JPCERT-PR-2013-03
発行日 : 2013-10-10

JPCERT/CC 活動概要 [2013 年 7 月 1 日 ～ 2013 年 9 月 30 日]

活動概要トピックス

—トピック 1— 本四半期におけるインシデント報告の件数が 1 万件を超過

—トピック 2— Android セキュアコーディングルールを作成中

—トピック 1—
本四半期におけるインシデント報告の件数が 1 万件を超過

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 10095 件、インシデント件数ベースでは 8284 件となり、報告件数が四半期ベースで初めて 1 万件を超えました。

> ※「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、「インシデント件数」は、各報告に含まれるインシデント件数の合計を示します。1 つのインシデントに関して複数件の報告が寄せられた場合にも、1 件として扱います。

報告されるインシデントの分類としては、Web サイト改ざんが最も多く、インシデント件数ベースでは全体の 33.5%に当たる 2774 件が該当します。これらの一部には、9 月中旬に報告された、Web サイトに侵入したことを誇示することを目的とする海外からの改ざんも一部含まれていますが、そのほとんどは、前四半期に引き続き、不審な iframe や難読化された JavaScript が Web サイトのページに挿入されたものでした。改ざんされた Web サイトにアクセスすると、他の URL に誘導され、誘導先の php スクリプトによって、さらに複数のアプリケーションの脆弱性を使用した攻撃を行うサイトに誘導されることを確認しています。

脆弱性が存在する古いバージョンの OS やアプリケーションがインストールされた PC が攻撃されると、マルウエアに感染して、PC に保存された様々な認証情報を窃取されたり、他のマルウエアをダウンロードされたりする可能性があります。改ざんの被害を受けた Web サイトの管理者から、不明な第三者による ftp の認証が記録されていたとの情報を複数いただいており、改ざんを許した一因として、Web サイトの管理用ソフトウエアの脆弱性の悪用以外にも、Web サイトの管理に使用する PC が ftp などの認証情報を窃取するマルウエアに感染していたか、ftp のパスワードが容易に推測できるものであったなどの問題点が考えられます。

改ざんを許さないよう平素から適切な Web サイトの管理を行うことが望ましいことは言うまでもありませんが、改ざんを許してしまった場合には、自組織において Web サイト改ざん以外のインシデントやそれによる情報窃取等の被害が発生している可能性を疑うべきであり、所要の調査や再発防止のため

の対策を実施する必要があります。また、改ざんされたページを閲覧した顧客等やその者が所属する組織等において、マルウエア感染等のインシデントが発生していないかを確認することができるよう、Web サイトが改ざんされていた期間や誘導先の URL その他の情報を適切な手法で提供することが期待されます。

また、Web サイト改ざんやマルウエア配布サイト等に分類されるインシデントのハンドリングの過程で、それらのインシデントが、いわゆる APT(Advanced Persistent Threat)と称される攻撃主体による攻撃キャンペーンの一部と見込まれることが判明した等の事情により、1 件のインシデント報告のハンドリングが実際には膨大なデータの分析等を要することになる場合もあり、インシデント対応調整活動については、インシデント件数の増加のみならず、1 件当たりの対応コストの増加も著しいといえます。

もちろん、この種のインシデントが発生した当事者組織等においては、攻撃に気がつくまでの期間が長くなれば長くなるほど、企業情報等窃取等の被害はもとより、状況把握のための調査等のコストも膨大なものにならざるを得ないところ、創造力に富んだ企業活動を安心して継続するためには、攻撃を受けている状況をより迅速に把握し、適切な初動の対応をとるための技術的、組織的な対応体制の整備が重要です。

JPCERT/CC インシデント報告対応レポート[2013 年 7 月 1 日～2013 年 9 月 30 日]
https://www.jpcert.or.jp/pr/2013/IR_Report201301010.pdf
CSIRT マテリアル
https://www.jpcert.or.jp/csirt_material/

―トピック 2―
Android セキュアコーディングルールを作成中

JPCERT/CC は、カーネギーメロン大学ソフトウエア工学研究所(CMU/SEI)とオラクル社が協同で開発した「Java セキュアコーディングスタンダード」の日本語版を JPCERT/CC の Web サイトに公開するなど、各コーディングルールの品質向上に貢献する活動を行っています。本年度も引き続き 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・研究を行っており、調査の過程で得られた知見をセキュアな Android アプリ開発に役立てていただくために、コーディングルール化する作業を進めています。

作成したコーディングルールは、CMU/SEI の協力のもと、Java セキュアコーディングスタンダードに新規カテゴリー「50. Android」を設け、その中で順次公開しています。本四半期は 6 つのルールを追加しました。

「Java セキュアコーディングスタンダード」の日本語版
https://www.jpcert.or.jp/java-rules/

The CERT Oracle Secure Coding Standard for Java

50. Android (DRD)

https://www.securecoding.cert.org/confluence/x/H4ClBg

CMU/SEI とはこれまでも、セキュアコーディングに関する研究や啓発活動を協力して行ってきましたが、より多くのエキスパートの意見を取り入れオープンに開発を進めるために、SEI の Wiki プラットフォームを活用しています。各ルールのページでは、脆弱なコード(アンチパターン)とその修正例を紹介するとともに、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。
また、ルール作成作業と並行して、既存の Java セキュアコーディングルールの中で Android アプリ開発にも適用可能なルールの一覧のアップデートを進めています。

Application of CERT Oracle Secure Coding Standard for Android Application Development

https://www.securecoding.cert.org/confluence/x/C4AiBw

セキュアな Android アプリ開発の情報源のひと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、公開済みのルールについても引き続き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は大歓迎です。上述の Wiki に直接コメントするか、もしくは、secure-coding@jpcert.or.jp にお送りいただければ、ルールの改善に役立てさせていただきます。

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、「8.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.執筆一覧」及び「13.開催セミナー等一覧」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 10095 件、インシデント件数ベースでは 8284 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 2414 件でした。前四半期の 2179 件と比較して 11%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などに対し、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 など）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/2013/IR_Report20131010.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 469 件で、前四半期の 287 件から 63%増加しました。また、前年度同期（273 件）との比較では、72%の増加となりました。
本四半期のフィッシングサイトの報告件数を、装っていたブランドが国内か国外かで分けた内訳を添えて[表 1-1]に示します。

[表 1-1 フィッシングサイトの国内・国外ブランド別の件数]

フィッシングサイト	7 月	8 月	9 月	合計 (割合)
国内ブランド	33	41	91	165(35%)
国外ブランド	73	68	78	219(47%)
ブランド不明(注 5)	21	25	39	85(18%)
月別合計	127	134	208	469(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などの理由により、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ています。フィッシングサイトのドメイン名には、7 月から 8 月はブランド名を装った文字列やアルファベット 4 文字に.asia、.pw、.cc などのトップレベルドメインを組み合わせたものが多く使用され、9 月はアルファベット 1 文字か同じ文字 2 文字の後が kiki.com となっているものが多く使用されていました。国内ゲーム会社を装ったフィッシングサイトの中には、国内通信事業者が動的に割り当てる IP アドレスを持ち、しかも、IP アドレスを付与した通信事業者が複数あって時間とともに移動したものがありました。また、このような IP アドレスを持つ国内ゲーム会社を装ったフィッシングサイトと同じ IP アドレスで、海外の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が存在していることも確認しています。

フィッシングサイトの調整先の割合は、国内が 56%、国外が 44%であり、前四半期(国内 54%、国外 46%)と比較して、国内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、2774 件でした。前四半期の 1847 件から 50%増加しています。

前四半期に引き続き、不審な iframe や難読化された JavaScript がページに挿入された Web サイトに関する報告が非常に多く寄せられています。改ざんされた Web サイトにアクセスすると、他の URL に誘導され、誘導先の php スクリプトによって、さらに複数のアプリケーションの脆弱性を使用した攻撃を行うサイトに誘導されることを確認しています。脆弱性が存在する古いバージョンの OS やアプリケーションがインストールされた PC が攻撃されると、マルウエアに感染して、PC に保存された様々な認証情報を窃取されたり、他のマルウエアをダウンロードされたりする可能性があります。改ざんの被害を受けた Web サイトの管理者から、不明な第三者による ftp の認証が記録されていたとの情報を複数いただいており、改ざんを許した一因として、Web サイトの管理に使用する PC が ftp などの認証情報を窃取するマルウエアに感染していたか、ftp のパスワードが容易に推測できるものであったなどの問題点が考えられます。

また、9 月中旬には Web サイトに侵入したことを誇示することを目的とした、海外のハッカーグループによる改ざんの報告も多く寄せられました。

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 改ざんなどのサイバー攻撃に関する情報を収集し、分析しています。これらの様々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なども併せて行い、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」（提供先限定）など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 26,000 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)などを通じて、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などについて、次のような注意喚起情報を発行しました。

発行件数：10 件　https://www.jpcert.or.jp/at/

2013-07-10　2013 年 7 月 Microsoft セキュリティ情報 (緊急 6 件含) に関する注意喚起
2013-07-10　Adobe Flash Player の脆弱性 (APSB13-17) に関する注意喚起
2013-07-19　Apache Struts の脆弱性 (S2-016) に関する注意喚起
2013-07-29　ISC BIND 9 サービス運用妨害の脆弱性 (CVE-2013-4854) に関する注意喚起
2013-08-14　2013 年 8 月 Microsoft セキュリティ情報 (緊急 3 件含) に関する注意喚起
2013-09-06　SIP サーバの不正利用に関する注意喚起
2013-09-11　2013 年 9 月 Microsoft セキュリティ情報 (緊急 4 件含) に関する注意喚起
2013-09-11　Adobe Flash Player の脆弱性 (APSB13-21) に関する注意喚起
2013-09-11　Adobe Reader 及び Acrobat の脆弱性 (APSB13-22) に関する注意喚起

