JPCERT-PR-2009-0005

# JPCERT/CC 活動概要［2009 年 4 月 1 日 ～ 2009 年 6 月 30 日 ］

2009-07-09 発行

【活動概要トピックス】



---

## ―トピック 1 ―
## JavaScript が埋め込まれる Web サイトの改ざんの増加

昨今、Web サイトが改ざんされ、当該サイトにアクセスしたユーザが悪意ある行為を行う別のサイトに誘導されてしまうインシデントが多数発生しています。
JPCERT/CC には、今期、74 件の事例が報告されており、前四半期と比べて約 3 倍の増加となっています。JPCERT/CC では、ユーザに対して注意喚起を行うとともに、報告があった不審な JavaScript が埋め込まれているサイトの管理者に修正を依頼する連絡・調整を行っています。

一連のインシデントでは、改ざんされた Web サイトにユーザがアクセスすると、攻撃者が用意した JavaScript により別のサイトへ誘導され、Adobe Flash や Adobe Acrobat、Adobe Reader の脆弱性を使用した攻撃により、マルウエアに感染してしまう可能性があります。このマルウエアに感染するとユーザが管理するウェブサイトなどで使用される FTP アカウント情報が盗まれる場合があります。攻撃者は、盗んだアカウント情報を用いてユーザが管理している Web サイトを改ざんし、当該ユーザの Web サイトを用いてさらなる攻撃を行います。

このような攻撃については、一般的なセキュリティ対策を実施することにより、影響を受ける可能性を低減することが可能です。
日頃の対策として、使用する PC の OS やインストールされているソフトウエアに常に最新のパッチを適用するなど基本的なセキュリティ対策の徹底をお願いします。

JavaScript が埋め込まれる Web サイトの改ざんに関する注意喚起の詳細
https://www.jpcert.or.jp/at/2009/at090010.txt

―トピック 2 ―

**フィッシング対策協議会事務局運営開始**

JPCERT/CC は、経済産業省からの委託を受け、平成 21 年度のフィッシング対策協議会の事務局運営を行うこととなりました。
フィッシング対策協議会は、経済産業省の支援により、日本国内におけるフィッシング被害を抑制することを目的に、国内の金融サービス事業者やオンラインサービス事業者などを会員として 2005 年 4 月に発足した団体です。 海外、特に欧米を中心に大きな被害が発生しているフィッシング詐欺に関する事例情報、 対策技術情報の収集及び提供を主な活動としてきました。

今年度の第 1 回総会は 6 月 25 日に開催され、次の 2 点が承認されました。

(1) JPCERT/CC への事務局の移管に伴う協議会会則の変更
(2) 21 年度における活動計画の概要

本年度は、特にワーキンググループ活動を通して会員向けの情報提供に力をいれるとともに、消費者からのフィッシング報告への対応の強化や教育用コンテンツの拡充などを計画しております。JPCERT/CC では、本協議会の事務局としての活動と、以前より行っていたインシデント対応業務におけるフィッシングサイトへの対応ノウハウや諸外国の関連機関との緊密な協力関係とを両輪とした駆動力を最大限に生かし、日本国内におけるフィッシング対策を進めてまいります。

フィッシング対策協議会の活動の詳細
http://www.antiphishing.jp/

―トピック 3 ―

**IT セキュリティ予防接種、USB メモリ経由の感染機能を持つマルウエアなど 3 種類の調査・研究資料を公開**

情報セキュリティに関する脅威は、攻撃手法の多様化や複雑化に伴って変化し続けており、企業等の組織にとっては、インシデントの発生等「事故前提社会」を踏まえた対策が重要になってきています。JPCERT/CC は、次の 3 編の調査報告書を順次公開しました。

(1) 新入社員等研修向け情報セキュリティマニュアル
http://www.jpcert.or.jp/magazine/security/newcomer.html
新年度を迎え、新入社員に対する情報セキュリティ意識の教育が重要となることから、企業等における内部研修においてご参照いただくことを目的とした、新入社員等研修向け情報セキュリティ対策資料です。

(2) IT セキュリティ予防接種調査報告書

http://www.jpcert.or.jp/research/#inoculation

製造業、金融業、地方公共団体など多岐にわたる企業・組織のご協力のもと、延べ 2,600 名に対して実施した IT セキュリティ予防接種の調査報告書です。

(3) USB メモリ経由の感染機能を持つマルウエアに関する調査報告書

http://www.jpcert.or.jp/research/2009/usbmalware_20090619.pdf

可搬型記憶媒体(USB)を媒介とするマルウエアの被害実態と、その仕組みや対策についての調査報告書です。

## ―トピック 4 ―
## 「CERT C セキュアコーディングスタンダード」を公開

C 言語でセキュアコーディングを実践する上で欠かせない要素のひとつに、プログラマが理解できる言葉で記述され、開発現場で実際に適用できるコーディングスタンダード(規約)があります。コーディングスタンダードを活用することで、プログラマ個人の得意な方法や好みではなく、プロジェクトや組織の要件が定める統一的なガイドラインに従わせることができます。また、ひとたびコーディングスタンダードを確立しておけば、それを評価基準として用い、ソースコードの評価にも利用することができます。

JPCERT/CC は、CERT/CC を中心として世界中の C プログラミング・コミュニティの協力により作成された "CERT C Secure Coding Standards" を翻訳し、「CERT C セキュアコーディングスタンダード」として 2009 年 4 月 9 日に公開しました。その目的は、脆弱性につながる恐れのある危険なコーディング作法や未定義の動作を削減することです。CERT C セキュアコーディングスタンダードでは、C 言語を使ってセキュアコーディングを行うためのルール（Rule）とレコメンデーション（Recommendation）を定めています。

現在、91 個の全てルールと 64 個のレコメンデーションが公開済みです。未公開のレコメンデーションに関しては、翻訳が完了したものから順次公開を進めています。
セキュアコーディングスタンダードを採用することで、堅牢で、攻撃に耐えられる、より品質の高いシステム開発が可能になるはずです。

CERT セキュアコーディングスタンダードの詳細

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

―トピック 5 ―
**脆弱性ハンドリングガイドラインの見直し**

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、制度運用の中核を担ってきました。毎四半期に届出されるソフトウエア製品等に関する脆弱性の件数は、50 件前後と安定的に推移していますが、1 年ほど前から、届け出られた脆弱性をもつ製品の開発者と連絡が取れず、調整に着手できないケースが急増しています。

