Japan Computer
Emergency Response
Team Coordination Center

JPCERT-PR-2013-01
発行日：2013-04-15

JPCERT/CC 活動概要 [2013 年 1 月 1 日 ～ 2013 年 3 月 31 日]

活動概要トピックス

―トピック 1― 制御システムセキュリティインシデント報告の Web フォームによる受付を開始

―トピック 2― APCERT 合同サイバー演習への参加及び APCERT 功労感謝記念賞の受賞

―トピック 3―「分析センターだより」の公開を開始

―トピック 1―
制御システムセキュリティインシデント報告の Web フォームによる受付を開始

JPCERT/CC では、国内の情報セキュリティインシデントの被害低減を目的として、広く一般からコンピュータセキュリティインシデントに関する対応依頼を受け付けてきましたが、昨今の制御システムに対する脅威の高まりに鑑み、制御システムに関するセキュリティインシデント報告用のフォームを準備し、2013 年 1 月から受付を開始しました。今後、制御システムにおけるインシデント対応に関するサービスの強化を図っていく予定です。詳細については、次の URL をご参照下さい。

制御システムインシデントの報告
https://www.jpcert.or.jp/ics/ics-form.html
制御システムインシデントの報告 (Web フォーム)
https://form.jpcert.or.jp/ics.html

―トピック 2―
22 経済地域 26 チームによる APCERT 合同サイバー演習の実施及び APCERT 功労感謝記念賞の受賞

アジア太平洋地域の CSIRT コミュニティである APCERT（Asia Pacific Computer Emergency Response Team）は、1 月 29 日、サイバー攻撃への即時対応能力を確認するため、合同サイバー演習を実施しました。8 回目となる今回の合同サイバー演習のテーマは「大規模な DoS 攻撃への対処」でした。APCERT の加盟チームのみならず、イスラム諸国会議機構に加盟する CSIRT の集まりである OIC-CERT よりエジプト、オマーン、チュニジア、パキスタンのチームも加わって、22 の経済地域から計 26 チームが参加しました。JPCERT/CC は、この演習にプレーヤー(演習者)として参画するとともに、ExCon と呼ばれるシナリオ作成などを行う演習の進行調整役も務め、スムーズな演習の実施を支えました。

また、本年は、APCERT 設立から 10 周年という節目の年であったことから、3 月にオーストラリアのブリスベンで開催された APCERT の 年次総会では、 “APCERT & Cyber Security: Then, Now and Beyond”というテーマのもと、過去 10 年間の活動を振り返りつつ、メンバ制度の見直しや情報共有のあり方を議論しました。JPCERT/CC は、APCERT に対する 10 年間に亘っての貢献が認められ、本年次

総会において APCERT 功労感謝記念賞を受賞しました。

APCERT
http://www.apcert.org/

ートピック 3ー

「分析センターだより」の公開を開始

JPCERT/CC では、「分析センター」という部門がアーティファクトの収集や分析を担っています。これまでは、分析センターの活動で得られた情報は、対策等の目的でその情報を必要とする組織や同様に分析を行っている技術者に対してのみ提供し、「公開」という形での情報発信を控えてきましたが、既に情報が公開されている事例に関する考察や問題認識など、公開可能な話題もあり、多くの方々に知っていただきたいテーマがあるとの思いから、「分析センターだより」の公開を始めました。
分析センターだよりの第 1 号では DLL 検索パスの問題を取り上げています。DLL 検索パスの問題自体は脆弱性の種類としては古典的ですが、近年でも新たな脆弱性が報告されており、その中には実際の攻撃において悪用されているものもあります。
分析センターだよりでは、このような良く知られた問題であっても、技術的な特徴や悪用の実態について言及することで、研究者や分析技術者が研究や分析を行うきっかけとなるような情報を提供することを目指しています。

分析センターだより
https://www.jpcert.or.jp/magazine/acreport.html

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」および「8. フィッシング対策協議会会費による活動」に記載の活動については、この限りではありません。また、「2.5.セキュアコーディング啓発活動」、「6.国際連携活動関連」、「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 5453 件、インシデント件数ベースでは 5692 件でした(注 1)。

(注 1)「報告件数」は、報告者から寄せられた Web フォーム、メール、FAX による報告の総数を示します。また、「インシデント件数」は、各報告に含まれるインシデントの件数の合計を示し、1 つのインシデントに関して複数の報告が寄せられた場合にも 1 件のインシデントとして扱います。

JPCERT/CC が国内外のインシデントに関連するサイトとの調整を行った件数は 2230 件でした。前四半期の 1497 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/2013/IR_Report20130415.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 474 件で、前四半期の 360 件から 32%増加しました。また、前年度同期（324 件）との比較では、46%の増加となりました。
本四半期のフィッシングサイトの報告件数を、装っていたブランドが国内か国外かで分けた内訳を添えて[表 1-1]に示します。

[表 1-1 フィッシングサイトの国内・国外ブランド別の件数]

フィッシングサイト	1 月	2 月	3 月	合計 (割合)
国内ブランド	42	40	30	112(24%)
国外ブランド	84	103	98	285(60%)
ブランド不明(注 2)	23	31	23	77(16%)
月別合計	149	174	151	474(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、国内金融機関を装ったフィッシングサイトと、国内通信事業者の Web メールサービスを装ったフィッシングサイトの報告を多数受領しています。これらのフィッシングサイトは、海外の特定の無料ホスティングサービスを使って構築される傾向があることを確認しています。国内金融機関を装ったフィッシングサイトでは、見た目はインターネットバンキングのログイン画面を装っていながら、クレジットカードの情報を入力させることを目的としたものが多くありました。

フィッシングサイトの調整先の割合は、国内が 36%、国外が 64%と、前四半期の割合（国内 44%、国外 56%）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、1184 件でした。前四半期の 737 件から 61%増加しています。

本四半期は、不審な iframe タグがページの末尾に挿入される改ざんを受けた Web サイトの報告を非常に多く受領しました。iframe によって誘導される先のサイトにアクセスすると、複数のアプリケーションの脆弱性を使用した攻撃が行われることを確認しています。そのため、古いバージョンのアプリケーションがインストールされている PC でサイトを閲覧すると、PC がマルウエアに感染する可能性があります。

2013 年 3 月半ばには、特定のブラウザのユーザエージェントを使用して Web サイトにアクセスしたときにだけ、iframe が埋め込まれた Web ページが返され、不審な別のサイトに誘導されるという改ざんに関する報告が寄せられました。この iframe は、攻撃によってサーバに不正に設置された apache モジュールが、html ファイルや JavaScript ファイルをブラウザに渡す際に動的に埋め込んでいるものであることが分かりました。この iframe は直接ファイルに埋め込まれるものではないため、Web サーバ上のファイルを調査しても改ざんのコードを確認することはできません。原因を特定するためには、apache の設定ファイルが改ざんされていたり、インストールしていない apache モジュールが存在したりしていないかを確認する必要があります。

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し、分析しています。これらの様々な脅威情報を多角的に分析し、必要に応じて脆弱性やウイルス検体の検証なども併せて行い、分析結果に応じて、国内の企業、組織のシステム管理者を対象とした「注意喚起」（一般公開）や、国内の重要インフラ事業者等を対象とした「早期警戒情報」（提供先限定）などを発信することにより、国内におけるサイバーインシデントの発生・拡大の抑止を目指しています。

1.2.1. 情報提供

JPCERT/CC の Web ページ(https://www.jpcert.or.jp)や RSS、約 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：17 件　https://www.jpcert.or.jp/at/

2013-01-09　Adobe Flash Player の脆弱性 (APSB13-01) に関する注意喚起
2013-01-09　Adobe Reader 及び Acrobat の脆弱性 (APSB13-02) に関する注意喚起
2013-01-09　2013 年 1 月 Microsoft セキュリティ情報 (緊急 2 件含) に関する注意喚起
2013-01-15　Microsoft Internet Explorer の脆弱性 (MS13-008) に関する注意喚起
2013-01-15　Oracle Java SE のクリティカルパッチアップデートに関する注意喚起
2013-01-31　Portable SDK for UPnP の脆弱性に関する注意喚起
2013-02-04　2013 年 2 月 Oracle Java SE のクリティカルパッチアップデートに関する注意喚起
2013-02-08　Adobe Flash Player の脆弱性 (APSB13-04) に関する注意喚起
2013-02-13　Adobe Flash Player の脆弱性 (APSB13-05) に関する注意喚起
2013-02-13　2013 年 2 月 Microsoft セキュリティ情報 (緊急 5 件含) に関する注意喚起
2013-02-20　2013 年 2 月 Oracle Java SE のクリティカルパッチアップデート (定例) に関する注意喚起
2013-02-21　Adobe Reader 及び Acrobat の脆弱性 (APSB13-07) に関する注意喚起
2013-02-27　Adobe Flash Player の脆弱性 (APSB13-08) に関する注意喚起

2013-03-05　2013 年 3 月 Oracle Java SE のクリティカルパッチアップデートに関する注意喚起
2013-03-13　Adobe Flash Player の脆弱性 (APSB13-09) に関する注意喚起
2013-03-13　2013 年 3 月 Microsoft セキュリティ情報 (緊急 4 件含) に関する注意喚起
2013-03-27　ISC BIND 9 サービス運用妨害の脆弱性 (CVE-2013-2266) 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：12 件　https://www.jpcert.or.jp/wr/

Weekly Report で扱った情報セキュリティ関連情報の項目数は、合計 49 件、「今週のひとくちメモ」のコーナーで紹介した情報は、次の 12 件でした。

2013-01-09　D.ROOT-SERVERS.NET の IP アドレス更新その後
2013-01-17　Java 7 のコントロールパネル
2013-01-23　Java 6 のサポート終了
2013-01-30　CVE ID Syntax Change - Call for Public Feedback
2013-02-06　情報セキュリティ月間
2013-02-14　スマートフォン情報セキュリティサイト「I Love スマホ生活」
2013-02-20　BIND 10 RC 版リリース
2013-02-27　Java 6 のサポート終了
2013-03-06　Microsoft Windows XP と Office 2003 の延長サポート終了について
2013-03-13　新人研修に役立つ JPCERT/CC のコンテンツ
2013-03-21　IPA が「2013 年版 10 大脅威」を公開
2013-03-27　DNS キャッシュサーバの設定に注意

