JPCERT/CC 活動四半期レポート

2022 年 10 月 1 日 ～ 2022 年 12 月 31 日

一般社団法人 JPCERT コーディネーションセンター

2023 年 1 月 19 日

活動概要トピックス

ートピック1ー　JPCERT/CC ベストレポーター賞 2022

インシデントや脆弱性といったサイバーセキュリティに関する問題をいち早く発見し正確な情報を提供いただける報告者（レポーター）の皆さまは、サイバーセキュリティにおける問題解決に向けて JPCERT/CC が調整業務を的確に進めるための重要な情報源であり協力者でもあります。
また、インシデントや脆弱性の数が増加し、また問題が複雑化し高度化している現状においては、レポーターの皆さまの協力を得て、より多くの問題を迅速に解決していくことの重要性がさらに増してきています。
このような状況を踏まえ JPCERT/CC では、日々情報を提供いただいている報告者の皆さまのお力添えに感謝の意をお伝えするとともに、特に優れた報告者の活動事例を広く世に知っていただく機会になればと考え、「ベストレポーター賞」を贈呈させていただく制度を昨年度から設けています。

ベストレポーター賞は、インシデント報告と脆弱性報告のそれぞれの部門において、情報提供を通じて JPCERT/CC の活動に顕著な貢献をいただいた方に年 1 回、感謝の意を表し記念品を贈らせていただくものです。なお、インシデント報告部門ではインシデント報告の件数とその内容に基づいて、脆弱性報告部門では JPCERT/CC や JVN に相談・報告をいただいた脆弱性情報の件数とその内容に基づいて、それぞれ受賞者を選定することにしています。

2 回目となる本年度は次の方々にベストレポーター賞をお贈りしました。

日本電気株式会社 岩田 友臣 様（インシデント報告部門）
Michael Heinzl 様（脆弱性報告部門）

岩田 友臣様からは、個人の活動として、国内の Web サイト改ざんインシデントに関する質の高い報告を数多くいただきました。また、JPCERT/CC が主催するコミュニティーにおいて、その手口の傾向や調査方法等について共有いただき、対策の普及の面でも多大な貢献をしていただきました。
Michael Heinzl 様からは、個人の活動として、日本製を含む数多くの産業用／制御システムや機器の脆弱性を発見し報告していただきました。Heinzl 様は JPCERT/CC を介して製品開発者との連携を行う Responsible Disclosure を実践されており、Heinzl 様の報告への対応が国内製品開発者における PSIRT 体制の整備や脆弱性対応手順の改善につながった複数の事例がありました。これらの好ましい対応事例は、JPCERT/CC が主催する国内制御システム開発者コミュニティーでの PSIRT 活動の普及啓発にも活かされています。
受賞者の皆さまをはじめ JPCERT/CC の活動に協力していただいている多くのレポーターの方々に改めて感謝申し上げます。

JPCERT/CC ベストレポーター賞 2022
https://www.jpcert.or.jp/award/best-reporter-award/2022.html

ートピック2ー　海外との往来が再開され JPCERT/CC の活発な国際連携活動が戻り始めました

2019 年度末から、新型コロナウイルスの感染拡大やそれに伴う各国の渡航制限などの影響により、多くの国際会議やイベントが中止になり、オンライン開催に限定されてきました。今年度の半ば頃から渡航制限の緩和が進み、多くの国際会議がコロナ前に準じた開催形態に戻りつつあります。日本の水際対策も緩和され、本四半期から JPCERT/CC でも、職員が海外に出張して国際会議に参加する、また、海外から来訪した CSIRT 担当者などを迎えて打ち合わせを持つなど、海外との交流が再び活発になってきました。例えば「4. 国際連携活動関連」で詳しく述べるように、10 月にはアメリカの CISA（Cybersecurity and Infrastructure Security Agency）を JPCERT/CC オフィスに迎え、コロナ禍以降初めてとなる対面での意見交換を行いました。また、シンガポール CSA（Cyber Security Agency）をはじめ海外の複数のサイバーセキュリティ関係機関の来訪もあり活動状況や今後の連携に関する議論をしました。
また、11 月末にはエチオピアで開催された国連が主催するインターネットガバナンスに関する最大規模の会議 Internet Governance Forum に 3 年ぶりに対面で参加し、パネルセッションに登壇しました。また、エチオピアの CSIRT やサイバーセキュリティ専門家などとの意見交換も実現し、その後、ルワンダに立ち寄って現地の CSIRT などを訪問することもできました。

多くの国際会議は、対面開催とオンライン配信のハイブリッド形式あるいは現地開催のみの実施形態に徐々に戻りつつあり、すでに今後の国際会議参加のための出張の予定が複数固まり、海外からの来訪の調整も進んでいます。これらの対面での会議参加や、CSIRT 間の往来の復活により、組織間の連携の再開や活性化が期待されています。2023 年は、さらに出張や来訪対応が増えることが見込まれており、JPCERT/CC では国際連携活動をより一層強化していきたいと考えています。

JPCERT CC®

目次

1. 早期警戒 6
1.1. インシデント対応支援 6
1.1.1. インシデントの傾向 6
1.1.2. インシデントに関する情報提供のお願い 8
1.2. 情報収集・分析 8
1.2.1. 情報提供 9
1.2.2. 情報収集・分析・提供（早期警戒活動）事例 11
1.3. インターネット上の脆弱なノード数の分布の分析 12
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 13
2. 脆弱性関連情報流通促進活動 17
2.1. 脆弱性関連情報の取り扱い状況 17
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 17
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 18
2.1.3. 連絡不能開発者とそれに対する対応の状況等 22
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 22
2.2. 日本国内の脆弱性情報流通体制の整備 23
2.2.1. 日本国内製品開発者との連携 24
2.2.2. 製品開発者との定期ミーティング等の実施 24
2.3. VRDA フィードによる脆弱性情報の配信 25
3. 制御システムに関するセキュリティ対策活動 27
3.1. 情報収集分析 27
3.1.1. 情報提供 27
3.2. 制御システム関連のインシデント対応 28
3.3. 関連団体との連携 29
3.4. 制御システム向けセキュリティ自己評価ツールの提供 29
3.5. 連載「標準から学ぶ ICS セキュリティ」2 回目の記事を公表 29
4. 国際連携活動関連 30
4.1. 海外 CSIRT 構築支援および運用支援活動 30
4.2. 国際 CSIRT 間連携 30
4.2.1. APCERT（Asia Pacific Computer Emergency Response Team） 30
4.2.2. FIRST（Forum of Incident Response and Security Teams） 31
4.3. その他国際会議への参加 31
4.3.1. インド太平洋地域向け日米 EU 産業制御システムサイバーセキュリティウィークでの講演（10 月 26 日） 31
4.3.2. ASEAN CERTs Incident Drill (ACID)参加（10 月 27 日） 32

4.3.3. Internet Governance Forum (IGF)への参加（11 月 28 日～12 月 2 日） 32
4.3.4. 38th TWNIC Open Policy Meeting での登壇（12 月 1 日） 32
4.4. 海外 CSIRT 等の来訪および往訪 32
4.4.1. 米国 CISA の来訪（10 月 25 日） 32
4.4.2. シンガポール CSA の来訪（11 月 29 日） 33
4.4.3. ルワンダ Rw-CSIRT の訪問（12 月 6 日） 33
4.4.4. エチオピア Ethio CERT の訪問（12 月 9 日） 33
4.5. 国際標準化活動 33
5. フィッシング対策協議会事務局の運営 33
5.1. フィッシングに関する報告・問い合わせの受付 34
5.2. 情報収集／発信 34
5.2.1. フィッシングの動向等に関する情報発信 34
5.2.1. 定期報告 38
5.2.2. フィッシングサイト URL 情報の提供 38
5.2.3. フィッシング対策ガイドライン等の改定作業 38
6. フィッシング対策協議会の会員組織向け活動 39
6.1. 運営委員会開催 39
6.2. ワーキンググループ会合等 開催支援 39
7. 公開資料 40
7.1. インシデント報告対応レポート 40
7.2. インターネット定点観測レポート 40
7.3. 脆弱性関連情報に関する活動報告 41
7.4. JPCERT/CC Eyes～JPCERT コーディネーションセンター公式ブログ～ 41
8. 主な講演活動 41
9. 協力、後援 42

本活動は、経済産業省より委託を受け、「令和４年度サイバー攻撃等国際連携対応調整事業」として実施したものです。ただし、「6.フィッシング対策協議会の会員組織向け活動」に記載の活動についてはこの限りではありません。また、「4. 国際連携活動関連」、「8. 主な講演活動」、「9. 協力、後援」には、受託事業以外の自主活動に関する記載が一部含まれています。

1. 早期警戒

1.1. インシデント対応支援

JPCERT/CC が本四半期に受け付けたコンピューターセキュリティインシデント（以下「インシデント」という。）に関する報告は、報告件数ベースで 11,923 件、インシデント件数ベースでは 8,425 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 5,759 件でした。前四半期の 6,444 件と比較して 11%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_Report2022Q3.pdf

