Japan Computer Emergency Response Team Coordination Center

JPCERT/CC®

JPCERT-PR-2015-01
発行日 : 2015-01-14

JPCERT/CC 活動概要 [2014 年 10 月 1 日 ～ 2014 年 12 月 31 日]

活動概要トピックス

ートピック1ー　セキュリティ人材育成の海外支援　～ タイで開催された学生向けマルウエア解析競技会に講師派遣 ～

JPCERT/CC は ASEAN 諸国をはじめとするアジア太平洋や、アフリカ地域において、CSIRT の設立運営や、それを支えるセキュリティ人材の育成に継続的に尽力しています。その一環として、本四半期には、タイで開催されたマルウエア解析競技会「Malware Analysis Competition 2014」に 3 名の講師を派遣しました。

この競技会は、ThaiCERT/ETDA が主催してマルウエア解析技術を学ぶ学生を対象に 10 月 30 日～31 日にバンコクで開催されました。タイ国内の 9 大学から 13 チーム、約 40 名の学生が参加し、競技を通じてマルウエアの解析の技術と実務を競い合いました。ThaiCERT/ETDA によると、この種の催し物としてはタイで最初の企画となりました。これを成功させるために、まず ThaiCERT/ ETDA が学生らにマルウエア解析技術を教えられるようになるための講習「Train the Trainer」を JPCERT/CC が 2014 年 5 月に実施し、その後の約半年で ThaiCERT/ ETDA が学生のトレーニングを行ってきました。

競技会の初日には、JPCERT/CC が、マルウエア解析の手法について講義とハンズオン演習を含むトレーニングが実施され、2 日めには、競技会が行われ、技術とプレゼンテーションの 2 つの部門で技量を競い合いました。技術部門では解析技術が評価され、プレゼンテーション部門では問題を解くにあたっての着眼点やアプローチに関する発表の方法と内容が評価されます。JPCERT/CC は後者の審査員を務めるとともに、プレゼンテーション部門の優勝チームに対して記念品を贈呈しました。

ThaiCERT/ETDA
https://www.thaicert.or.th/events/2014/ev2014-11-08-1.html

ートピック2ー　TSUBAME トレーニングをスリランカで実施

インターネット定点観測システム TSUBAME を十分に活用するには、複数の観測用センサーの配備などのハード面ばかりでなく、収集データを分析し解釈するソフト面における整備が併せて重要です。2007 年から着手したセンサー配備については、一部の国を除き、アジア・太平洋地域のほぼすべての国を既にカバーしています。JPCERT/CC では、中近東地域へのセンサー配備拡大の可能性を模索するとともに、TSUBAME プロジェクト参加組織の技術向上による運用の安定化や利用の高度化などのソフト面の強化

に努めています。
前四半期から本四半期にかけて、スリランカ民主社会主義共和国の Sri Lanka CERT|CC および TechCERT を訪問し、TSUBAME システムとセンサー機能の解説やシステムから得られた情報を分析し活用する方法などを紹介する、TSUBAME トレーニングを実施しました。TSUBAME の観測結果はシステムを通じて日頃からプロジェクトチーム間で共有していますが、このような対面で情報や意見を交換する機会は、TSUBAME プロジェクト参加組織の技術力の向上に大きく資するとともに、CSIRT 間の協力連携関係を緊密化する環境づくりとしても役立っています。
日本に影響するインシデントの中には、スリランカにあるコンピュータが関連した事例もこれまで散見されており、今回の関係強化により、今後のインシデント対応や注意喚起情報の発行などの対処が迅速化できるものと期待しています。

TSUBAME Training and Annual National Conference on Cyber Security in Sri Lanka
http://blog.jpcert.or.jp/2014/10/tsubame-training-and-annual-national.html

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

ートピック3ー　国際コミュニティへの情報の発信～5 年目を迎えた英語ブログ～

情報セキュリティ対策における国際連携のための環境づくりの一環として、日本の取組みを世界の人々に理解してもらうために、JPCERT/CC では英語による情報発信を強化しています。特に、英語ブログではホットな情報をタイムリに発信することに努めてきました。

JPCERT/CC の英語ブログは 2010 年 9 月に開設され、本四半期で 5 年目を迎えました。開設当初は、おおむね隔月の更新頻度でしたが、今年度はほぼ毎月新たな記事を投稿するよう努め、前年度の 2 倍の情報発信となっています。記事は、日本語で公表している資料の翻訳ではなく、すべて英語ブログ用に書き下ろしたもので、内容は、日本のインシデント動向を海外の読者向けに解説した記事から JPCERT/CC の活動紹介まで多岐にわたっており、海外の読者に日本のセキュリティ事情を少しでも理解していただき、円滑な国際連携の基盤となるよう工夫を重ねています。

英語ブログ
http://blog.jpcert.or.jp/

ートピック4ー　組織内 CSIRT 構築の動きが拡大　～企業等におけるセキュリティインシデントへの備え～

セキュリティ対策と言えばかつては未然防止に重点が置かれていましたが、巧妙化する攻撃の増加とともに、インシデントの発生を前提に効果的な対処を実現するための組織体制として、組織内 CSIRT への関

心や設置の動きが企業等の組織において高まっています。しかしながら、日進月歩の攻撃側に対抗できるよう、組織内 CSIRT の要員のスキルを高めるとともに使命感を維持し、組織内の他の部門にどのように働きかけていくべきかなどの組織内 CSIRT の運営には種々の悩みが伴います。
そうした悩みを持ち寄り、組織内 CSIRT の運営のグッド・プラクティスや、新たな脅威に関する情報を効果的に共有するために日本シーサート協議会(NCA：Nippon CSIRT Association)が 2007 年に設立され、その事務局として JPCERT/CC は同協議会をサポートしています。加盟組織数も、本四半期には 22 増えて 69 となり、業種も IT、通信、金融、保険、物流、宿泊業、小売業と多岐に渡っています。

JPCERT/CC では、同協議会に対するサポートだけでなく、CSIRT のあり方のバイブルとも言うべき「CSIRT マテリアル」を作成して公表する等、組織内 CSIRT の構築に向けた情報提供や働きかけを続けてきました。今日その趣旨が広く理解され始めたものとして組織内 CSIRT 構築の動きの拡大を歓迎するとともに、多数の会員を擁するようになった日本シーサート協議会の効果的な運営方法の工夫や、既設の組織内 CSIRT には情報提供の拡充などの、これから新たに CSIRT 設置を計画している組織には構築の支援などのサポートを、事務局として引き続き努めてまいります。

日本シーサート協議会
http://www.nca.gr.jp/index.html

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.セキュアコーディング啓発活動」、「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」、「12.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 6231 件、インシデント件数ベースでは 5606 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 2337 件でした。前四半期の 2125 件と比較して 10%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_Report20150114.pdf

1.1.1. インシデントの傾向

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 406 件で、前四半期の 417 件から 3%減少しました。また、前年度同期(601 件)との比較では、32%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	10 月	11 月	12 月	国内外別合計（割合）
国内ブランド	41	23	11	75(18%)
国外ブランド	78	91	67	236(58%)
ブランド不明	27	29	39	95(23%)
月別合計	146	143	117	406(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。

本四半期は、国内のブランドを装ったフィッシングサイトの数が前四半期に比べて大幅に減少しました。これは、前四半期に非常に多く確認されていた国内金融機関を装ったフィッシングサイトが、10 月には減少し、11 月以降には確認されなかったことが原因となっています。国内オンラインゲームサービスを装ったフィッシングサイトの数も前四半期に比べて減少していますが、10 月末以降、継続的に報告が寄せられています。

フィッシングサイトの調整先の割合は、国内が 70%、国外が 30%であり、前四半期(国内 58%、国外 42%)にくらべ、国内への調整が増加しています。

本四半期に報告が寄せられた Web サイト改ざんの件数は、781 件でした。前四半期の 968 件から 19%減少しています。

Web サイトが改ざんされていて、そこから誘導される先のページに埋め込まれている Microsoft の脆弱性(MS14-064)を悪用するコードによって、マルウエアに感染させられる事例を 11 月後半から 12 月半ばに複数確認しました。

この脆弱性は 11 月のセキュリティアップデートで公表され、限定的な範囲で標的型攻撃に使用されていたとされたものです。前述の事例では、攻撃者が、11 月の公表から非常に短期間のうちに、修正プログラムを分析して脆弱性の情報を入手し、それを悪用するコードを開発して Web サイトに組み込んだものと推測されます。この事例からも、セキュリティアップデートの公開後は、攻撃の被害を防ぐために、できる限り早く適用することが推奨されます。

また、12 月初めごろから、難読化された JavaScript がページの末尾に埋め込まれた改ざんで、tag[数字 1,2 文字].php のような URL の不審なサイトに誘導するものを多数確認しています。その他にも、難読化された JavaScript と外部サイトのリンクが埋め込まれた改ざんで、Web の検索結果で特定のサイトを上位に表示させるための SEO ポイズニングを目的としたと見られるものや、薬の販売や宣伝を目的としたとみられるサイトへの転送設定のみが記述されたページなどが不正に設置される事例を多数確認しています。

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元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：18 件　https://www.jpcert.or.jp/at/

2014-10-10　TCP 10000 番ポートへのスキャンの増加に関する注意喚起
2014-10-15　2014 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
2014-10-15　Adobe Flash Player の脆弱性 (APSB14-22) に関する注意喚起
2014-10-15　2014 年 10 月 Microsoft セキュリティ情報 (緊急 3 件含) に関する注意喚起
2014-10-21　Drupal の脆弱性に関する注意喚起
2014-10-22　2014 年 10 月 Microsoft OLE の未修正の脆弱性に関する注意喚起
2014-11-05　登録情報の不正書き換えによるドメイン名ハイジャックに関する注意喚起
2014-11-12　Adobe Flash Player の脆弱性 (APSB14-24) に関する注意喚起
2014-11-12　2014 年 11 月 Microsoft セキュリティ情報 (緊急 4 件含) に関する注意喚起
2014-11-13　2014 年 11 月一太郎シリーズの脆弱性に関する注意喚起
2014-11-19　2014 年 11 月 Kerberos KDC の脆弱性に関する注意喚起
2014-11-26　Adobe Flash Player の脆弱性 (APSB14-26) に関する注意喚起

