JPCERT/CC 活動四半期レポート

2023 年 4 月 1 日 ～ 2023 年 6 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 7 月 13 日

活動概要トピックス

－トピック1－　FIRST の理事に JPCERT/CC スタッフが再選

FIRST（Forum of Incident Response and Security Teams）の理事選挙に JPCERT/CC から立候補していた国際部マネージャーの内田有香子が当選しました。FIRST は、2023 年 6 月現在、105 の国・地域にわたる 679 の CSIRT 組織を会員に擁する世界最大のコミュニティーです。JPCERT/CC は、1998 年に日本で最初の会員となって以来、FIRST の活動に積極的に参加し海外の CSIRT との連携を深めてきました。

FIRST の活動は、Board of Directors を構成する 10 名の理事により企画・立案されています。理事の任期は 2 年間で、毎年その半数が参加組織による選挙で選出されることになっています。6 月上旬にカナダのモントリオールで開催された年次総会で、オンライン投票の結果が発表され、内田を含む 5 名の新理事が決まりました。内田は 2021 年から理事を務めており 2 期目になります。今回の選挙結果は、JPCERT/CC の FIRST に対する継続的な貢献に対する認識と信頼感が寄与したと考えられます。なお、現在の理事の多くは欧米の出身で、アジアからの理事は内田のみとなっています。

再選を受けて内田は「引き続き日本から FIRST の理事活動を続け、アジア太平洋地域における FIRST の活動をますます発展させていきたい。また、次回の FIRST 年次会合は 2024 年 6 月に福岡で開催されることが決まっており、日本国内の協力体制の確立と強化など、同会合の成功に向けても全力を傾けたい」と抱負を述べました。

Board of Directors の他のメンバーや歴任者については、次の URL をご参照ください。

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

FIRST appoints new chair as organization continues to grow globally
https://www.first.org/newsroom/releases/20230608

－トピック2－　2023 年度の JPCERT/CC 感謝状を贈呈

JPCERT/CC は、さまざまな国内のサイバー攻撃の被害を低減するために、インシデントへの対応支援活動、インシデントを未然に防ぐための早期警戒活動、マルウェア分析、ソフトウェア製品等の脆弱性に関する調整活動を行っています。これらの活動を円滑かつ効果的に進めるためには、皆さまからの情報提供やさまざまなご協力が欠かせません。JPCERT/CC では、サイバーセキュリティ対策活動に対する皆

さまからのご厚意とお力添えに深く思いをいたし、特に大きなご貢献をいただいた方に感謝状を贈呈する制度を設けています。
今年度は 6 月に、NTT コム エンジニアリング株式会社の近藤和弘様と、株式会社コンテック PSIRT 様へ感謝状をお贈りいたしました。

NTT コム エンジニアリング株式会社の近藤和弘様は、長年にわたり OCN の Abuse 対応窓口として JPCERT/CC のインシデント調整活動へのご協力をいただいているほか、JPCERT/CC 主催のものを含むコミュニティーやカンファレンス等の場で数多くの有益な情報発信をされ、インシデントの予防や対策の普及への多大な貢献をされました。

これまで株式会社コンテック PSIRT 様は、海外の発見者や調整機関からのものを含む、さまざまな製品脆弱性の報告を受け取り、それらにタイムリーで的確な対応を重ねられてきました。日本製機器に関する海外からの脆弱性報告が近年増えており、その対応に多くの国内企業 PSIRT が苦慮している中にあって、同社の対応体制や取扱手順は模範例の一つと言えます。また脆弱性調整を行う JPCERT/CC にとっても、同社との連携を通じて、より円滑な調整のための示唆を得ることができました。

今年度の感謝状贈呈の詳細については次の Web ページで紹介しています。

JPCERT/CC 感謝状 2023
https://www.jpcert.or.jp/award/appreciation-award/2023.html

－トピック3－　インシデント報告受付先の統合について

JPCERT/CC では、国内のセキュリティインシデントの被害低減を目的としてインシデント報告の受け付けを行っています。組織の立ち上げ当初から行っている情報セキュリティインシデントの報告受け付に加えて、制御システムへの脅威の高まりを背景にして 2013 年 1 月からは制御システムインシデントの報告受け付けも行っています。

制御システムのインシデント報告受付については、受付開始当初から専用のインシデントの報告受付窓口を用意し受付対応を行ってきましたが、制御システムを取り巻く環境の変化や制御システムが関係するインシデントの複雑化などの状況を踏まえ、よりスムーズにインシデント報告をいただけるよう、2023 年 6 月 29 日をもって JPCERT/CC としてのインシデント報告受付を一つに統合し、統合した受付先で情報セキュリティインシデントと制御システムセキュリティインシデント双方の報告を受け付けるよう変更しました。今後のインシデント報告については、制御システムインシデントの報告も含め、次の窓口からお願いします。

- **Web フォームでのインシデント報告受付 URL**

  https://form.jpcert.or.jp/

- **メールでのインシデント報告受付**

  info@jpcert.or.jp

今後ともインシデントの報告にご協力をよろしくお願いします。

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 26,908 件、インシデント件数ベースでは 7,925 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 4,604 件でした。前四半期の 4,326 件と比較して 6%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_Report2023Q1.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 6,186 件で、前四半期の 5,553 件から 11%増加しました。また、前年度同期（8,088 件）との比較では、24%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	4 月	5 月	6 月	本四半期合計（割合）
国内ブランド	1,127	1,351	1,222	3,700(60%)
国外ブランド	587	482	499	1,568(25%)
ブランド不明 (注 2)	226	284	408	918(15%)
全ブランド合計	1,940	2,117	2,129	6,186

（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 81.3%、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 57%で，それぞれ最も多くを占めました。

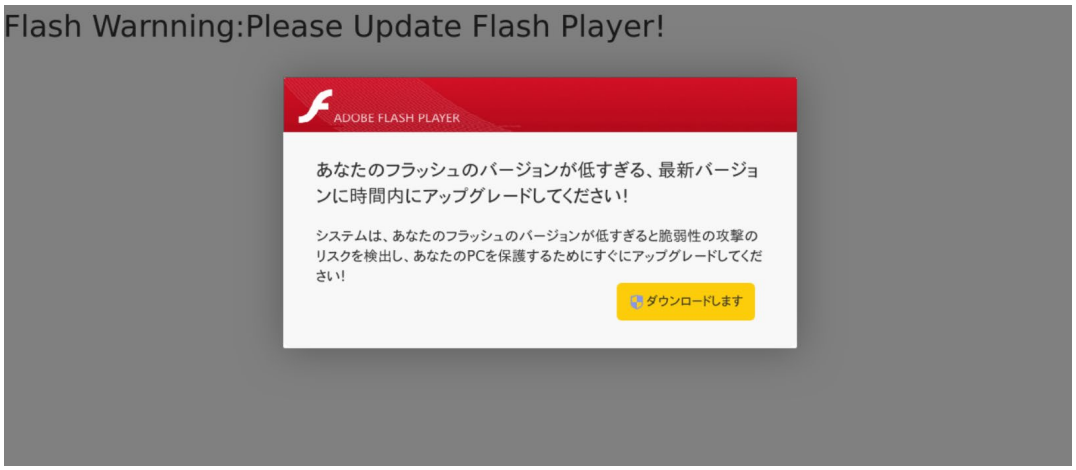
海外ブランドでは、Amazon を装ったフィッシングサイトが全体の半数以上を占めていました。
国内ブランドでは、JR 東日本が提供する Web サイト「えきねっと」や ETC の利用照会サービスを装ったフィッシングサイトが多く報告されました。
国内金融機関では、前四半期に引き続きエポスカード、セゾンカード、イオンカード、そして、三井住友カードを装ったフィッシングサイトが引き続き多く報告されました。

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 25%、国外が 75%であり、前四半期（国内が 24%、国外が 76%）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、311 件でした。前四半期の 362 件から 14%減少しています。

本四半期は、Web サイトの閲覧時に［図 1-1］のような偽の Adobe Flash Player のアップグレード表示することで、マルウェアに感染させる Web サイトを改ざん事例が寄せられました。表示された偽のアップグレード画面の指示にしたがってファイルをダウンロードし、インストールすると Cobalt Strike と呼ばれる攻撃ツールがホスト上にインストールされます。



