JPCERT-PR-2015-03
発行日：2015-07-14

JPCERT/CC 活動概要 [2015 年 4 月 1 日 ～ 2015 年 6 月 30 日]

活動概要トピックス

ートピック1ー　66 組織に対して高度なサイバー攻撃に遭っている可能性を連絡

本四半期、JPCERT/CC は、標的型攻撃等の高度なサイバー攻撃に遭っている可能性のある 66 組織に対し、その旨を通知しました。そのうち 44 組織への連絡は、Emdivi と呼ばれる遠隔操作マルウエアに関連したものでした。Emdivi を使った攻撃は、多数の国内組織に対して長期間に亘って行なわれ、内部ネットワークにまで侵入された組織では、Active Directory サーバやファイルサーバ等が侵害を受け、個人情報等の様々な情報が窃取される被害も出ています。

JPCERT/CC では標的型攻撃に関するインシデント報告等をもとに、使用されたマルウエアやその通信先となる C&C サーバ等の攻撃基盤に関する調査を実施し、調査で得られた情報をもとに、攻撃対象になるかも知れない他の組織への情報提供と、実際に攻撃に遭っていると推察される組織への通知・連絡を行う活動に取り組んでいます。また、調査活動を通じて JPCERT/CC が得た攻撃基盤や攻撃手法に関する情報を集約し、侵害実態の把握を目的に各組織が行う各種ログ調査や汚染端末の特定等の初動対応のために、提供しています。

このような攻撃は、発覚後も手口を変えながら執拗に行われ、外部から不正にアクセスできる状態が維持され続けることもあるため、早期の適切な初動対応が被害拡大の防止のために重要です。攻撃に関する通知・連絡を外部から受けた場合は、まず事実確認を行ない、セキュリティベンダ等と相談をして被害拡大防止のための措置と組織全体に対する影響範囲の調査を行なって下さい。また、事実確認等の初動対応において不明なことがありましたら JPCERT/CC にご相談下さい。

標的型攻撃に関する連絡への対応のお願い
https://www.jpcert.or.jp/incidentcall/index.html

また、本四半期から、インシデント報告対応レポートのインシデント件数のカテゴリ分類項目として「標的型攻撃」を新しく追加しました。インシデント報告対応状況は、JPCERT/CC Web サイト「インシデント報告対応状況」において、毎日速報数値を公開しています。正式な統計情報については四半期のレポートをご覧ください。

インシデント対応状況
https://www.jpcert.or.jp/ir/status.html

ートピック2ー　フィッシング対策協議会　創立 10 周年

フィッシング対策協議会は、平成 17 年 4 月 28 日に創立され、今年度創立 10 周年を迎えることとなりました。平成 27 年 6 月 1 日現在で 81 組織 (正会員 : 23 社、賛助会員 : 48 社、リサーチパートナー : 3 名、オブザーバー : 7 団体) の会員を擁しています。6 月に開催された協議会の定時総会の終了後には、創立 10 周年を記念した祝賀会が開催されました。

祝賀行事では、経済産業省及び警察庁の御来賓から御祝辞を賜り、参加した会員の間では今後の協議会運営や活動に関する活発な意見交換がなされました。また、祝賀会においては、フィッシング対策協議会が海外とも連携しながら行っている、サイバーセキュリティ・リスクへの注意を促す個人向けの啓発キャンペーン「Stop.Think.Connect. (STC)」の Facebook ページを開設したことが担当のワーキンググループから紹介されました。フィッシング対策協議会では、ホームページのみならず、Facebook 等も利用して啓発活動を積極的に行っていく予定です。

フィッシング対策協議会
https://www.antiphishing.jp/
Stop.Think.Connect. (STC) 公式ページ
http://stopthinkconnect.jp/
Stop.Think.Connect. Facebook ページ
https://www.facebook.com/StopThinkConnectJapan

本活動は、経済産業省より委託を受け、「平成２６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、「2.3.1. セキュアコーディングに関する講演活動」、「4.国際連携活動関連」、「9.主な講演活動一覧」、「10. 主な執筆一覧」、「11.協力、後援一覧」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」といいます。)に関する報告は、報告件数ベースで 5187 件、インシデント件数ベースでは 4188 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 2593 件でした。前四半期の 3088 件と比較して 16%減少しています。「調整」とは、フィッシングサイトが設置されているサイトや、改ざんにより JavaScript が埋め込まれているサイト、ウイルス等のマルウエアが設置されたサイト、「scan」のアクセス元等の管理者等に対し、状況の調査や問題解決のための対応を依頼する活動です。

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

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.jpcert.or.jp/pr/2015/IR_Report20150714.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 491 件で、前四半期の 466 件から 5%増加しました。また、前年度同期(509 件)との比較では、4%の減少となりました。

本四半期のフィッシングサイトの報告件数を、装っていたブランドが国内か国外かで分けた内訳を添えて[表 1-1]に示します。

[表 1-1 フィッシングサイトの国内・国外ブランド別の件数]

フィッシングサイト	4 月	5 月	6 月	国内外別合計（割合）
国内ブランド	53	35	44	132(27%)
国外ブランド	92	74	73	239(49%)
ブランド不明	46	35	39	120(24%)
月別合計	191	144	156	491(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。

国内金融機関を装ったフィッシングサイトの件数が、前四半期に比べて大きく増加しました。国内金融機関を装ったフィッシングサイトのドメインには 5 月後半までは cn.com 配下のものが多く使用されていましたが、それ以降は.pw、.ml、.gq、.ga などの ccTLD 配下のものが多く見られました。フィッシングサイトのほとんどは海外の IP アドレスを使用しており、日本の IP アドレスは 4 月の半ばに少数確認されたのみでした。

また、以前は国内金融機関を装ったフィッシングサイトが、国内 ISP によって割り当てられた動的な IP アドレスを使うケースが多くありましたが、そうしたケースが現在は韓国の省庁を装ったフィッシングサイトで継続的に確認されています。

フィッシングサイトの調整先の割合は、国内が 52%、国外が 48%であり、前四半期(国内 73%、国外 27%)に比べ、国外へ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、649 件でした。前四半期の 792 件から 18%減少しています。

本四半期は、改ざんされた Web サイトにアクセスして不正なサイトに誘導され、いわゆるランサムウエアに感染したという報告が多く寄せられました。改ざんされた Web サイトを確認したところ、埋め込まれる不正なコードには、body タグの直後に cookie を送信する JavaScript と、攻撃サイトに誘導する iframe が埋め込まれているという特徴がありました。また、誘導先の攻撃サイトでは、マルウエアに感染させるために、Internet Explorer や Adobe Flash Player の脆弱性が使用されていました。

上記のような改ざんが行われた Web サイトでは、WordPress を使用しているという共通点が見られました。WordPress のような CMS を使用している Web サイトは、CMS やそのプラグインのバージョンが古い場合、脆弱性をつかれて改ざんされてしまう恐れがあります。Web サイトの管理者は、CMS を常に最新のバージョンに維持し、不要なプラグインを削除するなどの対策を取ることが重要です。

1.1.1.3. その他

JPCERT/CC では、国内組織を標的とした高度な攻撃に関して、使用されたマルウエア、C&C サーバなどの調査、被害組織への調査協力を行うなどの活動に取り組んでいます。

本四半期は、標的型攻撃に関する連絡を 66 組織に行っており、そのうち 44 組織への連絡は Emdivi と呼ばれる遠隔操作マルウエアに関連したものでした。Emdivi に感染した組織では、社内のアクティブディレクトリやファイルサーバなどにも侵入され、様々な機密情報や個人情報が漏えいするなどの被害が発生しています。

JPCERT/CC では、引き続き、被害組織への対応支援、調査協力を行うとともに、被害の可能性のある組織への連絡、調査協力などの活動を通じて被害拡大防止の活動に取り組んで参ります。

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エア製品の脆弱性情報、国内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、必要に応じて脆弱性やウイルス検体の検証等も併せて行い、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 25,000 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. 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：11 件（うち 1 件更新） https://www.jpcert.or.jp/at/

2015-04-15 2015 年 4 月 Microsoft セキュリティ情報 (緊急 4 件含) に関する注意喚起(公開)
2015-04-15 2015 年 4 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)
2015-04-15 Adobe Flash Player の脆弱性 (APSB15-06) に関する注意喚起 (公開)
2015-04-16 Adobe Flash Player の脆弱性 (APSB15-06) に関する注意喚起 (更新)
2015-05-13 2015 年 5 月 Microsoft セキュリティ情報 (緊急 3 件含) に関する注意喚起 (公開)
2015-05-13 Adobe Flash Player の脆弱性 (APSB15-09) に関する注意喚起 (公開)
2015-05-13 Adobe Reader および Acrobat の脆弱性 (APSB15-10) に関する注意喚起 (公開)
2015-05-26 ランサムウエア感染に関する注意喚起 (公開)
2015-06-10 2015 年 6 月 Microsoft セキュリティ情報 (緊急 2 件含) に関する注意喚起 (公開)
2015-06-10 Adobe Flash Player の脆弱性 (APSB15-11) に関する注意喚起 (公開)
2015-06-24 Adobe Flash Player の脆弱性 (APSB15-14) に関する注意喚起 (公開)

1.2.1.2. Weekly Report

JPCERT/CC が収集したセキュリティ関連情報のうち重要と判断した情報の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：12 件 https://www.jpcert.or.jp/wr/

Weekly Report で扱った情報セキュリティ関連情報の項目数は、合計 75 件、「今週のひとくちメモ」のコーナーで紹介した情報は、次の 12 件でした。

2015-06-24 SMS で誘導される銀行のフィッシングサイトに注意
2015-06-17 総務省、2 つの注意喚起を公開
2015-06-10 産業制御システムで使用される PLC の脆弱性を標的としたアクセスを観測
2015-06-03 IPA「サイバー情報共有イニシアティブ（J-CSIP） 2014 年度 活動レポート」を公開
2015-05-27 金融機関のフィッシングサイトが増加
2015-05-20 IPA、「SSL/TLS 暗号設定ガイドライン」を公開
2015-05-13 US-CERT「Top 30 Targeted High Risk Vulnerabilities」を公開
2015-04-30 「Interop Tokyo 2015」開催
2015-04-22 Java SE JDK/JRE 7 の公式アップデート終了
2015-04-15 なりすまし EC サイト対策協議会「なりすまし EC サイト 対策マニュアル」公開
2015-04-08 NoSQL データベースに対する探索行為について

