Japan Computer Emergency Response Team Coordination Center

電子署名者 : Japan Computer Emergency Response Team Coordination Center
DN : c=JP, st=Tokyo, l=Chiyoda-ku, email=office@jpcert.or.jp, o=Japan Computer Emergency Response Team Coordination Center, cn=Japan Computer Emergency Response Team Coordination Center
日付 : 2013.01.16 18:16:58 +09'00'

JPCERT-PR-2012-03

発行日 : 2013-01-17

JPCERT/CC 活動概要 [2012 年 10 月 1 日 ～ 2012 年 12 月 31 日]

活動概要トピックス

―トピック 1―　FIRST Technical Colloquium in Kyoto の運営支援
―トピック 2―　ThaiCERT（タイ）と共同で LaoCERT（ラオス）の構築支援活動
―トピック 3―　関係者の協力・連携によるスマートフォン関連の脆弱性情報の調整
―トピック 4―　制御システム技術者向けのインシデント対応トレーニングを開催

―トピック 1―　FIRST Technical Colloquium in Kyoto の開催

11 月 13 日から 15 日まで" FIRST Technical Colloquium in Kyoto"が京都市国際交流会館で開催されました。FIRST Technical Colloquium は、FIRST 加盟 CSIRT 間での情報共有を目的として、世界各地で年に数回開催されています。今回は山口英(JPCERT/CC 理事)、寺田真敏氏((株)日立製作所　HIRT)の共同委員長のもと、日本に拠点を置く FIRST 加盟 CSIRT が共同でその企画と運営にあたりました。JPCERT/CC は運営委員の一員として、特に"Future of Global Vulnerability Reporting Summit"という企画の運営に携わりました。

"Future of Global Vulnerability Reporting Summit"では、各国の脆弱性情報流通の専門家が集い、3 日間にわたって現在の脆弱性情報流通の課題と今後の改善策について議論を行いました。新たに指摘された様々な課題については、新たにワーキンググループを組織して関係者間での議論を継続することを FIRST に提案することが、承認されました。

本会議の詳細については、次の URL をご参照ください。

Kyoto 2012 FIRST Technical Colloquium
http://www.first.org/events/colloquia/kyoto2012

―トピック 2―　ThaiCERT（タイ）と共同で LaoCERT（ラオス）の構築支援活動

JPCERT/CC は、アジア太平洋地域やアフリカなどにおける National-CSIRT 機能の構築支援に積極的に取り組んできているところですが、10 月 15 日から 19 日までの 5 日間にわたって実施した、ラオスの National CSIRT である LaoCERT に対するトレーニングは、タイの National CSIRT である ThaiCERT のスタッフと共同で実施しました。タイ語がラオ語と言語的に近いことから、一部の講義を ThaiCERT のスタッフがタイ語で行うことで、英語による講義よりも受講生の理解が深まることが期待されると同時に、ThaiCERT が CSIRT 構築支援活動を経験する機会にもなりました。JPCERT/CC が機能構築・強化支援を行った先が、

他のチームに対する支援を行う機能を備えていくことで、一層密な連携・協力関係が構築されていくことが期待されます。

このトレーニングでは、LaoCERT のスタッフ及びその母体組織である LANIC（Lao National Internet Center）のスタッフ計 15 名に対し、インシデントハンドリングの手法や PGP の使い方、JPCERT/CC が運営している TSUBAME について等の講義とハンズオン演習を行いましたが、今回は、独立法人国際協力機構(JICA)がラオスで行っている「国立大学 IT サービス産業人材育成プロジェクト」とも連携し、本トレーニングを受講する LaoCERT と LANIC のスタッフが、トレーニングに先立って JICA のネットワーク研修を受講し、基礎知識を身につけた上でトレーニングに臨めるよう調整しました。

―トピック 3―　関係者の協力・連携によるスマートフォン関連の脆弱性情報の調整

本年度に入り、Android およびその関連製品の届出の増加傾向が続いていますが、本四半期には、携帯端末の脆弱性および Android 搭載スマートフォンに関する脆弱性情報 5 件のほか、いわゆるフィーチャーフォンに関する脆弱性情報も 1 件公表しました。

11 月 14 日に公表した JVN#74829345「Android OS を搭載した複数の端末におけるサービス運用妨害(DoS) の脆弱性」は、日本国内の全携帯通信キャリアおよび同各社に製品を納入している国内外の携帯端末開発者との調整を経て、最終的には携帯端末販売元である携帯通信キャリアからのベンダステータスを掲載するという形で公表に至った初の事例となりました。また本件は、調整に着手した当初から、幅広い製品における影響が想定されたため、JPCERT/CC から、米国 CERT/CC、英国 CPNI、フィンランド CERT-FI、韓国 KrCERT/CC、中国 CNCERT/CC への国際展開も行いました。

スマートフォンは、ユーザ層も幅広く、プライバシー情報などが保存されている可能性も高いことから、実際に攻撃が発生したときの影響の広がりは測り知れません。その一方で、通常のパッケージソフトウエア製品とは異なり、脆弱性に対する修正プログラム等の開発を携帯端末開発者に、利用者への通知を販売元である通信キャリアに、それぞれ実施していただく必要があり、脆弱性情報への対応については、携帯端末開発者と販売元である携帯通信キャリア各社の協力・連携が欠かせません。JPCERT/CC は、今後も引き続き国内外の携帯端末開発者およびその製品を販売している通信キャリアとの調整を行い、脆弱性問題への速やかな対応促進に努めてまいります。

―トピック 4―　制御システム関係者向けのインシデント対応トレーニングを開催

制御システム関係者（ユーザ・ベンダ・研究者）の方々を対象としたセキュリティインシデント対応トレーニングを、11 月 20 日、21 日の 2 日間、福岡で実施しました。本トレーニングは、制御システムネットワークで代表的な３階層ネットワークと制御システムシミュレータを用いた模擬的な環境で、制御システムに携わる方々に、セキュリティインシデントへの気付きやインシデント対応に必要な技術を体感していただくものです。今後、今年度内に、大阪/名古屋および東京（2 回）での開催も予定しています。

本活動は、経済産業省より委託を受け、「平成２４年度情報セキュリティ対策推進事業（不正アクセス行為等対策業務）」として実施したものです。
ただし、「平成２４年度情報セキュリティ対策推進事業（フィッシング対策業務）」として経済産業省から受託して実施した「7.フィッシング対策協議会事務局の運営」、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」、「8.フィッシング対策協議会会費による活動」「10.講演活動一覧」、「11.執筆一覧」及び「12.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 5064 件、インシデント件数ベースでは 5293 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ます。ただし、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は 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 1497 件でした。前四半期の 1123 件と比較して 33%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、国際的な調整・支援が必要となるインシデントにおいて、日本の窓口組織として、国内や国外 (海外の CSIRT など) の関係機関と調整活動を行っています。この活動を通じて、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しています。

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_Report20130117.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 360 件で、前四半期の 273 件から 32%増加しました。また、前年度同期（314 件）との比較では、15%の増加となりました。
本四半期のフィッシングサイトが装っていたブランドの国内・国外別の内訳を[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	25	25	24	74(21%)
国外ブランド	87	71	69	227(63%)
ブランド不明(注 2)	18	24	17	59(16%)
月別合計	130	120	110	360(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、国内通信事業者を装ったフィッシングの報告が寄せられています。10 月半ばには、ケーブルネットワークなど複数通信事業者の Web メールサービスを装ったフィッシングサイトが確認されました。また、異なるブランドに関するフィッシングメールに、共通の文面が使用されている事例も確認されました。

10 月末には、国内金融機関のインターネットバンキングのページに利用者がアクセスした際に、第二認証情報などを入力させるための不正なポップアップ画面を表示し、入力された情報を窃取するマルウエアが確認されました。また、国内金融機関を装った一般的な手法のフィッシングサイトも継続して確認されています。

フィッシングサイトの調整先の割合は、国内が 44%、国外が 56%と、前四半期の割合（国内 56%、国外 44%）と比較して、国内への調整が増えました。

本四半期に報告が寄せられた Web サイト改ざんの件数は、737 件でした。前四半期の 796 件から 7%減少しています。

Web サイト改ざんでは、ページに不正に挿入された JavaScript や iframe によってサイト閲覧者を攻撃サイトに誘導し、複数の脆弱性を使用した攻撃により PC をマルウエアに感染させるものが多く確認されています。

2012 年 11 月には、2012 年 10 月に修正された Java の脆弱性(CVE-2012-5076)を悪用してマルウエアに感染させる手法が、誘導先の攻撃サイトで使用されていることを確認しました。古いバージョンの Java を使用していると、その脆弱性を使用した攻撃により、マルウエアに感染する危険性があります。

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 改ざんなどのサイバー攻撃に関する情報を収集、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。

1.1.2. 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)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。

1.1.2.1. 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：9 件　https://www.jpcert.or.jp/at/

2012-10-09　Adobe Flash Player の脆弱性 (APSB12-22) に関する注意喚起
2012-10-10　2012 年 10 月 Microsoft セキュリティ情報 (緊急 1 件含) に関する注意喚起
2012-10-10　ISC BIND 9 サービス運用妨害の脆弱性 (CVE-2012-5166) に関する注意喚起
2012-11-07　Adobe Flash Player の脆弱性 (APSB12-24) に関する注意喚起
2012-11-14　2012 年 10 月公開の Java SE の脆弱性を狙う攻撃に関する注意喚起
2012-11-14　2012 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
2012-11-16　2012 年 10 月公開の Java SE の脆弱性を狙う攻撃に関する注意喚起
2012-12-12　2012 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
2012-12-12　Adobe Flash Player の脆弱性 (APSB12-27) に関する注意喚起

1.1.2.2. 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 67 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。

2012-10-03　情報セキュリティ国際キャンペーン
2012-10-11　次世代ハッシュ関数 SHA-3 アルゴリズム
2012-10-17　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 13 版
2012-10-24　地方公共団体における情報システムセキュリティ要求仕様モデルプラン（Web アプリケーション）
2012-10-31　Adobe Acrobat/Adobe Reader XI リリースと 9 のサポート期間
2012-11-07　担当者ノート: TSUBAME プロジェクト
2012-11-14　Windows 8 のセキュリティ - Windows Defender
2012-11-21　JNSA が「SNS の安全な歩き方」を公開
2012-11-28　オンラインバンキングマルウエアに注意
2012-12-05　Web サイト改ざん報告の増加
2012-12-12　インターネット接続機器へのスキャン
2012-12-19　D.ROOT-SERVERS.NET の IP アドレス更新
2012-12-27　担当者が選ぶ 2012 年重大ニュース

1.1.2.3.　早期警戒情報

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における情報セキュリティ関連部署や組織内 CSIRT に向けて、大きな影響を与え得る脅威に関する「早期警戒情報」を、JPCERT/CC が推奨する対策を添えて提供しています。

早期警戒情報の提供について
https://www.jpcert.or.jp/wwinfo/

1.1.3.　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。

(1)Java SE の既知の脆弱性を狙う攻撃に関する情報収集・提供

購入時に既にインストール済みであることも多い Java SE は、利用者がその存在に気づかず脆弱性対策の必要性を認識していなかったり、「使っていないのに煩わしい」と意図的に自動アップデートを無効にしていたりするケースも見られるようです。また、Java SE の脆弱性は、ネットワーク越しに攻撃しやす

