JPCERT Coordination Center

**電子署名者** : JPCERT Coordination Center
DN : c=JP, st=Tokyo, l=Chuo-ku, o=JPCERT Coordination Center, cn=JPCERT Coordination Center, email=office@jpcert.or.jp
**日付** : 2022.01.21 14:55:44 +09'00'

# JPCERT/CC インシデント報告対応レポート

## 2021 年 10 月 1 日 ～ 2021 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

**2022** 年 **1** 月 **20** 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 ..... 10
   3.3. 標的型攻撃の傾向 ..... 11
   3.4. その他のインシデントの傾向 ..... 12
4. インシデント対応事例 ..... 13
5. 参考文献 ..... 14

付録-1. インシデントの分類 ..... 16

## 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 10 月 1 日から 2021 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及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、及び、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) | 2,834 | 4,170 | 4,866 | 11,870 | 12,469 |
| インシデント件数 (注 3) | 3,045 | 3,302 | 3,460 | 9,807 | 8,786 |
| 調整件数 (注 4) | 1,995 | 2,163 | 2,396 | 6,554 | 4,714 |

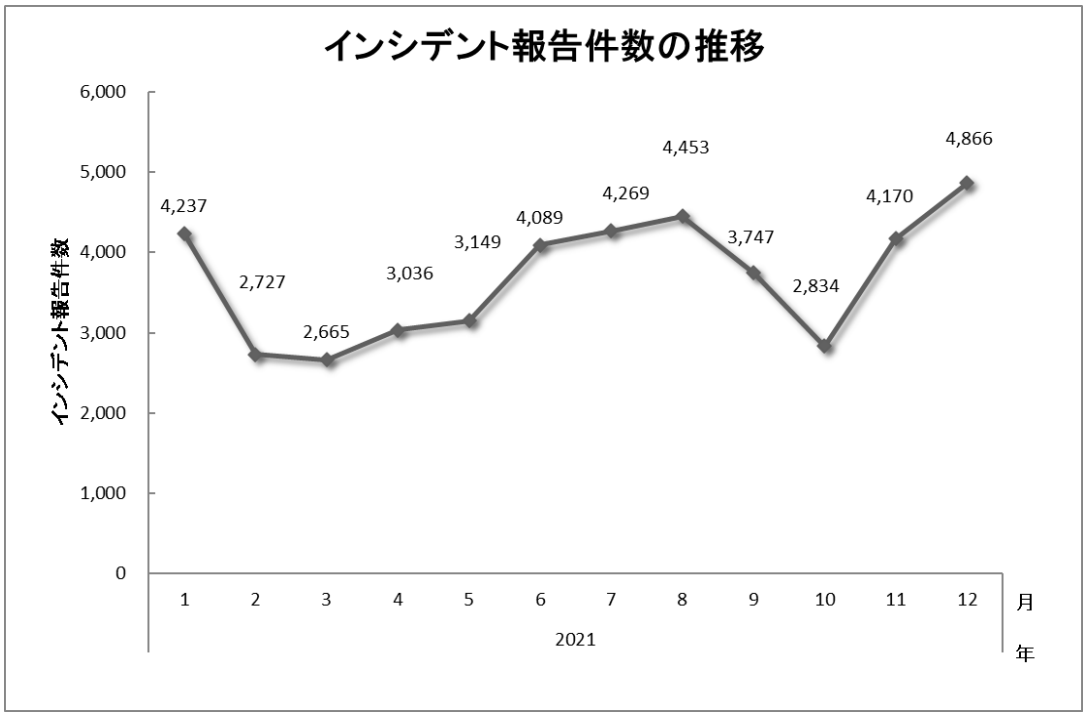
（注 2）「報告件数」は、報告者から寄せられた Web フォーム、メール、FAX による報告の総数を示します。

