Japan Computer Emergency Response Team Coordination Center

JPCERT-PR-2018-03
発行日 : 2018-7-12

JPCERT/CC 活動概要 [2018 年 4 月 1 日 ～ 2018 年 6 月 30 日]

活動概要トピックス

ートピック1ー　脆弱性情報コーディネーションの効率化に向けた VDO に関する取り組み

JPCERT/CC は、脆弱性情報コーディネーションの効率化に向けて行っている VDO に関する取り組みを、FIRST（Forum of Incident Response and Security Teams）の第 30 回年次会合で発表しました。この取り組みは、米国 NIST が提案している Vulnerability Description Ontology（VDO）に基づいた共通言語を用いて脆弱性情報を表現し、それを機械処理することを目指しています。本発表は、会合のプログラム中、脆弱性をテーマとするセッションの一つとして位置づけられており、この分野の有識者を含む約 100 名の方が聴講しました。発表後、複数の会議参加者から VDO の適用範囲や VDO へ変換する方法といった基本的な質問や、VDO のプロジェクトへ参加したいという意見をいただくなど活発な意見交換が行われ、今後この構想をオープンな枠組みの中で発展させていく足掛かりにすることができました。

この技術はまだ開発の初期段階にありますが、技術開発がすすめば、脆弱性情報コーディネーションプロセスの一部が自動化によって効率化されるばかりでなく、記述の定型化によって脆弱性情報が読みやすいものになる等の効果が期待されます。

"Removing the Pain From the Repetitive Processing of Vulnerability Reports Using a Vulnerability Ontology", Masanobu Katagi (JPCERT/CC, JP), Takayuki Uchiyama (JPCERT/CC, JP), Masaki Kubo (NICT, JP)
https://www.first.org/conference/2018/program#premoving-the-pain-from-the-repetitive-processing-of-vulnerability-reports-using-a-vulnerability-ontology

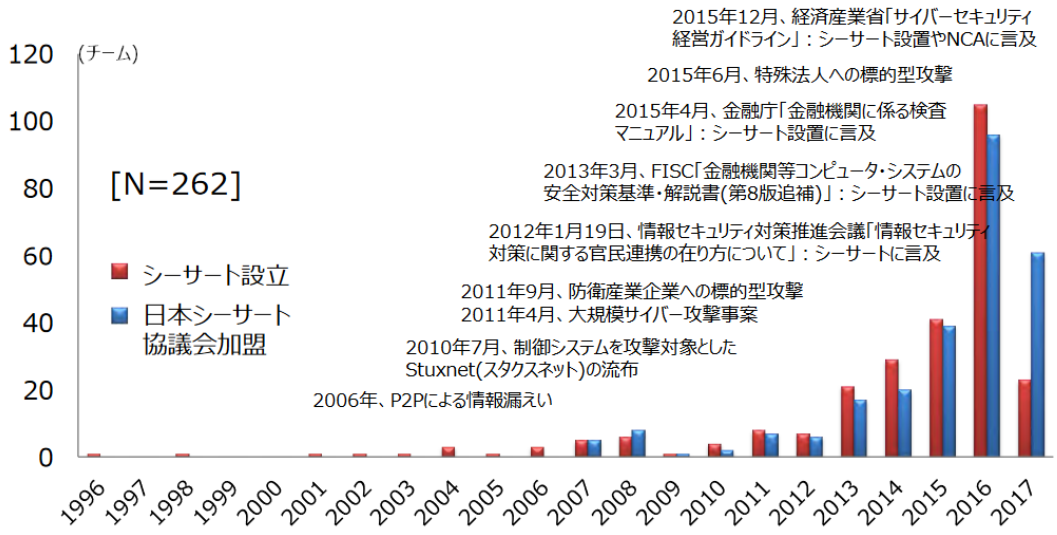
NISTIR 8138 (DRAFT) Vulnerability Description Ontology (VDO): a Framework for Characterizing Vulnerabilities
https://csrc.nist.gov/publications/detail/nistir/8138/draft

ートピック2ー　日本シーサート協議会の加盟会員数が 300 組織に

日本シーサート協議会（NCA：Nippon CSIRT Association）に加盟するシーサート（CSIRT：Computer Security Incident Response Team）の数が 2018 年 6 月末で 300 に達しました。

NCA は、国内の民間の CSIRT が互いに協調し、連携して共通の問題を解決する場をつくるべく 2007 年に設立された協議会です。

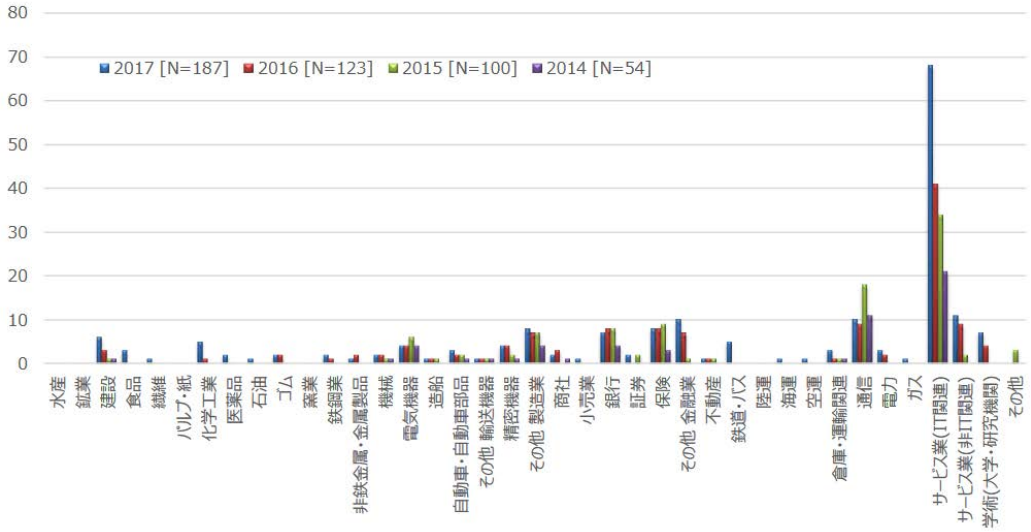
JPCERT/CC を含めた 6 つの CSIRT で活動を開始しましたが、その後、2012 年に情報セキュリティ対策の官民連携のあり方の議論において CSIRT についての言及があったことを契機に、サービス業（IT 関連）、金融業、通信業等の組織内 CSIRT を中心に 2013 年より顕著に加盟が増え始め、2015 年 9 月末には会員数が 100 組織に達しました。さらに、経済産業省が 2015 年に「サイバーセキュリティ経営ガイドライン」を公表し、これに後押しされて、2016 年には約 100 組織の CSIRT を NCA の新たな会員として迎えました。



［NCA 加盟 CSIRT の数の推移］

出典：日本シーサート協議会加盟組織一覧　2017 年版

2017 年 11 月に実施した会員へのアンケートによれば、NCA 加盟組織の業種による内訳は「サービス業（IT 関連）」が約 3 割、続いて金融分野（銀行、証券、保険など）が約 1 割となっています。これ以外の 6 割は多種多様な業種にわたっており、2016 年頃からは大学の CSIRT および鉄道業界の組織内 CSIRT の加盟も増えました。最近では、観光業界と製薬業界のそれぞれからリーディングカンパニーの加盟があり、この 2 つの業界からの加盟も今後増えるものと期待されます。



［NCA 加盟 CSIRT の業種別内訳］

出典：日本シーサート協議会加盟組織一覧　2017 年版

日本シーサート協議会の詳細は、次の URL をご参照ください。

日本シーサート協議会(NCA)

http://www.nca.gr.jp/

本活動は、経済産業省より委託を受け、「平成 30 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、「7.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」、「9.主な講演活動」、「10. 主な執筆」、「11. 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。

JPCERT CC®

目次

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 3,815 件、インシデント件数ベースでは 3,595 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 2,124 件でした。前四半期の 2,203 件と比較して 4%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エ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/2018/IR_Report20180712.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

本四半期に報告をいただいたフィッシングサイトの件数は 1,214 件で、前四半期の 924 件から 31%増加しました。また、前年度同期（736 件）との比較では、65%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の国内・国外ブランド別の件数］

フィッシングサイト	4 月	5 月	6 月	本四半期合計（割合）
国内ブランド	67	85	76	228(19%)
国外ブランド	166	298	258	722(59%)
ブランド不明 (注 5)	78	112	74	264(22%)
全ブランド合計	311	495	408	1,214(100%)

（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。

前四半期に引き続き、特定の国外ブランドのアカウント窃取を目的としたフィッシングサイトに関する報告が非常に多く寄せられており、本四半期における国外ブランドのフィッシング件数の半数以上を占めました。

国内ブランドのフィッシングサイトでは、前四半期と同様に、通信事業者、SNS、金融機関を装ったフィッシングサイトに関する報告が多く寄せられました。通信事業者を装ったフィッシングでは、大手携帯キャリアの複数ブランドを装ったサイトを確認していますが、これらのサイトのドメインを登録したメールアドレスが共通していました。SNS を装ったフィッシングサイトでは.cn ドメインが使用され、金融機関を装ったフィッシングサイトでは、異なる 2 つのブランドで、.club、.top、.xyz のドメインが共通して使用されているという特徴が見られました。

これらの国外、国内ブランドのフィッシングサイトの多くが、正規のブランド名に類似したドメイン名の一部を少しずつ置き換えて、特定のレジストラから次々に取得して利用していました。このようなドメイン登録は、フィッシング目的であろうことを容易に判断できるため、ドメインの登録申請を受けたレジストラが検知し、却下するような運用が望まれます。

フィッシングサイトの調整先の割合は、国内が 30%、国外が 70%であり、前四半期と同じ割合でした。

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、320 件でした。前四半期の 268 件から 19%増加しています。

本四半期は、正規の Web サイトが改ざんされていて、それにアクセスすると、商品の当選を装ってクレジットカード番号などを入力させる、あるいは「マルウエアを検知した」との偽のメッセージを表示するサイトなどに最終的に転送される事例を多数確認しました。こうした不正な転送では、.tk ドメインの URL

を経由する事例を多く確認しています。転送の手法として、ページの最上部に埋め込まれた JavaScript や、ページ内に埋め込まれた難読化された JavaScript など、異なる複数の手口を確認しましたが、転送先 URL のパスには共通のパターンが見られました。また、検索サービスの検索結果から初めて Web サイトにアクセスした時にのみ、.loan ドメインの偽のアンケートサイトに転送が行われるような改ざん事例も多く確認しています。

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、9 件でした。前四半期の 6 件から 50%増加しています。本四半期に対応を依頼した組織は 3 組織でした。