1.1.1. インシデントの傾向

1.1.1.1. フィッシングサイト

本四半期に報告が寄せられたフィッシングサイトの件数は 7,520 件で、前四半期の 8,088 件から 7%減少しました。また、前年度同期（6,311 件）との比較では、19%の増加となりました。

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

［表 1-1：フィッシングサイト件数の国内・国外ブランド別内訳］

フィッシングサイト	10 月	11 月	12 月	本四半期合計（割合）
国内ブランド	1,413	888	1,112	3,413(54%)
国外ブランド	850	773	767	2,390(38%)
ブランド不明（注 2）	143	181	139	463(7%)
全ブランド合計	2,406	1,842	2,018	6,266

（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 71.4%、国内ブランド関連の報告では金融機関のサイトを装ったものが 11.9%で，それぞれ最も多くを占めました。

海外ブランドでは、Amazon を装ったフィッシングサイトが全体の半数以上を占めていました。
国内ブランドでは、JR 東日本が提供する Web サイト「えきねっと」や国税庁を装ったフィッシングサイトが多く、ETC の利用照会サービスや楽天・楽天カードを装ったフィッシングサイトも引き続き多く報告されました。

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

フィッシングサイトテイクダウンのために調整したサイトの割合は、国内が 20%、国外が 80%であり、前四半期（国内が 28%、国外が 72%）と比較し国外が増加しました。

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、427 件でした。前四半期の 695 件から 39%減少しています。

本四半期は、CMS を利用している正規の Web サイトが改ざんされる事例が複数確認されました。改ざんされた Web サイトには［図 1-1］のような難読化された JavaScript が挿入されていることを確認しました。該当のスクリプトは、Web サイト上で入力されたクレジットカード情報等の窃取を行います。

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

［図 1-1：難読化されたスクリプトの一部抜粋］

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

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、1 件でした。
次に、確認されたインシデントを紹介します。

(1) LinkedIn 経由で不正なヘルプファイルをダウンロードさせる攻撃

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

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

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

1.1.2. インシデントに関する情報提供のお願い

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

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

1.2. 情報収集・分析

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

の抑止を目指しています。

1.2.1. 情報提供

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

1.2.1.1. 注意喚起

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

発行件数：14 件（うち更新情報が 4 件）　https://www.jpcert.or.jp/at/

2022-10-11　Fortinet 製 FortiOS、FortiProxy および FortiSwitchManager の認証バイパスの脆弱性（CVE-2022-40684）に関する注意喚起
2022-10-11　bingo!CMS の認証回避の脆弱性（CVE-2022-42458）に関する注意喚起
2022-10-12　2022 年 10 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
2022-10-12　Adobe Acrobat および Reader の脆弱性（APSB22-46）に関する注意喚起
2022-10-14　Fortinet 製 FortiOS、FortiProxy および FortiSwitchManager の認証バイパスの脆弱性（CVE-2022-40684）に関する注意喚起（更新）
2022-10-19　2022 年 10 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
2022-11-02　OpenSSL の脆弱性（CVE-2022-3602、CVE-2022-3786）に関する注意喚起
2022-11-04　マルウェア Emotet の感染再拡大に関する注意喚起（更新）
2022-11-09　2022 年 11 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
2022-12-13　FortiOS のヒープベースのバッファーオーバーフローの脆弱性（CVE-2022-42475）に関する注意喚起
2022-12-14　Citrix ADC および Citrix Gateway の脆弱性（CVE-2022-27518）に関する注意喚起
2022-12-14　2022 年 12 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
2022-12-14　FortiOS のヒープベースのバッファーオーバーフローの脆弱性（CVE-2022-42475）に関する注意喚起（更新）
2022-12-19　FortiOS のヒープベースのバッファーオーバーフローの脆弱性（CVE-2022-42475）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 85 件、「今週のひとくちメモ」のコーナーで紹介した情報は次の 13 件でした。

2022-10-05　IPA が「ビジネスメール詐欺（BEC）対策特設ページ」を公開
2022-10-13　JPCERT/CC が「TLP v2 の日本語版が公開されました」を公開
2022-10-19　JIPDEC が注意喚起「EC サイトにおける個人情報の漏えい（クレジットカード情報等）事故が増えています」を公開
2022-10-26　JPCERT/CC が 2022 年 7 月～2022 年 9 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
2022-11-02　JPCERT/CC が 2022 年 7 月~2022 年 9 月分の「インターネット定点観測レポート（2022 年 7~9 月）」「TSUBAME レポート Overflow（2022 年 7~9 月）」を公開
2022-11-09　マルウェア Emotet の感染に至るメールの配布再開に関する注意喚起
2022-11-16　Internet Week 2022 開催のお知らせ
2022-11-24　FIRST が「PSIRT Services Framework 1.1 日本語版と PSIRT Maturity Document 1.1 日本語版」を公開
2022-11-30　JSAC2023 参加申し込み開始
2022-12-07　NISC と警察庁が「学術関係者・シンクタンク研究員等を標的としたサイバー攻撃について（注意喚起）」を公開
2022-12-14　JPCERT/CC ベストレポーター賞 2022
2022-12-21　日本シーサート協議会が「CSIRT 人材の育成 Ver1.0」を公開
2022-12-28　JPCERT/CC が「2022 年 10 月から 12 月を振り返って」を公開

1.2.1.3. 早期警戒情報

重要インフラを支える組織の情報セキュリティ関連部署もしくは組織内 CSIRT のうち、「早期警戒情報」という枠組みに参加いただいた方々に向けて、セキュリティ上の深刻な影響をもたらす可能性のある脅威情報やその分析結果、対策方法に関する「早期警戒情報」と呼ばれる情報を、各組織における必要性を勘案して、提供しています。本四半期には 3 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：7 件（うち更新情報が 1 件）　https://www.jpcert.or.jp/newsflash/

2022-10-12　複数のアドビ製品のアップデートについて
2022-10-20　2022 年 7 月から 9 月を振り返って
2022-10-25　Apple 製品のアップデートについて（2022 年 10 月）
2022-10-28　Apple 製品のアップデートについて（2022 年 10 月）（更新）
2022-11-09　Intel 製品に関する複数の脆弱性について
2022-12-14　Apple 製品のアップデートについて（2022 年 12 月）
2022-12-22　2022 年 10 月から 12 月を振り返って

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) Fortinet 社製 FortiOS、FortiProxy および FortiSwitchManager の認証バイパスの脆弱性（CVE-2022-40684）に関する情報発信

2022 年 10 月 10 日（米国時間）、Fortinet 社から FortiSwitchManager における認証バイパスの脆弱性（CVE-2022-40684）に関するアドバイザリが公表されました。

本脆弱性により、認証されていない遠隔の第三者が、同製品の管理インタフェースに細工した HTTP あるいは HTTPS リクエストを送信し、結果として任意の操作を行う可能性があります。Fortinet 社によると、本脆弱性を悪用した攻撃をすでに確認しているとのことで、JPCERT/CC は 11 日に注意喚起を公表しました。また、JPCERT/CC は、公表されていた本脆弱性の実証コードを入手し、検証を行いました。実際に実証コードが動作することを確認できたため、14 日に注意喚起を更新し、早期の対策の実施を呼びかけました。また、本脆弱性の対応時の参考情報として 18 日に早期警戒情報を公表し、実証コードの動作検証結果を CISTA ユーザーに共有しました。その後、追加の検証結果を得たため、21 日に早期警戒情報を更新し、さらなる注意を呼びかけました。

Fortinet 製 FortiOS、FortiProxy および FortiSwitchManager の認証バイパスの脆弱性（CVE-2022-40684）に関する注意喚起
https://www.jpcert.or.jp/at/2022/at220025.html

(2) FortiOS のヒープベースのバッファーオーバーフローの脆弱性（CVE-2022-42475）に関する情報発信

2022 年 12 月 12 日（米国時間）、Fortinet 社から FortiOS SSL-VPN におけるヒープベースのバッファーオーバーフローの脆弱性（CVE-2022-42475）に関するアドバイザリが公表されました。
本脆弱性により、認証されていない遠隔の第三者が、細工したリクエストを送信し、任意のコードやコマンドを実行する可能性があります。加えて、Fortinet 社は同アドバイザリ内にて、本脆弱性を悪用する攻撃を確認していると報告しており、JPCERT/CC は、早期の対応を呼びかけるために、13 日に注意喚起を公表しました。
また、Fortinet 社は本脆弱性の影響を受ける対象バージョンなどの情報を更新しており、JPCERT/CC もそれにあわせて、14 日と 19 日に注意喚起を更新しました。

FortiOS のヒープベースのバッファーオーバーフローの脆弱性（CVE-2022-42475）に関する注意喚起
https://www.jpcert.or.jp/at/2022/at220032.html

