JPCERT CC®

JPCERT-PR-2010-0003

発行日：2010-07-07

JPCERT/CC 活動概要 [2010 年 4 月 1 日 ～ 2010 年 6 月 30 日]

【活動概要トピックス】

—トピック 1 —

Internet Summit of Africa—アフリカ大陸での CERT ネットワーク構築と指導者トレーニングを展開

5 月 29 日から 6 月 3 日の日程で、ルワンダのキガリにおいて「Internet Summit of Africa」が開催され、アフリカ地域とアジア地域の IT 分野における連携を促進するフォーラムである AAF (Africa Asia Forum on Network Research & Engineering) が主催した複数のセッションで、JPCERT/CC が講師を務めましました。JPCERT/CC の国内外における活動や APCERT の国際連携活動を紹介するとともに、CERT 指導者トレーニングコースにおいてインシデントハンドリングの基礎、CSIRT 構築手法、最近の国際サイバーセキュリティ動向などについて講義を行いました。また、この機会を生かし、IT 利用が急速に進んでいるアフリカ各国のインターネットセキュリティ事情に関する情報の収集や、情報セキュリティ対策に関する人的・技術的ネットワークの構築を進めました。

AAF：Africa Asia Forum on Network Research & Engineering
http://africaasia.net/meetings.html

Internet Summit of Africa の CERT トレーニングセッションプログラム
http://africaasia.net/2010-6-CERT.html

—トピック 2 —

JPCERT/CC が CVE 採番機関に—国内初、調整機関としては世界で 2 組織め

JPCERT/CC は 6 月 23 日に、米国 MITRE 社から、国内初の CNA（CVE Numbering Authorities：CVE 採番機関）に認定されました。CVE は、全世界でソフトウエアの脆弱性情報を一元管理する

ためのデータベースであり、米国 MITRE 社がその運営を行なっています。発見または届出のあった脆弱性情報に一意の ID を割り当て、CVE データベースに登録できるのは、MITRE 社の他は、Microsoft 社、Oracle 社、Adobe 社などグローバルに展開する一部の大手製品ベンダーや脆弱性情報ベンダーのみで、日本の組織としては初の認定となります。また、調整機関として脆弱性情報に採番できるのは、これまでは米国の CERT/CC のみでしたが、JPCERT/CC が世界で 2 組織めとして認定されました。

今般の CNA 認定は、JPCERT/CC の脆弱性情報ハンドリングや分析活動の実績が認められたことによるものであり、日本のソフトウエアに関し、グローバルに影響を与える可能性のある脆弱性情報を、CVE の枠組みを利用して正しく発信するイニシアティブが発揮できるようになったという意味で重要です。

プレスリリース：JPCERT/CC、国内初の CNA に認定
https://www.jpcert.or.jp/press/2010/PR20100624_cna.pdf

CVE：Common Vulnerabilities and Exposures
https://cve.mitre.org/

―トピック 3 ―

FIRST Conference MIAMI 参加―インシデントの高度化に伴う組織内インシデント対応体制強化及び CSIRT/CERT 組織間、政府機関などとの連携強化の必要性を再確認

2009 年の京都での FIRST Conference 開催から 1 年が経過し、今年の FIRST Conference は、米国フロリダ州マイアミにおいて、6 月 13 日から 18 日の日程で開催されました。JPCERT/CC からも理事およびメンバーとして参加しました。今回は、アメリカの IT 系企業や政府機関が高度に計画されたサイバー攻撃を受け、内部ネットワークへの進入を許してしまったことなどを受け、各組織におけるインシデント対応体制の整備について、その重要性がさらに高まっていること、また国家間の連携として CERT/CSIRT 組織間、及び政府系機関などとの連携強化が活発化していることなどが注目を集めていました。

JPCERT/CC では、米国やアジア太平洋地域をはじめとする各国の National CERT、政府機関との意見交換を行なうなど、連携関係の一層の強化に努めました。

22nd Annual First Conference MIAMI
http://conference.first.org/

JPCERT CC®

—活動概要—

目次

本活動は、経済産業省より委託を受け、「平成２２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２２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「**5.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、「**7.講演活動一覧**」及び「**8.執筆・執筆記事一覧**」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。

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報告のうち、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 3,113 件、インシデントの件数は 3,185 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 847 件でした。前四半期の 1,005 件と比較して約 16%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、現状の調査と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/2010/IR_Report20100707.pdf

1-1-1-1. インシデントの傾向

本四半期は、特に国内のポータルサイトを装った「フィッシングサイト」と「Web サイト改ざん」の報告が多く寄せられました。

本四半期のフィッシングサイトのインシデント件数は、388 件でした。前四半期の 373 件から若干増加しました。このうち、国内のブランドを装ったフィッシングサイトの件数は、157 件でした。前四半期の 77 件から増加しています。

フィッシングサイトの被害ブランドの国内・国外別の件数は次のとおりです。

国内のブランドを装ったフィッシングサイトの件数： 157 件
国外のブランドを装ったフィッシングサイトの件数： 186 件
被害ブランドの国内外の別が不明な件数： 45 件

また、Web サイト改ざんのインシデント件数は、561 件でした。前四半期の 809 件から減少しています。本四半期の 561 件の大半は、いわゆる Gumblar ウイルスによる Web サイト改ざん攻撃でした。この攻撃は時とともに変化し続けており、2010 年 4 月には JDK および JRE の未修正の脆弱性を攻撃する手法が確認されました。また、この攻撃で感染するマルウエアの中に新たに DDoS 攻撃を行うものが追加されたことを確認しています。さらに、2010 年 6 月には、Windows XP/2003 に含まれる Windows のヘルプとサポートセンター機能の未修正の脆弱性を攻撃する手法を確認しています。今後も新しく発見される脆弱性が組み込まれるなど攻撃が変化していく可能性があります。

Oracle Sun JDK および JRE の脆弱性に関する注意喚起
https://www.jpcert.or.jp/at/2010/at100010.txt

いわゆる Gumblar ウイルスによってダウンロードされる
DDoS 攻撃を行うマルウエアに関する注意喚起
https://www.jpcert.or.jp/at/2010/at100011.txt

Windows のヘルプとサポートセンターの未修正の脆弱性に関する注意喚起
https://www.jpcert.or.jp/at/2010/at100016.txt

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。

インシデントの報告方法の詳細
https://www.jpcert.or.jp/form/

インシデントの報告 （Web フォーム）
https://form.jpcert.or.jp/

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を対象とした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ながら、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」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」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

本四半期においては、JPCERT/CC のホームページ、RSS、約 24,000 名の登録者を擁するメーリングリストなどを通じて、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関する情報を提供しました。

発行件数：10 件　https://www.jpcert.or.jp/at/

2010-06-30　Adobe Reader 及び Acrobat の脆弱性に関する注意喚起 (公開)
2010-06-28　Windows のヘルプとサポートセンターの未修正の脆弱性に関する注意喚起 (公開)
2010-06-11　Adobe Flash Player および Adobe Acrobat/Reader の脆弱性に関する注意喚起 (公開)
2010-06-09　2010 年 6 月 Microsoft セキュリティ情報 (緊急 3 件含) に関する注意喚起 (公開)
2010-06-01　社内 PC のマルウエア感染調査を騙るマルウエア添付メールに関する注意喚起 (公開)
2010-05-12　2010 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 (公開)
2010-04-28　いわゆる Gumblar ウイルスによってダウンロードされる DDoS 攻撃を行うマルウエアに関する注意喚起 (公開)
2010-04-16　Oracle Sun JDK および JRE の脆弱性に関する注意喚起 (公開)
2010-04-14　Adobe Reader 及び Acrobat の脆弱性に関する注意喚起 (公開)
2010-04-14　2010 年 4 月 Microsoft セキュリティ情報 (緊急 5 件含) に関する注意喚起 (公開)

1-2-1-2. Weekly Report

JPCERT/CC が得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/

JPCERT/CC レポート内で扱った情報セキュリティ関連情報の項目数は、合計 59 件、「今週のひとくちメモ」のコーナーで紹介した情報は 12 件でした。

1-2-2. 脅威の動向について

前四半期に続き、いわゆる Gumblar ウイルスによる Web サイトの改ざん被害が続いています。6 月に発表された Adobe の Flash や Acrobat の脆弱性、Microsoft Windows のヘルプとサポートセンターの脆弱性などについては、ベンダーが更新プログラムを公開する前から攻撃が行われていました。中にはいわゆる Gumblar ウイルスの攻撃手法に組み込まれたものもありました。
OS やアプリケーションについて最新のセキュリティアップデートの適用を励行するとともに、ウイルス対策ソフトの定義ファイルを最新に維持してください。同時に未修正の脆弱性に対するワークアラウンドの実施などを慎重に検討してください。