2018 年 4 月初めに、Word 文書を含む zip ファイルが添付された不審なメールに関する報告が寄せられました。Word 文書には、vbs ファイルを作成、実行するマクロが組み込まれており、マクロの実行によってマルウエアがダウンロードされ、最終的にリモートデスクトップツール Ammyy Admin と、通信先からファイルをダウンロードするマルウエアがインストールされることを確認しました。不審メールは、悪用されたメールアカウントから国内のメールサーバを介し送信された可能性がありました。また、vbs ファイルおよび最終的に感染するマルウエアがアクセスする URL のホスト部は、いずれも侵入されて悪用されたと見られる国内 IP アドレスを持つ Web サイトを示していました。不審メールに添付された Word 文書を開くことで Ammyy Admin がインストールされる事例は、2017 年 4 月にも確認されており、今回攻撃に使用された Word 文書のファイル名や、マクロで作成した vbs ファイルを実行する手法などは、以前のものと共通していました。

5 月後半に、標的型攻撃と見られるなりすましメールの報告が寄せられました。メールに添付された zip ファイルにはパスワードがかけられており、展開用のパスワードが別のメールに記載されていました。zip ファイルに含まれている Word 文書を開くと、Windows の VBScript エンジンの脆弱性（CVE-2018-8174）を悪用する攻撃コードがダウンロードされ、マルウエアが実行される仕組みになっていました。CVE-2018-8174 の脆弱性は、2018 年 5 月の Microsoft のセキュリティ更新プログラムで修正されたもので、攻撃者が脆弱性の公表から時を置かずに攻撃に悪用した事例と言えます。攻撃の最終段階で実行されるマルウエアは、C&C サーバから HTTP で命令を受信して動作するボットでした。

JPCERT/CC では、感染拡大の防止や攻撃範囲の特定を目的として、報告元から提供されたマルウエアの分析によって判明した通信先 URL などの情報を関連する組織に共有する取り組みを、報告元の許可を得て行っています。

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、国内の企業ユーザが利用するソフトウエア製品の脆弱性情報、国内のインターネットユーザが影響を受ける可能性のあるコンピュータウイルス、Web サイト改ざん等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脅威情報を多角的に分析し、併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）等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・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 34,000 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 WAISE（Watch and Warning Analysis Information for Security Experts）等を通じて情報提供を行いました。

1.2.1.1. JPCERT/CC からのお知らせ

JPCERT/CC で収集したセキュリティ関連情報のうち、各組織のセキュリティ対策に有用であると判断した情報を「お知らせ」としてまとめ公表しています。本四半期には次のようなお知らせを発行しました。

発行件数：1 件　https://www.jpcert.or.jp/update/2018.html

2018-04-19　長期休暇に備えて 2018/04

1.2.1.2. 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。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 1 件は更新情報）　https://www.jpcert.or.jp/at/

2018-04-06 Cisco Smart Install Client を悪用する攻撃に関する注意喚起 (公開)
2018-04-10 Spring Framework の脆弱性に関する注意喚起 (公開)
2018-04-11 Adobe Flash Player の脆弱性 (APSB18-08) に関する注意喚起 (公開)
2018-04-11 2018 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)
2018-04-16 Drupal の脆弱性 (CVE-2018-7600) に関する注意喚起 (更新)
2018-04-17 Spring Data Commons の脆弱性に関する注意喚起 (公開)
2018-04-18 2018 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)
2018-04-26 Drupal の脆弱性 (CVE-2018-7602) に関する注意喚起 (公開)
2018-05-09 Adobe Flash Player の脆弱性 (APSB18-16) に関する注意喚起 (公開)
2018-05-09 2018 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)
2018-05-15 Adobe Reader および Acrobat の脆弱性 (APSB18-09) に関する注意喚起 (公開)
2018-05-15 メールクライアントにおける OpenPGP および S/MIME のメッセージの取り扱いに関する注意喚起 (公開)
2018-06-08 Adobe Flash Player の脆弱性 (APSB18-19) に関する注意喚起 (公開)
2018-06-13 2018 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)

1.2.1.3. 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抜粋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 88 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。

2018-04-04 IPA が「サイバーレスキュー隊（J-CRAT）技術レポート 2017」を公開
2018-04-11 「TRANSITS Workshop NCA Japan 2018 (夏)」募集開始
2018-04-18 テレワークセキュリティガイドライン（第 4 版）の公表
2018-04-25 長期休暇にそなえて 2018/04
2018-05-09 「Internet Week ショーケース in 広島」参加登録開始のお知らせ
2018-05-16 JNSA が「CISO ハンドブック」を公開
2018-05-23 IPA シンポジウム 2018
2018-05-30 GDPR (一般データ保護規則) が施行
2018-06-06 JPCERT/CC がマルウエア「PLEAD ダウンローダ」に関する分析センターだよりを公開
2018-06-13 フィッシング対策協議会が「フィッシングレポート 2018」を公開

2018-06-20　日本ネットワークセキュリティ協会が「SECCON 2018」の実施計画を公表
2018-06-27　Japan Security Analyst Conference 2019 (JSAC2019) の講演者を募集開始

1.2.1.4. 早期警戒情報

JPCERT/CC では、生活や社会経済活動を支えるインフラ、サービスおよびプロダクト等を提供してい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/

1.2.1.5. CyberNewsFlash

CyberNewsFlash は、情報収集・分析・情報発信を行っている早期警戒グループのメンバーが、最新のインシデント情報、対策情報、情報の読み方などをタイムリーにお届けする情報です。注意喚起とは異なり、発行時点では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　https://www.jpcert.or.jp/newsflash/

2018-04-04　適切なパスワードの設定・管理方法について
2018-04-10　Apache Tomcat のリリースについて
2018-04-11　複数の Adobe 製品のアップデートについて
2018-05-09　複数の Adobe 製品のアップデート (APSB18-12、APSB18-16、APSB18-18) について
2018-05-21　ISC BIND 9 の脆弱性 (CVE-2018-5736、CVE-2018-5737) について
2018-05-24　ネットワーク機器を標的とするマルウェア「VPNFilter」について
2018-06-06　アーカイブファイルの展開処理における脆弱性「Zip Slip」について
2018-06-07　ネットワーク機器を標的とするマルウェア「VPNFilter」について (追加情報)
2018-06-13　OpenSSL の脆弱性 (CVE-2018-0732) について
2018-06-13　ISC BIND 9 の脆弱性 (CVE-2018-5738) 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) 脆弱な Cisco Smart Install Client を悪用する攻撃に関する情報発信

Smart Install は、Cisco 製スイッチの導入時の設定を簡易化するためにイメージ管理等を行う機能です。そのコンポーネントである Cisco Smart Install Client について、2018 年 4 月 5 日 （現地時間）に、Cisco Talos や US-CERT などの複数の組織から情報が公開されました。 Cisco は、2017 年 2 月に、Cisco Smart Install Client の設定不備の問題に関するアドバイザリを公開し、2017 年 3 月には、リモートから任意のコードが実行可能となる脆弱性の情報 (CVE-2018-0171) に関する情報を公開しています。脆弱性の情報 (CVE-2018-0171) については、脆弱性を悪用する攻撃コードが公開されています。JPCERT/CC では、2018 年 4 月 6 日に Cisco Smart Install Client を悪用する攻撃に関する注意喚起を Cisco Smart Install Client が使用する 4786/tcp ポートに対するスキャンの観測結果とともに公開し、Cisco Smart Install Client への対策を呼びかけました。

Cisco Smart Install Client を悪用する攻撃に関する注意喚起
https://www.jpcert.or.jp/at/2018/at180013.html

(2) Drupal の脆弱性に関する情報発信

2018 年 3 月 28 日（現地時間）に Drupal は、リモートから任意のコードが実行可能となる脆弱性 (CVE-2018-7600) に関するアドバイザリ (SA-CORE-2018-002) を公開しました。Drupal はこの脆弱性の Security risk を Highly critical と評価しており、遠隔の第三者によって非公開データの窃取や、システムデータの改変などが行われる可能性があるため、JPCERT/CC では、2018 年 3 月 29 日に Drupal の脆弱性 (CVE-2018-7600) に関する注意喚起を発行し、早期の対策を呼びかけました。さらに、その後に公開された本脆弱性に関する攻撃コードの検証で、Drupal を実行しているユーザ権限内において任意のコードが実行できること、ならびに、本脆弱性を悪用する攻撃のための探索行為と思われるインターネット上のスキャン活動を確認したため、2018 年 4 月 16 日に注意喚起を更新し、改めて早期の対策を呼びかけました。

Drupal の脆弱性 (CVE-2018-7600) に関する注意喚起
https://www.jpcert.or.jp/at/2018/at180012.html

1.3. インターネット定点観測

JPCERT/CC では、インターネット上に複数の観測用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収集する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、既に公開されている脆弱性情報やマルウエア、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努めています。

2007 年以降、TSUBAME の観測用センサーは、海外の National CSIRT 等の協力のもと、国外にも設置しています。JPCERT/CC はセンサーを設置した海外の National CSIRT 等と、国内外の観測データを共同で分析する「TSUBAME プロジェクト」を推進しています。

2018 年 6 月末時点で、海外の 20 の経済地域の 26 組織に観測用センサーの設置への協力をいただいて

います。さらなるセンサー設置地域の拡大と共同分析の深化を目指して、海外の National CSIRT 等に対して TSUBAME プロジェクトへの参加を呼びかけています。

TSUBAME プロジェクトの詳細については、次の Web ページをご参照ください。

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

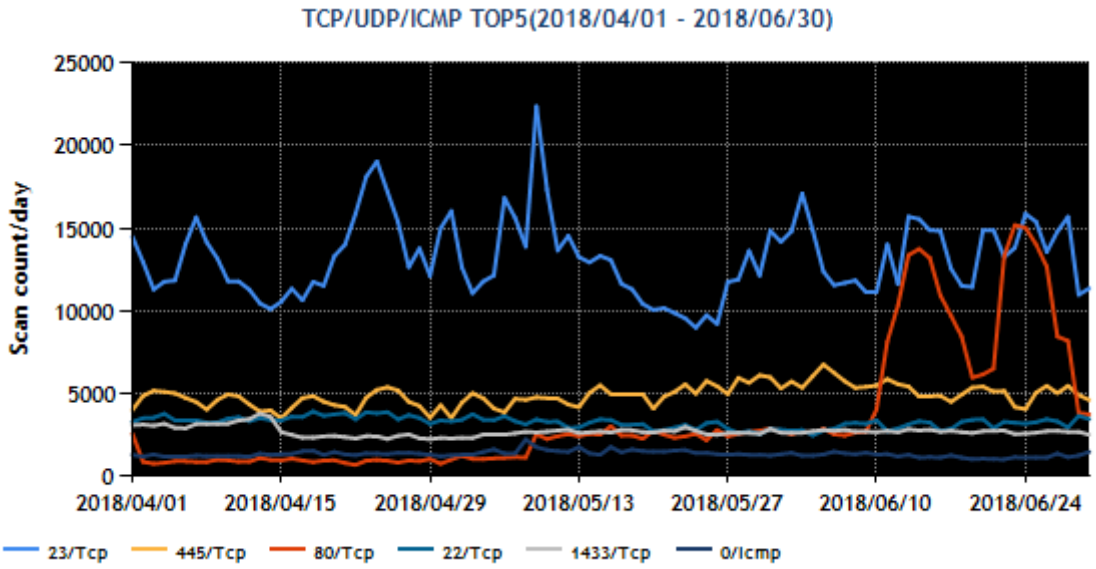
1.3.1. インターネット定点観測システム TSUBAME の観測データの活用