(3) Citrix ADC および Citrix Gateway の脆弱性（CVE-2022-27518）に関する情報発信

2022 年 12 月 13 日（米国時間）、Citrix 社から Citrix Application Delivery Controller（Citrix ADC）および Citrix Gateway の脆弱性（CVE-2022-27518）に関するアドバイザリが公表されました。本脆弱性により、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可能性があります。Citrix 社は同アドバイザリで、本脆弱性を悪用する攻撃を確認していると述べています。JPCERT/CC は、早期の対応を呼びかけるために、14 日に注意喚起を公表しました。

Citrix ADC および Citrix Gateway の脆弱性（CVE-2022-27518）に関する注意喚起
https://www.jpcert.or.jp/at/2022/at220033.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。

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

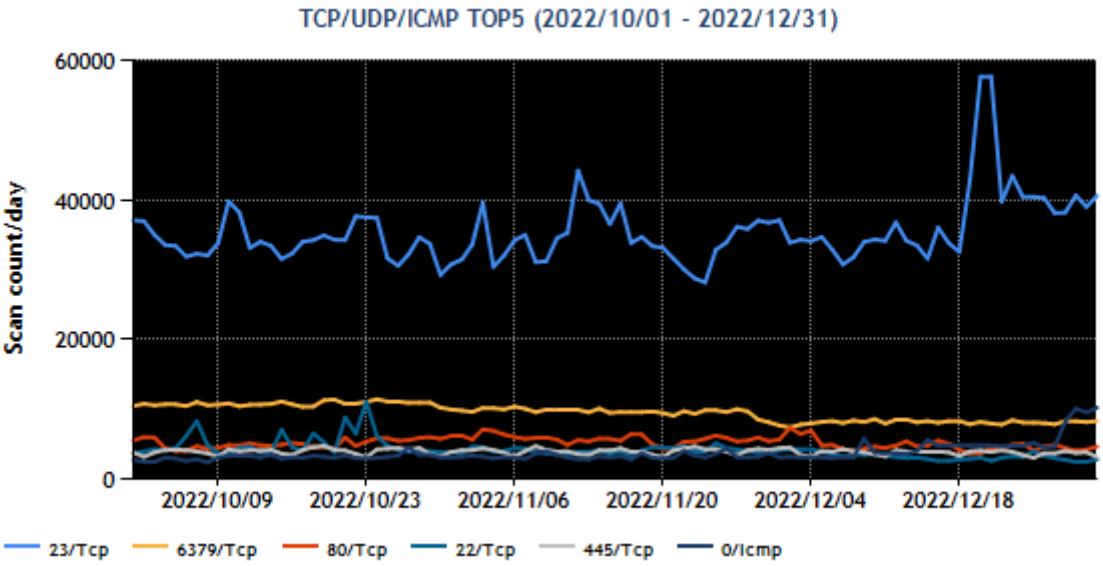
1.3.2.1.1. TSUBAME の観測データの活用

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 7 月から 9 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。

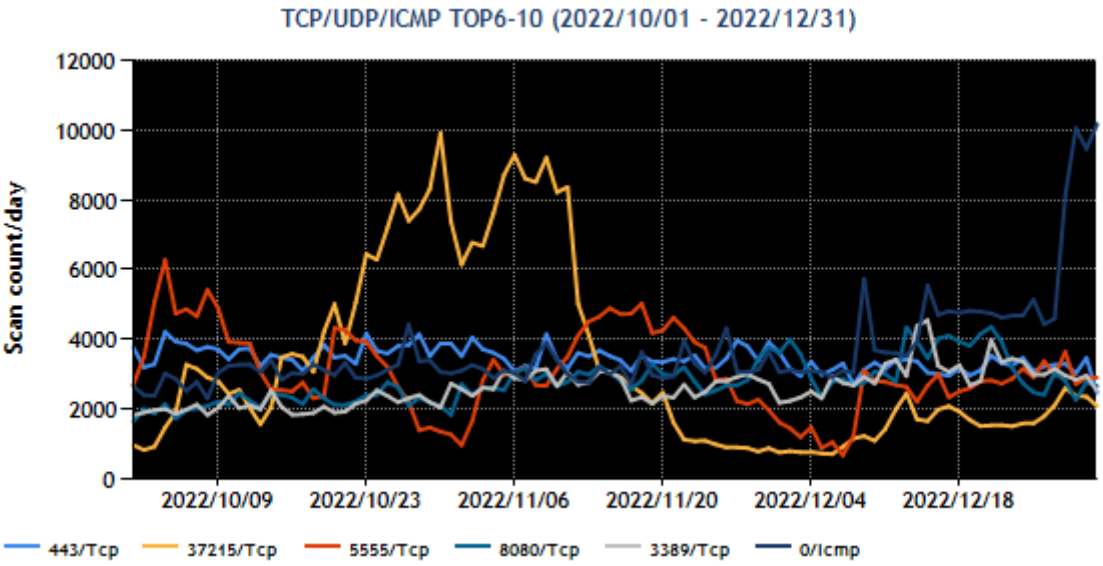
TSUBAME 観測グラフ
https://www.jpcert.or.jp/tsubame/index.html#examples
インターネット定点観測レポート（2022 年 7～9 月）
https://www.jpcert.or.jp/tsubame/report/report202207-09.html
TSUBAME レポート Overflow（2022 年 7～9 月）
https://blogs.jpcert.or.jp/ja/2022/10/tsubame_overflow_2022-07-09.html

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 1-2］と［図 1-3］示します。

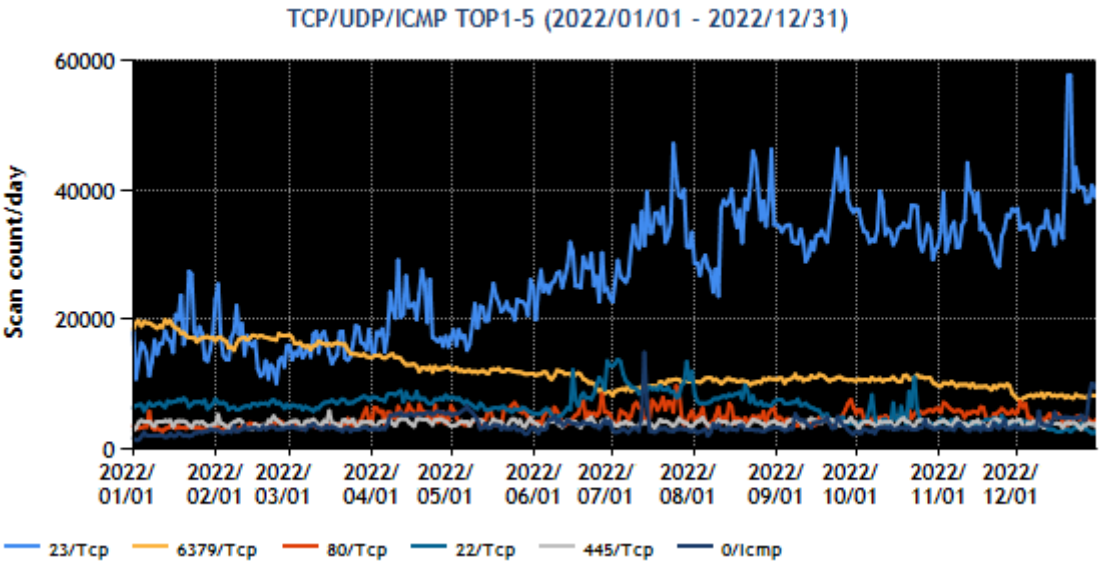


［図 1-2：宛先ポート別グラフ トップ 1-5（2022 年 10 月 1 日-12 月 31 日）］

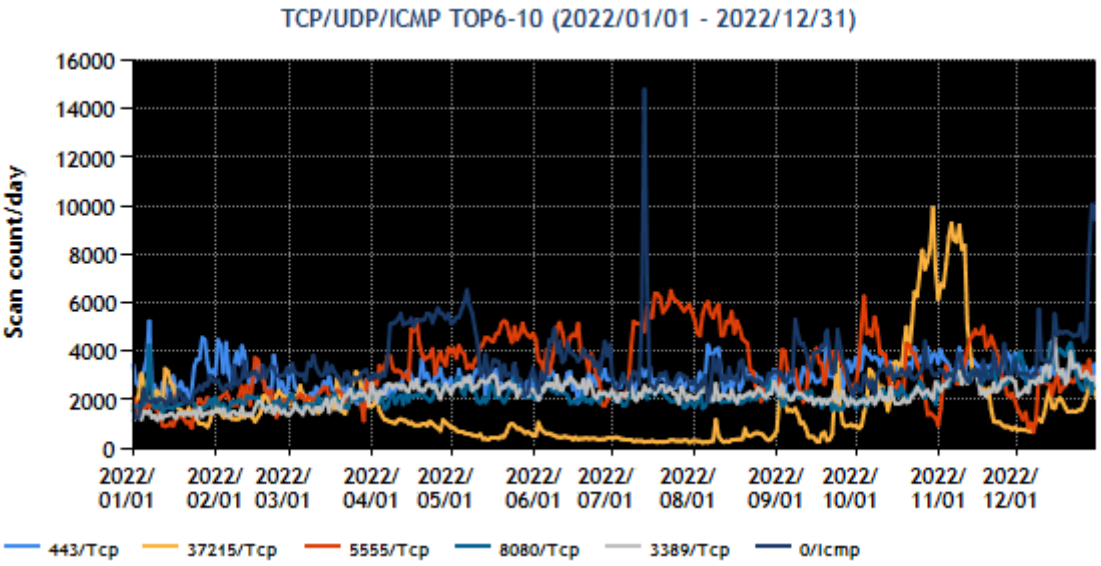


［図 1-3：宛先ポート別グラフ トップ 6-10（2022 年 10 月 1 日-12 月 31 日）］

また、過去 1 年間（2022 年 1 月 1 日-12 月 31 日）における、宛先ポート別パケット数の上位 1～5 位および 6～10 位を［図 1-4］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（2022 年 1 月 1 日-12 月 31 日）］