2014-12-09　ISC BIND 9 サービス運用妨害の脆弱性 (CVE-2014-8500) に関する注意喚起
2014-12-10　2014 年 12 月 Microsoft セキュリティ情報 (緊急 3 件含) に関する注意喚起
2014-12-10　Adobe Flash Player の脆弱性 (APSB14-27) に関する注意喚起
2014-12-10　Adobe Reader および Acrobat の脆弱性 (APSB14-28) に関する注意喚起
2014-12-19　Active Directory のドメイン管理者アカウントの不正使用に関する注意喚起
2014-12-19　TCP 8080 番ポートへのスキャンの増加に関する注意喚起

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：16 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 70 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。

2014-10-01　PHP 5.4 系最後のリリース
2014-10-08　10 月は「情報セキュリティ国際キャンペーン」
2014-10-16　「iLogScanner V4.0」が公開
2014-10-22　日米サイバーセキュリティシンポジウム 2014
2014-10-29　Internet Week 2014 のプログラム紹介
2014-11-06　「情報ネットワークの強さと弱さ　大規模自然災害からサイバー空間まで」シンポジウム開催
2014-11-12　サイバーセキュリティ基本法が成立
2014-11-19　DNSSEC で ECDSA アルゴリズムを使うのはまだ早い？
2014-11-27　EMET 5.1 リリース
2014-12-03　「SECCON CTF 2014 online 予選」開催
2014-12-10　日本版「STOP. THINK. CONNECT.」サイト公開
2014-12-17　第 10 回 IPA 「ひろげよう情報モラル・セキュリティコンクール」受賞作品決定
2014-12-25　『仮想戦争の終わり - サイバー戦争とセキュリティ - 』発売

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内 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。

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。

【登録情報の不正書き換えによるドメイン名ハイジャックに関する注意喚起】

JPCERT/CC は、ドメイン名ハイジャックのインシデント報告を複数受領しました。.com 配下の国内組織のドメイン名の登録情報がレジストラまたはレジストリ内で、攻撃者が用意したネームサーバを参照するよう不正に書き換えられ、当該組織の Web サイトを閲覧しようとすると不正なサーバに誘導されることが確認されました。
確認した事例においては、攻撃者が、ドメイン名の登録情報を不正に書き換えた後、長い期間をおかず元に戻して、ドメイン名管理者やユーザが気づいて原因の調査と対処を始めるのを遅らせようとしていた点が特筆できます。また、誘導先のサーバの一部については、アクセスしたユーザ端末がマルウエアに感染してしまうことを実際に確認しました。
この種のインシデントは日本だけでなく、世界的に頻発しており、被害の拡大が懸念されたため、JPCERT/CC は、「登録情報の不正書き換えによるドメイン名ハイジャックに関する注意喚起」を公開し、ドメイン名登録者やドメイン名管理担当者に向けて、攻撃に対する事前対策を促す注意喚起情報を提供しました。

【Kerberos KDC の脆弱性に関する注意喚起】

11 月 19 日、マイクロソフト社から Kerberos KDC に関する緊急のセキュリティ情報が公開されました。攻撃者が、一般のドメインユーザアカウントを得れば、当該脆弱性を使用することにより、ドメイン管理者アカウントの権限に昇格できるというものです。

最近の標的型攻撃では、攻撃者がまずは内部ネットワークの端末に一般ユーザの権限で侵入した後に、他の端末への侵害と他のユーザのアカウント窃取を進め、最終的には、さらに高い権限を得るため管理者アカウントを奪取してネットワーク全体を乗っ取る経過をたどることがしばしばあります。管理者アカウントを取った攻撃者は、気づかれないように長期にわたり情報窃取を行うための仕組みを密かに作り込むこともできます。
今回の脆弱性は、このような攻撃シナリオの実現可能性を高めるものでした。実際、マイクロソフトのセキュリティ情報によると、限定的な標的型攻撃が観測されています。

JPCERT/CC は、「Kerberos KDC の脆弱性に関する注意喚起」を公開し、サーバ管理者などに対し広く注意を呼びかけました。

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。2014 年 12 月末時点で、観測用センサーはアジア・太平洋地域の 23 地域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

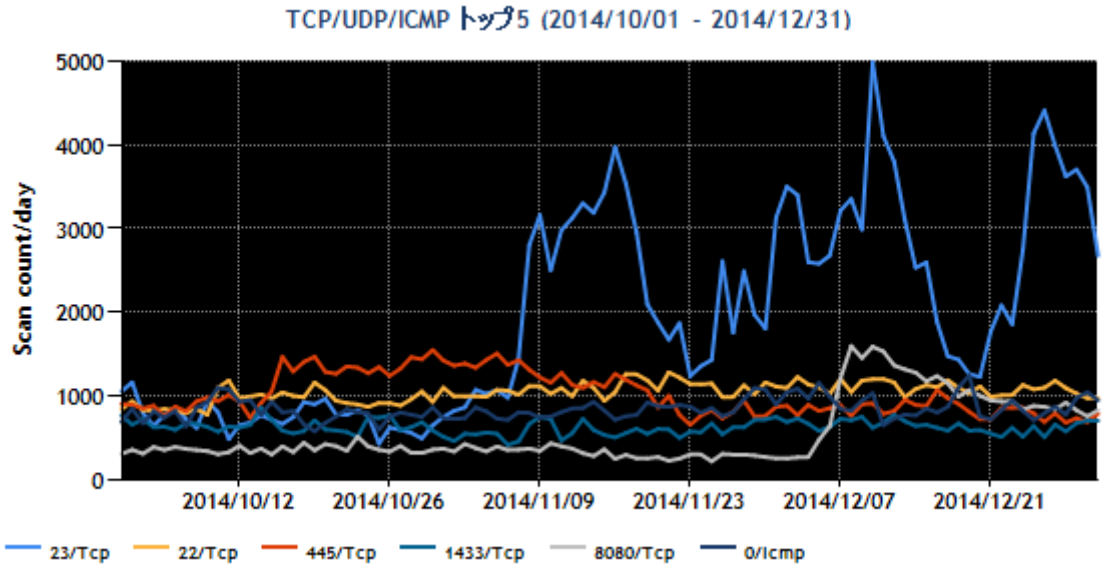
JPCERT/CC は、TSUBAME で収集したデータを宛先ポート番号や送信元地域ごとに分類して統計分析し、既知の脆弱性情報やマルウエア、攻撃ツール等との関連を考察することで、攻撃活動や準備活動の捕捉に努めています。

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、2014 年 7 月から 9 月分のレポートを 10 月 28 日に公開しました。

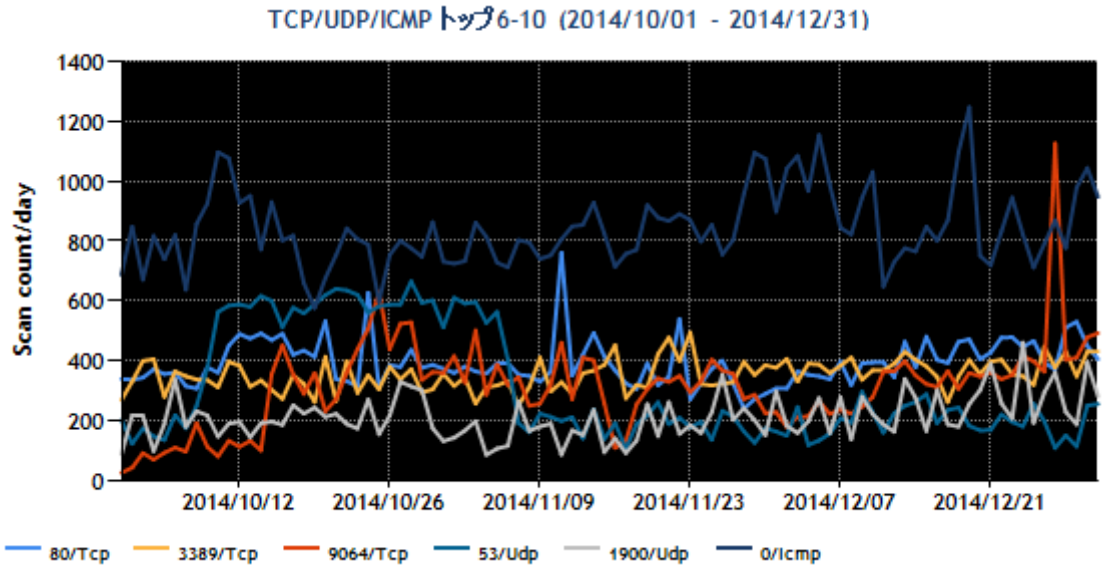
TSUBAME 観測グラフ
https://www.jpcert.or.jp/tsubame/index.html#examples

インターネット定点観測レポート(2014 年 7～9 月)
https://www.jpcert.or.jp/tsubame/report/report201407-09.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。

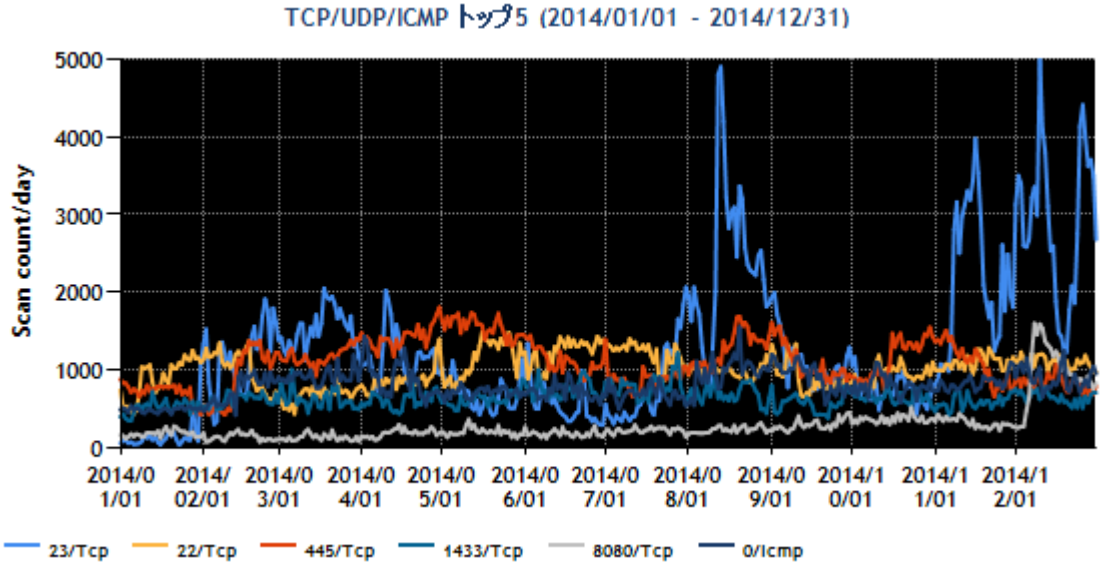


[図 1-1 宛先ポート別グラフ トップ 1-5 (2014 年 10 月 1 日-12 月 31 日)]

