JPCERT CC®

JPCERT-PR-2010-0001

JPCERT/CC 活動概要［2009 年 10 月 1 日 ～ 2009 年 12 月 31 日 ］

2010-1-12 発行

【活動概要トピックス】

—トピック 1— 急増した Web ページ改ざん届出への対応—いわゆる Gumblar をはじめとする FTP アカウント盗用攻撃によるインシデントへの対応
—トピック 2— 中国インターネットセキュリティ事情等の海外動向を IW2009 で発表
—コンテンツフィルタリング、大規模なネットワーク障害など
—トピック 3— セキュアコーディング技術の普及活動の拡大—海外を含む東京以外の地域や出版メディアへの展開
—トピック 4— 「Security Day 2009」を共催
—セキュリティ実務家が最近の動向を知るためのイベントとして定着
—トピック 5— FIRST TC やマルウエア対策研究人材育成プログラムへの技術的貢献
—トピック技術やマルウエアの解析技術など

—トピック 1 —

急増した Web ページの改ざんの届出への対応——いわゆる Gumblar をはじめとする FTP アカウント盗用攻撃によるインシデントへの対応

2009 年 12 月には、著名な大企業の Web サイトの改ざんに関する報道が相次ぎ、JPCERT/CC にも類似の届出が多数寄せられました。この大半は、前々四半期(2009 年 4 月 1 日から 2009 年 6 月 30 日)に多数発生した JSRedir-R/Gumblar と呼ばれるウイルスによる攻撃が高度化・複雑化した事例(以下「本四半期の FTP アカウント盗用攻撃」といいます。)ですが、本四半期の FTP アカウント盗用攻撃では、改ざん件数の増加もさることながら、改ざんされたサイトを閲覧した利用者が誘導されるマルウエア配布サイトが大幅に増加し、また、その構成が複雑化しました。

JPCERT/CC では、本四半期の FTP アカウント盗用攻撃が活発化した 10 月から、数回の注意喚起等を公表し、システム管理者やユーザに注意を呼びかけました。これらの注意喚起等については、複数のニュースメディアに取り上げていただきました。

また、本四半期の FTP アカウント盗用攻撃の特徴を踏まえて、マルウエアに感染した PC からアカウント情報を集める情報収集サーバの特定とその停止のための調整に力を入れました。前々四半期の事例では、改ざんサイトから誘導されるマルウエア配布サイトの数が比較的限定されていたため、主に、そのマルウエア配布サイトを停止させる調整を行いましたが、本四半期の攻撃では、誘導先のマルウエア配布サイトの数が格段に増えたため、少数にとどまっていると考えられ

るアカウント情報収集サーバの停止に向けた調整を優先して行うことで、より効率的にアカウント窃取等の被害の拡大防止を図ろうとしたものです。

注意喚起 － Web サイト経由でのマルウエア感染拡大に関する注意喚起
http://www.jpcert.or.jp/at/2009/at090023.txt

技術メモ － 安全な Web ブラウザの使い方
https://www.jpcert.or.jp/ed/2008/ed080002_1104.pdf

JPCERT/CC からのお知らせ － 冬期の長期休暇を控えて Vol.2
http://www.jpcert.or.jp/pr/2009/pr090008.txt

―トピック 2 ―

中国インターネットセキュリティ事情等の海外動向を IW2009 で発表――コンテンツフィルタリング、大規模ネットワーク障害など

11 月 24 日から 27 日かけて都内で開催された「InternetWeek 2009」(主催：社団法人日本ネットワークインフォメーションセンター (JPNIC))において、JPCERT/CC の鎌田敬介および Jack YS LIN が、海外でのセキュリティインシデント動向に関する講演を行いました。

中国に関しては、2009 年 5 月に発生した大規模なネットワーク障害の問題や政府によるフィルタリング導入等の政策の実施状況、同国内のコンピュータセキュリティインシデントの動向などが、韓国に関しては 7 月の DDoS 攻撃後の関係機関の取り組みなどが、それぞれ報告され、参加者の関心を集めました。急成長する中国のインターネット事情に関する情報は社会的関心も高く、また、米韓における DDoS 被害に関する報道の記憶も未だ新しかったことから、講演内容が IT 系ニュースメディアで取り上げられました。

海外のインターネット事情に関する情報は、国境を越えて発生するインシデントへの対応を円滑に進めるために、各国 CSIRT との日頃の連携活動を通じて収集しているものですが、国内の利用者にとって意義のある情報については、各種セミナー等の機会を利用して提供を図っていきたいと考えています。

InternetWeek 2009
https://internetweek.jp/

海外におけるインターネットセキュリティインシデント概観
「～2009 年 7 月の韓国大規模 DDoS インシデントのその後」

http://www.jpcert.or.jp/present/2009/IW2009091124_DDoS.pdf

―トピック 3 ―

セキュアコーディング技術の普及活動の拡大――海外を含む東京以外の地域や出版メディアへの展開

JPCERT/CC では、ソフトウエア等の脆弱性関連情報の公開に向けた調整だけでなく、セキュリティ上の脆弱性を作り込まないソフトウエアの開発に有効な手法の分析、及び普及活動にも力を入れています。

その活動のひとつとして「C/C++言語によるセキュアコーディングセミナー」を国内外で開催しています。2009 年 10 月からは、大阪、九州など東京以外の地域におけるセミナーの展開に力を入れました。自動車産業や家電メーカーを多く抱える愛知県、大阪府、広島県、福岡県など含む西日本地域は、とくに組込みソフトウエア開発企業の集積度が高く、コンシューマ製品などの組込みソフトウエアを C や C++言語を用いて開発しているエンジニアも多いことから、組込みソフトウエアのセキュア化への効果が期待できるからです。

JPCERT/CC イベント情報
http://www.jpcert.or.jp/event/

海外については、前四半期のタイに続き、インドネシアにおいて、ID-SIRTII(Indonesia Security Incident Response Team on Internet Infrastructure)の協力を得て「C/C++ セキュアコーディングセミナー」を実施しました。JPCERT/CC では、日本企業のソフトウエア開発の委託が拡大している東南アジア各国にセキュアコーディングの考え方を普及させることの重要性を認識し、その実現に向けて指導的な役割を担うとともに周辺各国とのネットワークを強化しています。

また、より多くの方々にセキュアコーディングを理解していただくため、セミナーだけでなく、文書などの形での体系化、整理・保存にも努めています。2009 年 10 月には、米国 CERT/CC との共同研究の成果である「The CERT C Secure Coding Standard」の翻訳書(「CERT C セキュアコーディングスタンダード」アスキー・メディアワークス刊)の発行、ソフトウエアエンジニア向け雑誌(「組込みプレス Vol.17」技術評論社刊)への特集記事寄稿などを行い、プログラマ向けウェブメディア(「CodeZine」翔泳社)での記事連載も開始しました。

JPCERT/CC 出版・執筆活動一覧
http://www.jpcert.or.jp/kouen/

―トピック 4 ―

「Security Day 2009」を共催――セキュリティ実務家が最近の動向を知るためのイベントとして定着

2009 年 12 月 16 日に都内で開催された「Security Day　2009」は、社団法人日本インターネットプロバイダ協会(JAIPA)、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)、財団法人日本データ通信協会(Telecom-ISAC-Japan)、一般社団法人日本電子認証協議会および JPCERT/CC の 5 団体共催によるセミナーです。プロフェッショナル同士が情報セキュリティに関する議論及び発表を行う場として企画されました。

今回が 6 回目の開催となる本セミナーは、約 100 名の参加者を得、 昨今の電子政府に対する議論の高まりから、電子認証のあり方に関するセッションにはテレビ放送局の取材が入るなど、IT 業界以外からの注目も高いものとなりました。

Security Day 2009
http://securityday.jp/

―トピック 5 ―

FIRST TC やマルウエア対策研究人材育成プログラムへの技術的貢献――トラフィックモニタリング技術やマルウエアの解析技術など

2009 年 12 月 1 日、2 日にマレーシアで開催された「FIRST Technical Colloquium」において、JPCERT/CC の鎌田敬介及び佐藤しおりの 2 名が、セッション講師を務めました。

このセッションは、トラフィックモニタリングとウェブアプリケーションのセキュリティに関するもので、ハンズオン(実習)形式で行いました。

December 2009 FIRST Technical Colloquium のプログラム
http://www.first.org/events/colloquia/dec2009/program/#d20091202

また、2009 年 10 月 26 日から 28 日にかけて開催された「マルウエア対策研究人材育成ワークショップ 2009(MWS2009)」(ボット対策プロジェクト運営委員会及び情報処理学会が共催)では、JPCERT/CC が、ボット対策プロジェクト/ボットプログラム解析グループとして、マルウエア分析の研究用データセットを構成するための検体の選定及び提供を行いました。

この取り組みは、ボットやマルウエアに関する専門的な知識を持つ研究者/実務者の育成や、対策技術の高度化につながるものであることから、来年度以降の継続開催に期待が寄せられています。