いことが多く、Web ベースの攻撃に使用される攻撃ツール(Exploit kit など)の多くが、Java SE の脆弱性を利用しており、Java SE の新たな脆弱性は迅速に多くの攻撃ツールに組み込まれる傾向にあります。
2012 年 10 月 17 日には、Oracle 社より Oracle Java SE JDK および JRE 7 の脆弱性に関する情報が公開されました。この脆弱性は、PC 上で任意のコード実行を許容するもので、Oracle 社によると本情報の公開時点で既にこの脆弱性を狙う攻撃が海外で確認されていました。
JPCERT/CC では、国内での攻撃活動に関する情報収集を行い、2012 年 11 月中旬に国内でもこの脆弱性を狙った攻撃を確認したため、これらの攻撃への注意と対策の実施を広く呼び掛ける注意喚起を行いました。

2012 年 10 月公開の Java SE の脆弱性を狙う攻撃に関する注意喚起
https://www.jpcert.or.jp/at/2012/at120036.html

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。

1.3.1. JPCERT/CC インターネット定点観測システムの TSUBAME への移行

JPCERT/CC は、**2003** 年から ISDAS と名付けたインターネット定点観測システムを運用し、日本国内にセンサーを配置してデータを収集してきました。しかしながら、国内外の PC 等の上で活動するマルウエアなどが対象とする製品や地域の変化を把握するため、さらには国境を越えたネットワーク攻撃などの環境変化の中で National CSIRT 間でインターネット上の不正パケットの広域的な観測データを共有するためにも、海外にもセンサーを配置して観測を行う必要性が高まってきました。

そこで JPCERT/CC では、「TSUBAME プロジェクト」と命名されたプロジェクトを 2007 年から開始して、新たな観測用センサーと観測データ収集用サーバを開発し、アジア太平洋州を中心とする海外の National CSIRT の協力を得て、観測用のセンサーを海外にも分散配置してきました。これにより、広い地域の各国のセンサーで観測された結果が一元化されたデータとして共有され、例えば日本国内に向けられた感染活動や弱点探索のためのスキャンと、海外の観測点での傾向や動向との比較が行えるようになりました。また、海外の特定の地域で先行して発生した攻撃の様子なども把握できるようになりました。

JPCERT/CC では、TSUBAME の観測用センサーに ISDAS の観測用センサーとしても機能する互換性機能を組み込み、ISDAS と TSUBAME の 2 種類のインターネット観測システムを並行運用しつつ、2009 年から既存の ISDAS 用センサーを TSUBAME 用センサーに順次置き換えてきました。今期この作業が完了

し、JPCERT/CC のインターネット定点観測システムを ISDAS から TSUBAME に完全に移行し終えることができました。これに伴い、公開している観測情報も TSUBAME プロジェクトのデータを使用した内容にリニュアルしました。TSUBAME センサーでは、TCP/UDP のヘッダ情報やペイロードなど、より多くの情報を得られるようになりました。また、パケットから得られる情報量が増えたことにより、脆弱性情報やマルウエアの動向との情報を紐付けることで攻撃手法の推測もより効果的に行えるようになりました。本情報は、インシデント通知などに活用しています。

公開情報はこれまでの形式を踏襲していますが、ポート別グラフなどは TSUBAME プロジェクトで収集したデータを使用するように変更しました。ポート別グラフでは ISDAS 時と比較して情報量に変化はありませんが、研究者向けの観測データの提供では TCP/UDP の IP アドレスやポート番号に加えて、ヘッダー情報などより多くの情報の提供を始めました。また、観測データの動向を 4 半期毎にまとめた観測動向のレポートの公開を始めました。

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

1.3.2. インターネット定点観測レポート

TSUBAME プロジェクトの一環として、収集したデータの概要を四半期毎にまとめ分析や考察を添えた、「インターネット定点観測レポート」を、2012 年 1～3 月期分まで遡って、今期から公表し始めました。本レポートは、システム管理者の皆さまに自分が管理しているネットワーク環境との比較や対策の検討のために読んでいただくことを想定して作成しています。レポートは、2 部構成になっており、第 1 部では、宛先ポートや送信元地域の Top5 のグラフと、対象となったプロトコルやプラットフォームにどのような特徴が見られたかをまとめた概況を、第 2 部では、期間中の変化や特異な変動を取り上げた分析や考察を、それぞれ 1 ページ程度にまとめて記載しています。

インターネット定点観測レポート 2012 年 7～9 月 (2012 年 12 月 19 日)
https://www.jpcert.or.jp/tsubame/report/report201207-09.html
インターネット定点観測レポート 2012 年 4～6 月 (2012 年 10 月 25 日)
https://www.jpcert.or.jp/tsubame/report/report201204-06.html
インターネット定点観測レポート 2012 年 1～3 月 (2012 年 10 月 25 日)
https://www.jpcert.or.jp/tsubame/report/report201201-03.html
2012 年度の TSUBAME 定点観測レポート
https://www.jpcert.or.jp/tsubame/report/index.html

1.3.3. 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、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。本四半期における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。

1） 日本国内の企業や大学の IP アドレスを送信元とする、SSH サーバが使用するポートへのパケットが観測されました。JPCERT/CC では、当該パケットの送信元の IP アドレスの管理者に情報を提供し、SSH のスキャンや辞書攻撃を行っているツール設置の有無の確認と除去を依頼しました。その後、該当 IP アドレスから同様のパケットは観測されなくなったことから、ツールの除去等の対処が行われ、その後の被害拡大の抑止につながったと考えられます。

また、情報提供先のサーバの管理者の一部からは、当該サーバが攻撃者に侵入され、第三者のサーバに対して SSH の稼働状況の確認や辞書攻撃を行うための IRC 通信用のプログラムや SSH の辞書攻撃を行うツールが設置されていたとの情報提供をいただきました。

2） 前期に引き続き、日本の企業や大学の IP アドレスを送信元とする、SIP サービス用ポートへのパケットが観測されました。JPCERT/CC では、当該パケットの送信元の IP アドレスの管理者に情報を提供し、SIP サーバのスキャンや、SIP アカウントの ID やパスワードを試行するための辞書攻撃を行うツール設置の有無の確認と除去を依頼しています。

また、情報提供先のサーバの管理者の一部からは、通常のサーバ以外にもビデオ会議システムなどのアプライアンスからもこのようなパケットを送信する状態になっていたという情報をいただきました。該当の IP アドレスから同様のパケットは観測されなくなったことから、マルウエアの駆除等の対処が行われ、その後の被害拡大の抑止につながったと考えられます。さらに、JPCERT/CC の Weekly Report でアプライアンスがマルウエアに感染している事例を紹介し、対策を行ってもらうよう一般向けに周知しました。

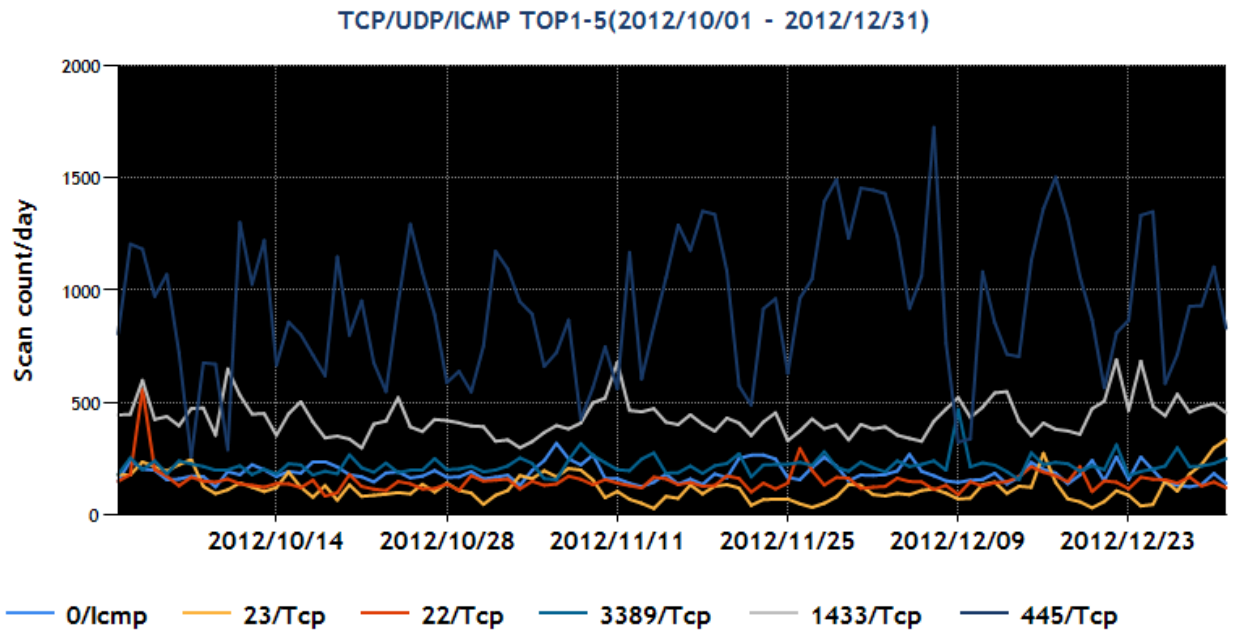
1.3.4. ポートスキャン概況

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/

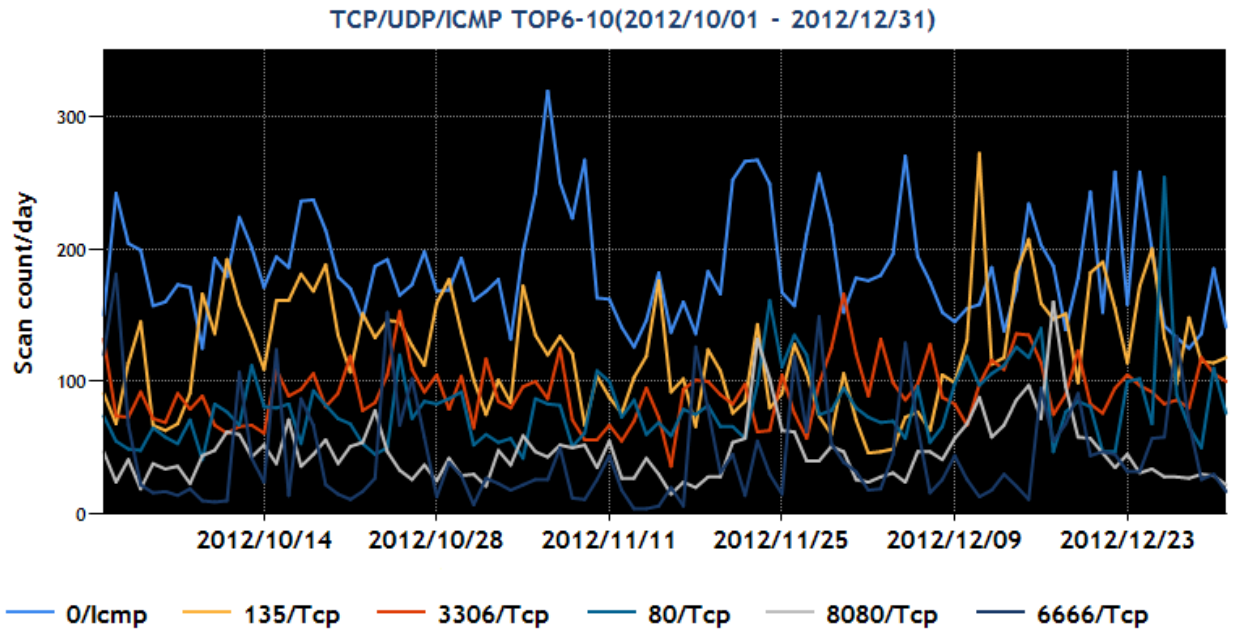
本四半期に定点観測システムで観測された宛先ポート別の上位 1 位～5 位及び 6 位～10 位のそれぞれについて、パケット数の時間的推移を[図 1-1]と[図 1-2]に示します。

