JPCERT CC®

JPCERT-PR-2012-01

発行日 : 2012-04-12

JPCERT/CC 活動概要 [2012 年 1 月 1 日 ～ 2012 年 3 月 31 日]

【活動概要トピックス】

—トピック 1—
定点観測データから組込み機器のボット感染を発見

JPCERT/CCでは、インターネット定点観測システムによって、2011年12月からポート23/TCPへのスキャンが増加したことを検知しました。その後の観測および詳細調査の結果、このスキャンは、ボットに感染したと思われる、主に韓国国内に設置された組込みLinuxを搭載した非PC機器（ブロードバンドルータなど）から行われていたものであったことがわかりました。スキャンの主な発信元が韓国であったため、KrCERT/CCに連絡・情報提供を行い、スキャンの発信源である機器の特定や、ボットの感染が確認された組込み機器ベンダへの連絡、マルウエア検体の回収および解析につなげることができました。

また、このスキャンは近隣探索によってIPアドレスの近い範囲に対して行われており、マルウエア感染は韓国以外の日本やその周辺国にも及んでいたため、同様なスキャンパケットを発信している国や地域に対しても一連の情報を提供しました。

インターネット定点観測データは、既知の脆弱性に対する攻撃動向や、既知のマルウエアの活動状況についての情報を収集する手段として活用されることが一般的ですが、この事例のように、観測データを契機に、異常を引き起こしている原因に迫ることができるケースがあります。

—トピック 2—
制御システムセキュリティカンファレンス 2012 を開催

制御システムセキュリティカンファレンス 2012 を 2 月 3 日（金）に東京（品川）で開催しました。「After Stuxnet」をテーマに、制御システムのセキュリティの実態を掘り下げて紹介し、制御システムの提供ベンダや利用事業者が対策に向けてどのように取り組むべきかを論じた講演やパネルディスカッションを行いました。

経済産業省からは、制御システムのセキュリティに関する標準化やテストベッド構築を含む認証制度を整備することで制御システム分野のセキュリティを向上させる施策が紹介され、情報セキュリティの専門家からは、Stuxnet 以降、制御システムが標的とされる現実や PLC や HMI といった機器やソフトウエアが、これらの攻撃に対していかに脆弱かという実態が指摘されました。制御システムの業界からは、業務系と制御系のネットワークの分離や新しいポリシーの導入などの対策事例とともに、業界が取り組むべき今後の課題が紹介され、熱い議論と意見交換が行われました。

制御システムセキュリティカンファレンス 2012
https://www.jpcert.or.jp/ics/conference2012.html

制御システムセキュリティカンファレンス 2012 においての講演資料
https://www.jpcert.or.jp/present/#year2012

―トピック 3―
標的型攻撃に関する情報共有の枠組み構築に向けて

執拗に行われる巧妙な標的型攻撃については、既存の情報セキュリティ対策だけでは防御ができない場合があり得ますが、そのような場合であっても攻撃に使われるマルウエアや侵入の手口に共通性があるときは、対策を講じる者間での情報流通によって攻撃を検知したり、被害の発生を抑止したりすることができる可能性があります。しかしながら、このような攻撃に使われるマルウエアについては、標的組織の内部情報が埋め込まれているために攻撃対象組織を伏せた攻撃手口の情報の流通が難しかったり、攻撃の検知や被害抑止のための情報として使うためには他の情報と併せた分析が必要になったりすることから、関係者間で必要な情報を適切かつ有効に流通させる枠組みの検討を進め、全体としての対処力を高めることが必要になってきているといえます。

そのための取組みの一つとして、2 月 14 日に開催された「サイバー情報共有のためのワークショップ」（主催：経済産業省、共催：JPCERT/CC、および特定非営利活動法人日本ネットワークセキュリティ協会（JNSA)、後援：情報セキュリティ政策会議）では、先行的な情報共有の枠組みを展開している海外のセキュリティ専門家を迎え、国内での取組みに向けて関係者と種々の可能性や課題について議論しました。

JPCERT/CC では、ご提供いただいたインシデント情報や収集した脅威情報、分析情報の活用をめざして、情報提供者に決して不利益が及ぶことのないような、情報共有の取組みの実現に向けて、今後も関係者の方々と共に議論と工夫を重ねてまいります。

サイバー情報共有のためのワークショップ
https://www.jpcert.or.jp/event/CTAPP.html

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、「2-5.セキュアコーディング啓発活動」、「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 2699 件、インシデント件数ベースでは 2535 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 754 件でした。前四半期の 752 件と比較して 0.3%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_Report20120412.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 324 件で、前四半期の 314 件から 3%増加しました。また、前年度同期（405 件）との比較では、20%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	1 月	2 月	3 月	国内外別合計（割合）
国内ブランド	30	7	21	58(18%)
国外ブランド	72	55	94	221(68%)
ブランド不明（注 5）	13	18	14	45(14%)
月別合計	115	80	129	324(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 58 件と、前四半期の 65 件から 11%減少しました。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 221 件と、前四半期の 198 件から 12%増加しました。

本四半期に確認された、国内の SNS やオンラインゲームを装った複数のフィッシングサイトは、正規サイトの画像や Flash などのコンテンツを直接参照していて、見た目には正規サイトとまったく変わらないものでした。見分ける手立てはアドレス・バーに表示される URL しかありません。

WordPress で構築されたサイトについては、前四半期に改ざんされるインシデントが多くありましたが、本四半期はフィッシングサイトが設置された事例を多数確認しています。

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 63%、ポータルサイトを装ったものが 13%を占めています。
国内金融機関を装ったフィッシングは、昨年から続いており、3 月に報告を受領したフィッシングサイトでは、前四半期にも見られたダイナミック DNS サービスのドメインを使用していました。また、複数の国内 ISP の Web メールサービスを装ったフィッシングサイトも、前四半期に引き続き確認しています。

フィッシングサイトの調整先の割合は、国内が 64%、国外が 35%と、前四半期の割合（国内 62%、国外 38%）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、142 件でした。前四半期の 164 件から 13%減少しています。

本四半期には、オンラインゲームの RMT (Real Money Trading: オンラインゲーム内のアイテムや通貨などを、現金で取引する行為) サイトなどへのリンクを埋め込む Web ページの改ざんの報告を受領しました。報告をもとに調査したところ、同様のリンクを埋め込む改ざん事例を国内

で多数確認しました。これは、リンクが埋め込まれたサイトを大量に作り出すことで、RMT サイトの検索エンジンにおけるランキングを上昇させる、検索エンジン用の最適化（SEO: Search Engine Optimization）を目的とした改ざんであると考えられます。

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：13 件　https://www.jpcert.or.jp/at/

2012-01-04　Microsoft .NET Framework の複数の脆弱性に関する注意喚起
2012-01-11　2012 年 1 月 Microsoft セキュリティ情報 (緊急 1 件含) に関する注意喚起
2012-01-11　Adobe Reader 及び Acrobat の脆弱性に関する注意喚起
2012-02-06　PHP 5.3.9 の脆弱性に関する注意喚起

2012-02-15　2012 年 2 月 Microsoft セキュリティ情報 (緊急 4 件含) に関する注意喚起
2012-02-16　Adobe Flash Player の脆弱性に関する注意喚起
2012-02-21　2012 年 2 月 Microsoft セキュリティ情報 (緊急 4 件含) に関する注意喚起
2012-03-06　Adobe Flash Player の脆弱性に関する注意喚起
2012-03-06　DNS 設定を書き換えるマルウエア (DNS Changer) 感染に関する注意喚起
2012-03-07　DNS 設定を書き換えるマルウエア (DNS Changer) 感染に関する注意喚起
2012-03-14　2012 年 3 月 Microsoft セキュリティ情報 (緊急 1 件含) に関する注意喚起
2012-03-23　2012 年 2 月公開の Java SE の脆弱性を狙う攻撃に関する注意喚起
2012-03-29　Adobe Flash Player 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：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 68 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。

2012-01-12　各国 CSIRT の定期レポート
2012-01-18　Firefox/Thunderbird の法人向け延長サポート版について
2012-01-25　ハッシュテーブル処理の問題
2012-02-01　情報セキュリティ月間
2012-02-08　Firefox/Thunderbird 法人向け延長サポート版 (ESR) リリース
2012-02-15　Windows Vista 家庭向け製品サポート終了
2012-02-22　Windows 家庭向け製品サポート延長について
2012-02-29　DNS Changer マルウエア
2012-03-07　PHP 5.4.0 リリース
2012-03-14　マイクロソフト Internet Explorer の自動アップグレード
2012-03-22　RDP サービスの脆弱性に注意
2012-03-28　ユーザアカウントとメールアドレスの整理