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 ページなどでも公開しています。

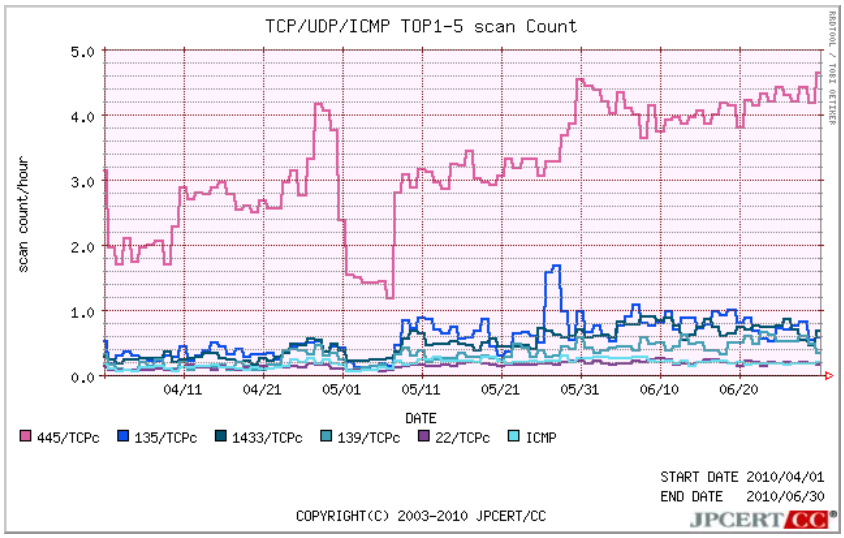
1-3-1. ポートスキャン概況

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

JPCERT/CC インターネット定点観測システムの説明
https://www.jpcert.or.jp/isdas/readme.html

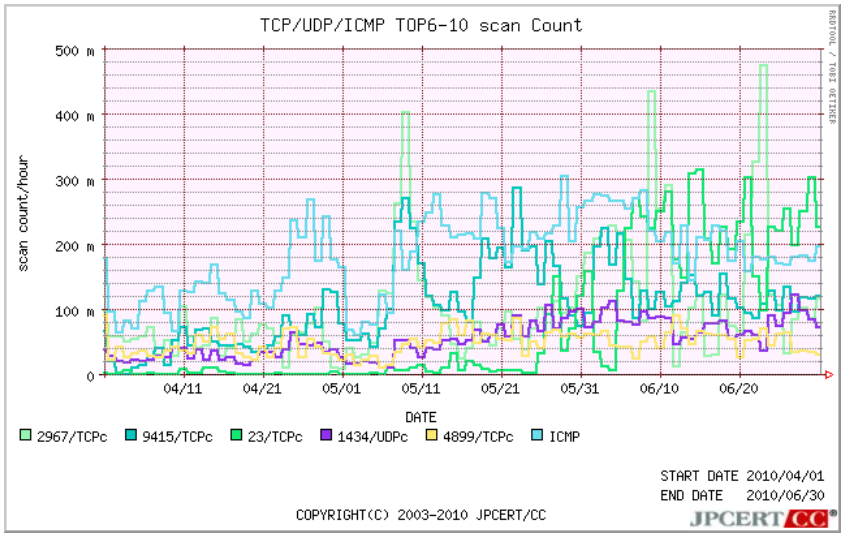
本四半期に ISDAS で観測されたアクセスの宛先ポートの上位 1 位～5 位および 6 位～10 位のそれぞれについて、アクセス数の時間的の推移を[[図 1-1]と[[図 1-2] に示します。

- アクセス先ポート別グラフ top1-5 (2010 年 4 月 1 日-6 月 30 日)



[図 1-1 アクセス先ポート別グラフ top1-5]

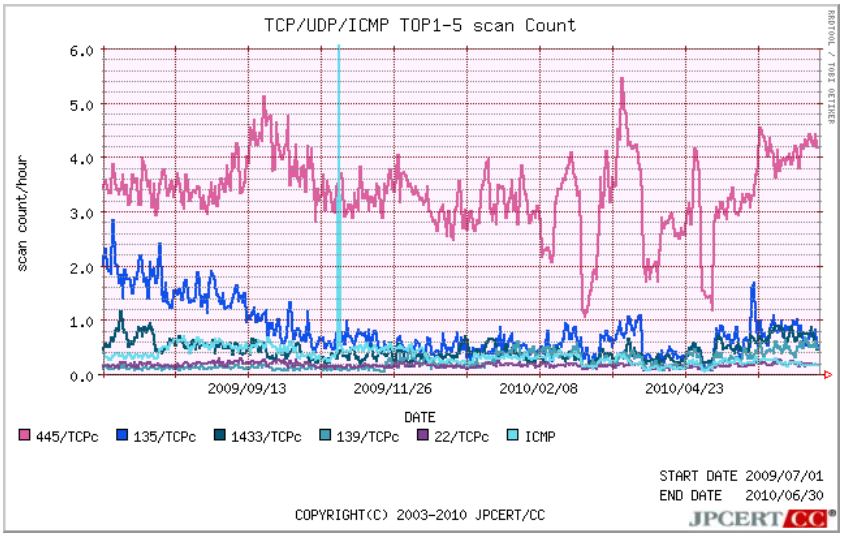
- アクセス先ポート別グラフ top6-10 (2010 年 4 月 1 日-6 月 30 日)



[図 1-2 アクセス先ポート別グラフ top6-10]

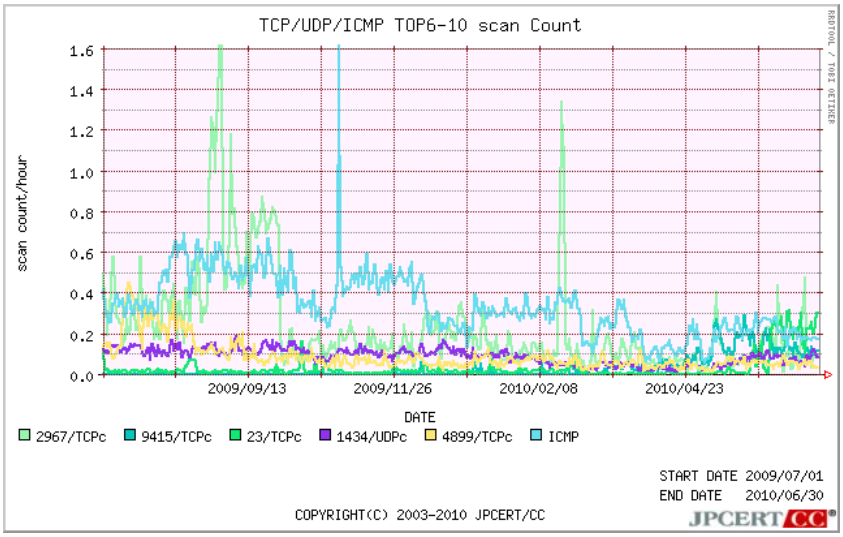
また、より長期間のスキャン推移を見るため、2009 年 7 月 1 日から 2010 年 6 月 30 日までの期間における、アクセスの宛先ポートの上位 1 位～5 位および 6 位～10 位のそれぞれについて、アクセス数の時間的の推移を[図 1-3]と[図 1-4]に示します。

- アクセス先ポート別グラフ top1-5 (2009 年 7 月 1 日-2010 年 6 月 30 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 (2009 年 7 月 1 日-2010 年 6 月 30 日)



[図 1-4　アクセス先ポート別グラフ top6-10]

引き続き、Windows や Windows 上で動作するソフトウエア、リモート管理を行うためのプログラムが利用するポートを対象とした攻撃や弱点探索活動が上位を占めています。新しく脆弱性が見つかっていないソフトウエアに対しても Scan が行われています。既知の脆弱性の対策漏れが探索されている可能性もありますので、OS やアプリケーションに脆弱性を修正する修正プログラムを適用しているか、ファイアウォールやウイルス対策ソフトなどが正しく機能しているか、今一度確認することが重要です。今期は「9415/TCP」という日本国内ではあまり使われていないポートへの Scan が増加しました。これは中国国内に利用者がいると考えられる、Proxy ソフトが使っているポート番号です。適切なアクセス制御がされていない場合、第三者がこの Proxy ソフトが動作しているコンピュータを経由して Web サーバなどへの攻撃を行う可能性があります。

また、Microsoft 社 Windows 2000 製品群の延長サポートや、Windows XP の SP2 は 2010 年 7 月 13 日（米国時間）でサポートが終了し、その後はセキュリティ・パッチなどの提供がなくなる予定です。これらの製品をまだお使いの場合、速やかにサポート期間中の製品への移行を検討してください。

1-4. 日本シーサート協議会 (NCA) 事務局運営

JPCERT/CC は、国内のシーサート(CSIRT: Computer Security Incident Response Team)の活動を支援する日本シーサート協議会の事務局運営を行っています。事務局では、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 ページ、メーリングリスト等の管理を行っています。