- 宛先ポート別グラフ top1-5 (2012 年 10 月 1 日-12 月 31 日)



[図 1-1 宛先ポート別グラフ top[1-5]

- 宛先ポート別グラフ top6-10 (2012 年 10 月 1 日-12 月 31 日)

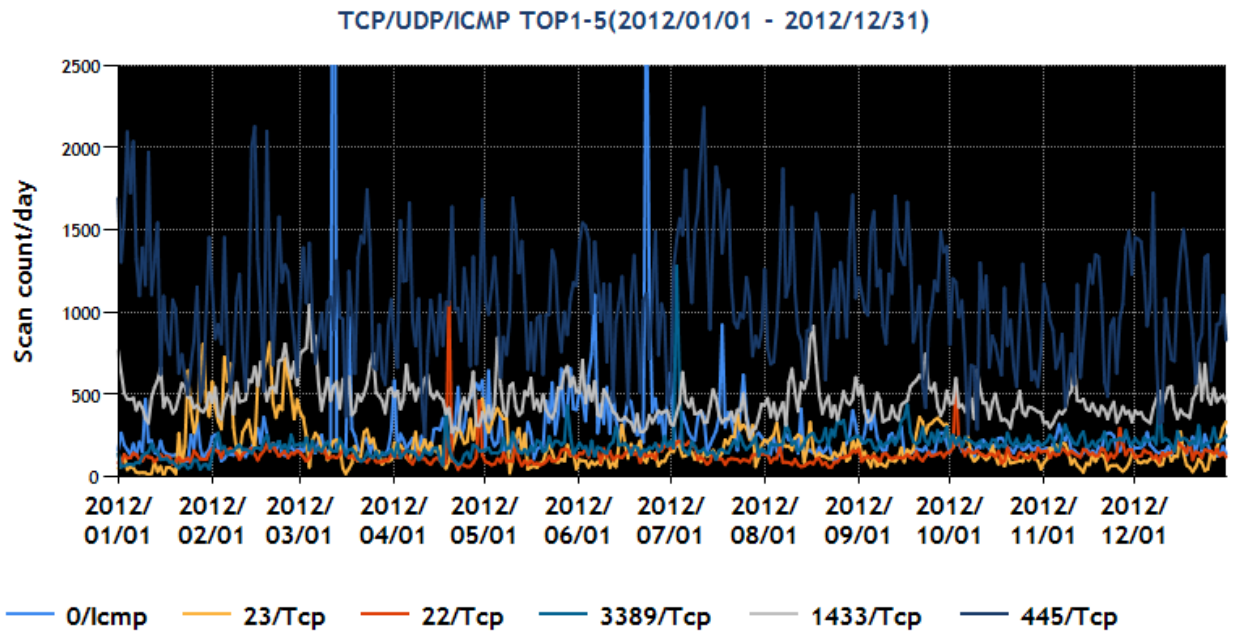


[図 1-2 宛先ポート別グラフ top[6-10]

また、より長期間のパケット数の推移を見るため、2011 年 10 月 1 日から 2012 年 9 月 30 日までの期間

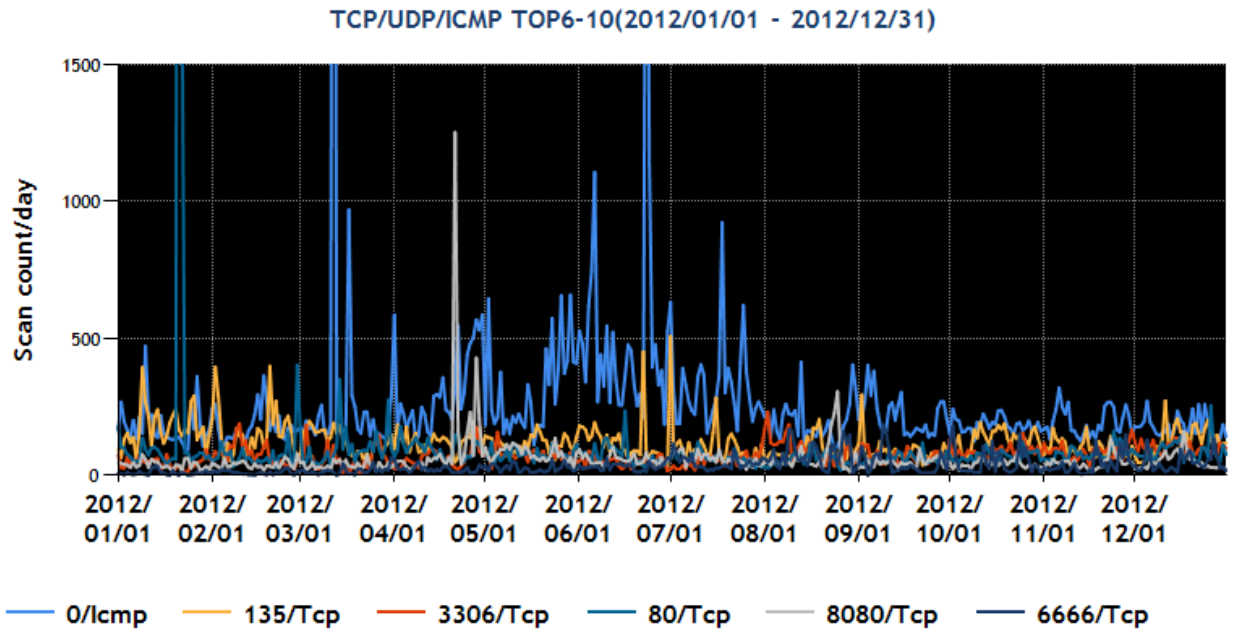
における、宛先ポート別の上位 1 位～5 位及び 6 位～10 位のそれぞれについて、パケット数の時間的推移を[図 1-3]と[図 1-4]に示します。

- 宛先ポート別グラフ top1-5 (2012 年 1 月 1 日-2012 年 12 月 31 日)



[図 1-3 宛先ポート別グラフ top[1-5]

- 宛先ポート別グラフ top6-10 (2012 年 1 月 1 日-2012 年 12 月 31 日)



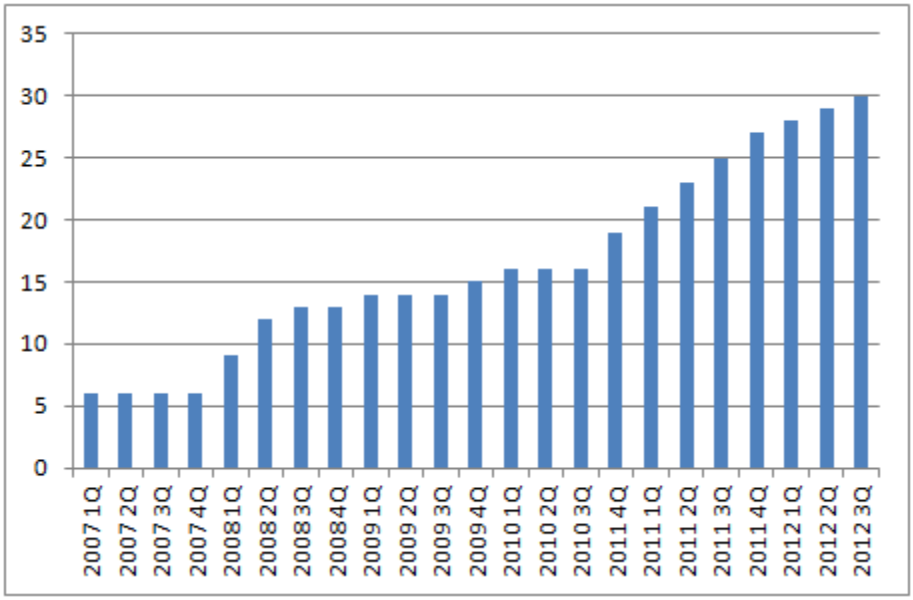
[図 1-4 宛先ポート別グラフ top[6-10]

順位には変動がありますが、これまでの傾向と同様、 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 サーバなどコンピュータを遠隔操作で使う場合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。

1.4. 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、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、株式会社みずほフィナンシャルグループ(Mizuho-CIRT)が新規に加盟しました。本期末時点で 30 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 1-5 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/

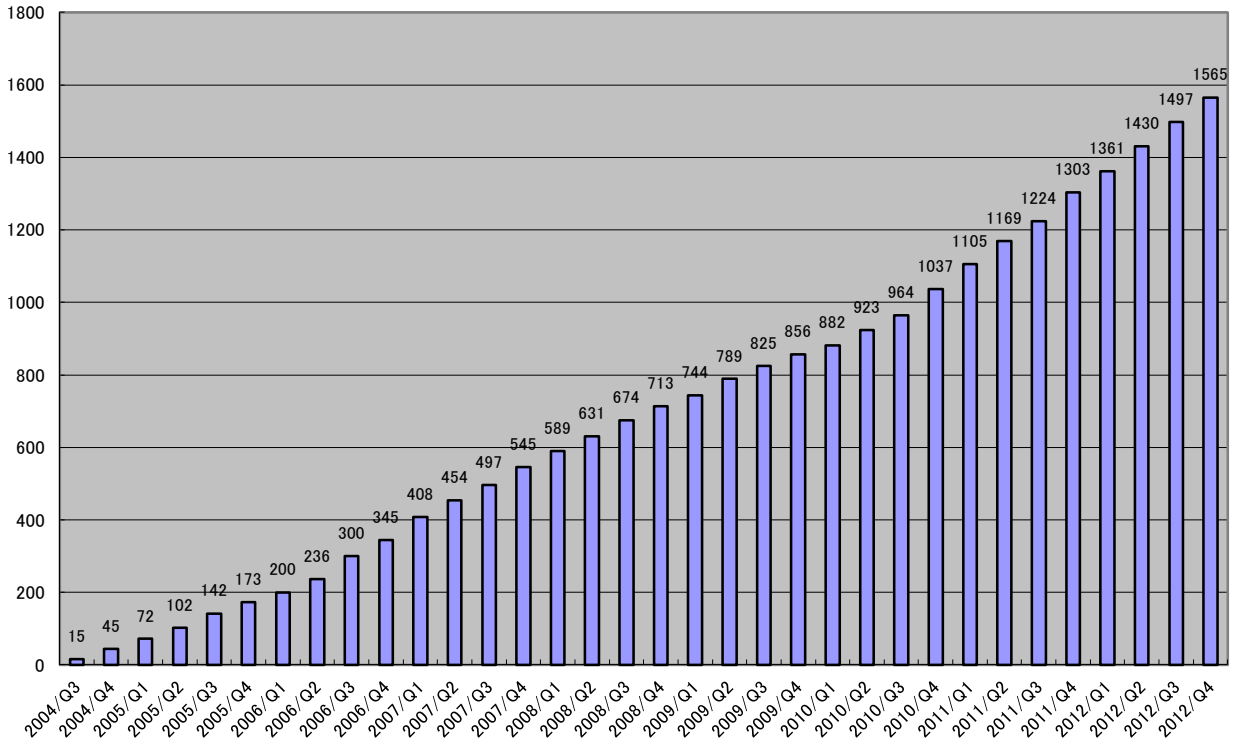
2. 脆弱性関連情報流通促進活動

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) に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。）において、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」に詳述された調整機関の役割を担うとともに、対策が整った脆弱性について原則として JVN で公表する活動を行っています。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、68 件(累計 1565 件) [図 2-1] でした。