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) PHP の脆弱性情報に関する情報収集・提供

2012 年 2 月に PHP Group から PHP 5.3.9 の脆弱性に関する情報が公開されたことに加え、当該脆弱性を実証する実証コードが公開されたことを受けて、PHP 5.3.9 を使用した Web サイトへの攻撃が発生する懸念が高まっていると判断し、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。

PHP 5.3.9 の脆弱性に関する注意喚起
https://www.jpcert.or.jp/at/2012/at120004.html

2) DNS 設定を書き換えるマルウエア(DNS Changer)感染に関する情報収集・提供

JPCERT/CCは、海外のセキュリティ対策組織より「PCのDNS設定を書き換えるマルウエア(以下「DNS Changer」といいます。)」に感染した国内のPCについて情報提供を受けました。DNS Changerは、攻撃者が用意した不正なDNSサーバを参照するように、感染したPCのDNS設定を変更することで、ユーザがブラウザ上で正しくURLを入力しても、まったく別のWebサイトを表示させたり、ページの一部(広告など）だけを書き換えたりします。この不正なDNSサーバは、2011年11月に米国連邦捜査局(FBI)によって差し押さえられ、暫定的に正常なDNSサーバに置き換えられています。これにより、当面は本来のWebサイトが閲覧できていますが、国内でも相当数のPCがDNS Changerに感染したままの状況にあり、FBIによる暫定的なDNSサーバの運用が2012年3月9日(日本時間)に停止(*1)すると予告されたため、広く注意喚起を行いました。

*1) その後、置き換えられた正常なDNSサーバの運用が4ヶ月延長されることとされました。

DNS 設定を書き換えるマルウエア (DNS Changer) 感染に関する注意喚起
https://www.jpcert.or.jp/at/2012/at120008.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. 定点観測での事例

2011 年 12 月上旬より、ポート 23/TCP へのスキャンが増加しました。このスキャンは、日本国内外のセンサーで観測され、韓国国内の数百の IP アドレスから行われていました。
JPCERT/CC では、スキャンの傾向などの情報から、ブロードバンドルータなど PC 以外の機器が攻撃を受けてボットに感染し、その機器からポート 23/TCP へスキャンが行われていると推測しました。推測に基づき、KrCERT/CC とともに調査をした結果、組込 Linux を使用した複数の機器がマルウエア感染の影響を受け、スキャンが増加していることが確認でき、対策に向けた動きにつなげることができました。

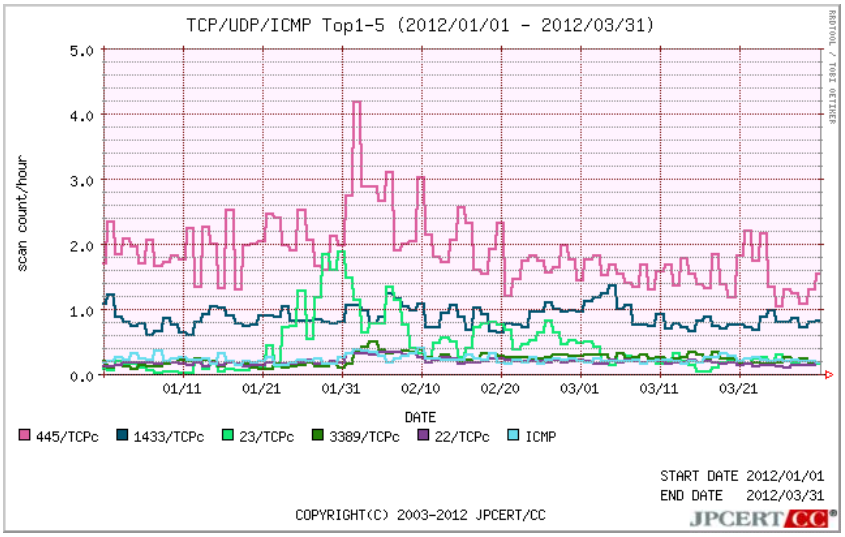
1-3-2. ポートスキャン概況

インターネット定点観測システムの観測結果を、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 ページで公開しています。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

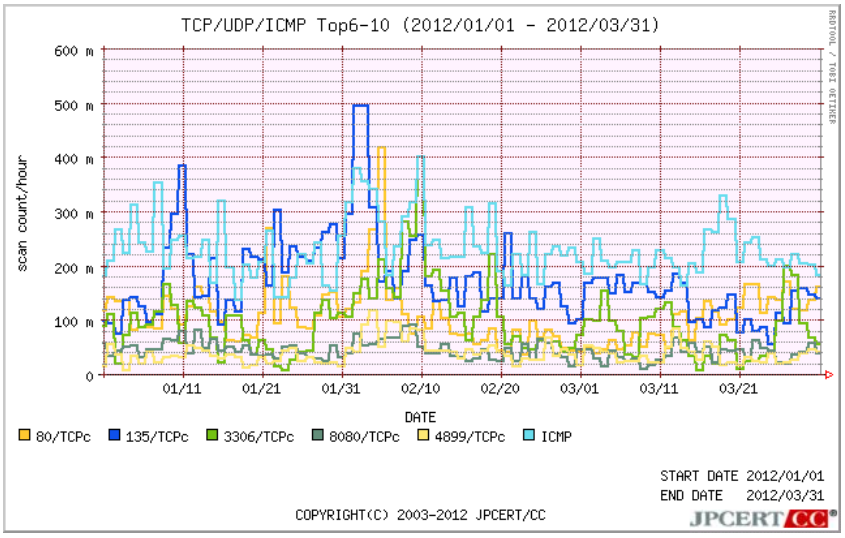
本四半期に定点観測システムで観測されたアクセスの宛先ポートの上位 1 位～5 位及び 6 位～10 位のそれぞれについて、アクセス数の時間的推移を[図 1-1]と[図 1-2]に示します。

- アクセス先ポート別グラフ top1-5 (2012 年 1 月 1 日-3 月 31 日)



[図 1-1 アクセス先ポート別グラフ top1-5]

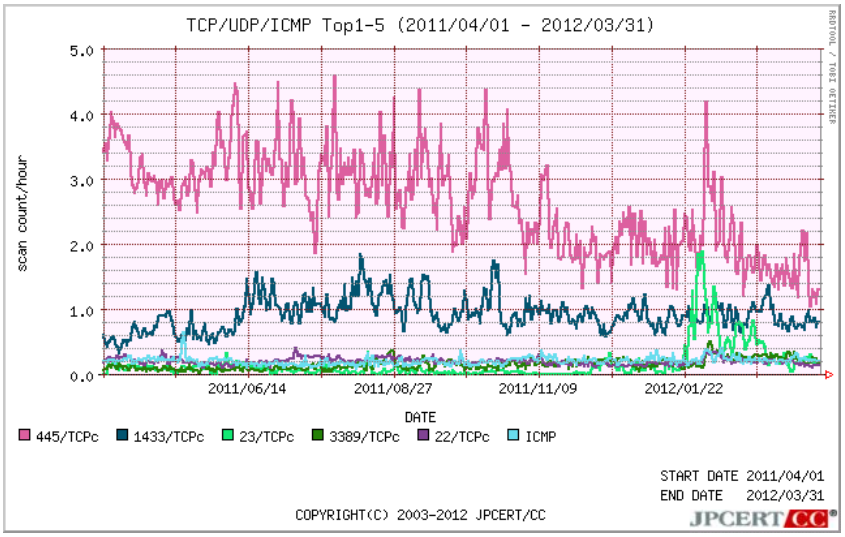
- アクセス先ポート別グラフ top6-10 (2012 年 1 月 1 日-3 月 31 日)



[図 1-2 アクセス先ポート別グラフ top6-10]