活動の詳細については、以下の URL をご参照ください。

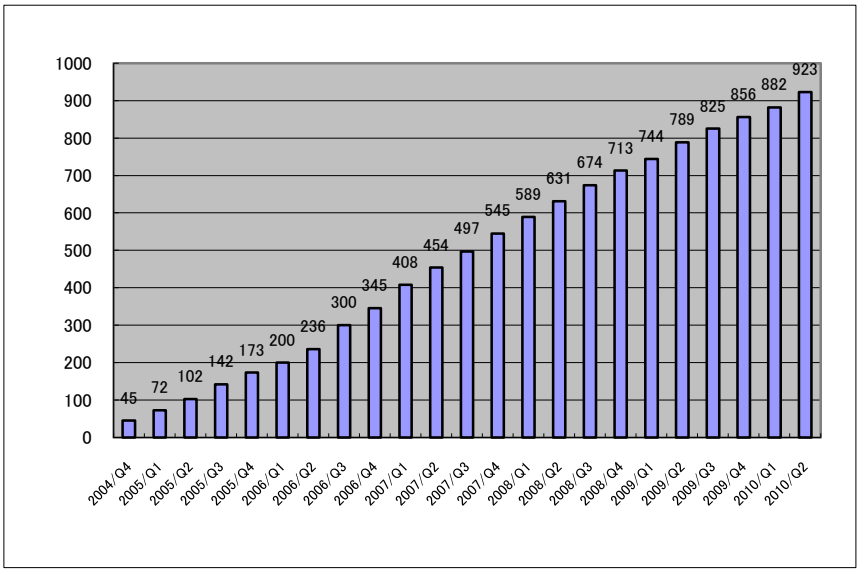
日本シーサート協議会 Web ページ
http://www.nca.gr.jp/

2. 脆弱性関連情報流通促進活動

JPCERT/CC では、脆弱性情報を適切な範囲に適時に開示し、対策の促進を図るための活動を行っています。国内では、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」に指定されています。
また、米国 CERT/CC (http://www.cert.org/)や英国 CPNI (http://www.cpni.gov.uk/) と協力関係を結び、国内のみならず世界的な規模で脆弱性関連情報の流通促進業務を進めています。

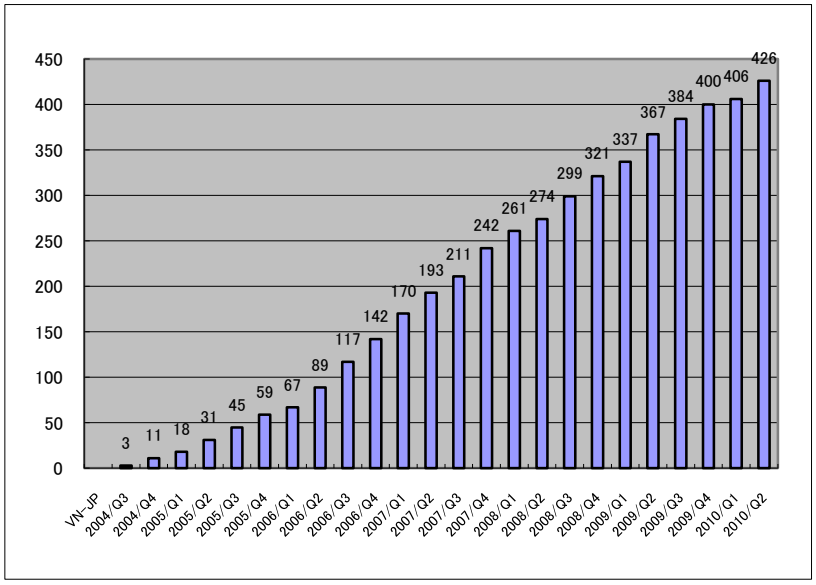
2-1. Japan Vulnerability Notes (JVN) において公開した脆弱性情報および対応状況

本四半期に JVN において公開した脆弱性情報は 41 件 (累計 923 件) [図 2-1] でした。公開された個々の脆弱性情報に関しては、JVN(https://jvn.jp/)をご覧ください。



[図 2-1　累計 JVN 公表累積件数]

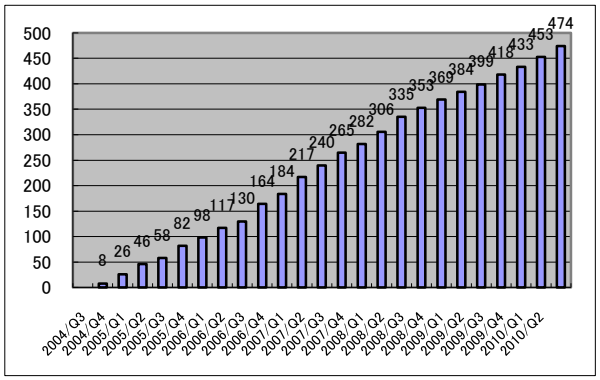
このうち、本基準に従って調整を行い、JVN で公開した脆弱性情報は 20 件(累計 426 件) [図 2-2] でした。これは、前四半期（6 件）と比較すると約 3 倍となりました。今期の公開数が増加した要因としては、複数の脆弱性が併せて修正、公開された製品が多かったことが挙げられます。



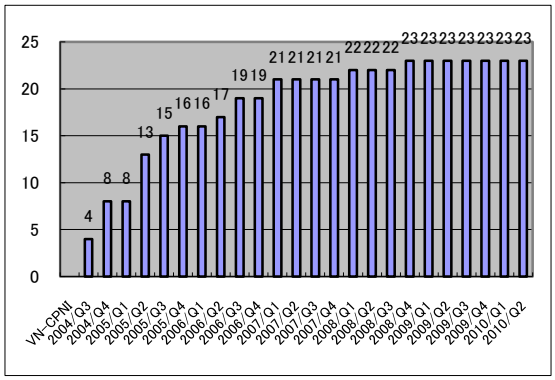
[図 2-2　累計 VN-JP 公表累積件数]

また、CERT/CC とのパートナーシップに基づいて調整を行い、JVN にて VN-CERT/CC として 公開した脆弱性情報は 21 件(累計 474 件) [図 2-3]でした。このうち 1 件(JVNVU#545953)は、フィンランドの CERT-FI が国際調整を担当しました。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 VN-CPNI として公開した脆弱性情報は 0 件(累計 23 件) [図 2-4] でした。

本四半期中に VN-CERT/CC として公開された脆弱性情報には、Microsoft 製品に関するものが 4 件、Adobe 製品に関するものが 4 件含まれています。また、今期は Oracle 製品に関するものが 3 件公開されました。



[図 2-3　VN-CERT/CC 公表累積件数]



[図 2-4　累計 VN-CPNI 公表累積件数]

2-2.　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 では、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、米国 CERT/CC や英国 CPNI などの海外 CSIRT との間で、報告され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、脆弱性情報の公表時期の設定などの調整活動を行っています。

また、2008 年 5 月 21 日から JVN 英語版サイト(https://jvn.jp/en)の運用を開始し、2008 年 8 月からは、JVN 上で公表する脆弱性情報に対する CVE (Common Vulnerabilities and Exposures) 番号の取得を積極的に推進しました。それ以降に JVN で公開されたものについては、約 9 割に CVE 番号が付与されています。また、JVN 英語版サイトへのアクセス数も徐々に増加しており、海外の主要セキュリティ関連組織などからも注目されるようになっていることがうかがえます。昨今は、海外の組織から公開されるアドバイザリの多くが、JVN 英語版サイトへのリンクを掲載しています。

JPCERT/CCは、2010年6月23日、米国MITRE社より、日本においては初の、中立調整機関としてはCERT/CCに次いで2組織めとなるCNA（CVE Numbering Authorities、CVE採番機関）に認定されました。これは、世界の脆弱性関連情報流通の枠組みにおいて、代表的な調整機関として重要な役割を担うJPCERT/CCの機能と実績が認められたものです。CNA に認定されたことにより、国内のパートナーシップや海外から報告された脆弱性関連情報に自らの判断でCVE 番号を付与できるようになりました。情報セキュリティ早期警戒パートナーシップの運用においては、これまでも個々の脆弱性ごとにMITRE社に対して採番依頼を行い、CVEに準拠した脆弱性情報の開示を行ってきましたが、JPCERT/CC がCNA になったことにより、より一貫したCVE との整合性

が確保されることになります。

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

MITRE 社は、CVE に関連して、CVE 識別番号の正確な表示、適切な情報関連付け、CVE 識別番号による情報の検索などを条件に、脆弱性情報ポータルサイトに対して「CVE 互換(CVE Compatibility)」のブランドを認定しています。JPCERT/CC および IPA も、2009 年 1 月に、JVN、JVN iPedia、MyJVN について CVE 互換宣言（Declaration of CVE Compatibility）を行い、約 1 年の審査期間を経て 2010 年 1 月に正式な CVE 互換の脆弱性対策情報提供サイトとして認定されました。これを受け、6 月 24 日より、これらのサイト上に CVE 互換ロゴを表示しています。

CVE 互換に関する詳細は、次の URL をご参照ください。

News & Events January 8, 2010
“Three Products and Services from Two Organizations now registered as Officially CVE-Compatible”
http://www.cve.mitre.org/news/index.html#jan082010a

CVE-Compatible Products and Services
https://cve.mitre.org/compatible/compatible.html#j

