JPCERT-PR-2008-0006

JPCERT/CC 活動概要 [2008 年 7 月 1 日 ～ 2008 年 9 月 30 日]

2008-10-09 発行

【 活動概要トピックス 】

― トピック 1 ― SQL インジェクション

前四半期と同様 SQL インジェクションによる Web サイト改ざんのインシデントが発生しており、「多数の国から SQL インジェクション攻撃を受けている 」とする攻撃元に関する情報の届出もありました。JPCERT/CC では、SQL インジェクションを行っている IP アドレスの管理者に対し、攻撃の停止を目的とする調査対応依頼を行っています。

また、SQL インジェクション攻撃により改ざんされた Web サイトの管理者に対する調査対応依頼や、改ざんされた Web サイトから誘導される先の Web サイトの管理者に対する「マルウエア配布の停止等」を目的とする調査対応依頼も行っています。

さらに、10 月に入り、新しい手法による SQL インジェクション攻撃に関する届出を受けています。SQL インジェクション攻撃は、依然として継続していますのでご注意ください。

― トピック 2 ― 複数の DNS サーバ製品におけるキャッシュポイズニングの脆弱性

JPCERT/CC では、2008 年 7 月に一般公開された、複数の DNS サーバ製品におけるキャッシュポイズニングの脆弱性に関し、さまざまな活動を行いました。当該脆弱性情報に関する国内関係組織への事前情報提供を行ったほか、注意喚起文書の発行、早期警戒情報の発行、国内関係組織との技術情報の共有などを行いました。さらに、海外関連機関から提供された情報に基づき、当該 脆弱性の影響を受ける可能性ある国内 DNS サーバについて、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)、株式会社日本レジストリサービス(JPRS)と共同で、個別に注意喚起を行いました。なお、本件については、海外では被害事例 が報告されていること、この攻撃が成功すると DNS キャッシュサーバのユーザが悪意のあるサイトに誘導されウイルスに感染する可能性があることなどから、可能な限り早急な対策が必要です。

― トピック 3 ― IT Keys「リスクマネージメント演習」講義実施

「IT Keys」は、文部科学省の「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」の一つとして実施されているプロジェクトです。このプロジェクトにおいて開講される「リスクマネージメント演習」は、ボット対策（サイバークリーンセンター）プロジェクトで行なわれる実習科目であり、JPCERT/CC はボット対策プロジェクトの一員として講義の一部を担当し、ボット分析業務の手法と教材検体を用いた解析演習を行いました。

IT Keys　情報セキュリティ運用リテラシー
http://it-keys.naist.jp/course/advance/literacy.html

JPCERT/CC では、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は欠かせないものであるととらえており、来年度にむけて、教材や講義方法の見直しをさらに進めて行きたいと考えています。

― トピック 4 ―　ボット対策事業に関する平成 19 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 19 年度の活動内容をまとめた「平成 19 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。

平成 19 年度サイバークリーンセンター活動報告
https://www.ccc.go.jp/report/h19ccc_report.pdf

― トピック 5 ―　プロセス監視・制御系システム、SCADA セキュリティに関する情報専用 Web ページを新たに開設

制御系システムは、製造業を含むさまざまな産業領域で利用されている他、大規模な石油化学プラントの制御や、電力システムの監視制御、 ダムや水供給システムの監視制御など国民生活の基盤サービスを提供する重要なシステムに利用されています。その一方で制御系システムに関するソフトウエアに脆弱性が発見されるという事案も散見され始めています。このような状況に鑑み、JPCERT/CC は、国内外のプロセス監視・制御系システムセキュリティのコミュニティにとって有益な情報を集約・提供する目的で、「プロセス監視・制御系システム、SCADA セキュリティ」に関する情報の専用 Web ページを開設しました。

公開内容は、次のとおりです。

・開発者、研究者との情報共有タスクフォース（準備中）
・脆弱性情報の通知、対策調整 脆弱性情報の情報公開 制御系プロトコルに関する脆弱性調査
・プロセス監視・制御系システムセキュリティに関する各種情報収集
・プロセス監視・制御系システム運用者への早期警戒情報発信（準備中）

