# JPCERT/CC 活動四半期レポート

## 2022 年 7 月 1 日 ～ 2022 年 9 月 30 日

一般社団法人 JPCERT コーディネーションセンター

2022 年 10 月 20 日

## 活動概要トピックス

### ートピック1ー　「標準から学ぶ ICS セキュリティ」の連載を開始

ICS（産業用制御システム）のセキュリティに関する国際標準である IEC 62443 シリーズへの注目度が関係者の中で高まっています。この標準は、2 段階の分冊番号を付与された十数分冊からなっており、ICS のコンポーネントの対策を論じたものあれば、ICS のセキュリティ管理の方法を論じたものもあるといったように、さまざまな観点から ICS のセキュリティを記述しています。現在も新たな分冊の開発や発行済みの分冊の改定作業が進められるとともに、産業用以外の自動制御システムへ適用を拡大する可能性についても検討が開始されることになっています。実際に、すでに医療用機器などで IEC 62443 を参照するケースが散見されます。

JPCERT/CC が毎年開催している制御システムセキュリティカンファレンスの過去の講演資料の中でも IEC 62443 に関するものは今でも多くの皆さまにダウンロードいただいていますし、日ごろの情報交換の場でもしばしば IEC 62443 が話題になります。一方で、IEC 62443 というシリーズ標準の存在は知っているが、多数の分冊が心理的な障壁となっていて、内容を理解し活用するまでには至っていないとの声も聞かれます。

IEC 62443 の開発グループの中でも、十年数年の期間をかけて順次策定されてきた多数の分冊の中で定義された概念の整合性の確認や整理も始まりました。このタイミングをとらえ、JPCERT/CC でも IEC 62443 シリーズ標準で定義されたさまざまなセキュリティ上の概念を現場の方々にご理解いただき、IEC 62443 の活用に向けた橋渡しになることを期待して、IEC 62443 に登場する主なセキュリティ概念を順次取り上げて紹介する「標準から学ぶ ICS セキュリティ」と題した連載をはじめることにしました。この連載は、厳密で固い標準の解説というよりは、気軽に読んでいただける読み物をめざして執筆していくことにしています。そのような意味で役立てていただければ幸いです。
連載記事は次の Web ページをご参照ください。

標準から学ぶ ICS セキュリティ
https://www.jpcert.or.jp/ics/information07.html

目次

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。ただし、「6.フィッシング対策協議会の会員組織向け活動」に記載の活動についてはこの限りではありません。また、「4. 国際連携活動関連」、「8. 主な講演活動」、「9. 協力、後援」には、受託事業以外の自主活動に関する記載が一部含まれています。

# 1. 早期警戒

## 1.1. インシデント対応支援

JPCERT/CC が本四半期に受け付けた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。）
に関する報告は、報告件数ベースで 13,564 件、インシデント件数ベースでは 10,656 件でした (注 1)。

（注 1）「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。また、「インシデント件数」は、各報告に含まれるインシデントの件数の合計を示し、1 つのインシデントに関して複数の報告が寄せられた場合にも 1 件のインシデントとして扱います。

JPCERT/CC が国内外のインシデントに関連するサイトとの調整を行った件数は 6,444 件でした。前四半期の 7,890 件と比較して 18%減少しています。「調整」とは、フィッシングサイトが設置されているサイトや、改ざんにより JavaScript が埋め込まれているサイト、ウイルス等のマルウェアが設置されたサイト、「scan」のアクセス元等の管理者等に対し、状況の調査や問題解決のための対応を依頼する活動です。

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。

インシデント報告対応活動の詳細については、別紙「JPCERT/CC インシデント報告対応レポート」をご参照ください。

JPCERT/CC インシデント報告対応レポート
https://www.jpcert.or.jp/pr/2022/IR_Report2022Q2.pdf

### 1.1.1. インシデントの傾向

#### 1.1.1.1. フィッシングサイト

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 7,520 件で、前四半期の 8,088 件から 7%減少しました。また、前年度同期（6,311 件）との比較では、19%の増加となりました。

本四半期のフィッシングサイトの報告件数を、装っていたブランドが国内か国外かで分けた内訳を添えて［表 1-1］に示します。

［表 1-1：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 | 7 月 | 8 月 | 9 月 | 本四半期合計（割合） |
|---|---|---|---|---|
| 国内ブランド | 1,410 | 1,394 | 1,387 | 4,191(56%) |
| 国外ブランド | 884 | 854 | 924 | 2,662(35%) |
| ブランド不明 (注 5) | 186 | 225 | 256 | 667(9%) |
| 全ブランド合計 | 2,480 | 2,473 | 2,567 | 7,520 |

（注 2）「ブランド不明」は、報告されたフィッシングサイトが停止していた等の理由により、JPCERT/CC が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。

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 69.4%、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 50.7%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多く、海外ブランド全体の半分以上を占めていました。
国内ブランドでは、三井住友カードや三菱 UFJ ニコスカードといったクレジットカード会社を装ったものが非常に多く、ETC の利用照会サービスやえきねっと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。

8 月頃からは、国税庁を装ったフィッシングサイトの報告が多く寄せられました。フィッシングサイトにアクセスすると税金の滞納があると通知され、プリペイドカードやクレジットカード情報の入力を求められるもので、中にはサブドメインに「ntago-jp」や「jpnta」といった国税庁を思わせる文字列が含まれるものもありました。

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 28%、国外が 72%であり、前四半期（国内が 26%、国外が 74%）と比較し国内が増加しました。

#### 1.1.1.2. Web サイト改ざん

本四半期に報告が寄せられた Web サイト改ざんの件数は、695 件でした。前四半期の 557 件から 25%増加しています。

本四半期は、正規の Web サイトに不正に WebShell を設置し、その WebShell を用いて E コマースサイトやメールサービスを装ったフィッシングサイトのコンテンツを設置したり、Web サイトに不審なサイトへの転送スクリプト（［図 1-1］）を挿入したりする事例が複数報告されました。［図 1-2］に、設置された WebShell の例を示します。この WebShell を使用することで、ファイルのアップロード等が可能になります。

```
<script>
window.location = "https://[redacted]";
</script>
```

［図 1-1：転送スクリプト］


［図 1-2：設置された WebShell］

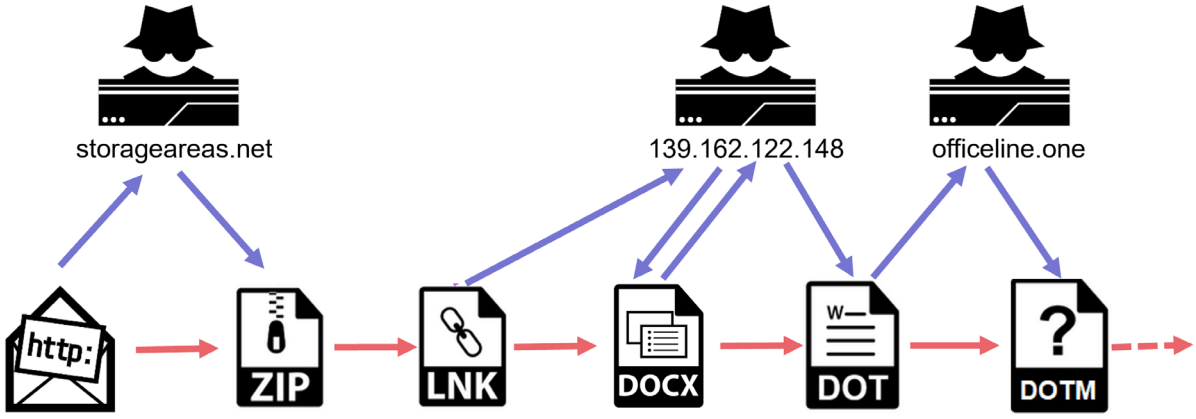
#### 1.1.1.3. その他

標的型攻撃に分類されるインシデントの件数は、2 件でした。
次に、確認されたインシデントを紹介します。

(1) 不正なショートカットファイルをダウンロードさせる攻撃

本四半期は、不正なショートカットファイルをダウンロードさせる標的型攻撃メールを複数確認しました。確認された手口は、問い合わせメールを送り付け、何度かメールのやり取りを行った後に、短縮 URL リンクを記載したメールを送り付け、そのリンクをクリックさせることにより、不正なショートカットファイルが格納された ZIP ファイルをダウンロードさせるというものでした。

［図 1-3］に、この攻撃の流れを示します。不正なショートカットファイル（［図 1-3］の LNK ファイル）は、インターネット経由で Word 文書（［図 1-3］の DOCX ファイル）をダウンロードし開きます。この Word 文書は、さらに Word 文書のテンプレートファイル（［図 1-3］の DOT ファイル）をダウンロードし開きます。このテンプレートファイルが開かれる際に利用者が求めに応じてマクロを有効化すると、テンプレート内のマクロにより、このテンプレートファイルが Microsoft Word のスタートアップフォルダーに保存されます。以降 Word ファイルを開くたびに、スタートアップフォルダーに保存されたテンプレートファイル中のマクロが、新たなファイル（［図 1-3］の DOTM ファイル）をダウンロードする仕組みになっていました。




［図 1-3：攻撃の流れ］

本攻撃は、前四半期から確認されており、継続して攻撃活動が行われていることがうかがえます。

(2) マルウェア FlowCloud を使用した攻撃

マルウェア FlowCloud を端末に感染させる攻撃を確認しました。FlowCloud は、攻撃グループ TA410 が使用している RAT です。FlowCloud に感染した端末から情報を窃取することを目的としていたと考えられます。

### 1.1.2. インシデントに関する情報提供のお願い

Web サイト改ざん等のインシデントを認知された場合は、JPCERT/CC にご報告ください。JPCERT/CC では、当該案件に関して攻撃に関与してしまう結果となった機器等の管理者への対応依頼等の必要な調整を行うとともに、同様の被害の拡大を抑えるため、攻撃方法の変化や対策を分析し、随時、注意喚起等の情報発信を行います。

インシデントによる被害拡大および再発の防止のため、今後とも JPCERT/CC への情報提供にご協力をお願いいたします。

## 1.2. 情報収集・分析

JPCERT/CC では、国内の企業ユーザーが利用するソフトウェア製品の脆弱性情報や国内のインターネットユーザーが影響を受ける可能性のあるコンピューターウイルス、Web サイト改ざんなどのサイバー攻撃に関する情報を収集し、分析しています。これらのさまざまな情報を多角的に分析し、あわせて脆弱性やウイルス検体の検証等も必要に応じて行っています。さらに、分析結果に応じて、国内の企業、組織のシステム管理者を対象とした「注意喚起」（一般公開）や、国内の重要インフラ事業者等を対象とした「早期警戒情報」（限定配付）などを発信することにより、国内におけるサイバーインシデントの発生や拡大の抑止を目指しています。

### 1.2.1. 情報提供

JPCERT/CC の Web ページ（https://www.jpcert.or.jp/）や RSS、約 33,000 名の登録者を擁するメーリングリスト、早期警戒情報の提供用ポータルサイト CISTA（Collective Intelligence Station for Trusted Advocates）等を通じて情報提供を行いました。

#### 1.2.1.1. 注意喚起

深刻かつ影響範囲の広い脆弱性等が公表された場合には、「注意喚起」と呼ばれる文書を発行し、利用者に対して広く対策を呼びかけています。本四半期は次のような注意喚起を発行しました。

発行件数：8 件（うち更新情報が 0 件）　https://www.jpcert.or.jp/at/

2022-07-13　2022 年 7 月マイクロソフトセキュリティ更新プログラムに関する注意喚起 (公開)
2022-07-13　Adobe Acrobat および Reader の脆弱性（APSB22-32）に関する注意喚起 (公開)
2022-07-20　2022 年 7 月 Oracle 製品のクリティカルパッチアップデートに関する注意喚起 (公開)
2022-08-10　2022 年 8 月マイクロソフトセキュリティ更新プログラムに関する注意喚起 (公開)
2022-08-10　Adobe Acrobat および Reader の脆弱性（APSB22-39）に関する注意喚起 (公開)
2022-08-24　Movable Type の XMLRPC API の脆弱性に関する注意喚起 (公開)
2022-09-13　Trend Micro Apex One および Trend Micro Apex One SaaS の脆弱性に関する注意喚起 (公開)
2022-09-14　2022 年 9 月マイクロソフトセキュリティ更新プログラムに関する注意喚起 (公開)