1.2.1.3. 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 CSIRT に向けて、それらの組織やサービス提供先に深刻なセキュリティ上の問題を惹起する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.jpcert.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。

【ランサムウエア感染に関する注意喚起】
2015 年 5 月 26 日、ランサムウエア感染に関する注意喚起を発行いたしました。ランサムウエアは、感染端末内のファイルを暗号化し、復号の為に金銭を要求するマルウエアです。攻撃者は何らかの手法を用いて Web サイト のコンテンツを改ざんし、攻撃用サイトへと誘導を試みます。攻撃用サイトではアクセスした PC に対して OS や各種ソフトウエアの脆弱性を悪用した攻撃が行われ、脆弱性があるとランサムウエアに感染してしまいます。ランサムウエアに感染するリスクを低減するとともに、万一感染して重要なファイルが暗号化され利用できなくなった事態に備えるため、JPCERT/CC では、定期的なデータバックアップや OS、各種ソフトウエアを最新版にアップデートすることを推奨しています。

【2015 年 4 月 MS15-034 で修正された HTTP.sys の脆弱性(CVE-2015-1635)】
マイクロソフト社より、米国時間 4 月 14 日に HTTP.sys の脆弱性に関するセキュリティ更新プログラムが公開されました。その直後に、この脆弱性を攻撃する実証コードが一般に公開されました。
JPCERT/CC が実証コードを検証したところ、細工された HTTP リクエストを Internet Information Services が稼働するサーバに送信することで、DoS 攻撃が成功することが確認できたため、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、2015 年 4 月 16 日、早期警戒情報を発行しました。

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状況を把握することに努めています。

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 と共同で分析を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。2015 年 6 月末時点で、観測用センサーはアジア・太平洋地域の 20 地域 23 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関係機関と交渉を続けています。

TSUBAME プロジェクトの目的等詳細については、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

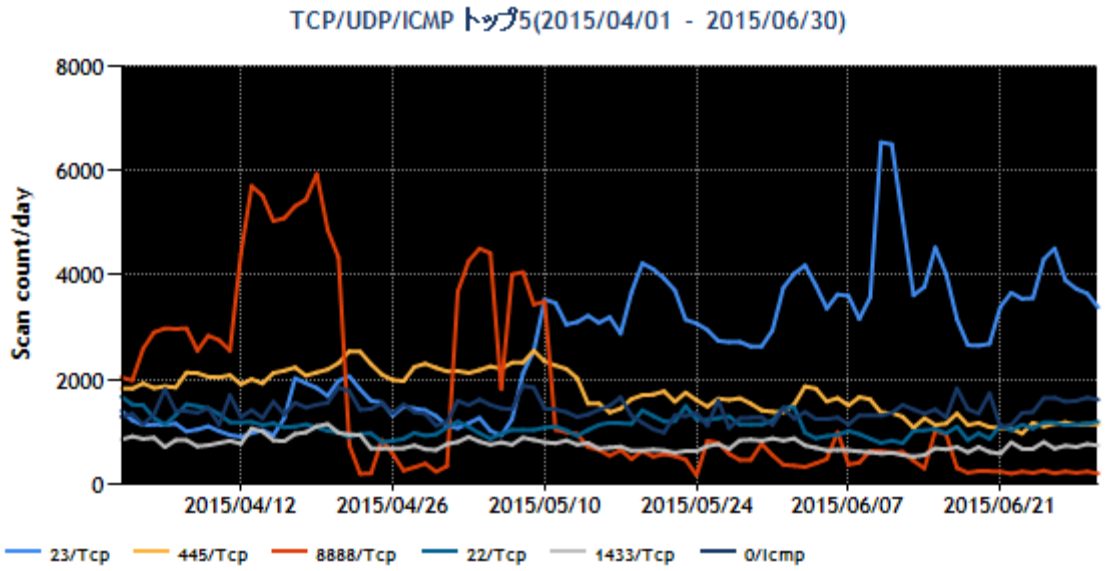
JPCERT/CC は、TSUBAME で収集したデータを宛先ポート番号や送信元地域ごとに分類して統計分析し、既知の脆弱性情報やマルウエア、攻撃ツール等との関連を考察することで、攻撃活動や準備活動の捕捉に努めています。

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、2015 年 1 月から 3 月分のレポートを 2015 年 4 月 27 日に公開しました。

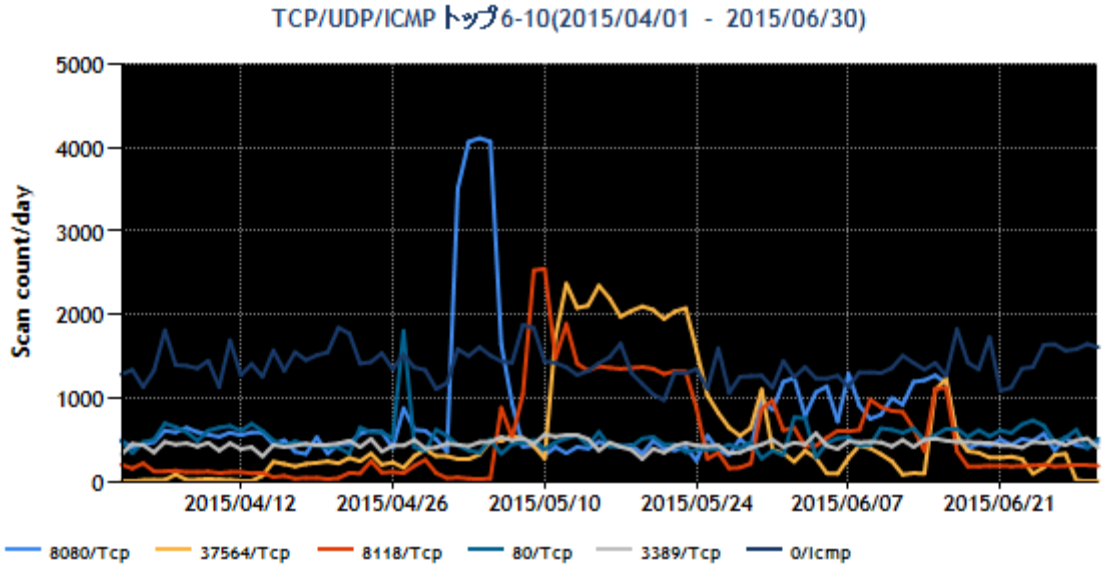
TSUBAME 観測グラフ
https://www.jpcert.or.jp/tsubame/index.html#examples

インターネット定点観測レポート(2015 年 1～3 月)
https://www.jpcert.or.jp/tsubame/report/report201501-03.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。

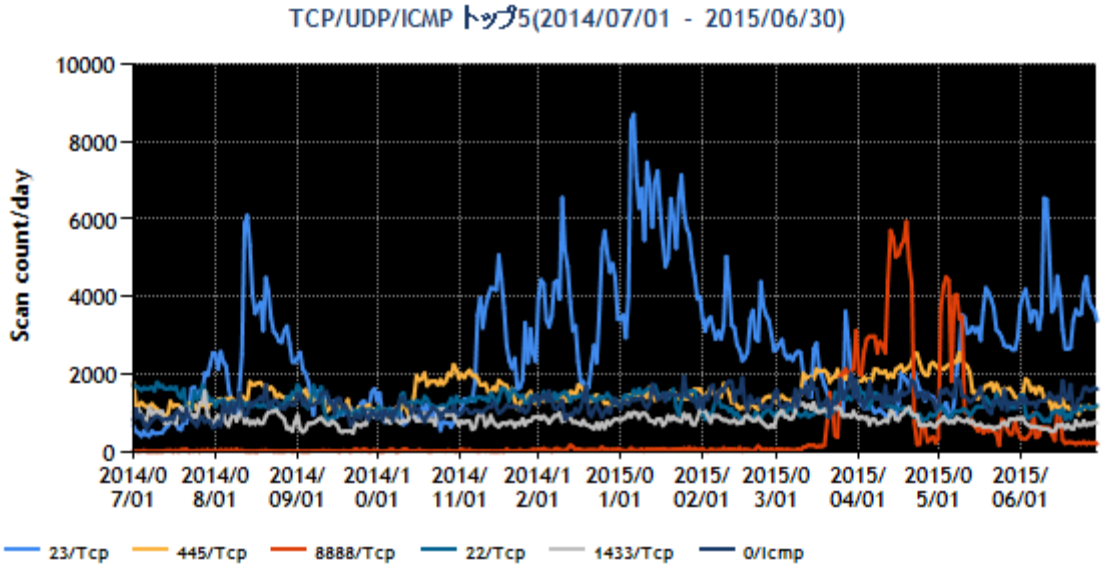


[図 1-1 宛先ポート別グラフ トップ 1-5 (2015 年 4 月 1 日-6 月 30 日)]

