JPCERT Coordination Center

JPCERT/CC 活動四半期レポート

2023 年 7 月 1 日 ～ 2023 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

2023 年 10 月 17 日

活動概要トピックス

－トピック1－　カスタマイズ可能なマルウェア検知ツール YAMA の公開

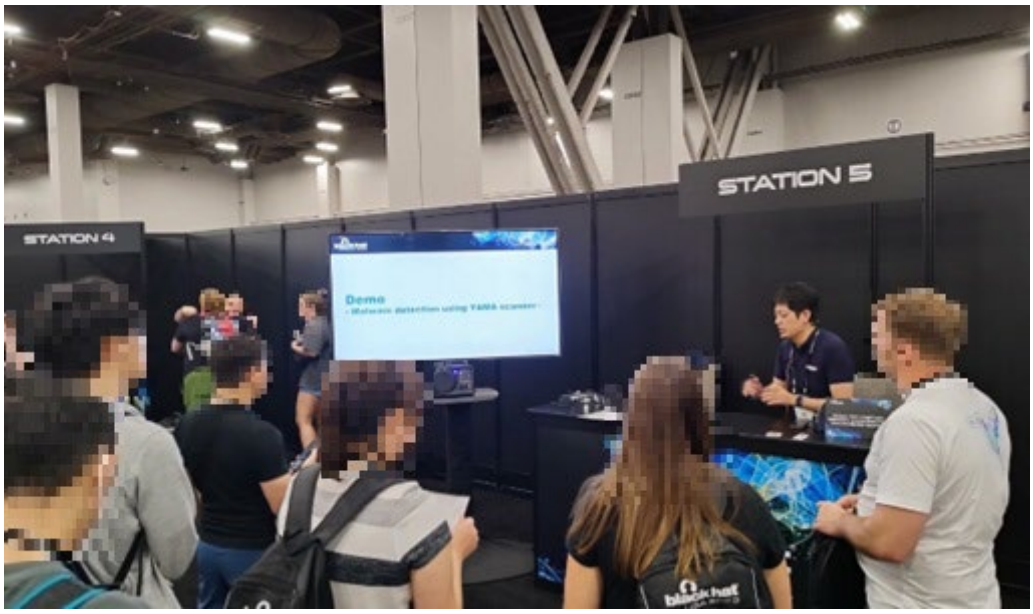
マルウェアの難読化やファイルレス化が進むにつれて、既存のファイルスキャンによる悪性判定だけではマルウェアを検知することが難しくなっています。そのため、現在ではサンドボックスや AI などを活用したマルウェア検知手法や EDR などのマルウェア感染後の不審な挙動からマルウェアを検知する技術の活用が進んでいます。
しかし、インシデントレスポンスの現場ではサンドボックス機能を持ったセキュリティ製品や EDR などでも検知できないマルウェアが見つかることがあります。このようなマルウェアが見つかると、ネットワーク内部に潜伏している同種のマルウェアを網羅的に調査することが必要になります。この調査では、ウイルス対策ソフトが役立たないため、人手による 1 台ずつの調査に多くの時間がかかって大きな問題になっていました。

このような問題を解決するために JPCERT/CC では、マルウェア検知をサポートする目的で YAMA というツールを作成し、公開しました。YAMA は、利用者が作成した YARA ルールを使用してメモリスキャンをします。そのため、ファイルレスのマルウェアであっても、メモリ上に展開されていれば検知することが可能です。また、難読化されていたとしてもメモリ上で実行中の難読化解除後のマルウェアをスキャンすれば検知できる可能性があります。YAMA は、次の GitHub レポジトリで公開していますので、ご自由にお使いください。

GitHub JPCERTCC/YAMA
https://github.com/JPCERTCC/YAMA

本ツールについては、Black Hat USA 2023 Arsenal でも発表し、多くのセキュリティ研究者と YAMA の機能について意見交換をしました。得られたフィードバックをもとに今後も機能強化を行っていく予定です。

Black Hat USA 2023 Arsenal
https://www.blackhat.com/us-23/arsenal/schedule/#yama-yet-another-memory-analyzer-for-malware-detection-33633



［カスタマイズ可能なマルウェア検知ツール YAMA 説明風景］

目次

本活動は、経済産業省より委託を受け、「令和 5 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. 主な執筆活動」、「10. 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 16,768 件、インシデント件数ベースでは 5,903 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 5,070 件でした。前四半期の 4,604 件と比較して 10%増加しています。「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/2023/IR_Report2023Q2.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 4,754 件で、前四半期の 6,186 件から 23%減少しました。また、前年度同期（7,520 件）との比較では、37%の減少となりました。

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数を添えて［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・国外ブランド別数］

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	1,052	980	997	3,029 (64%)
国外ブランド	438	310	249	997 (21%)
ブランド不明 (注 2)	233	260	235	728 (15%)
全ブランド合計	1,723	1,550	1,481	4,754

（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 79.1%、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 63.8%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、ETC の利用照会サービスを装ったフィッシングサイトが多く報告されました。国内金融機関では、前四半期に引き続きエポスカード、セゾンカード、イオンカード、そして、三井住友カードを装ったフィッシングサイトが引き続き多く報告されました。全四半期と比較すると、TEPCO、モバイル Suica、横浜銀行、厚生労働省、au じぶん銀行を装ったフィッシングサイト数の減少が目立ちました。

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 27%、国外が 78%であり、前四半期（国内が 25%、国外が 75%）と比較しほぼ同じ割合となりました。

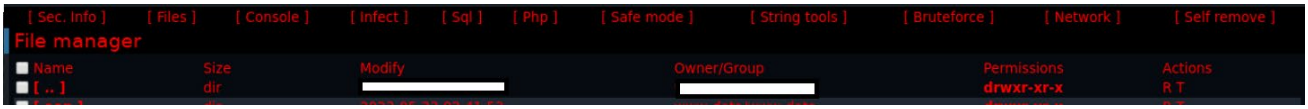
1.1.1.2. Web サイト改ざん

本四半期に報告が寄せられた Web サイト改ざんの件数は、124 件でした。前四半期の 311 件から 60%減少しています。

本四半期は、不審なサイトへの転送スクリプト（［図 1-1］）を挿入する事例やフィッシングキットを設置事例、メール送信プログラムを設置する事例など、正規の Web サイトに対するさまざまな攻撃を確認しました。これらの Web サイトには［図 1-2］のような WebShell が設置され、外部からサーバー内のファイルの閲覧やファイルのアップロード・ダウンロード、任意のコマンドを実行することが可能になっていました。

```
<meta http-equiv="refresh" content="0; url=https://[redacted]" />
```

［図 1-1：不正に挿入された転送スクリプトの例］

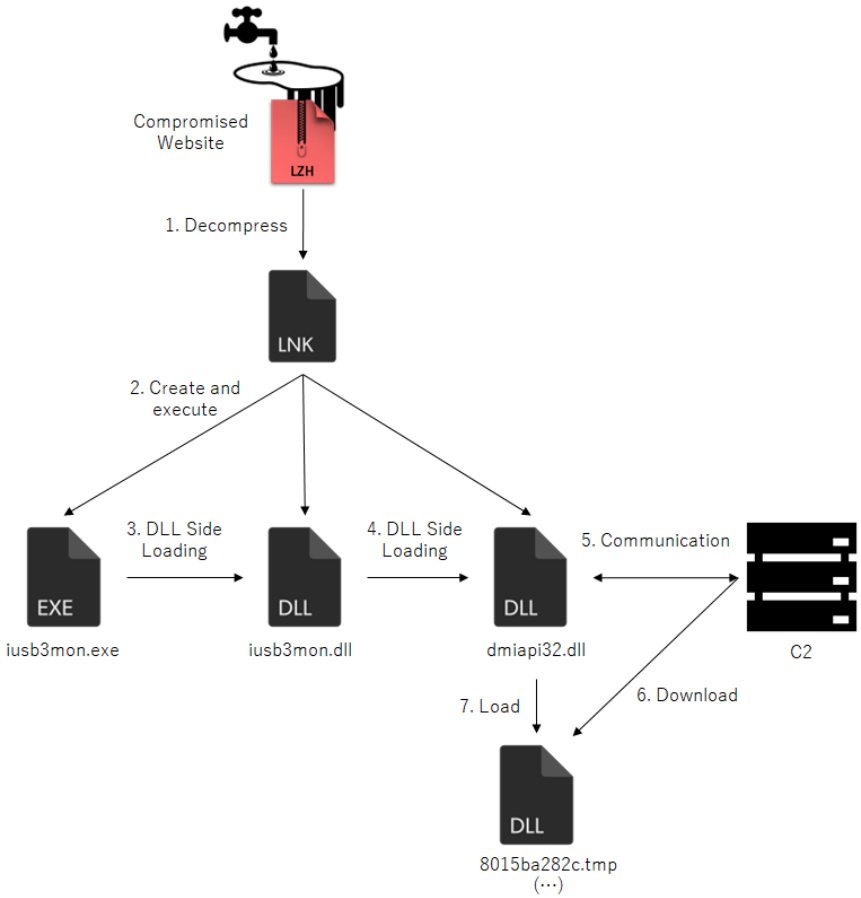


［図 1-2：不正に設置された WebShell の例］

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。そのうちの確認されたインシデントの例を紹介します。

本四半期は、有料会員向け購読サービスを提供している Web サイトが改ざんされ、有料コンテンツにアクセスしたユーザーが不正に設置されたマルウェアをダウンロードさせられる報告が寄せられました。ユーザーが改ざんされた Web サイトにアクセスすると LZH 形式の圧縮ファイルがダウンロードされ、その中のファイルを実行するとマルウェアに感染します。圧縮ファイルの中にはショートカットファイルが格納されており、ショートカットファイルを実行すると、端末内に複数のファイルが生成され、最終的に攻撃者のサーバーと通信し、追加のマルウェアがダウンロードされます。LZH 形式の圧縮ファイルを実行後、マルウェアに感染するまでの流れを［図 1-3］に示します。



