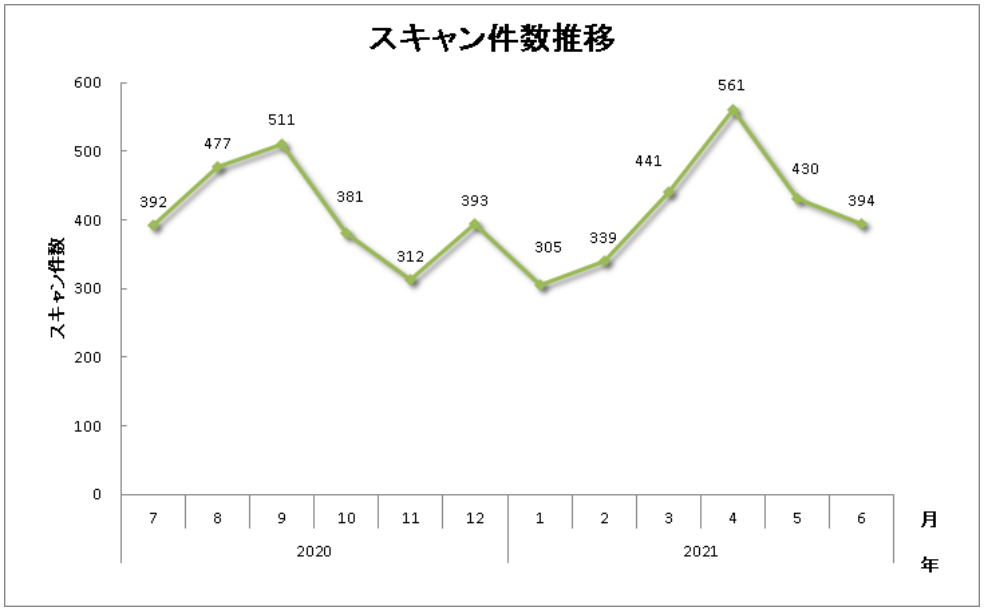
［図 4：フィッシングサイト件数の推移］



［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

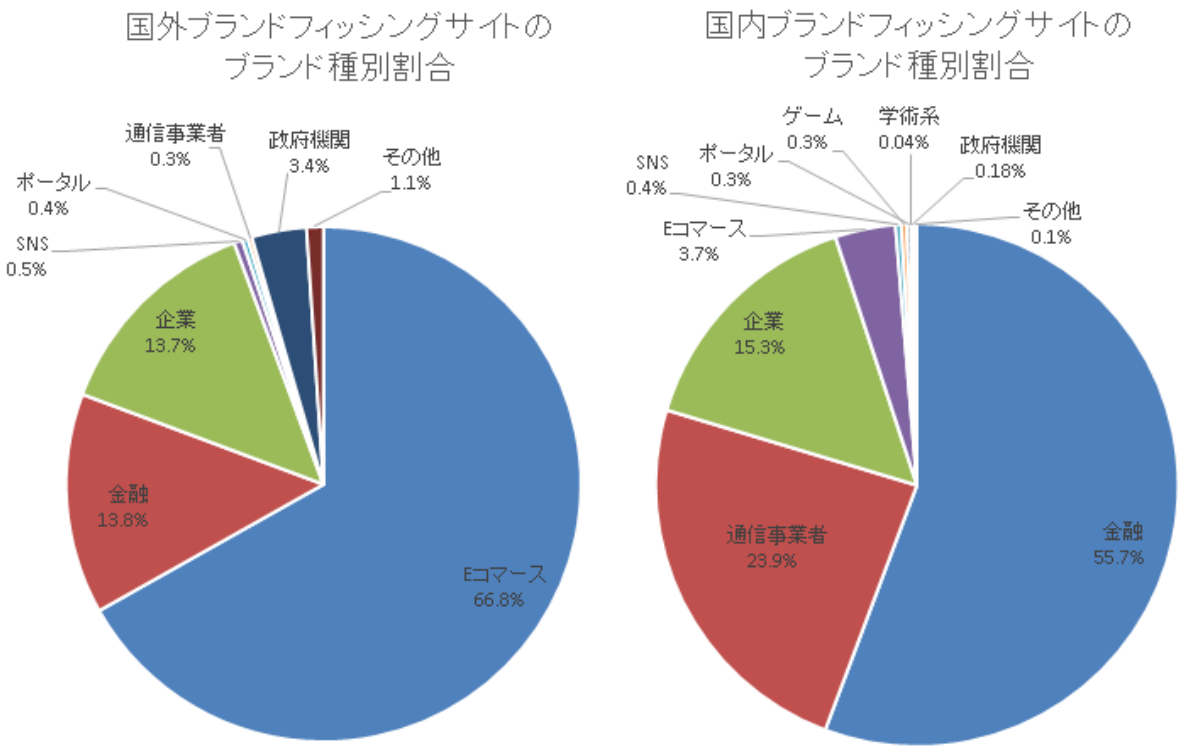
本四半期に報告が寄せられたフィッシングサイトの件数は 4,841 件で、前四半期の 4,831 件とほぼ同数でした。また、前年度同期（5,262 件）との比較では、8%の減少となりました。

