JPCERT CC®

JPCERT-PR-2009-0006

JPCERT/CC 活動概要［2009 年 7 月 1 日 ～ 2009 年 9 月 30 日 ］

2009-10-08 発行

【活動概要トピックス】

—トピック 1 —
国際インシデント対応演習への参加、人気セミナーの海外展開、アジア諸国の National CSIRT 構築支援活動などによる国際貢献、連携強化

インシデント対応に関する調整を円滑に実施するためには、グローバルな情報共有や各国の窓口 CSIRT 等との間の緊密な連絡・連携体制の構築、強化のための継続的な活動が重要です。JPCERT/CC では、このような観点から、国際連携強化のための様々な活動を行っています。7 月から 9 月にかけての国際連携・協力活動について、そのうちの 3 つを紹介します。

(1) ACID (ASEAN CERT Incident Drill)：ASEAN 諸国等 12 カ国の CSIRT による合同インシデント対応演習に参加

JPCERT/CC は、7 月 23 日に、ASEAN(東南アジア諸国連合)の各国 CSIRT が合同で実施したインシデント対応演習 ACID (ASEAN CERT Incident Drill)に参加しました。本演習は、国境を越えて発生するセキュリティインシデントに備え、ASEAN 加盟国及び周辺各国の CSIRT 間の連携の強化を目的に毎年実施されているもので、今回が 4 度目になります。今年は 12 カ国(日本、オーストラリア、ブルネイ、中国、インド、インドネシア、韓国、マレーシア、ミャンマー、シンガポール、タイ、ベトナム)から 14 のチームが参加しました。今回は、大規模なボット感染を想定したシナリオをもとに、マルウェア解析やボット制御用（Command and

Control) サーバの追跡・停止を含む、迅速なインシデント調査及び対応能力の向上を目標とした、実践的演習が行われました。

(2) セキュアコーディングセミナーをタイで開催

JPCERT/CC は 2006 年以降、C/C++言語を使用する製品開発者を対象に、脆弱性を作り込まないプログラミング「セキュアコーディング」に関する教材を開発し、多数のセミナーを開催してきました。2008 年度においては 2200 名以上のプログラマの方々に受講いただき、今年度も既に、700 名ものプログラマの方々に受講いただいています。

今年度は、さらに、海外でのセミナーのため英語教材を新たに開発し、9 月 1 日及び 3 日の 2 日間、タイ王国バンコク郊外にある Thailand Science Park で初の海外セミナーを実施しました。本セミナーは、タイ王国を代表する CERT 機関である ThaiCERT をはじめ、タイ国内の連携組織(T-NET、WiNS、NECTEC)*の協力を得て、タイ国内の C/C++プログラマを対象に実施しました。
タイ国内で C/C++セキュアコーディングに関する技術セミナーが行われるのが今回が初めてであったことから、できるだけ多数の方に聴講いただけるよう、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"と題した座学セミナーと、受講者が実際に脆弱なコードをレビューするハンズオンとの 2 部からなる 1 日コースの構成で、対象者別に 2 日間行いました。ハンズオンでは、受講者が自ら発見した脆弱性を積極的に発表し、その内容について講師と議論する場面もあり、受講者の意識の高さが感じられました。2 日間で約 100 名のプログラマの方々に参加していただき好評のうちに終了しました。

本年 10 月にはインドネシアで、2010 年 1 月にはベトナムで、それぞれ同様のセミナーを実施する予定です。

* T-NET: T-Net Company Limited
WiNS: Wireless Innovation and Security Laboratory
NECTEC: National Electronics and Computer Technology Center

(3) モンゴル及びラオスにおいて、情報セキュリティ啓発セミナーの開催、セキュリティインシデント対応機能の構築・運用に協力

日本とアジア地域各国との間の社会経済活動の IT 依存度の高まりを受け、円滑なインシデント対応調整のためには、アジア各国におけるセキュアな IT 利用環境の構築や窓口となる CSIRT の機能強化が重要になってきています。JPCERT/CC では、各国の窓口 CSIRT の機能強化を支援するとともに、各国の IT 利用環境をよりセキュアにするためのセミナー開催への協力等の活動を行っています。

9 月には、財団法人国際情報化協力センター(CICC)と協力し、モンゴル（9 月 9 日～11 日）及びラオス（9 月 14 日～18 日）において、情報セキュリティセミナーの開催や窓口 CIRST の構築・運用支援等の活動を行いました。

モンゴルにおいては、MonCIRT、Information Communications Technology and Post Authority (ICTPA)、CICC、JPCERT/CC が共同で情報セキュリティセミナーを開催し、モンゴルの政府機関、金融機関、ISP、IT 関連企業、教育機関等、約 60 名の参加者に向けて啓発活動を行いました。JPCERT/CC からは、昨今の情報セキュリティインシデントの傾向や CSIRT の対応活動について発表を行いました。また、MonCIRT 職員に向けて、個別にネットワークモニタリングのトレーニングを行い、MonCIRT のインシデント対応体制の強化に協力しました。さらに、モンゴルの情報セキュリティ事情を把握するため、CICC と合同で、モンゴルの政府組織、金融機関、ISP、IT 関連企業等に向けて、情報セキュリティ調査を実施しました。

ラオスにおいては、ラオスの政府機関、CICC、JPCERT/CC、IMPACT（International Multilateral Partnership Against Cyber Threats）等が協力して情報セキュリティセミナーを開催し、ラオスの政府機関や IT 関連企業等に向けて啓発活動を行いました。JPCERT/CC からは、昨今の情報セキュリティインシデントの傾向や CSIRT の重要性及び対応調整活動、APCERT(Asia Pacific Computer Emergency Response Team)におけるアジア太平洋地域の連携体制について発表を行いました。また、ラオス政府は 2010 年に National CSIRT を構築する予定であり、JPCERT/CC はラオスの政府機関、ISP、IT 関連企業等、約 30 名に向けて 3 日半にわたる CSIRT 構築トレーニングを実施し、ラオスの National CSIRT 構築に協力しました。

―トピック 2 ―

FIRST Annual Conference Kyoto 2009：世界のセキュリティチームによる国際会議の日本開催が成功裏に終了

6 月 28 日から 7 月 3 日まで、京都で、FIRST(Forum of Incident Response and Security Teams）の第 21 回年次会合が開催されました。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、及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るもので、今回は、セキュリティチーム、ベンダ、ユーザ企業、政府機関、法執行機関、教育機関等、世界 52 経済地域から約 400 名の参加者が集いました。日本での開催は、今回が初めてです。JPCERT/CC はローカルホストとして、国内の CSIRT メンバーや関係機関の協力を得ながら、世界でも最大規模のセキュリティ会議を成功に導く一助を担いました。