1.2.1.3. 早期警戒情報

JPCERT/CC では、国民の社会活動に大きな影響を与えるインフラ、サービス及びプロダクトなどを提供している組織の情報セキュリティ関連部署もしくは組織内 CSIRT に向けて、それらの組織やサービス提供先に深刻なセキュリティ上の問題を惹起する可能性のある脅威情報やその分析結果、対策方法に関する情報等を「早期警戒情報」として提供しています。

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

1.2.2. 情報収集・分析・提供（早期警戒活動）事例

本四半期における情報収集・分析・提供（早期警戒活動）の事例を紹介します。

(1)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、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。 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 等と連携して、特に注意深く情報収集を行っています。
本四半期では、3 月 1 日が特異日に当たりました。2013 年 2 月下旬に、韓国のサイトで「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たことを受け、JPCERT/CC では、KrCERT/CC(KISA)との非常連絡態勢を整えてモニタリング情報を共有するなど、サイバー攻撃発生に備えた対応態勢をとりました。併せて、攻撃関連情報（正確な攻撃日時、攻撃手法やツール、攻撃への参加状況など）の収集・分析態勢を強化しました。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短時間確認されたものの、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。

(2) Portable SDK for UPnP の脆弱性に関する調査

2013 年 1 月、Portable SDK for UPnP の脆弱性に関する情報が公開されました。公開されたホワイトペーパーに、攻撃に直結する情報が含まれていたことに加え、Portable SDK for UPnP がブロードバンドルータなど多くの市販の製品に使用されていることから、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。
公開されたホワイトペーパーによると、Portable SDK for UPnP に含まれるライブラリ libupnp には、バッファオーバーフローの脆弱性があり、Portable SDK for UPnP を用いて UPnP 機能を実装しているルータなどにおいて、第三者によって細工された SSDP パケットを処理する際に、任意のコードが実行される可能性があります。
この脆弱性について、実際のブロードバンドルータを使用して検証を行った結果、細工された SSDP パケットをブロードバンドルータに送信することにより、ブロードバンドルータの UPnP 機能を停止できる事を確認しました。
注意喚起では、各製品ベンダから対策済みソフトウエアが公開されている場合は対策済みソフトウエアに更新する、または UPnP 機能を一時的に無効とするよう呼びかけました。

1.3. インターネット定点観測システム

インターネット定点観測システムは、ポートスキャンの受信情報をインターネット上に設置した複数のセンサーから収集します。JPCERT/CC では、ポートスキャンがネットワーク経由の攻撃の準備活動としてなされることを踏まえて、既に公開されている脆弱性情報や攻撃ツール、攻撃コードを悪用した攻撃活動の動向と、新たな脆弱性情報の公開をきっかけとした攻撃活動の活発化等の状況を把握することを目的にインターネット定点観測システムを運用しています。観測情報の一部は、ネットワーク管理者

や研究者向けの参考情報として、 JPCERT/CC Web ページなどでも公開しています。

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

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

JPCERT/CC では、TSUBAME プロジェクトで収集したデータを宛先ポート番号や送信元地域ごとに分類して統計分析し、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。

前四半期に引き続き、日本国内の企業などの 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が設置されていないか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が観測されなくなり、ツールの除去等の対処が行われ、その後の被害拡大が抑止されたと考えられます。
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。

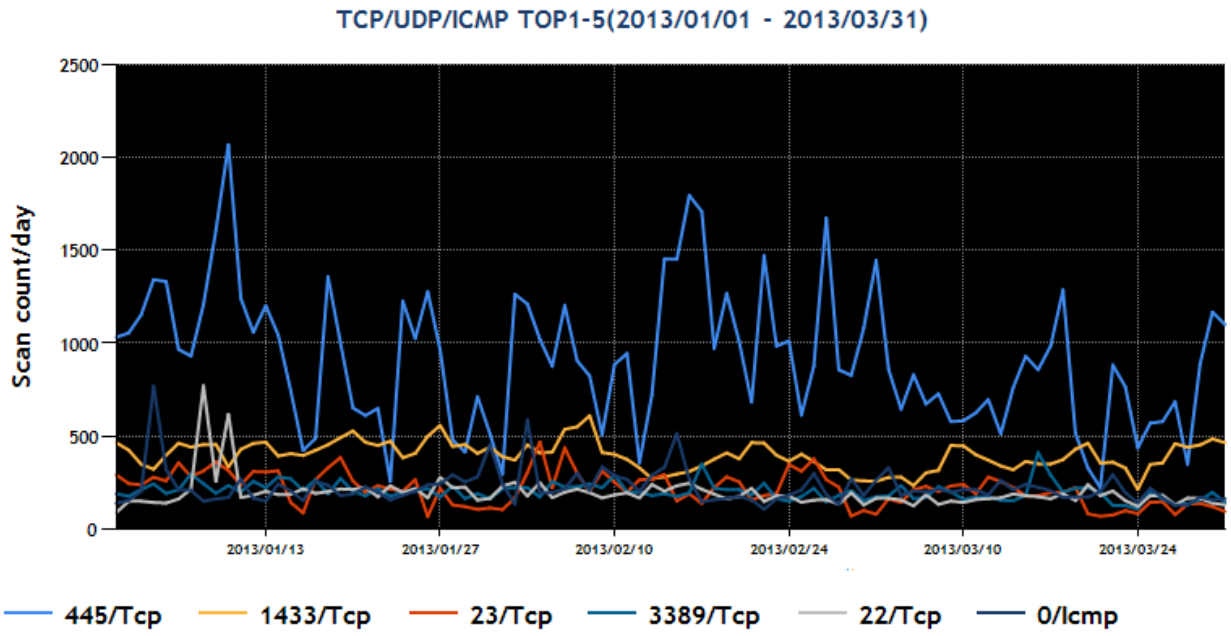
1.3.2. ポートスキャン概況

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
https://www.jpcert.or.jp/tsubame/

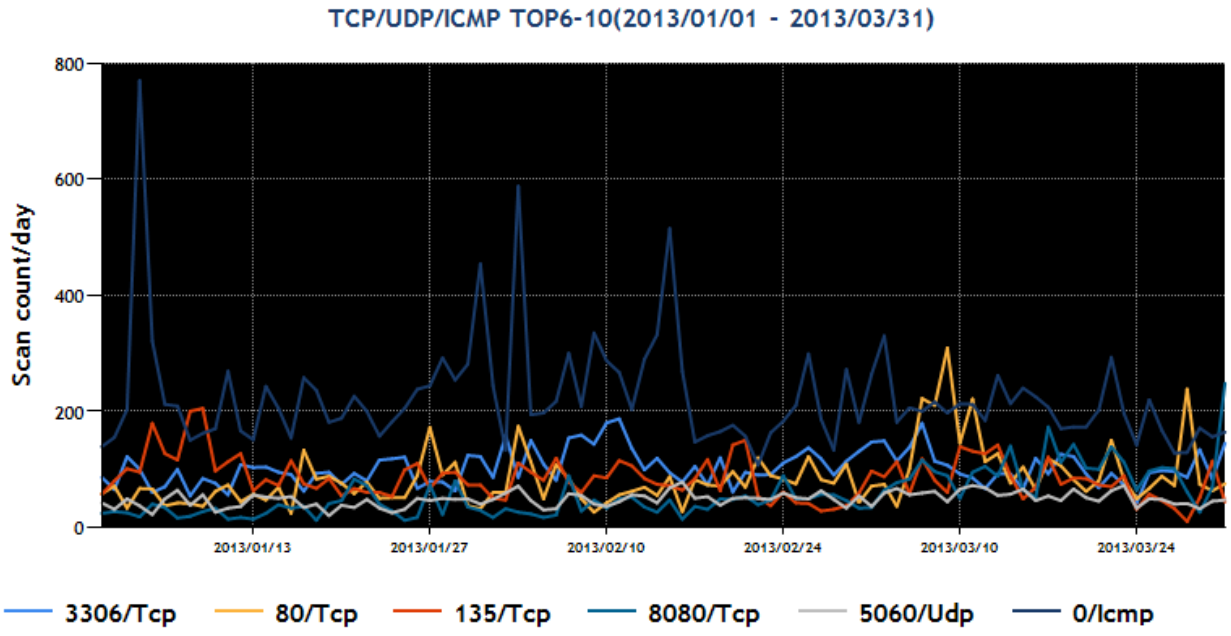
本四半期に定点観測システムで観測された宛先ポート別の上位 1 位～5 位及び 6 位～10 位のそれぞれについて、パケット数の時間的推移を[図 1-1]と[図 1-2]に示します。

- 宛先ポート別グラフ top1-5 (2013 年 1 月 1 日-3 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 (2013 年 1 月 1 日-3 月 31 日)

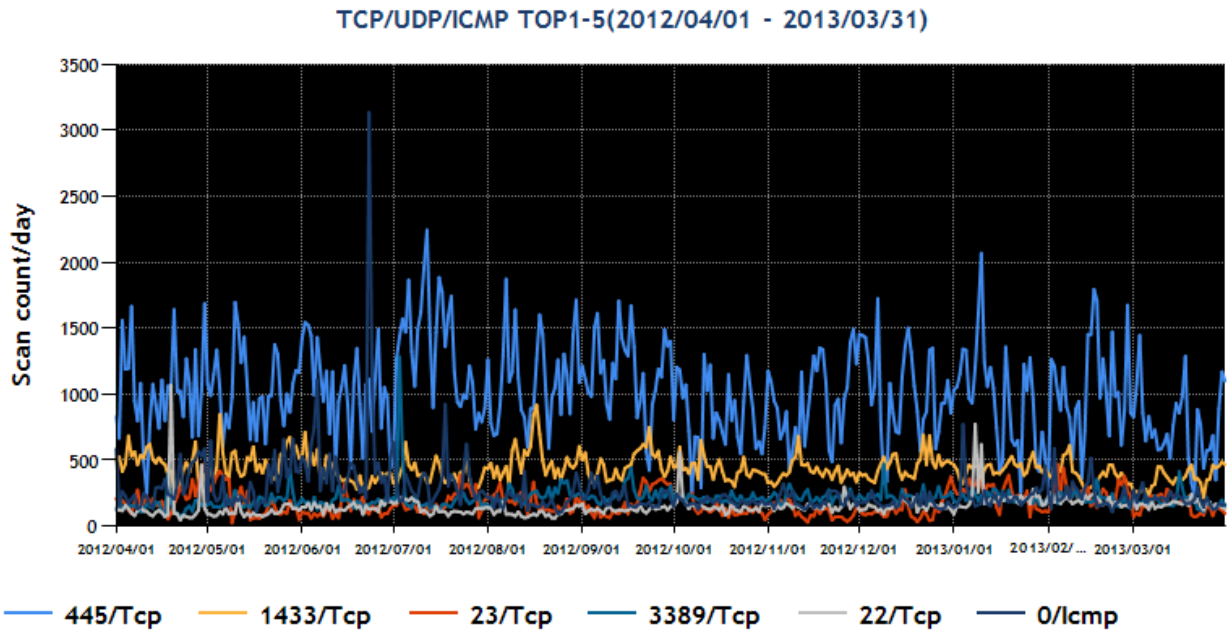


[図 1-2 宛先ポート別グラフ top[6-10]