（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。

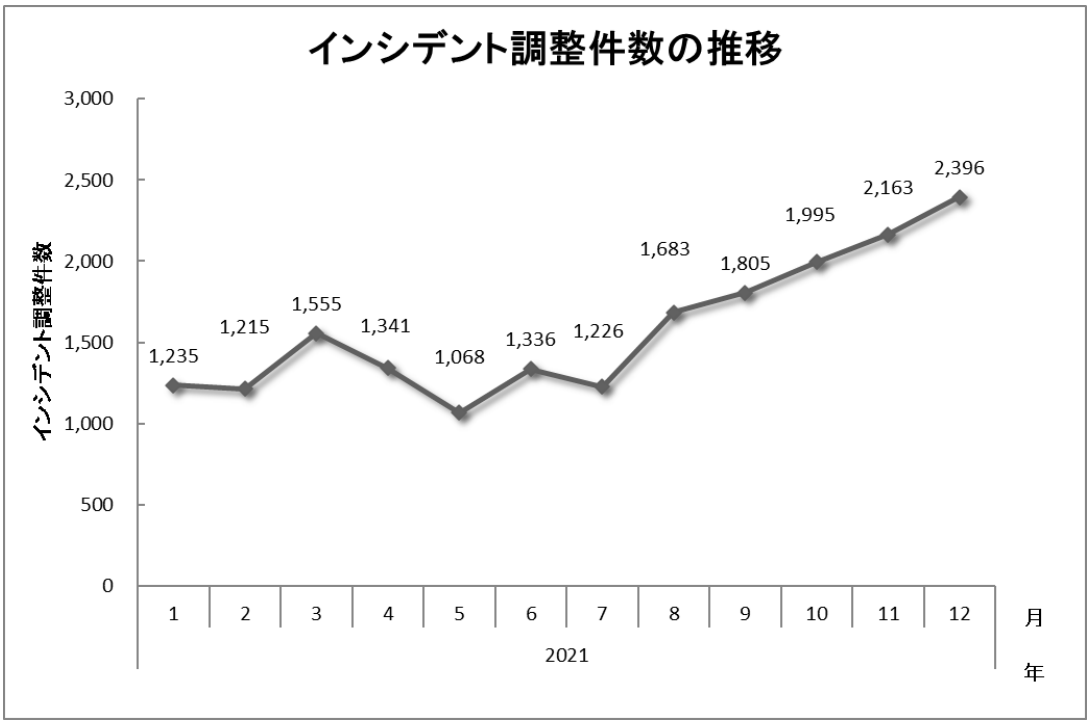
（注 4）「調整件数」は、インシデントの拡大防止のため、サイトの管理者等に対し、現状の調査と問題解決のための対応を依頼した件数を示します。

本四半期に寄せられた報告件数は、11,870 件でした。このうち、JPCERT/CC が国内外の関連する組織との調整を行った件数は 6,554 件でした。前四半期と比較して、報告件数は 5%減少し、調整件数は 39%増加しました。また、前年同期と比較すると、報告数は 9%減少し、調整件数は 55%増加しました。