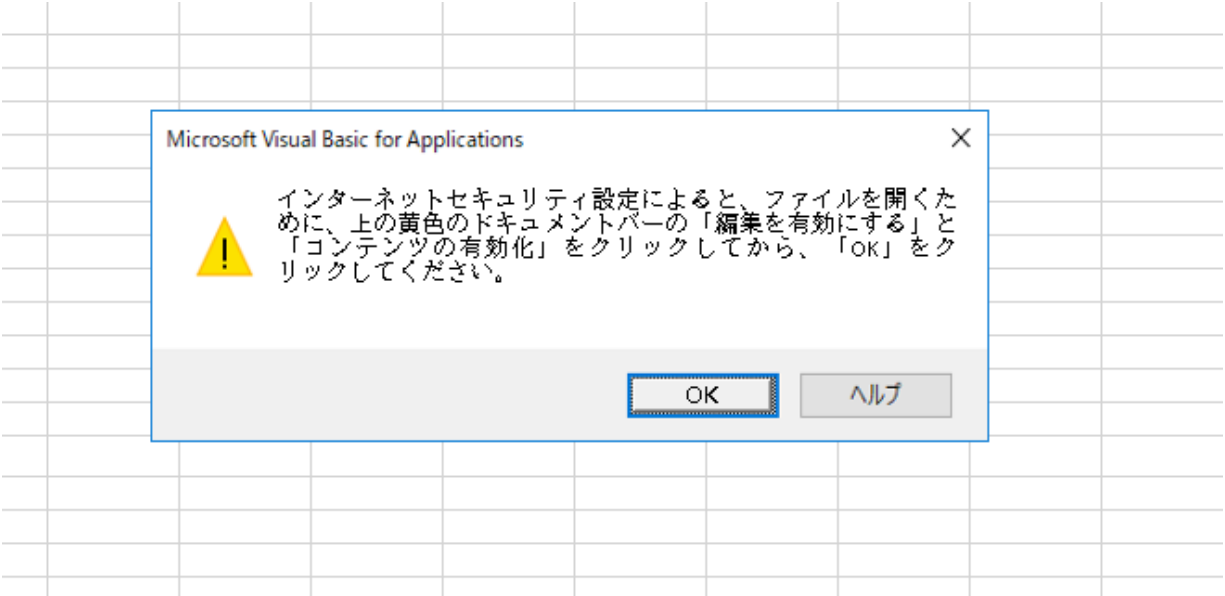
［図 1-1：改ざんされたサイトへアクセス時の表示画面］

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、4 件でした。次に、確認されたインシデントを紹介します。

(1) マルウェア LODEINFO を用いた攻撃

本四半期は、マルウェア LODEINFO を感染させようとする標的型攻撃の報告が寄せられました。本攻撃では、過去にメールでやり取りのあった人物に詐称してターゲットに対してメールを送信し、何回かのメールのやり取りを経て、不正な Excel ファイルが送られてきます。不正な Excel ファイルは［図 1-2］のように、マクロの実行を促す内容が記載されており、マクロを実行すると PEM ファイルを装った LODEINFO（[図 1-3]）がダウンロード・実行されます。



［図 1-2：マクロの実行を誘導する Excel ファイル］

［図 1-3：PEM ファイルを装って暗号化された LODEINFO］

現在、LODEINFO のバージョンは v0.6.8、v0.6.9 などを確認しており、継続してマルウェアの開発が続けられていることが分かっています。

(2) DangerousPassword に関連すると考えられる暗号資産交換事業者への攻撃

本四半期は、攻撃キャンペーン DangerousPassword（CryptoMimic または SnatchCrypto とも呼ばれる）に関連する暗号資産交換事業者への攻撃を確認しています。
ターゲットとなった組織のホスト上で、外部から Windows インストーラー（MSI ファイル）をダウンロードして、実行する不正な Python スクリプトが見つかっており、攻撃者は、何らかの方法で Python スクリプトをターゲットホスト上で実行させたと考えられます。ダウンロードされる MSI ファイルは、以前に弊センターのブログでも紹介したものと同種であり、感染ホストの情報を外部に送信する機能があります。DangerousPassword は、従来のショートカットファイルを用いた攻撃手法以外にさまざまな攻撃手法を用いてマルウェア感染を狙っていることが判明しており、活発な活動がうかがえます。

JPCERT/CC Eyes「攻撃キャンペーン DangerousPassword に関連する攻撃動向」
https://blogs.jpcert.or.jp/ja/2023/05/dangerouspassword.html

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：5 件　https://www.jpcert.or.jp/at/

2023-04-12　2023 年 4 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
2023-04-12　Adobe Acrobat および Reader の脆弱性（APSB23-24）に関する注意喚起
2023-04-19　2023 年 4 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
2023-05-10　2023 年 5 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
2023-06-14　2023 年 6 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

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：12 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」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：9 件（うち更新情報が 1 件）　https://www.jpcert.or.jp/newsflash/

2023-04-10　Apple 製品のアップデートについて（2023 年 4 月）
2023-04-11　Apple 製品のアップデートについて（2023 年 4 月）（更新）
2023-04-12　複数のアドビ製品のアップデートについて
2023-04-26　2023 年 1 月から 3 月を振り返って
2023-05-10　Intel 製品に関する複数の脆弱性について
2023-05-19　Apple 製品のアップデートについて（2023 年 5 月）
2023-06-14　複数のアドビ製品のアップデートについて
2023-06-22　Apple 製品のアップデートについて（2023 年 6 月）
2023-06-22　ISC BIND 9 における複数の脆弱性について（2023 年 6 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) WeeklyReport のリニューアル
2023 年 4 月 5 日、JPCERT/CC は、Web サイトやメーリングリストで毎週提供している Weekly Report をリニューアルしました。今回のリニューアルでは、適切な情報をわかりやすく、正確に伝えられるよう、Weekly Report の構成などを変更しています。

JPCERT/CC Weekly Report リニューアルのお知らせ
https://www.jpcert.or.jp/wr/wrrenewal02303.html

(2) PaperCut MF/NG のリモートコード実行の脆弱性に関する情報発信

2023 年 3 月 8 日（現地時間）、豪 PaperCut Software は、複合機などを管理する製品である「PaperCut MF/NG」における脆弱性に関するアドバイザリを公開しました。
同年 4 月 19 日に同社はアドバイザリを更新し、修正された 2 件の脆弱性のうち、リモートコード実行の脆弱性（CVE-2023-27350）を悪用する攻撃が行われていることを明らかにしました。
その後、JPCERT/CC は同脆弱性を悪用する事案の情報や、脆弱性の実証コード（PoC）の公開を確認し、国内組織でも同製品が利用されている事例を確認したため、国内の関係組織などとも協力の上、同製品の利用組織へ通知し、早期の対策適用を呼びかけました。

PaperCut Software Pty Ltd
APRIL 19 UPDATE | PaperCut MF/NG vulnerability bulletin (March 2023)
https://www.papercut.com/kb/Main/PO-1216-and-PO-1219

1.3. インターネット上の脆弱なノードの多寡に関する分析

JPCERT/CC では、Shodan や Censys、Shadowserver などのインターネットスキャンデータを用い、インターネット上の脆弱なノードの特徴や推移を分析しています。特に、Distributed Reflection Denial of Service（リフレクション型 DoS 攻撃）へ悪用される恐れのあるポートに注目し、それぞれの国・地域の特徴をインターネットスキャンデータから分析、その結果を Web ページ (Mejiro) にて提供しています。対策の必要性や方向性を判断する参考にしていただけるよう、本四半期には、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 カ国の National CSIRT 等の組織に対して分析結果を提供しました。

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. 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

1.3.1.1. 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、インターネットノードから送られてくるパケットを分析する目的で、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。JPCERT/CC は TSUBAME から得られる情報を、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は一つのデータベースにまとめ、分析を行い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

1.3.1.1.1. TSUBAME の観測データの活用

JPCERT/CC では、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 1 月から 3 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 TSUBAME レポート Overflow（2023 年 1～3 月）と題したブログで公開しました。