JPCERT/CC では、主に日本企業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、2018 年 1 月から 3 月分のレポートを 2018 年 4 月 26 日に公開しました。

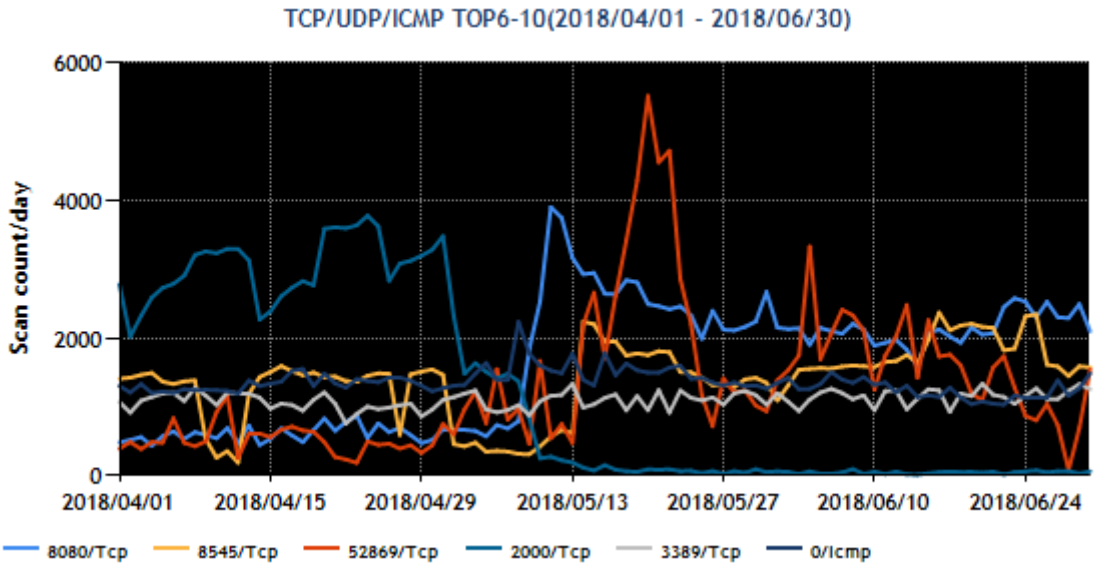
TSUBAME 観測グラフ
https://www.jpcert.or.jp/tsubame/index.html#examples
インターネット定点観測レポート（2018 年 1～3 月）
http://www.jpcert.or.jp/tsubame/report/report201801-03.html

1.3.2. 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。

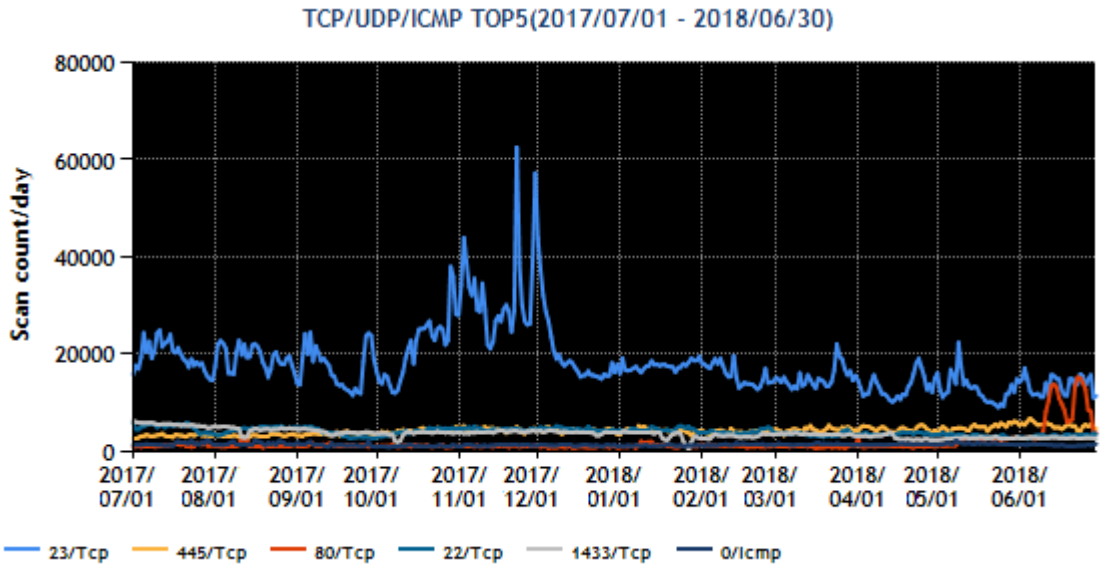


［図 1-1 宛先ポート別グラフ トップ 1-5（2018 年 4 月 1 日-6 月 30 日）］

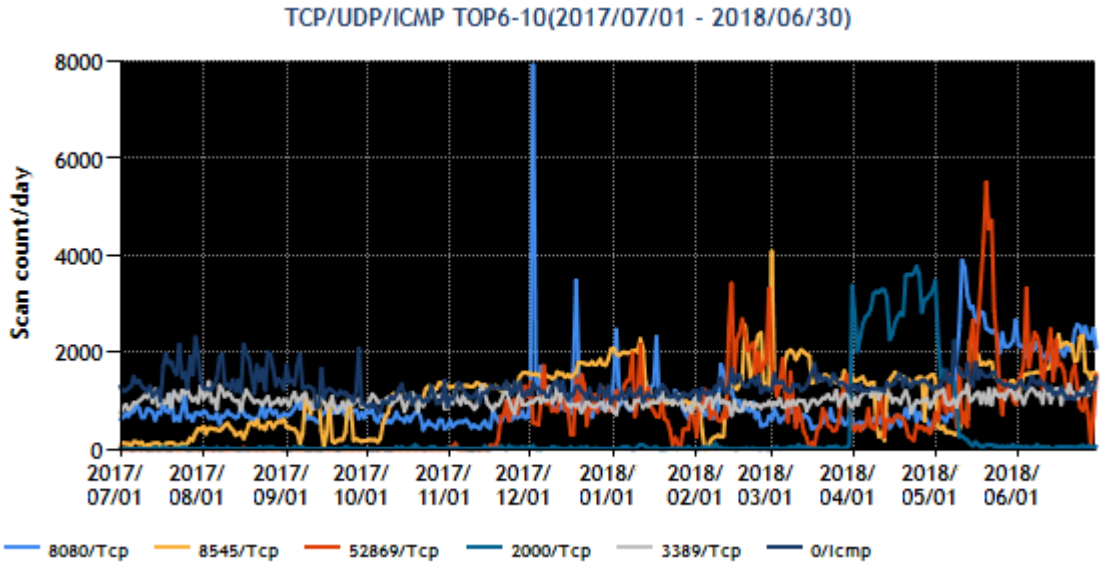


［図 1-2 宛先ポート別グラフ トップ 6-10（2018 年 4 月 1 日-6 月 30 日）］

また、過去 1 年間（2017 年 7 月 1 日-2018 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 1-3］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（2018 年 7 月 1 日-2018 年 6 月 30 日）］



［図 1-4 宛先ポート別グラフ トップ 6-10（2017 年 7 月 1 日-2018 年 6 月 30 日）］

本四半期に観測されたパケットの宛先としては 23/TCP がもっとも多くを占めました。それら 23/TCP 宛のパケットについて、変化の様子を送信元ごとに次に述べます。まず、2017 年 11 月頃から確認され始めた Mirai 等のマルウエアに感染した国内ベンダ製ルータを送信元とするパケットは、その後に対策や機器の入れ替えなどが進み、送信元 IP アドレス数が初めて観測された時期と比較して徐々に減少しているようです。一方、上述のルータ以外の国内機器を送信元とする送信元 IP アドレスについては、機器へのセキュリティ対策が行われる一方、新たに設置された機器が感染する事象が発生しているため、送信元 IP アドレスは入れ替わりつつも減っていません。海外の送信元の IP アドレスを調べると、入れ替わりつつ総数として増加しました。このような送信元の入れ替わりはありましたが、全体としては本四半期も先四半期とほぼ同水準の数のパケットの送信が観測される結果となりました。

1.3.3. TSUBAME 観測データに基づいたインシデント対応事例

JPCERT/CC では、日々TSUBAME の観測情報を分析し、不審なパケットが見つかった場合に、必要に応じて送信元 IP アドレスの管理者に連絡する等の対応を行っています。本四半期における事例として、インターネットに直接接続された TV チューナー（以下「TV box」）のインシデントについて次に述べます。
日本国内の複数の IP アドレスから、Port5555/TCP 宛にパケットを送信する活動が TSUBAME で観測されました。調査を行ったところ、当該 IP アドレスでは Port5555/TCP で通信を待ち受けていることを確認しました。このポートは、Android OS で稼働する機器がデバッグ用の adb コマンドを受け付けるために使用するもので、開発完了後は必要ないものです。攻撃者は、ネットワーク経由で遠隔から接続してデバッグ機能を利用できる機器の探索や、デバッグ機能を利用した攻撃を行っていた可能性が高いと考えられます。当該 IP アドレス全ての管理者に連絡したところ、一部の管理者で TV box 等を直接インターネットに接続した状態で利用していたことがわかりました。プライベート IP アドレス環境下に設置するように環境を変更していただいたところ、当該パケットは観測されなくなりました。デバッグ機能が開いたままの TV box 製品のメーカーや機種は複数あることから、情報収集を継続して行っています。
このように JPCERT/CC では、観測したパケットの分析等を行い、必要に応じて関連する機器の管理者に調査を依頼するなど、感染した機器の発見やマルウエアの駆除等の対策に努めています。

