JPCERT/CC®

JPCERT-PR-2012-02
発行日 ：2012-10-10

JPCERT/CC 活動概要 [2012 年 7 月 1 日 ～ 2012 年 9 月 30 日]

活動概要トピックス

—トピック 1—
いわゆる攻撃の特異日前後に発生するサイバー攻撃への対応

歴史上の出来事等に起因する、いわゆるサイバー攻撃の特異日（8 月 15 日や 9 月 18 日など）の前後には、日本の政府関係組織等に向けた反日的なサイバー攻撃が発生する可能性が高まることから、JPCERT/CC では、関係する各国の National CSIRT と連携して、特に注意深く情報収集を行っています。

本年度は、2012 年 8 月中下旬 に一部の民間サイトに対する DDoS や国内の複数のサイトにおける Web サイトの改ざんが発生したほか、9 月上旬に中国のサイト上で日本のサイトへの攻撃の呼びかけが行われたこと、9 月 18 日の前後を中心に国内の複数のサイトに対する DDoS 攻撃や Web サイトの改ざんが発生したことを確認しています。
JPCERT/CC では攻撃に備えた対応態勢をとるとともに、攻撃への事前対策を促す早期警戒情報の提供や、攻撃用に配付されたツールの分析、改ざんされたサイトの管理者に対する情報提供や問題解決の支援を行いました。

これらの一連の Web サイト改ざんでは、尖閣諸島に関する中国側の意見を主張する画像が挿入されていましたが、改ざんの対象となったサイトについては、業種や規模などに共通性は見いだせませんでした。日本のサイトを対象に検索ツールを使って脆弱性を探しまわり、発見した脆弱点をついてサイトに不正に侵入し、用意した画像を設置する手法がとられたと考えられます。

―トピック 2―

増加する Android 関連の脆弱性情報の報告と製品開発者による積極的な対応等

JPCERT/CC が独立行政法人情報処理推進機構（以下「IPA」といいます。）と連携して運用するソフトウエア等の脆弱性関連情報の流通の枠組み（「2. 脆弱性関連情報流通促進活動」 参照）においては、2012 年初頭から、Android およびその関連製品の脆弱性情報の報告が増加し続けています。これら製品の脆弱性の報告の増加は、スマートフォンやタブレット機器の普及によって、多くのアプリケーション開発者が参入し、非常に多数のアプリケーションが開発され、提供されていることに伴う傾向とも言えますが、本四半期を含む最近の報告については、Android WebView の使い方に起因した、アプリケーションが管理するユーザ情報を窃取できる脆弱性または任意の Java メソッドが実行可能になる脆弱性のカテゴリに分類されるものが多くを占めています。

一部の製品開発者におかれては、このタイプの脆弱性を意識して Android WebView の使い方の見直しに着手されている模様で、製品開発者が自ら発見した脆弱性を、対策とともに JVN の枠組みにそって速やかに公表されたケースも複数見られ、脆弱性問題に対するプロアクティブな製品開発者の対応事例として注目されます。

また、JPCERT/CC では、Java・Android のセキュアコーディングセミナーを通じた啓発活動にも力を入れています。このコースでも WebView の使い方に由来する脆弱性への対策を取り上げており、開発時から脆弱性を作り込まないための実践的な内容であると高い評価を得ています。本四半期には、札幌と東京で学生向けのセキュアコーディングセミナーを開催した他、技術誌などへの寄稿を通じた啓発活動にも力を注ぎました。

Android 関連の脆弱性情報の報告は今後も増加傾向が続くものと考えられ、JPCERT/CC では報告される脆弱性関連情報の取扱いによる事後対策と、セキュアコーディングセミナー等を通じた事前対策の両面からの対応を強化していきます。

―トピック 3―

制御システム・セキュリティ対応に向け体制整備から業務拡充へ

JPCERT/CC では、2008 年頃から制御システムのセキュリティ問題に注目し、問題提起や海外の関連技術資料の邦訳や普及啓発を行ってきました。2011 年度に経済産業省が実施した制御システム・セキュリティ・タスクフォースにおける検討を受けて、JPCERT/CC では、脆弱性およびインシデントに対する対応のための国内体制の整備やそのために必要な関係者との合意形成を進めています。9 月には主な業界関係者を委員とする「制御システム用製品の脆弱性情報の取扱に関する研究会」(委員長は土居中央大学教授)を開始するなど、徐々に本格的な活動をスタートしています。

この分野の技術開発やテストベッドの構築を行う技術研究組合「制御システム・セキュリティ・センター」や、標準化への貢献と認証プログラムの策定を目指すIPA、さらには関連の業界団体との連携協調を図りつつ、制御システムのセキュリティ強化に向けて、一層の取組み強化を進めます。

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」、「9.講演活動一覧」、「10.執筆一覧」及び「11.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 5430 件、インシデント件数ベースでは 5266 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 1123 件でした。前四半期の 756 件と比較して 49%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/2012/IR_Report20121010.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 273 件で、前四半期の 367 件から 26%減少しました。また、前年度同期（226 件）との比較では、21%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	7 月	8 月	9 月	国内外別合計(割合)
国内ブランド	17	26	14	57(21%)
国外ブランド	56	54	51	161(59%)
ブランド不明(注 2)	15	15	25	55(20%)
月別合計	88	95	90	273(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。

本四半期は、国内のブランドを装ったフィッシングサイトの件数が 57 件と、前四半期の 68 件から 16%減少しました。国外ブランドを装ったフィッシングサイトの件数は 161 件と、前四半期の 225 件から 28%減少しました。

本四半期は、国内通信事業者を装ったフィッシングサイトの報告が複数寄せられました。複数の異なるブランドのフィッシングサイトを確認しましたが、ブランドが異なっていても同じドメインを使用しているものや、サブディレクトリ名が類似しているものがありました。その背景としては、横断的に日本の通信事業者のアカウントの窃取を狙っている攻撃者か、日本の通信事業者を装うフィッシングサイトを構築するためのツールが存在するといった可能性が考えられます。

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%と、前四半期の割合（国内 50%、国外 50%）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、796 件でした。前四半期の 139 件から 473%増加しています。

本四半期は、Web サイトが使用する JavaScript ファイルが改ざんされているという報告が非常に多く寄せられたため、Web サイト改ざんの件数が大きく増加しています。この改ざんは、ホスティング・サービス業者などが利用している、あるサーバ管理ツールの脆弱性を使用して大規模に行われた可能性があります。

2012 年 8 月には、同月にゼロデイ脆弱性として公開された Java の脆弱性(CVE-2012-4681)が、改ざんされた Web サイトから誘導されるマルウエア配布サイトの攻撃に組み込まれたことを確認しました。この脆弱性を使用した攻撃により、古いバージョンの Java を使用していると、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。

1.2.1. 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)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：11 件　https://www.jpcert.or.jp/at/

2012-07-11　2012 年 7 月 Microsoft セキュリティ情報 (緊急 3 件含) に関する注意喚起
2012-08-15　2012 年 8 月 Microsoft セキュリティ情報 (緊急 5 件含) に関する注意喚起
2012-08-15　Adobe Flash Player の脆弱性 (APSB12-18) に関する注意喚起
2012-08-15　Adobe Reader 及び Acrobat の脆弱性 (APSB12-16) に関する注意喚起
2012-08-22　Adobe Flash Player の脆弱性 (APSB12-19) に関する注意喚起
2012-08-23　MS-CHAP v2 の認証情報漏えいの問題に関する注意喚起
2012-08-31　2012 年 8 月 Java SE の脆弱性に関する注意喚起
2012-09-03　2012 年 8 月 Java SE の脆弱性に関する注意喚起
2012-09-13　ISC BIND 9 サービス運用妨害の脆弱性 (CVE-2012-4244) に関する注意喚起

2012-09-20　2012 年 9 月 Microsoft Internet Explorer の未修正の脆弱性に関する注意喚起
2012-09-24　2012 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 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。

2012-07-04　今一度、DNS Changer マルウエアの確認を
2012-07-11　Thunderbird の開発方針に関する新たな提案
2012-07-19　システム管理者の日 (System Administrator Appreciation Day)
2012-07-25　APWG Phishing Trends Report, 1st Quarter 2012
2012-08-01　Mac OS X のセキュリティアップデートの提供期間に注意
2012-08-08　1024 ビット未満の暗号キーをブロックする Windows 更新プログラム
2012-08-15　Java 6 のサポート期限延長される
2012-08-22　1024 ビット未満の暗号キーをブロックする Windows 更新プログラム提供開始
2012-08-29　JPCERT/CC Web コメントフォーム追加のお知らせ
2012-09-05　Windows Defender Offline
2012-09-12　はじめての暗号化メール (Thunderbird 編) 公開
2012-09-20　DNS Summer Days 2012
2012-09-26　CTF チャレンジジャパン 2012

1.2.1.3. 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、大きな影響を与えうる脅威について「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/

1.2.2. 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。

(1)脆弱性検査ツールを使用した Web サイトに対する攻撃に関する情報収集・提供

2012 年 6 月頃から、地方自治体や都道府県警察の Web サイトの問合せ窓口に、大量の通知メールが届くと言うインシデントが発生しました。
JPCERT/CC では、被害を受けた組織および関係組織から情報提供を受け、原因の調査を行ったところ、Web サイトに設置された問合せフォームに対して、脆弱性検査ツールを使用した無意味な投稿が大量に行われていた事が判明しました。攻撃を受けたシステムでは、問合せフォームに入力された内容を担当者に電子メールで送信する仕様であったため、大量のメールが担当者に届いてインシデントが表面化しました。
今後、同様の Web サイトの脆弱性を狙った攻撃が発生する可能性に鑑み、政府系組織および、重要インフラ等事業者における被害発生防止を目的に早期警戒情報を発行し、セキュリティ対策の実施状況と攻撃の有無、およびそれに伴う実害発生状況を確認するよう促しました。