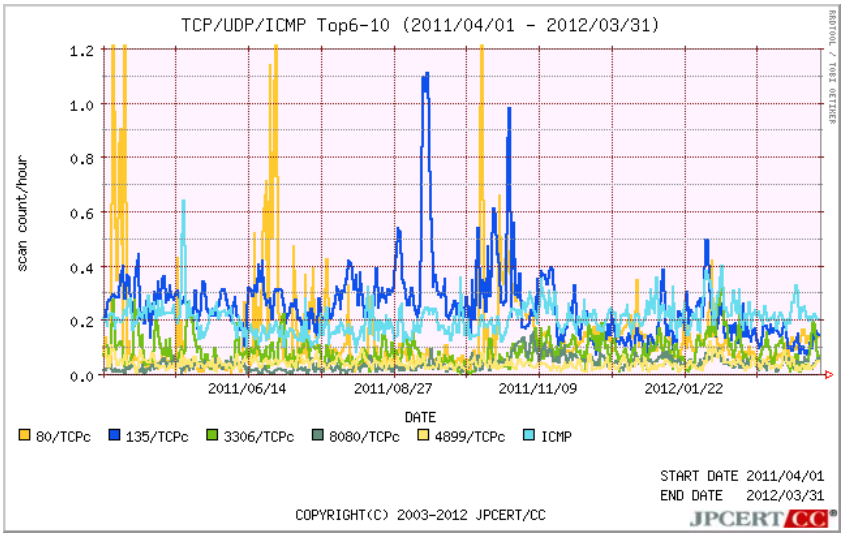
また、より長期間のスキャン推移を見るため、2011 年 4 月 1 日から 2012 年 3 月 31 日までの期間における、アクセスの宛先ポートの上位 1 位～5 位及び 6 位～10 位のそれぞれについて、アクセス数の時間的推移を[図 1-3]と[図 1-4]に示します。

- アクセス先ポート別グラフ top1-5 (2011 年 4 月 1 日-2012 年 3 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 4 月 1 日-2012 年 3 月 31 日)



[図 1-4 アクセス先ポート別グラフ top6-10]

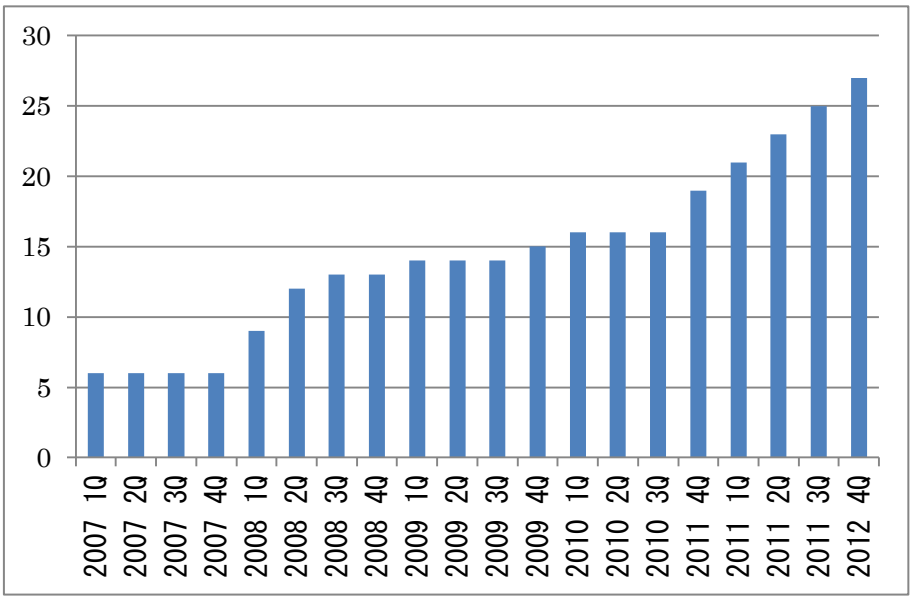
順位には変動がありますが、これまでの傾向と同様、 Windows や Windows 上で動作するソフトウエアへの スキャン 活動や、Telnet、SSH サーバなどコンピュータを遠隔操作で使う場合にサーバ側が待ち受けているポートへのスキャン活動が多く観測されています。

1-4. 日本シーサート協議会 (NCA) 事務局運営

国内のシーサート(CSIRT: Computer Security Incident Response Team) が互いに協調し連携して共通の問題を解決する場として設立された日本シーサート協議会（Nippon CSIRT Association: NCA）の事務局として、JPCERT/CC は、協議会の問合せ窓口、会員情報の管理、加盟のための

ガイダンスの実施および手続の運用、Web サイト、メーリングリストの管理等の活動を行っています。

本四半期においては、株式会社ディー・エヌ・エー(DeNA CSIRT)とグリー株式会社(GREE-IRT)が、新規に加盟しました。本期末時点で 27 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。

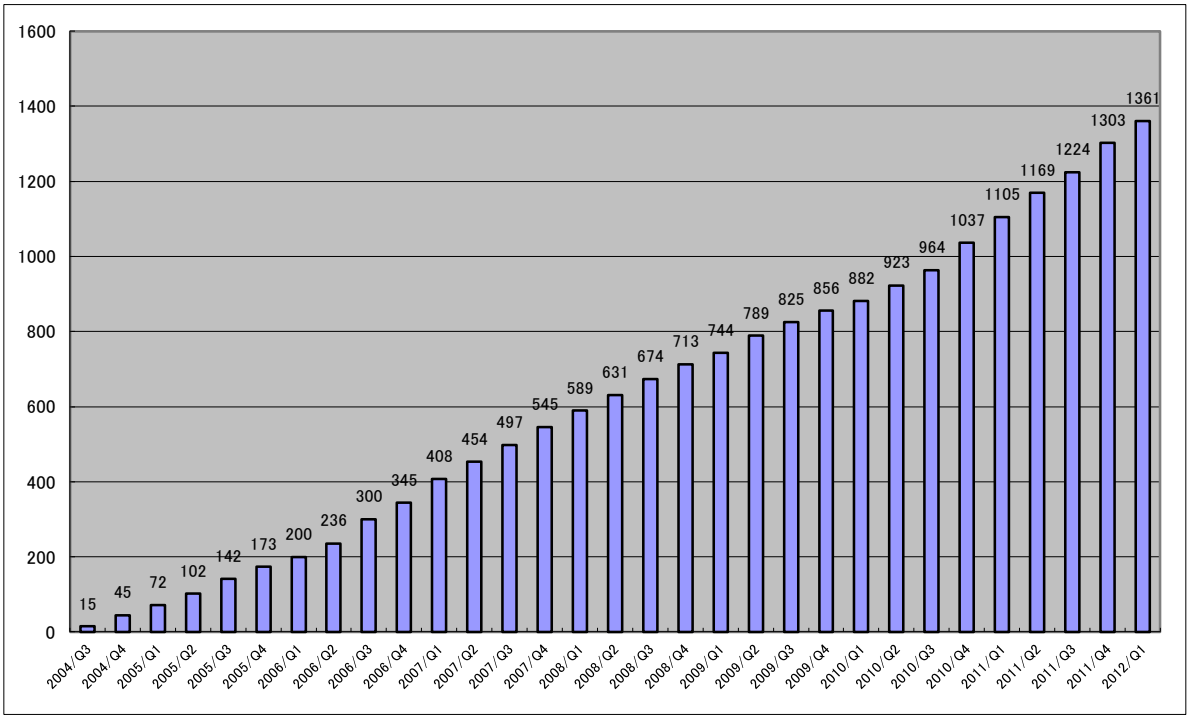
日本シーサート協議会 Web ページ
http://www.nca.gr.jp/