2. 脆弱性関連情報流通促進活動

JPCERT/CC は、ソフトウエ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、用意された対策情報と脆弱性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、脆弱性を作り込まない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。本規程の受付機関に指定されている IPA から届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等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等、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。

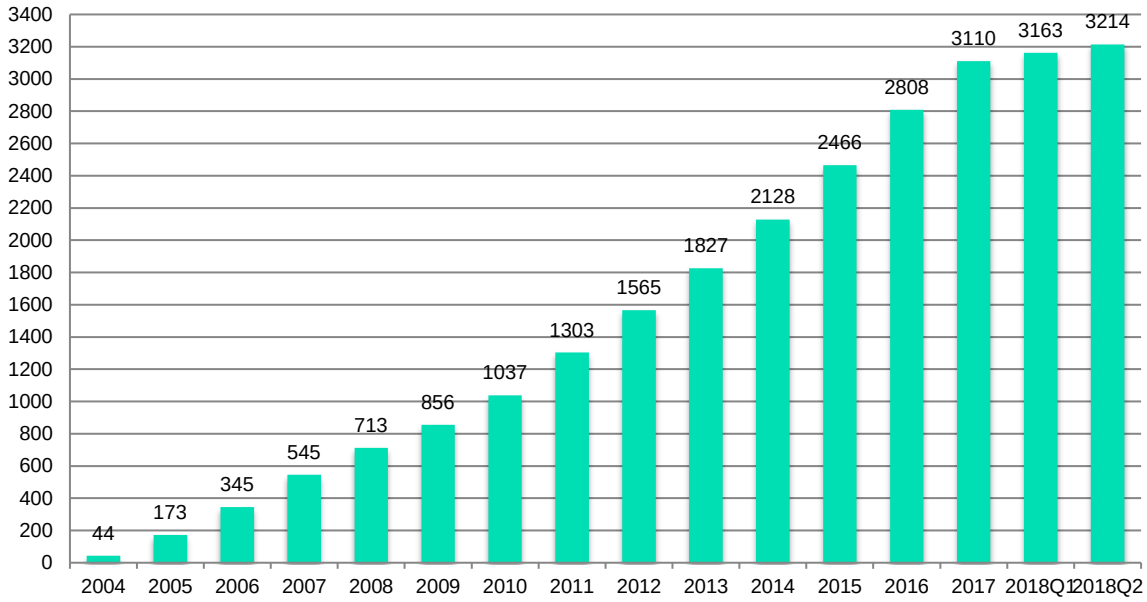
独立行政法人情報処理推進機構（IPA）脆弱性対策
https://www.ipa.go.jp/security/vuln/

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［例えば、JVN#12345678 等］を付与している）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［例えば、JVNVU#12345678 等］を付与している）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 NCSC-FI といった海外の調整機関に届け出ら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 に直接届け出られた自社製品の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 51 件（累計 3,214 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/



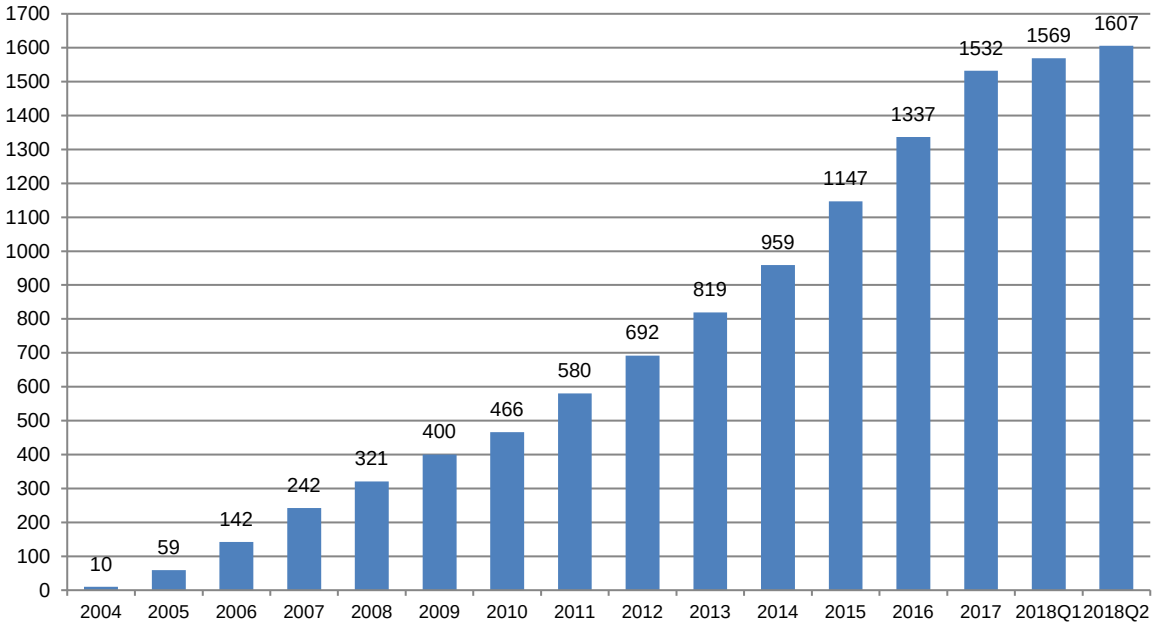
［図 2-1 JVN 公表累積件数］

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 38 件（累計 1,607 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 38 件すべてが単一の製品開発者の製品に影響を及ぼすもので、うち 23 件が国内製品開発者に、残り 15 件は海外の製品開発者に関わるものでした。また、23 件の国内製品開発者の製品に関する脆弱性情報のうち、6 件が自社製品の届出によるものでした。自社製品における脆弱性の届出は年々増加しており、毎四半期に一定数の届出があります。

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の内訳は、［表 2-1］のとおりです。本四半期は前四半期同様に、Windows アプリケーションが 10 件と最も多く、2017 年第 2 四半期から継続して多数公表されています。これは、2010 年に公表された「Windows アプリケーションにおける任意の DLL 読込みの脆弱性」と同類の脆弱性をもつ Windows アプリケーションがあると考えた特定の発見者が、2017 年以降多数の Windows アプリケーションで検証を行い、脆弱性が確認されたものを順次届出たことに起因しています。
次いで本四半期の公表で多数を占めた製品カテゴリは、CMS プラグイン（8 件）と CMS（5 件）でした。これは特定の発見者が、特定の CMS およびそのプラグインについて脆弱性を探索して順次届け出ていることによるものです。

［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内訳］

製品分類	件数
Windows アプリケーション	10
プラグイン	8
CMS	5
組込系	4
グループウエア	3
iOS アプリケーション	2
ウェブアプリケーション	2
Android アプリケーション	1
サーバ製品	1
スマホアプリケーション	1
マルチプラットフォームアプリケーション	1



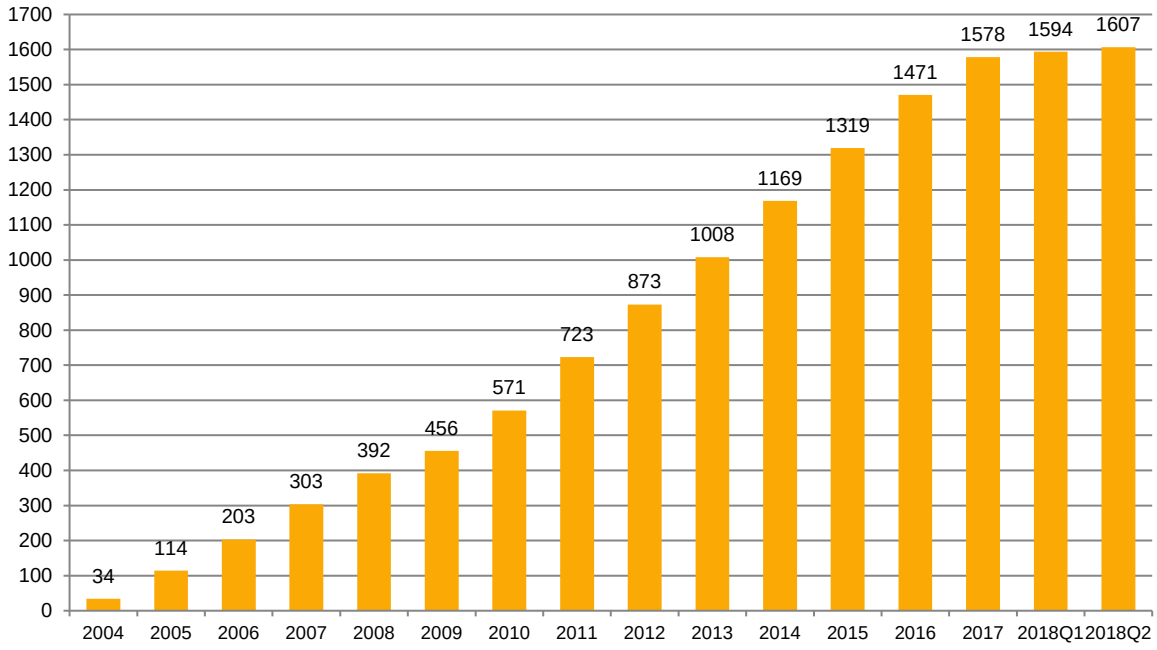
［図 2-2 公表を行った国内取扱脆弱性情報の累積件数］

本四半期に公表した国際取扱脆弱性情報は 13 件（累計 1,607 件）で、累計の推移は［図 2-3］に示すとおりです。

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内訳は、［表 2-2］のとおりです。本四半期は、制御系製品に関するものが 3 件と最も多く、これら 3 件の内訳は、ICS-CERT に届出られた脆弱性情報の国際展開および調整依頼を受け、JPCERT/CC が国内の製品開発者との調整を実施し公表に至ったものが 1 件、自社製品における脆弱性の届出によるものが 2 件でした。
DNS、macOS アプリケーション、Windows 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、サーバ製品といった脆弱性の公表が、合わせて 7 件ありました。
本四半期に公表された脆弱性の特徴として、前四半期に公表をした「JVNVU#93823979 CPU に対するサイドチャネル攻撃」から派生ないしは類似した CPU の実装に関する 3 件の脆弱性が挙げられます。これらの脆弱性は、対象の CPU を利用している幅広いサービスや製品に影響を及ぼすことから、JVN 公表後、JPCERT/CC 製品開発者登録をしている複数の製品開発者へ通知し、ベンダ情報の掲載や情報提供等を呼びかけました。また、13 件中 4 件（先に述べた制御系製品の自社届出 2 件を含む）が、製品開発者自身による脆弱性情報の公表依頼に基づくものでした。
このように、JPCERT/CC では、米国 CERT/CC をはじめとする海外調整機関に届け出られた脆弱性情報の日本国内への展開や調整、製品開発者自身からの告知を目的とした公表依頼の受付など、脆弱性情報の流通、調整および公表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内訳］