［図 1-3：改ざんされた Web サイトからマルウェアが感染するまでの流れ］

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 35,000 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。本四半期は次の注意喚起を発行しました。

発行件数：16 件（うち更新情報が 5 件）　https://www.jpcert.or.jp/at/

2023-07-12　2023 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
2023-07-19　2023 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
2023-07-19　Citrix ADC および Citrix Gateway の脆弱性（CVE-2023-3519）に関する注意喚起
2023-07-21　Citrix ADC および Citrix Gateway の脆弱性（CVE-2023-3519）に関する注意喚起（更新）
2023-08-01　Proself の認証バイパスおよびリモートコード実行の脆弱性に関する注意喚起

2023-08-09　2023 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
2023-08-09　Adobe Acrobat および Reader の脆弱性（APSB23-30）に関する注意喚起
2023-08-14　Proself の認証バイパスおよびリモートコード実行の脆弱性に関する注意喚起（更新）
2023-08-16　Citrix ADC および Citrix Gateway の脆弱性（CVE-2023-3519）に関する注意喚起（更新）
2023-08-18　Proself の認証バイパスおよびリモートコード実行の脆弱性に関する注意喚起（更新）
2023-09-05　Barracuda Email Security Gateway（ESG）の脆弱性（CVE-2023-2868）を悪用する継続的な攻撃活動に関する注意喚起
2023-09-13　2023 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
2023-09-13　Adobe Acrobat および Reader の脆弱性（APSB23-34）に関する注意喚起
2023-09-14　Array Networks Array AG シリーズの脆弱性を悪用する複数の標的型サイバー攻撃活動に関する注意喚起
2023-09-19　複数のトレンドマイクロ製企業向けエンドポイントセキュリティ製品における任意のコード実行の脆弱性に関する注意喚起
2023-09-22　Array Networks Array AG シリーズの脆弱性を悪用する複数の標的型サイバー攻撃活動に関する注意喚起（更新）

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。
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/

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」の受け取りを希望して申込を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：13 件（うち更新情報が 5 件）　https://www.jpcert.or.jp/newsflash/

2023-07-11　Apple 製品のアップデートおよび緊急セキュリティ対応について（2023 年 7 月）
2023-07-12　Apple 製品のアップデートおよび緊急セキュリティ対応について（2023 年 7 月）（更新）
2023-07-12　複数のアドビ製品のアップデートについて
2023-07-18　Apple 製品のアップデートおよび緊急セキュリティ対応について（2023 年 7 月）（更新）
2023-07-25　Apple 製品のアップデートおよび緊急セキュリティ対応について（2023 年 7 月）（更新）
2023-08-09　Intel 製品に関する複数の脆弱性について
2023-08-09　複数のアドビ製品のアップデートについて
2023-09-08　Apple 製品のアップデートについて（2023 年 9 月）
2023-09-12　Apple 製品のアップデートについて（2023 年 9 月）（更新）
2023-09-13　複数のアドビ製品のアップデートについて
2023-09-21　ISC BIND 9 における複数の脆弱性について（2023 年 9 月）
2023-09-22　Apple 製品のアップデートについて（2023 年 9 月 第 2 号）
2023-09-27　Apple 製品のアップデートについて（2023 年 9 月 第 2 号）（更新）

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）Citrix ADC および Citrix Gateway の脆弱性（CVE-2023-3519）に関する情報発信

Citrix が 2023 年 7 月 18 日（現地時間）に Citrix NetScaler ADC（Citrix ADC）および NetScaler Gateway（Citrix Gateway）における複数の脆弱性に関する情報を公表しました。本脆弱性が悪用されると、認証されていない遠隔の第三者が任意のコードを実行するなどの可能性があります。
公表された脆弱性のうち、リモートコード実行の脆弱性（CVE-2023-3519）について、Citrix を含む複数の組織が、脆弱性を悪用する攻撃を確認したとの報告があり、7 月 20 日には米 CISA が本脆弱性を悪用する攻撃に関するアラートを公開しました。このアラートでは、2023 年 6 月に本脆弱性を悪用して Web シェルが設置された事案について、同製品の設定ファイルの読み取りや AD 資格情報の窃取などが行われていたことが報告されています。
また、国内でも本製品を利用していると思われる状況を確認しており、JPCERT/CC では、早期の対策適用を呼びかけるため、7 月 20 日に注意喚起を発行しました。また、8 月 14 日には Mandiant から本脆弱性を悪用する活動に関するブログとともに、脆弱性を悪用する既知の攻撃の被害を受けた可能性を示す痕跡を確認するスクリプトが GitHub で公開されたことを受け、JPCERT/CC でも注意喚起を更新しました。

また、本脆弱性を悪用して悪性のファイルが設置された可能性がある国内組織に対して、JPCERT/CC は関係組織などからの協力のもと、次のような通知を発しし対策適用および対処や調査の実施を呼びかけました。

Citrix ADC および Citrix Gateway の脆弱性（CVE-2023-3519）に関する注意喚起
https://www.jpcert.or.jp/at/2023/at230013.html

(2) Proself の認証バイパスおよびリモートコード実行の脆弱性に関する情報発信

2023 年 7 月 20 日、株式会社ノースグリッドはオンラインストレージ構築パッケージ製品「Proself」の認証バイパスおよびリモートコード実行の脆弱性に関する情報を公表しました。同社によると、本脆弱性を悪用する攻撃がすでに確認されており、利用者に対して、攻撃の影響を受けていないか確認するための調査の実施や、脆弱性の影響を緩和するための対策、回避策の適用の呼びかけが同社から行われました。
本脆弱性に関して、JPCERT/CC では開発元との調整や利用組織への通知を行いました。
開発元との調整の中で、開発元とコミュニケーションを直接取れている利用組織については対応できているものの、他のベンダーを通じて利用している利用組織の場合には、本件に関する通知が伝わっていないと想定される組織が存在したことから、JPCERT/CC では 8 月 1 日に注意喚起を公開して、広く問題の認識や調査、対策実施を呼び掛けました。

Proself の認証バイパスおよびリモートコード実行の脆弱性に関する注意喚起
https://www.jpcert.or.jp/at/2023/at230014.html

1.3. 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

1.3.1. 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、これを各地域に複数分散配置して、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。海外においても、ホスティングサービス等を利用することにより、独自の観測センサーを配備しています。TSUBAME の観測結果は一つのデータベースにまとめて分析しています。これを、公開された脆弱性情報やマルウェア、攻撃ツールの情報などと対比することで、攻撃活動や攻撃の準備活動等を把握できる場合があり、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

1.3.1.1. TSUBAME の観測データの活用

JPCERT/CC では、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」を公開しています。本四半期は、2023 年 4 月から 6 月の期間に関するレポートと、レポートで書き切れなかった内容を盛り込んだブログを公開しました。

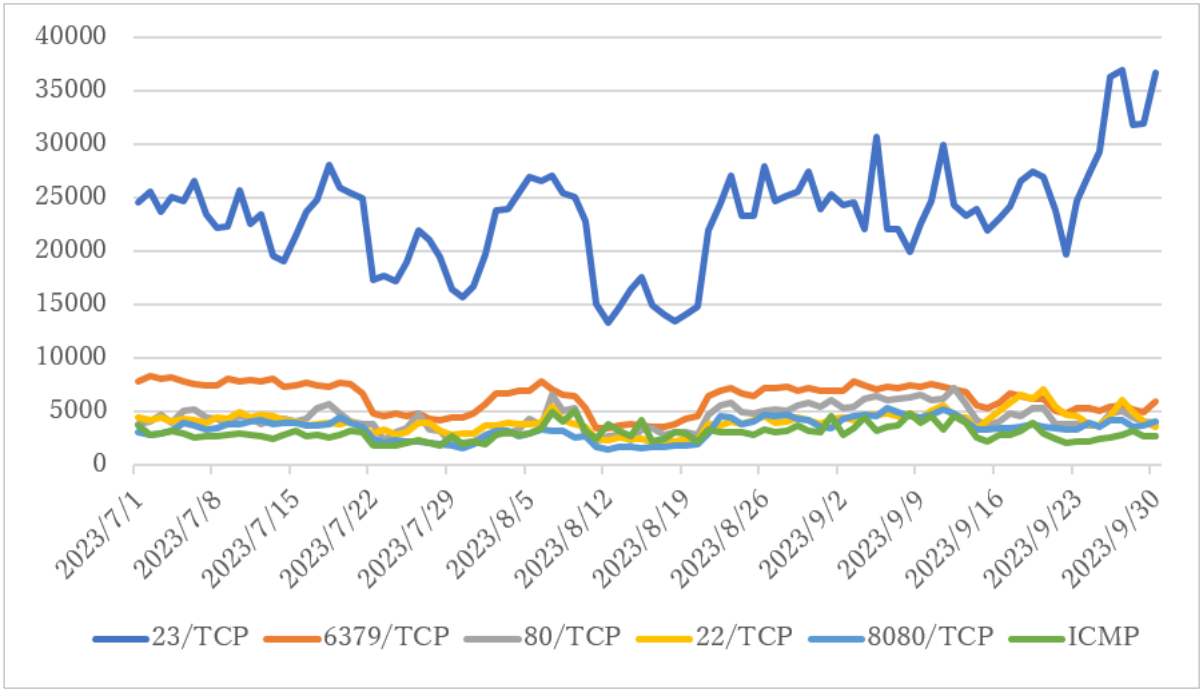
TSUBAME 観測グラフ
https://www.jpcert.or.jp/tsubame/index.html#examples