(2) Java SE JDK 及び JRE の未修正の脆弱性情報に関する情報収集・提供

JPCERT/CC では、2012 年 8 月下旬に Java SE JDK および JRE（以下 「Java SE」 といいます。）バージョン 7 の未修正の脆弱性に関する公開情報を入手しました。これによると、すでに脆弱性の実証コードが公開されており、海外では一部攻撃が発生しているとのことであり、その後、JPCERT/CC において、著名な攻撃ツールに本脆弱性を悪用する追加機能が組み込まれていること、国内においても攻撃サイトが現れだしたことを確認したことから、重要インフラ等事業者における被害発生防止を目的に、本脆弱性の影響を受けない Java SE バージョン 6 への一時的なダウングレードを促す早期警戒情報を発行しました。その後、Oracle 社から本脆弱性を修正した Java SE が公開されたため、国内の企業や組織のシステム管理者を対象に広く脆弱性への対処を呼び掛ける注意喚起を行いました。

(3) 日本に対するサイバー攻撃への対応

歴史上の出来事等に起因する、いわゆるサイバー攻撃の特異日には、日本の政府関係組織等に向けた反日的なサイバー攻撃が毎年のように発生しています。本四半期には、8 月 15 日と 9 月 18 日の 2 つの特異日がありました。JPCERT/CC では、そうした特異日の前後には、関係する各国の National CSIRT と連携して、特に注意深く情報収集を行っています。
2012 年 8 月中下旬には、一部の民間サイトに対する DDoS 攻撃が発生したり、国内の複数のサイトにおいて、一部のページを政治的な主張に書き換える Web 改ざんが発生したことを確認しました。
2012 年 9 月上旬には、中国のサイトで「日本のサイトに対してサイバー攻撃を行おう」との呼びかけ

がなされました。これをうけ、JPCERT/CC では攻撃に備えた対応態勢をとるとともに、攻撃に対する事前対策を促す早期警戒情報の提供を行いました。なお、本件では、一部のサイトで DDoS 攻撃の影響と思われる Web サイトの応答時間の悪化が確認されたものの、関係者の迅速な対応などもあり、おおむね深刻な被害は発生しなかったように見受けられます。一方、Web 改ざん（8 月の事例と類似）の被害も一定数確認されており、JPCERT/CC では、これらサイトの管理者に対して状況の確認の依頼を行うとともに、攻撃に関する情報提供や問題解決の支援を行いました（Web サイトの改ざんについては、「1.1.1.インシデントの傾向」参照）。

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では、インターネット上に設置した複数のセンサーから得られるポートスキャン情報を収集しています。ポートスキャンの動向を観測する目的は、ネットワーク経由の攻撃の準備活動としてポートスキャンが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、新たに公開された脆弱性情報等による攻撃活動の立上り状況を把握することです。観測情報の一部は JPCERT/CC Web ページなどでも公開しています。

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

1.3.1. 定点観測システム観測データを元にしたインシデント対応事例

本四半期において、定点観測システムの観測データを分析して判明した、マルウエア感染や侵入などのインシデント事例と JPCERT/CC による対応について紹介します。

(1) 日本国内の複数企業の IP アドレスを送信元とする、SIP 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。過去の同様の事例では、改造された脆弱性検査ツールが設置されていたサーバ等が異常なパケットを送信していたことが判明しています。
今期増加したパケットや通信の挙動は、以前観測されたものと酷似しているため、同じツールを使用した攻撃活動が引き続き行われていると考えられます。
このツールは、第三者の SIP サーバのアカウントを取得するために、SIP サーバに対し辞書攻撃を行い、取得した SIP サーバのアカウントを攻撃者に送信する機能を有しています。JPCERT/CC では、異常な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、この種のツールの有無の確認と除去を依頼しました。その後、該当サーバから同様のパケットは観測されなくなり、ツールの除去およびその後の被害拡大の抑止ができたと考えられます。

(2) 2011 年 8 月に感染活動が活発化した Morto.Worm は、複数のアンチウイルスベンダの情報などからマルウエアの亜種が複数登場していることがわかっています。検知できない新たな亜種を繰り出す攻撃者と、それらに対応しようとするアンチウイルス・ベンダとの力比べの状況の推移が、3389/TCP へのスキャン数の増減に大きく影響していると考えられます。
今期は新たにファイル感染型の Morto が登場し、同マルウエアの活動と思われるスキャン数の増加を観測しました。JPCERT/CC では、本マルウエアに感染したと思われる IP アドレスの管理者に情報を提供しました。その後、該当サーバから同様のパケットは観測されなくなり、マルウエアの駆除およびその後の被害拡大の抑止ができたと考えられます。

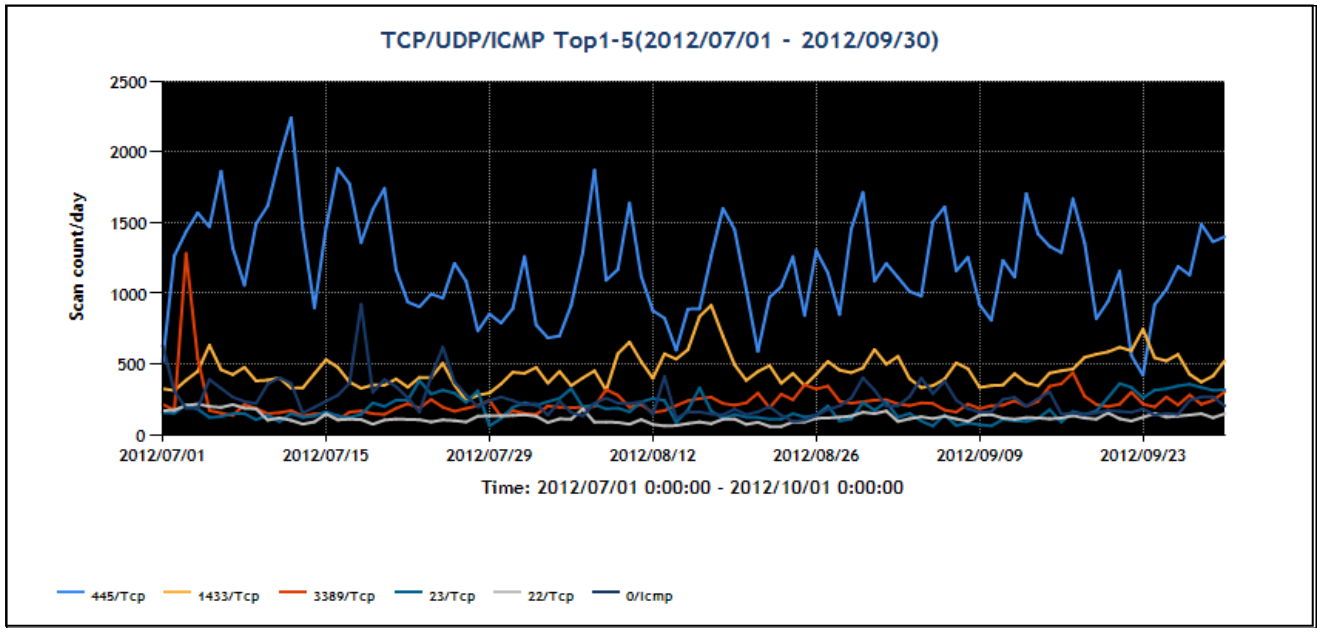
1.3.2. ポートスキャン概況

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の説明
https://www.jpcert.or.jp/isdas/readme.html

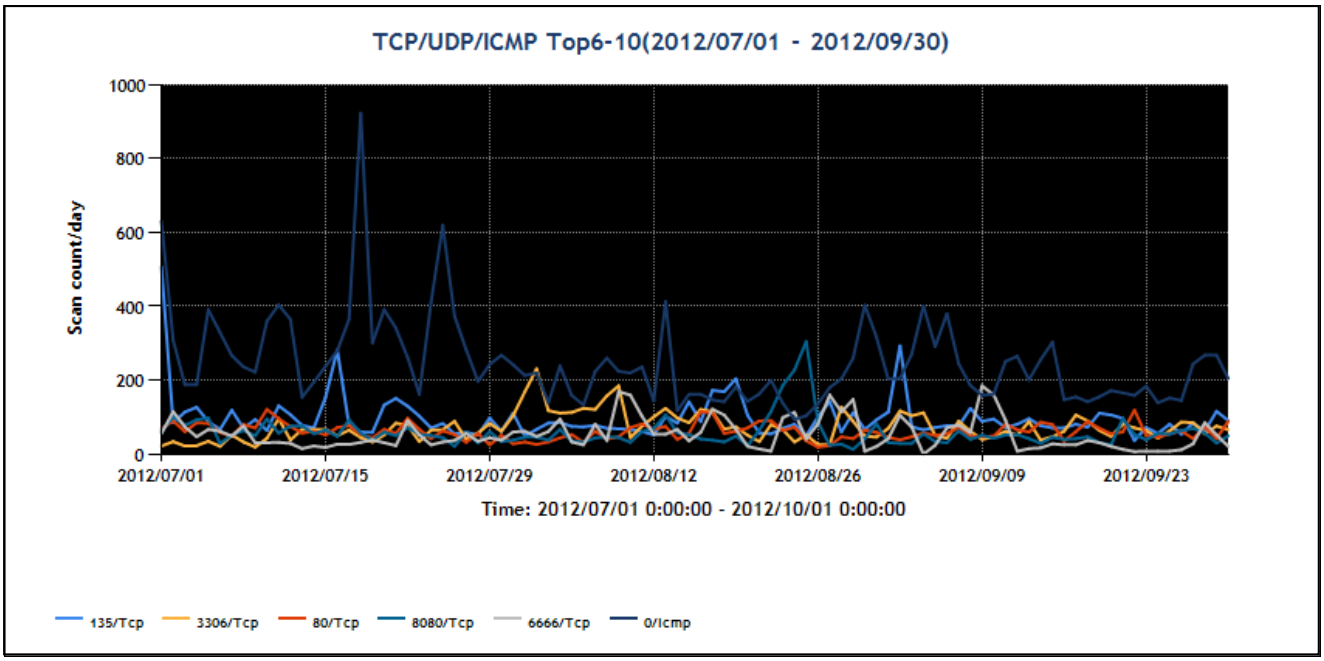
本四半期に定点観測システムで観測された宛先ポート別の上位 1 位～5 位及び 6 位～10 位のそれぞれについて、パケット数の時間的推移を[図 1-1]と[図 1-2]に示します。

