JPCERT/CC®

JPCERT-PR-2014-01
発行日：2014-01-16

JPCERT/CC 活動概要 [2013 年 10 月 1 日 ～ 2013 年 12 月 31 日]

活動概要トピックス

—トピック 1— HTML5 を利用した Web アプリケーションのセキュリティ問題に関する調査報告書の公開

HTML5 は、WHATWG 及び W3C が HTML4 に代わる次世代の HTML として策定を進めている仕様です。HTML5 の採用により、Web 利用者の利便性が向上しますが、その一方で、例えば、従来の HTML4 を想定して作られた Web サイトがブラウザの HTML5 対応により脆弱となるケースや、HTML5 で追加された機能の誤った使用により脆弱性を作り込んでしまうケースが複数存在することが調査の結果分かりました。このような HTML5 及びその周辺技術を使用する上で懸念されるセキュリティ問題を抽出し、それらの問題について調査を行った結果を「HTML5 を利用した Web アプリケーションのセキュリティ問題に関する調査報告書」にまとめ、10 月 30 日に公開しました。

HTML5 を利用した Web アプリケーションのセキュリティ問題に関する調査報告書
https://www.jpcert.or.jp/research/html5.html

—トピック 2— 海外 National CSIRT 構築支援活動(ラオス及びアフリカ諸国)

10 月 1 日から 3 日の計 3 日間、JPCERT/CC は、タイの National CSIRT である ThaiCERT と協力して、ラオスの National CSIRT である LaoCERT に対し、同組織の機能強化を目的として、インシデントハンドリングの手法についての講義やネットワークフォレンジックのハンズオン演習を行いました。

また、11 月には、コートジボワールで開催された国際会議 AFRINIC-19 に参加するとともに、FIRST の講師による CSIRT 研修(11 月 24 日､25 日)について､FIRST の Steering Committee メンバの一員として、講師の手配・調整、現地での研修サポートを行いました。続く 11 月 26 日には、JPCERT/CC が主任講師として CSIRT 技術者向けにネットワークフォレンジックのハンズオン演習をグループワークで行う、アフリカ諸国向けの CSIRT トレーニングを実施しました。このトレーニングは 2010 年春から実施しており、今回で 7 回目の開催となります。今回はコートジボワールやその近隣のトーゴ、カメルーン等から合計 40 名以上が参加しました。

さらに、11 月 27 日の AfricaCERT Workshop では、AfricaCERT という地域 CSIRT の現状と今後の活動計画について事務局から説明が行われ、Workshop 参加各国からカントリーアップデートがありました。JPCERT/CC は AfricaCERT の年次活動報告書作成の提案を行い、パネルディスカッションに参加しました。

制度や技術がまだ成長段階にある国・地域などが関与するインシデントは、対処が後手になりがちで、日本のインターネットユーザにとっても脅威の一つとなっています。今後急速なインターネット普及が予想されているアフリカ地域に起因するインシデントが併せて増えることが予想され、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。

AFRINIC 及び AFRINIC-19 公式ページ
http://meeting.afrinic.net/afrinic-19/en/

―トピック 3―　APCERT を代表して、Seoul Cyber 2013 において講演

JPCERT/CC は、APCERT を代表して、Seoul Cyber 2013(以下「ソウルサイバー会議」といいます。)において講演を行いました。ソウルサイバー会議は、2011 年のロンドンサイバー会議、2012 年のブダペスト(ハンガリー)サイバー会議に続く国際協議の場であり、10 月 17、18 日に韓国ソウルで開催されました。合計 79 カ国以上から、政府関係者を中心に、国際機関、企業、学術機関等に属する関係者 1,600 名以上が参加しました。JPCERT/CC の講演では、APCERT の活動を紹介し、その活動がグローバルなサイバー空間での信頼醸成のプロセスに寄与するものであることを説明しました。またサイバー空間のセキュリティに関する諸問題について、国際的に比較可能な指標の必要性を訴え、それに向けた活動について各関係者の協力を求めました。

ソウルサイバー会議 公式ページ
http://www.seoulcyber2013.kr/en/

本活動は、経済産業省より委託を受け、「平成２５年度情報セキュリティ対策推進事業」として実施したものです。
ただし、「9.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、「2.5.セキュアコーディング啓発活動」、「6.国際連携活動関連」、「11.講演活動一覧」、「12. 開催セミナー等一覧」及び「13.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 4812 件、インシデント件数ベースでは 4788 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 2135 件でした。前四半期の 2414 件と比較して 12%減少しています。「調整」とは、フィッシングサイトが設置されているサイトや、改ざんにより JavaScript が埋め込まれているサイト、ウイルス等のマルウエアが設置されたサイト、「scan」のアクセス元等の管理者等に対し、状況の調査や問題解決のための対応を依頼する活動です。

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

インシデント報告対応活動の詳細については、別紙「JPCERT/CC インシデント報告対応レポート」をご参照ください。

JPCERT/CC インシデント報告対応レポート
https://www.jpcert.or.jp/pr/2014/IR_Report20140116.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 601 件で、前四半期の 469 件から 28%増加しました。また、前年度同期(360 件)との比較では、67%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	合計 (割合)
国内ブランド	34	99	120	253(42%)
国外ブランド	78	74	52	204(34%)
ブランド不明(注 5)	48	47	49	144(24%)
月別合計	160	220	221	601(100%)

(注 2)「ブランド不明」は、報告されたフィッシングサイトが停止していた等の理由により、JPCERT/CC がブランドを確認することができなかったサイトの件数を示します。

前四半期に引き続き、国内通信事業者が動的に割り当てる IP アドレスを持ち、国内及び海外のゲーム会社のオンラインサービスを装ったフィッシングサイトの報告を多数受領しました。11 月に入ってからは、このようなフィッシングサイトに誘導するためのページが設置された海外の Web サイトを多数確認しました。誘導元となるサイトは特定の CMS を使用している傾向が見られることから、CMS の脆弱性を悪用され、誘導するためのページを不正に設置された可能性があると考えられます。11 月半ばには、ゲーム会社を装ったフィッシングサイトが稼働しているサーバ上で、国内金融機関を装ったフィッシングサイトが同時に稼働していることを確認しており、それ以降は国内金融機関を装ったフィッシングサイトが増加しています。

また、国内通信事業者の Web メールサービスや、国内大学等で導入されている Web メール製品を装ったフィッシングサイトの報告を複数受領しており、これらについては海外の特定の無料ホスティングサービスを使用している傾向が見られました。

フィッシングサイトの調整先の割合は、国内が 43%、国外が 57%であり、前四半期(国内 56%、国外 44%)と比較して、国外への調整の割合が増えました。

本四半期に報告が寄せられた Web サイト改ざんの件数は、1604 件でした。前四半期の 2774 件から 42%減少しています。

不正な iframe や JavaScript がページに挿入された Web サイトに関する報告が、依然として多く寄せられています。改ざんによって挿入されるコードには前四半期から大きな変化は見られませんが、改ざんされたサイトを閲覧することでマルウエアに感染し、PC に保存されている認証に使用する情報等が窃取される可能性があります。サイトの管理に使用する PC がマルウエアに感染し、ftp のパスワードが盗まれた結果、不正な ftp 認証によって Web サイトの改ざんが行われるという循環が多くなっている可能性があります。マルウエアに感染することを防ぐためには、まずは、OS やアプリケーションのアップデートや、ウイルス対策ソフトの定義ファイルを最新の状態にする等の最低限の基本的な対策が重要となります。

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及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 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：8 件　https://www.jpcert.or.jp/at/

2013-10-09　2013 年 10 月 Microsoft セキュリティ情報 (緊急 4 件含) に関する注意喚起
2013-10-09　Adobe Reader 及び Acrobat の脆弱性 (APSB13-25) に関する注意喚起
2013-10-16　2013 年 10 月 Oracle Java SE のクリティカルパッチアップデート (定例) に関する注意喚起
2013-11-06　2013 年 11 月 Microsoft Graphics Component の未修正の脆弱性に関する注意喚起
2013-11-13　2013 年 11 月 Microsoft セキュリティ情報 (緊急 3 件含) に関する注意喚起
2013-11-13　Adobe Flash Player の脆弱性 (APSB13-26) に関する注意喚起
2013-12-11　2013 年 12 月 Microsoft セキュリティ情報 (緊急 5 件含) に関する注意喚起
2013-12-11　Adobe Flash Player の脆弱性 (APSB13-28) 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)に発行しています。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.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 31 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。

2013-10-02　Microsoft Message Analyzer 正式リリース
2013-10-09　10 月は情報セキュリティ月間
2013-10-17　Internet Explorer 11 Blocker Toolkit
2013-10-23　OWASP Top 10 2013
2013-10-30　Internet Week 2013 のセキュリティセッション紹介記事
2013-11-07　オープンリゾルバ確認サイト公開のお知らせ
2013-11-13　マイクロソフト セキュリティ インテリジェンス レポート 第 15 版
2013-11-20　EMET 4.1 リリース
2013-11-27　HTML5 を利用した Web アプリケーションのセキュリティ問題に関する調査報告書公開
2013-12-04　サーバアプリケーションのアップデート確認
2013-12-11　年末年始、フィッシング詐欺に注意
2013-12-18　ICANN Study on Whois Misuse コメント募集中
2013-12-26　担当者が選ぶ 2013 年重大ニュース

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、サービス及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。

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。

【マイクロソフト社製品の未修正の脆弱性を使用した標的型攻撃】

2013 年 11 月、マイクロソフト社製品の 2 件の未修正の脆弱性を悪用した攻撃が発生しました。攻撃に使用された脆弱性は、遠隔の第三者がユーザの PC 上で任意のコードを実行させる可能性がある非常に危険度の高いものであり、それぞれ標的型攻撃に使用されていました。また、マイクロソフト社によるセキュリティアドバイザリの公開時点では、Windows Update で最新のパッチを適用している場合にも影響を受ける深刻なものでした。同種の攻撃が継続して発生する場合、国内の広い範囲で深刻な被害が出る可能性がありました。

JPCERT/CC は、国内の組織から標的型攻撃メール及びメールに添付されたマルウエア検体の提供を受け、詳細な分析を行いました。導き出したマルウエアの通信先等の分析結果は、国内重要インフラ事業者等に提供し、過去のログ情報等の分析による攻撃検知に利用していただきました。一般企業等に対しては、これらの脆弱性についての対策または回避策を注意喚起「2013 年 11 月 Microsoft セキュリティ情報 (緊急 3 件含) に関する注意喚起」、「2013 年 11 月 Microsoft Graphics Component の未修正の脆弱性に関する注意喚起」として公開し、広く注意を呼びかけました。

