

JPCERT/CC 活動概要 [2016 年 10 月 1 日 ~ 2016 年 12 月 31 日]**活動概要トピックス****ー トピック1ー APCERT 年次総会 2016 の開催 (10 月 24 日 - 27 日)**

APCERT はアジア太平洋地域の各経済地域を代表する CSIRT を中心に構成されたコミュニティです。JPCERT/CC はその事務局を務めるとともに運営委員会メンバーとしてリーダーシップをとってきました。10 月には、JPCERT/CC が現地ホストとなり、その年次総会が 24 日から 27 日にかけて東京で開催され、各経済地域を代表するオペレーショナルメンバー 28 チームから 23 チーム (JPCERT/CC を含む) が参加しました。APCERT 年次総会は、各経済地域における最近のインターネットセキュリティ動向やインシデント対応の事例、調査・研究活動等を共有することを目的に、毎年開催されてきましたが、東京で開催されるのは 2003 年に APCERT が設立されて以来初めてです。JPCERT/CC はホストチームとして本会合の企画から当日の進行全体を主導しました。

また、一般に公開して 10 月 27 日に開催された講演会には、APCERT メンバー組織や国内外の CSIRT、サイバーセキュリティ関連組織からの参加者を中心に、約 30 の国・地域から、計 150 人余りが参加しました。

APCERT 年次総会についての詳細は、次の Web ページをご参照ください。

APCERT Annual General Meeting & Conference 2016

<https://www.apcert.org/apcert2016/>

ー トピック2ー 制御システムセキュリティに関する JPCERT/CC の新たな取り組み

制御システムにおけるサイバー脅威は年々増してきており、2015 年末に発生したウクライナの大規模停電に見るように、海外ではサイバー攻撃により制御システムが甚大な被害をこうむる事態が発生しています。

JPCERT/CC では、そのような制御システムに対するサイバー脅威が増大していることを鑑み、制御システムのセキュリティ対策の促進のため、本四半期に新たに制御システムセキュリティアセスメントサービスを開始するとともに制御システムセキュリティに関する次の 2 件の資料を公開しました。

- ・「制御システムセキュリティに関するアセットオーナー実態調査」の公開
- ・制御システムセキュリティ自己評価ツールのダウンロードサービス開始と英語版公開

JPCERT/CC が 2016 年 12 月に国内のアセットオーナーを対象として開始した制御システムセキュリティアセスメントサービスにより、アセットオーナーは社内体制やポリシー、システムなどの現状の問題点を、第三者の観点から包括的に把握することができます。また、本サービスの提供を通じて、JPCERT/CC はアセットオーナーの制御システムセキュリティの実態を把握し、それらから見えてくる改善策などを制御システムセキュリティの普及啓発に広く役立てていきます。

今四半期においては 3 組織に先行してアセスメントの実施調整、事前説明を行い、次の四半期のサービス開始に向けた準備を進めています。

制御システムセキュリティアセスメントサービスの詳細は次の Web ページをご参照ください。

制御システムセキュリティアセスメントサービス

<https://www.jpccert.or.jp/ics/ics-assessment.html>

また、国内のアセットオーナーのセキュリティに対する認識や対策状況の把握を目的として実施したアンケート調査をまとめた「2015 年度 制御システムセキュリティに関するアセットオーナー実態調査」を公開しました。

本調査では、制御システムのアセットオーナー 318 組織から回答いただき、制御システムネットワークの構成や、それら設備へのセキュリティ対策など 12 問にわたる設問への回答をまとめています。

2015 年度 制御システムセキュリティに関するアセットオーナー実態調査

<https://www.jpccert.or.jp/ics/document.html#asset-owner-survey>

さらに、これまで申込み頂いた国内企業や組織に個別に提供していましたが「制御システムセキュリティ自己評価ツール (J-CLICS)」を、より広く活用いただけるようダウンロードサービスを開始しました。また、日本法人の海外拠点などでの利用を念頭に J-CLICS 英語版の提供も開始しました。

制御システムセキュリティ自己評価ツール (J-CLICS) および英語版

<https://www.jpccert.or.jp/ics/jclics.html>

なお、JPCERT/CC Web 英語ページからもダウンロードサービスをご利用いただけます。

Industrial Control System Self-assessment Tool (J-CLICS)

<https://www.jpccert.or.jp/english/cs/jclics.html>

今日では、ソフトウェア等の脆弱性情報を公表する際に CVE 番号と呼ばれる符号を付して脆弱性を特定しやすいようにしています。JPCERT/CC では、情報セキュリティ早期警戒パートナーシップで公表する脆弱性に対する CVE 番号^{【注1】}の付与を 2008 年 5 月から開始し、2010 年には、CVE 番号を自組織で付与する権限をもつ CVE Numbering Authority (CNA) に認定されるなど、米国 MITRE 社が管理運営する Common Vulnerability and Exposures (CVE) プロジェクトと連携を図ってまいりました。

CVE プロジェクトには、運営方針等に関する意思決定を行う CVE Board と呼ばれる会議体があり、CVE 番号をグローバルに迅速かつ混乱なく安定的に付与するための運用について検討を行っています。このたび、情報流通対策グループに所属する情報セキュリティアナリスト内山貴之が推薦を受け CVE Board による投票を経て CVE Board のメンバーに選出されました。

CVE Board のメンバーへの選出について内山は、「日本の『情報セキュリティ早期警戒パートナーシップ』の脆弱性情報の流通活動のみならず、アジア太平洋地域における同様の取り組みを通じて得られた知見をフィードバックすることにより、CVE の仕組みを強化しグローバルな脆弱性情報の流通をより実効性の高いものにすべく貢献していきたい。」と述べています。

New CVE Board Member from JPCERT/CC

https://cve.mitre.org/news/archives/2016/news.html#december152016_New_CVE_Board_Member_from_JPCERT/CC

活動開始 20 周年を迎えて

JPCERT/CC は 2016 年 10 月 1 日をもちまして、活動開始 20 周年を迎えました。これもひとえに、インシデント被害の低減のためご協力いただいた、国内外の多くの皆様の支えがあったからこそと深く感謝申し上げます。これからも技術と人と人との信頼関係を大切に活動していく所存です。今後とも変わらぬご指導ご支援を心からお願い申し上げます。

本活動は、経済産業省より委託を受け、「平成 28 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. 主な執筆活動」、「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。

目次

1. 早期警戒.....	7
1.1. インシデント対応支援.....	7
1.1.1. インシデントの傾向.....	7
1.1.2. インシデントに関する情報提供のお願い.....	9
1.2. 情報収集・分析.....	10
1.2.1. 情報提供.....	10
1.2.2. 情報収集・分析・提供（早期警戒活動）事例.....	12
1.3. インターネット定点観測.....	12
1.3.1. インターネット定点観測システム TSUBAME の運用、および観測データの活用.....	13
1.3.2. TSUBAME 観測データに基づいたインシデント対応事例.....	16
1.3.3. TSUBAME WORKSHOP 2016 の開催（2016年10月25日）.....	16
2. 脆弱性関連情報流通促進活動.....	16
2.1. 脆弱性関連情報の取扱状況.....	16
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.....	16
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.....	17
2.1.3. 連絡不能開発者とそれに対する対応の状況等.....	21
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.....	21
2.2. 日本国内の脆弱性情報流通体制の整備.....	22
2.2.1. 日本国内製品開発者との連携.....	23
2.2.2. 製品開発者との定期ミーティングの実施.....	23
2.3. 脆弱性の低減方策の研究・開発および普及啓発.....	24
2.3.1. CERT コーディングスタンダードのルールを更新.....	24
2.3.2. セキュアコーディング出張 세미나.....	24
2.4. VRDA フィードによる脆弱性情報の配信.....	25
3. 制御システムセキュリティ強化に向けた活動.....	27
3.1 情報収集分析.....	27
3.2 制御システム関連のインシデント対応.....	27
3.3 関連団体との連携.....	28
3.4 制御システム向けセキュリティ自己評価ツールの配付.....	28
3.5 「制御システムセキュリティに関するアセットオーナー実態調査」の公開.....	28
3.6 制御システムセキュリティ自己評価ツールのダウンロードサービス開始と英語版公開.....	28
3.7 制御システムセキュリティアセスメントサービス開始.....	29
4. 国際連携活動関連.....	29
4.1 海外 CSIRT 構築支援および運用支援活動.....	29
4.1.1. インドネシア、カンボジア、ラオス、ミャンマー、ベトナム、東ティモールへの CSIRT 運用支援.....	29
4.1.2. アフリカ CSIRT 構築支援（11月22日 - 29日）.....	30
4.2 国際 CSIRT 間連携.....	31
4.2.1 APCERT (Asia Pacific Computer Emergency Response Team).....	31

4.2.2	FIRST (Forum of Incident Response and Security Teams).....	34
4.2.3	国際 CSIRT 間連携に係る海外カンファレンス等への参加.....	35
4.2.4	海外 CSIRT 等の来訪および往訪.....	38
4.3	その他の活動ブログや Twitter を通した情報発信.....	38
5.	日本シーサート協議会（NCA）事務局運営.....	39
5.1	概況.....	39
5.2	第 15 回シーサートワーキンググループ会.....	40
5.3	日本シーサート協議会 運営委員会.....	40
6.	フィッシング対策協議会事務局の運営.....	41
6.1	情報収集 / 発信の実績.....	41
6.2.	フィッシングサイト URL 情報の提供.....	44
6.3.	講演活動.....	44
6.4.	フィッシング対策協議会の活動実績の公開.....	45
7.	フィッシング対策協議会の会員組織向け活動.....	45
7.1	運営委員会開催.....	45
7.2	フィッシング対策セミナー 2016 開催.....	46
7.3	第 12 回 IPA「ひろげよう情報モラル・セキュリティコンクール」2016 にフィッシング対策協議会が後援....	46
8.	公開資料.....	47
8.1	脆弱性関連情報に関する活動報告レポート.....	47
8.2	インターネット定点観測レポート.....	47
8.3	分析センターだより.....	47
9.	主な講演活動.....	49
10.	主な執筆活動.....	51
11.	協力、後援.....	51

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」といいます。）に関する報告は、報告件数ベースで **4036** 件、インシデント件数ベースでは **4122** 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 **2883** 件でした。前四半期の **2122** 件と比較して **36%**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なっています。

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.jpccert.or.jp/pr/2016/IR_Report20160714.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 **521** 件で、前四半期の **467** 件から **12%**増加しました。また、前年度同期（**474** 件）との比較では、**10%**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	10月	11月	12月	国内外別合計 (割合)
国内ブランド	24	47	63	134(26%)
国外ブランド	88	106	85	279(54%)
ブランド不明 ^(注2)	27	32	49	108(21%)
月別合計	139	185	197	521(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。

国内ブランドを装ったフィッシングサイトについては、前四半期に引き続き、Webメールのアカウント情報を狙った事例が多く報告されました。国内通信事業者のWebメールのログイン画面を装ったフィッシングサイトが、10月末から継続して確認されており、これらのフィッシングでは、メールに記載された短縮URLから実際のフィッシングサイトへ誘導する傾向が見られました。また、10月末と11月後半には、国内の複数の大学のWebメールのログイン画面を装ったフィッシングサイトの報告が寄せられました。この中には、異なる大学で、同じ海外の無料Webサイト作成サービスが使用されているものもあることから、これらは同一の攻撃者によるフィッシングである可能性が考えられます。

オンラインゲームを装ったフィッシングサイトは、10月と11月以降とで、被害ブランドやサイトが設置されるホスティングサービスに変化が見られましたが、前四半期に引き続き、フィッシングサイトで使用されていたほとんどのドメインは、無料で取得できる.ccドメインでした。

金融関係の国内ブランドのフィッシングサイトでは、クレジットカード情報を窃取しようとするものが多く確認された一方、銀行を装ったフィッシングサイトはごく少数にとどまりました。

フィッシングサイトの調整先の割合は、国内が38%、国外が62%であり、前四半期(国内25%、国外75%)に比べ、国内での調整が増加しています。

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、688件でした。前四半期の554件から24%増加しています。

Webサイトのトップページに、index_old.phpという名の不正なPHPファイルを読み込むスクリプトが埋め込まれる改ざんについて情報提供があり、11月14日に、「Webサイト改ざんに関する注意喚起」を公開しました。不正なPHPファイルが読み込まれると、WebサイトにアクセスしたIPアドレスやブラウザのユーザーエージェント、アクセス時刻などをログとして記録するようになるため、攻撃のための情報を収集される可能性があります。