詳しくは、以下 URL をご参照ください。
http://www.jpcert.or.jp/ics/

【 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で情報提供をしています。

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ています。

発行件数：9 件　http://www.jpcert.or.jp/at/

2008-09-10　2008 年 9 月 Microsoft セキュリティ情報（緊急 4 件含）に関する注意喚起(公開)
2008-08-13　2008 年 8 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)
2008-07-31　[続報] 複数の DNS サーバ製品におけるキャッシュポイズニングの脆弱性（更新)
2008-07-25　複数の DNS サーバ製品におけるキャッシュポイズニングの脆弱性（更新)
2008-07-24　[続報] 複数の DNS サーバ製品におけるキャッシュポイズニングの脆弱性に関する注意喚起（公開）
2008-07-23　複数の DNS サーバ製品におけるキャッシュポイズニングの脆弱性（更新）
2008-07-11　複数の DNS サーバ製品におけるキャッシュポイズニングの脆弱性（更新）
2008-07-09　複数の DNS サーバ製品におけるキャッシュポイズニングの脆弱性（更新）
2008-07-09　複数の DNS サーバ製品におけるキャッシュポイズニングの脆弱性（公開）

II. JPCERT/CC レポート

JPCERT/CC が得たセキュリティ関連情報から重要と判断した抜粋情報で、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、セキュリティに関する豆知識情報も提供しています。

発行件数：13 件　http://www.jpcert.or.jp/wr/

JPCERT/CC レポート内で扱ったセキュリティ関連情報の項目数は合計して 61 件、「今週のひとくちメモ」のコーナーで紹介した情報は 13 件です。

III. 資料公開

各分野のセキュリティに関する調査・研究の報告書や論文、セミナー資料を提供しています。

(1) ソースコード解析ツールを活用した CERT セキュアコーディングルールの有効性評価 報告書 日本語版

市場に出荷された多くのソフトウエア製品に発見される脆弱性は、プログラミングエラーによっ

て引き起こされています。 製品出荷後に発見される脆弱性を修正するには、場合によっては、ソフトウエアのデザイン(設計)の見直し、大規模な再コーディング、再テストが必要になる上、修正プログラムの開発・周知および配付のためのコストがかかることとなります。さらに、利用者側においても、修正プログラムの適用のためのリスクと、コストがかかることになります。
このような問題を回避するためには、製品開発工程において、脆弱性の発生につながるような欠陥を作りこまないこと、仮に作りこまれたとしても出荷前の検証等の段階で発見して対応が行われること等が有効な対策となり得ると考えられます。そのための対策のひとつとして、「C/C++ セキュアコーディングスタンダード」というルールセットが開発されています。
CERT/CC と JPCERT コーディネーションセンターは、共同で、ソフトウエアの品質確認において、このルールセットの一部を実装した「ソースコード解析ツール」を実験的に利用することにより 、「C/C++ セキュアコーディングスタンダード」の有効性と、このルールセットへの適合状況を機械的に効率よく検出することが可能であるか(実用性)を評価するプロジェクトを実施し、その成果を報告書にまとめて公開しました。

・ソースコード解析ツールを活用した CERT セキュアコーディングルールの有効性評価 (PDF:853KB) (PGP 署名)

(2) プロセス監視・制御系システム、SCADA セキュリティに関する情報専用 Web ページを開設し情報を提供

制御系システムは、製造業を含むさまざまな産業領域で利用されている他、大規模な石油化学プラントの制御や、電力システムの監視制御、 ダムや水供給システムの監視制御など国民生活の基盤サービスを提供する重要なシステムとして利用されています。その一方で、制御系システムに関連するソフトウエアに脆弱性が発見されるという事案も散見され始めています。
JPCERT/CC では、脆弱性関連情報調整機関として、プロセス監視・制御系システムにおける開発者、研究者との情報共有タスクフォース、脆弱性情報の通知・対策調整 、脆弱性情報の情報公開 制御系プロトコルに関する脆弱性調査、プロセス監視・制御系システムセキュリティに関する各種情報収集 、プロセス監視・制御系システム運用者への早期警戒情報発信を実施しています。
また、JPCERT/CC では、国内外のプロセス監視・制御系システムセキュリティのコミュニティにとって有益な情報を集約・提供する目的で、「プロセス監視・制御系システム、SCADA セキュリティ」に関する情報の専用 Web ページを開設しました。