1 件目の脆弱性は、Internet Explorer で使用される ActiveX コントロールに関するもので、海外のセキュリティベンダによると、この時点で発生した攻撃には米国にある Web サイトが使用されており、いわゆる水飲み場攻撃であったとのことです。2 件目の脆弱性は、Microsoft Graphics Component に関するもので、2013 年 11 月にマイクロソフト社より、Windows XP にインストールされた Microsoft Office 2007 を介して脆弱性を使用する標的型攻撃が中東や南アジアで行われていることが公開されました。その後、IPA(独立行政法人情報処理推進機構)の情報*1)により、本脆弱性が、国内の民間企業に対する標的型メール攻撃にも悪用されていたことが判明しました。

マイクロソフト セキュリティ情報 MS13-090 - 緊急
ActiveX の Kill Bit の累積的なセキュリティ更新プログラム (2900986)
https://technet.microsoft.com/ja-jp/security/bulletin/ms13-090

マイクロソフト セキュリティ アドバイザリ (2896666)
Microsoft Graphics コンポーネントの脆弱性により、リモートでコードが実行される
https://technet.microsoft.com/ja-jp/security/advisory/2896666

*1) IPA(独立行政法人情報処理推進機構)
Microsoft Office 等の脆弱性(CVE-2013-3906)を悪用する国内の組織に対する標的型攻撃を確認
～不審メールへの警戒、緊急対策の実施を～
https://www.ipa.go.jp/security/topics/alert20131120.html

1.2.3. 調査

1.2.3.1. HTML5 を利用した Web アプリケーションのセキュリティ問題に関する調査報告書の公開

2013 年 10 月 30 日、JPCERT/CC は「HTML5 を利用した Web アプリケーションのセキュリティ問題に関する調査報告書」を公開しました。

HTML5 は、WHATWG 及び W3C が HTML4 に代わる次世代の HTML として策定を進めている仕様です。HTML5 及びその周辺技術を利用すると、Web サイト閲覧者のブラウザ内でのデータ格納や、クライアントとサーバ間での双方向通信、位置情報の取得等が可能になります。それにより、従来の HTML4 よりも柔軟かつ利便性の高い Web サイトを構築することができます。HTML5 の採用により、Web 利用者の利便性が向上しますが、こうした新技術が攻撃者によって悪用された場合の影響について十分な検証や周知がなされていないことが危惧されていました。そこで JPCERT/CC は、HTML5 及びその周辺技術を使用する上で懸念されるセキュリティ問題を抽出し、それらの問題について調査を行いました。

この調査の結果、従来の HTML4 を想定して作られた Web サイトが、ブラウザの HTML5 対応により脆弱となるケースや、HTML5 で追加された機能の誤った使用により脆弱性を作り込んでしまうケースが複数存在することが分かりました。

JPCERT/CC では、HTML5 を利用したセキュアな Web アプリケーション開発のための情報提供が急務になっていると考え、本調査結果の公開、及び調査結果を元にした啓発活動を行っています。

HTML5 を利用した Web アプリケーションのセキュリティ問題に関する調査報告書
https://www.jpcert.or.jp/research/html5.html

1.2.4. IPv6 プロトコルのセキュリティテスト実施への取組

ネットワーク機器、インターネット接続サービスのメニューにおいて IPv6 対応が急速に広がっており、IPv6 を利用できる環境が普通のものになりつつあります。セキュリティを含めたネットワーク管理の立場から IPv6 を見ると、IPv4 とは異なる考え方で対応する必要のある機能が含まれています。

こうした状況に鑑み、JPCERT/CC では、ネットワーク機器に IPv6 対応の機能を実装する場合や、それらの機器を利用する上での注意事項を調査し、整理しました。IPv6 対応機器ベンダの皆さまを対象に、調査結果を解説するセミナー形式での説明会を実施し、さらにこれらの注意事項に関する問題に自社製品が対応できているかどうか、公開ツール等を利用して簡便に検証する方法も紹介しました。

また、調査の一環として、上述の注意事項の中から主にルータや L3 スイッチにおいて対応が必要なセキュリティ上の問題を対象に絞り込み、これらの注意事項に関わる問題に対応できているかについてのテスト(IPv6 セキュリティテスト)を対応機器ベンダの皆さまのご協力の下に実施しています。

本テスト結果は、主にシステム管理者が今後購入する IPv6 対応機器を選定する際の材料等として活用できることを目的に、今冬公開予定です。

1.3. インターネット定点観測

JPCERT/CC は、ポートスキャンの受信情報をインターネット上に設置した複数のセンサーから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。ポートスキャンがネットワーク経由の攻撃の準備活動としてなされることを踏まえて、既に公開されている脆弱性情報や攻撃ツール、攻撃コードを悪用した攻撃活動の動向と、新たな脆弱性情報の公開をきっかけとした攻撃活動の活発化等の状況を把握することに努めています。

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

JPCERT/CC は TSUBAME の構築と、さまざまな地域に広く観測用のセンサーを設置するためのプロジェクト(TSUBAME プロジェクト)の事務局を担当しており、システムやセンサーの定常稼働に努めています。2013 年第 3 四半期現在、観測用のセンサーをアジア・太平洋地域の 23 地域に設置しています。今後も設置地域を拡大し、より充実したセンサー網を構築す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 URL をご参照ください。

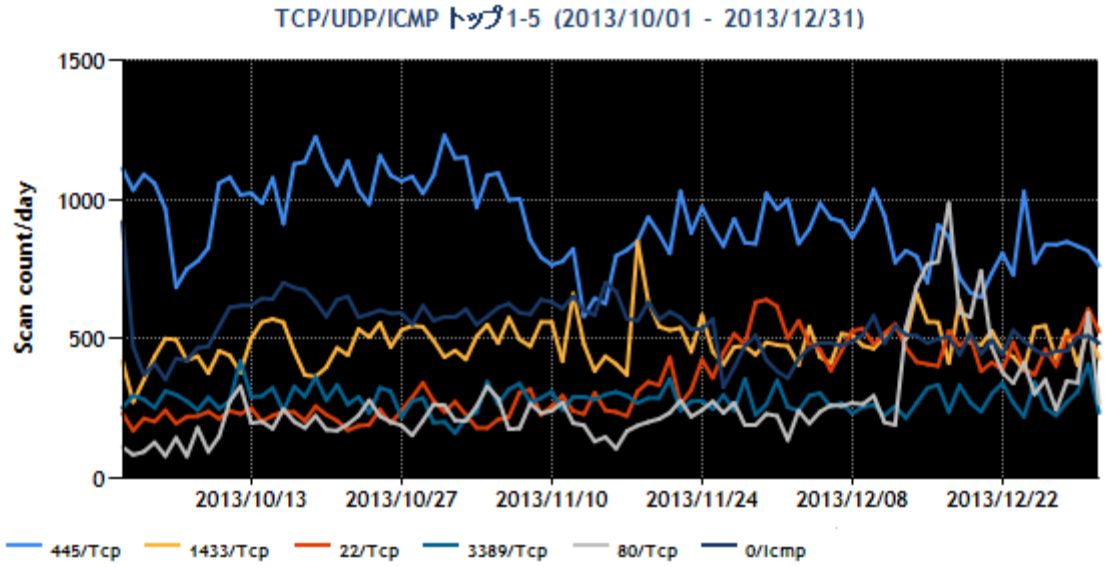
TSUBAME(インターネット定点観測システム)
https://www.jpcert.or.jp/tsubame/index.html

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。

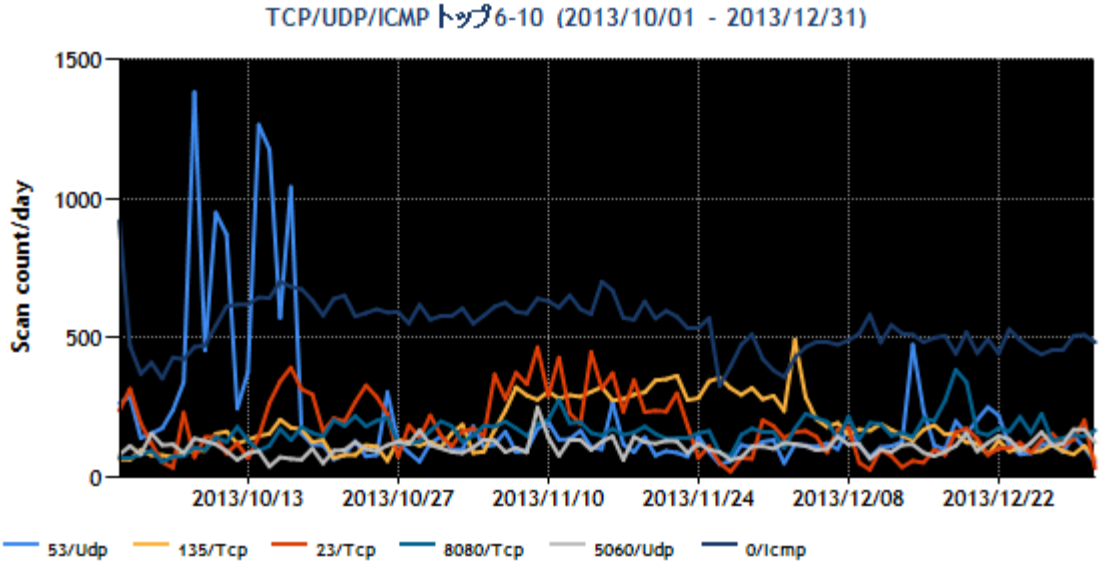
また、主に企業のシステム管理者等の方々に、自ネットワークに届いた意図しないパケットと比較してもらうことを目的とし、日本国内のセンサーで受信したパケットを宛先ポート別に集計してグラフ化し、毎週月曜日に JPCERT/CC の Web ページで公開しています。

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

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 位及び 6 位～10 位を、[図 1-1]と[図 1-2]に示します。