2013-09-18　2013 年 9 月 Microsoft Internet Explorer の未修正の脆弱性に関する注意喚起

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 49 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。

2013-09-26　Internet Week 2013 のプログラム公開
2013-09-19　流行の話題に便乗した攻撃に注意
2013-09-11　MBSA 2.3 Preview 版の公開
2013-09-04　Java 実行環境を最新に
2013-08-28　マイクロソフトが MD5 ハッシュの利用制限プログラムを公開
2013-08-21　SECCON 2013
2013-08-14　Microsoft Office 2010 SP2 提供開始
2013-08-07　EMET 4 の日本語ユーザガイド公開
2013-07-31　PHP 5.3 系最後のリリース
2013-07-24　Apache HTTP Server 2.0 最後のリリース
2013-07-18　EMET 4.0 正式リリース
2013-07-10　ICANN、"Initial Report from the EWG on gTLD Directory Services" を公開
2013-07-03　新しい CVE 番号体系が決定

1.2.1.3. 早期警戒情報

JPCERT/CC では、国民の社会活動に大きな影響を与えるインフラ、サービス及びプロダクトなど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。

【Apache Struts の脆弱性】
2013 年 7 月、Apache Software Foundation より Apache Struts 2 に関する脆弱性情報が公開されました。当該脆弱性は、Apache Struts の HTTP リクエスト内の OGNL※コードの処理に関するもので、Apache Struts を使用するアプリケーションを実行するサーバに対して、攻撃用 OGNL コードを含む HTTP リクエストを送りつけられた場合、任意の Java コードを実行されたり、Java コードを用いて任意の OS コマンドなどを実行されたりする可能性がありました。
当該脆弱性は悪用が容易で、脆弱性公開の数日後には複数の攻撃ツールがインターネット上に公開されていることが確認され、国内のセキュリティベンダからは国内の組織に対して当該脆弱性を狙った攻撃が急増しているとの情報が公開されました。

JPCERT/CC でも、「Apache Struts の脆弱性(S2-016)に関する注意喚起」を公開し、サーバ管理者や、Web サイト開発者などに対し広く注意を呼びかけました。また、公開された実証コードの検証結果、ログ情報からの攻撃検知方法や回避策についてまとめた「Apache Struts の脆弱性(S2-016)に関する検証レポート」を国内の重要インフラ事業者等に対して提供しました。

※ OGNL：Java オブジェクトのプロパティにアクセスしたりメソッドを呼び出したりすることが出来る言語

1.3. インターネット定点観測システム

インターネット定点観測システムは、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します。JPCERT/CC では、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を目的にインターネット定点観測システムを運用しています。観測情報の一部は、ネットワーク管理者や研究者向けの参考情報として、 JPCERT/CC Web ページなどでも公開しています。

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

1.3.1. インターネット定点観測システム観測データに基づいたインシデント対応事例

JPCERT/CC では、TSUBAME プロジェクト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、攻撃ツールなど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。本四半期において特筆すべきマルウエア感染や侵入などのインシデント事例について、JPCERT/CC の対応を含めて紹介します。

JPCERT/CC では、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 サーバ宛の特徴的なパケットが本四半期も観測されました。JPCERT/CC では、IP アドレスの管理者に観測システムで収集したログ情報を提供し、SSH サーバを探索するスキャンや辞書攻撃などを行う不審なツールが設置されていないかどうかの確認を依頼しました。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、サーバ上で SSH サーバを探索するためのツールや、リモートコントロール用のプログラムが動作している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。

1.3.2. インターネット定点観測システム観測データに基づいた情報発信

本四半期も、引き続き SIP サービス用ポートへのスキャンが増加傾向にありました。これらは SIP サーバをスキャンするためのツールによるものであり今後もこの攻撃が継続すると想定されることから、JPCERT/CC では、SIP サーバや SIP 対応機器などの不正利用防止を目的として、次の注意喚起を公開しました。

SIP サーバの不正利用に関する注意喚起
https://www.jpcert.or.jp/at/2013/at130036.html

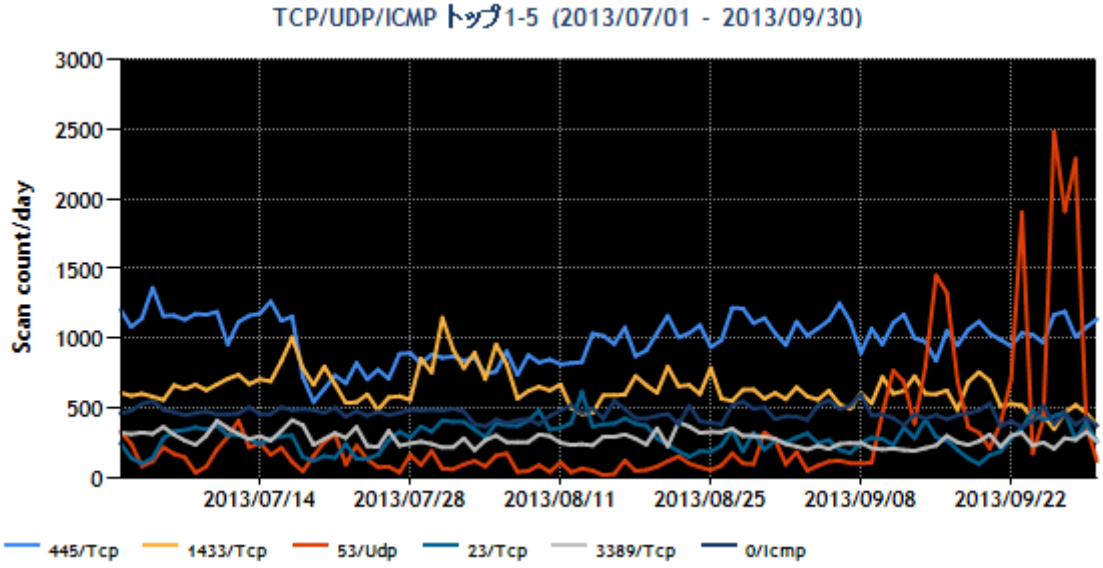
1.3.3. ポートスキャン概況

インターネット定点観測システムで観測されたポートスキャンの頻度や内訳の推移をグラフとして JPCERT/CC の Web ページで公開しています。宛先ポート別グラフは、各センサーに記録された宛先ポートごとに観測されたパケット数を表しています。

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

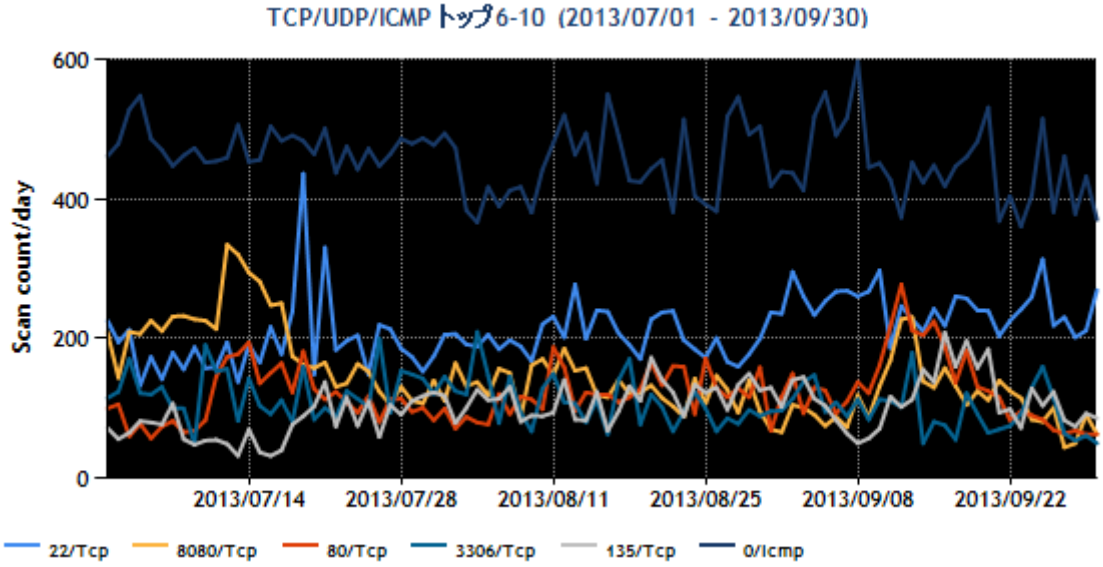
本四半期に定点観測システムで観測された宛先ポート別の上位 1 位～5 位及び 6 位～10 位のそれぞれについて、パケット数の時間的推移を[図 1-1]と[図 1-2]に示します。

- 宛先ポート別グラフ トップ 1-5 (2013 年 7 月 1 日-9 月 30 日)



[図 1-1 宛先ポート別グラフ トップ 1-5]