［図 1］と［図 2］に報告件数及び調整件数の過去 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］

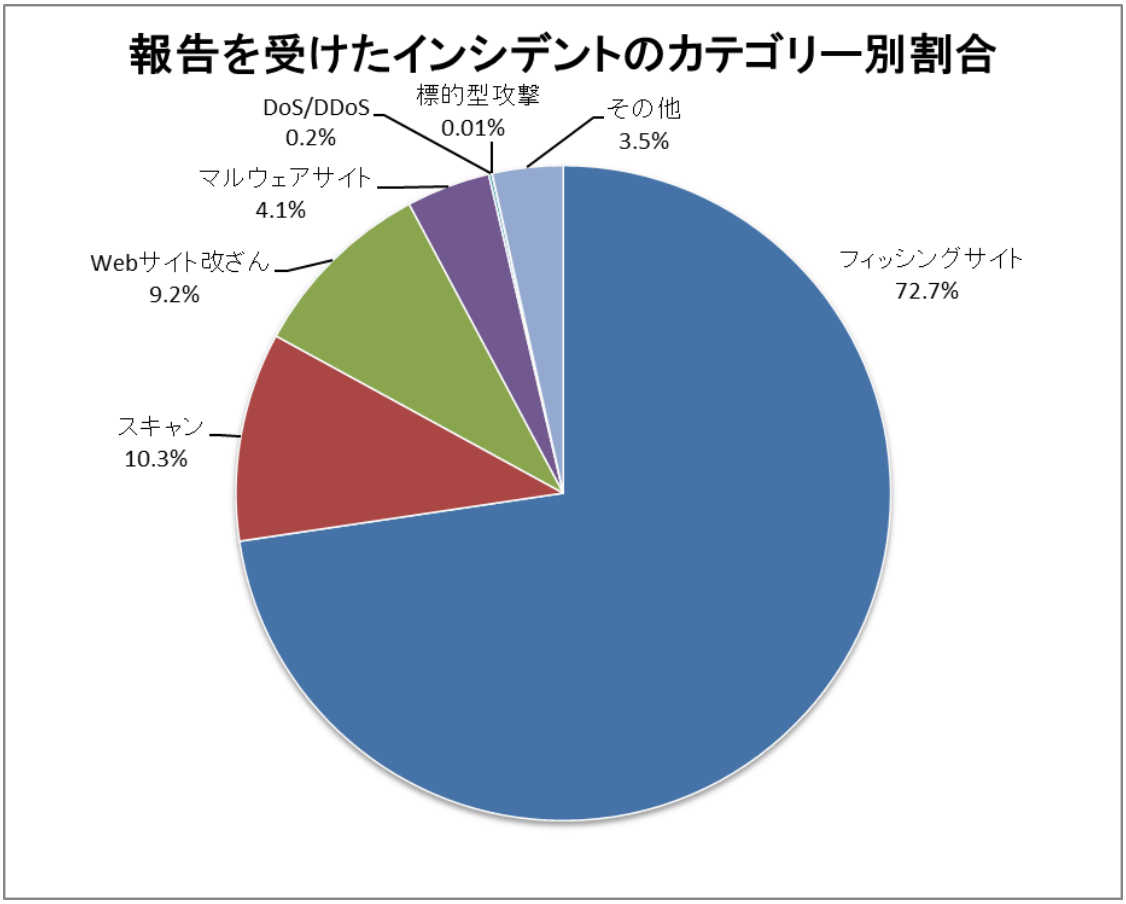



［図 2：インシデント調整件数の推移］

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］

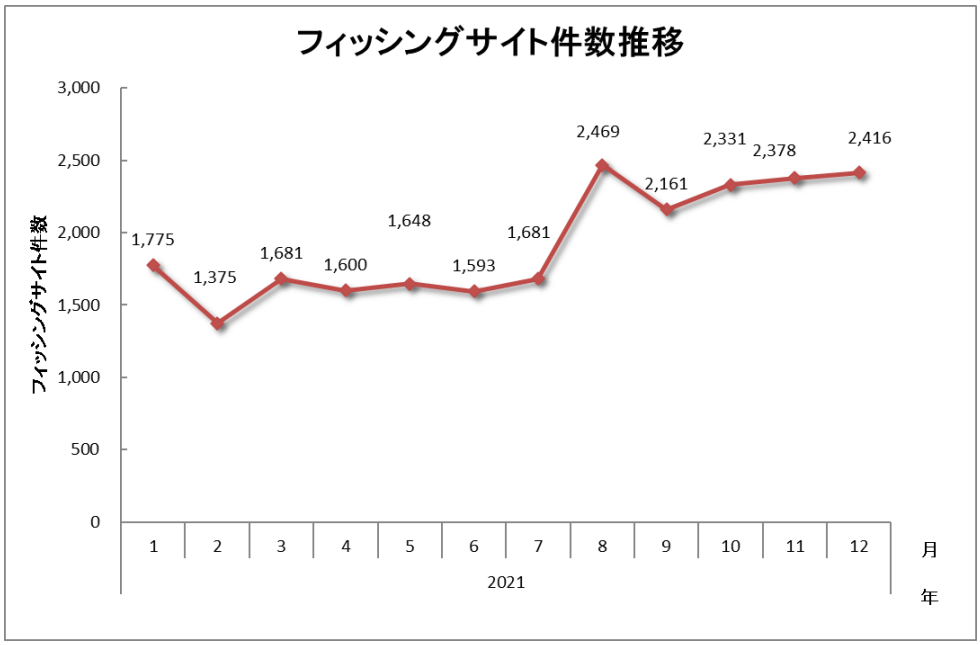
| インシデント | 10 月 | 11 月 | 12 月 | 合計 | 前四半期合計 |
|---|---|---|---|---|---|
| フィッシングサイト | 2,331 | 2,378 | 2,416 | 7,125 | 6,311 |
| Web サイト改ざん | 148 | 324 | 434 | 906 | 579 |
| マルウェアサイト | 160 | 146 | 100 | 406 | 119 |
| スキャン | 297 | 372 | 342 | 1,011 | 1,291 |
| DoS/DDoS | 12 | 2 | 2 | 16 | 7 |
| 制御システム関連 | 0 | 0 | 0 | 0 | 0 |
| 標的型攻撃 | 1 | 0 | 0 | 1 | 4 |
| その他 | 96 | 80 | 166 | 342 | 475 |