#### 1.2.1.2. Weekly Report

JPCERT/CC が収集したセキュリティ関連情報のうち重要と判断した情報の概要をレポートにまとめ、原則として毎週水曜日（週の第 3 営業日）に Weekly Report として発行しています。このレポートには、「ひとくちメモ」として、情報セキュリティに関する豆知識やお知らせ等も掲載しています。本四半期における発行は次のとおりです。

発行件数：13 件　https://www.jpcert.or.jp/wr/

Weekly Report で扱った情報セキュリティ関連情報の項目数は合計 78 件、「今週のひとくちメモ」のコーナーで紹介した情報は次の 13 件でした。

2022-07-06　JPCERT/CC 感謝状 2022
2022-07-13　オフィスと自宅の Wi-Fi 接続端末をサイバースパイから守る
2022-07-21　JPCERT/CC が「なぜ、SSL-VPN 製品の脆弱性は放置されるのか “サプライチェーン”攻撃という言葉の陰で見過ごされている攻撃原因について」を公開

2022-07-27　「製品セキュリティインシデント対応チーム（PSIRT）成熟度ドキュメント」の日本語訳が公開
2022-08-03　JPCERT/CC が「サイバー政策動向を知ろう Watch! Cyber World vol.3 | 中国の法整備」を公開
2022-08-10　連載「標準から学ぶ ICS セキュリティ」の初回を公表
2022-08-17　JPCERT/CC が「A File Format to Aid in Security Vulnerability Disclosure - 正しくつながる第一歩」を公開
2022-08-24　日本シーサート協議会が「メール訓練手引書一般公開版 v1.0」を公開
2022-08-31　JAIPA Cloud Conference 2022 開催のお知らせ
2022-09-07　SecurityDays Fall 2022 開催
2022-09-14　フィッシング対策協議会が「各ブラウザーによる SSL/TLS サーバー証明書の表示の違い」を更新
2022-09-22　JPCERT/CC が「攻撃グループ BlackTech による F5 BIG-IP の脆弱性（CVE-2022-1388）を悪用した攻撃」を公開
2022-09-28　JPCERT/CC が「「積極的サイバー防御」（アクティブ・サイバー・ディフェンス）とは何か ―より具体的な議論に向けて必要な観点について―」を公開

#### 1.2.1.3. 早期警戒情報

重要インフラを支える組織の情報セキュリティ関連部署もしくは組織内 CSIRT のうち、「早期警戒情報」という枠組みに参加いただいた方々に向けて、セキュリティ上の深刻な影響をもたらす可能性のある脅威情報やその分析結果、対策方法に関する「早期警戒情報」と呼ばれる情報を、各組織における必要性を勘案して、提供しています。本四半期には 2 件の早期警戒情報を発信しました。

「早期警戒情報」の枠組みへの参加については次の Web ページを参考にご検討ください。

早期警戒情報
https://www.jpcert.or.jp/wwinfo/

#### 1.2.1.4. CyberNewsFlash

JPCERT/CC は、脆弱性やマルウェア、サイバー攻撃などに関する最新情報を CyberNewsFlash としてタイムリーに発信しています。発行時点で注意喚起の基準に満たない脆弱性の情報やセキュリティアップデート予告なども含まれます。本四半期に公表した CyberNewsFlash は次のとおりです。

発行件数：11 件（うち更新情報が 2 件）　https://www.jpcert.or.jp/newsflash/

2022-07-12　2022 年 4 月から 6 月を振り返って
2022-07-13　Intel 製品に関する複数の脆弱性について
2022-07-13　複数のアドビ製品のアップデートについて

2022-08-10　Intel 製品に関する複数の脆弱性について
2022-08-10　複数のアドビ製品のアップデートについて
2022-08-18　Apple 製品のアップデートについて（2022 年 8 月）
2022-08-19　Apple 製品のアップデートについて（2022 年 8 月）（更新）
2022-09-01　Apple 製品のアップデートについて（2022 年 8 月）（更新）
2022-09-13　Apple 製品のアップデートについて（2022 年 9 月）
2022-09-14　複数のアドビ製品のアップデートについて
2022-09-22　ISC BIND 9 における複数の脆弱性について（2022 年 9 月）

### 1.2.2. 情報収集・分析・提供（早期警戒活動）事例

本四半期における情報収集・分析・提供（早期警戒活動）の事例を紹介します。

(1) Trend Micro Apex One および Trend Micro Apex One SaaS の脆弱性に関する情報発信
2022 年 9 月 13 日、トレンドマイクロ株式会社から、Trend Micro Apex One および Trend Micro Apex One SaaS の脆弱性（CVE-2022-40139）に関する情報が公表されました。
本脆弱性が悪用された場合、当該製品の管理コンソールにログイン可能な遠隔の第三者が、任意のコードを実行する可能性があり、トレンドマイクロ株式会社によると、本脆弱性を悪用した攻撃をすでに確認しているとのことで、JPCERT/CC は同日に注意喚起を公開しました。

Trend Micro Apex One および Trend Micro Apex One SaaS の脆弱性に関する注意喚起
https://www.jpcert.or.jp/at/2022/at220023.html

(2) Movable Type の XMLRPC API における脆弱性（CVE-2022-38078）に関する情報発信
2022 年 8 月 24 日、シックス・アパート株式会社から、Movable Type の XMLRPC API におけるコマンドインジェクションの脆弱性（CVE-2022-38078）に関する情報が公表されました。
本脆弱性が悪用された場合、遠隔の第三者が Movable Type が動作するシステム上で、任意の Perl スクリプトや任意の OS コマンドを実行する可能性があるため、JPCERT/CC は同日に注意喚起を公開しました。

Movable Type の XMLRPC API の脆弱性に関する注意喚起
https://www.jpcert.or.jp/at/2022/at220022.html

## 1.3. インターネット上の脆弱なノード数の分布の分析

### 1.3.1. インターネットリスク可視化サービス　― Mejiro ―

インターネットリスク可視化サービス Mejiro では、次のポートがインターネットに対して開いているノードを Distributed Reflection Denial of Service（リフレクション型 DoS 攻撃）に悪用される恐れのあるインターネット上のリスク要因と見なし、国や地域ごとにその分布状況を分析しています。

・19/udp（CHARGEN）
・53/udp（DNS）
・123/udp（NTP）
・161/udp（SNMP）
・445/tcp（MSDS）
・1900/udp（SSDP）
・5060/udp（SIP）

それらのノードの IP アドレスをもとにノードが設置された国・地域を判別して、リスク要因の分布状況を調べます。さらに、国・地域ごとのリスク要因となるノード数から、Mejiro 指標と呼ばれる指標値を算出します。各国・地域の Mejiro 指標の値を比較することで、それぞれの国・地域の相対的な特徴を明らかにして、対策の必要性や方向性を判断する参考にできると期待し、一般に公表する活動を継続しています。

#### 1.3.1.1. Mirai 型の特徴があるパケット送信元の地域差への注目

TSUBAME では前四半期から継続して Mirai 型の特徴がある国内外のノードを送信元とするパケットを観測しています。これらの送信元ノードについての地域差を Mejiro 指標の計算方法を当てはめて分析しました。それぞれの地域の指標を相互に比較してみると、いずれの地域でも同じように Mirai 型の特徴を持つ送信元ノードが観測されており、多くの地域で感染が放置されたままになっているのではないかと考えられます。
JPCERT/CC では感染の原因となった要因を調べ、関係者に情報を提供して、問題解決を図るよう努めています。
本四半期も、インドネシア、マレーシア、フィリピン、シンガポール、タイ、ブルネイ、ベトナム、ラオス、ミャンマー、カンボジアの 10 カ国に対して Mejiro 指標を提供しました。

> 実証実験:インターネットリスク可視化サービス―Mejiro―
> https://www.jpcert.or.jp/mejiro/index.html

#### 1.3.1.2. インターネット上の環境変化に対する分析

インターネット上のリスク環境分析の一環として、スキャンに応答するノード数の時系列推移も追跡しています。社会経済活動、自然災害などの影響が、観測できるインターネット・ノード数の変化として現れることもあり、長期的なトレンドとあわせて注視しています。
本四半期には、現在の国際情勢を鑑み、ウクライナにおけるスキャン応答の変化を前四半期から引き続き分析しました。この内容は CISTA 情報共有会内の「サイバーメトリクスグループ活動紹介～データでみるウクライナ」で紹介しました。

### 1.3.2. インターネット上の探索活動や攻撃活動に関する観測と分析

#### 1.3.2.1. インターネット定点観測システム TSUBAME を用いた観測

JPCERT/CC では、不特定多数に向けて発信されるパケットを収集する観測用センサーを開発し、海外の National CSIRT 等の協力のもと、これを各地域に複数分散配置した、インターネット定点観測システム「TSUBAME」を構築し運用しています。TSUBAME から得られる情報を、すでに公開されている脆弱性情報やマルウェア、攻撃ツールの情報などと対比して分析することで、攻撃活動や攻撃の準備活動等を把握できる場合があります。
センサーの観測結果を一つのデータベースにまとめて、観測用センサーの設置に協力した各地域 National CSIRT 等と共有しデータの共同での分析や、グローバルな視野から攻撃活動等の迅速な把握に努めています。TSUBAME については、次の Web ページをご参照ください。

TSUBAME（インターネット定点観測システム）
https://www.jpcert.or.jp/tsubame/index.html

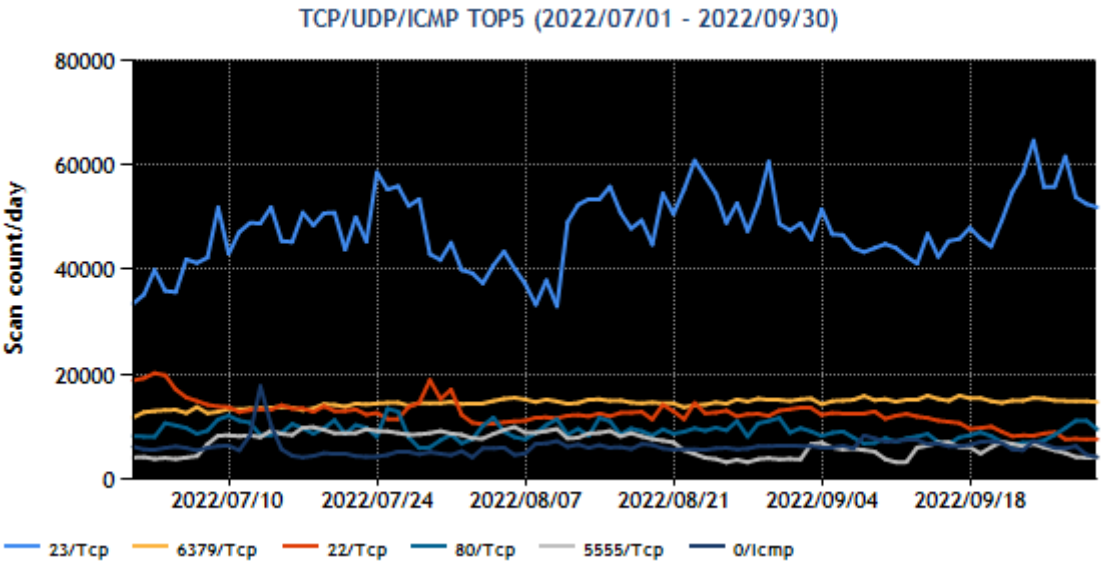
#### 1.3.2.2. TSUBAME の観測データの活用

JPCERT/CC では、主に各組織のシステム管理者の方々に、自組織のネットワークに届くパケットの傾向と比較していただけるよう、日本国内の TSUBAME のセンサーで受信したパケットを宛先ポート別に集計してグラフ化し、毎週月曜日に JPCERT/CC の Web ページで公開しています。また、四半期ごとに観測傾向や注目される現象を紹介する「インターネット定点観測レポート」を公開しており、2022 年 4 月から 6 月の期間に関するレポートを 7 月 28 日に公開し、書き切れなかった内容を 2022 年 8 月 4 日にブログで公開しました。