JPCERT/CC は、活動を通じて培ったマルウエア解析技術や解析技術の効率化に関する調査研究の成果を生かしつつ、引き続きこの取り組みを支援していきたいと考えています。

MWS 2009 のプログラム
http://www.iwsec.org/mws/2009/

JPCERT CC®

—活動概要—

目次

1. 早期警戒

1-1. インシデントハンドリング

JPCERT/CC が本四半期に受け付けた届出のうち、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。)に関する届出は 2,048 件(届出を受けたメール、FAX の延べ数は 2,414 通 *1)、IP アドレス別の集計では 2,229 アドレスでした。

*1:同一サイトに関するインシデント情報が、異なる届出者から届けられることがあるため、届出件数とメール及び FAX の延数に差異が発生しています。

前四半期と比較するとインシデントに関する届出数と IP アドレス数が、ともに約 3 割減少しています。これは 5 月以降定常的に寄せられていたマレーシアのセキュリティ機関からのマルウエア設置サイトに関する届出が減少したためです。

JPCERT/CC が国内外の関連するサイトに調査対応依頼を行う等の調整(コーディネーション)活動を行った件数は 576 件でした。前四半期と比較して約 3 割減少しています。JPCERT/CC が行う「調整」とは、インシデントの発生元に対する連絡調整等の依頼を含む届出に基づいて、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及び海外 CSIRT 等の関係協力組織に対し、現状の調査と善処の依頼の連絡を行うものです。

JPCERT/CC は、このような調整(コーディネーション)活動により、インシデントの認知と解決、インシデントによる被害拡大の抑止に貢献しています。

インシデントハンドリング業務の詳細については、別紙「JPCERT/CC インシデントハンドリング業務報告」をご参照ください。

JPCERT/CC インシデントハンドリング業務報告の詳細
https://www.jpcert.or.jp/pr/2010/IR_Report0100112.pdf

1-1-1. インシデントの傾向と分析

1-1-1-1. Web ページの改ざんの届出件数増加

本四半期は Intrusion の報告が前四半期の 28 件から 372 件に大幅に増加しました。この大半は、前々四半期(2009 年 4 月 1 日から 2009 年 6 月 30 日)にも多数発生した JSRedir-R/Gumblar(以下「Gumblar」といいます。)による攻撃がさらに高度化・複雑化した事例です。この攻撃による事

例では、不正なスクリプトを埋め込まれた Web ページ(以下「改ざんサイト」といいます。)をユーザが閲覧し、マルウエアを配布するサイトに誘導された場合、ユーザの PC 等がマルウエアに感染する可能性があります。

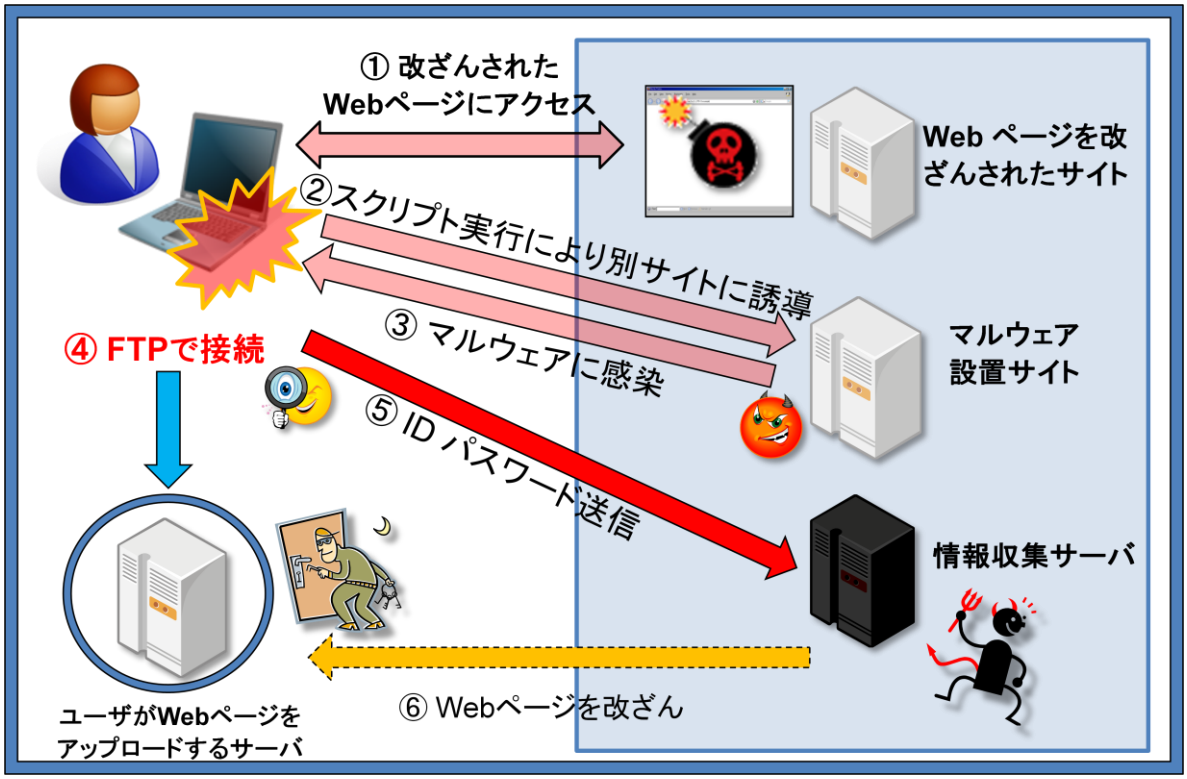

図 1-1: Gumblar によるインシデント

本四半期に多く報告された攻撃は、一見、前々四半期の Gumblar による攻撃に類似しているようにみえるものの、攻撃メカニズムが大きく変化しています。

表 1 -1　FTP アカウント盗用攻撃の比較

	2009 年 9 月以前	2009 年 10 月以降
Web ページを改ざんされたサイト	数百サイト	数百サイト
マルウエア配布サイト	数サイト	数百サイト
情報収集サイト	不明	数サイト

Gumblar をはじめとする FTP アカウント盗用攻撃によるインシデントでは、攻撃者は、まず、マルウエアに感染した PC から FTP のアカウント(ユーザ ID、パスワード)情報を窃取します。次に、窃取したアカウント情報を使って、Web サイトで公開されているページを改ざんすることで、その Web サイトを新たな攻撃用のサイトとして使用します。攻撃者は、このように攻撃用の改ざ

んサイトの数を徐々に増やして、被害を拡大させるという手法を取りました。前々四半期の事例では、改ざんサイトから誘導されるマルウエア配布サイトの数が比較的限定されていたため、JPCERT/CC では、その誘導先のマルウエア配布サイトを停止させる調整を行いました。

一方、本四半期の攻撃では、改ざんサイトから誘導されるマルウエア配布サイトの数が大幅に増加し、また、その構成が複雑化したため、攻撃の実態把握及びマルウエア配布サイトの停止等の調整が困難になりました。

そのため、本四半期は、外部組織からの届出情報や独自に調査した結果に基づき、マルウエアに感染した PC からアカウント情報が送信される先のサーバ(図 1 でいう情報収集サーバ)が比較的少数にとどまっていると考えられることに着目し、これらの情報収集サーバの特定のための調査および停止に向けた調整を優先して行いました。被害の拡大を抑止するためには、このように、攻撃手法の変化に応じた、より効率的な調整活動を行うことが重要であり、適切な調整先の発見のためには、関連する情報をインシデント報告等によりご提供いただくことが必要です。今後とも、インシデント報告へのご協力をお願いします。

現在、JPCERT/CC で確認した情報収集サーバは、大半が機能しなくなっていますが、今後、さらに攻撃のメカニズムが変化することが予測されます。また、12 月には、大手企業の Web サイトが改ざんされる事例がたて続けに発生しました。Web ページのアップロードに FTP を使用している場合はもちろん、それ以外の場合においても、今一度、管理している Web ページが改ざん(閲覧者をマルウエア配布サイトに誘導する不審なスクリプトの挿入等)されていないか確認してください。また、Web ページのアップロードに使用するコンピュータについては、OS を含むすべてのソフトウエアを最新の状態に保つとともに、ウイルス対策ソフトを導入し、ウイルス定義ファイルを常に最新の状態に保つなどの対策を行うことをお勧めします。

仮に、管理する Web ページの改ざんを発見した場合やウイルス対策ソフトにより Gumblar その他の類似のマルウエアを検知した場合は、すでに FTP のアカウント情報が盗まれている可能性がありますので、ウイルス対策ソフト等でマルウエアの駆除を行うとともに、FTP のパスワードを変更してください。なお、Gumblar 等のマルウエアを駆除していない状態でパスワードを変更しても、再度パスワードが盗まれてしまう可能性がありますので、ご注意ください。

また、攻撃方法の変化等により脅威の内容や有効な対策に変化が生じた場合には、随時、注意喚起等の情報発信を行いますので、JPCERT/CC からの発信情報も継続的にご確認ください。