製品分類	件数
制御系製品	3
プロトコル実装	3
DNS	2
macOS アプリケーション	2
Windows アプリケーション	1
サーバ製品	1
マルチプラットフォームアプリケーション	1



［図 2-3 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、48 件（製品開発者数で 28 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 203 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、公表できることに 2014 年から制度が改正されました。これまでに、公表判定委員会での審議を経て 11 件（製品開発者数で 8 件）を、JVN の「Japan Vulnerability Notes JP（連絡不能）一覧」に掲載しています。

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の脆弱性情報ハンドリングを行っている米国の CERT/CC、英国の NCSC、フィンランドの CERT-FI、オランダの NCSC-NL などの海外の調整機関と協力関係を結び連携して、それぞれが報告を受けた脆弱性情報の共有、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等の調整活動を行っています。さらに Android 関連製品や OSS 製品の脆弱性の増加に伴い、それらの製品開発者が存在するアジア圏の調整機関、特に韓国の KrCERT/CC や中国の CNCERT/CC、台湾の TWNCERT との連携も増えており、国際連携活動の幅が広がっています。また、米国の ICS-CERT との連携を 2013 年末に正式に開始し、本四半期までに合計 17 件の制御システム用製品の脆弱性情報を公表しています。

JPCERT/CC は、日本における脆弱性ハンドリングのコンタクトポイントとして、脆弱性情報ハンドリングにおける国際的活動を引き続き推進してまいります。

JVN 英語版サイト（https://jvn.jp/en）上の脆弱性情報も、日本語版とほぼ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。

また、JPCERT/CC は、CNA（CVE Numbering Authorities）として認定されています。JPCERT/CC は、本四半期に JVN で公表したもののうち、国内で届出られた脆弱性情報に 70 個の CVE 番号を付与しました。2008 年以降においては、MITRE やその他の組織への確認や照会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 番号が付与されています。

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。

News & Events　“JPCERT/CC Becomes CVE Numbering Authority”
https://cve.mitre.org/news/archives/2010_news.html#jun232010a

CVE Numbering Authorities
https://cve.mitre.org/cve/cna.html

About CVE
https://cve.mitre.org/about/index.html

2.2. 日本国内の脆弱性情報流通体制の整備

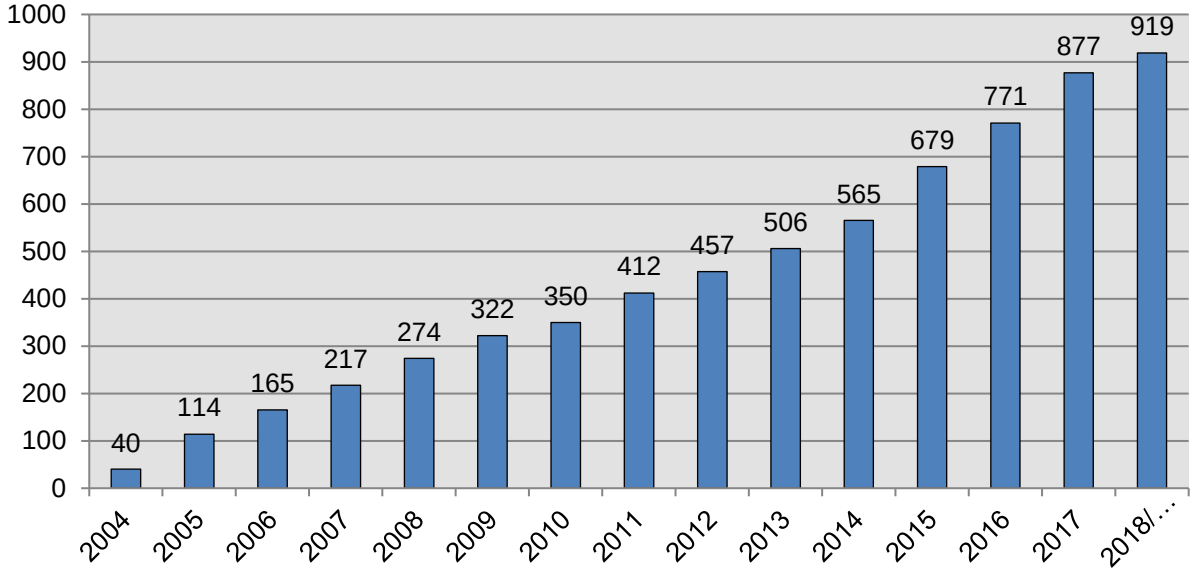
JPCERT/CC では、本規程に従って、日本国内の脆弱性情報流通体制を整備しています。
詳細については、次の Web ページをご参照ください。

脆弱性情報取扱体制
http://www.meti.go.jp/policy/netsecurity/vulhandlingG.html
脆弱性情報コーディネーション概要
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（2017 年版）
https://www.jpcert.or.jp/vh/partnership_guideline2017.pdf
JPCERT/CC 脆弱性情報取扱いガイドライン（2017 年版）
https://www.jpcert.or.jp/vh/vul-guideline2017.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、2018 年 6 月 30 日現在で 919 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/regist.html



［図 2-4 累計製品開発者登録数］

2.3. 脆弱性の低減方策の研究・開発および普及啓発

2.3.1. 講演活動

脆弱性コーディネーショングループでは、脆弱なソフトウエアの解析等を通じて得られた脆弱性やその対策方法に関する知見を、広く一般のソフトウエア開発者の方々に伝えるための活動を行っています。

本四半期は、次の 1 件の講演を行いました。

講演日時: 6 月 26 日
講演タイトル: Removing the Pain From the Repetitive Processing of Vulnerability Reports Using a Vulnerability Ontology
イベント名: 30th Annual FIRST Conference at Kuala Lumpur, Malaysia

ここ数年、情報セキュリティ早期警戒パートナーシップを通じて非常に多くのソフトウエア等の脆弱性関連情報が届けられています。2016 年には 1,000 件を超える届出がありました。このように多くの脆弱性情報の届出が集中した場合、調整機関の処理能力に限界があるため、調整機関がボトルネックとなってしまい、開発者へ脆弱性情報を届けるタイミングが遅れ、結果として脆弱性が修正されない状態が長期化してしまうことが懸念されます。この問題を避けるために、JPCERT/CC では、一部自動化を含む脆弱性コーディネーションプロセスの効率化に向けた検討を開始しています。

着目したポイントは脆弱性情報を共通のフォーマットに基づいて記述するという点です。現状は、届出に記載されている脆弱性情報はフリーフォーマットで記述されており、脆弱性情報の表現が書き手によってさまざまであるため、届出内容を把握・解釈するのに時間がかかります。また、母国語ではない言語で記

述されている場合には、言語の壁も内容理解の障害となります。こうしたフリーフォーマットに起因する問題を解決するため、JPCERT/CC は米国 NIST が提案している Vulnerability Description Ontology (VDO) に基づいた共通言語を用いて脆弱性情報を表現し、それを機械処理することを試みています。

NISTIR 8138 (DRAFT) Vulnerability Description Ontology (VDO): a Framework for Characterizing Vulnerabilities
https://csrc.nist.gov/publications/detail/nistir/8138/draft

手始めに、機械による脆弱性情報の自動処理化を可能にするために、VDO を JSON 形式で表現するモデルを定義しました。また VDO が定義している項目をテキストエディタの補完機能を用いて容易に入力するためのツール環境を開発・整備しています。これらは、次の Github リポジトリで公開し、広く意見を募りながら開発を進めています。

VDO JSON Schema
https://github.com/JPCERTCC/vdo-json-schema

今後は、このデータモデルを用いて VDO から CVSS Base スコアへの自動計算や JVN アドバイザリの自動生成などを実装することで、人手による冗長なプロセスを排除し、一部のコーディネーションプロセスの自動処理を実現することを目指します。

こうした構想の概要を、6 月 24 日から 29 日にかけてマレーシアのクアラルンプールで開催された FIRST（Forum of Incident Response and Security Teams）の第 30 回年次会合で発表しました。本発表は、会合のプログラム中、脆弱性をテーマとするセッションの一つとして位置づけられており、この分野の有識者を含む約 100 名の方が聴講しました。発表後、複数の会議参加者から VDO の適用範囲や VDO へ変換する方法といった基本的な質問や、VDO のプロジェクトへ参加したいという意見などをいただくなど、活発な意見交換が行われ、今後この構想をオープンな枠組みの中で発展させていく足掛かりにすることができました。

［図 2-5 30th Annual FIRST Conference の様子］

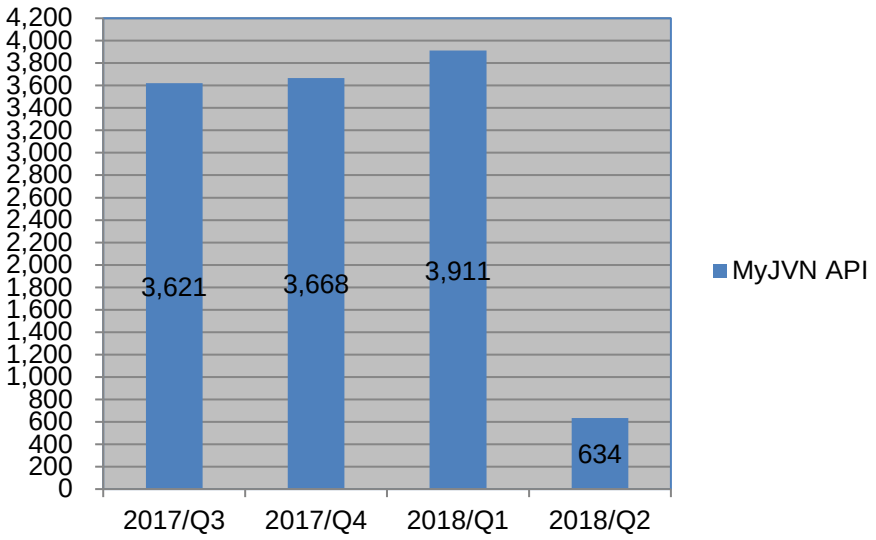
"Removing the Pain From the Repetitive Processing of Vulnerability Reports Using a Vulnerability Ontology", Masanobu Katagi (JPCERT/CC, JP), Takayuki Uchiyama (JPCERT/CC, JP), Masaki Kubo (NICT, JP)
https://www.first.org/conference/2018/program#premoving-the-pain-from-the-repetitive-processing-of-vulnerability-reports-using-a-vulnerability-ontology