開発者と連絡が取れない場合の取扱いについて、これまでのパートナーシップガイドラインには明確な規定がなく、進捗が見込めないままに取扱いが滞留した案件数が急増していました。この問題は 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」でも議論され、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ガイドラインを改定することが了承されました。

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版の公表に合わせて、JPCERT/CC では、製品開発者が関与できる機会を十分に確保しつつ、脆弱な製品を知らないで使い続ける利用者を減らすことを目標に、JPCERT/CC ガイドラインをはじめとする、脆弱性取扱い関連のルールの見直しを進めました。改定内容は 7 月には公表し、順次、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。

―トピック 6 ―
**IWWN 国際インシデント対応机上演習への参加**

JPCERT/CC は、内閣官房情報セキュリティセンター、警察庁とともに、欧米をはじめとする 15 ヶ国の政府機関、法執行機関、CSIRT 組織で構成される IWWN (International Watch and Warning Network) に参加しています。IWWN は 2004 年に設立され、インターネットセキュリティの状況を監視し、国際的なサイバー攻撃や脆弱性対応について情報共有を行う枠組みです。

IWWN では、国境を越えて発生し、広範囲に影響が派生するインシデントに対応する国家間の情報共有及び連携の強化を目的に、2009 年 6 月、ハンガリーにおいて国際インシデント対応に関する机上演習を実施しました。具体的には、Conficker の亜種の出現による新たな脅威の発生、また某国首都圏における大規模な停電による制御系システムへの影響を想定したシナリオが用いられました。

今回の演習には、IWWN メンバの 12 ヶ国（アメリカ、イギリス、オーストラリア、オランダ、カナダ、スイス、スウェーデン、ドイツ、日本、ニュージーランド、ノルウェー、ハンガリー）が参加し、国家間及び地域間の情報共有の強化につながる成果を得ることができました。

## 【 活動概要 】

### §1.情報提供活動

JPCERT/CC のホームページ、RSS、約 24,000 件の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。

#### I. 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：5 件　https://www.jpcert.or.jp/at/

2009-06-10　2009 年 6 月 Microsoft セキュリティ情報（緊急 6 件含）に関する注意喚起（公開）
2009-05-19　JavaScript が埋め込まれる Web サイトの改ざんに関する注意喚起（公開）
2009-05-13　Adobe Reader 及び Acrobat の脆弱性に関する注意喚起（公開）
2009-05-13　2009 年 5 月 Microsoft セキュリティ情報（緊急 1 件）に関する注意喚起（公開）
2009-04-15　2009 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）

#### II. 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抜粋情報をレポートにまとめ、毎週水曜日(祝祭日を除く)に発行しました。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：11 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 60 件、「今週のひとくちメモ」のコーナーで紹介した情報は 11 件でした。

#### III. 資料公開

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。

##### (1) CERT C Secure Coding Standards 日本語版資料

JPCERT/CC は、CERT/CC を中心とする世界中の C 言語コミュニティの協力により作成されている "CERT C Secure Coding Standards" の開発に貢献し、その日本語版資料を作成し

ています。

C セキュアコーディングを実践する上で欠かせない要素のひとつに、プログラマにとって分かりやすく記述され、現場で実際に適用できるコーディング規約があげられます。コーディング規約を活用することで、プログラマは、ひとりよがりに陥ることなく、プロジェクトや組織が定めたルールやガイドラインに沿ってコーディングすることができます。こうしたスタンダードはまた、一度確立しておけばソースコードを評価するための指標として用いることもできます。

CERT C セキュアコーディングスタンダードは、C 言語を使ってセキュアコーディングを行うためのルール（Rule）とレコメンデーション（Recommendation）から構成されています。これに従うことで、脆弱性につながる恐れのある危険なコーディング作法や未定義の動作を削減することができ、より品質の高い、攻撃に耐えられる堅牢なシステムの開発が可能になるはずです。

CERT C Secure Coding Standards 日本語版資料の詳細
http://www.jpcert.or.jp/sc-rules/

### (2) C/C++セキュアコーディングセミナー講演資料

2008 年 6 月から 2009 年 3 月までの期間、「脆弱性のない安全なプログラムを開発するために～ソフトウエアの脆弱性が作りこまれる根本的な原因を学び、問題を回避する～ 」を標榜した、「C/C++ セキュアコーディングトワイライトセミナー」や「C/C++セキュアコーディングハーフディキャンプ」の無料セミナーを開催してきました。これら教育コースで使用した教材資料を、さらに多くの技術者に広くご活用いただくために、公開しました。

**「C/C++ セキュアコーディングセミナー」は、無料セミナーの他、各企業のニーズに合わせてカスタマイズした有料セミナーも行っており、合計 2200 名以上の方々に参加いただきました。参加者からは**「単なる知識習得に留まらず、セキュリティ意識の向上、セキュアな製品開発へのモチベーション向上に繋がった。」といった意見が寄せられています。今後は、これらの活動を通じて得られた開発現場での課題などを抽出するなど、引き続き、ソフトウエアのセキュリティ品質の底上げを支援するための活動に取り組んでいく予定です。

C/C++セキュアコーディングセミナー講演資料の詳細
http://www.jpcert.or.jp/research/materials.html

### (3) ～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(日本語版、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として、CERT/CC と共同でまとめた技術報告書「～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(日本語版、英語版)』」を公開しました。

ソフトウエアのデプロイメント後に脆弱性を修正しなければならなくなるリスクやコストは、ソフトウエア開発者にとっても、エンドユーザにとっても、大きな負担となってしまうため、ソフトウエア製品出荷前の脆弱性対策が重要です。昨今、セキュリティ上の欠陥の根本原因に対する理解が深まるにつれ、実装とデプロイメントのフェーズだけでなく、ソフトウエア開発ライフサイクル全般を通して、セキュリティ対策の重要性に対する理解が深まってきています。