また、より長期間のパケット数の推移を見るため、2012 年 4 月 1 日から 2013 年 3 月 31 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

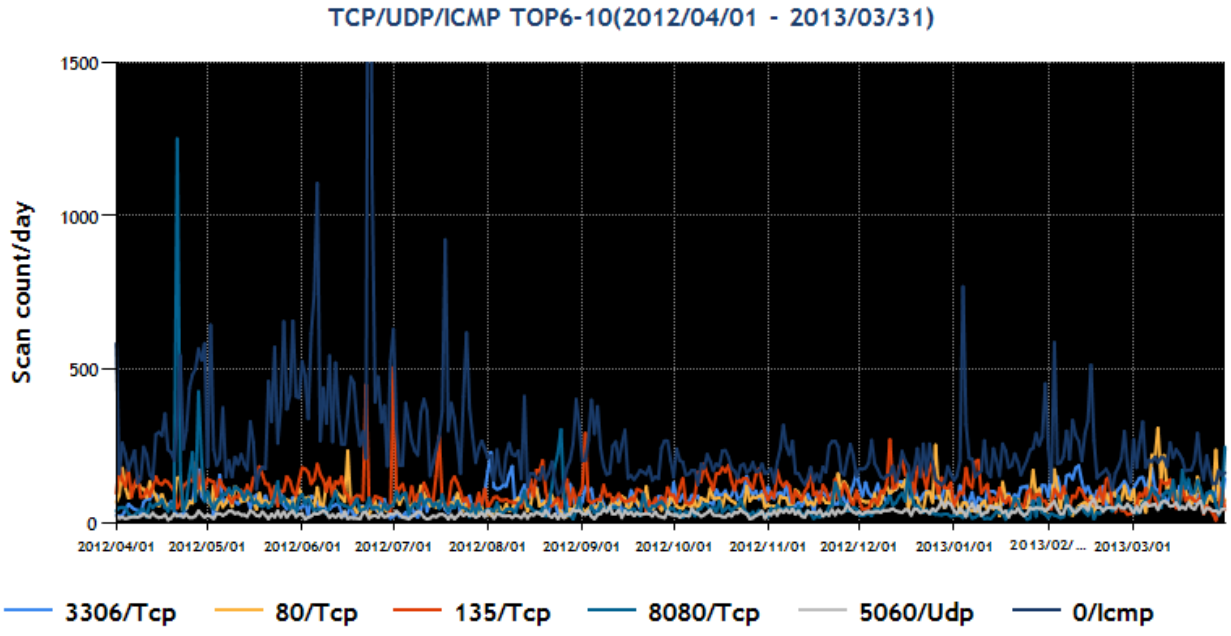
推移を[図 1-3]と[図 1-4]に示します。

- 宛先ポート別グラフ top1-5 (2012 年 4 月 1 日-2013 年 3 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 4 月 1 日-2013 年 3 月 31 日)



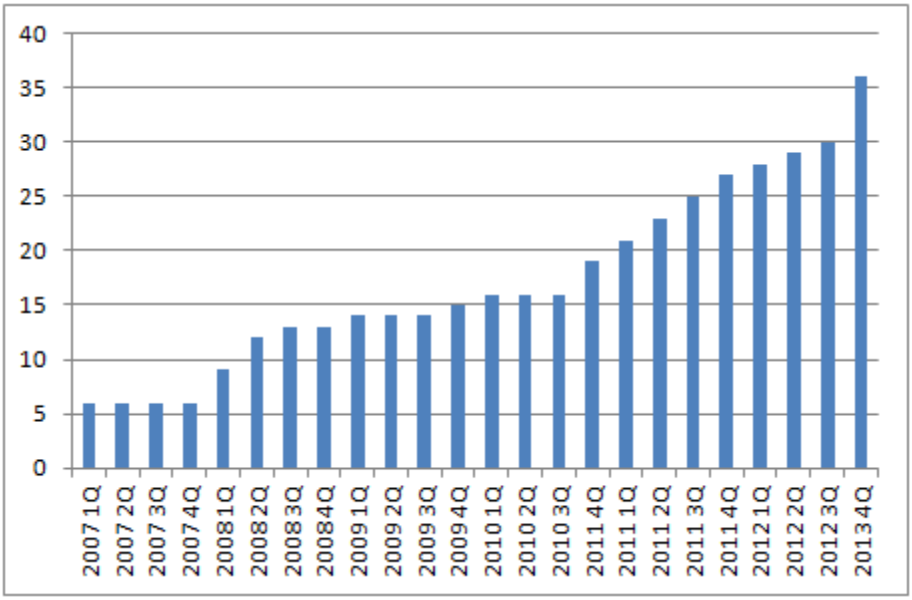
[図 1-4 宛先ポート別グラフ top[6-10]

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や会員情報の管理、加盟のためのガイダンスの実施および手続の運用、Web サイト、メーリングリストの管理等の活動を行っています。

本四半期においては、KDDI 株式会社(KDDI-CSIRT)とベライゾンジャパン合同会社(VZJ-CSIRT)、NHN Japan 株式会社(NHNJP-CSIRT)、大成建設株式会社(T-SIRT)、トレンドマイクロ株式会社(TM-SIRT)、NTT データ先端株式会社(Intelli-CSIRT)の 6 組織が新規に加盟しました。本四半期末時点で 36 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]

2 月に「KEK (高エネルギー加速器研究機構) 加速器見学会・第 11 回ワーキンググループ会」を開催し、各ワーキンググループ及び会員チームからの活動報告が行われました。
第 11 回ワーキンググループ会の詳細については、次の URL をご参照ください。

日本シーサート協議会第 11 回ワーキンググループ会を開催
http://www.kek.jp/ja/NewsRoom/Release/20130304160000/

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。

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。

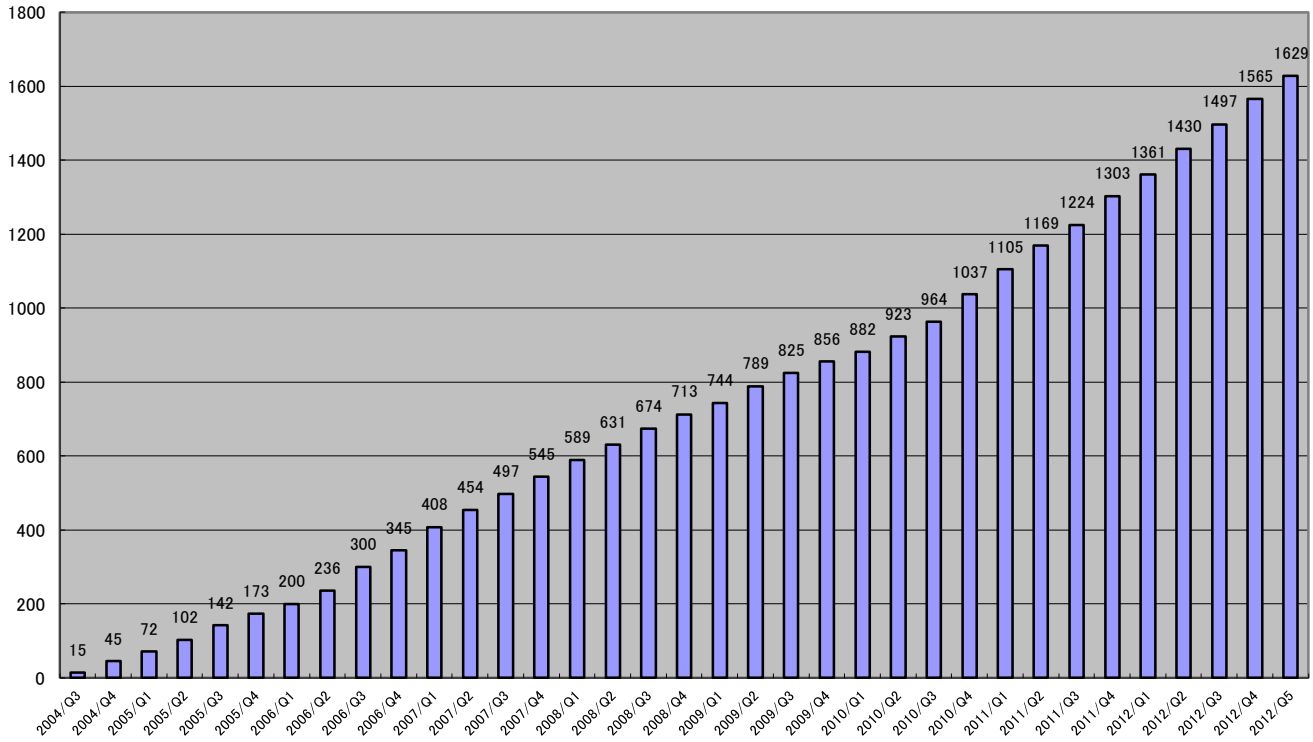
2.1. Japan Vulnerability Notes (JVN) において公表した脆弱性情報および対応状況

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。）に基づいて製品開発者とのコーディネーションを行う「調整機関」に指定されており、本基準を踏まえてとりまとめられた「情報セキュリティ早期警戒パートナーシップガイドライン」に規定された調整機関の役割を担い、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 64 件（累計 1629 件)で、累計の推移は[図 2-1]に示すとおりです。

