JPCERT-PR-2018-04
発行日 : 2018-10-16

JPCERT/CC 活動概要 [2018 年 7 月 1 日 ～ 2018 年 9 月 30 日]

活動概要トピックス

ートピック1ー　ランサムウエアの脅威動向および被害実態調査報告書を公開

JPCERT/CC が主に日本国内におけるランサムウエアの実態をまとめた「ランサムウエアの脅威動向および被害実態調査報告書」を 7 月 30 日に公開しました。

ランサムウエアの感染手口や攻撃手法は年々変化を遂げています。従来のランサムウエアは、メールを開く、あるいは改ざんされた Web サイトにアクセスする等の利用者側の行為によって伝染するものが大多数でしたが、2017 年以降は WannaCrypt（WannaCry）のような自己伝染機能を持つものが登場し、短時間のうちに世界各地で多数のコンピュータが感染するパンデミック（爆発的流行）を生じさせました。さらに、身代金を要求しているように見せかけつつもシステムを破壊する、または標的型攻撃の痕跡調査をかく乱することに真の目的があると見られるランサムウエアも確認されています。

JPCERT/CC では、国内の法人組織におけるランサムウエアの被害実態を明らかにするためのアンケート調査を 2017 年度に実施しました。その結果、35%の組織がランサムウエアに感染した経験をもち、ランサムウエアにより暗号化されたデータを復元できなかった組織も 16%あったこと等が明らかになりました。本報告書では、こうしたアンケート調査結果とその分析考察に加えて、ランサムウエアの感染経路や、国内における感染リスク拡大の背景、脅威動向などをまとめています。

ランサムウエアの脅威動向および被害実態調査報告書
https://www.jpcert.or.jp/research/Ransom-survey.html

ートピック2ー　「FIRST PSIRT Services Framework 1.0 Draft」の日本語版公開

JPCERT/CC は、CSAJ（一般社団法人コンピュータソフトウェア協会）内に設立された Software ISAC と共同で、FIRST (Forum of Incident Response and Security Teams) が公開している製品開発者向けドキュメント「PSIRT Services Framework Version 1.0 Draft」の日本語版を作成し、FIRST の Web サイトで公開しました。

PSIRT（Product Security Incident Response Team）とは、組織が提供する製品の脆弱性に起因するリスクに組織内で対応するための機能を指す言葉です。「PSIRT Services Framework」は、PSIRT のコンセ

プトと全体像を示すとともに、FIRST に加盟しているさまざまな PSIRT の活動を参考に、PSIRT の組織モデル、機能、サービスなどがまとめられています。これから PSIRT を立ち上げる場合や現状の活動の見直しを行う場合に、自社において必要な機能はなにか、どのような組織構成をとるべきかなどを検討する際の参考になる資料です。

日本国内でも、社内に PSIRT を設置運用する事例は増えていますが、まだ多くの製品開発者は PSIRT 機能の重要性は理解しつつも具体的な体制の整備はこれからといった段階にあると思われます。今回の日本語版は、そのような製品開発者のみなさんに活用していただけるものと期待しています。

なお、FIRST の Web サイトでは「Version 1.0 Draft」を改訂した「PSIRT Services Framework Version 1.0」が公開されており、すでに日本語版の改訂作業を進めています。さらに CSAJ、Software ISAC と連携して、製品開発者を対象とした啓発活動を展開できればと考えています。

PSIRT Services Framework Version 1.0 Draft 日本語抄訳
https://first.org/education/FIRST_PSIRT_Services_Framework_v1.0_draft_ja.pdf

JPCERT/CC 研究・調査レポート
「FIRST PSIRT Services Framework Version 1.0 Draft 日本語抄訳版」
https://www.jpcert.or.jp/research/psirtSF.html

CSAJ 一般社団法人コンピュータソフトウェア協会
「PSIRT Services Framework 1.0 Draft」の日本語翻訳文書公開
http://www.csaj.jp/NEWS/pr/180719_psirt.html

Cybozu Inside Out | サイボウズエンジニアのブログ
PSIRT Framework のご紹介
https://blog.cybozu.io/entry/2018/07/18/080000

ートピック3ー　「工場における産業用 IoT 導入のためのセキュリティ ファーストステップ」を公開

JPCERT/CC は、8 月 9 日に工場の制御システムに産業用 IoT を導入する際の基本的なセキュリティ対策を記した参考書「工場における産業用 IoT 導入のためのセキュリティ ファーストステップ」を公開しました。

近年、産業界においても、生産性改善や人手不足の解消などを期待して、IoT の活用が進みつつあります。しかしながら、IoT 導入にともなうセキュリティ・リスクの吟味や十分なリスク対策なしに導入さ

れているケースが多々あり、現場管理者からは「IoT に関連したセキュリティの実務ガイドが欲しい」との要望がありました。

本書は、産業用 IoT 導入におけるセキュリティの重要性とその考え方についての解説書であるとともに、IoT 導入時の仕様策定から運用にいたる各プロセスで行うべきマネジメント視点のセキュリティ対策ならびに導入先 IoT ネットワークの構成要素（IoT デバイス、工場内ネットワーク、サーバ、外部ネットワーク、クラウド）ごとに行うべき技術的なセキュリティ対策を述べた手引書となっています。また、IoT ネットワーク構成図の上に、各構成要素に対応した対策を記載したページ番号を書き込んだ「対策ナビゲーションマップ」を含めるなど、必要な箇所を簡易に拾い読みできるように工夫しており、また、セキュリティ専任担当者がいないことの多い中小の製造事業者の経営者や現場担当者（現場の管理者や技術担当者）に読んでいただくことを想定して、セキュリティ対策の基礎をわかりやすく記述しています。

詳細は、『3.5 「工場における産業用 IoT 導入のためのセキュリティ ファーストステップ」を公開』をご参照ください。

工場における産業用 IoT 導入のためのセキュリティ ファーストステップ
https://www.jpcert.or.jp/ics/information06.html

ートピック4ー　サイバーセキュリティ対策活動への協力者に感謝状贈呈

JPCERT/CC は、国内のサイバーセキュリティインシデント（以下「インシデント」）による被害を低減するために、インシデントへの対応支援、インシデントを未然に防ぐための早期警戒情報の発信、マルウエア分析、ソフトウエア製品等の脆弱性の取り扱いに関する調整などを行っています。これらの活動を円滑かつ効果的に進めるためには、さまざまな皆様からの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様からの御厚意と御力添えに深く思いをいたし、特に顕著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。本年度は、内田 勝也 様、野々下 幸治 様、および、島田 康晴 様を選ばせていただき、2018 年 7 月に感謝状と記念の盾を贈呈いたしました。内田様と野々下様は、フィッシング対策協議会においてワーキンググループの主査や副主査を務められる等、長年にわたって日本国内全体のフィッシング被害の低減に貢献されてきました。また、島田様は、株式会社アイ・オー・データ機器において、自社製品のセキュリティ向上に積極的に取り組み、広くユーザに周知するために自社で発見された脆弱性を積極的に JVN で公表されるなど、国内の業界全体の脆弱性取扱のレベル向上に貢献されてきました。

サイバーセキュリティ対策活動への協力者に感謝状贈呈
https://www.jpcert.or.jp/press/priz/2018/PR20180710-priz.html

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 3,908 件、インシデント件数ベースでは 3,411 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 2,216 件でした。前四半期の 2,124 件と比較して 4%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

本四半期に報告が寄せられたフィッシングサイトの件数は 1,302 件で、前四半期の 1,214 件から 7%増加しました。また、前年度同期（1,011 件）との比較では、29%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	7 月	8 月	9 月	本四半期合計（割合）
国内ブランド	110	97	102	309(24%)
国外ブランド	255	287	242	784(60%)
ブランド不明 (注 5)	77	63	69	209(16%)
全ブランド合計	442	447	413	1,302(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。

E コマースサイト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ています。フィッシングサイトのドメインは、正規サイトと紛らわしい名前で新規に登録されたものが多く、.com ドメインが特に多く使われていましたが、.jp ドメインの悪用も多数確認されています。

国内ブランドのフィッシングサイトでは、通信事業者、SNS、金融機関を装ったものが多く確認されており、それぞれ次のような特徴がありました。

- 通信事業者を装ったフィッシングサイトとしては、国内 ISP の Web メールのログイン画面を装ったものや、携帯キャリアのアカウントを狙ったものを確認している。携帯キャリアのフィッシングサイトは、正規サイトを装った.com ドメインのものが多く、異なるブランドのフィッシングサイトに同じ IP アドレスが割り当てられている場合があった
- SNS を装ったフィッシングサイトは、以前は.cn ドメインが継続的に使用されていたが、8 月半ば以降、.top ドメインも多く使用されている。その他に、ホスティングサービスが無償で提供している.jp ドメインを使用したものも 8 月末以降確認されている
- 国内金融機関を装ったフィッシングサイトでは、インターネットバンキングを装ったものがなく、すべてクレジットカード会社を装ったものだった。正規サイトと紛らわしい.com ドメインを使用したサイトが多く、特定のブランドのフィッシングサイトでは携帯キャリアのフィッシングサイトでも確認された IP アドレスが割り当てられている場合があった

フィッシングサイトの調整先の割合は、国内が 27%、国外が 73%であり、前四半期（国内が 30%、国外が 70%）と比べて国外への通知の割合が増加しました。

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、226 件でした。前四半期の 320 件から 29%減少しています。

前四半期に引き続き、改ざんされた Web サイトから、次のような URL で示される Web ページを経由し、不審なサイトに転送されるといった報告が多く寄せられました。

