JPCERT/CC インシデント報告対応レポート

2022 年 10 月 1 日 ～ 2022 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

2023 年 1 月 19 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」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、2022 年 10 月 1 日から 2022 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］

	10 月	11 月	12 月	合計	前四半期合計
報告件数 [注2]	4,165	4,243	3,515	11,923	13,564
インシデント件数 [注3]	3,274	2,452	2,699	8,425	10,656
調整件数 [注4]	2,383	1,624	1,752	5,759	6,444

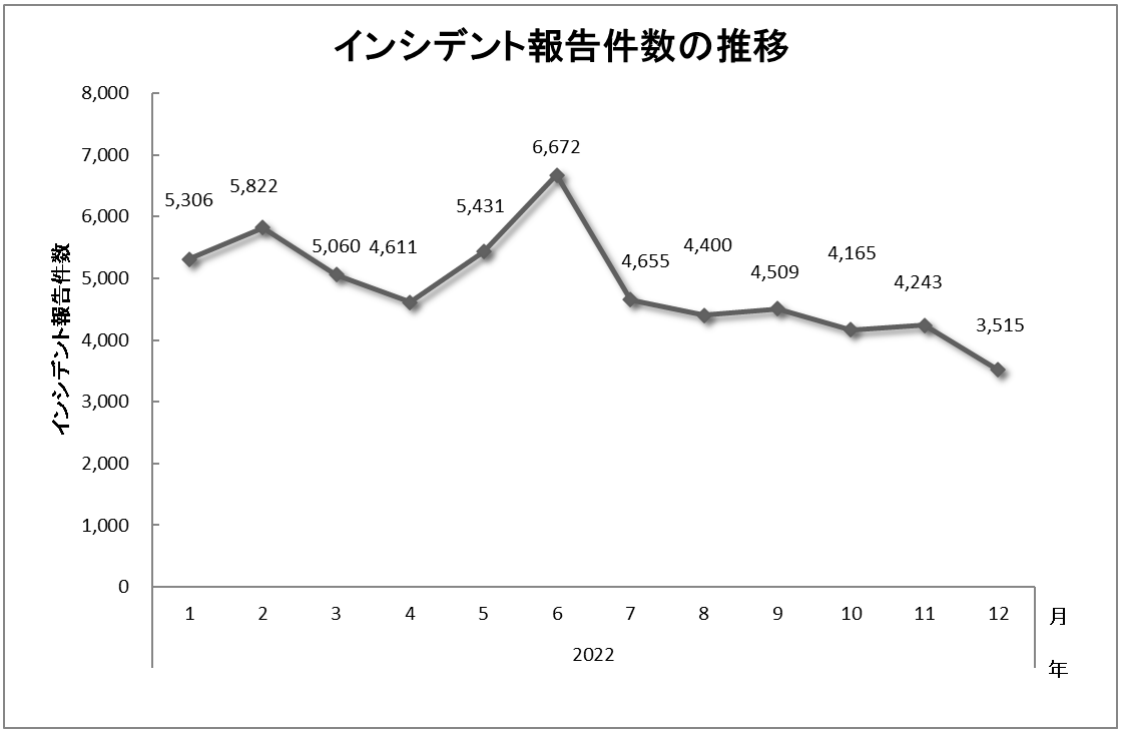
（注 2）「報告件数」は、報告者から寄せられた Web フォーム、メール、FAX による報告の総数を示します。