本四半期に公表された個々の脆弱性情報に関しては、次の URL をご参照ください。

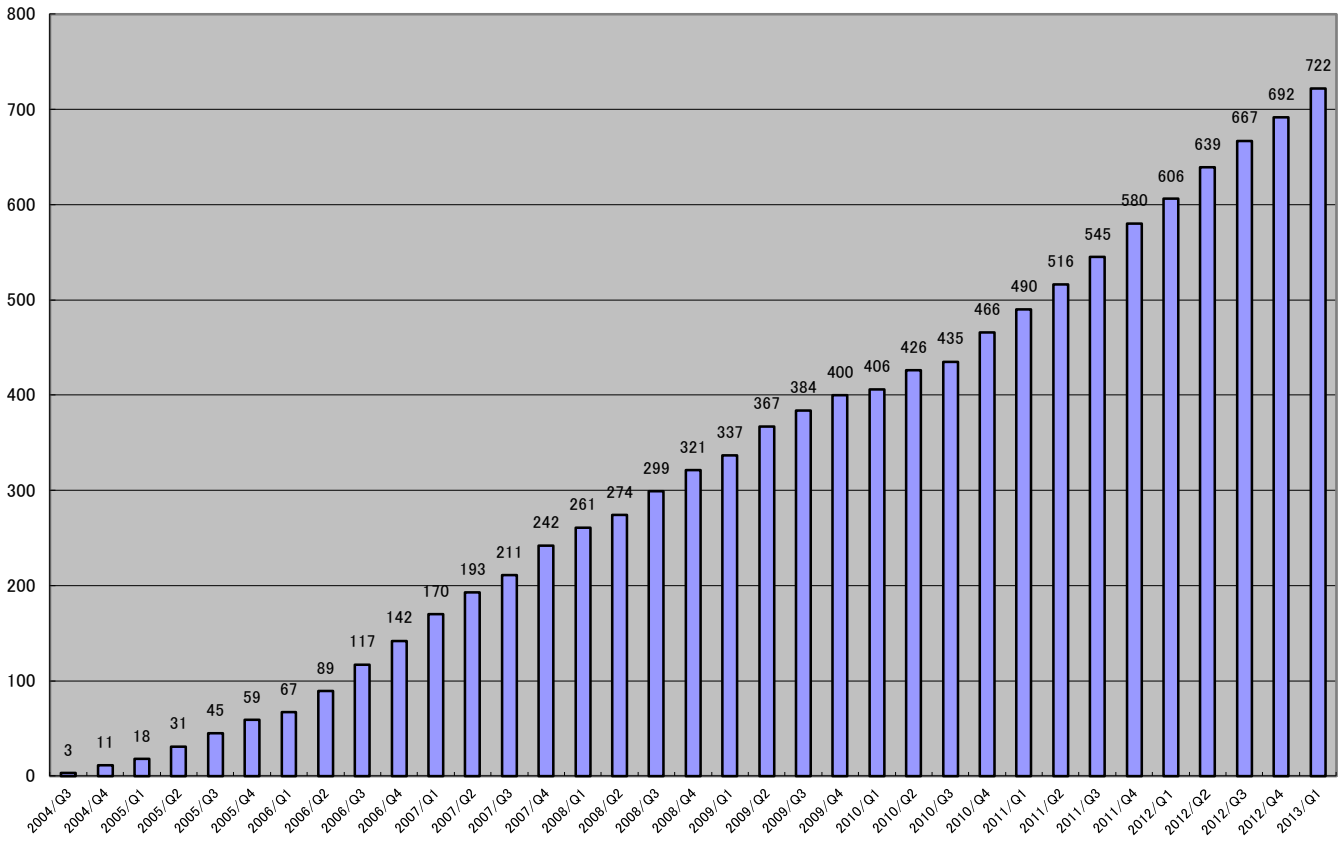
JVN(Japan Vulnerability Notes)
https://jvn.jp/



[図 2-1　JVN 公表累積件数]

本四半期において公表に至った脆弱性情報のうち、国内取扱脆弱性情報は 30 件(累計 722 件)で、累計の推移は[図 2-2]に示すとおりです。30 件うちの 11 件（約 37%）が海外製品開発者の製品です。本枠組みは日本の国内制度として創設されたものですが、このように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います。
昨年度から、Android およびその関連製品やモバイル端末関連製品の届出が増加傾向にあります。本四半期には、Android 向けアプリケーションに関する脆弱性情報を 7 件、iOS 向けアプリケーションに関する脆弱性情報を 2 件公表し、モバイル関連製品に関する脆弱性情報の公表が全体の約 30%を占めました。

また、サーバ関連製品における脆弱性情報を 4 件、プリンターやルータ等の組込み製品に関する脆弱性情報を 8 件、組込みシステム向けリアルタイム OS 製品の脆弱性情報を 6 件公表しており、サーバー関連製品や組込みシステム等で使用されている製品の脆弱性情報が 18 件と約 6 割を占めました。このようなタイプの製品では、製品開発者の対応において、対策の準備よりも対策の提供方法の検討に苦慮するケースが多く見られますが、当該製品の各製品開発者におかれては、本基準に従い、長期間に亘る調整にご協力いただき、最終的には対策と合わせて JVN にて情報公表を行うことができました。JPCERT/CC は、今後も引き続き国内外の関係者との調整を行い、脆弱性問題への速やかな対応促進に努めてまいります。



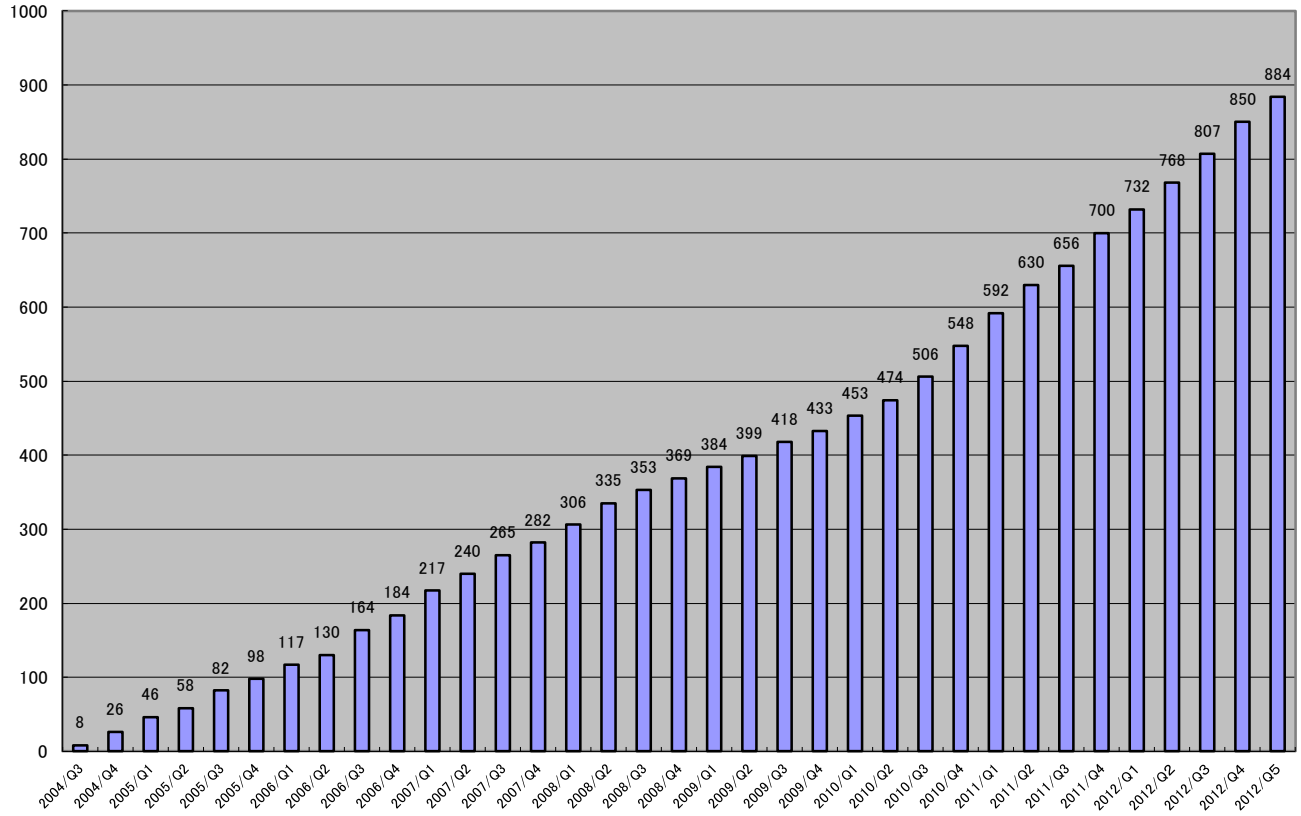
[図 2-2 公表を行った国内取扱脆弱性情報の累積件数]

本四半期に公表した国際取扱脆弱性情報は、34 件(累計 884 件)で、累計の推移は[図 2-3]に示すとおりです。34 件のうち 9 件を占める US-CERT の脆弱性注意喚起（JVNTA から始まる識別子を付して公表したもの）の内訳は、Oracle Java 製品におけるゼロデイ脆弱性情報に関する注意喚起が 3 件、Microsoft 製品に関する月例パッチの注意喚起が 3 件、Microsoft 製品におけるゼロデイ脆弱性情報に関する注意喚起が 1 件、Adobe 製品に関するアップデート公開の注意喚起が 1 件、Oracle の 4 半期パッチ Critical Patch Update（CPU）が 1 件でした。本四半期においては、ゼロデイ脆弱性情報の注意喚起が 5 件と多く、該当製品開発者の対応が急がれる状況にありました。
脆弱性注意喚起以外の 25 件の国際取扱脆弱性情報の中では、Apple、Adobe、DELL、HP(Hewlett Packard)、Novell といった著名な海外製品開発者の製品に関するものが目立ちました。

なお、本四半期においては、複数製品開発者に影響を及ぼす可能性がある”UPnP（Universal Plug and Play）”の脆弱性が米国 CERT/CC から国際展開され、JPCERT/CC は日本およびアジア圏への情報展開の依頼を受けました。JPCERT/CC から韓国 KrCERT/CC、中国 CNCERT/CC、台湾 TWNCERT への国際展開を行い、各国の製品開発者における該当製品の有無等の調査を依頼しました。UPnP は多くの組込系機器において使用されているプロトコルで、影響を受ける製品は多岐に亘ります。調整・対応等のため相当の猶予期間を置き、発見者からの情報公開に合わせて、米国 CERT/CC Vulnerability Notes、JVN、および該当製品をもつ製品開発者のサイトにおいて、対策を含む脆弱性情報を同時に公表しました。これまでに取り扱った複数製品開発者に影響を及ぼす案件の中では、本件は関連する製品開発者が比較的多く国際的な調整