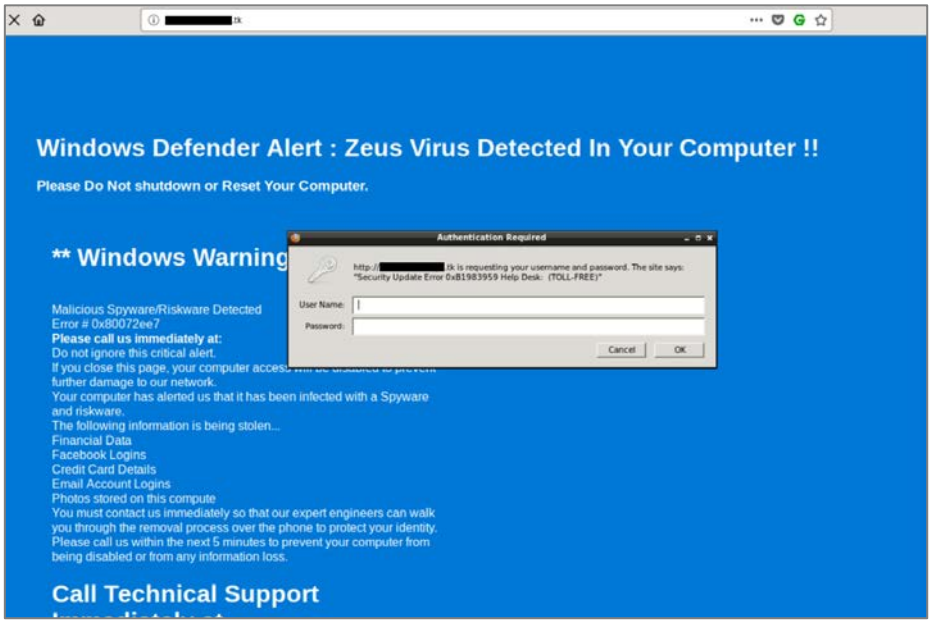
```
http://<ドメイン名>.tk/index/?<数字の列>
```

.tk ドメインの URL への転送は、ページの最上部に埋め込まれた JavaScript（[図 1-1] 参照）や、ページが読み込む JavaScript ファイル内に埋め込まれた難読化されたスクリプトなどによって行われることを確認しています。

```
<script>window.location.replace("http://[redacted].tk/index/?2601510941471");window.location.href = "http://[redacted].tk/index/?2601510941471";
</script><script>window.location.replace("http://[redacted].tk/index/?2601510941471");window.location.href = "http://[redacted].tk/index
/?2601510941471";</script><!DOCTYPE html>
<!--[if IE 7]>
<html class="ie ie7" lang="ja" prefix="og: http://ogp.me/ns#">
<![endif]-->
<!--[if IE 8]>
<html class="ie ie8" lang="ja" prefix="og: http://ogp.me/ns#">
<![endif]-->
<!--[if !(IE 7) & !(IE 8)]><!-->
<html lang="ja" prefix="og: http://ogp.me/ns#">
<!--<![endif]-->
<head>
```

［図 1-1 .tk ドメインの URL に転送する JavaScript］

改ざんされたサイトからの転送先として、偽のマルウエア感染の警告を表示するサイトや、広告を表示するサイト、「アンケートに回答すると賞品が入手できる」と書かれた不審なサイトなどを確認しています。また、.tk ドメインのサイトのドキュメントルートにアクセスすると、アクセスしたブラウザによっては、偽のマルウエア感染の警告が表示される場合がありました。（[図 1-2] 参照）



［図 1-2 偽のマルウエア感染の警告表示］

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、7 件でした。前四半期の 9 件から 22%減少しています。このうち対応を依頼した組織は 3 組織でした。

本四半期は、マクロ付きのファイルが添付された標的型攻撃メールに関する報告が複数寄せられましたが、最終的に実行されるマルウエアの種類は様々でした。次に、確認された 3 つの例を紹介します。

(1) マルウエア ANEL に感染させるマクロ付きの Word ファイル

2018 年 7 月から 8 月にかけて、ANEL と呼ばれる HTTP ボットに感染させることを目的とした標的型攻撃メールに関する報告が複数寄せられました。いずれの報告でも、攻撃者は無料の国内 Web メールサービスを使用し、パスワードがかかったマクロ付きの Word ファイルを添付したメールと、添付ファイルのパスワードが書かれたメールを送付していました。Word ファイルのマクロを実行すると、マルウエアが展開、実行され、ユーザのログオン時にマルウエアを自動実行する設定がレジストリに追加されるようになっていました。

(2) Cobalt Strike Beacon に感染させるマクロ付きの Word ファイル

7 月後半に複数の組織で確認された標的型攻撃メールでは、添付ファイルを実行することで、最終的にペネトレーションテストツール Cobalt Strike のペイロード（Cobalt Strike Beacon）が実行されることを確認しました。メールにはマクロ付きの Word ファイルが添付されており、マクロを実行すると、国内サイトから画像ファイルを装った不正なファイルをダウンロードするとともに、ファイルから展開した実行ファイルを実行するタスクを登録する仕組みになっていました。タスクに登録される実行ファイルはダウンローダであり、HTTP で C&C サーバと通信を行う Cobalt Strike Beacon をダウンロードし、メモリ上に展開して実行するものでした。

(3) マルウエア TSCookie に感染させるマクロ付きの Excel ファイル

8 月の後半に報告が寄せられた標的型攻撃メールには、マクロ付き Excel ファイル（xlsm ファイル）を含む RAR 形式の圧縮ファイルが添付されていました。Excel ファイルは暗号化されていましたが、開く際にパスワードを入力する必要がないように作成されていました。これは、Excel ファイルで使用可能な特別なパスワードが設定されていたためでした[(1)]。Excel ファイルのマクロを実行すると、スタートアップフォルダに実行ファイルが作成され、OS の起動時に自動実行されるようになっていました。実行ファイルは TSCookie と呼ばれるマルウエアで、2018 年 6 月末頃の標的型攻撃でも使用されていました。今回確認したマルウエアも、スタートアップフォルダにマルウエアが作成され、マルウエアを実行すると C&C サーバのポート 443/TCP に HTTP で接続するといった、以前のものと共通する特徴をもっていました。

1.1.2. 参考文献

(1) Cybozu Inside Out | サイボウズエンジニアのブログ
Excel の奇妙なパスワードとマクロウイルス
https://blog.cybozu.io/entry/2017/03/09/080000

1.1.3. 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

2018-07-30　研究・調査レポート「ランサムウエアの脅威動向および被害実態調査報告書」を公開

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：18 件（うち 4 件は更新情報）　https://www.jpcert.or.jp/at/

2018-07-11　Adobe Reader および Acrobat の脆弱性 (APSB18-21) に関する注意喚起 (公開)
2018-07-11　Adobe Flash Player の脆弱性 (APSB18-24) に関する注意喚起 (公開)
2018-07-11　2018 年 7 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)
2018-07-18　2018 年 7 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)
2018-07-23　Apache Tomcat における複数の脆弱性に関する注意喚起 (公開)
2018-07-23　2018 年 7 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)
2018-08-09　ISC BIND 9 サービス運用妨害の脆弱性 (CVE-2018-5740) に関する注意喚起 (公開)
2018-08-15　Adobe Reader および Acrobat の脆弱性 (APSB18-29) に関する注意喚起 (公開)
2018-08-15　Adobe Flash Player の脆弱性 (APSB18-25) に関する注意喚起 (公開)
2018-08-15　2018 年 8 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)
2018-08-22　Ghostscript の -dSAFER オプションの脆弱性に関する注意喚起 (公開)
2018-08-23　Apache Struts 2 の脆弱性 (S2-057) に関する注意喚起 (公開)
2018-09-06　Ghostscript の -dSAFER オプションの脆弱性に関する注意喚起 (更新)
2018-09-12　Adobe Flash Player の脆弱性 (APSB18-31) に関する注意喚起 (公開)
2018-09-12　2018 年 9 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)
2018-09-14　Ghostscript の -dSAFER オプションの脆弱性に関する注意喚起 (更新)
2018-09-20　Adobe Reader および Acrobat の脆弱性 (APSB18-34) に関する注意喚起 (公開)
2018-09-21　Adobe Reader および Acrobat の脆弱性 (APSB18-34) に関する注意喚起 (更新)

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：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 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 13 件でした。

2018-07-04　JPCERT/CC が「Linux と Windows を狙うマルウエア WellMess」に関する分析センターだよりを公開
2018-07-11　総務省が IoT 機器に関する脆弱性調査等の実施結果を公表
2018-07-19　Google Chrome に HTTP ページに対する警告が追加予定
2018-07-25　「PSIRT Services Framework Version 1.0 Draft 日本語抄訳」を公開
2018-08-01　「サイバーセキュリティ戦略」が閣議決定
2018-08-08　STOP! パスワード使い回し!キャンペーン 2018
2018-08-15　「工場における産業用 IoT 導入のためのセキュリティ ファーストステップ」を公開
2018-08-22　総務省が「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会第三次取りまとめ（案）」を公開
2018-08-29　仮想通貨を要求する不審な脅迫メールにご注意を
2018-09-05　日本語のメールを用いたビジネスメール詐欺
2018-09-12　Sysmon ログを可視化して端末の不審な挙動を調査する SysmonSearch を公開
2018-09-20　Microsoft が Windows や Office 製品のサポート期間などに関する情報を公開
2018-09-27　「フィッシング対策セミナー 2018」開催のお知らせ

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：7 件　https://www.jpcert.or.jp/newsflash/

2018-07-11　複数の Adobe 製品のアップデート (APSB18-22、APSB18-23) について
2018-07-18　Web サイトへのサイバー攻撃に備えて 2018 年 7 月
2018-07-25　Cisco Webex Teams の脆弱性 (CVE-2018-0387) について
2018-08-02　仮想通貨を要求する不審な脅迫メールについて
2018-09-12　Adobe 製品のアップデート (APSB18-33) について
2018-09-19　仮想通貨を要求する日本語の脅迫メールについて
2018-09-20　ISC BIND 9 の脆弱性 (CVE-2018-5741) 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) 仮想通貨を要求する不審な脅迫メールについての情報発信