インターネット定点観測レポート（2023 年 4～6 月）
https://www.jpcert.or.jp/tsubame/report/report202304-06.html

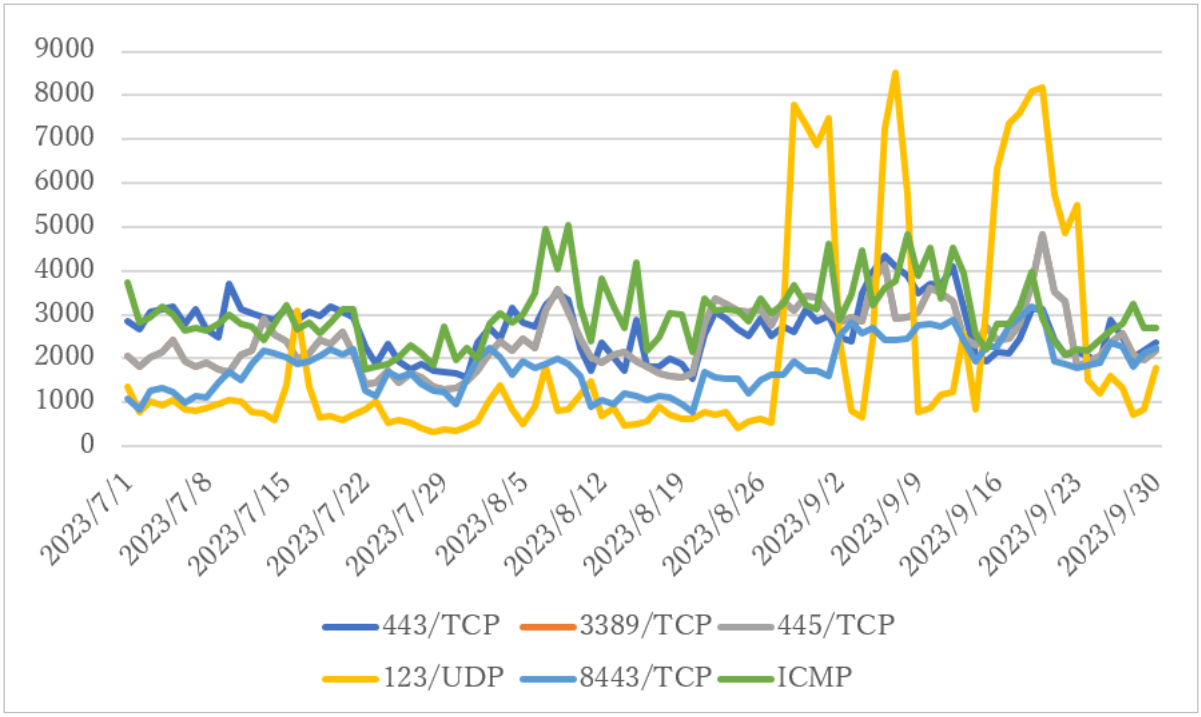
TSUBAME レポート Overflow（2023 年 4～6 月）
https://blogs.jpcert.or.jp/ja/2023/08/tsubame_overflow_2023-04-06.html

1.3.1.2. TSUBAME 観測動向

日本に設置されたセンサーが本四半期に観測したパケット数の、宛先ポートごとの内訳で上位 10 位になったものについて本四半期における増減の様子を、上位 1～5 位と 6～10 位とに分けて［図 1-4］と［図 1-5］に示します。

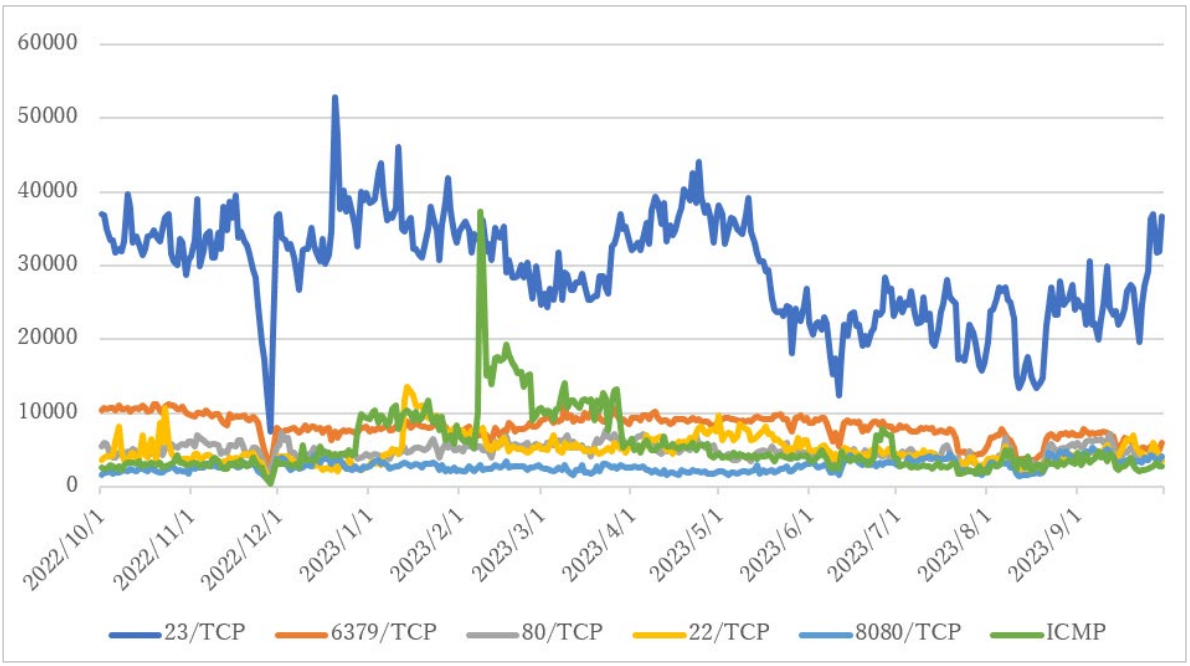


［図 1-4：TSUBAME で観測された宛先ポートの上位 1 位から 5 位のパケット数（2023 年 7 月 1 日-9 月 30 日）］

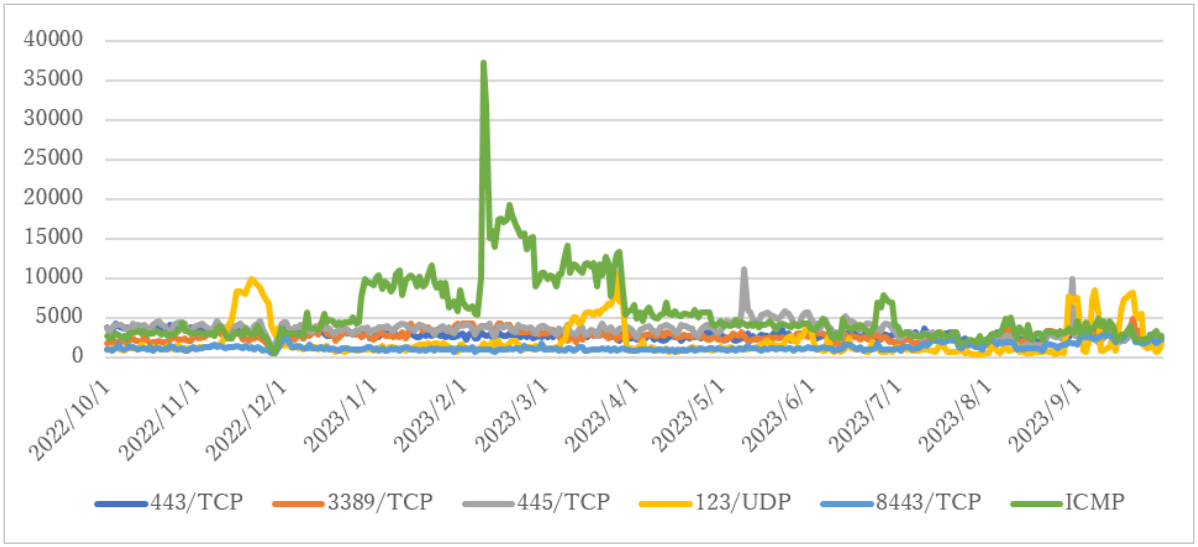


［図 1-5：TSUBAME で観測された宛先ポートの上位 6 位から 10 位のパケット数（2023 年 7 月 1 日-9 月 30 日）］

また、過去 1 年間（2022 年 10 月 1 日-2023 年 9 月 30 日）の、宛先ポート別パケット数の上位 1～5 位および 6～10 位の観測数の推移を［図 1-6］と［図 1-7］に示します。