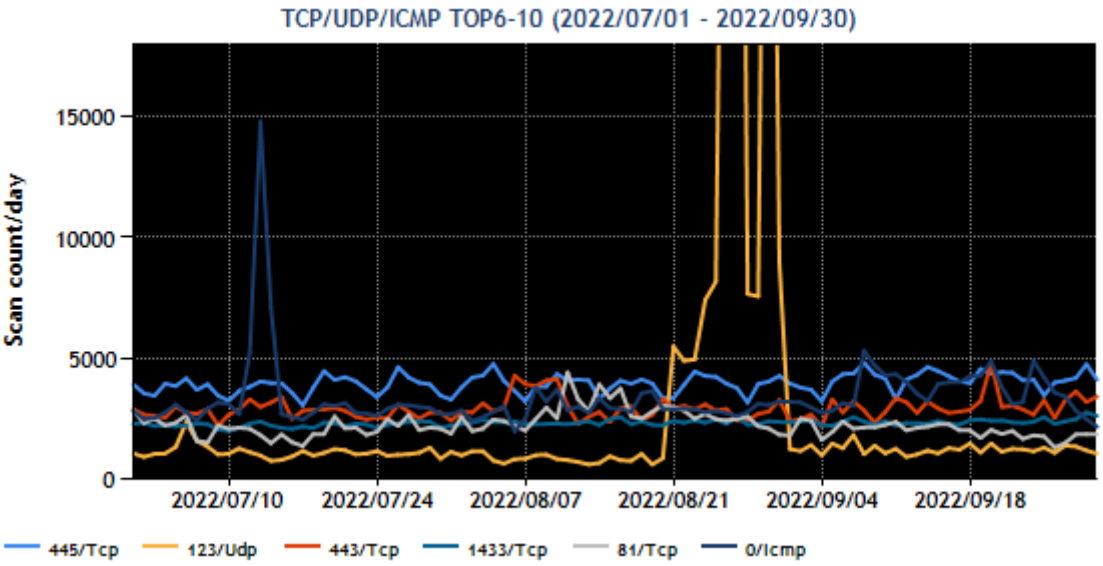
TSUBAME 観測グラフ
https://www.jpcert.or.jp/tsubame/index.html#examples
インターネット定点観測レポート（2022 年 4～6 月）
https://www.jpcert.or.jp/tsubame/report/report202204-06.html
TSUBAME レポート Overflow（2022 年 4～6 月）
https://blogs.jpcert.or.jp/ja/2022/08/tsubame_overflow_2022-04-06.html

#### 1.3.2.3. TSUBAME 観測動向

本四半期に TSUBAME で観測された宛先ポート別パケット数の上位 1～5 位および 6～10 位を［図 1-4］と［図 1-5］示します。

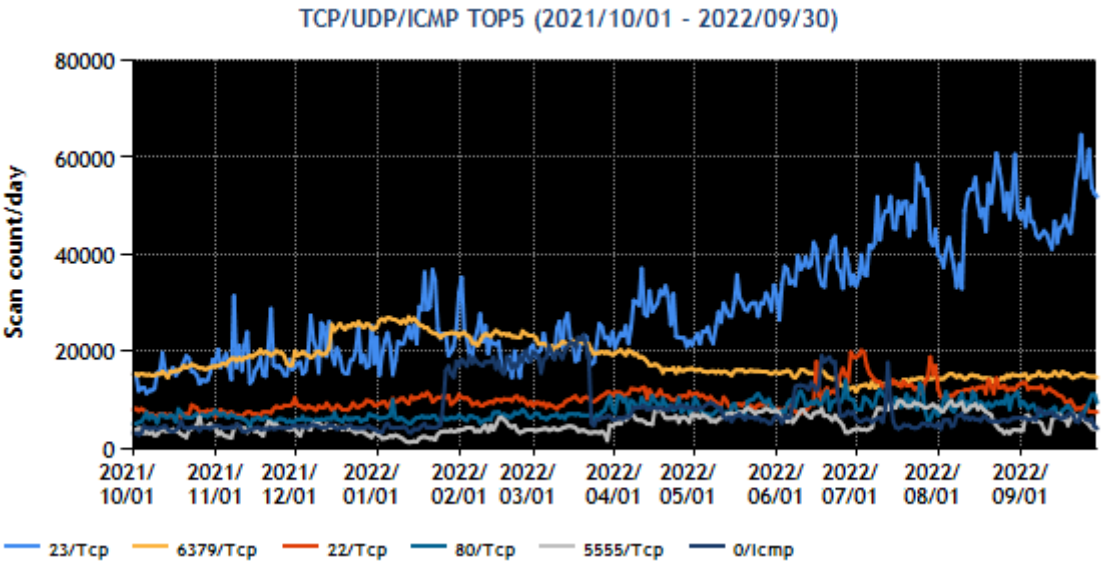



［図 1-4：宛先ポート別グラフ トップ 1-5（2022 年 7 月 1 日-9 月 30 日）］

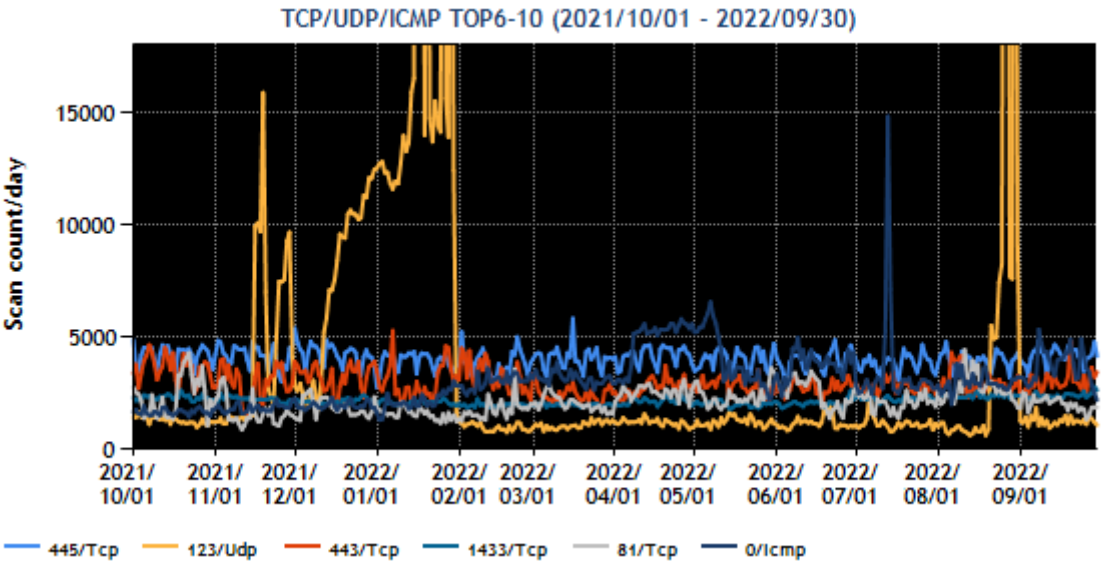



［図 1-5：宛先ポート別グラフ トップ 6-10（2022 年 7 月 1 日-9 月 30 日）］

また、過去 1 年間（2021 年 10 月 1 日-2022 年 9 月 30 日）における、宛先ポート別パケット数の上位 1～5 位および 6～10 位を［図 1-6］と［図 1-7］に示します。




［図 1-6：宛先ポート別グラフ トップ 1-5（2021 年 10 月 1 日-2022 年 9 月 30 日）］




［図 1-7：宛先ポート別グラフ トップ 6-10（2021 年 10 月 1 日-2022 年 9 月 30 日）］

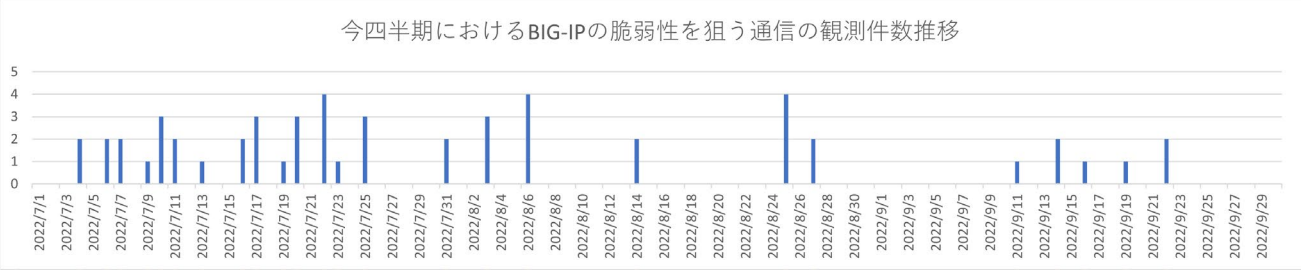
本四半期に最も多く観測されたパケットは 23/TCP（telnet）宛の通信でした。次いで多く観測されたパケットが 6379/TCP（redis）宛の通信です。それ以外の Port に対するパケットは増減があるものの順位がいれ変わるほどの変化はありませんでした。

#### 1.3.2.4. 定点観測網の拡充に向けた運用とその分析

JPCERT/CC では、インターネット上に低対話型ハニーポットを設置して攻撃者から送られてくる種々

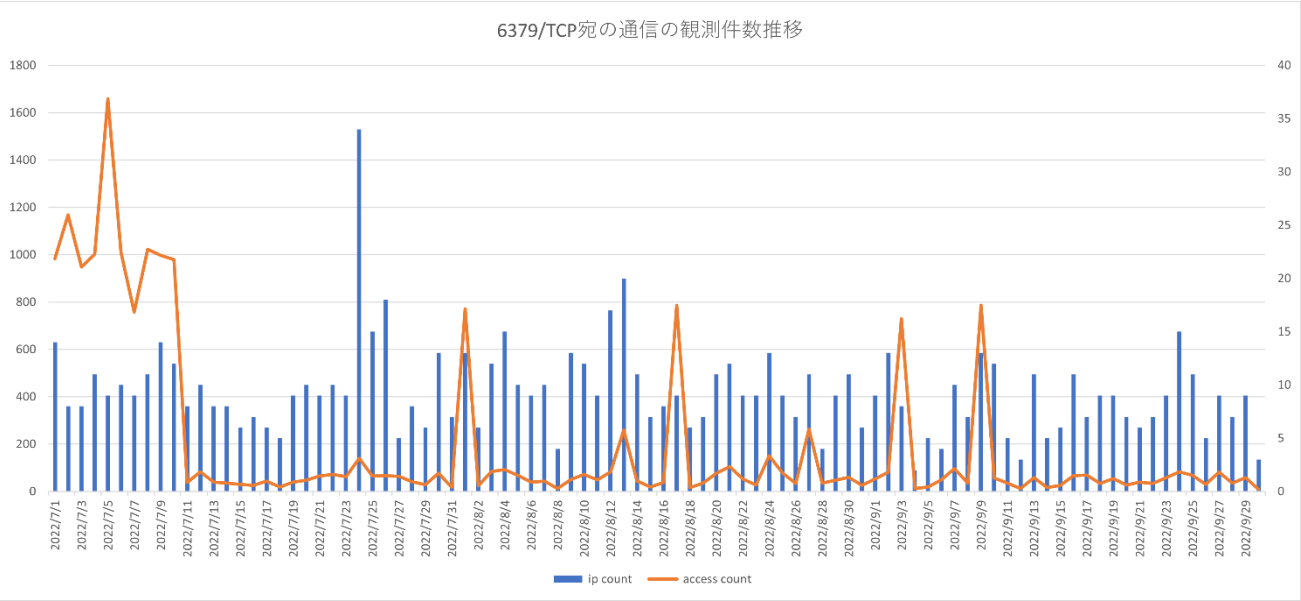
の通信内容を収集し、攻撃活動を分析しています。現在は、HTTP プロトコルと Redis で用いるプロトコル RESP（REdis Serialization Protocol）に応答する 2 種類のハニーポットを運用しています。

前四半期に公開された BIG-IP 製品の脆弱性（CVE-2022-1388）を狙う通信を今四半期も一日あたり平均 2 件程度の頻度で観測しています。通信のペイロード部の特徴については前四半期と変化なく、公開された概念実証コードをそのまま利用してコマンドの実行を試みるものでした。




［図 1-8：今四半期における BIG-IP の脆弱性を狙う通信の観測件数推移］

前四半期で増加傾向が見られていた Redis に対する攻撃活動が今四半期は減少傾向に転じました。攻撃の手法は以前と大差がなく、Config（Redis の設定情報を読み書き）、Set（値を設定）、Save（保存、データ永続化）コマンドを組み合わせることで悪意のあるスクリプトを Redis 上で実行させようとするものでした。