注意喚起 － Web サイト経由でのマルウエア感染拡大に関する注意喚起
http://www.jpcert.or.jp/at/2009/at090023.txt

注意喚起 － Adobe Reader 及び Acrobat の未修正の脆弱性に関する注意喚起
https://www.jpcert.or.jp/at/2009/at090027.txt

技術メモ － 安全な Web ブラウザの使い方
https://www.jpcert.or.jp/ed/2008/ed080002_1104.pdf

JPCERT/CC からのお知らせ － 冬期の長期休暇を控えて Vol.2
http://www.jpcert.or.jp/pr/2009/pr090008.txt

1-1-1-2. 国内のサイトを装ったフィッシングサイトに関する届出件数の増加

本四半期は、国内のサイトを装ったフィッシングサイトに関する届出件数が前四半期の 104 件から 141 件に増加しています。これは国内の有名ポータルサイトを装うフィッシングサイトの届出が依然として寄せられているためです。Web サイトで ID、パスワード等の重要な情報を入力する際には、情報を入力しようとしているサイトが、正規のサイトであることを慎重に確認してください。

JPCERT/CC では、フィッシングサイトが設置されている国内外のサイトの管理者に対して調整を行い、フィッシングサイトの停止を図っています。

不審なサイトを発見した場合は、JPCERT/CC にご報告ください。また、仮に、フィッシングサイトに ID、パスワード等の重要な情報を入力してしまったことに気づいた場合は、速やかに正規のサービス事業者にご相談いただき、ID、パスワード等の変更手続きを行ってください。

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。

インシデントの届出方法の詳細
https://www.jpcert.or.jp/form/

インシデントの届出（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：11 件　https://www.jpcert.or.jp/at/

2009-10-14　2009 年 10 月 Microsoft セキュリティ情報（緊急 8 件）に関する注意喚起（公開）
2009-10-14　Adobe Reader 及び Acrobat の脆弱性に関する注意喚起（公開）
2009-10-20　マイクロソフト社を騙るマルウエア添付メールに関する注意喚起（公開）
2009-10-23　マイクロソフト社を騙るマルウエア添付メールに関する注意喚起（更新）
2009-10-27　Web サイト経由でのマルウエア感染拡大に関する注意喚起（公開）
2009-10-28　Web サイト経由でのマルウエア感染拡大に関する注意喚起（更新）
2009-11-11　2009 年 11 月 Microsoft セキュリティ情報（緊急 3 件）に関する注意喚起（公開）
2009-12-09　2009 年 12 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）
2009-12-09　Adobe Flash Player の脆弱性に関する注意喚起（公開）
2009-12-24　Web サイト経由でのマルウエア感染拡大に関する注意喚起（更新）
2009-12-24　Adobe Reader 及び Acrobat の未修正の脆弱性に関する注意喚起（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　http://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 51 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

脅威の動向として特筆すべき点としては、Gumblar などと呼ばれるマルウエアが静かにその感染範囲を拡大したことがあげられます。詳細については、1-1-1-1.をご参照ください。

また、昨今、ウイルス対策ソフトなどに見せかけてユーザにインストールを求める偽セキュリティ対策ソフトの被害が多数確認されています。偽セキュリティソフトウエアを配布している Web ページは、ユーザに対して「あなたのコンピュータがマルウエアに感染しています。」などという警告メッセージを出して、偽セキュリティソフトウエアのインストールを求めます。現在、国内外の複数のセキュリティ組織が偽セキュリティソフトへの注意を呼び掛けています。

セキュリティソフトが真正か偽かについては専門家でも判断が難しいため、真正な製品であることが確実に判断できない場合には、量販店などでも販売されている製品を選ぶ等慎重を期してください。
また下記の文書中に偽セキュリティソフトの一覧が含まれていますので参考にしてください。

Microsoft 日本のセキュリティチーム　偽セキュリティソフトを振り返る
http://blogs.technet.com/jpsecurity/archive/2009/12/16/3300629.aspx

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について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
http://www.jpcert.or.jp/isdas/readme.html

本四半期に ISDAS で観測されたアクセス先ポートに関する平均値の上位 1 位～5 位、6 位～10 位までの推移を図 1-2、1-3 に示します。

- アクセス先ポート別グラフ top1-5 (2009 年 10 月 1 日-12 月 31 日)

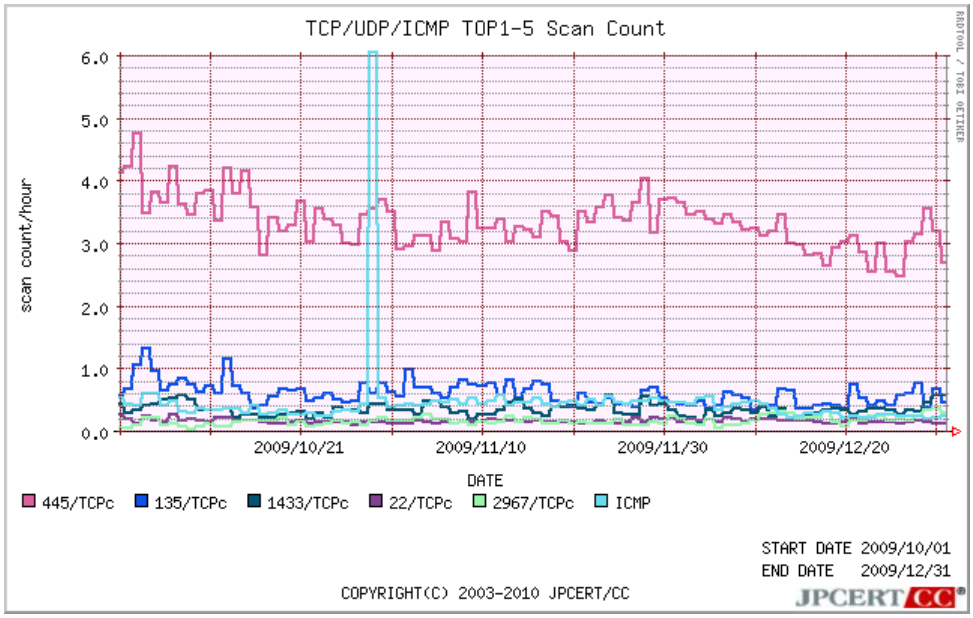

図 1-2：アクセス先ポート別グラフ top1-5

- アクセス先ポート別グラフ top6-10 (2009 年 10 月 1 日-12 月 31 日)

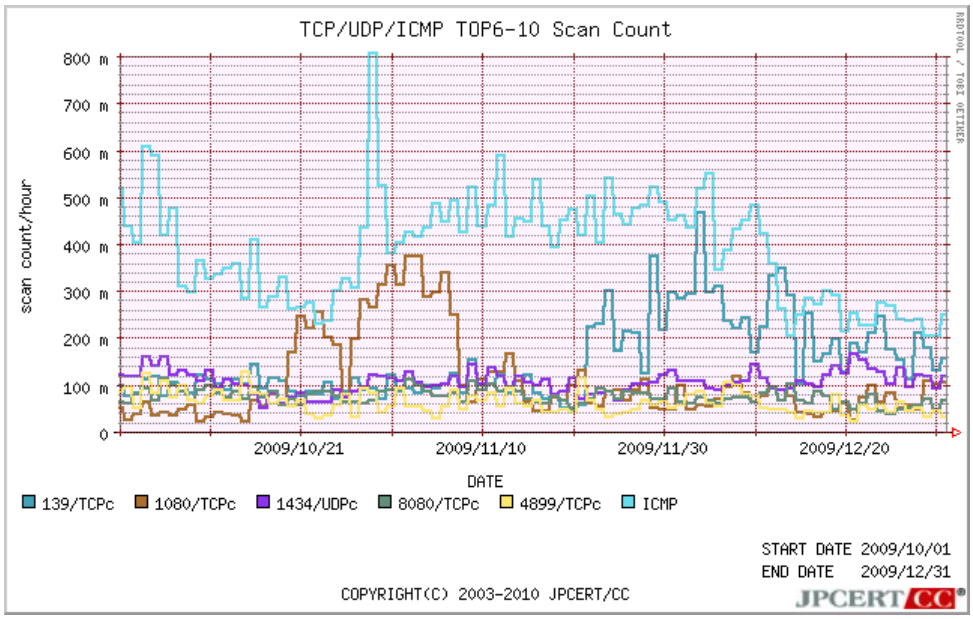

図 1-3: アクセス先ポート別グラフ top6-10

また、より長期間のスキャン推移を表すグラフとして、2009 年 1 月 1 日から 2009 年 12 月 31 日までの期間における、アクセス先ポートに関する平均値の上位 1 位～5 位、6 位～10 位までの推移を図 1-4、図 1-5 に示します。

- アクセス先ポート別グラフ top1-5 (2009 年 1 月 1 日-2009 年 12 月 31 日)