［図 1-6：TSUBAME で観測された宛先ポートの上位 1 位から 5 位のパケット数（2022 年 10 月 1 日-2023 年 9 月 30 日）］



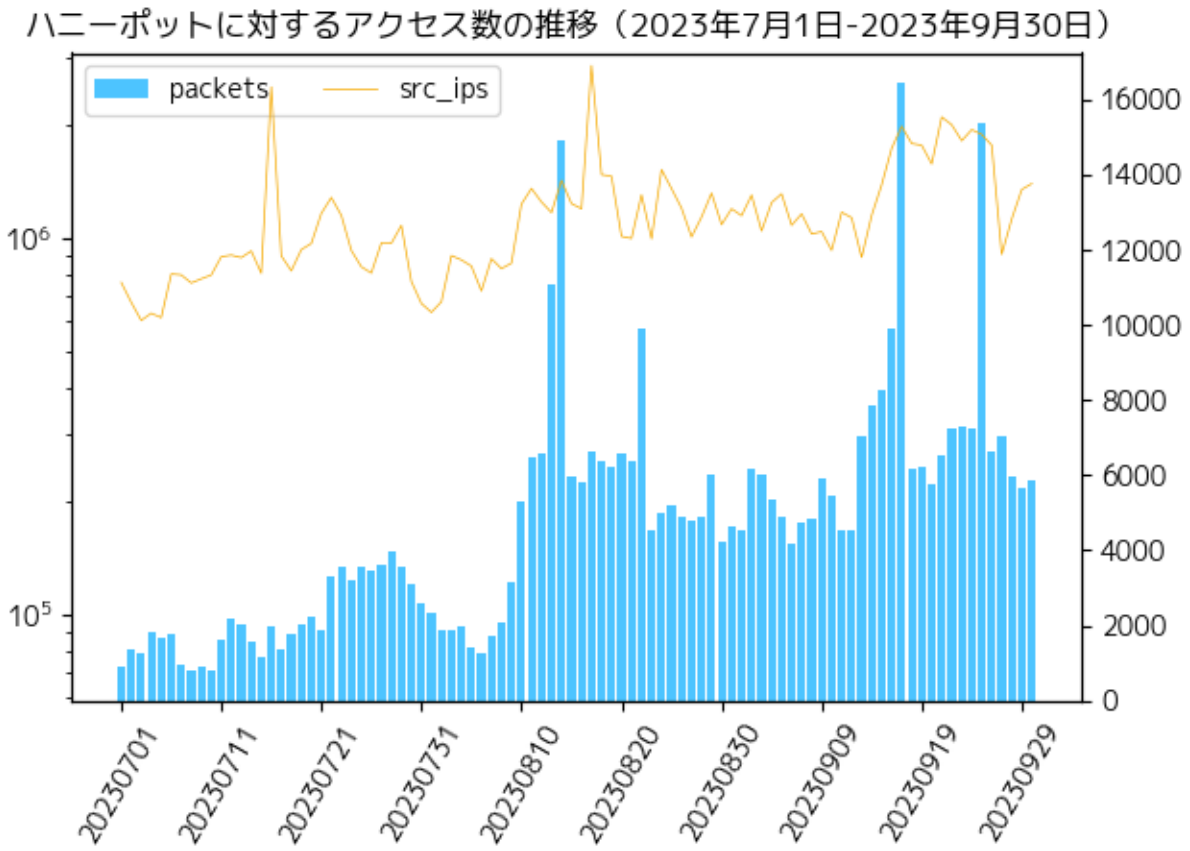
［図 1-7：TSUBAME で観測された宛先ポートの上位 6 位から 10 位のパケット数（2022 年 10 月 1 日-2023 年 9 月 30 日）］

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。増減をくりかえしていますが、2 番目以降のポート宛と比較してパケット数が多い状態が継続しています。3 番目と 4 番目の Port80/TCP と 22/TCP は、前者が後者を上回る日が多く順位が入れ替わりました。
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大きく入れ変わるほどの変化はありませんでした。

1.3.2. Web ハニーポットの運用とその分析

JPCERT/CC では、インターネット上に低対話型の Web 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。

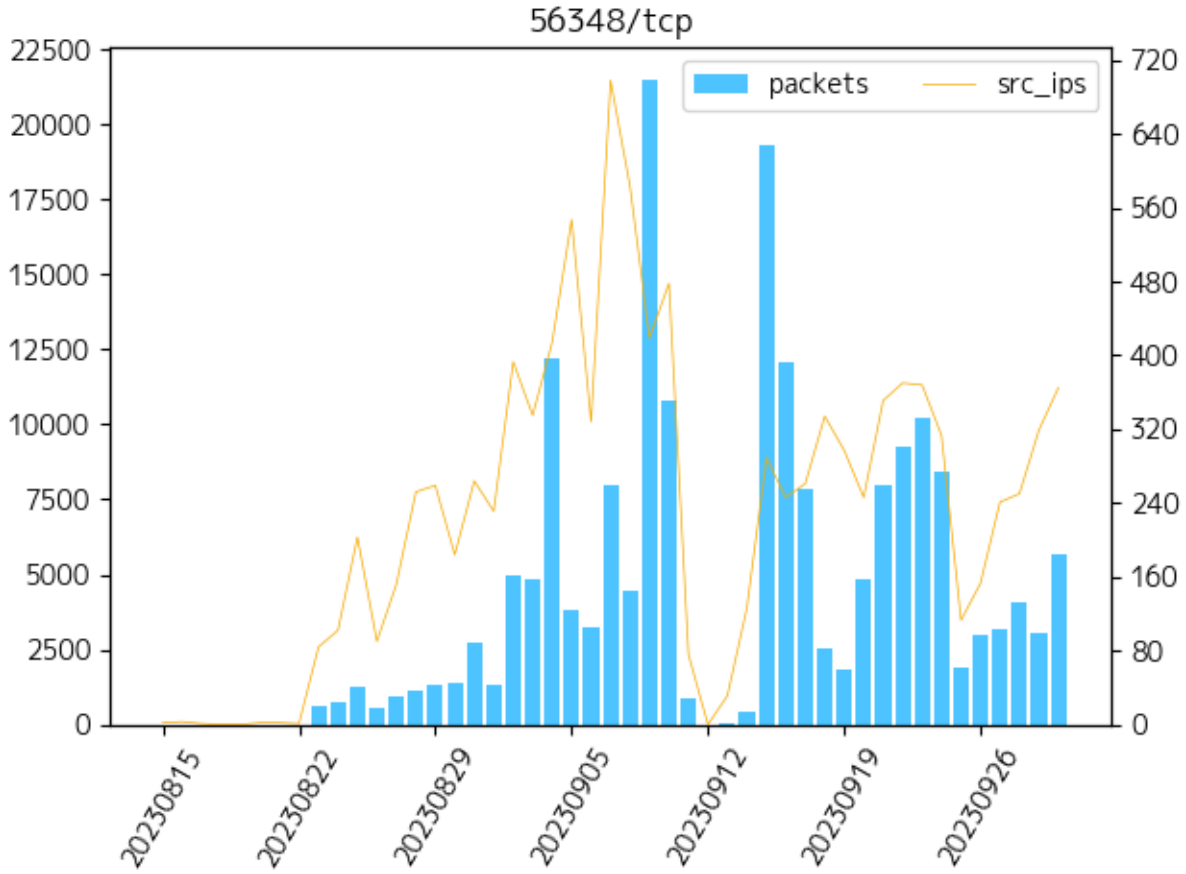
JPCERT/CC のハニーポットは、2023 年 8 月 10 日に仕様変更を行い、より多くの TCP ポートに対するパケットを受信、解析できるようになりました。[図 1-8] は 2023 年 7 月 1 日から 9 月 30 日までにハニーポットへのアクセス数と送信元ホスト数の推移ですが、8 月 10 日を境に受信数が増加しているのは前述の仕様変更の影響によるものと考えています。