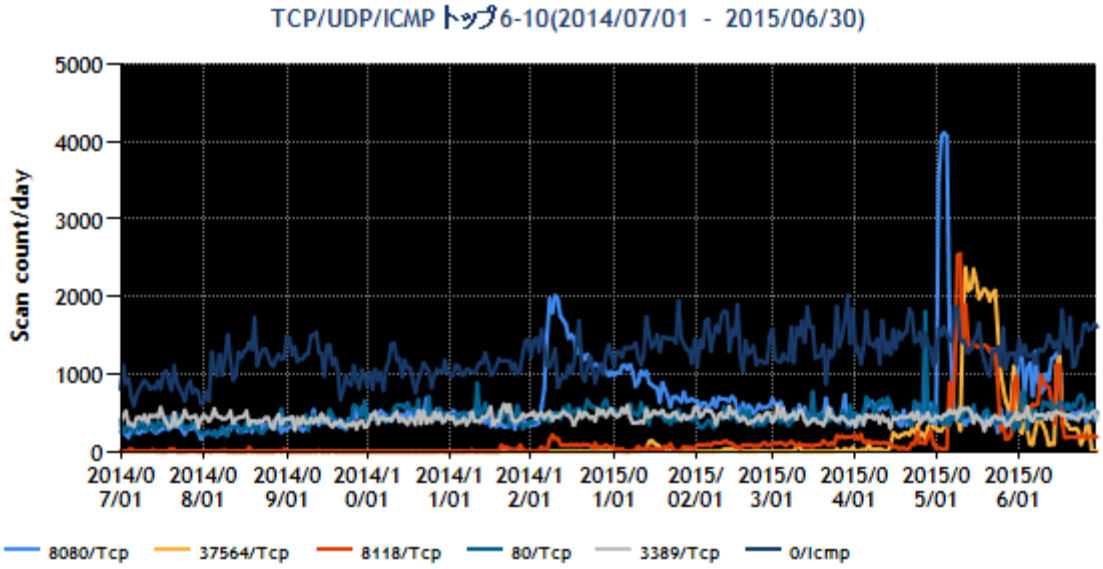


[図 1-2 宛先ポート別グラフ トップ 6-10 (2015 年 4 月 1 日-6 月 30 日)]

また、過去 1 年間(2014 年 7 月 1 日-2015 年 6 月 30 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。



[図 1-3 宛先ポート別グラフ トップ 1-5 (2014 年 7 月 1 日-2015 年 6 月 30 日)]



[図 1-4 宛先ポート別グラフ トップ 6-10 (2014 年 7 月 1 日-2015 年 6 月 30 日)]

本四半期は、4 月上旬から 5 月中旬にかけて 8888/Tcp、37564/Tcp など複数の Port 番号へのパケットが増加しました。特に 8888/Tcp 宛のパケット数は、増加数でみると、ポート別パケット受信数 1 位の 23/Tcp を上回るほど増加したため、これまでとは異なった TOP10 となりました。

これらの Port 番号宛の多量のパケットの発信目的を考察した時に最初に思い起こされるのが、オープンプロキシサーバのリストとして、IP アドレスと Port 番号を掲載している海外の複数の Web サイトの存在です。実際に、TSUBAME の過去の観測データ中で、宛先 Port 番号が 8888/Tcp や 37564/Tcp のパケ

ットと同じ送信元 IP アドレスをもつパケットを探してみると、従来から知られているオープンプロキシサーバの Port 番号宛のパケットが見つかるケースがあります。対応するオープンプロキシサーバのリストを調べると、8888/Tcp などの Port 番号の情報が新たにリストに追加されていて、このことからオープンプロキシサーバの探索を目的としたパケットであったことが高い確度で推測されます。これらの Port 番号を標準的に用いるメジャーなプロキシサーバ―ソフトは知られておらず、何らかのパッケージ・ソフトウェア製品が内部的に稼働させているプロキシ―サーバが、不適切なネットワーク・アクセス制御のために、インターネットに露出していることが疑われます。いずれにせよ，こうした Port 番号に気づいたオープンプロキシサーバのリストの管理者が、探索ポートとして追加したことが、この種のパケットの観測数が一時的に増えた原因であろうと推測しています。
その他、順位に変動はありますが、Windows や Windows 上で動作するサービスへのスキャン活動と見られるパケットや、SSH サーバ等遠隔操作のためにサーバ側が待ち受けているポートのスキャン活動と見られるパケットも、これまでと同様に多く観測されています。

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、不審な動きが認められた場合に、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。

(1) DDoS 攻撃に使用されうる OpenResolver となっている機器についての対応

本四半期も、前四半期に引き続き、DNS 応答パケットおよび DNS サービスのポート不達を示す ICMP エラーパケットが多数観測されました。それらのパケットの送信元 IP アドレスのうち国内のものを調査したところ、インターネット側からの DNS のリクエストに応答する OpenResolver が見つかりました。TSUBAME で観測されたパケットは、攻撃者が DNS 権威サーバに過剰な負荷を課そうとする DDoS 攻撃の余波と推測されます。JPCERT/CC が、TSUBAME で観測した DNS 応答パケットおよび DNS サービスのポート不達を示す ICMP エラーパケットを調査し、その送信元となっている国内の IP アドレスの管理者に対して調査を依頼したところ、多くの管理者から「DNS サーバやネットワーク機器の設定が不適切で OpenResolver になっていたことを確認し、必要な対応を行った」等の回答を得ました。

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「ソフトウエア等脆弱性情報取扱基準」(平成 26 年経済産業省告示第 10 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り扱い状況等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
http://www.ipa.go.jp/security/vuln/

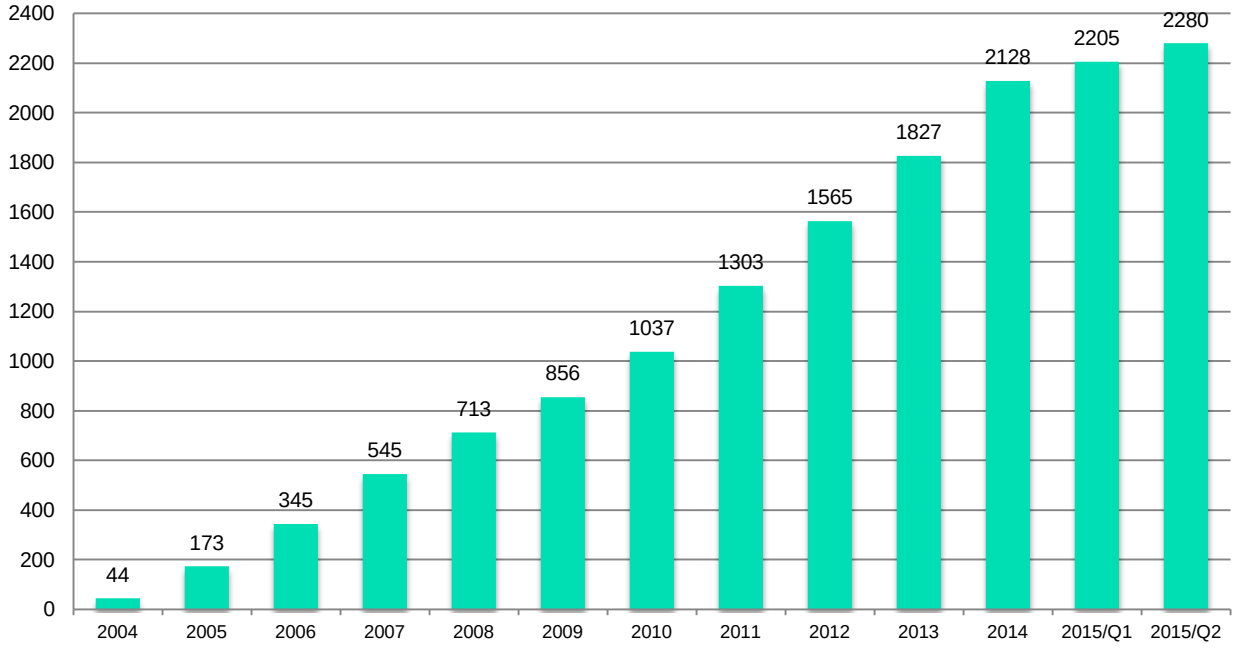
2.1.2. Japan Vulnerability Notes(JVN)において公表した脆弱性情報および対応状況

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 75 件(累計 2280 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。

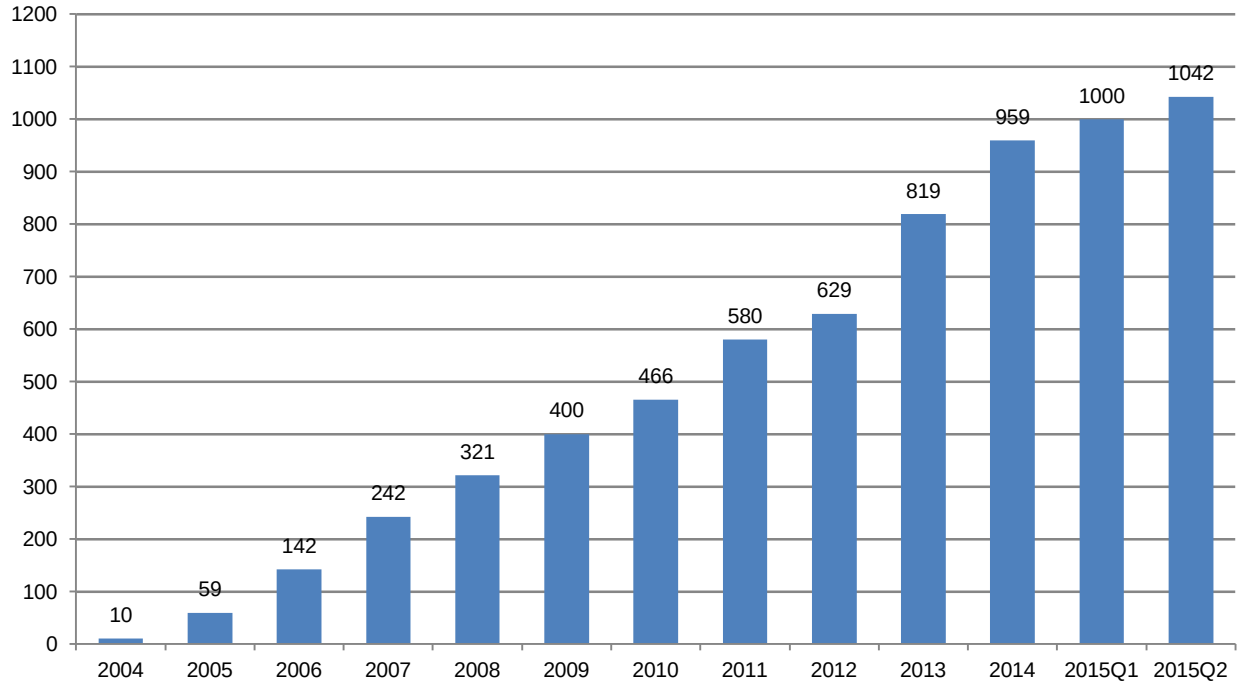
JVN(Japan Vulnerability Notes)
https://jvn.jp/



