JPCERT CC®

JPCERT-PR-2011-0004

発行日 : 2012-01-12

JPCERT/CC 活動概要 [2011 年 10 月 1 日 ～ 2011 年 12 月 31 日]

【活動概要トピックス】

—トピック 1 —
Java セキュアコーディングに関する取組み

今や Java は、C 言語や C++を抑えて、もっとも広く利用されているプログラミング言語であり、この傾向を Android の普及がさらに押し上げようとしています。Java はそれ以前の言語の欠点を克服すべく設計されていて、Java で開発されたソフトウエアは堅牢な実行環境で動作しますが、それでも不注意なコーディングがなされれば様々な脆弱性が作り込まれます。Java コーディングにおいて脆弱性の作り込みを減らすために、カーネギーメロン大学ソフトウエア工学研究所の CERT プログラムが専門家の協力を得つつ開発した標準が「CERT Oracle Java セキュアコーディングスタンダード」（原題：The CERT Oracle Secure Coding Standard for Java）です。

JPCERT/CC では、ソフトウエア開発者が脆弱性の芽をできるだけ早期に摘み取れるように、これまで C/C++のセキュアコーディング関連の活動を展開してきましたが、Java の本格的な普及を踏まえて Java セキュアコーディングにも取り組んでいます。上記の標準の開発作業に参加するとともに、その邦訳を進めて、同標準の本編の完訳を本四半期に JPCERT/CC のホームページ上で公開しました。

また、本標準は全体では千ページ近い文書になっていますが、手元に置いて学習や業務に役立てたいとの要望に応えるため、重要度の高いセクションだけを抽出してコンパクトにまとめた書籍版（The CERT Oracle Secure Coding Standard for Java, Addison-Wesley 発行）の出版計画とともに、開発者向けの啓発記事の執筆、個別企業向けの有償セミナーの開催などにも精力的に取り組んでいます。

CERT Oracle Java セキュアコーディングスタンダード
https://www.jpcert.or.jp/java-rules/

―トピック 2―

第二認証情報を狙うフィッシング詐欺への対応

本四半期においては、国内の金融機関を騙り、乱数表や第二暗証番号などの第二認証情報を詐取するフィッシング攻撃が確認されました。金融機関を騙るフィッシングは以前から確認していましたが、第二認証情報を詐取する国内のフィッシングが確認されたのは、今回が初めてです。

第二認証情報のうち、乱数表や第二暗証番号といわれる手法は、金融機関などが契約者ごとに異なる情報を記載したカードをあらかじめ配付しておき、ログイン時に ID とパスワードに加えて、カード上の指定した欄に記載された数字を入力させることにより認証を厳格化するものです。多くの金融機関では、第二認証を使うことにより、送金のような機微な操作もオンラインで実行できます。ログイン ID やパスワードに加えて、第二認証情報の情報まで詐取されてしまうと、預金残高によっては高額の金銭被害が発生する可能性があります。
フィッシング対策協議会では、名前を騙られた金融機関への情報提供や、同協議会の Web サイト上での緊急情報等の公開を行い、JPCERT/CC においては、フィッシングに使用されたサイトや電子メールに添付された実行ファイルが情報を送信する先のサイトを停止するための調整を行いました。

―トピック 3 ―

日中韓 3 カ国による情報セキュリティ対応の覚書調印

国境をまたぐサイバー攻撃が頻発する中、National CSIRT(各国の中心的な連絡窓口となる CSIRT)間の協調は欠かせません。そのような協調関係は、日常的な情報交換や連携作業等を遂行する中で醸成されていくものですが、こ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、JPCERT/CC では従前より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きました。

この種の覚書は、通常は 2 カ国間で締結しますが、このたび、JPCERT/CC と韓国の National CSIRT である KrCERT/CC 及び中国の National CSIRT である CNCERT/CC の 3 組織間で、各々2 カ国間で締結していた覚書を拡張して、3 カ国間の覚書とすることで合意が成立し、2011 年 12 月 20 日に調印しました。3 カ国による覚書調印は JPCERT/CC としても初の試みです。

日中韓の 3 カ国は、地理的に近く、経済的、文化的、歴史的に関係が深い親密な関係にありつつも、歴史認識や領土関係の問題などを抱えていることから、歴史的な記念日や国民が関心を寄せるイベント等を契機とするサイバー攻撃の当事国となり易く、JPCERT/CC と CNCERT/CC、KrCERT/CC との間においても、各種インシデントへの対応協力に関する緊密な連携関係を維持してきました。また、この 3 チームは、アジア・太平洋周辺地域をカバーするネットワーク定点観測システム Tsubame プロジェクトへの参画や、アジア太平洋地域に所在する CSIRT からなるコミュニティである APCERT の運営等においても相互に信頼できるパートナーとして協調してきた実績があります。このたびの覚書の拡張締結を機に、3 組織間での情報交換をより密なものに

し、高まる東アジア地域のサイバー脅威に協力して立ち向かうことを再確認しました。

本活動は、経済産業省より委託を受け、「平成２３年度コンピュータセキュリティ早期警戒体制の整備（不正アクセス行為等対策業務）」事業として実施したものです。
ただし、「平成２３年度コンピュータセキュリティ早期警戒体制の整備（フィッシング対策協議会運営）」事業として経済産業省から受託して実施した「6.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、「2-4-4.C/C++セキュアコーディング出張セミナー」、「5.国際連携活動関連」、「8.講演活動一覧」、「9.執筆一覧」及び「10.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®

—活動概要—

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 2501 件、インシデント件数ベースでは 2339 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 752 件でした。前四半期の 642 件と比較して 17% 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/2011/IR_Report20120112.pdf

1-1-1. インシデントの傾向

本四半期に報告を頂いたフィッシングサイトの件数は、314 件で、前四半期の 226 件から 29%増加しました。また、前年度同期（538 件）との比較では、42%の減少となりました。
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	国内外別合計（割合）
国内ブランド	22	19	24	65(21%)
国外ブランド	54	58	86	198(63%)
ブランド不明（注 2）	17	14	20	51(16%)
月別合計	93	91	130	314(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確認時に停止していたなどの理由により、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 65 件と、前四半期の 31 件から 110 % 増加しました。一方、国外ブランドを装ったフィッシングサイトの件数は 198 件と、前四半期の 165 件から 20%増加しました。

前四半期に引き続き、国内金融機関を装ったフィッシングの報告を多数受領しています。この国内金融機関を装ったフィッシングでは、以下のようにフィッシングの手法を変えてアカウント情報を詐取しようとしていることを確認しています。8 月には、メールに実行ファイル形式のマルウエアを添付し、金融機関のアカウント情報を詐取しようとする手法、9 月には、第三者の Web サイトを改ざんしてフィッシングサイトを設置し、そこにユーザを誘導する手法が使用されました。また本四半期に入り、海外のレンタルサーバ上にフィッシングサイトを設置し、ダイナミック DNS サービスを組み合わせる手法が増加していることを確認しています。

JPCERT/CC で報告を受領したフィッシングサイトのうち、金融機関のサイトを装ったものが 59%、通信事業者のサイトを装ったものが 8% を占め、通信事業者を標的としたフィッシングも増加しています。

フィッシングサイトの調整先の割合は、国内が 62%、国外が 38% と、前四半期の割合（国内 58%、国外 42%）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、164 件でした。前四半期の 73 件から 125% 増加しています。

本四半期は、WordPress で構築されたサイトの改ざんの報告を多数受領しました。この改ざんでは、WordPress の Timthumb プラグインの脆弱性を使用したとみられる攻撃により、Web ページに難読化された JavaScript が挿入されます。この JavaScript が挿入されたサイトを閲覧した

PC は、アプリケーションの脆弱性を攻撃するサイトに転送され、その結果マルウエアがインストールされることを確認しています。

Web サイト改ざん等のインシデントを認知された場合は、JPCERT/CC にご報告ください。
JPCERT/CC では、当該案件に関して攻撃元への対応依頼等の必要な調整を行うとともに、同様の被害の拡大を抑えるため、攻撃方法の変化や対策を分析し、随時、注意喚起等の情報発信を行います。

インシデントによる被害拡大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、本四半期においては、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：12 件　https://www.jpcert.or.jp/at/

2011-10-12　2011 年 10 月 Microsoft セキュリティ情報 (緊急 2 件含) に関する注意喚起 (公開)
2011-10-28　標的型メール攻撃に関する注意喚起 (公開)
2011-11-09　2011 年 11 月 Microsoft セキュリティ情報 (緊急 1 件含) に関する注意喚起 (公開)
2011-11-11　Adobe Flash Player の脆弱性に関する注意喚起 (公開)

2011-11-11　Adobe Flash Player の脆弱性に関する注意喚起 (更新)
2011-11-17　ISC BIND 9 サービス運用妨害の脆弱性に関する注意喚起 (公開)
2011-11-18　ISC BIND 9 サービス運用妨害の脆弱性に関する注意喚起 (更新)
2011-11-25　ISC BIND 9 サービス運用妨害の脆弱性に関する注意喚起 (更新)
2011-12-05　Java SE を対象とした既知の脆弱性を狙う攻撃に関する注意喚起 (公開)
2011-12-14　2011 年 12 月 Microsoft セキュリティ情報 (緊急 3 件含) に関する注意喚起 (公開)
2011-12-19　Adobe Reader 及び Acrobat の脆弱性に関する注意喚起 (公開)
2011-12-19　Adobe Reader 及び Acrobat の脆弱性に関する注意喚起 (更新)