2-3.　日本国内の脆弱性情報流通体制の整備

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

脆弱性情報取扱体制
http://www.meti.go.jp/policy/netsecurity/vulhandlingG.html

脆弱性情報コーディネーション概要
https://www.jpcert.or.jp/vh/
「情報セキュリティ早期警戒パートナーシップ」の運用を開始
https://www.jpcert.or.jp/press/2004/0708.txt
情報セキュリティ早期警戒パートナーシップガイドライン(改訂版)
https://www.jpcert.or.jp/vh/partnership_guide2009.pdf
JPCERT/CC 脆弱性情報取り扱いガイドライン
https://www.jpcert.or.jp/vh/guideline_2009.pdf

本四半期の主な活動は以下のとおりです。

2-3-1. 受付機関である独立行政法人情報処理推進機構 (IPA) との連携

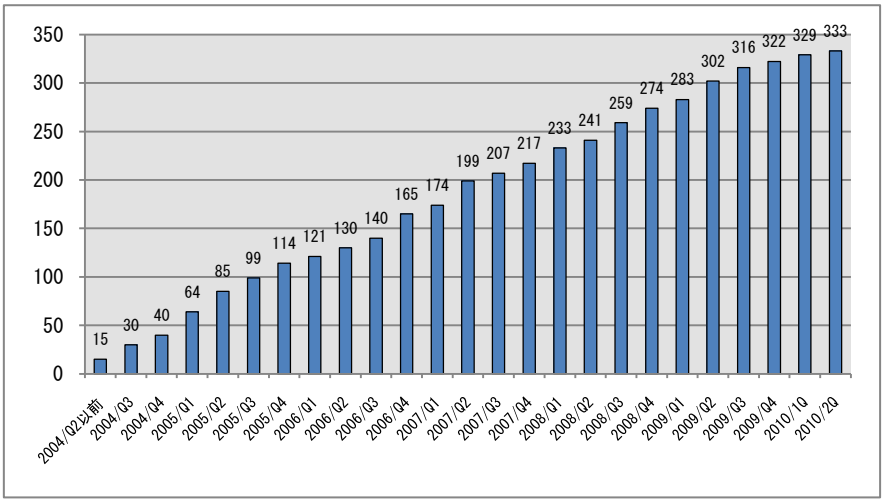
本基準では、受付機関に IPA (http://www.ipa.go.jp/)、調整機関に JPCERT/CC が指定されています。JPCERT/CC は IPA が受け付けた届出情報の転送を受けて、製品開発者への情報提供を行い、対策情報公開に至るまでの調整を行っています。最終的に IPA と共同で JVN にて対策情報を公開しています。両組織間においては緊密な情報の交換、脆弱性情報の分析等を行っています。なお、本基準における IPA の活動および四半期毎の届出状況については次をご参照ください。

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

2-3-2. 日本国内製品開発者との連携

本基準では、JPCERT/CC が脆弱性情報を提供する先として、日本国内の製品開発者リスト(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、やや増加率が鈍化してきているものの、2010 年 6 月 30 日現在で 333 社の製品開発者の皆様にご登録をいただいています。

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]

また、2009 年 7 月 10 日に改定した「JPCERT/CC 脆弱性関連情報取扱いガイドライン」に基づき、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なケースへの対応について、関係機関と協議をしながら、具体的な運用手順の整備を進めています。

2-3-3.　脆弱性情報流通体制の普及啓発

オープンソースソフトウエアやその他の製品開発者およびコミュニティに対して、日本国内の脆弱性情報流通体制の認知を向上し、相互理解を深めるため、2010 年 6 月 26 日に開催された Open Source Conference 2010 Hokkaido へ参加しました。脆弱性情報ハンドリング業務内容と活動状況、その他の JPCERT/CC の活動内容について紹介し、オープンソースソフトウエア分野における脆弱性対応に関する意見交換、情報交換を行いました。

2-3-4.　「脆弱性情報開示」の国際標準化活動への参加

ISO/IEC JTC-1/SC27 WG3 において検討されている、製品開発者による脆弱性関連情報の受取と発信のためのガイドラインである「脆弱性情報開示」(29147；以前の Responsible Vulnerability Disclosure (RVD)から単に Vulnerability Disclosure (VD)に名称を変更)の標準化は、4 月 19～23 日にマレーシアの Melaka で開催された SC27 国際会議での議論を経て改訂され、第 1 次委員会草案(CD: Committee Draft)として 6 月に参加各国に送付されました。

2010 年 1 月中旬に SC27 事務局を通じて参加各国に配付されていた第 4 次作業草案(WD: Working Draft)に対して、国内委員会でのメール議論も反映しつつ、後半部分を中心として、総数で 72 項目に及ぶ修正提案を用意して、4 月の SC27 国際会議に望みました。日本以外からも、ベルギーから 15 項目，カナダ 11，フィンランド 15，英国 46 (うち 33 項目は FIRST からのコメントを再掲)，米国 58，南アフリカ 19，FIRST から 33 項目の、合計 236 項目の修正提案がありました。

SC27 国際会議では、これらの取扱を一つ一つ審議しました。今回の大きな修正としては、名称から「責任ある」(Responsible)を取り除いたことや、「概念」と題して第 5 章に、脆弱性の取扱に関する一般的な説明を置くことになった点などが上げられます。また、一部の参加国からは、参考情報としてのガイドラインではなく、規範的な(normative)記述を中心とし、準拠性を判定できるような標準にすべしとの主張がなされましたが、1) このプロジェクトは、ガイドラインを作成する提案として承認されたものであり、これを WG3 の中で勝手に変更することに手続き的な疑問がある、2) 前回(Redmond)の会議で、オンライン・サービスまでを対象とすることになったため、ハードウェアからサービスにまで共通した要求条件は常識的な範囲に限定されることになり読者にとって得られるものが極端に少なくなる、の 2 つの問題点を指摘して反対した日本と米国の説得が受け入れられました。また、提案国であるカナダ他が、従来以上に多数の国から意見が得られるようになる等の理由を上げて、委員会草案(CD)への格上げを強く求めました。日本や米国は、まだ大幅な構成変更を含む修正提案コメントが出ていて時期早尚であると反対しましたが、最終的には格上げされることとなりました。

6 月に送付された第 1 次委員会草案に対しては、SC27 の参加各国は 9 月 10 日まで投票するよう求められており、JPCERT/CC では、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。

2-4. セキュアコーディング啓発活動

2-4-1. C/C++セキュアコーディングセミナー2010@福岡の開催

5 月 27 日、28 日の 2 日間にわたり、福岡ソフトリサーチパークにおいて C/C++セキュアコーディングセミナーを実施しました。今回が初めてとなる九州地区での開催は、両日ともにほぼ満員の約 50 名の方にご参加いただき、好評のうちに終了しました。

本セミナーは、5 月 27 日の「part1. セキュアコーディング概論・文字列」と 5 月 28 日の「part2. 整数・コードレビュー」の 2 回構成で実施しました。
「part1. セキュアコーディング概論・文字列」は、受講者にセキュアコーディングの必要性や重要性の理解を促す「セキュアコーディング概論」にはじまり、C/C++言語における「文字列」の脆弱性に関する講義、その講義内容について受講者の理解を深めるための「演習」という構成で実施しました。「part2. 整数・コードレビュー」は、C/C++言語における「整数」の脆弱性に関する講義とその内容に関する「演習」、最後に脆弱性を含むサンプルコードを実際にレビューしながら修正方法を検討する「コードレビュー」、という構成で実施しました。

受講者と講師の間で活発な議論や質疑応答が随所で行われるなど受講者の積極的な姿勢が見られ、受講者の意識の高さ、技術レベルの高さが感じられるセミナーとなりました。

[図 2-6　講義の様子]

2-4-2.　OWASP「ソフトウエアセキュリティ保証成熟度モデル」を公開

OWASP(Open Web Application Security Project) の OpenSAMM プロジェクトが作成した開発者向けドキュメント”Software Assurance Maturity Model”の日本語版「ソフトウエアセキュリティ保証成熟度モデル」を公開しました。

https://www.jpcert.or.jp/securecoding_materials.html

本ドキュメントは、既にセキュアなソフトウエア開発に取り組んでいる、あるいはこれから取り組もうとしている組織やプロジェクトによる、より成熟したセキュア開発を支援するために公開したものです。既存のセキュア開発プロセスの評価や、新たなプロセスの設計、実践のための指針などを提供しています。

セキュアコーディングに関する資料と合わせて、セキュア開発に取り組む際の手引きとしてご活用ください。

2-4-3.　開発者向けウェブマガジン CodeZine にセキュアコーディング解説記事の連載

翔泳社の開発者向けウェブマガジン CodeZine に「実例で学ぶ脆弱性対策コーディング」と題したシリーズで C/C++セキュアコーディングの解説記事を連載しています。これまでの連載では CERT C セキュアコーディングスタンダードの内容を紹介してきましたが、今回の連載記事では、実際に脆弱性が作り込まれたオープンソースソフトウエアのコードを例にコードレビューを行い