今年は、"Aftermath: Crafts and Lessons of Incident Recovery"のテーマのもと、フィッシング等に関するインシデントレスポンスから、ネットワークモニタリング等の技術、また CSIRT 運用や活動評価などのマネージメントに至るまで、情報セキュリティ全般にかかる様々な話題が取り上げられました。また、JPCERT/CC の国際部部長である伊藤友里恵がセッションチェアを務める"Law Enforcement Special Interest Group (LESIG)"も開催され、法執行機関の関係者らによる活発な議論が行われました。

さらに、7 月 4 日から 5 日まで、引き続き京都で、米国の CERT/CC が主催する National CSIRT Conference 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の状況や課題を共有するとともに、共同プロジェクトや各 CSIRT における独自の研究や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つながる成果を得ることができました。

The 21st Annual FIRST Conference 2009 Kyoto の詳細
http://conference.first.org/2009/

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

―トピック 3 ―

Web フォームによるインシデント報告の受付、注意喚起及び脆弱性情報の英語による発信等、利用者の利便性向上のための機能を追加

JPCERT/CC では、これまでメールと FAX で受け付けていたインシデントの届出について、Web フォームからも行うことができるよう機能追加を行い、7 月 10 日から受付を開始しました。また、JPCERT/CC Web サイト英語ページを拡充して、JPCERT/CC が発信する注意喚起の英訳と脆弱性対策ポータルサイト JVN の英語情報をご覧いただけるようにしました。

Web フォームによるインシデントの届出においては、従来のインシデント全般に関する届出フォームに加え、新たにフィッシング専用の届出フォームを新設しました。また、従来の届出フォームを見直して、どの項目に何を記入すべきか、内容をどのように記載すべきかをわかりやすくし、容易かつスピーディに届出ができるよう工夫しました。
この結果、これまで報告実績のなかった組織からの報告が増え、インシデント対応に関する相談や調整(コーディネーション)の依頼をいただきました。

また、国内外において英語による情報収集をされている方々への情報配信の強化を目的に、注意喚起の英訳と脆弱性対策ポータルサイト JVN の英語情報を JPCERT/CC Web サイト英語ページでご覧いただけるようにした結果、トップページへのアクセス数が前四半期より 10%強増

加しました。英語圏の拠点や顧客との間で、注意喚起や脆弱性情報を共有するなどの用途等でご活用いただくことを期待しています。

インシデント報告の届出の詳細
http://www.jpcert.or.jp/form/index.html

JPCERT/CC Web サイト英語ページの詳細
http://www.jpcert.or.jp/english/

―トピック 4 ―
「JPCERT/CC 脆弱性関連情報取扱いガイドライン」の改定

JPCERT/CC は、2004 年の経済産業省告示「ソフトウエア等脆弱性関連情報取扱基準」に基づく情報セキュリティ早期警戒パートナーシップの運用開始当初から、ソフトウエア製品等に関する脆弱性関連情報を取り扱う調整機関として、受付機関に指定されている IPA(独立行政法人情報処理推進機構)とともに、制度運用の中核を務めています。

JPCERT/CC では、「JPCERT/CC 脆弱性関連情報取扱いガイドライン」を改定し、7 月 10 日に公表しました。
今回の改定では、7 月 8 日に公開された「情報セキュリティ早期警戒パートナーシップガイドライン」の改定に対応し、開発者と連絡が取れない等の理由により進捗が見込めない脆弱性案件について、取扱いを滞留させることなく、既知の情報をもとに脆弱性の存在を公表し、利用者に注意を呼び掛けることができるようにすることを目的に、具体的な運用手順を定めています。
まもなく、改定された両ガイドラインに基づく運用を開始する予定です。引き続き、脆弱性の発見者として、対応する製品の開発者として、あるいは製品の利用者として、情報セキュリティ早期警戒パートナーシップへのご支援ご協力をお願いします。

「JPCERT/CC 脆弱性関連情報取扱いガイドライン」の詳細
http://www.jpcert.or.jp/vh/guideline_2009.pdf

―トピック 5 ―
文部科学省の先導的 IT スペシャリスト推進プログラムによる高度セキュリティ人材育成活動に協力

JPCERT/CC は、文部科学省「平成 19 年度先導的 IT スペシャリスト育成推進プログラム」の下で展開されている、IT Keys (IT specialist program to promote Key Engineers as securitY Specialists)と、「研究と実務融合による高度情報セキュリティ人材育成プログラム」(略称：

ISS スクエア)のプロジェクトの双方に対して、公的な情報セキュリティ専門機関の立場から協力を行いました。

2007 年度から 3.5 年計画で実施されている「IT Keys」プロジェクトに対しては、JPCERT/CC はボット対策プロジェクトの一員として、2008 年度に続き「リスクマネジメント演習」の講義の一部を担当し、ボット分析業務の手法の指導と教材用のマルウェア検体を用いた解析演習を行いました。

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

JPCERT/CC は、セキュリティエンジニアの育成が長期的な視点でのセキュリティ対策に欠かせないものであるととらえており、研究教育機関等と協力しながらこのような演習や講習を実施しています。とくに、教材用の検体を使った演習などは、継続してボット対策に取り組んでいる JPCERT/CC ならではの経験を反映した内容になっています。

また、平成 20 年 4 月にスタートした産学連携の人材育成プログラム「研究と実務融合による高度情報セキュリティ人材育成プログラム」(略称：ISS スクエア)に対しては、2 名のインターンシップ研修生を受け入れました。研修生には、約 1 カ月間にわたり、それぞれ「制御システム・セキュリティに関する調査と普及啓発資料の開発等」、「マルウェア分析におけるデータの安全な取り扱いに関する調査など」といったテーマで、実務の一端を体験してもらうことができました。

―トピック 6 ―
ボット対策事業に関する平成 20 年度活動報告を公開

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のポータルサイト「サイバークリーンセンター」において、平成 20 年度の活動内容をまとめた「平成 20 年度サイバークリーンセンター活動報告」を公開しました。

サイバークリーンセンターについて
https://www.ccc.go.jp/ccc/index.html

平成 20 年度サイバークリーンセンター活動報告の詳細
https://www.ccc.go.jp/report/h20ccc_report.pdf

JPCERT/CC はこのプロジェクトの中で「ボットプログラム解析グループ」としてボットプログラムの解析と駆除ツールの提供を担当しており、平成 20 年度は特定のボット配布サイトや

特定のボットファミリに注目した分析等も行いました。その経過については、本報告中にまとめられています。

―トピック 7―

制御システムのセキュリティに関する提供情報を拡充

生産設備の稼働，環境の管理や監視など、ますます広い分野で私たちの生活や企業活動を支えている制御システムは、機能の高度化と並行して、オフィス用コンピュータと同じ技術やコンポーネントを取り入れる方向に進みつつあります。したがって、オフィスのコンピュータと同様に、制御システムでもセキュリティ対策を真剣に考えるべき時期に入り始めています。しかしながら、システム要件の相違から、必ずしも既存のセキュリティ対策をそのまま適用できるわけではない、などの課題を抱えています。