2.4. 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。

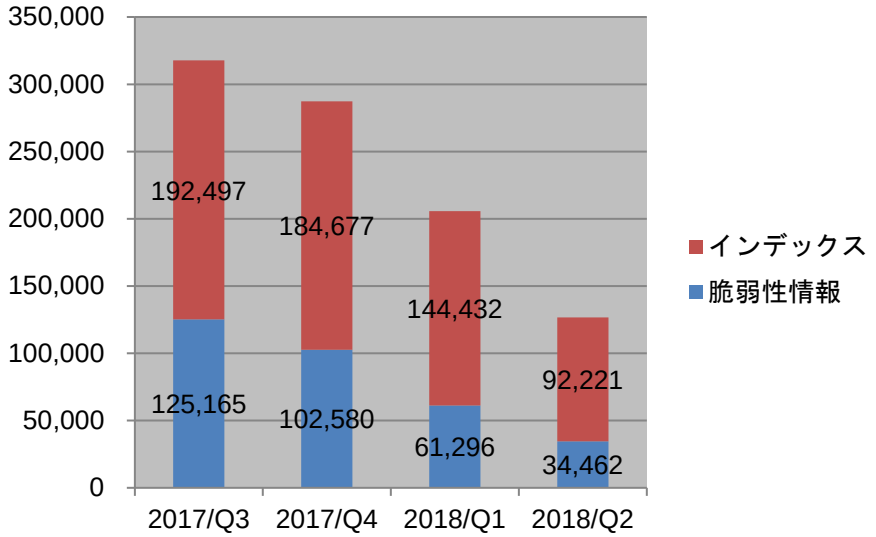
VRDA フィード 脆弱性脅威分析用情報の定型データ配信
https://www.jpcert.or.jp/vrdafeed/index.html

四半期ごとに配信した VRDA フィード配信件数を［図 2-6］に、VRDA フィードの利用傾向を［図 2-7］と［図 2-8］に示します。［図 2-8］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 2-8］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。



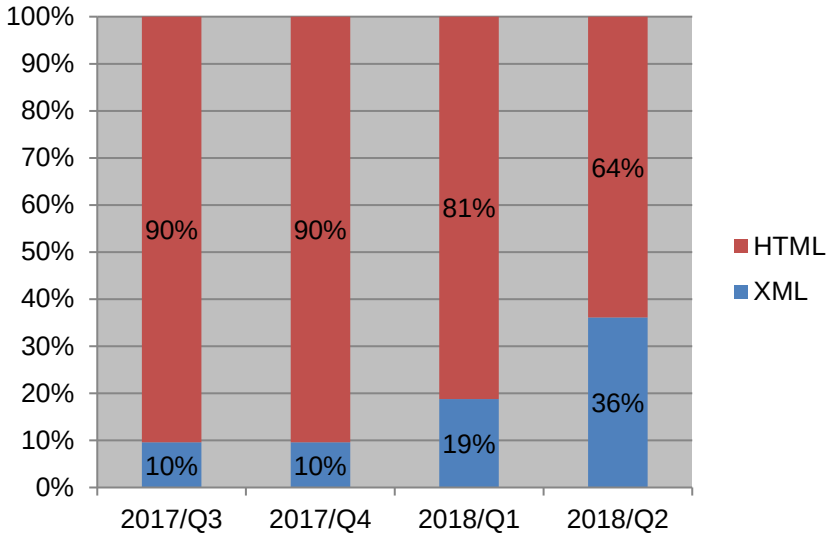
［図 2-6 VRDA フィード配信件数］

VRDA フィード配信件数については、［図 2-6］に示したように前四半期と比較して大幅に減少しています。これは VRDA フィード配信用システムの一部改訂作業において一定期間データ更新の停止が伴ったことが原因です。



［図 2-7 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 2-7］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も、約 44%減少しました。



［図 2-8 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 2-8］に示したように、前四半期と比較し、XML 形式の利用割合が 17%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インシデントに関わる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等を収集・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 541 件でした。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、制御システムセキュリティ情報共有コミュニティ（注 1）に提供しました。

（注 1）JPCERT/CC が運営するコミュニティで、制御システム関係者を中心に構成されています

本四半期に提供した参考情報は 8 件でした。

2018/04/09 【参考情報】Cisco Smart Install Client を使用する攻撃に関する注意喚起
2018/04/17 【参考情報】横河電機株式会社が提供している機器に関する脆弱性
2018/04/23 【参考情報】船舶業界のサイバーセキュリティに関する記事のご紹介
2018/04/27 【参考情報】ホテルのロックシステムに関する脆弱性
2018/05/17 【参考情報】デンマーク国有鉄道へのサイバー攻撃について
2018/05/25 【参考情報】ネットワーク機器を標的とするマルウエア「VPNFilter」について

2018/05/25　【参考情報】米国エネルギー省が「Multiyear Plan for Energy Sector Cybersecurity」を公表

2018/06/14　【参考情報】船舶業界のサイバーセキュリティに関する記事のご紹介

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。本四半期は計 3 件を配信しました。

2018/04/05　制御システムセキュリティニュースレター 2018-0003
2018/05/10　制御システムセキュリティニュースレター 2018-0004
2018/06/06　制御システムセキュリティニュースレター 2018-0005

制御システムセキュリティ情報共有コミュニティには、制御システムセキュリティ情報提供用メーリングリストと制御システムセキュリティ情報共有ポータルサイト ConPaS があり、メーリングリストには現在 845 名の方にご登録いただいています。今後も各サービスの充実を図り、さらなる利用を促進していく予定です。参加資格や申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
https://www.jpcert.or.jp/ics/ics-community.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分野で、インシデント報告の受付、およびインターネットからアクセスできる可能性がある制御システムの探索とそれら制御システムを保有している国内の組織に対する情報提供の 2 つの活動を展開しています。本四半期における活動は次のとおりです。

(1) インシデント報告の受付

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。

(2) インシデント未然防止活動

SHODAN をはじめとするインターネット・ノード検索システムで公開されている情報を分析し、インターネットから不正にアクセスされる危険性のある制御システム等が含まれていないかを調査しています。本四半期に発見した 10 件（57 IP アドレス）のシステムの情報を、それぞれのシステムを保有する国内の組織に対して提供しました。

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 に関して 2 件の利用申し込みがあり、直接配付件数の累計は、日本版 SSAT が 260 件となりました。

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

4.1. 海外 CSIRT 構築支援および運用支援活動

海外の National CSIRT（Computer Security Incident Response Team）等のインシデント対応調整能力の向上を図るため、研修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。本四半期は新規の研修教材の開発を進めました。

4.1.1. アフリカ CSIRT 構築支援（5 月 3 日- 4 日）

情報セキュリティに関する制度や技術が整備されていない国・地域等からのサイバー攻撃も日本のインターネットユーザの脅威の一つとなります。急速なインターネット普及が予想されるアフリカ地域に関連するインシデントの増加に備え、迅速かつ円滑な対応ができるよう、同地域におけるインシデント対応のための人材育成と連携の基盤づくりを目的に、JPCERT/CC では 2010 年から CSIRT の構築・運営とそれらを支える人材の育成に取り組んできました。
その一環として本四半期においては、セネガルの首都ダカールで開催された Africa Internet Summit（AIS）'18 に参加しました。AIS は AfNOG（African Network Operators' Group）と AFRINIC（The African Network Information Centre）が共同で主催する、アフリカのインターネットの発展に携わる産官学の実務

者を対象としたイベントで、アフリカの ICT における技術動向や政策等に関して、現状や課題を国際コミュニティとともに協議することを目的に 2013 年から毎年開催されています。今年は 4 月 29 日から 5 月 11 日にかけて開催されました。

JPCERT/CC は、AfNOG のメンバーである AfricaCERT（Africa Computer Emergency Response Teams）から依頼を受けて、AIS '18 の期間中の 5 月 3 日にインシデントレスポンストレーニング、4 日に OSINT と Web 改ざんインシデント対応のためのトレーニングを行いました。本トレーニングには、セネガル、ガーナ、ナイジェリアなどから約 40 名が参加しました。

［図 4-1　OSINT トレーニング風景］

AIS'18 および AfricaCERT の詳細については、次の Web ページをご参照ください。

Africa Internet Summit '18
https://www.internetsummit.africa/

AfricaCERT
https://www.africacert.org/home/

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、2003 年 2 月の APCERT 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、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 18 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。JPCERT/CC の国際部マネージャー 小宮山功一朗が FIRST の理事※として、組織運営に関わる議論に参画しました。また不定期に開催されるシンポジウムの準備調整を進めました。

※JPCERT/CC の小宮山は FIRST 理事として二期目の任期を終え、6 月 26 日に開催された FIRST 年次総会をもって理事を退任。

FIRST と理事業務の詳細については、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. 30th Annual FIRST Conference Kuala Lumpur への参加（6 月 25 日- 29 日）

第 30 回 FIRST 年次会合が 6 月 25 日から 29 日にかけてマレーシアの首都クアラルンプールで開催されました。本会合は、サイバーインシデントの予防、対応、技術分析等に関する最新動向の情報交換およびインシデント対応チームの連携強化を目的に毎年開催されています。今年は 68 の国と地域から約 830 名が参加しました。

JPCERT/CC は、6 月 26 日に” Removing the Pain From the Repetitive Processing of Vulnerability Reports Using a Vulnerability Ontology”と題して、脆弱性情報の記述に関する業務効率化の手法について発表しました。この中で、脆弱性情報の記述の書式である VDO による記述の平準化や VDO による記述を支援する JSON Scheme について紹介しました。

さらに、この機会を利用し、世界各国の National CSIRT や製品ベンダの CSIRT 等と個別に意見を交換するとともに、脆弱性ハンドリングや情報交換ポリシー等に関する SIG（Special Interest Group）やアジア太平洋地域の National CSIRT の集いに参加し、各分野の活動について情報を共有しました。このような会合への参加を通した、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 30 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。

30th Annual FIRST Conference San Juan
https://www.first.org/conference/2018

4.2.2.2. National CSIRT Meeting 参加（6 月 29 日- 30 日）

第 30 回 FIRST 年次会合に引き続き、米国 CERT/CC が主催する National CSIRT Meeting（NatCSIRT）2018 がマレーシアのクアラルンプールで開催されました。本会合は、世界各国の National CSIRT が一堂に会し、国を代表するインシデント対応チームとしての活動計画や課題を共有し、開発ツールや共同プロジェクト、調査研究等に関して発表や議論することを目的に毎年開催されております。JPCERT/CC は、” New Mirai Botnet Case Study in Japan: Investigation through Open Ports”と題した講演を行い、日本における Mirai ボットの対策から得た教訓を共有しました。NatCSIRT についての詳細は、次の Web ページをご参照ください。