2018 年 7 月 21 日頃より、仮想通貨のビットコインを要求する、複数パターンの不審な英文メールが広く出回っており、JPCERT/CC においても不審な英文メールの一例を確認しました。このメールの特徴として、メール受信者が実際に使用したことがあるパスワードが本文に記述されていることが挙げられます。

受信者によれば、脅迫メールに示されたパスワードを使用していたサービスは複数にわたっているケースもありました。パスワード自体が漏えいした原因については、ユーザ側の PC のマルウエア感染による情報窃取の可能性やサービス提供サイトへの不正アクセスによる情報漏えいの可能性も考えられ、特定には到りませんでした。

JPCERT/CC では、2018 年 8 月 2 日に CyberNewsFlash を公開し、メールを受信した場合には、攻撃者の要求には応じず、普段からも、パスワードの再設定やログイン履歴の確認を行い、ウイルス対策ソフトの利用やパスワードの使い回しをしないなどの対策に努めるよう注意を呼びかけました。

仮想通貨を要求する不審な脅迫メールについて
https://www.jpcert.or.jp/newsflash/2018080201.html

(2) Apache Struts 2 の脆弱性 (S2-057) に関する情報発信

Apache Software Foundation から Apache Struts 2 の脆弱性 (CVE-2018-11776) に関する情報が 2018 年 8 月 22 日（現地時間）に公開されました。JPCERT/CC でも本脆弱性に関する実証コードの検証を行った結果、特定の設定を行っている Apache Struts 2 が動作するサーバに細工した HTTP リクエストを送信することにより、任意のコードが実行されることを確認できました。そのため、8 月 23 日に注意喚起および早期警戒情報を公開し、早期の対策を一般に広く呼びかけました。

Apache Struts 2 の脆弱性 (S2-057) に関する注意喚起
https://www.jpcert.or.jp/at/2018/at180036.html

(3) ランサムウエアの脅威動向および被害実態調査報告書の公開

2017 年度に JPCERT/CC では、依然としてランサムウエアの脅威が世界各地に広がっており、感染事例が報告されている現状を踏まえて、ランサムウエアの感染経路や感染リスクが拡大している背景、脅威動向の変遷について公開情報をもとに調査し、また、2017 年度に国内の法人組織の被害実態を明らかにするために、ランサムウエアに関するアンケート調査を実施しました。
その結果を国内の法人組織におけるランサムウエアの被害実態を理解するための一助として、また対策を推進する際の参考資料として、活用していただくため、その調査結果を 2018 年 7 月 30 日に「ランサムウエアの脅威動向および被害実態調査報告書」としてまとめを、2018 年 7 月 30 日に公開しました。

ランサムウエアの脅威動向および被害実態調査報告書
https://www.jpcert.or.jp/research/Ransom-survey.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 9 月末時点で、海外の 22 の経済地域の 28 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

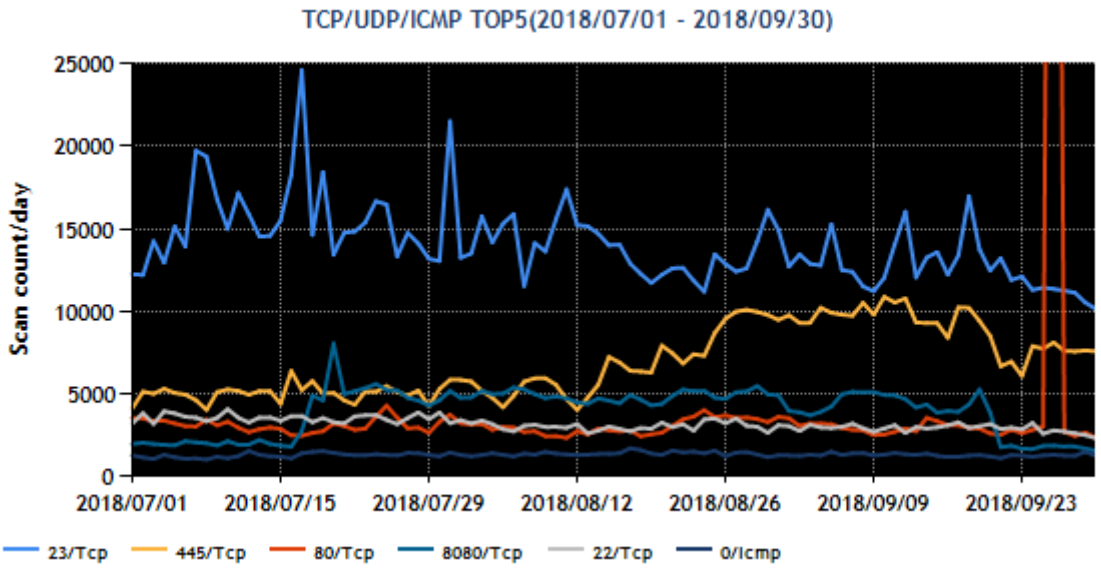
JPCERT/CC では、主に日本企業のシステム管理者の方々に、自組織のネットワークに届くパケットの傾向と比較していただけるよう、日本国内の TSUBAME のセンサーで受信したパケットを宛先ポート別に集計してグラフ化し、毎週月曜日に JPCERT/CC の Web ページで公開しています。また、四半期ごとに観測傾向や注目される現象を紹介する「インターネット定点観測レポート」を公開しており、2018 年

4 月から 6 月分のレポートを 2018 年 8 月 2 日に公開しました。

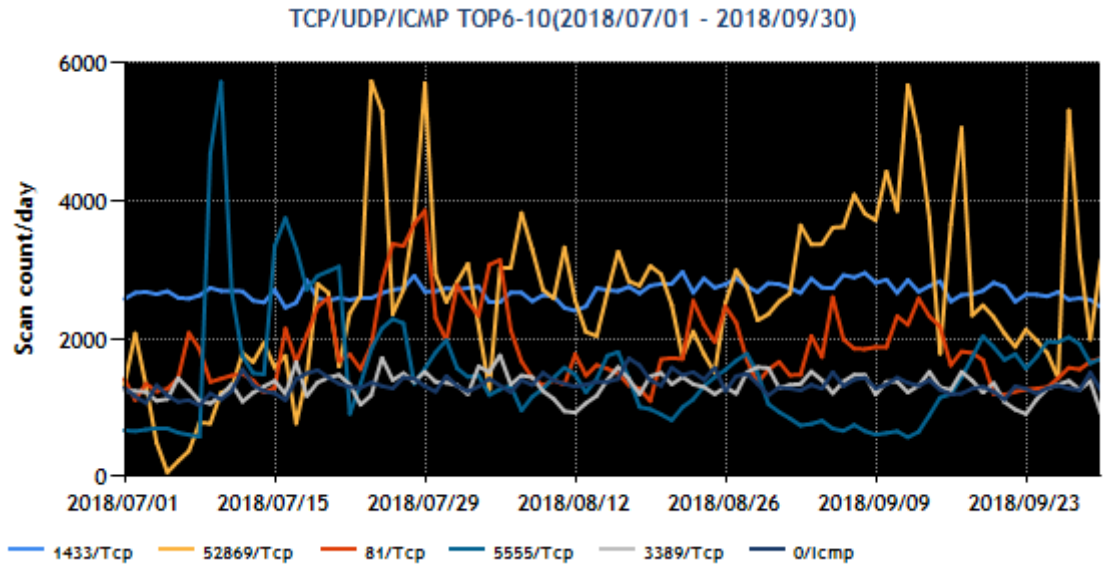
TSUBAME 観測グラフ
https://www.jpcert.or.jp/tsubame/index.html#examples
インターネット定点観測レポート（2018 年 4～6 月）
https://www.jpcert.or.jp/tsubame/report/report201804-06.html