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 70 件、「今週のひとくちメモ」のコーナーで紹介した情報は、次の 13 件でした。

2011-10-05　National Cyber Security Awareness Month 2011
2011-10-13　CVSS (Common Vulnerability Scoring System)
2011-10-19　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 11 版
2011-10-26　Oracle Java SE Critical Patch Update
2011-11-02　JBoss ワームに注意
2011-11-09　JP ゾーン DNSSEC 署名開始一年
2011-11-16　Firefox の法人向け延長サポート版について
2011-11-24　サーバアプリケーションのアップデート確認
2011-11-30　サイバーセキュリティ注意喚起サービス「icat」について
2011-12-07　サーバに対するブルートフォース攻撃への備え
2011-12-14　国内金融機関を標的とするフィッシングに注意
2011-12-21　担当者が選ぶ 2011 年重大ニュース
2011-12-28　23/TCP へのスキャンと telnetd の脆弱性

1-2-1-3. 早期警戒情報

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分析・対策情報を「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。

1) 標的型メール攻撃に関する情報発信
前四半期から本四半期にかけて特定組織や企業グループを狙った標的型メール攻撃によるマルウエア感染の事例が報道されました。JPCERT/CC で確認した標的型メールには、ドキュメント形式のマルウエアや実行ファイル形式のマルウエアが添付されていました。
ドキュメント形式のマルウエアは、そのほとんどが既知の脆弱性を使用しており、基本的なセキュリティ対策（OS やソフトウエア、ウイルス対策ソフトなどを最新の状態にするなど）を行うことで、被害を防げるものでした。実行ファイル形式のマルウエアの一部には、アイコンの変更と RLO（Right-to-Left Override）による拡張子偽装によって、メールに添付されたマルウエアが一見して実行ファイルに見えないようにするものがありました。この偽装によって、ユーザがメールに添付されたマルウエアをワードやエクセルなどのドキュメントファイルと誤認して開くことが懸念されました。
JPCERT/CC では、これらの攻撃による被害の発生を防ぐため、国内の組織や企業のシステム管理者に対して、標的型メール攻撃によるマルウエア感染の確認方法を紹介するとともに基本的な対策の実施を推奨し、併せて標的型メール攻撃に関する利用者の理解を深める手法としての IT セキュリティ予防接種の効果等を紹介する注意喚起を行いました。

標的型メール攻撃に関する注意喚起
https://www.jpcert.or.jp/at/2011/at110028.html

2) BIND の脆弱性情報に関する情報収集・提供
JPCERT/CCでは、11月中旬にInternet Systems Consortium, Inc.（ISC）からBIND 9 のサービス運用妨害の脆弱性に関する情報が公開されたことを受け、BIND 9を使用したキャッシュDNS サーバがサービス不能状態になった場合の影響を考慮し、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。注意喚起の発行にあたっては、事前に株式会社日本レジストリサービス（JPRS）と連絡を取り、相互に連携した情報公開を行いま

した。

ISC BIND 9 サービス運用妨害の脆弱性に関する注意喚起
https://www.jpcert.or.jp/at/2011/at110031.html

3) Java SE の既知の脆弱性を狙う攻撃に関する情報収集・提供

Java SE は、出荷時から PC にインストールされているケースが多い一方で、多くの一般利用者がそのことに気づいていないために、必要な更新がなされず、脆弱性のある古いシステムが長く残りがちで、以前から Java SE の脆弱性が攻撃の対象になる可能性が危惧されていました。JPCERT/CC では、Oracle Java SE JDK および JRE の既知の脆弱性（2011 年 10 月 11 日に Oracle 社から公開された脆弱性）を狙う攻撃が活発化しているとの情報を受け、関連マルウエアの入手、分析を行った結果、実際に Java SE の脆弱性を狙って攻撃を行い、外部サイトへ予期しない通信を行ったり、不審な挙動を行ったりするものであることを確認しました。また、併せて、改ざんされた国内サイトから誘導される攻撃サイトに、この脆弱性への対処が行われていない PC にマルウエアを感染させようと細工されたコンテンツが掲載されていることも確認しました。そのため、広くこれらの攻撃への注意と対策の実施を呼び掛ける注意喚起を行いました。

Java SE を対象とした既知の脆弱性を狙う攻撃に関する注意喚起
https://www.jpcert.or.jp/at/2011/at110032.html

1-3. インターネット定点観測システム(ISDAS)

インターネット定点観測システム (以下「ISDAS」といいます。) 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。これらの観測情報は、公開されている脆弱性情報などとあわせて、インターネット上のインシデントの脅威度などを総合的に評価するために利用しています。また、観測情報の一部は JPCERT/CC Web ページ等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

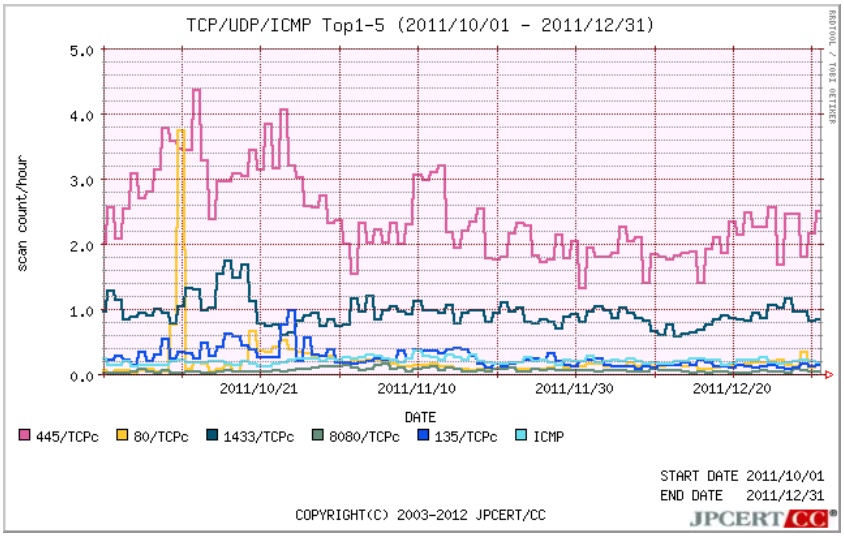
1-3-1. ポートスキャン概況

インターネット定点観測システムの観測結果は、ポートスキャンの頻度や内訳の推移を表すグラフとして JPCERT/CC の Web ページを通じて公開しています。アクセス先ポート別グラフは、各センサーに記録されたアクセス先ポートごとのスキャン件数の平均値を表しています。

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

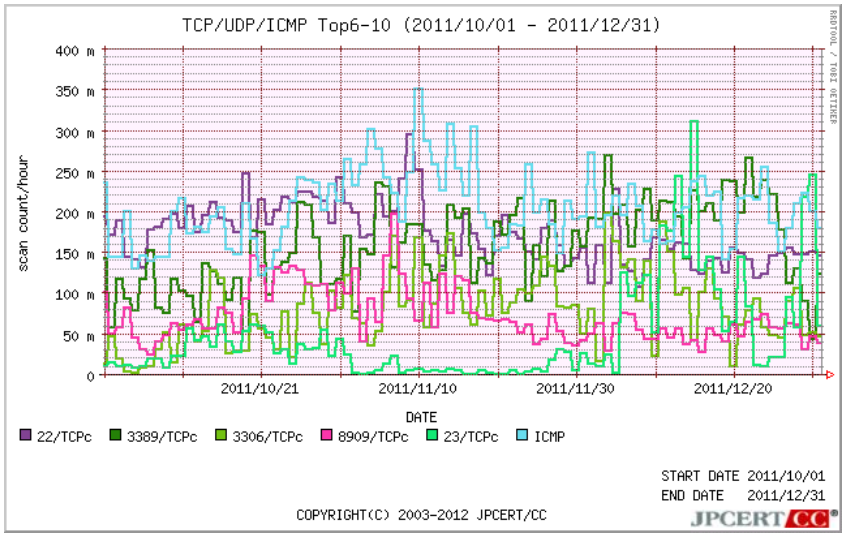
本四半期に ISDAS で観測されたアクセスの宛先ポートの上位 1 位～5 位及び 6 位～10 位のそれぞれについて、アクセス数の時間的の推移を[図 1-1]と[図 1-2]に示します。

- アクセス先ポート別グラフ top1-5 (2011 年 10 月 1 日-12 月 31 日)



[図 1-1 アクセス先ポート別グラフ top1-5]

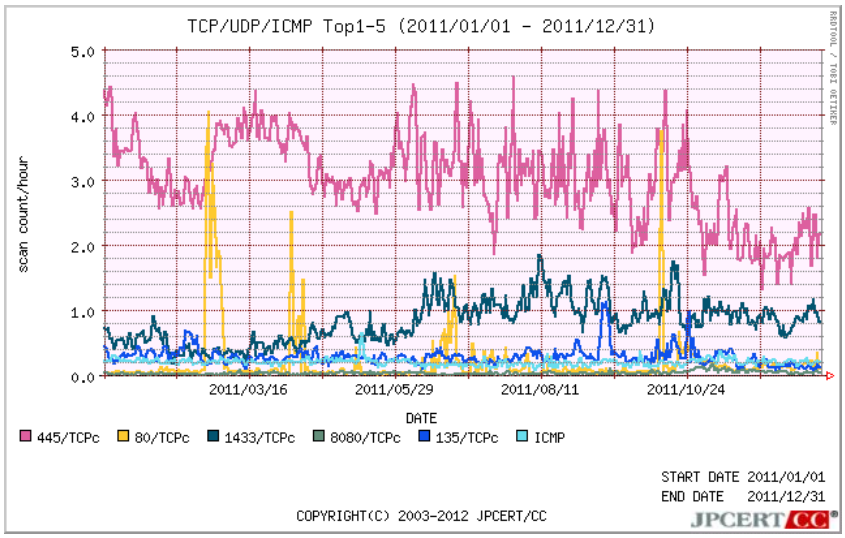
- アクセス先ポート別グラフ top6-10 (2011 年 10 月 1 日-12 月 31 日)