NatCSIRT 2018
https://www.cert.org/natcsirt/

4.2.3. AusCERT 2018 参加 （5 月 29 日- 6 月 1 日）

JPCERT/CC は 5 月 29 日から 6 月 1 日にかけてオーストラリアのゴールドコーストで開催された AusCERT 2018 に参加し、”Tracking APT Lateral Movement with Audit Policy and Sysmon”と題した講演を行いました。標的型攻撃の際にみられる横断的侵害を効率的に検知するため、攻撃者が頻繁に用いるツールやログから攻撃の実行痕跡を読み解く方法について解説しました。AusCERT 2018 の詳細は、次の Web ページをご参照ください。

AusCERT 2018
https://conference.auscert.org.au/

4.3. CyberGreen

国際的なプロジェクトである CyberGreen は、指標を用いて各国／地域インターネット全体の健全性を評価して比較し、各国の CSIRT や ISP、セキュリティベンダーが、関連する指標値を向上させる施策についてグッド・プラクティスを学びあい、目標を明確化することを通じて、より効率的に健全なサイバー空間を実現することを目的としています。2015 年 11 月に設立された国際 NPO である CyberGreen Institute がプロジェクトの中心を担っています。前四半期より、JPCERT/CC は、CyberGreen Institute が収集したデータに対し、検索条件や抽出方法の改善などデータを利用する立場から提案を行っていますが、本四半期においても継続して提案を行いました。

CyberGreen Institute
https://www.cybergreen.net/

4.3.1. 第 118 回 MPS・第 54 回 BIO 合同研究発表会への参加

情報処理学会の第 118 回 MPS・第 54 回 BIO 合同研究発表会が平成 30 年 6 月 13 日から 15 日まで沖縄科学技術大学院大学メインキャンパスで開催され、この中で JPCERT/CC は「ccTLD 別 UDP リフレクタ数の指標化と分析」と題する講演を行い、Mejiro の指標の概念を説明・提案しました。
Mejiro の指標がこのような理論構成を背景にしていることを学会で公開することで、専門家の方々から厳しいご指摘やご批判を得ることができ、今後の課題を明らかにすることができました。

情報処理学会 第 118 回 MPS・第 54 回 BIO 合同研究発表会
https://www.ipsj.or.jp/kenkyukai/event/mps118bio54.html

4.4. その他国際会議への参加

4.4.1. The Global Commission on the Stability of Cyberspace（GCSC）への参加（5 月 18 - 21 日）

2017 年 3 月にサイバー空間における規範を議論する場として The Global Commission on the Stability of Cyberspace (GCSC) が立ち上がりました。その中には技術、法律、インターネットガバナンスなどの分野ごとにオープンな議論を行うことを目的とする 4 つのワーキンググループが設けられています。JPCERT/CC の小宮山が技術ワーキンググループの副議長として、メーリングリストでの議論や調査の仕様作成などを行っています。2018 年 5 月に専門家による会合に小宮山が参加し、議論に参加しました。次の GCSC のページで公開されているとおり、委員会は本会合で選挙や国民投票のためのデジタルインフラへのサイバー攻撃を禁止するという規範を提案しました。

The Global Commission on the Stability of Cyberspace (GCSC)
https://cyberstability.org/

4.4.2. RSA Conference 2018 への参加（4 月 16 日- 20 日）

JPCERT/CC は、4 月 16 日から 4 月 20 日にかけてアメリカ合衆国のサンフランシスコで開催された RSA Conference 2018 に参加し、セキュリティ業界動向、最先端の脅威動向、脅威分析手法に関する情報を収集しました。イベントの詳細は、次の Web ページをご参照ください。

RSA Conference 2018
https://www.rsaconference.com/events/us18

4.4.3. CyCON X Workshop, CyCON 2018 への参加（5 月 29 日- 6 月 1 日）

JPCERT/CC は、5 月 29 日から 6 月 1 日にかけてエストニアのタリンで開催された CyCON X Workshop および CyCON 2018 に参加し、サイバー防護に関する政策や法整備、インフラ防護の技術、サイバー関連の国際法等について、情報を収集しました。イベントの詳細は、次の Web ページをご参照ください。

CyCON 2018
https://ccdcoe.org/cycon/

4.4.4. 海外 CSIRT 等の来訪および往訪

4.4.4.1. aeCERT 往訪（5 月 9 日）

aeCERT（アラブ首長国連邦緊急対応チーム）を往訪し、今後の協力関係等について議論を行いました。また、Mejiro の観測結果をもとにして、ポート番号 445 に関する同国の Mejiro 指標に改善の余地があること、すなわち、ポート番号 445 をインターネットに向けて解放している機器が同国に多数あることと、同国から日本に対してポート番号 445 へのスキャンパケットが多く送信されていることの 2 点の事実を示しました。それに関連すると推測されるマルウエア感染について説明するとともに、アラブ首長国連邦に TSUBAME センサーの設置を打診しました。

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）で検討されている脆弱性の開示と取り扱いに関する標準の改定と、WG4（セキュリティコントロールとサービス）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。

4 月 16 日から 20 日にかけて中国の武漢市で標準化会議が開催されましたが、脆弱性の開示（ISO/IEC 29147）についても脆弱性の取扱手順（ISO/IEC 30111）についても、会議までに改定草案をプロジェクト・エディタが用意できなかったため、議論を進めることができませんでした。こうした状況を改善すべく、副のプロジェクト・エディタが 1 名追加されることが決まり、6 月になってから脆弱性の開示（ISO/IEC 29147）の改定草案が国際事務局から配布されました。

4.6. ブログや Twitter を通した情報発信

英語ブログ（https://blog.jpcert.or.jp/）や Twitter（@jpcert_en）を通して、日本やアジア太平洋地域の情報セキュリティに関する状況や JPCERT/CC の活動等について英文による情報発信を継続して行っています。本四半期は次の記事をブログに掲載しました。

JPCERT/CC Publishes "Vulnerability Coordination and Disclosure Policy"（4 月 27 日）
https://blog.jpcert.or.jp/2018/04/jpcertcc-publishes-vulnerability-coordination-and-disclosure-policy.html

How to Describe Vulnerability Information? （6 月 5 日）
https://blog.jpcert.or.jp/2018/06/how-to-describe-vulnerability-information.html

PLEAD Downloader Used by BlackTech（6 月 8 日）
https://blog.jpcert.or.jp/2018/06/plead-downloader-used-by-blacktech.html

5. 日本シーサート協議会（NCA）事務局運営

5.1. 概況

日本シーサート協議会（NCA：Nippon CSIRT Association）は、国内のシーサート（CSIRT：Computer Security Incident Response Team）組織が互いに協調し、連携して共通の問題を解決する場として 2007 年に設立されました。その事務局として、JPCERT/CC は、NCA の Web サイトの管理や更新を通じた広報活動、協議会の問合せ窓口やメーリングリストを含む会員情報の管理、加盟のためのガイダンスの実施および手続きの運用を担当するとともに、自らも会員として協議会の活動に参加しています。さらに、2016 年 8 月からは JPCERT/CC 職員（山本 健太郎）が NCA の運営委員にも就任しています。

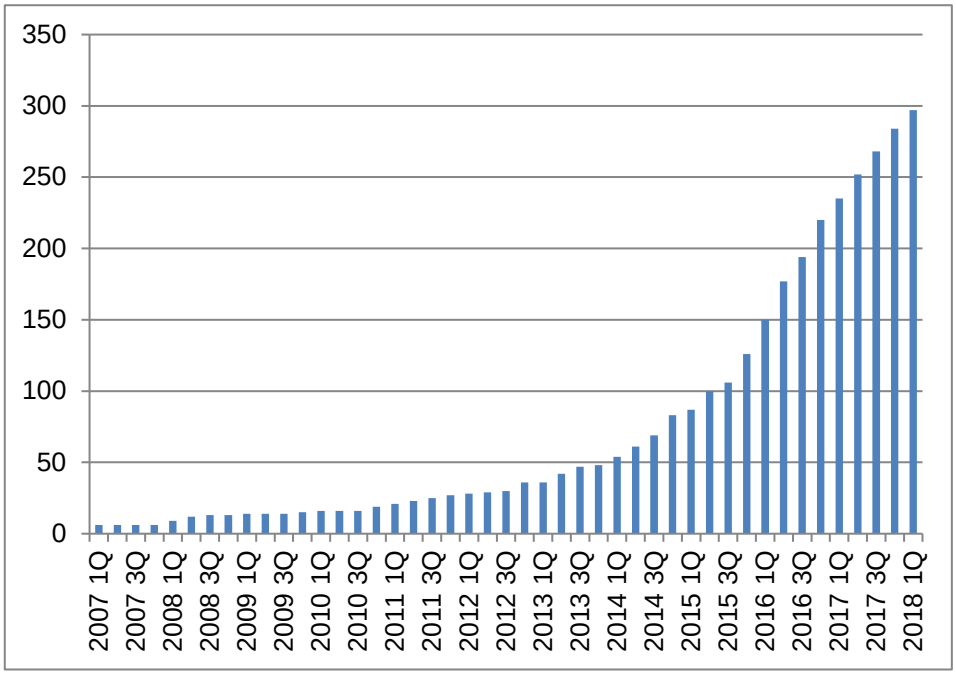
本四半期には、次の 13 組織（括弧内はシーサート名称）が新規に NCA の一般会員となりました。

株式会社 西武ホールディングス (SEIBU-CSIRT)
北陸通信ネットワーク株式会社 (HT-CSIRT)
国立大学法人 宮崎大学 (Miyadai-CSIRT)
アビームコンサルティング株式会社 (ABeam-CSIRT)

株式会社ハンモック (Hammock-CSIRT)
フジテック株式会社 (FUJITEC-CSIRT)
静岡ガス・システムソリューション株式会社 (SG-CSIRT)
株式会社デンソー (DENSO SIRT)
クオリティソフト株式会社 (QSIRT)
株式会社 アミューズ (AMUSE-SIRT)
株式会社 TSUTAYA (TSUTAYA-SIRT)
株式会社ジンズ (JINSIRT)
公益財団法人　東京都保健医療公社 (TMHH-CSIRT)

本四半期末時点で※297（一般会員 296、協力会員 1）の組織が加盟しています。これまでの参加組織数の推移は［図 5-1］のとおりです。

※集計は協議会 Web の掲載時期をもとに実施。実際の加盟承認時期と若干のタイムラグが生じる場合があります。



［図 5-1 日本シーサート協議会 加盟組織数の推移］

5.2. 第 21 回シーサートワーキンググループ会

第 21 回シーサートワーキンググループ会を次のとおり開催しました。

日時：2018 年 6 月 8 日
場所：京都リサーチパーク

シーサートワーキンググループ会は、NCA の会員および NCA への加盟を前提に組織内シーサートの構築を検討している組織が参加する会合です。会合では、各ワーキンググループからの活動報告や、新しく加盟した 8 チームによる自組織のシーサートの概要紹介に加えて、次の講演が行われました。