前四半期に引き続き、Web サイト改ざんについて多数の報告が寄せられており、改ざんされた Web サイトの多くは WordPress などの CMS が使用されていました。また、Magento という CMS を使用した国内の多数の E コマースサイトに、クレジットカード番号などを窃取するスクリプトが埋め込まれているという報告が寄せられました。各サイトを調査したところ、複数のサイトに不正なスクリプトが埋め込まれていることを確認したため、改ざんされたサイトの管理者へ対応を依頼しました。

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、15 件でした。前四半期の 10 件から 50%増加しています。本四半期は、延べ 7 組織に対応を依頼しました。

前四半期のインシデント報告対応レポートで紹介した、多数の C2 サーバを使用する高度な標的型攻撃について対応を進めています。この一連の攻撃で使用されたマルウェアの、C2 サーバとして使われた機器の管理者に対して、機器を調査し、攻撃者が設置したファイル・プログラムなどを採取して提供してもらえるよう依頼しました。

提供いただいた事例には、攻撃者が侵入した痕跡が残っているにも関わらず、マルウェアの通信先に指定された URL に該当するプログラムファイルが存在しない例や、既存のプログラムファイルに不審な変更の痕跡がない例がありました。これは、攻撃者が C2 サーバとして悪用できるように準備はしたが、実際には一度も使用されなかった事例の可能性があります。

その他に、本四半期は、マルウェアが添付されたなりすましメールに関する報告が複数寄せられました。10 月後半に報告されたなりすましメールに添付されていたのは、ダウンローダと呼ばれる種類のマルウェアであり、PlugX と呼ばれる遠隔操作マルウェアの通信先として 8 月末に確認されていた IP アドレスのホストから、別のマルウェアをダウンロードすることが確認されました。

11 月後半には、PDF ファイルと実行ファイルを含む ZIP ファイルが添付されたなりすましメールの報告が寄せられました。この実行ファイルは、外部から命令を受信して動作する遠隔操作型のマルウェアであることが分析により分かりました。このマルウェアの通信先サーバは、同時期に別の国内組織に送付された、なりすましメールに添付されていたマルウェアの通信先とも一致していることから、ほぼ同時期に複数の国内組織が同じような攻撃を受けていた可能性があります。

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ェ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」（限定配信）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.jpccert.or.jp>) や RSS、約 32,000 名の登録者を擁するメーリングリスト、早期警戒情報の受信者用のポータルサイト WAISE (Watch and Warning Analysis Information for Security Experts) 等を通じて、本四半期は次のような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まとめ、次のようなお知らせとして発行しました。

発行件数：1 件 <https://www.jpccert.or.jp/update/2016.html>

2016-12-15 長期休暇に備えて 2016/12

1.2.1.2. 注意喚起

深刻かつ影響範囲の広い脆弱性等について、次のような注意喚起情報を発行しました。

発行件数：17 件（うち 4 件更新） <https://www.jpccert.or.jp/at/>

2016-10-05 ISC BIND 9 サービス運用妨害の脆弱性 (CVE-2016-2776) に関する注意喚起 (更新)

2016-10-12 2016 年 10 月 Microsoft セキュリティ情報 (緊急 5 件含) に関する注意喚起 (公開)

2016-10-12 Adobe Flash Player の脆弱性 (APSB16-32) に関する注意喚起 (公開)

2016-10-12 Adobe Reader および Acrobat の脆弱性 (APSB16-33) に関する注意喚起 (公開)

2016-10-13 2016 年 10 月 Microsoft セキュリティ情報 (緊急 5 件含) に関する注意喚起 (更新)

2016-10-19 2016 年 10 月 Oracle Java SE 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)

- 2016-10-27 Adobe Flash Player の脆弱性 (APSB16-36) に関する注意喚起 (公開)
- 2016-10-28 2016年10月 Microsoft セキュリティ情報 (緊急 5件含) に関する注意喚起 (更新)
- 2016-10-28 Adobe Flash Player の脆弱性 (APSB16-36) に関する注意喚起 (更新)
- 2016-11-02 ISC BIND 9 サービス運用妨害の脆弱性 (CVE-2016-8864) に関する注意喚起 (公開)
- 2016-11-09 Adobe Flash Player の脆弱性 (APSB16-37) に関する注意喚起 (公開)
- 2016-11-09 2016年11月 Microsoft セキュリティ情報 (緊急 6件含) に関する注意喚起 (公開)
- 2016-11-14 Web サイト改ざんに関する注意喚起 (公開)
- 2016-12-14 Adobe Flash Player の脆弱性 (APSB16-39) に関する注意喚起 (公開)
- 2016-12-14 2016年12月 Microsoft セキュリティ情報 (緊急 6件含) に関する注意喚起 (公開)
- 2016-12-21 インターネットに接続された機器の管理に関する注意喚起 (公開)
- 2016-12-22 SKYSEA Client View の脆弱性(CVE2016-7836)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情報も掲載しています。

発行件数 : 13件 <https://www.jpccert.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 14 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 14 件でした。

- 2016-10-05 NISC が「サイバーセキュリティ国際キャンペーン」を開始
- 2016-10-13 経済産業省が広報誌「METI Journal 経済産業ジャーナル平成 28 年 10・11 月号」を公開
- 2016-10-19 IUS-CERT が「Heightened DDoS Threat Posed by Mirai and Other Botnets」公開
- 2016-10-26 第 9 回 日・ASEAN 情報セキュリティ政策会議
- 2016-11-02 IPA が「情報セキュリティ対策ベンチマーク バージョン 4.5」と「診断の基礎データの統計情報」を公開
- 2016-11-09 IPA が「セキュア・プログラミング講座 (2016 年 10 月)」を公開
- 2016-11-16 JPCERT/CC が「制御システムセキュリティ自己評価ツール(J-CLICS)」を公開
- 2016-11-24 JPCERT/CC が「インターネット定点観測レポート(2016 年 7~9 月)」を公開
- 2016-11-30 ネットワークカメラや家庭用ルータ等の IoT 機器を使用する際はパスワードの変更を
- 2016-12-07 LDAP サーバを探索するアクセスの増加
- 2016-12-14 2017 年 1 月 1 日に「うるう秒」を挿入
- 2016-12-21 NISC が「ネットワークビギナーのための情報セキュリティハンドブック」を公開
- 2016-12-28 長期休暇に備えて 2016/12

1.2.1.4. 早期警戒情報

JPCERT/CC では、国民の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等を「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.jpccert.or.jp/wwinfo/>

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。

【インターネットに接続された機器の管理に関する注意喚起】

監視カメラやストレージ機器、特定産業向け組み込み通信機器、DVR（デジタルビデオレコーダー）などがマルウェアに感染し、ボットネットとして大規模な DDoS 攻撃に悪用されていることが、世界中のセキュリティ専門家から指摘されています。JPCERT/CC では、国内においても脆弱性や設定の不備によりマルウェアに感染した機器が、対策が行われていない他の機器を探索するために送信するパケットの増加を確認したことから、2016 年 12 月 21 日に注意喚起を公開しました。同注意喚起では、定点観測システム TSUBAME による観測状況をお伝えするとともに、マルウェアの機能や機器の管理者が行う対策について説明しました。

【Web サイト改ざんに関する注意喚起】

Web サイトのトップページに index_old.php という名の不正なファイルを読み込ませる処理が追加された Web サイトが国内で複数確認されました。この改ざんにより、Web サイト閲覧者等の情報がログとして記録されることから、攻撃者は、Web サイトが水飲み場攻撃における「水飲み場」として悪用できるか調査している可能性が考えられます。これを受け、2016 年 11 月 14 日に、JPCERT/CC および警察庁から、Web サイト改ざんに関する注意喚起を公開しました。

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ェア、攻撃ツールの情報などと対比して分析することで、攻撃活動や攻撃の準備活動等の把握に努めています。

1.3.1. インターネット定点観測システム TSUBAME の運用、および観測データの活用

JPCERT/CC は、さまざまな地域に設置された観測用センサーを含むインターネット定点観測システム TSUBAME を構築運用するとともに、観測されたデータを各地域の CSIRT と共同で分析するためのプロジェクトである TSUBAME プロジェクトの事務局を担当しています。2016年12月末時点で、観測用センサーは21地域26組織に設置されています。今後も設置地域を拡大し、より充実したセンサー網の構築と共同分析の高度化を進めるべく、海外諸国のナショナル CSIRT 等に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.jpccert.or.jp/tsubame/index.html>

JPCERT/CC は、TSUBAME で収集したデータを宛先ポート番号や送信元地域ごとに分類して統計分析し、既知の脆弱性情報やマルウェア、攻撃ツール等との関連を考察することで、攻撃活動や準備活動の捕捉に努めています。

主に日本企業のシステム管理者等の方々に、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、2016年7月から9月分のレポートを2016年11月16日に公開しました。

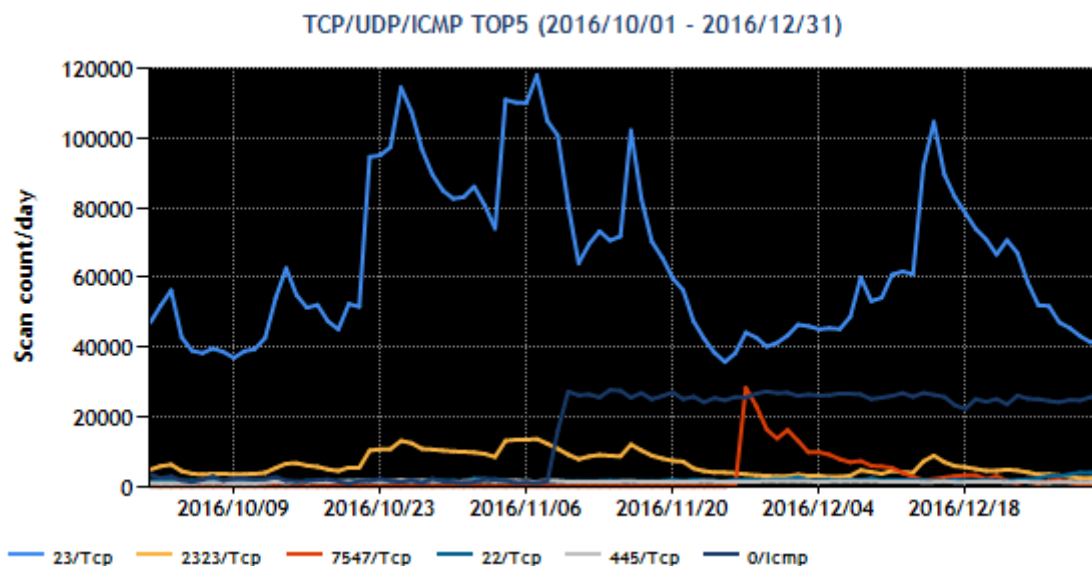
TSUBAME 観測グラフ

<https://www.jpccert.or.jp/tsubame/index.html#examples>

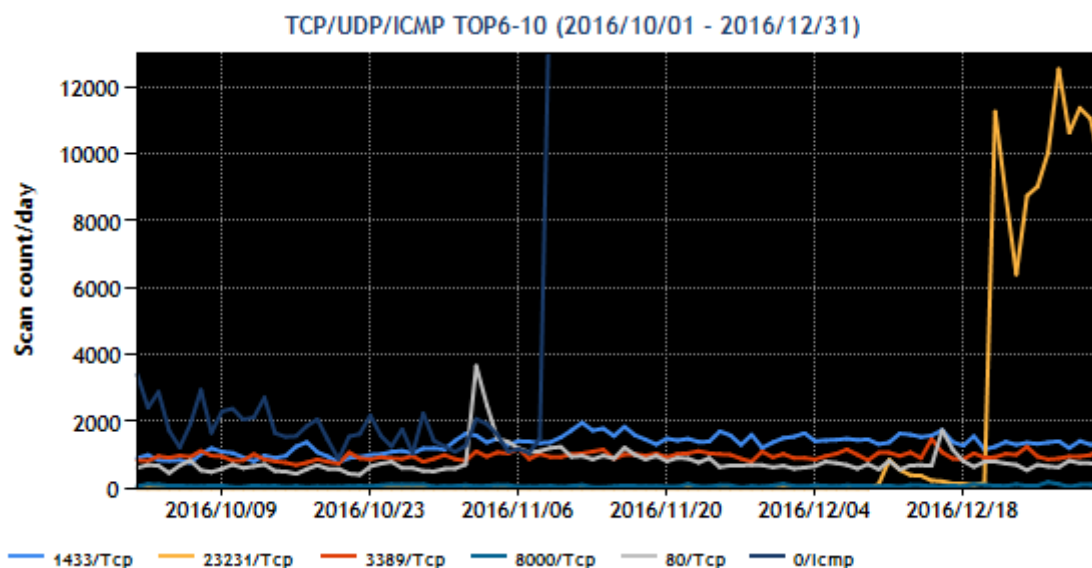
インターネット定点観測レポート (2016年7~9月)