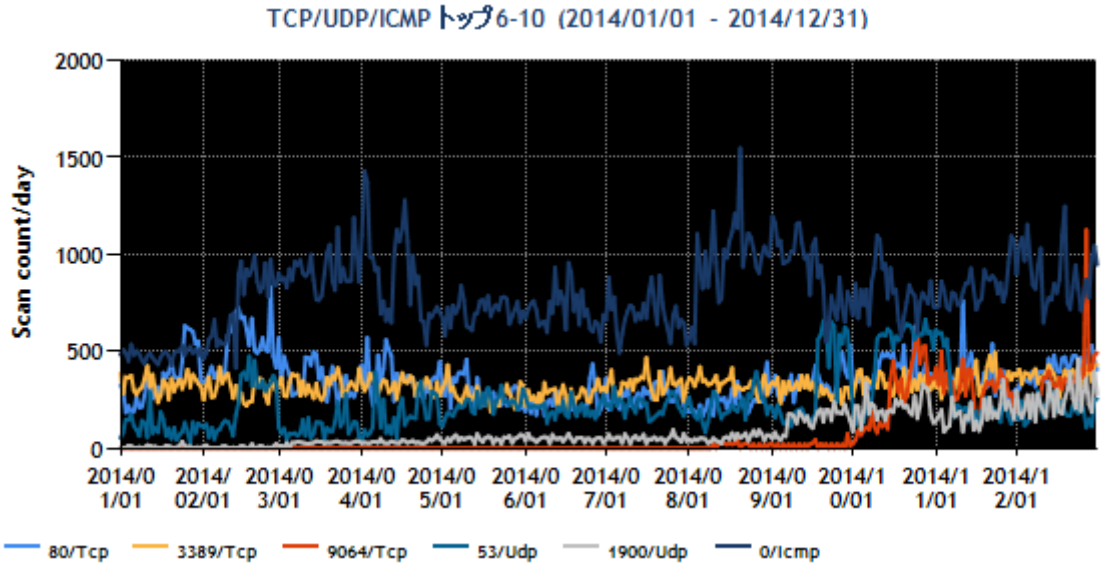


[図 1-2 宛先ポート別グラフ トップ 6-10 (2014 年 10 月 1 日-12 月 31 日)]

また、過去 1 年間(2014 年 1 月 1 日～2014 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。



[図 1-3 宛先ポート別グラフ トップ 1-5 (2014 年 1 月 1 日-2014 年 12 月 31 日)]



[図 1-4 宛先ポート別グラフ トップ 6-10 (2014 年 1 月 1 日-2014 年 12 月 31 日)]

今四半期は、23/TCP 宛のパケットが 11 月上旬に急増し、その状態が約一週間続いたあと減少しましたが、12 月に入ってからも数回大きな増減を繰り返しながら増加した状態が続くといった事象を観測しています。過去にパケットが増加した事例では、マルウエアに感染した海外製ネットワークカメラやブロードバンドルータが関与していましたが、今回はそれらの製品に加えて国内でも販売されている海外ベンダ製の NAS 製品が送信元になっている事例を複数確認しています。当該 NAS 製品もマルウエアに感染しパケットの送信元に加わったと推測されます。同マルウエアは、8080/TCP 宛のパケットも送信して

います。
該当 NAS 製品にはベンダが対応済みの既知の脆弱性が存在します。また、ネットワーク上の該当 NAS 製品を探索し、脆弱性を悪用してそれを感染させる機能をもつマルウエアも存在しています。
今回のパケット数の増加は、当該 NAS 製品の脆弱性対策が進んでいないため、これを悪用するマルウエアの活動が広まった結果によるものと推測しています。本事象については、該当 NAS 製品のベンダにも情報を共有しています。
その他、順位に変動はありますが、Windows や Windows 上で動作するソフトウエア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 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は、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。

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、本四半期もセンサー上で継続して多数観測されました。これらの観測されたパケットは、実際には存在しない FQDN を OpenResolver 経由で多数問い合わせることにより DNS 権威サーバに過剰な負荷を課そうとする攻撃において、攻撃者が応答パケットを受け取らずにすませるために詐称した送信元が，たまたまセンサーの IP アドレスだったために観測されたパケットであると推測されています。すなわち、攻撃者が OpenResolver だと思って利用したノードが，実際には OpenResolver でなかった場合には ICMP エラーが、本当に OpenResolver であった場合には「名前解決できなかった」旨の応答がセンサーに届いていると見られます。この考え方に基づく分析で、日本国内だけでも毎日 10 数件近くの OpenResolver が新たに見つかっています。JPCERT/CC は、この情報を DNS サーバの管理者に提供し、DNS サーバやネットワーク機器が OpenResolver となっていないか調査を依頼しまし、多くの管理者から「当該サーバの設定が不適切で OpenResolver であったことを確認し、必要な対応を行った」等の返事を得ています。

1.3.3. TSUBAME トレーニングの実施

本四半期は、TechCERT (スリランカ民主社会主義共和国の CSIRT) 向けに、次の要領で TSUBAME トレーニングを実施しました。

日時：2014 年 10 月 2 日 (火)
場所：スリランカ民主社会主義共和国 モラトゥワ (TechCERT 会議室)
参加人数：13 名(TechCERT のメンバが参加)

トレーニングの内容：
- TSUBAME プロジェクトの概要
- TSUBAME システム、センサーの機能の説明
- TSUBAME システムから得られた情報の活用方法の紹介など

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

本基準では、受付機関に IPA、調整機関に JPCERT/CC が指定されています。JPCERT/CC は IPA が受け付けた届出情報の転送を受けて、製品開発者への情報提供を行い、対策情報公開に至るまでの調整を行っています。最終的には、IPA と共同で、脆弱性情報ポータル JVN において対策情報を公開しています。両組織間においては、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、緊密な連携を行っています。なお、本基準における IPA の活動および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

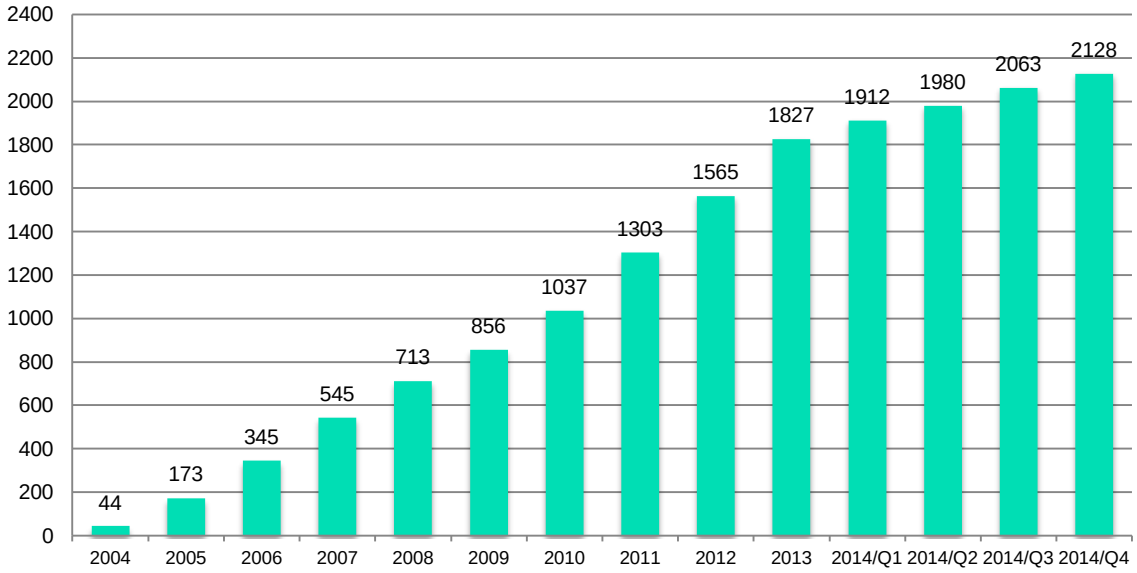
JPCERT/CC は、経済産業省告示「ソフトウエア等脆弱性情報取扱基準」（平成 26 年経済産業省告示 第 110 号。以下「本基準」といいます。)に基づいて製品開発者とのコーディネーションを行う「調整機関」に指定されており、本基準を踏まえて取りまとめられた「情報セキュリティ早期警戒パートナーシップガイドライン（以下「パートナーシップガイドライン」といいます。）に従って、対象となる脆弱性に関係する製品開発者の特定、脆弱性関連情報の適切な窓口への連絡、開発者による脆弱性の検証等の対応や脆弱性情報の公表スケジュール等に関する調整を行い、原則として、調整した公表日に JVN を通じて脆弱性情報等を一般に公表しています。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 65 件(累計 2128 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。