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。

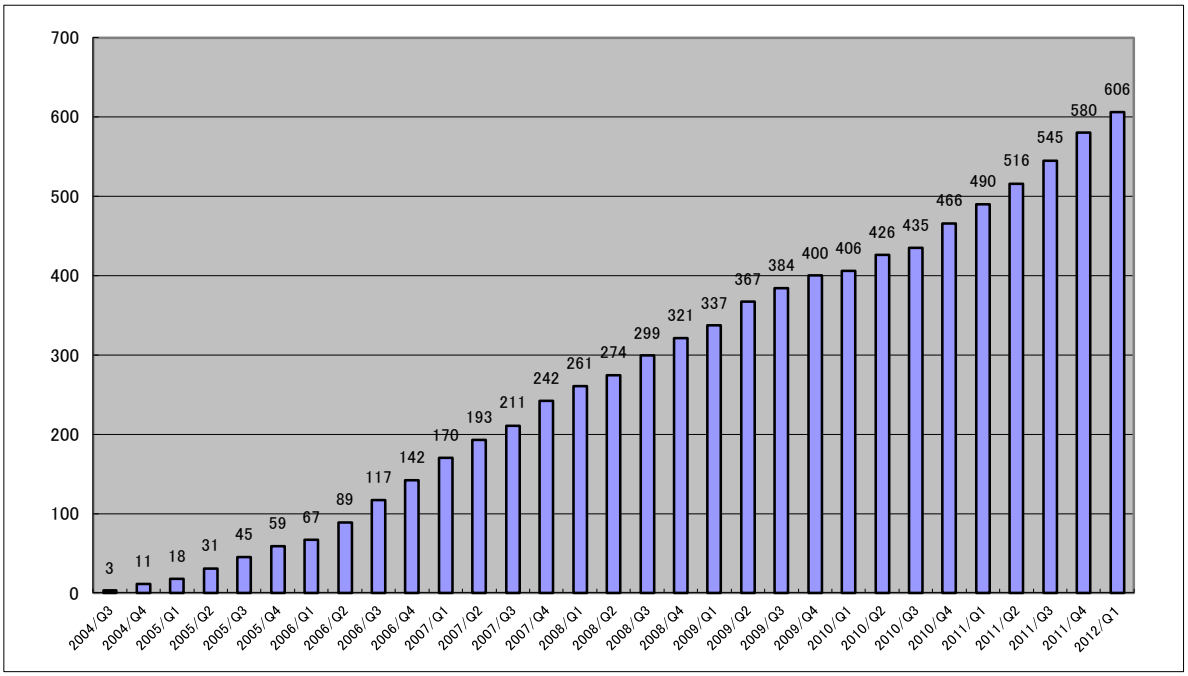
2-1. Japan Vulnerability Notes (JVN) において公開した脆弱性情報および対応状況

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、58 件(累計 1361 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。



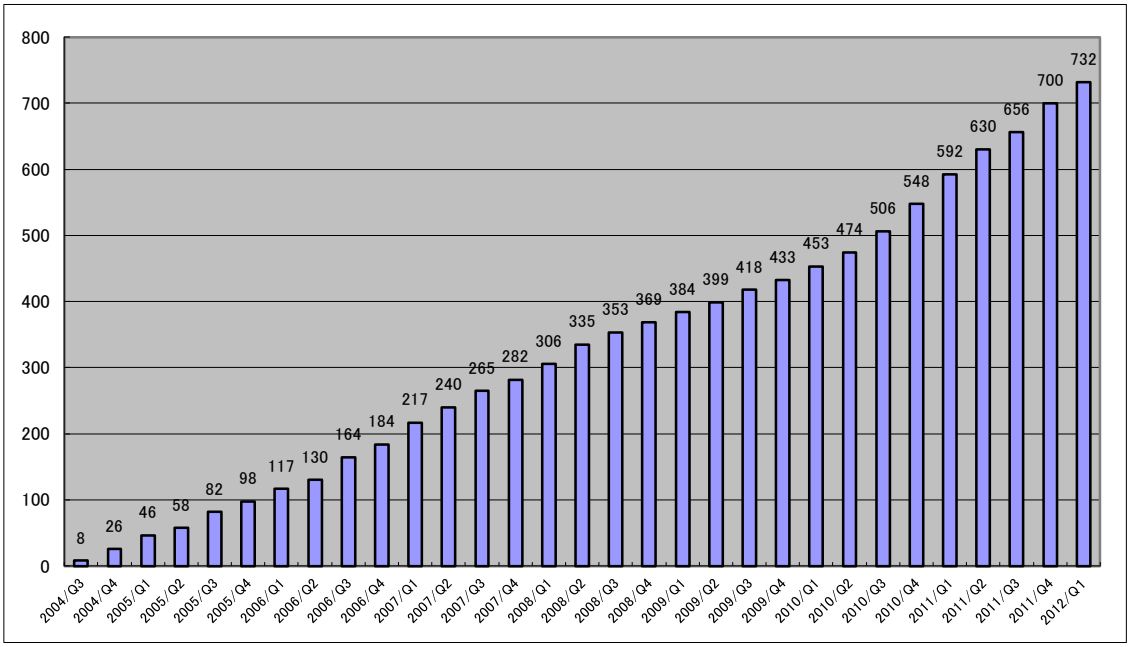
[図 2-1　JVN 公開累積件数]

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、26 件(累計 606 件) [図 2-2] でした。そのうちの半数を超える 13 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。本四半期には、android およびその関連製品の届出が増える前四半期からの傾向が続き、android 携帯端末の脆弱性および android アプリケーションの脆弱性を 3 件公開しました。また、JPCERT/CC として初めて、制御システム製品の脆弱性の報告を発見者から直接に受け取り、3 件の脆弱性情報に CVE を採番し、JVN にて公表しました。これは、海外 CSIRT の一つである台湾の ICST (Information and Communication Security Technology Center) of Taiwan（通称 TWNCERT）の研究員が、複数の制御系製品における複数の脆弱性を発見し、直接 JPCERT/CC へ届出を行ったものです。他の分野の製品のケースと同様、JPCERT/CC は、製品開発者へ速やかに連絡を行い、製品開発者との調整を経て JVN にて製品開発者の対策情報とともに情報公開を行いました。



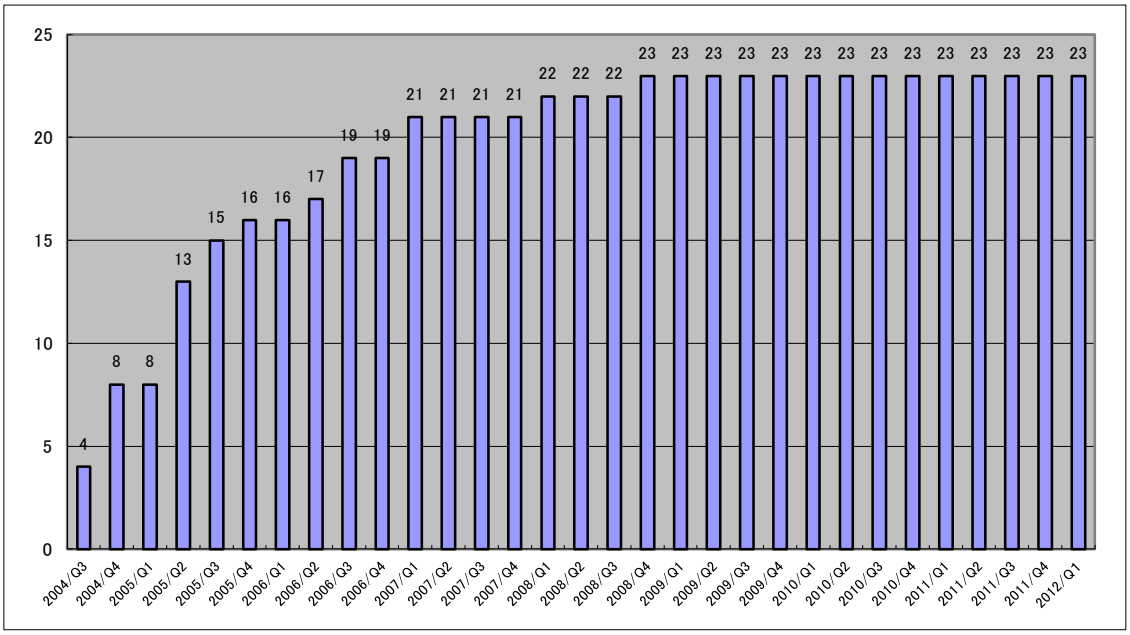
[図 2-2　JVN_JP(JVN#)公開累積件数]

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 として公開した脆弱性情報は、32 件(累計 732 件) [図 2-3]でした。これらの中には、Apple 製品に関するものが 7 件、Cisco の製品が 1 件、HP(Hewlett Packard)の製品が 1 件、Oracle の製品が 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。また著名な OSS 製品（ライブラリ、サーバ製品、OS 等）における脆弱性情報が 5 件と約 20%を占めました。また本四半期には、フィンランドの CERT-FI から、JPCERT/CC および米国 CERT/CC へ公開前情報展開された脆弱性情報が 2 件あり、この 2 件に関しても JVNVU#として公開を行いました。