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。

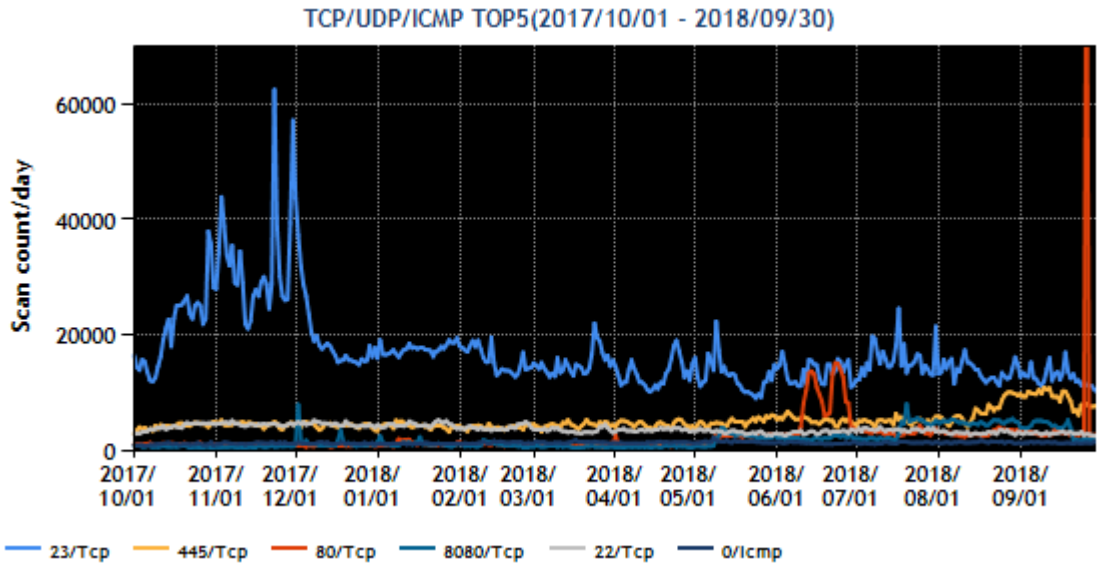


［図 1-1 宛先ポート別グラフ トップ 1-5（2018 年 7 月 1 日-9 月 30 日）］

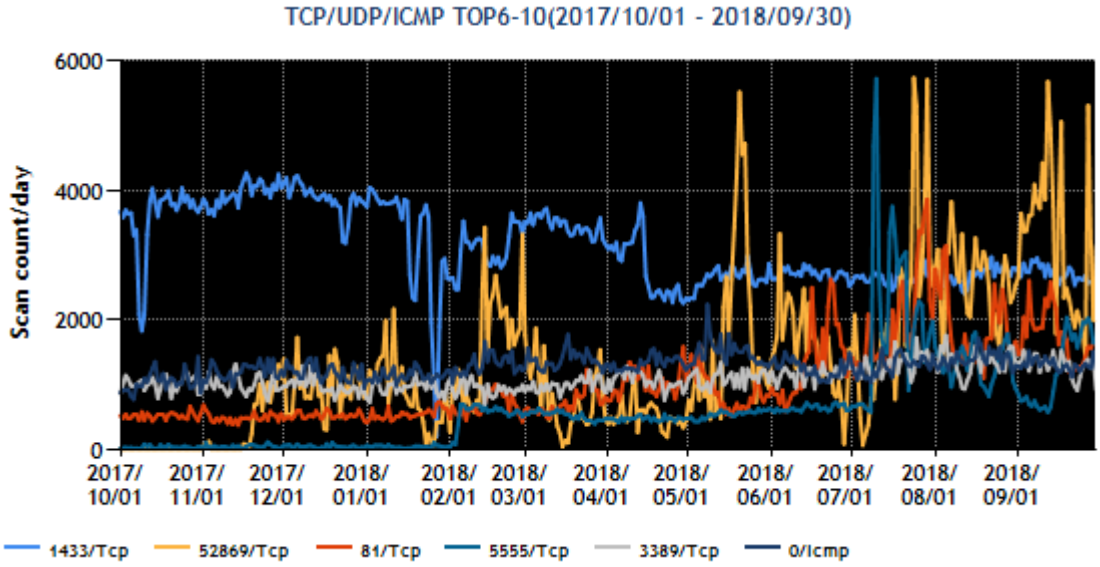


［図 1-2 宛先ポート別グラフ トップ 6-10（2018 年 7 月 1 日-9 月 30 日)］

また、過去 1 年間（2017 年 10 月 1 日-2018 年 9 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（2017 年 10 月 1 日-2018 年 9 月 30 日)］



［図 1-4 宛先ポート別グラフ トップ 6-10（2017 年 10 月 1 日-2018 年 9 月 30 日）］

本四半期に観測されたパケットを宛先ポートに着目して振り返ると、445/TCP 宛のパケットが、8 月 14 日以降増加傾向にあります。これまであまり見られなかった、52869/TCP 宛のパケットも本四半期中に多く観測されるようになりました。これは、一部のマルウエアが探索対象とする宛先ポートを変更した影響と考えられます。

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、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、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。本四半期における対応事例のうち、マルウエアに感染したホストが特定のパラメータをもつ 445/TCP 宛のパケットを送信するインシデントについて次に述べます。

本状況は 8 月 12 日前後に確認されました。送信元となっている日本の IP アドレスについて調査を行ったところ、8 割以上が Windows2003 を使用するホストでした。日本国内の企業等とみられる IP アドレスもあったため、当該の通信を行う IP アドレス管理者全てに連絡を行いました。いくつか返信をいただいた管理者によると、アンチウイルスソフトでマルウエアが発見されたということでした。

現時点では、感染の原因やマルウエアに関する詳細は不明です。JPCERT/CC では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。

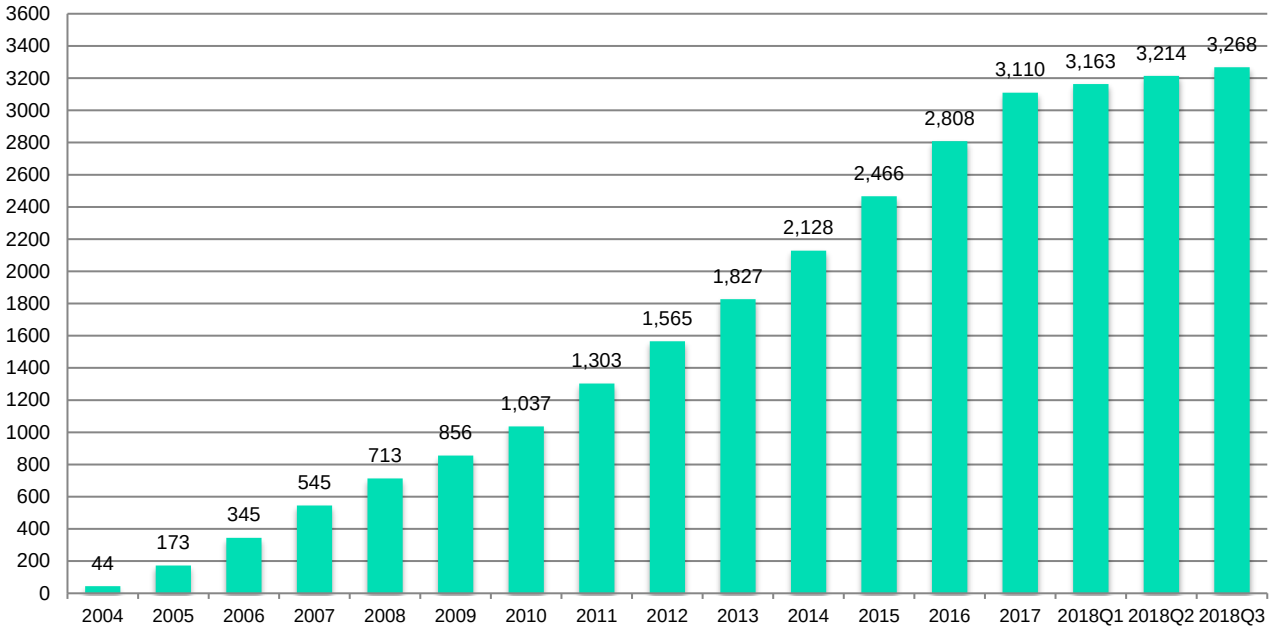
独立行政法人情報処理推進機構（IPA）脆弱性対策
https://www.ipa.go.jp/security/vuln/

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 54 件（累計 3,268 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/



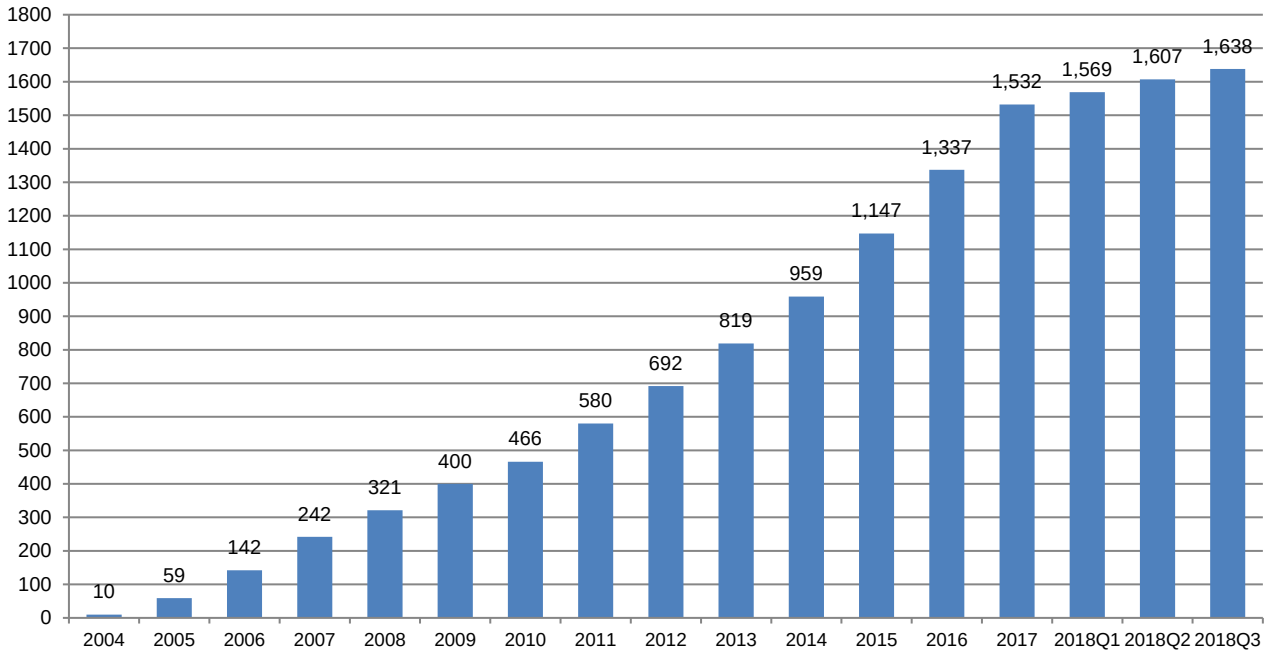
［図 2-1 JVN 公表累積件数］

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 31 件（累計 1,638 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 31 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 25 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 5 件、国内の複数の製品開発者の製品に影響を及ぼすものが 1 件ありました。31 件うち 4 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 9 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、組込系（8 件）でした。これは特定の発見者が、組込系製品についての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	9
組込系	8
Android アプリ	3
CMS	3
グループウエア	2
制御系製品	2
プラグイン	2
スマートフォンアプリ	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 23 件（累計 1,630 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、TCP 等といったプロトコルに関するものが 5 件と最も多く、これら 5 件のうち 3 件は、米国 CERT/CC、フィンランド NCSC-FI、オランダ NCSC-NL、JPCERT/CC に国際展開され、各国の複数の製品開発者と事前調整を経て公表に至ったものです。5 件中 2 件は、CERT/CC が発行した注意喚起を、JPCERT/CC が翻訳し JVN にて注意喚起を行ったものです。