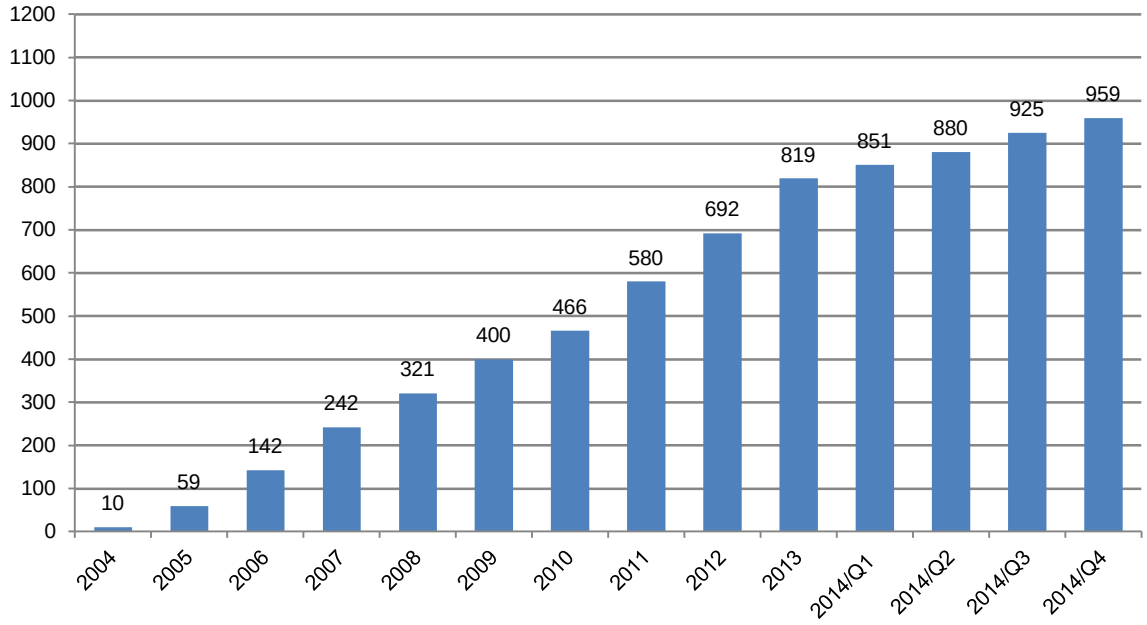
JVN(Japan Vulnerability Notes)
https://jvn.jp/



[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 34 件(累計 952 件)で、累計の推移は[図 2-2]に示すとおりです。34 件のうち、21 件が国内製品開発者の製品、11 件が海外の製品開発者の製品、2 件が国内外の複数の製品開発者の製品のものでした。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 4 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、ウェブアプリケーションフレームワークやサーバ関連製品が 8 件、Android 搭載携帯端末や Android アプリに関するものが 6 件、ルータ等組込系製品が 6 件、BSD や NAS 等の OS が 2 件、ガントチャートプラグイン製品が 2 件あり、それ以外では、グループウエア、ブログ作成ソフトウエア、アクセスログ検出ツール、制御系ソフトウエアパッケージ等がそれぞれ 1 件ずつとなり、多様な製品に関するものが混在していました。



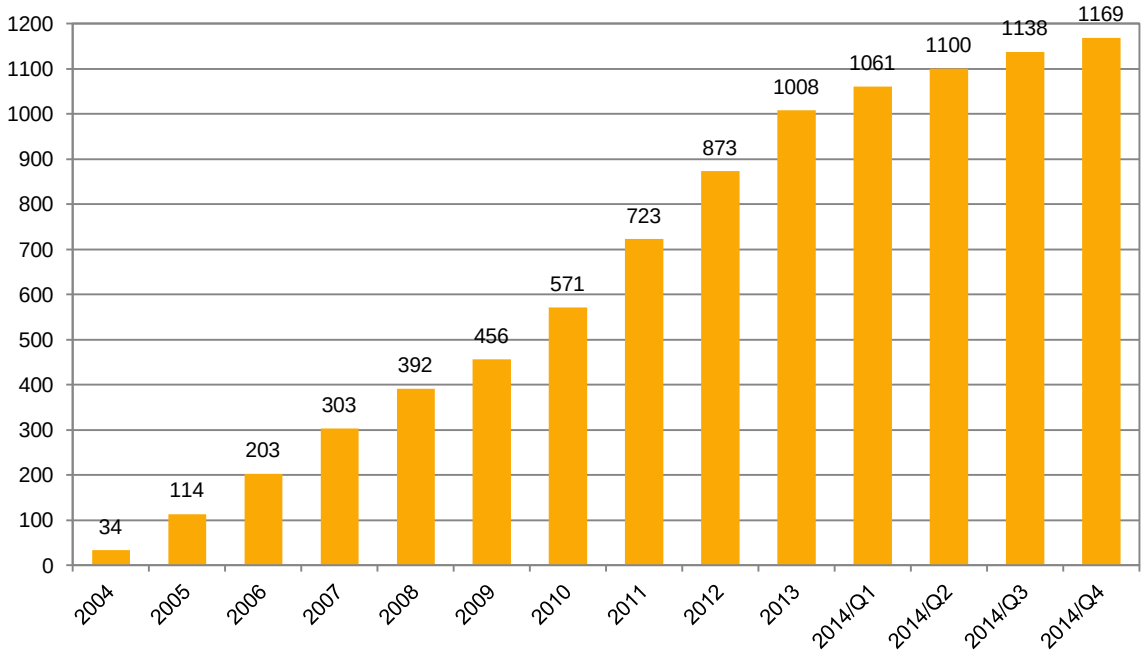
[図 2-2 公表を行った国内取扱脆弱性情報の累積件数]

本四半期に公表した国際取扱脆弱性情報は 31 件(累計 1169 件)で、累計の推移は[図 2-3]に示すとおりです。

2014 年 4 月には OpenSSL の Heartbleed と呼ばれる脆弱性が公になり、オープンソース製品や SSL 通信に関連する脆弱性として多くの注目を集めました。本四半期においても、暗号化通信プロトコルである SSL に新たな脆弱性が指摘されました。JPCERT/CC は、その脆弱性情報を JVNVU#98283300 「SSLv3 プロトコルに暗号化データを解読される脆弱性(POODLE 攻撃)」として CERT/CC よりも先に JVN で公開するとともに、影響範囲が大きいと考えられたので、日本国内の関連する製品開発者へ情報を展開し調整を行いました。

本四半期に公表した脆弱性情報の内訳を多いものから挙げると、ISC BIND や DNS 等サーバ関連製品に関するものが 5 件、上述の SSLv3（POODLE 攻撃）を含むプロトコルに関するものが 4 件、「緊急」として公開した Windows をはじめとする Microsoft 製品に関するものが 3 件、組込系製品（ルータ等）に関するものが 3 件ありました。また Apple による自社製品に関する脆弱性情報の届出によるものが 1 件でした。

本四半期においては、「緊急」の注意喚起として、JVNTA14-317A「Apple iOS に対する攻撃手法 Masque Attack」を、米国 US-CERT Technical Alert TA13-317A “Apple iOS "Masque Attack"と同期し、JVN においても公開しました。



[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

本基準に基づいて脆弱性が報告されたものの、調査と対策を期待して呼び掛けても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」として公表しています。これまでに 185 件(製品開発者数としては 117 件)を公表し、22 件(製品開発者の数としては 15 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製品開発者名は 12 件でした。本四半期末日時点で、合計 163 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、脆弱性情報を公表できる規定が、今年5月に改定された本規準およびパートナーシップガイドラインに盛り込まれました。この改訂を受けて、第一回目となる公表判定委員会が本四半期に開催されました。

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、2014 年上期においては 4 件、本四半期においても 1 件と合計 5 件の脆弱性情報の公開を行い、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（National CERT）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に対し、34 件全てに 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。

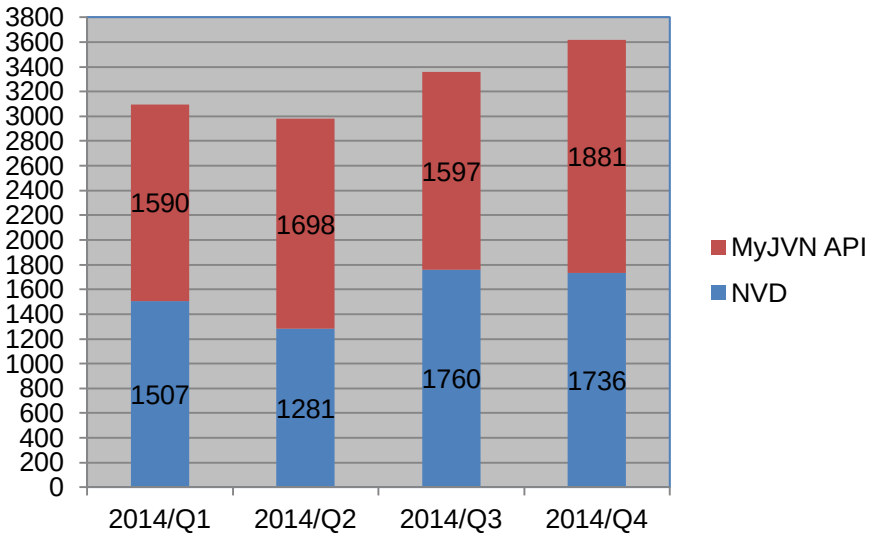
News & Events　“JPCERT/CC Becomes CVE Numbering Authority”
https://cve.mitre.org/news/archives/2010_news.html#jun232010a
CVE Numbering Authorities
https://cve.mitre.org/cve/cna.html
About CVE
https://cve.mitre.org/about/index.html

2.1.5. VRDA フィードによる脆弱性情報の配信

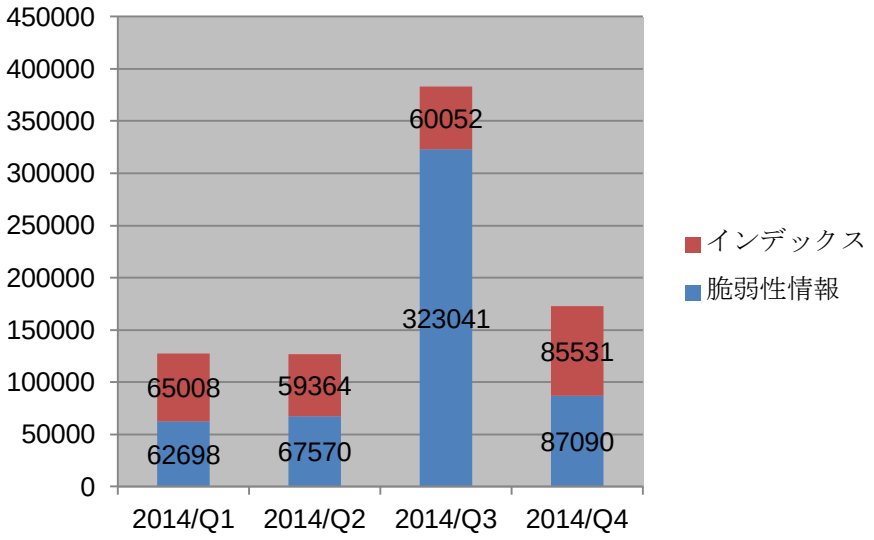
JPCERT/CC は、大規模組織の組織内 CSIRT 等での利用を想定して、KENGINE 等のツールを用いた体系的な脆弱性対応を可能とするため、IPA が運用する MyJVN API および NIST(National Institute of Standards and Technology)の NVD(National Vulnerability Database)を外部データソースとして利用した、VRDA(Vulnerability Response Decision Assistance)フィードによる脆弱性情報の配信を行っています。
VRDA フィードについての詳しい情報は、次の 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 2-4]に、VRDA フィードの利用傾向を[図 2-5]と[図 2-6]に示します。[図 2-5]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 2-6]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。