JPCERT/CC は、CERT/CC と共同で、ソフトウエア設計工程における脆弱性低減策の一つとして、一連の「セキュアデザインパターン」を定義しました。セキュアデザインパターンとは、再利用可能な設計のひな形であり、設計工程において脆弱性に繋がる要因の数と脆弱性の影響範囲を最小限にすることをめざしています。下流工程における対策であるセキュアコーディングと同様にその適用範囲は開発される製品の種類（アプリケーションドメイン）を選ばず、かつ、開発言語への依存性も低いことから、幅広い開発プロジェクトにおける脆弱性対応関連コストの削減とリストの低減などに資する効果が期待できます。また、セキュアコーディングとの併用により、より大きな効果が期待できます。

セキュアデザインパターン(日本語版)の詳細
http://www.jpcert.or.jp/research/2009/SecureDesignPatterns-J_090630.pdf

セキュアデザインパターン(英語版)の詳細
http://www.jpcert.or.jp/research/2009/SecureDesignPatterns-E_090519.pdf

### (4) IT セキュリティ予防接種実施調査報告書

JPCERT/CC が 2006 年度および 2007 年度に行った調査から、「IT セキュリティ予防接種」は、比較的小規模な企業・組織にとって、電子メールに起因する情報セキュリティ上の脅威に対する適切な対応方法のみならず、情報セキュリティ上の脅威情報を組織内で共有する必要があるという意識を向上させる意味でも、有効な教育手法であることがわかっています。

2008 年度は、2007 年度の基本的な予防接種実施手順を踏襲しつつ、より幅広い業種と企業規

模に対象を拡大し、延べ約 2600 人に対して予防接種を実施しました。

実施の経緯および結果に加え、企業の組織形態や従業員の属性に応じた IT セキュリティ予防接種の効果を高めるための実施方法についても考察を行って、報告書にとりまとめました。

IT セキュリティ予防接種実施調査報告書 概要の詳細
http://www.jpcert.or.jp/research/2009/inoculation-summary_20090619.pdf
IT セキュリティ予防接種実施調査報告書の詳細
http://www.jpcert.or.jp/research/2009/inoculation_20090619.pdf

### (5) USB メモリ経由の感染機能を持つマルウエア調査報告書

近年、USB メモリをはじめとするリムーバブルメディアを経由して感染を広げるマルウェアが観測されるようになりました。
2008 年末頃から世界的な話題になった Downad (あるいは Conficker, Kido) と呼ばれるマルウエアも、変化の過程でリムーバブルメディアを経由して感染する能力を獲得し、さらに感染力を強めたと言われています。
このようなリムーバブルメディアを経由して感染するマルウエアを理解し、効果的な対策を実施していただけるように、マルウエアの特徴や被害実態の事例や複数のマルウエアの分析結果の紹介もまじえて調査報告書にまとめ、公開しました。

USB メモリ経由の感染機能を持つマルウエア調査報告書の詳細
http://www.jpcert.or.jp/research/2009/usbmalware_20090619.pdf

## §2. 早期警戒 ーインシデントハンドリングー

JPCERT/CC が 2009 年 4 月 1 日から 2009 年 6 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 1197 件（届出を受けたメール、FAX の延数は 1611 通 *1）、IP アドレス別の集計では 1381 アドレスでした。インシデントに関する届出、IP アドレスともに前四半期から倍増しています。これは、5 月以降、海外の協力機関から、マルウエアの設置サイトに関する届出が定常的に寄せられるようになったことや、JSRedir-R/Gumblar と呼ばれるマルウエアによる Web サイト改ざんが多数発生しているとの届出が寄せられたことに因るものです。また、フィッシングサイトについては、海外の特定のホスティング事業者が管理するサーバに設置される事例が多く発生したため、海外の CSIRT と連携し対応を行いました。

*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。

上記のうち､JPCERT/CC が国内外の関連するサイトに調査対応依頼をした件数は 402 件でした。ここでいう「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、このようなコーディネーション活動により、当該サイトにおける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

## I. 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の届出が、前四半期の 25 件から今期は 58 件に増えています。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の流通が広く行われ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います。

また、2009 年 5 月より、海外の協力機関からマルウエ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、この組織が大規模にマルウエ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 に提供してくれているものです。この届出も含め、マルウエアに関連するインシデントの IP アドレスの数は 598 件に達しました。非常に多数のサイトが関連しており、マルウエアに関する脅威が潜在化して大規模に広がっていることが推察されます。JPCERT/CC では、マルウエ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関係組織に対して通知を行っています。

さらに、Web サイトが改ざんされ、当該サイトにアクセスしたユーザが悪意ある行為を行う別のサイトに誘導されてしまうインシデントが、前四半期の 20 件から今期は 74 件に増えました。これら全てが JSRedir-R/Gumblar による Web サイト改ざんの事例でした。改ざんされた Web サイトのページには他のサイトへ誘導する難読化された JavaScript が埋め込まれています。このページを閲覧すると、閲覧したユーザのコンピュータ上で特定のソフトウエアの脆弱性が使用され、マルウエアがインストールされる可能性があります。このマルウエアは感染した PC から FTP アカウントの情報を詐取します。攻撃者は、この情報を使用してユーザが管理する Web サイトをさらなる攻撃に使用します。この攻撃のサイクルにより改ざんサイトが多数発生しました。

JPCERT/CC では、改ざんされたサイトの管理者へ通知を行うとともに、被害拡大の抑止を目的として、一般ユーザに対する注意喚起の発行を行っています。

JavaScript が埋め込まれる Web サイトの改ざんに関する注意喚起の詳細
https://www.jpcert.or.jp/at/2009/at090010.txt

なお、今回の攻撃に使われたマルウエアの設置サイトはすでに停止しています。今後、別のサーバを使用する亜種の活動も考えられますので、引き続き注意が必要です。

一般ユーザにおかれましては、OS や Web ブラウザだけでなく、PC にインストールされているすべてのソフトウエアを最新の状態に保ち、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。詳細は以下の資料をご参照ください。

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

システム管理者におかれましては、管理しているサイトが改ざんされていないか、使用しているソフトウエアなどに脆弱性がないかなどについて定期的に確認してください。

独立行政法人 情報処理推進機構
「安全なウェブサイトの作り方　改訂第 3 版」
https://www.ipa.go.jp/security/vuln/websecurity.html

