JPCERT/CC 活動四半期レポート

2022 年 1 月 1 日 ～ 2022 年 3 月 31 日

一般社団法人 JPCERT コーディネーションセンター

2022 年 4 月 14 日

活動概要トピックス

ートピック1ー　半期刊の「ICS 脆弱性分析レポート」の公表開始

これまで、多くの制御システムユーザー組織のセキュリティ担当者から、制御システム関連製品の脆弱性への対応に苦慮しているという悩みを伺ってきました。脆弱性アドバイザリの内容を確認しても、脆弱性の意味やそれを悪用された場合に自分の担当している制御システムが受ける影響の全体像が良く分からないとのことです。こうした悩みを初心者が持つ背景として、アドバイザリが読者に一定レベルの前提知識を求めていて、この知識のギャップが障害になっていることが考えられます。脆弱性アドバイザリを的確に理解するために必要な知識を身に付けていただくため、直近の半期間に公表された ICS 関連の脆弱性アドバイザリの中から、類似した脆弱性がしばしば見られる、あるいは非常に重要な脆弱性に関するものであって、初心者にとって理解が難しいと思われる内容を含むものを選び、その内容や制御システム全体への影響などを詳細に解説した「ICS 脆弱性分析レポート」を半期ごとに発行することとし、その初回号を 2022 年 3 月 28 日に公表しました。初回号では、「JVNVU#92650134：Delta Electronics 製 DOPSoft に境界外読み取りの脆弱性」を例に、対策なしで公表された制御システム関連製品のファイル読み込みに関する脆弱性が制御システムに与えるリスクを論じました。この脆弱性を悪用した攻撃の成立条件、攻撃が行われた際に制御システム全体に与える影響、想定される攻撃シナリオを示し、それらにもとづいて制御システムユーザー組織で実施可能と思われる対策を提示していて、制御システム関連製品のファイル読み込みに関する脆弱性についての理解が深まるように工夫がなされています。

今後も読者からのフィードバックを得ながら本シリーズの改善を図り、制御システム関連製品の脆弱性への対応の促進と関係者の啓発に取り組んでいきます。

ICS 脆弱性分析レポート ― 2021 年度上期 ―
https://www.jpcert.or.jp/ics/ics-vuls-analysis-report.html

JPCERT/CC Eyes：ICS 脆弱性分析レポート ― 2021 年度上期 ―を公表
https://blogs.jpcert.or.jp/ja/2022/03/ics-vuls-analysis-report-2021H1.html

ートピック2ー　JSAC2022（Japan Security Analyst Conference 2022）を開催

2022 年 1 月 27 日～28 日に JSAC2022 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。5 回めの開催となる今回は、当初ハイブリット開催の予定でしたが、開催直前に東京都が「まん延防止等重点措置」の適用地域となったことを踏まえて、2 年連続してのオンライン形式のみでの開催となりました。
今回は、初の 2 日間開催でした。1 日めは Conference Day として、マルウェア分析やデジタルフォレン

ジック手法、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、分析ツールなどの発表が行われました。2 日めは Workshop Day として、2 件のワークショップを実施しました。JSAC2022 の講演資料を JSAC2022 の Web サイト上で、講演動画を YouTube 上で公開しています。また、カンファレンスの概要は JPCERT/CC Eyes でも紹介しています。
JSAC2022 終了後に、参加者によるアンケート結果を踏まえたプログラム選考委員による評議で最も評価の高かった次の講演者にベストスピーカー賞を贈呈しました。

タイトル: An Introduction to macOS Forensics with Open Source Software
講演者: 株式会社インターネットイニシアティブ 小林 稔

JPCERT/CC では今後も引き続きインシデント分析・対応を行う技術者に有益な情報発信や活動を実施してまいります。

JSAC 2022
https://jsac.jpcert.or.jp/

JSAC2022 開催レポート～DAY1～
https://blogs.jpcert.or.jp/ja/2022/02/jsac2022report1.html

JSAC2022 開催レポート～DAY2～
https://blogs.jpcert.or.jp/ja/2022/03/jsac2022report2.html

JPCERT/CC YouTube 公式チャンネル
https://www.youtube.com/watch?v=sOeQuN6OBKI&list=PLgEi6O-lWUIZxmHw0QGeAuIhUIuJZ11El

ートピック3ー　制御システムセキュリティカンファレンス 2022 を開催

2022 年 2 月 3 日（木）に「制御システムセキュリティカンファレンス 2022」をオンラインで開催し、440 名の方々にご参加いただきました。共催者である経済産業省のサイバーセキュリティ・情報化審議官江口純一氏から開会のご挨拶をいただき、その後、募集（CFP）に応じた 3 件を含む計 6 件の講演が行われました。各講演では、制御システムセキュリティの一年間の動向の振り返りや、生産システムにおけるセーフティおよびセキュリティ上のリスクと低減の取り組み、有事に備えた復旧計画の策定における制御システムの特徴に留意することの重要性と対策のポイント、ローカル 5G 導入時に実装しておくべきセキュリティ対策に関する製鉄所を模した実証環境での検討、自組織にフィットした制御システムセキュリティガイドライン策定上の課題と進め方、制御システム製品の脆弱性情報を収集し制御システムユーザー組織向けに発信している JPCERT/CC の取り組み、などが論じられました。開催後のアンケート結果によると参加者の内訳は、制御システムユーザーが 39.8%、制御システムベンダーが 9.5%、制御機器ベンダーが 10.2%、制御システムエンジニアリングが 9.5%、研究者が 7.2%でした。昨年に比べて制

御システムユーザーの占める割合がさらに増えており、制御システムユーザー組織におけるセキュリティへの関心がより高まっているようです。また参加者が全国各地にわたり、約 100 名近くが初参加でした。前回同様、オンライン開催により参加者の多様化が促進されたことが伺えました。

制御システムセキュリティカンファレンス 2022
https://www.jpcert.or.jp/event/ics-conference2022.html

制御システムセキュリティカンファレンス 2022 講演資料
https://www.jpcert.or.jp/present/#year2022

制御システムセキュリティカンファレンス 2022 開催レポート
https://blogs.jpcert.or.jp/ja/2022/03/ics-conference2022.html

目次

本活動は、経済産業省より委託を受け、「令和３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」）に関する報告は、報告件数ベースで 16,188 件、インシデント件数ベースでは 9,369 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 5,558 件でした。前四半期の 6,554 件と比較して 15%減少しています。「調整」とは、フィッシングサイトが設置されているサイトや、改ざんにより JavaScript が埋め込まれているサイト、ウイルス等のマルウェアが設置されたサイト、「scan」のアクセス元等の管理者等に対し、状況の調査や問題解決のための対応を依頼する活動です。

JPCERT/CC は、インターネット利用組織におけるインシデントの認知と対処、インシデントによる被害拡大の抑止に貢献することを目的として活動しています。国際的な調整・支援が必要となるインシデントについては、日本における窓口組織として、国内や国外（海外の CSIRT 等）の関係機関との調整活動を行っています。

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

JPCERT/CC インシデント報告対応レポート
https://www.jpcert.or.jp/pr/2022/IR_Report2021Q4.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 6,820 件で、前四半期の 7,125 件から 4%減少しました。また、前年度同期（4,831 件）との比較では、41%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	1 月	2 月	3 月	本四半期合計（割合）
国内ブランド	1,427	1,022	1,747	4,196（62%）
国外ブランド	721	771	551	2,043（30%）
ブランド不明 (注 5)	193	163	225	581 （9%）
全ブランド合計	2,341	1,956	2,523	6,820

（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。

国内ブランドのフィッシングサイトでは、携帯キャリアのユーザーを狙ったフィッシングサイトが多くを占めました。また、前四半期に引き続き ETC の利用照会サービスや EC サイトの会員用ログインページを装ったフィッシングサイトも多く確認されました。
その他、JR 東日本が提供する Web サイト「えきねっと」を装ったフィッシングサイトの報告が 3 月に入ってから増加しました。

国外ブランドのフィッシングサイトについては、通販サイトのログインページを装ったものが半数以上占めており、ブランドや報告数は前四半期と大きな変化がありませんでした。

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 62%、国外が 30%であり、前四半期（国内が 23%、国外が 77%）と比較し国内が増加しました。

1.1.1.2. Web サイト改ざん

本四半期に報告が寄せられた Web サイト改ざんの件数は、703 件でした。前四半期の 906 件から 22%減少しています。

本四半期も、改ざんされた Web サイトから、不審な Web サイトへ転送される事例が複数報告されました。また、VirtualHost を使って複数の Web サイトが管理されているホスト上で、複数の Web サイトが同時に改ざんされる事象を確認しました。この改ざんは、1 つの Web サイトを改ざんしてから、次の手順で他の Web サイトにも改ざんを拡大する方法でなされた可能性があります。

改ざんの手順

1. CMS 等の脆弱性を利用し、最初の Web サイト改ざんを行い、WebShell を設置
2. WebShell を用いて、権限昇格を行うツールを設置した後にそれを起動して root 権限に昇格
3. root 権限で、同じホスト上にある複数の Web サイトを改ざん

同じホスト上に複数の Web サイトが存在している場合、1 つの Web サイト上のコンテンツに脆弱性が存在すると、同じホスト上にある別の Web サイトに対しても改ざんが行われる可能性があります。

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、2 件でした。
次に、確認されたインシデントを紹介します。

(1) JavaScript をダウンロードさせるショートカットファイルを用いた攻撃
本四半期は、金融機関の社員を狙った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、標的の金融機関の社員に対して、乗っ取った暗号資産交換業者の社員の LinkedIn アカウントから、不正な ZIP ファイルを送信し、マルウェアを感染させようとするものでした。ZIP ファイルには不正な JavaScript をダウンロードして、実行するショートカットファイルが格納されていました。本攻撃は、弊センターのブログで公開した次の攻撃キャンペーンと類似しており、依然として攻撃活動が継続して行われていることがうかがえます。

JPCERT/CC Eyes「短縮 URL から VBScript をダウンロードさせるショートカットファイルを用いた攻撃」
https://blogs.jpcert.or.jp/ja/2019/07/shorten_url_lnk.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 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：15 件（うち更新情報が 7 件）　https://www.jpcert.or.jp/at/

2022-01-04　Apache Log4j の任意のコード実行の脆弱性（CVE-2021-44228）に関する注意喚起 (更新)
2022-01-12　2022 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 (公開)
2022-01-12　Adobe Acrobat および Reader の脆弱性（APSB22-01）に関する注意喚起 (公開)
2022-01-19　2022 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 (公開)
2022-01-25　SonicWall SMA100 シリーズの複数の脆弱性に関する注意喚起 (公開)
2022-02-09　2022 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 (公開)
2022-02-10　マルウェア Emotet の感染再拡大に関する注意喚起 (公開)
2022-02-15　マルウェア Emotet の感染再拡大に関する注意喚起 (更新)
2022-02-17　マルウェア Emotet の感染再拡大に関する注意喚起 (更新)
2022-03-03　マルウェア Emotet の感染再拡大に関する注意喚起 (更新)
2022-03-07　マルウェア Emotet の感染再拡大に関する注意喚起 (更新)
2022-03-08　マルウェア Emotet の感染再拡大に関する注意喚起 (更新)
2022-03-09　2022 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 (公開)
2022-03-14　マルウェア Emotet の感染再拡大に関する注意喚起 (更新)
2022-03-29　Trend Micro Apex Central 製品の脆弱性（CVE-2022-26871）に関する注意喚起 (公開)