・http://www.jpcert.or.jp/ics/

§2. 早期警戒 ーインシデントハンドリングー

JPCERT/CC が 2008 年 7 月 1 日から 2008 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）に関する届出は 1348 件です。実際に届出を受けたメール及び FAX の数は、延べ 1786 通（*1）で、インシデントの件数を IP アドレス別に集計すると 1493 アドレスです。

*1:同一サイトのインシデント情報が異なる届出者の方から届けられるため、届出件数とメール及び FAX の数が異なっています。

上記の届出のうち、JPCERT/CC が国内外の関連するサイトに通知・連絡を行った件数は 444 件です。この通知・連絡は、連絡の仲介依頼を含むインシデントの届出に基づいて、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 や iframe のスクリプトタグ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、マルウエアに感染した後に別のマルウエアを取得する為にアクセスする先のサイト、「scan」のアクセス元等の管理者及び関係協力組織に対し、調査対応依頼を行ったものです。

I.分析

前四半期に引き続き、断続的に SQL インジェクション攻撃に関連するインシデントの届出がありました。
JPCERT/CC では、SQL インジェクションを行っている IP アドレスの管理者に対し、攻撃の停止を目的とする調査対応依頼を行っています。
また、SQL インジェクション攻撃により改ざんされた Web サイトの管理者に対する調査・対応依頼や、改ざんされた Web サイトから誘導される先の Web サイトの管理者に対する「マルウエア配布の停止等」を目的とする調査対応依頼も行っています。
サイトの管理者におかれては、今一度、SQL インジェクション攻撃への対策状況を確認されるよう推奨します。

最近、徐々に、国内のサイトを装ったフィッシングサイトの届出が増えつつあります。今後もさらに国内サイトのフィッシングサイトが増えることが懸念されますので、オンラインサービスを利用する際は、個人情報を入力する前に、入力するサイトが正規のサイトであるかを確認することを推奨します。

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 インシデントレスポンス業務報告」をご参照ください。

http://www.jpcert.or.jp/pr/2008/IR_Report1009.pdf

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については、以下の URL をご参照ください。

http://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（場合によっては、脆弱性、ウイルスの検証などもあわせて行います。）し、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。

I. 2008 年 Q3(7-9 月)の動向について

2008 年 Q3(7-9 月)は、DNS キャッシュポイズニングに関する脆弱性が公開され、大きな話題を呼びました。本脆弱性の影響範囲は広く、多くのインターネット上に存在するシステムが影響を受けます。このため、DNS を運用しているシステム管理者は、管理しているシステムに対する影響の有無を確認し、早急に対策を検討する必要があります。

また、セキュリティ対策ソフト等を装って、ユーザにマルウエアをインストールさせようとする攻撃も増えており、そのような不審なソフトウエアのインストールを促すメールや Web サイトには十分注意してください。

II.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) 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。

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、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て作成しています。

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

2008 年 7 月 1 日から 2008 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 2-1、2-2 に示します。