JPCERT/CC でも、今年 2 月に開催した制御システムセキュリティカンファレンスをはじめとする各種の取組みに着手しており、7 月からは制御システムの開発者に向けたニュースレターの配信を開始し、9 月には JPCERT/CC のホームページ内の「制御システム・セキュリティ」のコーナー(http://www.jpcert.or.jp/ics/)を拡充ならびに刷新して公開致しました。

今回新たに公開した情報は、次のとおりです：

* 2009 年 2 月に開催された制御システムセキュリティカンファレンスの講演資料(講演者から公開の了承が得られなかった一部を除く。)

なお、今年度も、2010 年 2 月に、「ベンダがすべき事、ユーザがすべき事」(仮題）をテーマに、制御システムセキュリティカンファレンスを開催すべく準備を進めており、本年 12 月頃に開催のご案内を配信する予定です。

－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 2009 年 7 月 1 日から 2009 年 9 月 30 日までの間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 2983 件（届出を受けたメール、FAX の延数は 3228 通 *1)、IP アドレス別の集計では 3141 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。

インシデントに関する届出数、IP アドレス数ともに前四半期から倍増しています。これは、5 月以降定常的に寄せられている、マレーシアのセキュリティ対応機関からマルウエア設置サイトに関する届出が、今期に入って大幅に増加したことや、フィッシングサイトに関する届出が増加したことに因るものです。

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 837 件でした。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ェ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/2009/IR_Report090709.pdf

1-1-1. インシデントの傾向と分析

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 58 件から 104 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急増したためです。これらの事例では、設置されるコンテンツやフィッシングの手口が類似しており、なんらかの攻撃ツールが広く流通している可能性があります。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管理者に対して、「フィッシングサイトの停止」のための調査対応依頼を行っており、その時点においては、すべてのフィッシングサイトが停止しています。

マレーシアのセキュリティ対応機関からは、マルウェア設置サイトに関する届出を多数受領しています。これは、この機関が大規模にマルウェア設置サイトの調査を行った結果得られた情報のうち日本に関連するものを JPCERT/CC に提供しているものです。この届出も含め、マルウェアに関連して届け出られたインシデントに関係する IP アドレスの数は 2154 件に達しました。多数のサイトがインシデントに関連しており、マルウェアに関する脅威が広がっていることが推察されます。JPCERT/CC では、届出に係るマルウェア設置サイト上のマルウェアの解析や脅威分析を行い、影響が大きいと考えられるものについて、マルウェア設置サイトの管理者に対して調査対応依頼を行っています。

さらに、今四半期は、Scan の報告が前四半期の 278 件から 469 件に増加しました。増加分は、もっぱら TCP139、TCP445 番ポートに対する Scan であり、これらのアクセスは、MS03-026、MS08-067 など、Windows の脆弱性を攻撃するアクセスであると推察されます。かなり以前に公表された既知の脆弱性が今でも攻撃の対象として狙われています。TCP139、TCP445 番ポートが、ルータやファイアウォールなどの対策により、インターネットから直接アクセスすることができなくなっていても、マルウェアに感染したコンピュータがローカルネットワークに接続されるとローカルネットワーク内で感染が拡大する可能性もあります。ローカルネットワークに接続しているコンピュータであっても、OS を含む、コンピュータで使用している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、また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。

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/

1-2. 情報収集・分析

JPCERT/CC 早期警戒グループでは、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。
JPCERT/CC では、これら様々な脅威情報を多角的に分析し（一部、脆弱性やウイルスの検証などもあわせて行います。）、その分析結果に応じて、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

2009 年 7 月 1 日から 2009 年 9 月 30 日までの間において、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：9 件　https://www.jpcert.or.jp/at/

2009-09-09　複数製品の TCP プロトコルの脆弱性に関する注意喚起（公開）
2009-09-09　2009 年 9 月 Microsoft セキュリティ情報（緊急 5 件）に関する注意喚起（公開）
2009-08-12　2009 年 8 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）
2009-08-03　ISC BIND 9 の脆弱性を使用したサービス運用妨害攻撃に関する注意喚起（更新）
2009-07-31　ISC BIND 9 の脆弱性を使用したサービス運用妨害攻撃に関する注意喚起（公開）
2009-07-31　Adobe Flash Player 及び Adobe Acrobat/Reader の脆弱性に関する注意喚起　（公開）
2009-07-29　Microsoft ATL を使用した複数製品の脆弱性に関する注意喚起（公開）
2009-07-15　2009 年 7 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）
2009-07-10　韓国、米国で発生している DDoS 攻撃に関する注意喚起（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、毎週水曜日(祝祭日を除く)に発行しています。また、「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 65 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.　2009 年第 3 四半期(7-9 月)の動向について

2009 年 7 月、米国、韓国において政府系組織や金融機関などを対象としたサイバー攻撃(分散型サービス不能攻撃：DDoS 攻撃)が発生しました。攻撃は主に韓国国内の一般ユーザのコンピュータから行われ、一部日本のコンピュータも含まれていました。JPCERT/CC では、韓国 KrCERT/CC と連携し、情報収集・分析を行い、以下の注意喚起を発行いたしました。

2009-07-10 韓国、米国で発生している DDoS 攻撃に関する注意喚起
http://www.jpcert.or.jp/at/2009/at090012.txt

これら一連のサイバー攻撃は、韓国で広く利用されているソフトウエア配布サイトが攻撃者によって改ざんされ、ソフトウエアにウイルスが仕込まれた所から始まりました。このソフトウエアをダウンロード、インストールしたユーザがウイルスに感染し、今回のサイバー攻撃に利用されました。
また、2009 年 8 月日本国内でもソフトウエア配布サイトにウイルスに感染したソフトウエアが掲載され、それらソフトウエアをインストールしたユーザがウイルスに感染した事例が発生しています。
このような事から、業務で使用するコンピュータには必要最小限のソフトウエアのみインストールを許可するなど、組織としてコンピュータ利用に関するポリシーを徹底していくことが重要になります。

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情報を収集しています。これら観測情報は、世の中に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使用されます。また、ここで収集した観測情報の一部を JPCERT/CC Web ページなどで公開しています。

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、スキャン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

2009 年 7 月 1 日から 2009 年 9 月 30 日までの間に 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 4-1-1、4-1-2 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-9 月 30 日)