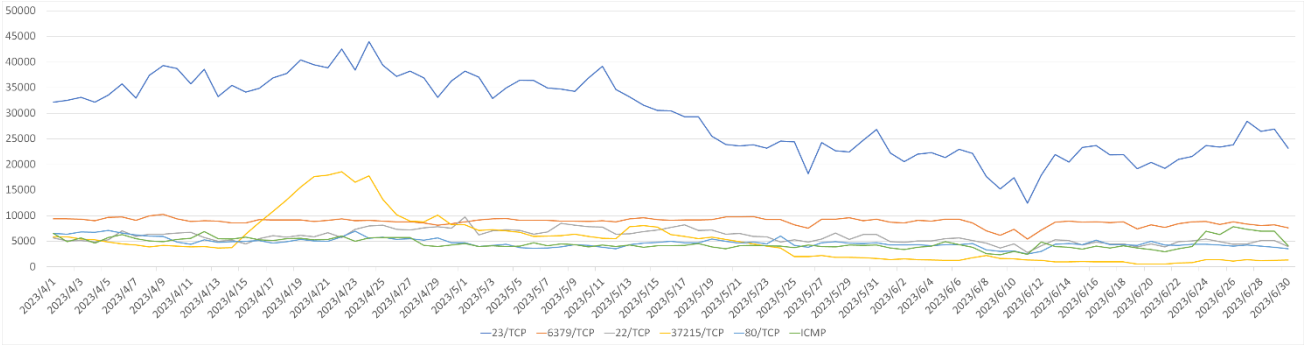
TSUBAME 観測グラフ
https://www.jpcert.or.jp/tsubame/index.html#examples

インターネット定点観測レポート（2023 年 1～3 月）
https://www.jpcert.or.jp/tsubame/report/report202301-03.html

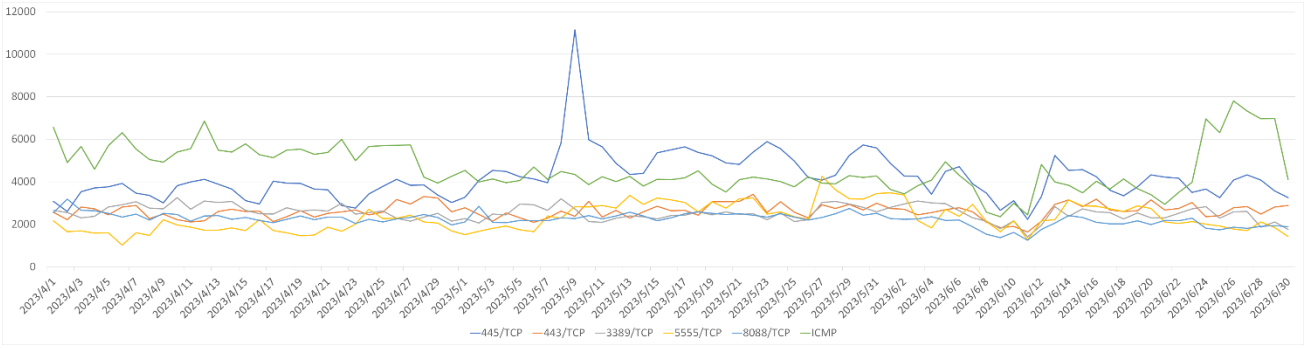
TSUBAME レポート Overflow（2023 年 1～3 月）
https://blogs.jpcert.or.jp/ja/2023/05/tsubame_overflow_2023-01-03.html

1.3.1.1.2. 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。

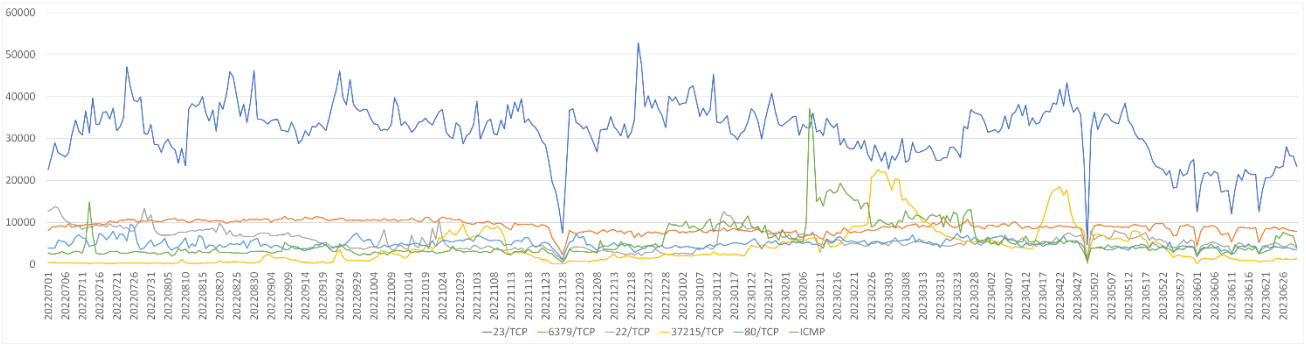


［図 1-4：TSUBAME で観測されたパケットの宛先ポート別内訳 トップ 1-5（2023 年 4 月 1 日-6 月 30 日)］

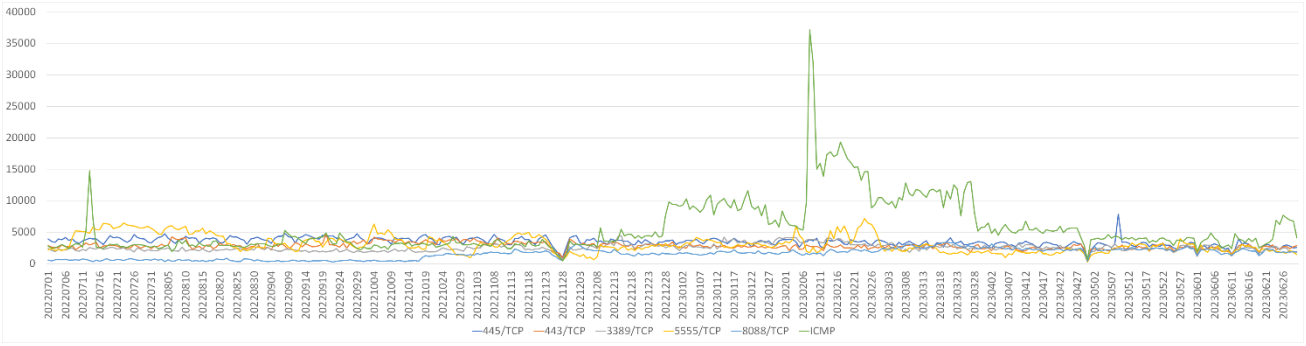


［図 1-5：TSUBAME で観測されたパケットの宛先ポート別内訳 トップ 6-10（2023 年 4 月 1 日-6 月 30 日)］

また、過去 1 年間（2022 年 7 月 1 日-2023 年 6 月 30 日）に観測された、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 1-6］と［図 1-7］に示します。



［図 1-6：TSUBAME で観測されたパケットの宛先ポート別内訳 トップ 1-5（2022 年 7 月 1 日-2023 年 6 月 30 日)］



［図 1-7：TSUBAME で観測されたパケットの宛先ポート別内訳 トップ 6-10（2022 年 7 月 1 日-2023 年 6 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。5 月 6 日頃をピークに増減を繰り返してはいますが、徐々に減少してきています。7 日間平均で 5 月 6 日頃のピークと 6 月末と