[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 42 件(累計 1042 件)で、累計の推移は[図 2-2]に示すとおりです。42 件のうち、25 件が国内製品開発者の製品、17 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、前四半期に引き続き本四半期も、自社製品届出による脆弱性情報を 1 件公表しました。

本四半期に公表した脆弱性情報を、影響を受けた製品のカテゴリで分類すると、CGI に関するものが 10 件、Android アプリが 4 件、ファイル圧縮解凍アーカイバーに関するものが 3 件、フォームメールやグループ宛メール処理用グループウエアに関するものが 3 件、ウェブアプリケーションフレームワークに関するものが 3 件、ネットワークトラフィック解析ツールに関するものが 3 件、関数やライブラリに関するものが 3 件、コンテンツ管理システム(CMS)に関するものが 2 件、PHP ライブラリに関するものが 2 件、それ以外では、掲示板、テキストエディタ、医療用情報管理ソフトウエア、ルータ(組込系)、ネットワークモニタリングソフトウエア、オンラインショッピング構築ソフトウエア、プラグイン、ブログソフトウエア、等がそれぞれ 1 件ずつとなり、多様なカテゴリの製品が混在していました。



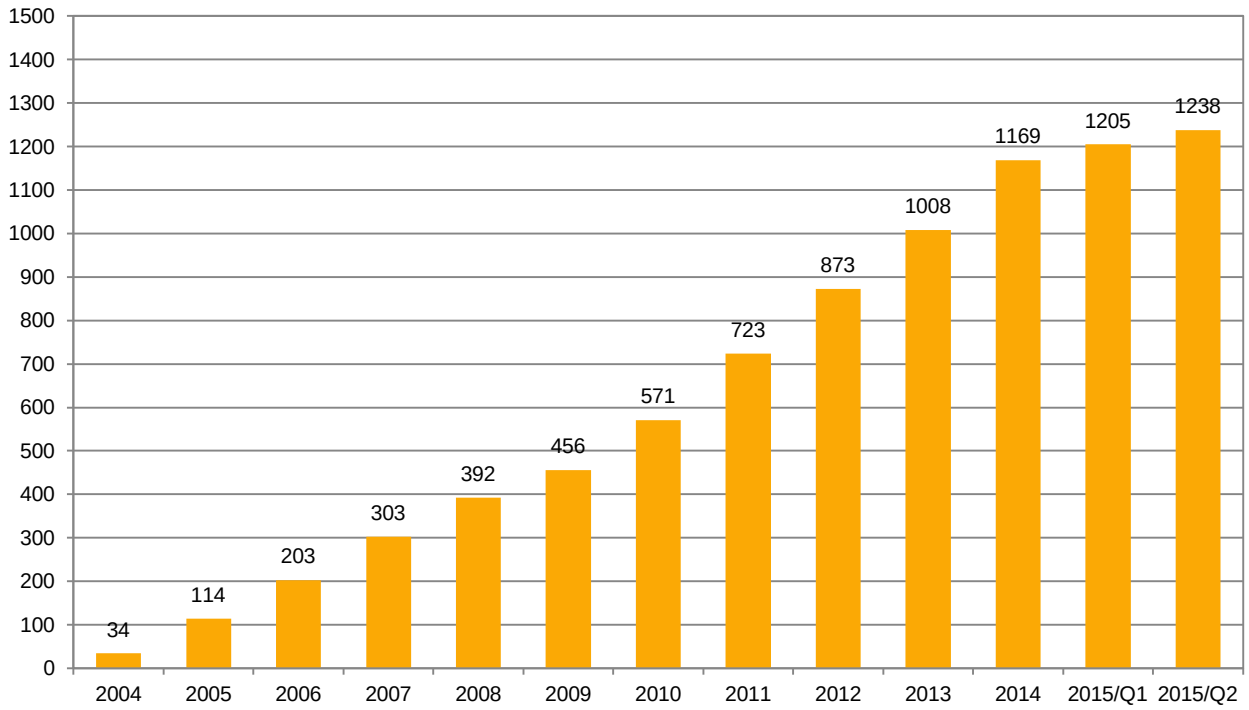
[図 2-2 公表を行った国内取扱脆弱性情報の累積件数]

本四半期に公表した国際取扱脆弱性情報は 33 件(累計 1238 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で特筆すべきものが 2 件ありました。一つめは、対策が無いいわゆるゼロデイの脆弱性情報の公開です。この脆弱性は最初に米国 CERT/CC から「VU#672268　Microsoft Windows NTLM automatically authenticates via SMB when following a file:// URL」として公開されたもので、それを受け JVN でも速やかに公開しました。また、この Windows コンポーネントを使用する複数の製品に影響があると考えられたため、日本国内の複数の製品開発者へ本件の JVN 公表通知を行い、注意喚起を実施しました。二つめは、「JVNVU#98282440『提督業も忙しい！』(KanColleViewer) がオープンプロキシとして動作する問題」です。こちらは、特定ポートのアクセス増加として警察庁から注意喚起が発行され、JPCERT/CC での調査により製品の脆弱性を特定し、製品開発者と調整して JVN での公表に至ったものです。

本四半期に公表した脆弱性情報の製品カテゴリ別内訳を多い順に挙げると、セキュリティアプライアンス製品に関するものが 3 件、OpenSSL や NTP 等プロトコルに関するものが 3 件、POS(Point of Sales)製品に関するものが 2 件、その他には、アセスメント管理システム、アンチウィルス、ウェブホスティングコントロールパネル、オンラインゲーム、コンテンツ管理システム、ウェブブラウザ、遠隔サポートソフトウエア、エンタープライズソフトウエア、検索アプライアンス、E コマース製品、Android スマートフォン、バックアップソフトウエア、ファイル共有サービス、不動産サービスアプリケーション、暗号化通信アプライアンス(組込系)、防犯カメラシステム(組込系)、カーネルドライバ、ライブラリ、サーバ製品等といった多様な製品に関するものが混在していました。また自社製品に関する届出は、Apple から 2 件でした。

本四半期においては、JVN Technical Alert(注意喚起)として、「2015/05/12 JVNTA#98308086 End-to-End 通信の保護」と「2015/05/08 JVNTA#99041988 標的型攻撃に使用されるリスクの高い脆弱性 Top 30」の 2 件を、米国 US-CERT Technical Alert「 (TA15-120A) Securing End-to-End Communications」と「(TA15-119A) Top 30 Targeted High Risk Vulnerabilities」と同期して、JVN で公開しました。



[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、広く連絡の手掛かりを求めています。これまでに 205 件(製品開発者数としては 132 件)を公表し、36 件(製品開発者の数としては 20 件)の調整を再開することができ、脆弱性関連情報の取扱いにおける「滞留」の解消に一定の効果を挙げています。

本四半期に新たに連絡不能開発者一覧に掲載した案数は 20 件(製品開発者の数としては 15 件)でした。本四半期末日時点で、合計 169 件の連絡不能開発者案件を引き続き掲載し、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掛けています。

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、利用者保護の観点から脆弱性情報を公表する手続きを定めた、本規準およびパートナーシップガイドラインが昨年5月に改正されており、第一回目となる公表判定委員会が2014年第4四半期開催されました。深刻な脆弱性については、製品開発者と連絡が取れない場合であっても、情報の公表をいつまでも先延ばしにしないための対応を着実に

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、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、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連携して行っています。さらに Android 関連製品や OSS 製品の脆弱性の調整活動の中では、製品開発者が存在するアジア圏の調整機関、特に韓国 KrCERT/CC や中国 CNCERT/CC、台湾 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 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 8 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。本四半期は、JVN で公表したもののうち、国内で届出られた脆弱性情報 37 件に、JPCERT/CC が 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。

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

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」の運用を開始

https://www.jpcert.or.jp/press/2004/0708.txt

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(2014 年版)

https://www.jpcert.or.jp/vh/partnership_guide2014.pdf

JPCERT/CC 脆弱性情報取扱いガイドライン

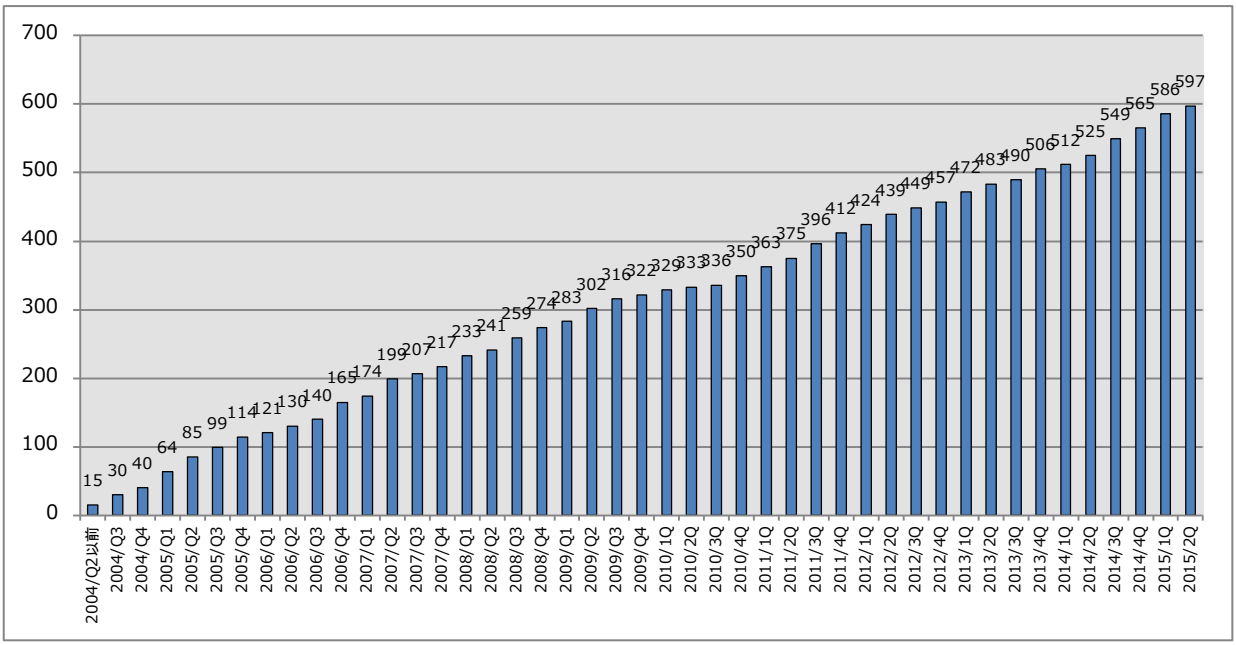
https://www.jpcert.or.jp/vh/vul-guideline2014.pdf