ながら脆弱性の原因とその対策を解説するというスタイルで、より実践的な内容を紹介しています。

第 1 回「glib ライブラリに潜む脆弱性をつぶすパッチ」(5 月 20 日公開)
第 2 回「TIFF ライブラリに潜む脆弱性をつぶすパッチ」(5 月 27 日公開)
第 3 回「画像処理ソフトウエア「ImageMagick」の脆弱性」(6 月 15 日公開)
第 4 回「Samba smbclient – 書式指定文字列に潜む脆弱性」(6 月 22 日公開)

CodeZine (コードジン)
http://codezine.jp/

2-4-4. 「CERT C Secure Coding Standards 日本語版」を改訂し 1 つのカテゴリと 76 のレコメンデーションを追加

「CERT C セキュアコーディングスタンダード」は、C 言語のソフトウエア開発においてソフトウエアの脆弱性につながりやすいコーディングエラーを特定し、その対策方法について解説したコーディング規約です。

6 個のレコメンデーションを含む新規カテゴリ Application Programming Interface (API)を追加するとともに、既存のカテゴリにも 76 個のレコメンデーションを追加しました。昨年 9 月に出版した書籍『CERT C セキュアコーディングスタンダード』(アスキー)と合わせて、本 Web 版もご利用ください。

https://www.jpcert.or.jp/sc-rules/

2-4-5. セキュアコーディングに関する講演

JPCERT/CC セキュアコーディングプロジェクトでは、セミナー開催以外にも各種イベントや大学等での講演、講義を行っております。本四半期に行った講演、講義は下記のとおりです。

「ソフトウエアセキュリティ保証成熟度モデル「SAMM」について」久保正樹
Fortify ソフトウエアセキュリティ・アシュアランスセミナー, 2010 年 5 月 19 日

「セキュアコーディング概論」久保正樹
セキュリティシステム特論@東京工科大学大学院, 2010 年 6 月 11 日

「あなたのコードにセキュアコーディングスタンダード」戸田洋三
オープンソースカンファレンス 2010 Hokkaido, 2010 年 6 月 26 日

講義、講演のご依頼、お問合わせについては secure-coding@jpcert.or.jp までご連絡下さい。

2-5. 制御システムセキュリティに関する啓発活動

2-5-1. 「グッド・プラクティス・ガイド パッチ管理」など新たに２つの文書を公開

次の２つの文書を新たに邦訳し、JPCERT/CC Web ページの制御システムセキュリティコーナー(https://www.jpcert.or.jp/ics/)で 5 月 31 日に公開しました。

1) 「グッド・プラクティス・ガイド　パッチ管理」
パッチ管理は、運用環境への暫定的なソフトウエアリリースの展開と保守を管理するための手順です。事業のためにシステムの実効性と効率を維持しつつ、セキュリティの脆弱性を最小限まで緩和し、実運用環境の安定性を維持するのに役立ちます。本書は、重要国家インフラに関わる組織向けにパッチ管理に関するガイドを示したもので、すべてのシステムにパッチを正しく適用するための 4 段階の手順と、パッチ適用計画の有効性を測定するための指標について説明しています。本書は、CPNI（国家インフラストラクチャ保護局）の前身である、NISCC（国家情報インフラ安全調整局）が 2006 年 10 月に発行した文書の邦訳です。

2) 「制御システム環境におけるサイバーセキュリティ文化の支援を目的とした運用セキュリティ（OPSEC）の使用」
大部分の組織は、制御システム領域においても堅牢なアーキテクチャを採用し、外部ネットワーク、業務ネットワーク、制御システムネットワークの統合を推し進めることで業務の強化とコスト削減を図っています。セキュリティは、関係者が形成するサイバーセキュリティ「文化」によって支えられ、運用セキュリティ(OPSEC）の手法を使用することでセキュリティ「文化」の維持・強化への取組みを促進できます。しかし、事務処理領域でのセキュリティを主眼に形成された文化は、制御システムの領域に簡単には持ち込めません。本書は、制御システム領域におけるサイバーセキュリティの開発、配備、改善を担当する管理者およびセキュリティ専門家を対象に、制御システムおよび産業ネットワークのサイバーセキュリティにとって非常に重要な運用セキュリティ(OPSEC）のいくつかの要素を示し、それらがセキュリティ文化の形成をどのように促進し得るかについて述べています。本書は 2007 年 2 月、INL（米国アイダホ国立研究所）から発行された文書の邦訳です。

今後も、JPCERT/CC に寄せられる要望等を参考に、ニーズや時宜を得た文書の翻訳や紹介を行っていく予定です。

2-5-2. セキュリティ・アセスメント・ツールの調査

前四半期に引き続き、セキュリティ・アセスメント・ツールを関係者に提供するための活動を進めました。米国 DHS が開発した CSET(CS^{2}SAT の後継版)と英国 CPNI が開発した SSAT の 2 種類のツールについて、どのような業界への適用が最も効果的かについて関係者の意見を聴取するため以下の説明会を開催し、併せてツールが準拠する複数の標準と制御システムを利用するセクターの適合関係マトリクスの作成などを進めました。

4 月 13 日 MfgX（Manufacturing XML Promotion Forum: 製造業 XML 推進協議会）運営委員会
6 月 16 日 SICE/JEITA/JEMIMA 合同 WG

前期に説明会を実施し WG 内で試用を開始しているため、CSET、SSAT 両者のさらに詳細な差異の説明や、どのように使い分けるべきかといった意見交換を行いました。

SICE/JEITA/JEMIMA 合同 WG が、今秋開催される「計測展 2010」において同ツールの紹介を行う予定であることから、今後もサポートを継続いたします。また MfgX 委員会の後継組織である IAF（Industrial Automation Forum）においても継続して活動する予定です。

2-5-3. 制御システムベンダーセキュリティ情報共有タスクフォースへの情報発信

制御システム開発関係者にセキュリティ関係の情報を提供するニュースレターを計 3 回 (4 月 2 日、5 月 13 日（いずれも号外）および 5 月 28 日) 配信しました。タスクフォースメンバー向けに、セキュリティインシデントに係る事例や関係する標準の動向、技術情報に関するニュースなどを収集して掲載しています。今回はセキュリティ関連資料の公開やセミナーの開催をいち早くお知らせするための号外を発信いたしました。
今後とも、タスクフォースメンバーの要望等を収集し、内容の充実を図っていく予定です。
このニュースレターは、制御システムベンダーセキュリティ情報共有タスクフォースのメンバーであれば、どなたでも受信できます。タスクフォースへの参加資格や申込方法については、次の URL をご参照ください。

制御システムベンダーセキュリティ情報共有タスクフォース
https://www.jpcert.or.jp/ics/taskforce.html

なお、今期中には、タスクフォースへの参加資格の拡充（制御系ユーザーも参加可能とする等）を検討する予定です。

2-5-4. 関連学界活動

ほぼ毎月開かれている SICE (計測自動制御学会) ネット部会や、JEMIMA (日本電気計測工業会) などによる合同セキュリティ検討 WG の活動に参加し、制御システムのセキュリティをめぐって、制御システムの専門の方々と意見交換を行いました。JPCERT/CC の今期以降のアクションプランのひとつである「ユーザ企業のために対策が必要な脆弱性情報抽出方法の検討」を推進するため、WG メンバーとの意見交換を今後も意欲的に実施して行く予定です。