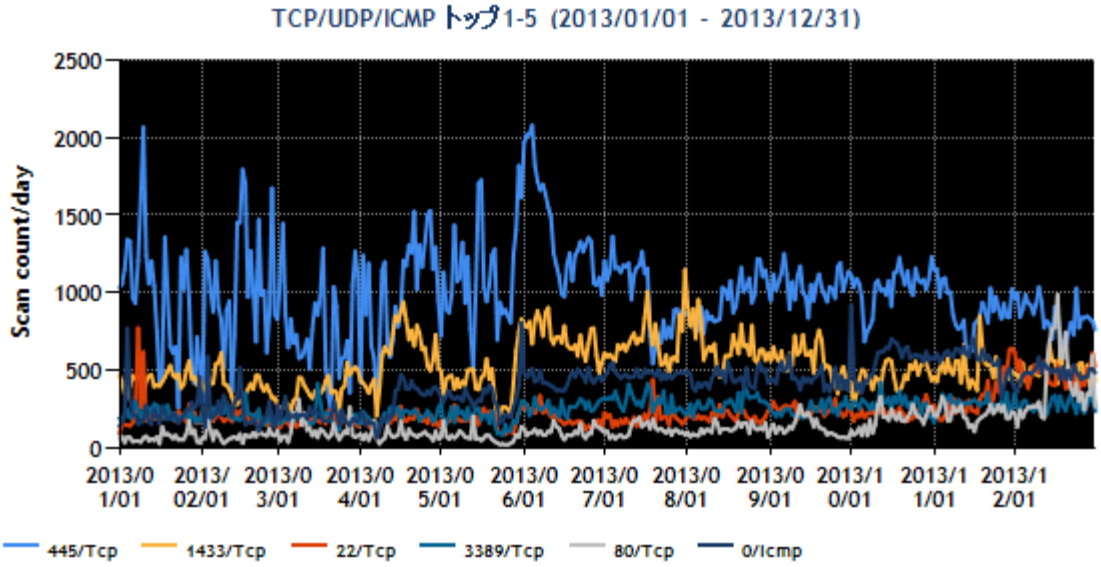


[図 1-1 宛先ポート別グラフ トップ 1-5(2013 年 10 月 1 日-12 月 31 日)]

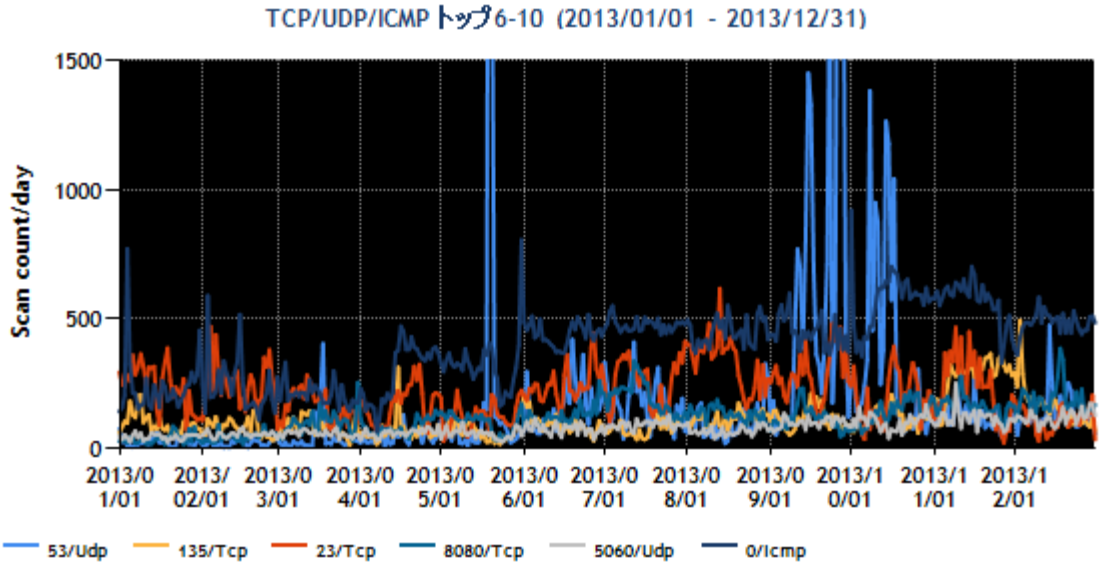


[図 1-2 宛先ポート別グラフ トップ 6-10(2013 年 10 月 1 日-12 月 31 日)]

また、過去 1 年間(2013 年 1 月 1 日～2013 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 位及び 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 (2013 年 1 月 1 日-2013 年 12 月 31 日)]



[図 1-4 宛先ポート別グラフ トップ 6-10 (2013 年 1 月 1 日-2013 年 12 月 31 日)]

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や、Telnet、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へのスキャン活動と見られるパケットが、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、日々観測情報の分析を行っており、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。

日本国内の組織に割り当てられた IP アドレスから送信された、SSH サーバ宛ての特徴的なパケットが本四半期も観測されました。JPCERT/CC は、当該 IP アドレスの管理者に情報を提供し、SSH サーバを探索するスキャンや辞書攻撃等を行う不審なツールの調査を依頼しました。その後、当該管理者から「当該サーバには何者かによる侵入の痕跡があり、サーバ上に SSH サーバを探索するためのツールや操作ツールが設置されて遠隔から操作可能な状態になっており、命令を受けてスキャンを行っていたことを確認したため、必要な対応を行った」との連絡をいただきました。

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。

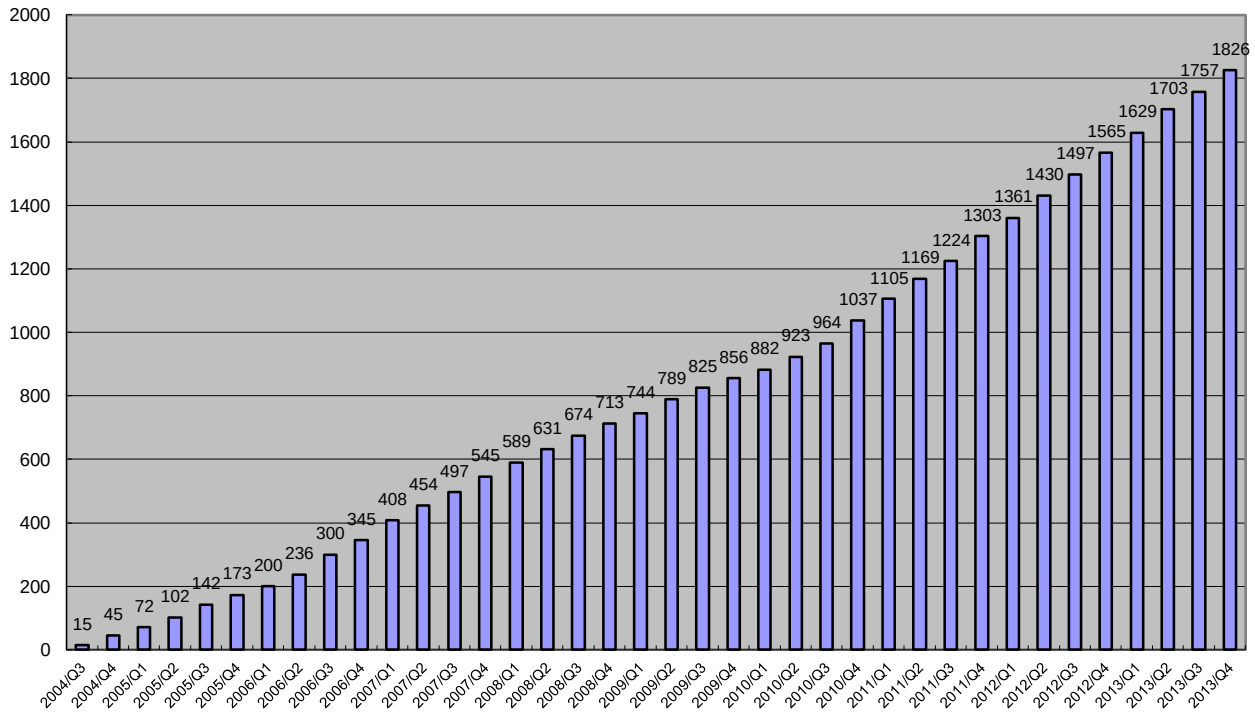
2.1. Japan Vulnerability Notes(JVN)において公表した脆弱性情報及び対応状況

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」(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」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 CERT-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、これには特別に、原典の識別子と対応した「JVNTA」に続く 2 桁数字－3 桁数字の形式の識別子(例えば、JVNTA12-345)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 69 件(累計 1829 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 URL 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]

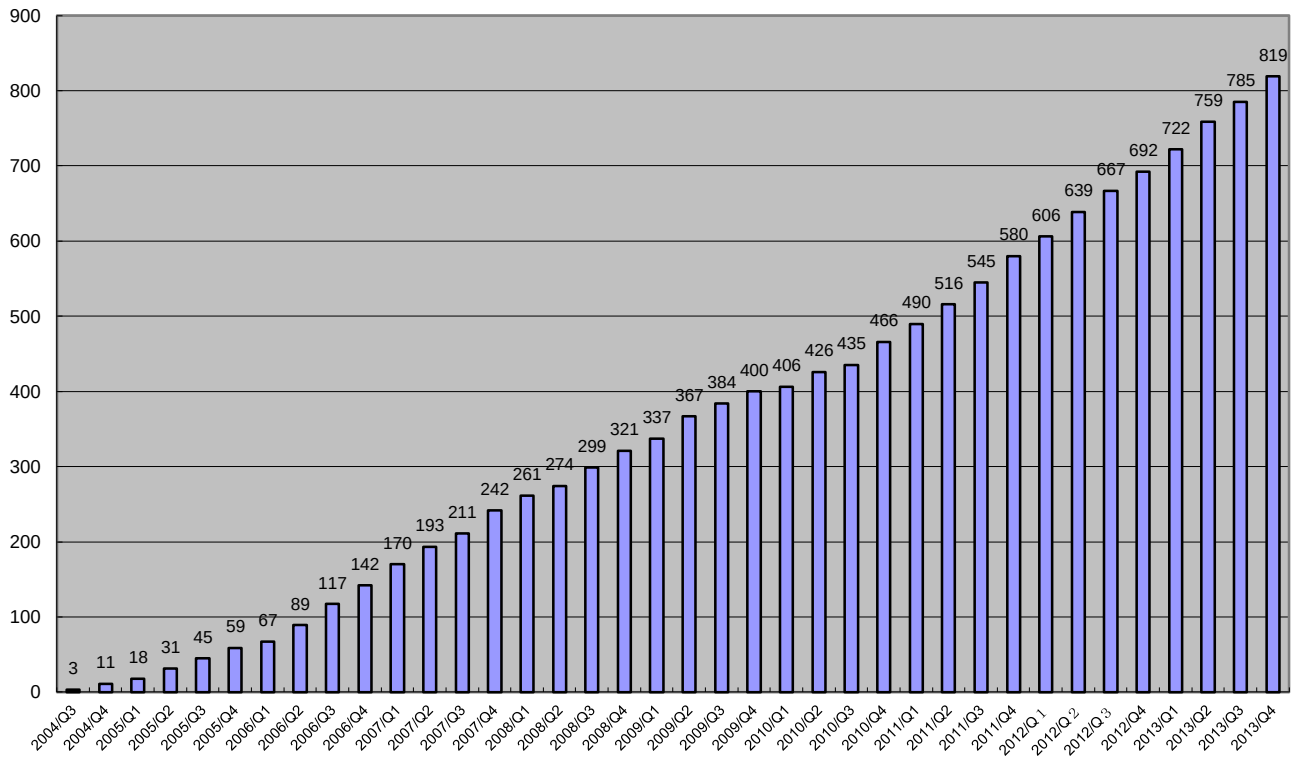
本四半期において公表に至った脆弱性情報のうち、国内取扱脆弱性情報は 34 件(累計 819 件)で、累計の推移は[図 2-2]に示すとおりです。