本四半期に公表された個々の脆弱性情報に関しては、以下 URLJVN をご覧ください。
https://jvn.jp/



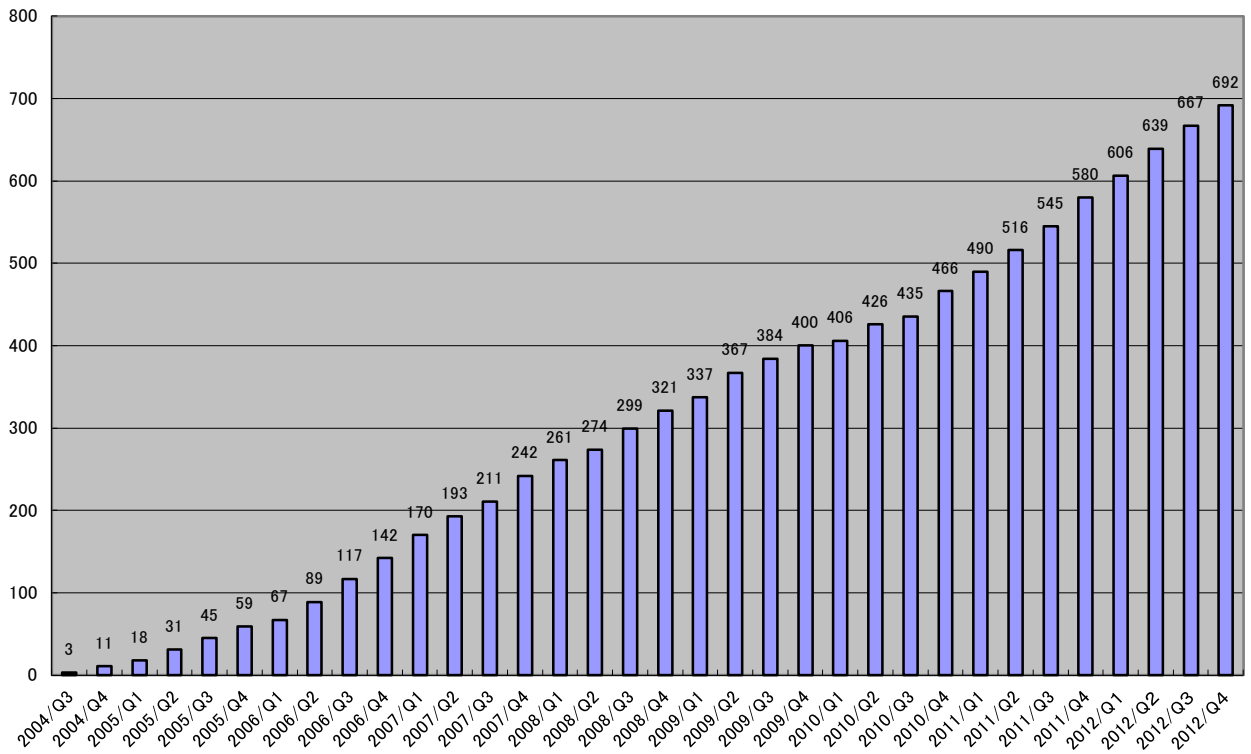
[図 2-1　JVN 公表累積件数]

本四半期において公表に至った国内取扱脆弱性情報は、25 件(累計 692 件) [図 2-2] でした。そのうちの 10 件（40%）が海外製品開発者の製品です。こうした統計値にも表れているように、本枠組みに基づく JPCERT/CC の調整活動は、海外の開発者にも理解され、協力が得られるようになってきています。
本年度に入り、Android およびその関連製品の届出の増加傾向が続いています。本四半期には、携帯端末の脆弱性および Android 搭載スマートフォンに関する脆弱性情報を 5 件公表し、いわゆるフィーチャーフォンにおける脆弱性情報も 1 件公表しました。

11 月 14 日に公表した JVN#74829345「Android OS を搭載した複数の端末におけるサービス運用妨害(DoS) の脆弱性」は、日本国内の全携帯通信キャリアおよび同各社に製品を納入している国内外の携帯端末開発者との調整を経て、最終的には携帯端末販売元である携帯通信キャリアからのベンダステータスを掲載するという形で公表に至った初の事例となりました。また本件は、調整に着手した当初から、幅広い製品における影響が想定されたため、JPCERT/CC から、米国 CERT/CC、英国 CPNI、フィンランド CERT-FI、韓国 KrCERT/CC、中国 CNCERT/CC への国際展開も行いました。

オープンソースである Android OS に関しては、昨今、本枠組みに届け出られる脆弱性のみならず、米国やその他の国々においても、多くの脆弱性が発見、指摘されています。スマートフォンは、ユーザ層も幅広く、プライバシー情報などが保存されている可能性も高いことから、実際に攻撃が発生したときの影響の広がりは測り知れません。その一方で、通常のパッケージソフトウエア製品とは異なり、脆弱性に対する修正プログラム等の開発を携帯端末開発者に、利用者への通知を販売元である通信キャリアに、それぞれ実施していただく必要があり、脆弱性情報への対応については、携帯端末開発者と販売元である携帯通信キャリア各社の協力・連携が欠かせません。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]

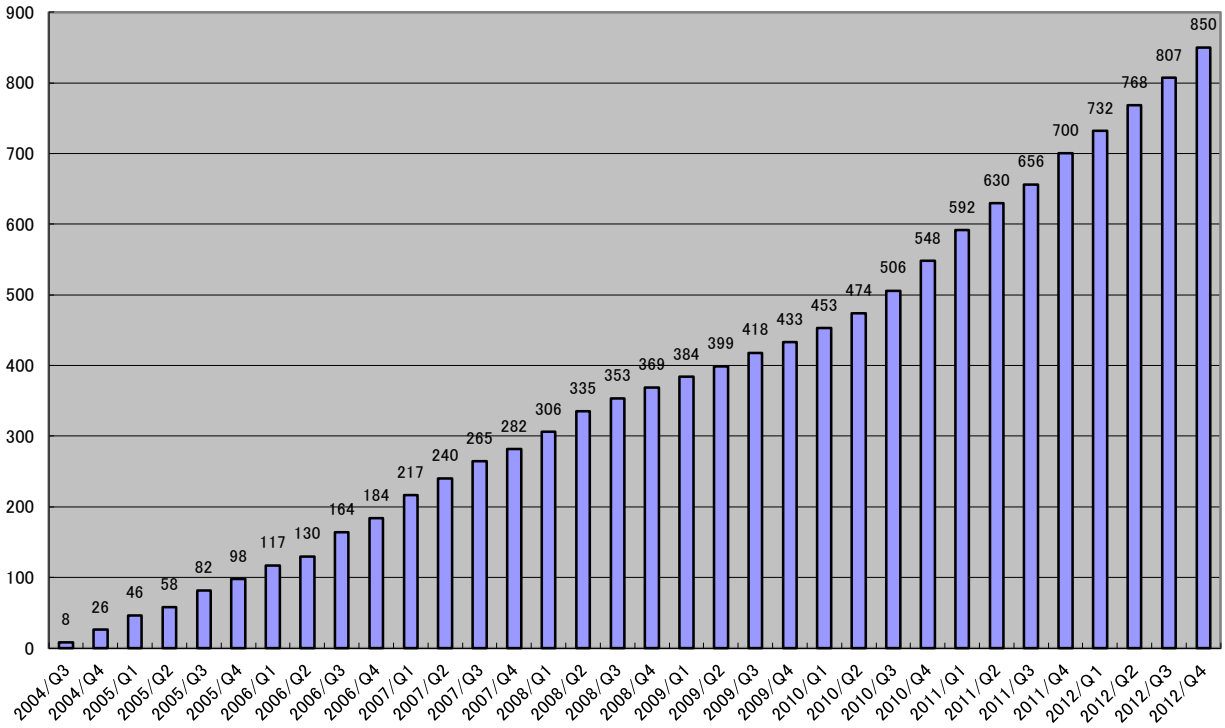
本四半期に公表した国際取扱脆弱性情報は、43 件(累計 850 件) [図 2-3]でした。このうち、3 件の US-CERT の脆弱性注意喚起（JVNTA から始まる識別子を付して公開したもの）は、いずれも Microsoft 製品に関する月例パッチの注意喚起でした。また、それ以外の国際取扱脆弱性情報の 40 件では、IBM、Symantec、DELL、CA(Computer Associates)、HP(Hewlett Packard)、Adobe といった著名な製品開発者の製品に関するものが多く目立ちました。また前四半期に続き、本四半期においても、ファーウェイ(Huawei)や Qualcomm といった携帯通信機器に関する脆弱性情報の公表を行いました。

なお、JVN で公表する国際取扱脆弱性情報は、2004 年 7 月の本基準の制定以来、取扱機関（たとえば、米国 CERT/CC や英国 CPNI など）ごとに分けて、それぞれの取扱機関が公表した脆弱性情報との対応関係が類推できるような識別子を付与して公表してきました。しかしながら、例えば、海外のベンダー等から報告され海外のいずれの調整機関からも公表されないような変則的な国際取扱脆弱性情報が現れるなど、当初の計画とは整合しない運用実態となったため、2012 年 12 月 3 日公表分から、取扱機関ごと仕分けせず一元化して、「JVNVU# 」に続く 8 桁の数字（たとえば、JVNVU#12345678 等）という新たな形式の識別子を付与する方式に変更しました。詳しくは、以下の URL をご参照ください。

「過去のお知らせ」

2012/12/3 より JVNVU が変わります。

https://jvn.jp/nav/info2012112617.html



[図 2-3　国際取扱脆弱性情報の公表累積件数]

2.2.　情報セキュリティ早期警戒パートナーシップの改訂とその運用

前項 2 で述べたように、情報セキュリティ早期警戒パートナーシップに基づいて、着々と対策がとられ、情報公表されるものが多数を占めている一方で、製品開発者との連絡が取れないなどの理由から調整が止まってしまっている、いわゆる「長期滞留案件」の件数も 2004 年の本活動開始から約 8 年の間に徐々に累積してきています。こうした状況の改善を期して、昨年度から、専門家の方々から構成された委員会において、脆弱性情報の取扱手順を定めたガイドラインの改定が検討されてきました。

その第一段階として、2010 度に公表さ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改定版および JPCERT/CC 脆弱性関連情報取扱いガイドラインでは、脆弱性情報への対応が必要な製品開発者と連絡がとれない等の理由により調整が困難となった際に、当該の製品開発者への連絡手段に関する情報を広く一般に求める手順が追加されました。これを受けて 2011 年 9 月 29 日から、JVN 上に「連絡不能開発者一覧」というページを設け、連絡不能となっている製品開発者名の掲載を開始しました。連絡不能開発者一覧の掲載によって、16 件の案件（製品開発者の数としては 11 件）について、取扱いが再開されており、「滞留案件」の解消に一定の効果があることが確認されています。