[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　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、3 月 16 日に、連絡不能開発者一覧として製品開発者 8 件を追加公表しました。また同日、「連絡不能開発者一覧」に前回の公開（12 月 16 日）後も連絡がとれないままの 49 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 1 件について製品開発者から連絡がありました。3 月末日時点では、合計 96 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 で公開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。

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、26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

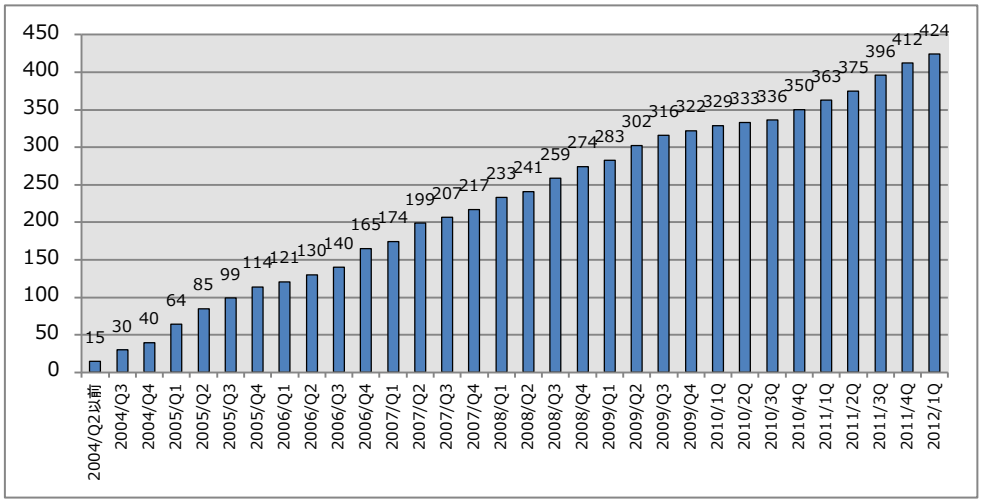
本基準では、受付機関に IPA、調整機関に JPCERT/CC が指定されています。JPCERT/CC は IPA が受け付けた届出情報の転送を受けて、製品開発者への情報提供を行い、対策情報公開に至るまでの調整を行っています。最終的には、 IPA と共同で、脆弱性情報ポータル JVN において対策情報を公開しています。両組織間においては、脆弱性情報の分析結果や脆弱性情報の取扱い状況等の情報交換を行うなど、緊密な連携をおこなっています。なお、本基準における IPA の活動および四半期毎の届出状況については、次の URL をご参照ください。

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 3 月 31 日現在で 424 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]

2-4-3. 製品開発者との定期ミーティングの実施

JPCERT/CC では、技術情報やセキュリティ・脆弱性の動向などの情報交換や、脆弱性情報ハンドリング業務に関する製品開発者との意見交換、また製品開発者間の情報交換を目的として、脆弱性情報ハンドリングにご協力いただいている製品開発者の皆様とのミーティングを定期的に開催しております。

本四半期は 2012 年 3 月 27 日にミーティングを開催し、脆弱性情報ハンドリングに関する活動状況の報告、海外における脆弱性やセキュリティに関する動向および技術情報等を紹介するとともに、それらに関する製品開発者との意見交換、脆弱性情報ハンドリング業務における課題等についてのディスカッションを行ないました。

[図 2-6　製品開発者との定期ミーティングの様子]

2-5.　セキュアコーディング啓発活動

2-5-1.　「Java セキュアコーディング スタンダード CERT/Oracle 版」出版

弊センター代表理事の歌代和正監修の下、セキュアコーディングプロジェクトのメンバが翻訳した書籍「Java セキュアコーディングスタンダード CERT/Oracle 版」（原著 : CERT Oracle Secure Coding Standard for Java）を刊行しました。

本書は、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 Java の専門家が加わり Wiki を通じて共同開発された Java のコーディング規約集をベースに、JPCERT/CC で書き起こした「Android アプリケーション開発へのルールの適用」を追加したものです。後者には、重要度の高いコーディングルールを厳選し、日本語版独自のコンテンツとして Android 環境で特に重要なルールにコメントを付してまとめた一覧表の形式になっています。

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ー、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本書をご一読いただき、Java アプリケーションのセキュリティ向上に役立てていただけることを期待しています。

「Java セキュアコーディングスタンダード CERT/Oracle 版」
著者：Robert C. Seacord, 他
監修：歌代 和正
翻訳：久保 正樹、戸田 洋三
発行：アスキーメディアワークス
発売：2012 年 1 月 27 日
384 ページ
定価：3,990 円(税込み)

2-5-2. 学生向けセミナー「Java セキュアコーディングセミナー」開催

学生等の若年層向けに Java 言語を使って脆弱性を含まない安全なプログラム開発を行うための具体的なテクニックとノウハウを学んで頂くためのセミナー「Java セキュアコーディングセミナー」を下記のとおり実施しました。

形式：講義
日時：2 月 15 日（水）13:30～16:30 キャンパスプラザ京都 京都大学サテライト
2 月 18 日（土）13:30～16:30 慶應義塾大学日吉キャンパス

[図 2-7　Java セキュアコーディングセミナー（慶応義塾大学）の様子]

講義中に活発な質疑応答が行われたほか、一部の受講生は講義終了後も講義の内容について講師と議論を行うなど、学生のセキュアコーディングに対する関心の高さが伺われました。今後も、若年層向けのセキュアなソフトウエア開発に関する啓発活動を継続していく予定です。

2-5-3. 「Android セキュアコーディングセミナー」開催

Android プラットフォームでアプリケーション開発を行うプログラマー向けのセミナーを翔泳社と共同で企画し、3 月 14 日（水）に実施しました。当日は、定員ほぼ満員となり、遠方から参加される方もおられる中、Android におけるセキュリティの問題について俯瞰し、実践的なセキュアコーディングのテクニックに関する座学と実機を使ったセキュリティコードレビューのデモを行い、安全な Android アプリ開発を行うためのノウハウを学んでいただきました。

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

2-5-4.「Developers Summit 2012」にて講演

以下のイベントで講演を行いました。

イベント名：Developers Summit 2012
開催日時：2012 年 2 月 17 日（金）
講演タイトル：Java/Android セキュアコーディング入門

講演では、モバイルアプリケーションを取り巻くセキュリティ問題を概観し、Java 言語を使った Android アプリケーション開発で見られる脆弱性事例と対策方法を織り交ぜながら、セキュアコーディング実践の重要性とその方法について紹介しました。
講演資料は、以下の Web サイトにて公開しています。

Java/Android セキュアコーディング入門
http://www.slideshare.net/bokuwa9bo/javaandroid

今年で 10 年目を迎える本イベントは、ソフトウエア開発等に携わる幅広い業種のエンジニアが参加しており、このような場で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。

2-5-5. 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」と題したシ

リーズで Java セキュアコーディングの解説記事を連載しています。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を、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つつ解説しています。本四半期は、以下の 2 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 4 回「ハッシュテーブルに対する攻撃手法のはなし」(2 月 20 日公開)
第 5 回「Android アプリにおける DB ファイルの正しい使い方」(3 月 29 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

2-5-6. セキュアコーディング 出張セミナー

JPCERT/CC では、ソフトウエア製品等の開発を行う企業・組織を対象に、セキュアコーディングに関する出張セミナー（有償）の実施を承っています。マネジメント層へのセキュリティ啓発や新人研修のメニュー等としてもご利用いただけます。本四半期から、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 言語版のセキュアコーディング出張セミナーの提供を開始しました。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 2 回実施しました。
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. 制御システムセキュリティ強化に向けた活動

2-6-1. 制御システムセキュリティカンファレンス 2012 の開催

制御システムセキュリティカンファレンス 2012 を 2 月 3 日（金）に東京（品川）で開催しました。4 回目となる今回は「After Stuxnet」をテーマに、産官学の関係者の方々に脅威に対する具体的な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にしました。午前中は、2011 年の制御システムへの取組みや最新の情報、制御システムセキュリティを題材に政府の取組みや動向報告などを行いました。午後からは、制御システムセキュリティ検討タスクフォースや業界団体、企業での取組み、弊センターの活動についての講演と質疑応答を行いました。本年度は、昨年度同様 300 名以上の参加申し込みがあり、会場はほぼ満席となりました。制御システムセキュリティに対する関心が非常に高くなってきたことが伺われます。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 2012
https://www.jpcert.or.jp/ics/conference2012.html