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/

## §3. 早期警戒 －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。

今期は、5 件の注意喚起を発行いたしました。（注意喚起の一覧は、§ 1 をご参照ください。）

【 2009 年第 2 四半期(4-6 月)の動向について】
2009 年第 2 四半期(4-6 月)は、Web サイトが改ざんされて意図しない JavaScript を埋め込まれる事象が多く確認されました。ユーザが改ざんされた Web サイトを閲覧した場合、別の Web サイトのコンテンツがダウンロードされ、結果としてウイルスに感染する可能があります。
JPCERT/CC では以下の注意喚起を発行し、広く注意をよびかけました。

2009-05-19 JavaScript が埋め込まれる Web サイトの改ざんに関する注意喚起の詳細
http://www.jpcert.or.jp/at/2009/at090010.txt

現在確認されている悪意ある JavaScript 挿入の事例においては、1) JavaScript は難読化されており、目視では接続先が分からない 2) HTML 文書中の</head>タグと<body>タグの間、あるいは</body>タグの後に JavaScript が挿入される、などの特徴が見られます。

Web サイト管理者の方は、自サイトが改ざんの被害にあっていないか、再度確認することを推奨いたします。
エンドユーザの方は Adobe Flash や Adobe Acrobat や Adobe Reader などが最新の状態である

ことを確認してください。またブラウザにプラグインをインストールその他のプログラム(例えば Quick Time プレーヤーや Windows Media プレーヤーなど)も同様に Web ページを閲覧するだけで脆弱性を攻撃される可能性があります。併せて最新の状態であることを確認して下さい。

## §4. 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、世の中に流布す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。

### I. 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スキャンログをアクセス先ポート別に集計し、総計をセンサーの台数で割った平均値を用い作成しています。

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 4 月 1 日から 2009 年 6 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 4 月 1 日-6 月 30 日)

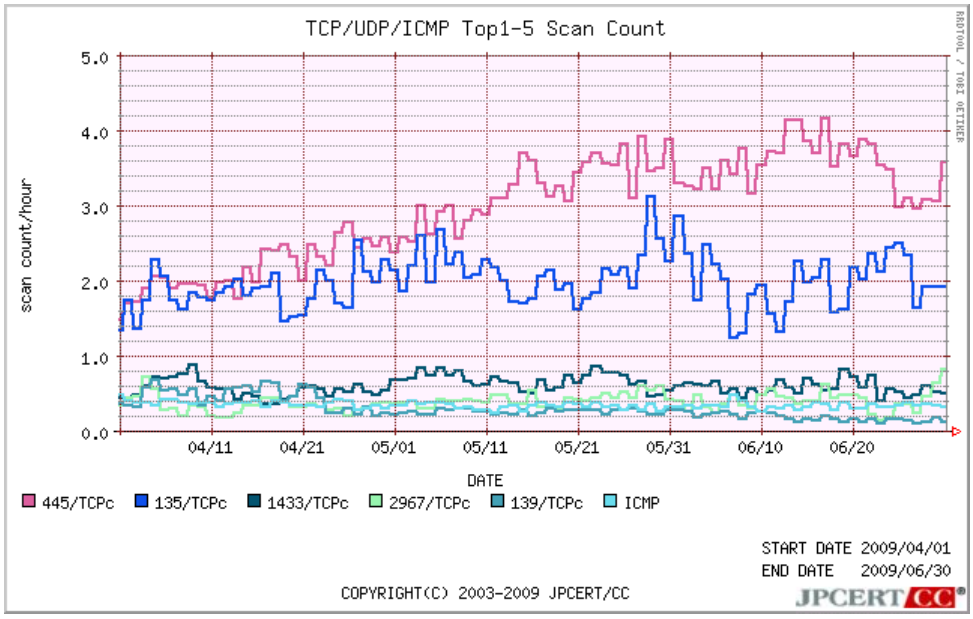


図 4-1-1: アクセス先ポート別グラフ top1-5

- アクセス先ポート別グラフ top6-10 (2009 年 4 月 1 日-6 月 30 日)

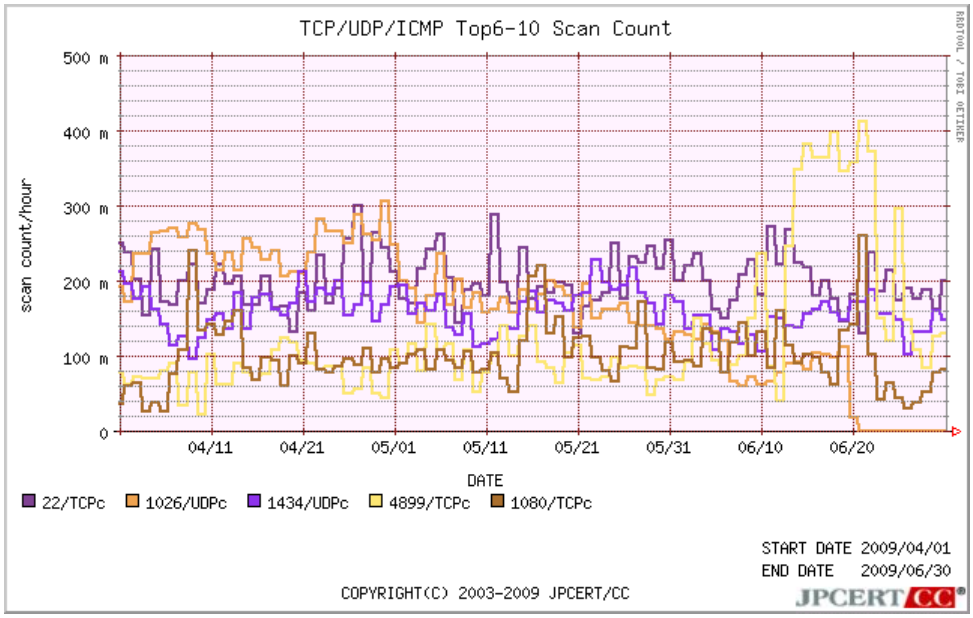


図 4-1-2: アクセス先ポート別グラフ top6-10

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 7 月 1 日から 2009 年 6 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 (2009 年 7 月 1 日-2009 年 6 月 30 日)