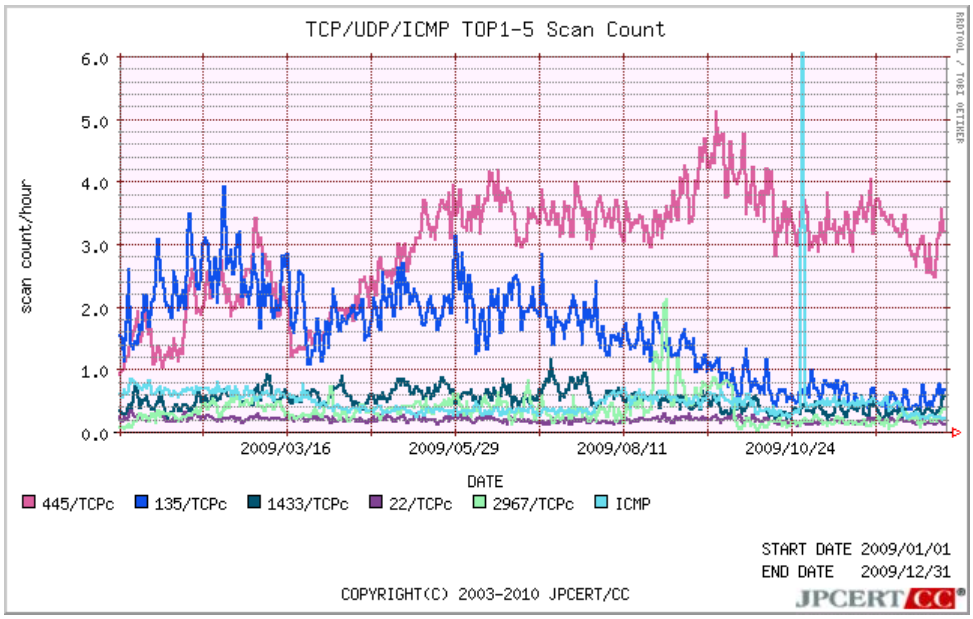

図 1-4: アクセス先ポート別グラフ top1-5

- アクセス先ポート別グラフ top6-10 (2009 年 1 月 1 日-2009 年 12 月 31 日)

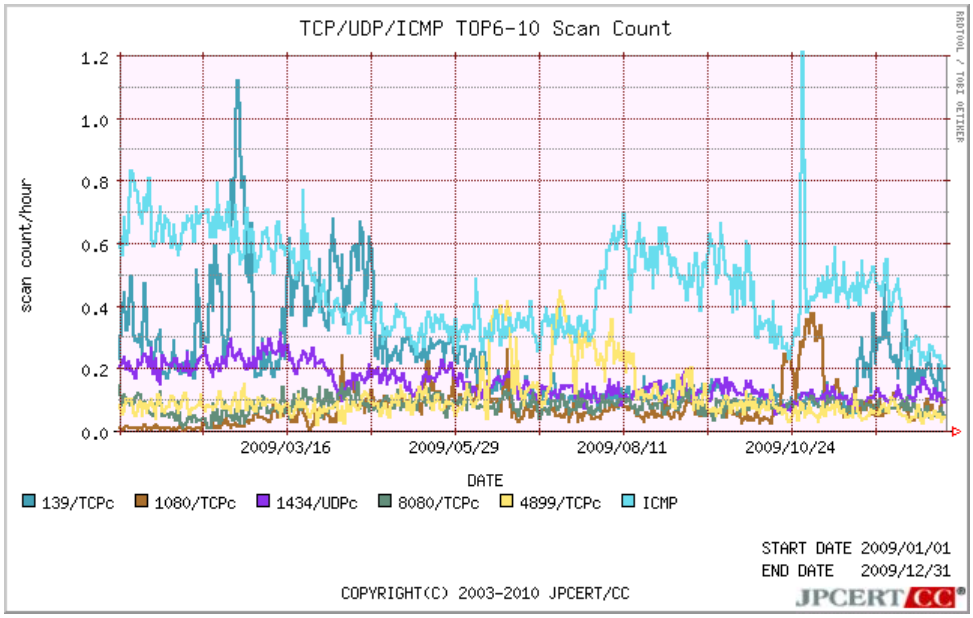

図 1-5: アクセス先ポート別グラフ top6-10

今四半期も、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探索活動が上位を占めています。新しい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。以前に見つかった旧知の脆弱性が探索されている可能性もありますので、脆弱性がないバージョンの OS やアプリケーションを使用しているか、ファイアウォールやアンチウイルス製品などが正しく機能しているかについて、今一度確認することが重要です。

1-4. フィッシング対策協議会 事務局の運営

JPCERT/CC 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 サイトの管理、一般消費者からの問い合わせに基づくフィッシングサイトの停止依頼、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。

1-4-1. 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ポータルサイトでは毎月の活動報告として「フィッシング情報届出状況」を公開しています。詳細については以下の URL をご参照ください。

フィッシング対策協議会
https://www.antiphishing.jp

フィッシング対策協議会 2009/10 フィッシング情報届出状況
http://www.antiphishing.jp/information/information1016.html

フィッシング対策協議会 2009/11 フィッシング情報届出状況
http://www.antiphishing.jp/information/information1020.html

フィッシング対策協議会 2009/12 フィッシング情報届出状況
http://www.antiphishing.jp/information/information1030.html

1-5. 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(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、協議会の問い合わせ窓口、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、ウェブサイト、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
http://www.nca.gr.jp/

2. 脆弱性情報流通関連活動

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情報の流通対策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および対応状況は 31 件 (総計 856 件) [図 2-1] でした。各公開情報に関しましては、JVN(http://jvn.jp/)をご覧ください。

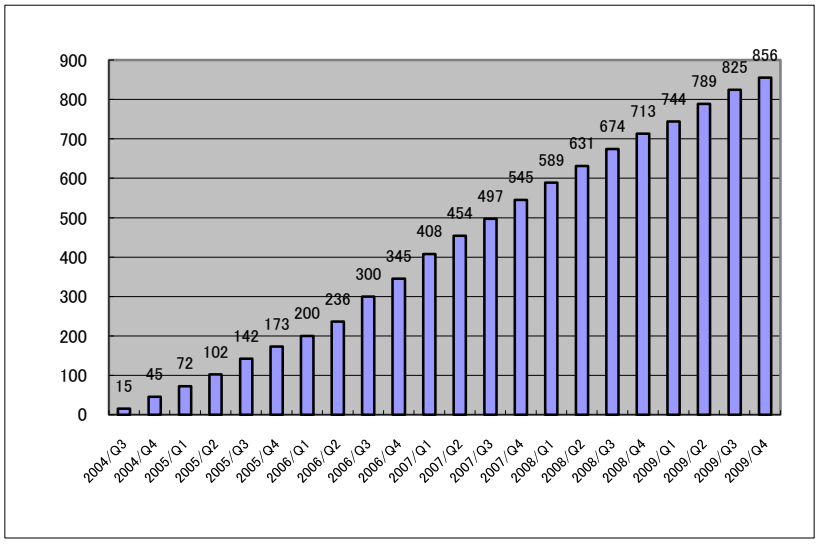

図 2-1: 累計 JVN 公表件数

このうち、本基準に従って、独立行政法人情報処理推進機構 (IPA) に報告され、公開された脆弱性情報は 16 件(累計 400 件) [図 2-2] でした。

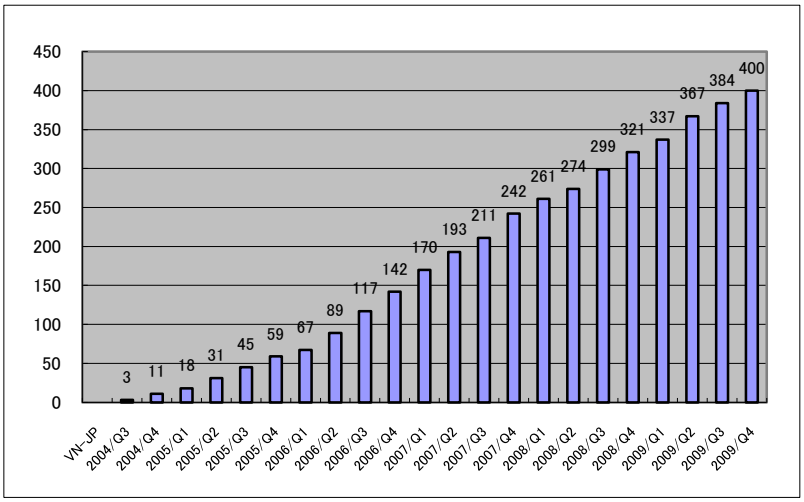

図 2-2: 累計 VN-JP 公表件数

また、CERT/CC とのパートナーシップに基づき、JVN にて VN-CERT/CC として 公開した脆弱性情報は 15 件(累計 433 件) [図 2-3]、また、CPNI とのパートナーシップに基づき、JVN にて VN-CPNI として公開された脆弱性情報は 0 件(累計 23 件) [図 2-4] でした。

本四半期 VN-CERT/CC として公開された脆弱性情報としては、Microsoft 製品に関するものが 5 件、Adobe 製品に関するものが 4 件と目立ちました。また、本四半期は、プロトコルの脆弱性情報が 4 件と比較的多く公開されました。