を必要としました。本脆弱性の発見者の論文の謝辞欄には、米国 CERT/CC および JPCERT/CC が国際調整に尽力したことが記載されました。

“Security Flaws in Universal Plug and Play　January 2013 HD Moore"
https://community.rapid7.com/servlet/JiveServlet/download/2150-1-16596/SecurityFlawsUPnP.pdf



[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

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、報告され、対策がとられて情報公表される脆弱性が多数を占めている一方で、報告されたものの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脆弱性、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、「情報システム等の脆弱性情報の取扱いに関する研究会」では、2010 年 6 月から法務専門家や有識者で構成された調整手続き検討ワーキンググループを設置して検討を重ね、2011 年 3 月に「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」および「JPCERT/CC 脆弱性関連情報取扱いガイドライン」を改訂し公開しました。

JPCERT/CC では、これらの新たなガイドラインに従った取扱いを、2011 年度より開始し、同年 9 月 29 日には、JVN 上に「連絡不能開発者一覧」が新たに設けられ、連絡不能となっている製品開発者名の掲載が始まりました。この一覧については、これまでに 124 件(製品開発者数としては 82 件)が掲載され、

16 件（製品開発者の数としては 11 件）の調整が再開できたことから、「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。

本四半期は、新たに 4 名の製品開発者名(案件数としては 5 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の公表から約 1 年 6 カ月が経過した本四半期末日時点で、合計 108 件の連絡不能開発者案件が引続き掲載されており、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、来年度の開始を視野に、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、脆弱性情報の円滑な国際的流通のため、米国の CERT/CC、英国の CPNI、フィンランドの CERT-FI などの脆弱性情報ハンドリングを行っている海外の調整機関と協力関係を結び、それぞれが報告を受けた脆弱性情報の共有、各国の製品開発者への情報通知および対応状況の集約、脆弱性情報の公表時期の設定などの調整活動を連携して行っています。昨年度より届出が増加傾向にある Android 関連の脆弱性の調整では、Android 関連製品を開発している製品開発者が存在するアジア圏、特に韓国 KrCERT/CC や中国 CNCERT/CC、台湾 TWNCERT との連携が活発に行われるようになり、JPCERT/CC もより幅広い国際連携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 日に運用を開始した JVN 英語版サイト(https://jvn.jp/en)では、日本語版公表とほとんど時間差なく、ほぼ同時に脆弱性情報を公表しています。国内取扱脆弱性情報の英語版として、第一次情報源となることも多く、海外のセキュリティ関連組織などからも注目されています。

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）に認定されており、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、29 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 が付与されています。
CNA および CVE に関する詳細は、次の URL ご参照ください。

News & Events “JPCERT/CC Becomes CVE Numbering Authority”
https://cve.mitre.org/news/archives/2010_news.html#jun232010a
CVE Numbering Authorities
https://cve.mitre.org/cve/cna.html

About CVE

https://cve.mitre.org/about/index.html

2.4. 日本国内の脆弱性情報流通体制の整備

JPCERT/CC では、本基準に従って、日本国内の脆弱性情報流通体制を整備しています。
詳細については、次の URL をご参照ください。

脆弱性情報取扱体制
http://www.meti.go.jp/policy/netsecurity/vulhandlingG.html
脆弱性情報コーディネーション概要
https://www.jpcert.or.jp/vh/
「情報セキュリティ早期警戒パートナーシップ」の運用を開始
https://www.jpcert.or.jp/press/2004/0708.txt
情報セキュリティ早期警戒パートナーシップガイドライン(2010 年版)
https://www.jpcert.or.jp/vh/partnership_guide2010.pdf
JPCERT/CC 脆弱性情報取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。

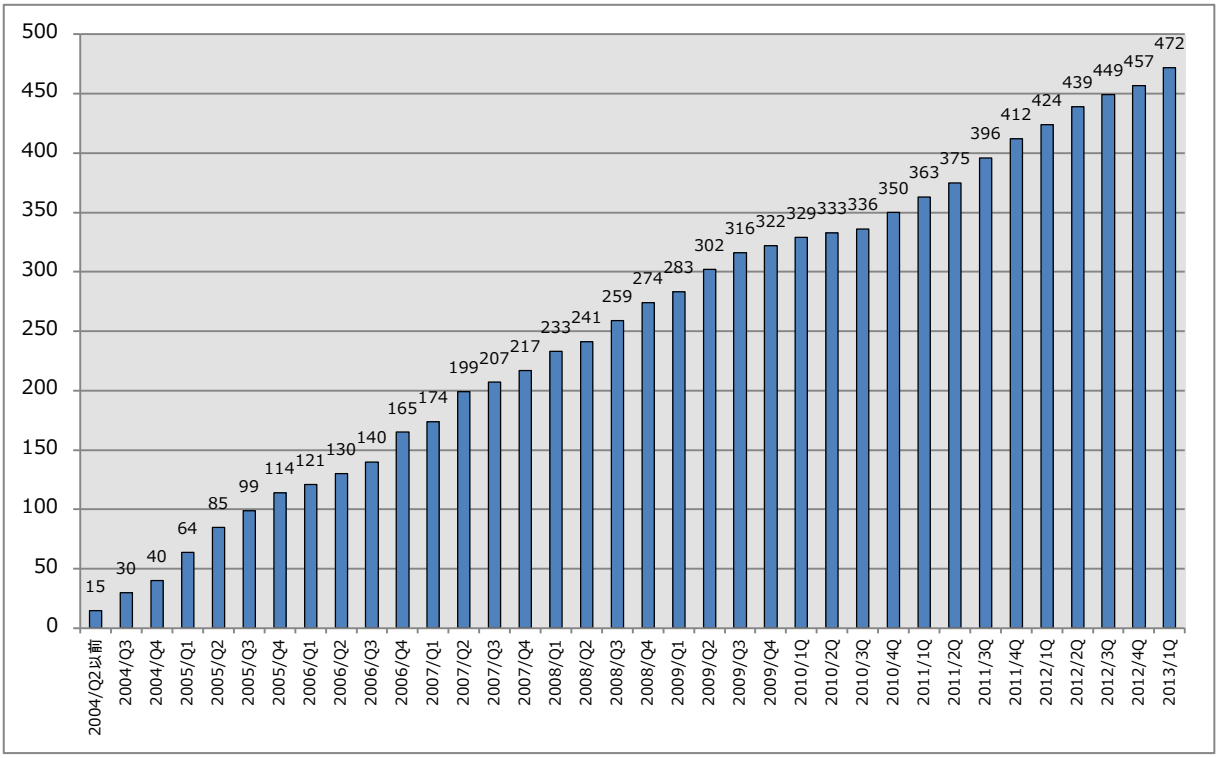
独立行政法人情報処理推進機構(IPA) 脆弱性対策
http://www.ipa.go.jp/security/vuln/

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、2013 年 3 月 31 日現在で 472 社となっています。

登録等の詳細については、次の URL をご参照ください。

JPCERT コーディネーションセンター製品開発者リスト登録規約
https://www.jpcert.or.jp/vh/agreement.pdf



[図 2-4 累計製品開発者登録数]

2.5. セキュアコーディング啓発活動

2.5.1. 制御用システムベンダ向け「C/C++セキュアコーディング概論」セミナーを開催

2 月 25 日、日本電機工業会（JEMA）と共同で、プロセス管理・制御システム開発者を対象とした「C/C++セキュアコーディング概論」セミナーを開催しました。
制御システムの分野においては近年、セキュリティ上の脅威が高まりつつある中、ソフトウエアの脆弱性に関する問題が顕在化してきています。JPCERT/CC では 2006 年から、脆弱性を作り込まないためのセキュアコーディング技術に関する研究や啓発活動を行っており、本セミナーはその一環として行われました。セミナーは午後半日の座学形式で行われ、開発現場で製品開発やコーディング規約の策定などに携わる約 40 名のエンジニアの方々にご参加いただきました。
JPCERT/CC は JEMA と協力して今後も制御システムのセキュリティに関する啓発・向上に努めて参ります。

2.5.2. Developers Summit 2013 にて「Android セキュアコーディグ」の講演

通称「デブサミ」の名で親しまれている、ソフトウエア開発者/エンジニアの祭典とも言われるカンファレンス「Developers Summit 2013」において、Android アプリの脆弱性とセキュアコーディングに関する

講演を行いました。講演は、日本スマートフォンセキュリティ協会（JSSEC）の技術部会において Android セキュアコーディングガイド作成リーダーを勤める松並勝氏と、JPCERT/CC 脆弱性解析チームリーダーの久保正樹が共同で行い、Android アプリの脆弱性の実態とその対策方法について、JSSEC が公開している『Android アプリのセキュア設計・セキュアコーディングガイド』の内容を交えつつ紹介しました。

【デブサミ 2013】14-C-1 レポート
知らずに危険なコードをリリースしてしまわないために―Android セキュアコーディングセミナー
http://codezine.jp/article/detail/7010

2.5.3. セキュアコーディング関連記事を連載中

情報流通対策グループ脆弱性解析チームのメンバーは各種ウェブマガジンにおいてセキュアコーディング関連の連載を担当しています。本四半期は、次の 2 つの記事を執筆しました。

Codezine 連載『Java セキュアコーディング入門』
第 8 回「Android アプリの配布パッケージ apk の解析について」（公開：2 月 19 日、執筆：熊谷裕志）
http://codezine.jp/article/detail/6992

アットマーク・アイティ連載『もいちど知りたい、セキュアコーディングの基本』
第 3 回「C でポピュラーな脆弱性とバッファオーバーフロー（後編）」(公開： 2 月 19 日、執筆：戸田洋三)
http://www.atmarkit.co.jp/ait/articles/1212/26/news006.html