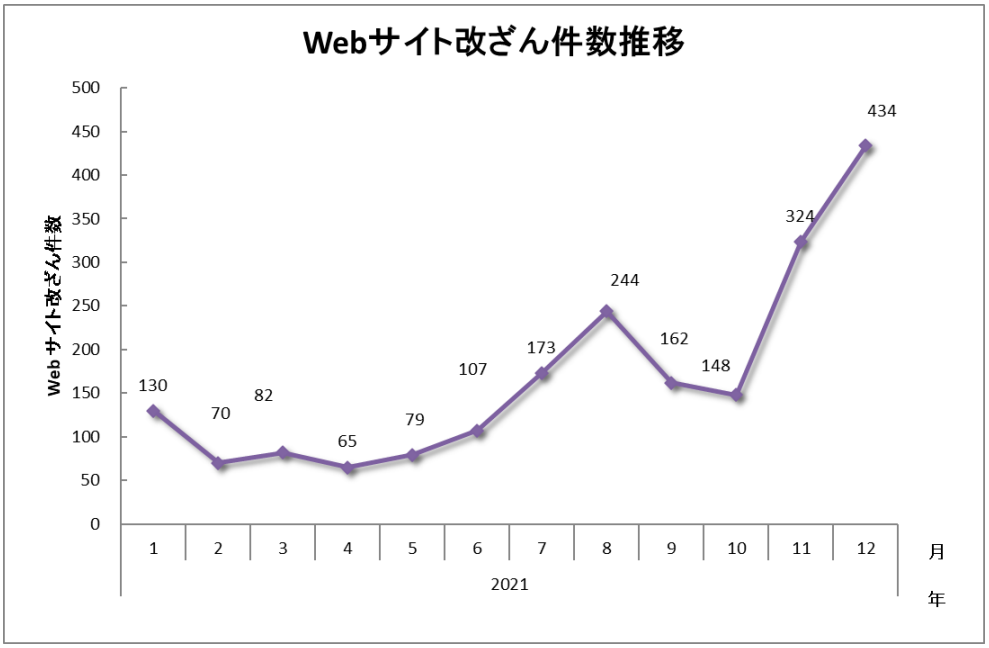

［図 3：報告を受けたインシデントのカテゴリー別割合］

フィッシングサイトに分類されるインシデントが 72.7%、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 10.3%を占めています。

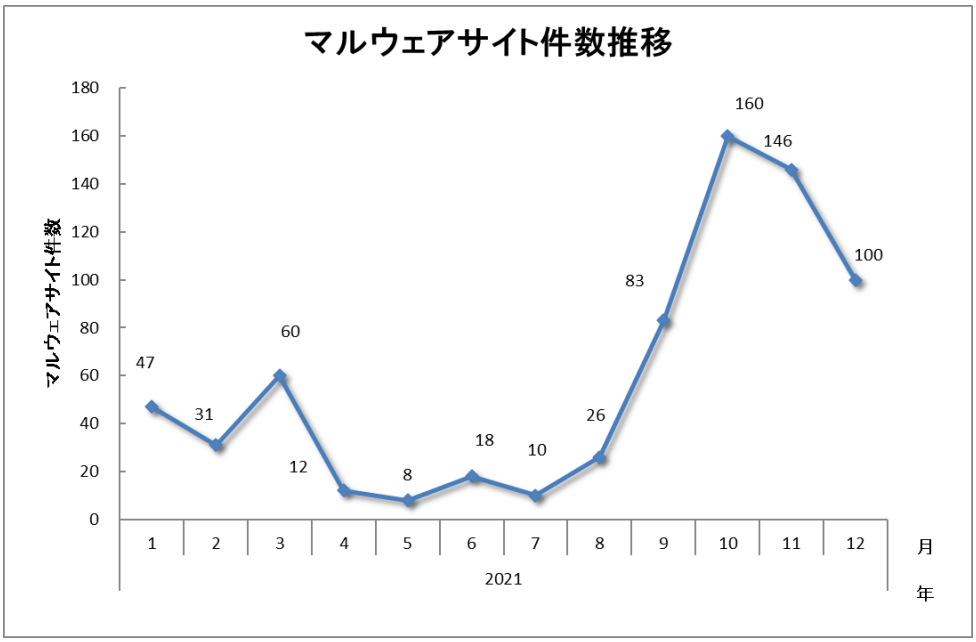
［図 4］から［図 7］に、フィッシングサイト、Web サイト改ざん、マルウェアサイト、スキャンのインシデントの過去 1 年間の月次の推移を示します。