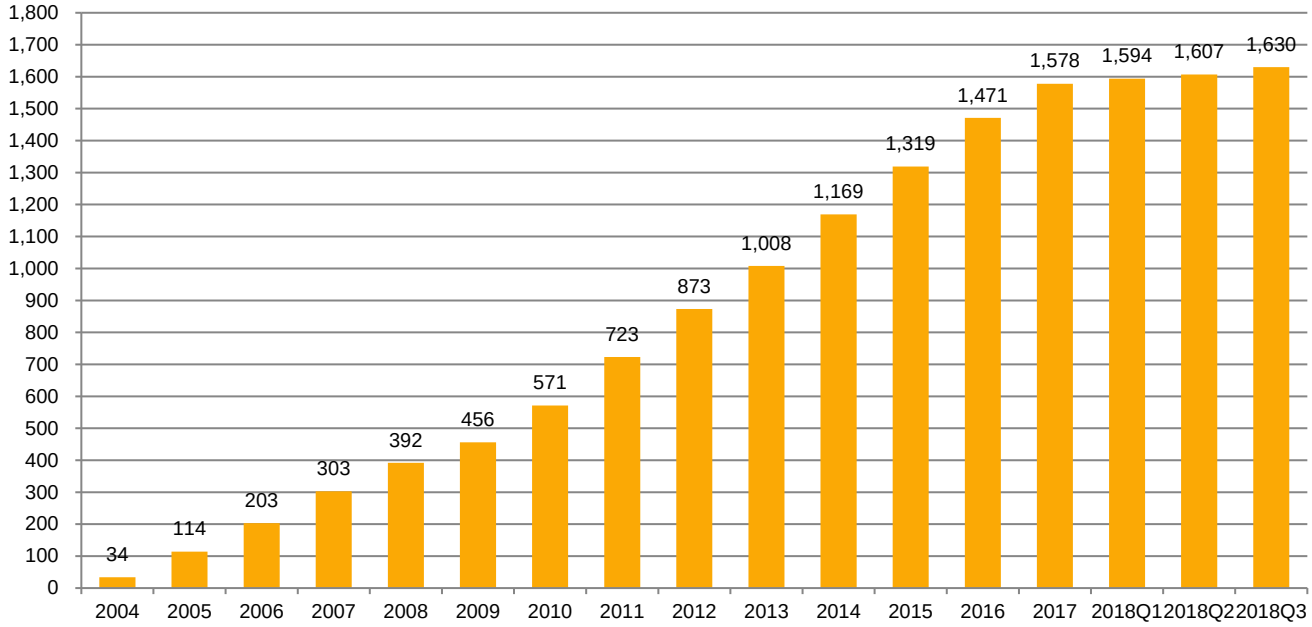
次いで多かったのは、macOS や macOS アプリケーションに関する脆弱性が 4 件、DNS に関する脆弱性が 3 件でした。DNS に関する脆弱性情報の公表は、製品開発者自身による脆弱性情報の公表依頼に基づき行ったものです。

また、本四半期においては、制御系製品を開発する製品開発者が、自社製品に関する脆弱性情報を JVN で広く情報発信することを目的とした自社製品の届出が 1 件ありました。

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
プロトコル	5
DNS	3
macOS アプリ	3
ウェブサーブレットコンテナ	2
組込系	2
マルチプラットフォームアプリケーション	2
Linux カーネル	1
macOS	1
Windows アプリケーション	1
ウェブアプリケーションフレームワーク	1
開発環境	1
制御系製品	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 18 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 62 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

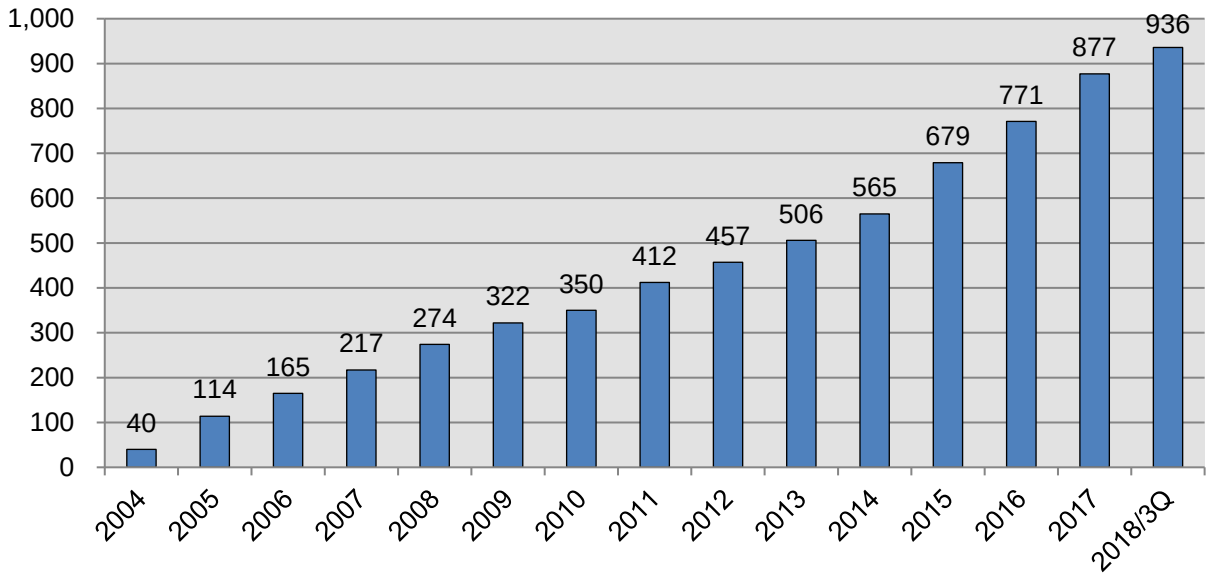
JPCERT/CC では、本規程に従って、日本国内の脆弱性情報流通体制を整備しています。
詳細については、次の Web ページをご参照ください。

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

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 9 月 30 日現在で 936 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: 9 月 29 日
講演タイトル: セキュアプログラミング演習（Web アプリケーション）
イベント名: 東京電機大学国際化サイバーセキュリティ学特別コース(CySec) 「セキュアシステム設計・開発」

本講演は、東京電機大学が開講している「国際化サイバーセキュリティ学特別コース」の科目の一部への講師派遣依頼を受けて、ソフトウエア開発者向け啓発活動の一環として脆弱性コーディネーショングループが行ったものです。「セキュアシステム設計・開発」科目のなかの「セキュアプログラミング: Web アプリケーション」の部分を担当しており、クロスサイトスクリプティングや SQL インジェクションといった Web アプリケーションの脆弱性を悪用する攻撃やその対策について、PHP で作成した簡単な Web アプリケーションを使って実習を行いました。

2.3.2. 「FIRST PSIRT Services Framework Version 1.0 Draft」の日本語版公開

JPCERT/CC は、CSAJ（一般社団法人コンピュータソフトウェア協会）内に設立された Software ISAC と共同で、FIRST が公開している製品開発者向けドキュメント「PSIRT Services Framework Version 1.0 Draft」の日本語版を作成しました。日本語版ドキュメントは FIRST の Web サイトで公開しています。

PSIRT (Product Security Incident Response Team) とは、組織が提供する製品の脆弱性に起因するリスクに組織内で対応するための機能を指す言葉です。PSIRT の活動は、自社製品の脆弱性への対応、製品のセキュリティ品質管理・向上を目的としており、国内の製品開発者においても、PSIRT 機能を整備する事例が徐々に広がっています。

FIRST（Forum of Incident Response and Security Teams）では、かねてより CSIRT 活動に関するドキュメント「CSIRT Services Framework」を作成公開しており、その改訂の過程で PSIRT 活動に関するドキュメントを独立させ、「PSIRT Services Framework」として執筆作業を進めてきました。昨年には 1.0 Draft 版を公開し、一般からのコメントを募集する状態となっていました。

「PSIRT Services Framework」では、PSIRT のコンセプトと全体像を示すとともに、FIRST に加盟しているさまざまな PSIRT の活動を参考に、PSIRT の組織モデル、機能、サービスなどがまとめられています。これから PSIRT を立ち上げる場合や現状の活動の見直しを行う場合に、自社において必要な機能はなにか、どのような組織構成をとるべきかなどを検討する際の参考になる資料です。

今回作成した日本語版ドキュメントは 1.0 Draft 版を元にしています。一方、FIRST では時期を前後して 1.0 Draft 版から 1.0 最終版に改訂した「PSIRT Services Framework Version 1.0」を公開しています。今後は、この 1.0 最終版に沿って日本語版ドキュメントの改訂を進める予定です。

PSIRT Services Framework Version 1.0 Draft 日本語抄訳
https://first.org/education/FIRST_PSIRT_Services_Framework_v1.0_draft_ja.pdf

JPCERT/CC 研究・調査レポート
FIRST PSIRT Services Framework
https://www.jpcert.or.jp/research/psirtSF.html

CSAJ 一般社団法人コンピュータソフトウェア協会
「PSIRT Services Framework 1.0 Draft」の日本語翻訳文書公開
http://www.csaj.jp/NEWS/pr/180719_psirt.html