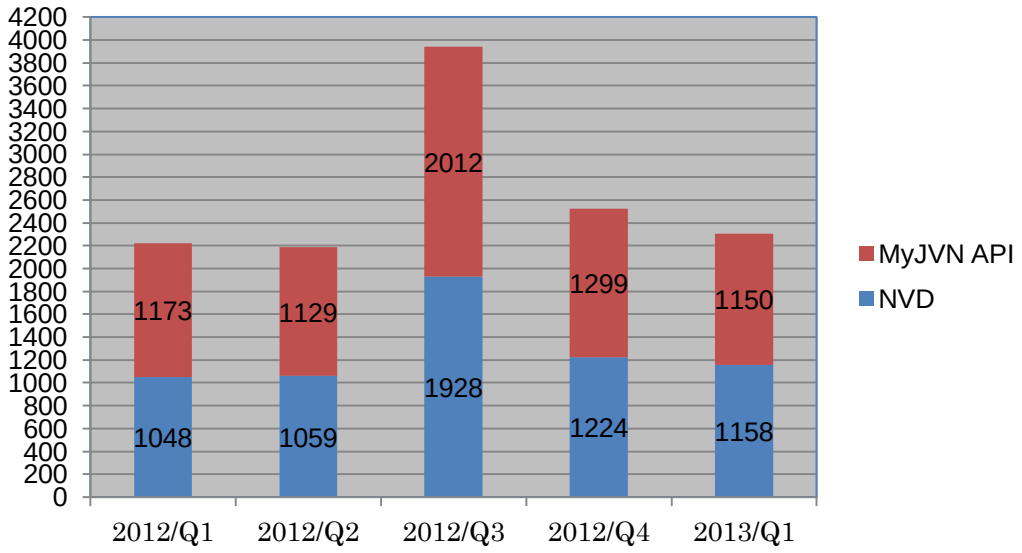
2.5.4. セキュアコーディング 出張セミナー

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

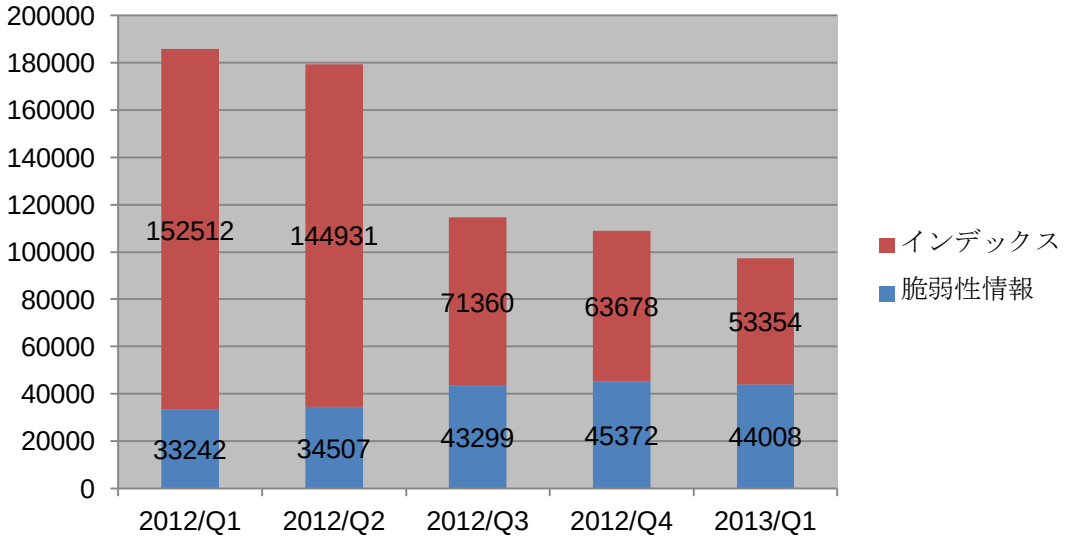
2.6. VRDA フィードによる脆弱性情報の配信

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

四半期ごとに配信した VRDA フィード配信件数のデータソース別の内訳を [図 2-5] に、VRDA フィードの利用傾向を [図 2-6] と [図 2-7] に示します。 [図 2-6] では、VRDA フィードインデックス（Atom フィード）と、脆弱性情報（脆弱性の詳細情報）の利用数を示します。VRDA フィードインデックスは、個別の脆弱性情報のタイトルと脆弱性の影響を受ける製品の識別子（CPE）を含みます。[図 2-7] では、HTML と XML の二つのデータ形式で提供している脆弱性情報について、データ形式別の利用割合を示しています。

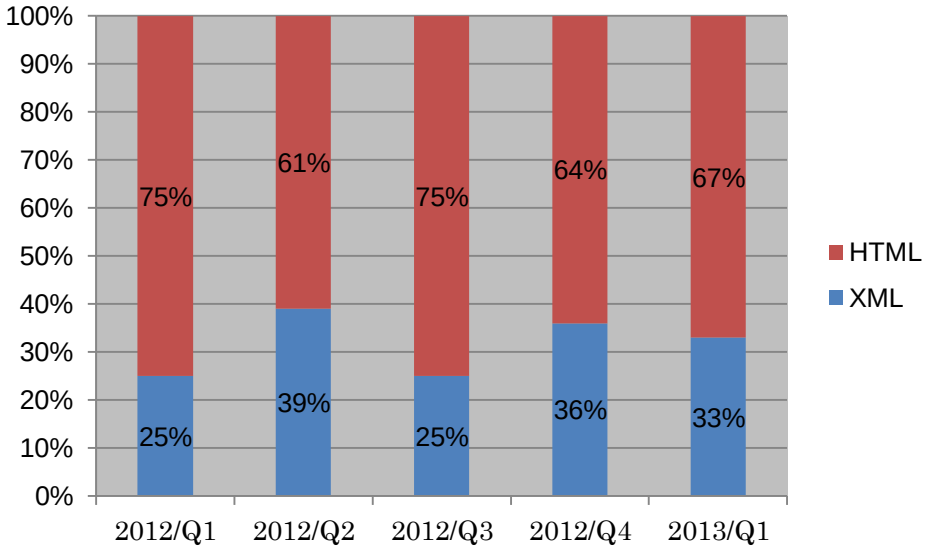


[図 2-5 VRDA フィード配信件数]



[図 2-6 VRDA フィード利用件数]

[図 2-6] に示したように、前四半期と比較して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が、VRDA フィードインデックスの利用数は減少しました。



[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大きな変化は見られませんでした。

3. アーティファクト分析

JPCERT/CC では、インシデントに関連して報告いただいた情報や収集した情報を確認し、実態を把握するアーティファクト分析という活動を行っています。分析対象はウイルスやボット等のマルウエアに限らず、攻撃に使われるツールを始めとするプログラムや攻撃手法等（アーティファクト）にまで及び、それらを技術的な観点から調査・解析します。アーティファクト分析を行うことで、より効果的なインシデント対応や、より精度の高い情報発信を目指すとともに、そのために必要な分析環境と分析能力の高度化に努めています。

3.1. 「分析センターだより」の公開開始

JPCERT/CC では、「分析センター」という部門がアーティファクトの収集や分析を担っています。分析センターは、取り扱っているもの（アーティファクト等）の性質上、活動の中で得られた情報を、対策等の目的でその情報を必要とする組織や同様に分析を行っている技術者に対してのみ提供し、「公開」という形での情報発信を控えてきました。

しかしながら、既に情報が公開されている事例に関する、分析センターの分析技術者の考察や問題認識など、公開可能な話題もあり、多くの方々に知っていただきたいテーマがあるとの思いから、「分析センターだより」の公開を始めました。

分析センターだよりの第 1 号では DLL 検索パスの問題を取り上げています。DLL 検索パスの問題自体は脆弱性の種類としては古典的ですが、近年でも新たな脆弱性が報告されており、その中には実際の攻撃

において悪用されているものもあります。
分析センターだよりでは、このような良く知られた問題であっても、技術的な特徴や悪用の実態について言及することで、研究者や分析技術者が研究や分析を行うきっかけとなるような情報を提供することを目指しています。また、公開という形をとることにより、分析を専門とされない方々に対して、JPCERT/CC に報告された情報がどのように扱われているかを知っていただく機会になればと考えています。

4. 制御システムセキュリティ強化に向けた活動

4.1. 制御システムセキュリティインシデント Web フォームによる受付を開始

JPCERT/CC では、国内の情報セキュリティインシデントの被害低減を目的として、広く一般からコンピュータセキュリティインシデントに関する対応依頼を受け付けてきましたが、昨今の制御システムに対する脅威の高まりに鑑み、制御システムに関するセキュリティインシデント報告用のフォームを準備し、2013 年 1 月から受付を開始しました。今後、制御システムにおけるインシデント対応に関するサービスの強化を図っていく予定です。詳細については、次の URL をご参照下さい。

制御システムインシデントの報告
https://www.jpcert.or.jp/ics/ics-form.html
制御システムインシデントの報告 (Web フォーム)
https://form.jpcert.or.jp/ics.html

4.2. 制御システムのインシデントおよび脆弱性に関する調整

本四半期は、制御システムセキュリティに関連するインシデント対応として、インターネットからアクセス可能な状態にある制御システムに関する調整活動を実施しました。また、制御システム製品に関連する脆弱性の取扱いに関しては、現在、制度の検討中ではありますが、弊センターへ連絡があった情報について関係組織との調整活動を実施しました。

4.3. 制御システムセキュリティカンファレンス 2013 開催

制御システムセキュリティカンファレンス 2013 を 1 月 23 日（木）に東京（品川）で開催しました。今回で 5 回目となる本カンファレンスでは、関係者の方々に制御システムの脆弱性とインシデントに対する取組みについて講演いただき、今後のセキュリティ改善活動に繋がるような情報交換に役立つプログラム構成としました。ほぼ満席の 264 名の方にご来場いただきました。プログラム等の詳細については、次の URL をご参照ください。

制御システムセキュリティカンファレンス 2013
https://www.jpcert.or.jp/ics/conference2013.html

制御システムセキュリティカンファレンス　2013　においての講演資料
https://www.jpcert.or.jp/present/#year2013

4.4.　制御システムセキュリティ自己評価ツール J-CLICS の公開

3 月 7 日、制御システムの構築・運用・保守に関わる制御システム関係者を対象に、制御システムのセキュリティ対策状況を確認できる自己評価ツール「J-CLICS」の提供を開始しました。同時に、J-CLICS を利用する際の手引きとなる各設問の意味や現場担当者が取り組むべき具体策等を説明した解説書「J-CLICS 設問ガイド」も提供しています。
制御システムセキュリティ自己評価ツール「J-CLICS (Check List for Industrial Control Systems of Japan)」は、JPCERT/CC が英国 CPNI から導入して配布してきた自己評価ツール「SSAT」をベースに、制御システム業界の方々のご協力を得て、日本のセキュリティ実態や商慣行に合わせて質問項目を絞り込むとともに解説書を添えたもので、セキュリティの初心者でも、各設問に回答していけば物理的セキュリティや機器接続手順、対応能力等について、セキュリティ上の問題点を抽出・把握することができます。詳細については、次の URL をご参照下さい。

