JPCERT-PR-2013-02
発行日：2013-07-11

JPCERT/CC 活動概要 [2013 年 4 月 1 日 ～ 2013 年 6 月 30 日]

活動概要トピックス

―トピック 1―
マルウエア配付サイトへの誘導を目的とする Web サイト改ざんの報告の急増

JPCERT/CC に寄せられる Web サイト改ざんの報告が急増しています。本四半期に報告された件数は 1847 件となり、前四半期の 1184 件から 56%増加しています。
JPCERT/CC で改ざんされたサイトを分析したところ、これらのサイトには、不審な iframe や難読化された JavaScript がページに挿入されており、挿入されているコードによって誘導先の URL やコメントタグなどの特徴が異なっていることが分かりました。さらに、改ざんされたサイトにアクセスした場合、アプリケーションの脆弱性を使用した攻撃を行うサイトに誘導され、古いバージョンのアプリケーションを使用している PC はマルウエアに感染する可能性が確認されました。
このような攻撃によって PC が感染するマルウエアとしては、PC 内に保存されている様々なアカウント情報を窃取するものや、PC をスパムメールの送信や DoS 攻撃の踏み台として使用するものなどを特定しています。Web サイトの管理に使用している PC が前者のマルウエアに感染すると、Web サイト管理用のアカウント情報が窃取され、それを利用して Web サイトがさらに改ざんされて、被害が拡大する恐れがあります。
JPCERT/CC では、報告に基づいて調査を行い、改ざんされたサイトの管理者等に対して対応依頼等の必要な連絡・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、注意喚起等の情報発信を行っています。
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 から依頼する調査等への対応および JPCERT/CC への情報提供にご協力をお願いいたします。

インシデントの報告
https://www.jpcert.or.jp/form/

―トピック 2―

FIRST Steering Committee メンバに JPCERT/CC 理事が再選

6 月 16 日から 20 日にかけて、FIRST (the Forum of Incident Response and Security Teams)の第 25 回年次会合がバンコクにて開催されました。FIRST は CSIRT(Computer Security Incident Response Team)をメンバとする会員組織で、**2013 年 7 月 11 日現在 60 カ国から 276 チームが参加しており、日本からの参加チーム数は 23 チームとアメリカに次いで第 2 位となっています。**

今回の年次会合では、Steering Committee の 10 名のメンバのうち 2 年の任期が満了した 5 名について改選が行われ、JPCERT/CC 理事の山口英が再選されました。Steering Committee のメンバのうち、アジア圏から選出されているメンバは山口のみであることから、日本国内の CSIRT はもとより、APCERT(Asia Pacific Computer Emergency Response Team)の活動や CSIRT 構築支援を通じて連携関係を強化してきているアジア太平洋地域やアフリカ地域のチームの FIRST 加盟の支援や、グローバルな活動を行う他の国際組織との連携に引き続き尽力することにより、FIRST をよりグローバルなフォーラムへと導き、国際連携の実効性を高めるべく貢献していきたいと考えています。

FIRST Steering Committee
http://www.first.org/about/organization/sc.html
FIRST Steering Committee "General Coordination and Organization"
http://www.first.org/about/policies/op-framework

―トピック 3―

法人における SNS 利用に伴うリスクと対策を公開

SNS(ソーシャル・ネットワーク・サービス)は、新しいコミュニケーション・ツールとして個人利用者が急拡大するとともに、企業その他の法人としての利用も増え始めています。しかしながら、従業員による利用上の不注意により、意図しないダメージが法人に及ぶ可能性もあり、法人としてのリスクの把握や対策の検討が求められています。

そこで、JPCERT/CC では、日本国内および諸外国における SNS に起因する脅威とセキュリティ対策の現状について、公表されている情報(文献・Web)を収集するとともに、国内 SNS 提供事業者およびセキュリティベンダにインタビューを行い、それらの情報を基礎として考察を加え、法人における SNS 利用に伴うリスクと対策を報告書としてまとめ、公開いたしました。法人において、SNS を安全に利用するための社内規程やポリシーを策定する際の参考資料としてご活用ください。

法人における SNS 利用に伴うリスクと対策
https://www.jpcert.or.jp/research/sns2012.html

JPCERT CC®

ートピック 4ー

セキュアコーディングの教材、Java アプリケーションの脆弱性事例解説資料を公開

JPCERT/CC では、既に、Java 言語によるセキュアなプログラムを開発するためのコーディング規約「Java セキュアコーディングスタンダード CERT/Oracle 版」(https://www.jpcert.or.jp/java-rules/)を公開しているほか、Java セキュアコーディングのセミナーで使用した講義資料の公開や、関連書籍の出版、執筆活動などを行っていますが、セキュアコーディングを学ぶ方々に向けて、新たに、「Java アプリケーション脆弱性事例解説資料」を公開いたしました。本資料では、Java 言語で書かれたアプリケーションの 5 種類の脆弱性の事例を取り上げ、脆弱性が引き起こされる経緯や、それによる影響、防止するための対策などを詳細かつ分かりやすく解説しています。自習や勉強会などの参考資料としてご活用ください。

Java アプリケーション脆弱性事例解説資料
https://www.jpcert.or.jp/securecoding/materials-java-casestudies.html

本活動は、経済産業省より委託を受け、「平成２５年度情報セキュリティ対策推進事業」として実施したものです。
ただし、「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 9386 件、インシデント件数ベースでは 9086 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 2179 件でした。前四半期の 2230 件と比較して 2%減少しています。「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、インターネット利用組織における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することを目的として活動しています。国際的な調整・支援が必要となるインシデントについては、日本における窓口組織として、国内や国外(海外の CSIRT など)の関係機関との調整活動を行っています。

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_Report20130711.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 287 件で、前四半期の 474 件から 39%減少しました。また、前年度同期(367 件)との比較では、22%の減少となりました。
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	4 月	5 月	6 月	合計 (割合)
国内ブランド	20	27	25	72(25%)
国外ブランド	62	37	41	140(49%)
ブランド不明(注 5)	25	29	21	75(26%)
月別合計	107	93	87	287(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。以前は、特定の海外無料ホスティングサービスを利用して多くのフィッシングサイトが構築されていましたが、本四半期は WordPress などの CMS(Contents Management System) を使用している海外のサーバに侵入して設置したと見られるものが多く確認されました。

5 月から 6 月にかけて、国内ゲーム会社のオンラインサービスを装ったフィッシングサイトの報告を複数受領しています。これらのフィッシングサイトのドメイン名は、正規サイトに似せたものになっており、フィッシングサイトを確認した日から遡って数日から 2 カ月以内に新しく登録されたものでした。確認したサイトの内の一つは IP アドレスが不定期に変化しており、これらの IP アドレスはいずれも国内通信事業者が割り当てる動的な IP アドレスでした。

フィッシングサイトの調整先の割合は、国内が 54%、国外が 46%であり、前四半期(国内 36%、国外 64%)と比較して、国内への調整の割合が増えました。

本四半期に報告が寄せられた Web サイト改ざんの件数は、1847 件でした。前四半期の 1184 件から 56%増加しています。

本四半期は、不審な iframe や難読化された JavaScript がページに挿入された Web サイトに関する報告が非常に多く寄せられました。改ざんされたサイトに挿入されているコードは、種類によって誘導先の URL やコメントタグなどの特徴が異なっています。改ざんされたサイトにアクセスした場合、アプリケーションの脆弱性を使用した攻撃を行うサイトに誘導され、古いバージョンのアプリケーションを使用している PC はマルウエアに感染する可能性があります。
このような攻撃によって PC が感染するマルウエアとしては、PC 内に保存されている様々なアカウント情報を窃取するものや、PC をスパムメールの送信や DoS 攻撃の踏み台として使用するものなどを確認しています。Web サイトの管理に使用している PC が情報を窃取するマルウエアに感染すると、サーバへの接続に使用する FTP アカウント情報が窃取され、管理している Web サイトのコンテンツを改ざんされてしまい、さらに被害が拡大するおそれがあります。

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：13 件　https://www.jpcert.or.jp/at/

2013-04-08　旧バージョンの Parallels Plesk Panel の利用に関する注意喚起
2013-04-10　2013 年 4 月 Microsoft セキュリティ情報 (緊急 2 件含) に関する注意喚起
2013-04-10　Adobe Flash Player の脆弱性 (APSB13-11) に関する注意喚起
2013-04-17　2013 年 4 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
2013-04-18　DNS の再帰的な問い合わせを使った DDoS 攻撃に関する注意喚起
2013-05-15　2013 年 5 月 Microsoft セキュリティ情報 (緊急 2 件含) に関する注意喚起
2013-05-15　Adobe Reader 及び Acrobat の脆弱性 (APSB13-15) に関する注意喚起
2013-05-15　Adobe Flash Player の脆弱性 (APSB13-14) に関する注意喚起
2013-06-05　ISC BIND 9 サービス運用妨害の脆弱性 (CVE-2013-3919) に関する注意喚起
2013-06-07　Web サイト改ざんに関する注意喚起
2013-06-12　2013 年 6 月 Microsoft セキュリティ情報 (緊急 1 件含) に関する注意喚起

2013-06-12　Adobe Flash Player の脆弱性 (APSB13-16) に関する注意喚起
2013-06-19　2013 年 6 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

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 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 13 件でした。

2013-04-03　IPA、「企業ウェブサイトのための脆弱性対応ガイド」を公開
2013-04-10　パスワードの設定について
2013-04-17　JNSA、「スマートフォン利用ガイドライン」を公開
2013-04-24　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 14 版
2013-05-02　25th FIRST Annual Conference、バンコクで開催
2013-05-09　Microsoft EMET v4.0 Beta テスト中
2013-05-15　IPA、「情報漏えいを防ぐためのモバイルデバイス等設定マニュアル」を公開
2013-05-22　Adobe 製品のサポート期限について
2013-05-29　「不正」なアクセスに備える
2013-06-05　Oracle Server JRE
2013-06-12　APCERT 設立 10 周年
2013-06-19　「フィッシングレポート 2013 公開」
2013-06-26　JPNIC、「インターネット歴史年表 ベータ版」を公開