<https://www.jpccert.or.jp/tsubame/report/report201607-09.html>

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位~5位および6位~10位を、[図 1-1] と [図 1-2] に示します。



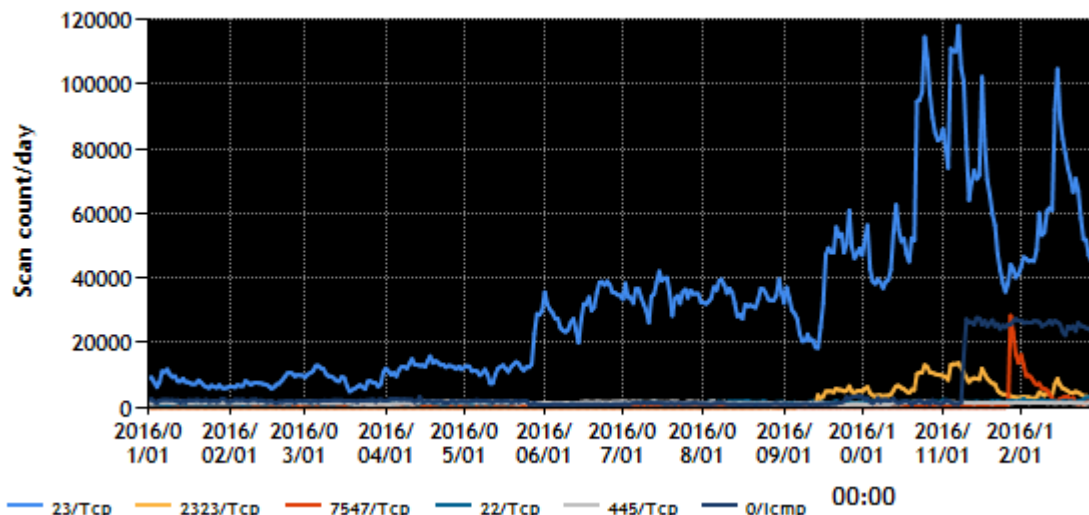
[図 1-1 宛先ポート別グラフ トップ 1-5 (2016 年 10 月 1 日-12 月 31 日)]



[図 1-2 宛先ポート別グラフ トップ 6-10 (2016 年 10 月 1 日-12 月 31 日)]

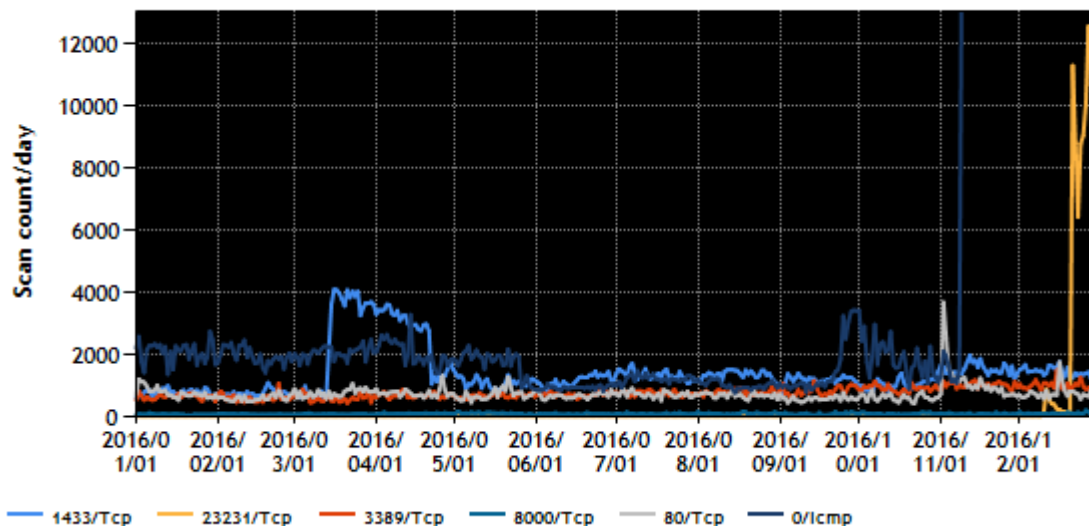
また、過去 1 年間 (2016 年 1 月 1 日-2016 年 12 月 31 日) における、宛先ポート別パケット数の上位 1 位～5 位および 6 位～10 位を [図 1-3] と [図 1-4] に示します。

TCP/UDP/ICMP TOP5 (2016/01/01 - 2016/12/31)



[図 1-3 宛先ポート別グラフ トップ 1-5 (2016年1月1日-2016年12月31日)]

TCP/UDP/ICMP TOP6-10 (2016/01/01 - 2016/12/31)



[図 1-4 宛先ポート別グラフ トップ 6-10 (2016年1月1日-2016年12月31日)]

本四半期は、23/TCP、2323/TCP 宛のパケットが多く観測されました。2323/TCP 宛パケットは9月6日頃から現在に至るまで継続して観測しています。

送信元であるインターネットに接続された監視カメラやルータ、NASなどのさまざまな専用機器にマルウェアを感染させ、さらなる感染拡大を目的にパケットを盛んに送信していると推測されます。

その他、Windows や同 OS 上で動作するサービスをスキャンする活動や、遠隔操作できる SSH サーバ等のサービスをスキャンする活動と見られるパケットも、順位に変動はありますが、これまで同様に多く観測されました。

1.3.2. 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処をしています。主な事例を次に掲げます。

(1) 国内外の 23/TCP,2323/TCP ポートを探索するサーバについての対応

複数の日本国内の IP アドレスを送信元とする、Telnet (23/TCP) ポート宛てのパケットが前四半期から継続して本四半期も多数観測されました。これら 23/ TCP 宛 や Telnet が動作している 23/TCP とは異なる Port 番号宛の多数のパケットが、Telnet ポートの探索や同ポートに対する攻撃を行うマルウェアと関連していると推測し、送信元 IP アドレスにどのような機器が接続されているかを調べました。その結果、これまで見つかっていなかった複数のベンダ製の機器がマルウェアに感染してパケットを送信していることが判明しました。JPCERT/CC では、当該機器の製造ベンダと送信元 IP アドレスの管理者が国内外であるか否かに拘わらず、各々に情報を提供して適切な対処を求めました。

1.3.3. TSUBAME WORKSHOP 2016 の開催 (2016 年 10 月 25 日)

2016 年 10 月の APCERT 年次会合において TSUBAME Workshop 2016 を開催しました。TSUBAME プロジェクト参加組織から約 50 名が参加しました。TSUBAME Workshop 2016 では、JPCERT/CC から TSUBAME プロジェクトの活動報告とハンズオン演習を実施しました。活動報告では、日本製の組み込み製品などが踏み台となった事例を報告し、ハンズオン演習では、TSUBAME で蓄積したデータから、パケット数の推移等をもとに傾向の変化を見極め、メンバー間での情報共有やインシデント対応を行うための方法を習得していただきました。

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、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扱状況

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「ソフトウェア等脆弱性情報取扱基準」(平成 26 年経済産業省告示第 110 号。以下「本基準」といいます。)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。本基準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、本基準を踏まえて取りまとめられた「情報セキュリティ早期警戒パートナーシップガイドライン (以下「パートナーシップガイドライン」といいます。))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扱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/>

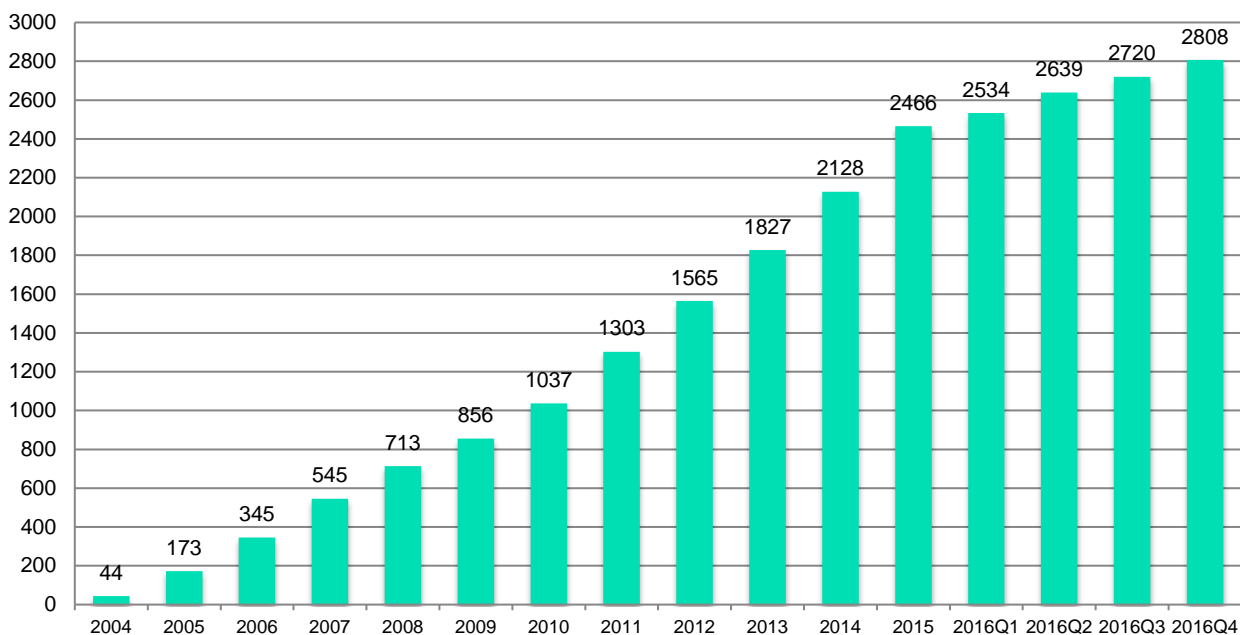
2.1.2. Japan Vulnerability Notes（JVN）において公表した脆弱性情報および対応状況

JVN で公表している脆弱性情報は、本基準に従って国内で届け出られた脆弱性に関するもの（「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。以下「国内取扱脆弱性情報」といいます。）と、それ以外の脆弱性に関するもの（「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。以下「国際取扱脆弱性情報」といいます。）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、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 88 件（累計 2,808 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/>



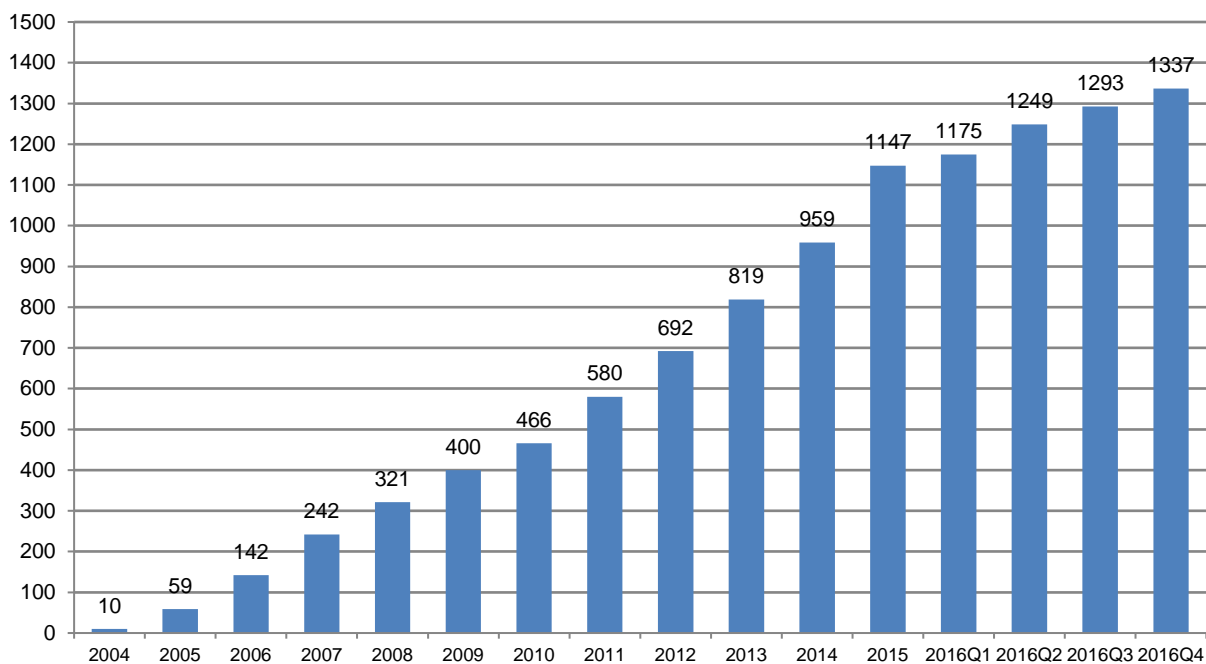
[図 2-1 JVN 公表累積件数]