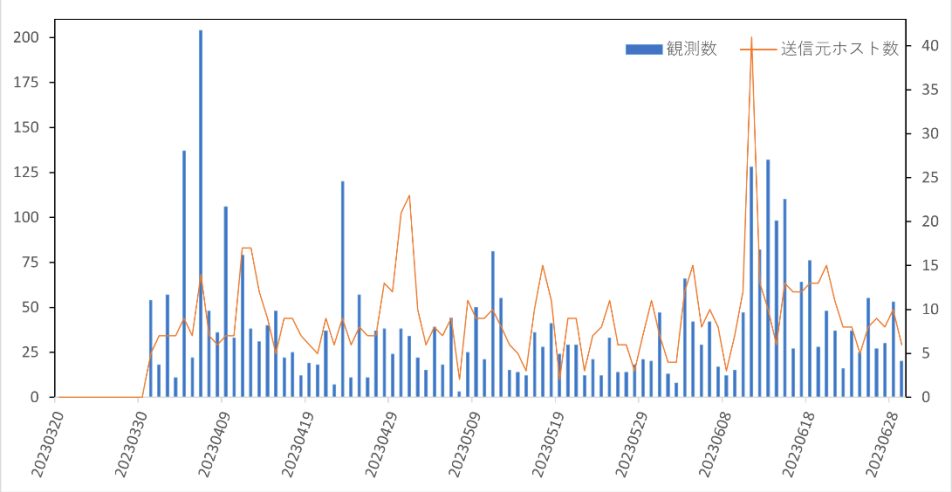
を比較すると半減しました。それ以外のポートでは、37215/TCP 宛のパケットは、4 月 15 日頃急増しましたが、一週間ほどで減少に転じました。それ以外の Port に対するパケットは増減があるものの順位が大きく入れ変わるほどの変化はありませんでした。

1.3.1.2. 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。

1.3.1.2.1. Laravel アプリケーションから設定情報の窃取を試みる通信の観測

2023 年 4 月 1 日以降、AndroxGh0st と呼ばれるマルウェアから発信されたと思われる通信を観測しています［図 1-8］。AndroxGh0st は、Web アプリケーションフレームワーク Laravel の「.env」設定ファイルから情報を窃取する Python で作られたマルウェアで、2021 年のはじめ頃から存在が知られるようになりました。
Laravel の「.env」設定ファイルは、アプリケーションの動作に必要な設定値を保存するために用いられるもので、アプリケーションが AWS 等の外部サービスと連携するための API Key やその他の認証情報が含まれているため、攻撃者による探索の対象となりやすいファイルです。インターネットからアクセス可能である必要はありませんが、アクセス可能なまま運用されている設定上の不備が散見されます。
Laravel フレームワークによるアプリケーションを運用する際は、デバッグ設定が有効になっていないか、不要なファイルをインターネットからアクセス可能な場所に配置していないか、などを注意深く確認する必要があります。



［図 1-8：AndroxGh0st マルウェアが発信したと推測される
通信の観測数（2023 年 3 月 20 日-6 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。
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。）に基づいた国内の脆弱性関連情報の取り扱いにおいて、製品開発者とのコーディネーションを行う「調整機関」として活動しています。この調整活動では、本規程で脆弱性情報の「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。具体的には、本規程に基づく「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。）に基づき活動を実施するとともに、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っています。
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への対応や調整依頼も取り扱っています。

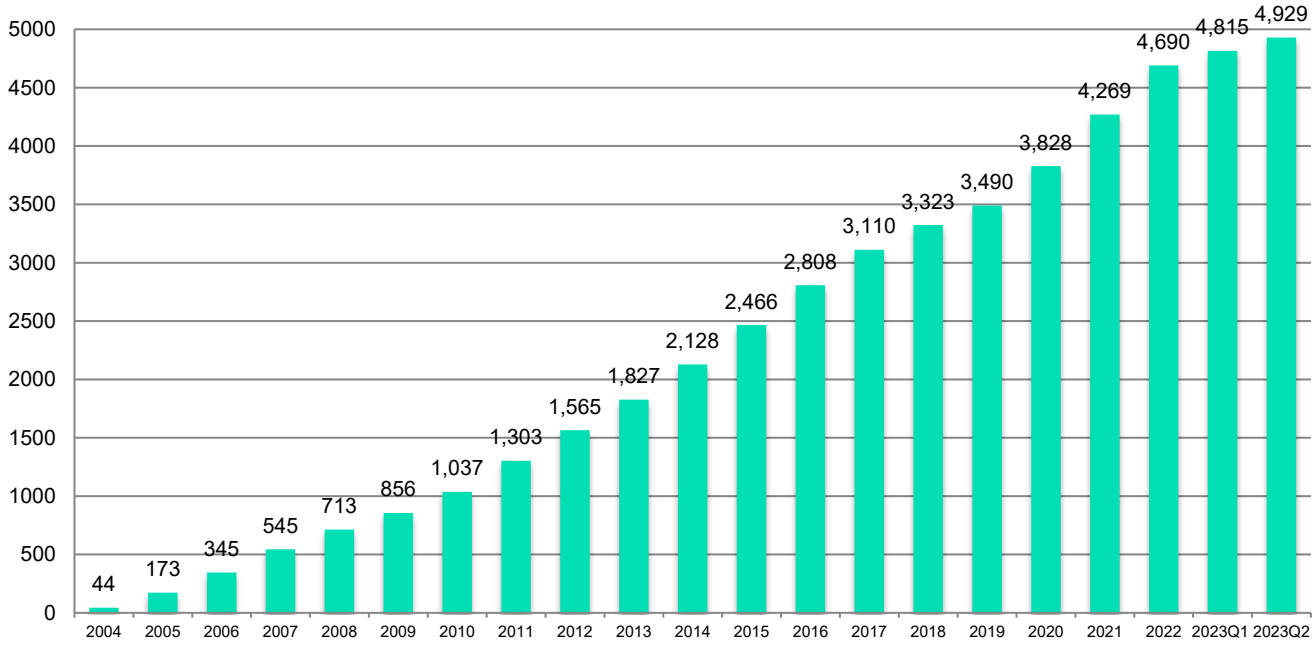
2.1.2. Japan Vulnerability Notes（JVN）において公表した脆弱性情報および対応状況

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 114 件（累計 4,929 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：39 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：74 件
- 脆弱性情報に関連する技術情報等に関するもの：1 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/

本四半期の中で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#1477824
ティアンドデイ製およびエスペックミック製データロガーにおける複数の脆弱性
https://jvn.jp/jp/JVN14778242/

温湿度を記録するデータロガーにおいて、認証なしで設定を改ざんされる脆弱性（CVE-2023-23545）など 4 件の脆弱性が報告され、JPCERT/CC で調整と公表を行ったものです。報告は一つの製品に対するものでしたが、製品開発者との調整の過程で、OEM 製品として他の販売事業者に供給されているものにも同じ脆弱性があることが判明し、報告された製品とともに修正されました。これを受け、アドバイザリでは影響する製品の提供者として 2 社（株式会社ティアンドデイおよびエスペックミック株式会社）を挙げています。このように、個別の製品の脆弱性として報告があった場合でも、複数の開発者や製品が影響を受けるケースを考慮して調整を行っています。

JVN#14492006
TONE ファミリーにおける認証回避の脆弱性
https://jvn.jp/jp/JVN14492006/

本件は、スマホの利用制限や、見守り機能などを提供するサービス「TONE ファミリー」における認証回避の脆弱性です。本件の TONE ファミリーのアプリケーションの脆弱性として報告されましたが、調整の過程で、API サーバーの脆弱性と判明し、製品開発者により脆弱性が除去されました。アプリケーションの更新など利用者側の対応は不要でしたが、サービス提供事業者において、本脆弱性について利用者に周知することが有益と判断し公表が行われました。最近の脆弱性の中には、このように自動アップデートやサーバー側の修正で脆弱性が除去され、アプリケーション利用者の対応を要しないことも多くなっていますが、そうであったとしても脆弱性があったこととそれに関する情報を利用者にわかりやすく伝えることが重要であると考えます。

(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

JVNTA#91513661
FINS プロトコルにおけるセキュリティ上の問題について
https://jvn.jp/ta/JVNTA91513661/

本アドバイザリは、FINS（Factory Interface Network Service）プロトコルとそれを利用する製品を使っている利用者に向けた注意喚起です。FINS プロトコルは、クローズドな FA ネットワークの利用を想定し、オムロン株式会社により開発されました。FA ネットワークの接続先も増えてきており、拡張を重ねる間に意図せずに外部ネットワークに接続されることすらあります。こうした実態に鑑み、FINS プロトコルが前提としているセキュリティ条件や、不用意な利用がもたらすセキュリティ・リスクについて注意を喚起しておきたいとの認識の下で、JPCERT/CC とオムロン株式会社が共同執筆し公表しました。