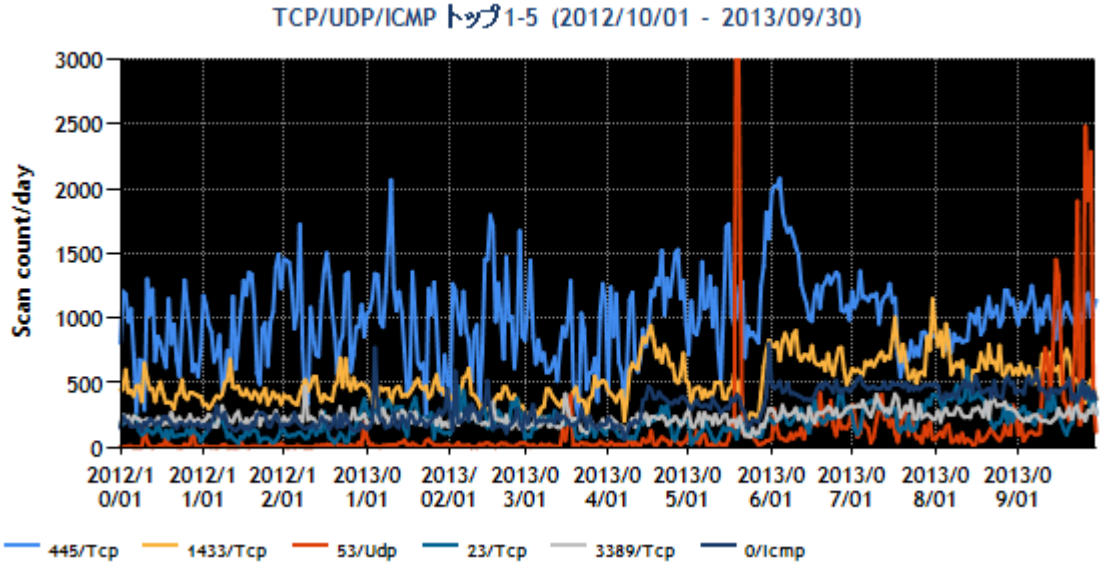
- 宛先ポート別グラフ トップ 6-10 (2013 年 7 月 1 日-9 月 30 日)



[図 1-2 宛先ポート別グラフ トップ 6-10]

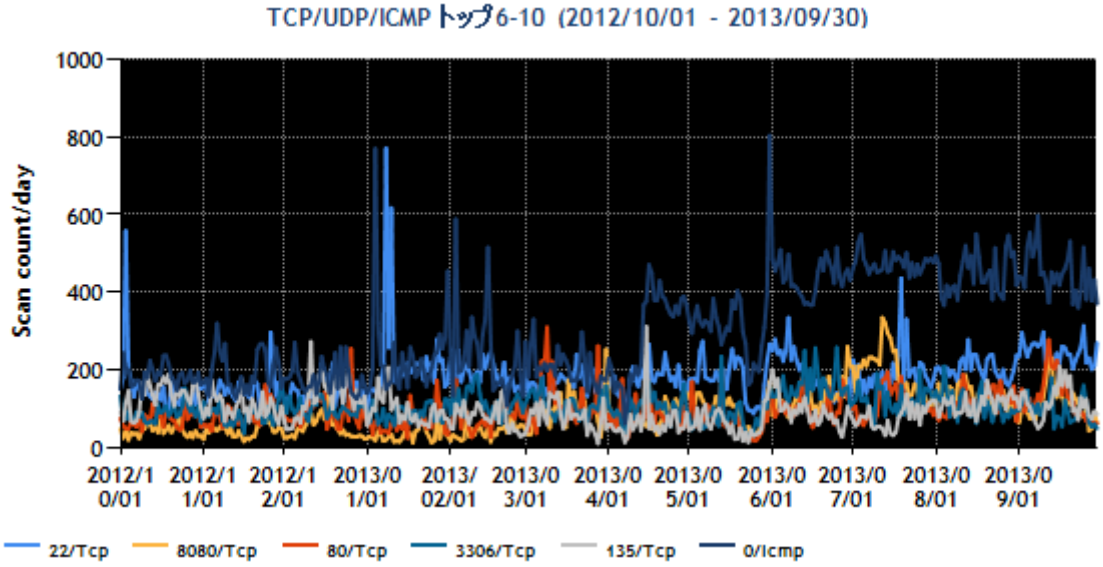
また、より長期間のパケット数の推移を見るため、過去 1 年間(2012 年 10 月 1 日から 2013 年 9 月 30 日まで)における、宛先ポート別の上位 1 位～5 位及び 6 位～10 位のそれぞれについて、パケット数の時間的推移を[図 1-3]と[図 1-4]に示します。

- 宛先ポート別グラフ トップ 1-5 (2012 年 10 月 1 日-2013 年 9 月 30 日)



[図 1-3 宛先ポート別グラフ top1-5]

- 宛先ポート別グラフ トップ 6-10 (2012 年 10 月 1 日-2013 年 9 月 30 日)



[図 1-4 宛先ポート別グラフ トップ 6-10]

順位に変動はありますが、これまでと同様、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 サーバなど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が多く観測されています。

2. 脆弱性関連情報流通促進活動

JPCERT/CC は、ソフトウエア製品利用者の安全確保を図ることを目的として、発見された脆弱性情報を適切な範囲に適時に開示して製品開発者による対策を促進し、用意された対策情報と脆弱性情報を脆弱性情報ポータル JVN （Japan Vulnerability Notes ; 独立行政法人情報処理推進機構（IPA）と共同運営）を通じて公表することで広く注意喚起を行う活動を行っています。さらに、脆弱性を作りこ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。

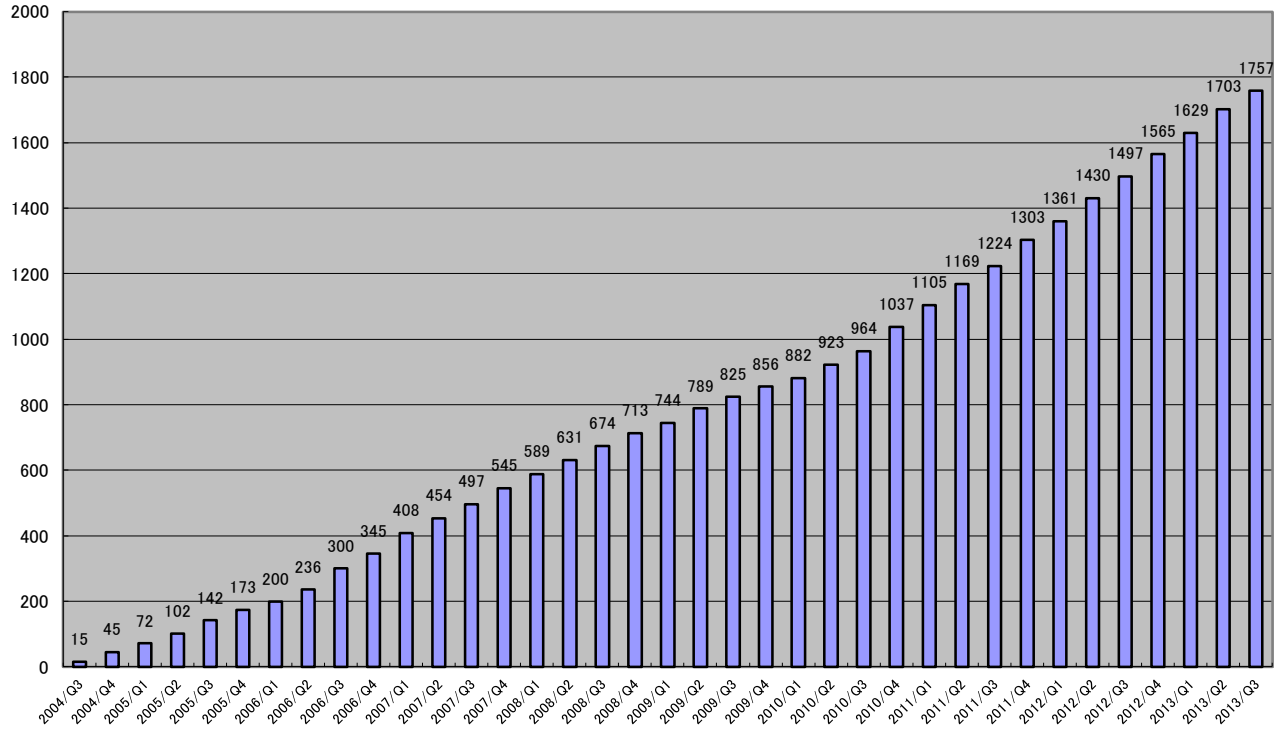
2.1. Japan Vulnerability Notes (JVN) において公表した脆弱性情報および対応状況

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」（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、本基準を踏まえてとりまとめられた「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など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（たとえば、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（たとえば、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などが含まれます。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（たとえば、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 54 件（累計 1757 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/

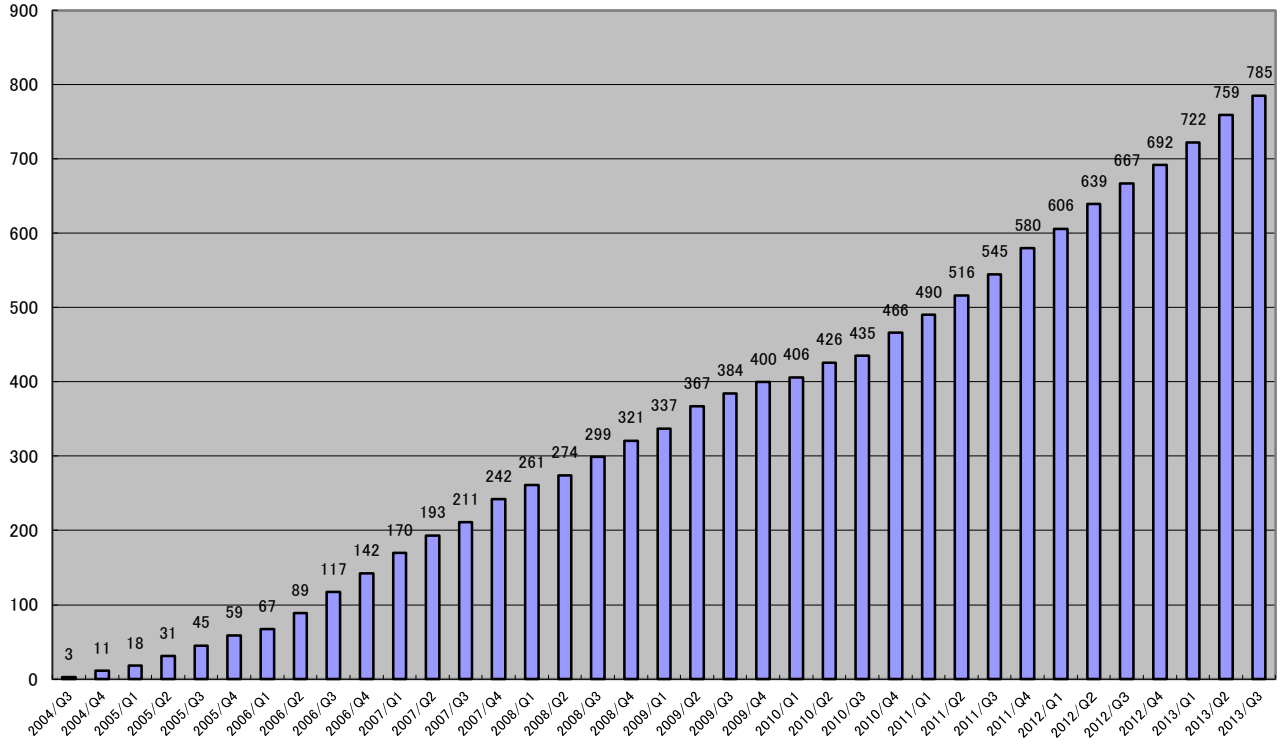


[図 2-1　JVN 公表累積件数]