1.2.1.2. Weekly Report

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

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

Weekly Report で扱った情報セキュリティ関連情報の項目数は、合計 100 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。

2022-01-06　JPCERT/CC が「モバイル端末を狙うマルウェアへの対応 FAQ」などを公開
2022-01-13　JASA が「2022 年 情報セキュリティ十大トレンド」を公開
2022-01-19　JPCERT/CC が「侵入型ランサムウェア攻撃を受けたら読む FAQ」を公開
2022-01-26　フィッシング対策協議会が「第４回フィッシング対策勉強会」の参加申し込み受付けを開始
2022-02-02　NISC が「東京 2020 大会におけるサイバーセキュリティ対策結果報告（総括）」を公開
2022-02-09　NISC がサイバーセキュリティ戦略（令和 3 年 9 月 28 日閣議決定）のカラーパンフレットを掲載
2022-02-16　JPCERT/CC が「マルウェア Emotet の感染再拡大に関する注意喚起」を公開
2022-02-24　JPCERT/CC が「マルウェア Emotet の感染再拡大に関する注意喚起」を更新
2022-03-02　経済産業省が「昨今の情勢を踏まえたサイバーセキュリティ対策の強化について（注意喚起）」を公開
2022-03-09　JPCERT/CC が「マルウェア Emotet の感染再拡大に関する注意喚起」を再び更新
2022-03-16　JPCERT/CC が「制御システムセキュリティカンファレンス 2022」「JSAC2022」の開催レポートを公開
2022-03-24　JPCERT/CC が「サイバー政策動向を知ろう Watch! Cyber World vol.2｜ランキング」を公開
2022-03-30　IPA が「情報セキュリティ対策ベンチマーク」Ver.5.1 診断データの統計情報を公開

1.2.1.3. 早期警戒情報

JPCERT/CC は、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 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、対策方法に関する情報を「早期警戒情報」として提供しています。

早期警戒情報の提供について
https://www.jpcert.or.jp/wwinfo/

1.2.1.4. CyberNewsFlash

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

発行件数：13 件（うち更新情報が 4 件）　https://www.jpcert.or.jp/newsflash/

2022-01-05　2021 年 12 月に公表された Log4j の脆弱性について（更新）
2022-01-07　2021 年 12 月に公表された Log4j の脆弱性について（更新）
2022-01-12　複数のアドビ製品のアップデートについて
2022-01-17　Apple 製品のアップデートについて（2022 年 1 月）
2022-01-27　Apple 製品のアップデートについて（2022 年 1 月）（更新）
2022-02-09　Intel 製品に関する複数の脆弱性について
2022-02-09　複数のアドビ製品のアップデートについて
2022-02-14　Apple 製品のアップデートについて（2022 年 2 月）
2022-03-09　Intel 製品に関する複数の脆弱性について
2022-03-09　複数のアドビ製品のアップデートについて
2022-03-15　Apple 製品のアップデートについて（2022 年 3 月）
2022-03-16　Apple 製品のアップデートについて（2022 年 3 月）（更新）
2022-03-17　ISC BIND 9 における複数の脆弱性について（2022 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

2021 年 1 月にマルウェア Emotet が Europol によってテイクダウンされました。しかし、その後 2021 年 11 月後半よりマルウェア Emotet を利用した攻撃活動が再び始まったことが確認されました。JPCERT/CC でも 2021 年 11 月後半以降、Emotet の感染に関して相談を多く受けてきました。

さらに、2022 年 2 月の第一週から Emotet の感染が急速に拡大し、メール送信に悪用される可能性がある、Emotet に感染した.jp ドメインのメールアドレスの総数が、Emotet の感染が大幅に拡大した 2020 年に迫る水準にまで増加しました。このため、2022 年 2 月 10 日に注意喚起を発行し、改めて適切な対策や対処ができているかの確認や点検を推奨して、感染や被害の拡大を防ぐことに努めました。

本注意喚起では、新たに確認している Emotet の特徴と Emotet を利用した攻撃の動向に加え、対策や対応としてすでに公開している Emotet に感染した際の対応を記載した資料へのリンクを掲載しました。

注意喚起公開後、JPCERT/CC に Emotet への感染に関する問い合わせが多数寄せられたことを受け、自組織が Emotet に感染しているか否かを確認する際の参考にしていただくために、2 月 15 日に注意喚起を更新して、Emotet の感染によってメールが送信されるパターンを追記しました。

さらに、2022 年 3 月に入り、メール送信に悪用される可能性のある Emotet に感染した.jp ドメインのメールアドレスの総数が、2020 年の感染ピーク時の約 5 倍以上に急増したことから、

JPCERT/CC が新たに確認した Emotet に感染させるメールのサンプルを加えて、3 月 3 日に注意喚起を改めて更新し、さらなる注意を呼びかけました。

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) Apache Log4j の任意のコード実行の脆弱性（CVE-2021-44228）に関する情報発信

Java ベースのオープンソースのロギングライブラリ Apache Log4j で任意のコードの実行が可能な脆弱性（CVE-2021-44228）に関する情報が 2021 年 12 月 10 日に The Apache Software Foundation（The ASF）から公表されました。本脆弱性が悪用された場合、遠隔の第三者が Apache-Log4j が動くシステム上で任意のコードを実行する可能性があります。

公表されたのと同じ日に本脆弱性を実証するコード（PoC）が公開されていることを JPCERT/CC で確認し、影響を受けるバージョンの範囲などが不確かな状況ではありましたが、Apache Log4j の利用が広い範囲にわたっていることを考慮し、早期の対応を促すために早期警戒情報を公開しました。

その後、本脆弱性の影響バージョンなどの詳細情報が The ASF から公開されました。また、本脆弱性の悪用を試みる通信を JPCERT/CC でも観測したため、広く注意を促すべく 2021 年 12 月 11 日に注意喚起を発行しました。

2021 年 12 月 15 日には、特定の条件下で同ライブラリに影響を及ぼす新たな脆弱性 CVE-2021-45046 が、対策を施した更新版とともに、The ASF から公開されたため、JPCERT/CC も同日に注意喚起を更新しました。

さらに 2021 年 12 月 18 日に The ASF から、CVE-2021-45046 について、一部の環境では任意のコード実行が可能であるとの情報が、翌日 19 日には新たにサービス運用妨害攻撃の脆弱性（CVE-2021-45105）について修正バージョンが公開されたことをうけ、JPCERT/CC も 2 月 20 日に注意喚起の更新を行いました。12 月 28 日には、新たなリモートコード実行の脆弱性（CVE-2021-44832）の対策バージョンが公開されたため、2022 年 1 月 4 日に注意喚起を更新しました。

本ライブラリに関する脆弱性については、対策情報の更新や新たに公開された脆弱性や対応する修正バージョン等、注意喚起の追記が度重なってきたため、Apache Log4j への対応状況を確認してもらいやすくするため、2022 年 1 月 5 日時点での Apache Log4j に関する脆弱性の状況をまとめて整理し、2022 年 1 月 7 日に CyberNewsFlash として公開しました。

Apache Log4j の任意のコード実行の脆弱性（CVE-2021-44228）に関する注意喚起
https://www.jpcert.or.jp/at/2021/at210050.html

2021 年 12 月に公表された Log4j の脆弱性について
https://www.jpcert.or.jp/newsflash/2021122401.html

(3) 侵入型ランサムウェア攻撃に関する情報発信

2022 年 1 月 13 日、JPCERT/CC は「侵入型ランサムウェア攻撃を受けたら読む FAQ」を公開しました。

いわゆるランサムウェアを用いた攻撃の被害は、一台から数台の端末の感染から、業務停止を引き起こす大規模な感染に至るものまでさまざまです。今回、ランサムウェアを用いた攻撃の内、「企業や組織の内部ネットワークに攻撃者が『侵入』した後、情報窃取やランサムウェアを用いたファイルの暗号化などを行う攻撃」を「侵入型ランサムウェア攻撃」と区別し、「侵入型ランサムウェア攻撃」の被害を受けてしまった場合に、被害組織や初動対応支援にあたる関係者が初動対応時の意思決定や対応の円滑化などを迅速に行えるように、被害に遭った場合の初動対応のポイントや留意点などを FAQ 形式で記載しました。

また、2022 年 3 月 8 日には、ポイントをまとめたウェビナー動画を Youtube で公開しました。

侵入型ランサムウェア攻撃を受けたら読む FAQ
https://www.jpcert.or.jp/magazine/security/ransom-faq.html

1.3. インターネット上でリスク源となり得るノードの活動と状態の観測と分析

JPCERT/CC では、インターネットのセキュリティ状況を俯瞰的に理解し、いち早く異常を検知するために、継続的に定量的観測データを収集して分析するとともに、より効果的な分析に資する相対的評価指標の算出法を開発しています。得られた分析結果は、例えば各地域の CSIRT や ISP、セキュリティベンダーが指標値を用いて自らの相対的なセキュリティ水準を知り、優れたところからセキュリティ向上施策のグッドプラクティスを学ぶなど、サイバー空間全体の健全性を向上させる施策の基礎として活用できます。

具体的には、サイバー空間全体の健全性を次の 2 つの側面から観測し分析しています。インターネット・ノード（以下「ノード」）のうち攻撃の踏み台として利用されやすいものの多寡と、攻撃活動の多寡です。

JPCERT/CC では、前者を「インターネットリスク可視化サービス Mejiro」により、後者を「インターネット定点観測システム TSUBAME」により継続的に観測して、時間的な変化や異常事象を特定する観測分析活動を通じて、インターネットのセキュリティ状況を定量的に把握し、対策が必要なセキュリティ課題を明らかにすることに努めています。

Mejiro では、インターネット上のノードを検索するサービス等からデータの提供を受け、それから攻撃に悪用されるノード数を国や地域ごとに数え上げ、それを統計的に処理して指標値に変換し、指標値を国や地域のセキュリティ状況を表現したものとして公開しています。

TSUBAME では、インターネット上に設置したセンサーに送られてくるパケットを収集して、インターネット上のスキャン活動の動向を監視し、必要に応じて受信パケットを、公表された脆弱性情報などの関連情報と対比するなどして、探索活動の詳細を分析しています。