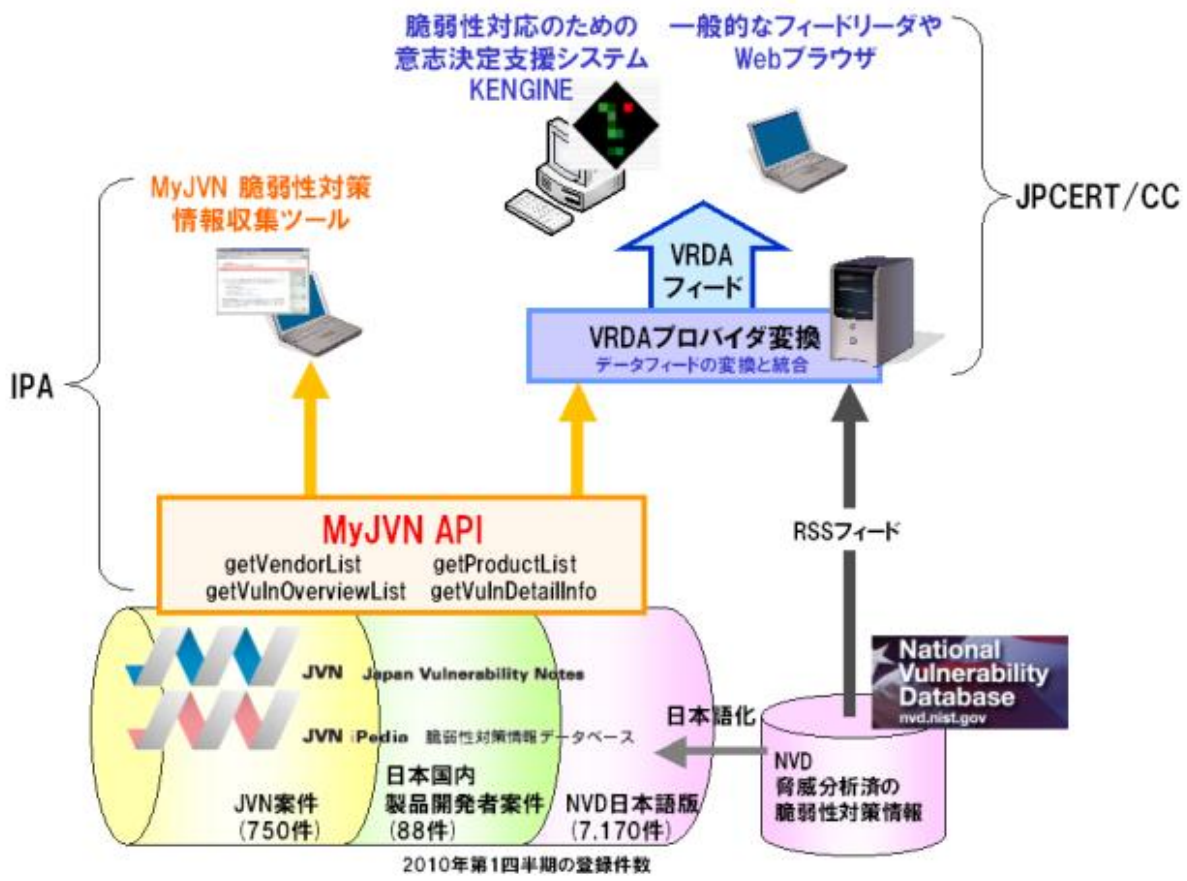
2-5-5. 国際連携活動

米国 DHS 傘下に昨秋設置された ICS-CERT (Industrial Control System CERT)を訪問し、活動概要などを中心に情報交換と意見交換を行いました(6 月 9 日)。この組織の現在の活動は、次の 4 項目を柱として展開されており、連携できる分野を模索しつつ、継続的な情報交流をはかっていきたいと考えています。

1) **情報の提供を含む注意喚起**： 大統領府の CNCI (Comprehensive National Cyber security Initiative)の下で収集された情報を含む各種の注意喚起情報を公開(Web サイト)または非公開(US-CERT のポータルサイト)で関係者に配布しています。
2) **脆弱性とマルウエアの解析**： 多数の脆弱性情報を取り扱ってきていますが、関係者に通知するのみで、一般公開したものはほとんどありません。
3) **インシデント対応**： 制御システムのインシデント発生に際して、ICS-CERT から専門家を現地に派遣して当事者とともに対応や原因解析を行っています。
4) **国内外の官民連携**： 政府内の DHS 以外の省庁や米国の大学や研究所、さらには海外の制御システム関係者と幅広い連携関係を維持しています。

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、KENIGINE などのツールを用いて脆弱性に対する対応を体系的に判断できるようにするため、VRDA (Vulnerability Response Decision Assistance)フィードによる脆弱性情報の配信を行ってきました。この VRDA フィードに関し、データ配信数の増加などの利便性を向上させるため、6 月 2 日より 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する、[[図 **2-7**]に示すような方式への切り替えを行いました。



[図 2-7　MyJVN API を利用した VRDA フィード]

なお、MyJVN API との連携に伴い、VRDA フィードで配信する脆弱性の脅威分析項目として、共通脆弱性評価システム CVSS (Common Vulnerability Scoring System) における、脆弱性評価基準の基本評価基準で定義された分析項目を新たに採用することにしました。

VRDA フィード、MyJVN API についてのより詳しい情報は以下をご参照ください。

- VRDA フィード
  脆弱性への対応判断を行う際に必要となる脆弱性の脅威を把握するための情報を、基準となる分析項目とそれら項目に対応する分析値としてとりまとめ、定型データフォーマットで表現して配信するものです。

  https://www.jpcert.or.jp/vrdafeed/index.html

- MyJVN API
  処理推進機構（IPA）により提供されている MyJVN API は、JVN iPedia の情報を、Web を通じて利用するためのソフトウエアインタフェースです。

https://jvndb.jvn.jp/apis/index.html

3. ボット対策事業

JPCERT/CC は、総務省・経済産業省連携プロジェクトであるボット対策プロジェクトにボットプログラム解析グループとして参加し、収集されたボット検体の特徴や技術の解析、および駆除ツールの作成を担当しています。さらに、効率的な解析手法の検討や、駆除ツール開発事業者と連携して対策技術の開発なども行っています。

3-1. ボット対策事業の活動実績の公開

ボット対策事業のポータルサイトである「サイバークリーンセンター」では毎月の活動報告として「サイバークリーンセンター活動実績」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。

サイバークリーンセンター
https://www.ccc.go.jp/

2010 年 4 月度 サイバークリーンセンター活動実績
https://www.ccc.go.jp/report/201004/1004monthly.html

4. 国際連携活動関連

4-1. 海外 CSIRT 構築支援および運用支援活動

主に各国の National CSIRT (Computer Security Incident Response Team) に対し、トレーニングやイベントでの講演等を通して CSIRT の構築・運用支援活動を行い、各国のインシデント対応調整能力の向上と、各国との相互信頼と連携の強化を図っています。

4-1-1. アジア太平洋地域における活動

本四半期は、アジア太平洋地域における CSIRT 構築支援および運用支援活動は、平素からの情報連携活動を除き、特にありませんでした。

4-1-2. その他地域における活動

4-1-2-1. Internet Summit of Africa への参加(2010 年 5 月 29 日-6 月 3 日)

アフリカ地域におけるインターネットに関する様々な会合をまとめて開催する Internet Summit of Africa がルワンダのキガリにて開催され、アフリカ地域とアジア地域の IT 分野における連携を促進するフォーラムである AAF (Africa Asia Forum on Network Research & Engineering) が主催した複数のセッションで、JPCERT/CC が講師を務めましました。具体的には、サイバーセキュリティワークショップ（5 月 30 日）において、JPCERT/CC の国内外における活動、APCERT の国際連携活動を紹介し、CERT 指導者トレーニングコース（5 月 31 日）においてインシデントハンドリングの基礎、CSIRT 構築手法、最近の国際サイバーセキュリティ動向、アジア太平洋地域に見られる新たなセキュリティ脅威の展望、などについて講義を行いました。ワークショップおよびトレーニングには、約 30 名の参加者が集い、今後アフリカ各国で CERT 構築を主導する立場として熱心に受講されました。
その他、ルワンダ政府の ICT 政策担当高官と意見交換を行なったり、同時に開催された AfNOG や AfriNI のミーティングに参加したりし、アフリカのインターネットセキュリティ事情に関する情報を収集するとともに、アフリカ各国の政策担当者などと意見交換を行い、今後のアフリカ地域各国 National CSIRT との連携に備えて相互の連絡先や連絡方法を確認しました。

4-2. 国際 CSIRT 間連携

各国との間のインシデント対応に関する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り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。アジア太平洋地域における APCERT (Asia Pacific Computer Emergency Response Team) の枠組みや、国際的な FIRST (Forum of Incident Response and Security Teams) の枠組みに則って活動しています。

4-2-1. アジア太平洋地域における活動

4-2-1-1. APEC TEL 41 への参加および TWNCERT 訪問(2010 年 5 月 6 日-12 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) の第 41 回会議が 5 月に台湾で開催されました。APEC TEL は 3 つの運営グループに分かれて活動しています（1. DSG: ICT Development Steering Group, 2. LSG: Liberalisation Steering Group, 3. SPSG: Security and Prosperity Steering Group）。JPCERT/CC はこのうち、セキュリティ分野を取り扱う SPSG に参加し、日本におけるウェブ改ざんの事例 (JsRedirector) について発表し、APEC 地域の各国の被害状況等について情報を収集しました。また、APEC TEL の General Guest である APCERT は、今年 1 月に実施した APCERT のサイバー演習、およびアジア太平洋地域に見られる新たなセキュ

リティ脅威の展望について講演を行いました。サイバー演習は、国境を越えて広範囲に影響が派生するインシデントに対する迅速な対応技術および意思決定能力の向上と、各地域 CSIRT 間の連携の強化等を目的に毎年実施されており、JPCERT/CC は APCERT 加盟チームとして参加しています。また、新たなセキュリティ脅威の展望に関する講演は、各地域 CSIRT の視点を纏めた内容で、日本では（いわゆる Gumblar ウイルスによる）Web サイト改ざんの被害が多く見られる状況等を報告し、講演内容に反映されました。このような講演を通して、APCERT としての活動や視点をワーキンググループに還元しています。
また、台湾の窓口 CSIRT である TWNCERT を訪問し、インシデント動向やボットネット対策における連携について意見交換を行いました。

4-2-2. その他の地域における活動

4-2-2-1. 「情報セキュリティインシデントマネジメント」の国際標準化活動への参加(2010 年 4 月 19 日-23 日)