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 44 件（累計 1,337 件）で、累計の推移は [図 2-2] に示すとおりです。44 件のうち、36 件が国内製品開発者の製品、8 件が海外の製品開発者の製品に関連したものでした。また、36 件の国内製品開発者の製品のうち半数の 18 件が自社製品届出による脆弱性情報でした。本制度を利用した自主的な脆弱性情報公開が、日本国内の製品開発者において徐々に浸透してきていると考えられます。

本四半期に公表した脆弱性情報の件数の、影響を受けた製品のカテゴリ別の内訳は、[表 2-1] のとおりでした。本四半期は、グループウェア、無線 LAN ルータ等の組込系製品、Windows アプリの脆弱性情報が多く、それに続いて Android アプリ、CMS、ウェブアプリ、ライブラリ等の脆弱性情報が多くありました。

[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別内訳]

製品分類	件数
グループウェア	13
組込系	10
Windows アプリ	6
Android アプリ	2
CMS	2
ウェブアプリ	2
ライブラリ	2
API	1
BBS	1
IT 資産管理用ツール	1
ウェブブラウザ	1
サーバ製品	1
プラグイン	1
ミドルウェア	1



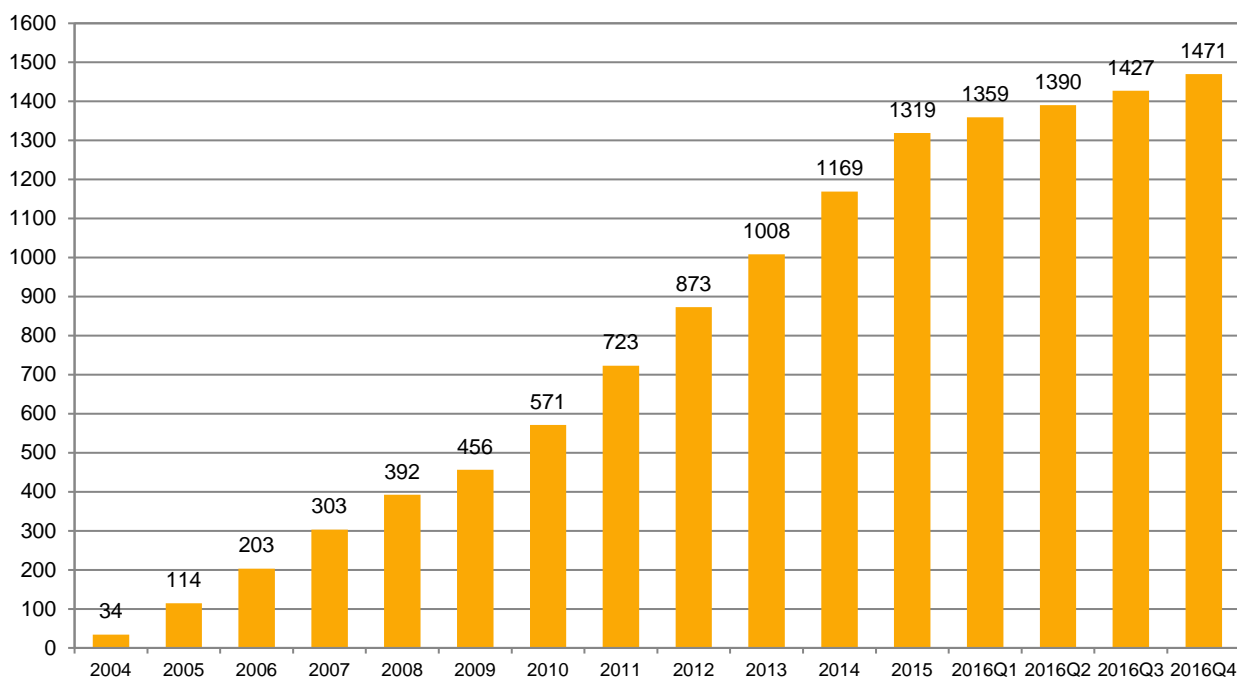
[図 2-2 公表を行った国内取扱脆弱性情報の累積件数]

本四半期に公表した国際取扱脆弱性情報は 44 件（累計 1,471 件）で、累計の推移は [図 2-3] に示すとおりです。この 44 件には、大規模な攻撃に悪用された複数の IoT 機器の脆弱性に関する情報や、攻撃コードが公開されている特定製品に対する注意喚起（Technical Alert）が含まれます。

本四半期に公表した脆弱性情報の、影響を受けた製品のカテゴリ別内訳は、[表 2-2] のとおりでした。2016 年を通して、非常に多くの組込系製品に関する脆弱性情報を公表してきましたが、本四半期においても、10 件の組込系製品の脆弱性情報を公表しました。その中でもルータ機器に関する脆弱性情報が特に多くありました。また、国内製品開発者と同様に、海外製品開発者からも、自社製品の脆弱性対応に関する事前通知等が JPCERT/CC に報告される事例が徐々に増えてきています。

[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別内訳]

製品分類	件数
組込系	10
MacOS アプリ	4
ウェブサーブレットコンテナ	3
サーバ製品	3
スマホアプリ	3
ライブラリ	4
DNS	2
Windows アプリ	2
ウェブアプリ	2
Android アプリ	1
iOS アプリ	1
Linux カーネル	1
Linux 用アプリ	1
ウェブサービス	1
ウェブブラウザ	1
制御系	1
データ処理ツール	1
プラグイン	1
メディアプレイヤー	1
衛星テレビアンテナ	1



[図 2-3 国際取扱脆弱性情報の公表累積件数]

2.1.3. 連絡不能開発者とそれに対する対応の状況等

本基準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 250 件（製品開発者数で 163 件）を公表し、45 件（製品開発者数で 27 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、新たに 3 件を連絡不能開発者一覧に掲載しました。本四半期末日時点で、合計 205 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ケースについて、本規準およびパートナーシップガイドラインが 2014 年 5 月に改正され、利用者保護の観点から脆弱性情報を公表する手続きが定められました。この規定に従って、2014 年 11 月より、公表判定委員会が定期的開催されており、その審議により、これまでに 2 案件を公表し、その他に、公表すべきと判定されている 5 案件の公表準備を進めています。

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 CPNI、フィンランドの CERT-FI 等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一層広がっています。また、米国の ICS-CERT との連携も、2013 年末より活発化しており、本四半期までに合計 13 件の制御システム用製品の脆弱性情報を公表しました。新たな分野での国際的活動が定着しつつあると言えます。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 63 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合を必要とする特殊なケース (全体の 1 割弱) を除いて、JVN 上で公表する脆弱性のほぼすべてに CVE 番号が付与されています。

CVE の運営や管理に係る意思決定を行う CVE Board と呼ばれる会議体に今期 JPCERT/CC のスタッフが選出されました。今後 CVE の運営により密接に関わり、脆弱性情報の流通を円滑にする調整機関としての役割を果たすことが JPCERT/CC に期待されています。CVE Board への選出については、【トピック 3- JPCERT/CC 職員が CVE Board のメンバーに JPCERT/CC スタッフが就任】をご参照ください。

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、本基準に従って、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>

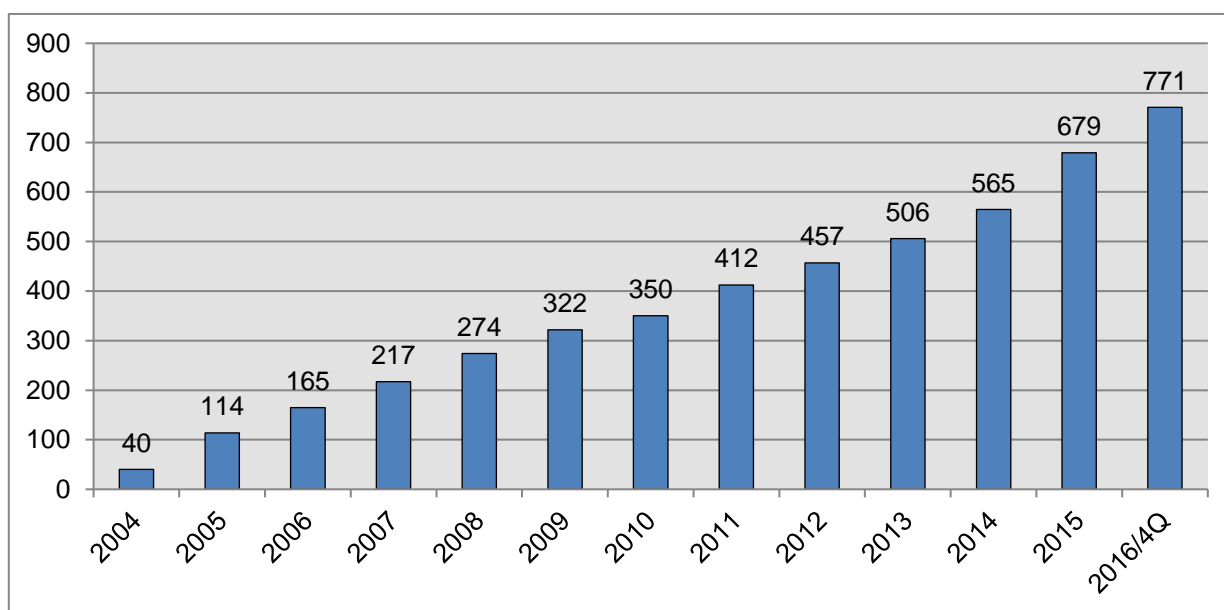
2.2.1. 日本国内製品開発者との連携

本基準では、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、2016年12月31日現在で 771 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。

JPCERT コーディネーションセンター製品開発者リスト登録規約

<https://www.jpccert.or.jp/vh/agreement.pdf>



[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、脆弱性情報ハンドリング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、脆弱性情報ハンドリングにご協力いただいている製品開発者の皆さまとのミーティングを定期的に開催しています。

本四半期は 2016 年 11 月 18 日にミーティングを開催し、最近の脆弱性の動向や事例分析、製品開発者による脆弱性再現手法の研究事例、攻撃活動の収集事例などを紹介するとともに、それらに関する製品開発者との意見交換を行いました。



[図 2-5 製品開発者との定期ミーティングの様子]

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. CERT コーディングスタンダードのルールを更新

JPCERT/CC では、CMU/SEI のセキュアコーディングプロジェクトが提供している CERT C Coding Standard および CERT Oracle Coding Standard for Java を邦訳して提供しています。これは C 言語や Java 言語におけるセキュアコーディングを実践するためのルール集で、その内容は日々更新されています。本四半期に邦訳を更新したルールは次のとおりです。

内容の更新 (2 件)

- FLP30-C. 浮動小数点変数をループカウンタに使用しない
- FLP32-C. 数学関数における定義域エラーおよび値域エラーを防止または検出する

CERT C コーディングスタンダード

<https://www.jpccert.or.jp/sc-rules/>

2.3.2. セキュアコーディング出張 세미나

JPCERT/CC では、ソフトウェア製品等の開発を行う企業・組織を対象に、セキュアコーディングに関する出張セミナー (有償) の実施を承っています。本四半期は、C/C++ セキュアコーディングセミナーおよび Java セキュアコーディングセミナーを、それぞれ国内ベンダ 1 社に対して実施しました。

