JPCERT-PR-2014-02
発行日 : 2014-07-10

JPCERT/CC 活動概要 [2014 年 4 月 1 日 ～ 2014 年 6 月 30 日]

活動概要トピックス

ートピック1ー　認証関連情報を窃取する手口の高度化と被害防止への取組み

フィッシング対策協議会と JPCERT/CC では、偽の Web サイトに利用者を誘引して本人認証等のための情報を入力させ窃取する行為をフィッシングと呼んで、フィッシングに使用されるサイトの情報やそれらのサイトへの誘引メール等の報告を受け付けています。本四半期の報告は、サイト数ベースで、金融機関を装うものが 61.2%、オンラインゲームサービスを装うものが 15.9%でした。このようにフィッシングサイトの報告では、金融機関を装うものが多数を占める状態が続いています。

また、国内金融機関のオンラインサービス利用者を狙ったマルウエアに関する報告の増加も近年の特徴です。この種のマルウエアに感染すると、パソコン内にある認証関連情報を窃取されたり、正規のサイトにアクセスした際に認証関連情報の入力を求める偽の画面が表示され、入力した情報を詐取されたりします。このようなマルウエアに盗み取られた情報が悪用されると、不正送金などの金銭的被害につながる危険性があります。さらに、法人向けに発行したクライアント証明書を窃取するマルウエアや、MITB (Man in the Browser)と呼ばれる手法により不正送金を行うマルウエアも報告されています。また、メール攻撃や Web 改ざんがこれらのマルウエアの配布手段となっており、一見の別のインシデントに見える複数の事象が、大規模な攻撃の要素を構成している可能性がうかがえます。攻撃の脅威を適切に把握するためには、関係する個別インシデントに係る詳細情報についても丁寧に把握することが重要です。

このように高度化した攻撃にさらされているオンラインサービス利用者を守るために、攻撃実態の把握やそれに基づく対策の実施、利用者への注意喚起といった活動が関連業界によって続けられています。JPCERT/CC も、関連業界の活動に参加し、さらに関係機関やセキュリティサービス事業者とも連携して、被害の拡大防止に努めています。

ートピック2ー　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表

経済産業省の告示「ソフトウエア等脆弱性情報取扱基準」に基づいた脆弱性関連情報の取扱いの詳細を定めているのが、関連業界団体および IPA と JPCERT/CC が連名で発行している「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」であり、その下で進められる製品開発者と JPCERT/CC 間での

調整の細目を定めているのが、「JPCERT/CC 脆弱性関連情報取扱いガイドライン」です。5 月 14 日の経済産業省告示の改正を受け、所定の努力を尽くしても製品開発者と連絡が取れないケースについて、中立的な委員会での審議を経て脆弱性情報を公表できることが上述の 2 つのガイドライン中に記載され、5 月 30 日に公表されました。改正告示およびガイドラインを踏まえた運用により、開発者と全く連絡が取れず、対策が提供されない場合にも、製品利用者に脆弱性情報が開示され得ることとなり、リスクや被害の低減に資すると期待されます。今後、委員会運用則などの詳細ルール策定などを行い、早期に運用を開始する予定です。その他、脆弱性情報の一般公表を取りやめる場合についての記述や、製品開発者が顧客等の製品利用者に対し脆弱性情報を一般公表の前に通知する場合についての記述なども追加されています。

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
https://www.jpcert.or.jp/vh/partnership_guide2014.pdf
JPCERT/CC 脆弱性関連情報取扱いガイドライン
https://www.jpcert.or.jp/vh/vul-guideline2014.pdf

ートピック3ー　FIRST の Board of Directors メンバに JPCERT/CC スタッフが当選

世界の 65 ヶ国 301 チーム(2014 年 7 月 10 日現在)の CSIRT(Computer Security Incident Response Team)からなる FIRST（Forum of Incident Response and Security Teams）の第 26 回年次会合が、6 月 22 日から 27 日まで米国ボストンで、 “Back to the ‘root’ of incident response” のテーマのもと開催されました。JPCERT/CC は 6 月 23 日に「Open DNS Resolver Check Site」と題して講演を行うとともに、「Developing Cybersecurity Risk Indicators – Metrics」と題したパネルセッションのモデレータを務めました。

この FIRST の活動の企画および立案等は、Board of Directors が行うこととされており、そのメンバは、任期 2 年で、年次会合における選挙により順次改選されています。本年の選挙には、JPCERT/CC の国際部シニアアナリスト小宮山功一朗が立候補し、関係組織の皆様にも厚いご支援をいただいて当選いたしました。日本国内はもとより、APCERT (Asia Pacific Computer Emergency Response Team)をはじめとするアジア太平洋地域やアフリカ地域での CSIRT 連携の促進に向けた活動への期待に支えられた結果と受け止め、今後とも、FIRST 加盟を希望するチームの支援や、他の国際組織との連携に尽力し、FIRST を通じた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.Org,Inc., Board of Directors
http://www.first.org/about/organization/directors

本活動は、経済産業省より委託を受け、「平成２６年度サイバー攻撃等国際連携対応調整事業」として実施したものです。
ただし、「9.フィッシング対策協議会の会員組織向け活動」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」、「11.主な講演活動一覧」、「12. 主な執筆一覧」および「13.協力、後援一覧」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 4517 件、インシデント件数ベースでは 4260 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 2134 件でした。前四半期の 1989 件と比較して 7%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等に対し、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 等)の関係機関との調整活動を行なっています。

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/2014/IR_Report20140710.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 509 件で、前四半期の 557 件から 9%減少しました。また、前年度同期(287 件)との比較では、77%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	国内外別合計（割合）
国内ブランド	50	36	81	167(33%)
国外ブランド	71	79	76	226(44%)
ブランド不明	44	40	32	116(23%)
月別合計	165	155	189	509(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等の理由により、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。

6 月半ば頃から、国内金融機関を装ったフィッシングサイトが増加しています。フィッシングの仕組みは以前から確認されているものと同様に、転送設定が埋め込まれたページを不正に設置されたと見られる海外の Web サイトから、国内通信事業者が動的に割り当てる IP アドレスを持ったフィッシングサイトに誘導されるようになっていました。フィッシングサイトは”英字 3 文字.co.in”というドメインを持っており、ドメイン登録者のメールアドレスなどの情報が一致しているという共通性がありました。誘導先のフィッシングサイトでは、一つの IP アドレスのホストに、3 種類の国内金融機関のフィッシングサイトが併存している事例を確認しました。

国内オンラインゲームサービスを装ったフィッシングサイトの報告も、非常に多く受領しています。オンラインゲームのフィッシングサイトには、.tk、.co.vu といった無料のドメインや、.pw ドメインを使用しているという特徴がありました。.tk ドメインのフィッシングサイトは、他のドメインに置かれたフィッシングサイトの本体をフレームを使用して表示し、フィッシングメールには.tk ドメインの URL を記載していました。これは、本体となるサイトをブロックリストに登録され難くするための方策と考えられます。

フィッシングサイトの調整先の割合は、国内が 55%、国外が 45%であり、前四半期(国内 43%、国外 57%)と同じ割合になっています。

本四半期に報告が寄せられた Web サイト改ざんの件数は、1123 件でした。前四半期の 1501 件から 25%減少しています。

4 月初め頃、古いバージョンの Movable Type を使用している国内企業の Web サイトが改ざんされたという報告を複数受領しました。これらのサイトでは、Web ページが読み込む JavaScript ファイルが改ざんされ、外部の Web サイトに誘導する iframe を挿入するコードが埋め込まれていました。誘導先の Web サイトでは、攻撃者によって設置されたと見られる php スクリプトによって、複数のアプリケーションの脆弱性を攻撃するサイトに転送される仕組みになっていました。JPCERT/CC は、被害拡大の防止を目的として、5 月 15 日に旧バージョンの Movable Type の利用に関する注意喚起を公開しました。

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およ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 サイト改ざん等のサイバー攻撃に関する情報を収集し、分析しています。これらのさまざま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等も併せて行い、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」(限定配付)等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)等を通じて、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等について、次のような注意喚起情報を発行しました。

発行件数：15 件　https://www.jpcert.or.jp/at/

2014-04-08　OpenSSL の脆弱性に関する注意喚起
2014-04-09　Adobe Flash Player の脆弱性 (APSB14-09) に関する注意喚起
2014-04-09　2014 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
2014-04-15　DNS キャッシュポイズニング攻撃に関する注意喚起
2014-04-16　2014 年 4 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
2014-04-28　2014 年 4 月 Microsoft Internet Explorer の未修正の脆弱性に関する注意喚起
2014-04-30　Adobe Flash Player の脆弱性 (APSB14-13) に関する注意喚起
2014-05-02　マイクロソフト セキュリティ情報(MS14-021)に関する注意喚起
2014-05-14　2014 年 5 月 Microsoft セキュリティ情報 (緊急 3 件含) に関する注意喚起
2014-05-14　Adobe Flash Player の脆弱性 (APSB14-14) に関する注意喚起
2014-05-14　Adobe Reader および Acrobat の脆弱性 (APSB14-15) に関する注意喚起
2014-05-15　旧バージョンの Movable Type の利用に関する注意喚起
2014-06-11　2014 年 6 月 Microsoft セキュリティ情報 (緊急 2 件含) に関する注意喚起

2014-06-11　Adobe Flash Player の脆弱性 (APSB14-16) に関する注意喚起
2014-06-12　ISC BIND 9 サービス運用妨害の脆弱性 (CVE-2014-3859) 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 57 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。

2014-04-02　新人研修に役立つ JPCERT/CC のコンテンツ 2014 年版
2014-04-09　Microsoft Windows XP と Office 2003 のサポート終了について
2014-04-16　ネットバンキング被害に注意
2014-04-23　担当者ノート: JVN で CVSS 評価を採用
2014-05-01　EMET 使ってますか？
2014-05-14　APCERT Annual Report 2013 公開
2014-05-21　「インターネットバンキングの不正送金にあわないためのガイドライン」公開
2014-05-28　不正送金の被害にあわないために
2014-06-04　J-CSIP 2013 年度活動レポートの公開
2014-06-11　名前衝突問題 (Name Collision)
2014-06-18　IT 製品の調達におけるセキュリティ要件リスト
2014-06-25　セキュアライフ 2020