1.3.1. インターネット上の脆弱なノード数の分布の分析

1.3.1.1. インターネットリスク可視化サービス　— Mejiro —

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

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

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

1.3.1.2. オープンリゾルバー確認サイト

Mejiro では、オープンリゾルバーを踏み台とする DRDoS の被害を減らすことを目的として、世界中のオープンリゾルバーについて指標値を掲載して注意を呼びかけています。日本では、オープンリゾルバーと判定されるノード数が減っているものの、皆無ではなく、減少の速度も緩やかです。これは、対策が進む中で、現状では対応が困難なノードが残されているのではないか、と JPCERT/CC では考えています。オープンリゾルバーは設定不備が根本的な原因ですが、インターネット利用者のルーター等がオープンリゾルバーとして機能し、意図せずオープンリゾルバーを作り出してしまっているケースもあります。JPCERT/CC では、利用者が自ら利用する環境がオープンリゾルバーとして機能していないかを確認する方法として、オープンリゾルバー確認サイトを提供しています。本サイトでは、ユーザーが用いているゲートウェイとフルリゾルバーに関してオープンリゾルバーが否かを検査します。2021 年 12 月から 2022 年 3 月までの月ごとの本サイトへの来訪者数と訪問者のゲートウェイとフルリゾルバーがオープンリゾルバーと判定された件数を［表 1-2］に示します。「オープン率」は全体の中でオープンリゾリルバと判定された割合です。なお、ゲートウェイとフルリゾルバーそれぞれで同じ IP アドレスは一つにまとめています。

［表 1-2：ゲートウェイとフルリゾルバーがオープンリゾリルバとして確認された割合］

年月	訪問者数	オープンリゾルバー数	オープン率
2021-12	816	24	2.9%
2022-01	1096	22	2.0%
2022-02	1132	19	1.7%

オープンリゾルバー確認サイトの運用を 2013 年 10 月から開始しましたが、これにより、オープンリゾルバーとなっているノードの運用者に状況の確認を呼びかけ、簡単な操作をしてもらうだけで、その結果を JPCERT/CC と共有していただくことができるようになしました。この情報をもとに、オープンリゾルバーがどんな背景で生み出され、対策していくにはどうしたらよいかを、JPCERT/CC では考えていくことにしています。

参考文献

(1) オープンリゾルバー確認サイト
https://www.openresolver.jp/
(2) JPCERT/CC オープンリゾルバー確認サイト
https://www.jpcert.or.jp/magazine/security/openresolver.html
(3) 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
(4) SHODAN
https://www.shodan.io/

1.3.2. インターネット上の探索活動や攻撃活動に関する観測と分析

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

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

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

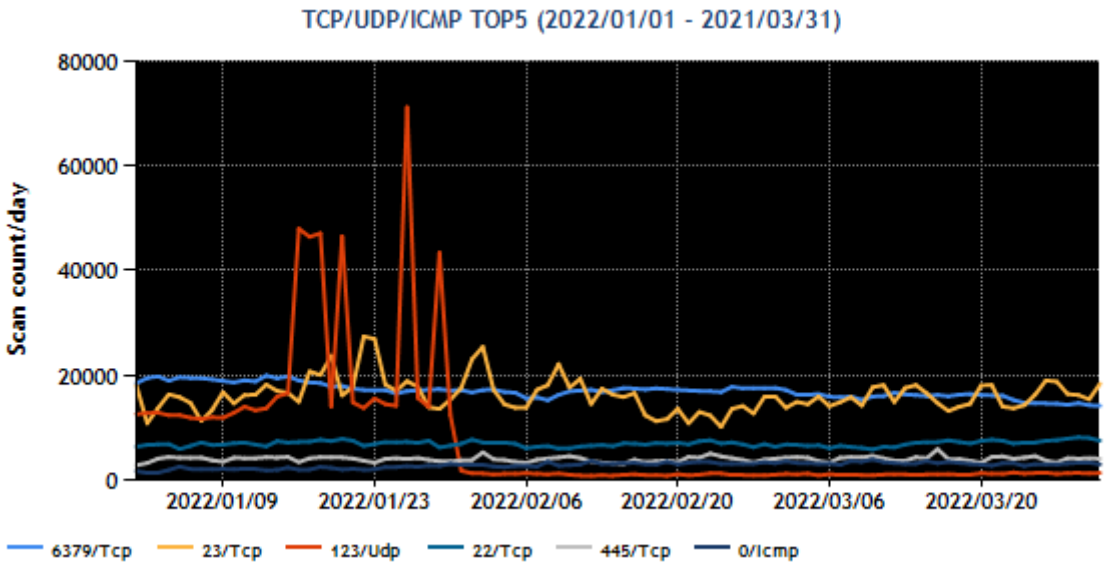
1.3.2.2. TSUBAME の観測データの活用

JPCERT/CC では、主に各組織のシステム管理者の方々に、自組織のネットワークに届くパケットの傾向と比較していただけるよう、日本国内の TSUBAME のセンサーで受信したパケットを宛先ポート別に集計してグラフ化し、毎週月曜日に JPCERT/CC の Web ページで公開しています。また、四半期ごとに観測傾向や注目される現象を紹介する「インターネット定点観測レポート」を公開しており、2021 年 10 月から 12 月の期間に関するレポートを 2022 年 1 月 25 日に公開しました。またレポートに書き切れなかった内容を 2022 年 1 月 25 日にブログで公開しました。

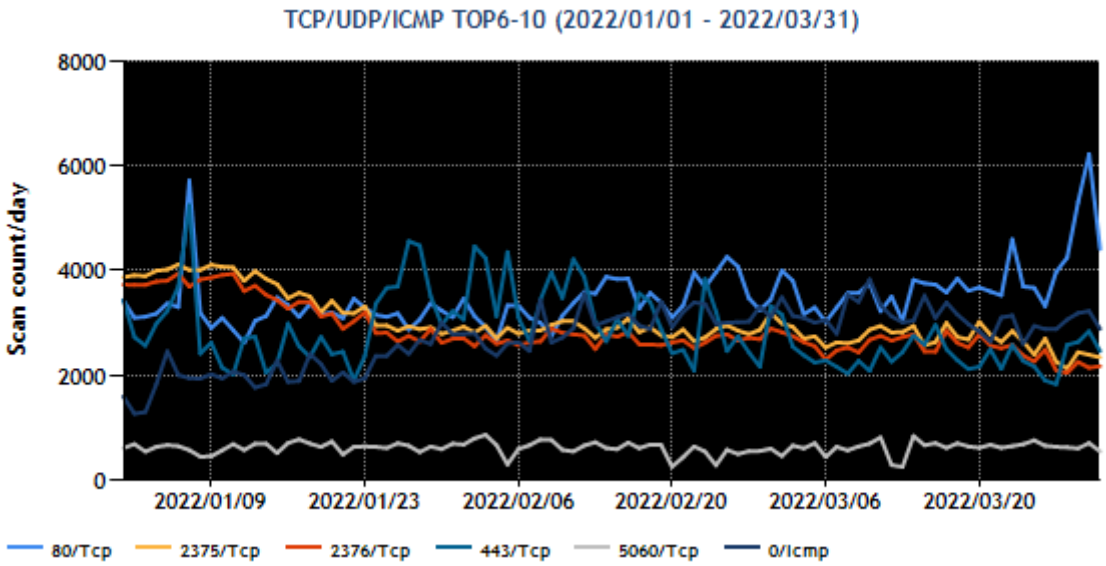
TSUBAME 観測グラフ
https://www.jpcert.or.jp/tsubame/index.html#examples
インターネット定点観測レポート（2021 年 10～12 月）
https://www.jpcert.or.jp/tsubame/report/report202110-12.html
TSUBAME レポート Overflow（2021 年 10～12 月）
https://blogs.jpcert.or.jp/ja/2021/10/tsubame_overflow_2021-10-12.html

1.3.2.3. TSUBAME 観測動向

本四半期に TSUBAME で観測された宛先ポート別パケット数の上位 1～5 位および 6～10 位を［図 1-1］と［図 1-2］に示します。

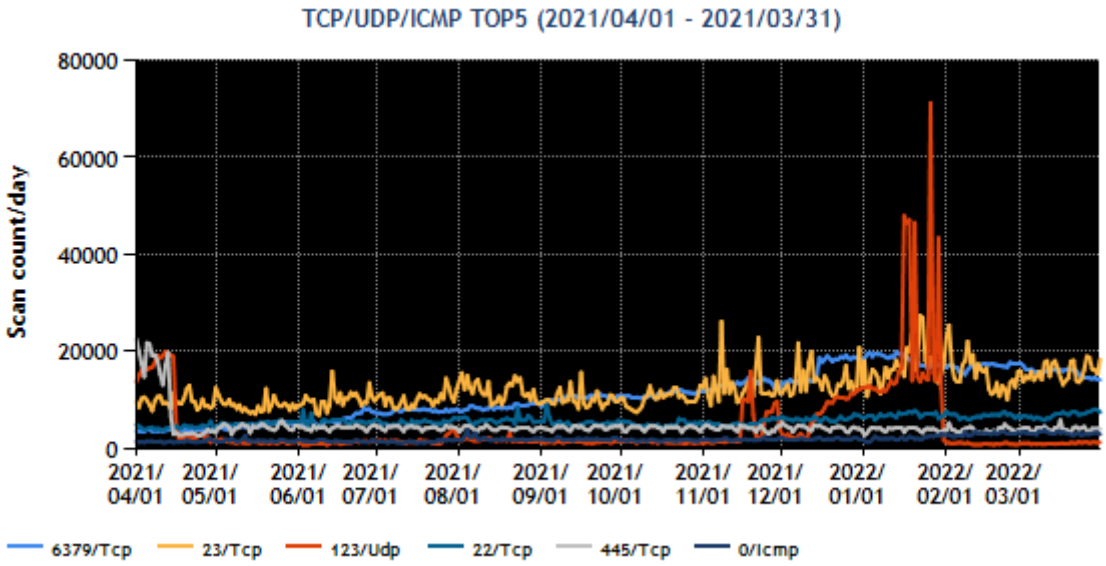


［図 1-1：宛先ポート別グラフ トップ 1-5（2022 年 1 月 1 日-3 月 31 日）］

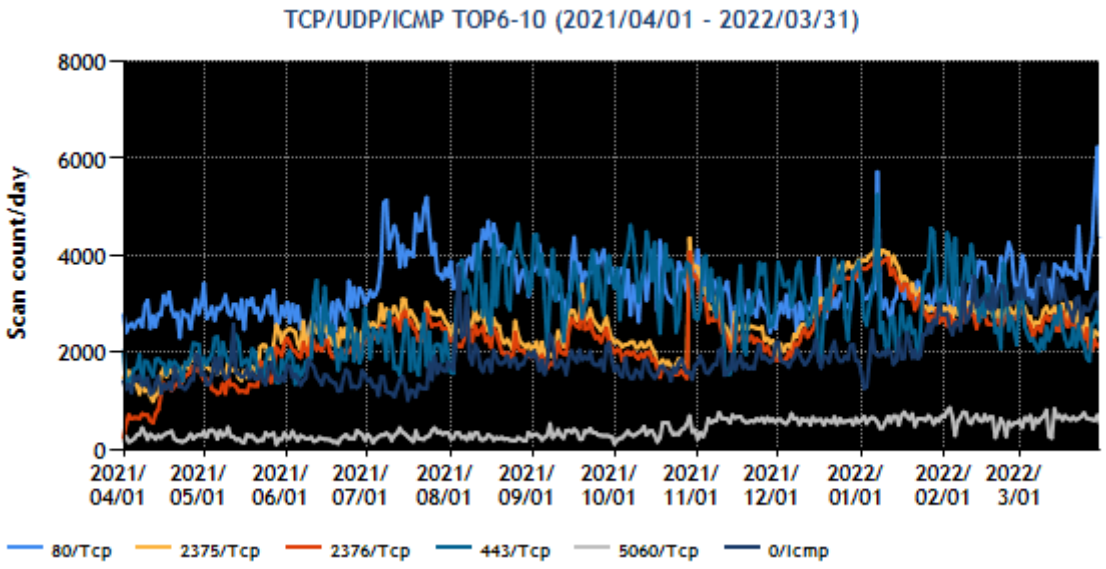


［図 1-2：宛先ポート別グラフ トップ 6-10（2022 年 1 月 1 日-3 月 31 日）］

また、過去 1 年間（2021 年 4 月 1 日-2022 年 3 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 1-3］と［図 1-4］に示します。