- 出張セミナーのご依頼、お問い合わせは、secure-coding@jpccert.or.jp までご連絡ください。

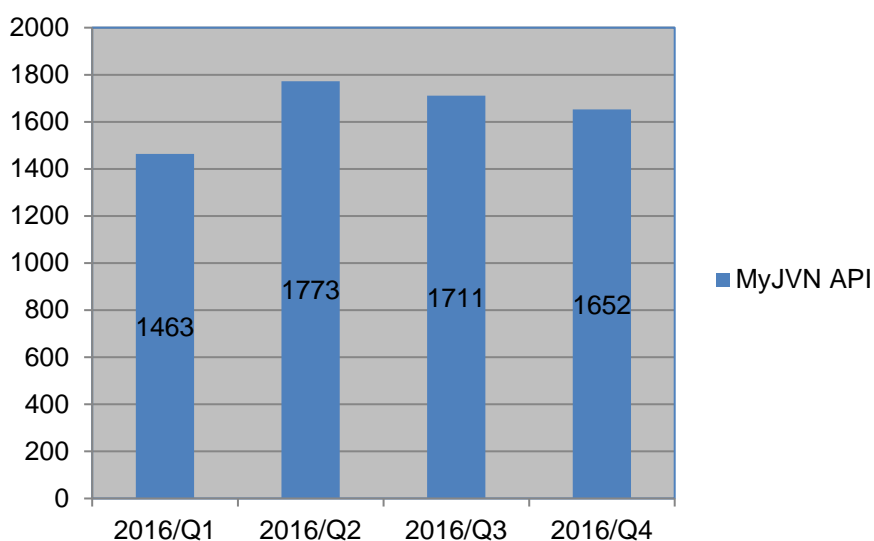
2.4. VRDA フィードによる脆弱性情報の配信

JPCERT/CC は、大規模組織の組織内 CSIRT 等での利用を想定して、KENGINE 等の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。

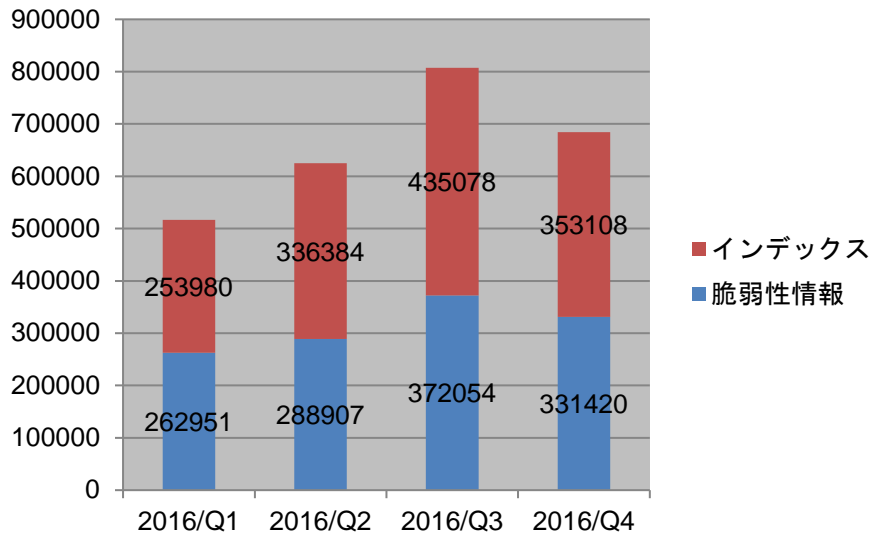
VRDA フィード 脆弱性脅威分析用情報の定型データ配信

<https://www.jpccert.or.jp/vrdafeed/index.html>

四半期ごとに配信した VRDA フィード配信件数のデータソース別の内訳を [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 2-7] 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 2-8] 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。

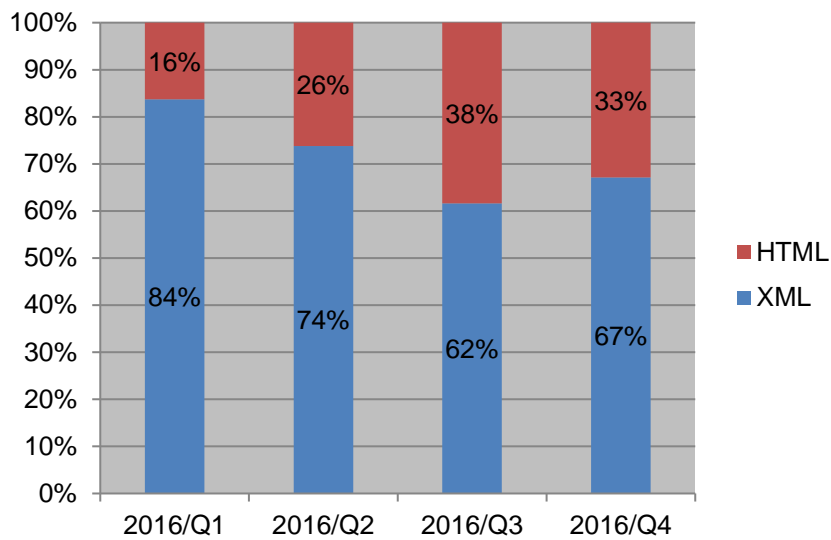


[図 2-6 VRDA フィード配信件数]



[図 2-7 VRDA フィード利用件数]

[図 2-7] に示したように、インデックスの利用数については、前四半期と比較し、約 19%減少しました。脆弱性情報の利用数についても、約 11%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]

[図 2-8] に示したように、本四半期の脆弱性情報のデータ形式別利用傾向については、前四半期と比較し、目立った変化は見られませんでした。

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。本四半期で収集・分析した情報は **381** 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 **2** 件でした。

- 2016/11/30 【参考情報】 サンフランシスコ市交通局でのランサムウェア感染について（個社向け）
- 2016/12/20 【参考情報】 ウクライナのキエフ周辺で再び停電発生（個社向け）

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。

発行件数：3 件

2016-10-06 制御システムセキュリティニュースレター 2016-0009

2016-11-10 制御システムセキュリティニュースレター 2016-0010

2016-12-06 制御システムセキュリティニュースレター 2016-0011

制御システムセキュリティ情報共有コミュニティには、現在 **590** 名の方にご登録いただいています。今後も内容の充実を図っていく予定です。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

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** 件でした。本四半期に寄せられた、インターネットからアクセスできる制御システム関連機器に関する報告のうち、ISP 管理の **48** 件の IP アドレスについて調査を行い、外部から不正に操作される可能性がある **41** 件に対して危険性を伝えました。また、SHODAN をはじめとするインターネット・ノード検索システム等のインターネット上の公開情報を分析し、外部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を保有する国内の組織に対して情

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配付

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）や J-CLICS（制御システムセキュリティ自己評価ツール）を配付しています。本四半期は、日本版 SSAT に関して 8 件、J-CLICS に関して 7 件の利用申込みがありました。直接配付件数の累計は、日本版 SSAT が 216 件、J-CLICS が 329 件となりました。

3.5 「制御システムセキュリティに関するアセットオーナー実態調査」の公開

11 月 15 日に JPCERT/CC から「2015 年度 制御システムセキュリティに関するアセットオーナー実態調査」を公開しました。本資料は、制御システムを所有する国内のアセットオーナーの方々のセキュリティに対する認識や対策状況の把握を目的として、アンケート方式による実態調査を実施し、その結果をまとめたものです。制御システムネットワークの構成や、それら設備へのセキュリティ対策、マルウェアの感染経験、セキュリティ動向や今後の制御システムセキュリティ対策への取り組みに対する認識など、12 問にわたるアンケート調査を、さまざまな業界をカバーするよう選んだ、従業員 300 人以上を擁し制御システムを所有する国内のアセットオーナー（2,308 組織）に対して行い、318 組織からいただいた回答をもとに本資料は作成されています。本資料の詳細については、次の Web ページをご参照ください。

制御システムセキュリティに関するアセットオーナー実態調査

<https://www.jpccert.or.jp/ics/document.html#asset-owner-survey>

3.6 制御システムセキュリティ自己評価ツールのダウンロードサービス開始と英語版公開

これまで JPCERT/CC では、制御システムセキュリティ自己評価ツールの提供について、お申し込みを頂いた国内企業や組織に個別に提供してまいりましたが、より多くの皆さまにご利用いただけるように 11 月 10 日よりダウンロード提供を開始いたしました。

J-CLICS は、制御システムセキュリティの問題点を抽出・把握していただくことを目的としたチェックリストと、チェックリストの各設問で問われている対策項目について解説した設問項目ガイドで構成されており、制御システムにおける効果的なセキュリティ対策を立案・実施するための参考資料としてご活用いただけます。

また、日本法人の海外拠点でもご利用いただけるように J-CLICS 英語版も 12 月 15 日にあわせて公開いたしました。

J-CLICS についての詳細は、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自己評価ツール (J-CLICS) および英語版

<https://www.jpccert.or.jp/ics/jclics.html>

なお、JPCERT/CC Web 英語ページからもダウンロードサービスをご利用いただけます。

Industrial Control System Self-assessment Tool (J-CLICS)

<https://www.jpccert.or.jp/english/cs/jclics.html>

3.7 制御システムセキュリティアセスメントサービス開始

JPCERT/CC は、日本国内の制御システムセキュリティの実態把握と利用組織におけるセキュリティの向上を目的として、制御システムセキュリティアセスメントサービスを開始すべく、準備を進めています。本四半期においては、アセスメントに先行する実施調整と事前説明を 3 組織に対して行いました。次の四半期にサイトアセスメントを実施する予定です。3 組織に加えて、さらに実施組織を増やすことを目的として、JPCERT/CC の Web ページにて、一般募集も開始しました。今後応募のあった組織に対しては実施可否を判断し、次の四半期にて順次アセスメントを実施する予定です。

本アセスメントの実施にあたっては、アセスメントのベースとなる評価基準（日本版 SSAT、および、米国 NIST のドキュメント）をもとにチェックシートを作成し、各評価項目に対する判断基準を決めました。また、その判断基準に基づいてスコア配分を決め、アセスメント結果レポートのフォーマットを作成しました。

本アセスメントの実施により得られた知見・データに関しては、関連する組織名等が特定できないように配慮した上で、JPCERT/CC が開催する制御システムセキュリティカンファレンスなどの場において、制御システム利用者の注意を喚起するためなどに広く活用していく予定です。

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、トレーニング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。

4.1.1. インドネシア、カンボジア、ラオス、ミャンマー、ベトナム、東ティモールへの CSIRT 運用支援 (10 月 4 日 - 6 日)

独立行政法人国際協力機構 (JICA) が「情報セキュリティ能力向上プロジェクト」の一環としてインドネシアのジャカルタでログ解析研修を開催し、JPCERT/CC 職員が講師として派遣されました。インドネ

シア、カンボジア、ラオス、ミャンマー、ベトナム、東ティモール、ブルネイの7ヶ国の National CSIRT および関係組織の技術者に対して、JPCERT/CC は APT 攻撃の概要説明と、ログ分析ハンズオン、Active Directory への攻撃デモ、ネットワークフォレンジックのトレーニングを行いました。JICA の「情報セキュリティ能力向上プロジェクト」の詳細については、次の Web ページをご参照ください。

JICA 情報セキュリティ能力向上プロジェクト

<http://www.jica.go.jp/project/indonesia/014/index.html>



[図 4-1 研修参加者との集合写真]

4.1.2. アフリカ CSIRT 構築支援（11 月 22 日 - 29 日）

本四半期に、モーリシャスで開催された AFRINIC-25 にアフリカ CSIRT 構築支援の一環として参加しました。AFRINIC-25 は AFRINIC（African Network Information Centre）が主催する、アフリカのインターネットの発展に携わる産官学の多様な人々を対象としたイベントです。アフリカの ICT における技術動向や政策等に関して、国際コミュニティとの交流を図るとともに、現状と課題について話し合うことを目的に 2004 年から毎年 2 回開催（前期は Africa Internet Summit（AIS）と同時開催）されており、今回で 25 回目になります。11 月 25 日から 11 月 30 日のイベント中に 240 名が参加しました。

JPCERT/CC は、AfricaCERT（アフリカコンピュータ緊急対応チーム）から依頼を受けて、情報技術の向上を目的としたワークショップにおいて 11 月 25 日から 3 日間にわたってネットワークフォレンジック、マルウェア解析トレーニングを行いました。JPCERT/CC が行ったトレーニングには、地元のモーリシャスをはじめ、ケニアやマダガスカルといった近隣の国々から、のべ 21 名が参加しました。



[図 4-2 マルウェア解析トレーニング参加者との集合写真]

情報セキュリティに関する制度や技術が成長段階にある国・地域からのサイバー攻撃は、日本のインターネットユーザの脅威の一つとなっています。JPCERT/CC では、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起因するインシデントの増加に備え、事態が発生した際に迅速かつ円滑な対応ができるよう、同地域の技術力の向上と連携の基盤づくりを目的に、CSIRT の構築・運営とそれらを支える人材の育成に 2010 年から取り組んでいます。

4.2 国際 CSIRT 間連携

インシデント対応における連携強化および各国のインターネット環境の整備や情報セキュリティ関連活動の取り組み状況の共有を目的として、海外の National CSIRT との国際連携を強化するための活動を行っています。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、継続して APCERT の事務局を担当しています。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.jpccert.or.jp/english/apcert/>