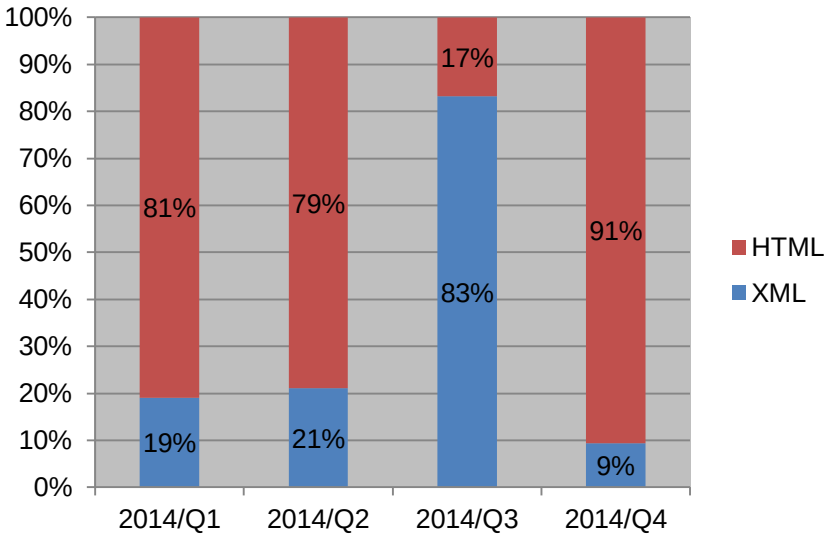


[図 2-4 VRDA フィード配信件数]



[図 2-5 VRDA フィード利用件数]

[図 2-5] 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 42%増加しました。一方、前四半期に急激な増加が見られた脆弱性情報の利用数については、前四半期と比較し、約 73%減少しました。



[図 2-6 脆弱性情報のデータ形式別利用割合]

[図 2-6] 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、前四半期とは大きく異なり、第二四半期以前と同様に HTML 形式が利用される割合が高い利用傾向が見られました。

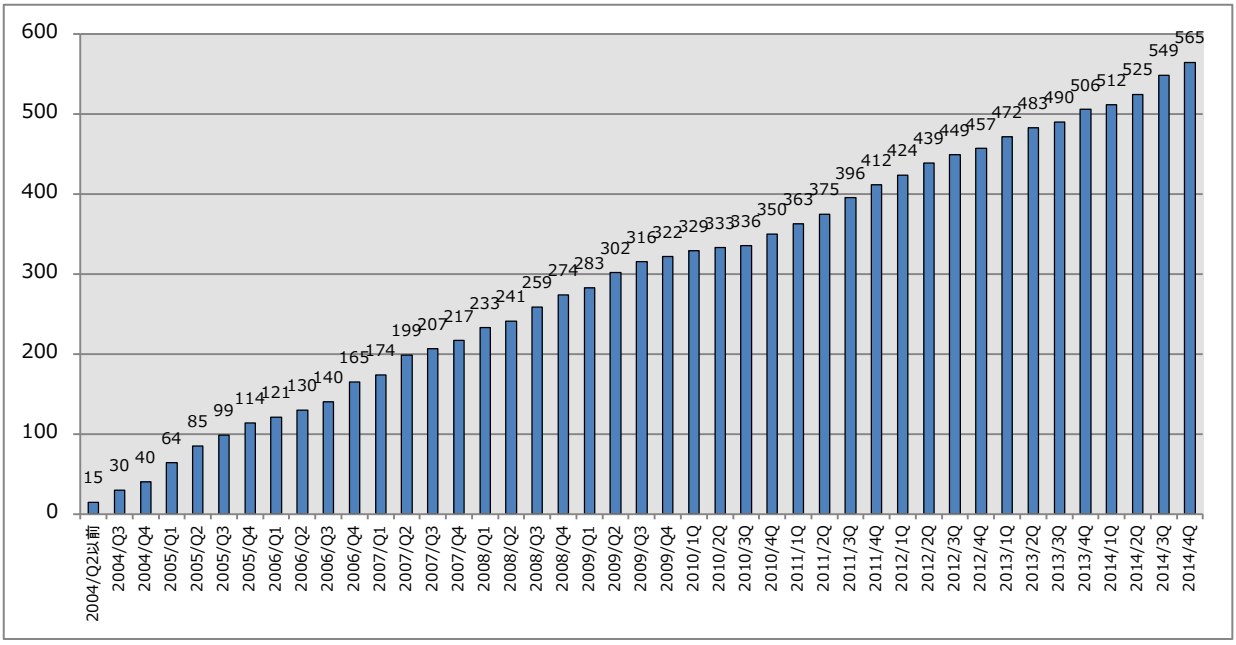
2.2. 日本国内の脆弱性情報流通体制の整備

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、2014 年 12 月 31 日現在で 565 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。



[図 2-7 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 2014 年 11 月 11 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、製品開発者における脆弱性診断や脆弱性対応の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. セキュアコーディング啓発活動

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おり、その一環として、カンファレンス等での講演を行っています。
今四半期は、CMU CERT プログラムの研究者とともに JRE のライブラリの脆弱性事例に関する発表を JavaOne2014 で行った他、デジタルボンド社が主催する制御システムセキュリティに関するカンファレンス「S4xJapan 2014」で制御システム用製品の脆弱性の傾向とその対策に有効な CERT C コーディングルールに関する調査結果の発表を、オープンソースソフトウエアの利用推進に関するコミュニティのカンファレンス「関西オープンフォーラム 2014」や「オープンソースカンファレンス 2014 福岡」では脆弱性やセキュアコーディングに関する講演を行いました。

JavaOne2014
[CON2120] Anatomy of Another Java Zero-Day Exploit
https://oracleus.activeevents.com/2014/connect/sessionDetail.ww?SESSION_ID=2120

S4xJapan 2014
ICS 脆弱性の調査およびその対策としての CERT C コーディングルール
http://digitalbond.jp/S4xjapan-論文・プレゼンテーション募集/2014-s4xjapan-プレゼンテーション/

KOF2014
脆弱性に学ぶセキュアコーディング「SSL/TLS 証明書検証編」
https://k-of.jp/2014/session/563

オープンソースカンファレンス 2014 Fukuoka
Lessons (to be) Learned from Handling OpenSSL Vulnerabilities
https://www.ospn.jp/osc2014-fukuoka/modules/eguide/event.php?eid=13

また、講演の資料は次の Web ページからも閲覧できます。
http://www.slideshare.net/jpcert_securecoding

2.3.2. CERT C コーディングスタンダードのルールを最新版にアップデート中

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通りです。

削除(1 件)

- INT03-C. セキュアな整数ライブラリを使用する

内容の更新(15 件)

- PRE08-C. ヘッダファイル名が一意であることを保証する
- PRE09-C. セキュアな関数を非推奨関数や時代遅れの関数に置き換えない
- PRE10-C. 複数の文からなるマクロは do-while ループで包む
- PRE11-C. マクロ定義をセミコロンで終端しない
- PRE12-C. 安全でないマクロを定義しない
- PRE13-C. あらかじめ定義された標準マクロで準拠規格やバージョンを確認する
- PRE30-C. 文字列連結によってユニバーサル文字名を作成しない
- PRE31-C. 安全でないマクロの引数では副作用を避ける
- PRE32-C. マクロの引数内で前処理指令を使用しない
- INT00-C. 処理系のデータモデルについて理解する
- INT01-C. オブジェクトのサイズを表現するすべての整数値に rsize_t もしくは size_t を使用する
- INT02-C. 整数変換のルールを理解する
- INT04-C. 信頼できない入力源から取得した整数値は制限する
- INT31-C. 整数変換によってデータの消失や解釈間違いが発生しないことを保証する
- INT33-C. 除算および剰余演算がゼロ除算エラーを引き起こさないことを保証する

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 432 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 2 件でした。

・2014/10/30 [参考情報] ICS-ALERT-14-281-01 Ongoing Sophisticated Malware Campaign Compromising ICS について

・2014/11/06 【参考情報】Kabona 社製のビル管理用製品について

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 回配信しました。

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 399 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

本四半期に報告された制御システムに関連するインシデントの件数は 0 件でした。
今期より、「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する情報提供を開始しました。悪用されてしまう危険性のあるシステムに関する今期の情報提供件数は、3 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. 制御システム向けツールの配布情報

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)の配布を行っています。本四半期は、日本版 SSAT に関して 3 件、J-CLICS に関して 10 件の利用申込みがありました。直接配布件数の累計は、日本版 SSAT が 163 件、J-CLICS が 221 件となりました。

3.5. 制御システム用製品開発ベンダにおける脆弱性対応窓口の設置支援

2014 年 8 月に「参考資料：制御システム用製品の開発ベンダにおける脆弱性対応について」を公開したことにあわせて、国内の制御システム用製品の開発ベンダが、脆弱性情報を受け取る窓口を開設する支援活動を行っています。今四半期に、新たに脆弱性情報の窓口を設置し、製品開発者リストへの登録を行った制御システム製品開発ベンダは 1 社となります。また、累計で 9 社となりました。

3.6. 海外セミナー参加報告会の開催

2014 年 12 月 18 日、弊センター会議室にて「海外カンファレンス参加報告会」と題したセミナーを開催いたしました。本セミナーでは、制御システムセキュリティに関する最近の海外カンファレンスから「ISC2014」(中国)と「ICSJWG 2014 Fall Meeting」(米国)と「ICS Cyber Security Conference 2014」(米国)に関して、背景にある問題意識を交えながら技術動向や注目された講演に関して概要をまとめ報告いたしました。セミナーには、主に制御システム関連のアセットオーナーやベンダの方を中心に 20 名の方にご参加頂きました。