一方、本四半期の全体的な公開数は、本四半期前四半期までの各期と比較するとかなり少ない状況でした。その背景としては、海外特に米国の製品開発者・製造業者等の Thanks Giving Day、クリスマス休暇による対応の遅れや脆弱性情報の届出の減少等が考えられます。

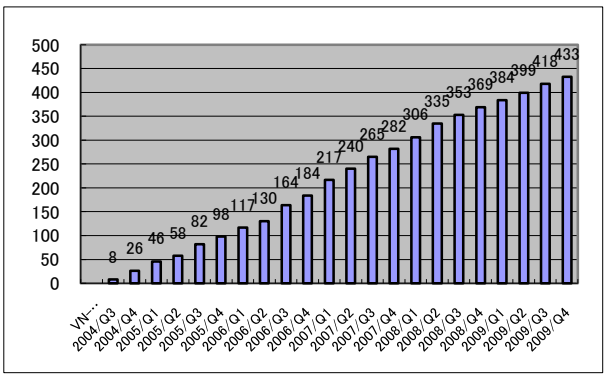

図 2-3: 累計 VN-CERT/CC 公表件数図

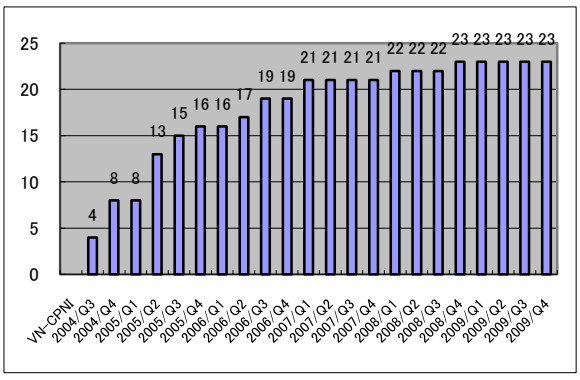

図 2-4: 累計 VN-CPNI 公表件数

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、米国の 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のオペレーション、公開日の調整、各国製品開発者の対応状況の集約等、脆弱性情報の公開のための調整活動を行っています。

また、国際的な活動の一環として、2008 年 5 月 21 日から JVN 英語版サイト(http://jvn.jp/en)の運用を開始し、それに併せて 2008 年 8 月から CVE(Common Vulnerabilities and Exposures) 識別子の取得も積極的に推進しました。その結果、運用開始後に JVN で公開されたものの 9 割以上に CVE 識別子が付与されています。実際に、JVN 英語版サイトへのアクセス数も半年前と比較して倍増しており、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り、その他の組織から公開されるアドバイザリにも、JVN 英語版サイトへのリンクが多くの場合掲載されるようになっています。
なお、CVE に関する JPCERT/CC の国際的な活動の詳細は、以下の URL をご参照ください。

CVE
http://cve.mitre.org/

Requirements and Recommendations for CVE Compatibility
http://cve.mitre.org/compatible/questionnaires/104.html

Organizations Participating
http://cve.mitre.org/compatible/organizations.html#j

本四半期さらに、2009 年第 2 四半期に公開された「JVNVU#943657 複数の TCP の実装におけるサービス運用妨害 (DoS) の脆弱性」(2009 年 9 月 9 日)および本四半期に公開された「JVN#75368899 IPv6 を実装した複数の製品にサービス運用妨害 (DoS) の脆弱性」(2009 年 10 月 26 日)に関しては、これまで脆弱性情報流通の枠組みに参加していなかった国内外の製品開発者にも JVN の情報に関心を持っていただく契機となり、脆弱性情報流通体制の拡充につながりました。このように、日本国内で発見された脆弱性に関連する情報が、日本国内のみならず国際的に流通し、より安全な製品開発が行われるよう、国際的な活動も引き続き積極的に行ってまいります。

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、以下の 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
http://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
http://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)
http://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
http://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 からの届出情報をもとに、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以下をご参照ください。

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示されています。
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。2009 年 12 月 31 日現在で 322 社 [図 2-5] 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、http://www.jpcert.or.jp/vh/agreement.pdf をご参照ください。

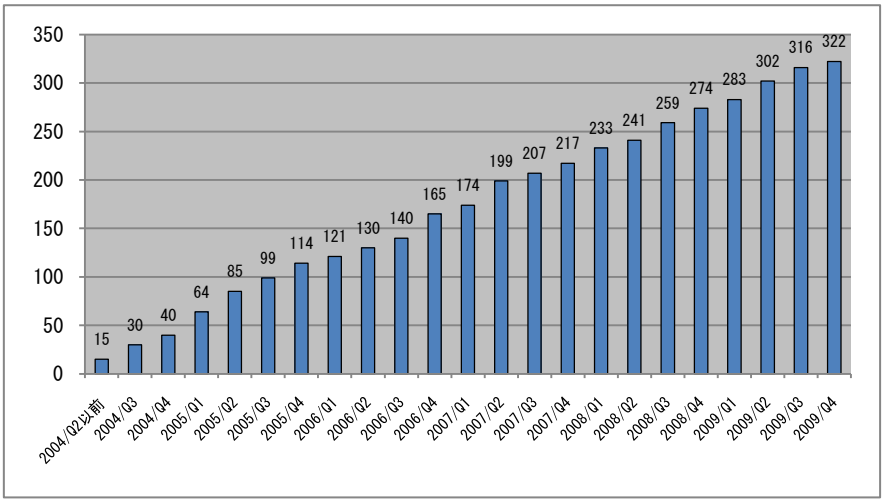

図 2-5: 累計製品開発者登録数

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。

2-3-4. 「責任ある脆弱性情報開示」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 RVD (29147: Responsible Vulnerability Disclosure)の標準化は、11 月に開催された SC27 の国際会議において、第 3 次作業草案に対する各国からのコメントの取扱いが審議され、第 4 次作業草案に向けた改訂方針が合意されました。

第 3 次作業草案(3rd WD: Working Draft)に対しては, メンバー国のうち 9 ヶ国から合計 245 項目、さらにアライアンス団体として FIRST(Forum of Incident Response and Security Teams)から 26 項目に及ぶコメントが寄せられました。日本も 63 項目のコメントを出しました。11 月 2～6 日に米国 Redmond の Microsoft 社で開催された SC27 国際会議では、これらコメントを一つ一つ審議し、草案の前半の各節については、ほぼ全面的な書替えを、後半については、章節構造の組替えを含む大幅な書替えをすることで合意され、この方針に基づいて第 4 次作業草案が作成されることになりました。稚拙さの目立った従来の草案は、今回の改訂により標準化文書としての完成度が大きく向上する見通しです。内容に関する特筆すべき点としては、対象として想定される製品の範囲を、パッケージ・ソフトウエア等だけに限定せず、ウェブ等によるオンライン・サービスまで含める方針が確認されたことや、発見者から脆弱性の報告を受けた製品開発者が 7 暦日以内に受領した旨の返事を送るべきことが合意されたことが挙げられます。

本標準化作業の当初計画では、今回の会議で委員会草案(CD: Committee Draft)に格上げすることになっていました。カナダや南アフリカ、韓国、マレーシアなどは、この国際標準化を急ぐ何ら

かの国内事情があるためか、格上げを主張しましたが、文書として期待すべき完成度に達していないとする日本や米国などの反対で見送られ、さらに作業草案として改訂を重ねることになりました。

今後は、第 4 次作業草案をエディタが用意し、2010 年 1 月 15 日までに SC27 事務局を通じて参加各国に配付し、各国は 3 月 15 日までにコメントを提出するよう求められる予定となっています。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計画です。

2-4. セキュアコーディング啓発活動

2-4-1. 安全なソフトウエア開発を行うための C/C++ セキュアコーディングセミナー実施

C/C++言語を使って安全なプログラムを開発するために、脆弱性を作り込まないコーディングを実践するための具体的なテクニックとノウハウを提供するセミナー「C/C++ セキュアコーディング　ハーフデイキャンプ 2009 秋@大阪」を 10 月 6 日、20 日、11 月 2 日の全 3 回にわたり実施しました。定員を上回る参加希望をいただき、延べ約 210 名の C/C++プログラマの方が受講されました。

セミナー後の受講者アンケートでは、回を重ねるにつれ高い評価をいただき、平均でも 8 割以上の受講者の方から「セミナーに価値があった」または「業務の役に立つ」との回答を得ました。また、今後のセミナーの題材に関する要望として、「静的/動的解析ツールの活用方法」や「セキュアな製品開発のための設計手法」、「C/C++セキュアコーディングスタンダードの活用方法」を希望する意見が多かったことから、今後これらの内容のセミナーを提供できるよう準備を進める予定です。

また、個々の開発現場のニーズに沿ってコース内容をアレンジし、講師が企業等に出向いて行う個別セミナーを、合計 2 回、のべ約 100 名のプログラマやエンジニアの方を対象に実施しました。個別セミナーの自社内開催にご興味のある企業の担当者様は、seminar-secure@jpcert.or.jp までご連絡ください。