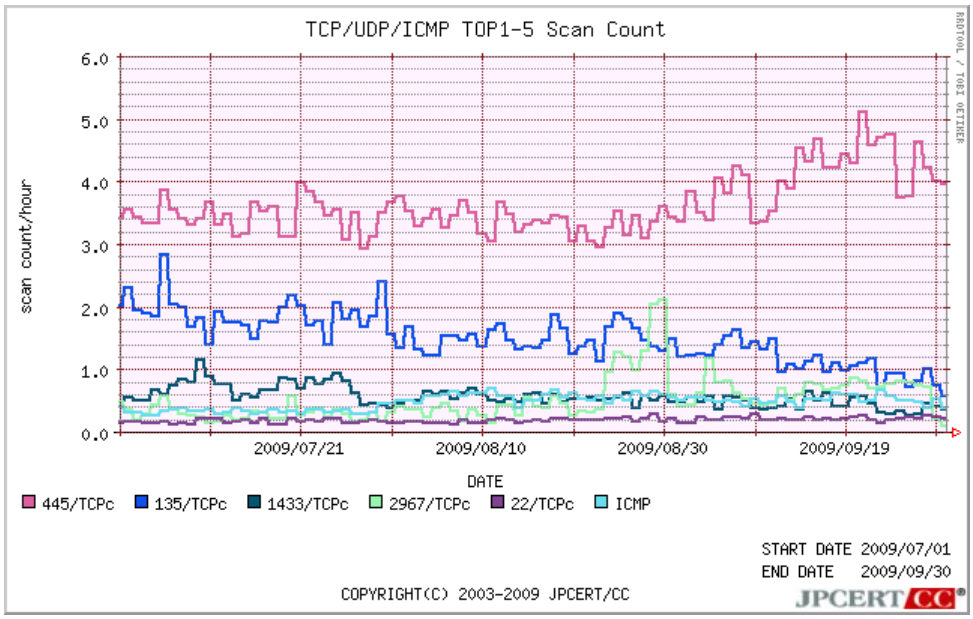


図 4-1-1: アクセス先ポート別グラフ top1-5

- アクセス先ポート別グラフ top6-10 (2009 年 7 月 1 日-9 月 30 日)

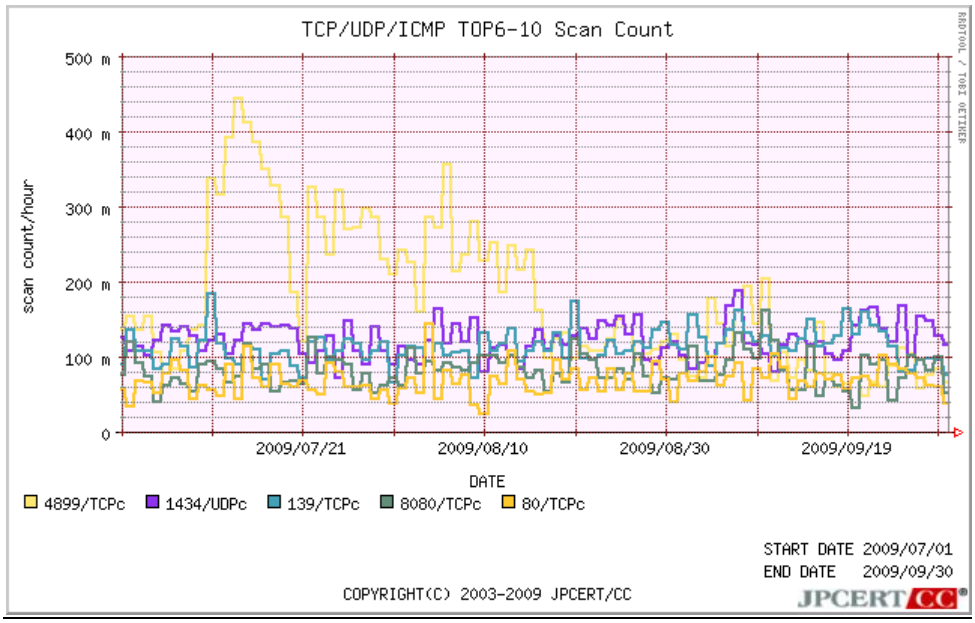


図 4-1-2: アクセス先ポート別グラフ top6-10

また、より長期間のスキャン推移を表すグラフとして、2008 年 10 月 1 日から 2009 年 9 月 30 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 2-3、図 2-4 に示します。

- アクセス先ポート別グラフ top1-5 (2008 年 10 月 1 日-2009 年 9 月 30 日)

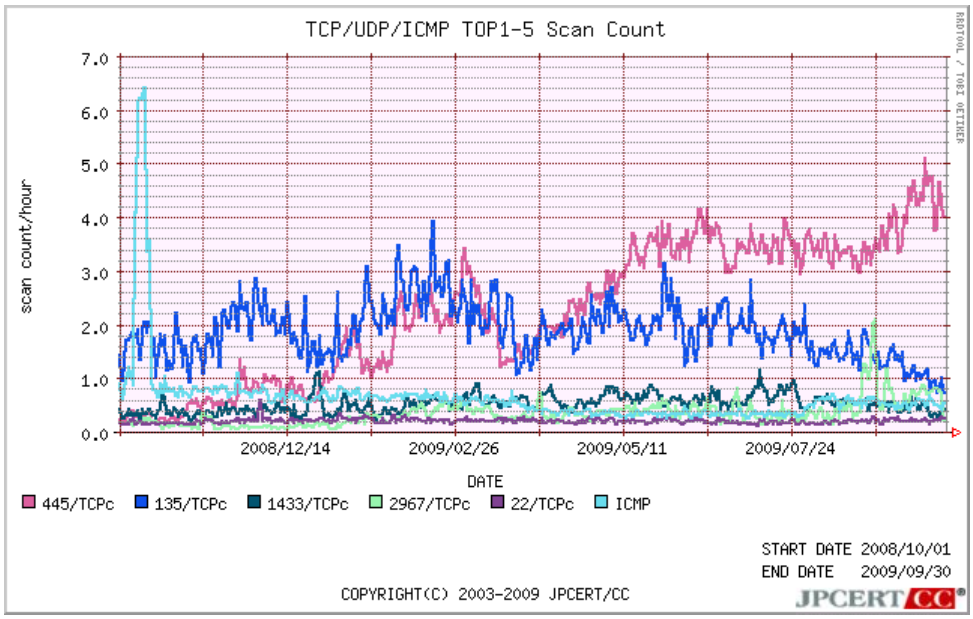


図 4-1-3: アクセス先ポート別グラフ top1-5

- アクセス先ポート別グラフ top6-10 (2008 年 10 月 1 日-2009 年 9 月 30 日)