- アクセス先ポート別グラフ **top1-5 (2008 年 7 月 1 日-9 月 30 日)**

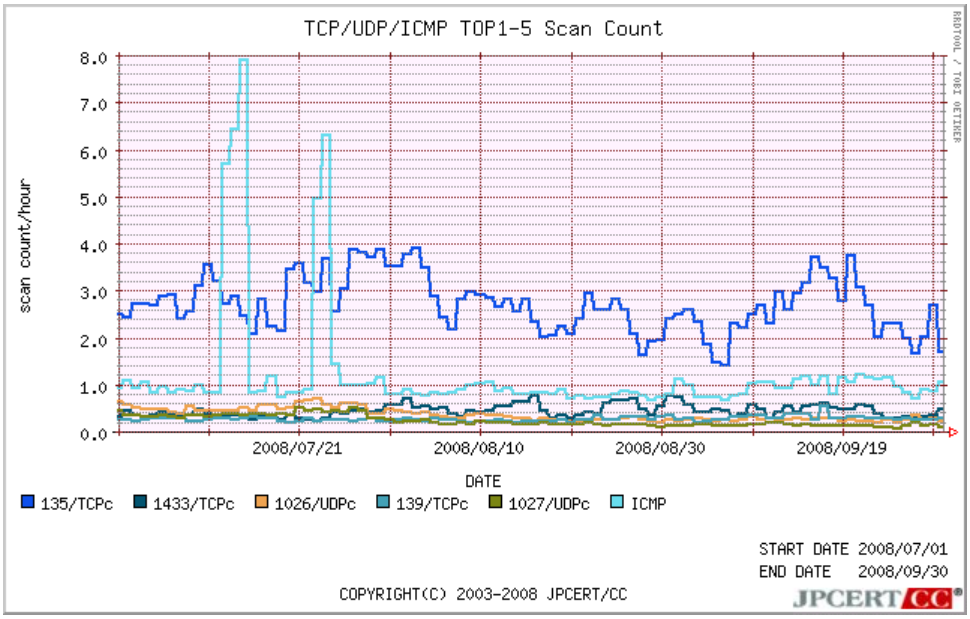

図 2-1: アクセス先ポート別グラフ top1-5

- アクセス先ポート別グラフ **top6-10 (2008 年 7 月 1 日-9 月 30 日)**

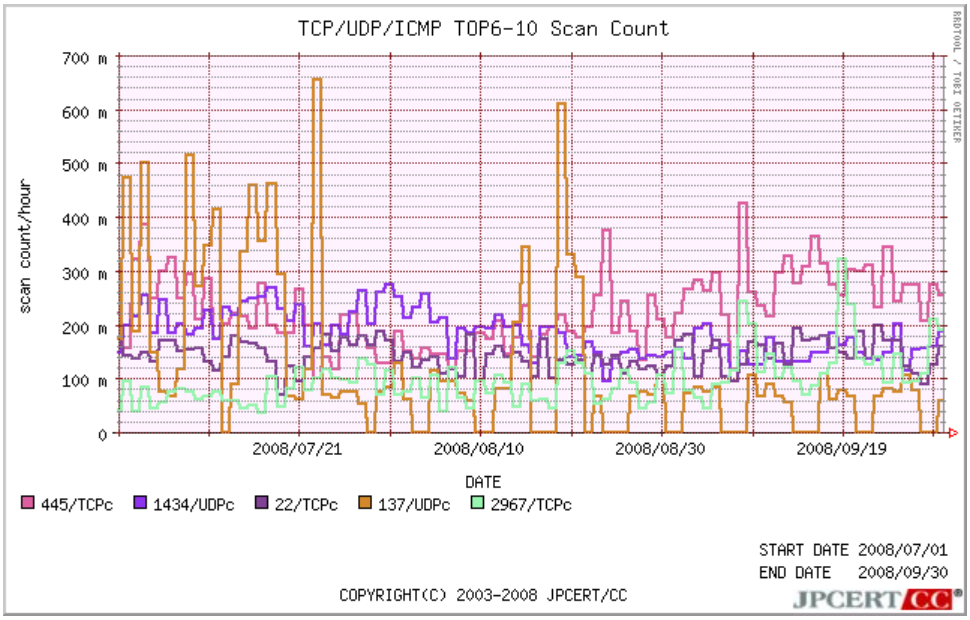

図 2-2: アクセス先ポート別グラフ top6-10

また、より長期間のスキャン推移を表すグラフとして、2007 年 10 月 1 日から 2008 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 (2007 年 10 月 1 日-2008 年 9 月 30 日)**