（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。

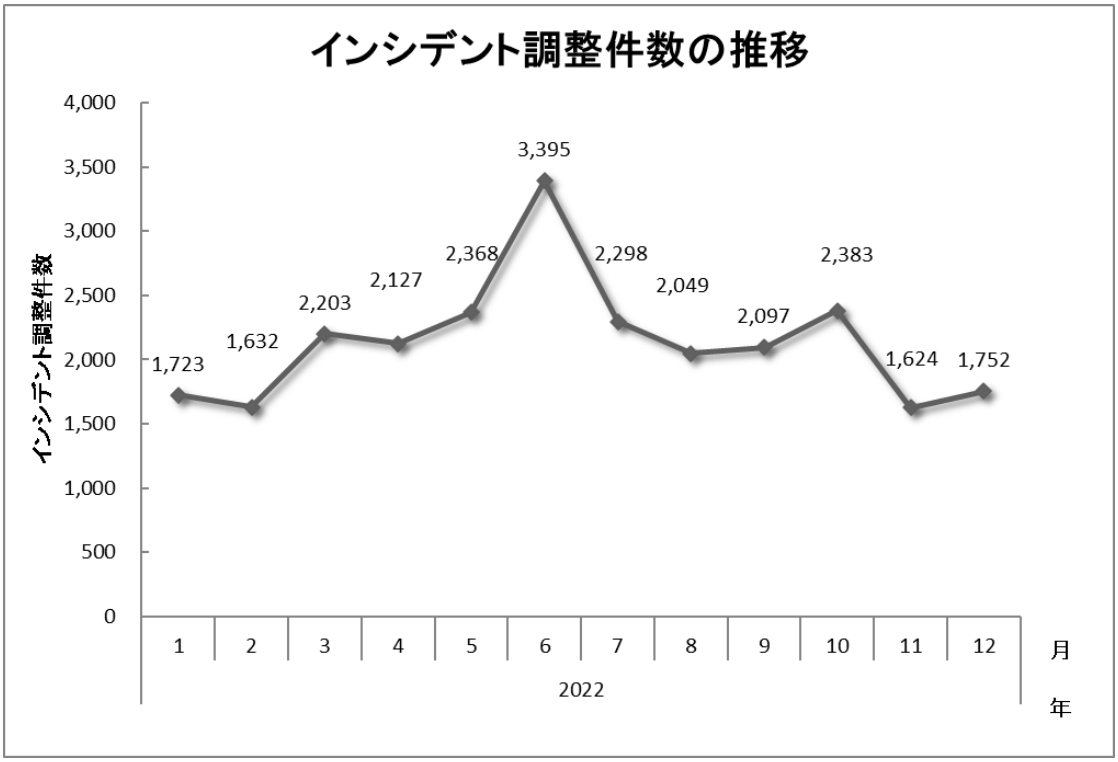
（注 4）「調整件数」は、インシデントの拡大防止のため、サイトの管理者等に対し、現状の調査と問題解決のための対応を依頼した件数を示します。

本四半期に寄せられた報告件数は、11,923 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 5,759 件でした。前四半期と比較して、報告件数は 12%減少し、調整件数は 11%減少しました。また、前年同期と比較すると、報告数はほぼ同数で、調整件数は 12%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］