制御システムセキュリティカンファレンス 2012 においての講演資料
https://www.jpcert.or.jp/present/#year2012

2-6-2. インシデントハンドリング体制 WG の活動のとりまとめ

前四半期から継続して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、取りまとめに向けた検討を行いました。ここで得られた結論は、2012 年 4 月に開催される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。

2-6-3. 制御システム向けインシデント対応訓練トライアル開催

2012 年 3 月 13 日と 14 日の 2 日間、制御システム業界におけるインシデント対応訓練のあり方を検証するとともに、インシデント対応の実態を把握するため、制御システム向けインシデント対応訓練トライアルを開催しました。

制御システムのベンダと運用事業者の技術者を対象に参加者を募り、一般的な攻撃手法や防御手法を座学で学んでいただいた後、制御システムネットワークに典型的な 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環境で、ハンズオン(実地演習)に取組んでいただきました。今後のインシデント対応訓練の改善や実施に向けた検討のための基礎情報として、受講者にどの様な意識の変化が起きたか、今後制御システムを保有する立場、開発する立場としてどのような取組みが必要なのかなどについて、意見交換の時間とアンケートにより受講者の意見を収集しました。

2-6-4. 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 4 回（1 月 6 日、3 月 2 日(2 通)、3 月 21 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 213 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

2-6-5. 国内外情報収集活動

2012 年 1 月に SCADA Security Scientific Symposium（以下 S4）が開催されました。制御システムセキュリティに特化した研究発表および技術発表の場であり、本年で 5 年目を迎えます。

今回の S4 では、制御システムにおいて利用される PLC（Programmable Logic Controller）に関しての研究発表や制御システムにおける脆弱性情報の動向、SHODAN 検索エンジンを用いたインターネット接続されている制御システム機器についての調査結果などの発表が行われました。

研究発表内容に関しては、制御システムにて用いられる製品単体のセキュリティ対策について、制御システムベンダがどのようにセキュリティに取組むのかを問う発表でもありました。本件に関しては、制御システムセキュリティカンファレンス 2012 においてもその情報共有を行ないました。

S4 2012
http://www.digitalbond.com/s4/

2-6-6. 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 9 件の申込みがあり、直接配布件数の累計が 94 となりました。

2-6-7. 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ブラッシュアップをはかる活動を行いました。

2-6-8. 講演活動

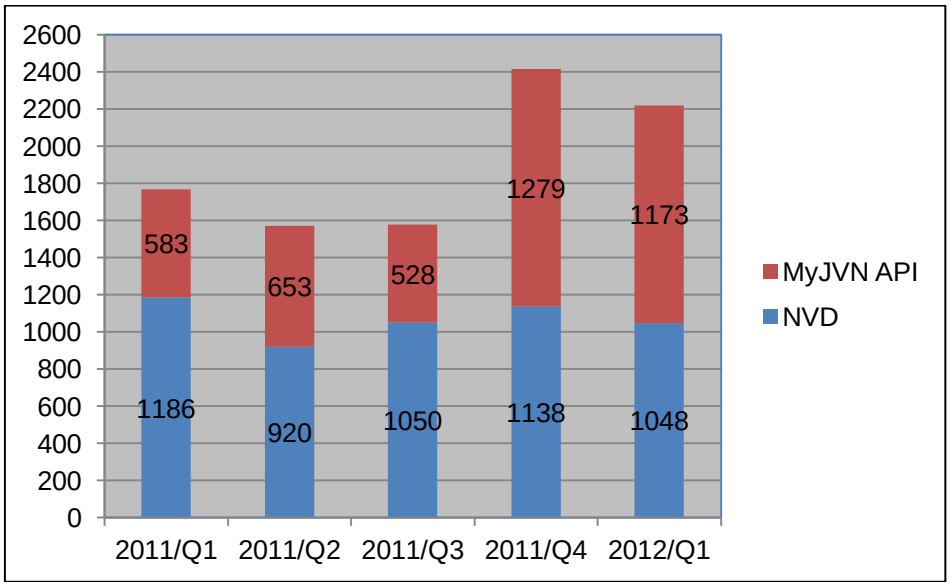
2012 年 2 月 24 日に東京・学士会館にて開催された「ISA-J2012 テクニカルフォーラム（技術講演会）」（ISA-J（国際計測制御学会日本支部）主催）において、「制御システムのセキュリティとインシデント対策」と題する講演を行いました。

2-7. VRDA フィードによる脆弱性情報の配信

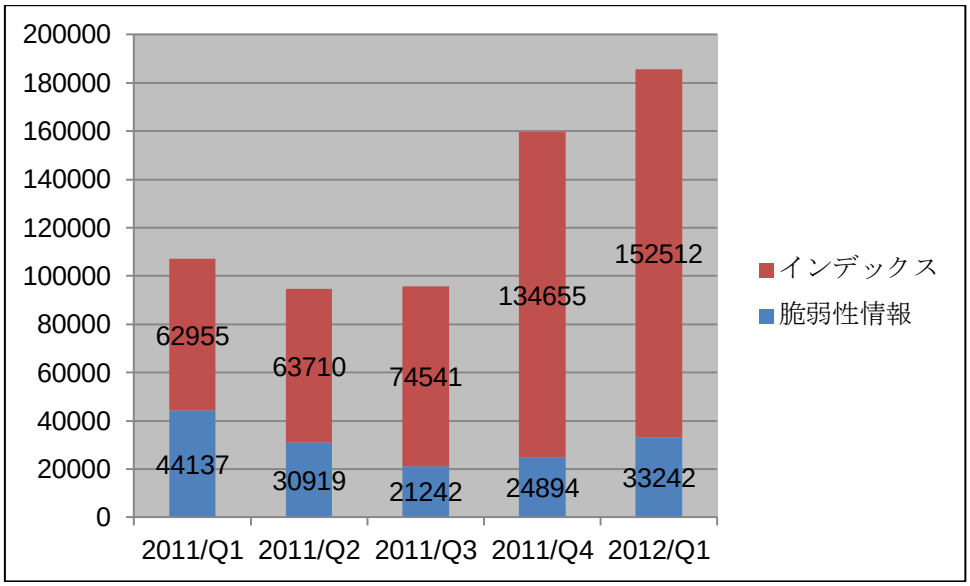
JPCERT/CC は、大規模組織の組織内 CSIRT などでの利用を想定して、KENGINE などのツールを用いた体系的な脆弱性対応を可能とするため、IPA が運用する MyJVN API および NIST (National Institute of Standards and Technology)の NVD (National Vulnerability Database) を外部データソースとして利用した、VRDA (Vulnerability Response Decision Assistance)フィードによる脆弱性情報の配信を行っています。VRDA フィードについての詳しい情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

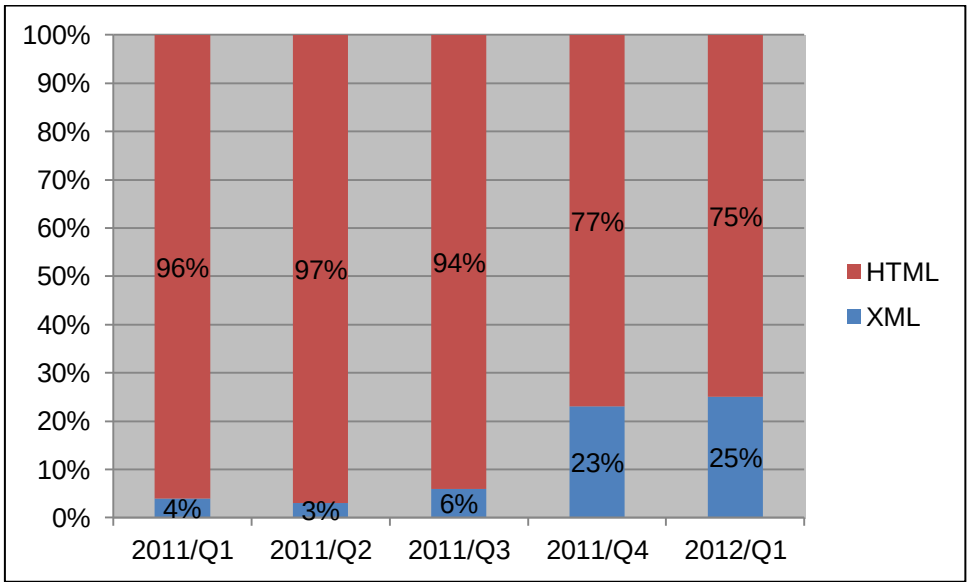


[図 2-8 VRDA フィード配信件数]