- 宛先ポート別グラフ top1-5 (2012 年 7 月 1 日-9 月 30 日)



[図 1-1 宛先ポート別グラフ top[1-5]

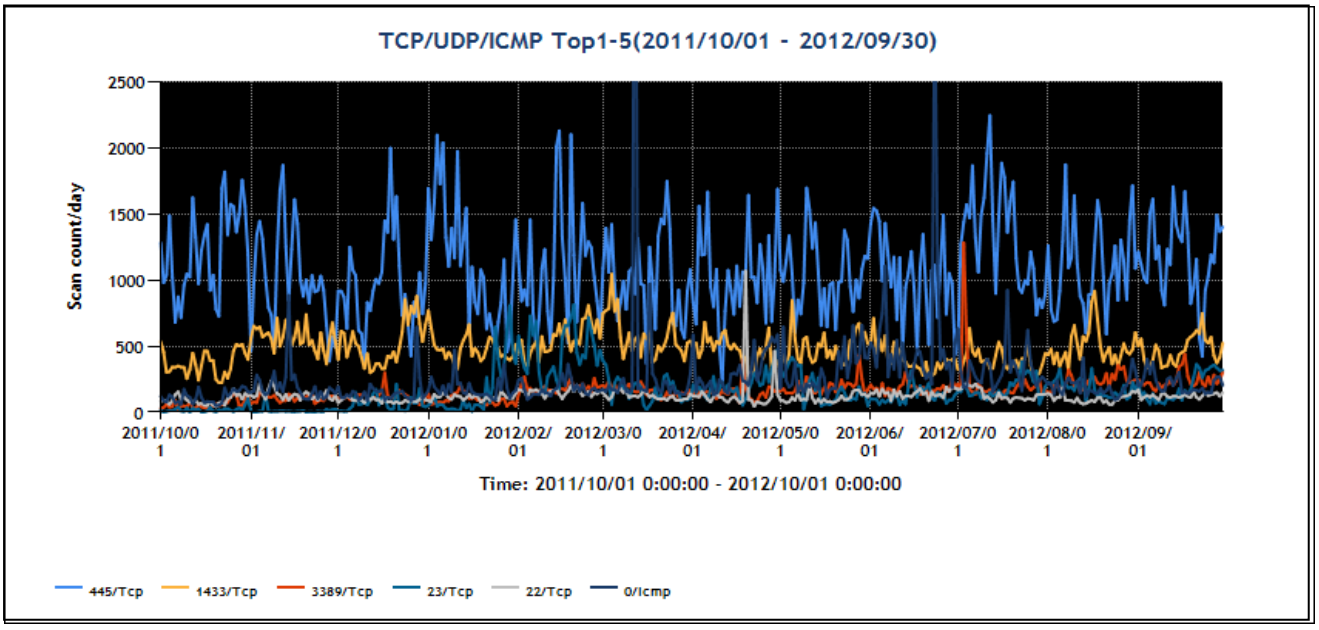
- 宛先ポート別グラフ top6-10 (2012 年 7 月 1 日-9 月 30 日)



[図 1-2 宛先ポート別グラフ top[6-10]

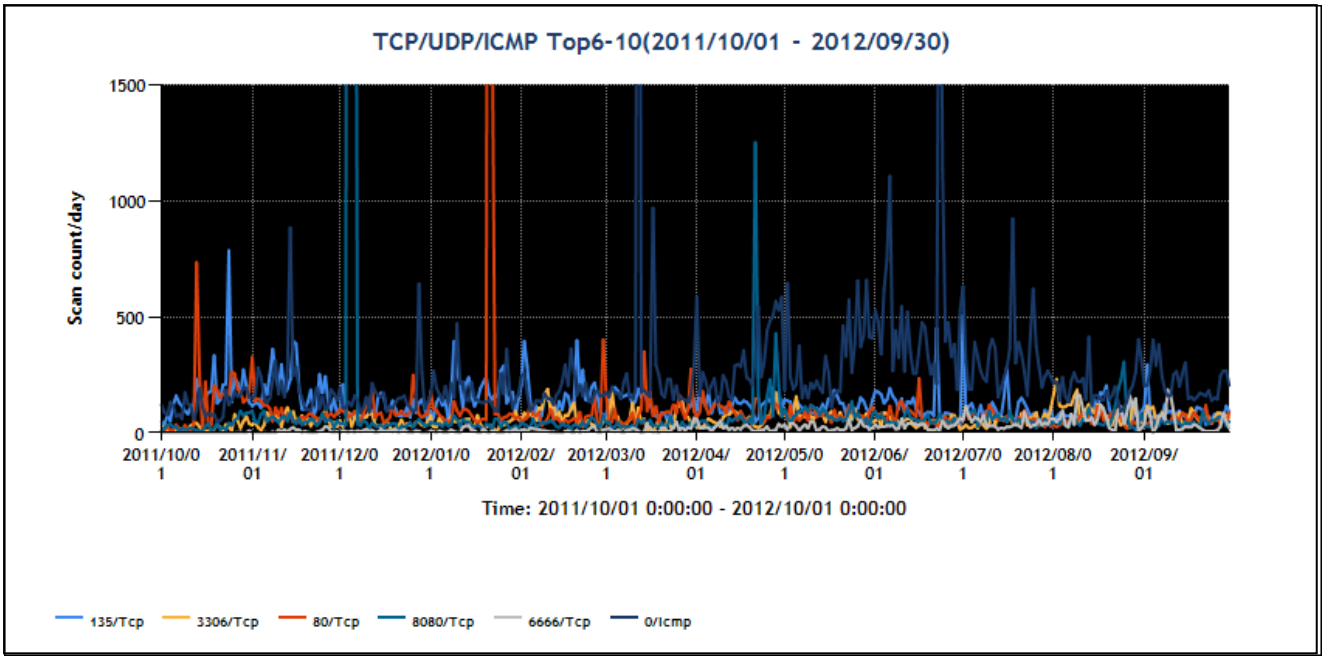
また、より長期間のパケット数の推移を見るため、2011 年 10 月 1 日から 2012 年 9 月 30 日までの期間における、宛先ポート別の上位 1 位～5 位及び 6 位～10 位のそれぞれについて、パケット数の時間的推移を[図 1-3]と[図 1-4]に示します。

- 宛先ポート別グラフ top1-5 (2011 年 10 月 1 日-2012 年 9 月 30 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 (2011 年 10 月 1 日-2012 年 9 月 30 日)



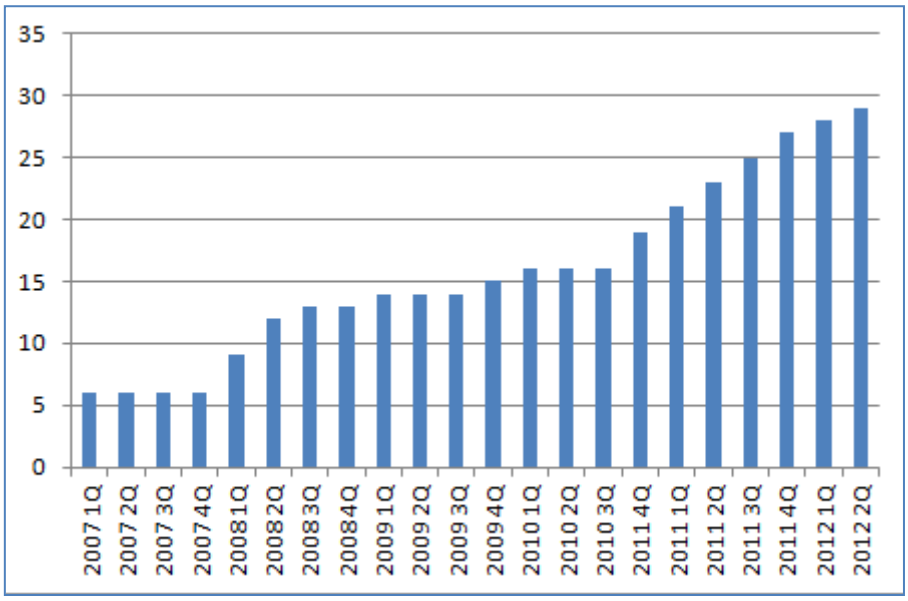
[図 1-4 宛先ポート別グラフ top[6-10]

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、SCSK 株式会社 (SCSK CSIRT)が新規に加盟しました。本期末時点で 29 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]

8 月に「第 6 回総会・第 10 回 WG(ワーキンググループ)会」を開催しました。総会において、JPCERT/CC が引き続き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、第 62 回運営委員会において、JPCERT/CC の代表運営委員である村上晃が引き続き運営委員長に選任されました。