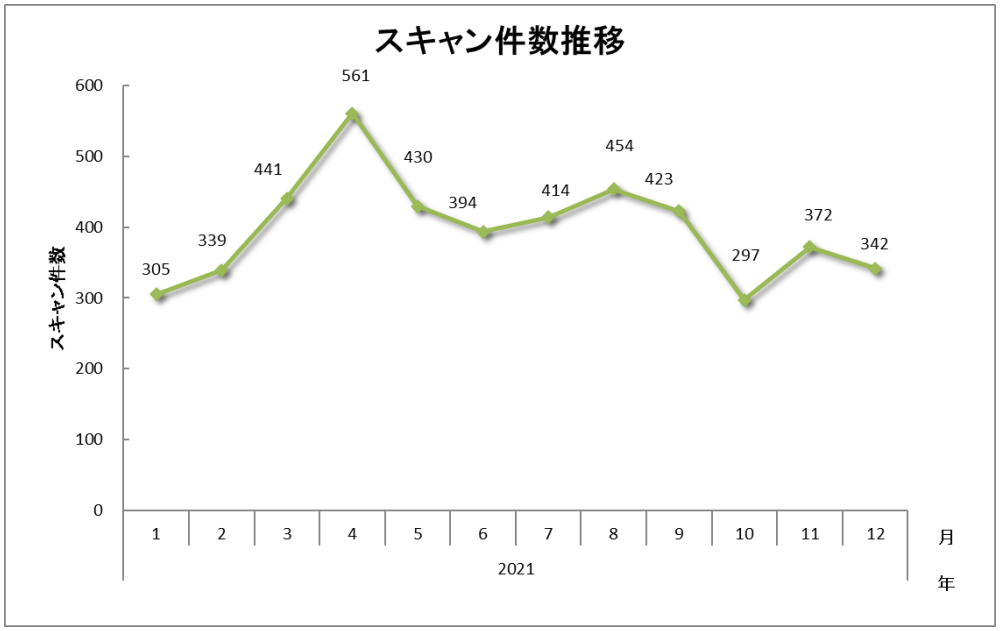

［図 4：フィッシングサイト件数の推移］




［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及び調整・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

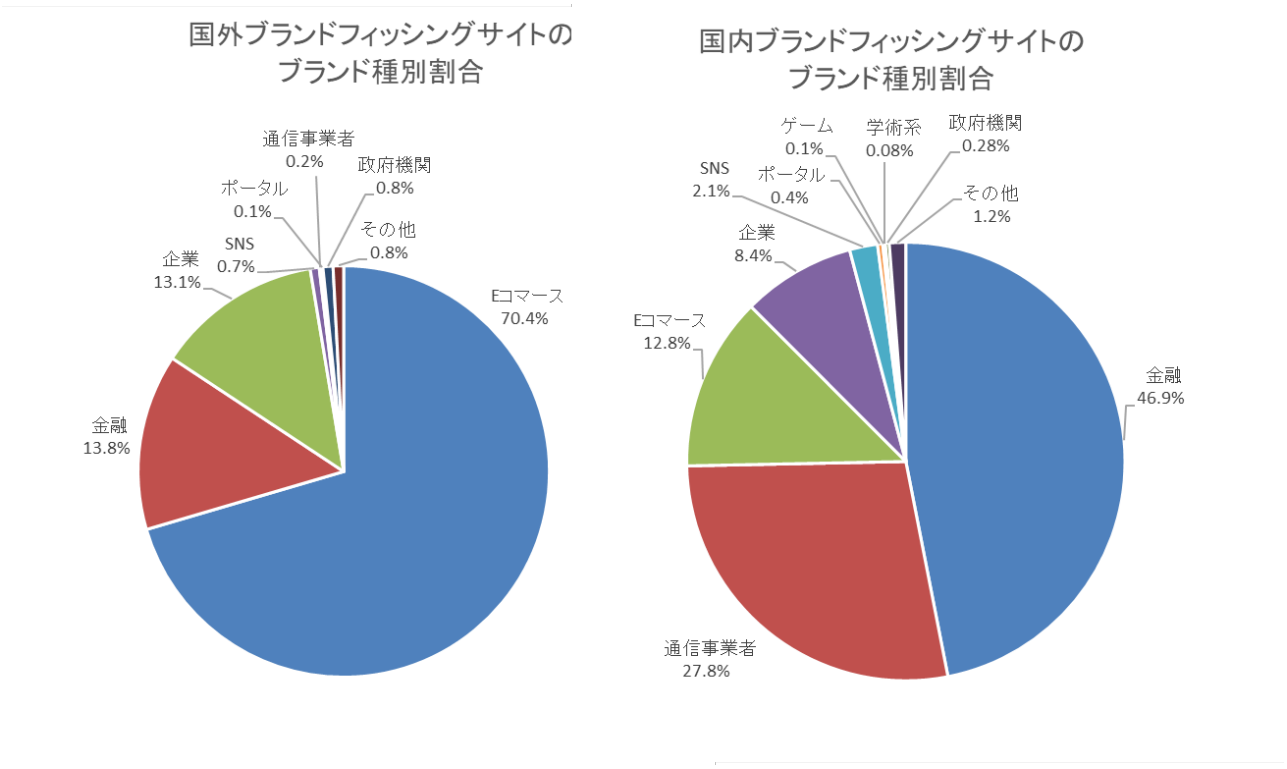
本四半期に報告が寄せられたフィッシングサイトの件数は 7,125 件で、前四半期の 6,311 件から 13%増加しました。また、前年度同期（5,015 件）との比較では、42%の増加となりました。