JVNVU#98434809
複数のプリンタ機器連携用 Android アプリにおけるアクセス制限不備の脆弱性
https://jvn.jp/vu/JVNVU98434809/

相互に似た機能を持つ複数のスマートフォン向けアプリケーションについて、提供元企業が別々でも、開発元が同一だったり、同じコンポーネントを用いて開発されたものであったりするケースが見られます。こうしたケースでは同じ脆弱性が複数の製品に内在する可能性があります。本件においても、発端は海外の発見者からの一つのアプケーションの脆弱性報告でしたが、調整の中で、アプリケーションの提供元や開発元に検証していただいた結果、同じ脆弱性を持つ複数のアプリケーションが特定され、それぞれ修正されることになりました。JPCERT/CC では、複数のアプリケーションの提供元および開発元と協力し、関連製品への影響を含めて脆弱性情報を公表しました。

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) 35th Annual FIRST Conference にて Coordinator Rules を提案

ソフトウェア製品は世界中で広く利用されています。そのため、JPCERT/CC や日本の製品開発者が、海外の脆弱性発見者から直接に、あるいは海外の調整組織を通じて報告を受け取る機会からの報告を受け取る機会が増えています。国際的な脆弱性情報の調整では、国内での調整以上に課題に直面します。各地域の慣習の相違から、関係者の期待にズレが生じることや、そのズレが大きくなることで調整そのものが破綻することがあります。JPCERT/CC では、そうしたトラブルを避け、円滑に情報流通ができるようそれぞれの関係者が協力していくことを、さまざまな組織やコミュニティーに訴えてきました。FIRST では、JPCERT/CC のこれまでの主張をまとめ、各プレーヤーを円滑に繋ぐ考え方について提案しました（2023 年 6 月）。発表後、複数の組織からさまざまなコメントをいただき、調整組織らと今後の国際的な協力活動を進め方について意見交換をしました。JPCERT/CC では、寄せられた意見を参考に、今後も各プレーヤーの共通認識を持てるように協力や提案を進めていく予定です。

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 83 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/

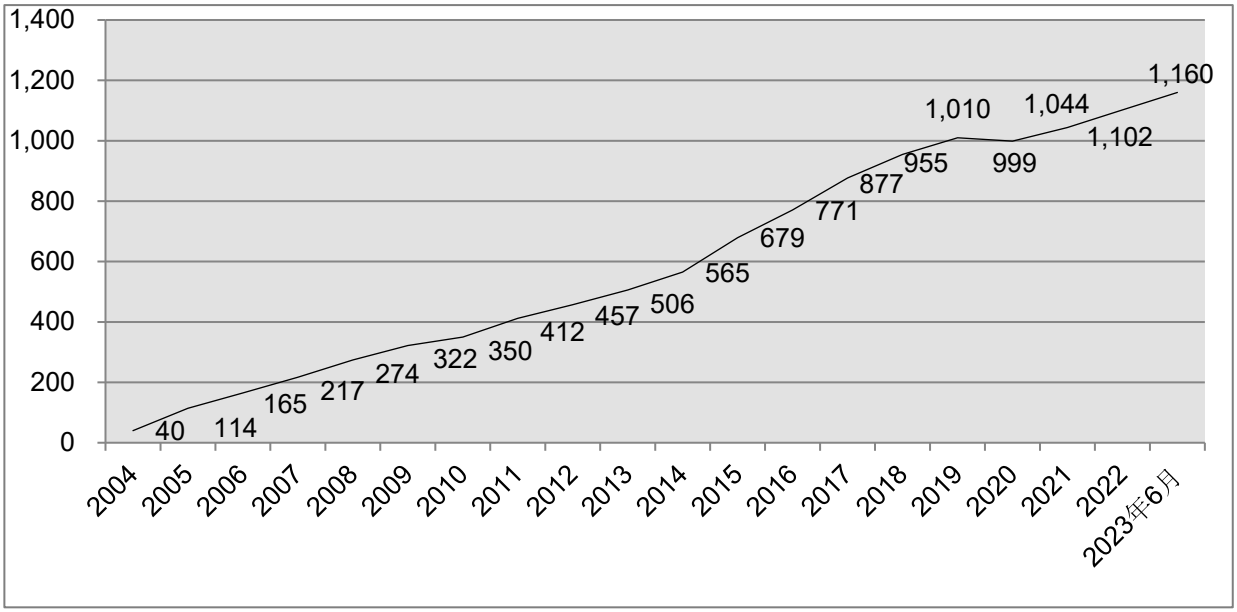
情報セキュリティ早期警戒パートナーシップガイドライン（2019 年版第 2 刷）
https://www.jpcert.or.jp/vh/partnership_guideline2019_r2.pdf

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 2-2］に示すとおり、2023 年 6 月 30 日現在で 1,160 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

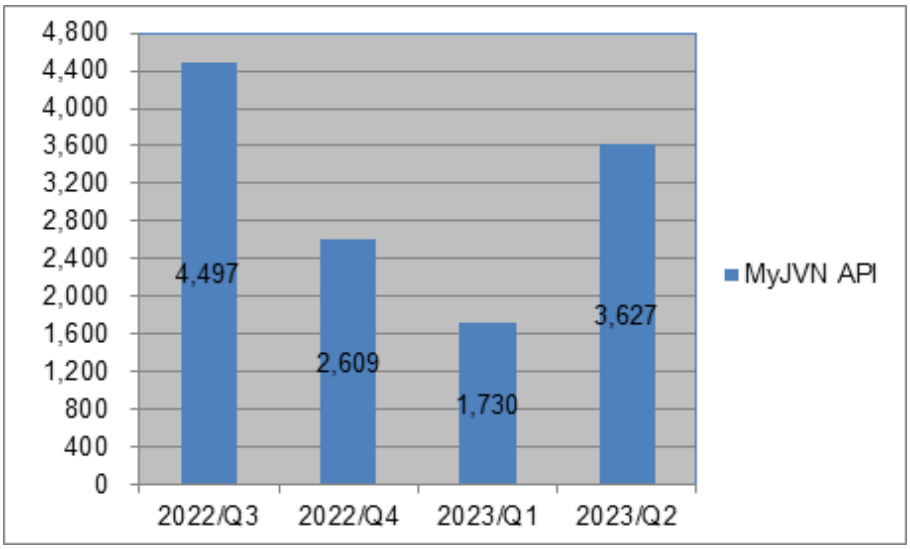
JPCERT/CC では、技術情報やセキュリティ・脆弱性の動向などの情報交換や、脆弱性情報流通業務に関する製品開発者との意見交換、また、製品開発者間の情報交換を目的として、脆弱性情報流通の活動にご協力いただいている製品開発者の皆さまとの定期ミーティングや特定のテーマに関する個別ミーティングを開催しています。
本四半期においては、製品開発者登録ベンダー全体を対象とした定期ミーティングを 6 月 28 日に開催しました。当日は、脆弱性を悪用する攻撃活動の観測状況の説明、製品開発者へ通知する脆弱性情報の選定に使用するキーワードリストの改定についての説明、SLP 実装機器の脆弱性（CVE-2023-29552）についての解説、製品開発者からの PSIRT 活動紹介を行いました。また、それらに関する活発な意見交換も行われました。