［図 1-9：今四半期における 6379/TCP 宛の通信の観測件数推移］

上記の他、今四半期において特筆すべき攻撃活動は観測されませんでした。今後 JPCERT/CC ではハニーポットの種類を増やし、観測の幅を増やしていく予定です。

## 2. 脆弱性関連情報流通促進活動

JPCERT/CC は、ソフトウェア製品利用者の安全確保を図ることを目的として、発見された脆弱性情報を適切な範囲に適時に開示して製品開発者による対策を促進し、脆弱性情報と製品開発者が用意した対策情報を脆弱性情報ポータル JVN（Japan Vulnerability Notes；独立行政法人情報処理推進機構［IPA］と共同運営）を通じて公表することで広く注意喚起を行う活動を行っています。さらに、脆弱性の作り込みを防ぐためのセキュアコーディングの普及や、制御システムの脆弱性の問題にも取り組んでいます。

### 2.1. 脆弱性関連情報の取り扱い状況

#### 2.1.1. 受付機関である独立行政法人情報処理推進機構（IPA）との連携

JPCERT/CC は、経済産業省告示「ソフトウエア製品等の脆弱性関連情報に関する取扱規程」（平成 29 年経済産業省告示第 19 号（以下「本規程」という。）に基づいて製品開発者とのコーディネーションを行う「調整機関」に指定されています。本規程で受付機関に指定されている IPA から届け出情報の転送を受け、本規程を踏まえて取りまとめられた「情報セキュリティ早期警戒パートナーシップガイドライン（以下「パートナーシップガイドライン」という。）に従って、対象となる脆弱性に関係する製品開発者の特定、脆弱性関連情報の適切な窓口への連絡、開発者による脆弱性の検証などの対応や脆弱性情報の公表スケジュール等に関する調整を行い、原則として、調整した公表日に JVN を通じて脆弱性情報等を一般に公表しています。JPCERT/CC は、脆弱性情報の分析結果や脆弱性情報の取り扱い状況の情報交換を行うなど、IPA と緊密な連携を行っています。なお、脆弱性関連情報に関する四半期ごとの届け出状況については、次の Web ページをご参照ください。

独立行政法人情報処理推進機構（IPA）脆弱性対策
https://www.ipa.go.jp/security/vuln/

#### 2.1.2. Japan Vulnerability Notes（JVN）において公表した脆弱性情報および対応状況

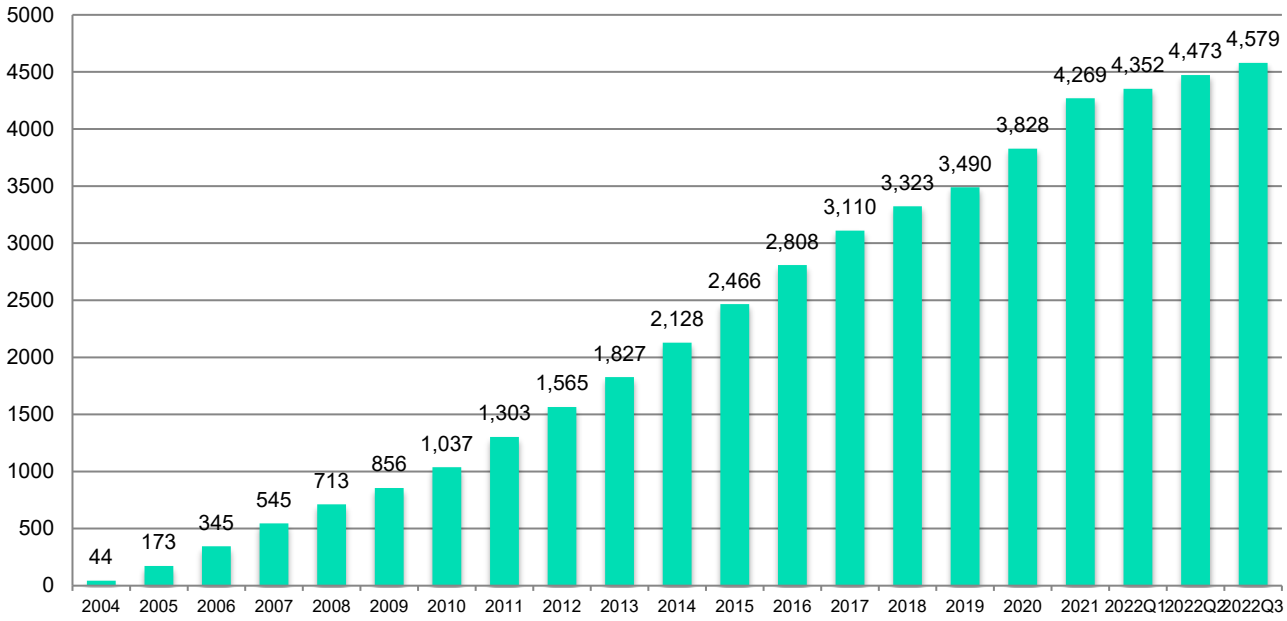
JVN で公表している脆弱性情報は、本規程に従って国内で届け出られた脆弱性に関するもの（以下「国内取扱脆弱性情報」という。;「JVN#」に続く 8 桁の数字の形式の識別子を付与している；例：JVN#12345678）と、それ以外の脆弱性に関するもの（以下「国際取扱脆弱性情報」という。;「JVNVU#」に続く 8 桁の数字の形式の識別子を付与している；例：JVNVU#12345678）の 2 種類に分類されます。

国際取扱脆弱性情報には、CERT/CC や CISA ICS 、NCSC-NL、NCSC-FI といった海外の調整機関に届け出がなされ国際調整が行われた脆弱性情報や、海外の製品開発者から JPCERT/CC に直接届け出がなされた自社製品の脆弱性情報、海外の発見者から JPCERT/CC に直接届け出がなされた脆弱性情報等が含まれます。なお、国際取扱脆弱性情報には、US-CERT からの脆弱性注意喚起等の邦訳を含めていますが、これには「JVNTA」に続く 8 桁数字の形式の識別子（例えば JVNTA#12345678）を使っています。

本四半期に JVN において公表した脆弱性情報は 106 件（累計件 4,579）で、累計の推移は［図 2-1］に

示すとおりです。本四半期に公表された個々の脆弱性情報に関しては、次の Web ページをご参照ください。

JVN（Japan Vulnerability Notes）
https://jvn.jp/



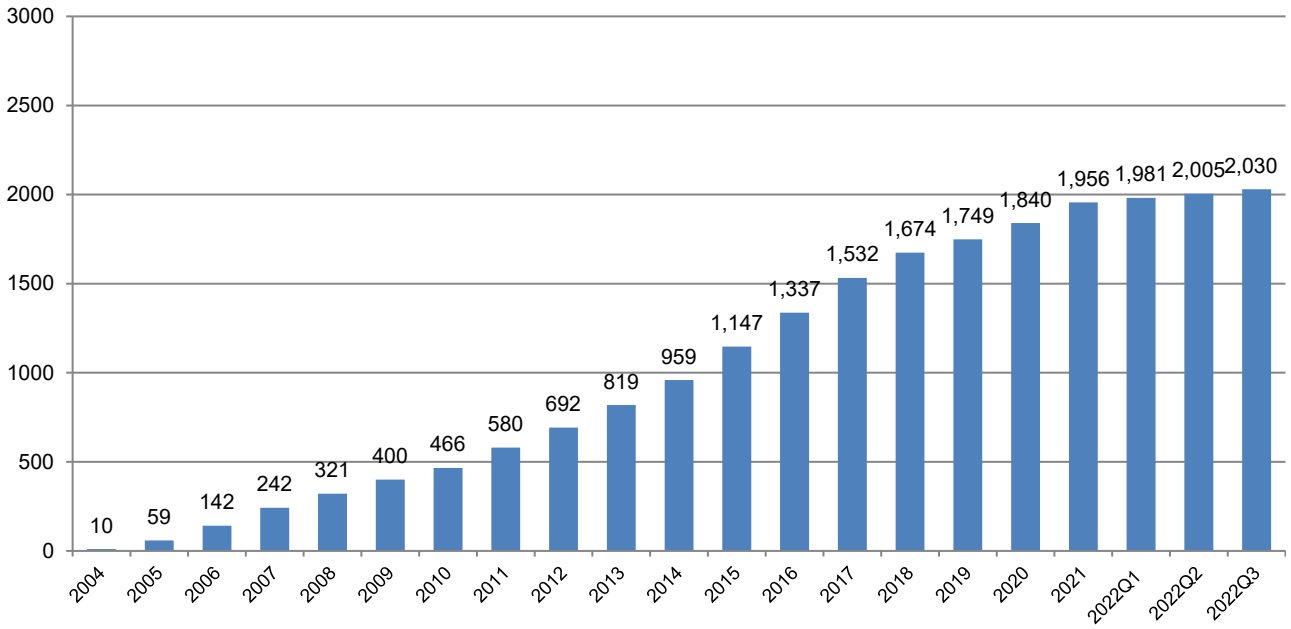

［図 2- 1：JVN 公表累積件数］

本四半期において公表に至った脆弱性情報のうち、国内取扱脆弱性情報は 25 件（累計 2,030 件）で、累計の推移は ［図 2-2］に示すとおりです。本四半期に公表した 25 件の内訳は、国内の単一の製品開発者の製品に影響を及ぼすものが 18 件（このうち自社製品の届け出によるものが 7 件）、海外の単一の製品開発者の製品に影響を及ぼすものが 7 件ありました。

本四半期に公表した脆弱性の影響を受けた製品のカテゴリーごとの内訳は、［表 2-1］のとおりです。本四半期は、CMS が 5 件と最も多く、次いでウェブアプリケーション、グループウェア、プラグイン、Windows アプリケーションがそれぞれ 3 件、続いてライブラリが 2 件、Android アプリケーション、iOS アプリケーション、アプリケーションフレームワーク、アンチウイルス製品、マルチプラットフォームアプリケーション、組込系製品がそれぞれ 1 件でした。

［表 2-1：公表を行った国内取扱脆弱性情報の件数の製品カテゴリー内訳］

| 製品分類 | 件数 |
|---|---|
| CMS | 5 |
| ウェブアプリケーション | 3 |
| グループウェア | 3 |
| プラグイン | 3 |
| Windows アプリケーション | 3 |
| ライブラリ | 2 |
| Android アプリケーション | 1 |
| iOS アプリケーション | 1 |
| アプリケーションフレームワーク | 1 |
| アンチウイルス製品 | 1 |
| マルチプラットフォームアプリケーション | 1 |
| 組込系製品 | 1 |




［図 2- 2：公表を行った国内取扱脆弱性情報の累積件数］

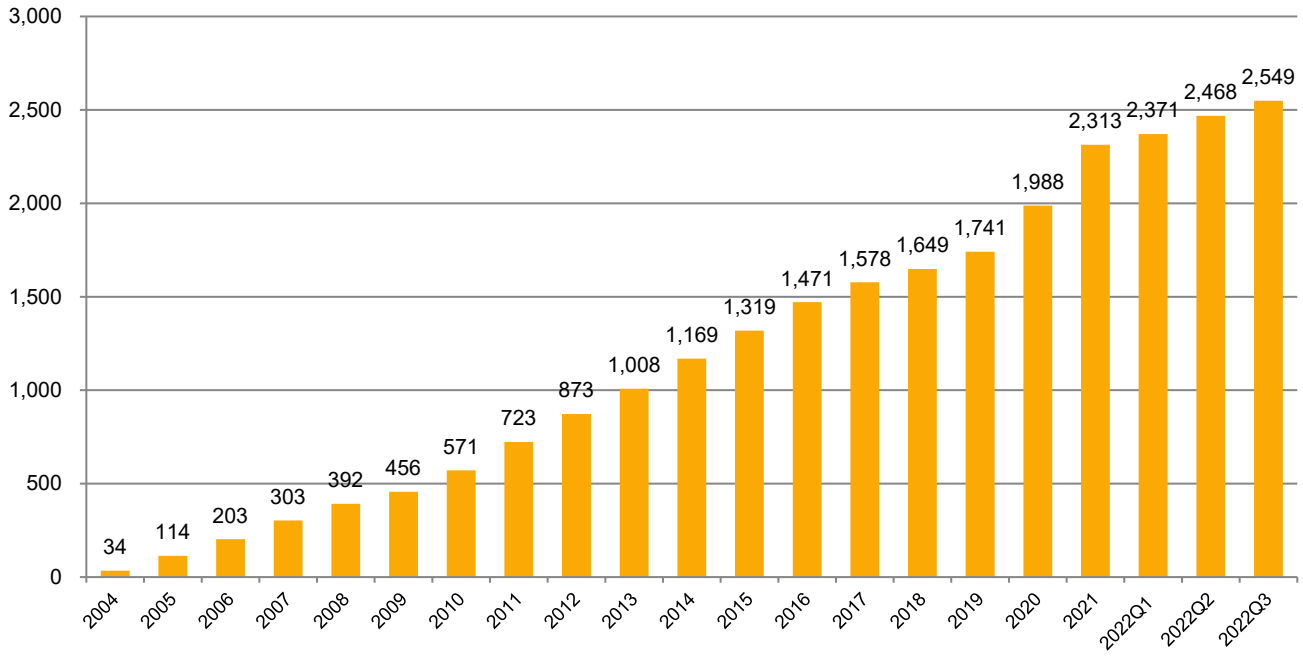
本四半期に公表した国際取扱脆弱性情報は 81 件（累計 2,549 件）で、累計の推移は［図 2-3］に示すとおりです。81 件のアドバイザリのうち、海外調整機関や製品開発者等からの届け出によるものおよび製品開発者による脆弱性情報公開の事前通知によるものは 16 件（このうち複数製品開発者の製品に影響を及ぼすものは 5 件）、国内外の発見者からの届け出によるものは 7 件、JPCERT/CC が注意喚起として発行したものは 58 件でした。