3.7. 制御システムに関するセキュリティセミナーの開催

2014 年 12 月から 2015 年 2 月にかけて岡山、福岡、名古屋、東京で制御システムセキュリティセミナーを開催しています。本セミナーでは、制御システム環境におけるセキュリティ対策の必要性が叫ばれる中、どのように取り組んでいくべきなのか弊センターが実施した情報収集や独自の調査結果をもちいて、今後の対策を考える上で考慮すべき点について紹介します。本四半期は、岡山で本セミナーを開催し 17 名の方にご参加頂きました。

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. タイ CSIRT 構築支援等(2014 年 10 月 30 日-31 日)

ThaiCERT/ETDA がタイの首都バンコクで 10 月 30 日と 31 日に開催したタイ国内の学生向けのマルウエア解析競技会（Malware Analysis Competition 2014）に、JPCERT/CC は 3 名の講師を派遣しました。10 月 30 日には、タイの大学生約 40 名に対して、マルウエア解析の手法について講義とハンズオン演習を含めたトレーニングを行いました。10 月 31 日には、解析技術を競う技術部門と発表能力を競うプレゼンテーション部門から構成される競技会が行われ、JPCERT/CC はプレゼンテーション部門の審査員を務めました。また、日本国内のセキュリティシンポジウムで行われている同様の競技会の概要を紹介しました。

[図 4-1 トレーニングの様子]

4.1.2. アフリカ CSIRT 構築支援 等(2014 年 11 月 22 日-27 日)

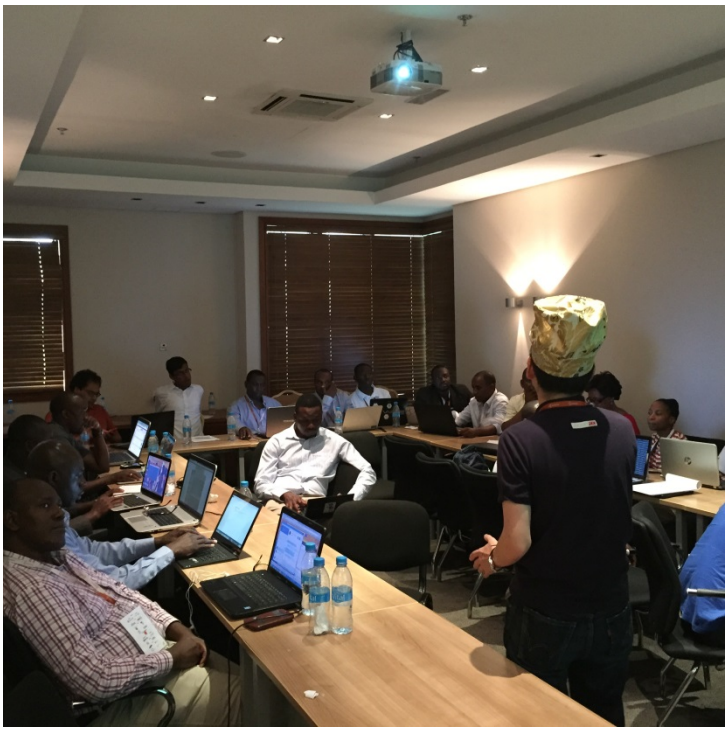
JPCERT/CC は、11 月下旬にモーリシャス共和国のエビン・シティで開催された国際会議 Afrinic-21 に参加するとともに、アフリカ諸国向けに 1 日コースの CSIRT トレーニングを行いました。また 11 月 26 日には AfricaCERT Cybersecurity Day に参加しました。

JPCERT/CC が担当した CSIRT トレーニングは、アジア地域との連携を促進する AfricaCERT が Afrinic-21 のトレーニングプログラムの一つとして開催したプログラムです。同様のトレーニングは 2010 年春からほぼ半年ごとに実施しており、今回で 9 回目の開催となります。今回のトレーニングにはモーリシャスやその近隣の南アフリカ、ボツワナ等からの参加者を中心に合計 25 名以上が参加しました。

11 月 22 日から 24 日は、FIRST の講師による CSIRT 研修が行われました。JPCERT/CC は、FIRST の Board of Directors メンバの一員として、講師の手配・調整を行うとともに、現地での研修サポートを行いました。

11 月 25 日は、JPCERT/CC は、CSIRT 技術者向けにグループワークで行った Web サイトインシデントレスポンス演習の主任講師を担当しました。

11 月 26 日の AfricaCERT Workshop では、地域 CSIRT としての AfricaCERT の現状と今後の活動計画が事務局から説明され、参加各国からはそれぞれの近況報告がありました。JPCERT/CC は APCERT などの地域 CSIRT の重要性について講演しました。



[図 4-2 トレーニングの様子]

Afrinic 及び CSIRT トレーニングと AAF についての詳細は、次の Web ページをご参照下さい。

Afrinic 及び Afrinic 21 公式ページ
http://meeting.afrinic.net/afrinic-21/en/

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

制度や技術が成長段階にある国・地域などからの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。

4.1.3. インドネシアの CSIRT 構築支援活動(12 月 9 日-12 日)

インドネシアの CSIRT の構築・運用支援活動として、独立行政法人国際協力機構（JICA）の依頼の下、2 名の講師派遣を行い、インドネシア通信省職員 6 名に対して CSIRT 研修を行いました。また 12 月 11 日には、独立行政法人国際協力機構（JICA）が主催した重要インフラ防護セミナーにおいて、「Establishing Critical Information Infrastructure Protection」と題する講演を行いました。JPCERT/CC の活動概要や、重要インフラ防護に向けた日本の取り組みについて、インドネシアの産学官の関係者等約 100 名に向けて紹介しました。

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、12 月 3 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、これらの会議の主導およびサポートを行いました。

4.2.1.2. APCERT を代表しての会議出席

・OIC-CERT 年次会合
ブルネイで 10 月 20 から 22 日まで開催された OIC-CERT 年次総会において、JPCERT/CC は APCERT を代表して登壇し、インターネットガバナンスに携わる関係者に対して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るとともに、サイバー分野での官民連携、APCERT の取組み等の紹介／報告を行いました。

OIC-CERT 2014 公式ページ
http://oic-cert.org/event2014/

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、今期は、組織運営に関わる議論にメールや電話で参画しました。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

4.2.3. スリランカ Sri Lanka CERT|CC 主催の会議での講演（2014 年 10 月 1 日）

スリランカの National CSIRT である Sri Lanka CERT|CC がコロンボにて開催した会議” Cyber Security Week 2014 - 7th Annual National Conference on Cyber Security”にて JPCERT/CC 職員が JPCERT/CC の国際連携を伴う活動やプロジェクトに関する講演を行いました。通常の活動に加え、脆弱性ハンドリングや TSUBAME プロジェクトに関する解説をスリランカ政府、ISP の関係者、開発者等約 250 名に向けて紹介しました。

4.2.4. ルーマニア CERT-Ro 主催の会議での講演（2014 年 11 月 3 日）

ルーマニアの National CSIRT である CERT-RO が 11 月 3 日にブカレストで開催した、同組織主催の第 4 回年次会合にて JPCERT/CC 職員が講演を行いました。JPCERT/CC の活動概要や最近のサイバーセキュリティ上の脅威の動向等を、ルーマニアの産学官の関係者等約 60 名に向けて紹介しました。

4.2.5. 経済産業省の委託事業によるタイへの専門家派遣（2014 年 11 月 7 日）

「平成 26 年度 貿易投資促進事業（制度・事業環境整備）」の一環で実施されたタイの重要インフラ関係者に対する情報セキュリティ強化支援の目的で、JPCERT/CC から制御セキュリティ専門家を派遣しました。
本事業は一般財団法人海外産業人材育成協会（HIDA）及び独立行政法人日本貿易振興機構（JETRO）が、経済産業省からの委託を受け実施しているものです。
JPCERT/CC の専門家は、11 月 7 日のセッションで、約 50 名の受講生に対して制御システムにおいて発生が想定される典型的なサイバーインシデントと、それらに対する基本的な対策や課題に関する講義・指導を行いました。

4.2.6. 10th U.S.-Japan Critical Infrastructure Protection Forum 参加（2014 年 12 月 4 日-5 日）

JPCERT/CC は、12 月 4 日と 5 日にワシントン D.C.で開催された 10th U.S.-Japan Critical Infrastructure Protection Forum に参加しました。本会議はバンダービルド大学の日米研究協力センターが主催するもので、JPCERT/CC は重要インフラ保護に関する情報を収集し、関係者との関係構築に努めました。また、JPCERT/CC は、同フォーラムで「サイバーグリーン：リスク指標と低減化の取り組みを通したサイバー空間の健全化」というタイトルで講演を行いました。サイバーグリーンプロジェクトについては「4.2.9」をご参照下さい。

また、訪米の機会を捉え、US-CERT/ICS-CERT/NCCIC 等のインシデント対応で協力関係にある組織とも別途個別の打ち合わせを行いました。

4.2.7. OECD セキュリティ専門家会合出席（2014 年 12 月 9 日-12 日）

経済協力開発機構（OECD）のセキュリティ専門家が集まる各種会合において、JPCERT/CC 職員が専門家として OECD Security Guideline のレビューを行い、また、OECD とアジア太平洋地域の CSIRT 間のプロジェクト連携等について協議を行いました。

4.2.8. 台湾 TWCERT/CC の来訪 (2014 年 12 月 3 日)

TWCERT/CC You-Quan Chen 氏 他 4 名が 12 月 3 日に JPCERT/CC の事務所を来訪し、日本と台湾それぞれの国で発生しているインシデントの動向やインフラ防護対策や TWCERT/CC および JPCERT/CC における最新の活動状況に関し、情報交換を行いました。

4.2.9. サイバーグリーンプロジェクト実証実験の開始

JPCERT/CC は、かねてより「サイバーグリーン」と名付けた取組みの計画立案を進めており、この度、JPCERT/CC のホームページで日本国内向けの初めて情報を公開しました。
この取組みでは、まず、健全なインターネット利用を妨げるリスクから定量的に観測可能なものを「リスク環境要因」として列挙します。次に、各リスク環境要因について、世界各国のセキュリティベンダーなどの協力を得てデータを収集します。このデータを、国または経済地域ごと、あるいは時期ごとに整理し、関係者が自由に参照できるようデータベース化して提供します。インターネットの健全性を示す比較可能な指標として共有されたこのデータベースにより各国 CSIRT や ISP などと課題認識の擦り合わせが可能になり、サイバー空間が攻撃や犯罪のインフラストラクチャとして悪用されること防ぐ、インターネットの「クリーンアップ」作戦に連携して取り組む時の基点となります。サイバーグリーン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。