本四半期においては、自社製品に関する脆弱性情報の届出が 15 件と、全届出の半数に及んだことが特徴的でした。15 件の自社製品届出のうち 2 件は、調査の結果、その届出を行った製品開発者の製品のみならず、国内外の多くの製品開発者の製品に影響を及ぼす可能性がある脆弱性情報であると判明したため、JPCERT/CC は国内外の複数の製品開発者へ脆弱性情報を通知し、公表に至るまでの調整を行いました。

本年度に入り、自社製品届出は増加傾向にあります。これは、発見された脆弱性に関する情報を周知し、ユーザに対策を促す製品開発者の前向きな姿勢が広がった一端と捉えることができます。脆弱性情報を周知する手段として JVN の一層の活用が期待されます。

19 件の通常届出のうち、公表数が多かったものは、組込み系(ルータやハードディスク等)が 5 件、オープンソースソフトウエア(OSS)製品が 4 件(海外開発者 2 件、国内開発者 2 件)、E コマース製品が 2 件、コンテンツ管理システム(CMS)が 2 件でした。

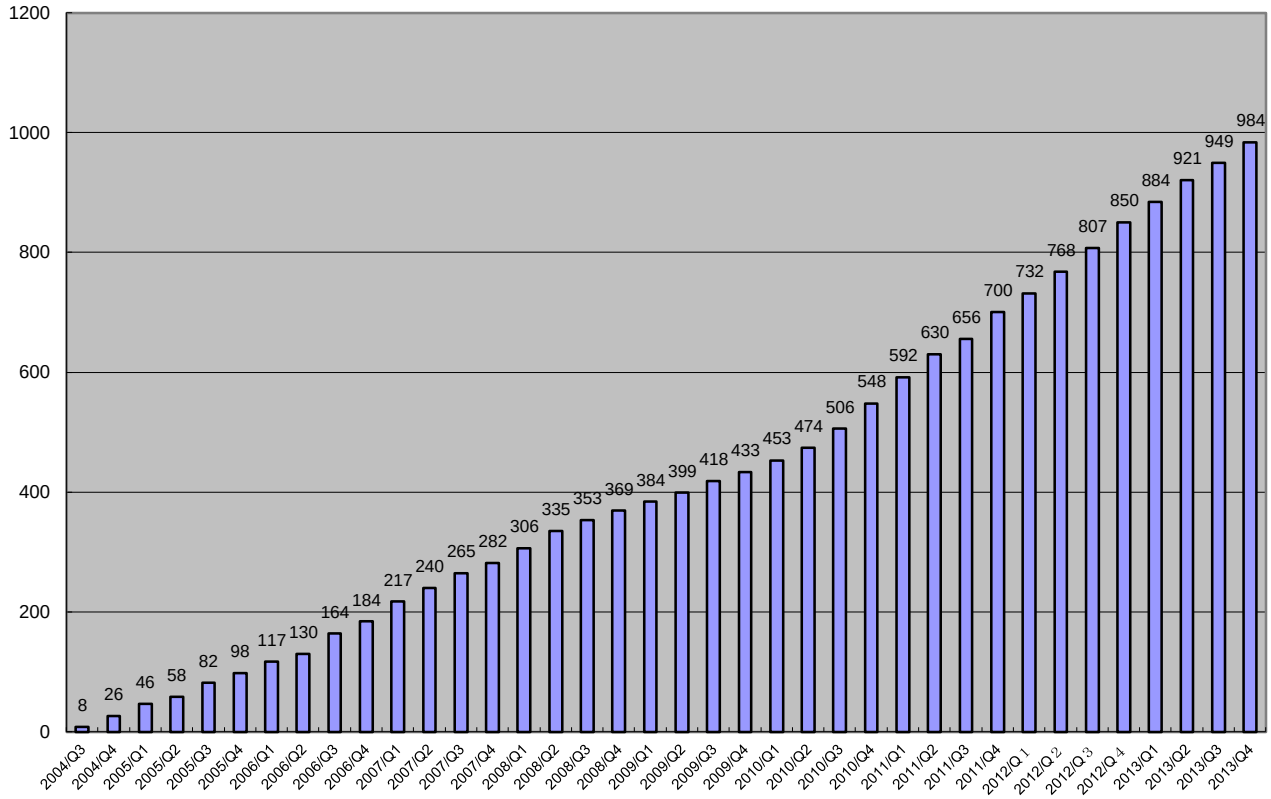
JPCERT/CC は、今後も引き続き国内外の関係者との調整を行い、脆弱性問題への速やかな対応の促進に努めてまいります。



[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 35 件(累計 984 件)で、累計の推移は[図 2-3]に示すとおりです。35 件のうち 2 件を占める US-CERT の脆弱性注意喚起(JVNTA から始まる識別子を付して公表したもの)は、Microsoft 製品に関する月例パッチの注意喚起でした。

また、US-CERT の脆弱性注意喚起以外の 33 件の脆弱性の影響を受ける製品は、多種多様にわたりましたが、企業において使用されるアプライアンス製品、統合システム製品等が 10 件と多く、次いでルータやデジタルビデオレコーダ(DVR)といった組込み系製品が 5 件でした。



[図 2-3　国際取扱脆弱性情報の公表累積件数]

2.2.　連絡不能開発者とそれに対する対応の状況

本基準に基づいて脆弱性が報告されたものの、調査と対策をしていただくべき製品開発者に、しかるべき手続きを踏んでも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 144 件(製品開発者数としては 88 件)を公表し、18 件(製品開発者の数としては 12 件)の調整が再開でき、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 16 件でした。連絡不能開発者一覧の公表開始からちょうど 2 年が経過した本四半期末日時点で、合計 126 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及び情報提供を呼び掛けています。

こうした対応によってもなお製品開発者への連絡が取れない脆弱性に関し、再現性を確認できた場合には、利用者のリスクを低減するため、JVN で公表するための手順や手続き等の準備を進めています。

2.3.　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情報通知及び対応状況の集約、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。2011 年より増加傾向にある Android 関連の脆弱

性の調整活動の中では、Android 関連製品を開発している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。

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、CVE 採番機関)として認定されています。本四半期は、JVN 上で公表した脆弱性情報のうち 34 件に対し CVE 識別子が付与されており、そのうち 28 件は JPCERT/CC が採番しました。JVN 上で公表する脆弱性に CVE 識別子を付与し始めた 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、ほぼすべてに CVE 識別子が付与されています。

CNA 及び CVE に関する詳細は、次の URL 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

2.4. 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 URL 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(2010 年版)
https://www.jpcert.or.jp/vh/partnership_guide2010.pdf
JPCERT/CC 脆弱性情報取扱いガイドライン
https://www.jpcert.or.jp/vh/vul-guideline2010.pdf

本四半期の主な活動は、以下のとおりです。

2.4.1. 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 の活動及び四半期ごとの届出状況については、次の URL をご参照ください。

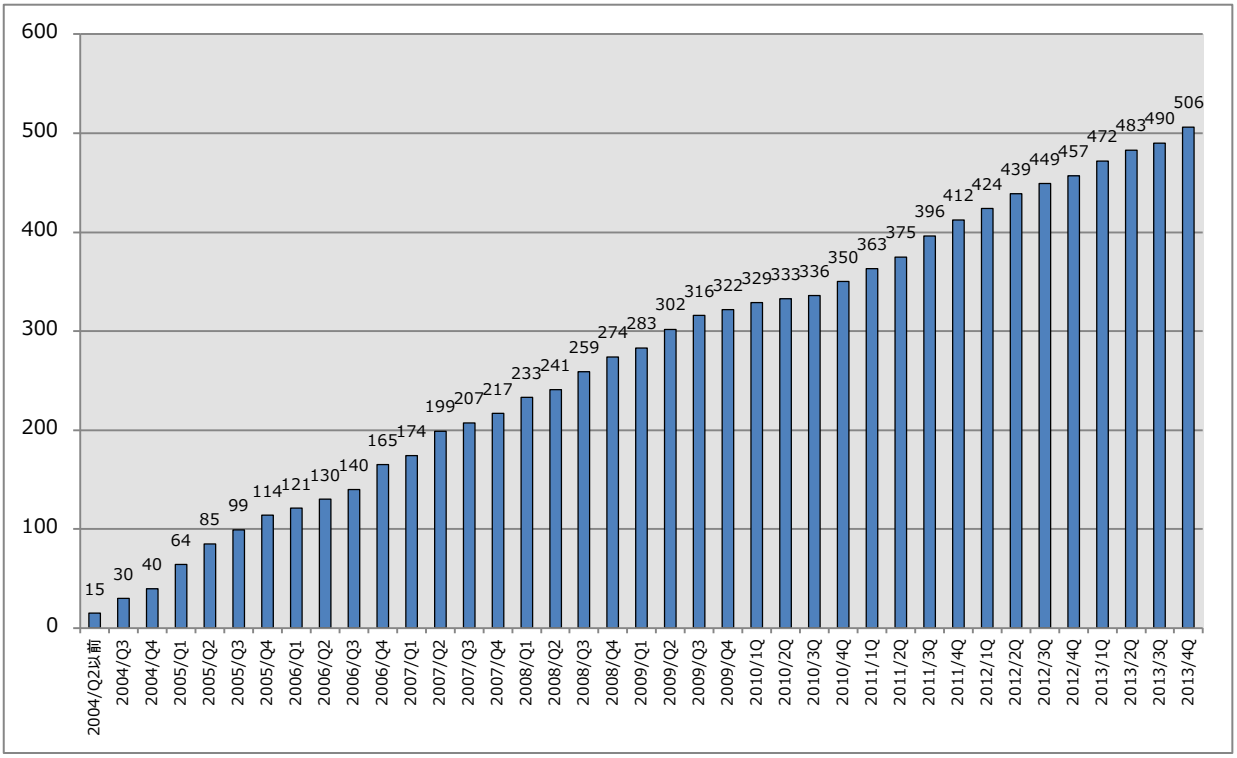
独立行政法人情報処理推進機構(IPA) 脆弱性対策
http://www.ipa.go.jp/security/vuln/

2.4.2. 日本国内製品開発者との連携

本基準では、JPCERT/CC が脆弱性情報を提供する先として、製品開発者リストを作成し、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、2013 年 12 月 31 日現在で 506 となっています。

登録等の詳細については、次の URL 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 2-4 累計製品開発者登録数]