[図 1-2　アクセス先ポート別グラフ top6-10]

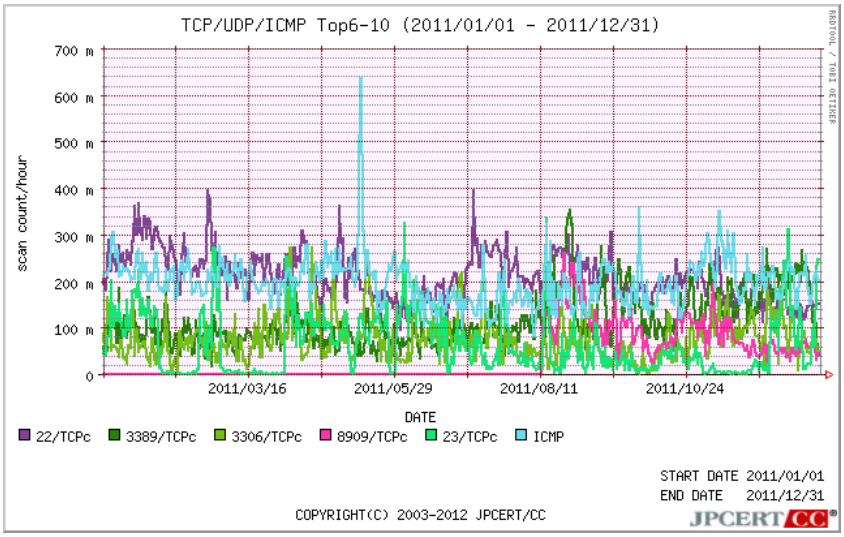
また、より長期間のスキャン推移を見るため、2011 年 1 月 1 日から 2011 年 12 月 31 日までの期間における、アクセスの宛先ポートの上位 1 位～5 位及び 6 位～10 位のそれぞれについて、アクセス数の時間的の推移を[図 1-3]と[図 1-4]に示します。

- アクセス先ポート別グラフ top1-5 (2011 年 1 月 1 日-2011 年 12 月 31 日)



[図 1-3　アクセス先ポート別グラフ top1-5]

- アクセス先ポート別グラフ top6-10 (2011 年 1 月 1 日-2011 年 12 月 31 日)



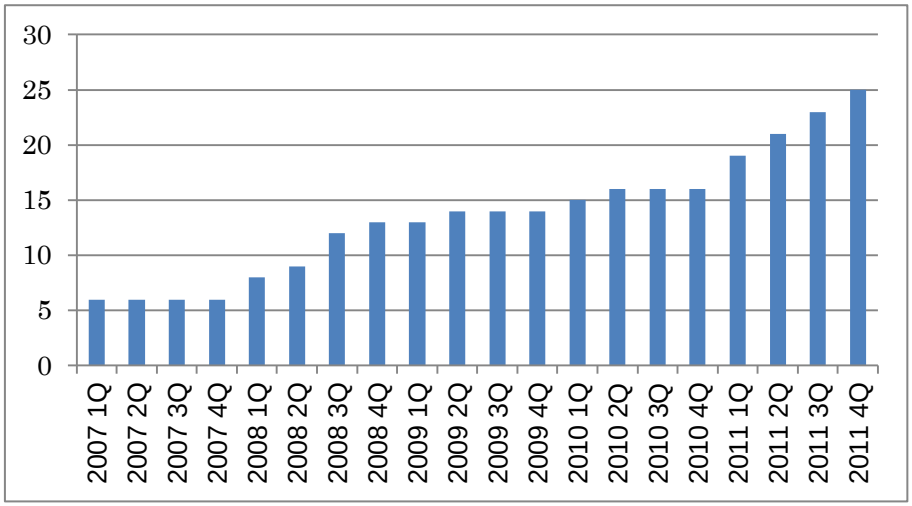
[図 1-4　アクセス先ポート別グラフ top6-10]

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観測されています。そのほか、アクセス制御が不十分な、Proxy サーバへの スキャン が引き続き観測されています。

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、三菱東京 UFJ 銀行(BTMU-CERT)とサイバーエージェント(Amebe CIRT)が、新規に加盟しました。本期末時点で 25 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/

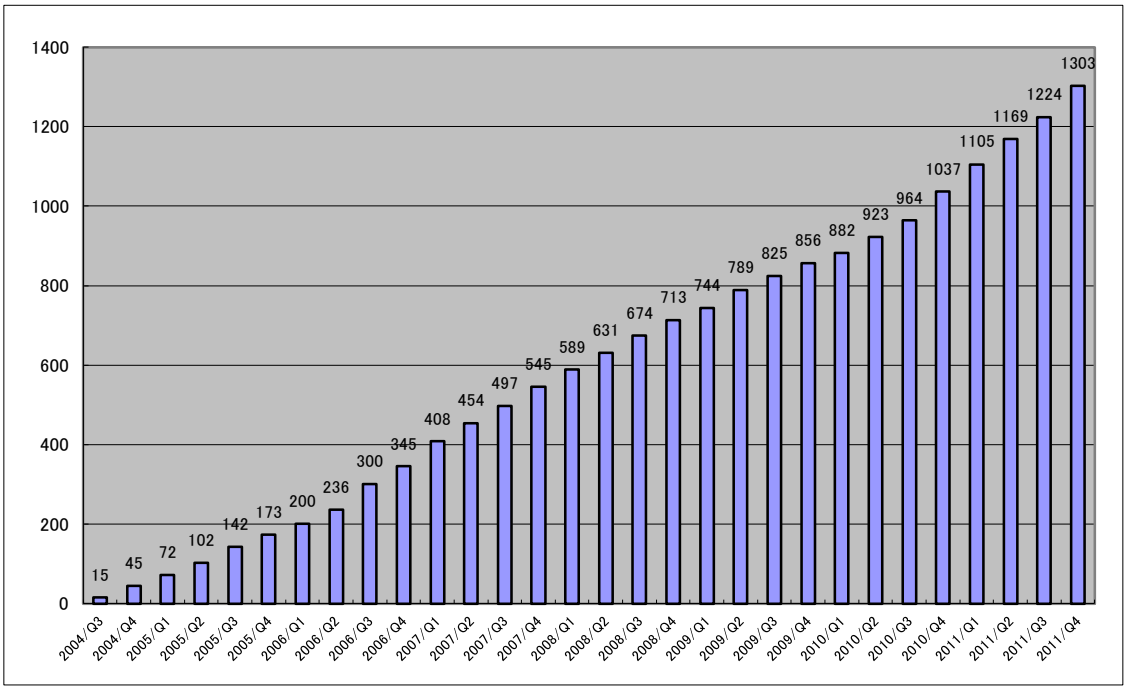
2. 脆弱性関連情報流通促進活動

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) において公開した脆弱性情報および対応状況

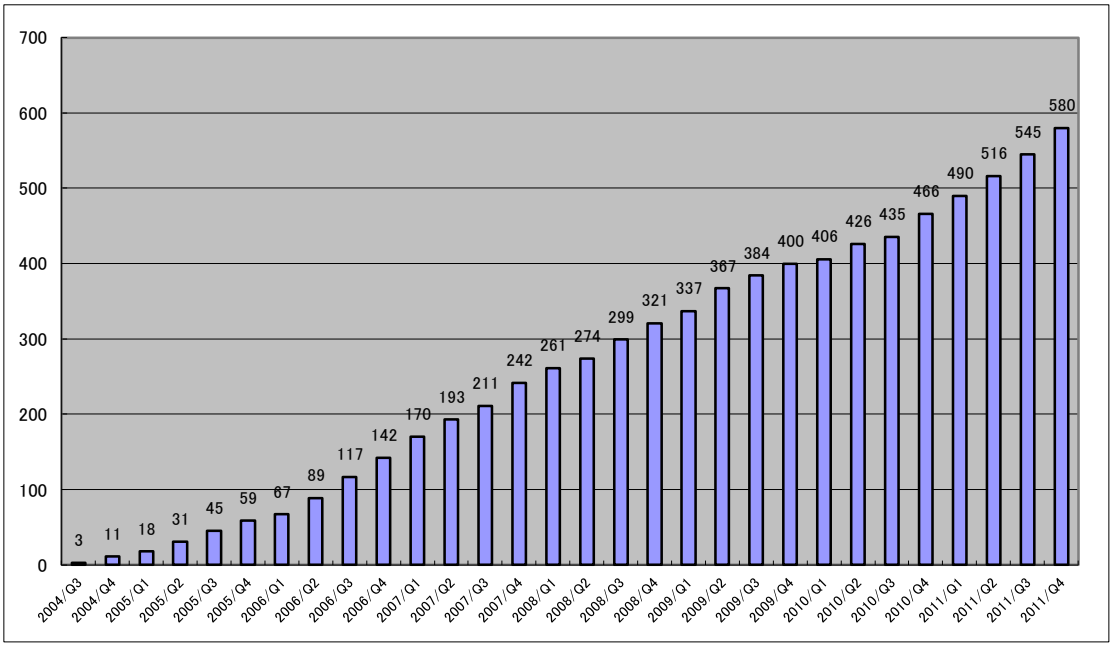
JPCERT/CC は、経済産業省告示「ソフトウエア等脆弱性情報取扱基準」（以下「本基準」といいます。）において、製品開発者とのコーディネーションを行う「調整機関」に指定されており、本基準を踏まえてとりまとめられた「情報セキュリティ早期警戒パートナーシップガイドライン」に詳述された調整機関の役割を担う活動を行っています。