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。

【DNS の再帰的な問い合わせを使った DDoS 攻撃への対応】
2013 年 2 月、シンガポールで開催された APRICOT(Asia Pacific Regional Internet Conference on Operational Technologies)で、DNS の再帰的な問合せを使用した DDoS 攻撃に関する講演が行われました。インターネットからの再帰的な問合せを許可している DNS キャッシュサーバ(以下「オープンリゾルバ」といいます。)を探し出しておき、攻撃対象の IP アドレスに送信元 IP アドレスを偽装した再帰的な問合せパケットを複数のオープンリゾルバに送信することで、巨大なサイズの応答パケットを大量に攻撃対象(Web サイトなど)に送りつけて、対象のサーバなどをサービス不能状態に陥れる DNS アンプ攻撃の事例報告です。この講演では、攻撃に使用されたオープンリゾルバの地域毎の IP アドレス数が開示され、日本の IP アドレス数が 4625 とアジア地域で最多と報告されていました。これに対し、JPCERT/CC では、攻撃に使用された IP アドレスのリストを入手し、当該 IP アドレスを保有する国内の ISP、ホスティング事業者などに個別に連絡し対処を依頼しました。
また、入手したリストが国内のオープンリゾルバ全体の一部に過ぎないことがうかがわれたため、JPNIC、JPRS と連携して、国内の組織や企業のシステム管理者に対して広く DNS サーバへの対策の実施を推奨する注意喚起を行いました。

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/

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、既知の脆弱性情報やマルウエア、攻撃ツールなどとの関連を考察することで、攻撃活動や準備活動の捕捉に努めています。本四半期において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。

本四半期に、日本国内の組織に割り当てられた IP アドレスを送信元とする、リモート管理機能が使用する Telnet サーバ用を含む複数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、スキャンや辞書攻撃などを行う不審なツールが設置されていないかどうかの確認を依頼しました。その後、当該管理者から、「攻撃者に侵入されたサーバ上で別のサーバをスキャンするための複数のツールが動作しており、サーバのログ情報が消去、改ざんされていたことも判明したため、当該サーバの運用を停止した」との連絡をいただきました。

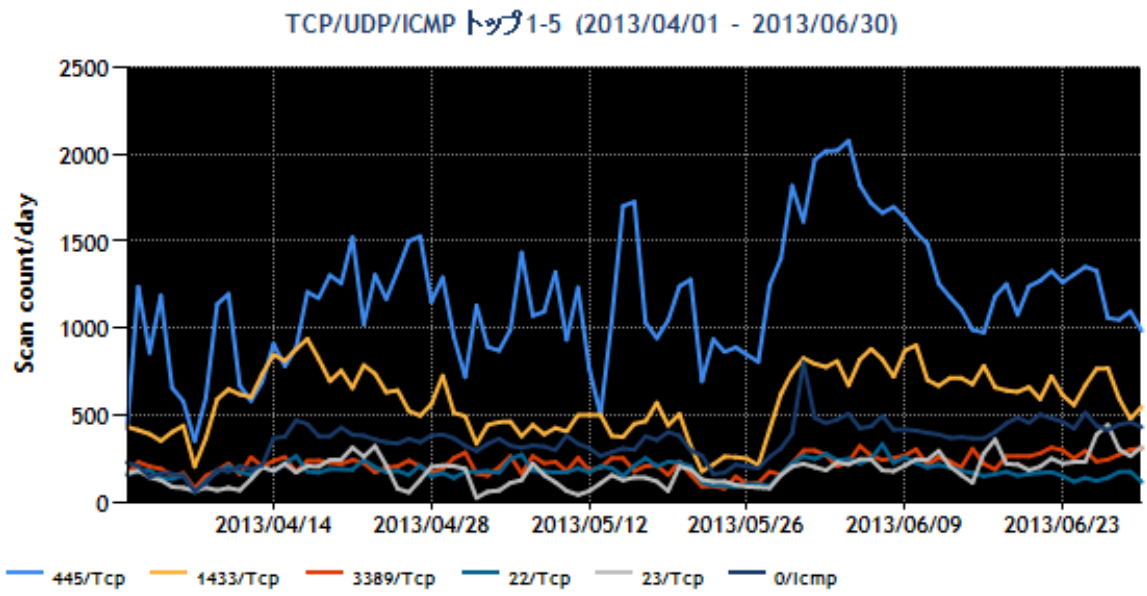
1.3.2. ポートスキャン概況

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/#examples

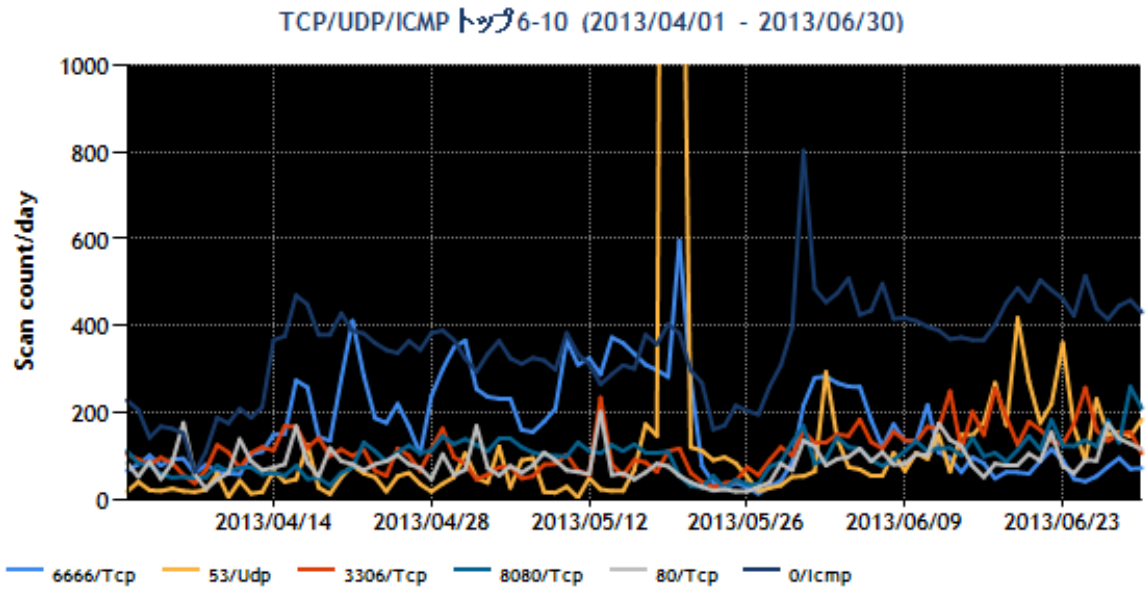
本四半期に定点観測システムで観測された宛先ポート別の上位 1 位～5 位及び 6 位～10 位のそれぞれについて、パケット数の時間的推移を[図 1-1]と[図 1-2]に示します。

- 宛先ポート別グラフ トップ 1-5 (2013 年 4 月 1 日-6 月 30 日)



[図 1-1 宛先ポート別グラフ トップ 1-5]

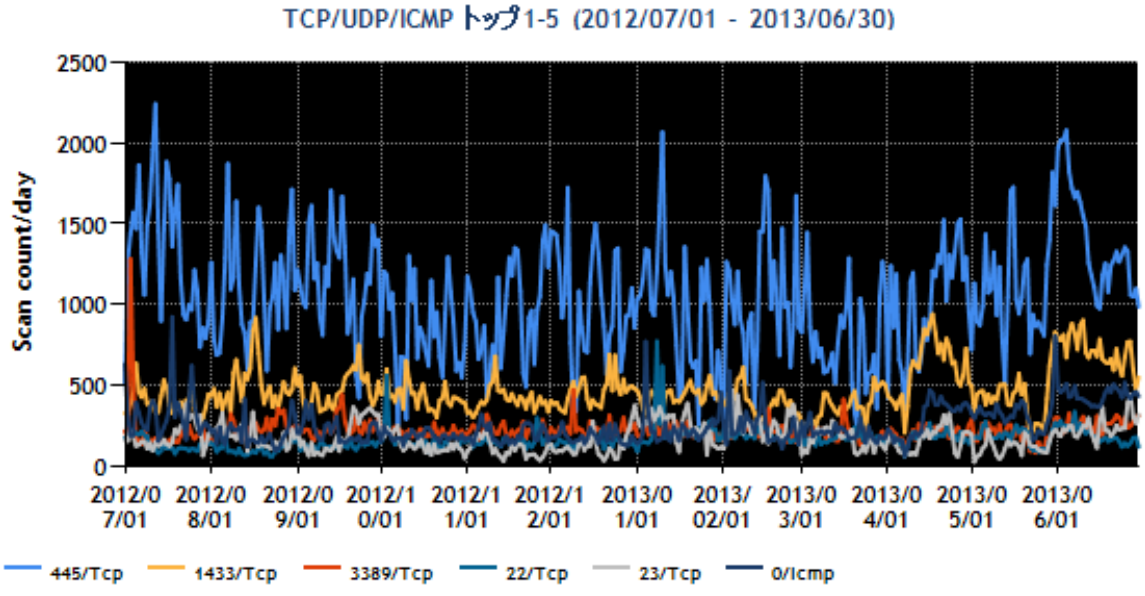
- 宛先ポート別グラフ トップ 6-10 (2013 年 4 月 1 日-6 月 30 日)