本四半期に公表した脆弱性の影響を受けた製品のカテゴリー内訳は、［表 2-2］のとおりです。本四半期は、制御系製品が 62 件と最も多く、次いで組込系製品が 8 件、医療機器が 3 件、アンチウイルス製品が 2 件、CMS、DNS、ウェブサーブレットコンテナ、サーバー製品、プロトコル、ライブラリがそれぞれ 1 件でした。

本四半期も、国際取扱脆弱性情報の中には、製品開発者自身が届け出たものや、自社製品に関する脆弱性情報を公開に先立って JPCERT/CC へ事前に通知したものが比較的多く見られました。また、国外の発見者からの届け出によるものも、本四半期においては比較的多くありました。このような製品開発者自身から広く一般への告知を目的としたものや、国内外の発見者から直接 JPCERT/CC に届け出られるもの等も含めて、脆弱性情報の流通、調整および公開を幅広く行っています。

［表 2-2：公表を行った国際取扱脆弱性情報の件数の製品カテゴリー内訳］

| 製品分類 | 件数 |
|---|---|
| 制御系製品 | 62 |
| 組込系製品 | 8 |
| 医療機器 | 3 |
| アンチウイルス製品 | 2 |
| CMS | 1 |
| DNS | 1 |
| ウェブサーブレットコンテナ | 1 |
| サーバー製品 | 1 |
| プロトコル | 1 |
| ライブラリ | 1 |




［図 2- 3：国際取扱脆弱性情報の公表累積件数］

### 2.1.3. 連絡不能開発者とそれに対する対応の状況等

本規程に基づいて報告された脆弱性について、製品開発者と連絡が取れない場合には、2011 年度以降、当該製品開発者名を JVN 上で「連絡不能開発者一覧」として公表し、連絡の手掛かりを広く求めています。これまでに 251 件（製品開発者数で 164 件）を公表し、52 件（製品開発者数で 32 件）の調整を再開することができ、脆弱性関連情報の取り扱いにおける「滞留」の解消に一定の効果を上げています。本四半期に連絡不能開発者一覧に新たに掲載した案件はありませんでした。本四半期末日時点で、合計 199 件の連絡不能開発者案件を掲載しており、継続して製品開発者や関係者からの連絡および情報提供を呼びかけています。

こうした呼びかけによっても製品開発者と連絡が取れない場合、IPA が招集する公表判定委員会が妥当と判断すれば公表できるように 2014 年から制度が改正されました。これまでに 2015 年度、2017 年度、2019 年度に公表判定委員会が開催され、そこでの審議を経て、累計で 30 件（製品開発者数で 19 件）を JVN の「Japan Vulnerability Notes JP（連絡不能）一覧」に掲載しています。

連絡不能開発者一覧
https://jvn.jp/reply/index.html

Japan Vulnerability Notes JP（連絡不能）一覧
https://jvn.jp/adj/

### 2.1.4. 海外 CSIRT との脆弱性情報流通協力体制の構築、国際的な活動

JPCERT/CC は、脆弱性情報の円滑な国際的流通のために、米国の CERT/CC および CISA ICS、英国の NCSC、フィンランドの NCSC-FI、オランダの NCSC など脆弱性情報ハンドリングを行っている海外の調整機関と協力関係を結び、必要に応じて脆弱性情報の共有、各国の製品開発者への通知および対応状況の集約、脆弱性情報の公表時期の設定などの調整活動を行っています。

JVN 英語版サイト（https://jvn.jp/en）上の脆弱性情報も日本語版と同時に公表しており、脆弱性情報の信頼できるソースとして、海外のセキュリティ関連組織等からも注目されています。

JPCERT/CC では、2008 年 5 月以降 JVN 英語版サイトの公開を機に CVE 採番を行っており、Top Level Root である MITRE やその他の組織への確認や照会を必要とする特殊なケース（全体の 1 割弱）と製品開発者等 CNA によって採番されたケースを除いて、JVN 上で公表する脆弱性のほぼすべてに CVE 番号を付与しています。本四半期には、JVN で公表したものに対し 54 個の CVE 番号を付与しました。

最初は CVE 番号の付与を、MITRE 社に採番依頼することで実施していましたが、2010 年 6 月には CNA（CVE Numbering Authorities）として CVE 番号を付与し始めました。2018 年には Root の役割を

付与され、製品開発者を新しい CNA に招致する活動やトレーニングなどの活動も行っています。CNA 招致活動の結果として、これまでに三菱電機株式会社、株式会社 LINE、日本電気株式会社（NEC）、株式会社東芝、パナソニック株式会社、株式会社日立製作所の 6 社が JPCERT/CC を Root とする CNA として登録されています。
CNA および CVE に関する詳細は、次の Web ページをご参照ください。

CNA（CVE Numbering Authority）
https://www.jpcert.or.jp/vh/cna.html

CVE Numbering Authorities
https://www.cve.org/PartnerInformation/Partner#CNA

About CVE
https://www.cve.org/About/Overview

JPCERT/CC Eyes「CNA 活動レポート ～日本の 2 組織が新たに CNA に参加～」
https://blogs.jpcert.or.jp/ja/2020/12/cna-2cna.html

Our CVE Story: JPCERT/CC
https://cve.mitre.org/blog/July072021_Our_CVE_Story_JPCERT_CC.html

### 2.2. 日本国内の脆弱性情報流通体制の整備

JPCERT/CC では、本規程に従って、日本国内の脆弱性情報流通体制を整備しています。
詳細については、次の Web ページをご参照ください。

脆弱性情報取扱体制
https://www.meti.go.jp/policy/netsecurity/vulinfo.html

脆弱性情報ハンドリングとは？
https://www.jpcert.or.jp/vh/

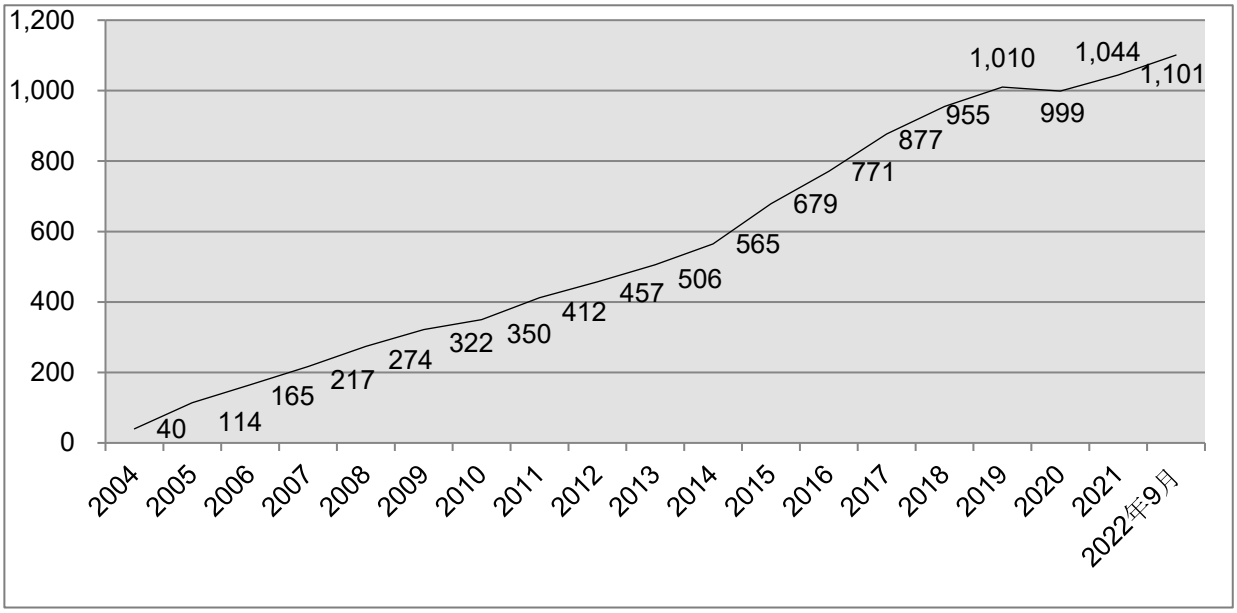
情報セキュリティ早期警戒パートナーシップガイドライン（2019 年版第 2 版）
https://www.jpcert.or.jp/vh/partnership_guideline2019_r2.pdf

JPCERT/CC 脆弱性情報取扱いガイドライン（2019 年版）
https://www.jpcert.or.jp/vh/vul-guideline2019.pdf

### 2.2.1. 日本国内製品開発者との連携

本規程では、脆弱性情報を提供する先となる製品開発者のリストを作成し、各製品開発者の連絡先情報を整備することが、調整機関である JPCERT/CC に求められています。JPCERT/CC では、製品開発者の皆さまに製品開発者リストへの登録をお願いしています。製品開発者の登録数は、[図 2-4]に示すとおり、2022 年 9 月 30 日現在で 1,101 となっています。登録等の詳細については、次の Web ページをご参照ください。

製品開発者登録
https://www.jpcert.or.jp/vh/register.html




［図 2-4：累計製品開発者登録数］

### 2.2.2. 製品開発者との定期ミーティング等の実施

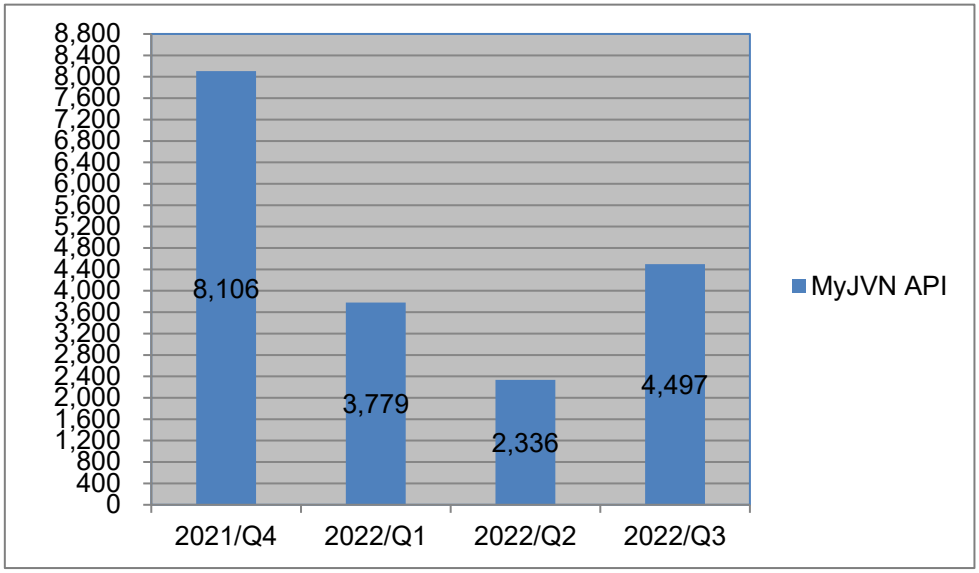
JPCERT/CC では、技術情報やセキュリティ・脆弱性の動向などの情報交換や、脆弱性情報流通業務に関する製品開発者との意見交換、また、製品開発者間の情報交換を目的として、脆弱性情報流通の活動にご協力いただいている製品開発者の皆さまとの定期ミーティングや特定のテーマに関する個別ミーティングを開催しています。
本四半期においては、製品開発者登録ベンダー全体を対象とした定期ミーティングを 9 月 30 日に開催し、製品開発者へ通知する脆弱性情報の選定に使用するキーワードリストの改定作業の進捗報告、SBOM 関連の動向の紹介、複数の製品開発者が関与する脆弱性情報コーディネーションにおける課題の紹介、および、意見交換を行いました。