[図 2-9 VRDA フィード利用件数]

[図 2-9] に示したように、VRDA フィードインデックスの利用数は、前四半期に引き続き、大きな増加傾向が見られます。



[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は、前四半期と比較して大きな変化は見られません。

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では、技術的な深耕だけではなく、得られた知見を活用者の視点に合わせて加工していくことも重要です。本四半期においては、引き続き攻撃に関する情報共有の取組みに参加するとともに、研究者や分析技術者を対象とした分析技術情報の発信活動を実施しました。

3-1. IT Keys「リスクマネジメント演習」

JPCERT/CCは過去3年間にわたり、サイバークリーンセンタープロジェクトの一員として、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実施されてきた「IT Keys」において、「リスクマネジメント演習」の講義を担当してきました。本年度も同プロジェクトの講義の一部を担当し、教材検体を用いた解析演習を行いました。
近年のインシデント調査においては、初動段階でいかにして多くのデータが抽出できるかが重要になってきています。本年度は、侵入されたコンピュータのメモリからデータを抽出する作業を追加し、初動段階も体験していただけるような演習シナリオを作成しました。

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

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。昨年 10 月にナイロビ(ケニヤ)で開催された SC27 の国際会議で合意された方針に基づいて各エディタが作業を行い、昨年 12 月前後までに改訂された標準草案が各国に配付されています。今期は改訂草案を検討し、次の SC27 国際会議に向けてコメントの作成を行いました。

「脆弱性情報の開示」については、第 4 次委員会草案(CD； Committee Draft)を調査し、これに対する 29 項目からなる修正要求コメントを取りまとめ、国内委員会の審議を経て日本のコメントとして SC27 事務局に提出しました。主な論点としては、「脆弱性取扱手順」の標準との切分けや、オンライン・サービスを対象に含めることの是非などを挙げています。

「脆弱性情報の取扱手順」については、第 2 次作業草案(WD； Working Draft)を調査し、これに対する 8 項目からな修正要求コメントを取りまとめ、国内委員会の審議を経て日本のコメントとして 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。

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が行われました。これに対して日本として「賛成」投票をするよう国内委員会に提案しました。

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）

なお、投票の結果この再構成について合意が得られれば、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）、次回のストックホルム会議から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(2012 年 2 月 28 日-3 月 11 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。
2011 年 7 月、10 月、11 月に続いて、第 4 回目の専門家派遣となる今回は、フィジーの ISP、政府、重要インフラ企業を対象にした CSIRT セキュリティセミナにてネットワークフォレンジックとウェブセキュリティに関する 3 日間の講義を行いました。また、JICA や PacCERT の関係者とともにプロジェクトの進捗確認を行うとともに、今後の計画について協議しました。

5-1-2. その他地域における活動

本四半期は、その他地域における CSIRT 構築支援および運用支援活動はメールでの問合せ及び次の四半期に向けた計画立案が中心でした。

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、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

1 月 31 日及び 2 月 22 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。

5-2-1-1-2. APCERT 合同サイバー演習 (APCERT Drill 2012) に参加 (2012 年 2 月 14 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、広範囲に影響が派生するインシデントに対応する各経済地域 CSIRT 間の連携の強化を目的として、毎年実施されています。
今回で 9 度目となった合同サイバー演習のテーマは「APT 攻撃と国際連携」で、約 4 時間にわたり実施されました。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 よりチュニジア、エジプト、パキスタンのチームも加わって、20 の経済地域から計 25 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にも加わり、スムーズな演習の実施を支えました。

5-2-1-1-3. APCERT 年次総会 2012 への参加(2012 年 3 月 25 日-28 日)

アジア太平洋地域の CSIRT コミュニティである APCERT の年次総会がインドネシアのバリ島で開催され、JPCERT/CC を含め 22 の加盟チームが参加しました(2012 年 3 月末現在、20 の経済地域から 29 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：
3/25（日） 午前：APCERT ワーキンググループ会合
APCERT ステアリングコミッティー(運営委員会)

午後：APCERT 年次総会準備会(Pre-Annual General Meeting)
3/26（月） 午前：APCERT 年次総会(Annual General Meeting)
午後：APCERT カンファレンス（限定公開）
3/27（火） 終日：APCERT カンファレンス（一般公開）
3/28（水） 終日：APCERT 加盟チーム交流イベント

２）場所：Padma Hotel, バリ島, インドネシア

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。

昨年度の年次総会では、“APCERT to help create a safe, clean and reliable cyber space in the Asia Pacific region through global collaboration”というビジョンのもとに活動を活性化するという方向性が共有されましたが、今年度の年次総会（3 月 26 日午前）はこの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在り方を議論しました。

また、ステアリングコミッティー(運営委員会)のメンバの一部改選が行われるとともに、APCERT 議長チーム/副議長チームの改選が行われ、JPCERT/CC は議長チームに再選されました（2 期目、任期は 2013 年 3 月まで）。これにより、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。

[図 5-1 APCERT 年次総会集合写真]

5-2-1-1-4. TSUBAME ネットワークモニタリングワークショップの開催(2012 年 3 月 25 日)

APCERT 年次総会の直前の日程を選んで、JPCERT/CC は、アジア太平洋地域の CSIRT 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。本プロジェクトでは、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。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、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、今年度観測された主な事象に関する報告とシステムの新機能の紹介を行いました。また、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。

5-2-1-1-5. APCERT と他組織間との連携

1) APSTAR Retreat (2012 年 2 月 26 日)
APSTAR Retreat は、APNIC、APTLD、 APIA などのアジアパシフィック地域の関連団体が集まる国際会議です。インドのニューデリーで開催された同会議において、APCERT の議長チームとして「Introducing APCERT New Vision」という演題で遠隔講演を行いました。

5-2-1-2. 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。
1 月 27 日に日本クレジット協会 で開催された会合に参加し、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講演を行いました。また、2 月 6 日に開催された SecurityDay2012 に参加し、「中国の今そこにある情報セキュリティ危機」を題とした講演を行いました。さらに、3 月 29 日に台灣網路資訊中心 TWNIC が台北で開催した「2012 網際網路趨勢研討會」にパネラーとして参加し、日本におけるサイバー攻撃傾向を説明しました。
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。

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 Steering Committee 出席（1 月 16 日-20 日、3 月 25 日-30 日）

FIRST の Steering Committee のメンバである JPCERT/CC の理事 山口英が次の Steering Committee に出席しました。

・1 月 16 日-20 日 タイ・バンコク
・3 月 25 日-30 日 ブラジル・サンパウロ

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

5-2-2-1-2. 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、富士通株式会社のクラウド・コンピューティングにおけるセキュリティを専門に扱う組織内CSIRTであるFujitsu Cloud CERT (FJC-CERT)のスポンサーを務め、同組織は2月に正式にFIRST 加盟に至りました。2012 年3月末現在、日本からのFIRST 加盟チームは、22チームとなっています。

5-2-2-2. 「サイバー情報共有のためのワークショップ」開催(2 月 14 日)

経済産業省の事業として実施されている「平成 23 年度コンピュータセキュリティ早期警戒態勢の整備事業（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）（英語名称: Counter Threats and Attack Partner Program < CTAPP>）」の一環として、海外におけるサイバー攻撃に関する情報共有の事例の把握や、国内における関連情報の共有の促進のため、「サイバー情報共有のためのワークショップ」を開催に協力しました。
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。

5-2-2-3. RSA Conference 2012 への参加(2012 年 2 月 27 日-3 月 2 日)

米国のサンフランシスコで開催された RSA Conference 2012 に参加し、講演やパネルディスカッションを通して、モバイル端末等に対する最新の脅威に関するトピックスや、脆弱性を作り込まないソフトウエア開発に関する業界の取組みについて情報収集を行いました。

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、以下に関してブログにエントリーを掲載しました。
・TCP23 番ポート（テルネット）に対するスキャンの増加とその分析結果

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

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（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 を通じて、フィッシングに関するニュースや緊急情報を 7 件発信しました。