［図 1-5：宛先ポート別グラフ トップ 6-10（2022 年 1 月 1 日-12 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。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. 定点観測網の拡充に向けた運用とその分析

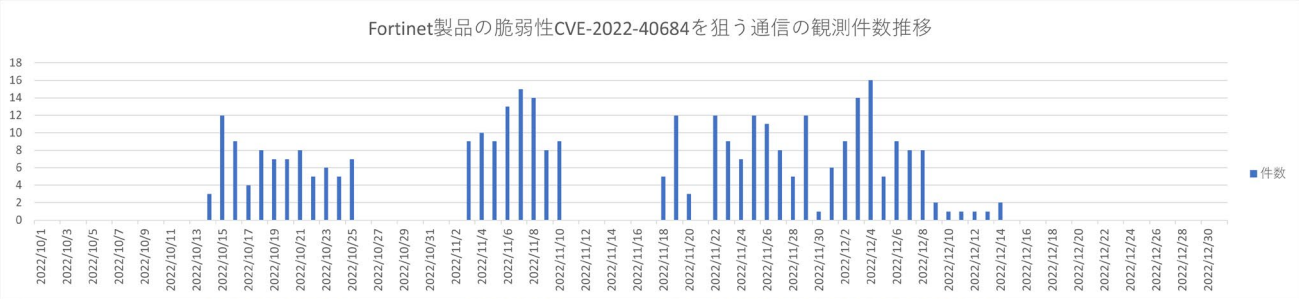
JPCERT/CC では、インターネット上に低対話型ハニーポットを設置して攻撃者から送られてくる種々の通信内容を収集し、攻撃活動を分析しています。現在は、HTTP プロトコルと Redis で用いるプロトコル RESP（REdis Serialization Protocol）に応答する 2 種類のハニーポットを運用しています。

1.3.2.2.1. Fortinet 製品の脆弱性（CVE-2022-40684）を狙う通信の観測

2022 年 10 月 10 日に公表された Fortinet 社製の FortiOS、FortiProxy および FortiSwitchManager における認証バイパスの脆弱性（CVE-2022-40684）を悪用する通信を観測しました。10 月 13 日に実証コードがインターネット上に公開され、その後 1 カ月以上にわたり攻撃パケットが観測されました。
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、同製品の管理インタフェースへアクセスする際の認証情報を変更することができ、結果としてシステム上で任意の操作を行うことができるようになります。

観測した攻撃パケットの多くは、公開された実証コードが生成する HTTP ヘッダー情報や実行コマンドをそのまま使用するものでした。追加される SSH 鍵の多くは文字列“Fake key”であり、応答の有無を確認するためのスキャン活動と推測されますが、一部は実際の攻撃での使用を想定しているであろう SSH 鍵文字列を含むコマンドも観測されました。上記のような“Fake key”を含む通信は、その前後のパターンがインターネット上に公開されているスキャンツールのものと一致しています。このことから、ハニーポットで観測された通信の多くはスキャンツールを用いたものであると考えられます。

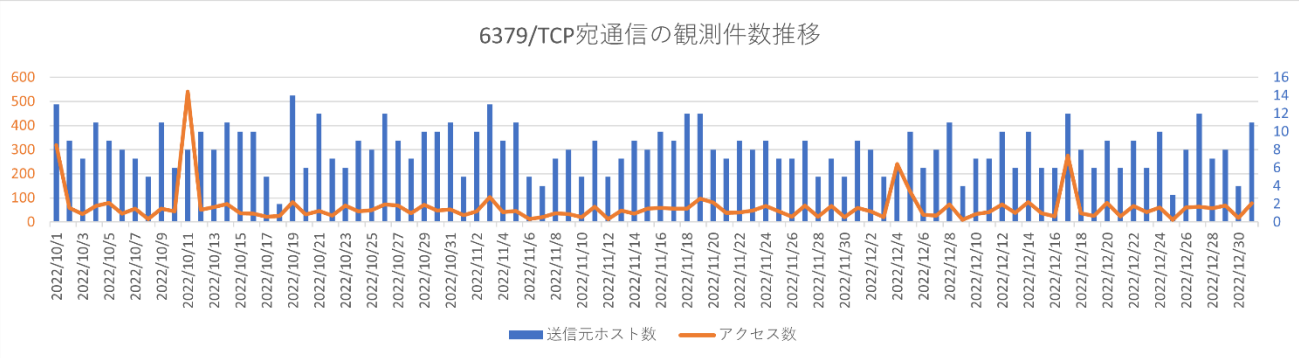
10 月 25 日から 11 月 3 日の間は通信が観測されていません。ただし、他の期間に観測された複数の IP アドレスが、10 月 25 日から 11 月 3 日の間に日本国外のサーバーに対して同じ内容のスキャン活動を行っていることを確認しています。そのため、スキャン活動を行っているボット群は期間ごとに対象国を変えながら稼働しているのではないかと考えられます。また、11 月 11 日から 17 日にかけても通信が確認されていませんが、これは同期間に実施したハニーポットシステムのメンテナンスによるものです。



［図 1-6：Fortinet 製品の脆弱性を狙った通信の観測件数の推移］

1.3.2.2.2. アクセス制限に不備のある Redis サーバーを狙う通信の観測

RESP（6379/TCP）に対するアクセスは、今四半期でも低い水準ながら継続して観測されています。ただし、今四半期においては Censys 等の検索エンジンからのスキャンアクセスが多数を占めており、前四半期で観測されていたような、Redis コマンドを悪用して任意の OS コマンドを実行させようとする、実質的な攻撃活動は減少しています。このような攻撃活動は、パスワードが設定されていない、もしくは弱いパスワードが設定された Redis を無差別に狙うボットによるものであると考えられます。Redis を運用する際は、適切なアクセス制御や認証設定について注意が必要です。



［図 1-7：RESP（6379/TCP）宛通信の観測件数の推移］

2. 脆弱性関連情報流通促進活動

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

2.1. 脆弱性関連情報の取り扱い状況

2.1.1. 受付機関である独立行政法人情報処理推進機構（IPA）との連携

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

など、IPA と緊密な連携を行っています。
なお、脆弱性関連情報に関する四半期ごとの届け出状況については、次の Web ページをご参照ください。

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

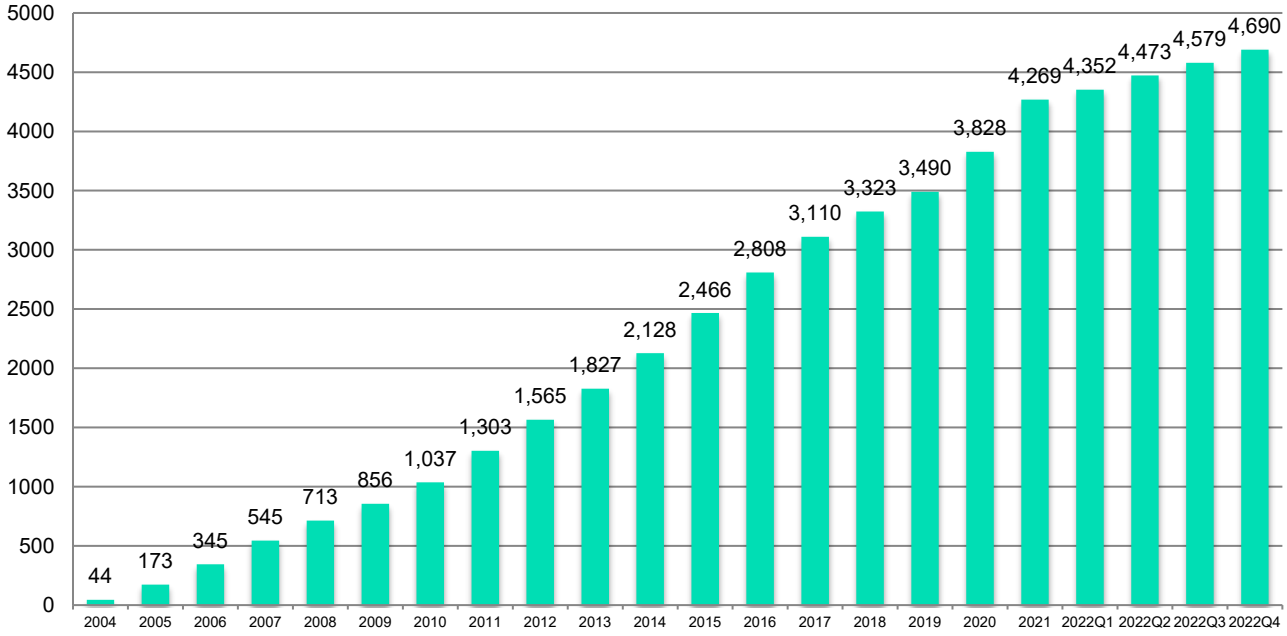
2.1.2. Japan Vulnerability Notes（JVN）において公表した脆弱性情報および対応状況