本四半期に JVN において公開した脆弱性情報は、前四半期比約 43%増の 79 件(累計 1303 件) [図 2-1] でした。本四半期に公開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。



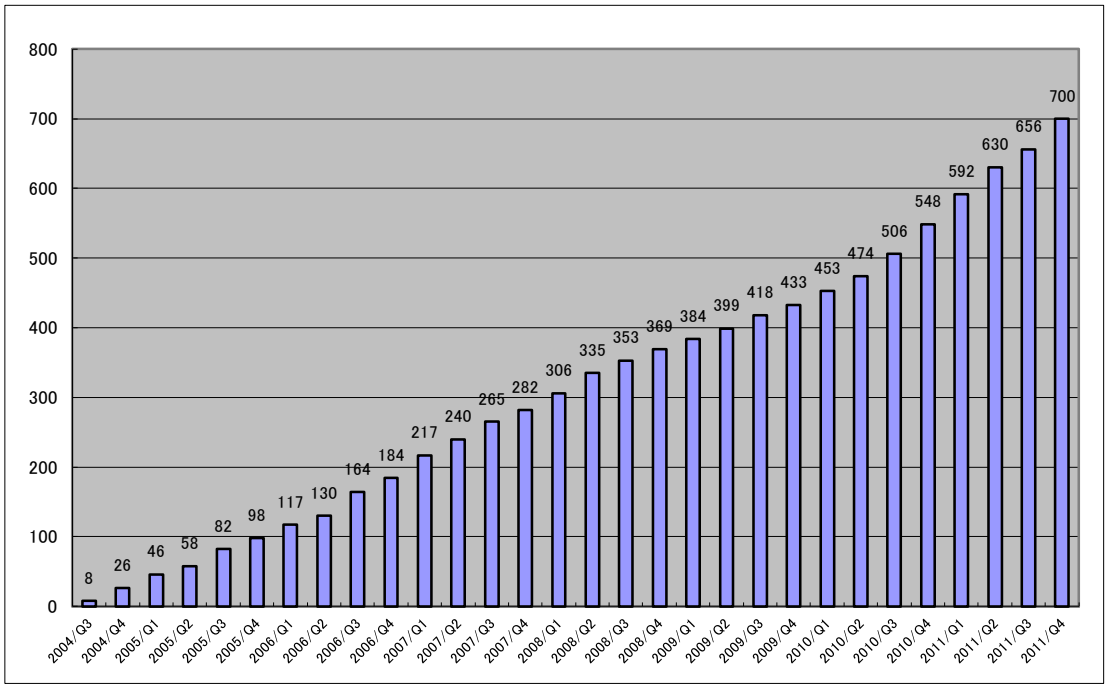
[図 2-1　累計 JVN 公開累積件数]

このうち、本基準に従って調整を行い、JVN で JVN#として公開した脆弱性情報は、35 件(累計 580 件) [図 2-2] でした。そのうちの半数にあたる 15 件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が得られるようになってきています。



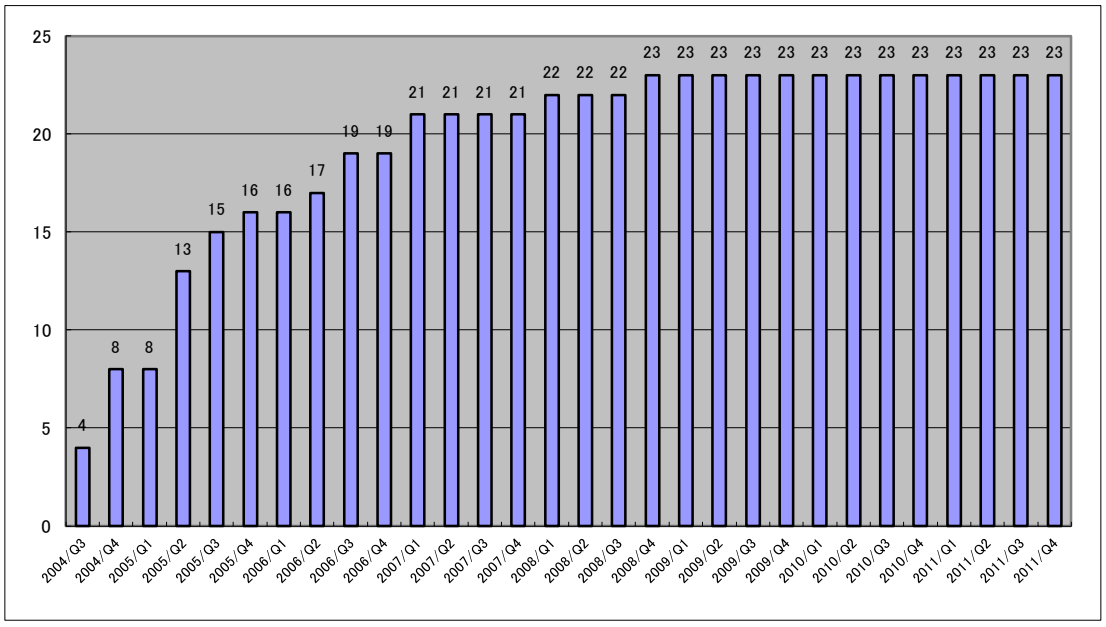
[図 2-2　累計 JVN_JP(JVN#)公開累積件数]

また、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 として公開した脆弱性情報は、前四半期比 69%増の 44 件(累計 700 件) [図 2-3]でした。これらの中には、Adobe 製品に関するものが 2 件、Apple 製品に関するものが 11 件、CA Technologies の製品が 1 件、DELL Computer に関するものが 4 件、HP(Hewlett Packerd)の製品が 1 件、ISC BIND のものが 1 件、Microsoft 製品に関するものが 3 件ありました。このカテゴリで公開された脆弱性には、比較的著名な大手製品開発者の製品における脆弱性情報が多くありました。その一方、今回初めて JVN に登場した製品開発者や製品に関する脆弱性情報の件数も多く、15 件(約 34%)を占めました。このように本四半期は多種多様な製品における多くの脆弱性情報が公開されたため、前四半期に比べ公開件数が大幅に増えました。



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

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 にて公開した脆弱性情報は 0 件(累計 23 件) [図 2-4] でした。



[図 2-4　累計 VN_CPNI(CPNI) 公開累積件数]

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、情報公開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 7 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にお願いして行っています。

その第一段階として、昨年度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。初回公開時には、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、10 月に入って、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、12 月 16 日に、連絡不能開発者一覧として製品開発者 51 件を追加公表しました。また同日、「連絡不能開発者一覧」に 9 月 29 日に掲載した後も連絡がとれないままの 40 件について、掲載済みの製品開発者名に加えて、脆弱性が報告された製品名およびバージョンを追記して、連絡不能開発者一覧を更新しました。更新後、このうちの 2 件について製品開発者から連絡がありました。12 月末日時点では、合計 89 件について連絡不能開発者が公表されています。

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ついて、脆弱性の存在が検証できた製品についてその内容を JVN で公開するための手順や手続き等について、IPA および関係機関とともに検討を行いました。

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、脆弱性情報の公開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(http://jvn.jp/en)の運用を開始し、3 年が経過しました。JVN 英語版での情報公開は、日本語版公開とほとんど時間差なく、ほぼ同時公開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、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、28件の脆弱性情報についてJPCERT/CCがCVEを採番し、1件の脆弱性情報については製品開発者であるApache Struts開発チームが自らCVEを採番していたため、合計29件のCVEがJVN上に掲載されました。

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

2-3. 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。

2-3-1. 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、受付機関に独立行政法人情報処理推進機構（以下「IPA」といいます。
http://www.ipa.go.jp/)、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、緊密な連携をおこなっています。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。

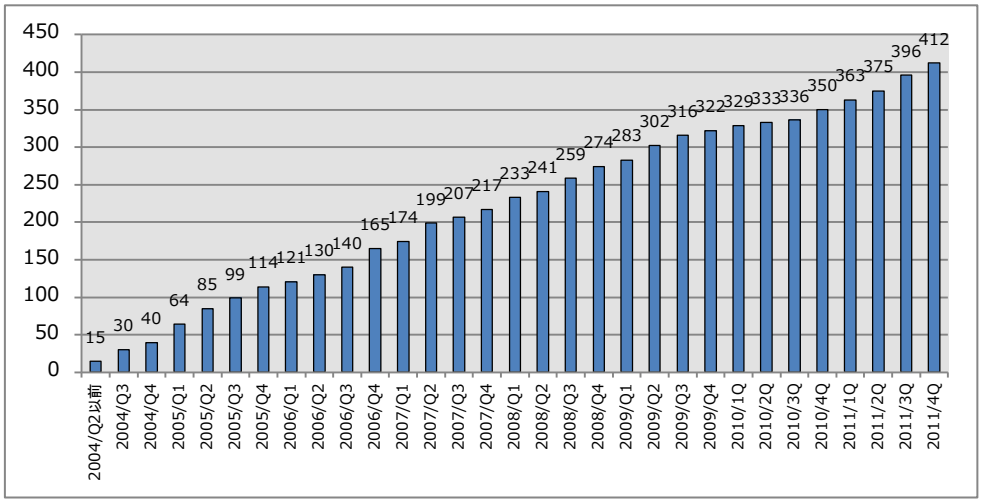
http://www.ipa.go.jp/security/vuln/

2-3-2. 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、2011 年 12 月 31 日現在で 412 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]