実証実験：サイバーグリーンプロジェクト
https://www.jpcert.or.jp/research/green.html

サイバーグリーンの背景について
https://www.jpcert.or.jp/research/GreenConcept-20141117_ja.pdf

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。

JPCERT/CC attends MNSEC-2014 in Ulaanbaatar(2014 年 10 月 6 日)
http://blog.jpcert.or.jp/2014/10/jpcertcc-attends-mnsec-2014-in-ulaanbaatar.html

Android Secure Coding Seminars in India(2014 年 10 月 16 日)
http://blog.jpcert.or.jp/2014/10/android-secure-coding-seminars-in-india.html

TSUBAME Training and Annual National Conference on Cyber Security in Sri Lanka(2014 年 10 月 30 日)
http://blog.jpcert.or.jp/2014/10/tsubame-training-and-annual-national.html

Malware Analysis Competition in Thailand(2014 年 11 月 19 日)
http://blog.jpcert.or.jp/2014/11/malware-analysis-competition-in-thailand.html

Year in Review – Vulnerability Handling and Changing with the Times：：2014 年 12 月 11 日公開
http://blog.jpcert.or.jp/2014/12/year-in-review---vulnerability-handling-and-changing-with-the-times.html

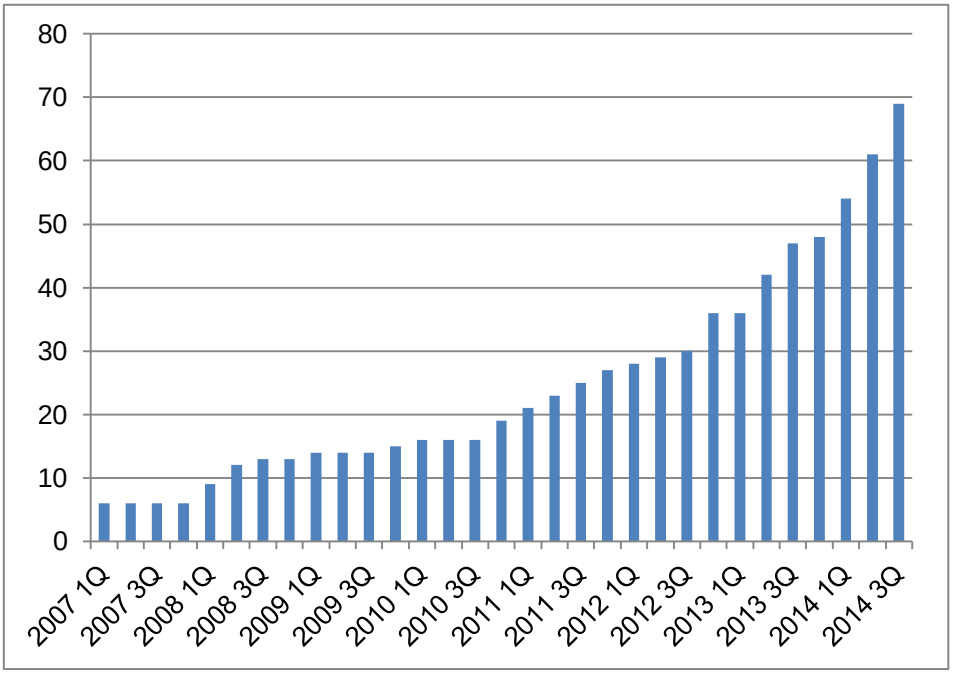
Increase in Possible Scan Activity from NAS Devices：(2014 年 12 月 25 日)
http://blog.jpcert.or.jp/2014/12/increase-in-possible-scan-activity-from-nas-devices.html

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主催の会議およびイベントに参加しています。

本四半期においては、パナソニック株式会社 (Panasonic CSIRT)、プライスウォーターハウスクーパース株式会社、あらた監査法人 (PwC Japan CSIRT)、ニッセイ情報テクノロジー株式会社 (NISSAY IT

CSIRT)、スターティア株式会社 (STARTIA-CSIRT)、MS&AD インシュアランス グループホールディングス株式会社 (MS&AD-CSIRT)、株式会社 DMM.com ラボ (DMM.CSIRT)、ダイハツ工業株式会社 (D-SIRT)、キーウェアサービス株式会社(KEYWARE-CSIRT)の 8 組織が新規に加盟しました。本四半期末時点で 69 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]

12 月に第 9 回シーサート WG を開催しました。

2014 年 12 月 5 日 (金) 16:00-17:45
会場：株式会社 リクルートテクノロジーズ 会場
参加人数：128 名

WG 会において加盟組織の CSIRT 担当者 128 名（加入手続き初期段階までは済んでいるけど運営委員会の加盟承認までは完了していない組織を含む）が、10 チームに分かれて「新しい WG を作るとしたら」をテーマにグループディスカッションを行い、非常に活発な議論がなされました。今四半期末現在シーサート構築推奨 WG など 13 の WG が設置され活動していますが、NCA 加盟組織の増加に伴って関心分野も多様化しており、今後新しい WG が多く設立されることになりそうです。また、NCA の加盟手続きが今後変更され、その説明が行われました。

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(本章において「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。

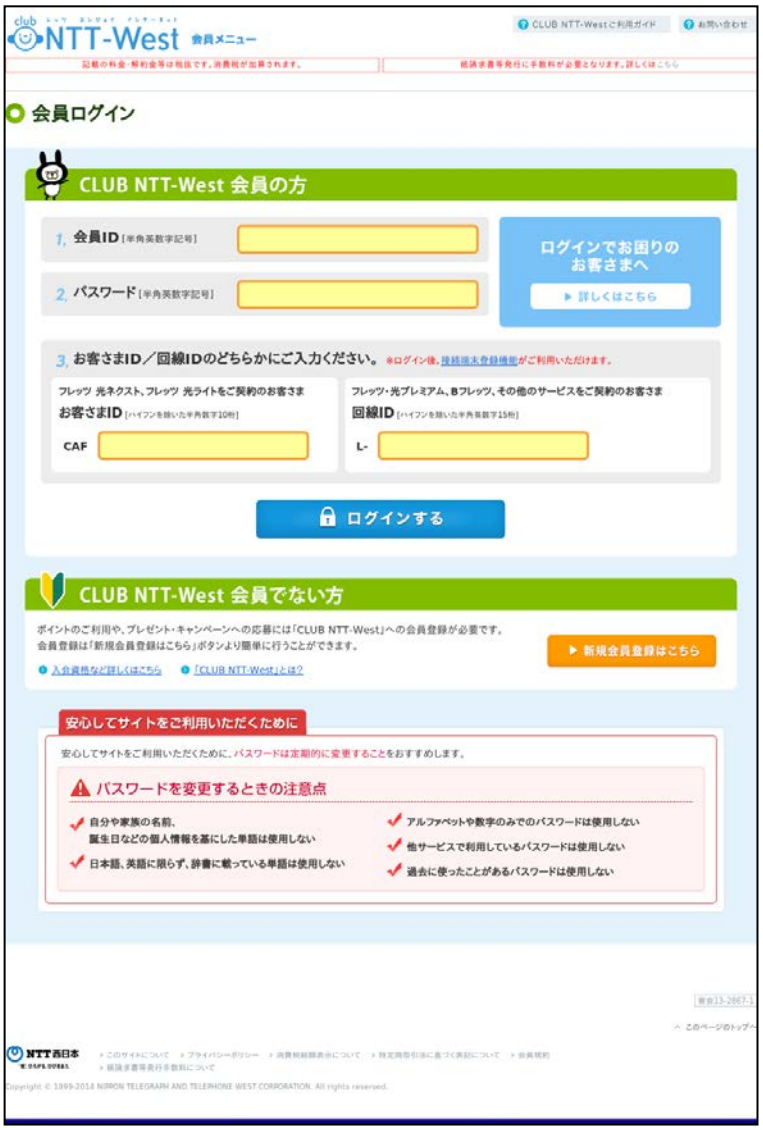
6.1. 情報収集/発信の実績

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。

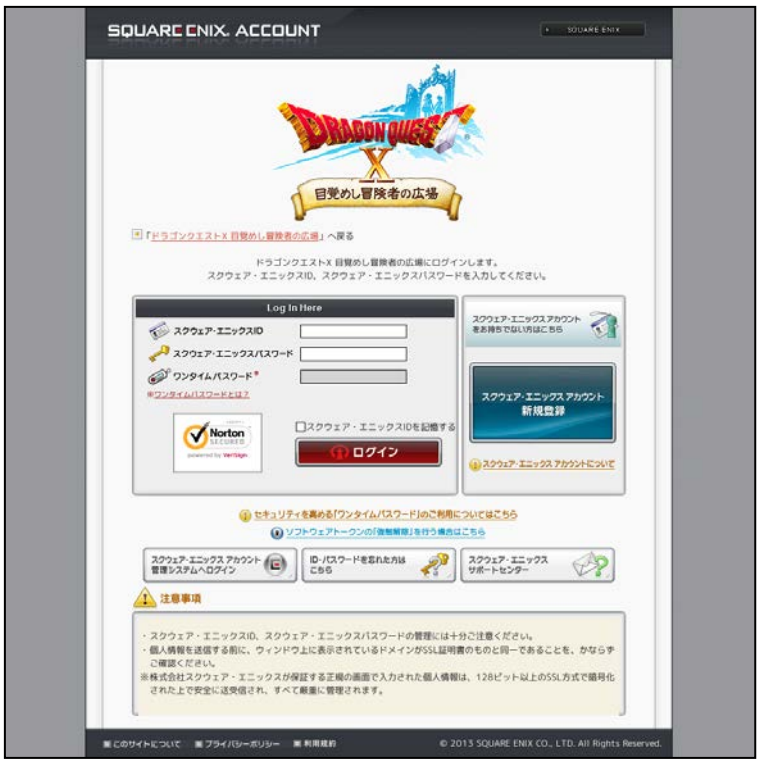
本四半期も、金融機関をかたるフィッシングや通信事業者をかたるフィッシングのサイトが新たに見つかったとの報告を受けました。特にオンラインゲーム事業者をかたるフィッシングについては、数百件の報告を受けました。協議会では、名前をかたられた事業者に、メール本文やサイトの URL 等の関連情報を提供しました。また、金融機関をかたるフィッシングに関しては[図 6-1]の「[2014 年 10 月 21 日更新] 三菱東京 UFJ 銀行をかたるフィッシング」、通信事業者をかたるフィッシングに関しては[図 6-2]の「[2014 年 11 月 11 日新規] Club NTT-West をかたるフィッシング」を、オンラインゲーム事業者をかたるフィッシングに関しては[図 6-3]の「[2014 年 10 月 28 日更新] スクウェア・エニックス（ドラゴンクエスト X）をかたるフィッシング」を、緊急情報として協議会の Web 上で公開し、広く注意を喚起しました。