1.2.1.3. 早期警戒情報

JPCERT/CC では、国民の生活や社会経済活動を支えるインフラ、サービスおよびプロダクト等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。

【OpenSSL の脆弱性】
2014 年 4 月 8 日、OpenSSL プロジェクトより、OpenSSL の heartbeat 拡張と呼ばれる機能に関する脆弱性情報が公開されました。

当該脆弱性は、遠隔の第三者が OpenSSL を使用するアプリケーションに対して、細工したパケットを送ることで、アプリケーションが利用しているメモリ上の情報を外部から参照できるというものです。多くの Web サイトにおいて OpenSSL が使用されており、サーバ証明書の秘密鍵やサーバが保持するユーザ情報が漏えいする可能性があり、非常に危険度の高い脆弱性でした。

また当該脆弱性の有無を検証する複数のツールがインターネット上に公開されていることが確認され、セキュリティベンダなどからは、国内の Web サイトに対して当該脆弱性を狙った攻撃が急増しているとの情報も公開されました。

JPCERT/CC でも、「OpenSSL の脆弱性に関する注意喚起」を公開し、サーバ管理者や、Web サイト管理者などに対し広く注意を呼びかけました。

【旧バージョンの Movable Type を使用した Web サイトの改ざんへの対応】
2014 年 5 月頃から、Movable Type という CMS(Content Management System) を使用している Web サイトが多数改ざんされるインシデントが発生しました。JPCERT/CC では、被害を受けた組織などから情報提供を受け、原因の調査を行ったところ、被害を受けた多くの Web サイトで古いバージョンの Movable Type が使用されていたことが判明し、その既知の脆弱性を悪用して Web サイトの改ざんが行われていたものと推測されました。

今後、当該脆弱性を狙った攻撃が継続して発生する可能性に鑑み、「旧バージョンの Movable Type の利用に関する注意喚起」を公開し、サーバ管理者や、Web サイト管理者などに対し広く注意を呼びかけました。

1.3. インターネット定点観測

JPCERT/CC では、インターネット上に複数の観測用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収集するためのインターネット定点観測システム TSUBAME を構築し、運用しています。TSUBAME から得られる情報を、既に公開されている脆弱性情報やマルウエア、攻撃ツールの情報などと対比して分析することで、攻撃活動や攻撃の準備活動等の状況を把握することに努めています。

1.3.1. TSUBAME(インターネット定点観測システム)の運用、および観測データの活用

JPCERT/CC は、さまざまな地域に広く設置された観測用センサーを含む TSUBAME を構築するとともに、各地域の CSIRT と共同で分析をするためのプロジェクト(TSUBAME プロジェクト)の事務局を担当し、システムやセンサーの定常稼働に努めています。2014 年 6 月にラオスがプロジェクトに参加し、2014 年 6 月末時点で、観測用センサーをアジア・太平洋地域の 24 地域に設置しています。今後も設置地域を拡大し、より充実したセンサー網の構築と共同分析の高度化を進めるべく関係機関と交渉を続けています。

TSUBAME プロジェクトの目的等詳細については、次の URL をご参照ください。

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

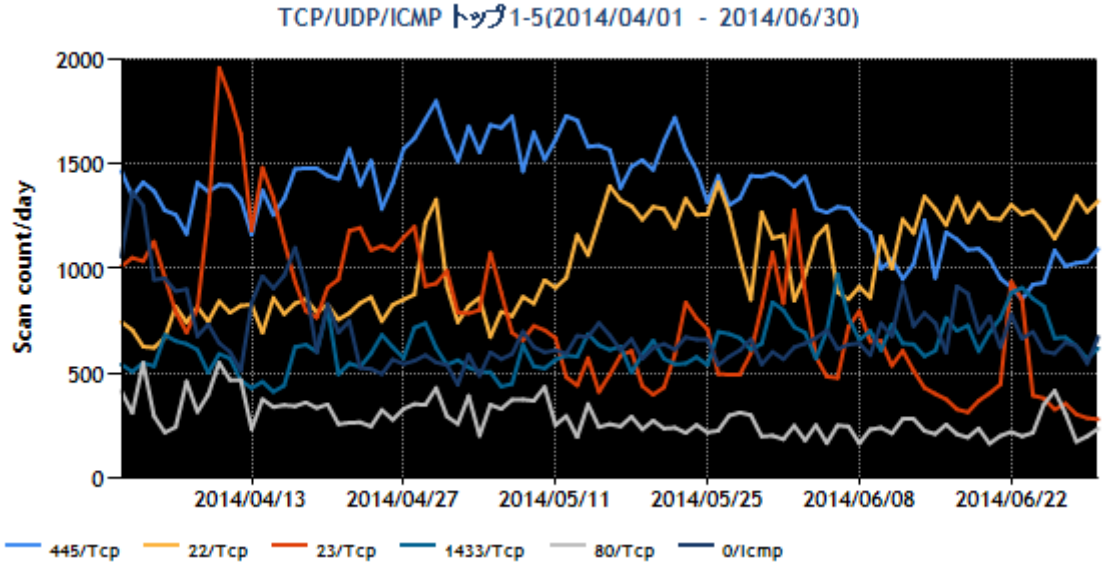
JPCERT/CC は TSUBAME で収集したデータを宛先ポート番号や送信元地域ごとに分類して統計分析し、既知の脆弱性情報やマルウエア、攻撃ツール等との関連を考察することで、攻撃活動や準備活動の捕捉に努めています。

主に日本企業のシステム管理者等の方々に、自ネットワークに届いた意図しないパケットと比較していただけるよう、日本国内のセンサーで受信したパケットを宛先ポート別に集計してグラフ化し、毎週月曜日に JPCERT/CC の Web ページで公開しています。また、四半期ごとに観測傾向や注目される現象を紹介する「インターネット定点観測レポート」を公開しており、2014 年 1 月から 3 月分のレポートを 4 月 21 日に公開しました。

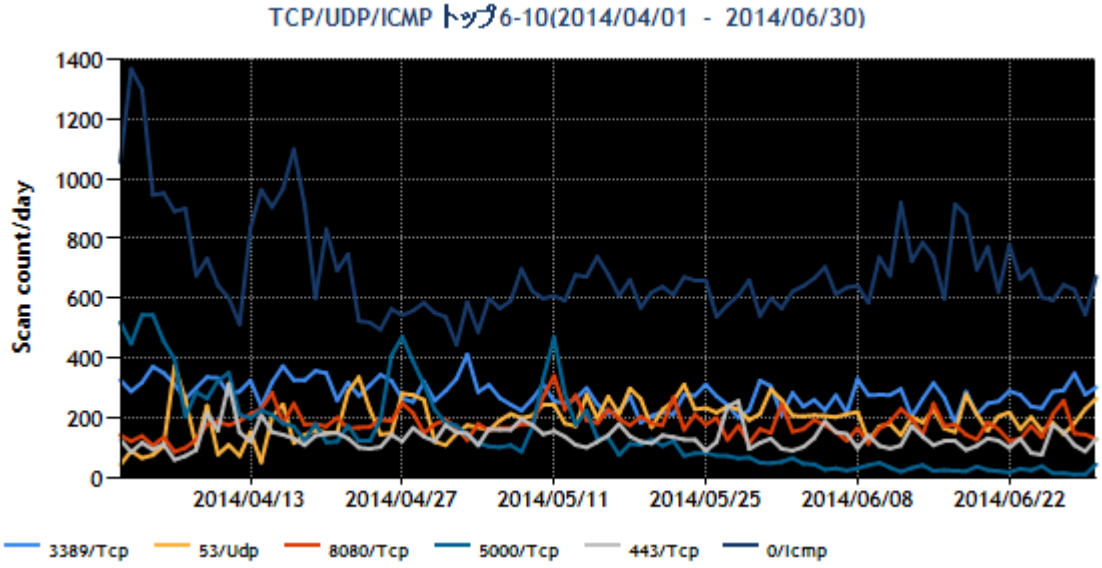
TSUBAME 観測グラフ
https://www.jpcert.or.jp/tsubame/index.html#examples

インターネット定点観測レポート(2014 年 1～3 月)
https://www.jpcert.or.jp/tsubame/report/report201401-03.html

本四半期に TSUBAME で観測された宛先ポート別パケット数の上位 1 位～5 位および 6 位～10 位を、[図 1-1]と[図 1-2]に示します。

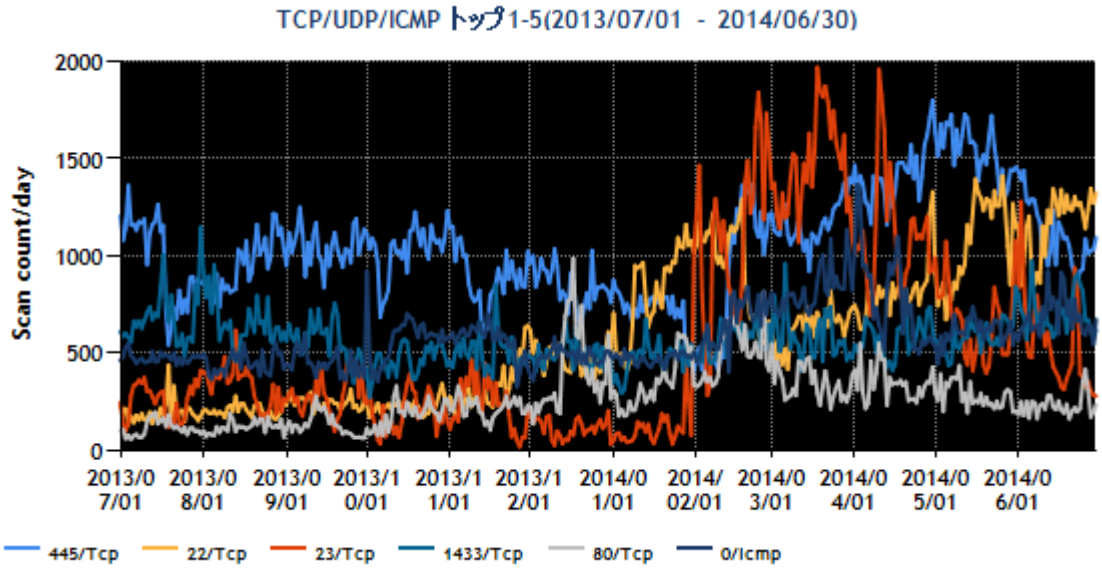


[図 1-1 宛先ポート別グラフ トップ 1-5(2014 年 4 月 1 日-6 月 30 日)]