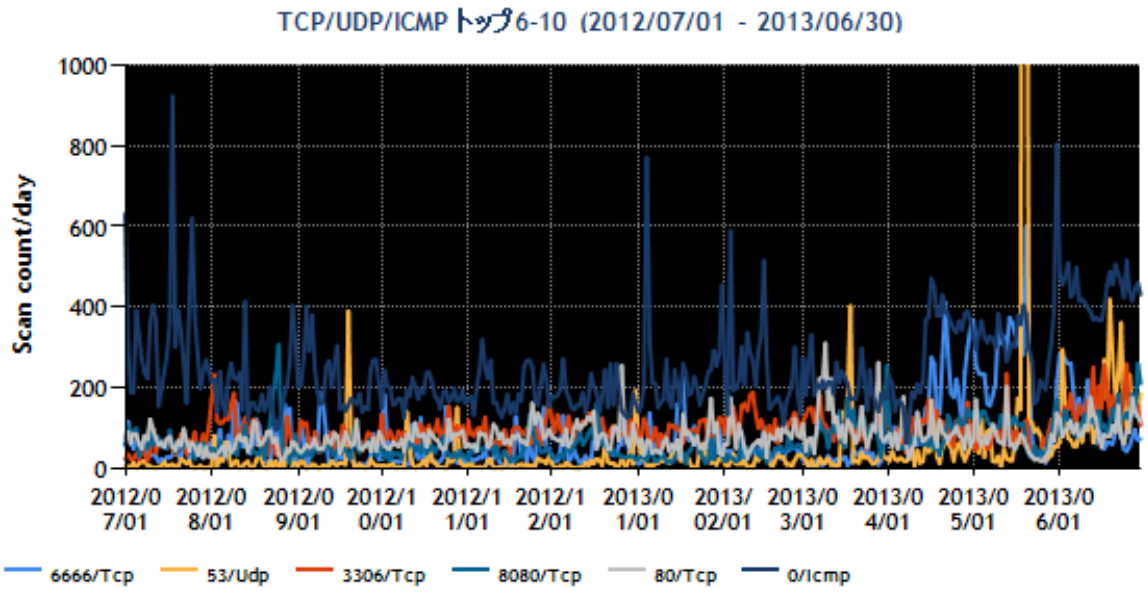
[図 1-2 宛先ポート別グラフ トップ 6-10]

また、より長期間のパケット数の推移を見るため、過去 1 年間(2012 年 7 月 1 日から 2013 年 6 月 30 日まで)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 トップ 1-5 (2012 年 7 月 1 日-2013 年 6 月 30 日)



[図 1-3 宛先ポート別グラフ top1-5]



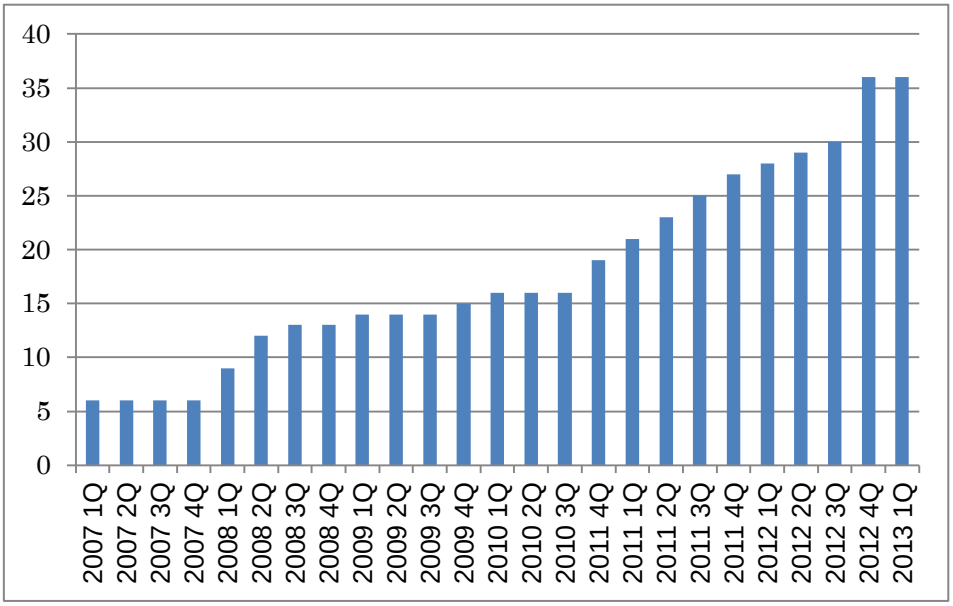
[図 1-4 宛先ポート別グラフ トップ 6-10]

順位に変動はありますが、これまでと同様、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 サーバなど遠隔操作のため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、新規加盟組織はありません。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]

4 月 15 日には、日本アイ・ビー・エム株式会社(IBM-CSIRT)の会議室をお借りして「シーサート WG」を開催しました。「シーサート WG」は NCA の会員と NCA に加盟を検討している組織の方が参加でき、2 ヶ月に 1 回程度、様々なテーマで開催しています。今回の参加人数は約 90 名で、今年 3 月に発生した「韓国大規模サイバー攻撃」について NCA 会員である株式会社アンラボ(AhnLab CIRT)が報告を行い、その後に参加した組織がチームに分かれて、日本で同様の攻撃が起きた場合、どのような影響が出るのかについてディスカッションをしました。

5 月 24 日には、株式会社ディー・エヌ・エー(DeNA CERT)の会議室をお借りして「CSIRT フォーラム 2013」を開催しました。フォーラムへの参加人数は約 70 名でした。「CSIRT フォーラム 2013」では、内閣官房情報セキュリティセンター(NISC)総合対策担当参事官を特別講師としてお招きし、セキュリティインシデントに対する政府の対応方針をご講演いただきました。また、各メンバが CSIRT としての日々の活動内容と活動環境を発表しました。「CSIRT フォーラム 2013」の詳細については、次の URL をご参照ください。

CSIRT フォーラム 2013 -これから CSIRT を構築したい方々へ- 開催のご案内
http://www.nca.gr.jp/2013/csirt-forum/index.html

6 月 10 日には、LINE 株式会社(LINE-CSIRT)の会議室をお借りして「TRANSITS Workshop NCA Japan」を開催しました。参加人数は約 30 名でした。TRANSITS とは、CSIRT の設立の促進、既存の CSIRT の対応能力向上を目的としてヨーロッパで開発された教育プログラムです。その教育プログラムを日本で開催したのが「TRANSITS Workshop NCA Japan」です。「TRANSITS Workshop NCA Japan」の詳細については、次の URL をご参照ください。

TRANSITS Workshop NCA Japan
http://www.nca.gr.jp/2013/transits/index.html

日本シーサート協議会の活動の詳細については、次の URL をご参照ください。

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

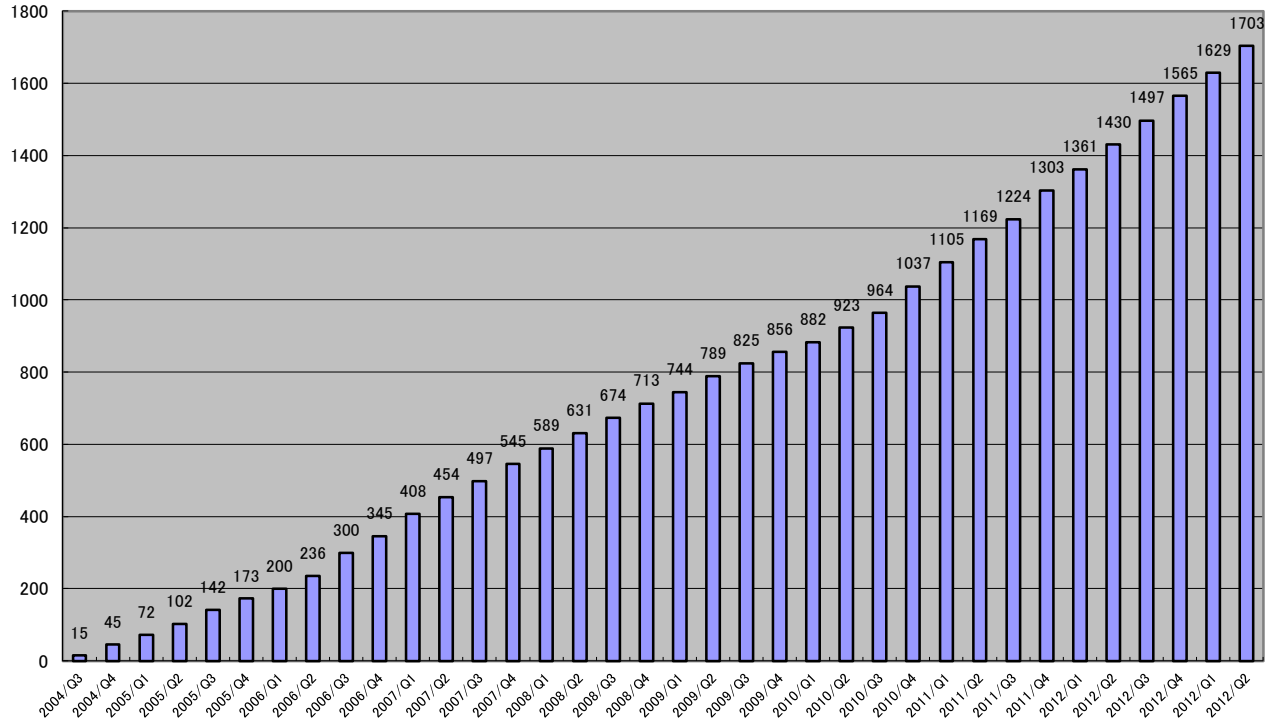
2. 脆弱性関連情報流通促進活動

JPCERT/CC は、ソフトウエア製品利用者の安全確保を図ることを目的として、発見された脆弱性情報を適切な範囲に適時に開示して製品開発者による対策を促進し、用意された対策情報と脆弱性情報を脆弱性情報ポータル JVN (Japan Vulnerability Notes ; 独立行政法人情報処理推進機構(IPA)と共同運営)を通じて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」に従って、対象となる脆弱性に関係する製品開発者の特定、脆弱性関連情報の適切な連絡、開発者による脆弱性の検証などの対応や脆弱性情報の公表スケジュール等に関する調整を行い、原則として、調整した公表日に JVN を通じて脆弱性情報等を一般に公表しています。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 74 件(累計 1703 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/