2-3-3.　脆弱性情報流通体制の普及啓発

オープンソースソフトウエアやその他の製品開発者およびコミュニティに対して、日本国内の脆弱性情報流通体制の認知を向上し、相互理解を深めるため、2011 年 11 月 11 日に開催された関西オープンソース 2011 へ参加しました。脆弱性情報ハンドリング業務内容と活動状況、その他の JPCERT/CC の活動内容について紹介し、オープンソースソフトウエア分野における脆弱性対応について出展コミュニティや一般来場者との意見交換、情報交換を行いました。

[図 2-6　関西オープンソース 2011 会場の様子]

2-4. セキュアコーディング啓発活動

2-4-1. 「CERT Oracle Java セキュアコーディング スタンダード」日本語版公開

「CERT Oracle Java セキュアコーディングスタンダード」（原題：The CERT Oracle Secure Coding Standard for Java）は、カーネギーメロン大学ソフトウエア工学研究所の CERT プログラムの下で、Oracle 社やその他の Java の専門家も加わって Wiki を通じて共同開発された Java のコーディング規約集です。JPCERT/CC は、この開発に貢献するとともに、ドキュメントを日本語に翻訳し、公開しました。

コーディングルールは 17 のカテゴリーに渡る 156 個の規約で構成されており、Java 言語を使って安全なソフトウェア開発を行うための注意点を、コード例を示しながらわかりやすく解説しています。対象プラットフォームは Java SE 6 および Java SE 7 です。さらに、日本語版には、Android 環境で特に重要なルールにコメントを付して一覧表としてまとめた「Android アプリケーション開発へのルールの適用」を追加しました。

Android アプリケーション開発者のみならず、広く Java を使ったソフトウエア開発に携わるプログラマ、プロジェクトマネージャ、コードレビュー担当者、品質管理担当者、教育担当者、その他 Java のセキュリティに関心のある皆様にご一読いただき、Java アプリケーションのセキュリティ向上に役立てられることを期待しています。

CERT Oracle Java セキュアコーディングスタンダード
https://www.jpcert.or.jp/java-rules/

2-4-2. 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」連載開始

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」と題したシリーズで Java セキュアコーディングの解説記事の連載を始めました。昨年の C セキュアコーディングに関する連載に引き続き、今度の連載では、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を解説します。最近話題の Android アプリケーションの脆弱性についても取り上げます。本四半期は、以下の 3 つの記事を掲載しました。次回以降の連載も是非ご一読ください。

第 1 回「Android アプリ開発者なら押さえておきたい Java セキュアコーディングの意味と効果」(11 月 24 日公開)
第 2 回「ContentProvider のアクセス範囲―Dropbox における脆弱性の修正」(11 月 29 日公開)
第 3 回「整数オーバーフロー検出の 3 つのアプローチ―mezzofanti のバグ修正」(12 月 16 日公開)

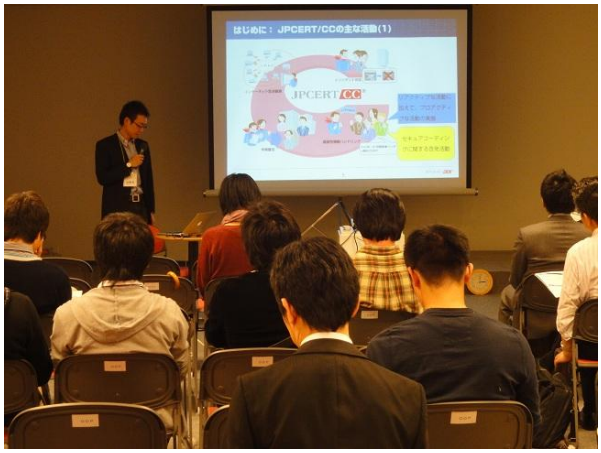
CodeZine (コードジン) Java セキュアコーディング入門
http://codezine.jp/article/corner/437

2-4-3.「関西オープンソース 2011」にて講演

本四半期は、以下のイベントで講演を行いました。

イベント名：関西オープンソース 2011
開催日時：2011 年 11 月 11 日 (金)
講演タイトル：セキュアコーディングノススメ（Java 編）

講演では、ソフトウエア開発における脆弱性の混入を防ぎコード品質向上に寄与するセキュアコーディングについて概説し、特に Java 言語での開発を題材に、OSS での事例や Android アプリケーション開発でのポイントなどを織り交ぜて紹介しました。
本イベントはプログラミングを学び始めたばかりの学生から社内で開発プロジェクトに携わっている方まで幅広い層が参加しており、このような場で定期的に講演を行うなどの活動を通じて、セキュアコーディングの普及啓発を続けていくことが重要であると考えています。



[図 2-7　関西オープンソース 2011 での講演の様子]

2-4-4.　C/C++セキュアコーディング 出張セミナー

JPCERT/CC では、C/C++言語を使用した開発を行う企業・組織を対象に、C/C++セキュアコーディングに関する出張セミナー（有償）のご要望を承っています。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。本四半期は、国内大手メーカ様 1 社向けに出張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。

2-5. 制御システムセキュリティ強化に向けた活動

2-5-1. 情報発信活動

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て、制御システム関係者向けに原則として隔月で提供しているニュースレターを本四半期は計 2 回（12 月 13 日、12 月 27 日）配信しました。

なお、本活動は、2009 年にベンダ技術者を主体とする「制御システムベンダーセキュリティ情報共有タスクフォース」として発足し、2010 年からは対象を制御システムセキュリティに携わるすべての関係者へと広げ活動を進めて参りました。そのような中で、本年度、経済産業省において「制御システムセキュリティ検討タスクフォース」が別に設置されたことから、名称の類似性による混乱を避けるため、本活動の名称を 11 月より「制御システムセキュリティ情報共有コミュニティ」に変更しています。

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 188 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。参加資格や申し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

2-5-2. 国内外情報収集活動

米国 CSSP の ICSJWG が半年ごとに定期開催している「ICSJWG カンファレンス」が 10 月下旬にカリフォルニア州ロングビーチで開催されました。JPCERT/CC からも参加し、運用と管理と技術の領域における米国での取組みと現状について情報収集に努めました。制御システムセキュリティへの取組みが強化され始めているなかで、JPCERT/CC では、海外の先進事例の収集とその国内への展開や、海外パートナーとの情報共有にこれからも取り組んでいきます。

ICSJWG
http://www.us-cert.gov/control_systems/icsjwg/index.html

2-5-3. 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 10 件の申込みがあり、直接配布件数の累計が 85 となりました。

2-5-4. 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、前年度公開したセキュリティ・アセスメント・ツール「日本版 SSAT」のバージョンアップに向けて、各業界のユーザからの意見も伺いながらツールのブラッシュアップをはかる活動や計測展に向けた資料の作成、開催準備等を行いました。

2-5-5. 制御システムセキュリティカンファレンスの開催準備

制御システムに関係する産官学のスピーカーを招いて意見交換・情報交換を行う制御システムセキュリティカンファレンスの開催に向けた準備を進めています。今回は「After Stuxnet」をテーマに、Stuxnet 登場以降のユーザ、ベンダおよび国の取組みなどを中心に事例や情報を紹介する予定です。制御システムセキュリティ情報共有コミュニティのメンバーおよび関係者向けの事前連絡としてカンファレンスプログラムの詳細および参加案内を 12 月 27 日に公表しました。

2-5-6. インシデントハンドリング体制 WG の活動開始

本四半期から開始した経済産業省主催の制御システムセキュリティ検討タスクフォースに設置されたインシデントハンドリング体制 WG の事務局として、制御システム業界におけるインシデント発生時の対応体制の整備や制御システム関連製品における脆弱性の取扱いなどをテーマに検討を始めております。検討結果は、来春、制御システムセキュリティ検討タスクフォースに報告される予定です。

2-5-7. 講演活動

東京三田 NN ホールにて開催された「2011 計装制御技術会議」（日本能率協会主催）の 2 日目に当たる 10 月 28 日のプログラム「深刻になった制御システムセキュリティの脅威」において、「制御システムセキュリティの新たなる脅威について」と題する講演を行いました。

また、11 月 15 日に東京工業大学で開催された、「2011 年度産業応用部門大会」（SICE 産業応用部門主催）の、計測・制御ネットワークシンポジウムにおいて、「Stuxnet で明らかにされた制御システムセキュリティの神話と現実」と題する講演を行いました。