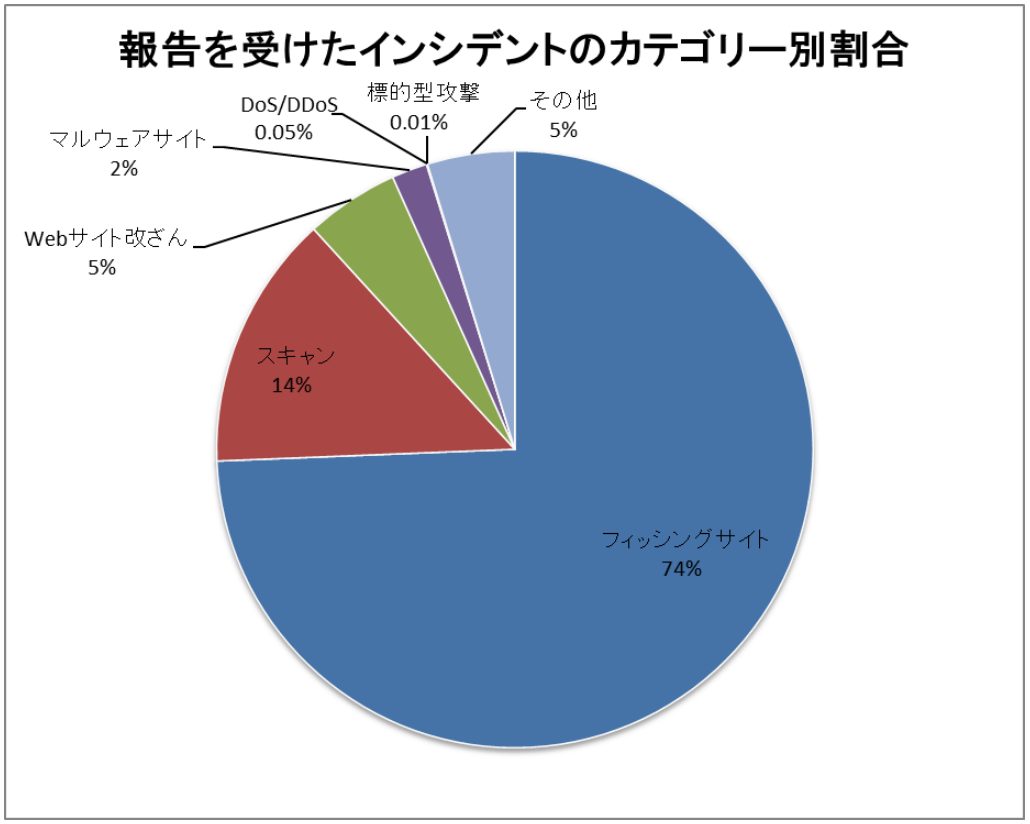


［図 2：インシデント調整件数の推移］

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	10 月	11 月	12 月	合計	前四半期合計
フィッシングサイト	2,406	1,842	2,018	6,266	7,520
Web サイト改ざん	253	94	80	427	695
マルウェアサイト	83	36	43	162	199
スキャン	443	339	384	1,166	1,917
DoS/DDoS	0	4	0	4	8
制御システム関連	0	0	0	0	0
標的型攻撃	0	0	1	1	2
その他	89	137	173	399	315