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 26 件(累計 785 件)で、累計の推移は[図 2-2]に示すとおりです。例年、7 月～9 月期は、夏期休暇等の影響もあり、公表件数が他の四半期と比較して少なくなる傾向にあります。公表した 26 件のうち 12 件（約 46%）が海外製品開発者の製品でした。また、本四半期においては海外の研究者から JPCERT/CC へ直接、2 件の脆弱性情報の届出がありました。届け出られた脆弱性が存在する製品は、日本国内においても広く使用されている著名な仮想化用ソフトウエアで、脆弱性対応を行うのは米国本社だけであったため、米国本社との国際調整を経て公開に至っています。このように海外の製品開発者のみならず発見者にも本制度への理解が浸透し、協力が得られるようになってきていると言えます。

昨年度から、Android およびその関連製品やモバイル端末関連製品の届出が増加傾向にあります。本四半期の公表においても、 Android 向けアプリケーションに関する脆弱性情報が 3 件（全体の 16%に相当）ありました。

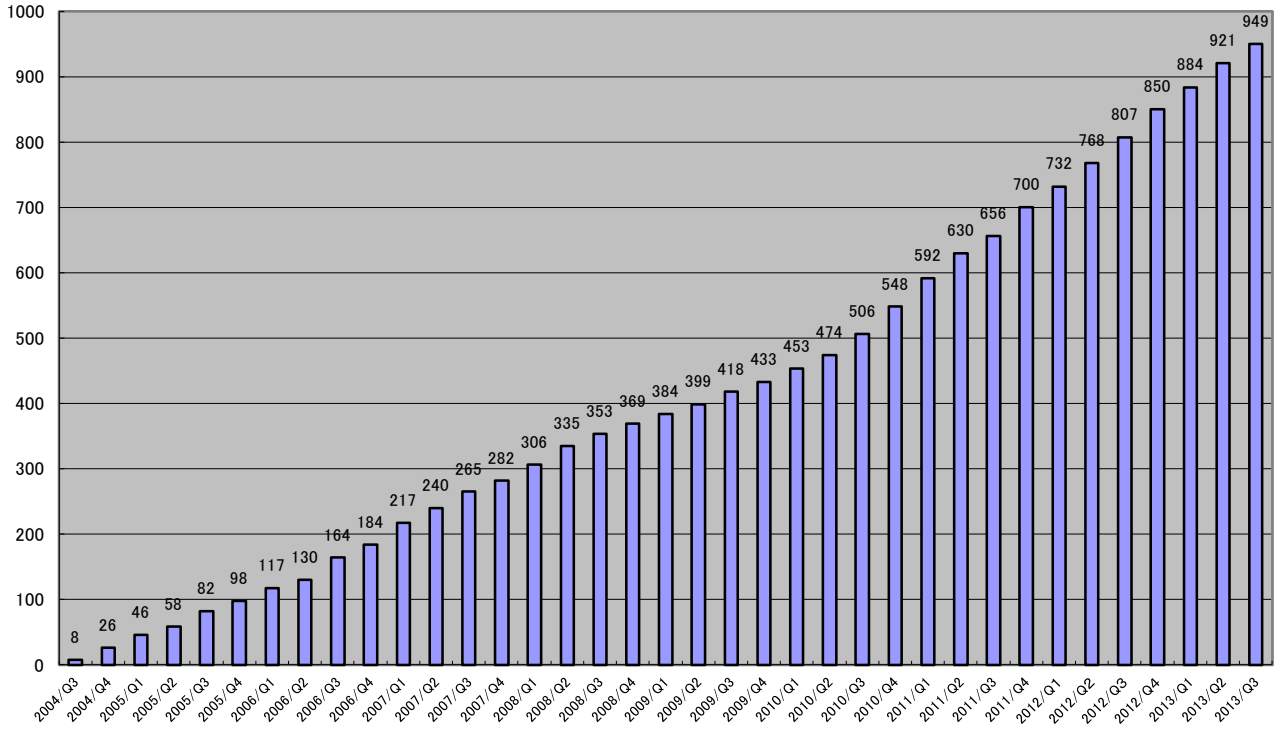
モバイル関連製品以外で公表数が多かった製品としては、海外 OSS 製品が 3 件、グループウエアが 3 件、E コマース製品が 2 件、仮想化用ソフトウエアが 2 件、データベース製品が 2 件でした。なお、前四半期と同様に本四半期においても、製品開発者からの自社製品の脆弱性情報の報告をもとに JVN で公表した事例が 5 件ありました。JPCERT/CC は、今後も引き続き国内外の関係者との調整を行い、脆弱性問題への速やかな対応の促進に努めてまいります。



[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、28 件（累計 949 件）で、累計の推移は[図 2-3]に示すとおりです。28 件のうち 3 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 25 件は、Oracle Javadoc の注意喚起が 1 件、DELL のサーバ関連製品および BIOS に関する注意喚起が 2 件、Hewlett-Packard（HP）のサーバ関連製品に関する注意喚起が 1 件、Apple による自社製品に関する脆弱性情報の届け出によるものが 4 件ありました。本四半期は、Cisco、VERIZON、Huawei などの海外製品開発者が提供するネットワーク機器に関する脆弱性情報の公表が 4 件と比較的多かったのが特徴的でした。



[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、しかるべき手続きを踏んでも調査と対策をしていただくべき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」として公表することになりました。これまでに 128 件（製品開発者数としては 85 件）が掲載され、16 件（製品開発者の数としては 11 件）の調整が再開でき、脆弱性関連情報の取扱における「滞留」の解消に一定の効果をあげています。

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 3 件でした。連絡不能開発者一覧の公表からちょうど 2 年が経過した本四半期末日時点で、合計 110 件の連絡不能開発者案件が引続き掲載されており、継続して製品開発者や関係者からの連絡および情報提供を呼びかけています。

こうした対応によってもなお調整ができない場合に関し、脆弱性の存在が検証できた製品について、その内容を JVN で公表するための手順や手続き等を、IPA および関係機関とともに検討しており、体制整備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 など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および対応状況の集約、脆弱性情報の公表時期の設定などの調整活動を連携して行っています。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、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、取扱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などからも注目されています。
本四半期においては、オーストラリアの研究者から AusCERT（オーストラリア）を経由し、JPCERT/CC に、2 件の脆弱性の届出がありました。情報セキュリティ早期警戒パートナーシップに基づく届出として取り扱われ、約 2 ヶ月の調整を経て JVN での公表に至りました。これまでにも、海外在住の研究者から、直接 JPCERT/CC に脆弱性情報が届け出られ、製品開発者との調整を経て JVN での公表に至った事例は多くありますが、AusCERT との脆弱性情報ハンドリングにおける連携は、これが初の事例でした。

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 25 件に対し CVE 識別子が付与されており、そのうち 18 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 および 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

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扱い状況等の情報交換を行うなど、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毎の届出状況については、次の URL をご参照ください。