本四半期においては、新たに 4 件の製品開発者名(案件数としては 8 件)を、連絡不能開発者として公表しました。連絡不能開発者一覧公表の 4 日後、そのうち 1 件については製品開発者から連絡があり、当該案件は取扱い再開となりました。連絡不能開発者一覧の公表から 1 年 3 カ月が経過した本四半期末日時点で、合計 103 件の連絡不能開発者案件が公表されており、今もなお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。

さらに、第二段階として、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ました。第二段階目の活動については、本年度内の開始を視野に、さらなる検討および体制整備等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、国内のみならず国際的な枠組みにおける脆弱性情報の円滑な流通のため、国際調整機関である米国の CERT/CC、英国の CPNI、フィンランドの CERT-FI などの海外 CSIRT 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。

国際的な活動の一つとして、2008 年 5 月 21 日に JVN 英語版サイト(https://jvn.jp/en)の運用を開始し、4 年が経過しました。JVN 英語版での情報公表は、日本語版公表とほとんど時間差なく、ほぼ同時公表で運用を行っています。国内取扱脆弱性情報の海外への発信という点では、第一次情報発信源となることも多く、海外の主要セキュリティ関連組織などからも注目されています。

また、JPCERT/CC は、米国 MITRE 社より、2010 年 6 月 23 日付で CNA（CVE Numbering Authorities、CVE 採番機関）に認定されました。その後は、JPCERT/CC が CNA として、自ら、よりタイムリーに CVE 番号を採番できることになりました。本四半期は、22 件の脆弱性情報について JPCERT/CC が CVE を採番し、JVN 上に掲載しました。2008 年に CVE の採番を開始して以降、取扱い案件のうち、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を除いた、90%を超える案件に対し 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/index.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 脆弱性情報取り扱いガイドライン
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

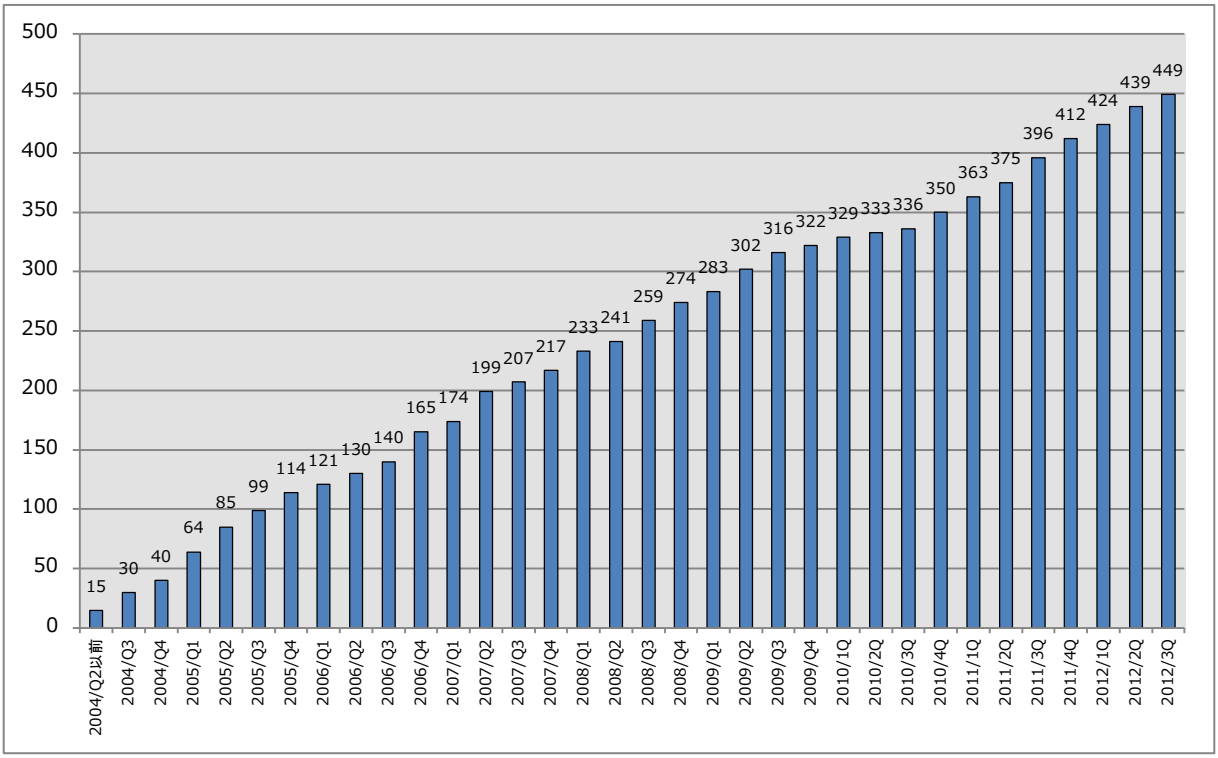
本基準では、受付機関に IPA、調整機関に JPCERT/CC が指定されています。JPCERT/CC は IPA が受け付けた届出情報の転送を受けて、製品開発者への情報提供を行い、対策情報公開に至るまでの調整を行っています。最終的には、 IPA と共同で、脆弱性情報ポータル JVN において対策情報を公開しています。両組織間においては、脆弱性情報の分析結果や脆弱性情報の取扱い状況等の情報交換を行うなど、緊密な連携を行っています。なお、本基準における IPA の活動および四半期毎の届出状況については、次の URL をご参照ください。

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、2012 年 12 月 31 日現在で 449 社となっています。

登録等の詳細については、以下をご参照ください。
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. 学生向けセミナー「Java セキュアコーディングセミナー@福岡」を開催

Android の普及とともに Java プログラムの開発量が急増しています。その脆弱性削減を目的として、脆弱性を含まない安全なプログラムを Java 言語でコーディングするための具体的なテクニックやセキュリティ上の視点について学んでいただく学生等の若年層向け 1 日セミナーを、12 月 9 日(日)福岡市内で開催しました。

14 名の受講生の方にご参加いただいた本セミナーは、講義と演習を交え、最後は受講者自らが実機を使ってセキュアコーディングを体験するという構成で実施しました。

第 1 部、講義「オブジェクトの生成と消滅におけるセキュリティ」

クラスローディングのメカニズム、オブジェクトの生成、クラスの設計といった Java の基本概念とセキュリティ上の注意点について解説

第 2 部、演習「クイズと解説」

第 1 部の講義でカバーしたトピックスに関するクイズ形式の問題

第 3 部、講義「リソース枯渇攻撃とその対策」

Java アプリケーション実行時に使用されるリソースと、それらを大量に消費させることによってアプリケーションの動作を妨害するリソース消費攻撃について紹介。とくに Zip Bomb の詳細を解説

第 4 部、実習「ハンズオン」

受講者各自が端末を使い、脆弱な Java のコードの問題点を見つけ出し、正しいコードに修正する実習

地方開催のセミナーは、8 月の札幌に引き続く 12 月の福岡での開催をもって、本年度は終了となります。多数のご参加ありがとうございました。

2.5.2. 学生向け「Java セキュアコーディング連続セミナー@東京」好評のうちに終了

9 月から月 1 回のペースで「Java セキュアコーディング連続セミナー」を東京で開催してきました。本四半期は、以下の 3 回を実施し、多くの受講生の方にご参加いただきました。これで本年度の全 4 回のセミナーは終了しました。

第 2 回「数値データの取扱いと入力値の検証」（10 月 14 日（日）開催）
第 3 回「入出力(File, Stream)と例外時の動作」（11 月 11 日（日）開催）
第 4 回「メソッドとセキュリティ」（12 月 16 日（日）開催）

このセミナーは、座学とハンズオンを組み合わせた二部構成を特色とし、前半では、各回のトピックに関連した Java の基本概念とセキュリティ上の注意点について解説しました。後半のハンズオンでは、受講者が自ら、課題として与えられた脆弱なソースコードを修正し、また脆弱性の修正方法について他の受講生とディスカッションすることを通じて、セキュアコーディングを体験しました。

受講後のアンケート結果には、「何も考えずにコーディングをしていると気がつかないような問題がたくさんあり、気をつけなければと思いました」「『例外にセンシティブな情報が含まれる』というのは新しい気づきでした」など、セキュリティに関する気づきが得られたというコメントや、「そもそも大学ではセキュアコーディングを学ぶ機会がないため貴重なセミナーだった」という意見も寄せられました。

セミナーの講義資料は、下記の URL からご覧いただけます。Java プログラミングを学ぶ学生の方はもちろん、業務で Java を使ったアプリケーション開発に携わるプログラマの皆様も、セキュアコーディングを学ぶ教材としてぜひご利用ください。

講義・演習資料
http://www.slideshare.net/jpcert_securecoding

2.5.3. 翔泳社と共催で「Android セキュアコーディングセミナー」開催

今年の 3 月に翔泳社と共催し、多数の Android アプリ開発者の皆様にご参加いただいた「Android セキュアコーディングセミナー」の第 2 弾を 10 月 17 日（水）に実施しました。

3 部から構成される本セミナーでは、まず第 1 部で Android アプリを巡るセキュリティの現状を概観し、セキュアなアプリ開発の重要性を確認しました。第 2 部では脆弱な Android アプリの実例を題材に、アプリの設計やコーディングの何が問題で脆弱性が作り込まれてしまったのか、問題を回避するためにはどのような設計やコーディングをすべきであったかについて解説しました。第 3 部では、あらかじめ複数の脆弱性が作り込まれたサンプルの Android アプリ（RSS リーダー）を受講者に提供し、アプリを実際に動かしたり、各自用意した開発環境を使ってデバッグやコードレビューを行ったりすることを通じて、脆弱な箇所の特定と修正を体験していただきました。

今後も JPCERT/CC は、安全な Android アプリケーション開発を行うための技術情報収集や啓発活動を継続していく予定です。

2.5.4. 「関西オープンソース 2012」および「オープンソースカンファレンス 2012 Fukuoka」にて Android アプリのセキュリティについて講演

オープンソースソフトウェアに関わる方や Android アプリケーション開発に携わるディベロッパーの方々に JPCERT/CC の活動を知っていただくとともに、近年脆弱性の届け出が増加傾向にある Android アプリの脆弱性とその対策の重要性についての啓発を行うことを目的として、関西オープンソース 2012（以下 KOF2012）およびオープンソースカンファレンス 2012 Fukuoka（OSC 2012 Fukuoka）に参加し、以下の講演を行いました。

関西オープンソース 2012
「Android セキュアコーディングのツボ」講演者：熊谷 裕志
講演資料 http://2012.k-of.jp/session/258

オープンソースカンファレンス 2012 Fukuoka
「Android セキュアコーディング - 安全な Android アプリ開発のための心得」講演者：戸田 洋三
講演の動画 http://www.ustream.tv/recorded/27567367

オープンソースカンファレンス 2012 Fukuoka での講演の様子

2.5.5. @IT「もいちど知りたい、セキュアコーディングの基本」連載開始

ITmedia が運営するウェブマガジン、アットマーク・アイティにおいて「もいちど知りたい、セキュアコーディングの基本」と題した連載を担当することになりました。C/C++言語を使ったコーディング上の注意点や脆弱性を作り込まない作法を、2011 年に改訂された最新の言語仕様に関するトピックスや脆弱なプログラムの事例なども交えつつ紹介していきます。本四半期は、次の 2 つの記事が掲載されました。