2.5. セキュアコーディング啓発活動

2.5.1. 関西オープンフォーラム 2013 で講演

11 月 8 日、9 日に大阪南港 ATC で開催された関西オープンフォーラム 2013 において、脆弱性解析チームの戸田洋三が「～ヒトの振り見て我が振り直せ～脆弱性事例に学ぶ Java セキュアコーディング（KOF2013 編）」と題した講演を行いました。この講演では、9 月に公開した 5 編を含む計 10 編からなる Java アプリケーション脆弱性事例解説資料を紹介しました。また、展示スペースでは、同資料だけでなく JPCERT/CC の活動全般を紹介する展示を行いました。

講演後や展示スペースで、資料の内容に関する質問やご意見、また、セキュリティ啓発活動の進め方に関するご相談もいただきました。

本講演で使用した資料は下記の URL で公開されています。

～ヒトの振り見て我が振り直せ～ 脆弱性事例に学ぶ Java セキュアコーディング（KOF2013 編）
http://k-of.jp/2013/sites/all/files/slides/javacasestudies_KOF2013.pdf

2.5.2. Android セキュアコーディングルールを作成中

前四半期に続き、Android アプリの脆弱性と脆弱性の原因となるコーディング上のアンチパターンに関する調査・研究を行っています。セキュアな Android アプリ開発に役立てていただくため、調査の過程で得られた知見をコーディングルール化する作業を進めています。本四半期は新たに 2 つのルールを追加

しました。

The CERT Oracle Secure Coding Standard for Java
50. Android (DRD)
https://www.securecoding.cert.org/confluence/x/H4ClBg

追加したルール：
DRD09-J. Restrict access to sensitive activities
https://www.securecoding.cert.org/confluence/x/uoBRBw
DRD10-J. Do not release apps that are debuggable
https://www.securecoding.cert.org/confluence/x/XgGKBw

各ルールでは、脆弱なコード(アンチパターン)とその修正例とともに、JVN 等で公開されている関連する事例や、参考文献、関連する Java セキュアコーディングルール等も紹介しています。セキュアな Android アプリ開発の方法に関する情報源の一つとして活用していただければ幸いです。

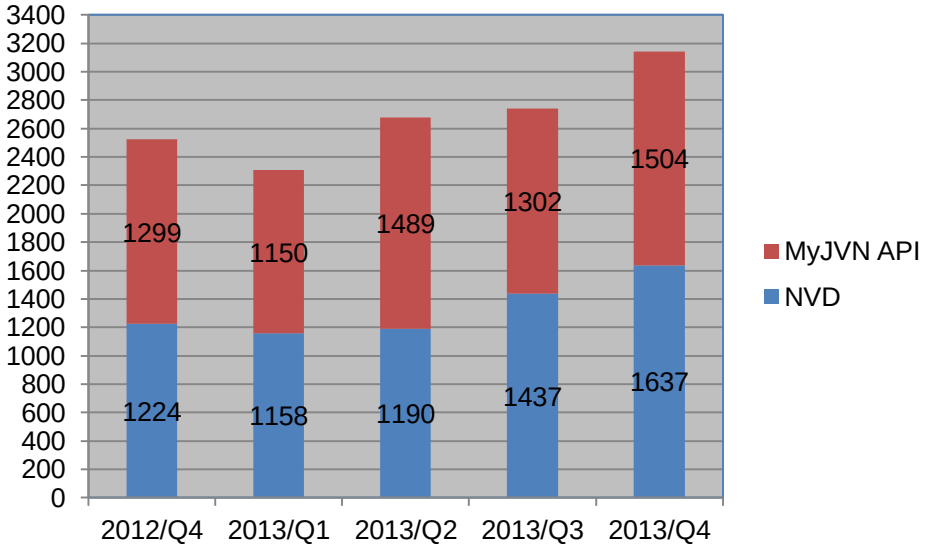
今後も新たなルールを追加していくとともに、公開済みのルールも随時アップデートしていく予定です。ルールの内容に関するコメントや改善案については Wiki に直接コメントするか、もしくは、secure-coding@jpcert.or.jp にお送りください。ルールの改善に活用させていただきます。

2.6. VRDA フィードによる脆弱性情報の配信

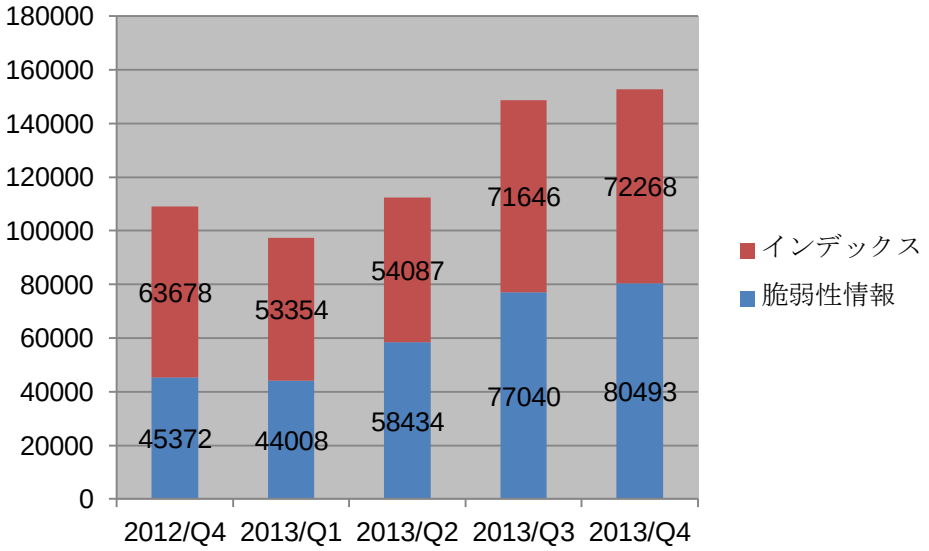
JPCERT/CC は、大規模組織の組織内 CSIRT 等での利用を想定して、KENGINE 等のツールを用いた体系的な脆弱性対応を可能とするため、IPA が運用する MyJVN API 及び NIST(National Institute of Standards and Technology)の NVD(National Vulnerability Database)を外部データソースとして利用した、VRDA (Vulnerability Response Decision Assistance)フィードによる脆弱性情報の配信を行っています。VRDA フィードについての詳しい情報は、次の URL 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 2-5]に、VRDA フィードの利用傾向を[図 2-6]と[図 2-7]に示します。[図 2-6]では、VRDA フィードインデックス(Atom フィード)と、脆弱性情報(脆弱性の詳細情報)の利用数を示します。VRDA フィードインデックスは、個別の脆弱性情報のタイトルと脆弱性の影響を受ける製品の識別子(CPE)を含みます。[図 2-7]では、HTML と XML の 2 つのデータ形式で提供している脆弱性情報について、データ形式別の利用割合を示しています。

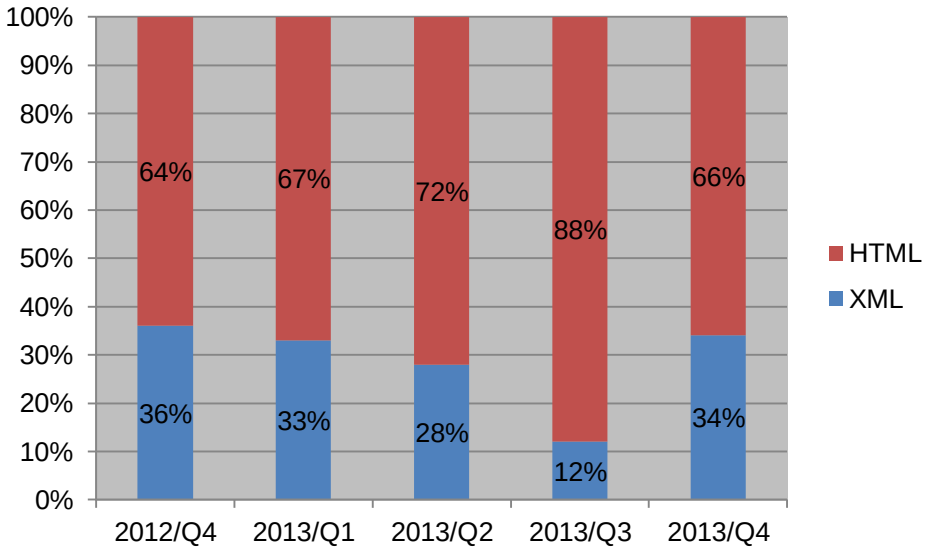


[図 2-5 VRDA フィード配信件数]



[図 2-6 VRDA フィード利用件数]

[図 2-6] に示したように、インデックスと脆弱性情報の利用数については、ほぼ前四半期と同じ水準でした。



[図 2-7 脆弱性情報のデータ形式別利用割合]

[図 2-7] に示したように、脆弱性情報のデータ形式別利用傾向は、前四半期と比較して、XML 形式の利用割合が大きく増加しました。

3. アーティファクト分析

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確認し、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。分析対象はウイルスやボット等のマルウエアに限らず、攻撃に使われるツールをはじめとするプログラムや攻撃手法等(アーティファクト)にまで及び、それらを技術的な観点から調査・解析します。アーティファクト分析を行うことで、より効果的なインシデント対応や、より精度の高い情報発信を目指すとともに、そのために必要な分析環境と分析能力の高度化に努めています。

また、JPCERT/CC は、実際のインシデントにおけるアーティファクト分析で得た知見を国内外で対策技術の研究開発を行う組織や活動と共有することが重要であると考え、研究機関や研究会等へも積極的に参加しています。

3.1. 「マルウェア対策研究人材育成ワークショップ 2013(MWS 2013)」への参画

「マルウェア対策研究人材育成ワークショップ 2013(MWS 2013)」(情報処理学会 コンピュータセキュリティ研究会 MWS 組織委員会主催)が 10 月 21 日から 3 日間の日程で、かがわ国際会議場(高松市)で開催されました。MWS は、「MWS Datasets」と呼ばれる主催者が用意した共通の研究用データセットを用いて行ったマルウエア対策に関する研究について発表を行うワークショップです。また、参加チームが、規定時間内にマルウエア解析やインシデント調査の課題に取り組み、解析や調査結果の精度や分析手法の洗練度等を競う MWS Cup 2013 も同時開催されました。

JPCERT/CC は実行委員や審査員、座長として MWS の運営に参加しました。また、MWS Cup 2013 では出題や採点等を行いました。このような取組を通して、解析技術そのものだけではなく、実際のインシデントの場面での解析技術への期待等についても研究者や学生と共有していくことが、総合的な分析能力の向上につながるものと考えています。