日本シーサート協議会の活動の詳細については、次の 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/

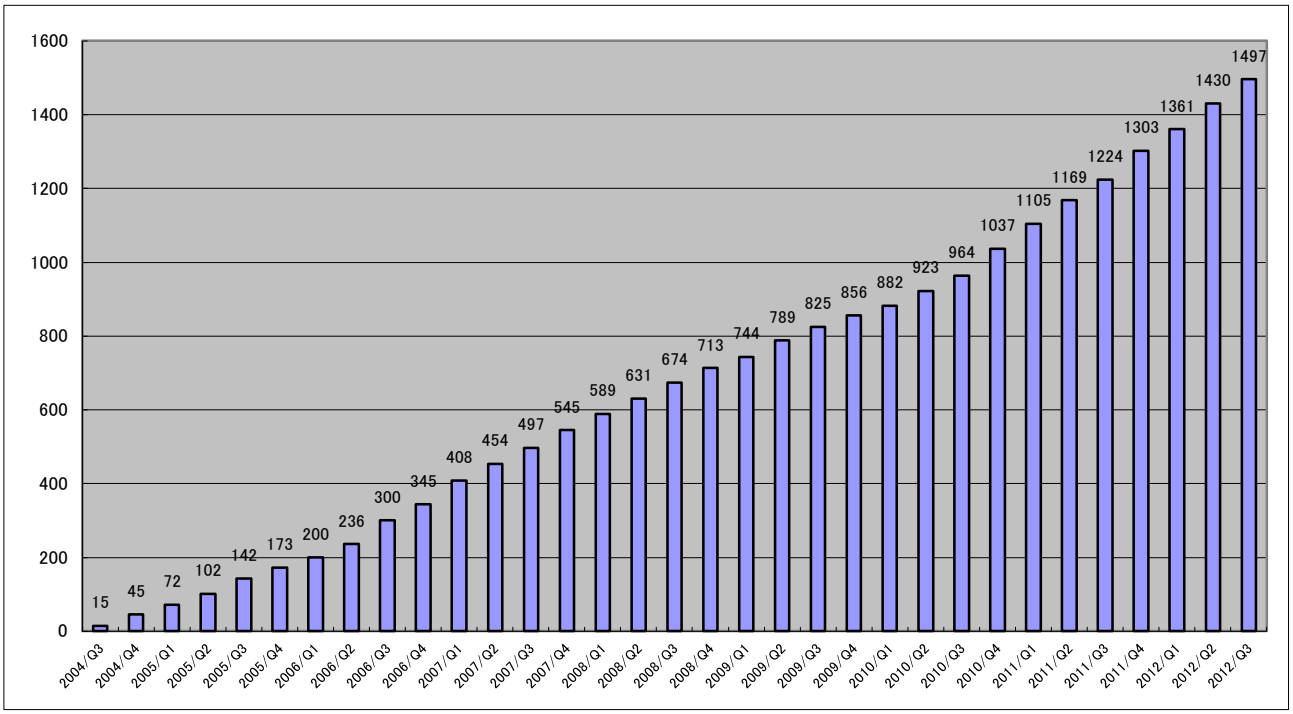
2. 脆弱性関連情報流通促進活動

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）との共同運営) 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

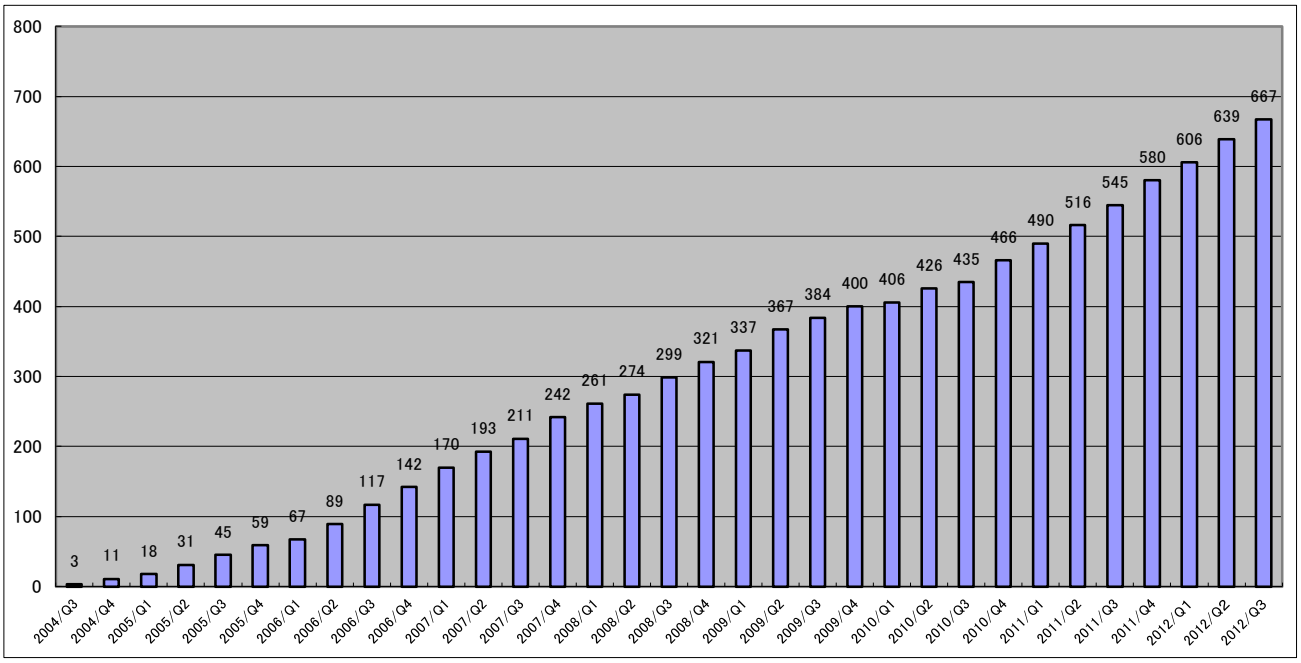
えてとりまとめられた「情報セキュリティ早期警戒パートナーシップガイドライン」に詳述された調整機関の役割を担う活動を行っています。
本四半期に JVN において公表した脆弱性情報は、67 件(累計 1497 件) [図 2-1] でした。本四半期に公表された個々の脆弱性情報に関しては、JVN(https://jvn.jp/)をご覧ください。



[図 2-1　JVN 公表累積件数]

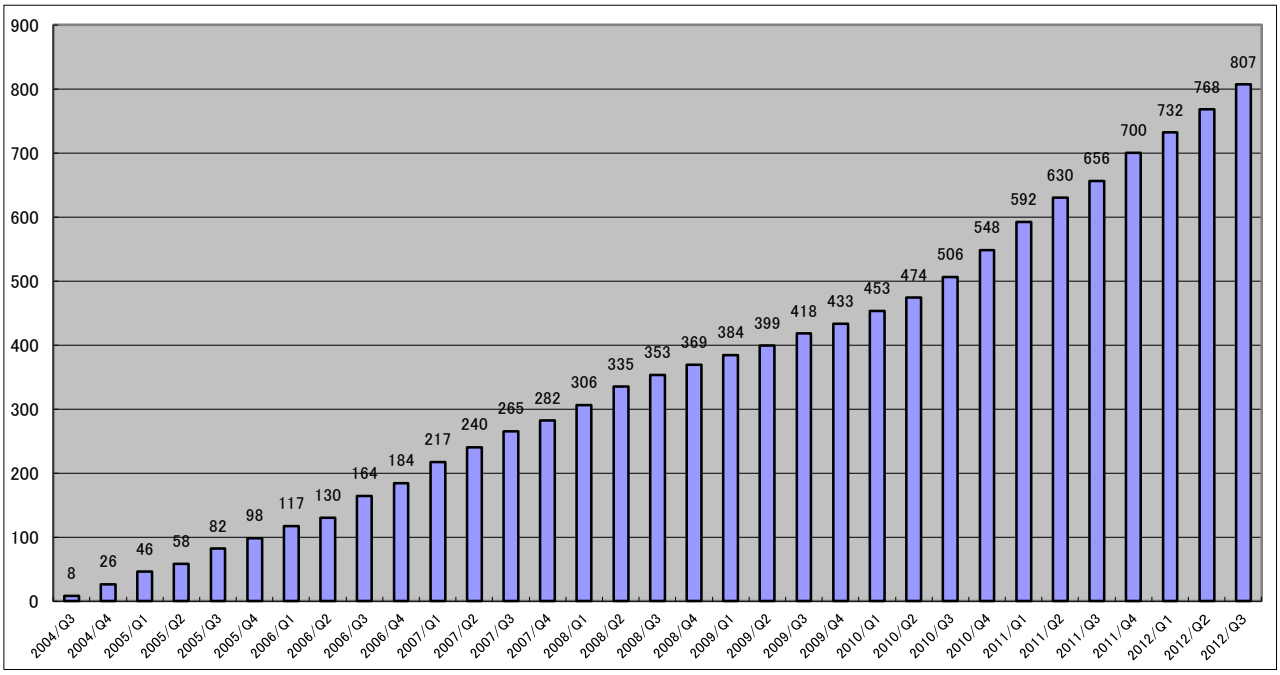
このうち、本基準に従って調整を行い、JVN で JVN#として公表した脆弱性情報は、28 件(累計 667 件) [図 2-2] でした。そのうちの 6 件（約 20%）が海外製品開発者の製品です。こうした統計値にも現れているように、本枠組みに基づく JPCERT/CC の調整活動が、海外の開発者にも理解され協力してもらえるようになってきています。
本年度に入り、Android およびその関連製品の届出の増加傾向が続いており、本四半期には、携帯端末の脆弱性および Android 向けアプリケーションの脆弱性を 13 件、iPhone 向けアプリケーションを 1 件公表しました。また多様な SNS（ソーシャルネットワーキングサービス）の普及に伴い、SNS 関連製品における脆弱性届出も増加傾向にあります。本四半期には、Android 版 SNS 関連ソフトウエアに関する脆弱性情報を 2 件公表しました。
本四半期に公表した 28 件中 4 件は、サイボウズ社が自社製品の脆弱性に関し自ら届出を行い、JPCERT/CC との調整を経て、JVN にて公表を行なったというものでした。サイボウズ社は、発見された Android WebView クラスの脆弱性および任意の Java メソッドの実行の脆弱性に関し、当初発見された製品への対策のみならず、自社の他の Android 向け製品でも調査を行い、届出による指摘ではなく自ら自主的に対策を講じ、その旨 JPCERT/CC へ届出を行って下さいました。これは、「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」中に、「製品開発者自身による脆弱性関連情報の発