第 1 回「なぜ、いま『セキュアコーディング』なのか？」(10 月 25 日公開)
http://www.atmarkit.co.jp/ait/articles/1210/24/news005.html
第 2 回「C でポピュラーな脆弱性とバッファオーバーフロー（前編）」(12 月 26 日公開)
http://www.atmarkit.co.jp/ait/articles/1212/26/news006.html

2.5.6. 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。今年度から、これまで提供していた 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、新たに 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。本四半期は、国内メーカー3 社に対して、Java および Android アプリ開発におけるセキュアコーディングセミナーを実施しました。

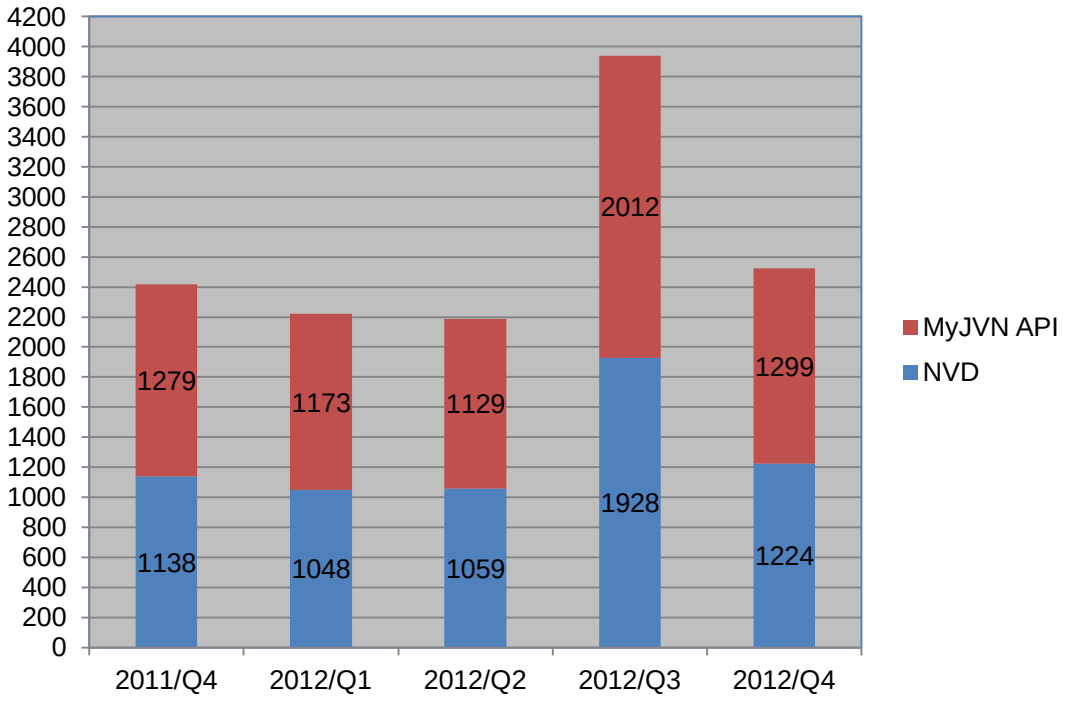
※出張セミナーのご依頼、お問合せは、secure-coding@jpcert.or.jp までご連絡下さい。

2.6. VRDA フィードによる脆弱性情報の配信

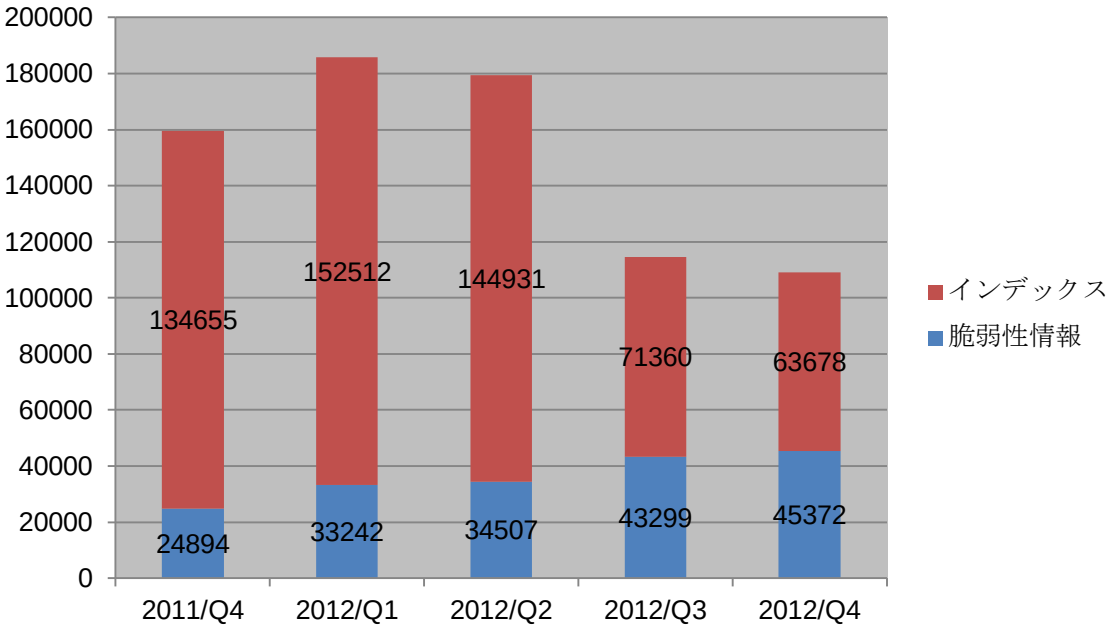
JPCERT/CC は、大規模組織の組織内 CSIRT などでの利用を想定して、KENGINE などのツールを用いた体系的な脆弱性対応を可能とするため、IPA が運用する MyJVN API および NIST (National Institute of Standards and Technology)の NVD (National Vulnerability Database) を外部データソースとして利用した、VRDA (Vulnerability Response Decision Assistance)フィードによる脆弱性情報の配信を行っています。VRDA フィードについての詳しい情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

本四半期に配信した 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。

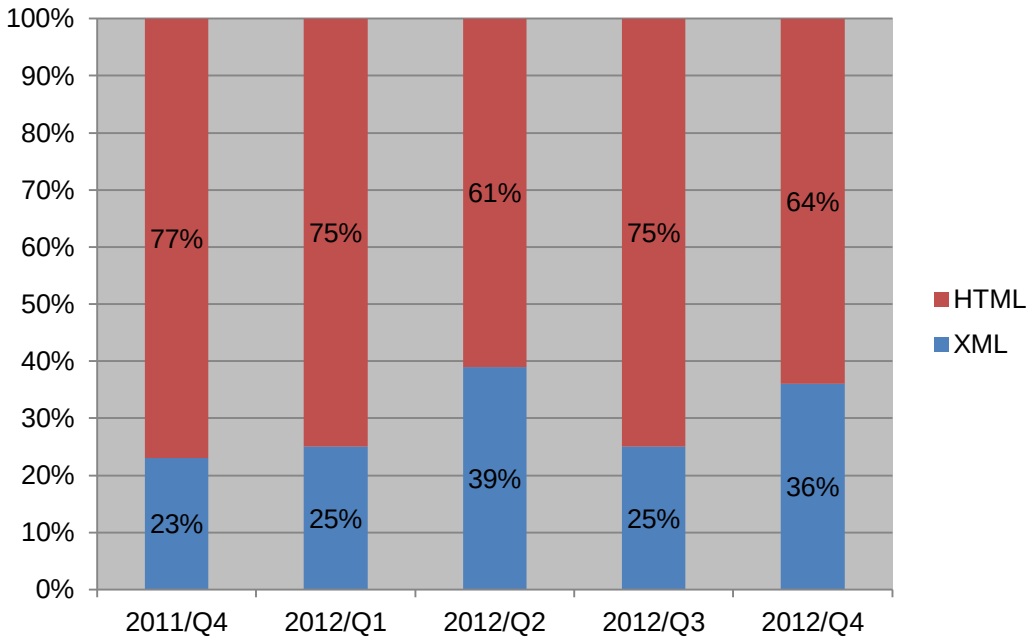


[図 2-5 VRDA フィード配信件数]



[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と脆弱性情報の利用数に大きな変化は見られませんでした。



[図 2-7 脆弱性情報のデータ形式別利用割合]

[図 2-7] 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 形式の脆弱性情報の利用割合が増加しました。

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。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）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。

3.1. 「マルウエア対策研究人材育成ワークショップ 2012(MWS 2012)」への参画

「マルウエア対策研究人材育成ワークショップ 2012(MWS 2012)」(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 30 日から 3 日間の日程で島根県立産業交流会館（くにびきメッセ）にて開催されました。MWS は、「MWS データセット」と呼ばれる共通の研究用データセットを対象として、分析手法等に関する研究発表を行うワークショップです。

MWS の参加者に解析への関心や理解を高めていただくために、「MWS ハンズオン」という新しい取組みが今回から行われることになりました。この取組みの中で、JPCERT/CC は、これから解析を始めようとしている研究者や学生を主なターゲットとしたコースを企画し、「はじめての静的解析」として実施しました。このコースは、10 月 30 日の午前中に MWS Cup 2012 と同じ会場で 30 名以上の参加者を迎えて開催されました。

マルウエア対策研究人材育成ワークショップ 2012（MWS 2012）
http://www.iwsec.org/mws/2012/

はじめての静的解析コースの様子

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、本年度より月刊で、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。本四半期は号外も含め計 7 回（10 月 31 日、11 月 6 日、11 月 9 日、11 月 30 日、12 月 6 日、12 月 13 日、12 月 28 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 232 名のメンバー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. 国内外情報収集活動

米国国土保安省（DHS）の下で Control Systems Security Program（CSSP）として進められている活動の一環として、2012 年 10 月にコロラド州デンバーにおいて「ICSJWG コンファレンス」が開催されました。また、ICS-CERT 連携先関係者よる「国際パートナー・ディ」の第 2 回も開催され、経済産業省による日本の制御システムセキュリティへの取り組みの紹介も行われました。JPCERT/CC はこれら両行事に参加し、制御システムセキュリティにおける米国の取り組みや現状についての情報収集に努めました。また、それ以外にも、制御システムセキュリティに関連する各種コンファレンスへ参加し、情報共有や収集情報の展開にも取り組んでいきます。

ICSJWG 2012 Fall Conference Agenda
http://www.us-cert.gov/control_systems/icsjwg/2012/fall/agenda-tue.html
http://www.us-cert.gov/control_systems/icsjwg/2012/fall/agenda-wed.html
http://www.us-cert.gov/control_systems/icsjwg/international-partners/2012/fall/agenda.html

4.3. 制御システム関係者向けセキュリティインシデント対応トレーニングを実施

制御システム関係者（ユーザ・ベンダ・研究者）の方々を対象としたセキュリティインシデント対応トレーニングを、11 月 20 日、21 日の 2 日間、福岡で実施しました。本トレーニングは、制御システムネットワークで代表的な３階層ネットワークと制御システムシミュレータを用いた模擬的な環境で、制御システムに携わる方々に、セキュリティインシデントへの気付きやインシデント対応に必要な技術を体感していただくものです。今年度内に、大阪/名古屋、および東京（２回）でも開催を予定しています。