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 2,732 件となり、前四半期の 2,585 件から 6%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 1,134 件となり、前四半期の 1,700 件から 33%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	4 月	5 月	6 月	本四半期合計（割合）
国内ブランド	894	817	1,021	2,732（56%）
国外ブランド	479	431	223	1,134（23%）
ブランド不明 (注 5)	227	403	349	975（20%）
全ブランド合計	1,600	1,651	1,593	4,841

（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 66.8%、国内ブランドでは金融機関のサイトを装ったものが 55.7%で，それぞれ最も多くを占めました。

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、前四半期とほぼ同数でした。国外ブランドでは、特定の通販サイトに偽装したフィッシングサイトおよび、金融機関を装ったものが多く見られました。また、通信事業者の会員向けサイトを装ったものが、増加傾向にありました。

フィッシングサイトに使用されるドメインは、ランダムな文字列を用いた.com や.cn、.xyz、.top ドメインが多く使用されていました。また、1 つサーバー上に複数のブランドのフィッシングサイトが建てられており、それぞれのサイトのサブドメインには正規サイトのドメインに似せた文字列が付けられているものもありました。

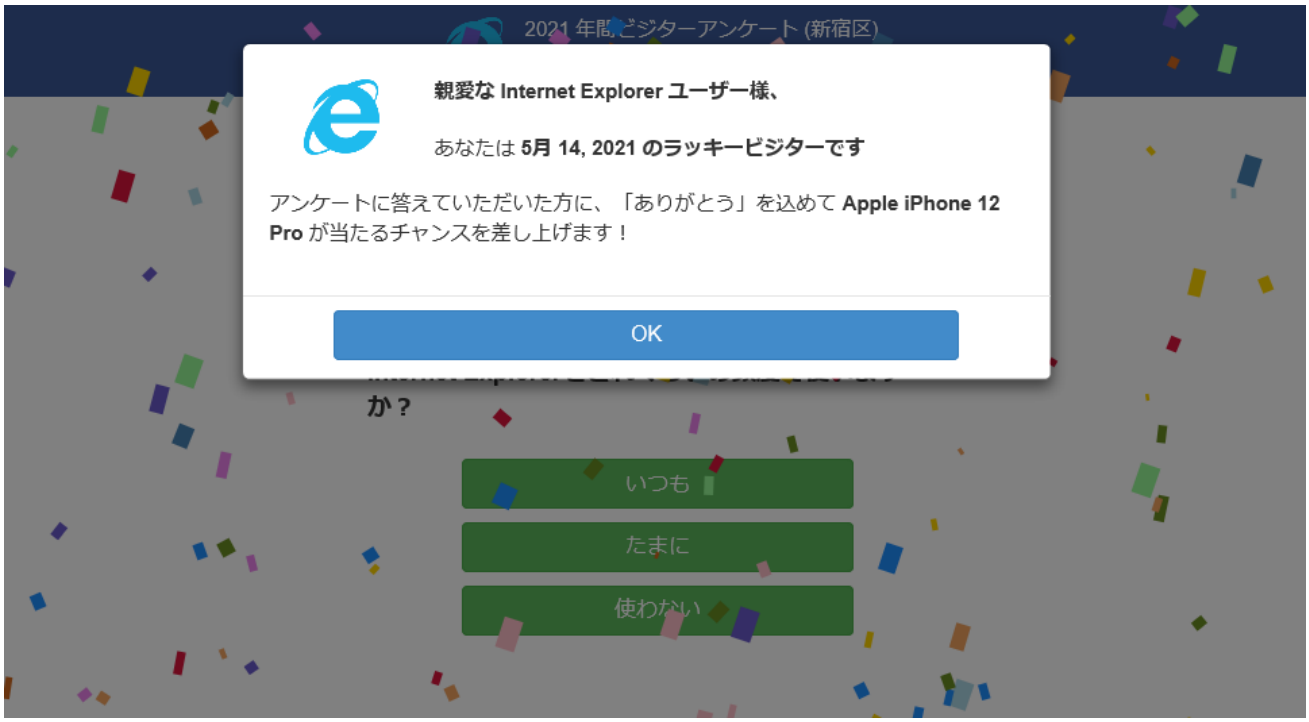
その他に、本四半期は Duck DNS を使ったフィッシングサイトの報告が多く寄せられました。Duck DNS は、無料のダイナミック DNS サービスで、短時間でサイトにアクセスできなくなることが多く、またサイトにアクセスするタイミングによってはメンテナンス中の画面やルーターの管理画面などが見えました。