[図 6-1 [更新] 三菱東京 UFJ 銀行をかたるフィッシング(2014/09/19)
https://www.antiphishing.jp/news/alert/ufj20140919.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 Club NTT-West をかたるフィッシング（2014/11/11）
https://www.antiphishing.jp/news/alert/clubnttwest20141111.html]



[図 6-3 [更新] スクウェア・エニックス (ドラゴンクエスト X)をかたるフィッシング (2014/06/11)
https://www.antiphishing.jp/news/alert/square_enix20140611.html]

6.2. 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。

山本健太郎「最新のフィッシング動向と対策について」フィッシング対策セミナー 2014 2014 年 12 月 16 日

6.3. 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 URL 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 2014 年 10 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201410.html
フィッシング対策協議会 2014 年 11 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201411.html
フィッシング対策協議会 2014 年 12 月 フィッシング報告状況

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. フィッシング対策セミナー2014 の開催

フィッシング対策協議会では、「フィッシング対策ガイドライン」を協議会の Web サイトで公開しています。本四半期には、「フィッシング対策ガイドライン」を詳しく解説する場として、「フィッシング対策セミナー 2014」を次のような要領で開催し、楽天株式会社より「楽天市場における詐欺対策」、警察庁より「インターネットバンキングに係る不正送金事犯の現状と対策」、フィッシング対策協議会より「最新のフィッシング動向と対策について」、APWG から「Global Internet Threats and APWG Initiatives to fight Cyber-Crime and Fraud」（逐次通訳）の講演をしていただきました。

フィッシング対策セミナー 2014
開催日程：2014 年 12 月 16 日（火）13:00-18:00
会場：コクヨホール
参加人数：219 名

7.2. 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 19 回運営委員会
日時：2014 年 10 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 20 回運営委員会
日時：2014 年 11 月 14 日 16:00 - 18:00
場所：NTT コミュニケーションズ株式会社

フィッシング対策協議会 第 21 回運営委員会
日時：2014 年 12 月 12 日 16:00 - 18:00
場所：トレンドマイクロ株式会社

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. IPv6 セキュリティテスト手順書および検証済み製品リスト(2014/12/16)

「IPv6 セキュリティテスト手順書」に従って IPv6 対応機器ベンダが検証した結果をリスト化した「IPv6 セキュリティテスト検証済み製品リスト(2014/08/01)」を公開しました。これは、IPv6 対応機器の購入を検討されている企業や組織のシステム担当者の方に、機器選定時の参考資料としてご利用いただくことを目的としています。12 月 16 日公開版の検証済み製品リストには、製品開発ベンダ 1 社と 4 製品の検証結果を追加しました。

IPv6 セキュリティテスト検証済み製品リスト
(2014 年 12 月 16 日公開)
https://www.jpcert.or.jp/research/ipv6product_list.html

8.2. 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（現行版は平成 26 年経済産業省告示 第 110 号）に基づき、2004 年 7 月から受付機関(IPA)や調整機関(JPCERT/CC)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、2014 年 7 月 1 日から 2014 年 9 月 30 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[2014 年第 3 四半期(7 月～9 月)]
(2014 年 10 月 22 日)
https://www.jpcert.or.jp/press/2014/vulnREPORT_2014q3.pdf

8.3. 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し、宛先ポート番号や送信元地域ごとに分類して分析するインターネット定点観測を継続的に実施しています。これを、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 2014 年 7 月～9 月
(2014 年 10 月 28 日)
https://www.jpcert.or.jp/tsubame/report/report201407-09.html

9. 主な講演活動一覧

(1) 満永 拓邦(早期警戒グループ 情報分析ライン リーダー)：
パネルディスカッション
SecurityDay2014,2014 年 12 月 17 日

(2) 真鍋 敬士(理事・分析センター長)：
「攻撃の傾向にみるサイバー脅威への対応と対策」
標的型サイバー攻撃リスクマネジメントセミナー2014,2014 年 12 月 12 日

(3) 真鍋 敬士(理事・分析センター長)：
「サイバーセキュリティの脅威動向と取り組み」
TCG 日本支部 第 6 回公開ワークショップ,2014 年 12 月 3 日

(4) 久保正樹(情報流通対策グループ 脆弱性解析チーム リーダー)：
「Lessons (to be) Learned from Handling OpenSSL Vulnerabilities」
オープンソースカンファレンス 2014 福岡, 2014 年 11 月 22 日

(5) 満永 拓邦(早期警戒グループ 情報分析ライン リーダー)：
「2014 年セキュリティ動向」
Internet Week2014, 2014 年 11 月 21 日

(6) 石川 貴博(インシデントレスポンスグループ 情報セキュリティアナリスト)：
「インシデント対応入門」
Internet Week2014, 2014 年 11 月 20 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)：
「DNS セキュリティイシューへの対応『セキュリティコーディネータの視点』」
Internet Week2014, 2014 年 11 月 20 日

(8) 満永 拓邦(早期警戒グループ 情報分析ライン リーダー)：
「情報セキュリティ対策」
日本新聞協会 第６１回新聞製作講座(上流専門講座),2014 年 11 月 20 日

(9) 椎木 孝斉(分析センター　マネージャ)：
「日本における最近の標的型攻撃とは～インシデント対応・調整活動から見えてきた傾向と対策～」
Internet Week2014,2014 年 11 月 19 日

(10) 小宮山 功一朗(エンタープライズグループマネージャ兼国際部シニアアナリスト)：
「試されるサイバー空間における国際連携」
明治大学 国際総合研究所 情報ネットワークの脆弱性問題研究会 情報ネットワークの強さと弱さ－大規模自然災害からサイバー空間まで」シンポジウム,2014 年 11 月 12 日

(11) 小林 裕士(インシデントレスポンスグループ 情報セキュリティアナリスト)：
「攻撃者にならないための対策－DDoS について知る－」
OISEC,2014 年 11 月 12 日

(12) 戸田洋三(情報流通対策グループ 脆弱性解析チーム リードアナリスト)：
「～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』」
関西オープンフォーラム 2014, 2014 年 11 月 8 日

(13) 宮地 利雄 (経営企画室 技術顧問)

「ICS and Cyber Incidents」

海外産業人材育成協会 The Seminar on Enhancing Information Security(バンコク), 2014 年 11 月 7 日

(14) 村上 晃(経営企画室 兼 エンタープライズサポートグループ部門長):

「IT 変革時代に 企業が考えるべきセキュリティー対策～変化するサイバー攻撃への対応～」

中国地方 IBM ユーザ研究会,2014 年 10 月 24 日

(15) 久保正樹(情報流通対策グループ 脆弱性解析チーム リーダー):

「ICS の脆弱性調査およびその対策としての CERT C コーディングルール」

digital bond Sx4 Japan, 2014 年 10 月 15 日

10. 主な執筆一覧

(1) 早貸 淳子(専務理事)、小宮山 功一朗(エンタープライズグループマネージャ兼国際部シニアアナリスト):

「サイバーセキュリティの国際連携と信頼醸成措置」

角川インターネット講座シリーズ 13 巻「仮想戦争の終わり―サイバー戦争とセキュリティ―」 2014 年 12 月 25 日

11. 開催セミナー等一覧

(1) SecurityDay 2014

複雑化するインターネットインシデントの脅威に対抗するには、すべてのインターネット利用者がセキュリティ向上に取り組むことが不可欠です。その一助となるべく、インターネット利用者及び情報システムの運用・管理者を対象に、専門家とともにインターネット利用におけるセキュリティ上の問題点を議論し、解決策を考えるセミナーを開催しました。

・主 催：SecurityDay運営委員会
- 日本インターネットプロバイダー協会(JAIPA)
- 日本データ通信協会(Telecom-ISAC Japan)
- 日本ネットワークセキュリティ協会(JNSA)
- JPCERT/CC

・開催日時：2013年12月9日 10:00～16:30

・参加人数：84名

詳細については、次のWebページ をご参照ください。

SecurityDay2014

http://www.securityday.jp/home

12. 協力、後援一覧

本四半期においてJPCERT/CCは次の行事の開催に協力または後援をしました。

(1) CODE BLUE
主　催：CODE BLUE実行委員会
開催日：2014年12月18日(木)~19日(金)

(2) 第11回デジタル・フォレンジック・コミュニティ2014 in TOKYO
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
開催日：2014年12月8日(月)~12月9日(火)

(3) TCG日本支部第6回公開ワークショップ
主　催：TCG日本支部
開催日：2014年12月3日

(4) 「情報ネットワークの強さと弱さ　　大規模自然災害からサイバー空間まで」シンポジウム
主　催：明治大学　国際総合研究所　情報ネットワークの脆弱性問題研究会
開催日：2014年11月12日

(5) CSMS適合性評価制度に関する説明会
主　催：一般財団法人日本情報経済社会推進協会
開催日：2014年11月28日(金)

(6) Internet Week2014
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：2014年11月18日(火)~11月21日(金)

(7) 第4回日韓情報セキュリティシンポジウム
主　催：特定非営利活動法人　日本ネットワークセキュリティ協会
開催日：2014年11月7日(金)

(8) 第11回迷惑メール対策カンファレンス
主　催：一般財団法人インターネット協会
開催日：2014年10月8日(水)~10月9日(木)

(9) Email Security Conference 2014
主　催：株式会社ナノオプト・メディア
開催日：2014年10月3日(金)東京、10月17日(金)大阪

(10) 第10回 IPA 「広げよう情報モラル・セキュリティコンクール」2014
主　催：独立行政法人情報処理推進機構
開催日：2014年4月1日(火) ~11月

■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