2.3. VRDA フィードによる脆弱性情報の配信

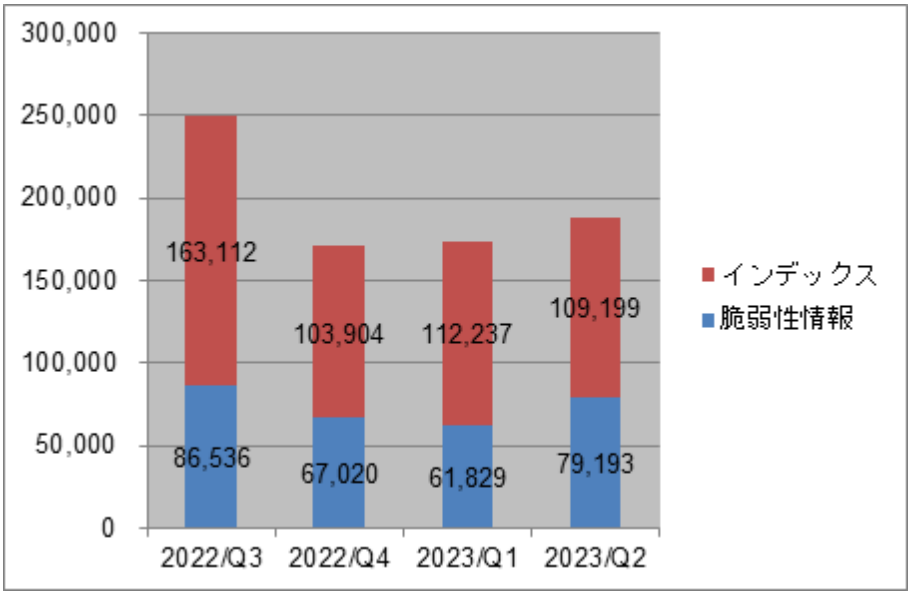
JPCERT/CC は、大規模組織の組織内 CSIRT 等での利用を想定して、ツールを用いた体系的な脆弱性対応を可能とするため、IPA が運用する MyJVN API を外部データソースとして利用した、VRDA（Vulnerability Response Decision Assistance）フィードによる脆弱性情報の配信を行っています。
VRDA フィードについての詳しい情報は、次の Web ページをご参照ください。

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。

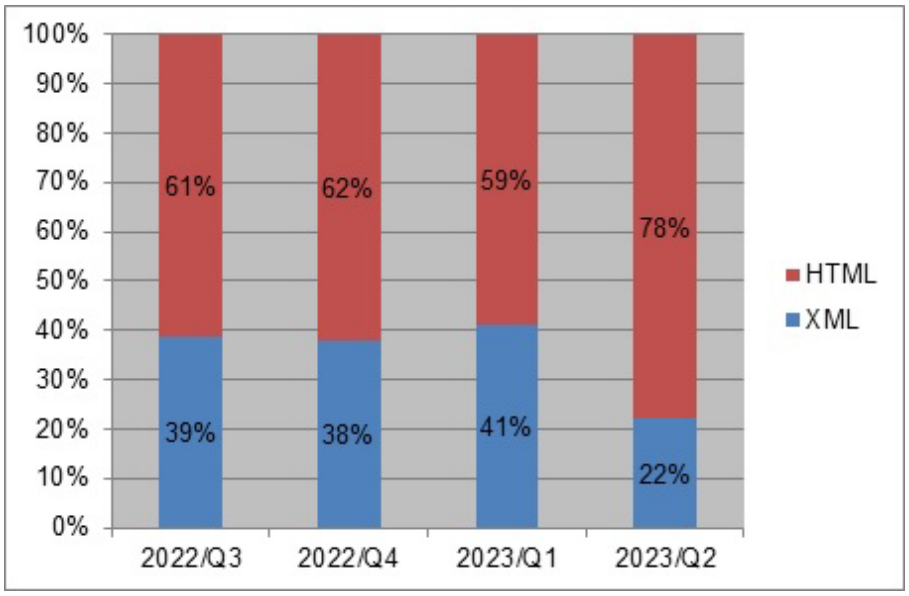


［図 2-3：VRDA フィード配信件数］



［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。脆弱性情報の利用数については、約 28%増加しました。



［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 19%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 204 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「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 1 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。その期間にどのような動きがあったのかがわかるよう同期間に収集した情報をコンパクトにまとめたもので、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

<< 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。

2023-05-02　JPCERT/CC ICS Security Notes FY2022_#Q4

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 1,318 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。

3.2.1. 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。

3.2.3. ICS 脆弱性分析レポート

日々分析を行っている制御システム関連製品の脆弱性情報について、その分析結果を半期ごとに取りまとめ、その中から特に注目すべき情報を解説するレポートを公表する取り組みを 2021 年度から行っています。本レポートは、制御システムユーザー組織のセキュリティ担当者に向けて、制御システム関連製品の脆弱性情報を読み解く際や組織内で利用する制御システム製品の脆弱性への対応を検討する際の参考情報を提供することを目的としています。

本四半期は、2022 年度下期の分析結果を取りまとめたレポートを 2023 年 6 月 29 日に公表しました。2022 年度下期に ICS 固有の通信プロトコルに関する脆弱性が複数公表されたことから、それらを悪用した攻撃シナリオおよび対策方法を説明しています。

ICS 脆弱性分析レポート ― 2022 年度下期 ―
https://www.jpcert.or.jp/ics/ics-vuls-analysis-report

3.3. 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報告件数は 1 件（1 IP アドレス）でした。報告内容は、マルウェアに感染した制御システム関連製品に関するもので、報告にもとづいて調査および調整を進めました。

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：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 に関する利用申し込みはなく、直接配付件数の累計は、日本版 SSAT が 291 件のままでした。

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

3.6. 制御システムインシデント報告の受付先変更

JPCERT/CC では 2023 年 6 月 29 日、制御システムインシデントの報告も、制御システム以外のインシデントと同じ報告受付窓口で受け付けることに変更しました。今後の制御システムインシデント報告受付 URL およびメールアドレスは次のとおりです。

Web フォームでの制御システムインシデント報告受付 URL
https://form.jpcert.or.jp/

メールでの制御システムインシデント報告受付
info@jpcert.or.jp

本件に関する詳細は次の URL をご確認ください。

制御システムインシデント報告の受付先変更完了に関するお知らせ
https://www.jpcert.or.jp/maintenance2023062901.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、5 月 25 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。

4.2.2. 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、下記の年次会合に先立ってモントリオールで行わ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

4.2.2.1. 35th Annual FIRST Conference への参加（6 月 4 日～9 日）

第 35 回 FIRST 年次会合が 6 月 4 日から 9 日にかけてカナダのモントリオールで開催されました。本会合は、サイバーインシデントの予防、対応、技術分析等に関する最新動向の情報交換およびインシデント対応チームの連携強化を目的に毎年開催されています。今回は、昨年と同様に現地開催を主体とし、一部セッションをオンラインで同時配信する形で行われました。今年は“Empowering Communities”のテーマの下に多種多様なトピックが取り上げられ、70 以上の国から約 850 名が現地参加しました。
今回 JPCERT/CC は“Creating the Coordinator Rules”と題した講演を行い、脆弱性情報流通に関わるステークホルダー間のルールやガイドライン策定の取り組みについて提案を発表しました。
さらに、この機会を利用し、世界各国の National CSIRT や製品ベンダーの CSIRT 等と個別に意見を交換しました。このような会合への参加をとおした、各地域間の情報共有の促進や信頼関係の醸成によって、国際間でのインシデント対応調整がより円滑に進められるよう今後も活動してまいります。

第 35 回 FIRST 年次会合についての詳細は、次の Web ページをご参照ください。

35th Annual FIRST Conference
https://www.first.org/conference/2023/

4.2.2.2. FIRST の理事に再選

FIRST の活動の企画・立案等を行う Board of Directors を構成する 10 名の理事は、加盟組織による選挙によって選出されます。理事の任期は 2 年間で、毎年半数が改選の対象となります。選挙はオンライン投票により行われ、6 月 5 日の総会で JPCERT/CC 国際部マネージャーの内田有香子を含む 5 名の当選が発表されました。これにより内田は 2 期目の理事を務めることになりました。他の Board of Directors のメンバーについては、次の URL をご参照ください。

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

FIRST appoints new chair as organization continues to grow globally
https://www.first.org/newsroom/releases/20230608

4.3. その他国際会議への参加

4.3.1. Locked Shields に参加（4 月 17 日～21 日）

4 月 17 日から 21 日にかけて、NATO サイバー防衛協力センター（Cooperative Cyber Defence Centre of Excellence：CCDCOE）が主催する国際的なサイバー演習 Locked Shields 2023 にオンライン参加しました。JPCERT/CC の職員 4 名は日本の政府や重要インフラ事業者の参加者とともにブルーチームの一員として、インシデントの対応および法務・広報の課題に取り組みました。