### 2.3. VRDA フィードによる脆弱性情報の配信

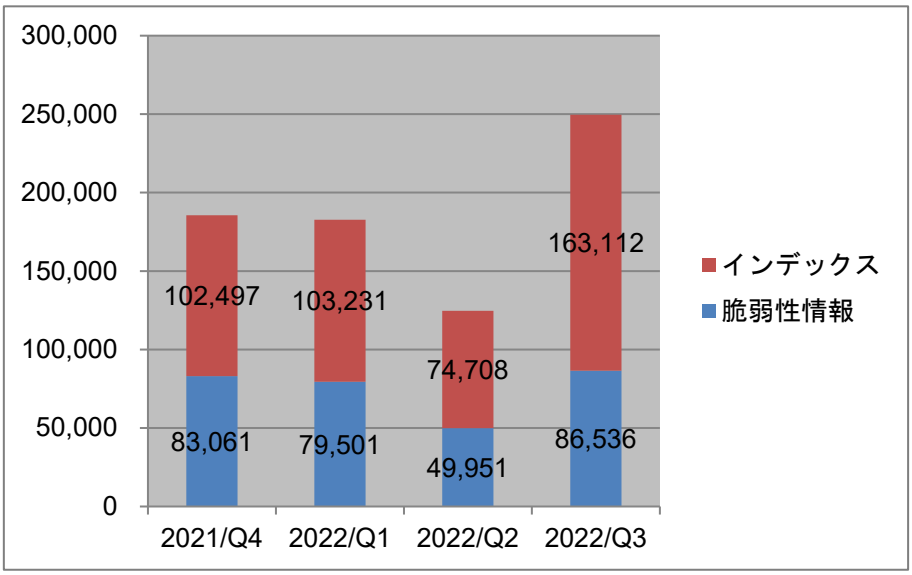
JPCERT/CC は、大規模組織の組織内 CSIRT 等での利用を想定して、ツールを用いた体系的な脆弱性対応を可能とするため、IPA が運用する MyJVN API を外部データソースとして利用した、VRDA（Vulnerability Response Decision Assistance）フィードによる脆弱性情報の配信を行っています。VRDA フィードについての詳しい情報は、次の Web ページをご参照ください。

VRDA フィード 脆弱性脅威分析用情報の定型データ配信
https://www.jpcert.or.jp/vrdafeed/index.html

四半期ごとに配信した VRDA フィード配信件数を［図 2- 5］に、VRDA フィードの利用傾向を［図 2- 6］と［図 2- 7］に示します。［図 2- 6］では、VRDA フィードインデックス（Atom フィード）と、脆弱性情報（脆弱性の詳細情報）の利用数を示します。VRDA フィードインデックスは、個別の脆弱性情報のタイトルと脆弱性の影響を受ける製品の識別子（CPE）を含みます。［図 2- 7］では、HTML と XML の 2 つのデータ形式で提供している脆弱性情報について、データ形式別の利用割合を示しています。

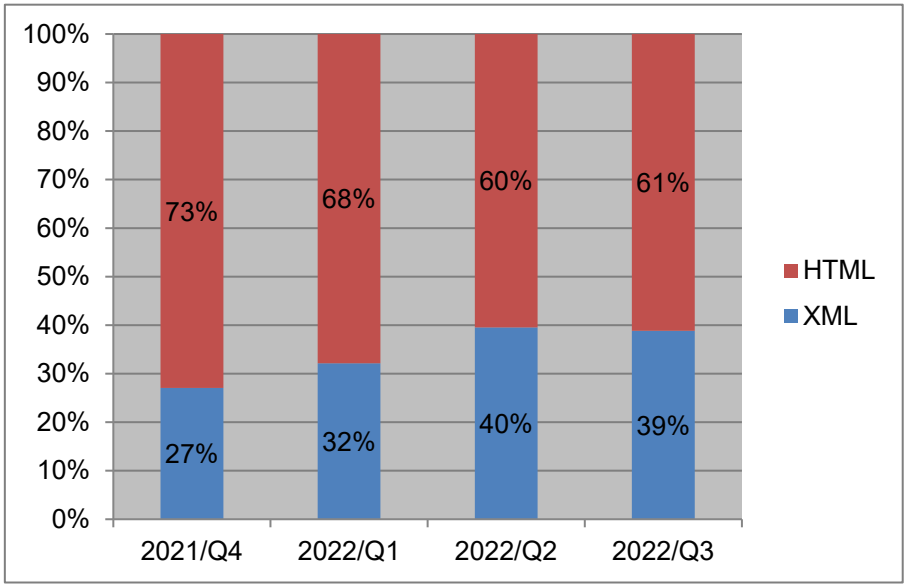



［図 2- 5：VRDA フィード配信件数］




［図 2-6：VRDA フィード利用件数］

インデックスの利用数については、［図 2-6］に示したように、前四半期と比較し、約 218%増加しました。脆弱性情報の利用数については、約 173%増加しました。




［図 2-7：脆弱性情報のデータ形式別利用割合］

脆弱性情報のデータ形式別利用傾向については、［図 2-7］に示したように、前四半期と比較し、大きな変化は見られませんでした。

# 3. 制御システムに関するセキュリティ対策活動

## 3.1. 情報収集分析

JPCERT/CC では、制御システムにおけるセキュリティに関わるインシデント事例や標準化活動の動向、その他セキュリティ技術動向に関するニュースや情報などを収集・分析し、必要に応じて国内組織等に情報提供を行っています。本四半期に収集・分析した情報は 92 件でした。

### 3.1.1. 情報提供

収集・分析した情報のうち、国内の制御システム関係者に影響があり注目すべきと判断したものを「参考情報」として適宜選んだ国内組織に提供しています。

本四半期に提供した参考情報は 3 件でした。

2022-07-29　石油・天然ガスパイプライン事業者向けのサイバーセキュリティ要件を定めた指令の改訂版を米国 TSA が公表
2022-08-08　CIP Standards の改訂を提案するホワイトペーパーのドラフト版を NERC が公表
2022-08-31　サイバーセキュリティ上のリスクにも配慮した新たな海洋安全保障戦略を英国が発表

また、海外での事例や、標準化動向などを JPCERT/CC からのお知らせとともに、制御システムセキュリティ情報共有コミュニティー（注 1）に登録いただいている関係者向けに制御システムセキュリティニュースレターとして配信していましたが、これを廃止し、今年度より「JPCERT/CC ICS Security Notes」を配信することになりました。

（注 1）JPCERT/CC が運営するコミュニティーで、制御システム関係者を中心に構成されています。

「JPCERT/CC ICS Security Notes」は、JPCERT/CC が収集する制御システムセキュリティ関連の公開情報のうち、特に着目していただきたい情報を選んでリスト形式で ICS ステークホルダーの方々へ四半期ごとに提供する情報サービスです。同期間に収集された情報をコンパクトにまとめてご提供いたしますので、その期間にどのような情報があったのかまとめてご覧いただくことができます。提供情報の形式は次のとおりです。

<< 1. ICS 関連の脆弱性情報 >>

- 脆弱性分析レポート（年 2 回公表予定）
  - ICS ユーザー組織の対策の参考として提供する JPCERT/CC が分析を行った ICS 関連製品の脆弱性分析レポート公表のお知らせ
- 脆弱性情報の一覧
  - JVN で公表した脆弱性情報のうち、ICS 関連製品の脆弱性情報の一覧

<< 2. ICS 関連の脅威情報 >>

- ICS 関連のインシデントやマルウェア等の脅威に関する情報

<< 3. ICS 関連のその他の情報 >>

- 調査レポートや国際標準、法規等、ICS セキュリティ対策の参考となるその他の情報

<< 4. JPCERT/CC からのお知らせ >>

- 脆弱性情報のご連絡、インシデント（セキュリティ事故）の調査やご相談等の連絡先、イベント告知等、JPCERT/CC からの各種お知らせ

また、JVN で公開された脆弱性情報のうち、ICS 関連製品の脆弱性情報もリスト形式で掲載しています。

本四半期に提供した ICS Security Notes は次の 1 件でした。

2022-07-06　JPCERT/CC ICS Security Notes FY2022_#Q1

JPCERT/CC では、制御システムセキュリティ情報共有コミュニティーに向けて、情報提供用メーリングリストと情報共有ポータルサイト ConPaS のサービスを設けており、メーリングリストには現在 1,283 名に登録していただいています。参加資格や申し込み方法については、次の Web ページをご参照ください。

制御システムセキュリティ情報共有コミュニティー
https://www.jpcert.or.jp/ics/ics-community.html

これらの情報提供以外にも、制御システムに関連するソフトウェアや機器において深刻かつ影響範囲の広い脆弱性等が公表された場合には、「注意喚起」と呼ばれる情報を発行し、利用者に対して広く対策を呼びかけています。また発行時点で注意喚起の基準に満たないものの、国内で利用が認められる制御システムに関連する製品の脆弱性情報について、特段の対策を呼びかけることを目的として情報提供しています。

#### 3.1.1.1. 注意喚起

本四半期に発行した注意喚起は 0 件でした。

#### 3.1.1.2. その他、特段の対策を呼びかけた脆弱性情報

本四半期に発行したその他、特段の対策を呼びかけた脆弱性情報は 0 件でした。

### 3.2. 制御システム関連のインシデント対応

JPCERT/CC は、制御システム関連のインシデント対応の活動として、インシデント報告の受付を行っています。本四半期における制御システムに関連するインシデントの報告件数は 0 件（0 IP アドレス）でした。

### 3.3. 関連団体との連携

SICE（計測自動制御学会）と JEITA（電子情報技術産業協会）、JEMIMA（日本電気計測器工業会）が定期的に開催している合同セキュリティ検討ワーキンググループに参加し、制御システムのセキュリティに関して専門家の方々と意見交換を行いました。

### 3.4. 制御システム向けセキュリティ自己評価ツールの提供

JPCERT/CC では、制御システムの構築と運用に関するセキュリティ上の問題項目を抽出し、バランスの良いセキュリティ対策を行っていただくことを目的として、簡便なセキュリティ自己評価ツールである日本版 SSAT（SCADA Self Assessment Tool：申し込み制）や J-CLICS（制御システムセキュリティ自己評価ツール：フリーダウンロード）を提供しています。本四半期は、日本版 SSAT に関し 4 件の利用申し込みがあり、直接配付件数の累計は、日本版 SSAT が 291 件でした。

日本版 SSAT（SCADA Self Assessment Tool）
https://www.jpcert.or.jp/ics/ssat.html

制御システムセキュリティ自己評価ツール（J-CLICS）
https://www.jpcert.or.jp/ics/jclics.html

### 3.5. 連載「標準から学ぶ ICS セキュリティ」の初回記事を公表

JPCERT/CC では、IEC 62443 シリーズという貴重な情報源を現場の方々に少しでも役立てていただくために、その中に書かれている主なセキュリティ概念を順次取り上げて紹介する、「標準から学ぶ ICS セキュリティ」と題した、気軽に読んでいただける連載を開始しました。

その初回の記事として「ICS セキュリティ標準 IEC 62443 シリーズの全体概要」を 2022 年 8 月 4 日に公表し、IEC62443 シリーズ標準の策定の経緯と全体構成の概要を紹介しました。現在進行中の策定作業の課題にも言及しています。

標準から学ぶ ICS セキュリティ：ICS セキュリティ標準 IEC 62443 シリーズの全体概要
https://www.jpcert.or.jp/ics/information07.html

連載「標準から学ぶ ICS セキュリティ」の初回を公表しました
https://blogs.jpcert.or.jp/ja/2022/08/ics-sec-standards-01.html