フィッシングサイトの調整先の割合は、国内が 19%、国外が 81%であり、前四半期（国内が 23%、国外が 77%）と比べて国外の調整が増加しました。

3.2. Web サイト改ざんの傾向

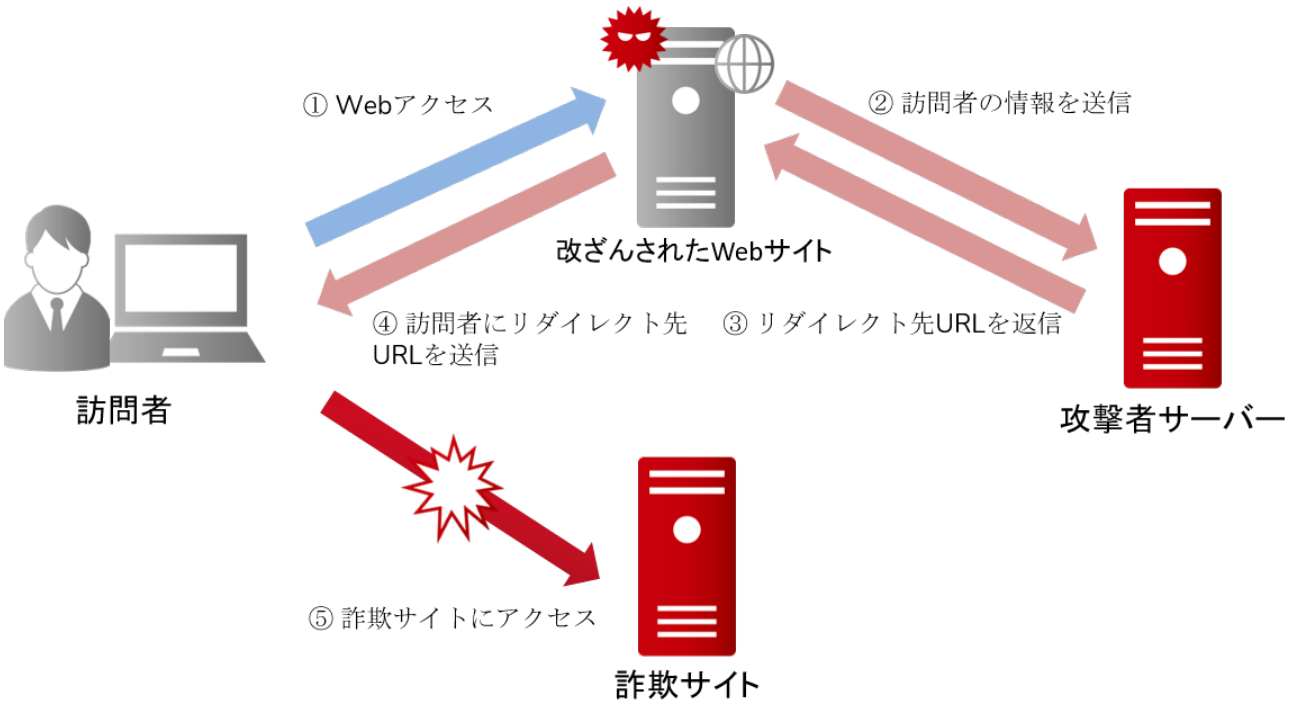
本四半期に報告が寄せられた Web サイト改ざんの件数は、251 件でした。前四半期の 282 件から 11%減少しています。