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 2-7]に示すとおり、2015 年 6 月 30 日現在で 597 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.jpcert.or.jp/vh/agreement.pdf



[図 2-7 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. セキュアコーディングに関する講演活動

情報流通対策グループの脆弱性解析チームでは、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

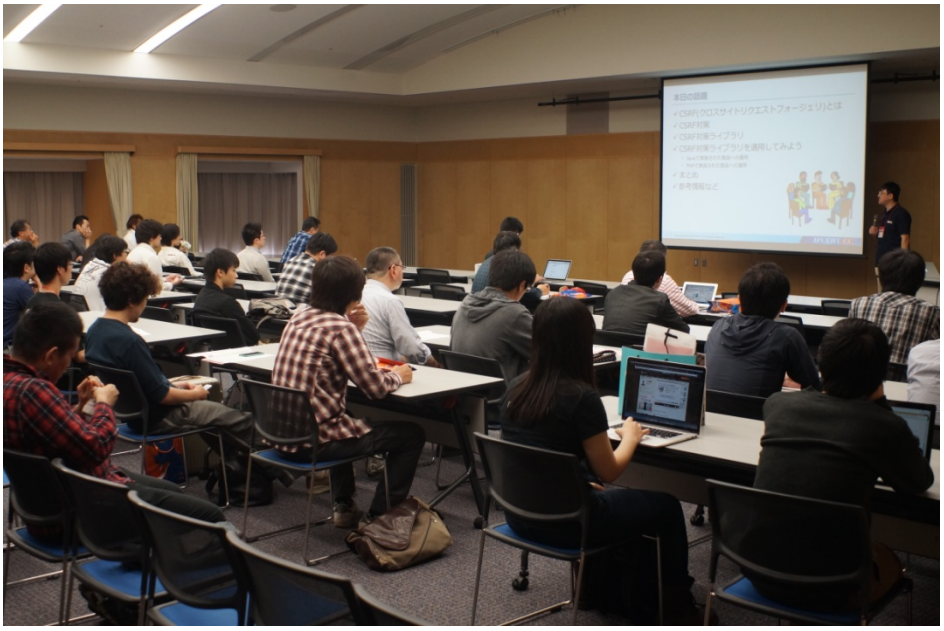
その対策方法に関する知見を、広く一般のソフトウエア開発者の方々に伝えるための活動を進めています。本四半期は、次の 5 件の講演、講義を行いました。

「～誰かの失敗を他山の石に～脆弱性事例に学ぶセキュアコーディング『SSL/TLS 証明書検証』編」
Java Day Tokyo 2015(4 月 8 日)
http://www.slideshare.net/jpcert_securecoding/cert-verif-javadaytokyo2015(講演スライド)

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(4 月 17 日)

「オープンソースを中心としたシステムのセキュリティ対応　～昨年の脆弱性を例にして～」
第 13 回情報セキュリティ EXPO 専門セミナー(5 月 15 日)
(ディー・エヌ・エー 杉山俊春氏との共同講演)

「CSRF 脆弱性とその対策について」
オープンソースカンファレンス 2015 Hokkaido(6 月 13 日)
http://www.slideshare.net/jpcert_securecoding/anti-csrf-osc2015hokkaido(講演スライド)



[図 2-8 オープンソースカンファレンス 2015 Hokkaido における講演の様子]

「セキュアコーディング概論」
一般社団法人 JASPAR 主催「会員企業向けセミナー」(6 月 16 日)

2.3.2. 英語ブログ "Fiddler Core's insecure Default flag may lead to Open Proxy Issue"

HTTP 通信を傍受して動作するアプリケーション(HTTP デバッガとも呼ばれます。)の多くは、プロキシー機能を併せ持っていますが、適切なアクセス制限をしていないと Open Proxy と呼ばれる脆弱性が生じま

す。本四半期に JVN で公表した「JVNVU#98282440『提督業も忙しい！』(KanColleViewer) がオープンプロキシとして動作する問題」もその一例でした。この種の脆弱性の作込みを減らすため、HTTP デバッガの実装によく利用される Fiddler Core と呼ばれるライブラリの使用上の注意点をまとめ、JPCERT/CC の英語ブログで公表しました。

2.3.3. ハイブリッドアプリフレームワーク「Apache Cordova」の脆弱性に関する調査報告書

前四半期の活動概要でご紹介したとおり、HTML5 や Javascript といったウェブ関連技術を使用してアプリを開発するハイブリッドアプリフレームワークである Apache Cordova について、アプリ開発の際に作りこまれ得る脆弱性に関して調査した結果を報告資料としてまとめています。5 月末日、JPCERT に製品開発者としてご登録いただいている企業や開発者の皆様に向けて、同資料のドラフト版を公開し、コメントの募集を開始しました。次四半期には、いただいたコメントを反映させた正式版を公開する予定です。

2.3.4. CSRF 対策ライブラリに関する調査報告書

前項と同様、前四半期の活動概要でご紹介した CSRF 対策を行うためのライブラリに関する調査結果についても、資料としてまとめ、5 月末、製品開発者登録をいただいている企業や開発者の皆様にドラフト版を公開しました。同資料の一部は、6 月 13 日に開催されたオープンソースカンファレンス 2015 Hokkaido にて、弊センターの戸田洋三が「CSRF 脆弱性とその対策について」と題して発表しています。本資料の正式版は次四半期に公開する予定です。

2.3.5. CERT C コーディングスタンダードのルールを更新中

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する CERT C Coding Standard を邦訳して提供しています。これは C 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。

移動(1 件)

- CON30-C. スレッド固有のメモリを適切に解放する

内容の更新(2 件)

- FIO33-C. 未定義の動作となる入出力エラーを検出して処理する
- FIO35-C. sizeof(int) == sizeof(char) の場合、ファイル終端およびファイルエラーの検出には feof() と ferror() を使用する

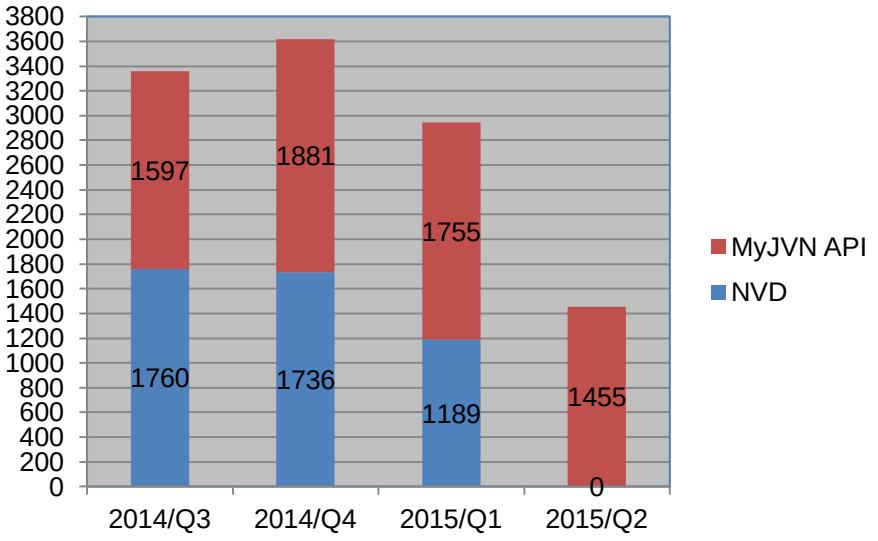
2.4. VRDA フィードによる脆弱性情報の配信

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

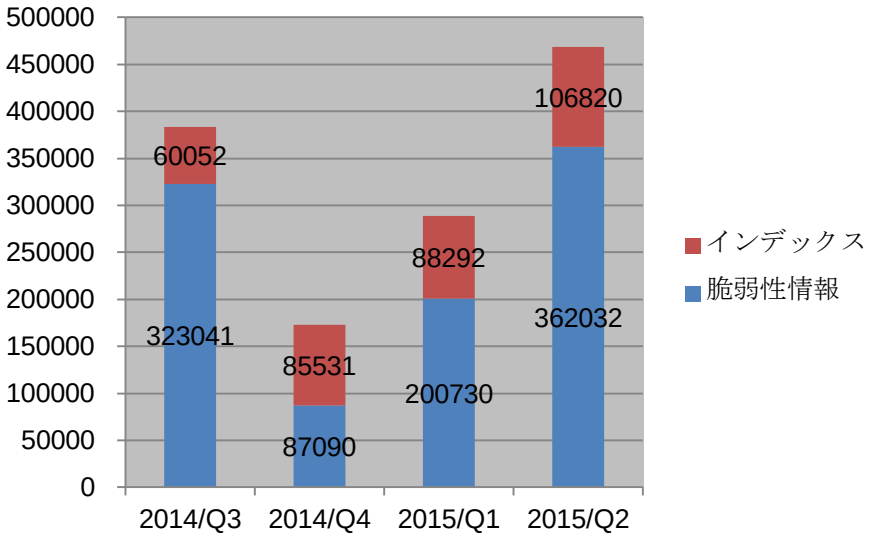
系的な脆弱性対応を可能とするため、IPA が運用する MyJVN API および NIST(National Institute of Standards and Technology)の NVD(National Vulnerability Database)を外部データソースとして利用した、VRDA(Vulnerability Response Decision Assistance)フィードによる脆弱性情報の配信を行っています。VRDA フィードについての詳しい情報は、次の Web ページをご参照ください。