［図 1-3：宛先ポート別グラフ トップ 1-5（2021 年 4 月 1 日-2022 年 3 月 31 日）］



［図 1-4：宛先ポート別グラフ トップ 6-10（2021 年 4 月 1 日-2022 年 3 月 31 日）］

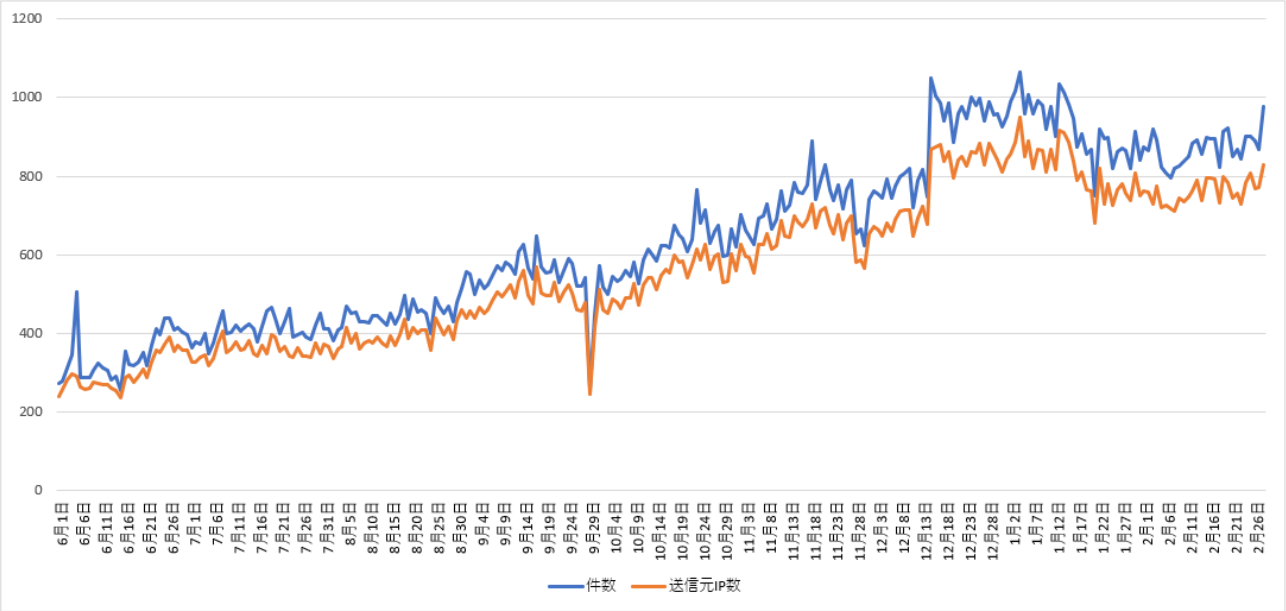
本四半期に最も多く観測されたパケットは 6379/TCP（redis）宛の通信でした。それらの送信元アドレスの大半は中国に割り振られている IP アドレスであり、日本国内のものは数十件と少数でした。次いで多く観測されたパケットが 23/TCP（telnet）宛の通信です。また Docker が使用するポートへの通信（2375/TCP:8 番目、2376/TCP:10 番目）の推移については、6379/TCP 宛の通信の推移との関連性に注目しています。Redis が使用するポートと Docker が使用するポート宛にパケットを送ってきたホストをそれぞれ調べてみました。6379/TCP 宛のポートにパケットを送ってきたホストのうち、2375/TCP もしくは 2376/TCP のポートに対してもパケットを送ってきたホスト数が 45%を占めていました。この背景は定点観測だけでは解りませんが、Redis と Docker に対しての攻撃には何らかの共通する目的があるのではないかと推測しています。それ以外のポートに関しては特筆すべき変化はありませんでした。

1.3.2.4. 定点観測網の拡充に向けた運用とその分析

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

(1) Redis に対する攻撃活動

前四半期に引き続き、今四半期においても 6379/TCP 宛の通信が観測されています。



［図 1-5：低対話型ハニーポットにおける 6379/TCP 宛の通信の観測件数推移］

RESP に応答するハニーポットで収集した通信を分析した結果、多くの送信元 IP アドレスから、Info（サーバーの情報を取得）や Command（Redis コマンドの詳細を取得）といったスキャンを目的としたコマンドが送信されていました。この傾向は前四半期から大きく変わっていません。観測したコマンドの一覧は［表 1-3］に示すとおりです。

スキャンの他に、Config（Redis の設定情報を読み書き）、Set（値を設定）、Save（保存、データ永続化）コマンドを組み合わせることで、悪意のあるスクリプトを Redis 上で実行させる攻撃も観測しています。このような攻撃を行う送信元 IP は、スキャンを行う送信元 IP よりも少数ですが、同種の攻撃を 1 日に複数回、数日に渡って継続する傾向にあるため、表中のコマンドのうち、Config、Set、Save の件数が多くなっています。

こうした観測結果を定点観測友の会や通信事業者等の組織にも提供するとともに、頻繁に攻撃を試みていた一部の攻撃元ホスト並びにマルウェアの配布元となっているホストのテイクダウンに向けたコーディネーションを実施しました。

［表 1-3：RESP に応答するハニーポットで 10/1 – 2/24 に観測されたコマンド一覧］

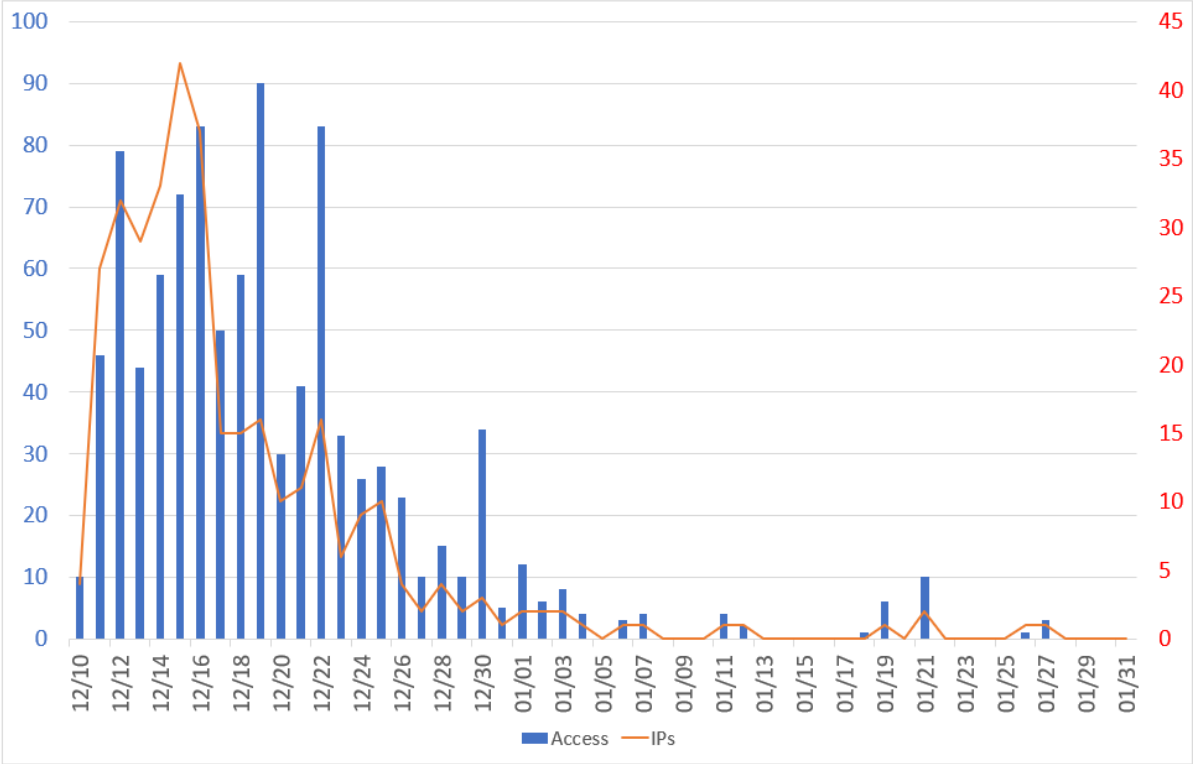
コマンド	件数
Config	3,321
Set	2,971
Save	1,828
Info	863
Flushall	607
Command	509
Auth	259
Ping	239
Quit	206
Nonexistent	203
Client	30
Scan	26
Cluster	15
Pubsub	15
Module	10
Saveof	10
System.exec	10
Keys	5

(2) Apache Log4j の脆弱性 CVE-2021-44228 を狙った攻撃パケット

2021 年 12 月 10 日に公表された Apache Log4j の脆弱性（CVE-2021-44228）を悪用する通信を観測しました。同日に概念実証コードがインターネット上に公開され、およそ 2 週間、攻撃パケットの観測件数が急に増えた状態が続いていましたが、その後は急速に減少し 1 月末にはほとんど観測されなくなりました。［図 1-6］

観測した攻撃パケットには、公開された概念実証コードに記載されている文字列「${jndi:ldap://」が含まれており、観測当初は LDAP プロトコルを悪用するものが多く見られましたが、徐々に DNS や RMI といったプロトコルの悪用を試みる通信や、Web Application Firewall の回避を意図したと思われる難読化された攻撃文字列も観測されるようになりました。

以上の観測結果は早期警戒情報や注意喚起、CyberNewsFlash、JPCERT/CC Eyes ブログで公開したほか、定点観測友の会、セプターカウンシル、JPCERT/CC 情報共有会などでも共有しています。



［図 1-6：ハニーポットにおける Apache Log4j の脆弱性を狙った通信の観測件数推移］

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」）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」）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/