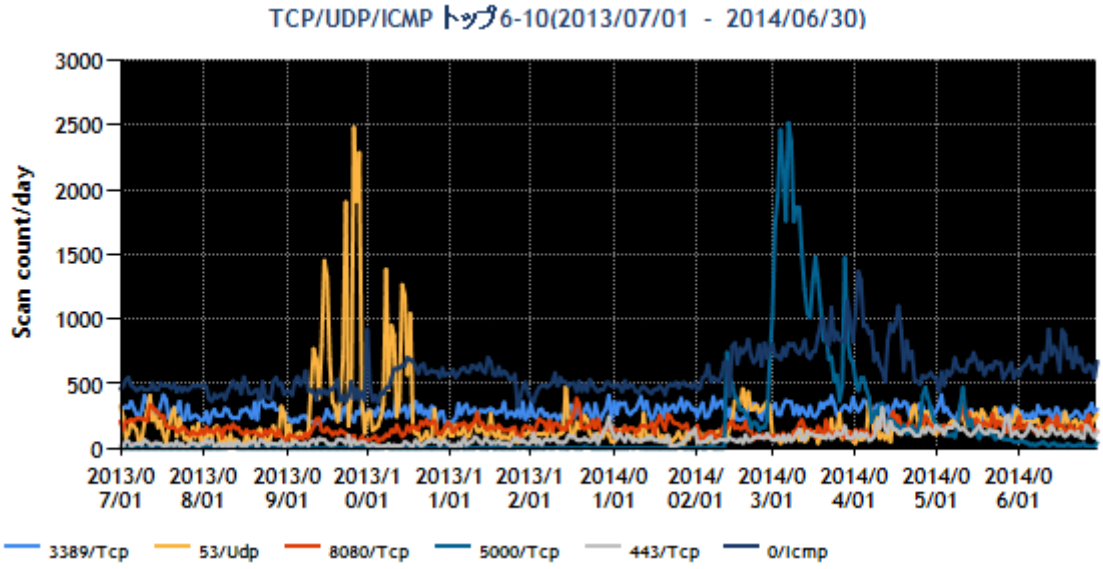


[図 1-2 宛先ポート別グラフ トップ 6-10(2014 年 4 月 1 日-6 月 30 日)]

また、過去 1 年間(2013 年 7 月 1 日～2014 年 6 月 30 日)における、宛先ポート別パケット数の上位 1 位～5 位および 6 位～10 位を[図 1-3]と[図 1-4]に示します。



[図 1-3 宛先ポート別グラフ トップ 1-5 (2013 年 7 月 1 日-2014 年 6 月 30 日)]



[図 1-4 宛先ポート別グラフ トップ 6-10 (2013 年 7 月 1 日-2014 年 6 月 30 日)]

23/TCP 宛のパケットを引き続き観測しています。これらには、日本の IP アドレスから発信されたパケットも含まれ、国外製のネットワークカメラなどによるスキャン活動と見られます。その他、順位に変動はありますが、Windows や Windows 上で動作するソフトウエアへのスキャン活動や、SSH サーバ等遠隔操作のためにサーバ側が待ち受けているポートのスキャン活動と見られるパケットも、これまでと同様に多く観測されています。

1.3.2. TSUBAME 観測データに基づいたインシデント対応事例

JPCERT/CC は、日々観測情報の分析を行っており、不審な動きが認められた場合には、必要に応じて送信元 IP アドレスの管理者に連絡する等の対処をしています。

DNS 応答パケットおよび、DNS サービスのポート不達を示す ICMP エラーパケットが、本四半期もセンサー上で多数観測されました。これらは、DNS 応答パケットなどの分析から、実際には存在しない FQDN を OpenResolver 経由で多数問い合わせることにより DNS 権威サーバに過剰な負荷を課そうとする攻撃において、攻撃者が応答パケットを受け取らずにすませるために詐称した送信元が，たまたまセンサーの IP アドレスだったために観測されたものと推測されています。すなわち、攻撃に利用されたノードが，OpenResolver でなかった場合には ICMP エラーが，OpenResolver であった場合には名前解決できなかった旨の応答がセンサーに届いていると見られます。この考え方に基づく観測で、日本国内だけでも毎日 10 件近くの OpenResolver が新たに見つかっています。JPCERT/CC は、この情報を DNS サーバの管理者に提供し、DNS サーバやネットワーク機器が OpenResolver となっていないか調査を依頼しまし、多くの管理者から「当該サーバの設定が不適切で OpenResolver であることを確認したため、必要な対応を行った」等の返事を得ています。

1.3.3. TSUBAME トレーニングの実施

本四半期には、LaoCERT (ラオス人民民主共和国の National CSIRT) の TSUBAME センサーの設置、および TSUBAME トレーニング(TSUBAME システムの利用方法の説明と TSUBAME システムの情報を活用して、インターネット上で行われている攻撃や探索活動などを分析する方法の紹介、TSUBAME センサーの設置方法や運用方法など) を実施しました。

日時：2014 年 5 月 21 日 (水) ～ 2014 年 5 月 22 日 (木)
場所：ラオス人民民主共和国 ヴィエンチャン
参加人数：22 名 (LaoCERT および LaoCERT の関係者が参加)

トレーニングの内容：
- 5 月 21 日
  - TSUBAME システムの概要
  - ネットワークモニタリングについて
  - TSUBAME センサーセットアップと運用について
- 5 月 22 日
  - TSUBAME システムの機能説明
    - TSUBAME portal サイトの使い方、TSUBAME Web サイトの使い方
  - TSUBAME システムを活用した分析事例の紹介
    - ラオス人民民主共和国を送信元地域とするパケットの分析事例
    - 前日 (5 月 21 日) に設置したセンサーから得られたデータの分析
  - トレーニング修了証書授与

6 月初めに LaoCERT が正式に TSUBAME Working Group に参加しました。これにより TSUBAME Working Group の参加組織数は、24 組織 (21 経済地域) となりました。

APCERT TSUBAME Working Group
http://www.apcert.org/about/structure/tsubame-wg/index.html#Members

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、脆弱性を作り込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。

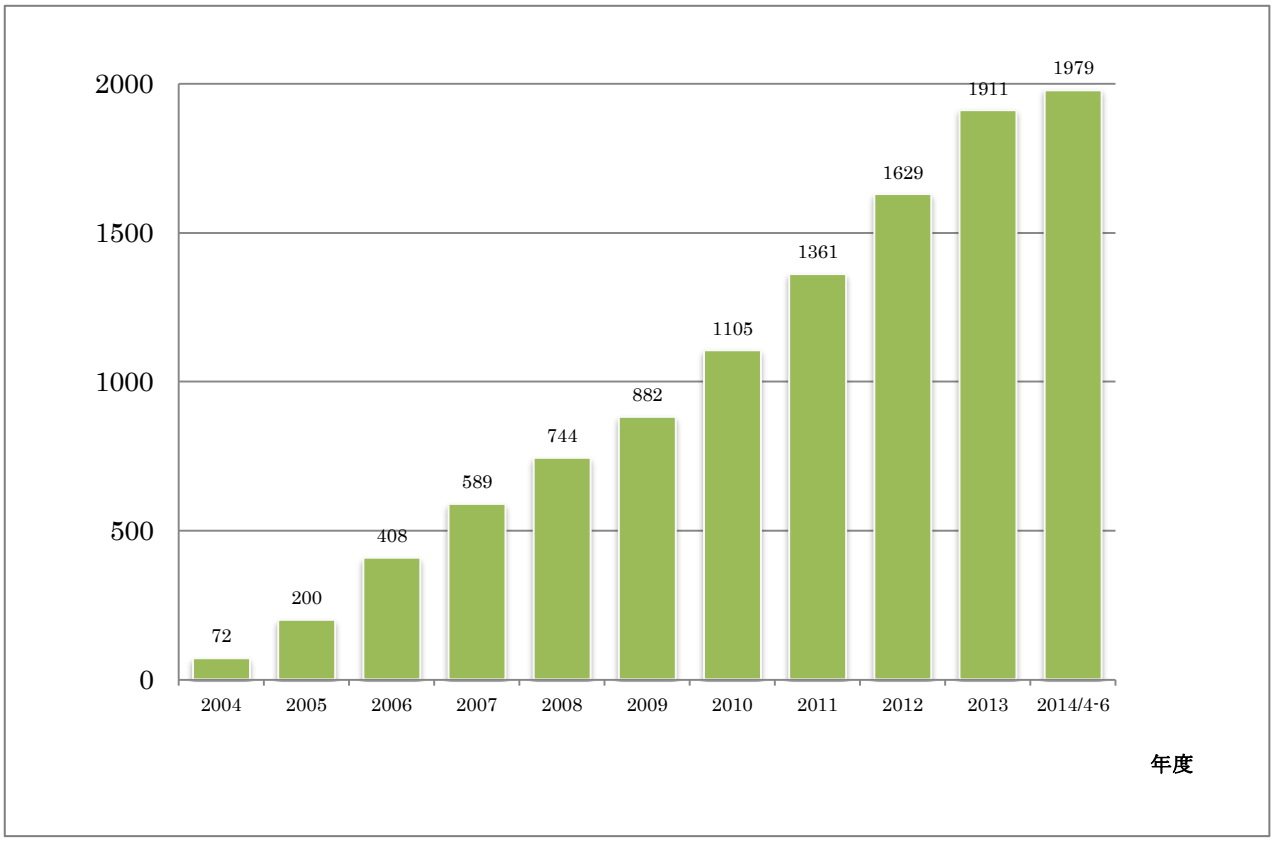
2.1. Japan Vulnerability Notes(JVN)において公表した脆弱性情報および対応状況