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

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

本四半期に JVN において公表した脆弱性情報は 111 件（累計 4,690 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/



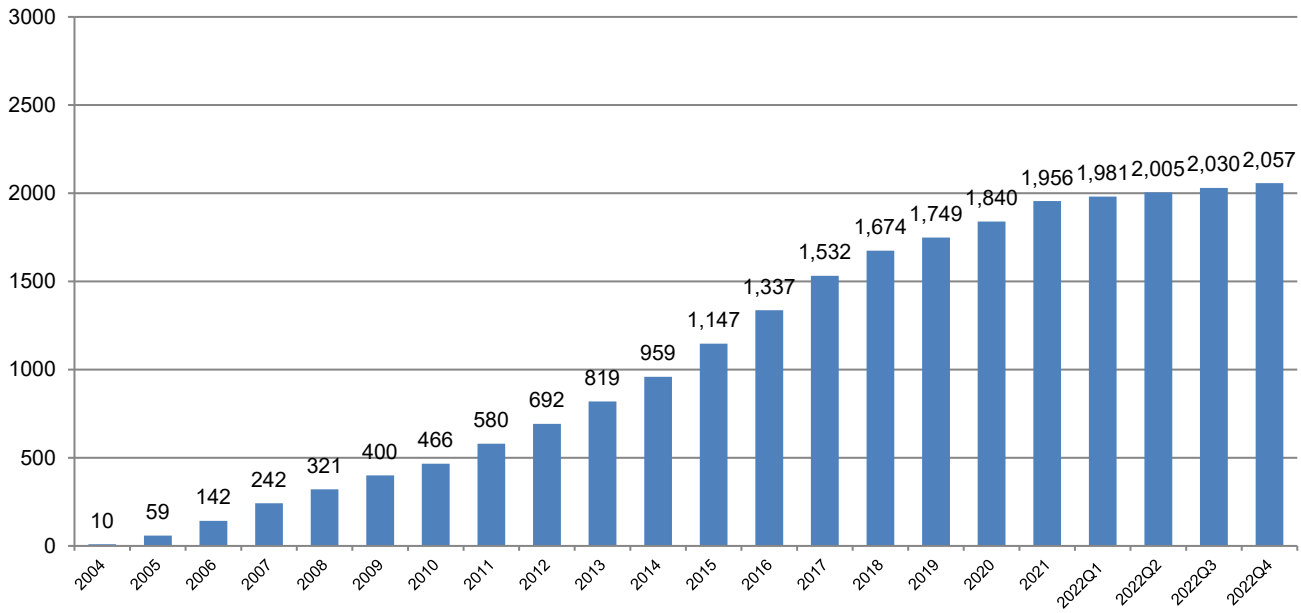
［図 2- 1：JVN 公表累積件数］

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 27 件（累計 2,057 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 27 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 15 件（うち自社製品の届け出によるものが 3 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 10 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 2 件（うち自社製品の届け出によるものが 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、CMS が 7 件と最も多く、次いで組込系製品が 6 件、続いて Windows アプリケーション、スマートフォンアプリケーション、プラグインが 2 件、Android アプリケーション、アプリケーションフレームワーク、組込系、開発支援、グループウェア、マルチプラットフォームアプリケーション、ミドルウェア、ライブラリがそれぞれ 1 件でした。

［表 2-1：公表を行った国内取扱脆弱性情報の件数の製品カテゴリー内訳］

製品分類	件数
CMS	7
組込系製品	6
Windows アプリケーション	2
スマートフォンアプリケーション	2
プラグイン	2
Android 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
組込系	1
開発支援	1
グループウェア	1
マルチプラットフォームアプリケーション	1
ミドルウェア	1
ライブラリ	1



［図 2-2：公表を行った国内取扱脆弱性情報の累積件数］

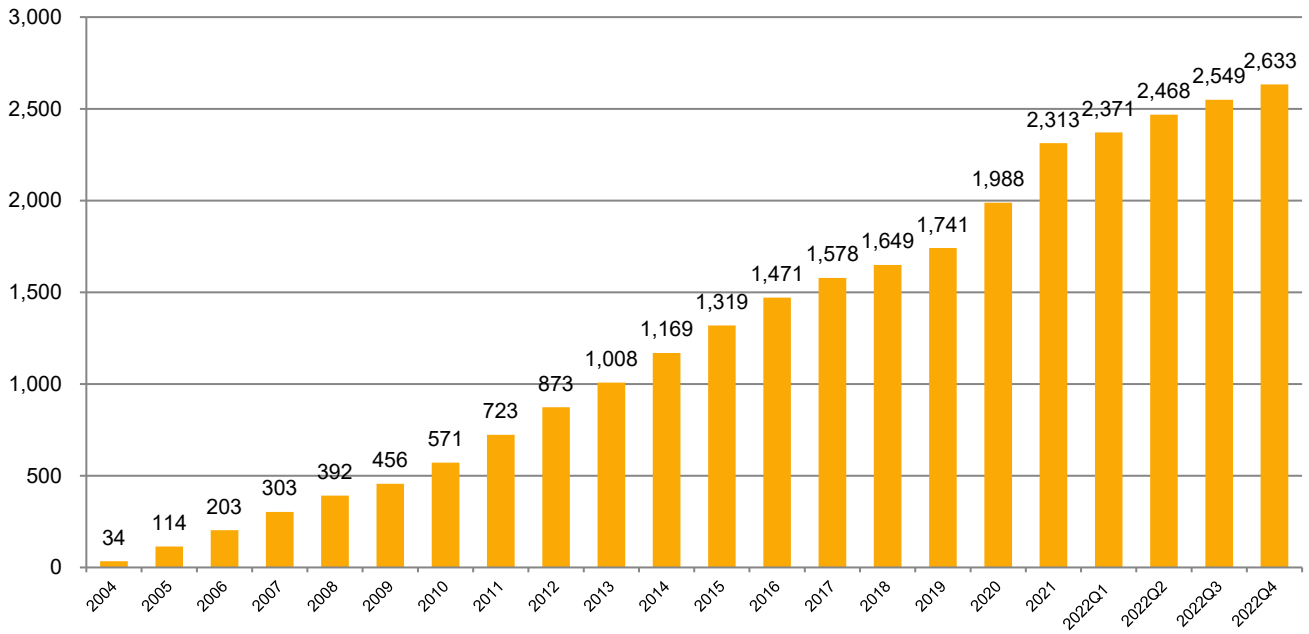
本四半期に公表した国際取扱脆弱性情報は 84 件（累計 2,633 件）で、累計の推移は［図 2-3］に示すとおりです。84 件のアドバイザリのうち、海外調整機関や製品開発者等からの届け出によるものおよび製品開発者による脆弱性情報公開の事前通知によるものは 28 件（うち複数製品開発者の製品に影響を及ぼすものが 8 件、複数の製品開発者向け Technical Alert として公表したものが 1 件）、国内外の発見者からの届け出によるものは 9 件、JPCERT/CC が注意喚起として発行したものは 47 件でした。

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 61 件と最も多く、次いで組込系製品が 9 件、アンチウイルス製品が 4 件、サーバー製品、プロトコルがそれぞれ 3 件、医療機器が 2 件、DNS、ウェブサーブレットコンテナがそれぞれ 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	61
組込系製品	9
アンチウイルス製品	4
サーバー製品	3
プロトコル	3
医療機器	2
DNS	1
ウェブサーブレットコンテナ	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 65 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の 6 社が JPCERT/CC を Root とする CNA として登録されています。
また、本四半期においては、新たな CNA としてキヤノン株式会社が加わり、現在 7 社が CNA として自社製品の脆弱性に対し CVE 番号を付与しています。
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/