本四半期は、改ざんされた Web サイトから詐欺サイトや不審な商品販売サイトなどに誘導される報告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 PHP スクリプトが設置されており、そのスクリプトを利用して多数の不正なページが作成されます。［図 10］は、作成された不正なページにアクセスした際に表示されるラッキービジター詐欺ページの例です。



［図 10：転送先の詐欺サイトの例］

ページにアクセスすることで発生する転送までの流れは［図 11］のようになっています。



［図 11：詐欺サイトに転送するまでの流れ］

改ざんされた Web サイトにアクセスすると、訪問者の情報が攻撃者サーバーに送信されます。次に、攻撃者サーバーは訪問者の情報をもとに転送先となる URL をレスポンスとして返し、最終的に、この URL 宛に、改ざんされた Web サイトが訪問者を転送します。本攻撃の詳細については JPCERT/CC Eyes で解説しています。

JPCERT/CC Eyes「ラッキービジター詐欺で使用される PHP マルウェア」
https://blogs.jpcert.or.jp/ja/2021/06/php_malware.html

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、5 件でした。前四半期の 7 件から 29%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) マルウェア LODEINFO による攻撃

本四半期は、前四半期から引き続きマルウェア LODEINFO を使用した標的型攻撃の報告が寄せられました。マルウェア LODEINFO は、標的型攻撃メールに添付された Word ファイルを開いた際に、それに含まれる悪意のあるマクロが実行されることで感染します。

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 38 件でした。前四半期の 138 件から 72%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 1,385 件でした。前四半期の 1,085 件から 28%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）、IMAP（143/TCP）、9530/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	97	134	102	333
143/tcp	252	68	11	331
9530/tcp	0	42	135	177
80/tcp	45	50	30	125
23/tcp	60	34	26	120
62223/tcp	26	24	39	89
443/tcp	18	24	23	65
37215/tcp	45	13	1	59
445/tcp	6	9	10	25
2323/tcp	10	10	1	21
25/tcp	1	9	7	17
1433/tcp	5	9	3	17
8080/tcp	4	5	0	9
6379/tcp	1	3	5	9
52869/tcp	4	1	1	6
3389/tcp	3	1	1	5
26/tcp	5	0	0	5
21/tcp	1	3	1	5
8000/tcp	1	3	0	4
その他	9	25	11	45
月別合計	593	467	407	1467

その他に分類されるインシデントの件数は、449 件でした。前四半期の 763 件から 41%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) EC-CUBE を利用したサイトにおける XSS 脆弱性を悪用したインシデントへの対応

本四半期は、EC-CUBE を利用した EC サイトの情報漏えいに関する報告が寄せられました。調査の結果、クロスサイトスクリプティングの脆弱性を悪用した改ざんがなされており、管理者画面上に認証情報を窃取する不審なコードが挿入されていることがわかりました。

被害のあった EC サイトでは、サイト利用者の ID、パスワード、クレジットカード情報等を窃取する不正なコードが設置されていたり、データベースを操作する WebShell が設置されていたりしたことを確認しました。

JPCERT/CC では、この報告をもとに IoC や具体的な攻撃内容、各種ログについて EC-CUBE 社と情報交換を行い、国内において複数の被害が確認されていることや攻撃者によって設置された WebShell へのアクセス元 IP アドレスが各被害事例ともに共通していたことから、Twitter で次のような注意喚起を行いました。