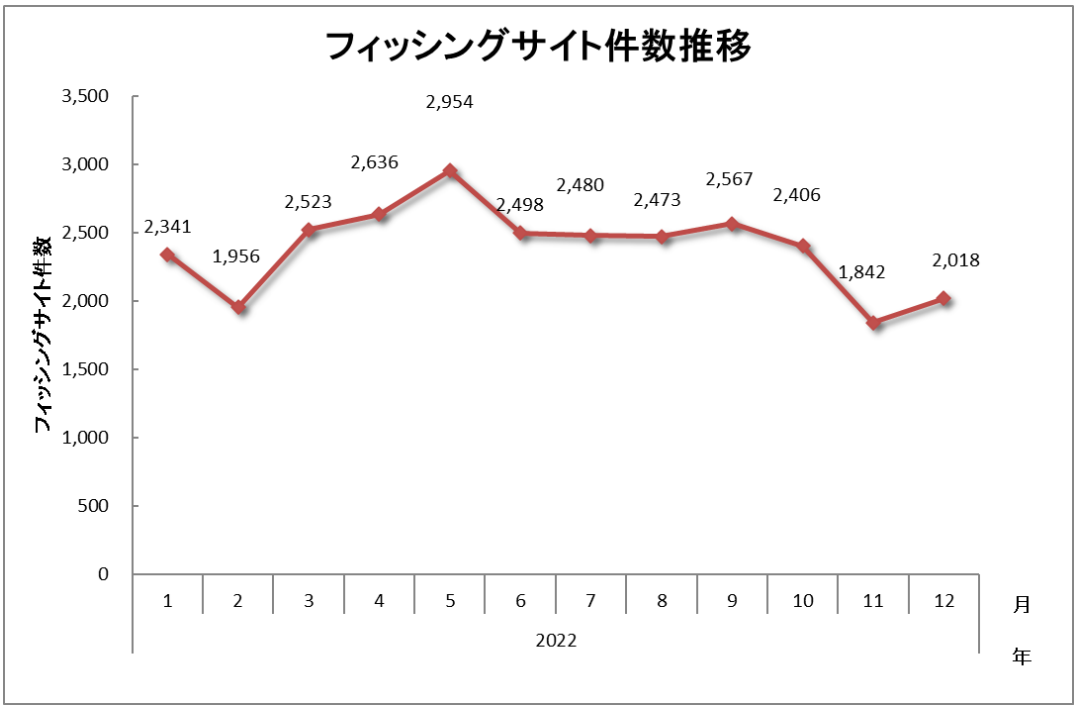


［図 3：報告を受けたインシデントのカテゴリー別割合］

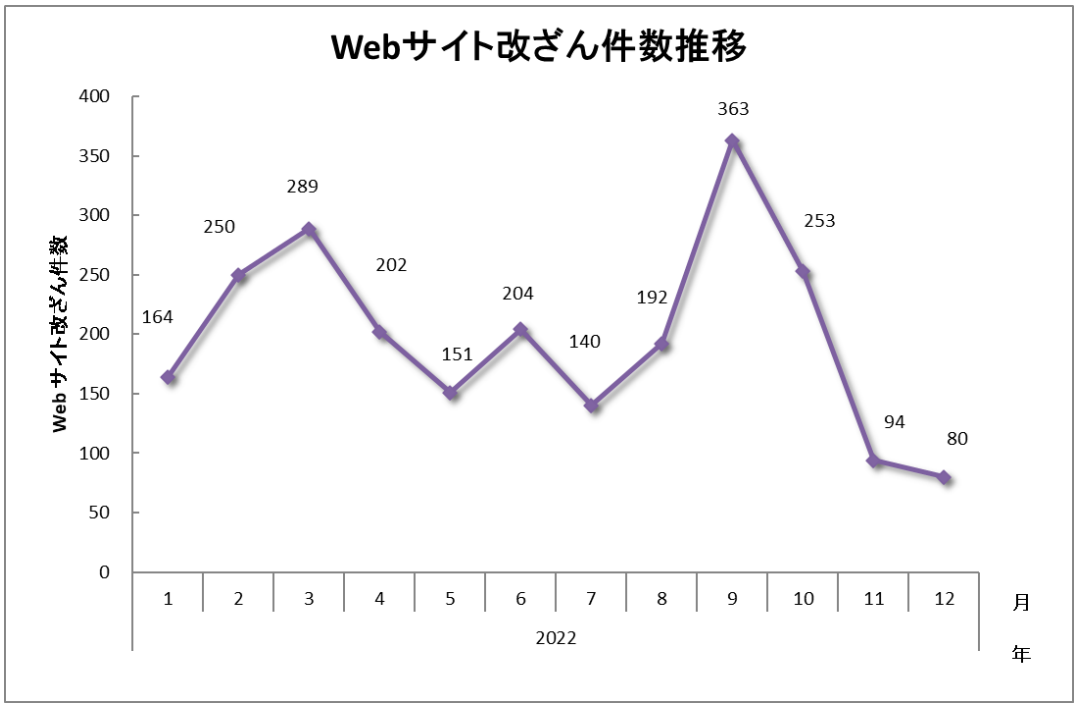
フィッシングサイトに分類されるインシデントが 74%、スキャンに分類される、システムの弱点を探索

するインシデントが 14%を占めています。

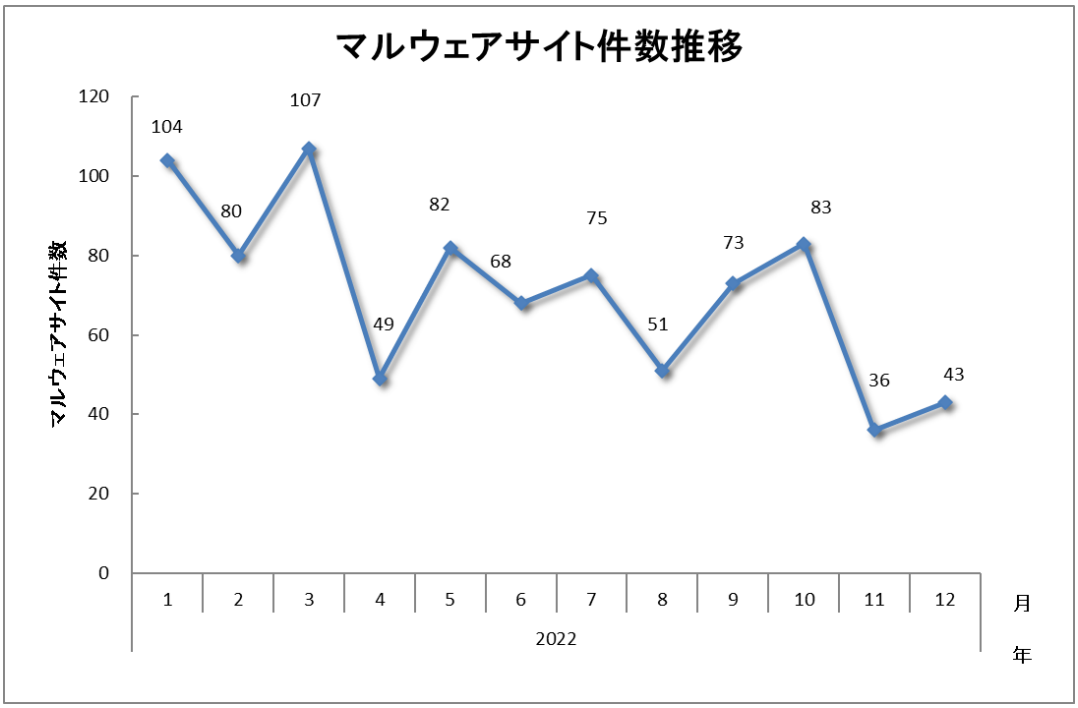
［図 4］から［図 7］に、フィッシングサイト、Web サイト改ざん、マルウェアサイト、スキャンのインシデントの過去 1 年間の月次の推移を示します。