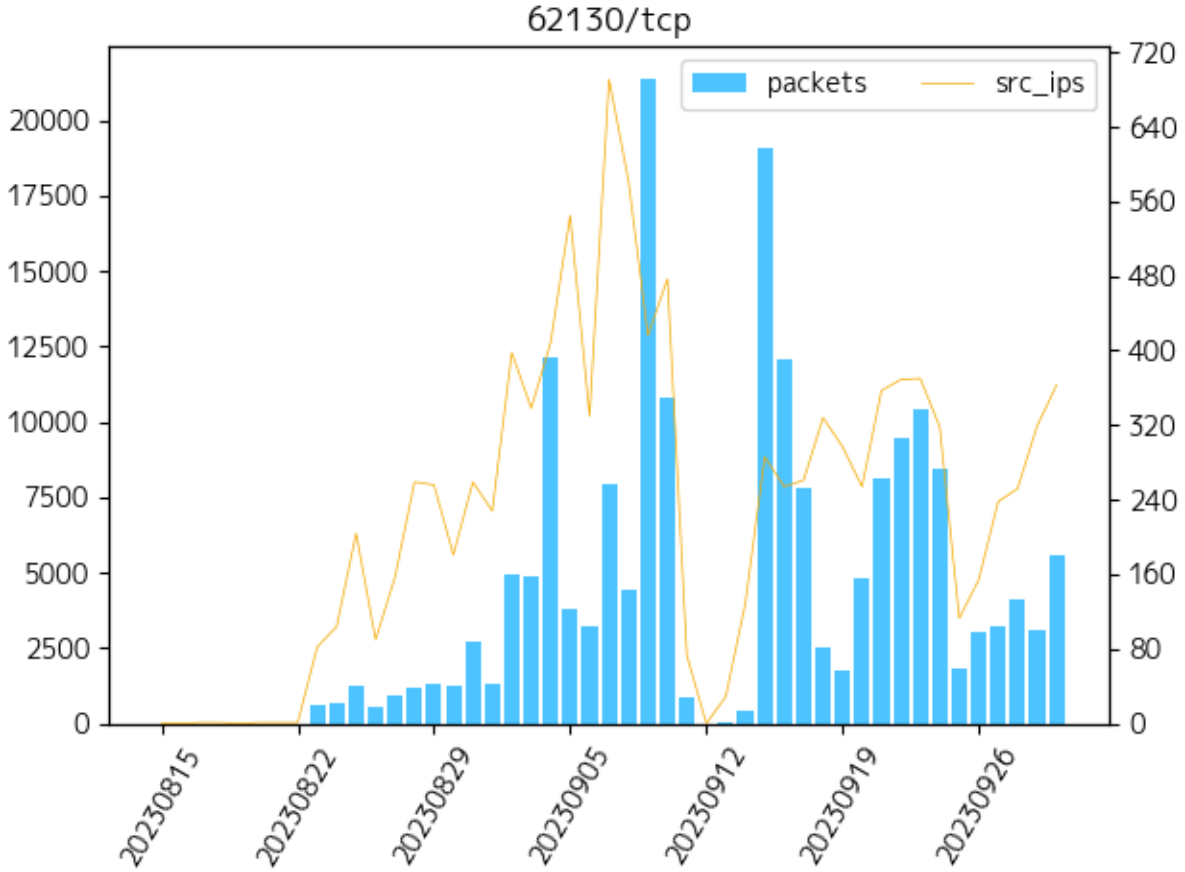
[図 1-8：ハニーポットに対するアクセス数の推移（2023 年 7 月 1 日-2023 年 9 月 30 日）]

1.3.2.1.1. 56348/TCP および 62130/TCP ポートに対するパケット数の増加現象について

2023 年 8 月 23 日以降 9 月 30 日に至る期間、56348/TCP および 62130/TCP ポートに対する SYN パケットの増加を観測しました。それぞれの推移を［図 1-9］および［図 1-10］に示します。このような特定の TCP ハイポートに対するスキャンパケットの増加は、それらのポートが有効な通信機器を探索して悪用する動きと関係することが多いことから、探索対象機器の特定に向けた調査を継続しています。



［図 1-9：56348/TCP ポートに対するパケット数の推移（2023 年 8 月 15 日-2023 年 9 月 30 日）］



［図 1-10：62130/TCP ポートに対するパケット数の推移（2023 年 8 月 15 日-2023 年 9 月 30 日）］

上記の他、特筆すべき攻撃活動は観測されませんでした。

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）共同運営）を通じて公表することで広く注意を促す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. JPCERT/CC における脆弱性関連情報の取り扱い

JPCERT/CC では、寄せられた脆弱性関連情報に対して、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、製品開発者による脆弱性の検証や対処に向けた調整を行い、

JVN を通じて脆弱性情報等を一般に公表しています。また、公表した脆弱性情報の国際的かつ効果的な情報流通のために、CVE（Common Vulnerabilities and Exposures）Program（個々の脆弱性を特定、記述、公に公表されたものをカタログ化することを使命として、専門家コミュニティーにより進められている国際的な活動。その事務局は米国の MITRE 社が務めています。）において配下の CNA を統括する Root の役割を担うとともに、CNA（CVE Numbering Authority、 CVE 採番機関）として、CVE 番号の付与を行っています。
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）に基づく、「調整機関」として、製品開発者とのコーディネーションを行っています。調整機関としての活動は、この規定に基づく「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。）に沿って、脆弱性情報の「受付機関」である独立行政法人情報処理推進機構（IPA）と緊密に連携して進めています。
また、CERT/CC や CISA、NCSC-NL、NCSC-FI といった海外の調整組織との国際調整、国内外から寄せられる報告や調整依頼にも対応しています。

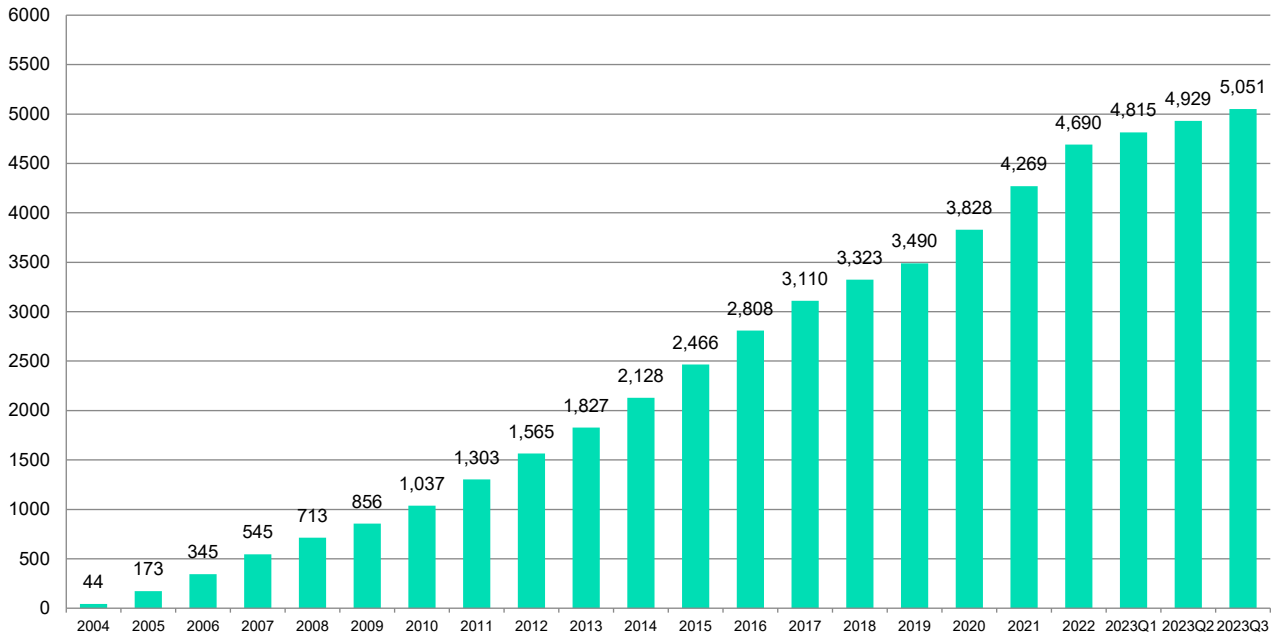
2.1.2. Japan Vulnerability Notes（JVN）において公表した脆弱性情報および対応状況

JVN で公表している脆弱性情報は、次の 3 種類に分類されます。

- パートナーシップガイドラインに基づき報告された脆弱性関連情報に関するもの（「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）
- 国際調整や独自調整に基づく脆弱性情報（「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）
- 脆弱性情報に関連する技術情報や影響範囲が広く個別の製品の脆弱性情報という範疇を超えた情報等（「JVNTA」に続く 8 桁数字の形式の識別子を付与している；例：JVNTA#12345678）

本四半期に JVN において公表した脆弱性情報は 122 件（累計 5,051 件）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内訳は次のとおりです。

- パートナーシップガイドラインに基づき報告された脆弱性情報に関するもの：27 件
- 国際調整や独自調整に基づく脆弱性情報に関するもの：95 件
- 脆弱性情報に関連する技術情報等に関するもの：0 件

なお、パートナーシップガイドラインに基づく脆弱性関連情報に関する四半期ごとの報告状況については、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）脆弱性対策情報
https://www.ipa.go.jp/security/vuln/

本四半期に公表に至った脆弱性情報について、特徴のあったものを紹介します。

(1) パートナーシップガイドラインに基づき報告された脆弱性関連情報における特徴的な事例

- JVN#83334799
  SIG 情報連携ポータルの API における複数の脆弱性
  https://jvn.jp/jp/JVN83334799/

本件は、JPCERT/CC が開発提供し、国内の ISAC 等で運用されている情報連携ポータルの脆弱性に関する情報です。本件では、製品開発者として JPCERT/CC 自身が、脆弱性の修正と関連情報の流通を実施することになりました。脆弱性への対応では、修正プログラムを開発する開発部門だけでなく、円滑な情報発信のために法務部門や広報部門など複数の社内部門との調整が不可欠であることを各製品開発者に説明してきましたが、本件を通じて、そのことを改めて強く実感することができました。今後の脆弱性調整時には、この経験を活かし製品開発者に寄り添ったより質の高い調整を目指していきたいと考えています。