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

四半期ごとに配信した VRDA フィード配信件数のデータソース別の内訳を[図 2-9]に、VRDA フィードの利用傾向を[図 2-10]と[図 2-11]に示します。[図 2-10]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 2-11]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。
なお、NVD から得られる脆弱性情報は、IPA が運用する MyJVN API からも取得可能であるため、本四半期からは、MyJVN API のみを VRDA フィードのデータソースとして配信することになりました。

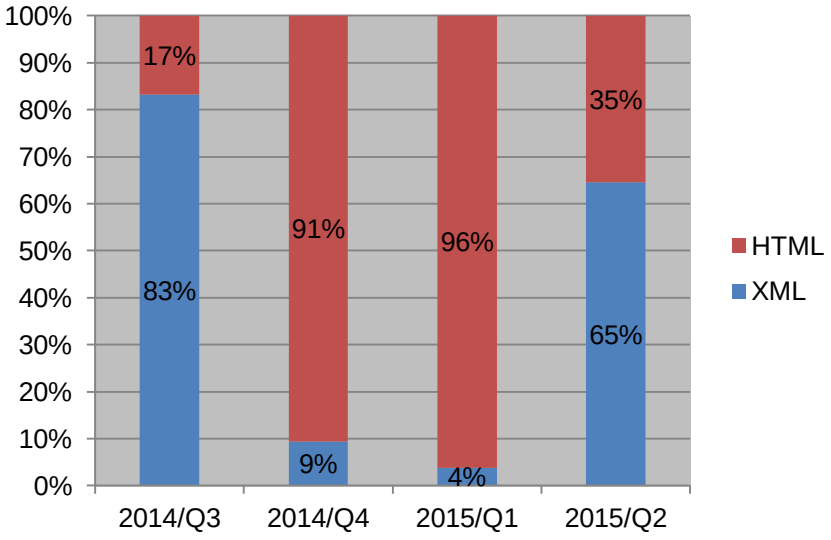


[図 2-9 VRDA フィード配信件数]



[図 2-10 VRDA フィード利用件数]

[図 2-10] 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、大きな変化は見られませんでした。一方、脆弱性情報の利用数については、前四半期と比較し、約 1.8 倍に増加しました。



[図 2-11 脆弱性情報のデータ形式別利用割合]

[図 2-11] 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、XML 形式の利用割合が HTML 形式を大きく上回りました。

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。本四半期の情報収集分析活動の中で収集し分析した情報は 625 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次の 3 件でした。

発行件数：3 件

2015-04-15　[参考情報] Windows Server 2003 のサポート終了について
2015-04-17　[参考情報] 2015 年 4 月 MS15-034 で修正された HTTP.sys の脆弱性(CVE-2015-1635) に関する早期警戒情報
2015-05-28　[参考情報] PLC の脆弱性を標的としたアクセスについて

また、海外での事例や、標準化動向などは JPCERT/CC からのお知らせとともに、制御システム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 件配信しました。

発行件数：3 件

2015-04-08　制御システムセキュリティニュースレター 2015-0003
2015-05-08　制御システムセキュリティニュースレター 2015-0004
2015-06-08　制御システムセキュリティニュースレター 2015-0005

本ニュースレター配信先の制御システムセキュリティ情報共有コミュニティについては、現在 483 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 0 件でした。
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において制御システム機器や関連プロトコルに対応した機能拡張が進んでいて、攻撃されるリスクが高まっていることに対する対策として、「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、国内の制御システム等で外部から悪用されてしまう危険性のあるシステムの保有組織に対して情報を提供しました。こうした危険性のあるシステムに関する本四半期の情報提供件数は、4 件でした。

3.3. 関連団体との連携

SICE(計測自動制御学会)と JEITA(電子情報技術産業協会)、JEMIMA(日本電気計測器工業会)が定期的に開催している合同セキュリティ検討 WG(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情報

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手軽に抽出し、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)の配付を行っています。本四半期は、日本版 SSAT に関して 3 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 171 件、J-CLICS が 238 件となりました。

3.5. 「SHODAN を悪用した攻撃に備えて(制御システム編)」の公開

2015 年 6 月、「SHODAN を悪用した攻撃に備えて(制御システム編)」と題した参考資料を公開しました。SHODAN とは、インターネット上に公開されている様々な機器に関する情報をデータベース化し、インターネット上のサービスとして検索可能にする Web サービスです。SHODAN は、使い方によっては攻撃対象にする制御システムの探索に悪用することができます。加えて、2014 年にはインターネットに接続された制御機器に感染するマルウエアの活動が確認されており、インターネットに接続された制御機器に対する脅威が徐々に高まりつつあります。
本資料では、SHODAN の仕組みや SHODAN を使用した制御システムへの攻撃シナリオ、アセットオーナが行うべき対策などをまとめました。

3.6. 制御システムセキュリティ情報共有ポータルサイトにてニュースクリップを公開

制御システム関係者向けにセキュリティ関連情報等を提供している制御システムセキュリティ情報共有ポータルサイト「ConPaS(Control System Security Partner's Site)」において、4 月 1 日よりニュースクリップの提供を開始しました。ニュースクリップは、各国のメディア等で日々公開されている制御システムセキュリティ関連のニュースのうち国内の関係者の参考となる情報をピックアップし、簡単なコメントと共にほぼ毎日掲載しています。

制御システムセキュリティ情報共有ポータルサイトについて
https://www.jpcert.or.jp/ics/conpas/index.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、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、ミャンマーの CSIRT 構築支援 (5 月 18 日-22 日)

独立行政法人国際協力機構(JICA)の「情報セキュリティ能力向上プロジェクト」の短期専門家として JPCERT/CC 職員が 5 月 18 日から 22 日までジャカルタに派遣され、カンボジア、ラオス、ミャンマーの National CSIRT の職員計 14 名に対して、ネットワークフォレンジックの技術研修を行いました。また JICA やインドネシアの関係者とともに今後のインドネシアでの CSIRT 構築支援計画等について協議しました。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

4.1.2. AfricaCERT Cybersecurity Day 参加者に向けたビデオメッセージ送付 (5 月 31 日)

5 月 31 日にチュニジア共和国の首都チュニスで開催された AfricaCERT Cybersecurity Day の参加者に向けて、APCERT の活動状況やウェブ改ざん等のインシデント対応に関する講演をビデオメッセージとして届けました。AfricaCERT Cybersecurity Day は、AFRINIC-22 のプログラムの一つとして、アジア地域との連携を促進する AfricaCERT が開催したものです。今回はビデオメッセージでの講演となりましたが、JPCERT/CC は AFRINIC 等の機会を捉えてアフリカ諸国に向けた CSIRT トレーニングを 2010 年春からほぼ半年ごとに実施しております。AFRINIC-22 および AfricaCERT についての詳細は、次の Web ページをご参照ください。

AFRINIC-22
http://internetsummitafrica.org/en/programme/afrinic-22/about-afrinic-22#

AfricaCERT
http://www.africacert.org/

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・地域等からのサイバー攻撃も日本のインターネットユーザにとっての脅威の一つとなっています。アフリカ地域に起因するインシデントが、予想されている今後の急速なインターネット普及に伴って増えることが懸念され、JPCERT/CC は、そのような事態が発生した際に迅速かつ円滑な対応ができるよう、同地域との連携強化の基盤づくりに努めています。

4.2. 国際 CSIRT 間連携

インシデント対応に関する海外の National CSIRT との間の連携の枠組みの強化、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への取組みの実施状況等に関する情報収集を目的として、国際連携活動等を行っています。また、APCERT や FIRST に参加し、主導的な役割を担う等、多国間の CSIRT 連携の取組みにも積極的に参画しています。

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)のメンバに選出されており、また、事務局を担当しています。2011 年 3 月からは、議長チーム(現在 4 期目)としてさまざまな活動をリードしています。JPCERT/CC の APCERT における役割および APCERT の詳細については、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、5 月 20 日に電話会議を行い、今後の APCERT の運営方針等について議論しました。JPCERT/CC は議長チームおよび事務局として、これらの会議を主導およびサポートしました。

4.2.1.2. APCERT を代表しての会議出席

(1) APEC TEL 51 (5 月 12 日-16 日)

5 月 12 日から 16 日にフィリピンのボラカイ島で開催された APEC TEL (APEC Telecommunications and Information Working Group) 51 において、JPCERT/CC は APCERT を代表して登壇し、APCERT の活動状況を報告するとともに、JPCERT/CC が推進している国際的に比較可能なサイバーセキュリティ評価指標の策定に関する取組み「サイバーグリーン」について講演しました。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。サイバーグリーンの詳細については、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

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

JPCERT/CC は 1998 年の FIRST 加盟以来、積極的に活動に参加しています。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 Board of Directors のメンバを務めており、4 月 20 日-23 日に韓国のソウルにて、また 6 月 12 日-13 日にドイツのベルリンにて開催された Board of Directors 会合

に出席しました。FIRST および Board of Directors の詳細については、次の Web ページをご参照ください。

FIRST
http://www.first.org/

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

4.2.2.1. 27th Annual FIRST Conference Berlin への参加 (6 月 14 日-19 日)