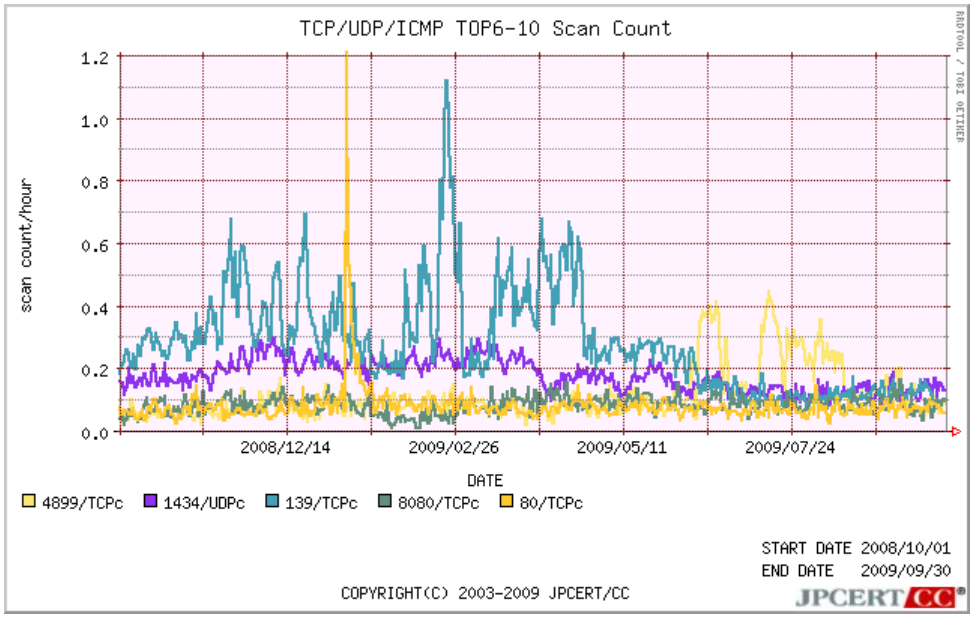


図 4-1-4: アクセス先ポート別グラフ top6-10

今期も、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、Scan 傾向の上位を占めています。特に TCP

445 宛の Scan は、9 月中旬に一段と Scan 数が増えていますが、これは Vista/2008 のゼロデイ脆弱性を対象とした Scan と考えられます。Microsoft からは暫定対策方法が公開されていますが、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。

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及び対応状況

2009 年 7 月 1 日から 2009 年 9 月 30 日までの間に JVN において公開した脆弱性情報及び対応状況は 36 件 (総計 825 件) [図 3-1] 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。

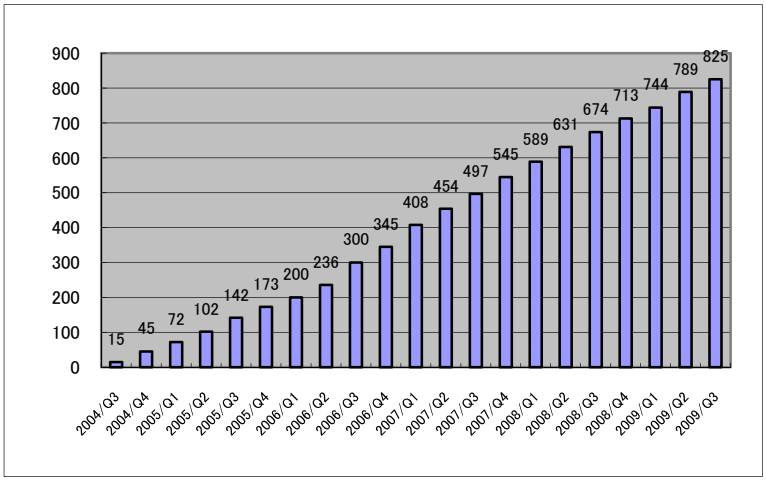


図 3-1: 累計 JVN 公表件数

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 17 件(累計 384 件) [図 3-2] でした。
今期は、公開数が 17 件と前期の公開数と比べると約半減しました。その背景としては、脆弱性情報の届出の減少、及び製品開発者・製造業者等の夏期休業などによる対応の遅れが考えられます。

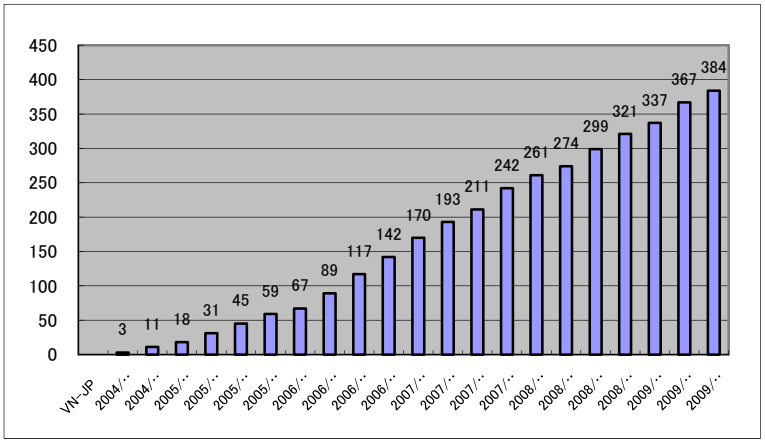
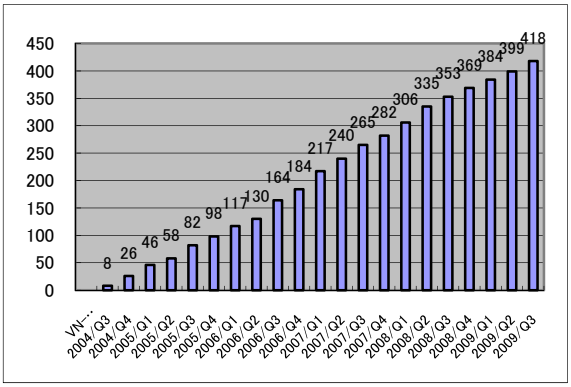


図 3-2: 累計 VN-JP 公表件数

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 19 件(累計 418 件) [図 3-3]、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 3-4] でした。
今期 JVN-CERT/CC として公開された脆弱性情報としては、Microsoft 製品や Adobe 製品に関するものが目立ちました。



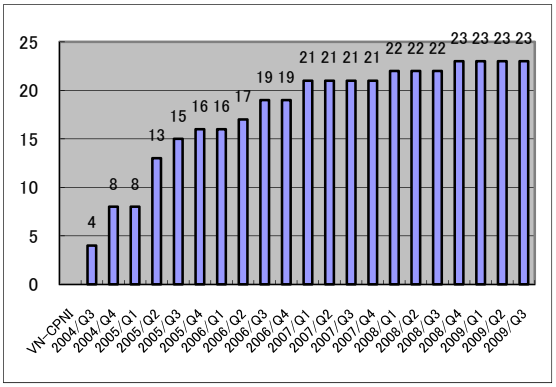


図 3-3: 累計 VN-CERT/CC 公表件数図　　図 3-4: 累計 VN-CPNI 公表件数

さらに今期は、CERT-FI（フィンランド）との国際調整を行い、TCP/IP に関する脆弱性関連情報の公開に至りました。

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 など海外 CSIRT と、報告された脆弱性情報の共有、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等、公開までの情報を共有し活動を行っています。