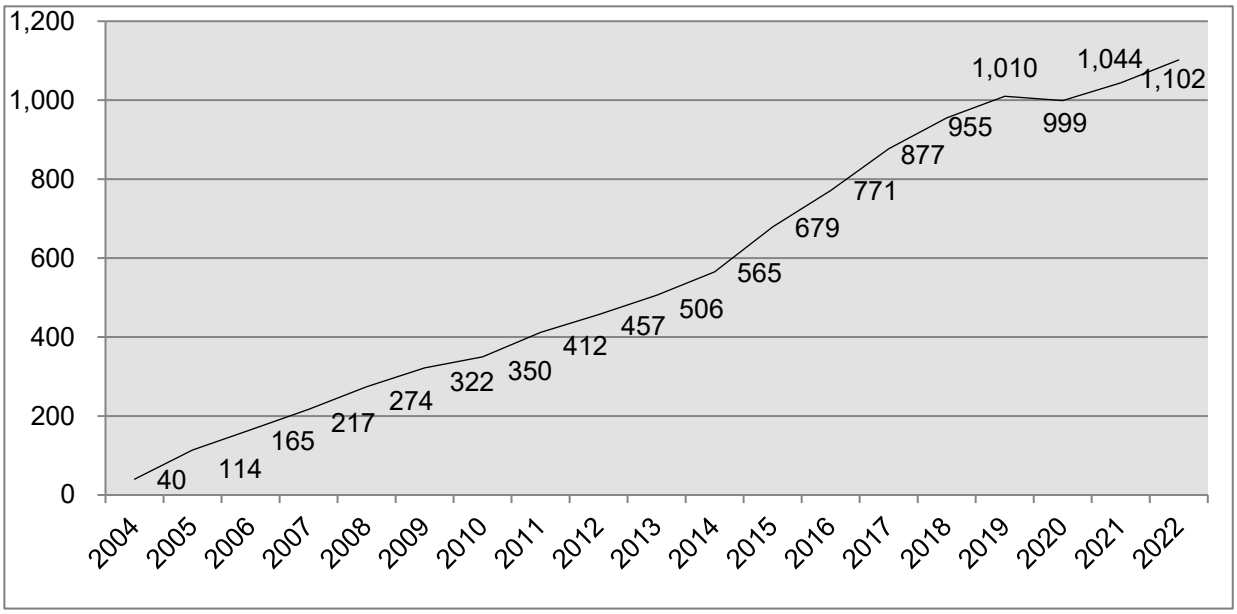
情報セキュリティ早期警戒パートナーシップガイドライン（2019 年版第 2 刷）
https://www.jpcert.or.jp/vh/partnership_guideline2019_r2.pdf

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、2022 年 12 月 31 日現在で 1,102 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

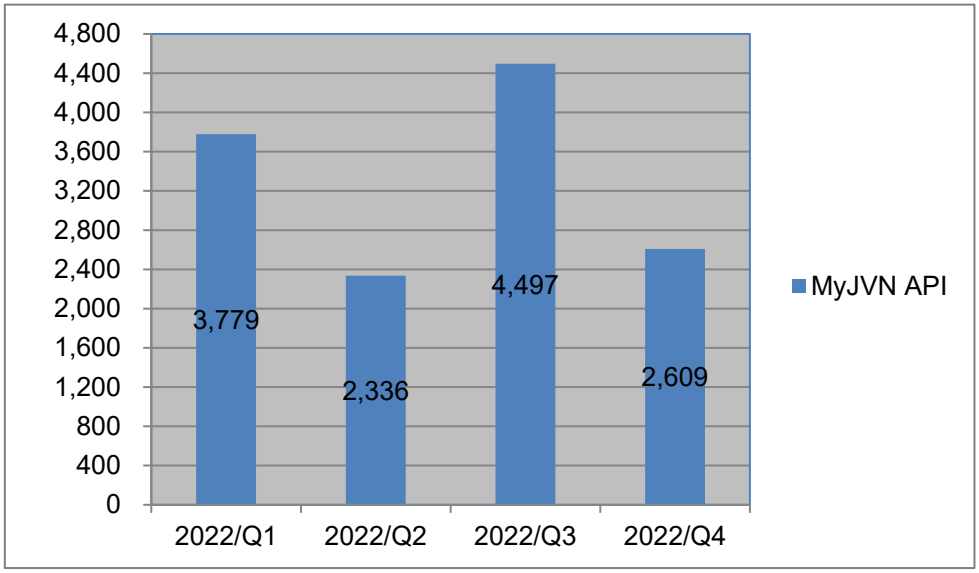
JPCERT/CC では、技術情報やセキュリティ・脆弱性の動向などの情報交換や、脆弱性情報流通業務に関する製品開発者との意見交換、また、製品開発者間の情報交換を目的として、脆弱性情報流通の活動にご協力いただいている製品開発者の皆さまとの定期ミーティングや特定のテーマに関する個別ミーティングを開催しています。
本四半期においては、11 月 21 日に制御・組込系の製品開発者との座談会を開催し、ISO/IEC TR 5895:2022 Cybersecurity — Multi-party coordinated vulnerability disclosure and handling に関する説明と意見交換、および、製品開発者の PSIRT 活動事例紹介と意見交換を行いました。

2.3. VRDA フィードによる脆弱性情報の配信

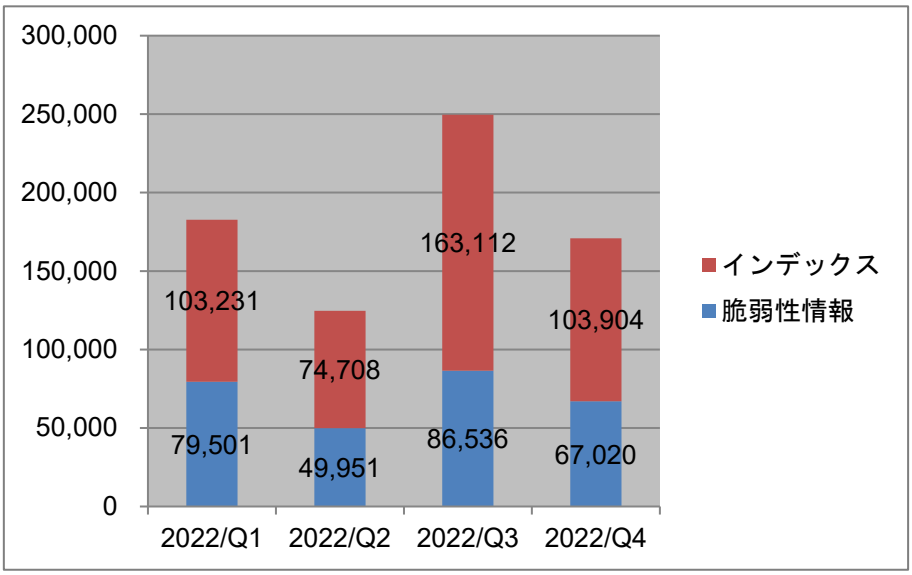
JPCERT/CC は、大規模組織の組織内 CSIRT 等での利用を想定して、ツールを用いた体系的な脆弱性対応を可能とするため、IPA が運用する MyJVN API を外部データソースとして利用した、VRDA（Vulnerability Response Decision Assistance）フィードによる脆弱性情報の配信を行っています。
VRDA フィードについての詳しい情報は、次の Web ページをご参照ください。

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

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

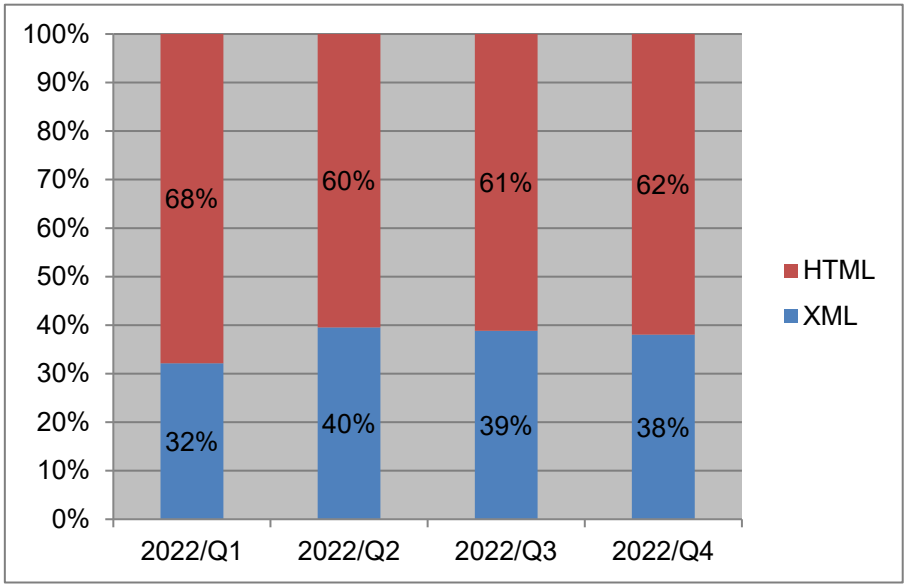


［図 2- 5：VRDA フィード配信件数］



［図 2- 6：VRDA フィード利用件数］

インデックスの利用数については、［図 2- 6］に示したように、前四半期と比較し、約 36%減少しました。脆弱性情報の利用数については、約 23%減少しました。



［図 2- 7：脆弱性情報のデータ形式別利用割合］

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

3. 制御システムに関するセキュリティ対策活動

3.1. 情報収集分析

JPCERT/CC では、制御システムにおけるセキュリティに関わるインシデント事例や標準化活動の動向、その他セキュリティ技術動向に関するニュースや情報などを収集・分析し、必要に応じて国内組織等に情報提供を行っています。本四半期に収集・分析した情報は 58 件でした。