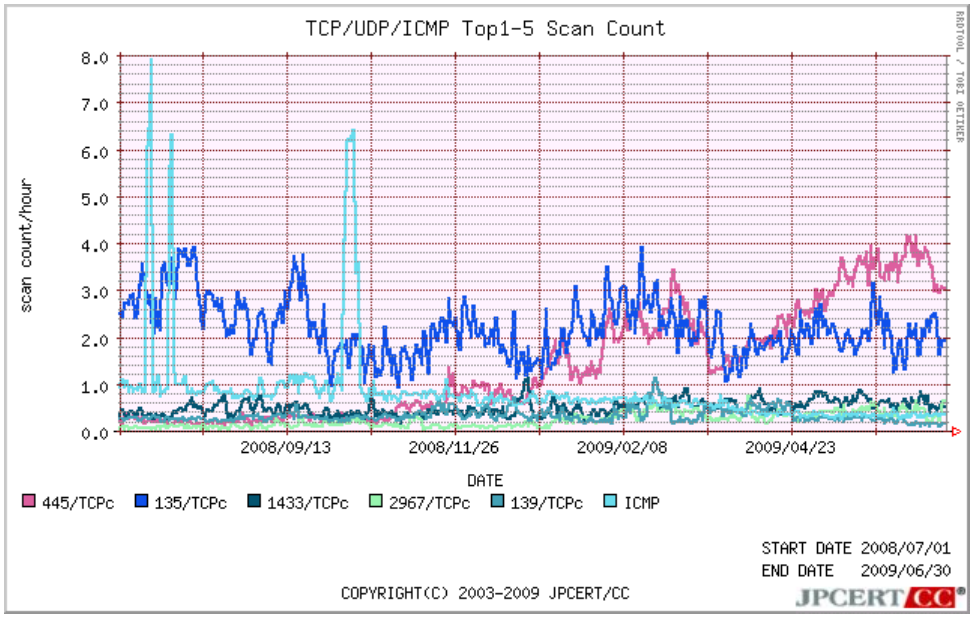


図 4-1-3: アクセス先ポート別グラフ top1-5

- アクセス先ポート別グラフ top6-10 (2008 年 7 月 1 日-2009 年 6 月 30 日)

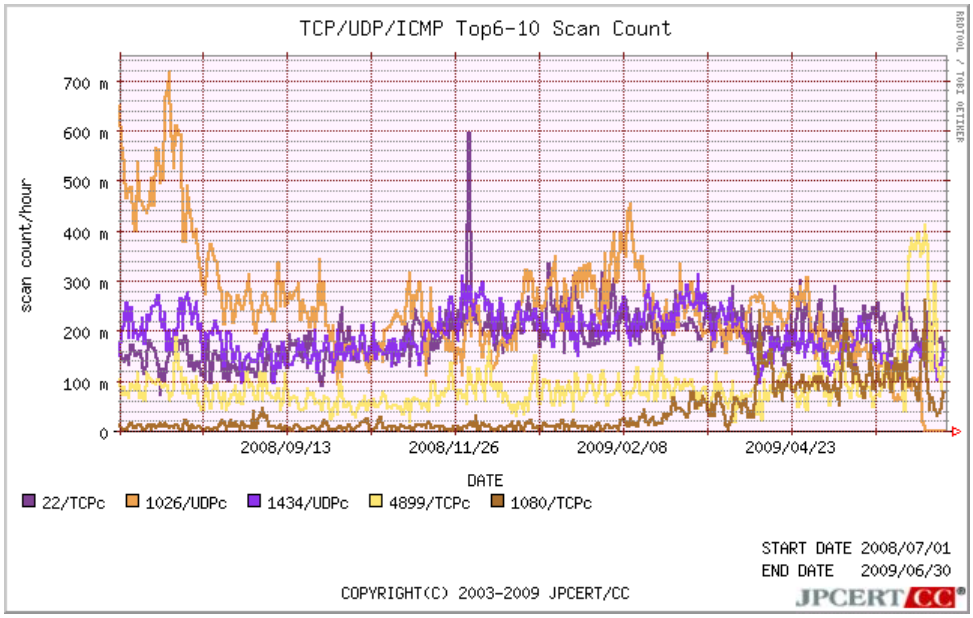


図 4-1-4: アクセス先ポート別グラフ top6-10

今期も、Windows や、同環境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 Scan 傾向の上位を占めています。特に 445/TCP 宛の Scan は、これまで 2 回の注意喚起を行いましたが、依然として増加傾向が見られます。OS や利用しているアプリケーションに脆弱性がないバージョンを使用しているか、Firewall やアンチウイルス製品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。

特に、Windows2000 の延長サポート期限まで 1 年を切りました。クライアントやサーバなどに利用しているものがある場合、セキュリティ修正プログラムが提供される環境へ、計画的に移行準備を進めましょう。

## §5. 脆弱性情報流通

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なっています。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なう調整機関として指定されています。
また、米国 CERT/CC (http://www.cert.org/ )や英国 CPNI (http://www.cpni.gov.uk/) との協力関係を結び、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。

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

2009 年 4 月 1 日から 2009 年 6 月 30 日までの間に JVN において公開した脆弱性情報および対応状況は 45 件 (総計 789 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。

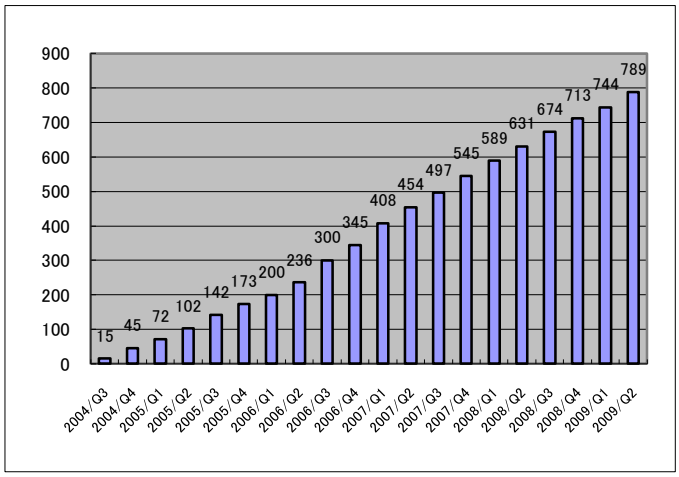


図 3-1: 累計 JVN 公表件数

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 30 件(累計 367 件) [図 3-2] でした。
今期は、公開数が 30 件と前期までの推移に比べて多く、その背景としては、同一開発者の複数製品における脆弱性の届出であったことや同一開発者製品における複数の脆弱性の届出があったことがあげられます。また、今期新たに製品開発者としてご登録いただいた開発者の脆弱性対応および公開までに要した時間が比較的短かったことも公開案件数に現れていると考えられます。