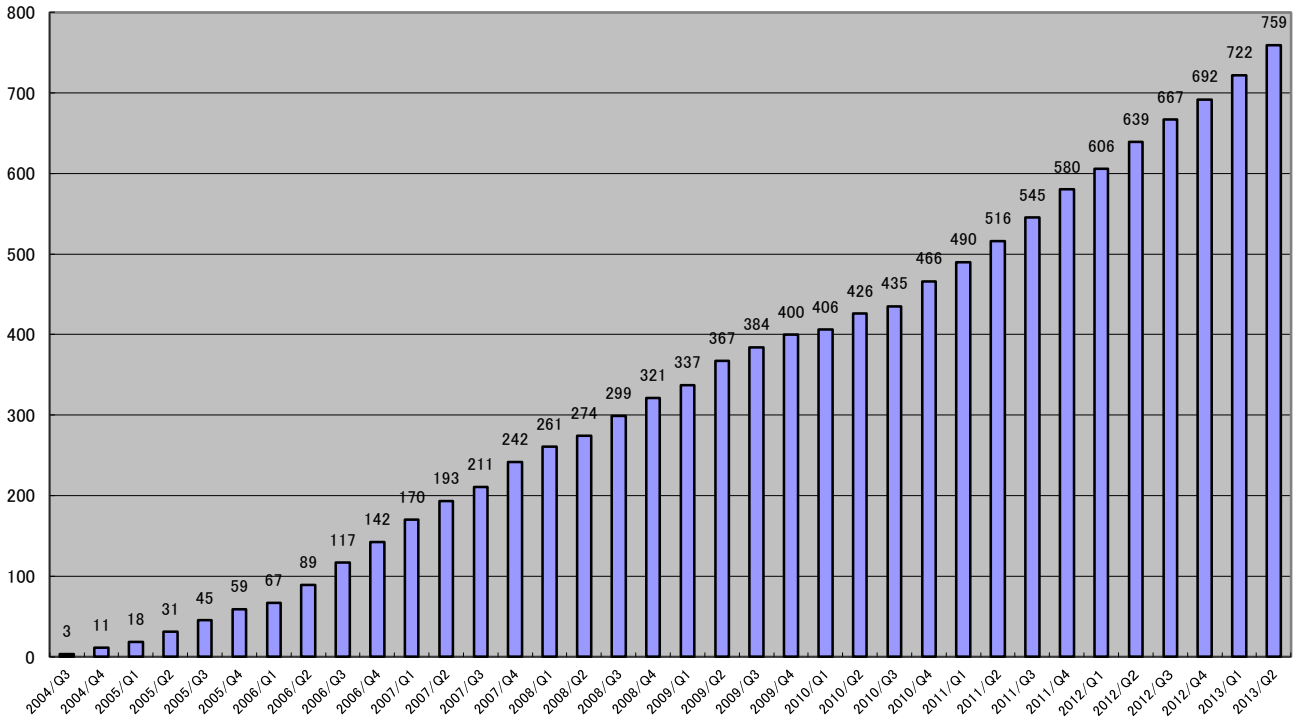


[図 2-1　JVN 公表累積件数]

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 37 件(累計 759 件)で、累計の推移は[図 2-2]に示すとおりです。37 件うちの 7 件(約 19%)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 向けウェブブラウザに関する脆弱性情報を 5 件、Android 向けアプリケーションに関する脆弱性情報を 4 件、携帯電話向けソフトウエアに関する脆弱性情報を 1 件、携帯電話およびモバイル機器の接続設定用ソフトウエアに関する脆弱性情報を 1 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 32%を占めました。

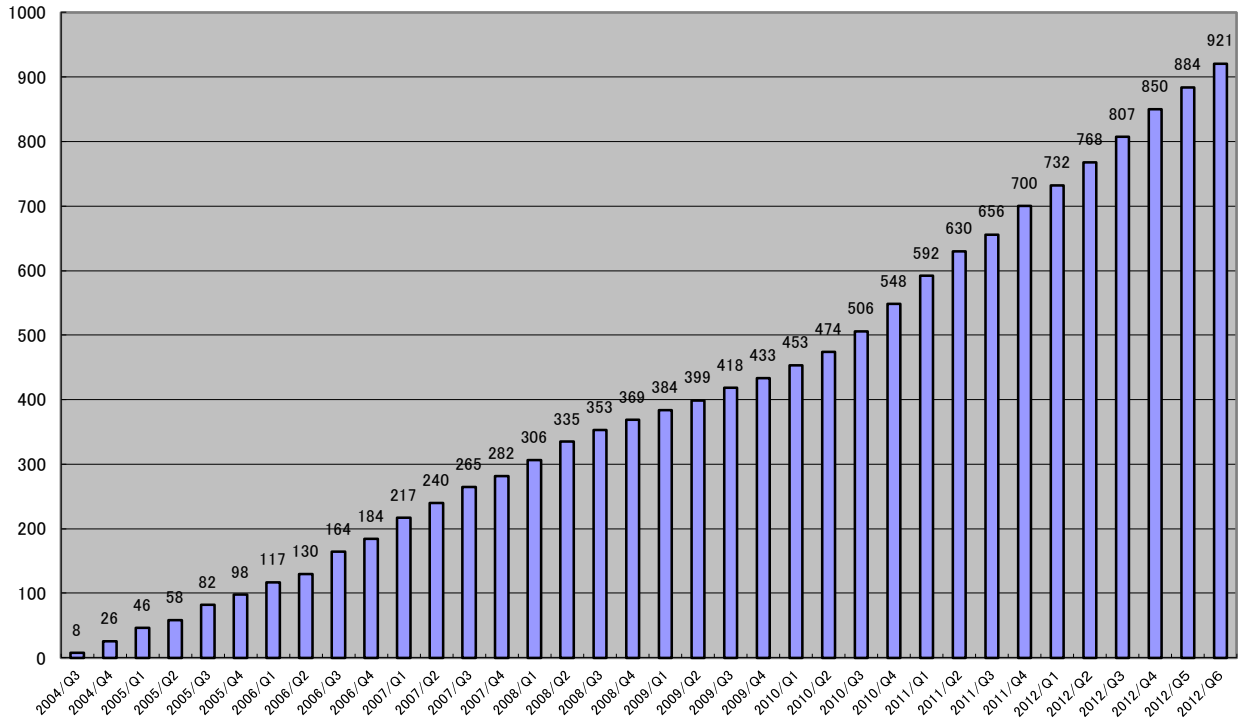
また、E コマース製品に関する脆弱性情報を 9 件、ウェブブラウザに関する脆弱性情報を 3 件、データベース製品に関する脆弱性情報を 2 件公開しました。なお、本四半期においては、製品開発者が自社製品の脆弱性情報を直接 JPCERT/CC に報告してくださったものが 4 件あり、いずれも迅速なご対応をいただき、速やかに JVN にて脆弱性情報を公開するに至りました。JPCERT/CC は、今後も引き続き国内外の関係者との調整を行い、脆弱性問題への速やかな対応の促進に努めてまいります。



[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、37 件(累計 921 件)で、累計の推移は[図 2-3]に示すとおりです。37 件のうち 5 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、Microsoft 製品に関する月例パッチの注意喚起が 3 件、Oracle の 4 半期パッチ Critical Patch Update(CPU)が 2 件でした。

また、US-CERT の脆弱性注意喚起以外の 32 件は、Microsoft Internet Explorer のゼロデイ脆弱性に関する注意喚起が 1 件、Oracle Javadoc の注意喚起が 1 件、Apple による自社製品に関する脆弱性情報の届け出によるものが 4 件などで、全体として、Adobe、マイクロソフト、HP(Hewlett Packard)、IBM 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。



[図 2-3　国際取扱脆弱性情報の公表累積件数]

2.2.　連絡不能開発者とそれに対する対応の状況

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、脆弱性が報告されたものの、調査と対策をしていただくべき製品開発者と連絡が取れない場合には、2011 年度より JVN 上で「連絡不能開発者一覧」として、当該製品開発者名を掲載することになりました。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、「滞留案件」の解消に一定の効果をあげています。

本四半期は、新たに掲載した製品開発者名はなく、前四半期に公表した連絡不能製品開発者情報に対し、さらに製品名およびバージョン名(案件数としては 3 件)を追加情報として掲載しました。連絡不能開発者一覧の公表から約 1 年 9 ヵ月が経過した本四半期末日時点で、合計 106 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。

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ており、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、脆弱性情報ハンドリングを行っている、米国の CERT/CC、英国の CPNI、フィンランドの CERT-FI などの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。増加傾向にある Android 関連の脆弱性の調整活動の中では、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 との連携も増えており、国際連携活動の幅が一層広がっています。

JVN 英語版サイト(https://jvn.jp/en)での脆弱性情報の公表も、日本語版とほぼ同時に公表しており、取扱脆弱性情報の信頼できるソースとして、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、CNA(CVE Numbering Authorities、CVE 採番機関)として認定されています。本四半期は、JVN 上で公表した脆弱性情報のうち 34 件について JPCERT/CC が採番した CVE 識別子を掲載しています。JVN 上で公表する脆弱性に CVE 識別子を付与し始めた 2008 年以降においては、1 割弱を占める 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て、ほぼすべてに CVE 識別子を付与しています。

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/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