その他にも、11 月 6 日には大阪南港 ATC で開催された「関西オープンソース 2009」で、12 月 5 日には九州産業大学で開催された「オープンソースカンファレンス 2009 Fukuoka」で、オープンソースソフトウエア(OSS)コミュニティの方を対象に OSS におけるセキュアコーディングの重要性に関する講演を行いました。

2-4-2. 書籍の出版、雑誌への寄稿、ウェブマガジン連載開始

JPCERT/CC の翻訳による書籍『CERT C セキュアコーディングスタンダード』(アスキー・メディアワークス刊)を出版しました。C 言語を使ったソフトウエア開発において、脆弱性を作り込まないセキュアコーディングを実践するために必要な知識やノウハウを、コード例と言語仕様上の問題をベースに解説し、コーディング規約としてコンパクトにまとめた実践的な内容です。
また、技術評論社の刊行による季刊技術誌「組込みプレス」第 17 巻(12 月発行)の特集「転ばぬ先の組込みセキュリティ」に、「実践セキュアコーディング」と題した寄稿をいたしました。
さらに、CERT C セキュアコーディングスタンダードの内容をより分かりやすく解説した連載記事「脆弱性の体質改善――C/C++セキュアコーディング入門」が、Web マガジン CodeZine (コードジン)で 11 月からスタートしました。詳細は以下 URL をご参照ください。

CodeZine
http://codezine.jp

2-4-3. セキュアコーディングセミナー in Indonesia

10 月 26 日、 27 日の 2 日間、インドネシアの首都ジャカルタにオフィスを構える ID-SIRTII (Indonesia Security Incident Response Team on Internet Infrastructure)を会場として C/C++ セキュアコーディングセミナーを実施しました。海外でのセキュアコーディングセミナーの実施はタイに続いて 2 カ国目です。本セミナーは、JPCERT/CC とインドネシアを代表する CERT 機関である ID-SIRTII の協力のもと、インドネシア国内の C/C++プログラマを対象に行われました。2 日間で約 50 名のプログラマの参加者を集め、好評のうちに終了しました。

本セミナーは、セキュアコーディングに必要な知識を 4 時間に凝縮した"C/C++ Secure Coding Essentials"と題する座学と、受講者が実際に脆弱なコードをレビューし、修正案を検討するハンズオンとの 2 部構成で行われました。ハンズオンでは、受講者が自ら発見したコードの欠陥を積極的に発表して講師と議論する場面などもあり、受講者の意識の高さが感じられました。

2-5. 制御システムセキュリティにおける啓発活動

2-5-1. 米国動向の調査報告書など新たに２つの文書を公開

以下の２つの文書を新たに作成し、JPCERT/CC ホームページの制御システムセキュリティコーナー(http://www.jpcert.or.jp/ics/)で 11 月 24 日に公開しました。

-「制御システムセキュリティガイドライン、標準、および認証への取り組みに関する分析」
制御システムのセキュリティに関する米国の取組み状況を日本国内の関係者に紹介するため、Digital Bond 社の調査資料をもとに、重要な制御システムのセキュリティガイドライン、標準お

よび認証への取組み、それぞれの取組みによって最も影響を受けるセクターおよび地理的地域、取組みの動向などについてまとめたものです。

-「重要社会インフラのためのプロセス制御システム（PCS）のセキュリティ強化ガイド」
プロセス制御システム（PCS: Process Control System）のセキュリティに関する意識向上を意図して、SEMA（スウェーデン緊急管理庁）がスウェーデン語で作成した文書の英訳版をJPCERT/CC が邦訳したものです。ヨーロッパの産官学の各界が、さまざまな共通課題に共同で取り組めるよう、また、必要に応じて集中的な取り組みとリソースの共有を行えるよう、制御系に特化したセキュリティに関する推奨事項が実例とともに分かりやすく述べられています。

JPCERT/CC ホームページの制御システムセキュリティコーナーは、一層のコンテンツの拡充を図るため、さらに３つの文書を来年１月中に公開することを目指しています。また、コーナー全体をより見やすいデザインにすべく改善を進める予定です。

2-5-2. 制御システムカンファレンス開催準備

昨年度に続き、制御システムセキュリティカンファレンスを 2010 年 2 月 9 日に東京(永田町)で開催する予定です。「ベンダの役割、ユーザの役割」をテーマに、制御システム関係者の複雑な役割の絡みあいを整理し、それぞれが何をすれば、セキュリティがより向上するのかという「気づき」の場を提供したいと考えています。
午前の第一部では国際的な制御システムセキュリティ検討 WG(MPCSIE)メンバーによる講演と活動紹介、午後の第二部では国内のユーザ、開発者、ベンダによる講演、パネルディスカッション等を企画しています。

2-5-3. 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準備を進めました。米国 DHS が開発した CSET(CS²SAT 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、入手方法の調査および試用を行うとともに、両者の特徴やその違いを理解した上で、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の説明会を開催し、併せて関連文書の一部日本語化などを進めました。これらのツールについては、広く公開する前に、モニターを募ってフィールド・トライアルを行うことも検討中です。

2-5-4. 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、2 回(10 月 1 日および 11 月 26 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。今後は、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、以下の URL をご確認ください。

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
http://www.jpcert.or.jp/ics/taskforce.html

2-5-5. 制御システム関連学界活動

10 月 22 日、12 月 3 日、および 12 月 11 日に 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。12 月 11 日には 2-5-4 に掲げたセキュリティ・アセスメント・ツールの説明を行いました。

11 月 5 日には「制御システムのオープン化におけるセキュリティ課題」と題して、(社)計測自動制御学会産業応用部門が主催する「2009 年度産業応用部門大会」において講演を行いました。

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ており、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なども行うほか、駆除ツール開発事業者と連携して対策技術の開発も行っています。

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、以下の 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/

2009 年 10 月度 サイバークリーンセンター活動実績
https://www.ccc.go.jp/report/200910/0910monthly.html

3-2. 「マルウエア対策研究人材育成ワークショップ 2009(MWS 2009)」への参画

「マルウエア対策研究人材育成ワークショップ 2009(MWS 2009)」(ボット対策プロジェクト運営委員会および情報処理学会が共催)は、ボット対策プロジェクトで収集しているボット観測データから抽出した「研究用データセット」を大学や研究機関等の参加組織に提供し、参加者が同じデータセットを活用して以下の3つの分野に関する研究発表を行うワークショップです。

(1) 検体解析技術の研究
(2) 感染手法の検知ならびに解析技術の研究
(3) ボットの活動傾向把握技術の研究

今回は、昨年度の MWS 2008 に続く 2 回目の開催であったことから、発表された研究内容も深さと広さを増したものとなりました。また、研究用データセットのうちの攻撃通信データを用いてマルウエアの挙動分析技術を競うセッション「MWS Cup 2009」が新たに設けられ、参加者がリアリティをもって技術を披露・交換し合う場となりました。

JPCERT/CC は、MWS 2009 の実行委員としてワークショップの企画・運営に参加し、ボット対策プロジェクトにおいてマルウエア解析や解析技術の効率化の調査研究を担当している立場から、研究用データセットを構成するマルウエア検体の選定を行いました。

この取り組みは、ボットやマルウエアに関する専門的な知識を持つ研究者/実務者の育成や、対策技術の高度化につながるものであることから、来年度以降の継続開催に期待が寄せられています。

マルウエア対策研究人材育成ワークショップ 2009(MWS 2009)
http://www.iwsec.org/mws/2009/

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

主にアジア太平洋地域の CSIRT(Computer Security Incident Response Team) に対し、イベントでの講演やトレーニング等を通して CSIRT の構築・運用支援活動を行い、各国とのインシデント対応調整における連携強化を図っています。

4-1-1. カンボジアにおける CSIRT 構築支援活動(2009 年 9 月 28 日-10 月 23 日)

カンボジアにおける CSIRT 構築支援活動として、JPCERT/CC の職員が JICA 短期専門家としてカンボジアに赴き、CSIRT の運用およびカンボジア国内 IT 関連企業等との関係構築を支援するとともに、カンボジア政府および民間企業を対象に情報セキュリティセミナーを開催しま

した。

4-1-2. フィリピン情報セキュリティセミナーへの参加(2009 年 12 月 9 日-12 月 11 日)

フィリピンの National CSIRT である PHCERT が主催した情報セキュリティセミナーに講師として参加し、フィリピンの政府関係者、ISP 事業者、金融機関等、約 30 名の参加者に向けて、CSIRT に関するトレーニングおよび啓発活動を行いました。JPCERT/CC からは、CSIRT 活動の重要性、国内連携および国際連携の重要性について紹介するとともに、情報セキュリティの最新動向、インシデント対応やインターネットセキュリティに関する技術知識、CSIRT の構築方法等について講義しました。

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、実施状況の情報収集を目的とした活動等を行いました。アジア太平洋地域における APCERT の枠組みや、国際的な FIRST の枠組みに則って活動しています。

4-2-1. インドネシア情報セキュリティセミナーへの参加(2009 年 10 月 29 日)