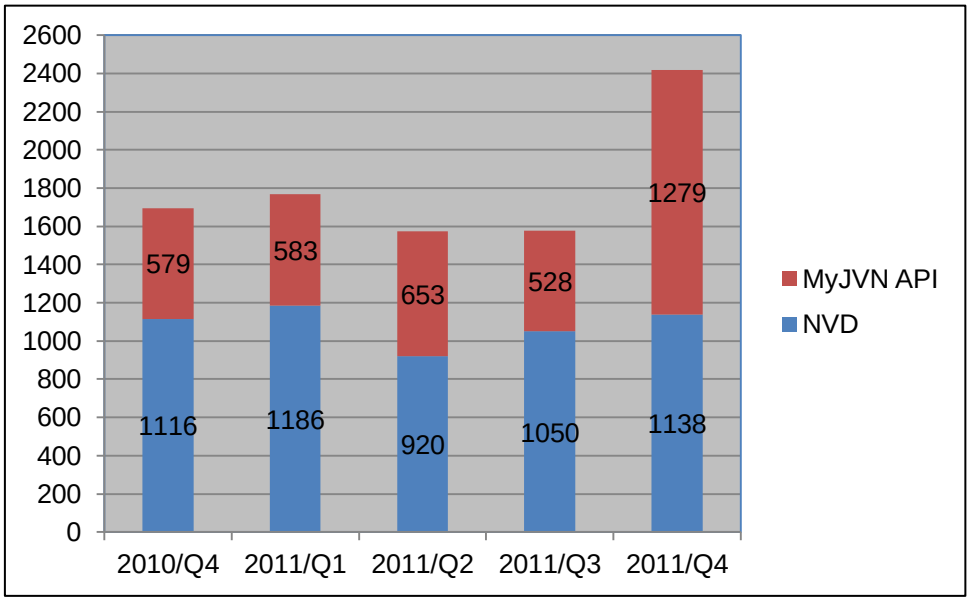
さらに、2011 年 11 月 16 日に東京国際展示場で開催された「ものづくり NEXT↑2011」トータル危機管理コーナーにおいて「制御システムセキュリティの新たなる脅威について」と題する講演を行いました。

2-6. VRDA フィードによる脆弱性情報の配信

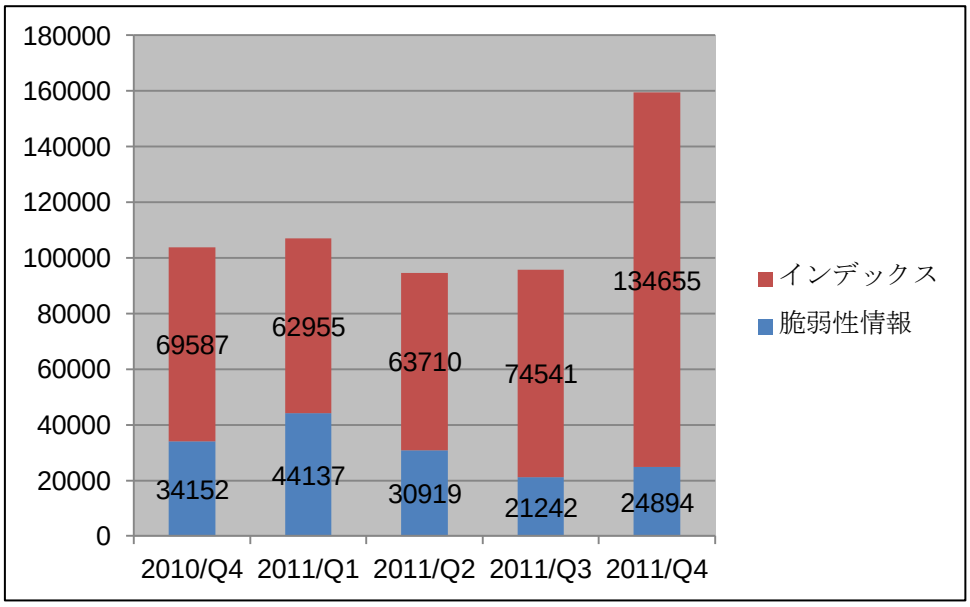
JPCERT/CC は、大規模組織の組織内 CSIRT などでの利用を想定して、KENGINE などのツールを用いた体系的な脆弱性対応を可能とするため、IPA が運用する MyJVN API および NIST (National Institute of Standards and Technology)の NVD (National Vulnerability Database) を外部データソースとして利用した、VRDA (Vulnerability Response Decision Assistance)フィードによる脆弱性情報の配信を行っています。VRDA フィードについての詳しい情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

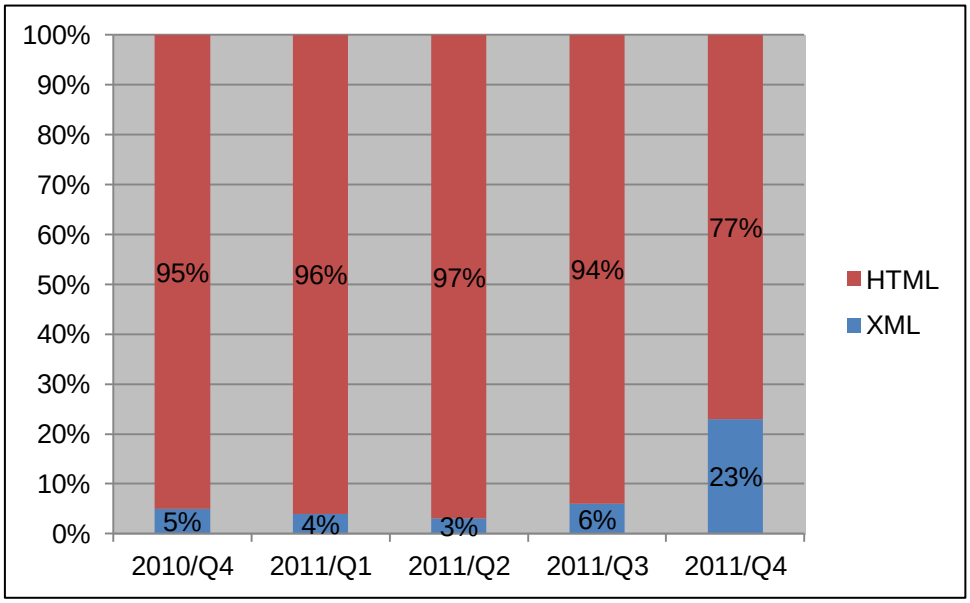


[図 2-8 VRDA フィード配信件数]



[図 2-9　VRDA フィード利用件数]

[図 2-9] に示したように、前四半期と比較すると、VRDA フィードインデックスの利用数に大きな増加が見られます。



[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では、本四半期に XML 形式の利用割合が大きく増加しています。

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。

アーティファクト分析から得られる知見の中には JPCERT/CC 外へ提供することでより有効に活用できるものが多々あります。インターンや講習を通した分析技術の共有もその一つですが、マルウエア等の検体そのものや分析結果といった"ナマモノ"も、サイバー攻撃への対処を行う関係者間でうまく共有されれば、強力な対抗手段に成り得ます。本四半期においても、他組織との間で検体やその関連情報を共有するためのいくつかの取組みに参加しました。

3-1. 「マルウエア対策研究人材育成ワークショップ 2011(MWS 2011)」への参画

「マルウエア対策研究人材育成ワークショップ 2011(MWS 2011)」(サイバークリーンセンター運営委員会および情報処理学会が共催)が 10 月 19 日から 3 日間の日程で新潟コンベンションセンター（朱鷺メッセ）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 データセット」には、2010 年度まで総務省・経済産業省連携プロジェクトとして実施されていたボット対策プロジェクトで収集したボット観測データから抽出した CCC データセットのほか、賛同する組織から提供されたデータが含まれています。

JPCERT/CC は、CCC データセットに含めるマルウエア検体の選定作業を担当するとともに、10 月 19 日に会場にて選定検体の解説発表を行いました。

マルウエア対策研究人材育成ワークショップ 2011(MWS 2011)
http://www.iwsec.org/mws/2011/

3-2. 攻撃に関する情報共有の取組み

経済産業省の事業として実施されている「標的型攻撃に関する情報共有枠組みのパイロットプロジェクト（CTAPP: Counter Threats and Attack Partner Program）」や、日本セキュリティオペレーション事業者協議会（ISOG-J）の「標的型攻撃対策検討ワーキンググループ」等の取組みに参加し、攻撃に関する情報共有の可能性や有効性について専門家や事業者との意見交換を行いました。

JPCERT/CC はこのような活動を通して、攻撃に関する情報を安全かつ適時に共有する方法の確立や、その有効性の確認を関係組織と協力しながら今後も進めて行きます。

4. 国際標準化活動

4-1.「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、ベンダーの外側から見える、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、ベンダー内部での対応を規定することになっています。10 月 10 日～14 日には、ナイロビ(ケニヤ)で SC27 の国際会議が開催され、JPCERT/CC からも日本の代表団の一員としてこれに参加し、双方の標準草案の改訂方針の検討を行いました。

「脆弱性情報の開示」については、第 3 次委員会草案(CD ; Committee Draft)をベースに、あらかじめ参加各国から寄せられた総計 140 件のコメント(ベルギー73 件, カナダ 3 件, ドイツ 13 件, 日本 25 件, 英国 87 件, 米国 12 件 ; ベルギーと英国は FIRST からのコメントを重複して含む)を処理するかたちで審議が進められました。大きな論点では、標準文書としての記述範囲について「取扱手順」との切分けがありましたが, 日本からのコメントが各国の賛同を得て、本節の冒頭で書いたような方針で進められることになりました。ストックホルムでの次の SC27 国際会議への準備を含めた、今後の改訂作業については、計画を 2 年遅らせて 2013 年春に次の標準化段階に進めることを目指し、今回の議論結果を踏まえて第 4 次委員会草案をプロジェクト・エディタが準備することになりました。