## 4. 国際連携活動関連

### 4.1. 海外 CSIRT 構築支援および運用支援活動

海外の National CSIRT 等のインシデント対応調整能力の向上を図るため、研修会やイベントでの講演等を通じた CSIRT の構築・運用支援を行っています。

### 4.2. 国際 CSIRT 間連携

国境をまたいで発生するインシデントへのスムーズな対応等を目的に、JPCERT/CC は海外 CSIRT との連携強化を進めています。また、APCERT（4.2.1.参照）や FIRST（4.2.2.参照）で主導的な役割を担う等、多国間の CSIRT 連携の枠組みにも積極的に参加しています。

#### 4.2.1. APCERT（Asia Pacific Computer Emergency Response Team）

JPCERT/CC は、アジア太平洋地域の CSIRT コミュニティーである APCERT において、2003 年 2 月の発足時から継続して Steering Committee（運営委員会）のメンバーに選出されており、また、その事務局も担当しています。APCERT の詳細および APCERT における JPCERT/CC の役割については次の Web ページをご参照ください。

JPCERT/CC within APCERT
https://www.jpcert.or.jp/english/apcert/

##### 4.2.1.1. APCERT Steering Committee 会議の実施

APCERT の Steering Committee は、8 月 16 日に電話会議を行い、今後の APCERT の運営方針等について議論しました。JPCERT/CC は Steering Committee メンバーとして会議に参加すると同時に、事務局として会議運営をサポートしました。

##### 4.2.1.2. APCERT サイバー演習（APCERT Drill）2022 への参加

本演習は、アジア太平洋地域で発生し、国境を越えて広範囲に影響を及ぼすインシデントへの対応における CSIRT 間の連携の強化ならびにサイバー攻撃を受けた際により迅速に対応するための APCERT 加盟組織の能力の向上を目的として、毎年実施されています。
18 回目となる今回のサイバー演習は「Data Breach through Security Malpractice（セキュリティ対策の失敗によるデータ漏えい）」をテーマに実施されました。参加組織は、関係する組織とのインシデント情報

のやり取りやマルウェアおよびログの分析などの手順を確認しました。本演習には、APCERT 加盟組織のうち 21 の経済地域から 25 チームが、また招待組織として OIC-CERT や AfricaCERT から 4 チームが参加しました。
JPCERT/CC は、プレーヤー（演習者）として参加するとともに、APCERT 事務局ならびに演習ワーキンググループ（Drill Working Group）のメンバーとして、シナリオの議論や運営においても主導的な役割を果たしました。APCERT Drill 2022 についての詳細は、次の Web ページをご参照ください。

APCERT Drill 2022 – Data Breach through Security Malpractice –
https://www.apcert.org/documents/pdf/APCERTDrill2022PressRelease.pdf

### 4.2.2. FIRST（Forum of Incident Response and Security Teams）

JPCERT/CC は、1998 年の加盟以来、FIRST の活動に積極的に参加しています。2021 年 6 月からは、JPCERT/CC の国際部マネージャー内田有香子が FIRST の理事を務めています。本四半期はオンライン・対面による理事会に出席するとともに、下記の年次会合に先立ってダブリンで行われた理事会に参加しました。
FIRST の詳細については、次の Web ページをご参照ください。

FIRST
https://www.first.org/

FIRST.Org, Inc., Board of Directors
https://www.first.org/about/organization/directors

#### 4.2.2.1. TRAFFIC LIGHT PROTOCOL (TLP) FIRST Standards Definitions and Usage Guidance Version 2.0 の日本語訳公開

FIRST は、インシデント対応チーム間の相互協力を促進するため、インシデント対応手順の標準化を進めています。そのために SIG（Special Interest Groups）を立ち上げて基準を開発することが奨励されており、実際に複数の SIG が活動しています。このうち、TLP（Traffic Light Protocol）SIG では、情報を共有する際に受信者側による情報の取り扱いの許容範囲を指定するためのラベリングである、TLP の定義を決定する役割を担っています。「TRAFFIC LIGHT PROTOCOL（TLP） FIRST Standards Definitions and Usage Guidance」は、TLP に関する定義、利用方法、注意事項について明記した文書で、情報の発信者および受信者が情報共有の際に留意すべき点をまとめています。

Version 2.0 が新たに公開されたことに伴って、JPCERT/CC が日本語訳を行い、HIRT、NTT-CERT、Panasonic PSIRT および AT-CSIRT によるレビューを経て、日本語版の TLP が FIRST の Web サイトに公開されました。
なお、Version 1.0 は 2022 年 12 月 31 日まで引き続き使用できますが、Version 2.0 の使用が強く推奨さ

れています。

TRAFFIC LIGHT PROTOCOL（TLP）FIRST Standards Definitions and Usage Guidance - Version 2.0 日本語版
https://www.first.org/tlp/docs/v2/tlp-v2_ja.pdf

#### 4.2.3. NatCSIRT 2022 への参加（7 月 1～2 日）

第 32 回 FIRST 年次会合に引き続き、米国 CERT/CC が主催する National CSIRT Meeting（NatCSIRT）2022 がアイルランドのダブリンで開催されました。本会合は、世界各国の National CSIRT が一堂に会し、国を代表するインシデント対応チームとしての活動計画や課題を共有し、開発ツールや共同プロジェクト、調査研究等に関して発表や議論することを目的に毎年開催されています。NatCSIRT についての詳細は、次の Web ページをご参照ください。

NatCSIRT 2022
https://www.cert.org/natcsirt/

#### 4.2.4. PSIRT SIG Technical Colloquium での登壇（9 月 28 日～29 日）

9 月 28 日から 29 日にかけて、JPCERT/CC はアメリカのペンシルベニア州ニュータウンスクウェアで開催された PSIRT SIG Technical Colloquium に参加しました。この会議は、主に企業の製品セキュリティ部門（PSIRT）その他の脆弱性調整に関わる組織が参加して意見を交換する会合です。JPCERT/CC は CVE 採番組織（CNA）の活動やその課題に関する発表、ならびに脆弱性情報の調整者間におけるルール作りに関する発表を行いました。PSIRT SIG Technical Colloquium についての詳細は、次の Web ページをご参照ください。

PSIRT SIG Technical Colloquium
https://www.first.org/events/colloquia/newtownsquare2022/

### 4.3. その他国際会議への参加

#### 4.3.1. BlackHat USA, DEF CON, BsidesLV への参加（8 月 9 日～14 日）

世界最大規模のサイバーセキュリティ技術に関するカンファレンスである BlackHat USA がアメリカのラスベガスで開催され、JPCERT/CC は現地とオンラインの双方で聴講参加しました。また、連続した日程で開催された DEF CON ならびに BsidesLV も現地で聴講しました。最新のサイバー攻撃の手法や、実際に使われたマルウェアの分析結果、フォレンジック調査などに関する技術的な知見を得ました。各イベントの詳細については、次の Web ページをご参照ください。

Blackhat USA
https://www.blackhat.com/us-22/

Defcon
https://defcon.org/html/defcon-30/dc-30-index.html

BsidesLV
https://bsideslv.org/

### 4.4. 国際標準化活動

IT セキュリティ分野の標準化を行うための組織 ISO/IEC JTC-1/SC27 で進められている標準化活動のうち、作業部会 WG3（セキュリティの評価・試験・仕様に関する標準化を担当）で検討されている標準化作業の一部と、WG4（セキュリティコントロールとサービスに関する標準化を担当）で検討されているインシデント管理に関する標準の改定に、情報処理学会の情報規格調査会を通じて参加しています。

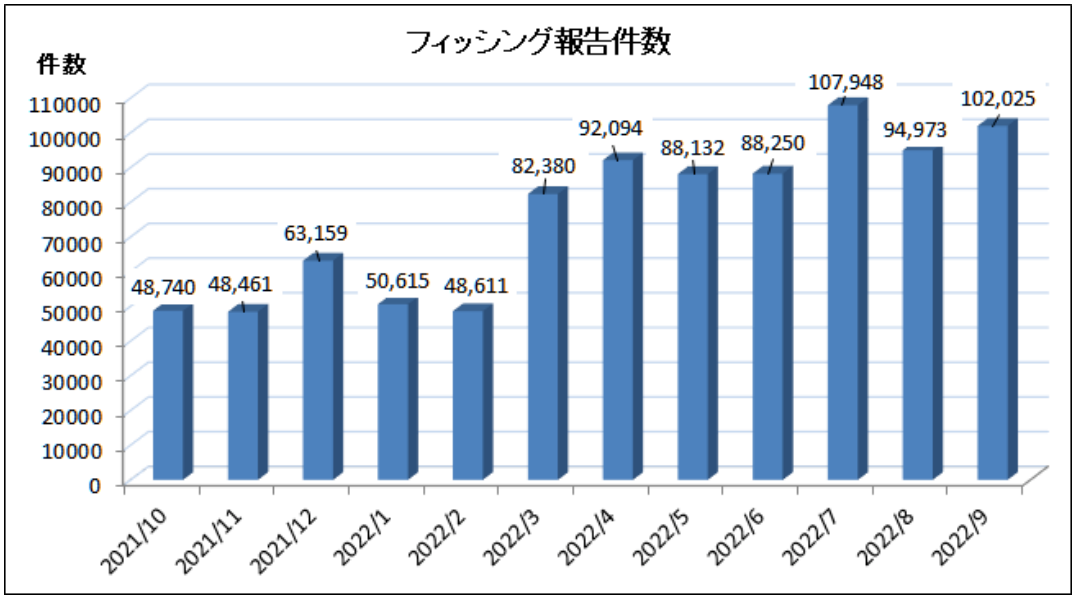
WG3 関連では、これまでコエディターとして開発に関与してきた技術報告書「ISO/IEC TR 5895:2022 Cybersecurity − Multi-party coordinated vulnerability disclosure and handling」が本年 6 月に発行された後を受けて、脆弱性の取扱に関する残存課題を整理し、新たな標準化作業の提案に向けた検討を開始しました。なお、ISO/IEC TR 5895 の発行に顕著な貢献があったと認められ、情報処理学会より国際規格開発賞の贈呈を受けました。
WG4「インシデント管理に関する標準」については、既存標準文書の複数パートの改訂および新しいパートの文書の作成が行われています。本四半期は、新しく作成中のパート 4（Coordination）の CD（Committee Draft）ステージの文書について個別会議に出席しコメントの処理作業を行いました。

## 5. フィッシング対策協議会事務局の運営

フィッシング対策協議会（本節において以下「協議会」という。）は、フィッシングに関する情報収集・提供と動向分析、技術・制度的対応の検討等を行う会員組織です。JPCERT/CC は、経済産業省からの委託により、協議会の活動のうち、一般消費者からのフィッシングに関する報告・問い合わせの受付、フィッシングサイトに関する注意喚起等、一部のワーキンググループの運営等を行っています。また、協議会は報告を受けたフィッシングサイトについて JPCERT/CC に報告しており、これを受けて JPCERT/CC がインシデント対応支援活動の一環として、フィッシングサイトを停止するための調整等を行っています。

### 5.1. フィッシングに関する報告・問い合わせの受付

フィッシング報告件数は、7 月に過去最高となる 107,948 件を記録し、その後も高止まりしています。




［図 5-1：1 年間のフィッシング報告件数（月別）］

報告件数の内訳では、6 月に緊急情報を掲載した「クレジットカードの利用確認を装うフィッシング」の報告数が多く、全体の約 28.8%を占めています。引き続き Amazon をかたるフィッシングの報告も多く、全体の約 15.9%を占めていました。

## 5.2. 情報収集／発信

### 5.2.1. フィッシングの動向等に関する情報発信

本四半期は、協議会 Web サイトや会員向けメーリングリストを通じて、フィッシングに関する緊急情報を計 19 件発信しました。
利用者が多いサービスに関する、影響範囲が大きいと思われるフィッシングについては、緊急情報を Web サイトに適宜掲載し、広く注意を喚起しました。詳細は次のとおりです。

- DMM をかたるフィッシング：1 件
- 日本郵便をかたるフィッシング：1 件
- セゾン Net アンサーをかたるフィッシング：1 件
- PayPay 銀行をかたるフィッシング：1 件
- ETC 利用照会サービスかたるフィッシング：1 件
- えきねっとをかたるフィッシング：1 件
- JR 西日本をかたるフィッシング：1 件
- 経済産業省 資源エネルギー庁をかたるフィッシング：1 件
- Google 翻訳の正規 URL から誘導されるフィッシング：1 件
- みずほ銀行をかたるフィッシング：1 件
- イオンカードをかたるフィッシング：1 件