マルウェア対策研究人材育成ワークショップ 2013(MWS 2013)
http://www.iwsec.org/mws/2013/

4. 制御システムセキュリティ強化に向けた活動

4.1. 情報発信活動

制御システムセキュリティインシデントに関わる事例や標準の動向、その他の技術動向に関するニュース等を収集し、JPCERT/CC からのお知らせとともにまとめ、制御システム関係者向けにニュースレターとして提供しています。本四半期は計 4 回(10 月 2 日、11 月 30 日、12 月 16 日、12 月 27 日)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 319 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 URL 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

4.2. 制御システム関連のインシデント対応及び情報収集分析活動

本四半期に制御システムに関連するとして報告されたインシデントの件数は 1 件でした。

また、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 743 件でした。これらの中から、国内の制御システム関係者にとって新しく、有益であると考えられる情報を厳選した上でニュースレターの形で配信しました。

4.3. 関連団体との連携

定期的に開催されている SICE (計測自動制御学会)、JEITA(電子情報技術産業協会)、JEMIMA(日本電気計測器工業会)によ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。

4.4. 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、JPCERT/CC に対して、日本語版 SSAT に関しては 6 件、J-CLICS に関しては 12 件の利用申込みがありました。直接配布件数の累計は、日本語版 SSAT が 155 件、J-CLICS が 180 件となりました。

4.5. 制御システムベンダにおける脆弱性取扱の社内体制整備促進

本年 10 月より「制御システムベンダにおける脆弱性取扱の社内体制整備促進検討会」を開始しました。全 7 回を予定し、制御システムベンダで脆弱性対応を行う場合に考えられる「必要な機能」「機能を担う体制の在り方」「実現に関わる課題」等を中心に検討会を行い、発見された脆弱性に対する情報流通の整備を進めています。

4.6. 講演活動

10 月 22 日に東京工業大学で行われた SICE 産業応用部門 2013 年度大会にて、「制御システム模擬環境におけるサイバーインシデント対応訓練の効果と考察」と題する発表を行いました。また、11 月 6 日～8 日に東京ビックサイトで行われたシステム コントロール フェア 2013 にて、「制御システムセキュリティ対策」と題する発表を行いました。

5. 国際標準化活動

5.1. 「脆弱性情報開示」の国際標準化活動への参加

脆弱性情報の開示(Vulnerability Disclosure[VD] ; 29147 ; 旧称 Responsible Vulnerability Disclosure)及び取扱手順(Vulnerability Handling Process [VHP] ; 30111)に関して、それぞれ並行して進められている ISO/IEC JTC-1/SC27 の WG3 における国際標準の策定作業に参加しています。VD(29147)は、ベンダの外側から見える、インターフェースに相当する部分だけを規定し、VHP(30111)は、外部からは見えない活動等を含む、ベンダ内部での対応を規定しています。

「脆弱性情報の開示」については、国際標準草案(DIS：Draft of International Standard)に対する国際投票に際して寄せられた合計 188 件のコメント(日本から 35 件、米国から 15 件、英国から 7 件、カナダから 106 件、メキシコから 25 件)で指摘された箇所について、4 月下旬に開催された SC27 国際会議での審議結果に基づいてエディタが草案の改訂作業を行い、さらに ISO の ITTF と呼ばれる組織が技術文書として読みにくかった箇所に手を入れたものが、10 月 2 日に国際標準最終草案(FDIS : Final draft of International Standard)として SC27 事務局から各国に配布され、国際投票に付されました。これを精査し、国内委員会での審議を経た上で、日本として 7 件のコメント付きで賛成するように提案し、そのように情報規格調

査会から投票がなされました。国際投票は 12 月 2 日に締め切られ、開票の結果は、賛成が 24 カ国で反対なし、棄権が 20 カ国の結果となり、承認されることになりました。賛成した国のうち、日英米及びカザフスタンの 4 カ国はコメントを付けており、それらを反映することを検討した上で、国際標準として発行される見通しです。

「脆弱性取扱手順」については、「脆弱性の開示」よりも遅くに開発がスタートしましたが、DIS(Draft of International Standard)段階での国際投票で承認され、11 月 1 日に国際標準として発行されました。

2008 年 4 月から始まった標準策定作業について、JPCERT/CC では SC27 国際会議への参加ならびに日本の標準化組織である情報規格調査会を通じて、わが国の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に整合したものとなるよう努めてきましたが、その策定作業も最終段階となりました。

5.2. インシデント管理の国際標準化活動への参加

現在 ISO/IEC JTC-1/SC27 の WG4 では、情報セキュリティインシデント管理に関する国際標準 27035:2011 を下記の 3 つの標準からなるマルチパート標準へと改訂する作業が進められています。

27035-1. インシデント管理の原理(Principles of Incident Management)
27035-2. インシデント対応の計画と準備のためのガイドライン(Guidelines to Plan and Prepare for Incident Response)
27035-3. インシデント対応の運用のためのガイドライン(Guidelines for Incident Response Operations)

JPCERT/CC は 27035:2011 の策定段階からこの標準化活動に関わっています。

本四半期は、10 月 21 日から 25 日に仁川(韓国)で開催された SC27 国際会議に日本の代表団の一員として参加し、SC27 事務局に事前に提出していた 3rd Working Draft に対する日本のコメントについて説明を行うとともに、各国の代表とコメントに関する議論を行いました。

インシデント管理の原理を規定する 27035-1 の草案には、4 カ国から 60 件のコメントが寄せられました。日本から提出した 17 件のコメントについては、一部のコメントを除き概ね受け入れられました。ドキュメントの成熟度は順調に向上しており、大きな課題はありません。

インシデント対応の計画と準備のガイドラインを規定する 27035-2 については、4 カ国から 58 件（うち日本からは 15 件)のコメントが寄せられました。章構成の大幅な変更を求める日本のコメント(JP2～JP13)はすべて受け入れられ、結果として Part1 の構成とも整合性の取れた、より見通しの良い構成に改善されることになりました。ドキュメントの完成度は順調に向上していて、各章の内容も既存の CSIRT の実態と整合性が取れており、国際標準としての記述の粒度にも問題がありません。章構成が大きく変更されることになったため、次期草案でドキュメント全体としての整合性を再検証することが残された課題です。

インシデント対応のオペレーションのガイドラインを規定する 27035-3 については、3 カ国から 39 件(うち日本からは 26 件)のコメントが寄せられました。章構成の見直しを求める日本のコメントについては、

Accepted in Principle となり、エディタが内容の重複を考慮しつつ、次期草案で新しい章構成を提示することになりました。インシデント対応の各フェーズにおけるオペレーションを記述した Clause 5 に対する日本のコメントには、韓国エディタの強い抵抗があり、すべては受け入れられませんでした。却下されたコメントの多くは、インシデント対応の実オペレーションの細部に関する内容について、必ずしも間違ってはいるとはいえないものの、特定の組織での対応を想定した偏りのある内容であるとの印象が否めないことからコメントしたものでした。また、見出しなしに 5～10 パラグラフもテキストが連続する節が散見されるばかりでなく、章の内容の重複を大幅に見直す必要がある等、今後の課題が少なくありません。

27035 全体の進捗状況としては、標準化のスケジュールの延長を求めることで各国の合意が得られ、すべてのパートで足並みを揃え、4th WD へと進むことになりました。

JPCERT/CC では、インシデントの管理と対応に関連した 3 つの国際標準について、SC27 国際会議への参加ならびに日本の標準化組織である情報規格調査会における活動を通じて、引き続き、この国際標準がわが国の CSIRT の取組と整合性の取れたものとなるよう努めていく所存です。

6. 国際連携活動関連

6.1. 海外 CSIRT 構築支援及び運用支援活動

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目指し、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。

6.1.1. ラオスにおける CSIRT 構築支援活動(2013 年 10 月 1 日-4 日)

JPCERT/CC は、ラオスの National CSIRT である LaoCERT のスタッフに対して、同組織の機能強化を目的としたトレーニングを、ラオスの首都ヴィエンチャンで 10 月 1 日から 3 日の計 3 日間にわたって行いました。LaoCERT のスタッフ計 20 名が受講した本トレーニングでは、JPCERT/CC のスタッフ 2 名とタイの National CSIRT である ThaiCERT のスタッフ 2 名が講師となり、インシデントハンドリングの手法についての講義やネットワークフォレンジックのハンズオン演習を行いました。また 10 月 4 日には、ラオス国立大学と独立行政法人国際協力機構(JICA)が共催した IT セキュリティカンファレンスにおいて、「Incident trends in Japan and roles of CSIRT」と題する講演を行いました。

LaoCERT は 2012 年 5 月に設立したばかりの新しい組織で、スタッフの育成が急務となっています。本トレーニングの実施に際しては、ThaiCERT に協力を仰ぎ、受講生の理解度が深まるよう、一部の講義を言語的にラオ語に近いタイ語で行いました。

[図 6-1　トレーニングの様子]

6.1.2. アフリカにおける CSIRT 構築支援活動(2013 年 11 月 24 日-28 日)

JPCERT/CC は、11 月にコートジボワールの旧首都アビジャンで開催された国際会議 AFRINIC-19 に参加するとともに、併催された 1 日コースのアフリカ諸国向けの CSIRT トレーニングを実施しました。また 11 月 27 日に開催された AfricaCERT Workshop に参加しました。

JPCERT/CC が実施を担当した CSIRT トレーニングは、AFRINIC-19 のトレーニング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 AAF(Africa Asia Forum on Network Research & Engineering)が主催したプログラムです。同様のトレーニングは 2010 年春から実施しており、今回で 7 回目の開催となります。今回はコートジボワールやその近隣のトーゴ、カメルーン等から合計 40 名以上が参加しました。

11 月 24 日と 25 日には、FIRST の講師による CSIRT 研修が行われました。JPCERT/CC は、FIRST の Steering Committee 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 26 日は、JPCERT/CC が主任講師として CSIRT 技術者向けにネットワークフォレンジックのハンズオン演習をグループワークで行いました。また同日、韓国 KrCERT/CC が同組織の紹介及びインシデン

トレスポンスに関する講演を行い、JPCERT/CC はそのサポートを行いました。

11 月 27 日の AfricaCERT Workshop では、AfricaCERT という地域 CSIRT の現状と今後の活動計画について事務局から説明が行われ、Workshop 参加各国からカントリーアップデートがありました。JPCERT/CC は AfricaCERT の年次活動報告書作成の提案を行い、パネルディスカッションに参加しました。

[図 6-2 トレーニングの様子]

AFRINIC 及び CSIRT トレーニングについての詳細は、次の URL をご参照ください。

AFRINIC 及び AFRINIC-19 公式ページ
http://meeting.afrinic.net/afrinic-19/en/

制度や技術がまだ成長段階にある国・地域等が関与するインシデントは、対処が後手になりがちで、日本のインターネットユーザにとっても脅威の一つとなっています。今後急速なインターネット普及が予想されているアフリカ地域に起因するインシデントが併せて増えることが予想され、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。