ISO/IEC JTC 1/SC27 WG4 において検討されている、情報セキュリティインシデントマネジメントのためのガイドラインである ISO/IEC 27035 “Information Security Incident Management” の標準化について、4 月にマレーシアにて開催された SC27 の国際会議において、第 3 次委員会草案 (3rd Committee Draft) に対する各国からのコメントの取扱いが審議されました。
このガイドラインは、今回の会議を経て、最終委員会草案 (Final Committee Draft) に進むことに決定しました。次回の会議（10 月ドイツにて開催予定）に向けて、このガイドラインが我が国のインシデントマネジメントの運用や既存の CSIRT 間の実務に整合するものとなるよう務めていく予定です。

4-2-2-2. 22nd Annual FIRST Conference Miami への参加(2010 年 6 月 13 日-18 日)

FIRST (Forum of Incident Response and Security Teams) の第 22 回年次会合が 6 月 13 日から 18 日まで米国のフロリダ州マイアミで開催されました。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 “Past the Faded Perimeter - Threat & 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、アジア太平洋地域や欧州の個別の National CSIRT や今回の会合からはじめて参加した National CSIRT などとの意見交換や、アジア太平洋地域から参加している複数の CSIRT 組織が集う意見交換会の開催など、国際間の CSIRT 連携をさらに強化させるための様々な活動を行いました。

また、脆弱性への対応に関するセッションも多く、国内から参加しているベンダーCSIRT や、脆

弱性対応を行っている海外 CSIRT、今後脆弱性対応を行っていきたいと考えている National CSIRT との意見交換なども実施し、脆弱性対応の観点からも情報収集、関係構築に努めました。

JPCERT/CC は、このような会合を通じて、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努めています。第 22 回 FIRST 年次会合年次会合についての詳細は、以下の URL をご参照ください。

22nd Annual FIRST Conference Miami
http://conference.first.org

また、本四半期は、KDDI-SOC（日本）および KF/ISAC（韓国）の FIRST 加盟に際して、それぞれサイバーディフェンス研究所の CSIRT である CDI-CIRT および韓国の National CSIRT である KrCERT/CC と共にスポンサー（FIRST の規約に従い加盟手続を支援するチーム）を務めました。両組織は 5 月 26 日に正式に FIRST 加盟に至り、日本からの FIRST 加盟チームは、17 チームとなりました。

4-2-2-3. National CSIRT Meeting への参加(2010 年 6 月 19 日-20 日)

第 22 回 FIRST 年次会合後に、引き続き米国のマイアミにて、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、アジア太平洋地域の途上国における CSIRT 構築支援活動の経験から見えた課題について発表し、好評を得ました。

National CSIRT Meeting についての詳細は、以下の URL をご参照ください。

Collaboration Meeting for CSIRTs with National Responsibility
http://www.cert.org/csirts/national/conference.html

4-3. APCERT 事務局運営

JPCERT/CC は、アジア太平洋地域の CSIRT のコミュニティである、APCERT の事務局を担当しています。APCERT についての詳細は、次の URL をご参照ください。

APCERT
https://www.jpcert.or.jp/english/apcert/

4-4. FIRST Steering Committee への参画

FIRST Steering Committee のメンバとして、JPCERT/CC の職員が FIRST の組織運営に関与しています。

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

5. 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の事務局運営を行っています。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。

5-1. フィッシング対策協議会の活動実績の公開

フィッシング対策協議会の Web ページでは、毎月の活動報告として「フィッシング報告状況」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
http://www.antiphishing.jp
フィッシング対策協議会 2010 年 4 月 フィッシング報告状況
http://www.antiphishing.jp/information/information1067.html
フィッシング対策協議会 2010 年 5 月 フィッシング報告状況
http://www.antiphishing.jp/information/information1077.html
フィッシング対策協議会 2010 年 6 月 フィッシング報告状況
http://www.antiphishing.jp/information/information1085.html

5-2. 情報収集と動向分析の強化

フィッシング対策協議会 Web ページや会員向け ML では、本四半期において、フィッシングに関するニュースや緊急情報を 16 件公開しました。また、フィッシングの動向や新対策技術に関して有識者にインタビューを行い、フィッシング対策協議会の Web ページに 2 件掲載したほか、会員向けに、勉強会の開催、フィッシングに関するトピックの提供などを実施しました。先進的な対

策技術の開発の観点からは、電気通信大学吉浦研究室が行っている「コンテンツベースのフィッシング検知技術」の共同研究に参画したほか、フィッシング対策ツールの検知効率調査を実施しました。これらの調査研究の成果は、フィッシング対策協議会の Web ページにて順次公開を予定しています。

5-3. 一般ユーザからの問合せ業務改善

フィッシング対策協議会に寄せられるフィッシング事例報告や各種の相談に対して、翌営業日までに対応を行うように業務の改善を行いました。また問合せに対する回答の電子メールに S/MIME を利用して署名を行うようにしました。メールのなりすましなどを防ぐ効果が期待できます。

5-4. フィッシングサイトの URL を会員（対策サービス事業者）へ情報提供開始

よりプロアクティブなユーザ保護の取り組みとして、フィッシング対策協議会に寄せられるフィッシングサイトの URL リストを、フィッシング対策ツールバーを提供している事業者やウイルス対策ソフトベンダである協議会会員に提供し、ブラックリストに追加する等の活用を図っていただくことになりました。提供先は、これまでは Yahoo! Japan(2010 年 2 月)、Kaspersky Labs Japan(2010 年 4 月)、ネットスター(2010 年 6 月)の 3 社ですが、現在も複数の事業者との間で情報提供に関する協議を行っており、順次拡大していく予定です。

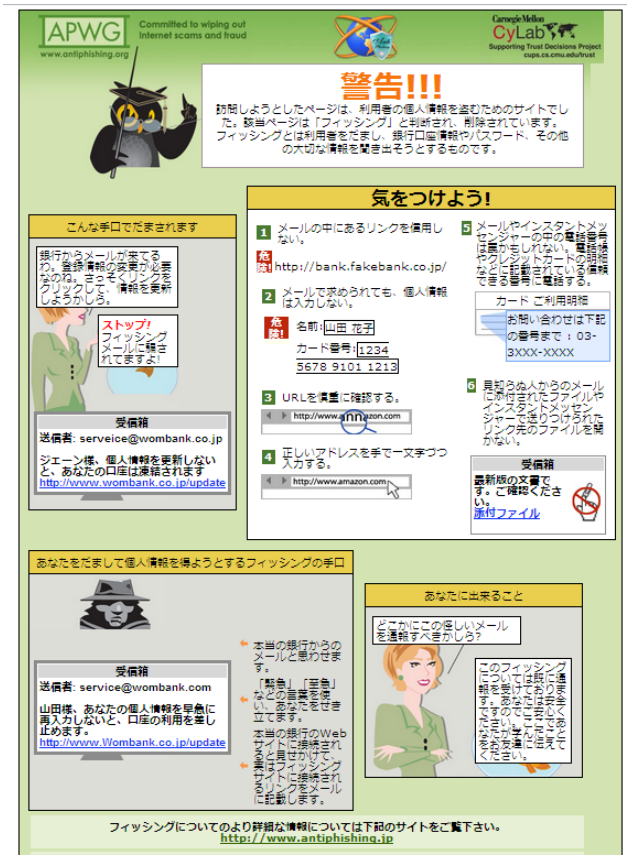
5-5. 海外機関との連携強化

海外でのフィッシングに関する脅威の状況を把握し、国内での今後の変化を予測するために、国際的にフィッシング対策に関する活動を推進している APWG(Anti-Phishing Working Group)との連携を強化しました。

2010 年 5 月に行われた APWG Counter-eCrime Operations Summit に参加し、セッションを聴講し、情報収集をおこないました。

また、昨期に引き続き APWG の教育プログラム（「フクロウ先生のフィッシング警告ページ」）に参加し、フィッシングサイトであったページに日本語の警告が表示されるように、ISP やホスティング事業者などに対する働きかけをおこなっています[図 5-1]。フィッシングサイトが公開されていたページにフィッシングに関する警告を表示させることで、利用者に、訪れたサイトがフィッシングサイトであったことや、フィッシングメールに誘導されてしまったことを認識しても

らい、フィッシングの手口紹介やフィッシングサイトに関する注意事項などの対応を学んでもらうことができます。



[図 5-1:
フクロウ先生のフィッシング教育 Web ページ:http://education.apwg.org/r/?forcelang=jp]

5-6. 普及啓発コンテンツの充実

今期は 2009 年度の協議会のワーキンググループ活動などで作成した 3 つの資料を公開いたしました。それぞれの資料の概要は以下のとおりです。

1) フィッシング対策ガイドライン(2010 年度版)

概要: 2008 年に公表したフィッシング対策ガイドラインについて、脅威の現状や新しい対策技術を反映した改版を行いました。

http://www.antiphishing.jp/antiphishing_guide.pdf

2) ブラウザ搭載フィッシング検出機能の検出精度に関する調査

概要: 現在、主要な Web ブラウザにはフィッシング検出機能が備わっており、ユーザ保護に役立っていると考えられていますが、これまで検出精度を調査したデータはありませんでした。当協議会で実施した事前調査において、海外のフィッシング URL 共有サイトから取 得したフィッシ