見・取得」の際の望ましい対応として掲げられている対応に合致するものです。このサイボウズ社の事例は、製品利用者の安全に資するという脆弱性関連情報ハンドリング活動の目的を果たすモデルケースと言えます。JPCERT/CC は、製品開発者によるこのような前向きな脆弱性への取り組みに敬意を払いつつ、引き続き製品開発者との調整を進めてまいります。



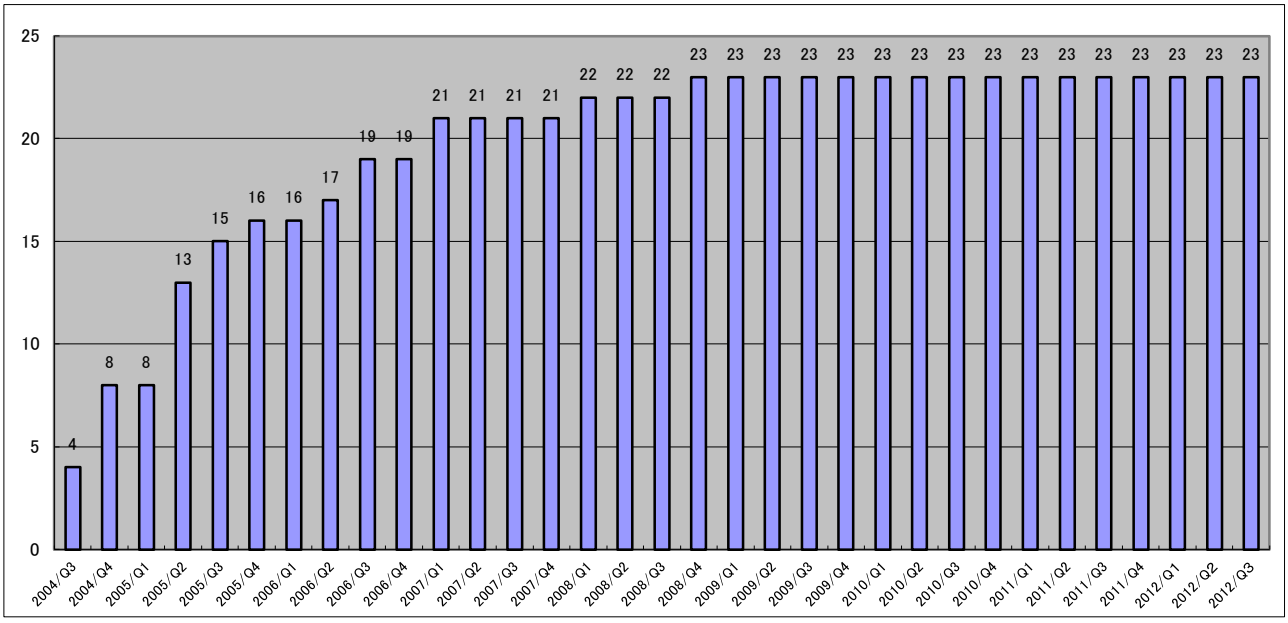
[図 2-2　JVN_JP(JVN#)公表累積件数]

CERT/CC とのパートナーシップに基づいて調整を行い、JVN において JVNVU#および JVNTA として公表した脆弱性情報は、39 件(累計 807 件) [図 2-3]でした。本四半期に公開した 6 件の JVNTA の内訳は、5 件が Microsoft 製品に関するもので、1 件が Oracle 製品に関するものでした。Microsoft 製品に関する公表が多かった理由は、9 月中旬に攻撃観測もされていた Internet Explorer のゼロデイ脆弱性への注意喚起や対策アドバイザリの公開が複数存在したことによるものです。本四半期に公表した 33 件の JVNVU#のうち、Oracle Java 7 の脆弱性は、ゼロデイ脆弱性として既に攻撃観測がされていたため特に深刻度が高いものでした。JVNVU#として公表した 33 件の脆弱性情報の内訳は、Microsoft 製品に関するものが 7 件、Apple 製品に関するものが 5 件、Hewlett Packerd（HP）製品に関するものが 2 件、Oracle 製品に関するものが 2 件、DELL 製品に関するものが 1 件、IBM 製品に関するものが 1 件、Symantec 製品に関するものが 1 件、Trend Micro 製品に関するものが 1 件でした。また、本四半期には、Samsung や HTC が提供する Android スマートフォンやマイクロソフトが提供する Windows Phone の脆弱性の情報も VU#として公表され、日本のみならず海外においても、スマートフォンの脆弱性情報が公表されるようになったと言えます。



[図 2-3　VN_CERT/CC(JVNVU#および JVNTA)公表累積件数]

なお、英国 CPNI とのパートナーシップに基づいて調整を行い、JVN にて公表した脆弱性情報は 0 件(累計 23 件) [図 2-4] でした。



[図 2-4　VN_CPNI(CPNI) 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 2-1 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く本活動が定着し、着々

と対策がとられ、情報公表が進んでいる一方で、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 年の間に徐々に増えてきています。昨年度から、こうした状況の改善を期して、脆弱性情報の取扱手順を定めたガイドラインの改定についての検討を専門家の方々から構成された委員会で行ってきました。

その第一段階として、2010 年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。初回公表時には、50 件の連絡不能開発者案件を掲載しましたが、その翌日には早速、3 件の案件を抱える 1 製品開発者から連絡がありました。また、2011 年 10 月には、2 件の案件を抱える製品開発者及び 3 件の案件を抱える製品開発者との連絡が取れるようになりました。さらに、12 月には、2 件の案件を抱える 1 製品開発者との連絡がついて、それぞれ調整手続きを始めることができました。連絡不能開発者一覧の掲載によって、1 週間以内に約 1 割、3 ヶ月以内に約 2 割の開発者と連絡がついて調整を開始できたこととなり、連絡不能開発者一覧の掲載が「滞留案件」の解消に一定の効果があることが確認されました。

本四半期においては、前回（6 月 22 日）に連絡不能開発者として公表した 2 名の製品開発者から応答が得られないまま 3 ヶ月が経過したため、製品開発者名だけでなく製品名およびバージョンを追記する連絡不能開発者一覧の更新を 9 月 27 日に行いました。連絡不能開発者一覧の公表から 1 年が経過した 2012 年 9 月末日時点で、合計 97 件の連絡不能開発者が公表されており、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、各国製品開発者の対応状況の集約、脆弱性情報の公表時期の設定などの連携した調整活動を行っています。

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。日本国内で取り扱われた脆弱性案件に関しての、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、本四半期には、JVN 英語版サイトを定期的に閲覧している海外（インドネシア）の研究者から、JPCERT/CC へ直接脆弱性の届出がなされました。JPCERT/CC による製品開発者との調整も円滑に進み、本四半期内に製品開者および JVN から対策を含む情報を公表することができました。この事例からも窺えるように、海外特にアジア圏でも JVN の知名度が向上し浸透し始めているようです。

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、24 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、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