第 27 回 FIRST 年次会合が 6 月 14 日から 19 日までドイツのベルリンで開催されました。本会合は、サイバーインシデントの予防、対応、技術分析等に関する最新情報の交換、および国や文化等の壁を越えたインシデント対応チームの連携強化を目的に毎年開催されており、今年は「Unified Security: Improving the Future」のテーマのもと、様々な話題が取り上げられました。JPCERT/CC は 6 月 15 日に「A Proposal for Cybersecurity Metrics Through Cyber Green」、18 日に「VRDX-SIG: Global Vulnerability Identification」と題する講演を各々連携している組織の関係者とともに行い、また 19 日に「Keeping Eyes on Malicious Websites – “ChkDeface” Against Fraudulent Sites」と題して講演を行いました。そのほか、JPCERT/CC ではこの機会を利用して、アジア太平洋地域や欧州各国の National CSIRT や製品ベンダの CSIRT 等との個別の意見交換や、APCERT 加盟組織が集う意見交換会の企画／主催等、国際間の CSIRT 連携をさらに強化させるための様々な活動を併せて行いました。

このような会合への参加を通じて、各地域間の情報共有を促進し、信頼関係を醸成して、国際間でのインシデント対応調整がより円滑に進められるよう今後も努めてまいります。第 27 回 FIRST 年次会合についての詳細は、次の Web ページをご参照ください。

27th Annual FIRST Conference Berlin
https://www.first.org/conference/2015

4.2.3. National CSIRT Meeting (NatCSIRT) 2015 への参加 (6 月 20 日-21 日)

第 27 回 FIRST 年次会合後に引き続きベルリンにて、CERT/CC が主催する National CSIRT Meeting (NatCSIRT) 2015 が開催されました。本会合は世界各国の National CSIRT が一堂に会し、国を代表するインシデント対応チームとしての活動や課題を共有するとともに、共同プロジェクトや研究調査についての発表や議論を行う場であり、今後の一層の連携強化に繋がる成果を得ることができました。JPCERT/CC は、サイバーグリーンの取組みについて発表を行うとともに、本会合に初めて参加した CSIRT をはじめ、各国の National CSIRT との個別の意見交換等を行いました。NatCSIRT についての詳細は、次の Web ページをご参照ください。

4.2.4. NCSC ONE Conference 2015 および Global Conference on CyberSpace 2015 への参加 (2015 年 4 月 13 日-17 日)

オランダのハーグにて、4 月 13 日から 14 日に開催された NCSC ONE Conference 2015 および 4 月 16 日から 17 日に開催された Global Conference on CyberSpace 2015 (GCCS2015) に参加しました。
NCSC ONE Conference 2015 はサイバーセキュリティにおける政策や官民連携に関するセッションから技術セッションまで幅広く網羅するオープンカンファレンスです。JPCERT/CC は、インターネット全体の健全性とリスクを各国／地域間で比較可能にする評価指標を打ち立て、その指標を用い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た、JPCERT/CC 主導による「サイバーグリーン」の取組みについて講演しました。
また、Global Conference on CyberSpace 2015 は、2011 年のサイバー空間に関するロンドン会議、2012 年の同ブダペスト会議、2013 年の同ソウル会議に続く第 4 回目となり、政府、民間企業、市民社会を代表するサイバーセキュリティの有識者が広く集いました。JPCERT/CC はオープニングセッションで「サイバーグリーン」について講演し、その取組みを広く紹介するとともに、国際的に比較可能なサイバーセキュリティ評価指標の策定の必要性を訴えました。
NCSC ONE Conference 2015、Global Conference on CyberSpace 2015、サイバーグ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。

NSCS ONE Conference 2015
https://www.ncsc.nl/english/conference

GCSC2015
https://www.gccs2015.com/

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

4.2.5. ACSC Conference 2015 への参加 (4 月 22 日-23 日)

4 月 22 日から 23 日にオーストラリアの首都キャンベラで開催された ACSC (Australian Cyber Security Centre) Conference 2015 に参加し、「International Cooperation on Cyber Space from CSIRT's Perspectives – JPCERT/CC's Outreach –」と題する講演を行い、JPCERT/CC における国際連携の取組みについて、オーストラリアの政府関係者や ISP、セキュリティ関連企業等の参加者約 100 名に向けて紹介しました。
本会合の主催者である ACSC は、オーストラリア国内におけるサイバーセキュリティの関係省庁や機関の集まりから成る組織であり、サイバーセキュリティインシデントに対して多角的な分析を行うことを目的に 2014 年 11 月に発足しました。本会合は、ACSC の設立を受けて開催された第 1 回目のサイバーセ

キュリティ会合です。ACSC Conference 2015 および ACSC についての詳細は、次の Web ページをご参照ください。

ACSC Conference 2015
http://www.acsc2015.com.au/

ACSC
https://www.acsc.gov.au/

4.2.6. 2015 CNCERT Annual Conference への参加 (5 月 26 日-28 日)

5 月 26 日から 28 日に中国の武漢市で開催された 2015 CNCERT Annual Conference に参加し、情報収集を行いました。また、同会合前日、中国の Anti Network-Virus Alliance of China (ANVA)のメンバや、中国国外の関係者の集まる技術会合において、JPCERT/CC が主導する「サイバーグリーン」の取組みについて紹介しました。2015 CNCERT Annual Conference についての詳細は、次の Web ページをご参照ください。

2015 CNCERT Annual Conference
http://2015.cert.org.cn/enl.html

4.2.7. オランダ NSCS-NL 来訪 (6 月 12 日)

6 月 12 日にオランダ NCSC-NL より 2 名が JPCERT/CC の事務所を来訪し、両組織の活動状況や両国におけるインシデント動向、インシデント対応における両組織の連携等について情報共有や意見交換を行い、今後も密な連携を維持することを確認しました。

4.3. その他の活動ブログや Twitter を通した情報発信

英語ブログ(http://blog.jpcert.or.jp/)や Twitter(@jpcert_en)を利用し、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 の活動等について継続的に英文による情報発信を行っています。本四半期は次の記事をブログに掲載しました。

Malware with a Fake Thumbnail Preview (4 月 10 日)
http://blog.jpcert.or.jp/2015/04/malware-with-a-fake-thumbnail-preview.html

Training in Myanmar (5 月 12 日)
http://blog.jpcert.or.jp/2015/05/training-in-myanmar.html

Speaking at Australian Cyber Security Centre Conference 2015 (5 月 27 日)
http://blog.jpcert.or.jp/2015/05/speaking-at-australian-cyber-security-centre-conference-2015.html

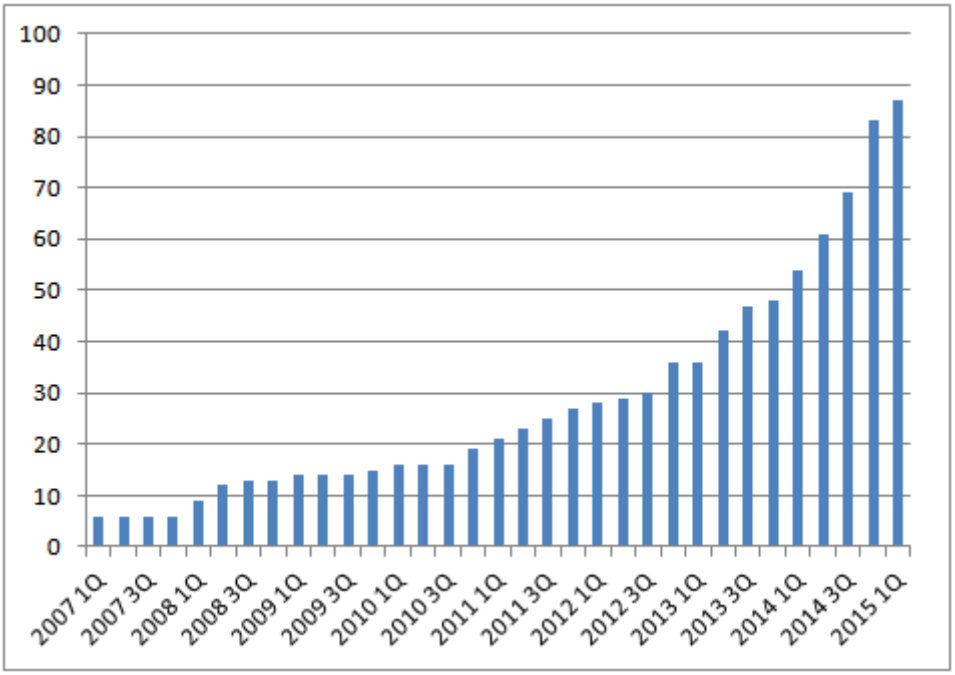
Fiddler Core's insecure Default flag may lead to Open Proxy Issue (5 月 28 日)
http://blog.jpcert.or.jp/2015/05/fiddler-cores-insecure-default-flag-may-lead-to-open-proxy-issue.html

APWG eCrime 2015 and Phishing Trends in Japan (6 月 30 日)
http://blog.jpcert.or.jp/2015/06/apwg-ecrime-2015-and-phishing-trends-in-japan.html

5. 日本シーサート協議会(NCA)事務局運営

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。

本四半期においては、野村ホールディングス株式会社 (Nomura Group CSIRT)、日本生命保険相互会社 (NLI-CSIRT)、株式会社ブロードバンドセキュリティ (B2SIRT)、グローバルセキュリティエキスパート株式会社 (GSX-CSIRT)の 4 組織が新規に加盟しました。本四半期末時点で 87 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]

6 月に「KEK 加速器見学会＆第 10 回シーサート WG 会」を開催いたしました。

2015 年 6 月 5 日 (金) 9:50-16:30
会場：高エネルギー加速器研究機構 (KEK) 小林ホール
参加人数：120 名

高エネルギー加速器研究機構にて SuperKEKB 加速器の見学会を行い、これに引き続いて、第 10 回シーサート WG 会を開催しました。運営委員と JPCERT/CC から講演を行い、また新規に加盟した 10 組織からチーム紹介が行われました。本四半期末現在 87 組織が加盟していて、来年度には 100 組織を超えると予想され、各 WG でも登録者が増えて活発な活動が行われることになりそうです。今後の課題として、会員数の増加に伴って増加する事務局業務の効率化を検討する必要があります。