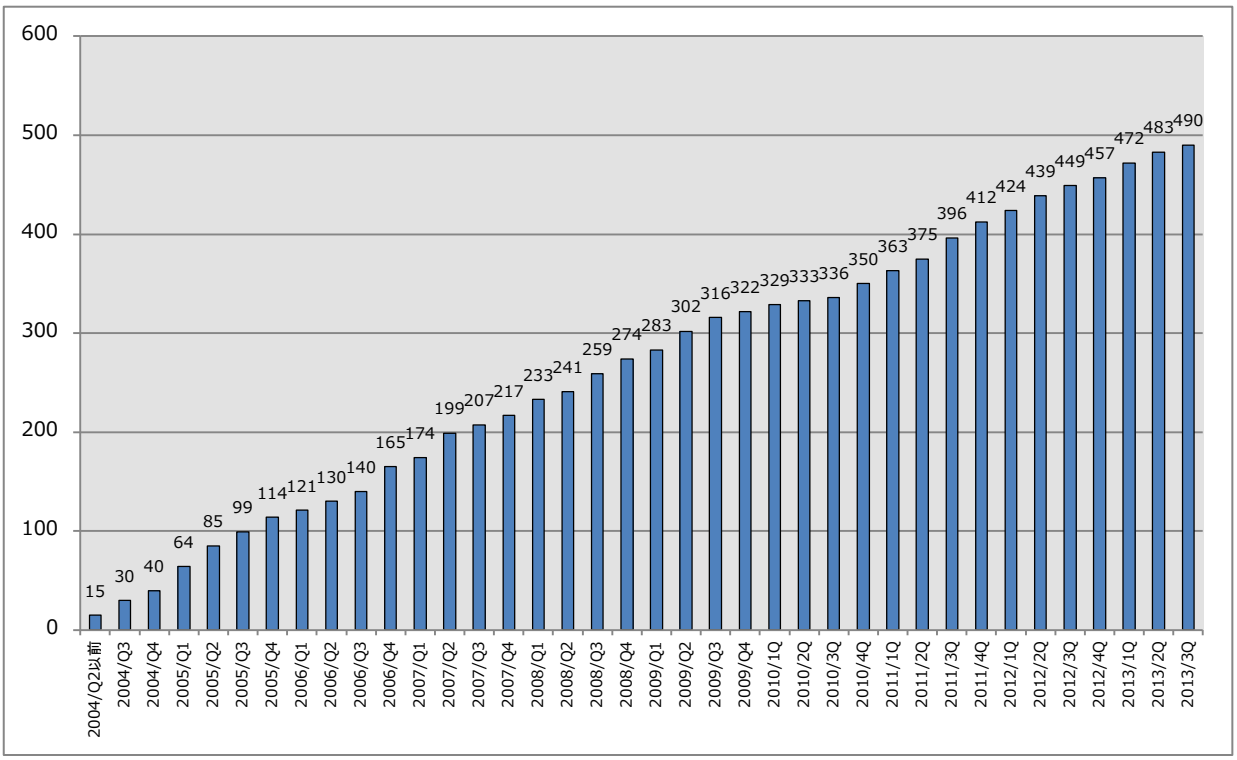
独立行政法人情報処理推進機構(IPA) 脆弱性対策
http://www.ipa.go.jp/security/vuln/

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、製品開発者の皆様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 9 月 30 日現在で 490 社となっています。

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. オープンソースカンファレンス 2013 Kansai@ Kyoto で講演

8 月 2 日､3 日に京都リサーチパークで開催されたオープンソースカンファレンス 2013 Kansai @ Kyoto 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」と題した講演を行いました。

本講演には 30 名を越える方々にご参加いただき､6 月に公開した Java アプリケーション脆弱性事例解説資料の紹介を行いました。限られた講演時間のなかで、資料の位置づけや各資料で扱う脆弱性を簡単に説明する内容でしたが、講演後にも様々な質問やご意見をいただくなど、多くの方から関心を寄せていただいていることをひしひしと感じることができました。

本講演で使用した資料はオープンソースカンファレンスのページ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
http://www.ospn.jp/osc2013-kyoto/pdf/osc2013kyoto_jpcert.pdf

2.5.2. Android セキュアコーディングルールを作成中

JPCERT/CC はカーネギーメロン大学ソフトウエア工学研究所(CMU/SEI)とオラクル社が協同で開発した「Java セキュアコーディングスタンダード」の日本語版を JPCERT/CC の Web サイトに公開し

(https://www.jpcert.or.jp/java-rules/)、併せて各コーディングルールの品質向上に貢献する活動をこれまで行ってきました。
本年度も引き続き 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・研究を行っており、調査の過程で得られた知見をセキュアな Android アプリ開発に役立てていただくために、コーディングルール化する作業を進めています。作成したコーディングルールは、CMU/SEI の協力のもと、Java セキュアコーディングスタンダードに新規カテゴリー「50. Android」を設け、その中で順次公開しています。本四半期は 6 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

CMU/SEI とはこれまでも、セキュアコーディングに関する研究や啓発活動を協力して行ってきましたが、より多くのエキスパートの意見を取り入れオープンに開発を進めるために、SEI の Wiki プラットフォームを活用しています。
各ルールのページでは、脆弱なコード(アンチパターン)とその修正例を紹介するとともに、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。
また、ルール作成作業と並行して、既存の Java セキュアコーディングルールの中で Android アプリ開発にも適用可能なルールの一覧のアップデートを進めています。

Application of CERT Oracle Secure Coding Standard for Android Application Development
https://www.securecoding.cert.org/confluence/x/C4AiBw

セキュアな Android アプリ開発の情報源のひと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、公開済みのルールについても引き続き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は大歓迎です。Wiki に直接コメントするか、もしくは、secure-coding@jpcert.or.jp にお送りいただければ、ルールの改善に役立てさせていただきます。

2.5.3. Java アプリケーションの脆弱性事例解説資料を追加

前四半期に、Java 言語で書かれたアプリケーションの脆弱性事例に関する解説資料を 5 件公開しましたが、本四半期は、さらに 5 件を公開しました。

1. Apache ActiveMQ における認証処理不備の脆弱性(AMQ-1272)
2. Apache Commons の HttpClient における SSL サーバ証明書検証不備(CVE-2012-5783)
3. Spacewalk におけるクロスサイトリクエストフォージェリ(CSRF)の脆弱性(CVE-2009-4139)
4. Apache Tomcat におけるクロスサイトリクエストフォージェリ(CSRF)保護メカニズム回避の脆弱性(CVE-2012-4431)
5. Apache Axis2 における XML 署名検証不備(CVE-2012-4418)

セキュアな Java アプリケーションの開発を目指すには、すでに知られている脆弱性の具体例を理解し、それを反面教師として同じ失敗を繰り返さないようにすることが重要です。Java 言語によるセキュアなプログラムを開発するためのコーディング規約「Java セキュアコーディングスタンダード CERT/Oracle 版」(https://www.jpcert.or.jp/java-rules/)や、Java セキュアコーディングのセミナー資料とともに、本資料を自習や勉強会などの参考資料としてご活用ください。

Java アプリケーション脆弱性事例解説資料
https://www.jpcert.or.jp/securecoding/materials-java-casestudies.html

2.5.4. セキュアコーディング関連記事を連載中

情報流通対策グループ脆弱性解析チームのメンバは各種ウェブマガジンにおいてセキュアコーディング関連の連載を担当しています。本四半期は、次の記事を執筆しました。

アットマーク・アイティ連載『もいちど知りたい、セキュアコーディングの基本』
第 5 回「見落としがちな整数関連の脆弱性（後編） (1/2)」(公開： 8 月 1 日、執筆：久保正樹)
http://www.atmarkit.co.jp/ait/articles/1307/29/news006.html

2.5.5. セキュアコーディング 出張セミナー

JPCERT/CC では、ソフトウエア製品等の開発を行う企業・組織を対象に、セキュアコーディングに関する出張セミナー（有償）の実施を承っています。マネジメント層へのセキュリティ啓発や新人研修のメニュー等としてもご利用いただけます。C/C++言語におけるセキュアコーディングセミナーに加え、Java 言語版および Android アプリケーション開発に関するセキュアコーディング出張セミナーも提供しています。

※出張セミナーのご依頼、お問合せは、secure-coding@jpcert.or.jp までご連絡下さい。

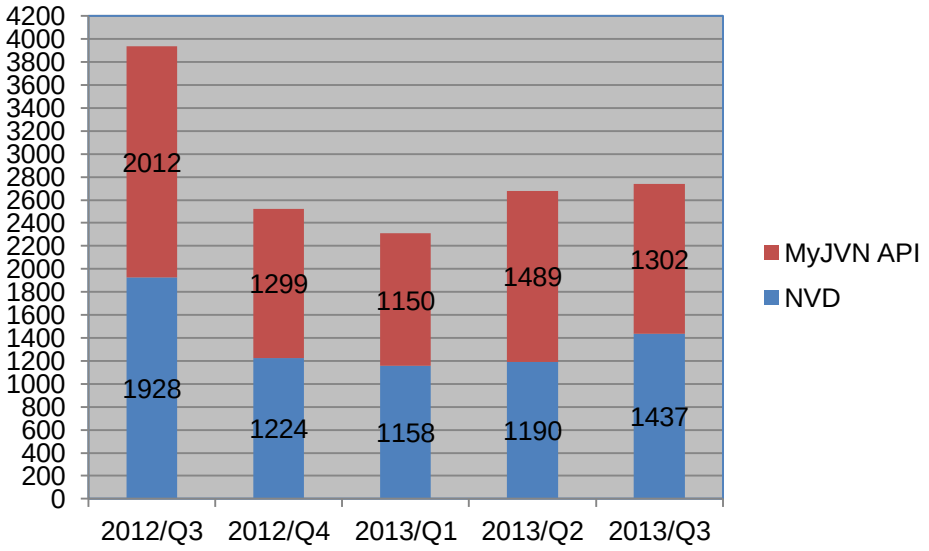
2.6. VRDA フィードによる脆弱性情報の配信

JPCERT/CC は、大規模組織の組織内 CSIRT などでの利用を想定して、KENGINE など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 URL を参照下さい。

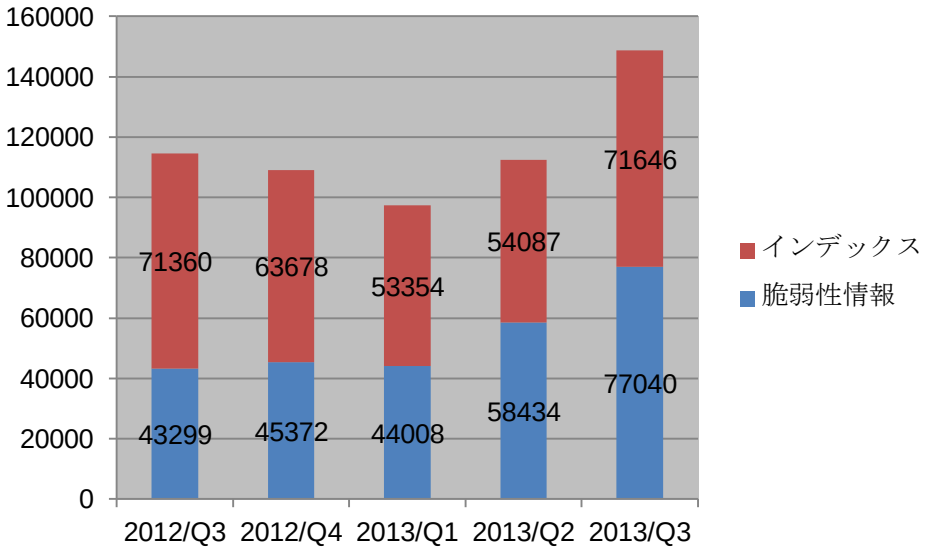
VRDA フィード 脆弱性脅威分析用情報の定型データ配信
https://www.jpcert.or.jp/vrdafeed/index.html