本四半期も前四半期と同様に金融機関の第二認証情報を詐取するフィッシングと、インターネットサービスプロバイダや検索プロバイダの Web メールを騙るフィッシングの報告を、それぞれ複数受けました。フィッシングメールやサイトの関連情報を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「ゆうちょ銀行をかたるフィッシング」(3 月 2 日)、および事例公開「BIGLOBE を騙るフィッシング」(1 月 20 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　ゆうちょ銀行を騙るフィッシングサイト
https://www.antiphishing.jp/news/alert/20120301.html]

6-2. フィッシングサイト URL 情報の提供

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。本四半期末の時点で協議会から情報を提供している事業者等は 16 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。

6-3.　講演活動

協議会ではフィッシングに関する現状を紹介し、効果的な対策を呼びかけるため講演活動を行っています。本四半期は次のとおり講演を行いました。

(1) 山本 健太郎「最新のフィッツシングの現状と企業側の対策」
　日本クレジットカード協会,勉強会 2012 年 1 月 26 日
(2) 山本 健太郎「最新のフィッツシングの現状と企業側の対策」
　埼玉県クレジットカード犯罪対策連絡協議会,勉強会 2012 年 3 月 29 日

6-4. フィッシング対策協議会の活動実績の公開

協議会の Web サイトにおいて、報告されたフィッシングサイト数を含む、毎月の活動報告などを公開しています。詳細については、次の URL をご参照ください。

フィッシング対策協議会 Web ページ
https://www.antiphishing.jp
フィッシング対策協議会 2012 年 1 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201201.html
フィッシング対策協議会 2012 年 2 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201202.html
フィッシング対策協議会 2012 年 3 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201203.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. 早期警戒情報フィールドレポート

【第 1 回】財団法人地方自治情報センター (LASDEC) ～厳選された情報が全国の地方公共団体の現場で役立っている ～

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、実際の組織や企業において具体的にどのように活用されているかをインタビュー記事として紹介しています。

【第 1 回】財団法人地方自治情報センター (LASDEC)
～厳選された情報が全国の地方公共団体の現場で役立っている～(2012 年 3 月 8 日)
https://www.jpcert.or.jp/magazine/security/fieldww-lasdec.html

8. 講演活動一覧

(1) 山本 健太郎 (早期警戒グループ 情報セキュリティアナリスト) :
「最新のフィッツシングの現状と企業側の対策」
日本クレジットカード協会（JCCA), 2012 年 1 月 26 日
(2) Jack YS LIN (早期警戒グループ 情報セキュリティアナリスト) :
「中国の今そこにある情報セキュリティ危機」

日本クレジットカード協会（JCCA),2012 年 1 月 26 日

(3) 村上 憲二(総務部部長),竹田 春樹(分析センター 情報セキュリティアナリスト) :
「情報セキュリティ対策研修(基本編）」
国立保健医療科学院情報セキュリティ対策研修,2012 年 1 月 30 日

(4) 歌代 和正 (代表理事) :
パネルディスカッション「情報セキュリティ対策に関する官民連携について」
国民を守る情報セキュリティシンポジウム, 2012 年 2 月 2 日

(5) Jack YS LIN (早期警戒グループ 情報セキュリティアナリスト) :
「中国のセキュリティ動向関連」
SecurityDay2012, 2012 年 2 月 6 日

(6) 真鍋 敬士 (理事,分析センター長) :
「CSIRT 活動における標的型攻撃への取り組み」
サイバー情報共有のためのワークショップ, 2012 年 2 月 14 日

(7) 久保 正樹 (情報流通対策グループ 脆弱性アナリスト) :
「Java/Android セキュアコーディング入門」
Developers Summit 2012, 2012 年 2 月 17 日

(8) 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) :
「ネットワーク・サーバ管理者のための情報セキュリティ」
名古屋大学ネットワーク・サーバ管理者のための情報セキュリティ講演会
2012 年 2 月 20 日

(9) 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」
ISA 日本支部技術講演会, 2012 年 2 月 24 日

(10) 村上 憲二(総務部部長),竹田 春樹(分析センター 情報セキュリティアナリスト) :
「情報セキュリティ対策研修(基本編、事例編）」
国立保健医療科学院情報セキュリティ対策研修,2012 年 2 月 29 日

(11) 梅村 香織(国際部 渉外担当) :
「海外 CSIRT の状況」
CSIRT ワークショップ 2012, 2012 年 2 月 29 日

(12) 真鍋 敬士 (理事,分析センター長) :
パネルディスカッション「2012 年の守る側が取らなければならない対策」
IBM X-FORCE セキュリティー・フォーラム, 2012 年 3 月 7 日

(13) 早貸 淳子 (常務理事) :
「クラウドと情報セキュリティ」
SECURITY SHOW 第 8 回 情報セキュリティ文化賞記念講演会, 2012 年 3 月 7 日

(14) 早貸 淳子 (常務理事) :
「変化するサイバー攻撃への対応　～防御策を検討するためのポイントは？～」
ソフトバンク ビジネス+IT セミナー, 2012 年 3 月 22 日

(15) 鹿野 恵祐(早期警戒グループ 情報セキュリティアナリスト) :
「Observation Results in 2011- Some Highlights」
APCERT Workshop 2012 on TSUBAME Network Traffic Monitoring Project－バリ, 2012 年 3 月 25 日

(16) 鹿野 恵祐(早期警戒グループ 情報セキュリティアナリスト) :
「最近のインターネット定点観測で発見した組込み系の脆弱性」
製品開発者定期ミーティング, 2012 年 3 月 27 日

(17) Jack YS LIN (早期警戒グループ 情報セキュリティアナリスト) :
パネル「各國資安趨勢」
TWNIC 2012 網際網路趨勢研討會－台湾, 2012 年 3 月 29 日

(18) 山本 健太郎 (早期警戒グループ 情報セキュリティアナリスト) :
「フィッシング詐欺の現状～狙われる金融機関、対策として何ができるのか～」
埼玉県クレジットカード犯罪対策連絡協議会, 2012 年 3 月 29 日

9. 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),久保 正樹(情報流通対策グループ 脆弱性アナリスト) :
「Java セキュアコーディングスタンダード CERT/Oracle 版」
アスキーメディアワークス, 2012 年 1 月 27 日

(2) 戸田 洋三 (情報流通対策グループ リードアナリスト) :
「ハッシュテーブルに対する攻撃手法のはなし」
翔泳社 Codezine「Java セキュアコーディング入門(4)」, 2012 年 2 月 20 日

(3) 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 アプリにおける DB ファイルの正しい使い方」
翔泳社 Codezine「Java セキュアコーディング入門」, 2012 年 3 月 29 日

10. 開催セミナー等一覧

(1) 学生向けJavaセキュアコーディングセミナー
※本セミナーの詳細は、「2-5-2」をご参照ください。

(2) Androidセキュアコーディングセミナー
※本セミナーの詳細は、「2-5-3」をご参照ください。

(3) 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、「2-5-6」をご参照ください。

(4) 制御システムセキュリティカンファレンス2012

※本セミナーの詳細は、「2-6-1」をご参照ください。

(5) SecurityDay2012

近年インターネットは、さまざまな社会経済活動の中で広く利用されるようになりその依存性が高まる一方で、インターネットを通じたコンピュータセキュリティインシデントが頻発し、ますます増大する傾向にあります。これら脅威は社会的なリスクであり、それらを低減させるひとつの方法として、プロフェッショナルや専門家の情報共有と議論の場が必要ではないかと考え、共催5社が、情報セキュリティに関わるユーザ、運用、管理といった立場の方を対象に、参加者とともに考え議論、問題提起を行うセミナーを開催しました。

・主　　催：SecurityDay運営委員会
(日本インターネットプロバイダー協会(JAIPA)、日本データ通信協会 (Telecom-ISAC Japan)、日本ネットワークセキュリティ協会(JNSA)、日本電子認証協議会(JCAF)、JPCERT/CC)
・開催日時：2012年2月6日 10:00～17:00
・参加人数：107名

詳細については、以下の URL をご参照ください。
http://securityday.jp/

11. 後援一覧

(1) IPA 重要インフラ情報セキュリティシンポジウム 2012
(主催：独立行政法人情報処理推進機構(IPA))
2012 年 2 月 23 日
(2) 情報セキュリティシンポジウム道後 2012
(主催：情報セキュリティシンポジウム道後 2012 実行委員会)
2012 年 2 月 16 日～2 月 17 日

JPCERT CC®

■ 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