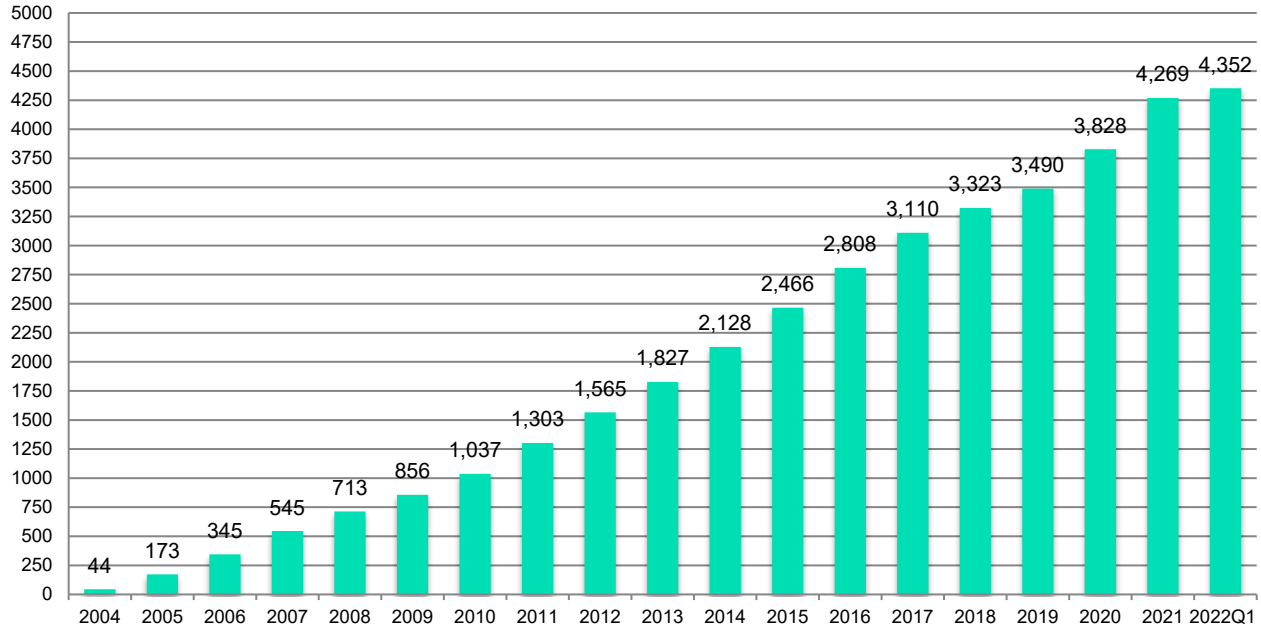
2.1.2. Japan Vulnerability Notes（JVN）において公表した脆弱性情報および対応状況

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」;「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」;「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 83 件（累計件 4,352）で、累計の推移は［図 2-1］に示すとおりです。本四半期に公表された個々の脆弱性情報に関しては、次の Web ページをご参照ください。

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



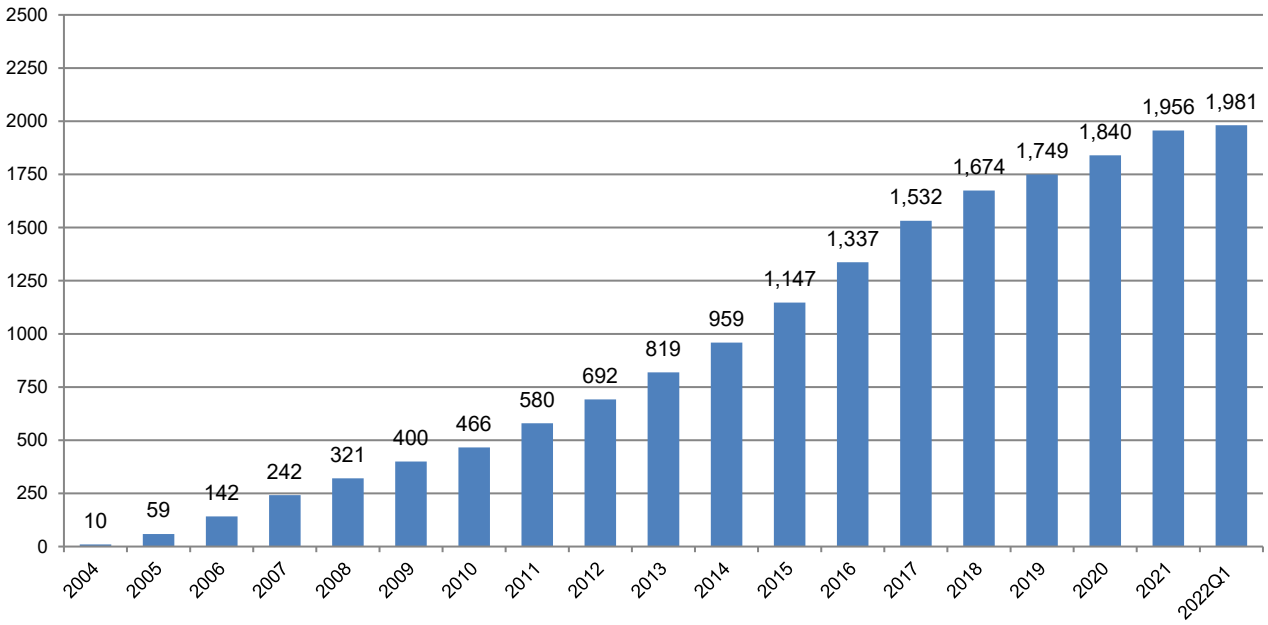
［図 2- 1：JVN 公表累積件数］

本四半期において公表に至った脆弱性情報のうち、国内取扱脆弱性情報は 25 件（累計 1,981 件）で、累計の推移は ［図 2-2］に示すとおりです。本四半期に公表した 25 件の内訳は、国内の単一の製品開発者の製品に影響を及ぼすものが 17 件（このうち自社製品の届け出によるものが 5 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、組込系製品が 7 件と最も多く、次いでウェブアプリケーションとマルチプラットフォームアプリケーションがそれぞれ 4 件、続いてプラグインが 3 件、CMS と macOS アプリケーションがそれぞれ 2 件、Android アプリケーション、Windows アプリケーション、サーバー製品がそれぞれ 1 件でした。

［表 2-1：公表を行った国内取扱脆弱性情報の件数の製品カテゴリー内訳］

製品分類	件数
組込系製品	7
ウェブアプリケーション	4
マルチプラットフォームアプリケーション	4
プラグイン	3
CMS	2
macOS アプリケーション	2
Android アプリケーション	1
Windows アプリケーション	1
サーバー製品	1



［図 2- 2：公表を行った国内取扱脆弱性情報の累積件数］

本四半期に公表した国際取扱脆弱性情報は 58 件（累計 2,371 件）で、累計の推移は［図 2-3］に示すとおりです。58 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 23 件（このうち複数製品開発者の製品に影響を及ぼすものは 6 件）、国内外の発見者からの届け出によるものは 5 件、JPCERT/CC が注意喚起として発行したものは 30 件でした。

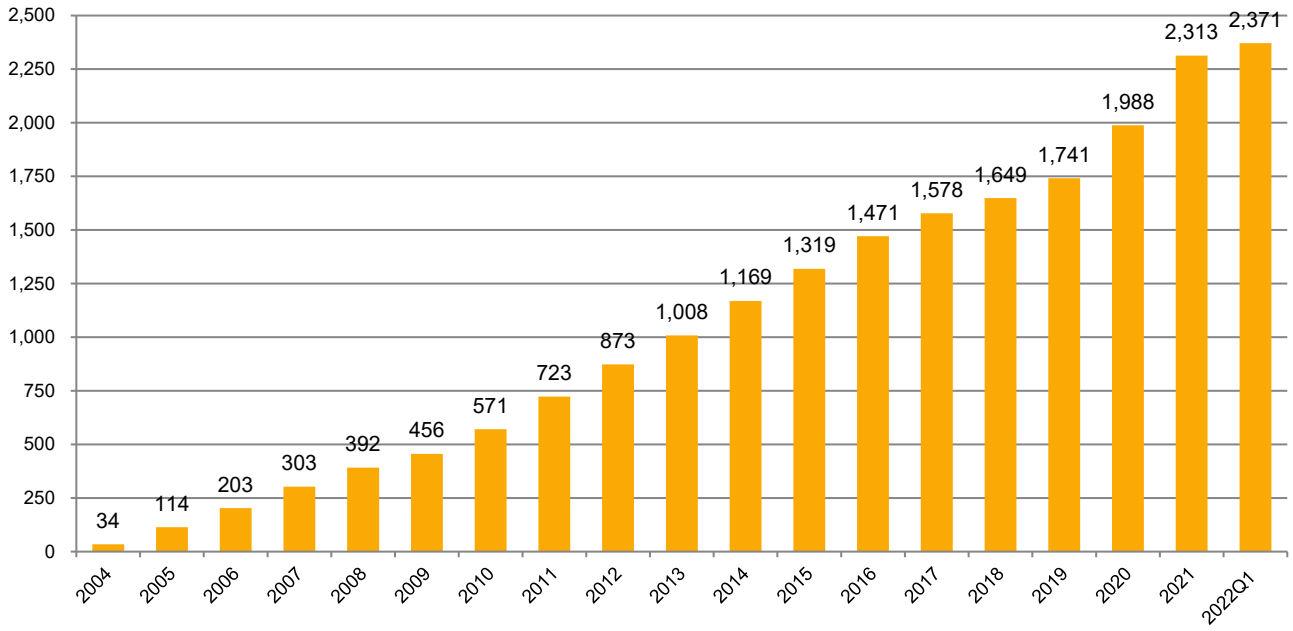
本四半期に公表した脆弱性の影響を受けた製品のカテゴリー内訳は、［表 2-2］のとおりです。本四半期は、制御系製品が 34 件と最も多く、次いで組込系製品が 5 件、Windows アプリケーションとアンチウイ

ルス製品がそれぞれ 4 件、医療機器が 3 件、サーバー製品とプロトコルがそれぞれ 2 件、CMS、DNS、macOS アプリケーション、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、国内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	34
組込系製品	5
Windows アプリケーション	4
アンチウイルス製品	4
医療機器	3
サーバー製品	2
プロトコル	2
CMS	1
DNS	1
macOS アプリケーション	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、50 件（製品開発者数で 30 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 200 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-NL など脆弱性情報ハンドリングを行っている海外の調整機関と協力関係を結び、必要に応じて脆弱性情報の共有、各国の製品開発者への通知および対応状況の集約、脆弱性情報の公表時期の設定などの調整活動を行っています。

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

JPCERT/CC では、2008 年 5 月以降 JVN 英語版サイトの公開を機に CVE 採番を行っており、Top Level Root である MITRE やその他の組織への確認や照会を必要とする特殊なケース（全体の 1 割弱）を除いて、JVN 上で公表する脆弱性のほぼすべてに CVE 番号を付与しています。本四半期には、JVN で公表したものに対し 51 個の CVE 番号を付与しました。

最初は CVE 番号の付与を、MITRE 社から番号プールの提供を受けて、その中から採番することにより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 に指定され、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と株式会社 LINE、日本電気株式会社（NEC）、株式会社東芝、パナソニック株式会社の 5 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/