3.1.1. 情報提供

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

本四半期に提供した参考情報は 2 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分かるよう同期間に収集され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

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

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

2022-11-08　JPCERT/CC ICS Security Notes FY2022_#Q2

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 1,300 名に登録していただいています。参加資格や申し込み方法については、次の Web ページをご参照ください。

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

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

3.1.1.1. 注意喚起

本四半期に発行した注意喚起は 0 件でした。

3.1.1.2. その他、特段の対策を呼びかけた脆弱性情報

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

3.2. 制御システム関連のインシデント対応

JPCERT/CC は、制御システム関連のインシデント対応の活動として、インシデント報告の受付を行っています。本四半期における制御システムに関連するインシデントの報告件数は 3 件（20 IP アドレス）でした。報告内容は、3 件ともインターネットからアクセス可能な制御システムに関するもので、そのうち 1 件について、報告にもとづいて調査および調整を行いました。報告者にその結果をお伝えし、本件についての調整を完了しました。残りの 2 件については調整対応中です。

3.3. 関連団体との連携

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

3.4. 制御システム向けセキュリティ自己評価ツールの提供

JPCERT/CC では、制御システムの構築と運用に関するセキュリティ上の問題項目を抽出し、バランスの良いセキュリティ対策を行っていただくことを目的として、簡便なセキュリティ自己評価ツールである日本版 SSAT（SCADA Self Assessment Tool：申し込み制）や J-CLICS（制御システムセキュリティ自己評価ツール：フリーダウンロード）を提供しています。本四半期は、日本版 SSAT に関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. 連載「標準から学ぶ ICS セキュリティ」2 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。

その 2 回目の連載記事として「ゾーンとコンジット」を 2022 年 10 月 27 日に公表し、IEC62443 シリーズで定義される ICS ネットワークのセキュリティ設計のための基本概念である「ゾーン（zone）」と「コンジット（conduit）」について紹介しました。

標準から学ぶ ICS セキュリティ#2：ゾーンとコンジット
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、10 月 12 日に電話会議を行い、今後の APCERT の運営方針等について議論しました。JPCERT/CC は Steering Committee メンバーとして会議に参加すると同時に、事務局として会議運営をサポートしました。

4.2.1.2. APCERT 年次総会 2022 への参加

APCERT の年次総会およびカンファレンスが 10 月 18 日と 19 日に、昨年に引き続きオンラインで開催されました。年次総会には APCERT の主要メンバーであるオペレーショナルメンバー（33 チーム）のうち JPCERT/CC を含む 23 チームが参加しました。
Steering Committee メンバーのうち任期が満了する 4 チームの改選選挙が行われ、ACSC（オーストラリア）、CNCERT/CC（中国）、KrCERT/CC（韓国）、TWNCERT（台湾）がいずれも再選されました。
また、議長チームおよび副議長チームの改選が行われ、CyberSecurity Malaysia（マレーシア）が議長チームに、CNCERT/CC が副議長チームにそれぞれ再選されました。JPCERT/CC も引き続き APCERT の事務局および Steering Committee メンバーとしてさまざまな活動をリードしてまいります。

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. 2022 FIRST Virtual Symposium: Asia Pacific Regions への参加

10 月 20 日と 21 日に、2022 FIRST Virtual Symposium: Asia Pacific Regions が開催されました。これは FIRST が主催するアジア太平洋地域向けのシンポジウムで、前節で報告した APCERT 年次総会およびカンファレンスと連続する日程で行われました。JPCERT/CC やアジア太平洋地域の 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。

2022 FIRST Virtual Symposium: Asia Pacific Regions
https://www.first.org/events/symposium/asia-pacific-regions2022/

4.3. その他国際会議への参加

4.3.1. インド太平洋地域向け日米 EU 産業制御システムサイバーセキュリティウィークでの講演（10 月 26 日）

10 月 24 日から 28 日にかけて、経済産業省および IPA の産業サイバーセキュリティセンターが米国・EU 政府と連携し、インド太平洋地域向け日米 EU 産業制御システムサイバーセキュリティウィークを実施しました。これは、インド太平洋地域の重要インフラ事業者や CSIRT のサイバーセキュリティ担当者などを対象にして行われました。JPCERT/CC は 26 日に行われたランサムウェアに関するセミナーに登壇し、インシデント対応の現状などについて講演を行いました。

経済産業省ニュースリリース
「インド太平洋地域向け日米 EU 産業制御システムサイバーセキュリティウィーク」を実施しました
https://www.meti.go.jp/press/2022/10/20221031001/20221031001.html

4.3.2. ASEAN CERTs Incident Drill (ACID)参加（10 月 27 日）

ACID（ASEAN CERTs Incident Drill）は、シンガポールの CSA（Cyber Security Agency）が主導して、ASEAN（東南アジア諸国連合）各国の CSIRT が合同で毎年実施してきたサイバーインシデント演習です。本演習は、国境を越えて発生するサイバーセキュリティインシデントに備え、ASEAN 加盟国および周辺各国の CSIRT 間の連携を強化することを目的にしています。17 回目になる今年は 10 月 27 日に実施され、これに JPCERT/CC も参加しました。今年の演習は「脆弱性の悪用に起因したサイバー攻撃への対処」をテーマに行われました。

4.3.3. Internet Governance Forum (IGF)への参加（11 月 28 日～12 月 2 日）

11 月 28 日から 12 月 2 日にかけて、IGF 2022 がエチオピアのアディスアベバで現地開催ならびにオンライン配信のハイブリッド形式で行われました。参加登録者数は 3700 人を超えました。この中で、JPCERT/CC は 12 月 1 日に行われた Toward a Resilient Internet: Cyber Diplomacy 2.0 と題したパネルセッションに登壇し、日本およびアジア諸国のサイバー外交の現状や、アクティブサイバー防衛などに関して議論を行いました。また、インターネットガバナンスに関する多数のセッションを聴講し、他の専門家との意見交換を行いました。
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。

Internet Governance Forum
https://www.intgovforum.org/en/content/igf-2022

4.3.4. 38th TWNIC Open Policy Meeting での登壇（12 月 1 日）

台湾の IP アドレスの管理などを行う TWNIC（Taiwan Network Information Center）が主催する TWNIC Open Policy Meeting が 12 月 1 日に台北市で開催され、オンラインでも同時配信されました。JPCERT/CC はサイバー規範に関するパネルに登壇し、国連などでのサイバー規範に関する議論や、それらが CERT コミュニティーに与えた影響などについて発言しました。
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。

38th TWNIC Open Policy Meeting
https://opm.twnic.tw/38th/

4.4. 海外 CSIRT 等の来訪および往訪

4.4.1. 米国 CISA の来訪（10 月 25 日）

アメリカの CISA（Cybersecurity and Infrastructure Security Agency）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。

4.4.2. シンガポール CSA の来訪（11 月 29 日）

シンガポールの CSA（Cyber Security Agency）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。

4.4.3. ルワンダ Rw-CSIRT の訪問（12 月 6 日）

ルワンダの Rw-CSIRT を訪問し、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。

4.4.4. エチオピア Ethio CERT の訪問（12 月 9 日）

エチオピアの Ethio CERT 訪問し、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。

4.5. 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。

WG3 関連では、前四半期から引き続き、新たな標準化作業の提案に向けた検討を行いました。そのほか 10 月に行われた国際会議に参加し、パッチマネージメントの技術仕様書作成に関する個別会議にてコメントの処理作業を行いました。
WG4 で作業中の「インシデント管理に関する標準」については、既存標準文書の複数パートの改訂および新しいパートの文書の作成が行われています。本四半期は、現在 FDIS（Final Draft International Standard）ステージにあるパート 1（原理とプロセス）とパート 2（インシデント対応のための計画と準備）の改訂文書に対する日本からの回答処理作業への協力を行いました。また新しく作成中のパート 4（コーディネーション）は 10 月の国際会議で DIS（Draft International Standard）に進むことが決まりました。