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、本基準を踏まえて取りまとめられた「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（以下「パートナーシップガイドライン」といいます。」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窓口への連絡、開発者による脆弱性の検証等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。なお、本四半期においては、本基準が 5 月 14 日付けで改正されており、これを受けて改訂されたパートナーシップガイドラインが、5 月 30 日付で公開されています（改訂内容等については、“2.2. 連絡不能開発者とそれに対する対応の状況” および”2.4.3.「JPCERT/CC 脆弱性情報取扱いガイドライン」の改訂”、を参照）。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[例えば、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[例えば、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 NCSC-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等が含まれます。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「JVNTA」に続く 8 桁数字の形式の識別子(例えば、JVNTA#12345678)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 68 件(累計 1979 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 29 件(累計 880 件)で、累計の推移は[図 2-2]に示すとおりです。29 件のうち、19 件が国内製品開発者の製品、10 件が海外の製品開発者の製品でした。

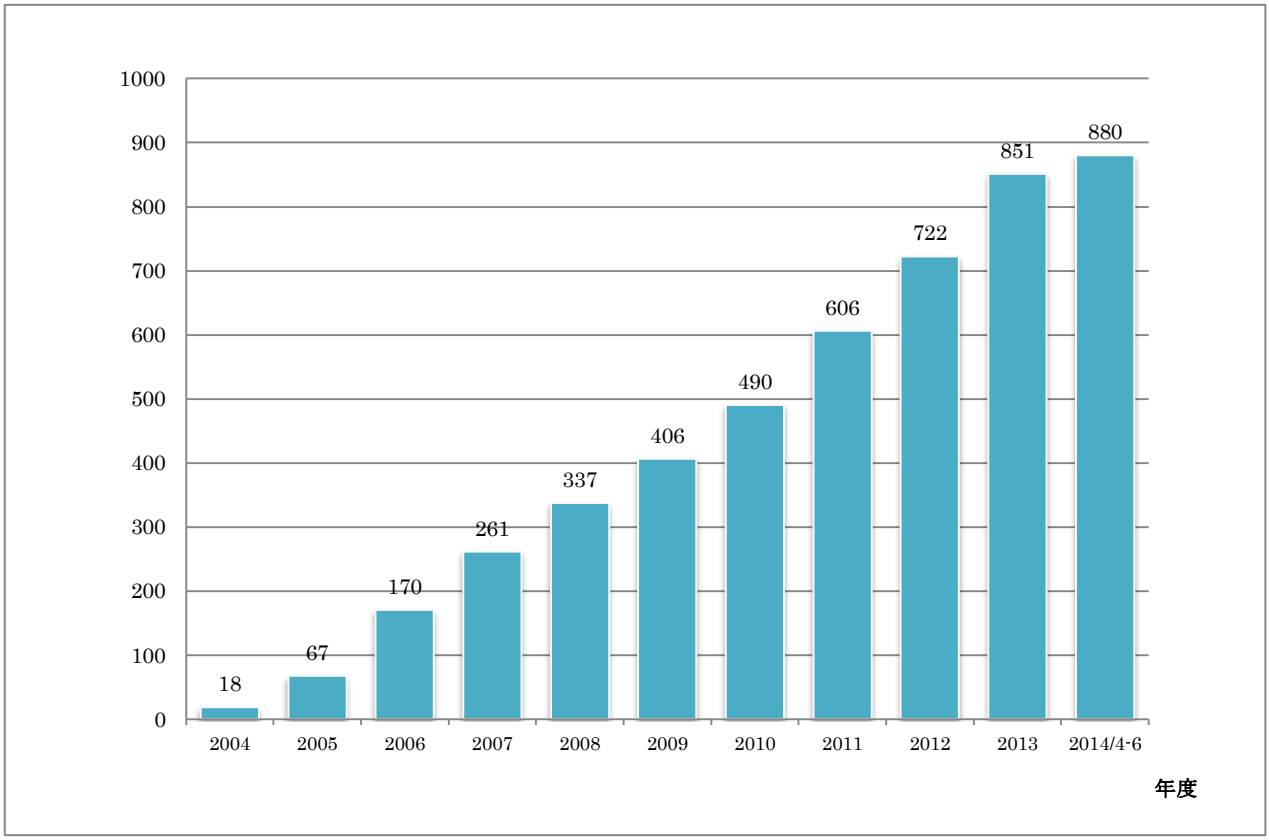
また、前四半期に引き続き本四半期も、自社製品届出による脆弱性情報を 7 件公表しました。これは本四半期で公表した全脆弱性情報の約 24%にあたります。

Android およびその関連製品の脆弱性情報の届出は 2012 年度から増加傾向にあり、本四半期には、JVN 上での公表ベースで、Android 向けアプリケーションに関する脆弱性情報が 5 件あり、全体の約 17%を占めました。

Android 関連製品以外で公表された脆弱性情報の内訳は、グループウェア製品に関するものが 9 件、Web サイト構築製品に関するものが 6 件、Open Source Software(以下、OSS といいます。)製品に関するものが 5 件、企業向けネットワーク機器およびサーバ製品が 2 件、モバイルルータ等の小型デバイスに関

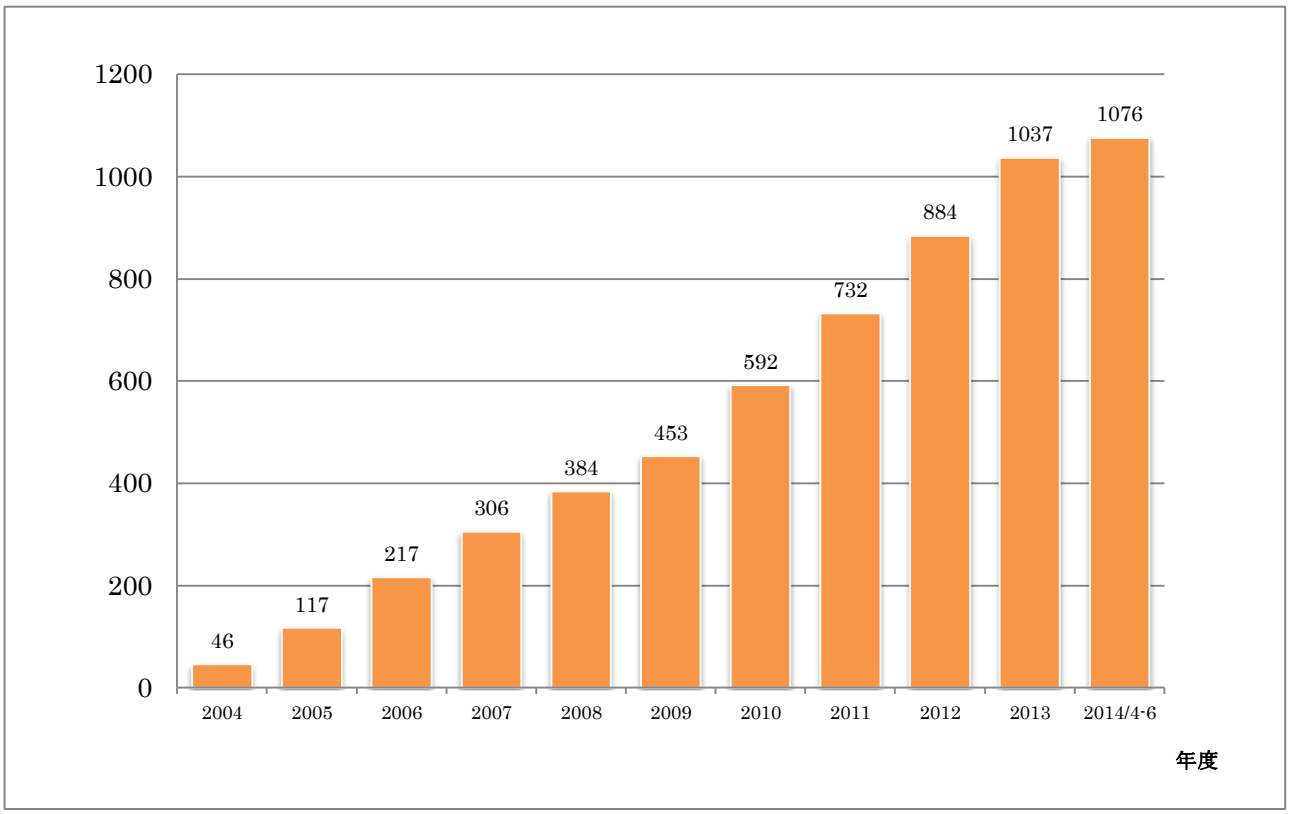
するものが 1 件、複合機に関するものが 1 件でした。このうち OSS 製品に関する脆弱性情報で、最初に公表されたパッチでは完全には修正されていないとして届出られた事例がありました。本件については、幸いにも、製品開発者によって速やかに対策がとられ、2 度目の届出から 7 日間で完全な修正パッチとともに公開できました。対応に手間取れば、公開された脆弱性に対する十分な対策が存在せず、当該 OSS を導入している製品も広範囲に及んでいるため影響が大きくなる可能性もありました。

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 39 件(累計 1076 件)で、累計の推移は[図 2-3]に示すとおりです。このうち OpenSSL と、Microsoft Internet Explorer の脆弱性については、影響を受ける製品ないしその製品利用者が多く、特に深刻度が高いものでした。この他、CMS、BPM、検索アプライアンス、グループウェアなど企業向けビジネスアプリケーション製品が 7 件、企業向けネットワーク機器およびサーバ製品が 9 件、海外 OSS 製品が 5 件、モバイルルータ等の小型デバイス製品が 5 件のほか、Apple による自社製品に関する脆弱性情報の届出によるものが 3 件ありました。本四半期は、海外製品開発者のうち、Huawei、ZyXEL など中国や台湾を拠点とするアジア系企業のネットワーク製品に関する脆弱性の公表が 5 件と比較的多かったのが特徴でした。



[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

本基準に基づいて脆弱性が報告されたものの、しかるべき呼び掛けをしても調査と対策をしていただくべき製品開発者に連絡が取れない場合には、2012 年度以降、当該製品開発者名を JVN 上で「連絡不能開発者一覧」として公表しています。これまでに 165 件(製品開発者数としては 101 件)を公表し、21 件(製品開発者の数としては 14 件)の調整が再開でき、脆弱性関連情報の取り扱いにおける「滞留」の解消に一定の効果を挙げています。

本四半期に新たに連絡不能開発者一覧に掲載した製品開発者名は 9 件でした。本四半期末日時点で、合計 144 件の連絡不能開発者案件を引き続き掲載し、継続して製品開発者や関係者からの連絡および情報提供を呼び掛けています。