ングサイトのデータを主要 4 ブラウザ（InternetExplorer7,InternetExplorer8,Firefox,Safari）で判定したところ、約 9 割以上を検出することを確認しましたが、JPCERT/CC に報告されるフィッシングサイトの URL を判定させると、約 1 割程度しか検出しないことがわかりました。この結果から、「日本のブランドを狙ったフィッシングサイトは海外のブランドを狙ったフィッシングサイトと比較してブラウザやツールバーでの検知率が低い」という仮説をたて、現在のブラウザ搭載フィッシング検出機能の性能を正しく理解することを目的とした調査を実施し、その調査結果をまとめました。

http://www.antiphishing.jp/Evaluate_Browser_Phishing_Protection_Effectiveness.pdf

3) コンテンツベースフィッシング検知手法の大規模実例評価と改良

概要: 現在、フィッシング詐欺への対策方法として、ブラックリスト方式、ホワイトリスト方式など様々なフィッシング検知方式が提案されています。その中でもコンテンツベース（以下「CB」といいます。）方式は、データベースのメンテナンスが不要であることから、 即時性の高いフィッシング検知方式であるといえます。

当協議会では、CB 方式に注目し、研究を行っている電気通信大学との間で CB 方式の有効性等に関する共同研究を行いました。CB 方式については、小規模な評価しか行われておらず、また、日本語のフィッシングサイトに対応する実装実験も行われていないなど、充分な評価が行われていないことから、今回、大量のフィッシング実例データを用いた CB 方式の評価ならびに日本語のフィッシングサイトに対応したシステムの実装実験を行い、その実験結果をまとめました。

http://www.antiphishing.jp/Content-based%20phishing%20detection%20methods.pdf

6. 公開資料

JPCERT/CC の各業務において実施した情報セキュリティに関する調査・研究の報告書や論文、セミナー資料を公開しました。

6-1. OWASP「ソフトウエアセキュリティ保証成熟度モデル」

本資料についての詳細は、「2-4-2.」をご参照ください。

OWASP「ソフトウエアセキュリティ保証成熟度モデル」
https://www.jpcert.or.jp/research/2010/SAMM_20100407.pdf

6-2. 新入社員等研修向け情報セキュリティマニュアル Rev2、新入社員等研修向け情報セキュリティクイズ

企業や組織の教育担当者や情報セキュリティ担当者に向けて、新入社員等に情報セキュリティに関する知識を教える際のガイドライン、セキュリティ対策やインシデント対応に関する社内ルールの教育、研修資料のベース となるような情報やトピックをまとめました。
また、本編の補助教材として、初心者にセキュリティ意識を高めてもらうために、簡単なセキュリティクイズも合わせて公開しました。

新入社員等研 修向け情報セキュリティマニュアル Rev2
https://www.jpcert.or.jp/magazine/security/newcomer-rev2_20100415.pdf

新入社員等研修向け情報セキュリティクイズ
https://www.jpcert.or.jp/magazine/security/newcomer_Quiz20100415.pdf

6-3. 「CERT C Secure Coding Standards 日本語版」を拡充

本資料についての詳細は、「2-4-4.」をご参照ください。

CERT C Secure Coding Standards 日本語版
https://www.jpcert.or.jp/sc-rules/index.html

6-4. グッド・プラクティス・ガイド パッチ管理

本資料についての詳細は、「2-5-1.」をご参照ください。

グッド・プラクティス・ガイド パッチ管理
https://www.jpcert.or.jp/research/2010/GPG_Patch_Management_20100531.pdf

6-5. 制御システム環境におけるサイバーセキュリティ文化の支援を目的とした運用セキュリティ（OPSEC）の使用

本資料についての詳細は、「2-5-1.」をご参照ください。

制御システム環境におけるサイバーセキュリティ文化の支援を目的とした運用セキュリティ（OPSEC）の使用
https://www.jpcert.or.jp/research/2010/UsingOPSEC_20100531.pdf

7. 講演活動一覧

(1) Jack YS LIN(早期警戒グループ 情報セキュリティアナリト) :
「諸外国のサイバーセキュリティ事情」(「サイバー攻撃の脅威とその対策の動向」
マルチメディア推進フォーラム-PART501,2010 年 4 月 22 日

(2) 鎌田 敬介(国際部部長代理) :
「Web Defacement Cases in Japan - JsRedirector」
APEC TEL 41―台湾 ,2010 年 5 月 11 日

(3) 久保 正樹(情報流通対策グループ 脆弱性アナリスト) :
「ソフトウエアセキュリティ保証成熟度モデル「SAMM」について」
Fortify ソフトウエアセキュリティ・アシュアランスセミナー ,2010 年 5 月 19 日

(4) 宮地 利雄(理事) :
「制御システムとそのサイバー・セキュリティ課題」
第 15 回 ISS スクエア水平ワークショップ,2010 年 5 月 21 日

(5) 山口 英（理事)、鎌田 敬介(国際部部長代理) :
「JPCERT/CC Activities - International and Domestic Cooperation」
「APCERT Activities & Challenges」
「Fundamentals of Computer Incident Handling」
「Creating a CSIRT」
「Introduction to International Cyber Security Situation」
「Emerging Security Threat Landscape - Perspectives of Asia Pacific Region」
Internet Summit of Africa/ Cyber Security Workshop, CERT Instructor Training Course
―ルワンダ ,2010 年 5 月 30～31 日

(6) 久保 正樹(情報流通対策グループ 脆弱性アナリスト) :
「セキュリティシステム概論」
東京工科大学大学院講義「セキュリティシステム特論」,2010 年 6 月 11 日

(7) 小宮山 功一朗(早期警戒グループ リーダ 情報セキュリティアナリスト) :
「WEB サイトなりすまし問題と対策」
ネットメディアの信頼性向上対策ワークショップ ,2010 年 6 月 16 日

(8) 鎌田 敬介(国際部部長代理) :
「Technical Challenges to Developing Country National CSIRTs」
National CSIRT Meeting―マイアミ ,2010 年 6 月 19 日

(9) 戸田 洋三(情報流通対策グループ リードアナリスト) :
「あなたのコードにセキュアコーディングスタンダード」
OSC2010Hokkaido ,2010 年 6 月 26 日

8. 執筆・取材記事一覧

(1) 小宮山　功一朗(フィッシング対策協議会) :
「フィッシング詐欺に新対策」
NHK ニュース,2010 年 4 月 11 日

(2) 戸田 洋三(情報流通対策グループ リードアナリスト) :
「glib ライブラリに潜む脆弱性をつぶすパッチ」
実例で学ぶ脆弱性対策コーディング 第 1 回
翔泳社 CodeZine,2010 年 5 月 20 日

(3) 久保 正樹(情報流通対策グループ 脆弱性アナリスト) :
「TIFF ライブラリに潜む脆弱性をつぶすパッチ」
実例で学ぶ脆弱性対策コーディング 第 2 回
翔泳社 CodeZine,2010 年 5 月 27 日

(4) 宮地 利雄(理事) :
「制御システムセキュリティー最新動向と課題」
工業技術社 月刊計装 6 月号,2010 年 6 月 1 日

(5) 早貸 淳子(常務理事) :
「セキュリティリスクはゼロにできない を前提に、被害を最小化する社内体制構築を」
セキュリティ新時代
株式会社ダイヤモンド社 週刊ダイヤモンド, 2010 年 6 月 7 日

(6) 久保 正樹(情報流通対策グループ 脆弱性アナリスト) :
「画像処理ソフトウエア「ImageMagick」の脆弱性」
実例で学ぶ脆弱性対策コーディング 第 3 回
翔泳社 CodeZine,2010 年 6 月 15 日

(7) 戸田 洋三(情報流通対策グループ リードアナリスト) :
「Samba smbclient―書式指定文字列に潜む脆弱性」
実例で学ぶ脆弱性対策コーディング 第 4 回
翔泳社 CodeZine,2010 年 6 月 22 日

9. 開催セミナー一覧

(1) C/C++ セキュアコーディングセミナー2010@福岡
本カンファレンスについての詳細は、「2-4-1.」を**ご参照ください。**

10. 後援・協力一覧

(1) 第８回迷惑メール対策カンファレンス
2010 年 5 月 31 日

(2) ネットメディアの信頼性向上対策ワークショップ
2010 年 6 月 16 日

11. その他

JPCERT/CC からの情報をより多くの方々にタイムリーにご活用いただけるよう、今期より、本格的に Twitter による配信を開始いたしました。

http://twitter.com/jpcert

■ インシデントの対応依頼、情報のご提供は ■

☐ Email：info@jpcert.or.jp
PGP Fingerprint ：
FC89 53BB DC65 BD97 4BDA D1BD 317D 97A4 69EC E048

☐ インシデント報告フォーム
https://www.jpcert.or.jp/form/