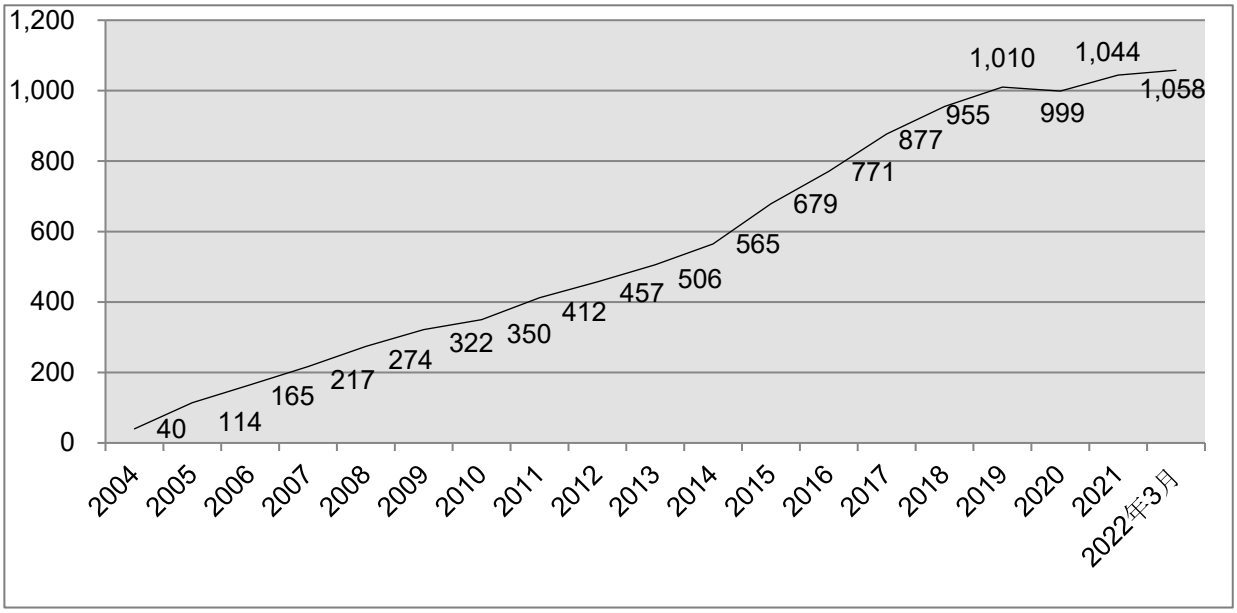
情報セキュリティ早期警戒パートナーシップガイドライン（2019 年版）
https://www.jpcert.or.jp/vh/partnership_guideline2019.pdf

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 3 月 31 日現在で 1,058 となっています。登録等の詳細については、次の Web ページをご参照ください。

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



［図 2-4：累計製品開発者登録数］

2.2.2. 製品開発者との定期ミーティング等の実施

JPCERT/CC では、技術情報やセキュリティ・脆弱性の動向などの情報交換や、脆弱性情報流通業務に関する製品開発者との意見交換、また、製品開発者間の情報交換を目的として、脆弱性情報流通の活動にご協力いただいている製品開発者の皆さまとの定期ミーティングや特定テーマ毎の個別ミーティングを開催しています。

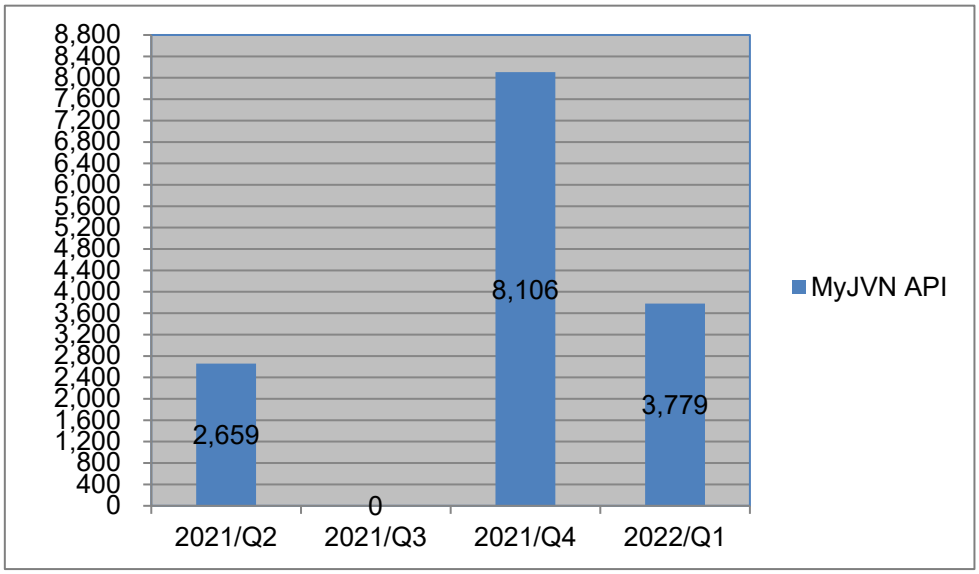
本四半期においては、2 月 3 日に制御・組込系の製品開発者に限定した座談会を開催し、海外の脆弱性調整機関等からの脆弱性報告への対応について意見交換を行いました。また 2 月 10 日には製品開発者登録ベンダー全体を対象とした定期ミーティングを開催し、公表を含む Log4j 脆弱性（CVE-2021-44228）への一連の対応に関する議論や、前四半期に実施した PSIRT 体制等に関するアンケートの結果報告、制御・組込系ベンダー向け座談会の実施報告を行い、それらについて参加者との意見交換を行いました。

2.3. VRDA フィードによる脆弱性情報の配信

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

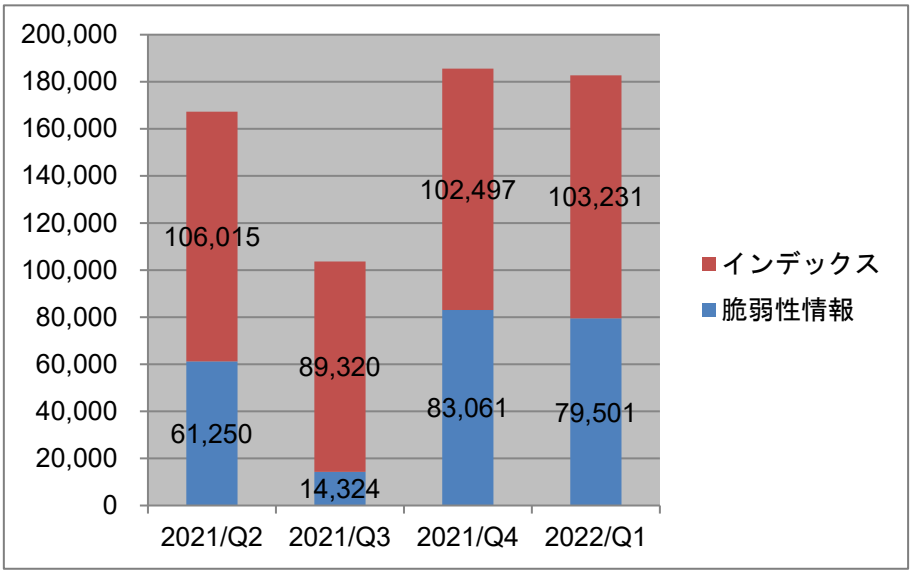
VRDA フィード 脆弱性脅威分析用情報の定型データ配信
https://www.jpcert.or.jp/vrdafeed/index.html

四半期ごとに配信した VRDA フィード配信件数を［図 2- 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。



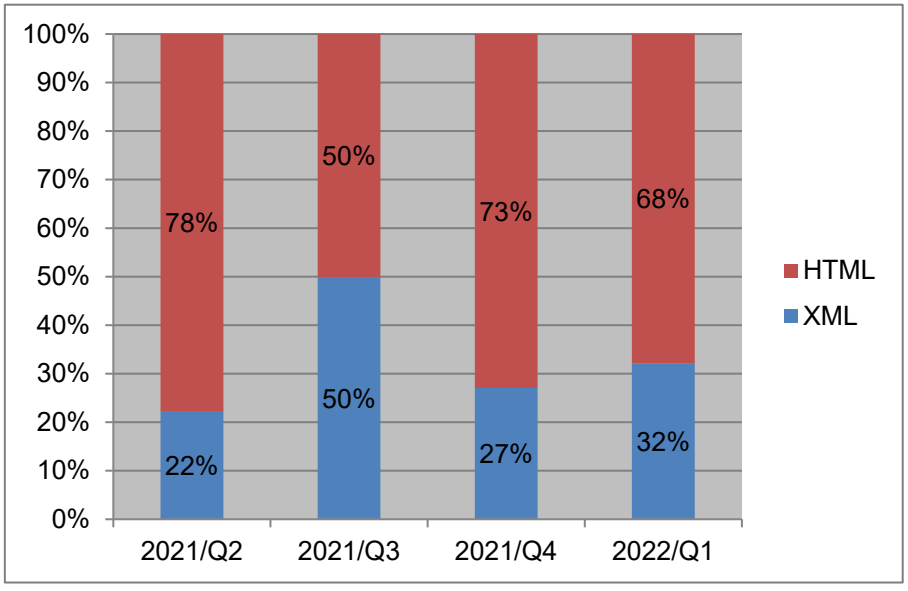
［図 2- 5：VRDA フィード配信件数］

VRDA フィード配信件数については、［図 2- 5］に示したように前年度第 3 四半期は配信件数が 0 となっています。これは VRDA フィード配信用システムの障害により、期間中データ更新が停止していたことが原因です。



［図 2-6：VRDA フィード利用件数］

インデックスおよび脆弱性情報の利用数については、［図 2-6］に示したように、前四半期と比較し、目立った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、XML 形式の利用割合が 5%増加しました。

3. 制御システムセキュリティ強化に向けた活動

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 183 件でした。

3.1.1. 情報提供

このうち、国内の制御システム関係者に影響があり、注目しておくべき事案を「参考情報」として、その情報を必要とする国内組織に提供しました。

本四半期に提供した参考情報は 4 件でした。

2022/02/25　Bently Nevada 社製 3500 機械保護システムの脆弱性に関する続報
2022/03/09　米国 NIST が分散型エネルギーリソースと基幹電力網との間でやり取りされる情報を保護するための実践ガイドを公表
2022/03/10　鉄道システムにおけるゾーンとコンジットの構築に関する設計ガイドを ENISA が公表
2022/03/15　上水道システムのセキュリティ計画の実現マニュアルを欧州の ERNCIP Chemical and Biological (CB) Risks to Drinking Water Thematic Group が公表

また、海外での事例や、標準化動向などを JPCERT/CC からのお知らせとともに、制御システムセキュリティ情報共有コミュニティー（注 1）に登録いただいている関係者向けに月刊ニュースレターとして配信しています。

本四半期は 2 件を配信しました。

2022/01/17　制御システムセキュリティニュースレター 2021-0012
2022/03/11　制御システムセキュリティニュースレター 2022-0002

（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 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 1,251 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次の 1 件でした。

2022/03/10　JVNVU#92837755：Moxa 製 MXview シリーズにおける複数の脆弱性

3.1.2. 提供情報の事例

本四半期における情報収集・分析・提供した事例を紹介します。これらの脆弱性情報は、すぐに悪用される可能性は低いものの、悪用された場合の影響が大きいため、国内の利用者に向けて注意を促す目的で発信しました。