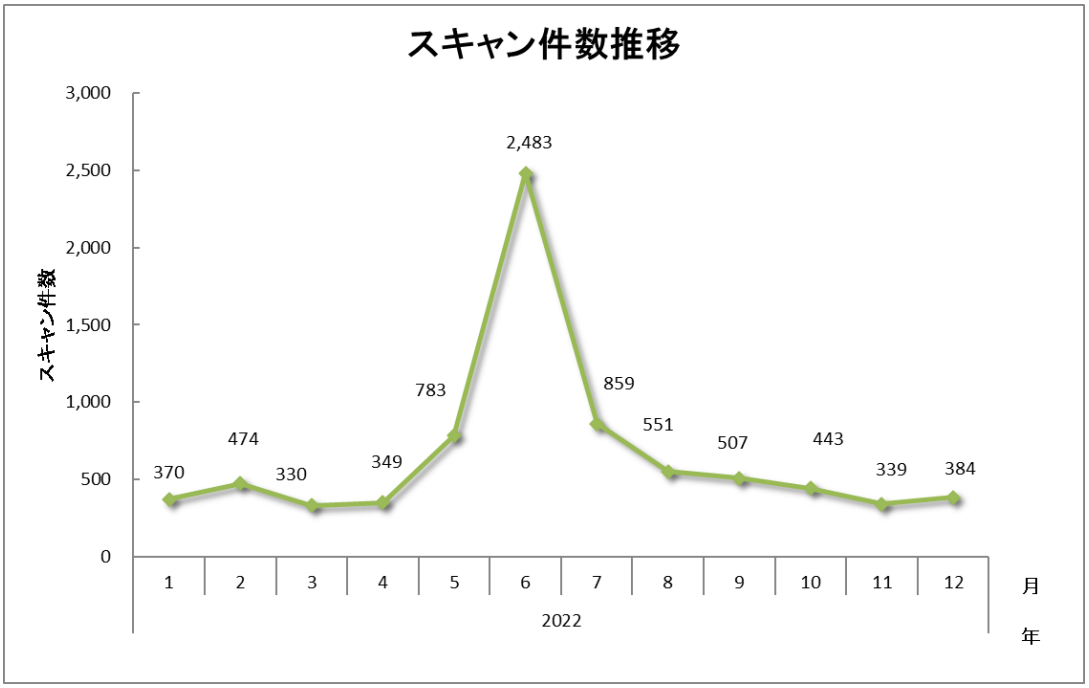
［図 4：フィッシングサイト件数の推移］



［図 5：Web サイト改ざん件数の推移］

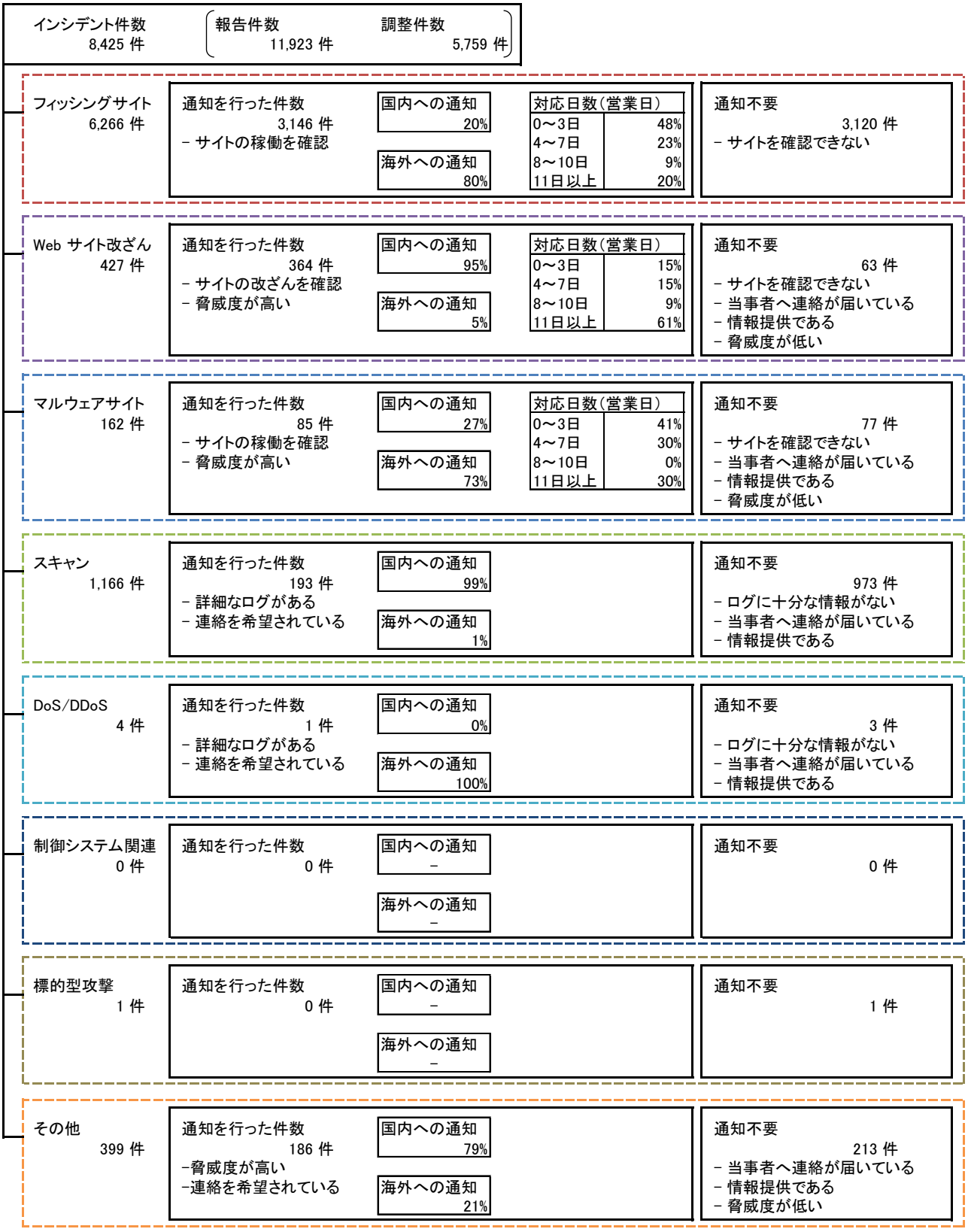


［図 6：マルウェアサイト件数の推移］