なお、5 月 30 日に公表されたパートナーシップガイドラインの改訂版に合わせて、「JPCERT/CC 脆弱性関連情報取扱いガイドライン」を改訂し、公表しました。これらの改訂によって、「連絡不能開発者一覧」の公表を実施しても、なお製品開発者と連絡が取れない脆弱性情報は、中立的な委員で構成された委員会での審議を経て、「連絡不能」であったことを明示した上で公表できるようになりました。この手続きの運用開始により、連絡不能な開発者の製品を利用する方々に、脆弱性情報をお届けすることができるようになり、リスクの認識や被害の低減に資すると期待されます。今後、詳細な手続きなどの運用ルールを決めた上で、連絡不能となっている案件の公表に向けた具体的な作業に着手する予定です。

プレスリリース 製品開発者と連絡が不能な「連絡不能案件」の脆弱性情報公表に向けた運用を開始～「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」を改訂(2014 年 5 月 30 日公開)
https://www.jpcert.or.jp/vh/PR20140530-vulPSG.pdf

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(2014 年 5 月 30 日公開)
https://www.jpcert.or.jp/vh/partnership_guide2014.pdf

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 等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等の調整活動を連携して行っています。さらに Android 関連製品や OSS 製品の脆弱性の調整活動の中では、製品開発者が存在するアジア圏の調整機関、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)上の脆弱性情報も、日本語版とほぼ同時に公表しており、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等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 27 件に CVE 識別子が付与されており、そのうち 25 件は JPCERT/CC が採番しました。2008 年以降においては、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(全体の 1 割弱)を除いて、JVN 上で公表する脆弱性のほぼすべてに 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/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(2014 年版)
https://www.jpcert.or.jp/vh/partnership_guide2014.pdf
JPCERT/CC 脆弱性情報取扱いガイドライン
https://www.jpcert.or.jp/vh/vul-guideline2014.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り扱い状況等の情報交換を行う等、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ごとの届出状況については、次の URL をご参照ください。

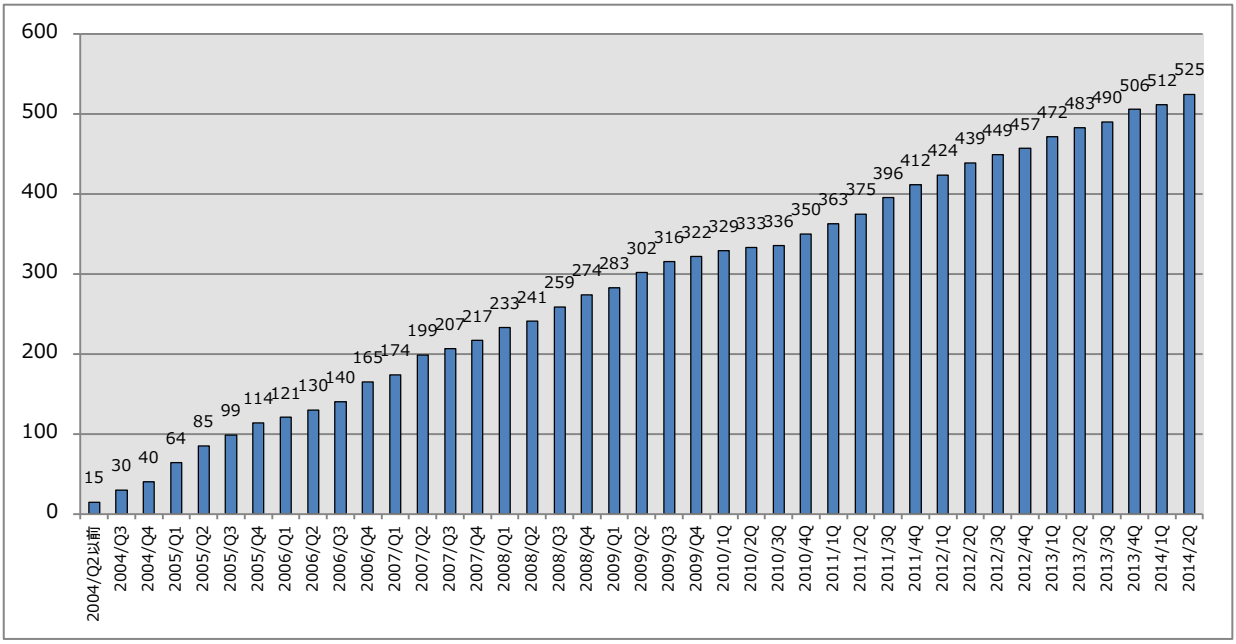
独立行政法人情報処理推進機構(IPA) 脆弱性対策
http://www.ipa.go.jp/security/vuln/

2.4.2. 日本国内製品開発者との連携

本基準では、脆弱性情報を提供する先となる製品開発者のリストを作成し、各製品開発者の連絡先情報を整備することが、調整機関である JPCERT/CC に求められています。JPCERT/CC では、製品開発者の皆さま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、2014 年 6 月 30 日現在で 525 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]

2.4.3. 「JPCERT/CC 脆弱性情報取扱いガイドライン」の改訂

2013 年度の「情報システム等の脆弱性情報の取扱いに関する研究会」において検討された結果をも踏まえ、5 月 14 日に本基準（経済産業省告示「ソフトウエア等脆弱性情報取扱基準」）が改正され、所定の努力を尽くしても製品開発者と連絡が取れないケースについて、中立的な委員会での審議を経て脆弱性情報公表できることとされました。この改正を受け、パートナーシップガイドラインが改訂され、5 月 30 日に公表されました。
これにあわせ JPCERT/CC では、「JPCERT/CC 脆弱性関連情報取扱いガイドライン」を改訂し、同日に公表しました。

このガイドライン改訂により、脆弱性関連情報の一般公表に関する取扱いや、連絡不能等の理由により製品開発者と調整ができない脆弱性案件の取扱いが変更されています。その他、脆弱性情報の一般公表を取りやめる場合についての記述や、製品開発者が顧客等の製品利用者に対し脆弱性情報を一般公表の前に通知する場合についての記述なども追加されています。ガイドライン改訂版の詳細につきましては、以下をご参照ください。

JPCERT/CC 脆弱性情報取り扱いガイドライン(2014 年 5 月 30 日公開)
http://www.jpcert.or.jp/vh/guideline_2014.pdf

2.5. セキュアコーディング啓発活動

2.5.1. 調査レポート『制御システム用ソフトウエアの脆弱性対策に有効な CERT C コーディングルールの調査』を公開

近年、制御システムのセキュリティに対する関心がますます高まりを見せる中、制御システム用ソフト

ウエアの脆弱性が多数発見されています。

JPCERT/CC では、制御システム開発者の方々に「CERT C コーディングスタンダード」を活用してセキュアな製品開発に取り組む契機としていただけるよう、ICS-CERT アドバイザリで公開された制御システム用ソフトウエアの脆弱性を調査し、それらの低減に役立つ 22 個のルールを CERT C コーディングスタンダードの中から抽出しまとめたレポートを 6 月 2 日に公開しました。

制御システム用ソフトウエアの脆弱性対策に有効な CERT C コーディングルールの調査
https://www.jpcert.or.jp/research/ics-codingrule.html

2.5.2. JJUG CCC 2014 Spring で JRE の脆弱性について講演

5 月 18 日にベルサール西新宿で開催された日本 Java ユーザーグループ主催のイベント「JJUG CCC 2014 @ Spring」において、脆弱性解析チームの戸田洋三が「JRE 標準ライブラリの脆弱性事例を理解する(AtomicReferenceArray クラスと Type Confusion)」と題した講演を行いました。

この講演では、JRE に同梱されている標準ライブラリ中の AtomicReferenceArray クラスに存在した脆弱性(CVE-2012-0507)をとりあげ、どのような問題だったのか、どのように修正されたのか、について解説しました。

本講演で使用した資料は JJUG CCC 2014 @ Spring のセッション一覧ページからご覧いただけます。

R2-6 JRE 標準ライブラリの脆弱性事例を理解する(AtomicReferenceArray クラスと Type Confusion)
http://www.java-users.jp/?page_id=1048#R2-6

2.5.3. CERT C コーディングスタンダードのルールを最新版にアップデート中

CMU/SEI のセキュアコーディングプロジェクトでまとめられている CERT C Coding Standard では、昨年来の作業において C11 を考慮した内容の追加や複数のルールの統廃合が行われ、2014 年時点での状態を反映した書籍「The CERT C Secure Coding Standard, Second Edition」も出版されました。

CERT C Coding Standard の JPCERT/CC による日本語訳版である CERT C コーディングスタンダードでもこの変更をとりこむべく、内容の更新を進めています。