(2) 国際調整や独自調整で取り扱った脆弱性における特徴的な事例

- JVNVU#90967486
  複数のトレンドマイクロ製企業向けエンドポイントセキュリティ製品において任意のコードを実行される脆弱性
  https://jvn.jp/vu/JVNVU90967486/

本件では、脆弱性を悪用された攻撃を確認していることが、製品開発者から脆弱性情報とあわせて報告されました。JVN でも製品開発者と歩調をあわせて情報を公表しました。さらに、JPCERT/CC では次の注意喚起を発行して製品利用者への周知に努めました。

> 複数のトレンドマイクロ製企業向けエンドポイントセキュリティ製品における任意のコード実行の脆弱性に関する注意喚起
> https://www.jpcert.or.jp/at/2023/at230021.html

上記の注意喚起と対応する JVN 上のアドバイザリとは相互にリンクして参照できるようにしました。
また、このように、脆弱性を悪用した攻撃が確認されている場合、JVN 公表時のタイトルに「緊急」のマークをつけたり「本脆弱性を悪用した攻撃が確認されています」との文言を加えたりしています。JVN をご覧いただく際には、これらの注意書きにも注意をお願いします。

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. 海外の脆弱性調整組織等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、米国の CISA および CERT/CC など各地域にて脆弱性情報のコーディネーションを行っている海外の調整組織と協力関係を結び、脆弱性情報の円滑な国際的調整、情報流通などで相互に連携しています。また、FIRST（Forum of Incident Response and Security Teams）をはじめとして脆弱性にまつわる国際的なコミュニティー活動にも参加し、国内外の組織との協力や情報の発信を行っています。本四半期での活動を紹介します。

(1) CISA による文書「Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by- Design and -Default」の公表への協力

JPCERT/CC では、CISA から文書「Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by- Design and -Default」について意見を求められ、技術的な観点からのコメントを送りました。本文書では、NIST の発行文書などを引用しつつ、製品開発においてセキュリティ上考慮することや、企業としての取り組み姿勢などを中心に、セキュアバイデザインについての一般論がまとめられています。製品開発者が、開発への向き合い方や開発プロセスの改善を考える参考になるものと考えます。これまでも JPCERT/CC では国内の製品開発者や学術機関からの要請を受けて、セキュアコーディングの普及啓発を行ってきました。こうした知見を踏まえて、今回の CISA の草案に対するコメントを取りまとめ送付しました。また、本文書が日本の製品開発者にとっても役立つものであると判断し、CISA の取り組みに対して賛同の意を表しました。

2.1.5. CNA としての活動

JPCERT/CC では、CVE Program の活動に協力し、国際的な脆弱性情報流通に資する上で、CNA として CVE ID の採番を行うことや、国内の製品開発者をスコープとする Root として活動を行っています。2008 年 5 月以降 JVN での脆弱性情報の公表の際に、他の CNA が採番するケースを除いて、CVE ID 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 85 個の CVE 番号を付与しました。

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 刷）
https://www.jpcert.or.jp/vh/partnership_guideline2019_r2.pdf

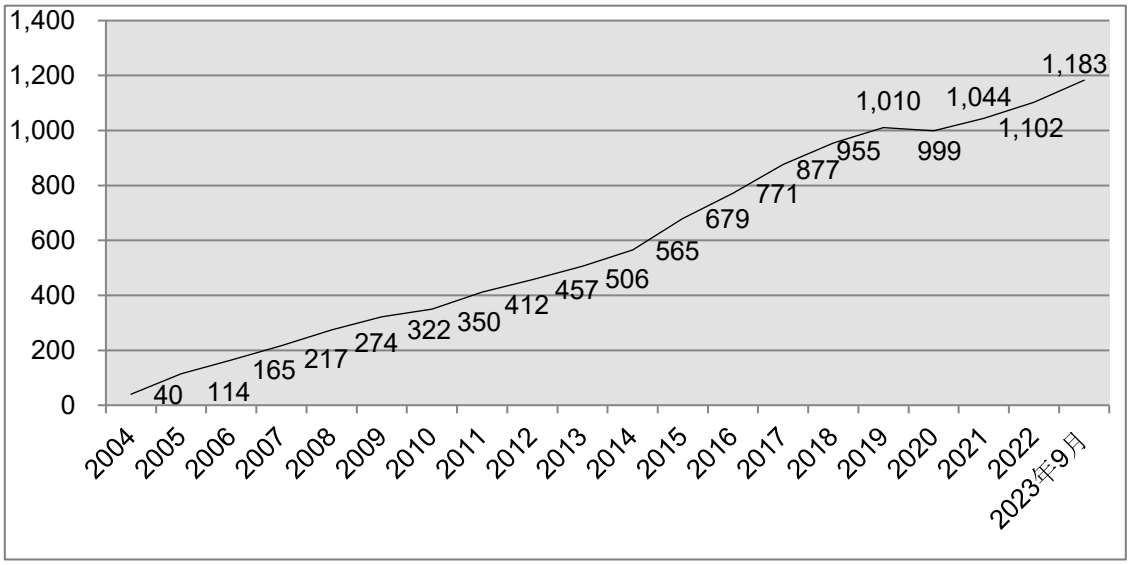
JPCERT/CC 脆弱性情報取扱いガイドライン（2019 年版）
https://www.jpcert.or.jp/vh/vul-guideline2019.pdf

2.2.1. 日本国内製品開発者との連携

本規程では、脆弱性情報の提供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 2-2］に示すとおり、2023 年 9 月 30 日現在で 1,183 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 2-2：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 27 日に開催しました。当日は、製品脆弱性を悪用するインシデントにおける情報共有と公表についての説明、PSIRT 向け脆弱性対応演習の紹介、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についての説明、早期警戒情報提供サービス（CISTA）の紹介を行いました。また、JVN で公表された脆弱性事例を題材にして当該事例の当事者である製品開発者と JPCERT/CC でのパネルディカッション行い、脆弱性コーディネーションの中で発生したさまざまな状況について製品開発者と調整機関の双方の目線からの課題や反省点等を共有するとともに、参加者との意見交換を行いました。

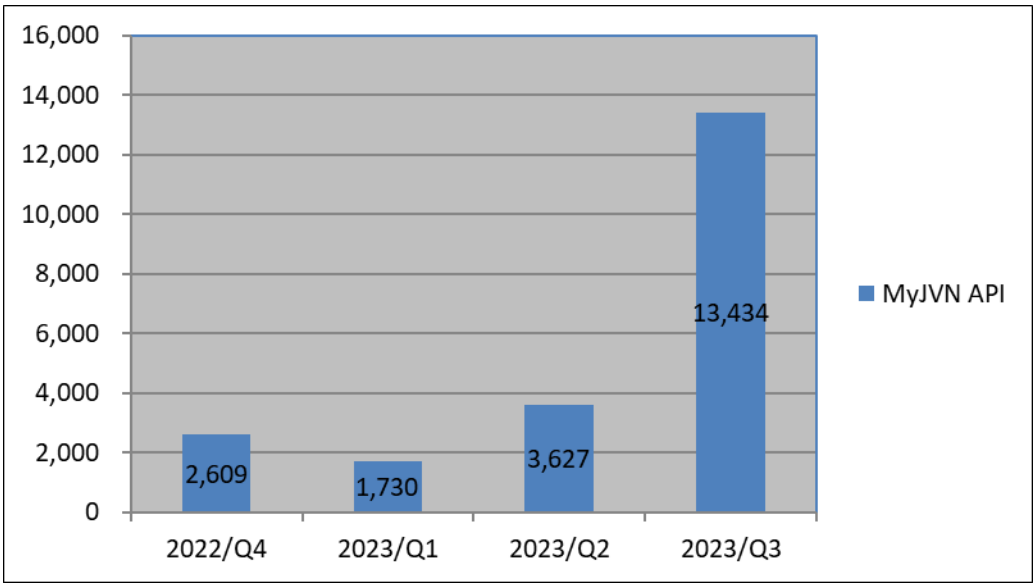
2.3. VRDA フィードによる脆弱性情報の配信

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

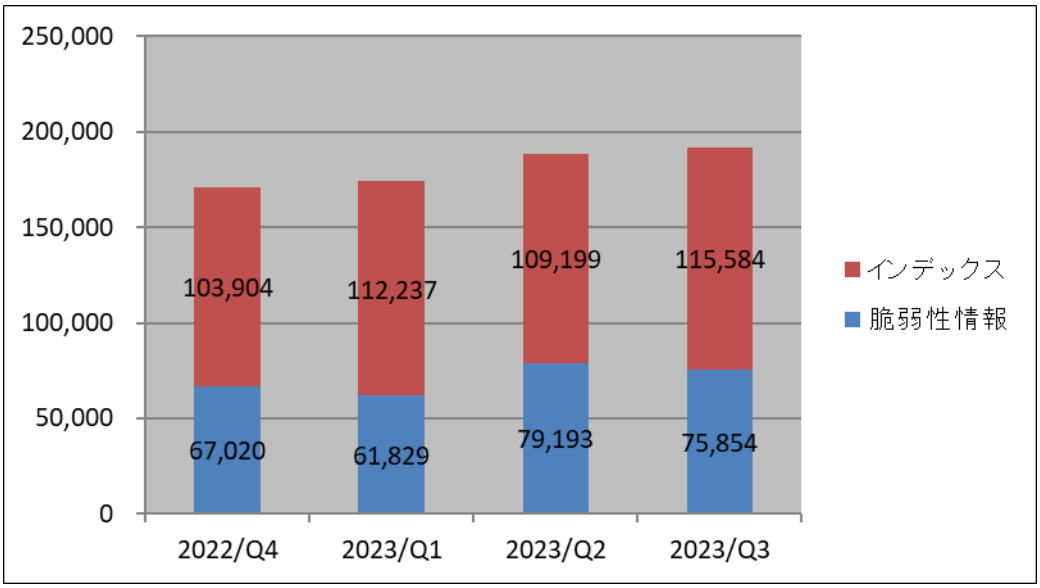
応を可能とするため、IPA が運用する MyJVN API を外部データソースとして利用した VRDA（Vulnerability Response Decision Assistance）フィードによる脆弱性情報の配信を行っています。VRDA フィードについての詳しい情報は、次の Web ページをご参照ください。