4.4. 日本版 SSAT 配布状況

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 の配布を行なっています。このツールに対してベンダや業界団体がカスタマイズを加えるなどして再配布することも許諾しています。本四半期は、JPCERT/CC に対して 21 件の利用申込みがあり、直接配布件数の累計が 129 件となりました。

4.5. 関連団体との連携活動

ほぼ毎月開かれている 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）の活動に参加し、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。本四半期は主として、制御システム向けのチェックツールの作成に向けて、各業界のユーザからの意見も伺いながら最終的にチェックリストとして配布するための調整活動を行いました。

4.6. 制御システム業界におけるインシデントおよび脆弱性ハンドリング活動開始準備

制御システム業界におけるインシデントおよび脆弱性ハンドリングの調整機関としての活動を本格的に展開するための準備を進めています。インシデントハンドリングに関しては、主として制御システム固有のインシデントを報告いただくための報告フォームの準備や情報システムに関する従来のインシデント対応調整スキームとの連携の仕組みの検討などを行いました。脆弱性ハンドリングに関しては、前四半期から継続して、主な制御システム・ベンダーや関連業界の代表者に参加いただき、国内での取扱いのあり方を議論いただくため、制御システム向け脆弱性研究会の第２回会合、ワーキンググループの第 1 回から第 3 回を開催しました。

4.7. 講演活動

大阪で行われた「計測展 2012OSAKA」（一般社団法人　日本電機制御機器工業会主催）の 2 日目にあたる 11 月 1 日に「制御システムセキュリティ動向と JPCERT/CC」「制御システムセキュリティ向上に向けた取り組み～J-CLICS 公開までの軌跡～」と題する講演を行いました。

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、改版された草案が国際標準草案(DIS： Draft of International Standard)として 9 月下旬に配布され、12 月 25 日を締切日とする投票に付されました。これは DIS の段階の最初の国際投票の前に各国における翻訳のための時間的を確保するため 6 か月間の猶予期間を置くための措置で、この間に開催された SC27 国際会議でも論議はなされていません。また、DIS の段階に達した草案に対しては技術的なコメントを行わない旨の紳士協定があります。投票に付された草案を分析したところ、作業中を示すエディターのコメントが残ったままになっている箇所があるなど、編集上の誤りや不整合が多数見つかりました。このため、国内委員会における審議を経て、国際標準として採択できる文書としての品質水準に達していないとの理由で、35 件の修正要求コメントを付して国際標準として採択することに反対する投票を情報規格調査会からしていただきました。

「脆弱性取扱手順」については、6 月に配付された第 1 次委員会草案(CD： Committee Draft)に対するコメントが 9 月に SC27 事務局に集められ、10 月 22 日から 26 日にローマ郊外にあるトゥールベルガータ大学を会場とした SC27 ローマ会合で対応方針が議論されました。その会合に JPCERT/CC は日本の代表団の一員として参加しました。各国からのコメントは合計 22 件(日本から 7 件、韓国から 5 件、米国から 2 件、FIRST から 8 件)ありましたが、ほとんどは編集上の不備の指摘であり、大きな意見の対立もなく対処方針について合意が得られ、改版後に国際標準草案(DIS： Draft of International Standard)として投票に付されることになりました。会合後にエディターが改版した草案は 11 月に配付され、2013 年 4 月 14 日を締切日とする投票に付されています。

JPCERT/CC では、脆弱性の取扱いに関連した 2 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を通じて、引き続き、この国際標準が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いく所存です。

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 SC27/WG4 において、次の 3 つのパートから構成されるインシデント管理に関する標準の策定作業が進められています。

Part 1. インシデント管理の原理（Principles of Incident Management）
Part 2. インシデント対応の計画と準備ためのガイドライン（Guidelines to Plan and Prepare for Incident Response ）
Part 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）

10 月 22 日から 26 日にローマ郊外にあるトゥールベルガータ大学を会場とした SC27 ローマ会合が開催され、JPCERT/CC は日本の代表団の一員としてこの会合に参加しました。

同会合に先立ち、現在 1st WD の段階にある各パートの草案に対して各国（日本、ベルギー、南アフリカ

共和国、スウェーデン、アメリカ）がコメントを提出しており、日本は Part1 に対して 14 件、Part3 に対して 10 件のコメントを提出ました。Part2 については、1st WD の内容が目次案レベルであることもあり、コメントの提出は見送りました。

会合では、各パートのスコープについて議論が行われ、結果的に Part2 と Part3 の構成が大幅に変更されることになりました。具体的には、Part3 で記述する計画だった CSIRT 構築に関する章（"Establishment of the Computer Security Incident Response Teams (CSIRTs)"）が Part1 および Part2 に移され、Part3 のスコープはインシデント対応のオペレーションに関する内容に特化したものになりました。Part2 のスコープについては、Part1 で示された"Plan and Prepare"フェーズおよび 4 章 5 節の"Lessons Learned"フェーズの一部を Part2 において記述することが合意されました。今後、これらの変更を反映した 1st WD の草案の再構成と、コメントの処理がエディターによって実施され、2nd WD の草案がまとめられることになります。

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標準化組織である情報規格調査会を通じて、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. ラオスの CSIRT 構築支援活動(2012 年 10 月 15 日-19 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計 5 日間に渡って行いました。LaoCERT のスタッフ及びその母体組織である LANIC（Lao National Internet Center）のスタッフ計 15 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や PGP の使い方、JPCERT/CC が運営している TSUBAME について等の講義とハンズオン演習を行いました。
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、一部の講義をラオ語と言語的に近いタイ語にて行いました。また、独立法人国際協力機構(JICA)がラオスで行っている「国立大学 IT サービス産業人材育成プロジェクト」とも連携し、本トレーニングを受講する LaoCERT と LANIC のスタッフが、トレーニングに先立って JICA のネットワーク研修を受講し、基礎知識を身につけた上でトレーニングに臨めるよう調整しました。

6.1.2. ミャンマーの CSIRT 構築支援活動（2012 年 11 月 4 日－17 日）

JPCERT/CC は、経済産業省の「貿易投資円滑化支援事業」を受託している財団法人海外貿易開発協会海外産業人材育成協会（HIDA）からの公募・選定を経て、ミャンマーにおける CSIRT 構築・運用支援のために現地に専門家を派遣する機関に指定され、11 月 5 日から 9 日に実施された高度マルウエア解析研修、11 月 12 日から 16 日まで実施されたインシデントハンドリング研修にそれぞれ 2 名ずつの講師を派遣しました。派遣先はミャンマーの National CSIRT である mmCERT で、同組織のスタッフと ISP など約 40 名の技術者に対して、技術指導を行いました。

6.1.3. アフリカ CSIRT 構築支援 等(2012 年 11 月 25 日-27 日)

JPCERT/CC は､11 月にスーダンの首都ハルツームで開催された国際会議 Afrinic-17 に参加するとともに、2 日間にわたるアフリカ諸国向けの CSIRT トレーニングを行いました。また 11 月 26 日に開催された AfricaCERT Workshop に参加しました。
JPCERT/CC が担当した CSIRT トレーニングは、Afrinic-17 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 5 回目の開催となります。今回 2 日間のトレーニングはスーダンと隣国のリビヤからの参加者を中心に合計 30 名以上が参加しました。
11 月 24 日は「CSIRT for Manager」と題し CSIRT のマネージャーとなるべき層に対して情報セキュリティの概括の説明、CSIRT を設置することの意義、その設置の具体的な方法を説明しました。JPCERT/CC は TA（Teaching Assistant)という形で現地講師のサポートを行いました。
11 月 25 日は「CSIRT for Technical Staff」と題し、CSIRT の技術者向けに、インシデントハンドリングという必須業務の概要の説明及び典型的な事例への対処法を座学で講習しました。その後演習形式をとり、現実に発生したインシデントへの対応をグループワークで行いました。JPCERT/CC は主任講師として講義とハンズオンを実施しました。
11 月 26 日の AfricaCERT Workhop 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､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 APCERT 事務局として、OIC-CERT との MOU 締結などの活動について説明を行いました。
Afrinic 及び Afrinic-17 についての詳細は、次の URL をご参照下さい。

Afrinic および Afrinic-17 公式ページ
http://meeting.afrinic.net/afrinic-17/

6.1.4. 国際的な情報セキュリティ組織加盟手続きに関する支援

アジア太平洋地域の CSIRT の協力連携の枠組みである APCERT (Asia Pacific Computer Emergency Response Team)や、インシデント対応組織による世界的なフォーラムである FIRST (Forum of Incident Response and Security Teams)などの国際組織への加盟を希望するアジア諸国の CSIRT に対して、APCERT や FIRST の活動を紹介し、加盟手続きに関する支援等を行いました。

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 連携の取組みにも積極的に参画しています。

6.2.1. アジア太平洋地域(オセアニア)における活動

6.2.1.1. 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 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/

6.2.1.1.1. APCERT Steering Committee 電話会議の実施

10 月 2 日および 12 月 4 日に Steering Committee(運営委員)のメンバ間で電話会議を行い、今後の APCERT 運営方針について議論を行いました。

6.2.1.1.2. APCERT チーム間および他組織間との連携

1) 10 月 15 日、APCERT チーム間でインシデントなどの情報共有を行う際に、取り扱う情報の機密性や共有可能範囲を明確にすることを目的とした情報分類ポリシーを公開しました。本ポリシーは、国際 CSIRT コミュニティで広く利用されている Traffic Light Protocol (TLP)に基づいて、APCERT のワーキンググループ(WG)の一つである情報分類 WG が主導的に纏めたものです。

2) APCERT のワーキンググループ(WG)の一つであるメンバーシップ WG (議長：KrCERT/CC)が 11 月中旬、APCERT への加盟基準やメンバーシップの分類などの見直しを目的としたアンケート調査を APCERT チームに対して実施しました。本アンケート調査の結果を受けて、APCERT の今後のメンバーシップのあり方があらためて検討される予定です。

3) Anti-Phishing Working Group (APWG)と National Cyber Security Alliance (NCSA)の主導により設立された米国の STOP. THINK. CONNECT. Messaging Convention と APCERT 間における今後の連携強化を目的とした MOU の締結に関する共同声明を 11 月 21 日に発表しました。

6.2.1.2. 覚書(MOU)締結

CSIRT 間の協調関係に明示的な根拠を与え、また、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 を締結しました。

-CERT.GOV.AZ(アゼルバイジャン)

6.2.1.3. 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(2012 年 11 月 5 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」を受講中の研修員 9 名（バングラデシュ、モンテネグロ、パナマ、フィリピン、サウジアラビアの政府系組織の IT 担当者等）が JPCERT/CC の事務所に来訪しました。JPCERT/CC から 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行った後、活発な意見交換が行われ、日本およ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。

6.2.1.4. 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。
10 月 30、31 日、11 月 1 日に中国杭州で開催された「2012 2nd IEEE International Conference on Cloud Computing and Intelligent Systems」のクラウド・コンピューティング・セキュリティ WG に、論文発表司会チェアとして参加しました。
11 月 7、8 日に中国上海で開催された「2012 首届工业控制系统信息安全峰会」、同月 22、23 日に中国上海で開催された「互联网安全论坛（ISF）」、同月 28、29、30 日に中国武漢で開催された「第一届全国网络与信息安全防护峰会」および 12 月 8、9 日に中国上海で開催された「2012 年网络计算与信息安全国际会议」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。講演内容や講演会にて行われた意見交換の内容等の情報については、日本国内の関係者会合などへ展開しました。