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 3,962 件となり、前四半期の 3,533 件から 12%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 2,406 件となり、前四半期の 1,570 件から 53%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 | 10 月 | 11 月 | 12 月 | 本四半期合計（割合） |
|---|---|---|---|---|
| 国内ブランド | 1,395 | 1,203 | 1,364 | 3,962（56%） |
| 国外ブランド | 732 | 839 | 835 | 2,406（34%） |
| ブランド不明 (注 5) | 204 | 336 | 217 | 757（11%） |
| 全ブランド合計 | 2,331 | 2,378 | 2,416 | 7,125 |

（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 70.4%、国内ブランドでは金融機関のサイトを装ったものが 46.9%で，それぞれ最も多くを占めました。

国内ブランドのフィッシングサイトでは、ETC の利用照会サービスや EC サイトの会員用ログインページを装ったものが増加しています。それぞれ、前四半期と比較して ETC の利用照会サービスのフィッシングサイトが 6 倍、EC サイトを装ったものが 10 倍と大幅な件数の伸びがみられました。

他方、国外ブランドのフィッシングサイトは、通販サイトのログインページを装ったものが半数以上占めており、報告件数上位ブランドの顔ぶれには変化がありませんでした。

フィッシングサイトテイクダウンのために調整したサイトの割合は、国内が 23%、国外が 77%であり、前四半期（国内が 23%、国外が 77%）と割合は同じでした。

### 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、906 件でした。前四半期の 579 件から 56%増加しています。

本四半期も、改ざんされた Web サイトから、不審な Web サイトへ転送される事例が複数報告されました。改ざんされた Web サイトにアクセスすると、［図 10］のような Location ヘッダーが挿入された、レスポンスが返り、それにより不審なサイトへリダイレクトされます。なお、このリダイレクトは、アクセス時の UserAgent が、iOS の Safari ブラウザーである場合のみ行われます。

```
Content-Length: 0
 X-Powered-By: PHP/7.4.12
 Server: Apache
 Connection: keep-alive
 Location: [redacted]
 Date: Thu, 02 Dec 2021 07:17:23 GMT
 Content-Type: text/html; charset=UTF-8
```

［図 10：不正な Location ヘッダーの例］

また，改ざんされた Web サイトに不正な PHP スクリプトが設置された結果、訪問者がラッキービジター詐欺ページへ転送される事例が前四半期から引き続き寄せられています。本攻撃の内容については JPCERT/CC Eyes で解説していますので、詳細については次の Web ページをご参照ください。

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、1 件でした。
次に、確認されたインシデントを紹介します。

(1) 「AppleJeus」と呼ばれる攻撃キャンペーンに関連する攻撃

本四半期は、AppleJeus と呼ばれる攻撃キャンペーンに関連する標的型攻撃の報告が寄せられました。この攻撃では、標的組織の社員に対して LinkedIn 経由でコンタクトし、マルウェアが埋め込まれたインストーラーを実行するように誘導するものです。インストーラーを実行した場合、UnionCrypto(1) と呼ばれるマルウェアに感染します。