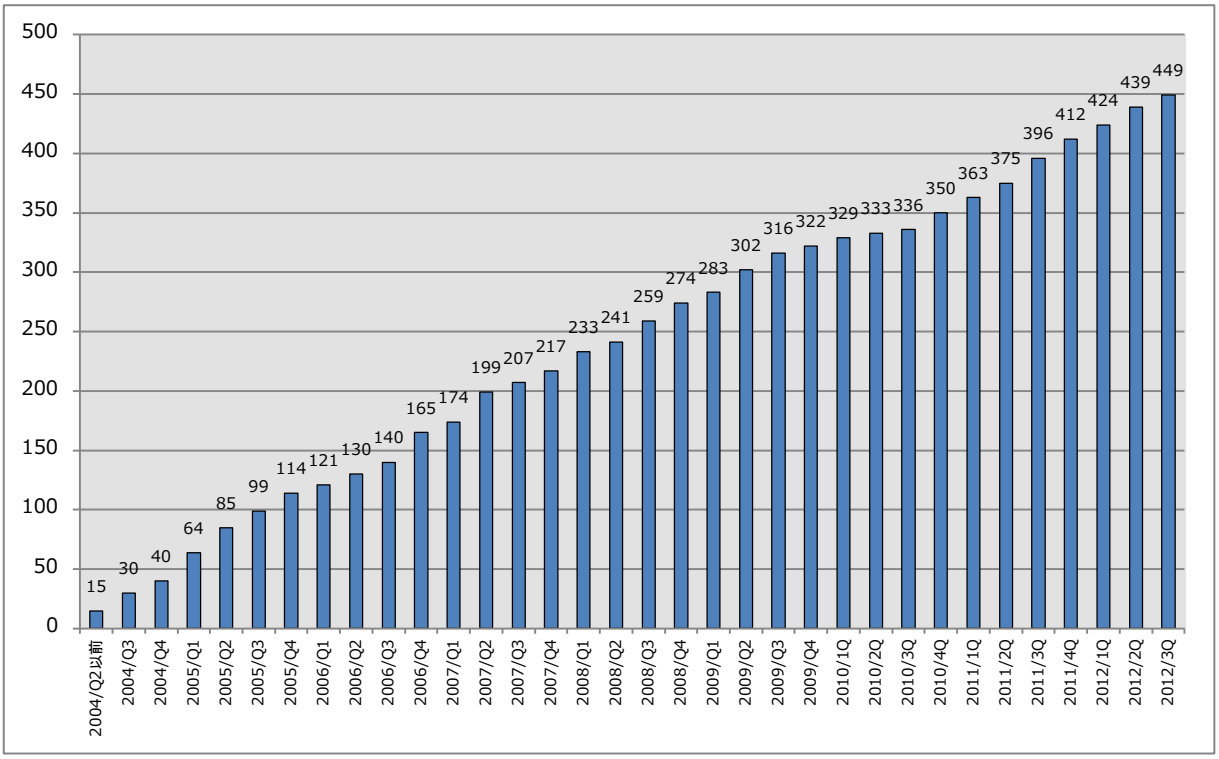
本基準では、受付機関に IPA、調整機関に JPCERT/CC が指定されています。JPCERT/CC は IPA が受け付けた届出情報の転送を受けて、製品開発者への情報提供を行い、対策情報公開に至るまでの調整を行っています。最終的には、 IPA と共同で、脆弱性情報ポータル JVN において対策情報を公開しています。両組織間においては、脆弱性情報の分析結果や脆弱性情報の取扱い状況等の情報交換を行うなど、緊密な連携を行っています。なお、本基準における IPA の活動および四半期毎の届出状況については、次の URL をご参照ください。

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 2-5]に示すとおり、2012 年 9 月 30 日現在で 449 社となっています。

登録等の詳細については、https://www.jpcert.or.jp/vh/agreement.pdf をご参照ください。



[図 2-5 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@札幌」を開催

Android の普及とともに開発量が急増している Java プログラムの脆弱性削減を目的として、Java 言語で脆弱性を含まない安全なプログラムをコーディングする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ための学生等の若年層向け1日セミナーを、8月29日(水)札幌で開催しました。24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

受講後のアンケートでは「基礎的な実装の面ばかりみていたので、セキュリティの面を深く考える良い機会になりました」「Java でシステムを構築する際にさまざまな攻撃手法から守る方法を学ぶことができた」等、セミナーがセキュリティに対する気づきを与える機会となったという受講者の声をいただく一方で、ハンズオンが期待より少なかった等、セミナーの改善点に関するコメントも多数寄せられました。アンケートでいただいたコメントは次回以降のセミナー資料等の改善に役立て、より効果的なセミナーの実施につなげていきたいと考えています。

2.5.2. 学生向けセミナー「Java セキュアコーディング連続セミナー@東京」第 1 回を開催

札幌セミナーに引き続き、9 月 9 日(日) 東京にて「Java セキュアコーディング連続セミナー@東京—第 1 回：オブジェクトの生成とセキュリティ」を開催しました。定員を上回るご応募をいただき、39 名の方にご参加いただきました。

月 1 回のペースで開催する本連続セミナー(全 4 回の予定)では、主に学生を対象に、Java 言語を使ったプログラミングを行う上で問題となるセキュリティ上の注意点について講義と演習を通じて学び、Java セキュアコーディングに関する知識やノウハウを身につけていただくことを目的としています。

この連続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ており、前半では、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しました。後半のハンズオンでは、課題として与えられた脆弱なソースコードを受講者自らが修正し、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。

[図 2-6 講義の様子]

セミナーの講義資料は下記の URL からご覧いただけます。

講義資料
http://www.slideshare.net/jpcert_securecoding/java1-14227881
演習資料
http://www.slideshare.net/jpcert_securecoding/java1-14227886

第 2 回以降のセミナーは、次の日程で企画しています。

第 2 回 10 月 14 日（日）「数値データの取扱いと入力値検査」
第 3 回 11 月 11 日（日）「入出力(File, Stream)と例外時の動作」
第 4 回 12 月 16 日（日）「メソッドとセキュリティ」
時間と場所(各回共通)：13:30～16:30（受付開始 13:00～）
エッサム神田ホール 401

お申し込み
https://www.jpcert.or.jp/event/securecoding-TKO201209-application.html

2.5.3. 開発者向けウェブマガジン Codezine に「Java セキュアコーディング入門」連載中

翔泳社の開発者向けウェブマガジン CodeZine に「Java セキュアコーディング入門」と題した連載記事を執筆しています。Java 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ととも

に、最近話題の Android アプリケーションの脆弱性なども解説しています。本四半期は、戸田洋三による次の記事が掲載されました。

第 7 回「Java の参照型変数とセキュリティ」(8 月 16 日公開)
CodeZine（コードジン）Java セキュアコーディング入門
http://codezine.jp/article/corner/437

2.5.4. セキュアコーディング 出張セミナー

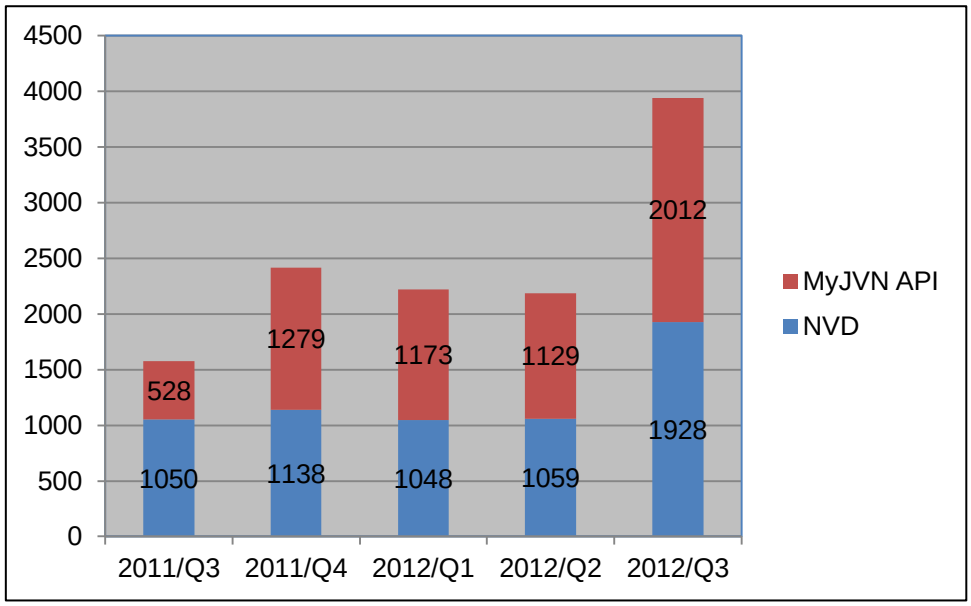
JPCERT/CC では、ソフトウエア製品等の開発を行う企業・組織を対象に、セキュアコーディングに関する出張セミナー（有償）の実施を承っています。マネジメント層へのセキュリティ啓発や新人研修のメニュー等としてもご利用いただけます。今年度から、これまで提供していた C/C++言語におけるセキュアコーディングセミナーに加え、新たに Java 言語版および Android アプリケーション開発に関するセキュアコーディング出張セミナーも提供しています。本四半期は、国内メーカー2 社に対して、Java および C/C++セキュアコーディングセミナーを実施しました。
※出張セミナーのご依頼、お問合わせは、secure-coding@jpcert.or.jp 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

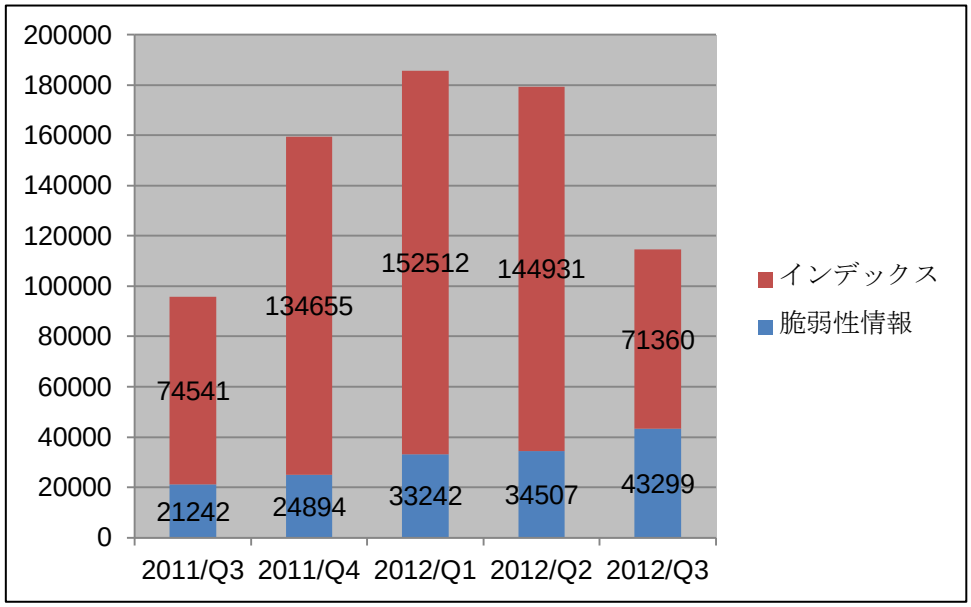
JPCERT/CC は、大規模組織の組織内 CSIRT などでの利用を想定して、KENGINE などのツールを用いた体系的な脆弱性対応を可能とするため、IPA が運用する MyJVN API および NIST (National Institute of Standards and Technology)の NVD (National Vulnerability Database) を外部データソースとして利用した、VRDA (Vulnerability Response Decision Assistance)フィードによる脆弱性情報の配信を行っています。VRDA フィードについての詳しい情報は、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 2-8] に、VRDA フィードの利用傾向を [図 2-9] と [図 2-10] に示します。 [図 2-9] 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 2-10] 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。