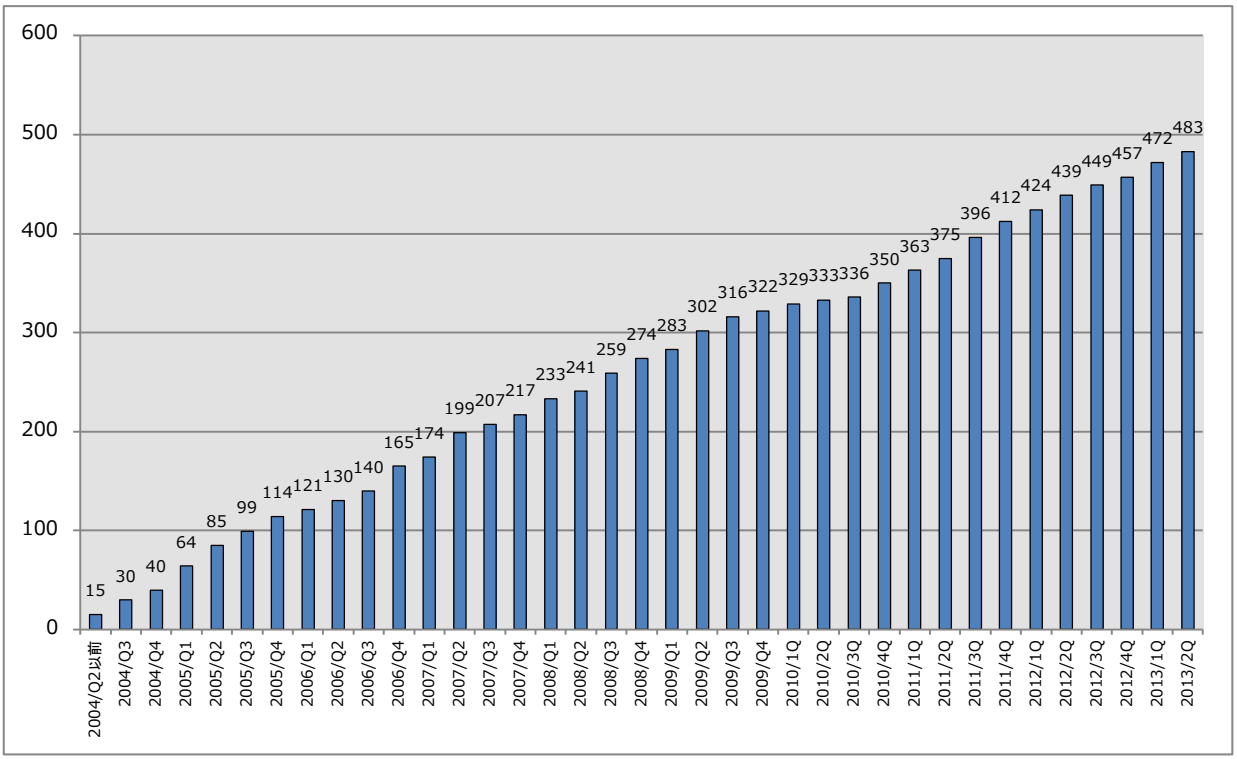
本基準では、受付機関に IPA、調整機関に JPCERT/CC が指定されています。JPCERT/CC は IPA が受け付けた届出情報の転送を受けて、製品開発者への情報提供を行い、対策情報公開に至るまでの調整を行っています。最終的には、 IPA と共同で、脆弱性情報ポータル JVN において対策情報を公開しています。両組織間においては、脆弱性情報の分析結果や脆弱性情報の取扱い状況等の情報交換を行うなど、緊密な連携を行っています。なお、本基準における IPA の活動および四半期毎の届出状況については、次の URL をご参照ください。

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 6 月 30 日現在で 483 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. 組込システム開発技術展(ESEC)で講演

5 月 8 日から 10 日に東京ビッグサイトで開催された組込システム開発技術展において、脆弱性解析チームの熊谷裕志が「Android セキュアコーディング～Android アプリケーション開発における注意すべきポイント～」と題した講演を行いました。

Android を搭載するスマートフォンの普及とともにそれ以外の分野でも Android が注目され、組込みの分野でもテレビや冷蔵庫、カメラといった伝統的な家電製品に加えて家庭用ロボット等にも Android が搭載され始めています。応用範囲の拡大に伴って、アプリ開発の容易さから多くのディベロッパーが開発に参入し多くのアプリがリリースされる一方で、セキュリティ上の欠陥である脆弱性を抱えるアプリも多数報告されています。本講演では、Android におけるセキュリティの考え方や脆弱性を作り込んだアプリの実例を取り上げ、セキュアなアプリ開発を実践するためのポイントを紹介しました。

2.5.2. JSSEC 刊「Android アプリのセキュア設計・セキュアコーディングガイド」の改訂に協力

JPCERT/CC は、日本スマートフォンセキュリティ協会(JSSEC)の技術部会による「Android アプリのセキュア設計・セキュアコーディングガイド」の作成に協力しています。解析チームの熊谷裕志が執筆に協力した「4.10 WebView を使う」を含む複数の新たな項目を追加した同ガイドの最新版が 2013 年 4 月 23 日に公開されました。

JPCERT/CC が協力した部分で論じられた WebView に関しては、特に多数の脆弱性が報告されており、海外の研究者が問題点を指摘しています。そうした落とし穴を避けるため、開発者は WebView について何が問題なのかを十分に把握しておく必要があります。このようにセキュアな Android アプリを開発するためには、フレームワークの特徴を開発者が正しく理解して使いこなすことが不可欠です。安全な Android アプリ開発のための手引きとして、下記のガイドをぜひご活用下さい。

Android アプリのセキュア設計・セキュアコーディングガイド
http://www.jssec.org/report/securecoding.html

2.5.3. C/C++セキュアコーディングセミナー@Bali を開催

インドネシアのバリで C/C++ セキュアコーディングセミナーを開催しました。このセミナーは、インドネシア国内の大学が参加する Academic CSIRT のイベントの一部として企画されたもので、Academic CSIRT および会場となった大学 STICOM Bali の協力のもと、5 月 14 日、15 日の 2 日間にわたり、文字列および整数のトピックに関するセミナーを開催しました。

現地の大学の学生や講師を中心に 80 名ほどの参加者が集まり、各トピックの講義と演習問題に取り組みました。休み時間に講義内容に関する質問をしてくる参加者がいる一方で、Java は知っているけれど C や C++のプログラミングは学習しはじめたばかりという参加者もおり、一部の参加者にとっては講義の

内容をその場で理解することは難しかったかもしれません。しかし、演習の時間には、友人などと相談しながら解答を考えたり、講師の解説で 4 択問題の正解に一喜一憂したりとそれなりにセミナーを楽しんでいる様子も見受けられ、将来必要となるセキュアコーディングへの手がかりを示すことはできたと考えています。

[図 2-5 セミナーの様子]

2.5.4. Java セキュアコーディング連続セミナー@東京の講義資料を公開

2012 年 9 月から 12 月にかけて開催した「Java セキュアコーディング連続セミナー@ 東京」の講義資料を公開しました。

Java セキュアコーディングセミナー資料
https://www.jpcert.or.jp/securecoding/materials-java.html

講義資料は次の 4 つのモジュールから構成されており、各モジュールに、セキュアコーディングのテクニックや関連する脆弱性を解説する講義用スライドと、簡単な実習課題とその解説スライドが用意されています。対象としては Java プログラミングの初級者を想定しており、自習用の資料として利用するほか、グループでの勉強会の教材としても活用いただけます。

1. オブジェクトの生成とセキュリティ
2. 数値データの取扱いと入力値検査
3. 入出力(File,Stream)と例外時の動作
4. メソッドとセキュリティ

2.5.5. Java アプリケーションの脆弱性事例解説資料を公開

セキュアコーディングを学ぶための教材として活用していただくことを目的として、Java 言語で書かれたアプリケーションの脆弱性事例に関する以下の解説資料を公開しました。

1. Apache Sling におけるサービス運用妨害(無限ループ)の脆弱性 (CVE-2012-2138)
2. Apache Struts2 における任意の Java メソッド実行の脆弱性 (CVE-2012-0838)
3. Blojsom におけるクロスサイトスクリプティングの脆弱性 (CVE-2006-4829)
4. MySQL Connector/J における SQL インジェクションの脆弱性(JVN#59748723)
5. JBoss Application Server におけるディレクトリトラバーサルの脆弱性 (CVE-2006-5750)

セキュアな Java アプリケーションの開発を目指すには、すでに知られている脆弱性の具体例を理解し、それを反面教師として同じ失敗を繰り返さないようにすることが重要です。

Java 言語によるセキュアなプログラムを開発するためのコーディング規約「Java セキュアコーディングスタンダード CERT/Oracle 版」(https://www.jpcert.or.jp/java-rules/)や、Java セキュアコーディングのセミナー資料とともに、本資料を自習や勉強会などの参考資料としてご活用ください。

Java アプリケーション脆弱性事例解説資料
https://www.jpcert.or.jp/securecoding/materials-java-casestudies.html

2.5.6. 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、次の記事を執筆しました。

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(4)」
「見落としがちな整数関連の脆弱性 (前編) (1/2)」(公開： 5 月 16 日、執筆：久保正樹)
http://www.atmarkit.co.jp/ait/articles/1304/26/news010.html

2.5.7. 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。

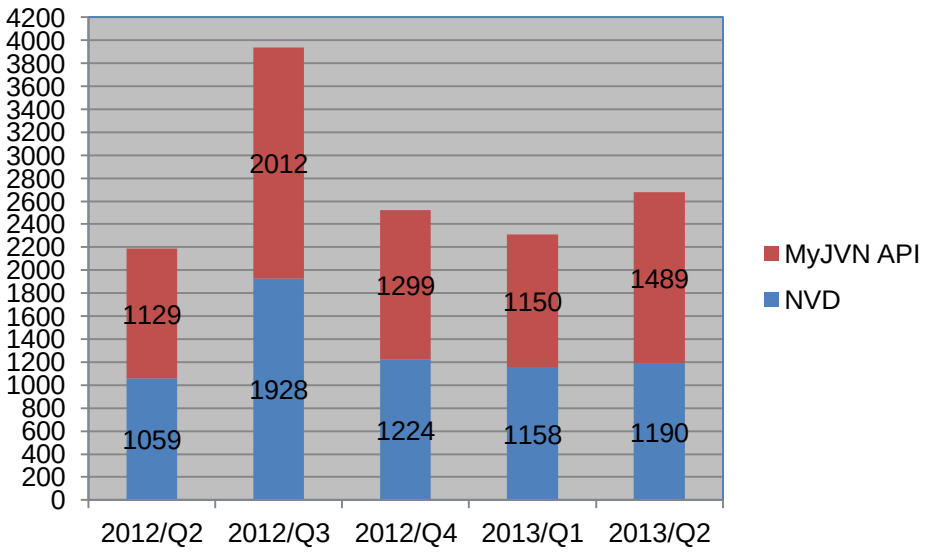
※出張セミナーのご依頼、お問合せは、secure-coding@jpcert.or.jp までご連絡下さい。