京都で開催された FIRST の年大会で関係者が来日した機会をとらえて、7 月 6 日に東京で「Vultures Meeting」を開催しました。これは、脆弱性情報を取り扱っている National CSIRT による情報や意見の交換会です。今回は、英国の CPNI とフィンランドの CERT-FI から各 2 名の担当者が参加し、各組織から、それぞれのチーム体制や各国内及び近隣地域における活動状況、最近の注目すべき脆弱性課題などが紹介され、意見交換を行いました（米国 CERT/CC は、事情により今回は欠席）。

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

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 の活動及び四半期毎の届出状況については
http://www.ipa.go.jp/security/vuln/ をご参照ください。

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、連絡先情報の整備に際し、製品開発者の皆様に製品開発者としての登録をお願いしています。2009 年 9 月 30 日現在で 316 社［図 3-5］の製品開発者の皆様に、ご登録をいただいています。

一方、脆弱性情報への対応が必要な製品開発者と連絡がとれず、連携した対応が困難なケースが増加してきており、関係組織との協議のもと、それらのケースへの対応について準備を進めております。
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。

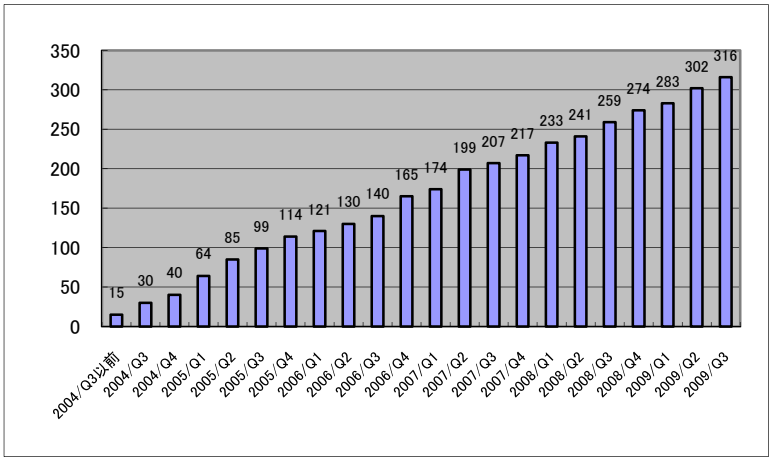


図 3-5: 累計製品開発者登録数

2-3-3. 「JPCERT/CC 脆弱性関連情報取扱いガイドライン」の改定

脆弱性情報ハンドリングにおいて、届け出られたソフトウエア製品等の脆弱性情報に関し、対象製品の開発者の応答が得られず連絡が取れず調整に着手できない、または調整が停滞するケースが増えている現状を踏まえ、2008 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、一定の努力を行ってもなお開発者と連絡が取れない場合には、既知の情報をもとに脆弱性の存在を公表し利用者に注意を呼び掛けることができるように「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」が改定され、7 月 8 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」において、開発者と連絡が取れない等の理由により進捗が見込めない脆弱性案件に関する具体的な運用手順を新たに定め、改定版として 7 月 10 日に公表しました。

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

このガイドラインでは、脆弱性情報に関係する製品開発者との連絡が取れないケースとなる判断基準、連絡が取れないケースにおける取扱いや、既知の情報をもとに脆弱性の存在を公表する手順等について定めています。この改定により、進捗が見込めない案件についても、ソフトウエア製品の利用者にむけて適切に注意を呼び掛けることができるようになると期待されます。

まもなく、改定された両ガイドラインに基づく運用を開始する予定です。引き続き、脆弱性の発見者として、対応する製品の開発者として、あるいは製品の利用者として、情報セキュリティ早期警戒パートナーシップへのご支援ご協力をお願いします。

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 RVD (29147: Responsible Vulnerability Disclosure)の標準化作業に引き続き参加しました。

5 月の北京会議における審議を踏まえて、エディタが内容を改訂して作成された、第 3 次作業草案(3rd WD: Working Draft)が 6 月末に参加各国に配付されました。日本から提出した、脆弱性情報の望ましい公表形式や脆弱性の発見者が届出に使うフォームなどが、参考資料として取り込まれています。ただ、全体的には、通常の標準化検討においては、第 3 次作業草案くらいまでには相当の完成度に達し、次の委員会草案に格上げされるケースも少なくありませんが、本草案は、まだ低い完成度のままです。

今四半期は、次回 11 月の国際会議に向けて、第 3 次作業草案に対する日本としてのコメント案を作成し、国内委員会に審議をお願いしました。その結果、50 項目以上の指摘事項を含むコメント案がまとまり、間もなく SC27 の国際事務局に送付される見通しです。次回の国際会議への参加など、引き続き、この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++ で脆弱性を含まない安全なプログラムをコーディングする具体的なテクニックとノウハウを学んでいただくための無料セミナー「C/C++ セキュアコーディング　ハーフデイキャンプ 2009 夏」を全 3 回にわたり実施し、約 200 名の C/C++プログラマの方にご参加いただきました。

また、組織ごとにコース内容を調整し、より現場に沿った形式にアレンジした上で実際の製品開発者の皆様にセキュアコーディングを学んでいただける場として提供している有償セミナーを合計 2 社、約 170 名のプログラマやエンジニアの方に受講していただきました。個別セミナー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。

2-4-2. セキュアコーディングセミナー in Thailand

JPCERT/CC は、これまで日本国内でのみ行っていた C/C++セキュアコーディングセミナーを、2009 年 9 月 1 日及び 2009 年 9 月 3 日の 2 日間、タイ王国バンコク郊外にある Thailand Science Park で実施しました。本セミナーは、JPCERT/CC とタイ王国を代表する CERT 機関である ThaiCERT をはじめ、タイ国内の連携組織(T-NET、 WiNS、 NECTEC)との協力の下、タイ国内の C/C++プログラマを対象に無償で行われました。タイ国内で C/C++セキュアコーディングに関する技術セミナーが行われるのは今回が初めてということで、2 日間で約 100 名のプログラマの方々の参加を得、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"と題した座学セミナーと、受講者が実際に脆弱なコードをレビューし修正案をするハンズオンの 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脆弱性を積極的に発表したり講師と議論したり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. JPCERT/CC ホームページの制御システムセキュリティのコーナーの更改