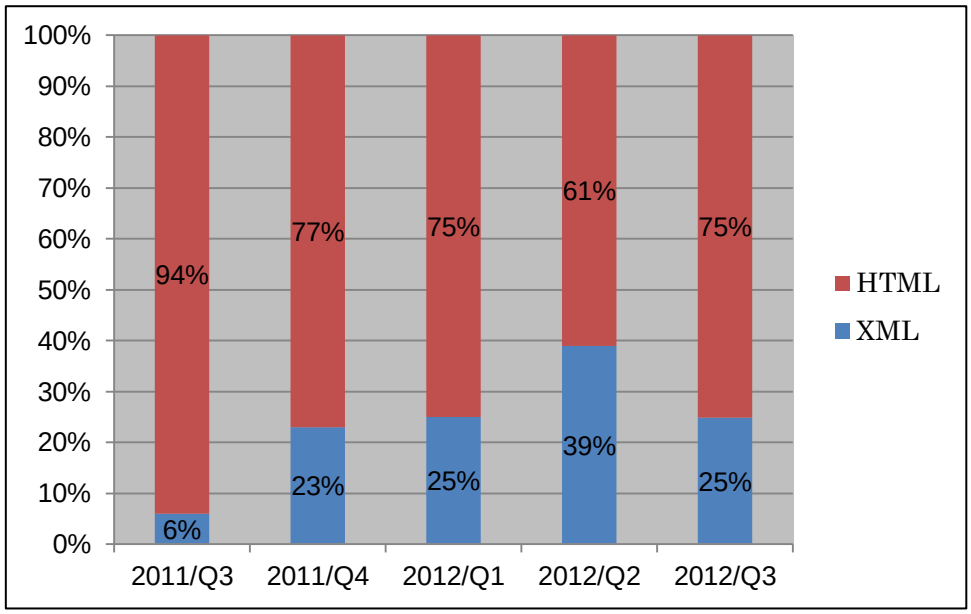


[図 2-8 VRDA フィード配信件数]



[図 2-9 VRDA フィード利用件数]

[図 2-9] 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大きく減少しましたが、脆弱性情報の利用数は増加しました。



[図 2-10 脆弱性情報のデータ形式別利用割合]

[図 2-10] 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。

近年、標的型攻撃に代表されるサイバー攻撃に対する取組みとして、各所で情報共有の枠組みが構築されています。さらに、各枠組みで得られた情報を適切な内容・範囲、そしてタイミングで他の枠組みと交換することにより、対抗手段の選択肢を広げる試みが始まっています。JPCERT/CC も、アーティファクト分析という手段を活用しながらコーディネーションセンターとしてそれらの取組みに参加しています。

3.1. サイバー攻撃解析協議会

経済産業省と総務省は、サイバー攻撃を高度解析する枠組みを連携して構築することとなり、そのための枠組みとして、7 月に「サイバー攻撃解析協議会」を発足させました。JPCERT/CC は、本協議会

の中核メンバー組織の一つとして参加することになりました。この協議会では、各参加団体が共有可能な情報を持ち寄り、解析を行うことでサイバー攻撃の実態把握を推し進めることを目指しています。

サイバー攻撃解析協議会
http://www.meti.go.jp/press/2012/07/20120711002/20120711002.html

3.2. IT KEYS「リスクマネジメント演習」

JPCERT/CC は IT Keys のリスクマネジメント演習の講義の一部を担当し、教材データを用いた解析演習を行いました。IT Keys は文部科学省の先導的 IT スペシャリスト育成推進プログラムの一つとして開始され、昨年度からは各参加大学により継続されています。

本年度は、改ざんされた Web サーバのログの解析から始まる演習シナリオを作成し、インシデントを絞り込みながら追跡する流れを体験していただくことを目指しました。

IT Keys 実践科目群
http://it-keys.naist.jp/course/practice/

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。本四半期は計 3 回（7 月 6 日、8 月 31 日、9 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

来日した米国 ICS-CERT 関係者と双方の活動に関する情報交換を行いました。JPCERT/CC は、今後

の活動計画や組織の在り方について情報を交換し、より密な協力連携関係を築くために、ICS-CERT をはじめとする海外パートナーとの交流にも取り組んでいきます。

4.3. 制御システム関係者向け第 1 回情報共有会開催

制御システム向けのユーザ・ベンダ・研究者を対象とした情報共有会を 7 月 12 日に実施しました。制御システムのセキュリティに関する情報も増えており、年一回のカンファレンスやメーリングリストでは、鮮度が落ちたり複雑で伝えきれなかったりする情報も増えてきたため、本四半期から始めた試みです。将来的には、やや機微な情報を取り上げる可能性も想定して、参加者の顔が相互に見える会をめざしています。第 1 回の共有会は、既に公開されている情報がほとんどでしたが、次回以降への参加者の期待も大きく、より現場の方々の必要に応じた情報提供を行うためにも、情報収集力を強化し、本会の質・価値の向上に取組んでいきます。

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 7 件の利用申込みがあり、直接配布件数の累計が 108 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活動を開始すべく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、関係者との調整、情報共有の仕組みの検討などを行い、脆弱性ハンドリングに関しては、制御システム向け脆弱性研究会の第 1 回会合を開催しました。

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。

本四半期は、春秋に開催される SC27 国際会議の間の期間にあたり、前回のストックホルム会議の討議結果を受けて改訂された標準案が配布され、その内容確認と、次回のローマ会議に向けたコメントの取りまとめ検討作業を行いました。両標準とも、修正要求の件数が減ってきており、標準化作業の最終ステージに近づきつつあると考えられます。

「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化草案(DIS： Draft of International Standard)として配布されました。DIS の段階では、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 か月間の猶予期間が取られるため、対応は半年後になる予定です。

「脆弱性取扱手順」については、改訂された草案が第 1 次委員会草案(CD： Committee Draft)として配布されました。ローマ会議に向けて、さらなる修正のためのコメントを用意し、国内会議での審議を経て SC27 事務局に提出しました。

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

インシデント管理に関しては ISO/IEC 27035:2011 (インシデント管理 ; Information security incident management)を早期改訂することが前回のストックホルム会議において正式に決まりました。現在、SC27/WG4 では、次の 3 つの標準から構成されるマルチパート標準の策定が進められており、JPCERT/CC はこの標準化作業に参加しています。

Part 1. インシデント管理の原理（Principles of Incident Management）
Part 2. インシデントの管理と対策のためのガイドライン（Guidelines for Incident Management Readiness）
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）

本四半期は、各パートについてエディターが用意した草案(1st Working Draft)について、Part 1 に対しては 14 件の、Part 3 に対しては 10 件のコメントを作成し、日本のコメントとして 9 月 30 日に提出しました。Part 2 に関しては、エディターが用意した草案が目次案程度の内容しかなく、具体的なコメントを行うことが困難であることから、今回はコメントを見送りました。

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. 大洋州地域の CSIRT 構築支援活動(7 月、9 月)

大洋州の島嶼国をカバーする CSIRT である PacCERT の構築・運用支援活動として、7 月に JPCERT/CC の職員が独立行政法人国際協力機構（JICA）の短期専門家として PacCERT の事務所があるフィジーに赴きました。2011 年 7 月、10 月、11 月、2012 年 3 月に続いて、第 5 回目の専門家派遣となる今回は、機材の設置支援及びシステムの引き渡しを行いました。また、JICA や PacCERT の関係者とともに今後の計画について協議しました。
9 月には PacCERT のスタッフ 2 名が来日し、9 日間に渡ってインシデントハンドリング及びマルウエア解析に関する OJT 研修を受講されました。

6.1.2. ThaiCERT の CSIRT 強化支援活動(9 月)

タイの National CSIRT である ThaiCERT のスタッフ 2 名が来日し、9 日間に渡ってインシデントハンドリング及びマルウエア解析に関する OJT 研修を受講されました。
2000 年に設立されたタイのナショナル CSIRT である ThaiCERT は、アジア太平洋地域の中では比較的歴史のある CSIRT の一つであり、これまでも、各種インシデント対応での協力、JPCERT/CC が主導しているネットワーク定点観測プロジェクト「TSUBAME」への参画、アジア太平洋地域の CSIRT コミュニティである APCERT の運営などを通じて、JPCERT/CC と強い連携活動を展開してきています。
ThaiCERT は 2011 年 1 月までは National Electronics and Computer Technology Center (NECTEC、タイ国家電子・コンピュータ技術センター) の下部機関に位置付けられていましたが、2011 年 2 月より

Ministry of Information and Communication Technology (MICT、情報通信省) 傘下にある Electronic Transactions Development Agency (ETDA、電子取引開発庁)の下部機関となりました。これを機に、2012 年 4 月、JPCERT/CC と ThaiCERT は MOU（覚書）を締結するするとともに、一層の連携強化をはかることで合意しました。今回の研修は、この MOU に基づく連携強化のための活動の一環として行われたものです。

6.1.3. 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/

6.2.1.2. APCERT Steering Committee 電話会議の実施

8 月 16 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。

6.2.1.3. APCERT チーム間および他組織間との連携

(1) 第一回 APCERT Study Call の実施(7 月 11 日)