6.2.2. その他の地域における活動

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

JPCERT/CC は FIRST に加盟しています。JPCERT/CC の理事 山口英は FIRST の Steering Committee のメンバを務めており、10 月 1 日-3 日に米国カリフォルニア州サンノゼで開催された SC 会合に出席しました。
FISRT 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

6.2.2.1.1. FIRST スポンサー（他の CSIRT の加盟手続き支援）

国内外の CSIRT のスポンサー（加盟チームに関する保証を与え、FIRST の規約に従い加盟手続を支援するチーム）を務めるべく、書類作成等を行いました。
今四半期は、モバゲーなどで知られる株式会社ディー・エヌ・エーの CSIRT（DeNA CERT）のスポンサーとなり、2012 年 11 月、同組織の加盟が FIRST より承認されました。

6.2.2.1.2. FIRST Technical Colloquium in Kyoto 開催支援（2012 年 11 月 13 日-15 日）

11 月 13 日から 15 日まで" FIRST Technical Colloquium in Kyoto"が京都市国際交流会館で開催されました。FIRST Technical Colloquium は FIRST 加盟 CSIRT 間での情報共有を目的として、世界各地で年に数回開催されています。今回は山口英(JPCERT/CC 理事)、寺田真敏氏((株)日立製作所　HIRT)の共同委員長のもと、日本に拠点を置く FIRST 加盟 CSIRT が共同でその企画と運営にあたりました。JPCERT/CC は運営委員の一員として、特に"Future of Global Vulnerability Reporting Summit"という企画の運営に携わりました。
"Future of Global Vulnerability Reporting Summit"は本会議のプログラムの 1 つで、各国の脆弱性情報流通の専門家が集い、3 日間にわたって現在の脆弱性情報流通(中でも脆弱性識別番号)の課題と今後の改善策について議論を行いました。新たに指摘された様々な課題について、今後ワーキンググループを組織して関係者間での議論を継続することを FIRST に提案することが、承認されました。
本会議の詳細については、次の URL をご参照ください。

Kyoto 2012 FIRST Technical Colloquium
http://www.first.org/events/colloquia/kyoto2012

6.2.3. 米 US-CERT/ICS-CERT への訪問（2012 年 11 月 28 日）

米国の US-CERT および ICS-CERT を訪問し、JPCERT/CC との連携活動（日米におけるインシデント動向の共有、マルウエア分析結果の共有、CSIRT 構築支援に係る日米連携）について協議を行いました。さらに、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 CIP-Forum に参加し、重要インフラ保護および制御系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。また同フォーラムでは JPCERT/CC からいわゆる APT 攻撃の現状と日本での対策の取り組みについて講演を行いました。

6.2.4. 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。

CSIRT Trainings for ThaiCERT and LaoCERT (2012/11/16)
http://blog.jpcert.or.jp/2012/11/csirt-trainings-for-thaicert-and-laocert.html

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

7. 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。

7.1. 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の報告を、それぞれ複数受けました。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やサイトの関連情報を提供しました。また、Web メールサービスをかたるフィッシングに関しては、「au をかたるフィッシング（10 月 26 日）」 [図 6-1]の緊急情報を、第二認証情報を詐取するフィッシングについては「三井住友銀行をかたるフィッシング(11 月 12 日)」、「みずほ銀行をかたるフィッシング(11 月 22 日)」を協議会の Web 上で公開しました。さらに、当該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、フィッシングサイトの停止を確認しました。

[図 6-1　au をかたるフィッシングサイト
https://www.antiphishing.jp/news/alert/au_20121025.html]

7.2.　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事業者である会員、フィッシングに関する研究を行っている学術機関である会員に対し、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。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が目的です。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 17 組織、現在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っており、提供先を順次拡大していく予定です。

7.3.　講演活動

本四半期の講演活動はありませんでした。

7.4.　ワーキンググループ会開催

本四半期は、ガイドライン策定 WG 及び国際連携 WG を開催いたしました。
ガイドライン策定 WG は、主に一般消費者におけるフィッシング被害の抑制のための啓発資料として、フィッシング被害の抑止のために有効な技術的対策やサービスなどの利用上の留意点、重要情報を盗まれたかもしれないと感じたときの事後対処のあり方などをまとめたガイドラインの検討を進めています。
国際連携 WG は、海外におけるフィッシングの状況や対策の取り組み事例、フィッシング対策に関する教育ツールなどについて、情報の収集、国内への展開の検討などを行っています。

本四半期のガイドライン策定 WG 及び国際連携 WG 開催実績は、以下のとおりです。

(1) ガイドライン策定 WG（第 1 回会合）
日時：2012 年 11 月 26 日　14:00 - 15:30
場所：一般社団法人 JPCERT コーディネーションセンター

(2) ガイドライン策定 WG（第２回会合）
日時：2012 年 12 月 21 日 16:00 - 18:00
場所：株式会社三菱総合研究所

(3) 国際連携 WG（第１回会合）
日時：2012 年 12 月 10 日 16:00 - 18:00
場所：株式会社日立システムズ

7.5. 海外カンファレンス参加

2012 年 10 月にプエルトリコで開催された eCrime Research Summit 2012 Puerto Rico に参加し、海外におけるフィッシング詐欺やフィッシング対策プロジェクトについて情報収集を行い、その結果を国際連携 WG で報告しました。

7.6. 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 2012 年 10 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201210.html
フィッシング対策協議会 2012 年 11 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201211.html
フィッシング対策協議会 2012 年 12 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201212.html

8. フィッシング対策協議会会費による活動

8.1. フィッシング対策セミナー2012 開催

2012 年 12 月 14 日に、東京の楽天株式会社において「フィッシング対策セミナー2012」を開催しました。定員を上回るご応募をいただき、227 名の方にご参加いただきました。セミナーのプログラムは次のとおりです。

13:10-14:00	「不正アクセス禁止法改正と警察の取り組みについて」 警察庁生活安全局 情報技術犯罪対策課 警視 吉田光広氏
14:10-15:00	「dkim.jp の取り組みについて」

	Japan DKIM Working Group 議長 赤桐壮人氏
15:10-16:00	「フィッシング対策と CSIRT について」 株式会社みずほ銀行 参事役 谷合通宏氏
16:10-16:50	「フィッシングの動向について ～狙われる金融機関～」 フィッシング対策協議会事務局 山本健太郎氏

8.2. 運営委員会開催

本四半期においては、以下のとおり、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。

(1)フィッシング対策協議会 第 2 回運営委員会
日時：2012 年 10 月 17 日 16:00 - 18:00
場所：JPCERT コーディネーションセンター

9. 公開資料

JPCERT/CC が今期に公開した調査・研究の報告書や論文、セミナー資料は次のとおりです。

9.1. 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います。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、これらインターネット定点観測の状況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 2012 年 7～9 月 (2012 年 12 月 19 日)
https://www.jpcert.or.jp/tsubame/report/report201207-09.html
インターネット定点観測レポート 2012 年 4～6 月 (2012 年 10 月 25 日)
https://www.jpcert.or.jp/tsubame/report/report201204-06.html
インターネット定点観測レポート 2012 年 1～3 月 (2012 年 10 月 25 日)
https://www.jpcert.or.jp/tsubame/report/report201201-03.html

10. 講演活動一覧

(1) 山本 健太郎(フィッシング対策協議会事務局)：
「フィッシングの動向について ～狙われる金融機関～」

フィッシング対策セミナー,2012 年 12 月 14 日

(2) 戸田 洋三(情報流通対策グループリードアナリスト):

「職業的情報学 I－インターネットとセキュリティ」

千葉大学理学部数学・情報数理学科,2012 年 12 月 13 日

(3) 有村 浩一(常務理事):

「最近の事例におけるサイバー攻撃の傾向と対策～JPCERT/CC の取り組みと情報連携のあり方～」

経済産業新報社 IT Forum 地方自治組織における危機管理～サイバー攻撃対応編～

2012 年 12 月 5 日

(4) 真鍋 敬士(理事,分析センター長):

「情報セキュリティにおけるインシデントの傾向紹介」

TCG 日本支部(JRF)東京ワークショップ,2012 年 11 月 28 日

(5) 真鍋 敬士(理事,分析センター長):

「攻撃事例に見る情報連携の役割と取り組みの紹介」

InternetWeek2012,2012 年 11 月 19 日(水)

(6) 早貸 淳子(専務理事):

「組織内 CSIRT（シーサート）～サイバー攻撃から逃れることができない理不尽さに向き合う組織の司令塔～」

Smart City Week 2012, 2012 年 10 月 31 日

(7) 小宮山 功一朗 (国際部マネージャ):

「サイバー空間における脅威の最新動向と連携の必要性」

情報セキュリティワークショップ in 越後湯沢 2012, 2012 年 10 月 12 日

(8) 満永 拓邦 (早期警戒グループ リーダ 情報セキュリティアナリスト):

「最近のセキュリティ動向」

千葉県インターネット防犯連絡協議会総会, 2012 年 10 月 10 日

(9) 満永 拓邦 (早期警戒グループ リーダ 情報セキュリティアナリスト):

「最近のセキュリティ動向」

第 10 回 NTT-CERT ワークショップ, 2012 年 10 月 04 日

(10) Jack YS LIN(制御システムセキュリティ対策グループ,早期警戒グループ 情報セキュリティアナリスト)

「Information Security trends in Japan」

Cyber Security UAE Summit 2012－ドバイ,2012 年 10 月 02 日

11. 執筆一覧

(1) 戸田 洋三(情報流通対策グループリードアナリスト):

もいちど知りたい、セキュアコーディングの基本(2)

「C アプリでポピュラーな脆弱性とバッファオーバーフロー（前編）」

アイティメディア ＠IT,2012 年 12 月 26 日

(2) 久保 正樹(情報流通対策グループ 脆弱性アナリスト)：
もいちど知りたい、セキュアコーディングの基本(1)
「なぜ、いま「セキュアコーディング」なのか？」
アイティメディア @IT,2012 年 10 月 25 日

12. 開催セミナー等一覧

(1) Java セキュアコーディングセミナー
※本セミナーの詳細は、「2.5.1~2.5.4」をご参照ください。
(2) 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、「2.5.6」をご参照ください。
(3) MWS Cup 解析／MWS ハンズオン(はじめての静的解析)
※本セミナーの詳細は、「3.1」をご参照ください。

13. 協力、後援一覧

(1) 第 9 回デジタルフォレンジックコミュニティ 2012inTOKYO
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 2012 実行委員会
開催日：2012 年 12 月 10 日(月)～11 日(火)
(2) TCG 日本支部(JRF)東京ワークショップ
主　催：TCG 日本支部(JRF)
開催日：2012 年 11 月 28 日(水)
(3) Internet Week 2012
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：2012 年 11 月 19 日(月)～22 日(木)
(4) 情報セキュリティワークショップ in 越後湯沢 2012
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：2012 年 10 月 12 日(金)～13 日(土)
(5) Email Security Conference2012
主　催：株式会社ナノオプト・メディア
開催日：東京 2012 年 10 月 5 日(金)、大阪 2012 年 10 月 19 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

■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　：cs-security-staff@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、その他のお問い合わせ　：office@jpcert.or.jp