(1) Moxa 製 MXview シリーズにおける複数の脆弱性

2022 年 2 月 11 日、海外セキュリティベンダーより、Moxa 社製 MXView における複数の脆弱性に関する情報が公表されました。本製品の初期インストール時に Polling Engine Port と称する 4430/tcp を使用するサービスが追加されます。このサービスは、デフォルトのユーザー名とパスワードが設定されていますが、パスワードの変更方法やアクセスを無効にする方法が明記されていません。また、80/tcp や 443/tcp の Web アプリケーションなど、別のサービスで当該ユーザーのパスワードを変更しても Polling Engine Port で使用するユーザーのパスワードが変更されない問題が存在します。そのため、遠隔の第三者によって細工された HTTP リクエストを送信され、管理者権限で当該アプリケーションの機能にアクセスされる可能性があります。その他にも、初期インストールでは Web アプリケーションが HTTP プロトコルで通信されるように設定されており、認証情報が平文でやり取りされる問題も存在します。

JPCERT/CC では、本脆弱性に関する PoC コードが海外セキュリティベンダーから公開されている

こと、本脆弱性に対応したアップデート等が提供されていることを確認し、3 月 10 日に JVN で脆弱性情報を公表しました。

JVNVU#92837755　Moxa 製 MXview シリーズにおける複数の脆弱性
https://jvn.jp/vu/JVNVU92837755/

3.1.3. 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今年度から始めました。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の読み解き方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指しています。

本四半期は、2021 年度上期の分析結果を取りまとめたレポートを 2022 年 3 月 28 日に公表しました。制御システム関連のソフトウェアにおけるファイル読み込みの脆弱性について特定の情報の例をとりあげ、JPCERT/CC における分析から情報発信に至るまでの経緯や、制御システムユーザー組織で実施可能と思われる対策などについて解説しています。

ICS 脆弱性分析レポート ― 2021 年度上期 ―
https://www.jpcert.or.jp/ics/ics-vuls-analysis-report.html

JPCERT/CC Eyes：ICS 脆弱性分析レポート ― 2021 年度上期 ―を公表
https://blogs.jpcert.or.jp/ja/2022/03/ics-vuls-analysis-report-2021H1.html

3.2. 制御システム関連のインシデント対応

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

3.3. 関連団体との連携

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

3.4. 制御システム向けセキュリティ自己評価ツールの提供

JPCERT/CC では、制御システムの構築と運用に関するセキュリティ上の問題項目を抽出し、バランスの良いセキュリティ対策を行っていただくことを目的として、簡便なセキュリティ自己評価ツールである日本版 SSAT（SCADA Self Assessment Tool：申し込み制）や J-CLICS（制御システムセキュリティ自己評価ツール：フリーダウンロード）を提供しています。本四半期は、日本版 SSAT に関する利用申し込みはなく、直接配付件数の累計 287 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. 制御システムセキュリティカンファレンス

2022 年 2 月 3 日（木）に「制御システムセキュリティカンファレンス 2022」をオンライン開催し、440 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 14 回目を迎えました。

新型コロナウイルス感染症対策のためのリモートアクセス活用拡大や DX を加速させる動きが産業界に見られる一方で、VPN の脆弱性を悪用した攻撃による被害やランサムウェア感染被害等、製造業をはじめとした国内外の制御システム関連事業者の被害事例が増加傾向にあります。こうした状況を踏まえると、制御システムセキュリティ対策の強化は、依然として制御システム関係者における重要な課題です。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プログラムを構成しました。また、本カンファレンスの開催趣旨に沿って、講演の一部を公募いたしました。

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 3 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 3 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 2022
https://www.jpcert.or.jp/event/ics-conference2022.html

制御システムセキュリティカンファレンス 2022 講演資料
https://www.jpcert.or.jp/present/#year2022

JPCERT/CC Eyes：制御システムセキュリティカンファレンス 2022 開催レポート
https://blogs.jpcert.or.jp/ja/2022/03/ics-conference2022.html

［図 3-1：制御システムセキュリティカンファレンス 2022 講演］

［表 3-1：制御システムセキュリティカンファレンスのプログラム］

(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)「情報通信技術等を利用した生産システムにおける人の安全確保を実現するための調査研究」 三菱電機株式会社 先端技術総合研究所 システム構築技術部 主席技師長 神余 浩夫
(3)「制御システムエンジニアによる実践的な制御システム復旧計画」 ABB 日本ベーレー株式会社 デジタル技術部テクノロジー課 大石 貴之
(4)「製造業へのローカル 5G 導入に伴うサイバーセキュリティリスク実証実験 ～製鉄所を模した環境での侵入経路と被害の実態～ トレンドマイクロ株式会社 グローバル IoT マーケティング室 セキュリティエバンジェリスト 石原 陽平
(5)「制御システムセキュリティガイドライン制定への道のり」 小林製薬株式会社 グループ統括本社 業務改革センター 生産システム部 製造システムグループ 佐々木 朝
(6)「JPCERT/CC における制御システム製品の脆弱性情報の収集および分析」 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

4. 国際連携活動関連

本四半期も引き続き、新型コロナウイルス感染症対策の観点から世界の多くの国で渡航制限が敷かれ、多くの国際会議がオンラインで開催されました。

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

Steering Committee は、2 月 9 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。本四半期は毎月の理事会に出席するとともに、国内企業の FIRST 新規加盟に関するサポートを実施しました。
FIRST の詳細については、次の Web ページをご参照ください。

FIRST
https://www.first.org/

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

4.3. 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「複数の開発者が関与する脆弱性の開示と取扱」の標準化作業と、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「複数の開発者が関与する脆弱性の開示と取扱」については、昨年 10 月の国際会議において承認

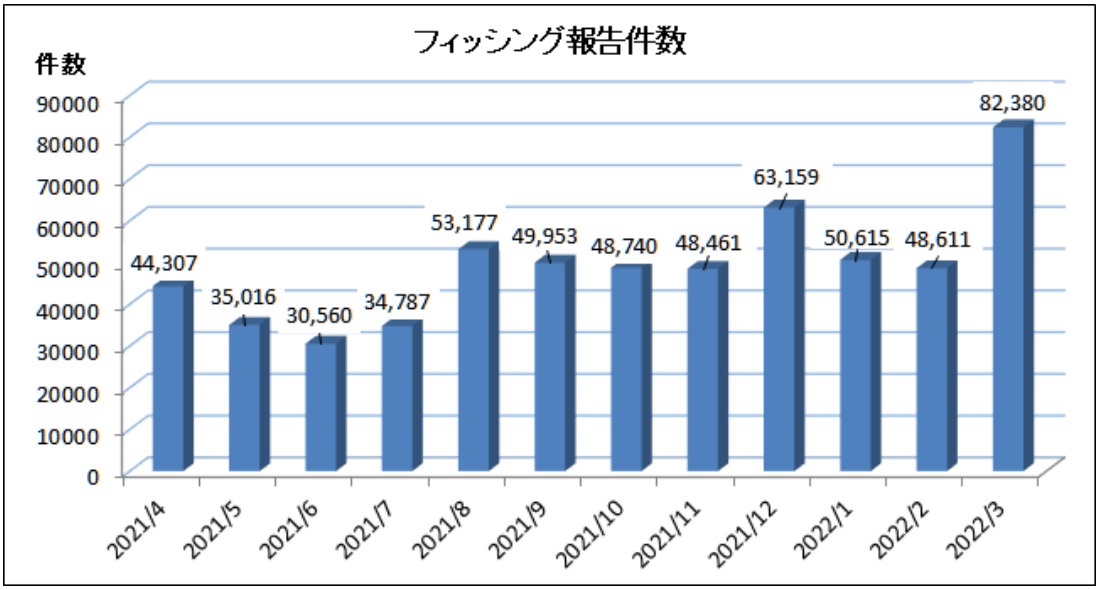
された技術報告書の公開へ向けて、国際投票時に提出されたコメントの反映等の作業を分担して行いました。WG4「インシデント管理に関する標準」については、引き続き標準文書の改訂に伴う CD 文書の作成ならびに新しいパートの WD 文書の作成が行われており、本四半期はコメントの提出等の作業を行いました。

5. フィッシング対策協議会事務局の運営

フィッシング対策協議会（本節の以下において「協議会」）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、Web 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が、1 月および 2 月は約 5 万件前後で推移しましたが、3 月に過去最高となる 82,380 件を記録しました。
例年の傾向にならい、2 月第 1 週の中国の春節期間は中国を送信元とするメール配信が減少しましたが、その終了後は増えています。



［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引き続き多く、全体の約 29.6%を占めています。次いで、メルカリ、えきねっと、MyJCB、三井住友カードのフィッシングの報告が多く、この 5 ブランドに関連する報告が全体の約 61.5%を占めました。

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 13 件（緊急情報：13 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。

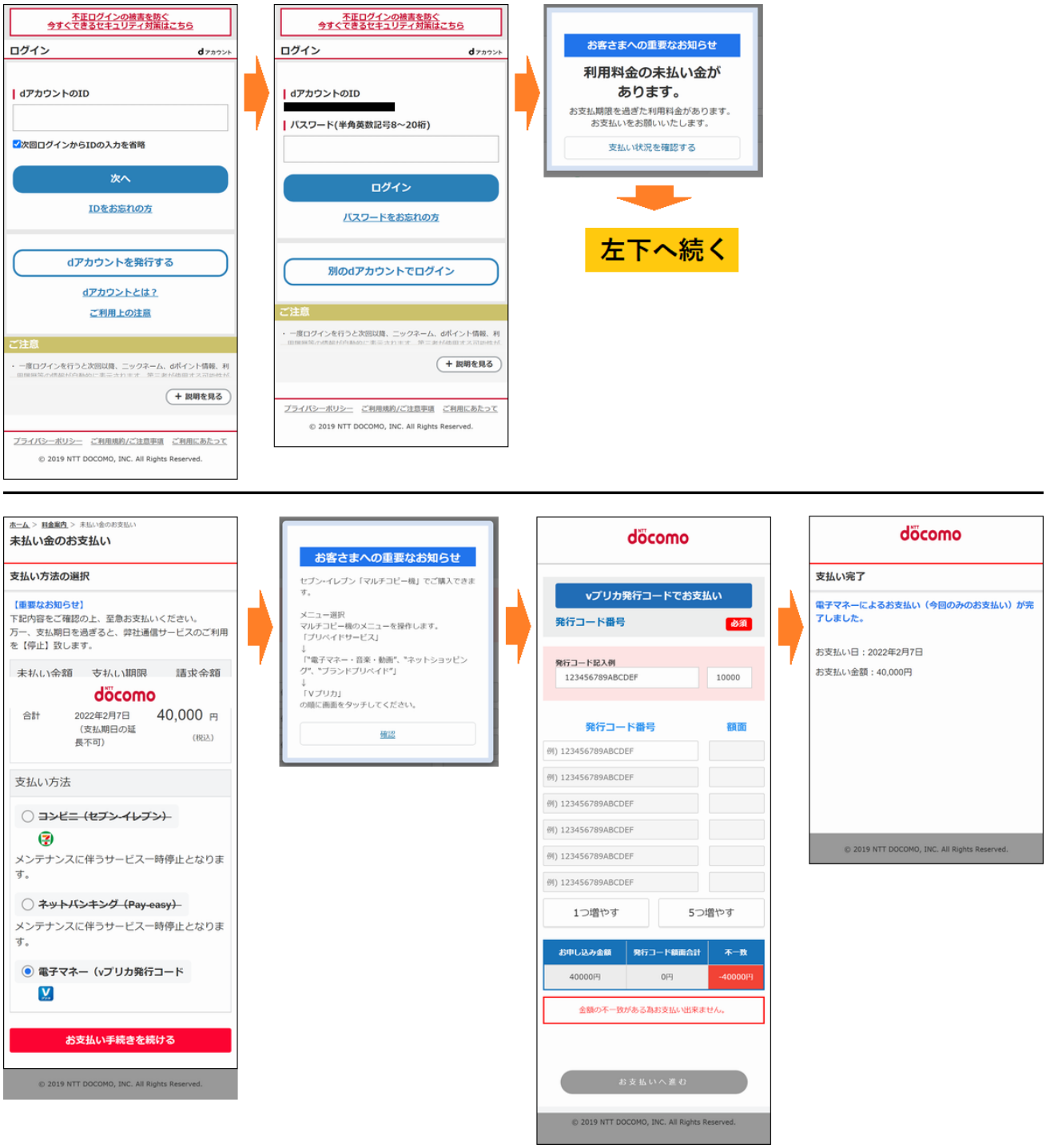
- LINE Pay をかたるフィッシング：1 件
- 三菱 HC キャピタルカードをかたるフィッシング：1 件
- プロミスをかたるフィッシング：1 件
- Uber Eats をかたるフィッシング：1 件
- TS CUBIC CARD をかたるフィッシング：1 件
- NTT ドコモをかたるフィッシング：1 件
- Yahoo! JAPAN をかたるフィッシング：1 件
- 千葉銀行をかたるフィッシング：1 件
- えきねっとをかたるフィッシング：1 件
- JR 西日本をかたるフィッシング：1 件
- JR 東日本 (モバイル Suica) をかたるフィッシング：1 件
- 出前館をかたるフィッシング：1 件
- FamiPay をかたるフィッシング：1 件