今四半期の作業で、次の更新がありました。

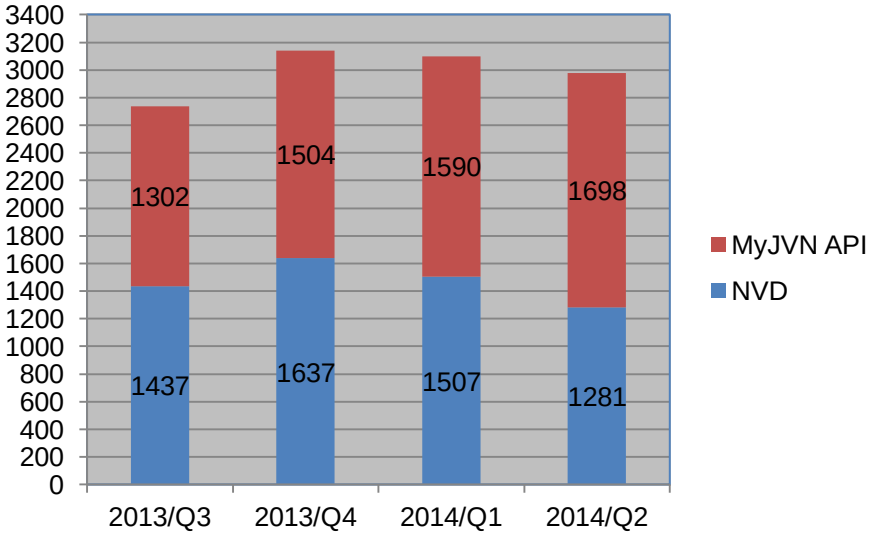
- 統廃合により移動したルール: 3
- 内容を更新したルール: 43

2.6. VRDA フィードによる脆弱性情報の配信

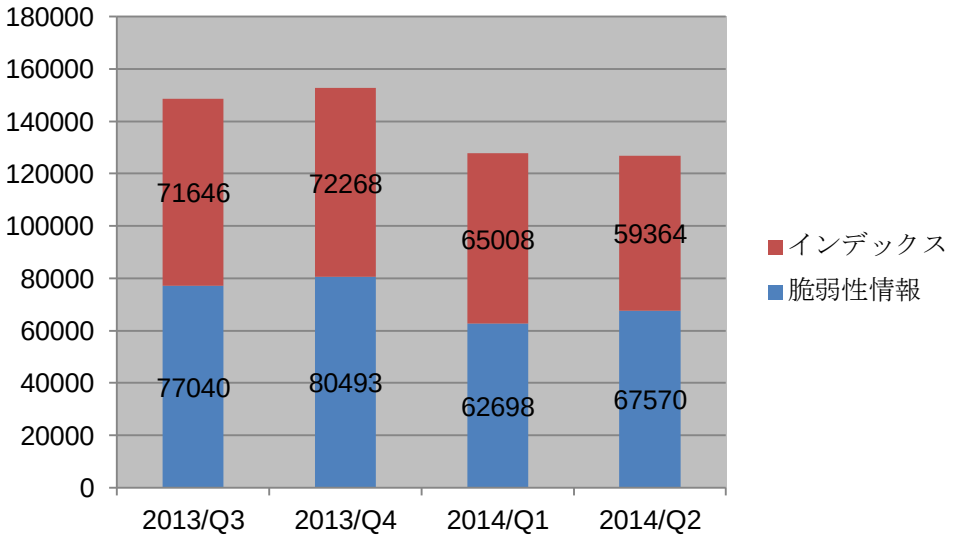
JPCERT/CC は、大規模組織の組織内 CSIRT 等での利用を想定して、KENGINE 等のツールを用いた体系的な脆弱性対応を可能とするため、IPA が運用する MyJVN API および NIST(National Institute of Standards and Technology)の NVD(National Vulnerability Database)を外部データソースとして利用した、VRDA(Vulnerability Response Decision Assistance)フィードによる脆弱性情報の配信を行っています。VRDA フィードについての詳しい情報は、次の URL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

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 2-5]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 2 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。

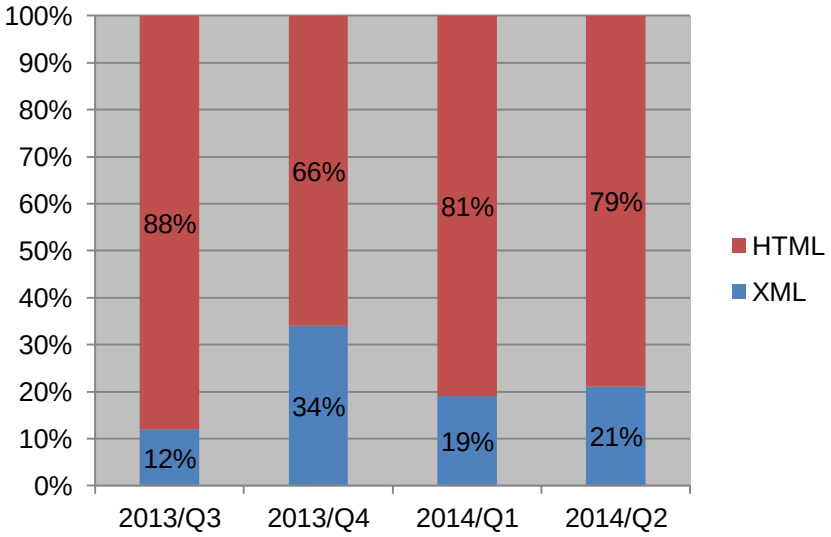


[図 2-5 VRDA フィード配信件数]



[図 2-6 VRDA フィード利用件数]

[図 2-6] に示したように、インデックスの利用数については、前四半期と比較し、約 9%減少しました。脆弱性情報の利用数については、前四半期と比較し、約 8%増加しました。



[図 2-7 脆弱性情報のデータ形式別利用割合]

[図 2-7] に示したように、脆弱性情報のデータ形式別利用傾向については、前四半期と比較して目立った変化は有りませんでした。

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調査し、インシデントをもたらした攻撃の手法やその影響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はじめとするプログラム

や攻撃手法等(アーティファクト)にまでおよび、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。

また、JPCERT/CC は、アーティファクト分析で得た知見を国内外で対策活動を行う組織と共有することが重要であると考えています。JPCERT/CC が取り扱った個別のインシデントの情報を第三者に開示することはありませんが、調査・分析により判明した攻撃手法やその調査・分析のために使った技術情報等を、適切に活用していただける組織と共有する活動も行っています。

4. 制御システムセキュリティ強化に向けた活動

4.1. 情報収集分析

JPCERT/CC では、制御システムにおけるセキュリティインシデントに関わる事例や標準の動向、その他セキュリティ技術動向に関するニュースや情報等を収集・分析し、必要に応じて国内組織等に情報提供を行っています。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 467 件でした。このうち、国内の制御システム関係者にとって、影響を与えうる・将来的に起こりえる脅威とその対策などを参考情報としてまとめ、提供いたしました。

本四半期に提供した参考情報は次の 4 件でした。

- 2014/04/21　[参考情報] ネットワーク機器等の障害による影響調査について
- 2014/04/22　[参考情報] OpenSSL の脆弱性に関する情報共有
- 2014/05/02　[参考情報] インターネットに接続された BACnet 対応機器について
- 2014/06/27　[参考情報] 制御システムを狙った Havex RAT について

また、海外での事例や、標準化動向などは 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月刊ニュースレターとして配信しています。本四半期は計 3 回配信しました。

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 363 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

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 0 件でした。

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。

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である日本版 SSAT(SCADA Self Assessment Tool)や J-CLICS(制御システムセキュリティ自己評価ツール)の配布を行っています。本四半期は、JPCERT/CC に対して、日本版 SSAT に関しては 2 件、J-CLICS に関しては 12 件の利用申込みがありました。直接配布件数の累計は、日本版 SSAT が 159 件、J-CLICS が 203 件となりました。

5. 国際標準化活動

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 つの標準からな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います。
本四半期は、4 月 7 日から 14 日にかけて香港で開催された SC27 国際会議に日本の代表団の一員として参加し、SC27 事務局に事前に提出していた 4th Working Draft に対する日本のコメントについて説明を行うとともに、各国の代表とコメントへの対処方法に関する議論を行いました。
今回の会議では、各草案を Working Draft の段階から Committee Draft の段階に進めるべきかどうかが大きな論点の一つでした。日本としては、Part 1 は CD に進んで問題ないと判断しましたが、Part 2, 3 については、成熟度が低く、更なる WD 審議が妥当と主張し、米国も同様の立場を表明しました。しかしながら、27035 のプロジェクトエディターである Geoff Clarke 氏の強い意向もあり、Part 1～3 が足並みをそろえて CD に進むことになりました。
27035-1 はインシデント管理の原理を規定しています。この草案には、5 カ国および SC27 のリエゾンメンバーである FIRST から計 66 件のコメントが寄せられました。日本から提出した 14 件のコメントについては、一部のコメントを除き概ね受け入れられました。規格の構造は固まっており、ドキュメントの成熟度は順調に向上しています。
27035-2 はインシデント対応の計画と準備のガイドラインを規定しています。この草案に対しては、4 カ

国から計 111 件(うち日本からは 15 件)のコメントが寄せられました。日本からのコメントは、一部のエディトリアルコメントを除き、概ね受け入れられました。依然として、規格本文に箇条書きメモのままで書き下せていない箇所が多いところが懸念されます。
27035-3 はインシデント対応のオペレーションのガイドラインを規定しています。この草案に対しては、4 カ国および FIRST から計 72 件(うち日本からは 8 件)のコメントが寄せられました。日本のコメントはすべて受け入れられました。一部の章が附属書に移動されたことで、特定の CISRT のオペレーションを想定した記述が本文から減少し、見通しが改善されました。しかし、内容的に 27035-1 との不整合や乖離を起こしており、さらにそれが理由で Part 3 の改善が阻害されている問題も残っており、章構成を含む全体の見直しがまだまだ必要であるように見受けられます。

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における活動を通じて、引き続き、この国際標準がわが国の CSIRT の取組と整合性の取れたものとなるよう努めていく所存です。

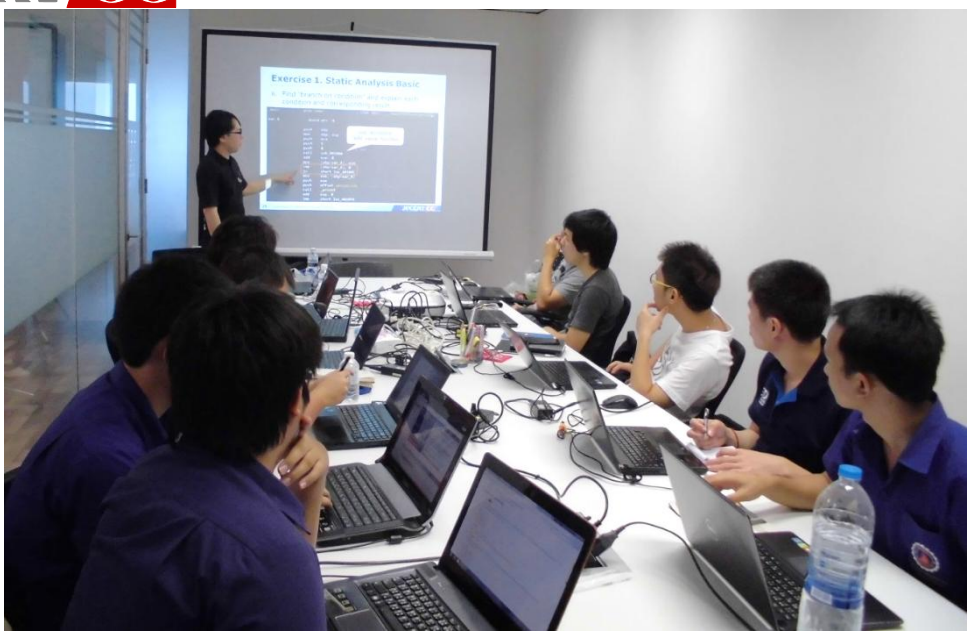
6. 国際連携活動関連

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. タイ CSIRT 構築支援等(2014 年 5 月 12 日-15 日)