演題 1 ：「FIRST CSIRT Framework Version 1.1」
講演者：NCA 教育コンテンツ STF　専門委員 石塚 元 氏

演題 2 ：「証拠保全の実践 - Web サーバが侵害された時にどうする？」
講演者：特定非営利活動法人デジタル・フォレンジック研究会「証拠保全ガイドライン」改訂ワーキンググループ委員　大徳 達也 氏

5.3. 日本シーサート協議会　運営委員会

本四半期は、次のとおり計 3 回の運営委員会を開催しました。

第 131 回運営委員会
開催日時：2018 年 4 月 25 日（水）16:00 - 18:00
開催場所：JPCERT/CC

第 132 回運営委員会
開催日時：2018 年 5 月 23 日（水）10:00 - 12:00
開催場所：TMC-SIRT

第 133 回運営委員会
開催日時：2018 年 6 月 20 日（水）16:00 - 18:00
開催場所：JSOC

日本シーサート協議会の活動の詳細については、次の Web ページをご参照ください。

日本シーサート協議会
http://www.nca.gr.jp/

6. フィッシング対策協議会事務局の運営

JPCERT/CC は、フィッシング対策協議会（本節の以下において「協議会」）の事務局を担当しており、経済産業省からの委託により、協議会における各ワーキンググループ活動の運営や、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、報告に基づいたフィッシングサイトに関する注意喚起等の活動を行っています。また、協議会が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、サイトを停止するための調整をインシデント対応支援活動の一環として行っています。

6.1 情報収集 / 発信の実績

6.1.1 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ニュースや緊急情報を計 29 件（ニュース：15 件、緊急情報：14 件）発信しました。

前四半期に引き続き、Apple や Amazon、大手クレジットカード会社などをかたりクレジットカード情報を詐取するフィッシングについて、多くの報告が寄せられました。特に Apple をかたるフィッシングが、同じ文面、URL で大量に何度も配信され、本四半期における報告数全体の約 57%を占めました。
また LINE をかたるフィッシングについては、数日おきに URL を変えて新たなフィッシングサイトが稼働しており、報告数が増加しました。また、仮想通貨関連サービス（bitFlyer、MyEtherWallet）をかたるフィッシングの報告も 5 月頃より多く寄せられるようになりました。
利用者数が多く影響範囲も大きい報告については、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。その件数と内訳は次のとおりです。

Apple をかたるフィッシング：3 件
MUFG カードをかたるフィッシング 2 件
セゾン Net アンサーをかたるフィッシング：2 件
Amazon をかたるフィッシング：2 件
Apple および Amazon をかたるフィッシング：1 件
LINE をかたるフィッシング：1 件
bitFlyer をかたるフィッシング：1 件
MyEtherWallet 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

本四半期の特筆すべきフィッシング事案として、MyEtherWallet をかたるフィッシングがありました。これまで仮想通貨関連サービスをかたったフィッシングは単発的で長く続くことはありませんでしたが、本事案は 5 月初旬の報告以来、6 月にかけて URL が異なるフィッシングの報告が継続的に寄せられています。またフィッシングメールの本文には、おそらくはメールフィルタ回避を目的に、HTML 形式表示では表示されない、さまざまな文の断片をランダムに羅列して埋め込んでおり、しかもそれを毎回変えるといった手法が使われていました。MyEtherWallet は仮想通貨イーサリアムのウォレットで、日本語の情報も豊富で国内ユーザも多いと思われるため、今後も注意が必要です。

［図 6-1 MyEtherWallet をかたるフィッシングサイト ］

https://www.antiphishing.jp/news/alert/myetherwallet_20180515.html

6.1.2　ガイドライン策定ワーキンググループの成果物の公開

6 月 4 日、協議会 Web ページにおいて「フィッシングレポート 2018」「フィッシング対策ガイドライン 2018 年度版」「利用者向けフィッシング詐欺対策ガイドライン　2018 年度版」を公開しました。これらのレポートおよびガイドラインは、フィッシングの被害状況、フィッシングの攻撃技術・手法やその対策方法などをとりまとめた文書で、協議会のガイドライン策定ワーキンググループが毎年改訂しています。

「フィッシングレポート 2018」
https://www.antiphishing.jp/report/wg/phishing_report2018.html

「フィッシング対策ガイドライン 2018 年度版」
https://www.antiphishing.jp/report/guideline/antiphishing_guideline2018.html

「利用者向けフィッシング詐欺対策ガイドライン　2018 年度版」
https://www.antiphishing.jp/report/guideline/consumer_guideline2018.html

6.2. 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ウイルス対策ソフト等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に該当する協議会の会員に対し、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 34 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進める予定です。

6.3. 講演活動

協議会ではフィッシングの動向を紹介し、効果的な対策を呼び掛ける講演活動を行っています。本四半期は次の講演を行いました。

(1) 駒場 一民（エンタープライズサポートグループ　情報セキュリティアナリスト）
eCrime 2018
日程：2018 年 5 月 17 日
講演タイトル：「Phishing Trend in Japan and the Counteraction taken as the Council of Anti-Phishing Japan」

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/

2018 年 4 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201804.html
2018 年 5 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201805.html

7. 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活動を、運営委員会の決定に基づいて行っています。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。

7.1 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 61 回運営委員会
日時：2018 年 4 月 13 日 16:00 - 18:00
場所：GMO グローバルサイン株式会社

第 62 回運営委員会
日時：2018 年 6 月 13 日 16:00 - 18:00
場所：エヌ・ティ・ティ・コミュニケーションズ株式会社

7.2 総会開催

本四半期においては、総会を次のとおり開催いたしました。

日時：2018 年 6 月 28 日 15:00 - 17:20
場所：エッサム神田ホール 2 号館

7.3 ワーキンググループ会合開催支援

本四半期においては、次のとおり開催された協議会のワーキンググループの会合の開催の支援と参加を行いました。

証明書普及促進ワーキンググループ会合
日時：2018 年 5 月 29 日 16:00 - 18:00
場所：JPCERT/CC

8. 公開資料

JPCERT/CC が本四半期に公開した調査・研究の報告書や論文、セミナー資料は次のとおりです。

8.1. 脆弱性関連情報に関する活動報告レポート

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。
本レポートは、この制度の運用に関連した前四半期の活動実績と、同期間中に届出ないし公表された脆弱性に関する注目すべき動向についてまとめたものです。

ソフトウエア等の脆弱性関連情報に関する届出状況[2018 年第 1 四半期（1 月～3 月)]
（2018 年 4 月 25 日）
https://www.jpcert.or.jp/press/2018/vulnREPORT_2018q1.pdf

8.2. 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、マルウエ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。
本レポートは、インターネット定点観測の結果を四半期ごとにまとめたものです。

インターネット定点観測レポート(2018 年 1～3 月)
（2018 年 4 月 26 日）
https://www.jpcert.or.jp/tsubame/report/report201801-03.html
https://www.jpcert.or.jp/tsubame/report/TSUBAMEReport2017Q4.pdf

8.3. 分析センターだより

JPCERT/CC では、インシデントに関連して収集または報告いただいた情報をもとに、攻撃に用いられた手法やその影響を把握するため、アーティファクトの調査・分析を行っています。また、分析技術の普及や技術者の育成にも努めており、その一環として日々のアーティファクト分析業務の中で感じたこと、発見したことを「分析センターだより」として発信しています。本四半期においては次の 2 件の記事を公開しました。

(1) 攻撃グループ BlackTech が使うマルウエア PLEAD ダウンローダ(2018-05-28)

本記事では、日本の組織をターゲットとして標的型攻撃を行っていることを確認している攻撃グループ Blacktech が使用していると考えられるマルウエア PLEAD ダウンローダと、それがメモリ上に読み込むモジュールの挙動や通信の特徴などを解説しています。なお、同グループが使用しているマルウエア TSCookie については 2018 年 3 月 1 日に発行した分析センターだよりで紹介しました。

攻撃グループ BlackTech が使うマルウエア PLEAD ダウンローダ
https://www.jpcert.or.jp/magazine/acreport-linopid.html

(2) Linux と Windows を狙うマルウエア WellMess(2018-06-28)

マルウエア「WellMess」は国内の組織で感染が報告されており、Windows だけでなく Linux サーバなどでも動作していることが確認されています。本記事では WellMess の挙動の概要や C2 サーバへの通信リクエストの特徴などを解説しています。また、WellMess 通信内容をデコードするツールも公開していますので、記事と合わせてご活用ください。

Linux と Windows を狙うマルウエア WellMess(2018-06-28)
https://www.jpcert.or.jp/magazine/acreport-wellmess.html

9. 主な講演活動

(1) 森崎 樹弥（早期警戒グループ）：
「高度化するサイバー攻撃の脅威と対策」
長野県インターネットプロバイダ防犯連絡協議会総会・研修会,2018 年 4 月 27 日

(2) 佐藤 祐輔（エンタープライズサポートグループ）：
「机上演習から見えてくる企業のサイバーインシデント対応戦略」
IPA 情報セキュリティ EXPO，2018 年 5 月 9 日

(3) 戸田 洋三（脆弱性コーディネーショングループ）：
「第 3 回 セキュアコーディング,その重要性」「第 4 回 セキュアコーディング,実践」
国立情報学研究所 トップエスイー セキュリティ概論，2018 年 5 月 15 日

(4) 竹田 春樹（分析センター マネージャー）：
「インシデント対応ハンズオン for ショーケース」
Internet Week ショーケース in 広島,2018 年 6 月 1 日

(5) 川居 裕人（早期警戒グループ）：
「最近のサイバー攻撃の傾向とその対策」
青森県インターネットプロバイダ防犯連絡協議会，2018 年 6 月 11 日

(6) 佐々木 勇人（早期警戒グループ）：
「「情報共有」なぜできない？なぜできる？」
Interop Tokyo 2018，2018 年 6 月 14 日

10. 協力、後援

本四半期は、次の行事の開催に協力または後援をしました。

(1) InternetWeekショーケースin広島
主　催：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：2018年5月31日～6月1日
(2) IPAシンポジウム2018
主　催：IPA 独立行政法人 情報処理推進機構
開催日：2018年6月8日
(3) Interop Tokyo 2018
主　催：Interop Tokyo 実行委員会
開催日：2018年6月13日～6月15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のお問い合わせ　：seminar-secure@jpcert.or.jp
■公開資料、講演依頼、資料使用、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