APCERT チーム間のマルウエア解析能力を高めることを目的に、APCERT Study Call と称したインターネット経由の勉強会が初めて実施されました。第一回はマレーシアのナショナル CSIRT である MyCERT が「Reversing Malicious Flash」について解説を行い、各 APCERT チームにおける解析手法の理解や解析能力の向上に向けた一助となりました。

(2) AP*Retreat での講演(7 月 17 日)

アジア太平洋地域のインターネット関連団体が一堂に会する AP*Retreat Meeting おいて、JPCERT/CC は APCERT 事務局チームの立場で「APCERT の活動」をテーマに講演を行いました。AP*Retreat Meeting は年に 2 回、アジア太平洋地域の都市で開催されており、今回は東京で開催されました。

AP* (AP Star)の概要については、以下 URL をご参照ください。
http://www.apstar.org/

(3) APEC TEL 46 SPSG 参加(7 月 30 日-8 月 4 日)

APEC 地域の情報電気通信分野を担当する政府機関を中核とするワーキンググループである APEC Telecommunications and Information Working Group (APEC TEL)の Security and Prosperity Steering Group (SPSG)の会合(サンクトペテルブルグで開催)に APCERT の議長チームとして、テレビ会議を通じて参加し、最近の APCERT の活動についての報告を行いました。

6.2.1.4. 覚書(MOU)締結

CSIRT との協調関係に明文化された根拠を与え、また、機微な情報の取扱いルールについて事前に合意しておくため、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。本四半期にはアジア太平洋地域の以下の組織と MOU を締結しました。

- Bangladesh Computer Emergency Response Team (BDCERT、バングラデシュ)
- Macau Computer Emergency Response Team Coordination Centre (MOCERT、マカオ)
- Sri Lanka Computer Emergency Readiness Team Coordination Centre (Sri Lanka CERT|CC、スリランカ)
- Taiwan National Computer Emergency Response Team (TWNCERT、台湾)
- CERT Australia (オーストラリア)

CERT Australia については、9 月 12 日に同機関の Executive Director を務める Carolyn Patteson 博士が

来訪し、MOU 署名式を行いました。

6.2.1.5. 2012 APISC Security Training Course 参加(7 月 9 日-13 日)

JPCERT/CC の職員が、韓国のソウルにて開催された 2012 APISC Security Training Course に参加しました。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)及び 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。参加者間で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情報交換を行うとともに、CSIRT 構築・強化やインシデント対応のあり方について議論等を行いました。

6.2.1.6. 国際部マネージャ小宮山功一朗が第 6 回アジア太平洋 ISLA 受賞(7 月 17 日)

JPCERT/CC 国際部マネージャ小宮山功一朗が、第 6 回アジア太平洋セキュリティー・リーダーシップ・アチーブメント(ISLA)を受賞しました。

本受賞の詳細については、以下 URL をご参照ください。
https://www.jpcert.or.jp/pr/2012/PR20120718-award.pdf

6.2.1.7. フィリピンに関する情報収集と ISACA Manila Chapter Meeting での講演(7 月 23 日-27 日)

JPCERT/CC は、フィリピンとの連携強化の可能性を探るべく、同国の情報セキュリティの現状や CSIRT の活動状況について、政府機関や日系企業の現地法人等へのヒアリング調査を行いました。
また、本調査出張の機会をとらえ、7 月 26 日にマニラ市内の銀行で開催された ISACA マニラ支部 (http://www.isaca-manila.org/) の定例会合に参加し、情報セキュリティのトレンドに関する基調講演を行いました。ISACA は、世界 180 ヵ国以上 100,000 人をこえる会員から構成され、情報システムのセキュリティおよび IT に関係するリスクやコンプライアンスなどについて、資格認定そして教育を推進する非営利組織です。ISACA マニラ支部は 200 名ほどの会員を擁し、活発に活動を行っています。

6.2.1.8. Cyber Security & Cyber Terrorism Conference での講演(8 月 23 日 - 24 日)

JPCERT/CC はシンガポールで行われたサイバーセキュリティに関する会議「Cyber Security & Cyber Terrorism Conference」に参加し、「Why is it Difficult to Establish Successful Public Private Partnership for Cyber Security」と題し、官民連携の取組みの必要性について基調講演を行いました。本イベントは、シンガポール大学、Association of Information Security Professionals (AISP)、米 National Defense University が共催したものです。

本会議の詳細については、以下 URL をご参照ください。
http://www.cybersecuritysingapore.com.sg/programme.html

6.2.1.9. ARF Cyber Incident Response Workshop 参加(9 月 6-7 日)

JPCERT/CC は ASEAN Regional Forum (ARF)の枠組みにおいて、SingCERT および CERT Australia が主催した Cyber Incident Response Workshop に参加しました。本ワークショップでは、ASEAN 全域に影響する大規模インシデントが発生したという想定のもと、各国の CSIRT、法執行機関および政府がいかに対応を行うかについてグループディスカッションが行われました。取りまとめでは、APCERT 等の既存の情報連携のスキームが有効な在り方であることが確認されました。

6.2.1.10. 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(9 月 12 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 加盟国および周辺各国の 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 7 度目になります。
今年は 10 カ国（日本、ブルネイ、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 12 チームの参加のもと、Android のオンラインバンキングのアプリケーションに係るインシデントの発生を想定した演習が行われました。

6.2.1.11. 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。
7 月 3、5 日に中国西安で開催された「中国計算機網絡安全応急(CNCERT/CC)年会)」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。
8 月 15、16 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。
8 月 17、18、19 日に中国成都で開催された「2012 中国通信行业信息安全大会」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 25、26 日に中国上海で開催された「信息安全国际峰会 2012」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 のメンバを務めています。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。

6.2.3. 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。

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 では、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、協議会においては、経済産業省からの委託により、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 8 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の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、「So-net をかたるフィッシング（7 月 13 日）」、「ODN をかたるフィッシング（8 月 28 日）」[図 6-1]の 2 件の緊急情報を、第二認証情報を詐取するフィッシングについては、「みずほ銀行をかたるフィッシング(9 月 12 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　ODN をかたるフィッシングサイト
https://www.antiphishing.jp/news/alert/odn20120828.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。本四半期は新たに、NTT コミュニケーションズ(2012 年 9 月より)に提供を開始しました。これにより協議会が情報を提供している事業者等は 17 組織となりました。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. 情報共有会開催

情報共有会は、フィッシング対策の推進を目的として、主に技術的対策及び制度的対策等について情報交換や外部専門家からの情報収集を目的として実施しています。
本四半期の情報共有会開催実績は以下のとおりです。

(1) 情報共有会（第 1 回会合）
日時：2012 年 7 月 26 日 15:00 - 17:30
場所：一般社団法人 JPCERT コーディネーションセンター

7.5. 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 7 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201207.html
フィッシング対策協議会 2012 年 8 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201208.html
フィッシング対策協議会 2012 年 9 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201209.html

8. 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。

8.1 はじめての暗号化メール (Thunderbird 編)

初めて PGP を使用することになった方々のための、PGP のインストールから PGP を使ったメッセージ交換までをカバーするクイックガイドブックです。PGP は CSIRT コミュニティで広く利用されてい

る暗号化メール・ソフトウェアです。本書は、Microsoft Windows 上で動作している Thunderbird の電子メール利用環境を前提としてまとめました。

はじめての暗号化メール（Thunderbird 編）(2012 年 8 月 30 日)
https://www.jpcert.or.jp/magazine/security/pgpquick.html

8.2 早期警戒情報フィールドレポート

JPCERT/CC が提供する「早期警戒情報」や「インシデント対応支援」を、組織や企業が具体的にどのように活用されているかについて、企業等を訪問して聞かせていただき、一連のインタビュー記事として JPCERT/CC ホームページに掲載しています。本四半期においては、次の組織について新たに掲載しました。

【第 3 回】NTT-CERT　～　通信事業者における早期警戒情報の活用事例　(2012 年 7 月 18 日)
https://www.jpcert.or.jp/magazine/security/fieldww-nttcert.html

9.　講演活動一覧

(1) 早貸 淳子 (専務理事) :
「金融機関に関連するインシデントの動向と対策、組織内 CSIRT の機能と役割」
FISC セキュリティセミナー, 2012 年 7 月 30 日
(2) 山田 秀和 (制御システムセキュリティ対策グループ リーダー) :
「サイバーセキュリティと制御システム」
計装研究会, 2012 年 7 月 25 日
(3) 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) :
「情報セキュリティインシデントの傾向と JPCERT/CC の活動」
情報セキュリティ対策セミナー（日本金融監査協会）, 2012 年 7 月 24 日
(4) 満永 拓邦 (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, 2012 年 7 月 11 日

10. 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) :
「Java セキュアコーディング入門（7） Java の参照型変数とセキュリティ」
翔泳社 Codezine,2012 年 8 月 16 日

(2) 早貸 淳子 (専務理事)：
「インターネット白書 2012」
インプレスジャパン,2012 年 7 月 1 日

11. 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」、「2-5-2」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、「2-5-4」をご参照ください。

12. その他

情報配信の強化を目的に、JPCERT/CC Web サイトで提供しているコンテンツの中で、利用頻度や資料性の高いものを中心にコメントフォームを追加しました。
追加したフォームは、公開した情報が役に立った/立たなかったかを簡単に評価いただけるラジオボタンと、ご意見、ご感想を入力いただけるフォームの 2 つの構成となっています。

コメントフォームを追加した主なコンテンツ

- 注意喚起
- Weekly Report
- ひとくちメモ
- セキュアコーディングスタンダード
- CSIRT 構築支援マテリアル
- 研究・調査レポート
- セキュリティ対策講座
- フィールドレポート

■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