JPCERT/CC ホームページの「制御システムセキュリティ」のコーナー（http://www.jpcert.or.jp/ics/）に新たな情報を追加するとともに構成を一部変更し、9 月 18 日に公開しました。今回の変更ポイントは次のとおりです。

＜構成の変更＞
-見ていただきたい情報の優先度付け
-JPCERT/CC の他のページとトーンを合せることによる、操作性、保守性の向上
-将来的な拡張性に配慮して、年別に資料を再構成
-必要な情報に直感的かつ容易にたどりつけるようにカテゴリを見直し

＜コンテンツの追加＞
-2009 年 2 月のカンファレンス講演資料を追加
-タスクフォース活動の紹介
-制御システムセキュリティ関連脆弱性情報（JVN）へのリンク
今後とも、一層のコンテンツ拡充と、より見やすいデザインへの改善を進める予定です。

2-5-3. 制御システムカンファレンス開催準備

昨年度同様、今年度も海外からスピーカーを招いて制御システムセキュリティカンファレンスを開催すべく準備を進めています。詳細につきましては、本年 12 月頃にご案内させていただく予定です。

2-5-4. アセスメントツールの検証

啓発活動の一手段として制御システム関係者へのセキュリティアセスメントツールの提供を計画しており、その準備として、米国 DHS が開発した CS2SAT と英国 CPNI が開発した SSAT の 2 種類のツールについて、次の観点から、試用・検証を行いました。

-どのような方々に使用していただくのが最も効率的かつ効果的かを検討
-それぞれの業態や規模による適用可能性の差異
-ツールの特徴の比較表及びツール選択ガイドの作成

広く公開する前にモニターを募り、いただいた意見のフィードバックを行うことも検討中です。

2-5-5. タスクフォースへの情報発信

制御システム開発関係者へのセキュリティ啓発活動として、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及び関係する標準の動向や技術情報に関するニュースなどを収集して掲載したニュースレターの配信を開始しました。今後も、さらに充実した内容の情報を発信していく予定です。

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、JPCERT/CC の以下のページからご確認ください。

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

2-5-6. 制御システム関連学界活動

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。

7 月 24 日には、学術振興会プロセスシステム工学第 143 委員会(委員長: 長谷部伸治京都大学教授)において、名古屋工業大学の越島教授とともに、プロセス制御システムにおけるセキュリティ課題について報告を行いました。

また、8 月 18 日～8 月 21 日に福岡国際会議場で、計測自動制御学会(SICE、日本）と韓国の制御システム学界 ICROS（Institute of Control, Robotics and Systems）が共同開催した国際会議 ICCAS-SICE 2009 において、「Control System Security in the Shift to Open Systems」(オープン・システムへの移行における制御システムセキュリティ)と題する講演を行いました。

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、及び駆除ツールの作成をしています。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。詳細につきましてはサイバークリーンセンターの Web サイトをご参照ください。

サイバークリーンセンター
https://www.ccc.go.jp/

2009 年 07 月度 サイバークリーンセンター活動実績

https://www.ccc.go.jp/report/200907/0907monthly.html

4. 国際連携活動関連

4-1. 海外 CSIRT 構築支援及び運用支援活動

主にアジア太平洋地域における CSIRT に対し、イベント等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. モンゴル情報セキュリティセミナー等への参加（2009 年 9 月 9 日-11 日）

モンゴルの National CSIRT である MonCIRT の運営支援活動として、MonCIRT、モンゴル政府、財団法人国際情報化協力センター(CICC) 等と連携して、情報セキュリティセミナーを開催しました。また、MonCIRT 職員に向けて技術トレーニングを行ったり、モンゴルにおけるインターネットセキュリティ事情の把握を目的としたヒアリングを実施したりしました（トピック 1 をご参照下さい)。

4-1-2. ラオス情報セキュリティセミナー等への参加（2009 年 9 月 14 日-18 日）

ラオスの National CSIRT 構築支援活動として、ラオス政府や財団法人国際情報化協力センター (CICC) 等と連携して、情報セキュリティセミナーや、CSIRT 構築トレーニングを行いました（トピック 1 をご参照下さい)。

4-1-3. CamCERT 構築支援活動（2009 年 9 月 28 日-10 月 23 日：実施中）

カンボジアの National CSIRT である CamCERT の構築支援活動として、JPCERT/CC の職員を JICA 短期専門家としてカンボジアに派遣しています。CamCERT の運営及びカンボジア国内 IT 関連企業等との関係構築を支援し、カンボジア政府及び民間企業を対象に情報セキュリティセミナーを開催する予定です。

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及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。

4-2-1. ベトナム 2009 Guarantee Information Security for e-Gov Conference への参加（2009 年 7 月 10 日）

ベトナム情報セキュリティ協会が主催した 2009 Guarantee Information Security for e-Gov Conference に参加しました。本カンファレンスは、ベトナムにおける電子政府のセキュリティについて考えることを目的に開催され、ベトナムの政府機関、ISP、ベンダ等から約 200 名の参加者が集いました。JPCERT/CC からは、日本における電子政府の電子申請システムに係るセキュリティ事例について紹介しました。

4-2-2. インドネシア情報セキュリティセミナーへの参加（2009 年 7 月 14 日）

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、インドネシアの政府関係者、ISP 等、約 50 名の参加者に向けて、啓発活動を行いました。JPCERT/CC からは、CSIRT 活動の重要性、国内連携及び国際連携の重要性等について紹介し、政府、ISP 等の各関係者との連携の重要性について認識を共有しました。

4-2-3. ACID：ASEAN 12 カ国 CSIRT による合同サイバー演習への参加（2009 年 7 月 23 日）

ASEAN（東南アジア諸国連合）の CSIRT が実施するサイバー演習 ACID (ASEAN CERT Incident Drill) に参加しました。本演習は、国境を越えて発生するセキュリティインシデントに備えて、ASEAN 加盟国及び周辺各国の CSIRT 間の連携の強化を目的に、毎年実施されています（トピック 1 をご参照下さい）。

4-2-4. スリランカ Cyber Security Week への参加（2009 年 8 月 24 日-25 日）

スリランカの National CSIRT である SLCERT、及び Information and Communication Technology Agency of Sri Lanka (ICTA) が共催した Cyber Security Week に参加し、スリランカの政府機関、ISP、ベンダ、通信事業者、金融機関、教育機関等、約 80 名の参加者に向けて啓発活動を行いました。JPCERT/CC からは、最近のインシデント傾向やアジア太平洋地域におけるネットワークモニタリングプロジェクト、APCERT におけるアジア太平洋地域 CSIRT の連携活動について紹介し、CSIRT のインシデント対応活動に関する認知度の向上と理解を得ることができました。