本四半期は、前期に引き続きクレジットカードブランド（30 種類）をかたるフィッシングの報告が多く寄せられました。また、キャッシュレス決済を狙うフィッシングも引き続き報告されています（[図 5-2]：LINE Pay をかたる）。それ以外では、モバイルキャリアをかたるフィッシングも多く報告されています（[図 5-3：NTT ドコモをかたるフィッシングの例]）この NTT ドコモをかたるフィッシングの例では、クレジットカード情報ではなくプリペイドカード番号を入力させるものでした。

これら大量配信されるフィッシングメールが、依然として正規のメールアドレス （ドメイン） を差出人とした「なりすまし」メールであることから、受信者による判別を容易にするために、送信ドメイン認証技術を活用するよう協議会として呼び掛けています。

［図 5-2：LINEPay をかたるフィッシングサイトの例 ］

https://www.antiphishing.jp/news/alert/line_pay_20220111.html



［図 5-3：NTT ドコモをかたるフィッシングサイトの例 ］

https://www.antiphishing.jp/news/alert/nttdocomo_20220210.html

5.2.2. 定期報告

協議会の Web サイトにおいて、報告されたフィッシングサイト数を含む、毎月の活動報告等を公開しています。詳細については、次の Web ページをご参照ください。

フィッシング対策協議会 Web ページ
https://www.antiphishing.jp/

2022 年 1 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/202201.html

2022 年 2 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/202202.html

2022 年 3 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/202203.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 50 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、フィッシング対策協議会の会員を中心とする有識者で構成される、フィッシング対策に関するガイドラインや動向レポートを作成・改訂を行う作業部会です。
今期は、2022 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 WG 会合（第 5 回）
  日時：2022 年 1 月 28 日 13:00-15:00

- 技術・制度検討 WG 会合　報告会（第 6 回）
  日時：2022 年 3 月 3 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 95 回運営委員会（オンライン）
  2022 年 2 月 24 日（木）16:00-18:00

- 第 96 回運営委員会（オンライン）
  2022 年 3 月 24 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 WG 会合
  日時：1 月- 3 月　毎週火曜日 9：00 - 9：30

- 第 4 回フィッシング対策勉強会
  日時：2 月 15 日　13：00 - 15：10

※ワーキンググループ会合等はすべてオンライン開催

6.3. ワーキンググループ等の成果物の公開支援

本四半期においては、次のようなワーキンググループ等の成果物の公開を支援しました。

証明書普及促進 WG

【更新】主要ブラウザのセキュリティ強化に対する施策について［ Chrome 98 で TLS1.0/1.1 が完全無効化］（2022/2/22）

https://www.antiphishing.jp/news/info/disabled_TLS_20220222.html

STC 普及啓発 WG

2021 年度においてフィッシング詐欺対策コミュニティーにて顕著な活動を行っている有識者などへ贈呈(2022/2/21)

https://www.antiphishing.jp/news/info/20220221.html

7. 公開資料

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

7.1. インシデント報告対応レポート

JPCERT/CC では、国内外で発生するコンピューターセキュリティインシデントの報告の受付、対応の支援、発生状況の把握、手口の分析、再発防止のための助言などを行っています。そうした活動の概要を紹介するために、インシデント報告数、報告されたインシデントの総数、および、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、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。

2022-01-20
JPCERT/CC インシデント報告対応レポート［2021 年 10 月 1 日～2021 年 12 月 31 日］
https://www.jpcert.or.jp/pr/2022/IR_Report2021Q3.pdf

2022-02-22
JPCERT/CC Incident Handling Report [October 1, 2021 - December 31, 2021]]
https://www.jpcert.or.jp/english/doc/IR_Report2021Q3_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。

2022-01-25
JPCERT/CC インターネット定点観測レポート［2021 年 10 月 1 日～2021 年 12 月 31 日］
https://www.jpcert.or.jp/tsubame/report/report202110-12.html
https://www.jpcert.or.jp/tsubame/report/TSUBAMEReport2021Q3.pdf
2022-02-22
JPCERT/CC Internet Threat Monitoring Report [October 1, 2021 - December 31, 2021]]
https://www.jpcert.or.jp/english/doc/TSUBAMEReport2021Q3_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。

2022-01-20
ソフトウェア等の脆弱性関連情報に関する届出状況［2021 年第 4 四半期（10 月～12 月）］
https://www.jpcert.or.jp/pr/2022/vulnREPORT_2021q4.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：7 件　https://blogs.jpcert.or.jp/ja/

2022-01-25　TSUBAME レポート Overflow（2021 年 10～12 月）
2022-02-28　JSAC2022 開催レポート～DAY1～
2022-03-08　JSAC2022 開催レポート～DAY2～
2022-03-10　制御システムセキュリティカンファレンス 2022 開催レポート
2022-03-15　Anti-UPX Unpacking テクニック
2022-03-17　サイバー政策動向を知ろう Watch! Cyber World vol.2｜ランキング
2022-03-28　ICS ユーザー組織の脆弱性対応に関する参考資料「ICS 脆弱性分析レポート ― 2021 年度上期 ―」を公表

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

2022-02-04	FAQ: Malware that Targets Mobile Devices and How to Protect Them
2022-02-22	TSUBAME Report Overflow (Oct-Dec 2021)
2022-03-15	Anti-UPX Unpacking Technique
2022-03-22	JSAC 2022 -Day 1-
2022-03-22	JSAC 2022 -Day 2-

8. 主な講演活動

(1) 平塚 伸世（エンタープライズサポートグループ リーダー）：
「フィッシングの現状（2021 年版）」
神奈川クレジットカード犯罪対策連絡協議会 定例会（主催：神奈川クレジットカード犯罪対策連絡協議会、開催日：2022 年 1 月 21 日）

(2) 平塚 伸世（エンタープライズサポートグループ リーダー）：
「フィッシング（メール配信）の傾向と対策（2021 年 7 月-12 月）」
JANOG49 Meeting（主催：JANOG49 Meeting、開催日：2022 年 1 月 26 日～28 日）

(3) 奥石 隆 （早期警戒グループ 脅威アナリスト）：
「演習 1」
TRANSITS Workshop Online 2022 Winter （主催：日本シーサート協議会、開催日：2022 年 2 月 3 日～4 日）

(4) 佐々木 勇人（早期警戒グループ マネージャー）：
「ランサムウェア対策の難しさと被害発生時の対応について」
学校法人岩崎学園「サイバーセキュリティセミナー 2022」（主催：学校法人岩崎学園、開催日：2022 年 2 月 8 日）

(5) 平塚 伸世（エンタープライズサポートグループ リーダー）：
「フィッシング報告から見るなりすましメールの現状（2021 年版）」
フィッシング対策協議会 勉強会（主催：フィッシング対策協議会、開催日：2022 年 2 月 15 日）

(6) 平塚 伸世（エンタープライズサポートグループ リーダー）：
「フィッシングの現状 (2021 年版)」
全国銀行協会 IB 不正送金対策に関するセミナー（主催：全国銀行協会、開催日：2022 年 3 月 2 日）

(7) 鹿野 恵祐（サイバーメトリクスグループ リーダー）：
「『定点観測友の会』というコミュニティー活動から見えること」
ITmedia Security Week 2022 春（主催：@IT、ITmedia エンタープライズ、ITmedia エグゼクティブ、開催日：2022 年 3 月 3 日）

(8) 小宮山 巧一朗（国際部 部長）：
「2022 年の CSIRT ~ サイバー空間はいくつに分割されるか? ~」
WIDE 合宿招待講演（主催：WIDE Project、開催日：2022 年 3 月 8 日）

(9) 持永 大（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」
令和三年度 松江高専 情報セキュリティ講習会（主催：松江工業高等専門学校、開催日：2022 年 3 月 9 日）

(10) 朝長 秀誠（インシデントレスポンスグループ マネージャー）：
「APT Case Study in Japan」
NTT データ セキュリティ DAY（主催：株式会社エヌ・ティ・ティ・データ 、開催日：2022 年 3 月 25 日）

9. 主な執筆活動

(1) 土居 毅彦（早期警戒グループ 脅威アナリスト）：
「2021 年の情報セキュリティ動向」
（発行：ImpressR&D、書籍名：インターネット白書 2022、発刊：2022 年 2 月 7 日）

(2) 佐々木 勇人（早期警戒グループ マネージャー）：
「ロシアを背景とするサイバー攻撃グループによるサボタージュ目的／偽情報作戦としての攻撃活動とその対策について」
（発行：一般財団法人安全保障貿易情報センター、掲載：CISTEC ジャーナル 2022 年 3 月号、発刊：2022 年 3 月 31 日）

10. 協力、後援

本四半期は次の行事開催に協力または後援等を行いました。

(1) 第 6 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 3 回 産業サイバーセキュリティコンファレンス
主　催：株式会社インプレス、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：2022 年 2 月 16 日（水）～17 日（木）

(2) Security Days Spring 2022
主　催：株式会社ナノオプト・メディア
開催日：2022 年 3 月 9 日（水）～3 月 11 日（金）

(3) セキュリティフォーラム 2022
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（JSSEC）、一般社団法人セキュア IoT プラットフォーム協議会（SIOTP 協議会）
開催日：2022 年 3 月 24 日（木）

■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