2.6. VRDA フィードによる脆弱性情報の配信

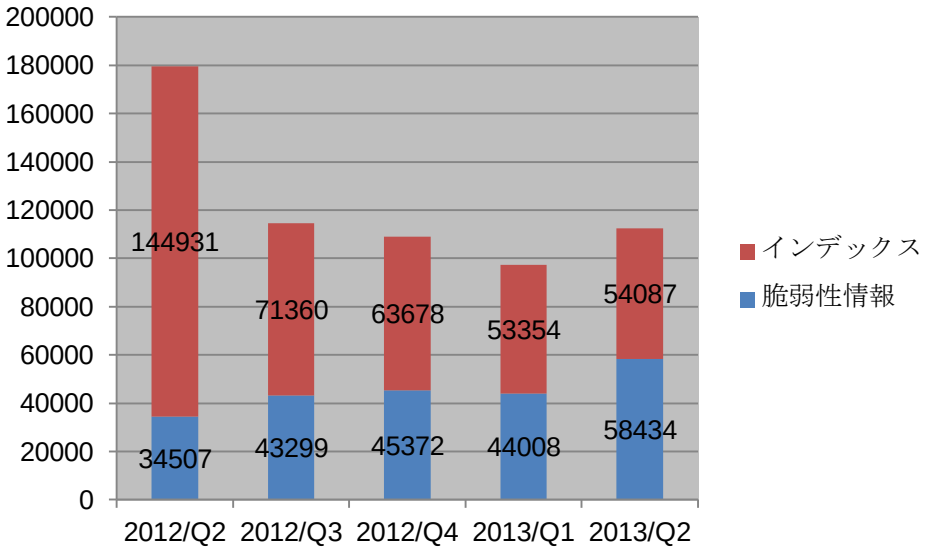
JPCERT/CC は、大規模組織の組織内 CSIRT などでの利用を想定して、KENGINE などのツールを用いた体系的な脆弱性対応を可能とするため、IPA が運用する MyJVN API および NIST (National Institute of Standards and Technology)の NVD (National Vulnerability Database) を外部データソースとして利用した、VRDA (Vulnerability Response Decision Assistance)フィードによる脆弱性情報の配信を行っています。VRDA フィードについての詳しい情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

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

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 2-6] に、VRDA フィードの利用傾向を [図 2-7] と [図 2-8] 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 2-8] 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。

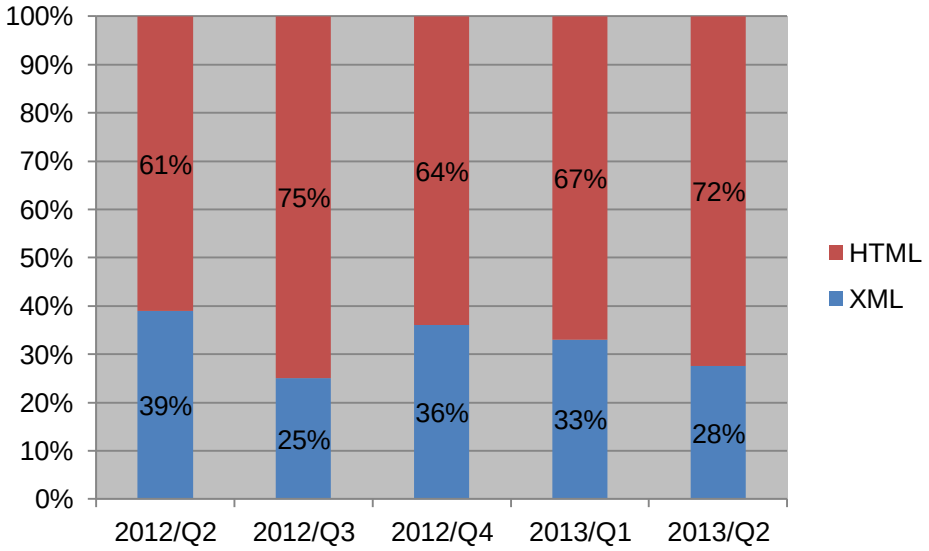


[図 2-6 VRDA フィード配信件数]



[図 2-7 VRDA フィード利用件数]

[図 2-7] に示したように、前四半期と比較して VRDA フィードインデックスの利用数に大きな変化は見られませんでしたが、脆弱性情報の利用数は約 30%の増加が見られました。



[図 2-8 脆弱性情報のデータ形式別利用割合]

[図 2-8] 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. サイバー攻撃解析協議会への参加

総務省と経済産業省の下で情報通信研究機構(NICT)と情報処理推進機構(IPA)、テレコム・アイザック推進会議、JPCERT/CC の 4 組織をメンバとして昨年 7 月に発足したサイバー攻撃解析協議会の第 2 回会議が 4 月 19 日に開かれ、昨年度の活動報告と、今後の活動内容の提案が行われました。協議会では、今後もメンバ組織が連携することで、複数の視点でサイバー攻撃を分析・把握し、各組織の活動を通して社会に還元する取組みを行っていきます。JPCERT/CC では、報告いただいた情報や収集した情報のうち、報告者から承諾が得られたものについて協議会で共有することにより、他の情報との組合せや異なる視点での分析から得られる知見を発掘する活動を進めています。

サイバー攻撃解析協議会
http://www.meti.go.jp/committee/kenkyukai/shoujo/cyber_attack/002_haifu.html

4. 制御システムセキュリティ強化に向けた活動

4.1. 情報発信活動

制御システムセキュリティインシデントに関わる事例や標準の動向、その他の技術動向に関するニュースなどを収集し、JPCERT/CC からのお知らせとともにまとめ、制御システム関係者向けにニュースレターとして提供しています。本四半期は計 3 回(4 月 30 日、5 月 31 日、6 月 28 日)配信しました。

本ニュースレター配信先の制御システムセキュリティ情報共有コミュニティについては、現在 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。参加資格や申込み方法については、次の URL をご参照ください。

制御システムセキュリティ情報共有コミュニティ
https://www.jpcert.or.jp/ics/ics-community.html

4.2. 制御システム関連のインシデント対応および情報収集分析活動

本四半期に制御システムに関連するとして報告されたインシデントの件数は 1 件でした。
また、本四半期の情報収集分析活動の中で収集し分析した情報は 489 件でした。これらの中から、国内の制御システム関係者にとって耳新しく、知っておくべき情報を厳選した上でニュースレターにて配信しました。

4.3. 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。

4.4. 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 8 件、J-CLICS に関しては 60 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 146 件、J-CLICS が 151 件となりました。

4.5. 講演活動

5 月 23 日に東京で行われたベライゾン・グローバルリスクセミナーにおいて「今求められる制御システムセキュリティへの取り組みと体制」、5 月 28 日に宮城県多賀城市の制御システムセキュリティセンター東北多賀城本部(CSS-Base6)開所記念シンポジウムのパネルディスカッション「制御システム セキュリティと国際連携」の中で「Activities of ICS Security in JPCERT/CC」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。4 月下旬にソフィア・アンチポリス (フランス)にある ETSI で SC27 の国際会議が開催され、その中で両標準案の改訂が検討されました。JPCERT/CC からも、日本代表団の一員としてこの会議に参加しました。
「脆弱性情報の開示」については、国際標準草案(DIS : Draft of International Standard)の段階まで策定が進み、2012 年 9 月 25 日～12 月 25 日に国際投票が行われた結果、賛成が 27 ヶ国、反対が 3 ヶ国(日米英)、棄権が 19 ヶ国となり、再度改訂して投票に付すことが承認されています。今回の国際会議では、前述の投票に付随して提出された、草案の修正を求める合計 188 件のコメント(日本から 35 件、米国から 15 件、英国から 7 件、カナダから 106 件、メキシコから 25 件)の取扱いを審議し、草案の改訂方法を決めました。それを受けてエディタに指名されているカナダの委員が本標準の改訂作業を行い、メーリングリストで関係者の非公式チェックを受けた後、SC27 事務局を通じて国際標準最終草案(FDIS : Final draft

of International Standard)として国際投票に付すことになりました。
遅れて開発がスタートした「脆弱性取扱手順」についても、国際標準草案(DIS： Draft of International Standard)の段階まで策定が進み、2013 年 1 月 14 日～4 月 14 日に国際投票に付されていました。投票結果は、賛成 22 ヶ国、反対無し、棄権 20 ヶ国で、ただちに国際標準とすべきものとして承認されました。投票に付随して合計 8 件(日本から 3 件、ルクセンブルグから 1 件、英国から 5 件)のコメントがありましたので、今回の国際会議では、その取扱について審議し改訂方法を決めました。これを受けてエディタに指名されている米国の委員が改訂作業を行った後に, できるだけ速やかに国際標準として発行する手続きを取ることになりました。
2008 年 4 月から始まった標準策定作業について、JPCERT/CC では 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、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きましたが、その策定作業も最終段階となりました。

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 JTC-1/SC27 の WG4 では、情報セキュリティインシデント管理に関する国際標準 27035:2011 を下記の 3 つの標準から成るマルチパート標準へと改訂する作業が進められています。

27035-1. インシデント管理の原理
(Principles of Incident Management)
27035-2. インシデント対応の計画と準備のためのガイドライン
(Guidelines to Plan and Prepare for Incident Response)
27035-3. インシデント対応の運用のためのガイドライン
(Guidelines for Incident Response Operations)

JPCERT/CC は 27035:2011 の策定段階からこの標準化活動に関わっており、今四半期は 4 月下旬にソフィア･アンチポリス(フランス)で開催された SC27 の国際会議に日本の代表団の一員として参加しました。インシデント管理の原理を規定する 27035-1 については、27035 の全体像を提示するパートとして位置づけられることから、用語や概念の統一、インシデント管理全体の構成要素を示す図やインシデント対応の流れを示すモデル等に対する意見を中心とする 82 件のコメントが寄せられ(日本は 10 件のコメントを提出)、活発な議論が行われました。他の 2 つのパートの章構成等にも影響を与える指摘が少なくないため、コメントの多くは受け入れられたものの、いったんエディタが宿題として持ち帰って各国の提案をとりまとめた文案を作成し、電話会議による非公式の議論と合意を得た上で、次期草案として ISO 事務局に提出されることになりました。
インシデント対応の計画と準備のガイドラインを規定する 27035-2 については、エディタが急遽辞任したことを受け、FIRST のリエゾンを務める Damir Rajnovic 氏がエディタに就任しました。草案にまだ歯抜けの章が散見される段階であり、会議では各国のコメントを元に記述すべき内容の方向性を議論するにとどまり、歯抜け箇所についてはエディタが方向性を踏まえた草案を用意するという重い作業を引き受ける結果となりました。
インシデント対応のオペレーションのガイドラインとなる 27035-3 については、最も多い 102 件のコメントが寄せられました(日本からのコメントは 25 件)。パート 1 との用語や概念、モデルの統一、ネット