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 の二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。

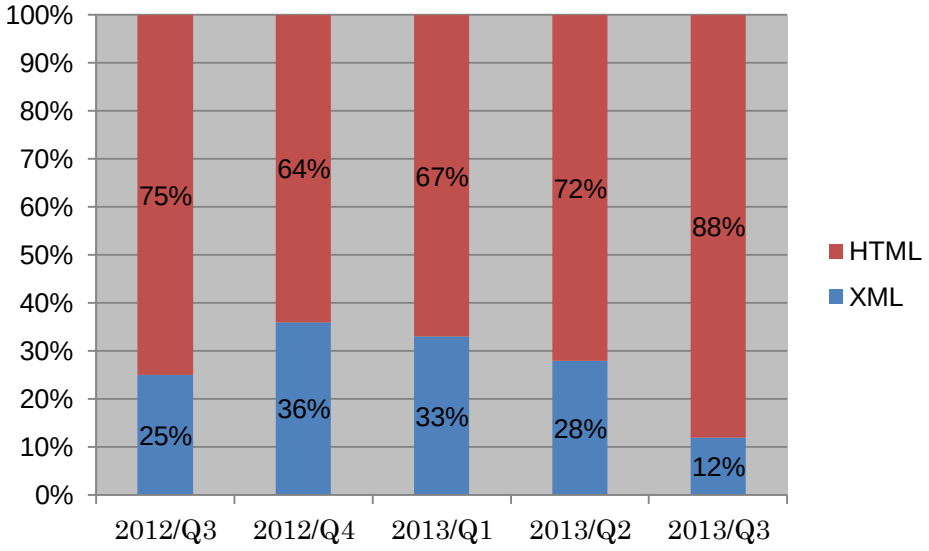


[図 2-5 VRDA フィード配信件数]



[図 2-6 VRDA フィード利用件数]

[図 2-6] に示したように、前四半期と比較して VRDA フィードインデックスの利用数は約 30%の増加が見られました。同じく、脆弱性情報の利用数も約 30%増加しています。



[図 2-7 脆弱性情報のデータ形式別利用割合]

[図 2-7] 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減少しました。

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、実態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始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、国内外で同様のアーティファクト分析を行っている多数の分析技術者や分析能力の向上を目指す技術者と情報交換を行い、協力しながら総合的な分析能力を高めて行くための活動が重要であると考え、これらの活動にも力を注いでいます。

3.1. SecCap「リスクマネジメント演習」

JPCERT/CC は SecCap における演習科目のひとつであるリスクマネジメント演習の講義の一部を担当しました。SecCap は、文部科学省の「情報技術人材育成のための実践教育ネットワーク形成事業」において本年度から開始されている「分野・地域を越えた実践的情報教育協働ネットワーク」（通称 enPiT）のセキュリティ分野プロジェクトです。
この演習は、昨年度まで IT Keys の演習科目として 4 大学院から受講生を迎えて開催されてきたリスクマネジメント演習をベースとする内容のコースで、本年度は SecCap の演習科目になったことで、6 大学院から 25 名の受講生を迎えて開催されました。JPCERT/CC が担当した講義では、インシデント発生後の調査を想定した演習シナリオを使って受講生に解析作業を体験していただきました。

JPCERT/CC の活動においてもインシデント発生後のコンピュータの解析作業に対する需要は増しており、そのような技術を持った技術者の育成が急務となっています。また、そういった解析作業を適切にマネージメントできる能力も必要です。SecCap への参加を通して、セキュリティ分野での活躍を目指す受講生のみなさんに、この分野に求められている人材や能力についてお伝えすることも JPCERT/CC の重要な役割であると考えています。

enPiT-Security【SecCap】
http://www.seccap.jp/

情報技術人材育成のための実践教育ネットワーク形成事業
http://www.mext.go.jp/a_menu/koutou/kaikaku/itjinzai/

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などを収集し、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 3 回（8 月 2 日、8 月 30 日、9 月 30 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 305 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およ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 0 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 562 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 や J-CLICS の配布を行なっています。本四半期は、JPCERT/CC に対して、SSAT に関しては 3 件、J-CLICS に関しては 16 件の利用申込みがありました。直接配布件数の累計は、SSAT が 149 件、J-CLICS が 167 件となりました。

4.5. 医療機器のサイバーセキュリティ課題への対応

6 月 13 日に米国 ICS-CERT が「医療用機器におけるハードコードされたパスワード」と題した注意喚起を、また同日これに関連して米国 FDA (食品医薬品局)が「医療用電子機器と病院ネットワークに関するサイバーセキュリティ」と題した安全通知を公表しました。「制御システム用機器にしばしば見られるものと似た脆弱性が約 300 種類の医療用機器にも内在している可能性がある」との報告を制御システムセキュリティ研究者が米国 ICS-CERT に行ったことに端を発した動きでした。疑いをもたれたものの中に日本ベンダの製品が含まれていたため、JPCERT/CC では、当該ベンダとの調整を行い脆弱性にはあたらないとの結論にいたりました。一方、出荷後の製品に対する脆弱性の報告があった場合におけるベンダとしての一般的な対応の在り方などについて、主な医療用機器の業界団体に説明会の開催をお願いし、ベンダの皆様へご説明しました。。

4.6. 講演活動

9 月 15 日に名古屋大学で行われた SICE Annual Conference 2013 にて「Analysis and Consideration on Mockup ICS Environment for Cyber Incident Response Training」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) および取扱手順(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部分を含む、ベンダ内部での対応を規定することになっています。
「脆弱性情報の開示」については、国際標準草案(DIS： Draft of International Standard)に対して修正を求める合計 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)の取扱いが 4 月下旬に開催された SC27 国際会議において審議され、その合意に基づいてエディタに指名されているカナダの委員が本標準の改訂作業を行いました。メーリングリストを通じて関係者に改訂後の草案を非公式にチェックするようエディタから依頼があり、JPCERT/CC も、この依頼を受け、情報規格調査会 SC27WG3 小委員会のメンバとも相談の上、23 項目からなる修正必要箇所の一覧

を 7 月上旬に提出しました。これらのコメントを踏まえた修正の後に非公式なチェックが再度依頼されるはずでしたが、その作業が割愛されて、明らかな誤りを含んだ草案が 7 月中旬に国際標準最終草案(FDIS : Final draft of International Standard)として SC27 事務局に提出されました。ITTF と呼ばれる組織が査閲した後に国際投票に付されるはずですが、その後の動きが止まっています。
遅れて開発がスタートした「脆弱性取扱手順」については、国際標準草案(DIS： Draft of International Standard)に対する国際投票の結果、ただちに国際標準とすべきものとして承認されました。いずれも軽微な合計 9 件(日本から 3 件、ルクセンブルグから 1 件、英国から 5 件)のコメントについて、4 月下旬に開催された SC27 国際会議で取扱いが話し合われ、その審議結果に基づいて、エディタに指名されている米国の委員が改訂作業を行ないました。これを国際標準として発行する旨の通知が、7 月下旬に SC27 事務局から発行されて標準策定作業が終結、後は正式の文書としての発行を待つのみとなりました。
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国内審議団体である情報規格調査会を通じて、我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 つの標準から成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)で開催される SC27 国際会議に向けて準備された 3rd Working Draft の段階にあるこれら 3 つの標準に対する日本のコメントを作成し、SC27 WG4 国内小委員会での承認を経て、9 月 13 日に SC27 事務局に提出しました。仁川会議には日本の代表団の一員として参加する予定です。
インシデント管理の原理を規定する 27035-1 の草案には、エディタが明示的にコメントを求める覚え書きを随所に記していました。それに答える形でコメントを作成し、計 17 件のコメントをまとめました。27035-1 は、27035:2011 をベースに作成されていることから、構成や内容に大きな破綻もなく、ドキュメントとして比較的順調に仕上がっています。
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、章の構成上の問題や、基本概念を誤って使用しているために不明瞭になっている箇所が散見されるなどの問題がありました。これらの問題の修正に関する 15 件のコメントをまとめています。
インシデント対応のオペレーションのガイドラインとなる 27035-3 については、章の構成と技術的内容に関する 25 件のコメントを提出しました。また、本標準のスコープがインシデント対応を含むインシデントハンドリング全体に及ぶことから、標準のタイトルを内容に即したものすべく、Guidelines for incident handling に変更する提案を行っています。

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国内審議団体である情報規格調査会における活動を通じて、引き続き、この国際標準が我が国の CSIRT の取組みと整合性のと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. モンゴルにおける CSIRT 構築支援活動(2013 年 8 月 12 日-16 日)

モンゴルにおける CSIRT 構築支援の一環で、MonCIRT および Mongolian National Data Center (MNDC) が主催した Information Security 2013 Conference and Training に 2 名の講師派遣を行いました。本カンファレンスおよびトレーニングは、モンゴル政府関係者や民間事業者の情報セキュリティに対する意識啓発や技術力向上を目的として、8 月 13 日と 14 日の 2 日間、開催されました。8 月 13 日のカンファレンスには、約 100 名の聴衆が集まり、JPCERT/CC から「Internet Security and CSIRT's Mission」および「Network and Incident Monitoring」と題する講演を行いました。8 月 14 日のトレーニングでは、MNDC のスタッフ等約 50 名に対して、インシデントハンドリングおよびネットワークフォレンジックのハンズオン研修を行いました。
また、モンゴル訪問の機会を捉え、National Security Council (NSC) や主要な ISP 等を訪問し、モンゴルの情報セキュリティを担うキーパーソンと意見交換を行いました。