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 2-3］に、VRDA フィードの利用傾向を［図 2-4］と［図 2-5］に示します。［図 2-4］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 2-5］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。

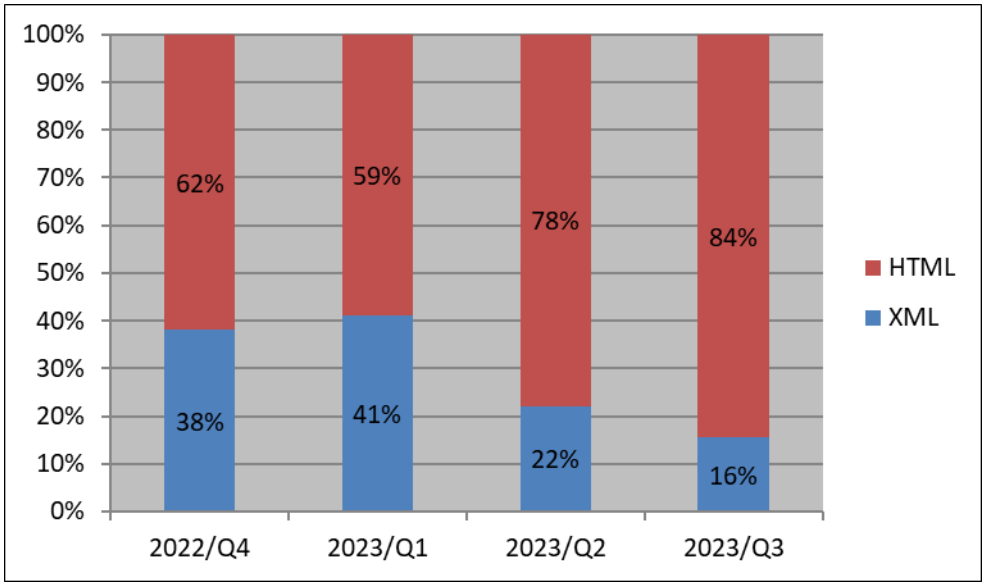


［図 2-3：VRDA フィード配信件数］



［図 2-4：VRDA フィード利用件数］

インデックスおよび脆弱性情報の利用数については、［図 2-5］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。



［図 2-5：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 2-5］に示したように、前四半期と比較し、HTML 形式の利用割合が 6%増加しました。

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 200 件でした。

3.2. 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、情報に応じて適宜選んだ国内組織に「参考情報」として提供しています。

本四半期に提供した参考情報は 2 件でした。

また、2022 年度より、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「JPCERT/CC ICS Security Notes」を配信しています。

（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 が収集した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び、四半期にどのような動きがあったのかがわかるよう、次の形式にコンパクトにまとめたものです。

<< 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

<< 付録. JVN で掲載した ICS 脆弱性情報一覧>>

- 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をリスト形式で掲載

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

2023-07-27　JPCERT/CC ICS Security Notes FY2023_#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を設けており、メーリングリストには現在 1,327 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。情報共有ポータルサイト ConPaS については、2023 年 10 月末にサービス終了を予定しており、7 月 31 日以降の新規利用申し込みの受付を停止しています。

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。

3.2.1. 注意喚起

本四半期に発行した注意喚起は 0 件でした。

3.2.2. 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。

3.3. 制御システム関連のインシデント対応

JPCERT/CC では、制御システム関連のインシデント報告を受け付け、頂いた報告内容に基づいて個別の対応を実施しています。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報告への対応件数は 0

件でした。

3.4. 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。

3.5. 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）を無償で提供しています。本四半期は、日本版 SSAT に関し 1 件の利用申し込みがあり、直接配付した件数の累計は、日本版 SSAT が 292 件でした。

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

J-CLICS STEP1／STEP2（ICS セキュリティ自己評価ツール）
https://www.jpcert.or.jp/ics/jclics.html

J-CLICS 攻撃経路対策編（ICS セキュリティ自己評価ツール）
https://www.jpcert.or.jp/ics/jclics-attack-path-countermeasures.html

3.6. 連載「標準から学ぶ ICS セキュリティ」4、5 回目の記事を公表

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 2022 年 8 月より開始しています。

本四半期においては、2023 年 7 月 13 日に「セキュリティ更新（パッチ）管理」を、9 月 14 日に「セキュアな製品開発プロセス」を公表しました。前者では、IEC 62443-2-3 で論じられているパッチ管理の概略とそれに関連する他の国際標準や脆弱性に関する最近の課題を、後者では、IEC 62443-4-1 が論じるセキュアな製品開発プロセスの概略を紹介しています。これで連載記事は 5 本となりました。

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

国境をまたがって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 が、7 月 28 日に電話会議を行い、また 9 月 11 日には京都で開催された APNIC カンファレンス期間中に対面での会議を行って、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）2023 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。
19 回目となる今回のサイバー演習は「Digital Supply Chain Redemption（デジタルサプライチェーンの救済）」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 24 チームが、また招待組織の OIC-CERT や AfricaCERT から 11 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、シナリオの作成や当日の運営において主導的な役割を果たしました。APCERT Drill 2023 についての詳細は、次の Web ページをご参照ください

APCERT Drill 2023 – Digital Supply Chain Redemption –
https://www.apcert.org/documents/pdf/APCERTDrill2023PressRelease.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、毎月のオンラインによる理事会に加え、9 月 20 日～23 日にノルウェーのオスロで開催された対面での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

4.3. 海外 CSIRT 等の来訪および往訪

4.3.1. インド CERT-In の来訪（9 月 15 日）

インドの CERT-In およびその関係者の来訪に対応し、活動の状況についてヒアリングを行うとともに、今後の協力について意見交換を行いました。

4.4. その他国際会議への参加

4.4.1. Blackhat USA, DEFCON, BSidesLV への参加（8 月 8 日～13 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。今回 JPCERT/CC は、Blackhat Arsenal のプログラム内で「YAMA: Yet Another Memory Analyzer for Malware Detection」と題した講演を行い、開発したマルウェア解析ツールの詳細を説明しました。また、BlackHat USA と連続した日程で開催された DEFCON 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。また、会議の全体概要や聴講したセッションなどについて、ブログ記事で紹介しました。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。

国際カンファレンス参加レポート ～Black Hat USA, DEF CON～
https://blogs.jpcert.or.jp/ja/2023/09/black-hat-usa-def-con.html