「脆弱性情報の取扱手順」については、第 1 次作業草案(WD ; Working Draft)をベースに, あらかじめ参加各国から寄せられた総計 40 件のコメント(カナダ 4 件, ドイツ 5 件, 日本 9 件, 韓国 2 件, 米国 20 件) を処理するかたちで審議が進められました。比較的大きな改訂としては、日本がコメントの中で提案をした、脆弱性情報を取り扱うためのベンダーの社内体制について新たな章を設けて記述を拡充することとなりました。今後の改訂作業については、今回の議論結果を踏まえて第 2 次作業草案をプロジェクト・エディタが次の SC27 国際会議に向けて準備することになりました。なお、社内体制に関する記述については、情報セキュリティ早期警戒パートナーシップの発足時に電子情報産業協会が中心になってまとめられた「製品開発ベンダーにおける脆弱性関連情報取扱に関する体制と手順整備のためのガイドライン」の中の関連する記述を参考に JPCERT/CC において文案を作成し、プログラム・エディタの改訂作業に間に合うように提供いたしました。

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。

4-2. インシデント管理の国際標準化活動への参加

インシデント管理やCSIRTの運営に関する国際標準の策定を行うISO/IEC JTC-1/SC27 WG4 の活動にも参加しています。2011年9月1日に発行されたISO/IEC 27035:2011 (インシデント管理；Information security incident management)を補完する標準として「インシデントの管理と運用と対応」(IMOP: Incident Management, Operation and Response)を作成する必要性が約1年間にわたり検討されてきましたが、2011年10月に開催されたナイロビ会議において、標準化作業開始の妥当性調査のフェーズを終了し、27035:2011を早期改訂し、以下の3つのパートからなるマルチパート標準へ再構成された標準化を進めるための国際投票を次回のストックホルム会議（2012年5月開催予定）に向けて行うことで、各国の合意が得られました。

Part 1. インシデントの管理の原理（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. CSIRT 運用のためのガイドライン（Guidelines for CSIRT Operations）

ナイロビ会議では、会議に先立ち提出された、今後の標準化の方針に関する日本の一般的なコメントと、マルチパート標準に拡張する英国の具体的提案をベースに議論が進められました。日本のコメントについては各国の理解が得られました。英国の提案については、インシデント対応成熟度モデル（Incident Response Maturity Model）に関する独立したパートの作成は時期尚早ではないかという日本の提案が受け入れられ、当初は付属書（Annex）の位置づけで標準化を進めることを提案するとの合意が得られました。

今後は、次回のストックホルム会議までに、英国が Part 2 の、韓国が Part3 の草案を用意し（Part 1 は既存の 27035:2011 を草案として使用する）、標準化に向けた検討が進められることになります。

インシデント管理と CSIRT の運営に関する標準化の動向についても、JPCERT/CC では引き続き 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たフォローアップを継続していく所存です。

5. 国際連携活動関連

5-1. 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。

5-1-1. アジア太平洋地域(オセアニア)における活動

5-1-1-1. 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。

5-1-1-2. 大洋州地域の CSIRT 構築支援活動(2011 年 10 月 22 日-11 月 13 日、11 月 13 日-12 月 2 日)

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、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フィジーに赴きました。
10 月の派遣においては CSIRT に必要なシステム構築を支援し、11 月の派遣においては CSIRT の根幹業務であるインシデントハンドリングに関する OJT 研修等を実施しました。

5-1-1-3. ミャンマーの CSIRT 構築支援活動(2011 年 12 月 5 日-12 月 9 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（JODC）から、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、9 月にはネットワークフォレンジック研修（座学とハンズオン）の講師を派遣していましたが、本四半期は、12 月 5 日から 9 日の計 5 日間、ヤンゴンで実施されたマルウエア解析研修（座学とハンズオン）に 2 名の講師を派遣し、ミャンマーの National CSIRT である mmCERT のスタッフと ISP などの技術者およそ 20 名に対して、解析ツールを利用した不正なプログラムの動的分析・静的分析手法を教授しました。

5-1-2. その他地域における活動

5-1-2-1. アフリカ CSIRT 構築支援(2011 年 11 月 19 日-11 月 25 日)

JPCERT/CC は、11 月にカメルーンで開催された国際会議 Afrinic-15 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。
JPCERT/CC は 2010 年春から合計 3 回、アフリカ諸国での CSIRT 構築を支援し、CSIRT 構築支援を指導する人材を育成することを目標にトレーニングを実施してきました。4 回目となる今回は、CSIRT 技術者向けネットワークフォレンジックコース(11 月 19 日及び 20 日)と、フランス語での CSIRT マネージャー向けコース(11 月 21 日)、AfricaCERT Workshop(11 月 22 日)の大きく 3 つのパートによって構成される、合計 4 日間のトレーニングを行いました。

CSIRT 技術者向けネットワークフォレンジックコースでは、JPCERT/CC が講師として、アフリカ各国から参加した約 30 名のエンジニアにネットワーク解析ツールを使ったインシデント対応の技術を伝えました。

フランス語での CSIRT マネージャー向けコースは、一連のアフリカ CSIRT 構築支援の中で初となるフランス語でのトレーニングです。アフリカにはフランス語を公用語とする国が多くあり、かねてから英語ではなくフランス語でのトレーニングが必要との声がありました。過去の JPCERT/CC のトレーニングを受講したフランス語を得意とするアフリカ人講師が主任講師をつとめ、JPCERT/CC は質疑応答などで講師をサポートする役割を担いました。

AfricaCERT Workshop は、アフリカにおける CSIRT 構築の取り組みを相互に共有する 1 日のセミナーで、先進的な取り組みを行う CSIRT がその活動を紹介し、併せて AfricaCERT というアフリカ地域の CSIRT 連合体の活動への参加と協力を求めました。

なお、本トレーニングは Afrinic 会議のトレーニングセッションの一つとして行われました。Afrinic はアフリカ諸国のインターネット政策担当者と技術者の連携と教育を目的とする非営利組織です。Afrinic は、アフリカ各地で年次会議を開催し、そこでトレーニングと最先端の技術を紹介する講演などを提供しています。今年の会議は、カメルーン政府などがスポンサーとなり、カメルーンの首都ヤウンデの中心部で開催されました。

JPCERT/CC は、アフリカにおける情報セキュリティ対策が進み、ひいてはインターネット全体が安全になるよう今後もこの取り組みを続けます。
Afrinic 15 及び CSIRT トレーニングのプログラムについての詳細は、次の URL をご参照下さい。

Afrinic 15 公式ページ
https://meeting.afrinic.net/afrinic-15/

5-2. 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。

5-2-1. アジア太平洋地域(オセアニア)における活動

5-2-1-1. APCERT (Asia Pacific Computer Emergency Response Team)

JPCERT/CC は APCERT に加盟しています。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/

5-2-1-1-1. APCERT Steering Committee 電話会議の実施

10 月 13 日及び 12 月 7 日に Steering Committee 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。

5-2-1-1-2. APCERT と他組織間との連携

1) 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(9 月 27 日にクアラルンプールで開催)に対して、APCERT の議長チームとして、APCERT の活動概要を紹介するビデオメッセージ送りました。

2) イスラム諸国会議機構(OIC)の創設した OIC-CERT と APCERT 間で、9 月 27 日、今後の連携強化を目的とした MoU を締結しました。同日、ドバイで開催された調印式には APCERT の議長チームとして出席しました。

3) 12 月 5 日-7 日まで開催された、国内外の情報セキュリティ関係者が一堂に会する The 2nd APT Cybersecurity Forum の 12 月 6 日のセッションにおいて、JPCERT/CC の職員が 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。

5-2-1-2. The 2nd APT Cybersecurity Forum での講演(12 月 5 日)

12 月 5 日-7 日まで開催された、国内外の情報セキュリティ関係者が一堂に会する The 2nd APT Cybersecurity Forum の 12 月 5 日のセッションにおいて、JPCERT/CC の活動紹介や CSIRT 構築及び連携の重要性をテーマとした講演を行いました。

5-2-1-3. 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(2011 年 12 月 13 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 11 名（ラオス、ミャンマー、ナイジェリア、ルワンダ、モンテネグロの政府系組織の 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 の事業紹介等を行った後、活発な意見交換が行われました。

5-2-1-4. 日中韓の National CSRIT 間で覚書(MOU)締結(2011 年 12 月 20 日)

JPCERT/CC 及び中国の National CSIRT である CNCERT/CC、韓国の National CSIRT である KrCERT/CC の 3 組織間で、各々２カ国間で締結してい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覚書（MOU）を拡張して、３カ国間の覚書とする合意が成立し、2011 年 12 月 20 日に調印しました。3 カ国による覚書調印は JPCERT/CC としても初の試みです。

5-2-1-5. 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。
11 月 2 日、3 日に北京で開催された、「RSA 2011 信息安全国际论坛」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。また、11 月 24 日、25 日に上海で開催された、「Internet Security Forum 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。収集した情報は、日本国内の関係者会合などへ展開しました。

5-2-2. その他の地域における活動

5-2-2-1. FIRST (Forum of Incident Response and Security Teams)