6.2. 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、及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た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。

6.2.1. 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 3 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 における役割及び APCERT の詳細については、次の URL をご参照ください。

JPCERT/CC within APCERT
https://www.jpcert.or.jp/english/apcert/

6.2.1.1. APCERT Steering Committee 会議の実施

Steering Committee は 11 月 15 日、12 月 4 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を行いました。JPCERT/CC は議長チーム及び事務局として、本会議の主導及びサポートを行いました。

6.2.1.2. APCERT を代表しての会議出席

・Seoul Cyber 2013

JPCERT/CC は APCERT を代表して Seoul Cyber 2013(以下「ソウルサイバー会議」といいます。)にて講演を行いました。ソウルサイバー会議は 2011 年のロンドンサイバー会議、2012 年のブダペスト(ハンガリー)サイバー会議に続く国際協議の場であり、10 月 17、18 日と韓国ソウルで開催されました。合計 79 カ国以上から、政府関係者を中心に、国際機関、企業、学術機関等に属する関係者 1,600 名以上が参加しました。JPCERT/CC の講演では、APCERT の活動を紹介し、その活動がグローバルなサイバー空間での信頼醸成のプロセスに寄与するものであることを説明しました。またサイバー空間のセキュリティに関する諸問題について、国際的に比較可能な指標の必要性を訴え、それに向けた活動について各関係者の協力を求めました。ソウルサイバー会議についての詳細は、次の URL をご参照ください。

ソウルサイバー会議 公式ページ
http://www.seoulcyber2013.kr/en/

・IGF 2013 Bali

インドネシアバリ島で開催された The Internet Governance Forum (IGF) 2013 で、JPCERT/CC は APCERT を代表して APNIC、ISOC/OECD、Workshop 143 Emerging Cybersecurity Threats の 3 つのパネルに登壇し、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、APCERT の取組等の紹介／報告を行いました。

IGF 2013 Bali 公式ページ
http://igf2013.or.id/

・LACNIC 20 - LACNOG 2013

JPCERT/CC は APCERT を代表して LACNIC 20 - LACNOG 2013 及び併催される FIRST TC、5th Latin American and Caribbean CSIRTs Regional Meeting に参加し、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、ラテンアメリカ及びカリブ海の地域 CSIRT に指標の実装を依頼しました。

LACNIC 20 - LACNOG 2013 公式ページ
http://www.lacnic.net/en/web/eventos/lacnic20

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

JPCERT/CC は FIRST に加盟しており、JPCERT/CC の理事 山口英は FIRST の Steering Committee のメンバを務めています。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 及び Steering Committee の詳細については、次の URL をご参照ください。

FIRST
http://www.first.org/

FIRST Steering Committee
http://www.first.org/about/organization/sc.html

6.2.3. ACID：ASEAN 及び周辺各国の CSIRT による合同サイバーインシデント演習への参加(10 月 4 日)

JPCERT/CC は、シンガポールの National CSIRT である SingCERT が主導した、ASEAN(東南アジア諸国連合)各国の CSIRT が合同で実施するサイバーインシデント演習である ACID(ASEAN CERTs Incident Drill)に参加しました。本演習は、国境を越えて発生するサイバーセキュリティインシデントに備え、ASEAN 加盟国及び周辺各国の CSIRT 間の連携の強化を目的に毎年実施されているもので、今回が 8 回目になります。

今年は 12 カ国(日本、オーストラリア、ブルネイ、カンボジア、中国、インド、インドネシア、マレーシ

ア、ミャンマー、シンガポール、タイ、ベトナム)から参加した 14 チームにより、DDoS を隠れみのとした APT 攻撃を想定した演習が行われました。

6.2.4. JICA 沖縄国際センターIT 研修生による実地見学の受け入れ(2013 年 10 月 30 日)

JICA 国際沖縄センターで「電子政府推進のためのセキュリティ強化」コースを受講中の研修生 5 名(バングラデシュ、モンテネグロ、フィリピンの政府系組織の IT 担当者等)が来訪しました。CSIRT の役割や JPCERT/CC の事業紹介、最近のインシデント動向、TSUBAME プロジェクトの紹介等を JPCERT/CC から行った後、活発な意見交換が行われ、日本及び各国におけるインターネットセキュリティの状況が共有されました。

6.2.5. ベトナム VNCERT 主催の会議での講演(2013 年 10 月 30 日）

ベトナムの National CSIRT である VNCERT がハノイにて開催した会議「BUILDING DOMESTIC AND INTERNATIONAL COORDINATION MECHANISM IN COMPUTER INCIDENT RESPONSE」で、JPCERT/CC 職員がサイバークリーンセンタープロジェクト(略称 CCC プロジェクト)に関する講演を行いました。同プロジェクトは、ボットウイルス等のインターネットの脅威に対処するために対処手順、駆除ツールの提供を行うもので、2006 年から 2011 年に国の事業として実施され、JPCERT/CC はボットプログラム解析において関与しました。ベトナムにおいてもボット対策が急務となっており、同プロジェクトの手法やノウハウをベトナム政府、ISP の関係者等約 200 名に向けて紹介しました。

6.2.6. OIC-CERT Conference での講演（2013 年 11 月 18 日-19 日）

JPCERT/CC はインドネシアのバンドンで開催された OIC-CERT の年次会合(11 月 18 日)に参加し、カンファレンス(11 月 19 日)にも登壇して、OIC-CERT と APCERT の協力の経緯を振り返り、今後の協力拡大(OIC-CERT によるネットワーク定点観測プロジェクト TSUBAME への参画等)を提案しました。

OIC-CERT は イスラム協力機構(OIC)に加盟する国々の National CSIRT、民間企業 CSIRT による情報共有や連携を図るために創設された組織です。その発足については 2005 年からマレーシア等の国を中心に検討が行われ、2009 年に OIC より関連機関としての正式承認を受けました。

JPCERT/CC は、インシデント対応におけるアジア大洋州と中東や北アフリカの連携強化の必要性から OIC-CERT の活動に着目し、APCERT と OIC-CERT 間の覚書締結の実現に注力してきました。また 2012 年より APCERT の演習に OIC-CERT のメンバを招き、共同で演習を行う等、実務レベルでの交流を拡大してきています。

OIC-CERT 及び OIC-CERT AGM/Conference の詳細については、次の URL をご参照ください。

OIC-CERT
http://www.oic-cert.net/v1/index.html

6.2.7. 9th U.S.-Japan Critical Infrastructure Protection Forum 参加（2013 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 9th U.S.-Japan Critical Infrastructure Protection Forum(以下「日米 CIP フォーラム」といいます。)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及び制御システム分野における情報を収集し、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「グローバルなリスク軽減のための日米協力」というタイトルで、国際間の情報共有の強化及び国際比較可能な指標の必要性について講演を行いました。

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。

6.2.8. OECD セキュリティ専門家会合出席（2013 年 12 月 10 日-13 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。

6.2.9. ブログや Twitter を通した情報発信

英語ブログ (blog.jpcert.or.jp) や Twitter (twitter.com/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。本四半期は以下に関してブログにエントリーを掲載しました。

SNS in Japan
http://blog.jpcert.or.jp/2013/10/sns-in-japan.html

Information Security Incident Management Standard under Revision
http://blog.jpcert.or.jp/2013/11/information-security-incident-management-standard-under-revision.html

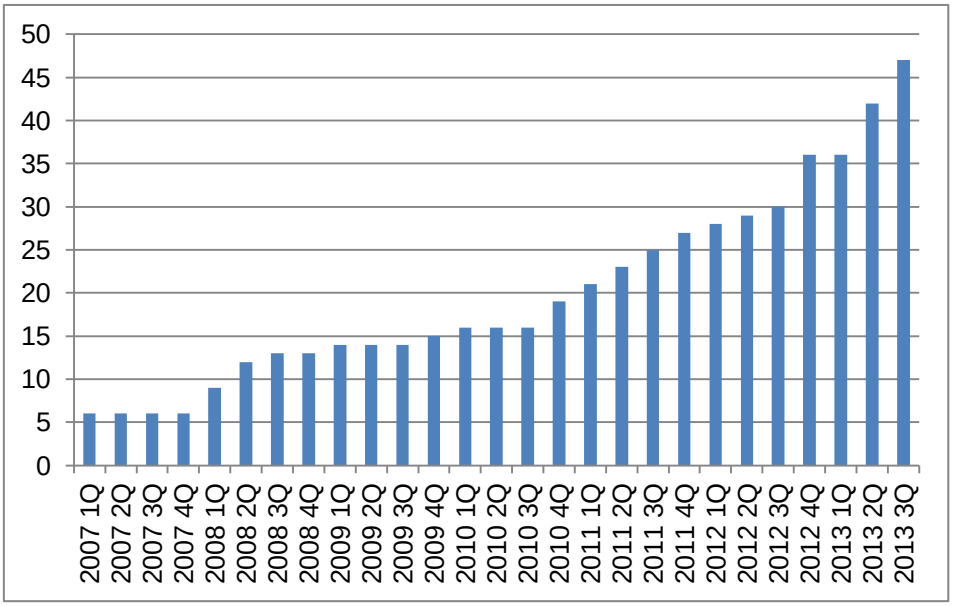
Analysis on Compromised Websites in Japan
http://blog.jpcert.or.jp/2013/12/analysis-on-compromised-websites-in-japan.html

JPCERT/CC 英語ブログ：http://blog.jpcert.or.jp/

7. 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、Web サイトを通じた広報活動、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及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及びイベントに参加しています。

本四半期においては、ANA システムズ株式会社(ASY-CSIRT)と株式会社ジャパンネット銀行(JNB-CSIRT)、株式会社三井住友フィナンシャルグループ(SMFG-CSIRT)、メットライフアリコ生命保険株式会社(MAJ-CIRT)、トヨタ自動車株式会社(TMC-SIRT)の 5 組織が新規に加盟しました。本四半期末時点で 47 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 7-1]のとおりです。



[図 7-1 日本シーサート協議会 加盟組織数の推移]

日本シーサート協議会では、11 月 19 日に「TRANSITS Workshop NCA Japan」を開催しました。TRANSITS とは、CSIRT の設立の促進、既存の CSIRT の対応能力向上を目的としてヨーロッパで開発された教育プログラムに基づいた教育訓練コースです。JPCERT/CC は TRANSITS マテリアルの翻訳や講師サポート等を担当しました。「TRANSITS Workshop NCA Japan」の詳細については、次の URL をご参照ください。