JPCERT/CC は、タイの National CSIRT である ThaiCERT の機能強化を目的としたトレーニングを、同組織のスタッフに対してタイの首都バンコクで 5 月 12 日、13 日、15 日の計 3 日間にわたって行いました。ThaiCERT のスタッフ計 10 名が受講した本トレーニングでは、JPCERT/CC のスタッフ 2 名が講師となり、マルウエア解析の手法についての講義やハンズオン演習を行いました。また 5 月 14 日には、タイの電子政府構築を推進する組織である Electronic Government Agency が主催した政府セキュリティカンファレンスにおいて、「Internet Security and CSIRT's mission」と題する講演を行いました。



[図 6-1 トレーニングの模様]

6.1.2. アフリカ CSIRT 構築支援 等(2014 年 5 月 26 日-31 日)

JPCERT/CC は、5 月にジブチ共和国で 2 日間にわたる CSIRT トレーニングを行いました。また 5 月 31 日に開催された AfricaCERT Cybersecurity Day に参加しました。

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およ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-15 は、ジブチ共和国の ISP などのスポンサーを得て、首都ジブチで開催されました。

JPCERT/CC が担当した CSIRT トレーニングは、AfNOG-15 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 8 回目の開催となります。

JPCERT/CC は、5 月 29 日から 30 日までの 2 日間、日本のサイバーセキュリティ状況や、サイバー衛生に向けた日本の国際協力に関する講演、およびネットワークフォレンジックに関するトレーニング(図 6-1 参照)を行いました。このトレーニングには、約 40 名のインターネット運用者および政策担当者が受講しました。これに先立って 5 月 26 日から 28 日に行われた FIRST の講師による CSIRT 研修に関しても、JPCERT/CC は FIRST の Steering Committee メンバの一員として、講師の手配・調整等の準備を行うとともに、現地での研修サポートを行いました。

5 月 31 日の AfricaCERT Cybersecurity Day では、AfricaCERT という地域 CSIRT の現状と今後の活動計画について事務局から説明が行われ、参加各国からカントリーアップデートがありました。JPCERT/CC は APCERT と AfricaCERT との連携を提案し、AfricaCERT として地域 CSIRT 間の連携の枠組みをもつことの重要性を訴えました。

[図 6-2 トレーニングの模様]

Afnog および 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 および Afnog 15 公式ページ
http://www.afnog.org/afnog2014/index.php

AAF（Africa Asia Forum on Network Research & Engineering)
http://www.africaasia.net/

情報セキュリティに関する制度や技術が成長段階にある国・地域などからのサイバー攻撃が、日本のインターネットユーザにとっての大きな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を震源とするインシデントが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とそのため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の実施状況等に関する情報収集を目的として、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等、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(運営委員)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 4 期目)としてさまざまな活動をリードしています。JPCERT/CC の APCERT における役割および 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 会議の実施

Steering Committee は 5 月 9 日に電話会議を行い、今後の APCERT の運営方針等について議論を行いました。JPCERT/CC は議長チームおよび事務局として、本会議の主導およびサポートを行いました。

6.2.2. FIRST (Forum of Incident Response and Security Teams)

JPCERT/CC は 1998 年の FIRST 加盟以来、積極的に活動に参加しています。FIRST 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. 26th Annual FIRST Conference Boston への参加(2014 年 6 月 22 日-27 日)

FIRST の第 26 回年次会合が 6 月 22 日から 27 日までボストンで開催されました。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 “Back to the ‘root’ of incident response” 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 23 日に「Open DNS Resolver Check Site」と題して講演を行いました。また同日、「Developing Cybersecurity Risk Indicators – Metrics」と題したパネルセッションのモデレータを務めました。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 26 回 FIRST 年次会合についての詳細は、以下の URL をご参照ください。

26th Annual FIRST Conference Boston
http://www.first.org/conference/2014

6.2.2.2. FIRST Board of Directors メンバ当選

FIRST の活動の企画・立案等を行う Board of Directors のメンバは、FIRST の年次会合において参加組織による選挙によって選出されます。本年の年次会合において執り行われた Board of Directors 選挙に、JPCERT/CC から国際部シニアアナリスト 小宮山功一朗が立候補し、当選を果たしました。今後、2 年間の任期を通して FIRST の運営や FIRST を通じた国際連携の実効性を高めるべく貢献して参ります。FIRST Board of Directors のメンバ構成については、次の URL をご参照ください。

FIRST.Org,Inc., Board of Directors
http://www.first.org/about/organization/directors

6.2.3. National CSIRT Meeting への参加(2014 年 6 月 28 日-29 日)

第 26 回 FIRST 年次会合後に引き続きボストンにて、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、CSIRT 統計に関する発表を行うとともに、オリンピックなどの大規模行事に関連したサイバーセキュリティ対策に関するパネルディスカッションに参加しました。National CSIRT Meeting についての詳細は、以下の URL をご参照ください。

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

6.3. その他の活動

6.3.1. ブログや Twitter を通した情報発信

英語ブログや Twitter(@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。

APCERT DAY at APRICOT and Open Resolver Check Site Launched by JPCERT/CC
http://blog.jpcert.or.jp/2014/04/apcert-day-at-apricot-and.html
Source Port Randomization for Caching DNS Servers Requested, yet again
http://blog.jpcert.or.jp/2014/04/source-port-randomization-for-cache-dns-servers-requested-yet-again.html

Presenting HTML5 security at OWASP AppSec APAC 2014
http://blog.jpcert.or.jp/2014/04/presenting-html5-security-at-owasp-appsec-apac-2014.html

APCERT Annual General Meeting and TSUBAME Workshop by JPCERT/CC
http://blog.jpcert.or.jp/2014/05/apcert-annual-general-meeting-and-tsubame-workshop-by-jpcertcc.html

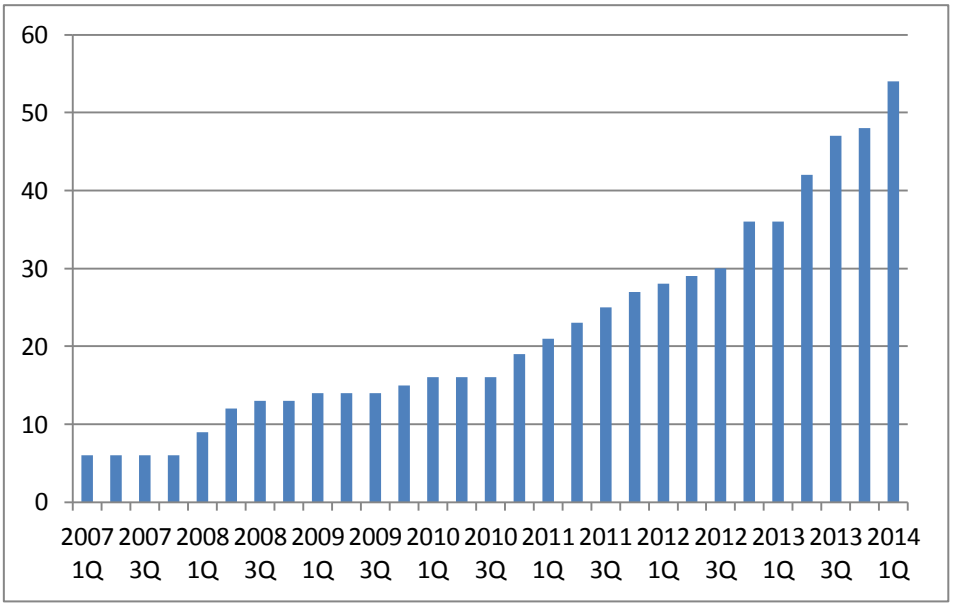
The Heartbleed bug – How Japanese Organizations confront the issue –
http://blog.jpcert.or.jp/2014/06/the-heartbleed-bug---how-japanese-organizations-confront-the-issue-.html

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

7. 日本シーサート協議会(NCA)事務局運営

日本シーサート協議会(NCA：Nippon CSIRT Association)は、国内のシーサート(CSIRT：Computer Security Incident Response Team)組織が互いに協調し、連携して共通の問題を解決する場として設立されました。その事務局として、JPCERT/CC は、NCA の Web サイトの管理や更新を通じた広報活動、協議会の問合せ窓口やメーリングリストを含む会員情報の管理、加盟のためのガイダンスの実施および手続きの運用を担当するとともに、自らも会員として協議会主催の会議およびイベントに参加しています。

本四半期においては、株式会社りそなホールディングス(Resona-CSIRT) 、東日本電信電話株式会社(NTT EAST-CIRT) 、ヤマハ発動機株式会社(YMC-CSIRT)、株式会社リクルートテクノロジーズ(R-Tech Cyber Incident Team) 、グローリー株式会社(G-CSIRT)、株式会社帝国ホテル(I-SIRT)、株式会社ゆうちょ銀行(JPBank CSIRT)、株式会社 FFRI(FFRI)の 8 組織が新規に加盟しました。本四半期末時点で 56 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 7-1]のとおりです。



[図 7-1　日本シーサート協議会 加盟組織数の推移]

4 月に「OpenSSL 情報漏えいを許してしまう脆弱性 ～Heartbleed 問題～ 」および「Struts: ClassLoader の操作を許してしまう脆弱性 (CVE-2014-0094, CVE-2014-0112, CVE-2014-0113) 」について、それぞれレポートを NCA の Web サイトに掲載しました。

OpenSSL 情報漏えいを許してしまう脆弱性 ～Heartbleed 問題～ について
http://www.nca.gr.jp/2014/heartbleed/

Struts: ClassLoader の操作を許してしまう脆弱性 (CVE-2014-0094, CVE-2014-0112, CVE-2014-0113) について
http://www.nca.gr.jp/2014/struts_s20/

5 月に「シーサートフォーラム 2014」を開催し CSIRT をこれから構築したいと考えている企業や組織の方々に約 115 名にご参加いただきました。

CSIRT フォーラム 2014
http://www.nca.gr.jp/2014/csirt-forum/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/