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、報告に基づく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 ML を通じて、フィッシングに関するニュースや緊急情報を 21 件発信しました。

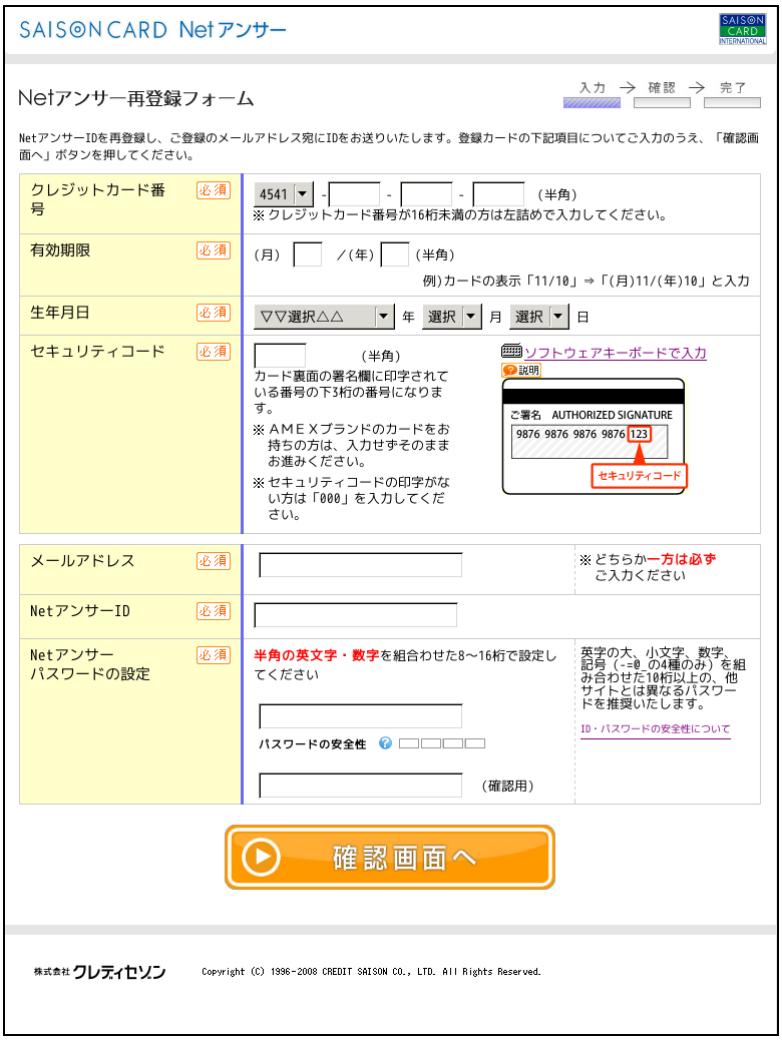
本四半期も、金融機関をかたるフィッシングや通信事業者をかたるフィッシングのサイトが新たに見つかったとの報告を受けました。4 月中旬からの金融機関をかたるフィッシングメールの報告の増加に加えて、5 月初旬からは、SMS (ショートメッセージサービス) を使った銀行のフィッシングサイトへの誘導が確認されました。6 月に入ってからも同様のフィッシングが続いたため、6 月 16 日に緊急情報を配信し、注意を喚起しました。協議会では、名前をかたられた事業者に、メール本文やサイトの URL 等の関連情報を提供しました。

また、金融機関をかたるフィッシングに関しては[図 6-1]の「[2015 年 4 月 15 日] 三菱東京 UFJ 銀行をかたるフィッシング」を含む 6 件、クレジットカード会社をかたるフィッシングに関しては[図 6-2]の「[2015 年 5 月 25 日] セゾン Net アンサーをかたるフィッシング」の 1 件、SMS (ショートメッセージサービス)

を使った銀行のフィッシングサイトに関しては[図 6-3]の「[2015 年 6 月 16 日]【注意喚起】SMS(ショートメッセージサービス)で誘導される銀行のフィッシングサイトにご注意ください」の 1 件、合計 8 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。

[図 6-1 三菱東京 UFJ 銀行をかたるフィッシング(2015/04/15)
https://www.antiphishing.jp/news/alert/mufg20150415.html]

さらに、これら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、すべてについて停止を確認しました。



[図 6-2 セゾン Net アンサーをかたるフィッシング (2015/05/25)
https://www.antiphishing.jp/news/alert/saison20150525.html]

[図 6-3【注意喚起】SMS(ショートメッセージサービス)で誘導される銀行のフィッシングサイトにご注意ください (2015/06/16)
https://www.antiphishing.jp/news/alert/_sms_20150616.html]

6.2. 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 2015 年 4 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201504.html
フィッシング対策協議会 2015 年 5 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201505.html
フィッシング対策協議会 2015 年 6 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201506.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 25 回運営委員会
日時：2015 年 4 月 17 日 16:00 - 18:00
場所：トッパン・フォームズ株式会社

フィッシング対策協議会 第 26 回運営委員会
日時：2015 年 5 月 19 日 16:00 - 18:00
場所：JPCERT/CC

フィッシング対策協議会 第 27 回運営委員会
日時：2015 年 6 月 12 日 16:00 - 18:00
場所：JPCERT/CC

7.2. フィッシング対策協議会総会ならびに創立 10 周年記念祝賀会開催

フィッシング対策協議会年次総会ならびに創立 10 周年記念祝賀会を次のとおり開催しました。

フィッシング対策協議会 平成 27 年度総会
日時：2015 年 6 月 19 日 15:00 - 16:00
場所：コンベンションルーム・AP 東京丸の内

フィッシング対策協議会創立 10 周年記念祝賀会
日時：2015 年 6 月 19 日 16:00 - 17:30
場所：コンベンションルーム・AP 東京丸の内

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、ソフトウエ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、2015 年 1 月 1 日から 2015 年 3 月 31 日までの活動実績と、本四半期に届出ないし公表

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[2015 年第 1 四半期(1 月～3 月)]
(2015 年 04 月 23 日)
https://www.jpcert.or.jp/press/2015/vulnREPORT_2015q1.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・運用をしています。収集したデータを、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 2015 年 1 月～3 月
(2015 年 04 月 27 日)
https://www.jpcert.or.jp/tsubame/report/report201501-03.html

8.3. SHODAN を悪用した攻撃に備えて －制御システム編－(2015/06/09)

攻撃対象にする制御システムの探索に SHODAN が悪用される可能性を指摘し、SHODAN のデータベースに登録されていないかを事前にチェックすることにより攻撃を受けるリスクを低減するために、アセットオーナが行うべき対策等をまとめたものです。

SHODAN を悪用した攻撃に備えて －制御システム編－
(2015 年 06 月 09 日)
https://www.jpcert.or.jp/ics/20150609ICSR-shodan.pdf

8.4. 分析センターだより「Internet Explorer の保護モード (2015-06-19)」

JPCERT/CC では、インシデントに関連して報告いただいた情報や収集した情報を調査し、インシデントをもたらした攻撃の手法やその影響を把握するアーティファクト分析という活動を行っています。分析技術者が日々のアーティファクト分析業務の中で感じたこと、発見したことを中心に執筆した「分析センターだより」として「Internet Explorer の保護モード (2015-06-19)」を公開しました。

Internet Explorer の保護モード (2015-06-19)
(2015 年 06 月 19 日)
https://www.jpcert.or.jp/magazine/acreport-ie.html

9. 主な講演活動一覧

(1) 早貸 淳子(専務理事)：
「サイバーセキュリティ・ソフトウェア企業への期待」
JASPA フェア 2015「セキュリティ対策と IoT」,2015 年 5 月 13 日
(2) 満永 拓邦(早期警戒グループ マネージャ)：
「企業における情報セキュリティ緊急対応体制～組織内 CSIRT の必要性～」
情報セキュリティ Expo IPA ブース,2015 年 5 月 13 日
(3) 小林 裕士(インシデントレスポンスチーム 情報セキュリティアナリスト)：
「レジストラに関連する脅威事例について」
JPRS ユーザ会,2015 年 5 月 21 日
(4) 満永 拓邦(早期警戒グループ マネージャ)：
「企業における情報セキュリティ緊急対応体制～組織内 CSIRT の必要性～」
Interop2015,2015 年 6 月 11 日
(5) 戸田 洋三(脆弱性流通対策グループリードアナリスト)：
「セキュリティ概論セキュアコーディングその 2: 実践」
JASPAR WG,2015 年 6 月 16 日
(6) 久保 正樹(脆弱性流通対策グループ脆弱性解析チーム リーダー)：
「セキュリティ概論セキュアコーディングその 1：その重要性」
JASPAR WG,2015 年 6 月 16 日
(7) 久保 啓司(インシデントレスポンスグループ マネージャ)：
「標的型攻撃への対応－JPCERT/CC－」
第 5 回 JNSA 記者懇談会 緊急時事ワークショップ～他人事ではない、サイバー攻撃を受けた組織の選択肢～, 2015 年 6 月 25 日

10. 主な執筆一覧

(1)宮地 利雄(技術顧問)：
「プロセス産業におけるセキュリティインシデントへの備え」
化学工学会会誌「化学工学」,2015 年 06 月 05 日

11. 協力、後援一覧

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11回IPAひろげよう情報モラル・セキュリティコンクール2015
主 催：独立行政法人情報処理推進機構(IPA)
募集期間：2015年4月1日(水)～9月7日(月)

(2) ISASecure SSA/SDLA/EDSA認証 説明会

主　催：技術研究組合制御システムセキュリティセンター(CSSC)

開催日：2015年5月14日(木)東京、2015年5月22日(金)大阪

(3) JAIPA Cloud Conference2015

主　催：JAIPA Cloud部会

開催日：2015年5月27日(水)

(4) Asia Pacific & Japan 2015

主　催：RSA Conference

開催日：2015年7月22日(水)～7月24日(金)

■インシデントの対応依頼、情報のご提供

info@jpcert.or.jp

https://www.jpcert.or.jp/form/

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：office@jpcert.or.jp