［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

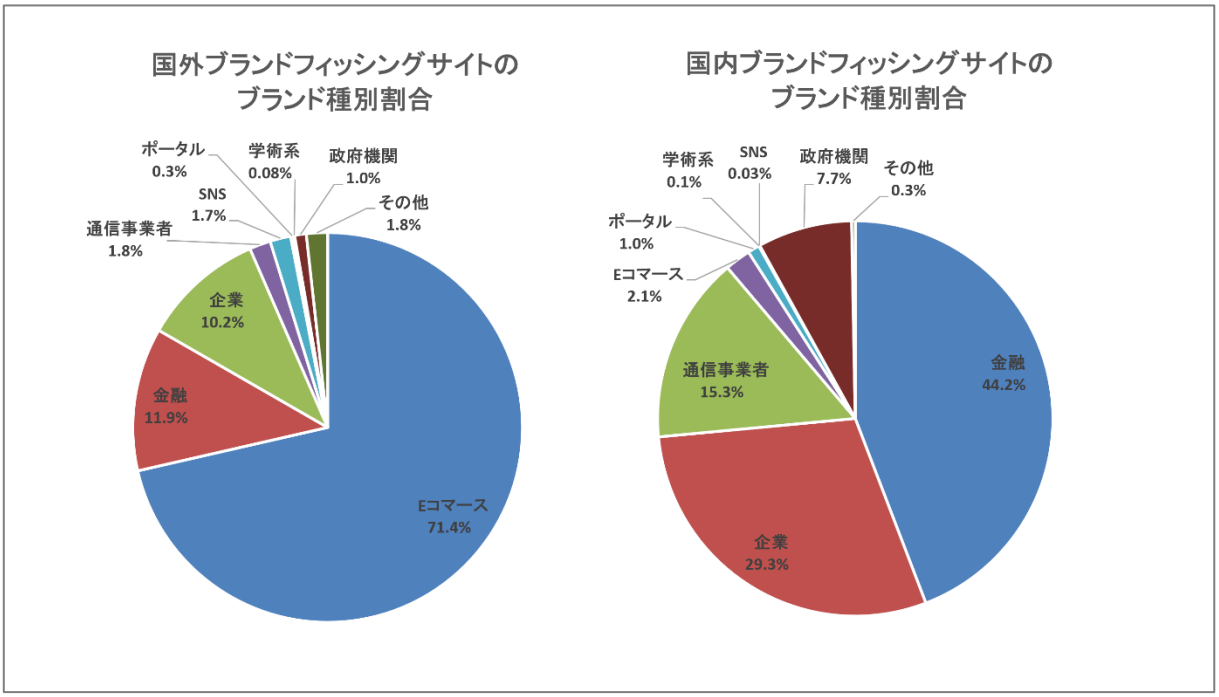
本四半期に報告が寄せられたフィッシングサイトの件数は 6,266 件で、前四半期の 7,520 件から 17%減少しました。また、前年度同期（7,125 件）との比較では、12%の減少となりました。