4-2-5. APECTEL 40 参加（2009 年 9 月 24 日-30 日）

メキシコにて開催された APECTEL 40 (40th Meeting of the APEC Telecommunications & Information Working Group) の SPSG (Security and Prosperity Steering Group) に参加

し、JPCERT/CC は APCERT の代表参加者として、アジア太平洋地域の CSIRT における情報セキュリティ啓発活動に関する紹介を行うとともに、APEC 地域における情報セキュリティ関連活動の取り組みについて情報収集を行いました。

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 の詳細
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 の詳細
http://www.first.org/about/organization/sc.html

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. 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

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べく、JPCERT/CC と CERT/CC が共同でデザインした脆弱性対応コンセプトです。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、各組織において実施すべき脆弱性対応を、どの程度正しく提示することができるかについて、米 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。

英語版報告書の詳細
「Effectiveness of the Vulnerability Response Decision Assistance (VRDA) Framework」
https://www.jpcert.or.jp/research/2009/VRDA_Effectiveness-E_20090903.pdf

6. 講演活動一覧

(1) 真鍋 敬士(理事), Chris Horsley(早期警戒グループ 情報セキュリティアナリスト):
「Anti-bot Countermeasures in Japan」
21st FIRST Annual Conference Kyoto , 2009 年 7 月 3 日

(2) 鎌田 敬介(国際部部長代理):
「Experiences for handling security issues of e-Government systems」
ベトナム 2009 Guarantee Information Security for e-Gov Conference ,
2009 年 7 月 10 日

(3) 鎌田 敬介(国際部部長代理), 佐藤 しおり(APCERT 事務局担当):
「JPCERT/CC Activities ~International and Domestic Cooperation~」
インドネシア情報セキュリティセミナー, 2009 年 7 月 14 日

(4) 早貸 淳子(常務理事):
「いまネットの問題に地域でいかに取り組むか」
おおいたネットあんしんセミナー, 2009 年 7 月 17 日

(5) 早貸 淳子(常務理事):
「情報セキュリティ最前線～CERT って何？世界は？日本は？」
おおいたネットあんしんセミナー, 2009 年 7 月 17 日

(6) 宮地 利雄(理事):
「プロセス制御システムにおけるセキュリティ課題」
学術振興会プロセスシステム工学第 143 委員会, 2009 年 7 月 24 日

(7) 村上 晃(分析センター マネージャー):
「インシデントレスポンスから見た Malware 対策 ～もう他人ごとでは済まされない～」
ボット対策プロジェクト ISP セミナー(東京) , 2009 年 7 月 29 日

(8) 早貸 淳子(常務理事):
「最近のセキュリティ事情」
東京大学情報基盤センターセミナー, 2009 年 8 月 5 日

(9) 村上 晃(分析センター マネージャー):
「インシデントレスポンスから見た Malware 対策 ～もう他人ごとでは済まされない～」

ボット対策プロジェクト ISP セミナー(大阪) , 2009 年 8 月 6 日

(10) 宮地 利雄(理事) :

「Control System Security in the Shift to Open Systems」

ICCAS-SICE 2009, 2009 年 8 月 21 日

(11) 鎌田 敬介(国際部部長代理), 佐藤 しおり(APCERT 事務局担当) :

「Recent trend of Internet security issues from JPCERT/CC」

「Internet Traffic Monitoring Project」

「APCERT Activities」

スリランカ Cyber Security Week , 2009 年 8 月 24 日-25 日

(12) 真鍋 敬士(理事) :

「インシデント事例から考えるネットワークセキュリティ」

日経 BP 社 Security Solution 2009 , 2009 年 9 月 3 日

(13) 早貸 淳子(常務理事) :

「Information Security Measures/Governance in Japan and National CSIRT Activities」

Information Security Conference 2009 (ISEC 2009) －Seoul , 2009 年 9 月 8 日

(14) 小宮山 功一郎(早期警戒グループ 情報セキュリティアナリスト リーダ) :

「Web サイト改ざんをとりまく現状」

文部科学省 Web サイト情報セキュリティ対策説明会,2009 年 9 月 15 日

(15) 鎌田 敬介(国際部部長代理) :

「Incident Handling Cases of Japan ~JPCERT/CC experiences~」

「Fight Against Cyber Security Issues」

モンゴル情報セキュリティセミナー, 2009 年 9 月 10 日

(16) 鎌田 敬介(国際部部長代理), 佐藤 しおり(APCERT 事務局担当) :

「Basic Understanding of Information Security and Activities of JPCERT/CC」

「Activities of APCERT and Regional Cooperation」

ラオス情報セキュリティセミナー, 2009 年 9 月 14 日

(17) 伊藤 友里恵(経営企画室 兼 国際部部長)

「APCERT Updates ~Asia Pacific Computer Emergency Response Team Activities & Challenges~」

APECTEL 40 , 2009 年 9 月 29 日

7. 執筆・掲載記事一覧

(1) 中尾 真二(事業推進基盤グループ 広報) :

「FIRST Annual Conference 京都について」

Scan NetSecurity , 2009 年 7 月 1 日

(2) 中尾 真二(事業推進基盤グループ 広報) :

「次世代セキュリティ情報配信のあり方を探る－JPCERT/CC の Web サイトについて【後編】」
Scan NetSecurity , 2009 年 7 月 2 日

(3) 中尾 真二(事業推進基盤グループ 広報) :
「迅速な災害復旧のポイント : インシデント対応に求められるチーム連携、JR 西の事例に学ぶ」
IT media エンタープライズ, 2009 年 7 月 17 日
http://www.itmedia.co.jp/enterprise/articles/0907/17/news011.html

(4) 中谷 昌幸(早期警戒グループ グループマネージャ) :
「米韓のサイトを襲ったサイバー攻撃」
日経 BP 社 日経パソコン, 2009 年 8 月 24 日

(5) 久保 啓司(早期警戒グループ 情報セキュリティアナリスト) :
「即効理解 旬のファイアウォール」
日経 BP 社 日経ネットワーク 9 月号, 2009 年 8 月 28 日

(6) 鎌田 敬介(国際部部長代理) :
「特定の Web サイトが見えない」
日経 BP 社 日経ネットワーク 9 月号, 2009 年 8 月 28 日

(7) 戸田 洋三(情報流通対策グループ リードアナリスト),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」
日経 BP 社 日経ネットワーク 9 月号, 2009 年 8 月 28 日

(8) 小宮山 功一郎(早期警戒グループ 情報セキュリティアナリスト リーダ) :
「偽造・不正利用にご用心・クレジットカード 4」
朝日新聞 Be,2009 年 9 月 12 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 10 月号, 2009 年 9 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), 久保 正樹（情報流通対策グループ 脆弱性アナリスト) :
「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,2009 年 9 月 30 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/