### 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 406 件でした。前四半期の 119 件から 241%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 1,011 件でした。前四半期の 1,291 件から 21.7%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、Telnet （23/TCP）、SSH（22/TCP）、37215/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 |
|---|---|---|---|---|
| 23/tcp | 115 | 131 | 102 | 348 |
| 22/tcp | 85 | 93 | 54 | 232 |
| 37215/tcp | 18 | 70 | 32 | 120 |
| 143/tcp | 27 | 29 | 53 | 109 |
| 80/tcp | 23 | 25 | 55 | 103 |
| 2323/tcp | 22 | 17 | 11 | 50 |
| 25/tcp | 6 | 4 | 21 | 31 |
| 52869/tcp | 4 | 15 | 1 | 20 |
| 26/tcp | 0 | 7 | 1 | 8 |
| 6379/tcp | 2 | 4 | 0 | 6 |
| 443/tcp | 1 | 0 | 5 | 6 |
| 3389/tcp | 1 | 3 | 2 | 6 |
| 3306/tcp | 3 | 0 | 3 | 6 |
| 445/tcp | 0 | 1 | 3 | 4 |
| 21/tcp | 2 | 2 | 0 | 4 |
| 81/tcp | 0 | 1 | 2 | 3 |
| 8081/tcp | 1 | 1 | 1 | 3 |
| その他 | 16 | 10 | 19 | 45 |
| 月別合計 | 326 | 413 | 365 | 1,104 |

その他に分類されるインシデントの件数は、342 件でした。前四半期の 475 件から 28%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) Movable Type の脆弱性 (CVE-2021-20837) を悪用した Web サイト改ざんに関する報告への対応

2021 年 10 月 20 日に公開された Movable Type の脆弱性（CVE-2021-20837）を悪用して Web サイトが改ざんされた報告を複数受けました。JPCERT/CC では、Web サーバーのアクセスログと、第三者により設置された可能性のあるファイルを分析し、被害サイトに共通する PHP バックドア（FoxWSO など）が設置されていることを確認しました。
被害を受けた Web サイトの中には、他の CMS を使用して作成した Web サイトであるものの、過去に使用していた Movable Type を Web サイト上に放置していたために、今回の攻撃の影響を受けた Web サイトもありました。

これらの攻撃への対策としては、Movable Type を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。Movable Type を使用している場合は、次の注意喚起を参照して、対策を実施してください。

Movable Type の XMLRPC API における脆弱性（CVE-2021-20837）に関する注意喚起
https://www.jpcert.or.jp/at/2021/at210047.html

(2) ランサムウェア感染被害に関する報告への対応

本四半期は、ランサムウェア感染被害（Snatch、AvosLocker、Magniber、Ragnar Locker など）に関する報告を複数受けています。JPCERT/CC では、報告者から被害範囲や調査状況、報告時点の対応状況などをヒアリングし、得られた情報もとに、関連するランサムウェア攻撃の特徴などの情報を提供し対応方針に関するアドバイスをしています。

(3) Apache Log4j の脆弱性 (CVE-2021-44228) の影響を受ける可能性があるホストについての対応

2021 年 12 月 11 日に公開した、以下の Apache Log4j の脆弱性が残っている国内ホストに関する情報を外部組織から受けました。

Apache Log4j の任意のコード実行の脆弱性（CVE-2021-44228）に関する注意喚起
https://www.jpcert.or.jp/at/2021/at210050.html

対象のホスト数は 150 件ほどで、多くが製品に含まれる脆弱性でしたが、一部クラウドサービスなども対象になっていました。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、ホストの影響有無の確認、さらに脆弱なシステムを利用している場合は対策を行うよう連絡しました。

## 5. 参考文献

(1) The Cybersecurity and Infrastructure Security Agency
MAR-10322463-3.v1 - AppleJeus: Union Crypto
https://www.cisa.gov/uscert/ncas/analysis-reports/ar21-048c

## 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。

本文書を引用、転載する際には JPCERT/CC 広報（pr@jpcert.or.jp）まで確認のご連絡をお願いします。最新情報については JPCERT/CC の Web サイトを参照してください。

JPCERT コーディネーションセンター（JPCERT/CC）
https://www.jpcert.or.jp/