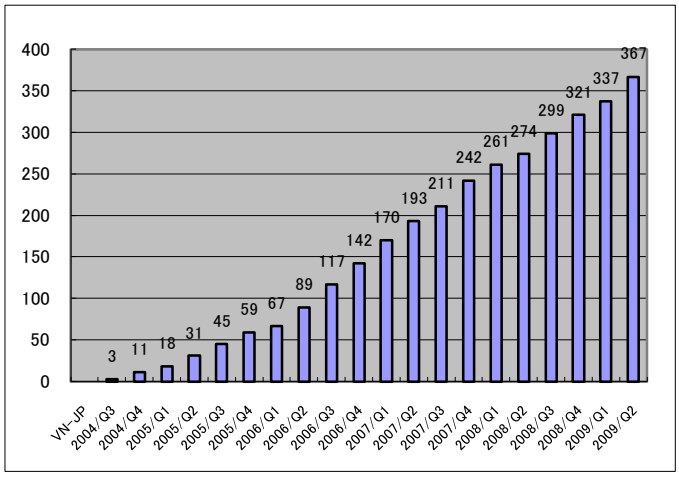


図 3-2: 累計 VN-JP 公表件数

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 15 件(累計 399 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。
この中には、画像処理における脆弱性の問題に関する対応、情報公開が 3 件含まれています。

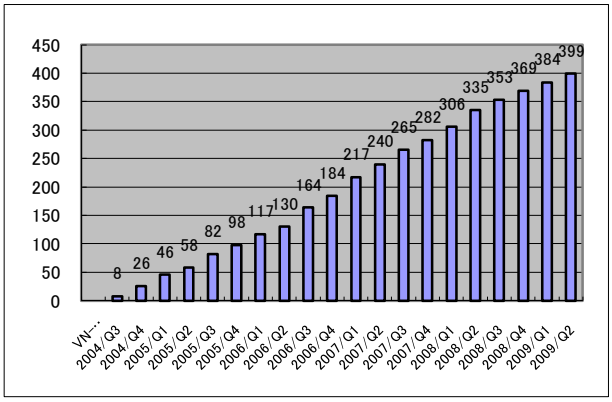


図 3-3: 累計 VN-CERT/CC 公表件数

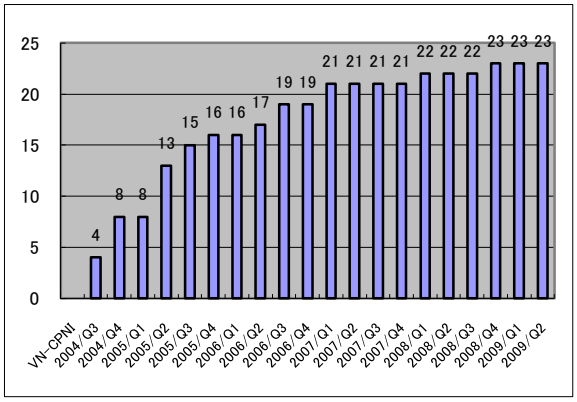


図 3-4: 累計 VN-CPNI 公表件数

**II. 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関連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、報告された脆弱性関連情報の共有、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、脆弱性関連情報の受領から公開までの情報を随時共有する枠組みを運用し、脆弱性関連情報の適正な流通のための国際連携活動を行っています。
また、脆弱性関連情報ハンドリング以外では、昨年度 JPCERT/CC において実施した「IPv6 プロトコルと IPv6 に付随したサービスに関する脆弱性の調査・研究」の資料の連携先 CSIRT 間での共有と各 CERT 経由でのベンダへの展開を実施しました。

## III. 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_guide2008.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.pdf

主な活動は以下のとおりです。

### (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ない、対策情報公開に至るまでの調整を行なっています。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 http://www.ipa.go.jp/security/vuln/ をご参照ください。

### (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 6 月 30 日現在で 302 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。

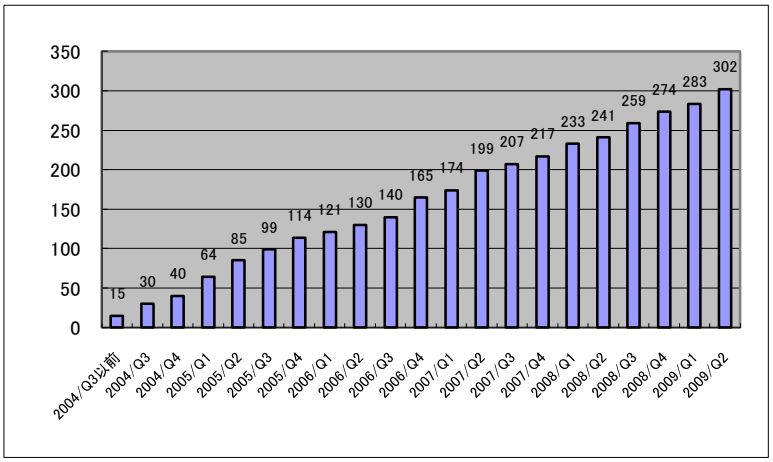


図 3-5: 累計製品開発者登録数

### (3) JPCERT/CC 脆弱性情報取扱いガイドラインの改訂

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に関する脆弱性に関し、対象製品の開発者に連絡が取れず、調整に着手できない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、このような脆弱性案件の取扱いに関する検討がおこなわれました。その結果、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」を改定することが了承されました。

これを受け JPCERT/CC では、開発者との連絡が取れず、脆弱性対応の協力が得られない等の理由により取扱いが長期化する案件への対応を含む、脆弱性取扱い関連のルールの見直しを進め、同ガイドライン改定版の公表にあわせ運用を開始できるよう準備を進めています。

具体的な運用手順等を盛り込んだ「JPCERT/CC 脆弱性情報取扱いガイドライン」の改定版は、7 月上旬に公開する予定です。この改定に基づき、JPCERT/CC は、製品開発者との連携のもと、製品利用者に向けての脆弱性情報の適切な公開が滞りなくおこなわれるよう努めて参ります。