インドネシア政府およびインドネシアの National CSIRT である ID-SIRTII が主催した情報セキュリティセミナーに参加し、政府関係者、ISP 事業者、IT 関連企業等の参加者に向けて、啓発活動を行いました。本セミナーは、2009 年 6 月から行われており、参加したセミナーは 5 回目に当たります。JPCERT/CC からは、情報セキュリティの最新動向の一環として、サイバー犯罪のモデル等について講演しました。

4-2-2. バミューダ Global Public Policy Summit への参加(2009 年 11 月 2 日)

WITSA (World Information Technology and Services Alliance) が主催した Global Public Policy Summit (GPPS) Bermuda 2009 に出席し、パネルディスカッション(テーマ：安全で回復機能を備えた技術インフラを推進し、かつ個人情報を保護する政策は、経済発展を推進する政策と相反するか否か)にパネリストとして参加しました。なお、本セミナーには、約 25 ヶ国から、政府や IT 関連企業等の関係者が集いました。

4-2-3. ISO/IEC JTC 1/SC 27 Redmond 会議への参加(2009 年 11 月 2 日-6 日)

米国ワシントン州 Redmond で開催された ISO/IEC JTC-1/SC27 会議に出席し、特に、「責任ある脆弱性開示 (RVD: Responsible Vulnerability Disclosure (29147))」(前述の 2-3-4.参照)および

「情報セキュリティのインシデントマネジメント（Information Security Incident Management (27035))」に関する作業に参加しました。国内の情報規格調査会 SC27/WG4 小委員会係者や FIRST 等の国際コミュニティと協力しながら、これらの標準が我が国における運用や既存の CISRT 間の実務に整合するものとなるよう貢献していく予定です。

4-2-4. ベトナム情報セキュリティトレーニングへの参加(2009 年 11 月 9 日-11 日)

ベトナム情報セキュリティ協会(VNISA)が主催した情報セキュリティトレーニングで、JPCERT/CC のスタッフが講師を務めました。政府関係者、ISP 事業者、IT エンジニア、学生等、多岐の分野に渡る約 50 名の参加者に向けて、情報セキュリティの最新動向、インシデント分析、トラフィックモニタリング、脆弱性情報の読み方、技術ドキュメントの公開方法、セキュリティツールの紹介等について講義を行いました。また、参加者との議論を通じてベトナムにおける情報セキュリティの実情に対する理解を深めることができました。なお、このトレーニングは現地で注目を集め、その様子がテレビ番組で放映されました。

4-2-5. 香港 Information Security Summit 2009 への参加(2009 年 11 月 18 日)

香港で毎年開催されている情報セキュリティサミットに参加し、JPCERT/CC の活動およびアジア太平洋地域への展開を進めているインシデント対応ツールやトラフィックモニタリングツールに関する講演を行いました。本サミットは、今年で 7 回目を迎え、アメリカ、オーストラリア、ポーランド、中国、香港、日本等、様々な経済地域から参加者が集い、クラウドコンピューティング、仮想化、ソーシャルネットワーキングの時代におけるセキュリティをテーマとしてプロジェクトや取組みを共有しました。

4-3. APCERT 事務局運営

JPCERT/CC は、アジア太平洋地域の CSIRT の集まりである、APCERT (Asia Pacific Computer Emergency Response Team) の事務局を担当しています。

APCERT
http://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

2009 年 12 月 1 日-2 日に、FIRST が主催する December 2009 FIRST Technical Colloquium がマレーシアのクアラルンプールにて開催され、JPCERT/CC はトラフィックモニタリングおよびウェブアプリケーションセキュリティに関するハンズオンセッションの講師を務めました。

December 2009 FIRST Technical Colloquium
http://www.first.org/events/colloquia/dec2009/

5. 公開資料

各分野の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。

5-1. CERT C セキュアコーディングスタンダード (書籍出版)

書籍出版についての詳細は、「2-4-2. 書籍の出版、雑誌への寄稿、ウェブマガジン連載開始」をご参照ください。

5-2. Vulnerability Response Decision Assistance (脆弱性対応意思決定支援システム) の有効性検証報告書 日本語版

Vulnerability Response Decision Assistance (脆弱性対応意思決定支援システム、略称:VRDA、読み:ヴァーダ) は、組織が、脆弱性情報に関し、効率よく、一貫した対応ができるように支援するために、JPCERT/CC と CERT/CC が共同でデザインした脆弱性対応フレームワークです。VRDA コンセプトを適用することにより、脆弱性情報と対応履歴のデータベースを基に、新しい脆弱性に対して、その組織にとって最適である可能性が高い対応を導き出すことが可能となります。

本報告書は、VRDA コンセプトを実装したシステムである KENGINE (試行運用中) を用いることにより、各組織において実施すべき脆弱性対応がどの程度正しく提示されるかについて、米国 CERT/CC 含む 3 つの組織の協力を得て評価した結果をまとめ、日本語に翻訳したものです。種々の脆弱性情報、ユーザ組織及び意思決定モデルに対する提示内容を評価した結果、KENGINE が提示する対応内容が十分に正確であり、脆弱性対応に関する意思決定を支援できることが確認されました。

「Vulnerability Response Decision Assistance (脆弱性対応意思決定支援システム) の有効性検証報告書 日本語版」
https://www.jpcert.or.jp/research/2009/VRDA_Effectiveness-J_20091029.pdf

5-3. 技術メモ － MACtime からわかるファイル操作

MACtime の調査ツールは、ファイル操作の実行時刻やその順序などの情報を提供することができ、サーバへの不正侵入時の被害調査や手口調査、マルウエア等の不正なプログラムのファイル操作調査などの場面において、ファイル操作の意図や背景の推測に活用できます。

本技術メモでは、多くのファイルシステムにおいてファイル操作の実行時刻を記録している MACtime と、その調査ツールの活用方法を紹介しています。

技術メモ － MACtime からわかるファイル操作
https://www.jpcert.or.jp/ed/2009/ed090002_20091102.pdf

5-4. ソフトウエア設計工程における脆弱性低減対策　セキュアデザインパターン(英語版)

ソフトウエア製品の開発者が、設計工程において、より安全なソフトウエア製品を提供するための対策を検討される場合に、参考資料として利用していただけるよう本年 5 月に公開した、「ソフトウエア設計工程における脆弱性低減対策　セキュアデザインパターン(英語版)」に新たに 6 つのパターンを追加し、公開しました。

追加されたパターンは、次の 6 つです。

設計レベルのパターン
- Secure Factory
- Secure Strategy Factory
- Secure Builder Factory
- Secure Chain of Responsibility

実装レベルのパターン
- Secure Logger
- Clear Sensitive Information

ソフトウエア設計工程における脆弱性低減対策 セキュアデザインパターン(英語版)
https://www.jpcert.or.jp/research/2009/SecureDesignPatterns-E_091104.pdf

5-5. 制御システムセキュリティガイドライン、標準、及び認証への取り組みに関する分析

本文書についての詳細は、「2-5-1.米国動向の調査報告書など新たに２つの文書を公開」をご参照ください。

5-6. 重要社会インフラのためのプロセス制御システム（PCS）のセキュリティ強化ガイド

本文書についての詳細は、「2-5-1.米国動向の調査報告書など新たに２つの文書を公開」をご参照ください。

6. 講演活動一覧

(1) 鎌田 敬介(国際部部長代理)：
「Role of CamCERT of ISMTT」
Workshop on ICT Plolicy & Information Security―カンボジア, 2009 年 10 月 1 日

(2) 久保 正樹(情報流通対策グループ 脆弱性アナリスト), 富樫 一哉(事業推進基盤グループ システム開発マネージャ)，戸田洋三(情報流通対策グループ リードアナリスト)：
「文字列・整数」
「ファイル入出力」
「動的メモリ管理・書式指定文字列」
C/C++セキュアコーディング ハーフディキャンプ@大阪 ,2009 年 10 月 6 日,20 日,11 月 2 日

(3) Jack YS LIN(早期警戒グループ 情報セキュリティアナリト)：
「日本近期資安事件」
2009 中国計算機網絡安全応急(CNCERT/CC)年会―中国,2009 年 10 月 23 日

(4) 久保 正樹(情報流通対策グループ 脆弱性アナリスト),戸田洋三(情報流通対策グループ リードアナリスト)：
「Secure Coding Essentials in C and C++」
C and C++ Secure Coding 2Day Seminar―インドネシア,2009 年 10 月 26 日-27 日

(5) 真鍋 敬士(理事/分析センター長)：
「MWS の新たな展開に向けて：動作記録データセットを用いたマルウエア対策研究」(パネル)
マルウエア対策研究人材育成ワークショップ 2009(MWS2009),2009 年 10 月 28 日

(6) 鎌田 敬介(国際部部長代理)：
「Overview of Information Security」
SECURING YOUR ASSET NOW―インドネシア, 2009 年 10 月 29 日

(7) 早貸 淳子(常務理事)：
「情報セキュリティインシデントの動向と JPCERT/CC の活動」
ISS Square ネットワーク分科会 , 2009 年 10 月 31 日