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 3,413 件となり、前四半期の 4,191 件から 19%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 2,390 件となり、前四半期の 2,662 件から 10%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	10 月	11 月	12 月	本四半期合計（割合）
国内ブランド	1,413	888	1,112	3,413(54%)
国外ブランド	850	773	767	2,390(38%)
ブランド不明 (注 5)	143	181	139	463(7%)
全ブランド合計	2,406	1,842	2,018	6,266

（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、国外ブランド関連の報告では E コマースサイトを装ったものが 71.4%、国内ブランド関連の報告では金融機関のサイトを装ったものが 11.9%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」や国税庁を装ったフィッシングサイトが多く、ETC の利用照会サービスや楽天・楽天カード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。

また、URL 短縮サービスである Rebrandly が、Amazon、三井住友カードおよびイオンカードを装ったフィッシングサイトへの誘導に使われていることを確認しました。

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 20%、国外が 80%であり、前四半期（国内が 28%、国外が 72%）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、427 件でした。前四半期の 695 件から 39%減少しています。

本四半期は、CMS を利用している正規の Web サイトが改ざんされる事例が複数確認されました。改ざんされた Web サイトには［図 10］のような難読化された JavaScript が挿入されていることを確認しました。該当のスクリプトは、Web サイト上で入力されたクレジットカード情報等の窃取を行います。

```
eval(function(p,a,c,k,e,r)
{e=function(c){return(c<a?''':e(parseInt(c/a)))+((c=c%a)>35?String.fromCharCode(c+29):c.toString(36))};if(!''.replace(/^/,String))
```

［図 10：難読化されたスクリプトの一部抜粋］

また、改ざんされた Web サイトの改ざん原因としては、プラグイン等の脆弱性の悪用の他に、CMS の管理ユーザーの認証情報が窃取されたことで改ざんが発生したケースが報告されています。

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、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) LinkedIn 経由で不正なヘルプファイルをダウンロードさせる攻撃

本四半期では、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。確認された手口では、標的の社員に対して LinkedIn 経由で接触を行い、チャットで複数回のやり取り行ったのち、最終的にマルウェアが含まれるアーカイブファイルを送り付けるものです。アーカイブファイルにはヘルプファイル（.chm）が格納されており、当該ファイルを実行することで外部から MSI ファイルがダウンロード、実行されます。ダウンロードされる MSI ファイルの中には感染端末の情報を収集する機能が含まれることを確認しています。

LinkedIn 経由の標的型攻撃については昨年度も類似の事案が観測されており、今後も同様の攻撃が継続する可能性があります。

JPCERT/CC 活動四半期レポート［2022 年 1 月 1 日～2022 年 3 月 31 日］
https://www.jpcert.or.jp/pr/2022/PR_Report2021Q4.pdf

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 162 件でした。前四半期の 199 件から 19%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 1,166 件でした。前四半期の 1,917 件から 39%減少しています。スキャンの対象となったポートの上位 10 位を［表 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）、5060/UDP、Telnet（23/TCP）、IMAP（143/TCP）でした。

［表 4：ポート別のスキャン件数の上位 10 位］

ポート	10 月	11 月	12 月	合計
22/tcp	191	186	232	609
5060/udp	85	60	24	169
23/tcp	33	25	72	130
143/tcp	74	25	28	127
80/tcp	18	19	20	57
37215/tcp	32	4	3	39
25/tcp	5	17	9	31
443/tcp	4	1	0	5
445/tcp	3	0	1	4
9530/tcp	1	0	0	1
その他	1	2	3	6
月別合計	447	339	392	1178

その他に分類されるインシデントの件数は、399 件でした。前四半期の 315 件から 27%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) 侵入型ランサムウェア攻撃に関する報告への対応