ワーク侵入のみをベースに記述されているインシデント対応オペレーションのモデルの見直し等に関するコメントの多くは受け入れられましたが、パート 1 と同様、エディタが各国の提案を取り込んだ文案を非公式の電話会議の場で議論し、参加者の合意を得た上で、次期草案にまとめられることになりました。27035 全体では、5 名のエディタが新任され、パート 2 のエディタを兼任する形でオーストラリアの Geoff Clarke 氏が 27035 のプロジェクトエディタを務めることになりました。全てのパートは作業文書の第 3 版に進むことで合意が得られました。
JPCERT/CC では、インシデントの管理と対応に関連した 3 つの国際標準について、SC27 国際会議への参加ならびに日本の標準化組織である情報規格調査会を通じて、引き続き、この国際標準が我が国の CSIRT の取組みと整合性のとれたものとなるよう努めていく所存です。

6. 国際連携活動関連

6.1. 海外 CSIRT 構築支援および運用支援活動

海外の National CSIRT (Computer Security Incident Response Team) 等のインシデント対応調整能力の向上を目指し、トレーニングやイベントでの講演等を通じた CSIRT の構築・運用支援を行っています。

6.1.1. アフリカ CSIRT 構築支援 等(2013 年 6 月 9 日-14 日)

JPCERT/CC は、6 月にザンビアで 5 日間にわたる CSIRT トレーニングを行いました。
このトレーニングの開催を企画した AfNOG は、アフリカ諸国のインターネット運用者及び政策担当者の連携と教育を目的とする非営利組織であり、アフリカ各地で年次会議を開催し、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。今年の年次会議 AfNOG-14 は、ザンビアの ISP などのスポンサーを得て、首都ルサカで開催されました。
JPCERT/CC が担当した CSIRT トレーニングは、AfNOG-14 のトレーニングプログラムの一つとして、アジア地域との連携を促進する AAF(Africa Asia Forum on Network Research & Engineering)が主催したプログラムです。同様のトレーニングは 2010 年春から実施しており、今回で 6 回目の開催となります。
JPCERT/CC は、6 月 10 日から 14 日までのトレーニングの間、講師として講義を行うだけでなく、アフリカ人インストラクターの指導を行いました。5 日間の日程の 3 日間が、過去のトレーニングを修了したアフリカ人が講師を務めるトレーニングに充てられ、2 日間は JPCERT/CC がネットワークフォレンジックおよびインシデントハンドリングに関するトレーニング(図 6-1 を参照)を行いました。このトレーニングは、約 13 名のインターネット運用者及び政策担当者が受講しました。

[図 6-1 トレーニングの模様]

AfNOG 及び CSIRT トレーニングと AAF についての詳細は、次の URL をご参照下さい。

AfNOG 及び AfNOG 14 公式ページ
http://www.afnog.org/afnog2013/index.php
AAF(Africa Asia Forum on Network Research & Engineering)
http://www.africaasia.net/

現在でも制度や技術が成長段階にある国・地域などからの攻撃が日本のインターネットユーザにとっての脅威の一つとなっています。今後急速なインターネット普及が予想されているアフリカ地域に起因するインシデントが併せて増えることが予想され、JPCERT/CC は、そのような事態が発生した際に迅速かつ円滑な対応ができるよう、同地域との連携強化の基盤づくりに努めています。

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(現在 3 期目)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

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

6.2.1.2. APCERT と他組織間との連携

APEC TEL 47 SPSG への参加(2013 年 4 月 24 日)
APEC 地域の情報電気通信分野を担当する政府機関を中核とするワーキンググループである APEC TEL (APEC Telecommunications and Information Working Group) の会合がインドネシアのバリで開催されました。その中の Security and Prosperity Steering Group (SPSG) 会合において、JPCERT/CC は APCERT を代表して APCERT の活動実績や今後の方向性をテーマとした発表を行いました。

6.2.2. 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/

6.2.2.1. 25th Annual FIRST Conference Bangkok への参加(2013 年 6 月 16 日-21 日)

FIRST の第 25 回年次会合が 6 月 16 日から 21 日までバンコクで開催されました。本会合は、サイバーインシデントの予防、対応、技術分析等に関する最新情報の交換、および国や文化等の壁を越えたインシデント対応チームの連携強化を目的に毎年開催されており、今年は “Incident Response: Sharing to Win” のテーマのもと、様々な話題が取り上げられました。JPCERT/CC は 6 月 17 日の「Global Disaster Recovery」と題したパネルセッションのモデレーターを務めました。
そのほか、JPCERT/CC では、この機会を利用して、アジア太平洋地域や欧州各国の National CSIRT や今回の会合からはじめて参加した CSIRT などとの個別の意見交換や、APCERT 加盟 CSIRT が集う意見交換会を企画/主催するなど、国際間の CSIRT 連携をさらに強化させるための様々な活動も併せて行いました。
このような会合への参加を通じて、各地域間の情報共有を促進し、信頼関係を醸成して、国際間でのインシデント対応調整がより円滑に進められるよう今後も努めてまいります。第 25 回 FIRST 年次会合につい

ての詳細は、次の URL をご参照ください。

25th Annual FIRST Conference Bangkok
http://conference.first.org

6.2.3. FIRST AGM 出席と Steering Committee メンバ再選

JPCERT/CC の理事 山口英が 6 月 16 日にバンコクで開催された FIRST の Steering Committee にメンバとして出席し、FIRST の運営方針に関する議論に参加しました。
FIRST では Steering Committee メンバの任期を 2 年後の年次会合までと定めており、山口は今年の年次会合で任期を満了しましたが、6 月 20 日に開催された年次会合において執り行われた選挙の結果、再選を果たし、さらに 2 年間 FIRST の運営に関与することになりました。FIRST Steering Committee のメンバ構成については、次の URL をご参照ください。

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

6.2.4. National CSIRT Meeting への参加(2013 年 6 月 22 日-23 日)

第 25 回 FIRST 年次会合後に引き続きバンコクにて、CERT/CC が主催する National CSIRT Meeting が開催されました。世界各国の National CSIRT が一堂に会し、国を代表するインシデント対応チームとしての活動や課題を共有するとともに、共同プロジェクトや研究調査について発表や議論を行ない、今後の一層の連携強化に繋がる成果を得ることができました。JPCERT/CC は、標的型攻撃に対応するためのインシデントハンドリング業務や IT セキュリティ予防接種について発表を行いました。National CSIRT Meeting についての詳細は、次の URL をご参照ください。

National CSIRT Meeting
https://www.cert.org/csirts/national/meeting/

6.2.5. OECD セキュリティガイドラインレビュー会合への参加 (2013 年 6 月 7 日)

JPCERT/CC のスタッフが、ベルギーのブリュッセルで開催された OECD(経済協力開発機構)のセキュリティガイドラインレビュー会合(MULTI-STAKEHOLDER CONSULTATION FOR THE REVIEW OF THE OECD 2002 SECURITY GUIDELINES)に専門家として参加しました。OECD では、2002 年にセキュリティガイドラインを発表しましたが、昨今の IT の利活用の進展や情報セキュリティ上の脅威の変化等を鑑みて、2012 年より様々なステークホルダーを集めて同ガイドラインの改訂作業を進めています。

6.2.6. 覚書(MOU)締結

CSIRT 間の協調関係に明文化された基礎的な根拠を与え、また、交換される機微な情報の取り扱いルー

ルを定めるため、関係する各国の組織との間で覚書の締結を積極的に進めています。本四半期は以下の組織と MOU を更新・締結しました。

- HKCERT (香港)
- PacCERT(大洋州地域)

6.2.7. JICA 沖縄国際センターIT 研修生による実地見学の受入れ(2013 年 6 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」を受講中の研修生 11 名(ラオス、リビア、ミャンマー、ナイジェリア、ルワンダ、ツバルの政府系組織の IT 担当者等)が来訪しました。CSIRT の役割や JPCERT/CC の事業紹介、最近のインシデント動向、TSUBAME プロジェクトの紹介等を JPCERT/CC から行った後、活発な意見交換が行われ、日本および各国におけるインターネットセキュリティの状況が共有されました。

6.2.8. 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。今四半期は、5 月 22 日に中国北京航空航天大学にて、大学院教授・院生を対象に講演し、日本のセキュリティ傾向及びインシデントへの取組み状況を紹介しました。

6.2.9. 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。

Phishing Situation in Japan (2013/06/28)
http://blog.jpcert.or.jp/2013/06/phishing-trends-in-japan.html
JPCERT/CC 英語ブログ
http://blog.jpcert.or.jp/

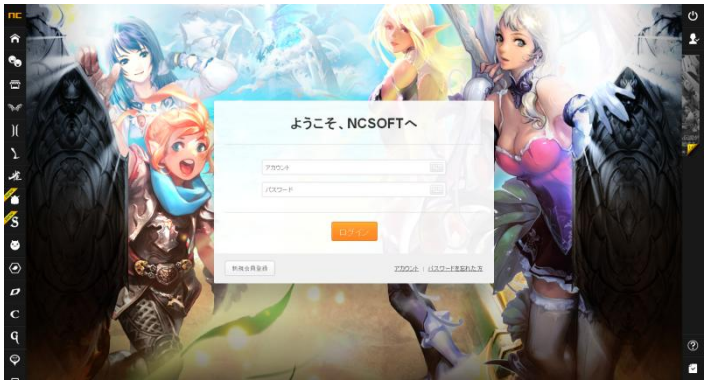
7. フィッシング対策協議会事務局の運営

JPCERT/CC は、フィッシング対策協議会(本章において「協議会」といいます。)の事務局を担当しており、経済産業省からの委託により、協議会における各ワーキンググループ活動の運営や一般消費者からのフィッシングに関する報告・問合せの受付、報告に基づくフィッシングサイトに関する注意喚起、JPCERT/CC のインシデント対応チームに対するフィッシングサイトの停止調整の依頼、国内外関連組織との共同研究などの活動を行っています。