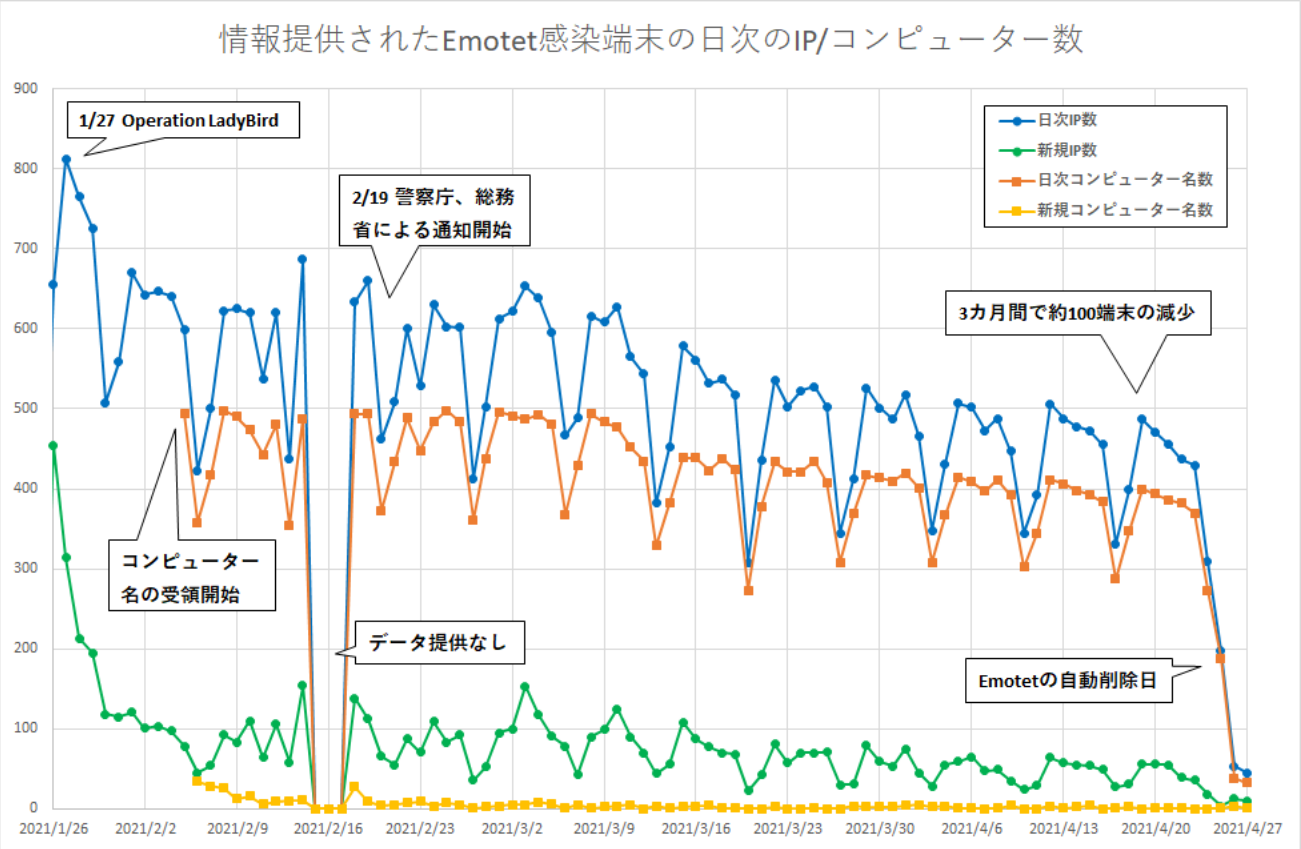
Twitter による EC-CUBE への注意喚起
https://twitter.com/jpcert_ac/status/1399604992059744256

これらの攻撃への対策としては、EC-CUBE や EC-CUBE プラグイン等について最新バージョンへアップデートすることが挙げられます。EC-CUBE 4.0 系使用している場合は、次の EC-CUBE における脆弱性関する注意喚起を参照して、対策を実施してください。

EC-CUBE のクロスサイトスクリプティングの脆弱性（CVE-2021-20717）に関する注意喚起
https://www.jpcert.or.jp/at/2021/at210022.html

(2) マルウェア Emotet に感染した端末への通知の結果

Emotet ボットネットのテイクダウン後、JPCERT/CC には関係組織から Emotet に感染した端末の情報が提供されました。Emotet に感染した端末では、Emotet がダウンロードした別のマルウェアに感染している恐れがあるため、Emotet が自動削除される 2021 年 4 月 25 日まで ISP 等と協力し、通知を行ってきました。［図 12］に示す通り、通知を開始した 2 月頃から 4 月 25 日までの約 3 カ月間で 100 台程度の端末が対処され、4 月 26 日以降では Emotet の感染がほぼ観測されなくなっていることがわかります。



［図 12：日本の Emotet に感染している端末数の推移（2021 年 4 月末）］

本通知活動の結果について JPCERT/CC Eyes で詳細を解説しています。

JPCERT/CC Eyes「マルウェア Emotet のテイクダウンと感染端末に対する通知」
https://blogs.jpcert.or.jp/ja/2021/02/emotet-notice.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、攻撃元や情報発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３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。