Locked Shields
https://ccdcoe.org/exercises/locked-shields/

4.3.2. Australia and Japan Cyber Security Workshop 2023 での講演（5 月 10 日）

JPCERT/CC は 5 月 10 日にオーストラリアのゴールドコーストで開催された Australia and Japan Cyber Security Workshop 2023 で講演しました。本会合は、日豪基金とオーストラリア外務貿易省の支援を受けて、クイーンズランド大学が主催しています。開催は昨年に引き続き 2 回目ですが、JPCERT/CC の参加は今年が初めてです。日豪のサイバーセキュリティ分野での連携強化を主たるテーマとし、50 名程度の専門家が集まりました。
JPCERT/CC は、通信インフラのセキュリティとレジリエンス確保がテーマのパネルディスカッションで日豪の間のインシデント対応の実績などについて説明をしました。
イベントの詳細は次の Web ページをご参照ください。

Australia and Japan Cyber Security Workshop 2023
https://www.cyber.uq.edu.au/event/1253/australia-and-japan-cyber-security-workshop-2023

4.3.3. NatCSIRT 2023 への参加（6 月 2～3 日）

第 35 回 FIRST 年次会合に連続した日程で、米国 CERT/CC が主催する National CSIRT Meeting（NatCSIRT）2022 がカナダのモントリオールで開催されました。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し議論することを目的に毎年開催されています。JPCERT/CC は、各国の National CSIRT からの情報提供の取り組みに関するパネルに登壇し、インターネットリスク可視化サービス Mejiro を活用したデータ共有を紹介しました。
NatCSIRT についての詳細は、次の Web ページをご参照ください。

NatCSIRT 2023
https://resources.sei.cmu.edu/news-events/events/natcsirt/index.cfm

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。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 においては、新規策定中の

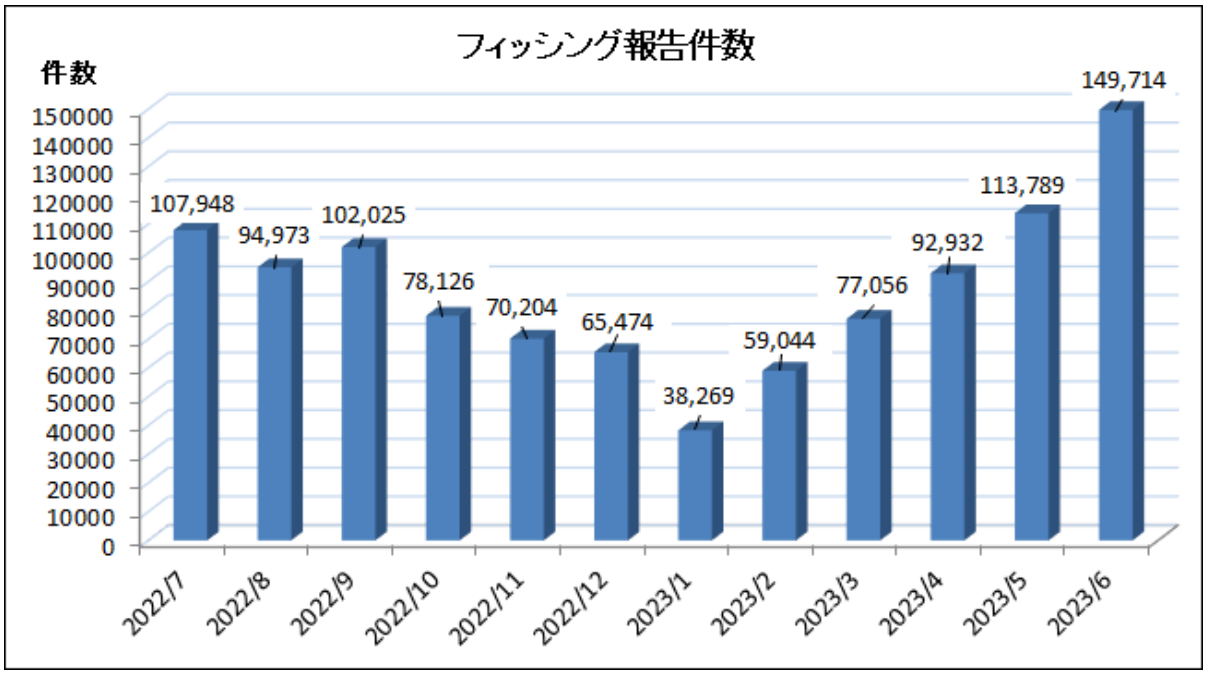
ISO/IEC 27404:Cybersecurity – IoT security and privacy – Cybersecurity labelling framework for consumer IoT についての議論に参加しました。

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、前四半期から引き続き増加傾向が続いていて、6 月は過去最高の報告件数となりました。



［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 17.5%を占めています。ついで、「イオンカード」をかたるフィッシングの報告も多く、全体の約 10.4%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

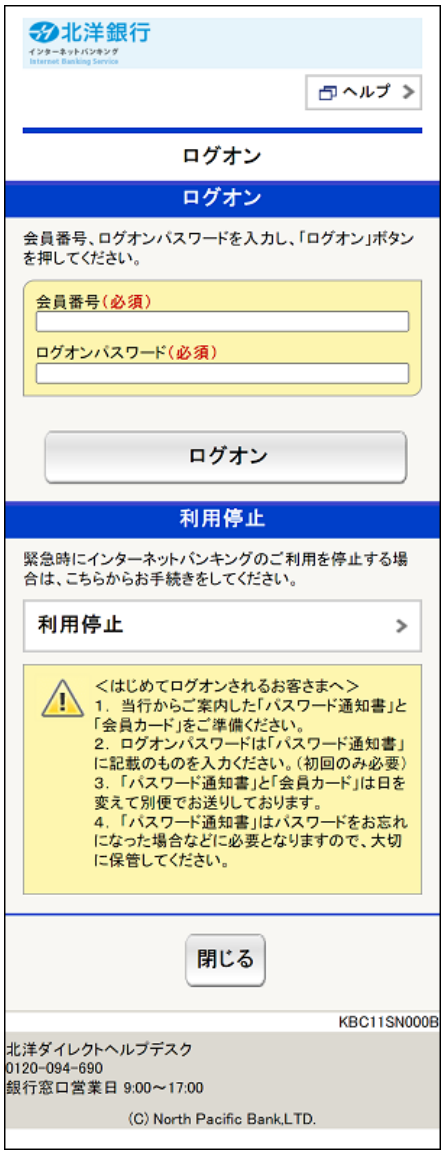
本四半期は、協議会 Web サイトや会員向けメーリングリストを通じて、フィッシングに関する緊急情報を計 39 件発信しました。
利用者が多いサービスに関する、影響範囲が大きいと思われるフィッシングについては、緊急情報を Web サイトに適宜掲載し、広く注意を喚起しました。詳細は次のとおりです。

- マイナポイント事務局をかたるフィッシング　：1 件
- 住信 SBI ネット銀行をかたるフィッシング　：1 件
- 厚生労働省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
- 関税等お支払いサイト（F-REGI 公金支払い）を装うフィッシング　：1 件
- 総務省をかたるフィッシング　：2 件
- 三菱 UFJ 信託銀行をかたるフィッシング　：1 件
- Uber Eats をかたるフィッシング　：1 件
- セブン銀行をかたるフィッシング　：1 件
- NTT グループカードをかたるフィッシング　：1 件
- 三井住友信託銀行をかたるフィッシング　：1 件
- アコムをかたるフィッシング　：1 件
- FamiPay をかたるフィッシング　：1 件
- au じぶん銀行をかたるフィッシング　：1 件
- 国土交通省をかたるフィッシング　：1 件
- Apple をかたるフィッシング　：2 件
- 大和ネクスト銀行をかたるフィッシング　：1 件
- 横浜銀行をかたるフィッシング　：1 件
- りそな銀行をかたるフィッシング　：1 件
- 福井銀行をかたるフィッシング　：1 件
- セゾンカード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　：1 件
- メルカリをかたるフィッシング　：1 件
- 楽天ラクマをかたるフィッシング　：1 件
- みなと銀行をかたるフィッシング　：1 件
- 秋田銀行をかたるフィッシング　：1 件
- エムアイカードをかたるフィッシング　：1 件
- じゃらんをかたるフィッシング　：1 件
- チューリッヒ保険会社をかたるフィッシング　：1 件
- 北海道電力をかたるフィッシング　：1 件
- 沖縄電力をかたるフィッシング　：1 件
- 北洋銀行をかたるフィッシング　：1 件