- GMO あおぞらネット銀行をかたるフィッシング：1 件
- りそな銀行・埼玉りそな銀行をかたるフィッシング：1 件
- 日本赤十字社をかたるフィッシング：1 件
- 国税庁をかたるフィッシング：3 件
- スルガ銀行をかたるフィッシング：1 件
- ビットキャッシュをかたるフィッシング：1 件

本四半期は、前期に引き続き「クレジットカードの利用確認を装うフィッシング」の報告が多く寄せられました。このフィッシングでは、大量のドメインとサブドメインを組みあわせたパターンの誘導先 URL を使用したフィッシングメールが配信されており、そのため報告件数が増加したと考えられます。

8 月以降は、SMS やメールを使用してフィッシングサイトへ誘導する「国税局をかたるフィッシング」（[図 5-2]）が継続して発生しました。当初、電子マネー（Vプリカ）を狙うものでしたが、その後、クレジットカード情報を詐取するものに変化しており、注意が必要です。

また、銀行をかたるフィッシングでは、フィッシングに端を発するインターネットバンキングによる不正送金被害が 2019 年 11 月頃多発しましたが、その後の銀行による対策で減少していました。ところが、9 月に入ってから 3 種類（みずほ銀行、GMO あおぞらネット銀行、りそな銀行・埼玉りそな銀行）のフィッシングが連続して発生したため、緊急情報を発信しました。([図 5-3])。


［図 5-2：国税庁をかたるフィッシングサイトの例 ］

https://www.antiphishing.jp/news/alert/nta_20220920.html


［図 5-3：りそな銀行・埼玉りそな銀行をかたるフィッシングサイトの例 ］

https://www.antiphishing.jp/news/alert/resona_20220915.html

### 5.2.2. 定期報告

協議会の Web サイトにおいて、報告されたフィッシングサイト数を含む、毎月の活動報告等を公開しています。

協議会 Web ページ
https://www.antiphishing.jp/

2022 年 7 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/202207.html

2022 年 8 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/202208.html

2022 年 9 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/202209.html

### 5.2.3. フィッシングサイト URL 情報の提供

フィッシング対策ツールバーやアンチウイルスソフトなどを提供している事業者やフィッシングに関する研究を行っている学術機関等である協議会の会員等に対し、協議会に報告されたフィッシングサイトの URL を集めたリストを提供しています。これは、フィッシング対策製品の強化や、関連研究の促進を目的としたものです。本四半期末の時点で 53 組織に対し URL 情報を提供しており、今後も要望に応じて提供を拡充する予定です。

### 5.2.4. フィッシング対策ガイドライン等の改定作業

「技術・制度検討ワーキンググループ」は、協議会の会員を中心とする有識者で構成される、フィッシング対策に関するガイドラインや動向レポートを作成・改訂を行う作業部会です。
今期は、2023 年版のガイドラインおよびレポートの改訂に向けて、次のとおり会合を開催し、最近のフィッシングの傾向、関連技術、法制度の整備状況等について情報共有しつつ、事業者および一般消費者が講ずべきフィッシング対策等について議論しました。

- 技術・制度検討ワーキンググループ会合（第 1 回）
  日時：2022 年 7 月 29 日 13:00-15:00

- 技術・制度検討ワーキンググループ会合（第 2 回）
  日時：2022 年 9 月 22 日 10:00-12:00

## 6. フィッシング対策協議会の会員組織向け活動

協議会では、経済産業省から委託された活動のほかに、協議会の会員組織向けの独自の活動を、運営委員会の決定に基づいて行っており、JPCERT/CC は事務局としてこれらの活動の実施を支援しています。ここでは本四半期における会員組織向けの活動の一部について記載します。

### 6.1. 運営委員会開催

本四半期においては、協議会の活動の企画・運営方針の決定等を行う運営委員会を次のとおり開催しました。

- 第 100 回運営委員会（オンライン）
  2022 年 7 月 21 日（木）16:00 - 18:00

- 第 101 回運営委員会（オンライン）
  2022 年 9 月 15 日（木）16:00 - 18:00

### 6.2. ワーキンググループ会合等 開催支援

本四半期においては、次のとおり開催された協議会のイベントやワーキンググループ等の会合の開催を支援しました。

- 学術研究ワーキンググループ会合
  日時：7 月- 9 月　毎週火曜日 9：00 - 9：30

- 証明書普及促進ワーキンググループ会合
  日時：9 月 30 日　16：00 - 18：00

- 認証方法調査・推進ワーキンググループ会合
  日時：7 月 6 日　16：00 – 17：30

- 第 6 回フィッシング対策勉強会
  日時：9 月 8 日　10：00 - 11：30

※ワーキンググループ会合等はすべてオンライン開催

## 7. 公開資料

本章では JPCERT/CC が本四半期に公開した調査・研究の報告書や論文、セミナー資料を一覧にまとめています。

### 7.1. インシデント報告対応レポート

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の報告の受付、対応の支援、発生状況の把握、手口の分析、再発防止のための助言などを行っています。そうした活動の概要を紹介するために、インシデント報告数、報告されたインシデントの総数、報告に対応して JPCERT/CC が行った調整の件数などの統計情報、およびインシデントの傾向やインシデント対応事例を四半期ごとにまとめて、邦文および英文のレポートとして公表しています。

2022-07-14
JPCERT/CC インシデント報告対応レポート［2022 年 4 月 1 日～2022 年 6 月 30 日］
https://www.jpcert.or.jp/pr/2022/IR_Report2022Q1.pdf

2022-09-09
JPCERT/CC Incident Handling Report [April 1, 2022 - June 30, 2022]
https://www.jpcert.or.jp/english/doc/IR_Report2022Q1_en.pdf

### 7.2. インターネット定点観測レポート

JPCERT/CC では、インターネット上に複数のセンサーを分散配置し、不特定多数に向けて発信されるパケットを継続して収集するインターネット定点観測システム「TSUBAME」を構築・運用しています。脆弱性情報、マルウェアや攻撃ツールの情報などを参考に、収集したデータを分析することで、攻撃活動やその準備活動の捕捉に努めています。こうしたインターネット定点観測の結果を四半期ごとにまとめて邦文および英文のレポートとして公表しています。

2022-07-28
JPCERT/CC インターネット定点観測レポート［2022 年 4 月 1 日～2022 年 6 月 30 日］
https://www.jpcert.or.jp/tsubame/report/report202204-06.html
https://www.jpcert.or.jp/tsubame/report/TSUBAME_Report2022Q1.pdf

2022-09-09
JPCERT/CC Internet Threat Monitoring Report [April 1, 2022 - June 30, 2022]
https://www.jpcert.or.jp/english/doc/TSUBAMEReport2022Q1_en.pdf

### 7.3. 脆弱性関連情報に関する活動報告

IPA と JPCERT/CC は、それぞれ受付機関および調整機関として、ソフトウエア製品等の脆弱性関連情報に関する取扱規程（平成 29 年経済産業省告示 第 19 号）等に基づく脆弱性関連情報流通制度の運用の一端を 2004 年 7 月から担っています。この制度の運用に関連した前四半期の活動実績と、同期間中に公表された脆弱性に関する注目すべき動向をまとめてレポートとして公表しています。

2022-07-21
ソフトウェア等の脆弱性関連情報に関する届出状況［2022 年第 2 四半期（4 月～6 月）］
https://www.jpcert.or.jp/pr/2022/vulnREPORT_2022q2.pdf

### 7.4. JPCERT/CC Eyes～JPCERT コーディネーションセンター公式ブログ～

JPCERT コーディネーションセンター公式ブログ「JPCERT/CC Eyes」は、JPCERT/CC が分析・調査した内容、国内外のイベントやカンファレンスの様子などを JPCERT/CC のアナリストの眼を通して、いち早くお届けする読み物です。
本四半期においては次の 14 件の記事を公表しました。

日本語版発行件数：9 件　https://blogs.jpcert.or.jp/ja/

| | |
|---|---|
| 2022-07-14 | JPCERT/CC Eyes「なぜ、SSL-VPN 製品の脆弱性は放置されるのか ～“サプライチェーン”攻撃という言葉の陰で見過ごされている攻撃原因について～」 |
| 2022-07-29 | JPCERT/CC Eyes「サイバー政策動向を知ろう Watch! Cyber World vol. 3 |中国の法整備」 |
| 2022-08-04 | JPCERT/CC Eyes「TSUBAME レポート Overflow（2022 年 4～6 月）」 |
| 2022-08-04 | JPCERT/CC Eyes「連載『標準から学ぶ ICS セキュリティ』の初回を公表しました」 |
| 2022-08-09 | JPCERT/CC Eyes「A File Format to Aid in Security Vulnerability Disclosure - 正しくつながる第一歩」 |
| 2022-08-31 | JPCERT/CC Eyes「JPCERT/CC が確認したフィッシングサイトの URL を公開」 |
| 2022-09-15 | JPCERT/CC Eyes「攻撃グループ BlackTech による F5 BIG-IP の脆弱性（CVE-2022-1388）を悪用した攻撃」 |
| 2022-09-21 | JPCERT/CC Eyes「積極的サイバー防御」（アクティブ・サイバー・ディフェンス）とは何か ―より具体的な議論に向けて必要な観点について― |
| 2022-09-29 | TLP v2 の日本語版が公開されました |

英語版発行件数：5 件 https://blogs.jpcert.or.jp/en/

| | |
|---|---|
| 2022-07-05 | JPCERT/CC Eyes: VSingle malware that obtains C2 server information from GitHub |
| 2022-07-07 | JPCERT/CC Eyes: YamaBot Malware Used by Lazarus |

2022-08-30 JPCERT/CC Eyes: A File Format to Aid in Security Vulnerability Disclosure – the first step to a proper connection
2022-09-06 JPCERT/CC Eyes: JPCERT/CC Releases URL Dataset of Confirmed Phishing Sites
2022-09-15 JPCERT/CC Eyes: F5 BIG-IP Vulnerability (CVE-2022-1388) Exploited by BlackTech

## 8. 主な講演活動

(1) 佐條 研（インシデントレスポンスグループ マルウェアアナリスト）：
「サイバー攻撃情勢とインシデント対応」
第１３回群馬県サイバーテロ対策協議会総会（主催：群馬県サイバーテロ対策協議会事務局、講演日：2022 年 7 月 29 日）
(2) 佐條 研（インシデントレスポンスグループ マルウェアアナリスト）：
「最近のサイバー攻撃とインシデント対応」
第 2 回企業リスクマネジメント研究会（主催：一般社団法人日本情報システム・ユーザー協会（JUAS）、講演日：2022 年 8 月 10 日）
(3) 佐々木 勇人（早期警戒グループ マネージャー 脅威アナリスト）：
「なぜ、SSL-VPN 製品の脆弱性は放置されるのか ～“サプライチェーン”攻撃という言葉の陰で見過ごされている攻撃原因について～」
情報セキュリティ戦略セミナー2022（主催：日経クロステック、講演日：2022 年 9 月 7 日）

## 9. 協力、後援

本四半期は次の行事開催に協力または後援等を行いました。

(1) TCG 日本支部（JRF）第 13 回公開ワークショップ
主催：TCG 日本支部（JRF）
開催日：2022 年 7 月 8 日
(2) Hardening Designers Conference 2022
主催：Hardening Project
開催日 2022 年 9 月 1 日～9 月 3 日
(3) JAIPA Cloud Conference 2022
主　催：一般社団法人 日本インターネットプロバイダー協会 クラウド部会
開催日：2022 年 9 月 8 日

■インシデントの対応依頼、情報のご提供
info@jpcert.or.jp
https://www.jpcert.or.jp/form/
■制御システムに関するインシデントの対応依頼、情報のご提供
icsr-ir@jpcert.or.jp
https://www.jpcert.or.jp/ics/ics-form.html
■脆弱性情報ハンドリングに関するお問い合わせ　：vultures@jpcert.or.jp
■制御システムセキュリティに関するお問い合わせ　：icsr@jpcert.or.jp
■セキュアコーディングセミナーのお問い合わせ　：secure-coding@jpcert.or.jp
■公開資料、講演依頼、その他のお問い合わせ　：pr@jpcert.or.jp

■PGP 公開鍵について　：https://www.jpcert.or.jp/jpcert-pgp.html