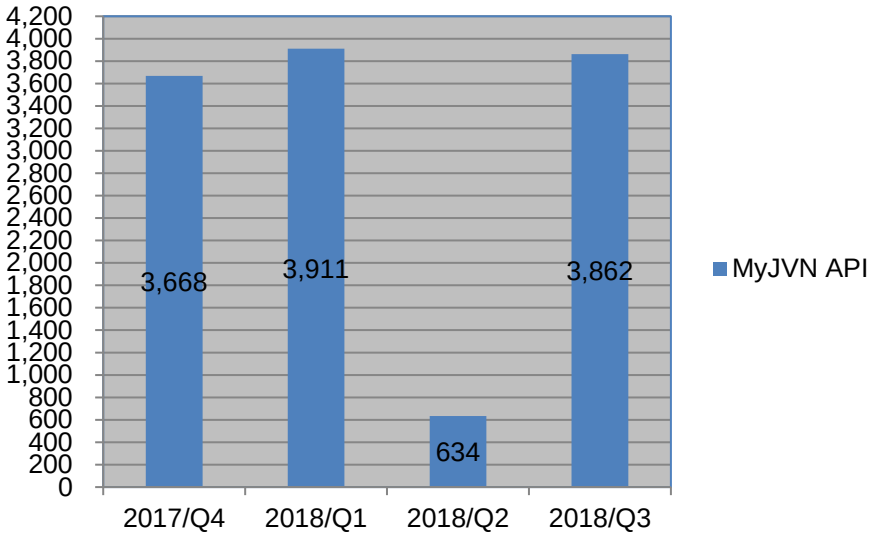
Cybozu Inside Out | サイボウズエンジニアのブログ
PSIRT Framework のご紹介
https://blog.cybozu.io/entry/2018/07/18/080000

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。

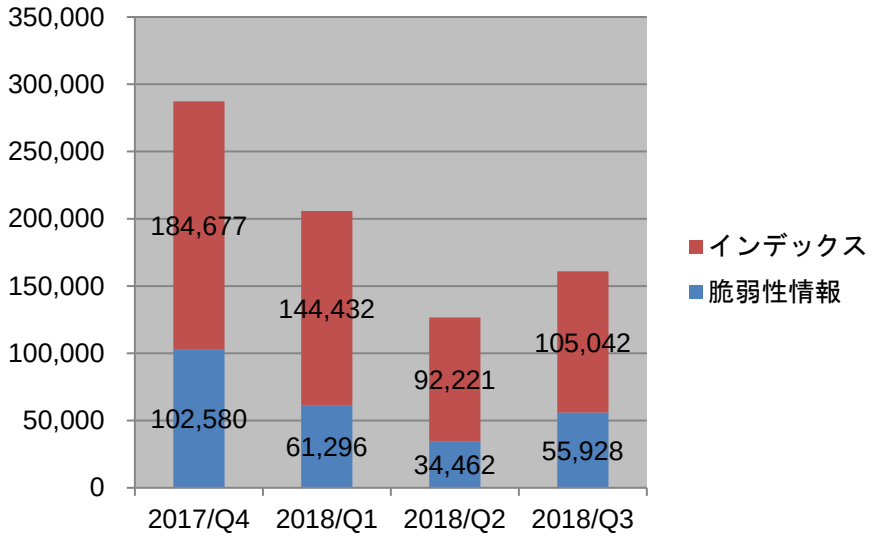
VRDA フィード 脆弱性脅威分析用情報の定型データ配信
https://www.jpcert.or.jp/vrdafeed/index.html

四半期ごとに配信した VRDA フィード配信件数を［図 2-5］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 2-7］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。



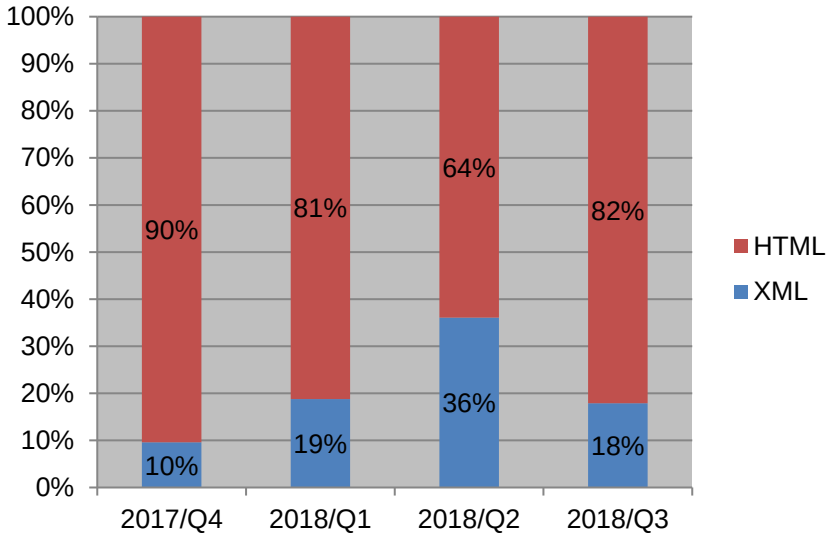
［図 2-5 VRDA フィード配信件数］

VRDA フィード配信件数については、［図 2-5］に示したように前四半期と比較して大幅に増加しています。これは前四半期に実施された VRDA フィード配信用システムの一部改訂作業におけるデータ更新の停止が復旧されたことが原因です。



［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 14%増加しました。脆弱性情報の利用数についても、約 62%増加しました。



［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 18%減少しました。

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 370 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 4 件でした。

2018/07/11 【参考情報】SEL 社が提供する製品の脆弱性について
2018/07/23 【参考情報】米国 FERC がサイバーインシデント報告の範囲拡大に関する規定の策定を NERC に指示
2018/09/11 【参考情報】KONE 社エレベータ関連製品の複数の脆弱性について
2018/09/14 【参考情報】Siemens 社製品に関する脆弱性について

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。

2018/07/05　制御システムセキュリティニュースレター 2018-0006
2018/08/03　制御システムセキュリティニュースレター 2018-0007
2018/09/07　制御システムセキュリティニュースレター 2018-0008

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 873 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システムの情報（45 IP アドレス）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 1 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 261 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

3.5 「工場における産業用 IoT 導入のためのセキュリティ ファーストステップ」を公開

産業用 IoT を工場などに導入する際に、最低限実施してほしいセキュリティ対策をまとめた「工場における産業用 IoT 導入のためのセキュリティ ファーストステップ」を 8 月 9 日に公開しました。

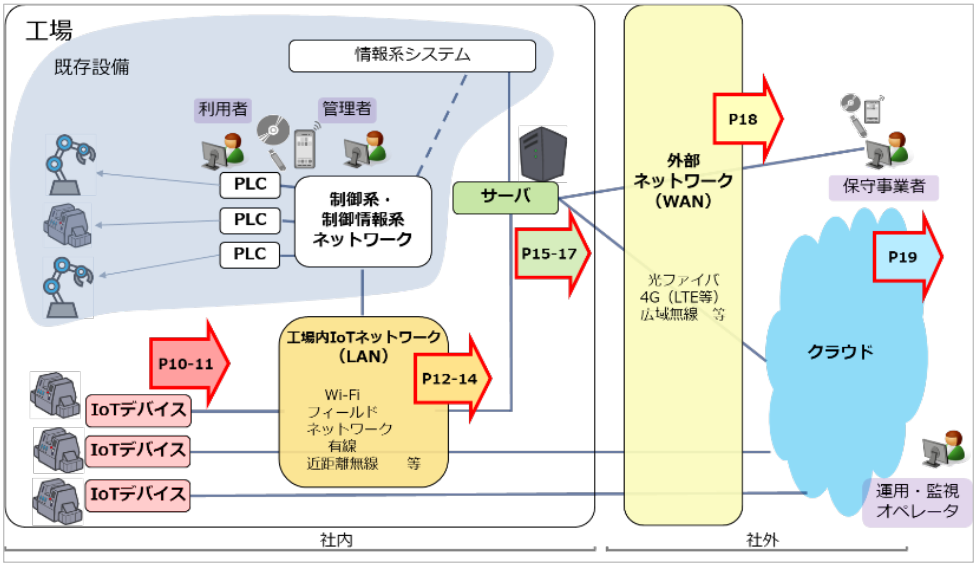
本書は、産業用 IoT の導入におけるセキュリティの重要性やその考え方の解説、さらには産業用 IoT の導入プロセスごとに行うべきマネジメント視点のセキュリティ対策ならびに導入先 IoT ネットワークの構成要素（IoT デバイス、工場内ネットワーク、サーバ、外部ネットワーク、クラウド）ごとに行うべき技術的なセキュリティ対策を述べた手引書となっています。また、特に「中小の製造業者」における「工場での IoT」の「導入時」にご利用いただけるよう、IoT 機器を導入する組織の経営者や制御システムの現場担当者（現場管理者や技術担当者）および構築を担うエンジニアリング会社の方を想定読者としています。

本書の特徴は、実際に被害を受けた企業の対応コストなどを例示しつつ産業用 IoT 導入におけるセキュリティの重要性とその考え方などを経営者向けに解説している点、産業用 IoT 導入に際して仕様策定から運用にいたるまでの各プロセスで行っていただきたいマネジメント視点のセキュリティ対策を現場担当者向けに掲載するとともに、5 つに分類された産業用 IoT ネットワークの構成要素（「IoT デバイス」、「工場内 IoT ネットワーク」、「サーバ」、「外部ネットワーク」、「クラウド」）ごとに行っていただきたい技術的なセキュリティ対策を掲載している点です。また、セキュリティに慣れていない現場担当者の方からあがった声を反映して、「対策ナビゲーションマップ」に 5 つの構成要素を配置して各要素に対応した対策のページ番号を併記し、対象の構成要素のセキュリティ対策ペ