本四半期も引き続き、侵入型ランサムウェア攻撃に関する報告を複数受けました。攻撃者が、組織内のネットワークに侵入した手段としては、SSL-VPN 製品の脆弱性や Log4j の脆弱性を悪用したと推測されるケースが確認されています。SSL-VPN 製品が侵入経路となったケースでは、侵入された時点では脆弱性への対応適用済み（パッチ適用済み）であるものの、対応前に認証情報が窃取されており、漏えいした認証情報を用いて侵害されるケースが散見されます。報告された侵入型ランサムウェア攻撃を行う攻撃グループとしては、TargetCompany や BianLian などを確認しています。

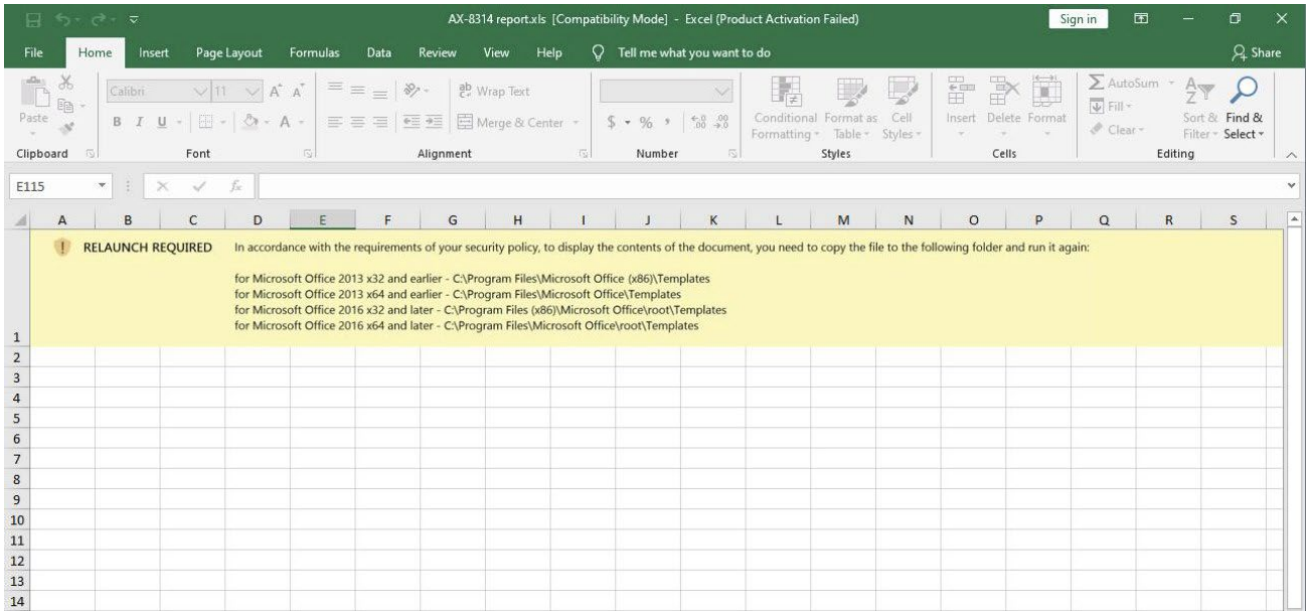
なお、JPCERT/CC では、侵入型ランサムウェア攻撃の被害を受けた際の初動対応についてまとめた FAQ、および動画を公開しているため、被害を受けた際にはご活用ください。

侵入型ランサムウェア攻撃を受けたら読む FAQ
https://www.jpcert.or.jp/magazine/security/ransom-faq.html

侵入型ランサムウェア攻撃の初動対応のポイント（ウェビナー）
https://www.youtube.com/watch?v=nDOSn_ss7zI

(2) マルウェア Emotet に関する報告への対応

2022 年 11 月 2 日以降、Emotet へ感染させようとする不審なメール送信が再開されたことを確認しています。その影響で、本四半期は、Emotet に関する報告を多数受けました。送信された不審なメールに添付された Excel ファイルは、[図 11] に示すように Excel ファイルを特定のフォルダー（Office ファイルの信頼できる場所）にコピーして実行するように書かれているものが観測されています。これは、マクロの実行を無効化している場合でも、コピー先のフォルダーが「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、不正なマクロが実行されることを狙っていると考えられます。



［図 11：特定の場所にコピーして実行することを求める Excel ファイル］

なお、JPCERT/CC では、国内での Emotet の感染拡大を受けて、以下の注意喚起を公開しました。

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

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。