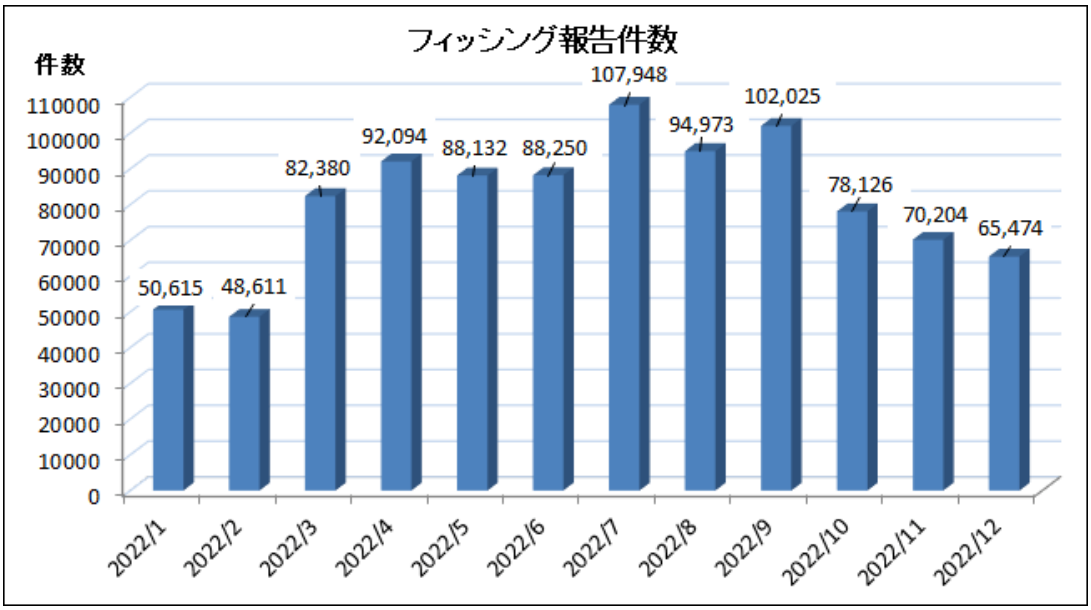
5. フィッシング対策協議会事務局の運営

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、前四半期と比較すると減少したものの、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 かたるフィッシングの報告数が多く、全体の約 35.5%を占めています。ついで、「えきねっと」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 15 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。

- 金融庁をかたるフィッシング　：1 件
- MyJCB をかたるフィッシング　：1 件
- 警察庁を装うフィッシング　：1 件
- 新生銀行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
- ソニー銀行をかたるフィッシング　：1 件
- ゆうちょ銀行をかたるフィッシング　：1 件
- 楽天市場および楽天カード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
- ETC 利用照会サービスをかたるフィッシング　：1 件
- BIGLOBE をかたるフィッシング　：1 件
- OCN 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
- オリコをかたるフィッシング　：1 件
- ビューカード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。これは、それまで報告の多かったドメインとサブドメインを組みあわせたパターンの誘導先 URL を使用したフィッシングメールを大量配信していたケースが減少した結果と考えられます。

報告件数割合の多かった Amazon や「えきねっと」をかたるフィッシングについては、大きなセールの前後や全国旅行支援が開始されたタイミングで増加していました。

ETC 利用照会サービスをかたるフィッシングが長く継続していますが、本四半期には誘導に QR コードを使用したものが発生しました。これは迷惑メールフィルターを回避する試みの一つと考えられます。（[図 5-2]）QR コードを使用した誘導は、2019 年頃にも確認していますが、いずれも短期間で終わっており、今回も犯罪者が試行の一環として行ったと考えられます。

また、ISP（OCN、So-net、BIGLOBE）をかたるフィッシングが久しぶりに行われたり、警察庁や金融庁をかたるフィッシングが発生したりしたため、注意喚起のため緊急情報を公開しました（[図 5-3]）。

［図 5-2：ETC 利用照会サービスをかたるフィッシングメールの例 ］

https://www.antiphishing.jp/news/alert/etcQR_20221115.html

［図 5-3：金融庁をかたるフィッシングサイトの例 ］

https://www.antiphishing.jp/news/alert/fsa_20221004.html

5.2.1. 定期報告

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

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

2022 年 10 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/202210.html

2022 年 11 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/202211.html

2022 年 12 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/202212.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。

また、電子メールで行っていた提供を事前に連絡した上で 10 月 31 日（月）に停止し、その後は WebAPI による提供のみとしました。

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 3 回）
  日時：2022 年 10 月 21 日（金）10:00-12:00

- 技術・制度検討ワーキンググループ会合（第 4 回）
  日時：2022 年 11 月 25 日 13:00-15:00

6. フィッシング対策協議会の会員組織向け活動

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

6.1. 運営委員会開催

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

- 第 102 回運営委員会（オンライン）
  2022 年 10 月 20 日（木）16:00 - 18:00

- 第 103 回運営委員会（株式会社日本レジストリサービス + オンライン）
  2022 年 11 月 17 日（木）16:00 - 18:00

- 第 104 回運営委員会（株式会社リクルート + オンライン）
  2022 年 12 月 15 日（木）16:00 - 18:00

6.2. ワーキンググループ会合等 開催支援

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

- 学術研究ワーキンググループ会合
  日時：10 月- 12 月　毎週火曜日 9：00 - 9：30

- 証明書普及促進ワーキンググループ会合
  日時：12 月 20 日（火）　16：00 - 18：00

- フィッシング対策セミナー2022（オンライン）
  日時：11 月 4 日（金）10：00 - 16：10

※ワーキンググループ会合等はすべてオンライン開催

7. 公開資料

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

7.1. インシデント報告対応レポート

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

2022-10-20
JPCERT/CC インシデント報告対応レポート［2022 年 7 月 1 日～2022 年 9 月 30 日］
https://www.jpcert.or.jp/pr/2022/PR_Report2022Q2.pdf

2022-12-09
JPCERT/CC Incident Handling Report [July 1, 2022 - September 30, 2022]
https://www.jpcert.or.jp/english/doc/IR_Report2022Q2_en.pdf

7.2. インターネット定点観測レポート

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

2022-10-26
JPCERT/CC インターネット定点観測レポート［2022 年 7 月 1 日～2022 年 9 月 30 日］
https://www.jpcert.or.jp/tsubame/report/report202207-09.html
https://www.jpcert.or.jp/tsubame/report/TSUBAME_Report2022Q2.pdf

2022-12-09
JPCERT/CC Internet Threat Monitoring Report [July 1, 2022 - September 30, 2022]
https://www.jpcert.or.jp/english/doc/TSUBAMEReport2022Q2_en.pdf

7.3. 脆弱性関連情報に関する活動報告

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

2022-10-20
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 3 四半期（7 月～9 月）］
https://www.jpcert.or.jp/pr/2022/vulnREPORT_2022q3.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 6 件の記事を公表しました。

日本語版発行件数：3 件　https://blogs.jpcert.or.jp/ja/

2022-10-26　TSUBAME レポート Overflow（2022 年 7～9 月）
2022-12-21　LogonTracer v1.6 リリース
2022-12-26　世界の CSIRT から ～エチオピア、ルワンダ～

英語版発行件数：3 件 https://blogs.jpcert.or.jp/en/

2022-10-05　TSUBAME Report Overflow (Apr-Jun 2022)
2022-12-09　TSUBAME Report Overflow (Jul-Sep 2022)
2022-12-21　LogonTracer v1.6 Released

8.　主な講演活動

(1) 宮地 利雄（技術顧問）：
「工場操業の安全と高度化におけるサイバーセキュリティの重要性」
富山県高圧ガス取扱事業者 講習会（主催：富山県、共催：富山県高圧ガス安全協会、講演日：2022 年 10 月 25 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）：
パネルディスカッション「グローバル IT 社会の深化、つながる世界の危機」
リスクシナリオ～リスクが新たな事業機会に～（主催：日経 BP 総合研究所、講演日：2022 年 11 月 25 日）

(3) 宮地 利雄（技術顧問）：
「制御システムに対するサイバー攻撃の動向」
アフターコロナ時代のプラント運転の安全と高度化を考える講演会（主催：計測自動制御学会、講演日：2022 年 12 月 15 日）

(4) 小宮山 功一朗（国際部 部長）：
「サイバー空間の地政学 ～新しい地図を求めて～」
NCA Annual Conference 2022（主催：一般社団法人日本コンピュータセキュリティインシデント対応チーム協議会、講演日：2022 年 12 月 16 日）

(5) 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）：
「サイバー攻撃に対する初動対応のポイント～研究者／研究機関を狙う攻撃のケーススタディから～」
情報システム管理者研修（主催：理化学研究所、講演日：2022 年 12 月 19 日）

9. 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) Security Days Fall 2022
主　催：株式会社ナノオプト・メディア
開催日：東京　2022 年 10 月 4 日～7 日、大阪　2022 年 10 月 13 日

(2) 情報セキュリティワークショップ in 越後湯沢 2022
主　催：特定非営利活動法人新潟情報セキュリティ協会
情報セキュリティ ワークショップ in 越後湯沢 実行委員会
開催日：2022 年 10 月 7 日、8 日

(3) Internet Week 2022
主　催：一般社団法人日本ネットワークインフォメーションセンター
開催日：2022 年 11 月 21 日～30 日

(4) 第 19 回デジタル・フォレンジック・コミュニティ 2020 in TOKYO
主　催：特定非営利活動法人デジタル・フォレンジック研究会コミュニティ 2022 実行委員会
開催日：2022 年 12 月 5 日、6 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