8. 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、協議会名での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、等の活動を行っています。

8.1. 情報収集/発信の実績

本四半期は、協議会 Web サイトや会員向け 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、金融機関をかたるフィッシングや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、金融機関をかたるフィッシングに関しては[図 8-1]の「三井住友カードをかたるフィッシング（2014/04/30）」や[図 8-2]の「りそな銀行をかたるフィッシング(2014/06/16)」を、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、JPCERT/CC のインシデント対応支援活動を通じて行い、すべてについて停止を確認しました。

[図 8-1　三井住友カードをかたるフィッシング（2014/04/30）
https://www.antiphishing.jp/news/alert/smbc_card20140430.html]

[図 8-2　りそな銀行をかたるフィッシング(2014/06/16)
https://www.antiphishing.jp/news/alert/20140220jpbank.html]

8.2. 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掛けるため、あるいは、関連組織との情報交流をはかるための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「Phishing Trends in Japan and the Counteraction as the Council of Anti-Phishing Japan」
APWG　CeCOS VIII　2014 年 4 月 9 日

8.3. 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、毎月の活動報告等を公開しています。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 2014 年 4 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201404.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/201405.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/201406.html

9. フィッシング対策協議会の会員組織向け活動

フィッシング対策協議会では、経済産業省から委託された活動以外に、会費による会員組織向けの活動を、運営委員会の決定に基づいて行っています。

9.1. 総会開催

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平成 25 年度活動および平成 26 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。

(1)平成 26 年度フィッシング対策協議会総会
日時：2013 年 6 月 4 日 14:00 - 16:00
場所：エッサム神田ホール 301 会議室

9.2. 運営委員会開催

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 13 回運営委員会
日時：2014 年 4 月 18 日 16:00 - 18:00
場所：トッパン・フォームズ株式会社

フィッシング対策協議会 第 14 回運営委員会
日時：2014 年 5 月 16 日 16:00 - 18:00
場所：エヌ・ティ・ティ・コミュニケーションズ株式会社

フィッシング対策協議会 第 15 回運営委員会
日時：2014 年 6 月 14 日 16:00 - 18:00
場所：トレンドマイクロ株式会社

10. 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。

10.1. 制御システム用ソフトウエアの脆弱性対策に有効な CERT C コーディングルールの調査レポート

本資料は、制御システム開発者の皆様が「CERT C コーディングスタンダード」を活用してセキュアな製品開発に取り組む契機としていただけるよう、ICS-CERT アドバイザリで公開された制御システム用ソフトウエアの脆弱性を調査し、それらの低減に役立つ 22 個のルールを CERT C コーディングスタンダードの中から抽出しまとめたものです。

本資料に関連した活動の詳細は、「2.5.1」をご参照ください。

制御システム用ソフトウエアの脆弱性対策に有効な CERT C コーディングルールの調査
(2014 年 6 月 2 日公開)
https://www.jpcert.or.jp/research/ics-codingrule.html

10.2. 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

本ガイドラインは、独立行政法人 情報処理推進機構(IPA)、一般社団法人 JPCERT コーディネーションセンター(JPCERT/CC)、一般社団法人 電子情報技術産業協会(JEITA)、一般社団法人 コンピュータソフ

トウェア協会(CSAJ)、一般社団法人 情報サービス産業協会(JISA)、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)が、脆弱性関連情報の適切な流通により、コンピュータ不正アクセス、コンピュータウイルスなどによる被害発生を抑制するために、関係者の方々に推奨する対応をとりまとめたもので、経済産業省告示「ソフトウエア等脆弱性関連情報取扱基準」の改正を踏まえた改訂を加えました。

本資料に関連した活動の**詳細は、「2.2」をご参照ください。**

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
(2014 年 5 月 30 日公開)
https://www.jpcert.or.jp/press/2014.html

10.3. JPCERT/CC 脆弱性関連情報取扱いガイドライン

本ガイドラインは、JPCERT/CC が製品開発者の連絡窓口である製品脆弱性対策管理者の方に期待する役割を中心に、脆弱性関連情報の受領から公表に至るまでのプロセスについて詳細に記述したものです。経済産業省告示「ソフトウエア等脆弱性関連情報取扱基準」の改正および「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」の改訂に対応して改訂しました。

本資料に関連した活動**の詳細は、「2.4.3」をご参照ください。**

JPCERT/CC 脆弱性関連情報取扱いガイドライン Ver5.0
(2014 年 5 月 30 日公開)
https://www.jpcert.or.jp/press/2014.html

10.4. IPv6 セキュリティテスト手順書および検証済み製品リスト

IPv6 対応機器の購入を検討されている企業や組織のシステム担当者の方に、機器選定時の参考資料としてご利用いただくことを目的として、RFC や Internet drafts で指摘されている既知の問題点から、企業がインターネット接続に使用するルータや L3 スイッチなどの IPv6 対応ネットワーク機器においてインターネット経由で攻撃が可能な問題を 15 項目選定し、テスト項目とその検証手順を「IPv6 セキュリティテスト手順書」としてまとめました。また、その手順書に従って IPv6 対応機器ベンダが検証した結果をリスト化した「IPv6 セキュリティテスト検証済み製品リスト(2013 年度版)」としてまとめ、公開しました。

IPv6 セキュリティテスト検証済み製品リスト
(2014 年 4 月 28 日公開、5 月 15 日更新)
https://www.jpcert.or.jp/research/ipv6product_list.html
IPv6 セキュリティテスト手順書(一般公開版)2013 年度版
(2014 年 4 月 28 日公開)
https://www.jpcert.or.jp/research/ipv6product_list.html

10.5. 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（平成 16 年経済産業省告示 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、2014 年 1 月 1 日から 2014 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[2014 年第 1 四半期(1 月～3 月)]
(2014 年 4 月 24 日)
https://www.jpcert.or.jp/press/2014/vulnREPORT_2014q1.pdf

10.6. 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分析するインターネット定点観測を継続的に実施しています。これを、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、インターネット定点観測の結果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 2014 年 1 月～3 月
(2014 年 4 月 21 日)
https://www.jpcert.or.jp/tsubame/report/report201401-03.html

11. 主な講演活動一覧

(1) 伊藤 友里恵(国際部部長,APCERT Chair)
「Developing Cybersecurity Risk Indicators - Metrics」モデレータ
26th annual FIRST Conference BOSTON,2014 年 6 月 23 日
(2) 内山 貴之 (情報セキュリティアナリスト),
小林 裕士(インシデント レスポンス グループ 情報セキュリティアナリスト) :
「Open DNS Resolver Check Site」
26th annual FIRST Conference BOSTON,2014 年 6 月 23 日
(3) 真鍋 敬士(理事,分析センター長) :
「官民一体のサイバー攻撃対策」パネリスト
ITForum & Roundtable,2014 年 6 月 12 日
(4) 真鍋 敬士(理事,分析センター長) :
「サイバー攻撃の傾向と対応への課題」パネリスト
日本 PTC フォーラム 2014,2014 年 6 月 5 日

(5) 重森友行(早期警戒グループ 情報セキュリティアナリスト) :

「今から始める HTML5 セキュリティ」

ばりかた勉強会,2014 年 5 月 24 日

(6) 中津留 勇(分析センター) :

「JPCERT/CC とマルウェアと私」

ばりかた勉強会,2014 年 5 月 24 日

(7) 戸田 洋三(情報流通対策グループ リードアナリスト) :

「JRE 標準ライブラリの脆弱性事例を理解する (AtomicReferenceArray クラスと Type Confusion)」

JJUG CCC 2014 Spring,2014 年 5 月 18 日

(8) 満永 拓邦(早期警戒グループ 情報分析ライン リーダー) :

「企業における情報セキュリティ緊急対応体制～組織内 CSIRT の必要性～」

情報セキュリティ EXPO IPA ブース,2014 年 5 月 14 日~15 日

(9) 佐々木 理(国際部 情報セキュリティアナリスト) :

「Internet Security and CSIRT's mission」

Government Security Day 2014-タイ,2014 年 5 月 14 日

(10) 満永 拓邦(早期警戒グループ 情報分析ライン リーダー 情報セキュリティアナリスト)

「ネットワークセキュリティ」

京都サイバー犯罪対策研究会,2014 年 4 月 18 日

(11) 山本 健太郎(エンタープライズサポートグループ 情報セキュリティアナリスト)

「Phishing Trends in Japan and the Counteraction as the Council of Anti-Phishing Japan」

APWG CeCOS VIII-HongKong,2014 年 4 月 9 日

(12) 真鍋 敬士(理事,分析センター長) :

「組織に期待されるサイバー脅威への取り組み」

テレコムアイザックセミナー新たな脅威に向けた今日と明日,2014 年 4 月 3 日

(13) 有村 浩一(常務理事) :

「JPCERT/CC の制御システムセキュリティへの取組の紹介」

テレコムアイザックセミナー新たな脅威に向けた今日と明日,2014 年 4 月 3 日

12. 主な執筆一覧

(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) :

制御システム用ソフトウェアの脆弱性対策～CERT コーディングスタンダードの活用～

翔泳社 CodeZine,2014 年 6 月 26 日

(2) 瀬古 敏智(エンタープライズサポートグループ 情報セキュリティアナリスト) :

情報システム担当者のための「突撃！ 隣のセキュリティ」(1)

「100 年前から情報セキュリティ」――凸版印刷に見る大規模企業の対策と現実

アイティメディア @IT,2014 年 6 月 11 日

(3) 宮地 利雄(顧問),山田 秀和(制御システムセキュリティ対策グループ リーダー):
「5 分で絶対に分かる制御システムセキュリティ」
アイティメディア @IT,2014 年 5 月 20 日

13. 協力、後援一覧

本四半期においてJPCERT/CCは次の行事の開催に協力または後援をしました。

(1) テレコム・アイザック・セミナー ―新たな脅威に向けた今日と明日―
主 催：一般財団法人日本データ通信協会 テレコム・アイザック推進
開催日：2014年4月3日(木)
(2) 第10回 IPA 「広げよう情報モラル・セキュリティコンクール」2014
主 催：独立行政法人情報処理推進機構
開催日：2014年4月1日(火) ~11月中旬

■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