Blackhat USA
https://www.blackhat.com/us-23/

Defcon
https://defcon.org/html/defcon-31/dc-31-index.html

BSidesLV
https://bsideslv.org/

4.5. 国際標準化活動

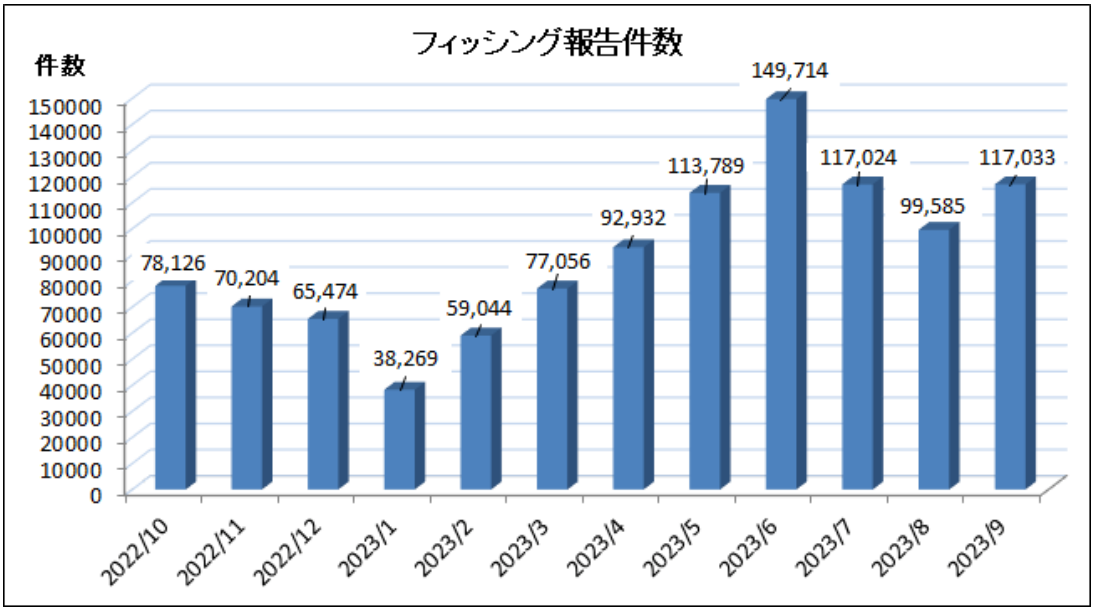
IT セキュリティ分野の標準化を行うための組織 ISO/IEC JTC-1/SC27 で進められている標準化活動のうち、作業部会 WG3（セキュリティの評価・試験・仕様に関する標準化を担当）で検討されている標準化作業の一部と、WG4（セキュリティコントロールとサービスに関する標準化を担当）で検討されているインシデント管理に関する標準の改定に、情報処理学会の情報規格調査会を通じて参加しています。
本四半期は、国内小委員会の会合に参加し国内外動向の情報収集に努め、WG4 において策定中の ISO/IEC 27404:Cybersecurity – IoT security and privacy – Cybersecurity labelling framework for consumer IoT についての議論に参加しました。

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、前四半期と比較して減少したものの、引き続き多数の報告を受けました。



［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、「Amazon」をかたるフィッシングの報告数が最も多く、全体の約 35.9%を占めています。ついで、「三井住友カード」をかたるフィッシングの報告も多く、全体の約 9.6%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 10 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。

- みずほ銀行をかたるフィッシング ：1 件
- 楽天銀行をかたるフィッシング ：1 件
- NTT ドコモをかたるフィッシング ：1 件
- アプラスをかたるフィッシング ：1 件
- LINE Pay をかたるフィッシング ：1 件
- ETC 利用照会サービスをかたるフィッシング ：1 件
- 日本生命をかたるフィッシング ：1 件
- マイナポイント事務局をかたるフィッシング ：1 件
- So-net をかたるフィッシング ：1 件
- ソフトバンクをかたるフィッシング：1 件

本四半期の報告件数は、前四半期と比較して減少傾向となりました。前四半期の 6 月に過去最高の報告件数を記録した主要原因となった、特定の海外クラウドサービスからのフィッシングメール配信が停止したことが減少の要因であると思われます。
一方で、EC 系および金融系ブランドをかたるフィッシングメールに限ると、前四半期と比較して報告件数が約 63.8%増となり、引き続き多くのフィッシングが報告されています。さらに、かたられるブランドが多様化していることも注目されます。本四半期には 21 の銀行ブランドについて報告がありました。今後もブランドの多様化が一層進むことが懸念され、今までフィッシングのなかった金融機関においても警戒を怠らないことが重要です（[図 5-2]）。
9 月には、マイナポイント事務局をかたるフィッシングが発生しました。これはマイナポイント受け取りの申し込みが 9 月に期限を迎えることから、「有効期限が近づいている」「ポイントが失効する」というような文面でフィッシングサイトへ誘導することを狙ったものと考えられ、その注意喚起のため緊急情報を公開しました（[図 5-3]）。

［図 5-2：楽天銀行をかたるフィッシングサイトの例 ］

https://www.antiphishing.jp/news/alert/rakutenbank_20230801.html

［図 5-3：マイナポイント事務局をかたるフィッシングメールの例 ］
https://www.antiphishing.jp/news/alert/myna_20230911.html

5.2.2. 定期報告

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協議会の Web サイトで次のとおり公開しています。

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

2023 年 7 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/202307.html

2023 年 8 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/202308.html

2023 年 9 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/202309.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 56 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。
本四半期は、2024 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：2023 年 8 月 29 日 15:00-17:00

- 技術・制度検討ワーキンググループ会合（第 2 回）
  日時：2023 年 9 月 26 日 15:00-17:30

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 110 回運営委員会（オンライン）
  2023 年 7 月 13 日（木）16:00 - 18:00

- 第 111 回運営委員会（オンラインおよび JPCERT/CC 会議室）
  2023 年 9 月 14 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（オンライン）

- 証明書普及促進ワーキンググループ会合
  日時：8 月 7 日　16：00 - 18：00（オンラインおよび JPCERT/CC 会議室）
  日時：9 月 19 日　16：00 - 18：00（オンライン）

- 認証方法調査・推進ワーキンググループ　資料公開
  インターネットサービス利用者に対する「認証方法」に関するアンケート調査 コロナ禍を経た利用者の変化について、追跡調査結果を公開（2023/07/21）
  https://www.antiphishing.jp/report/wg/authentication_20230721.html

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。

2023-07-13
JPCERT/CC インシデント報告対応レポート［2023 年 4 月 1 日～2023 年 6 月 30 日］
https://www.jpcert.or.jp/pr/2023/IR_Report2023Q1.pdf

2023-09-26
JPCERT/CC Incident Handling Report [April 1, 2023 - June 30, 2023]
https://www.jpcert.or.jp/english/doc/IR_Report2023Q1_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と照らし合わせて、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。

2023-08-16
JPCERT/CC インターネット定点観測レポート［2023 年 4 月 1 日～2023 年 6 月 30 日］
https://www.jpcert.or.jp/tsubame/report/report202304-06.html
https://www.jpcert.or.jp/tsubame/report/TSUBAME_Report2023Q1.pdf

2023-09-26
JPCERT/CC Internet Threat Monitoring Report [April 1, 2023 - June 30, 2023]
https://www.jpcert.or.jp/english/doc/TSUBAMEReport2023Q1_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。

2023-07-20
ソフトウェア等の脆弱性関連情報に関する届出状況［2023 年第 2 四半期（4 月～6 月）］
https://www.jpcert.or.jp/pr/2023/vulnREPORT_2023q2.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 12 件の記事を公表しました。

日本語版発行件数：8 件　https://blogs.jpcert.or.jp/ja/

2023-07-06　DNS の不正使用手法をまとめた技術ドキュメントの公開
2023-07-12　開発者の Windows、macOS、Linux 環境を狙った DangerousPassword による攻撃
2023-08-07　なぜ被害公表時に原因を明示するのか／しないのか～個別被害公表と事案全体のコーディネーションの観点から～
2023-08-09　カスタマイズ可能なマルウェア検知ツール YAMA
2023-08-16　TSUBAME レポート　Overflow（2023 年 4～6 月）
2023-08-22　MalDoc in PDF - 検知回避を狙って悪性な Word ファイルを PDF ファイルへ埋め込む手法 -
2023-08-29　「能動的サイバー防御」は効果があるのか？ ～注目が集まる offensive なオペレーションの考察～
2023-09-19　国際カンファレンス参加レポート ～Black Hat USA, DEF CON～

英語版発行件数：4 件 https://blogs.jpcert.or.jp/en/

2023-07-19　DangerousPassword attacks targeting developers'Windows, macOS, and Linux environments
2023-08-09　YAMA-Yet Another Memory Analyzer for malware detection
2023-08-28　MalDoc in PDF - Detection bypass by embedding a malicious Word file into a PDF file –
2023-09-26　TSUBAME Report Overflow (Jan-Mar 2023)

8. 主な講演活動

(1) 三浦 拓也（早期警戒グループ脅威アナリスト）：
「サイバー攻撃 2022－昨今のサイバー攻撃動向とその対応－」
Internet Week ショーケース in 札幌（主催：日本ネットワークインフォメーションセンター、講演日：2023 年 7 月 21 日）
(2) 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）：
「サイバー攻撃対策における“予防原則”からの脱却～事前の準備と発生時のコミュニケーションで早期事業復旧を目指す～」
サイバー攻撃から自社を守るためのセキュリティセミナー（主催：内田洋行 IT ソリューションズ、

講演日：2023 年 8 月 8 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）：
「この 3 年間で変わったこと・変わらなかったこと～脅威動向を振り返って『何に備えるべきか』考える～」
情報セキュリティ戦略セミナー2023（主催：日経クロステック、講演日：2023 年 9 月 4 日）

9. 主な執筆活動

(1)米澤 詩歩乃（国際部 脅威アナリスト）：
「アジア太平洋地域での CSIRT の動向」
（掲載書籍名：情報セキュリティ白書 2023、発行：独立行政法人情報処理推進機構（IPA）、発行日：2023 年 7 月 25 日）

(2) 佐條 研（レスポンスグループ マルウェアアナリスト）：
「消費者が知っておきたい情報セキュリティ対策」
（掲載書籍名：ウェブ版「国民生活」8 月号、発行：独立行政法人国民生活センター、発行日：2023 年 8 月 15 日）

10. 協力、後援

本四半期は次の行事の開催に協力または後援等を行いました。

(1) Internet Week ショーケース in 札幌（主催：日本ネットワークインフォメーションセンター、開催日：2023 年 7 月 20 日、21 日）

(2) JAIPA Cloud Conference 2023（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、開催日：2023 年 9 月 21 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/
■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