4.2.1.1. APCERT 年次総会 2016 の開催 (10 月 24 日 - 27 日)

アジア太平洋地域の CSIRT コミュニティである APCERT の年次総会を、10 月 24 日から 27 日にかけて東京で、JPCERT/CC が現地ホストとして開催しました。APCERT の主要メンバーであるオペレーショナルメンバー (全 28 チーム) から JPCERT/CC を含む 23 チームが参加しました。APCERT 年次総会は、各経済地域における最近のインターネットセキュリティ動向、インシデント対応の事例、調査・研究活動

等を共有することを目的に、毎年開催されています。今回は「Borderless Cooperation, Seamless Action – Towards a Cleaner, Greener Cyber Space」をテーマに掲げました。概要は次のとおりです。

1) 日程：

- 10/24 (月) 午前：APCERT ワーキンググループ会合
午後：APCERT Team Building, Welcome Cocktail (懇親会)
- 10/25 (火) 午前：TSUBAME, CyberGreen ワークショップ
午後：APCERT 運営委員会 (SC Meeting)
- 10/26 (水) 午前：メンバー向けカンファレンス (Closed Conference)
午後：APCERT 年次総会 (Annual General Meeting)
- 10/27 (木) 終日：一般公開講演 (Open Conference)

2) 会場：ロイヤルパークホテル (東京都中央区)

3) 主な決定事項等：

APCERT 運営委員会および年次総会では、APCERT 各チームの活動に関する調査やメンバー向けのオンライントレーニングを引き続き行うことでそれぞれのスキルを伸ばし、ひいては組織全体としてさらなる能力向上を目指していくことで合意しました。また、アジア太平洋地域の国にあって APCERT への加盟がまだ実現していない National CSIRT に対して継続してアプローチをするとともに、加盟へ向けた支援をメンバー間で協力して行い、APCERT の連携をさらに強化していくことが提案されました。

さらに、APCERT 議長チームおよび副議長チームの改選が行われ、CERT Australia (オーストラリアのコンピュータ緊急対応チーム) が議長チームとして、MyCERT (マレーシアコンピュータ緊急対応チーム) が副議長チームとしてそれぞれ再選されました。JPCERT/CC は、引き続き APCERT の主要メンバーとしてさまざまな活動をリードしてまいります。

メンバー向けカンファレンスや一般公開講演においては、インシデントや脆弱性への対応事例、サイバー脅威動向、IoT、クラウドセキュリティ、モバイルセキュリティ等に関する講演ならびに CSIRT としての組織の在り方について話し合うパネルディスカッションが行われました。



APCERT Annual General Meeting & Conference 2016
24 - 27 October, 2016 – Tokyo, Japan

[図 4-3 APCERT 年次総会集合写真]

APCERT 年次総会についての詳細は、次の Web ページをご参照ください。

APCERT Annual General Meeting & Conference 2016

<https://www.apcert.org/apcert2016/>

4.2.1.2. TSUBAME Workshop 2016 の開催（10 月 25 日）

JPCERT/CC が主導する「TSUBAME プロジェクト」は、APCERT ではワーキンググループの一つとして位置づけられた活動です。JPCERT/CC は APCERT 年次総会の会期中に本プロジェクトのワークショップを開催しました。TSUBAME Workshop 2016 の詳細については、本活動概要の次の項目をご参照ください。

1.3.3. TSUBAME Workshop 2016 の開催（10 月 25 日）

4.2.1.3. サイバークリーンワークショップの開催（10 月 25 日）

「サイバークリーン」は、インターネット環境の健全性と利用に伴うリスクを各国／地域間で比較できる定量的な評価指標を用いてセキュリティ対策の実効性を確認することで、健全なサイバー空間を効率的に実現することを目的とする、JPCERT/CC が主導している取り組みです。APCERT 年次総会の会期中に本プロジェクトのワークショップが開催され、APCERT や OIC-CERT（イスラム協力機構コンピュータ緊急対応チーム）の加盟チームを含む約 85 名が参加しました。ワークショップでは、指標（Green Index）の開発状況やサイバークリーンを活用したリスク削減（mitigation）の手法等について JPCERT/CC の国際部部長 伊藤友里恵から、現下のポータルサイトの使い方等について CSIRT Foundry のホズレイ氏から、また、ユーザの立場から見たサイバークリーンへの期待についてシンガポール CSA（サイバーセキュリティ庁）のチューン氏から講演があり、会場の参加者を交えた意見交換を行いました。サイバークリーン

についての詳細は、次の Web ページをご参照ください。

実証実験：サイバーグリーンプロジェクト（Cyber Green Project）

<https://www.jpCERT.or.jp/research/cybergreen.html>

サイバーグリーン情報サイト

<http://www.cybergreen.net/>

サイバーグリーン統計サイト

<http://stats.cybergreen.net/>

4.2.2 FIRST (Forum of Incident Response and Security Teams)

JPCERT/CC は、FIRST の活動にも 1998 年の加盟以来、積極的に参加しています。現在は JPCERT/CC の国際部シニアアナリスト 小宮山功一朗が FIRST の理事を務めており、本四半期は組織運営に関わる議論に参画しました。FIRST および理事の詳細については、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 FIRST Regional Symposium for Arab and African Regions への参加(11 月 2 日 - 3 日)

11 月 2 日から 3 日にエジプトのシャルム・エル・シェイクで開催された FIRST Regional Symposium for Arab and African Regions において、2 日間のマルウェア解析トレーニングを行いました。このシンポジウムは、アラブ諸国およびアフリカ地域の ICT 関係者に対する、セキュリティ技術の向上を目的として、FIRST が主催したイベントです。アラブ諸国を中心に約 120 名が参加しました。JPCERT/CC が行ったトレーニングには、エジプトをはじめ、アラブ諸国やアフリカ地域から約 30 名が参加しました。FIRST Regional Symposium for Arab and African Regions についての詳細は、次の Web ページをご参照ください。

FIRST Regional Symposium for Arab and African Regions

<https://www.first.org/events/symposium/egypt2016>



[図 4-4 FIRST Regional Symposium for Arab and African Regions トレーニング風景]

4.2.3 国際 CSIRT 間連携に係る海外カンファレンス等への参加

4.2.3.1 APEC TEL 54 への参加（11 月 1 日）

10 月 31 日から 11 月 4 日に京都で開催された APEC TEL（APEC Telecommunications and Information Working Group）54 において、JPCERT/CC が推進している取り組みであるサイバークリーンプロジェクトについて紹介し、APEC 地域におけるサイバークリーンの普及啓発活動を行いました。APEC TEL は、APEC に参加しているエコノミーにおいて情報電気通信分野を担当する政府機関を中核とする会合です。

4.2.3.2 Sri Lanka Cyber Security Week（CSW）2016 への参加（11 月 1 日 - 2 日）

Sri Lanka Cyber Security Week 2016 は Sri Lanka CERT|CC（スリランカコンピュータ緊急対応チームコーディネーションセンター）が主催する国際会議です。JPCERT/CC はサイバークリーンプロジェクトについて紹介し、現在作成中のグリーンインデックス（インターネットの健全性とリスクを表す指標）について発表を行いました。

具体的には、現在の取り組みの一環として、ShadowServer の Open Resolver / Open NTP（mode 6）/ Open NTP（mode 7）/ Open SSDP のリスクを評価するための計数として用い、各リスク要因の密度の偏差値を指標とする案を説明しました。この指標案により、以下のような状況把握が可能となります。

- ある国について偏差値を見ることで、その国が全体の中でどの程度のセキュリティレベルにあるかを知ることができる。
- ある国について各リスクの偏差値を比較することで、その国のインターネットセキュリティのレベル上の長所と弱点を知ることができる。
- 長所と弱点を知ることにより、対策を行う優先順位を決めることができる。

インターネットの健全性向上の一環として、具体的かつ客観的な指標の重要性について普及啓発活動を行う機会となりました。



[図 4-5 CSW 2016 発表風景]

4.2.3.3 OASIS 主催 Borderless Cyber Asia 2016 への参加（11 月 1 日 - 2 日）

11 月 1 日から 2 日に慶應義塾大学三田キャンパスで、グローバルな情報社会のためのオープン標準の策定や普及をしている国際的な非営利団体 OASIS および慶應義塾大学の共催による Borderless Cyber Asia 2016 が開催されました。JPCERT/CC は本カンファレンスを後援するとともに、サイバーグリーンプロジェクトの構想と取り組みについて講演し、政府関係者やセキュリティ関連企業等の参加者に向けて、本プロジェクトを通じたサイバー空間のクリーンアップ活動を呼びかけました。

4.2.3.4 HKICC2016 への参加（11 月 21 日 - 22 日）

The Hong Kong International Computer Conference (HKICC) 2016 は、HKCS（Hong Kong Computer Society）が主催し、今年で開催 39 回目を迎える香港の代表的な IT カンファレンスです。JPCERT/CC は本カンファレンスに参加し、サイバーインテリジェンスの共有とプライバシーをテーマとするセッションにおいて、APT 攻撃への備えと対応等に関する JPCERT/CC の活動を紹介し、関係者と意見交換を行いました。



[図 4-6 HKICC2016 発表風景]

4.2.3.5 米国 US-CERT との年次会合、第 12 回日米重要インフラ防護フォーラムへの参加（11 月 30 日 - 2 日）

JPCERT/CC は、インシデント対応で協力関係にある DHS（国土安全保障省）傘下の US-CERT（米コンピュータ緊急対応チーム）や ICS-CERT（産業制御システムサイバー緊急対応チーム）といった米国の組織との年次定期会合を 11 月 30 日にワシントン D.C.で行いました。各組織の活動状況や日米におけるインシデント動向、インシデント対応における連携等について情報共有および意見交換を行い、今後も密な連携を維持していくことを確認しました。

また、12 月 1 日から 2 日にかけて開催された第 12 回日米重要インフラ防護フォーラムに参加し、日米の重要インフラ事業者におけるサイバーセキュリティの問題について情報収集を行いました。

4.2.3.6 IGF 2016 への参加（12 月 6 日 - 9 日）

12 月 6 日から 9 日にかけてメキシコのグアダハラで開催された IGF (Internet Governance Forum) 2016 に参加し、JPCERT/CC の取り組みやサイバーグリーンプロジェクトについて IGF の参加者に紹介し、プロジェクトの推進に向けて意見交換を行いました。

4.2.3.7 OIC-CERT 年次総会 2016 への参加（12 月 11 日 - 14 日）

イスラム協力機構 (Organization of Islamic Cooperation: OIC) に加盟する国々の CSIRT コミュニティである OIC-CERT の年次総会が 12 月 11 日から 14 日にサウジアラビアのジッダで開催されました。JPCERT/CC は本会合に招聘を受けて参加し、サイバーグリーンプロジェクトの講演を行い、プロジェクトへの参加を呼びかけました。また、JPCERT/CC が行っている標的型攻撃への対応について関係者と情報共有を行うとともに、OIC-CERT の加盟 CSIRT との関係構築に努めました。



[図 4-7 OIC-CERT 年次総会の様子]

4.2.4 海外 CSIRT 等の来訪および往訪

4.2.4.1 英国 NCSC 来訪（10 月 14 日）

英国 NCSC（ナショナルサイバーセキュリティセンター）が来訪し、NCSC および JPCERT/CC の活動状況、英国のサイバーセキュリティ戦略や関連組織の体制等について情報を共有しました。また、今後も脅威情報の共有を通して一層の連携強化を図ることを確認しました。

4.2.4.2 Sri Lanka CERT|CC 往訪（11 月 1 日）

Sri Lanka CERT|CC を往訪し、JPCERT/CC が推進する TSUBAME や IT セキュリティ予防接種等について意見交換を行い、今後もこれらの活動を通して密な連携を維持していくことを確認しました。

4.2.4.3 米国 DHS 来訪（11 月 9 日）

米国 DHS が来訪し、DHS および JPCERT/CC の活動状況、米国のサイバーセキュリティ戦略や取り組みについて情報を共有しました。また、脅威情報の共有について意見交換を行い、今後も一層の連携強化を図ることを確認しました。

4.3 その他の活動ブログや Twitter を通じた情報発信

英語ブログ (<http://blog.jpccert.or.jp/>) や Twitter (@jpccert_en) を通じて、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的に行っています。本四半期は次の記事をブログに掲載しました。

Verification of Windows New Security Features – LSA Protection Mode and Credential Guard（10 月 31 日）

<http://blog.jpccert.or.jp/2016/10/verification-of-ad9d.html>

APT workshop and Log analysis training in Jakarta（11 月 10 日）

<http://blog.jpccert.or.jp/2016/11/apt-workshop-and-log-analysis-training-in-jakarta.html>