### (4) 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 5 時間コースの個別セミナー(有償)を 1 社に対して行いました。

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ます。個別セミナーを希望される組織のご担当者様は、seminar-secure@jpcert.or.jp までご連絡ください。

### (5)「CERT/CC セキュアコーディングスタンダード」の公開

JPCERT/CC は、CERT/CC を中心とする、世界中の C 言語コミュニティの協力により作成された "CERT C Secure Coding Standards" を翻訳し、その日本語版である「CERT C セキュアコーディングスタンダード」を 2009 年 4 月 9 日に公開しました。

英語版の 91 個のルールと 150 個のレコメンデーションのうち、現在 91 個の全てのルールと 64 個のレコメンデーションを翻訳し、日本語版として公開しています。未翻訳の 90 あまりのレコメンデーションに関しては、翻訳が完了したものから順次公開を進めています。

C セキュアコーディングを実践する上で欠かせない要素のひとつに、プログラマにとって分かりやすく記述され、現場で実際に適用できるコーディング規約があげられます。コーディング規約を活用することで、プログラマは、ひとりよがりに陥ることなく、プロジェクトや組織が定めたルールやガイドラインに沿ってコーディングすることができます。こうしたスタンダードはまた、一度確立しておけばソースコードを評価するための指標として用いることもできます。

CERT C セキュアコーディングスタンダードは、C 言語を使ってセキュアコーディングを行うためのルール（Rule）とレコメンデーション（Recommendation）から構成されています。これに従うことで、脆弱性につながる恐れのある危険なコーディング作法や未定義の動作を削減することができ、より品質の高い、攻撃に耐えられる堅牢なシステムの開発が可能になるはずです。

### (6) 制御システムセキュリティにおける啓発活動

2009 年 6 月 5 日午後に開催された製造業 XML フォーラム 2009 において、「情報通信技術セキュリティの技術史と制御システムの課題」の基調講演と、「ユーザが求めるセキュリティ体制について＜調査結果＞」の講演を行いました。

### (7)「責任ある脆弱性情報開示」の国際標準化活動への参加

JPCERT/CC は、5 月 4 日～5 月 8 日に北京友誼賓館で開催された ISO/IEC JTC1/SC27 北京会議に IPA とともに日本からの代表として出席し、情報規格調査会を通じて日本からのコメントとして 19 件の検討草案に対する修正意見を提出しました。

「責任ある脆弱性情報開示」については、2008 年末にエディタから参加各国に配付されていた第 2 次検討草案に対して提出された合計 200 件近いコメントについて、カナダと米国、英国、フィンランド、日本、中国の 6 カ国からの代表が参加した作業グループにおいて、取扱いが議論されました。

SC27 WG3 の計画では、今秋に予定されている SC27 Redmond 会議に向けて，第 3 次検討草案を用意し、同会議での議論の推移によっては、来春には標準候補草案とすることになっています。JPCERT/CC は、今後も継続的にフォローアップを行う予定です。

## §6. 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。

### I. 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 04 月度 サイバークリーンセンター活動実績
https://www.ccc.go.jp/report/200904/0904monthly.html

## §7. 国際連携活動関連

### I. 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における CSIRT に対し、設立・運用支援活動、イベント等での講演、トレーニング等を行い、各国とのインシデント対応に関する連携強化を図っています。

### (1) CamCERT 構築支援活動（2009 年 4 月 20 日-5 月 8 日）

カンボジアのナショナル 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ました。
カンボジア国内 IT 関連企業等と CamCERT との関係構築を支援し、カンボジア政府および民間企業を対象にワークショップを開催しました。

### (2) ラオスにおける情報セキュリティセミナー 参加（2009 年 6 月 15 日-19 日）

ラオスのナショナル CSIRT 構築支援活動として、財団法人国際情報化協力センターおよびタイのナショナル CSIRT である ThaiCERT と連携してラオス政府組織である National Authority for Science and Technology (NAST) を訪問しました。

ラオス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するとともに、情報セキュリティセミナーの開催や技術トレーニングの実施などの CSIRT の活動の概要を説明し、ナショナル CSIRT 構築の必要性を訴えました。

## II. 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。

### (1) APECTEL 39 参加（2009 年 4 月 16 日-18 日）

シンガポールにて開催された APECTEL 39 の SPSG (Security and Prosperity Steering Group) に参加し、APEC 地域における情報セキュリティ関連活動の取り組みの実施状況について情報収集を行いました。
JPCERT/CC からはアジア太平洋地域におけるリアルタイム情報連携・可視化のプロジェクトに関する紹介を行いました。

### (2) JTC 1/SC 27 Plenary and WG meetings in Beijing, P. R. China 参加（2009 年 5 月 3 日-8 日）

中国の北京にて開催された標準化の検討のための国際会議に参加し、責任ある脆弱性情報開示、および情報セキュリティインシデントマネジメントに関する標準化の議論に参加しました。

### (3) 2009 APISC Security Training Course 参加（2009 年 5 月 11-15 日）

韓国のソウルにて開催された 2009 APISC Security Training Course に参加し、アジア太平

洋地域を中心とした経済地域におけるインターネットセキュリティへの取り組み状況等について情報収集を行い、アジア太平洋地域における CSIRT 構築支援、および JPCERT/CC とのインシデント対応等の連携強化について議論を行いました。
さらに、新たな地域との関係を構築しました。

### (4) AusCERT Conference 2009 参加（2009 年 5 月 18 日-22 日）

オーストラリアのブリスベンで開催された AusCERT Conference 2009 に参加し、昨今のセキュリティ脅威に関する情報を収集すると共に、アジア太平洋地域のナショナル CSIRT、関連組織、セキュリティ専門家との関係性強化を図り、JPCERT/CC の活動やインシデントハンドリングツールについて共有しました。

### (5) IWWN 国際インシデント対応机上演習への参加（2009 年 6 月 11 日-12 日）

ハンガリーのブダペストにて開催された、IWWN の国際インシデント対応机上演習に参加し、国境を跨ぐ攻撃に対する迅速な情報共有と連携の向上を目的とする机上演習に参加しました（トピック 6 参照)。