ージをすばやく見つけ出せるように使い勝手も工夫しています。
産業用 IoT の導入を検討されている場合は、本書をぜひご活用ください。

■経営者向けの項目
- P.3 経営者の皆さまへ
- P.4 本書における産業用 IoT のセキュリティ対策の考え方

■現場担当者（現場管理者や技術担当者）向けの項目
- P.5 産業用 IoT の導入プロセス：外部事業者との役割・業務分担
- P.9 産業用 IoT の構成要素：対策ナビゲーションマップ



［図 3-3 対策ナビゲーションマップ］

工場における産業用 IoT 導入のためのセキュリティ ファーストステップ
～産業用 IoT を導入する企業のためのセキュリティガイド～
https://www.jpcert.or.jp/ics/information06.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。

4.2. 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、7 月 12 日、8 月 6 日、9 月 20 日に電話会議を行い、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。本四半期は、JPCERT/CC が支援したベトナムの VNCERT が FIRST に加盟を果たしました。

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. 第 4 回 日 ASEAN サイバーセキュリティ政策会議の参加（7 月 25 日-26 日）

JPCERT/CC は 7 月 25 日から 26 日にかけてフィリピンのマニラで開催された日 ASEAN サイバーセキュリティ政策会議に参加し、JPCERT/CC の主にアジア太平洋地域における CSIRT 構築支援の取り組み

をはじめとした海外向けの活動等について講演しました。

4.2.4. 第 6 回 日中韓 サイバーセキュリティインシデント対応年次会合の開催（8 月 27 日-28 日）

日中韓の National CSIRT（JPCERT/CC、CNCERT/CC、KrCERT/CC）による「日中韓 サイバーセキュリティインシデント対応年次会合」を、JPCERT/CC が主催し 8 月 27 日から 28 日にかけて東京で開催しました。本会合は、2011 年 12 月に三者が締結した覚書（MOU）に基づき毎年開催されています。
本会合では、前回の会合以降の、日中韓に影響を及ぼす重大なサイバーセキュリティインシデントにおける National CSIRT 間の連携実績を振り返るとともに、対応した主要なインシデントや各種取り組み等をそれぞれの CSIRT が報告しました。また、各 CSIRT が取り組んでいる海外向けの CSIRT 構築支援の活動状況について意見を交換しました。

4.2.5. 第 13 回 ASEAN CERTs Incident Drill（ACID）参加（9 月 5 日）

シンガポールの National CSIRT である SingCERT が主導し、ASEAN（東南アジア諸国連合）各国の CSIRT が合同で実施するサイバーインシデント演習である ACID（ASEAN CERTs Incident Drill）が 9 月 5 日に実施され、これに JPCERT/CC も参加しました。本演習は、国境を越えて発生するサイバーセキュリティインシデントに備え、ASEAN 加盟国および周辺各国の CSIRT 間の連携の強化を目的に毎年実施されており、今回で 13 回目になります。今年の演習は「システムの脆弱性と仮想通貨マイニング」をテーマに行われました。

4.2.6. Asia-Pacific Telecommunity Symposium on Cybersecurity への参加（9 月 12 日 - 14 日）

JPCERT/CC は 9 月 12 日から 14 日にかけて韓国のソウルで開催された Asia-Pacific Telecommunity Symposium on Cybersecurity に参加しました。このうち 9 月 14 日に ”Best Practices of national/regional Computer Emergency Response Team (CERT) and Computer Security Incident Response Team (CSIRT)” と題されたセッションにて、JPCERT/CC の海外 CSIRT コミュニティにおける活動等について発表するとともに、他の CSIRT から参加したパネリストと意見を交換しました。

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. インターネットリスク可視化サービス Mejiro

8 月 6 日にインターネットリスク可視化サービスを提供するポータル Mejiro の英語版を公開しました。今後は国際 CSIRT 間において「Mejiro 指標」を用いて要因について話し合うことができます。指標を用いることで各国間の比較が客観的にできるようになるだけではなく、当該国・地域において注力すべきセキュリティ課題の優先度付けにも役立つと期待されます。

Demonstration Test: Internet Risk Visualization Service -Mejiro-
https://www.jpcert.or.jp/english/pub/sr/mejiro/mejiro.html

4.4. その他国際会議への参加

4.4.1. U.S.-Singapore TCTP Cybersecurity Workshop への参加（8 月 13 日 - 16 日）

JPCERT/CC は 8 月 13 日から 16 日にかけてシンガポールで開催された、米国とシンガポールが共催する、主に ASEAN 諸国向けのトレーニングコースに講師として参加しました。
APCERT の事務局を運営する立場から、国の枠を超えた CSIRT 間の協力についての実績を共有しました。また JPCERT/CC が経験した高度なインシデント対応について ASEAN 諸国の CSIRT 職員および政府関係者向けに紹介しました。このトレーニングを通じて、ASEAN 諸国におけるインシデント対応能力が向上することにより、今後の協力が円滑化することが期待されます。

4.4.2. The Global Commission on the Stability of Cyberspace（GCSC）への参加（9 月 19 - 20 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。技術ワーキンググループでは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おり、JPCERT/CC の小宮山が副議長としてこれに関与しています。
今回の第三回全体会合では、委員から提案された 6 つの規範の提案について議論が行われました。

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

4.4.3. 2018 中国网络安全年会（CNCERT Annual Conference）への参加（8 月 15 日- 16 日）

JPCERT/CC は、8 月 15 日から 16 日にかけて中国の北京で開催された 2018 中国网络安全年会（CNCERT Annual Conference）に参加し、中国におけるサイバー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。

2018 中国网络安全年会
http://conf.cert.org.cn/

4.4.4. 海外 CSIRT 等の来訪および往訪

4.4.4.1. フィリピン CERT-PH 往訪（7 月 27 日）

フィリピンの情報通信技術省配下に新たに設立された CERT-PH（フィリピンコンピュータ緊急対応チーム）を往訪し、同組織の設備の準備状況についてヒアリングを行うとともに、今後の協力について意見交換を行いました。

4.4.4.2. ベトナム Authority of Information Security 来訪（8 月 2 日）

ベトナム Authority of Information Security の職員が来訪し、双方の活動状況について意見交換を行いました。特に、JPCERT/CC が行っている海外向けの CSIRT 構築支援の取り組みについて紹介するとともに、今後の協力について議論しました。

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。

脆弱性関連では、脆弱性の開示（ISO/IEC 29147）については 8 月 7 日から 10 月 2 日まで最終国際標準草案(FDIS；Final draft of international standard)として、脆弱性の取扱手順（ISO/IEC 30111）については 10 月 31 日から 2019 年 1 月 23 日まで国際標準草案(DIS；Draft of international standard)として、それぞれ国際投票に付すとして各草案が国際事務局から加盟各国に配布されました。JPCERT/CC では、このうち脆弱性の開示に関して国際投票への対応を検討し、情報企画調査会に対応案を提案しました。

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。

Malware “WellMess” Targeting Linux and Windows（7 月 6 日）
https://blog.jpcert.or.jp/2018/07/malware-wellmes-9b78.html

Volatility Plugin for Detecting Cobalt Strike Beacon（8 月 3 日）
https://blog.jpcert.or.jp/2018/06/how-to-describe-vulnerability-information.html

Visualise Sysmon Logs and Detect Suspicious Device Behaviour -SysmonSearch-
https://blog.jpcert.or.jp/2018/09/visualise-sysmon-logs-and-detect-suspicious-device-behaviour--sysmonsearch.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；本節の以下において「協議会」）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。

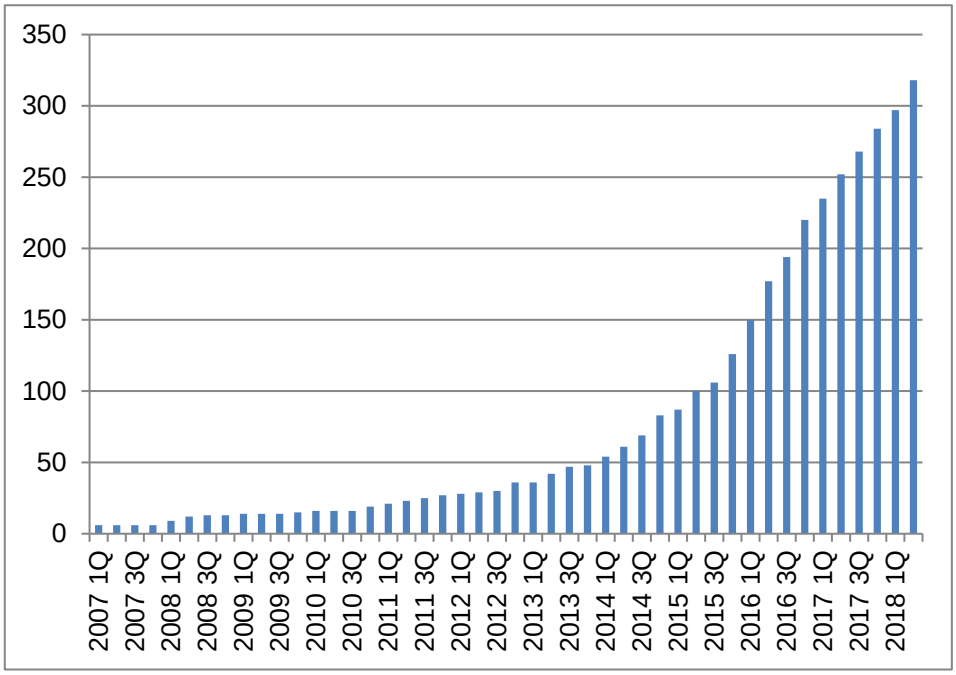
本四半期には、次の 17 組織（括弧内はシーサート名称）が新規に NCA の一般会員となりました。