APCERT Annual General Meeting & Conference 2016 in Tokyo and JPCERT/CC's 20th Anniversary（11 月 16 日）

<http://blog.jpccert.or.jp/2016/11/apcert-annual-g-3284.html>

Evidence of Attackers' Development Environment Left in Shortcut Files（12 月 5 日）

<http://blog.jpccert.or.jp/2016/12/evidence-of-att-3388.html>

A New Tool to Detect Known Malware from Memory Images – impfuzzy for Volatility –（12 月 16 日）

<http://blog.jpccert.or.jp/2016/12/a-new-tool-to-d-d6bc.html>

5. 日本シーサート協議会 (NCA) 事務局運営

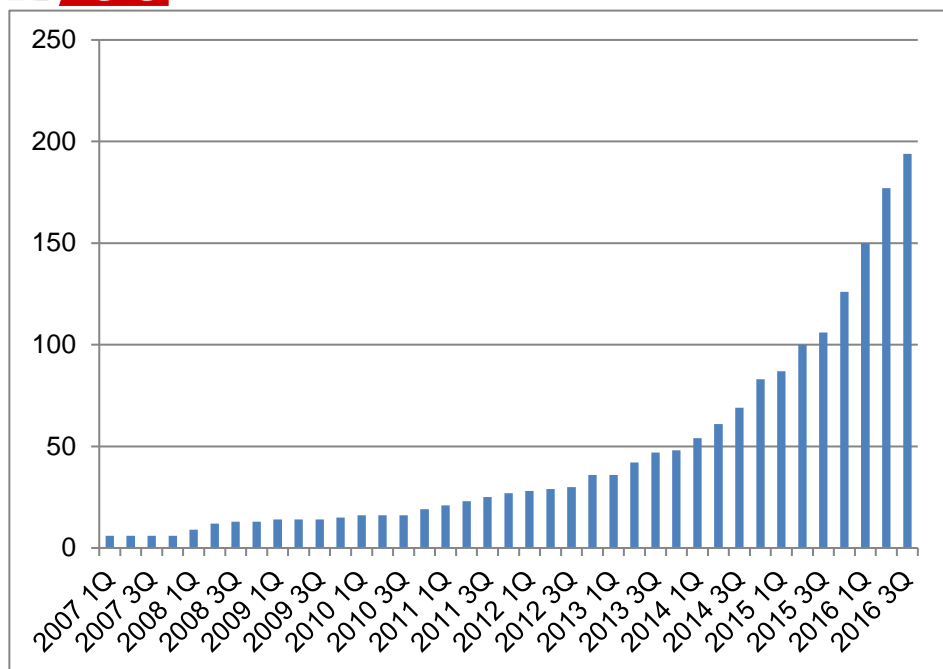
5.1 概況

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 に加盟しました。

株式会社マネーフォワード (MF-CSIRT)
株式会社 NTTPC コミュニケーションズ (NTTPC-CSIRT)
パナソニック ヘルスケアホールディングス株式会社 (PH-CSIRT)
東洋ビジネスエンジニアリング株式会社 (B-EN-G CSIRT)
エム・ユー・フロンティア債権回収株式会社 (MUFRC-CSIRT)
株式会社ニコン (Nikon-CSIRT)
ソニー株式会社 (SONY-JP-SIRT)
三井造船株式会社 (MES-SIRT)
総合警備保障株式会社 (ALSOK-CSIRT)
日商エレクトロニクス株式会社 (NELCO-SIRT)
有限責任 あずさ監査法人 (KJ-CSIRT)
アサヒグループホールディングス株式会社 (ASAHI-CSIRT)
帝人株式会社 (TEIJIN-CSIRT)
株式会社イオン銀行 (ABK-CSIRT)
住友化学株式会社 (SC-CSIRT)
成田国際空港株式会社 (NAA CSIRT)
株式会社ディアイティ (dit-CSIRT)

本四半期末時点で 194 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。



[図 5-1 日本シーサート協議会 加盟組織数の推移]

5.2 第 15 回シーサートワーキンググループ会

第 15 回シーサートワーキンググループ会を次のとおり開催いたしました。

日時：2016 年 12 月 5 日

場所：TDU-CSIRT（東京電機大学） 丹羽ホール

シーサートワーキンググループ会は、日本シーサート協議会の会員およびこれから組織内にシーサートを構築し、日本シーサート協議会への加盟を検討している方々が参加する会合です。会合では、各ワーキンググループの開催報告や特別講演、組織内シーサートの構築や運用に関する課題認識や意見の交換等が行われました。また、新しく加盟した 16 チームが自組織のシーサートチームの概要を紹介しました。

5.3 日本シーサート協議会 運営委員会

3 回の運営委員会を開催いたしました。

第 113 回運営委員会

日時：2016 年 10 月 26 日（水）16:00 - 18:00

場所：トレンドマイクロ株式会社

第 114 回運営委員会

日時：2016 年 11 月 30 日（水）16:00 - 18:00

場所：JPCERT/CC

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（以下「協議会」といいます。）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、協議会名での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。

6.1 情報収集 / 発信の実績

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 22 件発信しました。

本四半期は、LINE をかたるフィッシング事案が頻繁に発生しました。異常なログインがあったとして、「安全認証」と称した偽のサイトで、ログイン ID とパスワードを入力させようとするフィッシングサイトが確認されました。ユーザ数が非常に多いサービスのため、フィッシング対策協議会の緊急情報で注意を促しました。また、以前からあった、クレジットカード会社をかたるフィッシングは、本四半期においても報告が寄せられました。協議会では、名前をかたられた各事業者に、メール本文やサイトの URL 等の関連情報を提供しました。

また、合計 10 件の緊急情報を協議会の Web 上で公開し、広く注意を喚起しました。その内訳は、SNS サービスをかたるフィッシング関連が 3 件、クレジットカード会社をかたるフィッシング関連が 2 件、オンラインゲームをかたるフィッシング関連が 3 件、その他が 2 件でした。それぞれの例として、[図 6-1] に LINE をかたるフィッシング (2016/10/31)、[図 6-2] にセゾン Net アンサーをかたるフィッシング (2016/11/28)、[図 6-3] に NEXON をかたるフィッシング (2016/11/21)の注意喚起を示します。




[図 6-1] LINE をかたるフィッシング (2016/10/31)
https://www.antiphishing.jp/news/alert/line_20161031.html

Netアンサー利用登録フォーム

入力 → 確認 → 完了

Netアンサーにご登録されるカードについて、以下の項目をご入力の上、「確認画面へ」ボタンを押してください。

クレジットカード番号	4541 - - (半角) ※クレジットカード番号が16桁未満の方は左詰めでご入力ください。
有効期限	(月) / (年) (半角) 例)カードの表示「11/18」⇒「(月)11/(年)18」と入力
誕生日	日 選択 年 選択 月 選択 日
セキュリティコード	(半角) カード裏面に印字されている番号の下3桁をご入力ください。 

⚠ メールアドレスはお間違いのないよう、ご入力ください！
ドメイン指定を行っている方は「mail.saisoncard.co.jp」を受領できる様に設定してください。

メールアドレス	パソコン 携帯電話	<input type="text"/>	※どちらか一方は必ずご入力ください
メールマガジン	<input type="checkbox"/> ポイントのキャンペーンやプレゼントなどおトクなメールを受け取る メールマガジンを受け取る場合おトクなの？ 詳しくはこちら ※ メールマガジンの配信を希望されない場合も、ご利用明細のご案内(月1回)・ 重要なお知らせ などのメールは送信させていただきます。 ※ メールマガジンはNetアンサー内にて変更・解除できます。		

⚠ ※誕生日、電話番号、メールアドレスに含まれる数字・アルファベットはセキュリティ上、10・パスワードに使用しない様、お願い申し上げます。

NetアンサーIDの設定	半角の英文字・数字を組合わせた8~16桁で設定してください。	<input type="text"/>	IDの安全性 <input type="checkbox"/>
Netアンサーパスワードの設定	半角の英文字・数字を組合わせた8~16桁で設定してください。	<input type="text"/>	パスワードの安全性 <input type="checkbox"/>

英字の大、小文字、数字、記号(→8の4種のみ)を組合わせた18桁以上の、英文字とは異なる10・パスワードを推奨いたします。
[10・パスワードの安全性について](#)

Netアンサー規約(電磁的方法による請求通知に関する特約含む)及び書面による毎月の請求通知を含む当社からのご案内の送付を断り取り除くことにご同意し、Netアンサー利用登録をいたします。
※同意をいただいた場合であっても、当社の定める条件に該当する場合、当社が必要と認めた場合、及び一部のカードにつきましては、利用明細書を書面にてご自宅に送付する場合がございます。

《セゾン》Netアンサー規約

第1条(本サービス・申込等)

1.《セゾン》Netアンサーとは、株式会社クレディセゾン(以下「当社」といいます)が発行したクレジットカード(一部所定のカードを除く、以下「《セゾン》カード」といいます)の会員が、パーソナルコンピューター等(以下「端末」といいます)からインターネットを介して当社所定のウェブサイト(以下「ウェブサイト」といいます)にアクセスした上で当社所定の方法により依頼をした場合に、当社が提供するサービス(以下「本サービス」といいます)をい

[▶ 利用規約に同意して確認画面へ](#)

[図 6-2] セゾン Net アンサーをかたるフィッシング (2016/11/28)
https://www.antiphishing.jp/news/alert/saison_20161128.html



運営会社 | 利用規約 | プライバシーポリシー | 特定商取引法に基づく表記 | 資金決済法に基づく表記 | 著作権が作ライク | 防犯版 | ゲーム基本情報 | 採用情報

無料ゲームオンラインゲームはNEXON(ネクソン)

Copyright © 2011 NEXON Korea Corporation and NEXON Co., Ltd. All Rights Reserved.



[図 6-3] NEXON をかたるフィッシング (2016/11/21)

https://www.antiphishing.jp/news/alert/nexon_20161121.html

これらのフィッシングに使用されたサイトを停止するための調整を、JPCERT/CC のインシデント対応支援活動を通じて行い、全てのサイトの停止を確認しました。

6.2. フィッシングサイト URL 情報の提供

協議会員のうち、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と、フィッシングに関する研究を行っている学術機関に対し、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、日に数回の頻度で提供しています。この URL 情報の提供は、各社の製品のブラックリストへの追加等、ユーザ保護に向けた取り組みに活用していただくことや、研究教育機関における関連研究の促進を目的としています。本四半期末の時点における情報提供先は 23 組織でした。今後とも複数の事業者との間で新たに情報提供を開始するための協議を行い、提供先を順次拡大していく予定です。

6.3. 講演活動

協議会ではフィッシングに関する現状を紹介し、効果的な対策を呼び掛けるための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。

駒場 一民

「フィッシングの現状と対策 2016」

フィッシング対策セミナー 2016 , 2016 年 11 月 22 日

6.4. フィッシング対策協議会の活動実績の公開

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/>

フィッシング対策協議会 2016 年 10 月 フィッシング報告状況

<https://www.antiphishing.jp/report/monthly/201610.html>

フィッシング対策協議会 2016 年 11 月 フィッシング報告状況

<https://www.antiphishing.jp/report/monthly/201611.html>

フィッシング対策協議会 2016 年 12 月 フィッシング報告状況

<https://www.antiphishing.jp/report/monthly/201612.html>

7. フィッシング対策協議会の会員組織向け活動

フィッシング対策協議会では、経済産業省から委託された活動以外に、会費による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。

7.1 運営委員会開催

本四半期においては、フィッシング対策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。

フィッシング対策協議会 第 43 回運営委員会

日時：2016 年 10 月 13 日 16:00 - 18:00

場所：トレンドマイクロ株式会社

フィッシング対策協議会 第 44 回運営委員会

日時：2016 年 11 月 11 日 10:00 - 12:00

場所：株式会社日立システムズ

フィッシング対策協議会 第 45 回運営委員会

日時：2016 年 12 月 9 日 16:00 - 18:00

場所：トッパン・フォームズ株式会社

7.2 フィッシング対策セミナー 2016 開催

フィッシング対策セミナー 2016 を次のとおり開催しました。

フィッシング対策セミナー 2016

日時：2016年11月22日 13:00 - 18:00

場所：大崎ブライトコアホール（JR 大崎駅 新東口）

東京都品川区北品川5丁目5番15号 大崎ブライトコア3階

講演内容：講演1：「インターネットバンキングに係る不正送金事犯被害の実態と防止策」

講演者1：警察庁 生活安全局 情報技術犯罪対策課 官民連携推進官 宮西 健至氏

講演2：「フィッシングの現状と対策 2016」

講演者2：フィッシング対策協議会（JPCERT/CC）駒場 一民

講演3：「フィッシングサイト対策のこれまでの10年、これからの10年」

講演者3：東京大学 助教 宮本 大輔氏

講演4：「楽天グループにおけるフィッシング事案とその対策」

講演者4：楽天株式会社 サイバー犯罪対策室 室長 増村 洋二氏

講演5：「サイバー犯罪の最新動向と金融機関の取り組みについて」

講演者5：三菱東京UFJ銀行 コンプライアンス統括部 顧客保護推進室 / 室長 松野 善方氏

7.3 第12回 IPA 「ひろげよう情報モラル・セキュリティコンクール」 2016 にフィッシング対策協議会が後援

情報セキュリティが叫ばれる中、小中高生の皆様にもセキュリティ意識を持っていただくために開催された IPA 主催の第12回 IPA 「ひろげよう情報モラル・セキュリティコンクール」 2016 を後援致しました。