TRANSITS Workshop NCA Japan
http://www.nca.gr.jp/2013/transits/index2.html

12 月 6 日には、日本シーサート協議会のワーキンググループの１つである、シーサート構築推奨 SWG から、CSIRT 構築に際し、構築初心者／経営者向け説明時／構築担当者の企画・構築・運用の各段階における参考ドキュメント類を列挙した表「CSIRT 構築に役立つ参考ドキュメント類」が公開されました。

公開資料及びシーサート構築推奨 SWG の詳細は次の URL をご参照ください。

CSIRT 構築に役立つ参考ドキュメント類
http://www.nca.gr.jp/activity/build-wg-document.html
シーサート構築推奨 SWG の活動概要
http://www.nca.gr.jp/activity/build-wg.html

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

日本シーサート協議会 Web ページ
http://www.nca.gr.jp/

8. 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、JPCERT/CC のインシデント対応チームに対するフィッシングサイトの停止調整の依頼、国内外関連組織との共同研究等の活動を行っています。

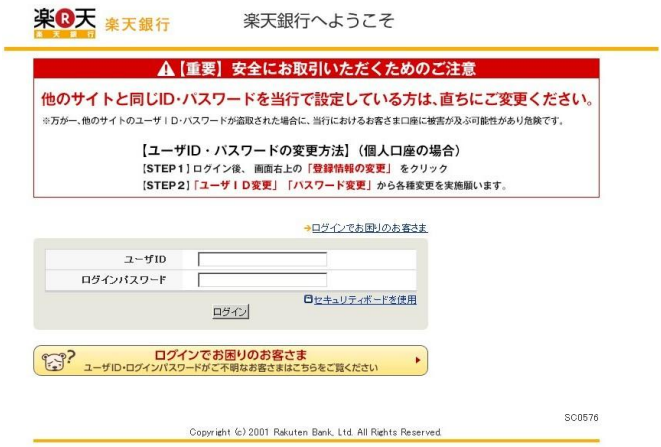
8.1. 情報収集/発信の実績

本四半期は、協議会 Web ページや会員向け 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 13 件発信しました。

本四半期は、金融機関をかたり第二認証情報を詐取するフィッシングやオンラインゲーム事業者をかたるフィッシング、インターネットサービスプロバイダ等が提供している Web メールサービスをかたるフィッシングの報告を多数受けました。協議会では、名前をかたられた事業者に、フィッシング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 8-1]の「三菱東京 UFJ 銀行をかたるフィッシング(2013/11/18)」や[図 8-2]の「楽天銀行をかたるフィッシング(2013/12/12)」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。

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行い、すべてについて停止を確認しました。

[図 8-1　三菱東京 UFJ 銀行をかたるフィッシング(2013/11/18)
https://www.antiphishing.jp/news/alert/mufg20131118.html]



[図 8-2　楽天銀行をかたるフィッシング(2013/12/12)
https://www.antiphishing.jp/news/alert/rakutenbank20131212.html]

8.2.　フィッシングサイト URL 情報の提供

協議会では、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協議会員の事業者と、フィッシングに関する研究を行っている協議会員の学術機関に対し、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、日に数回提供しています。この活動は、提供した URL 情報をブラックリストに追加していただく等、ユーザ保護に向けた取組に活用していただくことや、関連研究の促進を目的としています。本四半期末の時点で協議会から情報を提供している事業者等は 19 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。

8.3. 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「フィッシングの最新動向について」
新潟県サイバー脅威対策協議会サイバー対策分科会 2013 年 12 月 5 日

山本健太郎「フィッシングの現状と対策について」
埼玉県サイバー空間防犯推進連絡会 2013 年 12 月 19 日

8.4. 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 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 2013 年 10 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201310.html
フィッシング対策協議会 2013 年 11 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201311.html
フィッシング対策協議会 2013 年 12 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201312.html

9. 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。

9.1. 運営委員会開催

本四半期においては、次のとおり、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開催しました。

フィッシング対策協議会 第 8 回運営委員会
日時：2013 年 11 月 8 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 9 回運営委員会
日時：2013 年 12 月 13 日 16:00 - 18:00
場所：株式会社ジャックス

9.2. フィッシング対策セミナーの開催

日本国内におけるフィッシング詐欺被害の抑制を目的として、昨年に引き続き「フィッシング対策セミナー2013」を開催いたしました。主に金融機関の方に参加いただき、警察庁生活安全局 情報技術犯罪対策課、株式会社三菱東京 UFJ 銀行 MUFG-CERT、トレンドマイクロ株式会社、日本マイクロソフト株式会社及びフィッシング対策協議会の講師からフィッシング詐欺の最新の手口や傾向と、対応策や取組事例が紹介されました。会場には、パネル展示とフィッシング対策ガイドライン(2013 年度版)を使った説明及び個別のご相談をお受けする相談窓口を設けました。

フィッシング対策セミナー2013
開催日程：2013 年 12 月 17 日（火）13:30-17:15
会場：トッパン・フォームズ株式会社 1F
参加人数：144 名

10. 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。

10.1. HTML5 を利用した Web アプリケーションのセキュリティ問題に関する調査報告書

本資料は、HTML5 を利用した安全な Web アプリケーション開発のための技術書やガイドラインのベースとなる体系的な資料の提供を目的として、懸念されるセキュリティ問題を抽出して調査し、検討を加え、それらの問題に対して可能な限り検証を行った上で、調査結果をまとめたものです。
本資料の詳細は、「1.1.3」をご参照ください。

HTML5 を利用した Web アプリケーションのセキュリティ問題に関する調査報告書
(2013 年 10 月 30 日)
https://www.jpcert.or.jp/research/html5.html

11. 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 情報セキュリティアナリスト)：
「増大するセキュリティ事案と各組織に求められる体制」

「CSIRT 構築パッケージについて」
大学・高等教育機関におけるサイバーセキュリティ能力向上と体制整備に関するワークショップ, 2013 年 12 月 26 日

(2) 山本 健太郎(フィッシング対策協議会)：
「フィッシングの現状と対策について」
埼玉県サイバー空間防犯推進連絡会, 2013 年 12 月 19 日

(3) 竹田 春樹(分析センター リーダー) ：
「あなたも狙われている!? インターネットバンキングの不正送金とマルウエアの脅威」
SecurityDay 2013,2013 年 12 月 9 日

(4) 満永 拓邦(早期警戒グループ 情報分析ライン リーダー 情報セキュリティアナリスト) ：
「システム侵入・解析演習(セキュリティ PBL 演習 I)」
文科省セキュリティ人材育成 SecCap 関連演習講師 大阪大学,2013 年 12 月 7~8 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 情報セキュリティアナリスト) ：
「セキュリティアナリストの日常と最近のセキュリティ動向」
文科省セキュリティ人材育成 SecCap 関連演習講師 慶応義塾大学,2013 年 12 月 6 日

(6) 真鍋 敬士(理事,分析センター長) ：
「サイバー攻撃の傾向と JPCERT/CC の取組み」
サイバーワールド時限研究専門委員会, 2013 年 12 月 6 日

(7) 山本 健太郎(フィッシング対策協議会)：
「フィッシングの最新動向について」
新潟県産学官民合同対策プロジェクト推進協議会,2013 年 12 月 5 日満永 拓邦(早期警戒グループ 情報分析ライン リーダー 情報セキュリティアナリスト)：
「標的型攻撃に対する備えと対策」
Internet Week 2013,2013 年 11 月 26 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 情報セキュリティアナリスト) ：
「変化するサイバー攻撃への対応」
奈良先端科学技術大学院大学,2013 年 11 月 22 日

(9) 真鍋 敬士(理事,分析センター長)：
「脅威を知ることから始める インシデント対策」
在日米国大使館商務部後援 Panasonic「標的型攻撃」と「モバイルセキュリティ」対策セミナー, 2013 年 11 月 22 日

(10) 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～」
関西 IBM ユーザ研究会, 2013 年 11 月 21 日

(11) 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)：
「進化するインシデントレスポンス ～変化するサイバー攻撃への対応～」
第 3 回 FSA 技術委員会研究部会,2013 年 11 月 20 日

(12) 満永 拓邦(早期警戒グループ 情報分析ライン リーダー 情報セキュリティアナリスト) ：
「オペレーション」
日本シーサート協議会 TRANSITS Workshop,2013 年 11 月 19 日

(13) 満永 拓邦(早期警戒グループ 情報分析ライン リーダー 情報セキュリティアナリスト) ：
「APT 対応事例」
APT への備えと対応ガイド説明会第 2 回 JPCERT/CC,2013 年 11 月 15 日

(14) 有村 浩一(常務理事)：
パネル「制御システムセキュリティシンポジウム」
計測展 2013TOKYO シンポジウム,2013 年 11 月 8 日

(15) 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)：
「巧妙化するサイバー攻撃の実態と IT 変革時代に企業が考えるべきセキュリティ対策」
IBM セキュリティー・コンファレンス 2013 -秋-,2013 年 11 月 8 日

(16) 真鍋 敬士(理事,分析センター長)：
「最新のサイバーセキュリティの脅威」
TCG 日本支部第五回公開ワークショップ，2013 年 10 月 25 日

(17) 内山 貴之(情報流通対策グループ 脆弱性情報ハンドリンググループ 情報セキュリティアナリスト)：
「情報ネットワークの脆弱性問題」
明治大学国際総合研究所(MIGA),2013 年 10 月 11 日

12. 開催セミナー等一覧

(1) フィッシング対策セミナー
※本セミナーの詳細は、「9.2」をご参照ください。

(2) SecurityDay 2013
近年、インターネットは、さまざまな社会経済活動において広く利用されるようになりました。一方、脆弱性を悪用した攻撃方法の知識や攻撃ツールがインターネットを通じて売買されるなど、セキュリティ上の脅威は拡大しています。これら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：70名

詳細については、以下のURL をご参照ください。
http://securityday.jp/

13. 協力、後援一覧

(1) 第10回デジタル・フォレンジック・コミュニティ2013 inTOKYO
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2013 実行委員会
開催日：2013年12月16日(月)～17日(火)

(2) TCG日本支部(JRF)第五回ワークショップ
主　催：TCG日本支部(JRF)
開催日：2013年10月25日(金)

(3) グローバルで活躍するサイバーセキュリティ高度専門技術者育成のための研究討論会
主　催：東京電機大学
開催日：2013年11月28日(木)

(4) Internet Week 2013
主　催：社団法人日本ネットワークインフォメーションセンター(JPNIC)
開催日：2013年11月26日(火)～29日(金)

(5) CSMS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：2013年10月28日(月)

(6) 情報セキュリティワークショップin 越後湯沢2013
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：2013年10月11日(金)～12日(土)

(7) Email Security Conference2013
主　催：株式会社ナノオプト・メディア
開催日：東京2013年10月4日(金)、大阪2013年10月18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