株式会社 HBA (HBA-CSIRT)
マスミューチュアル生命保険株式会社 (MMJ-CSIRT)
東洋アルミニウム株式会社 (TOYAL-CSIRT)
国立大学法人大阪教育大学 (OK-CSIRT)
株式会社ファーストリテイリング (FRG ISO)
ミス・パリ・グループ (miss-paris-CSIRT)
株式会社 長谷工コーポレーション (HASEKO-CSIRT)
ロート製薬　株式会社 (Rohto-SIRT)
SBI 生命保険株式会社 (SBILIFE-CSIRT)

株式会社ＪＭＣリスクソリューションズ (RS-CIRT)
シンプレクス・ホールディングス株式会社 (Simplex-CSIRT)
古河電気工業株式会社 (FEC-CSIRT)
独立行政法人 国立高等専門学校機構 (KOSEN-CSIRT)
株式会社アルファ・ウェーブ (AW-CSIRT)
小田急電鉄株式会社 (OER-CSIRT)
株式会社ベネッセホールディングス (Bene-SIRT)
株式会社リコー (RICOH-CSIRT)

本四半期末時点で※318（一般会員 316、協力会員 2）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 14 回総会および第 22 回シーサートワーキンググループ会

第 14 回総会 とそれに続けて第 22 回シーサートワーキンググループ会が次のとおり開催されました。JPCERT/CC は事務局としてこの開催のための各種サポートを行いました。

日時：2018 年 8 月 24 日（金）
場所：東京電機大学 東京千住キャンパス 1 号館　2F 丹羽ホール

総会では、5 名の運営委員の任期満了に伴う運営委員の選出を行いました。定数 5 名に対して、3 名の現職の運営委員を含む計 5 名の立候補・推薦があったことから、投票に代えて各候補者に対する信認の是非を議論した結果、全員が選任されました。

再任された運営委員
TM-SIRT　萩原委員
JSOC　原子委員
JPCERT/CC　山本委員

新たに選任された運営委員
Canon-CSIRT 羽場委員
NTT-Com SIRT　林委員

また、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。この日の会合では、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 12 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　：「CSIRT 役割評価テンプレート Ver0.5-1」
講演者：CSIRT 人材 WG　SoftBank CSIRT 松本 勝之 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。

臨時運営委員会
開催日時：2018 年 7 月 12 日（木）16:00 - 18:00
開催場所：HIRT

第 134 回運営委員会
開催日時：2018 年 7 月 25 日（水）16:00 - 18:00
開催場所：TM-SIRT

臨時運営委員会
開催日時：2018 年 8 月 13 日（月）13:00 - 15:00
開催場所：JPCERT/CC

第 135 回運営委員会

開催日時：2018 年 8 月 22 日（水）16:00 - 18:00

開催場所：MBSD-SIRT

臨時運営委員会

開催日時：2018 年 8 月 27 日（水）16:00 - 18:00

開催場所：JPCERT/CC

第 136 回運営委員会

開催日時：2018 年 9 月 26 日（水）16:00 - 18:00

開催場所：HIRT

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・問合せの受付、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、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 14 件（ニュース：6 件、緊急情報：8 件）発信しました。

前四半期に引き続き、本四半期も Apple や Amazon、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の報告が多く寄せられました。また LINE をかたるフィッシングサイトについては、2017 年 3 月から.cn ドメインが使われていましたが、8 月中旬から.top や.com および .jp などのドメインも使われるようになりました。フィッシングサイトの IP アドレス等から、複数のグループが LINE のフィッシングに関与するようになった可能性があります。

またクレジットカードとは違う決済サービスを狙う新たなフィッシングとして、ソフトバンク、ドコモ、au などモバイルキャリアのキャリア決済サービスの不正利用を目的としたフィッシングの報告が増加しました。キャリア決済ではプリペイドカード購入やアプリ（ゲーム）課金等が可能であり、決済限度額まで使用されたという被害報告もありました。
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。

MUFG カードをかたるフィッシング件：1 件
セゾン Net アンサーをかたるフィッシング：1 件
MyJCB をかたるフィッシング：2 件
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
佐川急便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、佐川急便の不在通知メールサービスを装ったショートメッセージ（SMS）から誘導されるフィッシングがありました。SMS から誘導される先のサイトは、当初、Android 端末に不正アプリ（マルウエア）をインストールさせるように作られており、多くの被害が発生していました。それが、8 月になると、Android 端末であるか否かを判定し、Android 端末でない場合には、キャリア決済を不正利用するための情報（電話番号と認証コード）を詐取するフィッシングサイトとして動作するように作り替えられました。これにより一段と被害の件数が増えました。フィッシングサイトのドメインを取得した登録者は大量の類似ドメインを取得しており、それらのドメインへ誘導するフィッシング SMS の報告も少数ながら続いていることから、今後も注意が必要です。

［図 6-1 佐川急便をかたるフィッシングサイト ］

https://www.antiphishing.jp/news/alert/sagawa_20180810.html

6.1.2 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/
2018 年 7 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201807.html
2018 年 8 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201808.html
2018 年 9 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201809.html

6.1.3 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 35 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。

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独自の活動を、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 63 回運営委員会
日時：2018 年 7 月 13 日 16:00 - 18:00
場所：アルプス システム インテグレーション株式会社

第 64 回運営委員会

日時：2018 年 9 月 7 日 16:00 - 18:00

場所：トッパン・フォームズ株式会社

7.2 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ワーキンググループ等の会合の開催の支援と参加を行いました。

技術・制度検討ワーキンググループ会合

日時：2018 年 7 月 13 日 16:00 - 18:00

場所：JPCERT/CC

認証方法調査・推進ワーキンググループ設立タスクフォース会合

日時：2018 年 8 月 3 日 16:00 - 18:00

場所：アルプス システム インテグレーション株式会社

技術・制度検討ワーキンググループ会合

日時：2018 年 8 月 20 日 15:00 - 17:00

場所：JPCERT/CC

STOP. THINK. CONNECT.普及啓発ワーキンググループ会合

日時：2018 年 8 月 23 日 16:00 - 18:00

場所：株式会社 ISAO

認証方法調査・推進ワーキンググループ設立タスクフォース会合

日時：2018 年 9 月 7 日 16:00 - 18:00

場所：株式会社 ISAO

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（4 月～6 月）]
（2018 年 7 月 12 日）
https://www.jpcert.or.jp/press/2018/vulnREPORT_2018q2.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 4～6 月)
（2018 年 8 月 2 日）
https://www.jpcert.or.jp/tsubame/report/report201804-06.html
https://www.jpcert.or.jp/tsubame/report/TSUBAMEReport2018Q1.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) Cobalt Strike Beacon を検知する Volatility Plugin(2018-07-31)
Cobalt Strike はインシデント対応演習などで使用される商用のペネトレーションツールですが、一部で攻撃者に悪用されていることを確認しています。Cobalt Strike を使った攻撃を受けたマシンでは、Cobalt Strike Beacon と呼ばれるモジュールがメモリ上に送り込まれてエージェントとして機能しています。Cobalt Strike Beacon はメモリ上にしか存在しないので、ファイルを検査するタイプのウイルス対策ソフトでは検知できません。Cobalt Strike を使った攻撃を検知できるようにするため、JPCERT/CC では Cobalt Strike Beacon がメモリ上に存在しているかどうかを調べるツールを開発しました。このツールと使用方法を本記事では解説しています。

Cobalt Strike Beacon を検知する Volatility Plugin(2018-07-31)
https://www.jpcert.or.jp/magazine/acreport-cobaltstrike.html

(2) Sysmon ログを可視化して端末の不審な挙動を調査 ～SysmonSearch～(2018-09-06)
マイクロソフトが提供するツール Sysmon は Windows の詳細な挙動を記録することができるため、インシデント調査に有用なツールです。しかし、Sysmon によって記録されたログを分析するためのツールがないため、あまり活用されていません。そのため JPCERT/CC では、Sysmon ログを可視化して分析をサポートするツール SysmonSearch を作成し公開しました。本記事では、SysmonSearch のインストール方法を解説しています。

Sysmon ログを可視化して端末の不審な挙動を調査 ～SysmonSearch～(2018-09-06)
https://www.jpcert.or.jp/magazine/acreport-SysmonSearch.html

9. 主な講演活動

(1) 久保 啓司（脆弱性コーディネーショングループ マネージャー）:
「IoT 機器のインシデント対応の現場から」
IoT セキュリティフォーラム 2018,2018 年 7 月 31 日
(2) 藤井 吉弘（制御システムセキュリティ対策グループ）:
「制御システムセキュリティの動向とその対策」
いま OT が危ない！ RSA と始める制御系システムのセキュリティ対策，2018 年 8 月 22 日
(3) 佐々木 勇人（早期警戒グループ リーダー）:
「技術だけじゃない、インシデント対応に求められるポイント」
株式会社マイナビ「インシデント事例に学ぶ! 漏洩を前提とした備えと事故対応」 ，2018 年 9 月 14 日
(4) 洞田 慎一（早期警戒グループ マネージャー）:
「止まらない情報漏えい～ユーザができることサービス提供者ができること～」
日経 BP 社 情報セキュリティ戦略セミナー2018,2018 年 9 月 27 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) 第14回IPAひろげよう情報モラル・セキュリティコンクール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1日～9月7日

(2) Hardening Project 2018

主　催：Web Application Security Forum Hardening Project実行委員会,内閣府 沖縄総合事務局

開催日：2018年7月5日～7月7日

(3) Internet Week2018

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：2018年11月27日～11月30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　：secure-coding@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