(8) 伊藤 友里恵(経営企画室 兼 国際部部長)
「Do Policies that Promote Technology Infrastructures that Are Resilient and Secure,

and that Protect the Privacy of Personal Data Conflict with Policies that Encourage Economic Expansion?」
Global Public Policy Summit Bermuda 2009―バミューダ, 2009 年 11 月 2 日

(9) 小熊　信孝(情報流通対策グループ 情報セキュリティアナリスト) :
「制御システムのオープン化におけるセキュリティ課題」
計測自動制御学会 2009 年度 産業応用部門大会　計測・制御ネットワーク部会シンポジウム,2009 年 11 月 5 日

(10) 久保 正樹(情報流通対策グループ 脆弱性アナリスト) :
「セキュアコーディングノススメ」
関西オープンソース 2009,2009 年 11 月 6 日

(11) 鎌田 敬介(国際部部長代理), Chris Horsley(早期警戒グループ 情報セキュリティアナリスト) :
「Overview of Internet Security」
「Incident Analysis」
「Information Gathering and Analysis」
「Network Monitoring and Traffic Analysis」
「Publishing Technical Documents」
「Security Tools」
Technical Training on Information Security for IT managers―ベトナム, 2009 年 11 月 9 日-11 日

(12) 椎木 孝斉(分析センター センター次長) :
「不正アクセスの最新動向」
国立情報学研究所 ネットワークセキュリティ対策技術研修 ,2009 年 11 月 13 日

(13) Chris Horsley(早期警戒グループ 情報セキュリティアナリスト) :
「Tools for Monitoring Badness in the Asia Pacific」
Information Security Summit 2009―香港, 2009 年 11 月 18 日

(14) Jack YS LIN(早期警戒グループ 情報セキュリティアナリト) :
「中国における最新のインターネット事情」
Telecom-ISAC Japan SoNAR-WG,2009 年 11 月 20 日

(15) 真鍋敬士 (理事/分析センター長) :
「脅威のトレンド 2009: ソフトウエア、プロトコル、ウェブサイトをめぐる動向」(パネルディスカッション)
InternetWeek2009　,2009 年 11 月 24 日

(16) 鎌田 敬介(国際部部長代理), Jack YS LIN(早期警戒グループ 情報セキュリティアナリト) :
「海外におけるインターネットセキュリティインシデント概観」
InternetWeek2009　,2009 年 11 月 24 日

(17) Jack YS LIN(早期警戒グループ 情報セキュリティアナリト) :
「中国におけるフィルタリング導入政策」

InternetWeek2009　,2009 年 11 月 25 日

(18)　真鍋 敬士(理事/分析センター長)：
「不正アクセスの最新動向」
国立情報学研究所 ネットワークセキュリティ対策技術研修, 2009 年 11 月 27 日

(19)　早貸 淳子(常務理事)：
「コンピュータセキュリティインシデント対応支援の現場から―企業における対策の再確認につなげていただきたいこと」
2009 年度情報セキュリティ監査シンポジウム in Tokyo, 2009 年 11 月 30 日

(20)　真鍋 敬士(理事/分析センター長)，宮地 利雄(理事)：
「情報システムにおけるセキュリティ上の脅威 ～攻撃手法のトレンド～」
「制御システムのセキュリティを巡る動向」
セプターカウンシル 情報共有 WG(WG4),2009 年 12 月 1 日

(21)　鎌田 敬介(国際部部長代理),佐藤 しおり(国際部渉外担当リーダー)：
「Network Monitoring and Traffic Analysis」
「HTTP Protocol and Web application Security」
December 2009 FIRST Technical Colloquium―マレーシア, 2009 年 12 月 1 日-2 日

(22)　鎌田 敬介(国際部部長代理)：
「Network Monitoring and Traffic Analysis」
Lecture at University Putra Malaysia (Faculty of Computer Science and Information Technology)―マレーシア, 2009 年 12 月 4 日

(23)　久保 正樹(情報流通対策グループ 脆弱性アナリスト)：
「セキュアコーディングノススメ」
オープンソースカンファレンス 2009 福岡,2009 年 12 月 5 日

(24)　早貸 淳子(常務理事)：
「情報セキュリティインシデントへの対応と JPCEDRT/CC の活動」
セプターカウンシル サイバー攻撃対応力向上 WG,2009 年 12 月 9 日

(25)　鎌田 敬介(国際部部長代理),佐藤 しおり(国際部渉外担当リーダー)：
「Introduction of JPCERT/CC and APCERT Activities」
「Overview of Network Monitoring」
「International Network Monitoring Project: TSUBAME」
「Technical Overview of Internet Security」
「International IT Security Trends」
「Fundamentals of Computer Incident Handling」
「Creating a CSIRT」
The TSUBAME Project and Information Security Workshop―フィリピン, 2009 年 12 月 9-11 日

(26)　鹿野 恵祐(早期警戒グループ 情報セキュリティアナリスト)：
「インターネット定点観測における可視化の取り込み」

SecurityDay 2009,2009 年 12 月 16 日

7. 執筆・掲載記事一覧

(1) 早期警戒グループ：
「TCP のぜい弱性を突く DoS 攻撃 パッチがないなら機器の設定で対応を」
日経 BP 社 日経ネットワーク 11 月号, 2009 年 10 月 28 日

(2) 江田 佳領子(事業推進基盤グループ 広報)：
「新米セキュリティ担当者が行く！CSIRT 奮闘記 現場訪問編」
日経 BP 社 日経ネットワーク 11 月号, 2009 年 10 月 28 日

(3) 早期警戒グループ：
「ホームページ改ざんの被害増」
NHK おはよう日本, 2009 年 11 月 10 日

(4) 情報流通対策グループ制御システムセキュリティ：
「[調査リポート] 制御系プロトコルに関する調査研究～報告書サマリ」
月刊計装, 2009 年 11 月 10 日

(5) 久保 正樹(情報流通対策グループ 脆弱性アナリスト),富樫 一哉(事業推進基盤グループ システム開発マネージャ),戸田洋三(情報流通対策グループ リードアナリスト)：
「転ばぬ先の組込みセキュリティ「実践セキュアコーディング」」
技術評論社 組込みプレス, 2009 年 11 月 13 日

(6) 早期警戒グループ：
「転ばぬ先の組込みセキュリティ「組込み機器などでのセキュリティインシデント」」
技術評論社 組込みプレス, 2009 年 11 月 13 日

(7) 宮地 利雄(理事)：
「転ばぬ先の組込みセキュリティ「組込みシステムに必要なセキュリティとは？」」
技術評論社 組込みプレス, 2009 年 11 月 13 日

(8) 久保 正樹(情報流通対策グループ 脆弱性アナリスト)：
「動けばいいってもんじゃない」 脆弱性を作り込まないコーディング 第 1 回
「脆弱性体質の改善 ― C/C++セキュアコーディング入門 (1)」
翔泳社 CodeZine, 2009 年 11 月 19 日

(9) 江田 佳領子(事業推進基盤グループ 広報)：
「新米セキュリティ担当者が行く！CSIRT 奮闘記 現場訪問編」
日経 BP 社 日経ネットワーク 12 月号, 2009 年 11 月 28 日

(10) 戸田洋三(情報流通対策グループ リードアナリスト)：
「動けばいいってもんじゃない」 脆弱性を作り込まないコーディング 第 2 回
「ポインタ演算は正しく使用する ― C/C++セキュアコーディング入門 (2)」
翔泳社 CodeZine, 2009 年 12 月 1 日

(11) 早期警戒グループ：
「PART3 フィッシング詐欺」

日経 BP 社 日経パソコン 12 月 14 日号,2009 年 12 月 14 日

(12) 中尾 真二(事業推進基盤グループ 広報):
「国民 ID 時代の電子認証のあり方」SecurityDay2009 取材
翔泳社 CodeZine, 2009 年 12 月 17 日

(13) 中尾 真二(事業推進基盤グループ 広報):
「攻撃トラフィックの可視化」SecurityDay2009 取材
RBB TODAY, 2009 年 12 月 17 日

8. 開催セミナー一覧

(1) Security Day 2009

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

・主　　催 日本インターネットプロバイダ協会(JAIPA)、日本ネットワークセキュリティ協会(JNSA)、日本データ通信協会(Telecom-ISAC-Japan) 、日本電子認証協議会 JPCERT/CC
・開催時期 2009年12月16日
・集客人数 100名

詳細については、以下のURLをご参照ください。
Security Day 2009
http://securityday.jp/

9. 後援・協力一覧

(1) AVAR 2009: 12th Association of anti Virus Asia Researchers International Conference
2009 年 11 月 5 日～6 日

(2) Internet Week 2009
2009 年 11 月 24 日～27 日

(3) Email Security Expo & Conference2009
2009 年 11 月 26 日～27 日

(4) 第 6 回デジタル・フォレンジック・コミュニティ 2009 in TOKYO
2009 年 12 月 14 日～15 日

■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
http://www.jpcert.or.jp/form/