JPCERT/CC は FIRST に加盟しています。FISRT の詳細については、次の URL をご参照ください。

FIRST
http://www.first.org/

5-2-2-1-1. 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、サイトビジットや書類作成等を行いました。
本四半期は、三菱東京UFJ銀行の組織内CSIRTであるBank of Tokyo-Mitsubishi UFJ Computer Emergency Readiness Team (BTMU-CERT)のスポンサーを務め、同組織は11月に正式にFIRST加盟に至りました。2011 年12 月末現在、日本からのFIRST 加盟チームは、21チームとなっています。

5-2-2-3. GOVCERT.NL シンポジウム 2011 への参加 (2011 年 11 月 15 日-16 日)

オランダのロッテルダムで開催された GOVCERT.NL シンポジウム 2011 に参加し、講演やパネルディスカッションを通して、最新のトピックスや動向（オランダ政府におけるサイバーセキュリティの最新動向、SCADA システムを様々な脅威から守る手法、制御システム向け製品の脆弱性情報の取扱い、モバイル OS のセキュリティ等）に関する情報を収集しました。また、欧州各国の CSIRT 等との円滑な連携の継続のため、各チームと近況等に関する情報交換を行いました。さらに、ICS-CERT との連携活動を深めるべく、脆弱性情報の取扱いについてディスカッションを行いました。

5-2-2-4. 米国 US-CERT 訪問および CIP-Forum への参加(2011 年 11 月 28 日-30 日)

米国の US-CERT を訪問し、JPCERT/CC と US-CERT 間の連携活動（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 から日本の情報セキュリティに関する取り組みについて講演を行いました。

5-2-3. 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 の活動等について情報発信を行っています。本四半期は、ミャンマーでのネットワークフォレンジック研修に関してブログにエントリーを掲載しました。

CSIRT Training in Myanmar
http://blog.jpcert.or.jp/2011/11/csirt-training-in-myanmar.html

6. フィッシング対策協議会事務局の運営

JPCERT/CC では、経済産業省からの委託により、フィッシング対策協議会（以下、本章において「協議会」といいます。）の事務局として、協議会の総会や各ワーキンググループの運営、Web ページの管理、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。

6-1. 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 により、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。

本四半期の特徴的なフィッシング事例として、国内の金融機関を騙り、乱数表や第二暗証番号などの第二認証情報を詐取するフィッシングを確認しています。

第二認証情報のうち、乱数表や第二暗証番号を用いる手法は、金融機関などが契約者ごとに異なる情報を記載したカードをあらかじめ配付しておき、ログイン時に ID とパスワードに加えて、カード上の指定した欄に記載された数字を入力させることにより認証を厳格化するものです。
多くの金融機関では、第二認証を使うことにより、送金のような機微な操作もオンラインで実行できます。

金融機関を騙るフィッシングは以前より確認していましたが、当協議会において第二認証情報を詐取する国内のフィッシングを確認したのは、今回が初めてです。ログイン ID やパスワードに加えて、第二認証情報まで詐取されてしまうと、預金残高によっては高額の金銭被害が発生する可能性があります。

本四半期における第二認証情報の詐取では、実行ファイル添付型またはフィッシングサイト誘導型のいずれかの仕組みが使われました。実行ファイル添付型の場合には、電子メールに実行ファイル(Exe ファイル)が添付されており、そのファイルを開くと、プログラムが起動されて、ログイン ID やパスワードとともに、第二認証情報の入力を促します[図 7-1]。

フィッシングサイト誘導型の場合には、メールに記載された URL を開くとブラウザの画面に実行ファイル添付型と同様の記入欄が現れます。

協議会では、一般消費者から寄せられたメールや Web サイトについてフィッシングであるか否かの判定を行い、名前を騙られた事業者に情報提供するとともに、緊急情報 「三井住友銀行を騙るフィッシング」(10 月 6 日)と「セブン銀行を騙るフィッシング」(11 月 9 日)、および事例公開「みずほ銀行を騙るフィッシング」(12 月 5 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や実行ファイルの情報送信先サイトの停止を確認しました。

[図 7-1　三井住友銀行を騙るフィッシングサイト
https://www.antiphishing.jp/news/alert/smbc2011106.html]

6-2. フィッシングサイト URL 情報の提供先の拡大

協議会では、会員の中でフィッシング対策ツールバーなどを提供している事業者やウイルス対策ソフトベンダ、フィッシングに関する研究を行っている学術機関に対し、協議会に報告される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、東京大学 (2011 年 10 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合計で 16 組織となりました。現在も複数の事業者との間で情報提供に関する協議を行っており、提供先を順次拡大していく予定です。

6-3. 海外カンファレンス参加

2011 年 11 月にアメリカのサンディエゴで開催された APWC eCrime 2011 San Diego 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、その結果を協議会主催の情報共有勉強会で協議会会員に報告しました。

6-4. 講演活動

本四半期の講演活動はありませんでした。

6-5. 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 2011 年 10 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201110.html

フィッシング対策協議会 2011 年 11 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201111.html

フィッシング対策協議会 2011 年 12 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201112.html

7. 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。

7-1.セキュア開発支援資料「CERT Oracle Java セキュアコーディングスタンダード」

本資料についての詳細は、「2-4-1.」をご参照ください。

CERT Oracle Java セキュアコーディングスタンダード　(2011 年 11 月 7 日)
https://www.jpcert.or.jp/java-rules/

7-2. フィールドレポート「CSA ガイダンスの Ver.3 では Security as a Service を追加予定」の公開

JPCERT/CC が連携している海外組織の活動や海外のセキュリティ動向などを日本のセキュリティ関係者にも知っていただくことを目的に「フィールドレポート：海外セキュリティ関連機関・組織の動向」のコーナーを JPCERT/CC の Web サイト上に設けています。本四半期は、「CSA ガイダンスの Ver.3 では Security as a Service を追加予定」を公開しました。最新のクラウドセキュリティ動向や CSA の活動などについての紹介を含む Cloud Security Alliance(CSA)上席部長へのインタビュー記事です。

CSA ガイダンスの Ver.3 では Security as a Service を追加予定
(2011 年 11 月 8 日)
https://www.jpcert.or.jp/magazine/security/field-csa.html

8. 講演活動一覧

(1) 宮地 利雄 (理事) :
「現実化する『制御システムへのサイバー攻撃』その背景と実態、そして対策」
グローバルコモンズ Web セミナー.JP, 2011 年 10 月 13 日

(2) 宮崎 清隆 (分析センター 情報システムセキュリティアナリスト) :
「CCC DATAset 2011 マルウェア検体解説」
MWS2011,2011 年 10 月 19 日

(3) 宮地 利雄 (理事) :
「制御システムセキュリティの新たなる脅威について」
2011 計測制御技術会議, 2011 年 10 月 27 日

(4) 熊谷 裕志 (情報流通対策グループ 情報システムセキュリティアナリスト) :
「セキュアコーディングノススメ(Java 編)」

関西オープンフォーラム 2011, 2011 年 11 月 11 日

(5) 山田 秀和 (情報流通対策グループ 情報システムセキュリティアナリスト) :
「Stuxnet で明らかにされた制御システムセキュリティの神話と現実」
計測制御学会ネット部門大会, 2011 年 11 月 15 日

(6) 古田洋久 (情報流通対策グループ マネージャ) :
「制御システムセキュリティの新たなる脅威について」
ものづくり NEXT↑2011, 2011 年 11 月 16 日

(7) 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) :
「最近の脅威事例と取り組み」
JPRS ユーザ会, 2011 年 11 月 21 日

(8) 椎木孝斉(分析センター センター次長) :
「スマートフォンとセキュリティ脅威」
Internet Week2011, 2011 年 12 月 1 日

(9) 小宮山功一朗(国際部マネージャ) :「Role of a CSIRT and Activities of JPCERT/CC」
The 2nd APT Cybersecurity Forum, 2011 年 12 月 5 日

(10) 梅村香織(APCERT Secretariat) :
「APCERT Activities」
The 2nd APT Cybersecurity Forum, 2011 年 12 月 6 日

9. 執筆一覧

(1) 熊谷 裕志 (情報流通対策グループ 情報システムセキュリティアナリスト) :
「Android アプリ開発者なら押さえておきたい Java セキュアコーディングの意味と効果」
翔泳社 Codezine「Java セキュアコーディング入門」, 2011 年 11 月 24 日

(2) 熊谷 裕志 (情報流通対策グループ 情報システムセキュリティアナリスト) :
「ContentProvider のアクセス範囲―Dropbox における脆弱性の修正」
翔泳社 Codezine「Java セキュアコーディング入門」, 2011 年 11 月 29 日

(3) 久保 正樹(情報流通対策グループ 脆弱性アナリスト) :
「整数オーバーフロー検出の 3 つのアプローチ―mezzofanti のバグ修正」
翔泳社 Codezine「Java セキュアコーディング入門」, 2011 年 12 月 16 日

10. 開催セミナー等一覧

(1) 企業向けC/C++ セキュアコーディングセミナー
※本セミナーの詳細は、「2-4-4」をご参照ください。

11. 後援一覧

(1) 2011 日韓情報セキュリティシンポジウム
(主催：日本ネットワークセキュリティ協会(JNSA))
2011 年 11 月 10 日
(2) Internet Week 2011
(主催：日本ネットワークインフォメーションセンター(JPNIC))
2011 年 11 月 30 日～12 月 2 日
(3) 第 8 回デジタル・フォレンジック・コミュニティ 2011 in TOKYO
(主催：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 2011 実行委員会)
2011 年 12 月 12 日～13 日

■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