制御システムセキュリティ自己評価ツール(J-CLICS)
https://www.jpcert.or.jp/ics/jclics.html

4.5.　制御システムセキュリティ情報共有ポータルサイトの開設

3 月 8 日、制御システムにおけるセキュリティ上の脅威の把握、対策のための情報入手、また、制御システムセキュリティに携わる方々のコミュニティ拡大をテーマに、制御システム関係者向けの情報共有ポータルサイト「ConPaS(Control System Security Partner's Site)」を開設しました。制御システムユーザ、制御製品ベンダ、制御システムベンダを中心に、国内外の制御システムセキュリティ動向、ICS-CERT Advisory & Alert(邦訳)、セキュリティ関連ツールや各種ガイドラインなどの情報を公開するほか、コメント欄において、利用者間における意見の交換が可能です。詳細については、次の URL をご参照下さい。

制御システムセキュリティ情報共有ポータルサイトについて
https://www.jpcert.or.jp/ics/conpas/index.html

4.6.　制御システム関係者向けインシデント対応トレーニング実施

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、2 月 19 日、20 日に大阪で、3 月 12 日から 15 日に東京で、それぞれ実施しました。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を使用し、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の発見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。今年度は、のべ 56 名の方にご参加いただきました。

4.7. 情報発信活動

制御システムに関するセキュリティインシデント事例や規格・標準の動向、技術動向などの情報を収集し、制御システム関係者向けのニュースレターとして配信しています。ニュースレターでは、イベント情報やJPCERT/CC からのお知らせも提供しています。昨年度までは隔月で配信していましたが、本年度より月刊で配信し、本四半期は、号外も含め計 6 回（1 月 29 日、1 月 31 日、2 月 12 日、2 月 28 日、3 月 7 日、3 月 29 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 290 名の方にご登録いただいています。今後も内容の充実を図っていく予定です。詳細については、次の URL をご参照下さい。

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

4.8. 関連団体との連携

定期的に開催されている SICE (計測自動制御学会)、JEITA（電子情報技術産業協会）、JEMIMA (日本電気計測器工業会)による合同セキュリティ検討 WG（ワーキンググループ）に参加し、制御システムのセキュリティに関して専門家の方々と意見交換を行いました。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内容の確認やユーザからの意見の反映を行い、一般公開に向けた最終調整活動を行いました。

4.9. 制御システム向けツールの配布情報

JPCERT/CC では、制御システムの構築と運用に関するセキュリティ上の問題項目を手軽に抽出し、バランスの良いセキュリティ対策を行っていただくことを目的として、簡便なセキュリティ自己評価ツール日本版 SSAT や J-CLICS の配布を行なっています。本四半期は、JPCERT/CC に対して、SSAT に関しては 9 件、J-CLICS に関しては 81 件の利用申込みがありました。直接配布件数の累計は、SSAT が 138 件、J-CLICS が 81 件となりました。

4.10. 制御システム業界における脆弱性ハンドリング活動開始準備

制御システムの脆弱性ハンドリングにおいて、調整機関としての活動を本格的に開始するために準備を進めています。前四半期から継続して、主な制御システムベンダや関連業界の代表者に参加いただき、国内での脆弱性情報の取扱いのあり方を議論いただきました。本四半期は制御システム向け脆弱性研究会の第 3 回会合、ワーキンググループの第 4 回、第 5 回をそれぞれ開催しました。

4.11. 講演活動

1 月 29 日に大阪で行われたシステム情報シミュレーション部会プラントオペレーション分科会（化学工

学会主催）において「セキュリティインシデントの動向と求められる製造現場での対応」、2 月 15 日に神奈川県産業技術交流協会マネジメントシステム研究会で「産業用システムのセキュリティ・リスクー動向と課題」、2 月 19 日には情報セキュリティ大学院大学のワークショップで「制御システムのセキュリティ」と題する講演をそれぞれ行いました。

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、9 月下旬に配布された国際標準草案(DIS： Draft of International Standard)に対して 12 月 25 日を締切日として行われた投票の結果が 1 月に公表されました。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等の理由で、これまでの策定作業に積極的に関与してきた日本と米国、英国の 3 ヶ国は反対しましたが、他の投票権をもつ国々が賛成したため承認され、最終国際標準案(FDIS： Final Draft of International Standard)の段階に進むことになりました。通常は、DIS 投票以降の文書の更新は ISO の事務局が行うことになっていますが、文書としてのあまりの未成熟さに匙を投げだして、作業グループで実施するよう要請したため、次の SC27 国際会議の場でも編集検討作業が行われることになりました。

「脆弱性取扱手順」については、11 月に配付された国際標準草案(DIS： Draft of International Standard)に対する投票が 2013 年 4 月 14 日を締切日として行われています。こちらに対しては、文書品質にも問題がなく技術的も妥当な内容であると判断し、数件の編集上のコメントを付けたかたちで賛成投票を行う方向で国内委員会に提案しました。

両標準の策定状況については、脆弱性担当窓口の方々にお集まりいただき 3 月 8 日に開催された POC ミーティングでも紹介しました。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

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 ）

いずれのパートも現在 2nd WD の段階にあり、各パートの草案に対し日本は下記のとおりコメントを作成し、提出しました。

- 27035-1：コメント 10 件（technical 9 件、editorial 1 件）
- 27035-2：コメント 6 件（general 3 件、technical 1 件、editorial 2 件）
- 27035-3：コメント 25 件（general 4 件、technical 19 件、editorial 2 件）

日本を含む参加国から提出されたコメントは、4 月 22 日～26 日にフランスのソフィア・アンティポリスで開催される次回の国際会合において議論されることになります。JPCERT/CC は日本の代表としてこの国際会合に出席し、本標準化の作業に参加します。
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。本四半期は、メールでの問合せへの対応及び次年度に向けた計画立案が中心でした。

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. 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. APCERT Steering Committee 電話会議の実施

1月16日および2月27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運営方針等について議論を行いました。

6.2.1.2. 第2回 APCERT Study Call の実施(2013年1月25日)

APCERT加盟チームの技術力を高めることを目的に、インターネットを介しての勉強会(「APCERT Study Call」)が実施されましたが、この実施にあたり、JPCERT/CCはAPCERT事務局として企画段階から関与し、設備を提供する等の支援を行いました。今回で2回目となった本勉強会では、ベトナムの民間CSIRTであるBKISが講師となって「Manual malware detection and cleaning」について解説しました。APCERTチームにおけるマルウエア解析手法の理解や解析能力の向上の一助となりました。

6.2.1.3. APCERT 合同サイバー演習 (APCERT Drill 2013) に参加 (2013年1月29日)

APCERTは、サイバー攻撃への即時対応能力を確認するため、合同サイバー演習を実施しました。本演習は、アジア太平洋地域で国境を越えて発生し、広範囲に影響を及ぼすインシデントへの対応における各経済地域 CSIRT 間の連携の強化を目的として、毎年実施されています。
8回目となる今回の合同サイバー演習のテーマは「大規模なDoS攻撃への対処」でした。APCERTの加盟チームのみならず、イスラム諸国会議機構に加盟するCSIRTの集まりであるOIC-CERTよりエジプト、オマーン、チュニジア、パキスタンのチームも加わって、22の経済地域から計26チームが参加しました。JPCERT/CCは、この演習にプレーヤー(演習者)として参画するとともに、ExConと呼ばれる演習の進行調整役も務め、スムーズな演習の実施を支えました。

6.2.1.4. APCERT 年次総会 2013 への参加(2013年3月24日-27日)

アジア太平洋地域の CSIRT コミュニティである APCERT の年次総会がオーストラリアのブリスベンで開催され、JPCERT/CCを含め19の加盟チームが参加しました(2013年3月末現在、20の経済地域から 30チームがAPCERTに加盟しています。)。会合の概要は、以下のとおりです。

1) 日程：
- 3/24(日) 終日：APCERT 運営委員会 (SC Meeting) / APCERT ワーキンググループ会合
- 3/25(月) 終日：各種ワークショップ
- 3/26(火) 午前：APCERT 年次総会 (Annual General Conference)
  午後：APCERT カンファレンス (Closed Session)
- 3/27(水) 終日：APCERT カンファレンス (Open Session)

2) 場所：Novotel Brisbane

3) 概要

APCERT 年次総会は、各経済地域における最近のインターネットセキュリティ動向、インシデント対応の事例、調査・研究活動などを共有することを目的に、毎年開催されています。

本年は、APCERT 設立から 10 年目という節目の年であったことから、“APCERT & Cyber Security: Then, Now and Beyond”というテーマのもと、過去 10 年間の活動を振り返り、また、昨年度の年次総会で採択された “APCERT to help create a safe, clean and reliable cyber space in the Asia Pacific region through global collaboration”というビジョンを具現化すべく、メンバ制度の見直しや情報共有のあり方を議論しました。

[APCERT 年次総会集合写真]

運営委員会(Steering Committee)のメンバの一部とともに、APCERT 議長チーム/副議長/事務局チームの改選が行われ、JPCERT/CC は議長チーム（3 期目、任期は 2014 年 3 月まで）及び事務局チーム（任期 2015 年 3 月まで）に再選されました。JPCERT/CC は、引き続き APCERT の代表として様々な活動をリードすることとなりました。

なお、JPCERT/CC は、APCERT に対する 10 年間に亘っての貢献が認められ、本年次総会において、表彰を受けました。

[APCERT より表彰を受ける JPCERT/CC]

[APCERT 功労感謝記念賞]