## III. APCERT 事務局運営　http://www.jpcert.or.jp/english/apcert/

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 Rsponse Team) の事務局を担当しています。

2009 年 6 月 18 日　インドネシアの CSIRT である ID-SIRTII が APCERT General Member として加盟し、参加 CSIRT が合計 23 組織になりました。

## IV. FIRST Steering Committee への参画　http://www.first.org/about/organizations/sc/html

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。

## V．第 21 回 FIRST Conference 京都

第 21 回 FIRST Annual Conference 2009 (FIRST 年次会合)が、日本ではじめて京都において開催されました。JPCERT/CC は、当センター理事で、内閣官房情報セキュリティセンター情報セキュリティ補佐官でもある山口英氏を委員長とする、「国内開催委員会」を発足させ、開催国のローカルホストとして、国内の他の FIRST メンバや関係機関の協力を得ながら、開催支援を行いました。

今回のカンファレンスは、「余波：インシデント復旧の技術と教訓」をテーマに、世界の 43 の国と経済地域から集結する 400 名の専門家やセキュリティ対応チームが、災害復旧から学ぶインシデント対応などについて議論を深めました。
基調講演では、JR 西日本 代表取締役副社長兼執行役員 佐々木隆之氏に、阪神・淡路大震災（1995 年）の復興、震災が鉄道システムに与えた影響と復旧作業、そこで得た教訓をどのように対策に反映したかについてお話しいただいたほか、山口英氏や、ブルース・シュナイヤー氏といった、著名なセキュリティ専門家による基調講演も行われました。
各セッションは、技術、管理、インシデント対応の 3 つのトラックに分けられ、企業や政府機関の専門家による講演が、合計で 50 以上開催されました。エンジニア、セキュリティ担当者、研究者、経営者等の様々な視点からなされた講演内容は、有害サイトからマルウエアの動向、攻撃者の手口、ネットワーク監視の方法、リスクマネジメント、インシデント対応のベストプラクティスにまで及ぶ幅広いもので、世界各地域のサイバーインシデントや脅威、対策の傾向を日本国内において把握し、各国のインシデント対応関係者とのネットワークを構築することのできる絶好の機会となりました。

詳細：http://www.first.org/

## §8. 講演活動一覧

(1) 国際部　部長代理　鎌田　敬介
「Network Monitoring Cooperation and Visualization」
APEC-TEL 39 –Singapore / 2009 年 4 月 17 日

(2) 経営企画室 兼 国際部 部長 伊藤友里恵
「国内外の最新インシデント状況とその対策 ～ CSIRT の活動と国際連携～」
日経 BP セキュリティ・ソリューションフォーラム 2009 春/2009 年 4 月 23 日

(3) 国際部　部長代理　鎌田　敬介
「Experiences of Incident Handling - JPCERT/CC Cases -」
Incident Handling Mechanism –Cambodia/ 2009 年 5 月 6 日

(4) 早期警戒グループ 情報セキュリティアナリスト 小宮山 功一朗
「*Social Engineering Mail Drill*」
APWG CeCOS III/2009 年 5 月 12 日

(5) 早期警戒グループ　情報セキュリティアナリスト　Chris Horsley
「JPCERT/CC　Activity Update」
AusCERT Conference National CSIRT Meeting / 2009 年 5 月 22 日

(6) 理事　宮地利雄
「情報通信技術セキュリティの技術史と制御システムの課題」
製造業 XML フォーラム 2009 / 2009 年 6 月 5 日

(7) 情報流通対策グループマネージャ　古田洋久

「ユーザが求めるセキュリティ体制について＜調査結果＞」
製造業 XML フォーラム 2009 / 2009 年 6 月 5 日

(8) 早期警戒グループ 情報セキュリティアナリスト 小宮山 功一朗
「新たなソーシャルエンジニアリング、求められる新たなセキュリティ対策」
RSA CONFERENCE JAPAN 2009 /2009 年 6 月 10 日

(9) 理事　水越　一郎
パネル「IPv6 によってセキュリティはどう変化するか？」
RSA CONFERENCE JAPAN 2009 /2009 年 6 月 10 日

(10) 代表理事　歌代　和正
パネル「セキュアデベロップメントの現場を語る」
RSA CONFERENCE JAPAN 2009 /2009 年 6 月 10 日

(11) 国際部　部長代理　鎌田　敬介
「Introduction of JPCERT/CC activity and International Cooperation」
Seminar for Information Security –Laos/ 2009 年 6 月 18 日

(12) 国際部　部長代理　鎌田　敬介
「Network Monitoring, Incident Trend」
Technical training–Laos / 2009 年 6 月 18 日

(13) 理事　真鍋　敬士
「マルウエアに見る脅威の変遷」
エフセキュア株式会社 / 2009 年 6 月 24 日

## §9. 執筆・掲載記事一覧

(1) 早期警戒グループ グループマネージャ 中谷昌幸
JPCERT/CC 専門委員　名和　利男
「スタート！CSIRT 第 8 回 具体的なシナリオへのインシデント対応でスキル評価」
日経 BP 社 ITpro / 2009 年 4 月 24 日
http://itpro.nikkeibp.co.jp/article/COLUMN/20090421/328821/?ST=security

(2) 事業推進基盤グループ　広報　中尾真二
「インシデント対応チームの国際連携：CSIRT ネットワークの構築を担う FIRST とは？」
IT media エンタープライズ /2009 年 5 月 27 日
http://www.itmedia.co.jp/enterprise/articles/0905/27/news005.html

(3) 早期警戒グループ グループマネージャ 中谷昌幸
「悪化するウイルス」基本対策徹底を
朝日新聞朝刊 / 2009 年 5 月 29 日

(4) 事業推進基盤グループ　広報　中尾真二
「インシデント対応チームの国際連携：セキュリティ対策のネットワークインフラとなる FIRST」

IT media エンタープライズ /2009 年 6 月 3 日

http://www.itmedia.co.jp/enterprise/articles/0906/03/news009.html

(5) 理事　宮地　利雄

「セキュリティ技術史から浮かび上がる制御システムの課題」

月刊 IPG / 2009 年 6 月 27 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 ：
168C 2587 14DF E2BA 73D9 9B0C EB27 7FB5 3205 36EC

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