[図 6-1　カンファレンス参加者集合写真]

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、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など、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）として様々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 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 8 月 5 日、8 月 26 日に電話会議を行い、また 9 月 23 日から 24 日にインドネシアのジョグジャカルタに集まり、今後の APCERT の運営方針等について議論を行いました。JPCERT/CC

は議長チームおよび事務局として、本会議の主導およびサポートを行いました。

6.2.1.2. APCERT Technical Workshop on Security への講師派遣 (2013 年 9 月 23 日-24 日)

9 月 23 日から 24 日にインドネシアのジョグジャカルタで開催された APCERT Technical Workshop on Security に講師を 2 名派遣しました。本イベントは、APCERT の Steering Committee メンバで、研修分野を担当しているインドネシアの ID-SIRTII/CC が、APCERT 加盟チームのスタッフの技術力向上を目指して主催したもので、APCERT としては初の試みでした。
JPCERT/CC は 24 日のネットワークフォレンジックのハンズオン研修の講師を担当しました。同研修には、APCERT の加盟チームやインドネシアの IT 技術者を中心に約 20 名の受講者が集まりました。
APCERT Technical Workshop on Security の詳細については、次の URL をご参照ください。

APCERT Technical Workshop on Security
http://apcert-tws2013.idsirtii.or.id/

[図 6-2　研修の風景]

6.2.1.3. APCERT と他組織間との連携

6.2.1.4. APEC TEL 48 SPSG への参加　(2013 年 9 月 17 日-18 日)

APEC 地域の各国で情報電気通信分野を担当している政府機関を中核とするワーキンググループである APEC TEL (APEC Telecommunications and Information Working Group) の会合が米国のハワイで開催されました。JPCERT/CC は、APEC TEL の Security and Prosperity Steering Group (SPSG) が主催する複

数のセッションに参加しました。9 月 17 日は Workshop on Botnets に参加し、APCERT のボットネットクリーンアップに関する構想や取組み、および APCERT の複数の加盟国におけるボットネット対策活動等を紹介しました。翌 18 日は、APEC-OECD Symposium on Security Risk Management in the Internet Economy にパネリストとして参加し、OECD が主導するセキュリティリスク評価指標の策定プロジェクトの概要を報告しました。

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。FIRST および 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

6.2.2.1. FIRST Technical Colloquium in Yogyakarta (2013 年 9 月 25 日-26 日)

9 月 25 日から 26 日にインドネシアのジョグジャカルタで開催された FIRST Technical Colloquium (FIRST TC) に JPCERT/CC のスタッフが参加しました。FIRST TC は、FIRST 加盟 CSIRT 間での情報共有等を目的として、世界各地で年に数回開催されています。JPCERT/CC は、Steering Committee メンバの一員として、FIRST TC のトレーニング講師の手配・調整を行いました。また、JPCERT/CC から参加したスタッフは、「Establishing CSIRT」「Introduction to Volatility」の研修に参加し、技術向上を図るとともに、参加者と情報共有を行いました。FIRST Technical Colloquium in Yogyakarta の詳細については、次の URL をご参照ください。

FIRST Technical Colloquium in Yogyakarta
http://tcfirst2013.idsirtii.or.id/

6.2.3. 第一回 日中韓 サイバーセキュリティインシデント対応年次会合 (2013 年 7 月 30 日-31 日)

7 月 30 日から 31 日に、中国・上海において「第一回 日中韓 サイバーセキュリティインシデント対応年次会合」が開催されました。本会合には、日中韓の National CSIRT (JPCERT/CC、CNCERT/CC、KrCERT/CC) のリーダおよび担当職員が出席し、日中韓 3 ヵ国に影響を及ぼす重大なサイバーセキュリティインシデント対応におけるこれまでの連携の実績を確認するとともに、今後、これまで培ってきた連携関係を更に強化して、重大なインシデントに対するより効果的かつ効率的なコーディネーションを目指すことを確認しました。
情報セキュリティインシデント発生時における連携や情報の取り扱いに関するルール等を確認するため、これまで JPCERT/CC は CNCERT/CC と KrCERT/CC のそれぞれと 2 ヵ国間で覚書 (MOU) を結んでい

ましたが、両組織と協議の上 2011 年 12 月にこれを 3 ヵ国間の MOU へと拡張しました。本年次会合は、この MOU に基づく、各チームのトップが参集する初の会合でした。
三者は会合後、共同声明を発表し、重大なインシデントによる被害の軽減化に向けて連携・協力を強化すること、また、サイバー空間上の衛生レベルの向上とサイバーエコシステムの改善を通じて、域内のサイバー脅威リスクの低減に引き続き貢献する方針を表明しました。

ステートメントの原文（英語）については、次の URL をご参照ください
https://www.jpcert.or.jp/english/pub/pr.html
ステートメントの日本語抄訳については、次の URL をご参照ください
https://www.jpcert.or.jp/press/2013.html

6.2.4. 2013 APISC Security Training Course 参加 (2013 年 7 月 8 日-12 日)

韓国のソウルにおいて開催された 2013 APISC Security Training Course に JPCERT/CC のスタッフが参加しました。本研修は、CSIRT オペレーション等に関する知識の習得を目的として韓国の Korea Internet & Security Agency (KISA) および KrCERT/CC が主催したもので、アジアやアフリカ地域の情報セキュリティ関係者が受講生として招かれました。日本のインターネットセキュリティへの取組み状況等についての発表を行うとともに、参加者間で CSIRT 構築・強化やインシデント対応のあり方等について議論を行いました。

6.2.5. CSIRT インディケーター・ワーキングセッションへの参加と専門家招へい (2013 年 8 月 28 日-29 日)

経済協力開発機構 (OECD) では、各国の CSIRT の協力を得ながら、国際的に比較することが可能なセキュリティリスク評価指標の策定を進めています。JPCERT/CC はこの活動を支持し協力しています。JPCERT/CC のスタッフは、8 月 28 日から 29 日にワシントン D.C.で開催された「CSIRT インディケーター・ワーキングセッション」に参加するとともに、同セッションに OECD より専門家 3 名を招へいし、指標策定に向けた議論を行いました。

6.2.6. 「政策担当者のためのサイバーセキュリティ・セミナー」への参加 (2013 年 9 月 6 日)

9 月 6 日にインドネシアの ASEAN 事務局において、ASEAN 日本代表部および ASEAN 事務局の共催による「政策担当者のためのサイバーセキュリティ・セミナー」が開催され、JPCERT/CC のスタッフが講師として参加しました。本セミナーには、ASEAN 事務局、ジャカルタ駐在の ASEAN 諸国の外交団、インドネシアの政府関係者、研究者及び企業関係者等の 90 名以上が参加し、JPCERT/CC はサイバーセキュリティ分野における官民連携および国際連携の必要性と課題等に関する講演を行いました。
なお、本セミナーは日 ASEAN 友好協力 40 周年記念行事の一環として行われたもので、9 月 12 日から 13 日に東京で開催された「日 ASEAN サイバーセキュリティに関する閣僚政策会議」に合わせて、サイバーセキュリティ政策の現状と課題に関する関心を高め、日 ASEAN の連携のあり方等に関して理解を深めるために開催されたものです。本セミナーの詳細については、次の URL をご参照ください。

「政策担当者のためのサイバーセキュリティ・セミナー」の開催
http://www.asean.emb-japan.go.jp/release13_25j.html

6.2.7. 「日・ASEAN サイバーセキュリティ協力に関する閣僚政策会議」展示会への出展 (2013 年 9 月 12 日 - 13 日)

JPCERT/CC は、9 月 12 日から 13 日にホテルオークラ東京にて開催された「日・ASEAN サイバーセキュリティ協力に関する閣僚政策会議」に併催された展示会にブースを出展しました。本展示会は、日本の対 ASEAN の ICT 技術協力やサイバーセキュリティ等に関する取り組みをアピールすることを目的に開催されたものです。JPCERT/CC は、インターネット定点観測プロジェクト TSUBAME の事業紹介を行い、ASEAN 各国の参加者より TSUBAME の仕組み等に関する質問を受け、観測動画やグラフ等を活用しながら説明を行いました。

6.2.8. 覚書 (MOU) 締結

CSIRT 間の協調関係に明文化された基礎的・明示的な根拠を与え、また、交換される機微な情報の取り扱いルールを定めるため、関係する各国の組織との間で覚書の締結を積極的に進めています。本四半期は以下の組織と MOU を更新しました。

- New Zealand Government Communications Security Bureau（ニュージーランド）

6.2.9. 中国語圏における情報収集発信

JPCERT/CC は、中国語圏（中国／台湾）経済区域の情報セキュリティ関係会議やセキュリティチームの活動に参加し、セキュリティ関連情報の収集や現地セキュリティ専門家との情報交換を積極的に行っています。本四半期の活動は次のとおりです。

7 月 3、4、5 日に中国呼和浩特で開催された「中国計算機網絡安全応急 (CNCERT/CC) 年会」で講演し、日本のセキュリティ傾向及び制御システムセキュリティについての取組み状況を紹介しました。

7 月 19、20 日に台湾台北で開催された「台灣駭客年會 (HITCON)」で講演し、日本のセキュリティ傾向及び制御システムセキュリティについての取組み状況を紹介しました。