- 三菱 UFJ 銀行をかたるフィッシング　：1 件
- 日本航空をかたるフィッシング　：1 件
- 西日本シティ銀行をかたるフィッシング：1 件
- ジャックスをかたるフィッシング：1 件
- エポスカードをかたるフィッシング：1 件
- ANA をかたるフィッシング：1 件

本四半期は、前四半期から引き続き報告件数は増加傾向となりました。
本四半期で特筆すべきは、フィッシングの報告数でこれまでトップだった Amazon を上回るブランドが複数現れたことと、金融機関をかたるフィッシングの多発です。前者は、Amazon が送信ドメイン認証（DMARC 等）や正規メールの視認性を向上するためのロゴ表示（BIMI 等）に対応したことで、報告件数が減少していることも理由の一つとして考えられます。また、金融機関をかたるフィッシングは、短期間で次々とブランドを切り替えて行われていて（本四半期中で 12 ブランドをかたるフィッシングの緊急情報を掲載）、今後も同様のフィッシングが発生する可能性があるため、各金融機関は注意が必要です。［図 5-2］

本四半期には、月間の報告数で Amazon を超えるブランドが複数（FamiPay、イオンカード、ヤマト運輸、セゾン Net アンサー）発生し、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：北洋銀行をかたるフィッシングメールの例 ］
https://www.antiphishing.jp/news/alert/hokuyobank_20230614.html

［図 5-3：FamiPay カードをかたるフィッシングサイトの例 ］
https://www.antiphishing.jp/news/alert/famipay_20230421.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 4 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/202304.html

2023 年 5 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/202305.html

2023 年 6 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/202306.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 55 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。
2022 年度に技術・制度検討ワーキンググループにおいて作成と改定を進めた、「フィッシング対策ガイドライン 2023 年度版」（事業者と利用者向け）および「フィッシングレポート 2023」を 2023 年 6 月 1 日に Web に公開しました。それぞれの文書については、次の Web ページをご参照ください。

フィッシング対策ガイドライン 2023 年度版
https://www.antiphishing.jp/report/guideline/antiphishing_guideline2023.html

利用者向けフィッシング詐欺対策ガイドライン 2023 年度版
https://www.antiphishing.jp/report/guideline/consumer_guideline2023.html

フィッシングレポート 2023
https://www.antiphishing.jp/report/wg/phishing_report2023.html

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 107 回運営委員会（オンライン）
  2023 年 4 月 13 日（木）16:00 - 18:00

- 第 108 回運営委員会（オンラインおよび TOPPAN エッジ株式会社会議室）

2023 年 5 月 18 日（木）16:00 - 18:00

- 第 109 回運営委員会（オンライン）
  2023 年 6 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（オンライン）
  日時：4 月- 6 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（オンライン）
  日時：4 月 17 日　16：00 - 18：00
  日時：6 月 20 日　16：00 - 18：00

- 詐欺サイト対処机上演習タスクフォース主催 詐欺サイト被害対応机上演習（プロトタイプ版）
  日時：5 月 30 日　15：00 - 17：00

- フィッシング対策協議会　2023 年度総会
  日時：6 月 9 日　15：00 - 16：45

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。

2023-04-18
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］
https://www.jpcert.or.jp/pr/2023/IR_Report2022Q4.pdf

2023-06-20
JPCERT/CC Incident Handling Report [January 1, 2023 - March 31, 2023]
https://www.jpcert.or.jp/english/doc/IR_Report2022Q4_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。

2023-04-27
JPCERT/CC インターネット定点観測レポート［2023 年 1 月 1 日～2023 年 3 月 31 日］
https://www.jpcert.or.jp/tsubame/report/report202301-03.html
https://www.jpcert.or.jp/tsubame/report/TSUBAME_Report2022Q4.pdf

2023-06-20
JPCERT/CC Internet Threat Monitoring Report [January 1, 2023 - March 31, 2023]
https://www.jpcert.or.jp/english/doc/TSUBAMEReport2022Q4_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。

2023-04-20
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 1 四半期（1 月～3 月）］
https://www.jpcert.or.jp/pr/2023/vulnREPORT_2023q1.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：6 件　https://blogs.jpcert.or.jp/ja/

2023-04-13　暗号資産交換業者を標的とする Parallax RAT 感染を狙った活動
2023-05-01　攻撃キャンペーン DangerousPassword に関連する攻撃動向
2023-05-09　注意喚起や情報共有活動における受信者側の「コスト」の問題について ー情報発信がアリバイや成果目的の自己目的化した行為にならないためにー
2023-05-11　TSUBAME レポート Overflow（2023 年 1～3 月）
2023-05-29　Linux ルーターを狙った Go 言語で書かれたマルウェア GobRAT
2023-06-06　ELF マルウェアの静的分析における Yara ルールを活用した F.L.I.R.T シグネチャ作成手法

英語版発行件数：6 件 https://blogs.jpcert.or.jp/en/

2023-04-20　Activity Targeting Crypto Asset Exchangers for Parallax RAT Infection
2023-04-24　ICS Security Conference 2023
2023-05-12　Attack Trends Related to DangerousPassword
2023-05-29　GobRAT malware written in Go language targeting Linux routers
2023-06-06　How to Create F.L.I.R.T Signature Using Yara Rules for Static Analysis of ELF Malware
2023-06-20　TSUBAME Report Overflow (Jan-Mar 2023)

8. 主な講演活動

(1) 洞田 慎一（早期警戒グループ部門長）：
「CSIRT マネージメントについて ～動ける CSIRT を目指して～」
第 6 回電力 ISAC 総会カンファレンス（主催：電力 ISAC、講演日：2023 年 4 月 27 日）
(2) 三浦 拓也（早期警戒グループ 脅威アナリスト）：
「スピード感を持ったインシデント対処にむけて」
情報セキュリティに関する研修会（主催：公益財団法人高輝度光科学研究センター、講演日：2023 年 5 月 11 日）
(3) 世古 裕紀（早期警戒グループ 脅威アナリスト）：
「コーディネーターの立場から見る、製品開発者における脆弱性対応」
Macnica Security Forum 2023（主催：株式会社マクニカ、講演日：2023 年 5 月 15 日）
(4) 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）：
「サイバー空間の脅威情勢とインシデント対応のポイント ～複雑化する対外応答対応の観点から～」
サイバーセキュリティ・カレッジ（主催：熊本県サイバーセキュリティ推進協議会、講演日：2023 年 6 月 15 日）
(5) 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」
サイバー事件指定捜査員研修（主催：群馬県警察サイバーセンター、講演日：2023 年 6 月 23 日）

(6) 世古 裕紀（早期警戒グループ 脅威アナリスト）：
「業界連携での対応体制づくり／情報共有活動づくり」
情報セキュリティ専門委員会勉強会（主催：一般社団法人建設コンサルタンツ協会 情報セキュリティ専門委員会、講演日：2023 年 6 月 27 日）

9. 主な執筆活動

(1) 宮地利雄（技術顧問）：
「サイバーセキュリティリスクの動向」
（計測自動制御学会「計測と制御」2023 年 4 月号 第 62 巻第 4 号、2023 年 4 月 10 日発行）

(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～」
（掲載書籍名：ユクタス Vol.5、発行：株式会社内田洋行 IT ソリューションズ、発行日：2023 年 6 月 1 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）：
「2022 年度国連北朝鮮制裁委報告書から北朝鮮関連のサイバー攻撃動向を読み解く―新たな攻撃グループ登場の背景とその動向について―」
（掲載書籍名：ＣＩＳＴＥＣジャーナル 2023 年 5 月号、発行：一般財団法人安全保障貿易情報センター、発行日：2023 年 6 月 5 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) 第 27 回サイバー犯罪に関する白浜シンポジウム
主催：サイバー犯罪に関する白浜シンポジウム実行委員会
開催日：2023 年 5 月 25 日～27 日

(2) Interop Tokyo 2023
主催：株式会社ナノオプト・メディア
開催日：2023 年 6 月 14 日～16 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