「標語」、「ポスター」、「4コマ漫画」の3つの部門において、優秀な作品に対してフィッシング対策協議会の賞を冠し、表彰することといたしました。

3部門の選考結果についての「お知らせ」ページ

https://www.antiphishing.jp/news/info/ipa_competition2016.html

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、ソフトウェア等脆弱性関連情報取扱基準（平成 26 年改正：平成 26 年経済産業省告示 第 110 号）に基づき、2004 年 7 月からそれぞれ受付機関および調整機関として脆弱性関連情報流通制度の一端を担っています。

本レポートは、この制度の運用に関連した本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。

ソフトウェア等の脆弱性関連情報に関する活動報告レポート [2016 年第 3 四半期（7 月～9 月）]
(2016 年 10 月 26 日)

https://www.jpccert.or.jp/press/2016/vulnREPORT_2016q3.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的に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。

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 2016 年 7 月～9 月
(2016 年 11 月 16 日)

<https://www.jpccert.or.jp/tsubame/report/report201607-09.html>

<https://www.jpccert.or.jp/tsubame/report/TSUBAMEReport2016Q2.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基に、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 3 件の記事を公開しました。

(1) ショートカットファイル内に残る攻撃者の開発環境の痕跡(2016-10-11)

アプリケーションを起動したり、OLEのようなアプリケーション間連携を実現したりするための仕組みであるショートカットファイルには、ファイルを作成した日時や環境に関する様々な情報が記録されています。攻撃者が作成したショートカットファイルに記録された情報を抽出し関連付けることで、同じ攻撃者によって作成された可能性があるショートカットファイルを識別することができます。このファイル内に記録された情報から攻撃主体を分類する方法について解説するとともに、攻撃に使われたショートカットファイルを多数収集して、それらに記録された情報を統計的に処理した結果から分かった、攻撃者が使用しているシステム環境の傾向についても紹介しています。

ショートカットファイル内に残る攻撃者の開発環境の痕跡(2016-10-11)

<https://www.jpCERT.or.jp/magazine/acreport-lnkfile.html>

(2) 既知のマルウェアをメモリイメージから簡易に検知できるツールを開発 ～impfuzzy for Volatility～ (2016-11-01)

ファイル形式のマルウェア検体が既知のものかどうかの判定には、ファイル全体のハッシュ値 (MD5 や SHA256 など) を用いてマルウェアハッシュ値のデータベースと照合し、一致するかどうかを確認する方法が使われてきました。しかし、この手法はメモリフォレンジックには利用できないため、既知のマルウェアを発見するために Yara scan によるシグネチャマッチングなどの手法を用いなければならないといった課題がありました。この課題を解決するために開発した、メモリイメージの中から既知のマルウェアを抽出するツール「impfuzzy for Volatility」を紹介しています。

既知のマルウェアをメモリイメージから簡易に検知できるツールを開発 ～impfuzzy for Volatility～ (2016-11-01)

https://www.jpCERT.or.jp/magazine/acreport-impfuzzy_volatility.html

(3) 騙せる PE 解析ツールの Import API 表示機能(2016-11-28)

Windows 実行ファイル (PE ファイル) 形式のマルウェアを分析する際に、PE ファイルの構造をパースし表示をするツール (以下、PE 解析ツール) を使用して、マルウェアがインポートしている API (Import API) あるいはエクスポートしている関数の一覧を調べることがしばしばあります。マルウェアの分析に使用されることが多い PE 解析ツールですが、一方では、PE 解析ツールによる分析を攪乱する手法を持ったマルウェアの存在も既に確認されています。この PE 解析ツールの多くに搭載されている Import API の一覧を表示する機能に誤った情報を表示させて分析者を騙す手口と、それに対抗するために PE 解析ツールに組み込むべき対策方法について解説しました。

騙せる PE 解析ツールの Import API 表示機能(2016-11-28)

<https://www.jpCERT.or.jp/magazine/acreport-fakeINT.html>

9. 主な講演活動

- (1) 洞田 慎一（早期警戒グループ マネージャー）：
「高度サイバー攻撃への備えと対応」
Email Security Conference 2016/第 14 回迷惑メール対策カンファレンス,2016 年 10 月 4,5,7 日
- (2) 久保 正樹（情報流通対策グループ マネージャー）：
「JVN-ニッポンの脆弱性情報発信～脆弱性の届出と公表を支える仕組み～」
CEATEC JAPAN 2016 IPA ブース, 2016 年 10 月 4 日
- (3) 佐々木 勇人（早期警戒グループ 情報セキュリティアナリスト）：
「サイバー攻撃を恐れない会社づくり～社長と部下のリスクコミュニケーション～」
CEATEC JAPAN 2016 IPA ブース, 2016 年 10 月 5 日
- (4) 青木 翔（早期警戒グループ 情報セキュリティアナリスト）：
「SUPER CSIRT MAKER～CSIRT スタートガイド～」
CEATEC JAPAN 2016 IPA ブース, 2016 年 10 月 6 日
- (5) 佐藤 祐輔（エンタープライズサポートグループ リーダー）：
「高度サイバー攻撃（APT）対応のための演習プログラム」
CEATEC JAPAN 2016 IPA ブース, 2016 年 10 月 7 日
- (6) 久保 正樹（情報流通対策グループ マネージャー）、戸田 洋三（同グループ リードアナリスト）：
「セキュアプログラミング Web アプリケーション」
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」,
2016 年 10 月 8 日
- (7) 洞田 慎一（早期警戒グループ マネージャー）：
「組織内 CSIRT の必要性～効果的なインシデント対応体制の実現に向けて～」
一般社団法人衛星放送協会, 2016 年 10 月 13 日
- (8) 久保 正樹（情報流通対策グループ マネージャー）、戸田 洋三（同グループ リードアナリスト）：
第 3 回講義「セキュアコーディング-その重要性」、第 4 回講義「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, 2016 年 10 月 17 日
- (9) 佐々木 勇人（早期警戒グループ 情報セキュリティアナリスト）：
「EC サイトにおけるカード情報漏えい事案の近況と加盟店における対策強化に向けて」
一般社団法人日本クレジット協会 クレジットセプター運営会議, 2016 年 10 月 26 日
- (10) 阿部 真吾（制御システムセキュリティ対策グループ 情報セキュリティアナリスト）：
「インターネットに接続された機器に迫る脅威と JPCERT/CC の取り組み」
第 8 回 TCG 日本支部公開ワークショップ, 2016 年 11 月 2 日
- (11) 村上 晃（経営企画室、エンタープライズサポートグループ部門長兼早期警戒グループ担当部門長）
「組織内部における セキュリティ人材育成とインシデント対応体制の整備」
北海道サイバーテロ対策協議会第 7 回総会サイバーセキュリティセミナー,2016 年 11 月 16 日
- (12) 戸田 洋三（同グループ リードアナリスト）
「CERT コーディングスタンダードのご紹介 ～脆弱性を生まないセキュアコーディングのために～」
Embedded Technology/IoT Technology 2016,2016 年 11 月 17 日

(13) 有村 浩一 (常務理事)

パネルディスカッション「サイバーセキュリティマネジメントに今一番求められていること」
Cyber3 Conference Tokyo 2016, 2016年11月18日

(14) 洞田 慎一 (早期警戒グループ マネージャー) :

「サイバー攻撃への備えと対応体制の必要性」
名古屋大学情報連携統括本部公開講演会・研究会, 2016年11月22日

(15) 青木 翔 (早期警戒グループ 情報セキュリティアナリスト) :

「CSIRT ケーススタディ- 実態調査から見えた CSIRT 構築・運営の勘所」
ITC 埼玉経営研修セミナー, 2016年11月26日

(16) 松田 亘 (早期警戒グループ 情報セキュリティアナリスト) :

「ECサイトの未来を守るためにセキュリティができること」
MeetMagento 2016, 2016年11月22日

(17) 満永 拓邦 (早期警戒グループ 技術アドバイザー) :

「サイバー攻撃への備えと対応について」
JPCERT/CC サイバー攻撃対策セミナーin 関西, 2016年11月24日

(18) 阿部 真吾 (制御システムセキュリティ対策グループ 情報セキュリティアナリスト) :

「サイバー攻撃が制御系システムにもたらす脅威」
JPCERT/CC サイバー攻撃対策セミナーin 関西, 2016年11月24日

(19) 松田 亘 (早期警戒グループ 情報セキュリティアナリスト) :

「ログ分析の必要性と JPCERT/CC の取り組み」
JPCERT/CC サイバー攻撃対策セミナーin 関西, 2016年11月24日

(20) 村上 晃 (経営企画室、エンタープライズサポートグループ部門長兼早期警戒グループ担当部門長)

「高度サイバー攻撃を見据えたインシデント対応とは」
これから始めるサイバーセキュリティ対策セミナー, 2016年11月29日

(21) 村上 晃 (経営企画室、エンタープライズサポートグループ部門長兼早期警戒グループ担当部門長)

「セキュリティ対策における運用とインシデント対応体制～被害を極小化するための CSIRT の役割とその運用の勘所～」
富士通セキュリティ関連セミナー, 2016年11月30日

(22) 久保 正樹 (情報流通対策グループ マネージャー)

「情報セキュリティ早期警戒パートナーシップのいま」
Internet Week 2016, 2016年12月1日

(23) 清水 友基 (早期警戒グループ 情報セキュリティアナリスト) :

「CSIRT 構築・運用の勘所について～インシデントに迅速に対応するために～」
しんきん情報システム研究会, 2016年12月9日

(24) 戸田 洋三 (情報流通対策グループ リードアナリスト)

「職業的情報学 I」
千葉大学理学部数学・情報数理学科, 2016年12月22日

10. 主な執筆活動

- (1) 松田 亘（早期警戒グループ 情報セキュリティアナリスト）：
「第2章 構築と運用 4.設備やシステム」
エヌ・ティ・ティ出版株式会社 日本シーサート協議会 編著「CSIRT（シーサート）：構築から運用まで」，
2016年11月17日

11. 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) Security Days Fall 2016 / Email Security Conference 2016 / ID Management Conference 2016
主 催：株式会社ナノ・オプトメディア、一般財団法人インターネット協会
開催日：2016年10月3日～7日
- (2) 情報セキュリティワークショップ in 越後湯沢 2016
主 催：NPO新潟情報セキュリティ協会（ANISec） 情報セキュリティワークショップin越後湯沢
実行委員会
開催日：2016年10月7日～8日
- (3) CODE BLUE
主 催：CODE BLUE実行委員会
開催日：2016年10月18日～21日
- (4) Internet Week2016
主 催：一般社団法人日本ネットワークインフォメーションセンター
開催日：2016年11月29日～12月2日
- (5) 第13回デジタル・フォレンジック・コミュニティ2016inTOKYO
主 催：特定非営利活動法人デジタル・フォレンジック研究会、デジタル・フォレンジック・コミュニティ2016実行委員会
開催日：2016年12月12日～13日
- (6) 第12回IPAひろげよう情報モラル・セキュリティコンクール2016
主 催：独立行政法人情報処理推進機構（IPA）
開催日：2016年04月1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/>

PGP Fingerprint : FC89 53BB DC65 BD97 4BDA D1BD 317D 97A4 69EC E048

■ 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>

PGP Fingerprint : B3C2 A91C AE92 50A9 BBB2 24FF B313 E0E1 0DDE 98C1

■ 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 : 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

本文書を引用、転載する際には JPCERT/CC 広報 (pr@jpcert.or.jp) 宛にご連絡をお願いします。最新情報については JPCERT/CC の Web サイトをご参照ください。

■ JPCERT コーディネーションセンター(JPCERT/CC)

<https://www.jpcert.or.jp/>