8 月 22、23 日に中国北京で開催された「XCon 安全焦点信息安全技术峰会」に参加し、中国地域におけるセキュリティ業界・コミュニティの活動状況について情報収集を行いました。

9 月 12、13 日に台湾新竹清華大学で開催された「第五屆台灣區 Botnet 偵測與防治技術研討會」で講演し、日本のセキュリティ傾向及び制御システムセキュリティについての取組み状況を紹介しました。

これらの講演内容や講演会にて行われた意見交換の内容は、日本国内の関係者会合等において紹介しました。

6.2.10. 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。

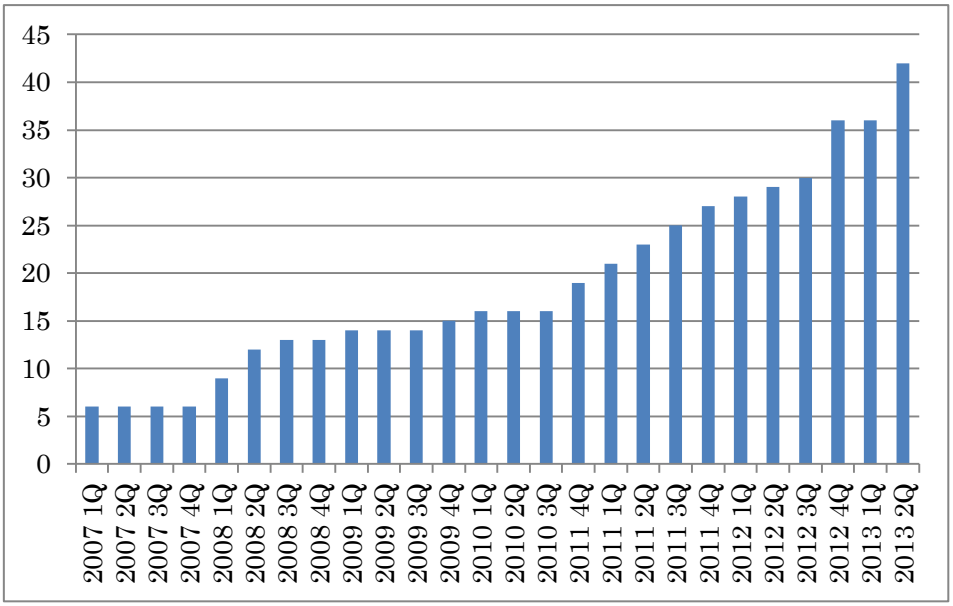
The votes are in - and we have a new CVE numbering scheme! (2013/07/09 公開, 08/01 更新)
http://blog.jpcert.or.jp/2013/07/the-votes-are-in---and-we-have-a-new-cve-numbering-scheme.html

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

国内のシーサート(CSIRT: Computer Security Incident Response Team) 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た日本シーサート協議会（Nippon CSIRT Association: NCA）の事務局として、JPCERT/CC は、協議会の問合せ窓口や会員情報の管理、加盟のためのガイダンスの実施および手続の運用、Web サイト、メーリングリストの管理等の活動を行っています。

本四半期においては、デロイト トーマツ リスクサービス株式会社(DT-CIRT)と株式会社セキュアブレイン(SecureBrain-ARL)、株式会社アラタナ(aratana-CSIRT)、サイボウズ株式会社(Cy-SIRT)、第一生命保険株式会社(DL-CSIRT)、GMO インターネット株式会社(GMO 3S)の 6 組織が新規に加盟しました。本四半期末時点で 42 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 1-5]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]

8 月 23 日には、日本電信電話株式会社(NTT-CERT)の会議室をお借りして「第 7 回総会・第 12 回ワーキンググループ会」を開催しました。総会において、運営委員選任及び事務局指定の審議が行われ、JPCERT/CC の村上晃が運営委員に選任され、今年度も引き続き JPCERT/CC が事務局を行うことが承認されました。また、総会後に行われた運営委員会では、村上晃が運営委員長に選任されました。前年

度に引き続いての運営委員長への就任です。

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/

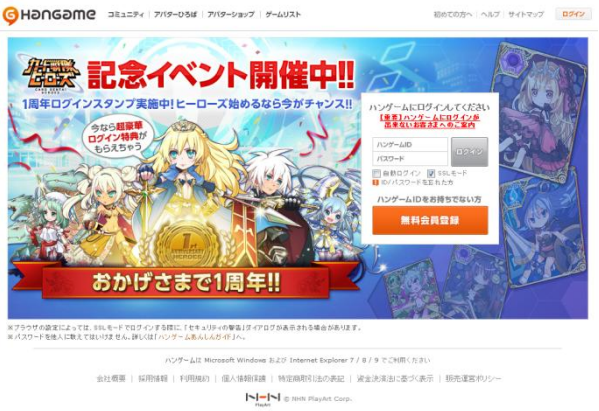
8. フィッシング対策協議会事務局の運営

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など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 7 件発信しました。

本四半期は、インターネットサービスプロバイダなどが提供している Web メールサービスをかたるフィッシングと、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に加えて、決算代行会社をかた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、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 7-1]の「ハンゲームをかたるフィッシング(2013/08/07)」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 7-1　ハンゲームをかたるフィッシング(2013/08/07)
https://www.antiphishing.jp/news/alert/hangame20130807.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など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、1 日に数回提供しています。この活動の目的は、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みに活用していただくことや、関連研究の促進です。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 18 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ない、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か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。

瀬古敏智「フィッシングに関する最新動向について」
神奈川県クレジットカード犯罪対策連絡協議会 2013 年 7 月 30 日

山本健太郎「フィッシングに関する最新動向について」
北海道クレジットカード犯罪対策連絡協議会 2013 年 8 月 30 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、毎月の活動報告などを公開しています。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 7 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201307.html
フィッシング対策協議会 2013 年 8 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201308.html
フィッシング対策協議会 2013 年 9 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201309.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 6 回運営委員会
日時：2013 年 9 月 6 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 7 回運営委員会
日時：2013 年 9 月 27 日 16:00 - 18:00
場所：トッパン・フォームズ株式会社

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. Java アプリケーションの脆弱性事例解説資料

本資料は、Java 言語で書かれたアプリケーションの脆弱性事例に関する解説資料です。
Java 言語によるセキュアなプログラムを開発するためのコーディング規約「Java セキュアコーディングスタンダード CERT/Oracle 版」(https://www.jpcert.or.jp/java-rules/)や、Java セキュアコーディングのセミナー資料とともに、自習や勉強会などの参考資料としてご活用ください。
本資料の詳細は、「2.5.3」をご参照ください。

Java アプリケーションの脆弱性事例解説(2013 年 9 月 30 日)
https://www.jpcert.or.jp/securecoding/materials-java-casestudies.html

10.2. 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 2013 年 4 月～6 月　(2013 年 8 月 5 日)
https://www.jpcert.or.jp/tsubame/report/report201304-06.html

10.3. 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（経済産業省告示 第 235 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を行っています。本レポートは、2013 年 4 月 1 日から 2013 年 6 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[2013 年第 2 四半期(4 月～6 月)]
(2013 年 7 月 22 日)
https://www.jpcert.or.jp/press/2013/vulnREPORT2013q2.pdf

11. 講演活動一覧

(1) 満永 拓邦(早期警戒グループリーダ) ：
「APT(Advanced Persistent Threat)への備えと対応について」
Hitachi アカデミックシステム研究会第 32 回研究会,2013 年 9 月 13 日

(2) 山本 健太郎(フィッシング対策協議会事務局)：
「フィッシングの最新動向について(狙われる金融機関)」
北海道クレジットカード犯罪対策連絡協議会総会,2013 年 8 月 30 日

(3) 竹田 春樹(分析センターリーダ) ：
「ウェブ改ざんの脅威を理解する」
ISOG-J 主催セミナー「止まらない！ウェブ改ざんの実態と対策」,2013 年 8 月 22 日

(4) 戸田 洋三(情報流通対策グループ 脆弱性解析リードアナリスト)：
「～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」
オープンソースカンファレンス 2013 Kansai,2013 年 8 月 3 日

(5) 瀬古 敏智(早期警戒グループ 情報セキュリティアナリスト)：
「フィッシングの最新動向について～狙われる金融機関～」
神奈川県クレジット犯罪対策協議会, 2013 年 7 月 30 日

(6) 宮地 利雄 (理事)：
「医療用電子機器とサイバー・セキュリティ」
電子情報技術産業協会(JEITA) 医用電子システム事業委員会，2013 年 7 月 25 日

(7) 小宮山 功一朗(国際部兼エンタープライズサポートグループマネージャ) ：
「サイバー戦争の時代」
国際大学 GLOCOM 研究ワークショップ,2013 年 7 月 18 日

(8) 重森 友行(早期警戒グループ 情報セキュリティアナリスト)：
「最近のセキュリティ動向」

千葉県クレジットカード犯罪対策連絡協議会総会, 2013 年 7 月 17 日

(9) 久保 啓司(インシデントレスポンスグループマネージャ) ：
「Open Resolver 問題について」
JPIX Users Meeting 2013,Summer,2013 年 7 月 10 日

(10) 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チーム情報セキュリティアナリスト)：
「Overview of Vulnerability Handling」
International Conference on Information Security (ICIS)－ソウル,2013 年 7 月 10 日

(11) 宮地 利雄 (理事)：
「医療用機器へのサイバー攻撃対策」
日本画像医療システム工業会，2013 年 7 月 4 日

12. 執筆一覧

(1) 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)：
もいちど知りたい、セキュアコーディングの基本(5)
第 5 回 見落としがちな整数関連の脆弱性（後編） (1/2)
アイティメディア ＠IT,2013 年 8 月 1 日

13. 開催セミナー等一覧

(1) 企業向けセキュアコーディングセミナー
※本セミナーの詳細は、「2.5.5」をご参照ください。

■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