7.1. 情報収集/発信の実績

本四半期は、協議会 Web ページや会員向け ML を通じて、フィッシングに関するニュースや緊急情報を 7 件発信しました。

本四半期は、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、オンラインゲーム事業者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本文やサイトの URL 等の関連情報を提供しました。また、Web メールサービスをかたるフィッシングに関しては「@nifty をかたるフィッシング(2013/04/05)」や「Nexyz.BB Web.Mail をかたるフィッシング(2013/05/15)」を、第二認証情報を詐取するフィッシングに関しては「新生銀行をかたるフィッシング(2013/05/29)」を、オンラインゲーム事業者をかたるフィッシングに関しては[図 7-1]の「NCSOFT をかたるフィッシング(2013/06/07)」を、それぞれ緊急情報として協議会の Web 上で公開し、広く注意を喚起しました。
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　NCSOFT をかたるフィッシング(2013/06/07)
https://www.antiphishing.jp/news/alert/ncsoft20130607.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や、関連研究の促進を期待した活動です。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 組織でした。今後と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ない、提供先を順次拡大していく予定です。

7.3. フィッシング対策ガイドラインの公開

フィッシング対策協議会のガイドライン策定ワーキンググループにおいて、フィッシングに係る技術動向や法制度の現状やあり方についてとりまとめたサービス事業者向け「フィッシング対策ガイドライン 2013 年度版」および「利用者向けフィッシング詐欺対策ガイドライン」を公開しました。

フィッシング対策ガイドライン 2013 年度版
https://www.antiphishing.jp/report/guideline/antiphishing_guideline2013.html
利用者向けフィッシング詐欺対策ガイドライン
https://www.antiphishing.jp/report/guideline/consumer_guideline2013.html

7.4. フィッシングレポート 2013 の公開

フィッシングの被害状況、フィッシングの攻撃技術・手法などをガイドライン策定ワーキンググループにおいてとりまとめ、「フィッシングレポート 2013 -フィッシング被害の社会問題化-」として公開しました

フィッシングレポート 2013
https://www.antiphishing.jp/report/wg/phishing_report2013.html

7.5. 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。本四半期は次の講演を行いました。

山本健太郎「フィッシングに関する最新動向について」
NPO 日本システム監査人協会，ＣＳＡ・ＡＳＡ継続教育セミナー 2013 年 6 月 15 日

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 4 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201304.html
フィッシング対策協議会 2013 年 5 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201305.html
フィッシング対策協議会 2013 年 6 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201306.html

8. フィッシング対策協議会会費による活動

8.1. 総会開催

本四半期においては、次のとおり、フィッシング対策協議会の平成 24 年度活動及び平成 25 年度活動計画(案)について報告等を行う総会を開催しました。

平成 25 年度フィッシング対策協議会総会
日時：2013 年 6 月 27 日 14:00 - 16:00
場所：エッサム神田ホール 301 会議室

8.2. 運営委員会開催

本四半期においては、以下のとおり、フィッシング対策協議会の活動の企画・運営方針の決定等を行う運営委員会を開催しました。

フィッシング対策協議会 第 5 回運営委員会
日時：2013 年 6 月 14 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. Java アプリケーションの脆弱性事例解説資料

本資料は、セキュアコーディングを学ぶための教材として活用していただくことを目的として、Java 言語で書かれたアプリケーションの脆弱性事例に関する解説資料です。
Java 言語によるセキュアなプログラムを開発するためのコーディング規約「Java セキュアコーディングスタンダード CERT/Oracle 版」(https://www.jpcert.or.jp/java-rules/)や、Java セキュアコーディングのセミナー資料とともに、本資料を自習や勉強会などの参考資料としてご活用ください。
本資料の詳細は、「2.5.5」をご参照ください。

Java アプリケーションの脆弱性事例解説(2013 年 6 月 27 日)
https://www.jpcert.or.jp/securecoding/materials-java-casestudies.html

9.2. Java セキュアコーディングセミナー資料

本セミナー資料は、2012 年 9 月から 12 月にかけて開催した「Java セキュアコーディング連続セミナー@ 東京」の講義資料です。

講義資料は 4 つのモジュールから構成されており、各モジュールに、セキュアコーディングのテクニックや関連する脆弱性を解説する講義用スライドと、簡単な実習課題とその解説スライドが用意されています。対象としては Java プログラミングの初級者を想定しており、自習用の資料として使う他に、グループでの勉強会の教材としても活用いただけます。
本資料の詳細は、「2.5.4.」をご参照ください。

Java セキュアコーディングセミナー資料(2013 年 6 月 27 日)
https://www.jpcert.or.jp/securecoding/materials-java.html

9.3. 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 ～ 重要インフラの包括的なセキュリティ政策に取り組む 台湾行政院

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」では、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紹介しています。今回は、台湾行政院でセキュリティ政策を担う専門家と TWCERT/CC3 名の方に、台湾の制御システムセキュリティに関する取組みについてインタビューしました。

重要インフラの包括的なセキュリティ政策に取り組む 台湾行政院(2013 年 6 月 11 日)
https://www.jpcert.or.jp/magazine/security/field-tw.html

9.4. 早期警戒情報フィールドレポート 【第 4 回】NEC-CSIRT ～ 社内セキュリティ運用部門と企業内 CSIRT との連携の強化と早期警戒情報の活用

JPCERT/CC が提供する「早期警戒情報」や「インシデント対応支援」が、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し、紹介しています。今回は、製品やサービスを多くの企業ユーザに提供している大手ベンダの NEC が、どのように情報セキュリティに取り組み、インシデントに対応する態勢をとっているのか、について企業内 CSIRT の運営に携わる 2 名の方にお話しいただきました。

【第 4 回】NEC-CSIRT
～ 2011 年以降社内セキュリティ運用部門と企業内 CSIRT との連携強化(2013 年 5 月 14 日)
https://www.jpcert.or.jp/magazine/security/fieldww-neccsirt.html

9.5. 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 2013 年 1 月～3 月　(2013 年 4 月 23 日)
https://www.jpcert.or.jp/tsubame/report/report201301-03.html

9.6. 脆弱性関連情報に関する活動報告レポート

IPA と JPCERT/CC は、ソフトウエア等脆弱性関連情報取扱基準(経済産業省告示 第 235 号)に基づき、2004 年 7 月から受付機関(IPA)や調整機関(JPCERT/CC)として脆弱性関連情報流通を行っています。本レポートは、2013 年 1 月 1 日から 2013 年 3 月 31 日までの活動実績と、本四半期に届出ないし公表された脆弱性に関する注目すべき動向についてまとめたものです。

ソフトウェア等の脆弱性関連情報に関する活動報告レポート[2013 年第 1 四半期(1 月～3 月)]
(2013 年 4 月 23 日)
https://www.jpcert.or.jp/press/2013/vulnREPORT2013q1.pdf

9.7. 経営者が知っておくべきセキュリティリスクと対応について

本報告書は、APT(Advanced Persistent Threat)による攻撃への対策について、国内の企業等でも着手していただくために、海外における攻撃事例と企業経営への影響について調査したものです。
企業経営者の方々にもご理解いただけるように、APT および APT による攻撃とはどのようなものか、CEO や経営陣にとっての脅威は何か、経営陣が果たすべき役割と責任は何かなどを解説し、脅威の発見と軽減のための 10 のステップ等を紹介しています。

経営者が知っておくべきセキュリティリスクと対応について(2013 年 4 月 9 日)
https://www.jpcert.or.jp/research/APTRiskReport20130409.pdf

9.8. 法人における SNS 利用に伴うリスクと対策

日本国内および諸外国における SNS に起因する脅威とセキュリティ対策の現状について、公表されている情報(文献、Web)を収集し分析するとともに、国内 SNS 提供事業者およびセキュリティベンダへインタビューを行った結果に考察を添えて、法人自身および個人としての従業員による SNS の利用に関して法人が取るべき対策についてまとめたものです。

法人における SNS 利用に伴うリスクと対策(2013 年 4 月 1 日)
https://www.jpcert.or.jp/research/SNSrisk-biz20130328.pdf

10. 講演活動一覧

(1) 満永 拓邦(早期警戒グループリーダ) ：
「脅威の変化とアップデートの重要性」
日本マイクロソフト株式会社 MSXP 説明会, 2013 年 4 月 9 日

(2) 熊谷 裕志(情報流通対策グループ脆弱性解析チーム リードアナリスト)
「Android セキュアコーディング～Android アプリケーション開発における注意すべきポイント～」
第 17 回組込システム開発技術展, 2013 年 5 月 10 日

(3) 有村 浩一(常務理事)：
「今求められる制御システムセキュリティへの取り組みと体制」
ベライゾン グローバルリスクセミナー, 2013 年 5 月 23 日

(4) 有村 浩一(常務理事)：
パネル「制御システムセキュリティと国際連携」
制御システムセキュリティセンター東北多賀城本部開所記念シンポジウム, 2013 年 5 月 28 日

(5) 満永 拓邦(早期警戒グループリーダ) ：
「標的型攻撃に対する JPCERT/CC の取り組みと情報連携について」
マルチメディア推進フォーラム 2013, 2013 年 6 月 14 日

(6) 山本 健太郎(フィッシング対策協議会事務局)：
「フィッシングに関する最新動向について」
特定非営利活動法人日本システム監査人協会, 2013 年 6 月 15 日

11. 執筆一覧

(1) 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)：
もいちど知りたい、セキュアコーディングの基本(4)
「見落としがちな整数関連の脆弱性(前編)(1/2)」
アイティメディア アットマーク・アイティ, 2013 年 5 月 16 日

12. 開催セミナー等一覧

(1) 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、「2.5.7」をご参照ください。

■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