6.2.2. TSUBAME ネットワークモニタリングワークショップの開催(2013 年 3 月 25 日)

APCERT 年次総会の会期中、JPCERT/CC は、アジア太平洋地域の CSIRT から参加した 33 名を対象として、「TSUBAME ネットワークモニタリングプロジェクト」のワークショップを開催しました。本プロジェクトは、APCERT のワーキンググループ活動の一つとして位置づけられており、アジア太平洋地域における連携した定点観測のために、各地域のインターネット上にセンサーを配置し、ワームの感染活動や弱点探索を目的としたスキャンなどのセキュリティ上の脅威となるトラフィックの観測を行っています。JPCERT/CC は、このプロジェクトの提案組織として、運営を主導しています。
ワークショップでは、TSUBAME プロジェクトメンバを対象に、今年度 JPCERT/CC が観測した主な事象に関する報告や、TSUBAME により蓄積したデータから脅威を発見するハンズオン演習を行いました。また、マカオ、インドネシアのチームよりゲストスピーカを迎え、それぞれのチームの TSUBAME 活用方法の紹介を行いました。さらに、プロジェクトメンバ間で意見交換を行い、モニタリング結果の共有を一層強化することを確認しました。

6.2.3. 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、1 月 27 日-31 日にポルトガルのリスボンで開催された SC 会合に出席しました。FIRST 及び Steering Committee の詳細については、次の URL をご参照ください。

FIRST
http://www.first.org/

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

6.2.3.1. 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、AfricaCERT のスポンサーとなり、2013 年 2 月、同組織代表者の Liaison Member としての加盟が FIRST より承認されました。

6.2.4. ベトナム情報通信省の来訪（2013 年 1 月 21 日）

ベトナム情報通信省 VNCERT 次長 Nguyen Thanh Hai 氏を代表としたベトナム関係省庁の来訪団計 9 名が情報セキュリティ政策等に関する意見交換を行うことを目的に来日し、関係各所を訪問した一環として、1 月 21 日に JPCERT/CC の事務所に来訪しました。本ミーティングでは、日越それぞれの国で発生しているインシデントの動向やそれらに対する対応方法を始め、VNCERT および JPCERT/CC における最近の活動状況、JPCERT/CC が主導する TSUBAME ネットワークモニタリングプロジェクトの概要や観測

データ、観測事例等に関し、情報共有と意見交換を行いました。

6.2.5. 台湾行政院の来訪（2013 年 1 月 25 日）

台湾行政院の国土安全室 林俊甫氏、同情報セキュリティ室 王弘儒氏、国立中山大（TWCERT/CC）范俊逸氏が 1 月 25 日に JPCERT/CC の事務所に来訪し、担当者と日台それぞれの制御システムセキュリティへの対応や現状等に関する情報交換を行いました。

6.2.6. 覚書(MOU)締結

協調関係にあることを明文化して確認し、また、CSIRT 間での機微な情報の共有に際しての取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-RO (ルーマニア)
- MECIRT (モンテネグロ)

6.3. その他の活動

6.3.1. 中国語圏における情報収集発信

JPCERT/CC は、中国語圏（中国／台湾）経済区域の情報セキュリティ関係会議やセキュリティチームの活動に参加し、セキュリティ関連情報の収集や現地セキュリティ専門家との情報交換を積極的に行っています。本四半期は、1 月 29 日に中国上海で開催された「中国情報セキュリティ連絡会」会合に参加し、中国地域におけるセキュリティ傾向全般について講演を行いました。本連絡会は、中国進出の日系企業の情報セキュリティ対策と競争力向上の支援を目的として開催されているものです。

6.3.2. 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。

CVE is about to undergo a change in syntax for CVE identifiers (2013/2/13)
http://blog.jpcert.or.jp/2013/02/cve-is-about-to-undergo-a-change-in-syntax-for-cve-identifiers.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 9 件発信しました。

本四半期は、昨年から継続して発生しているインターネットサービスプロバイダなどが提供している Web メールサービスをかたるフィッシングと、金融機関をかたり第二認証情報を詐取するフィッシングに加えて、クレジットカード会社をかたるフィッシングの報告を多数受けました。協議会では、名前をかたられた事業者に、フィッシングメールやサイトの関連情報を提供しました。また、広く注意を喚起するために、Web メールサービスをかたるフィッシングに関しては「eoWEB メールをかたるフィッシング(2013/2/15)」や[図 7-1]の「ODN をかたるフィッシング（2013/02/20)」を、第二認証情報を詐取するフィッシングに関しては「三菱東京 UFJ 銀行をかたるフィッシング(2013/1/8)」を、クレジットカード会社をかたるフィッシングに関しては「MasterCard をかたるフィッシング(2013/2/14)」を、それぞれ緊急情報として、協議会の Web 上で公開しました。
さらに、これらフィッシングに使用されたサイトを停止するための調整を行い、すべてについて停止を確認しました。

[図 7-1 ODN をかたるフィッシングサイト
https://www.antiphishing.jp/news/alert/odn20130220.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協議会員の事業者と、フィッシングに関する研究を行っている協議会員の学術機関に対し、協議会に報告されたフィッシングサイトの URL を集めたリストを、日に数回提供しています。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、ないし研究の支援が目的です。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 18 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、ガイドライン策定ワーキンググループ（WG）及び国際連携ワーキンググループ（WG）を開催いたしました。
ガイドライン策定 WG では、主に一般消費者向けの啓発資料として、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 では、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 3 回会合）
日時：2013 年 1 月 22 日 15:00 - 17:00
場所：株式会社三菱総合研究所

(2) ガイドライン策定 WG（第 4 回会合）
日時：2013 年 3 月 4 日 13:30 - 15:30
場所：株式会社三菱総合研究所

(3) 国際連携 WG（第 2 回会合）
日時：2013 年 3 月 1 日 10:00 - 12:00
場所：株式会社三菱総合研究所

7.5. 情報共有会の開催

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 2 回会合）
日時：2013 年 3 月 7 日 15:30 - 17:30

場所：JPCERT コーディネーションセンター

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 2013 年 1 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201301.html
フィッシング対策協議会 2013 年 2 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201302.html
フィッシング対策協議会 2013 年 3 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201303.html

8. フィッシング対策協議会会費による活動

8.1. 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 3 回運営委員会
日時：2013 年 1 月 17 日 16:00 - 18:00
場所：JPCERT コーディネーションセンター

(2)フィッシング対策協議会 第 4 回運営委員会
日時：2013 年 3 月 8 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 が本四半期に公開した調査・研究の報告書や論文、セミナー資料は次のとおりです。

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 10 月～12 月　(2013 年 3 月 6 日)
https://www.jpcert.or.jp/tsubame/report/report201210-12.html

9.2. 制御システムセキュリティカンファレンス 2013 講演資料

2013 年 1 月 24 日に、品川コクヨホール(東京都港区)において開催した「制御システムセキュリティカンファレンス 2013」の講演資料を公開しました。

制御システムセキュリティカンファレンス 2013 講演資料
https://www.jpcert.or.jp/present/

本カンファレンスについての詳細は、「4.3」をご参照ください。

10. 講演活動一覧

(1) 宮地 利雄(理事)：
「セキュリティ・インシデントの動向と求められる製造現場での対応」
化学工業会プラントオペレーション分科会，2013 年 1 月 28 日

(2) 宮地 利雄(理事)：
「産業におけるリスク・セキュリティの事例」
神奈川県産業技術交流協会第 10 回マネジメントシステム研究会 ,2013 年 2 月 15 日

(3) 宮地利雄(理事)：
「制御システム・セキュリティ ～事後対策を中心とする動向と課題～」
情報セキュリティ大学院大学水平ワークショップ「制御システム・セキュリティ」，2013 年 2 月 19 日

(4) 早貸 淳子(専務理事)：
「サイバー攻撃の動向とインシデント対応の状況」
情報セキュリティ月間 キックオフ・シンポジウム, 2013 年 02 月 01 日

(5) 久保正樹(情報流通対策グループ 脆弱性解析チームリーダー)：
「Android セキュアコーディング」
Developers Summit 2013,2013 年 2 月 14 日

(6) 久保正樹・戸田洋三(情報流通対策グループ 脆弱性解析チーム)：
「C/C++セキュアコーディング概論」
日本電機工業会(JEMA),2013 年 2 月 25 日

(7) 真鍋 敬士(理事,分析センター長)：
「攻撃事例に学ぶ情報共有のススメ」

セプターカウンシルセミナー,2013 年 02 月 13 日

(8) 早貸 淳子(専務理事)：
「サイバー攻撃の多様化とセキュリティ対策のこれから」
@IT セキュリティソリューション Live ! in Tokyo, 2013 年 02 月 21 日

(9) 真鍋 敬士(理事,分析センター長)：
パネル「サイバー攻撃の高度な解析と情報共有のあり方について」
IPA 重要インフラ情報セキュリティシンポジウム 2013,2013 年 02 月 22 日

11. 執筆一覧

(1) 熊谷裕志(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(8)
「Android アプリの配布パッケージ apk の解析について」
翔泳社 CodeZine,2013 年 2 月 19 日

(2) 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(3)
「C でポピュラーな脆弱性とバッファオーバーフロー(後編)」
アイティメディア @IT,2013 年 2 月 19 日

12. 開催セミナー等一覧

(1) 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。

(3) 制御システムセキュリカンファレンス 2013
※本セミナーの詳細は、「4.3」をご参照ください。

13. 協力、後援一覧

(1) LOVE PC2013
主　催：情報セキュリティ対策推進コミュニティ運営事務局
開催日：2013 年 02 月 01 日(金)～28 日(木)

(2) IPA 重要インフラ情報セキュリティシンポジウム 2013
主　催：独立行政法人 情報処理推進機構
開催日：2013 年 02 月 22 日(金)

■インシデントの対応依頼、情報のご提供
info@jpcert.or.jp
https://www.jpcert.or.jp/form/
PGP Fingerprint ： FC89 53BB DC65 BD97 4BDA D1BD 317D 97A4 69EC E048
■制御システムに関するインシデントの対応依頼、情報のご提供
icsr-ir@jpcert.or.jp
https://www.jpcert.or.jp/ics/ics-form.html
PGP Fingerprint ： B3C2 A91C AE92 50A9 BBB2 24FF B313 E0E1 0DDE 98C1
■脆弱性情報ハンドリングに関するお問い合わせ ：vultures@jpcert.or.jp
■制御システムセキュリティに関するお問い合わせ ：icsr@jpcert.or.jp
■セキュアコーディングセミナーのお問い合わせ ：seminar-secure@jpcert.or.jp
■公開資料、講演依頼、資料使用、その他のお問い合わせ：office@jpcert.or.jp