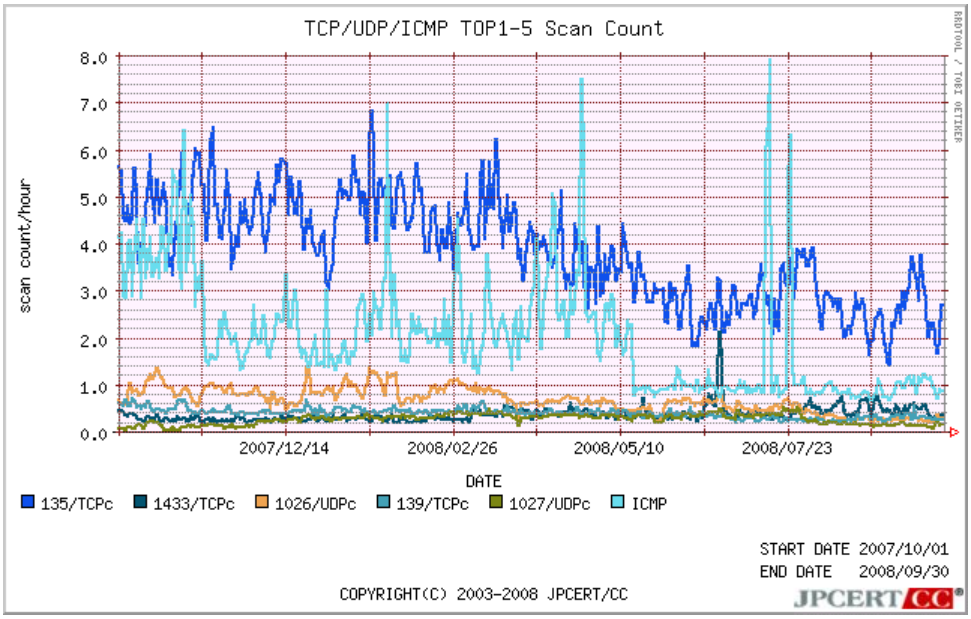

図 2-3: アクセス先ポート別グラフ top1-5

- アクセス先ポート別グラフ **top6-10 (2007 年 10 月 1 日-2008 年 9 月 30 日)**

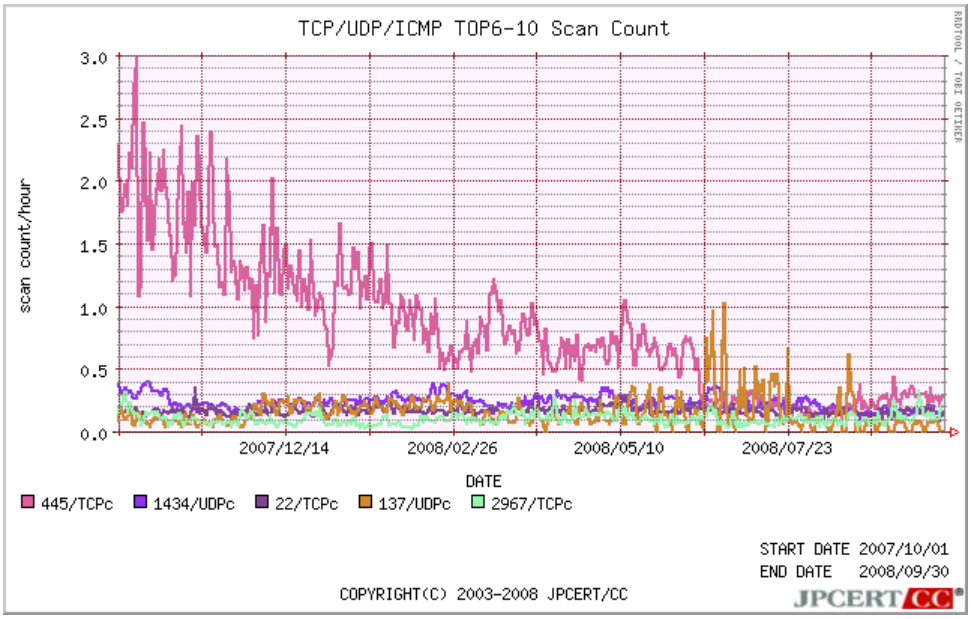

図 2-4: アクセス先ポート別グラフ top6-10

引き続き Scan 数は減少傾向が見られますが、Windows 環境を対象としたものが Scan の上位を占めています。OS や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 ・アンチウイルスなどの製品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。

III.調査

1. 標的型攻撃対策調査(平成 19 年度)

JPCERT/CC では、企業、組織に対するヒアリングにより標的型攻撃の動向を調査し、それに適した標的型攻撃対策のあり方を検討しました。特に「IT セキュリティ予防接種」という、疑似標的型攻撃を組織に対して行う手法で社員などのセキュリティ意識を向上し、教育効果を引き上げるというアプローチに着目しました。平成 19 年度は、5 社の企業に協力をいただき、延べ 100 人以上に IT セキュリティ予防接種を行い、対策の利点を確認いたしました。本調査の報告書は、平成 20 年 8 月に公開いたしました。

標的型攻撃対策手法に関する調査報告書
http://www.jpcert.or.jp/research/#targeted2

2. 効果的な IT セキュリティ予防接種手法の調査(平成 20 年度)

JPCERT/CC では、平成 19 年度の調査を基に、より大規模に IT セキュリティ予防接種を実施し、その効果を測定する調査を行っています。現在は、数社の企業に協力いただき、実際に各社の従業員殿に対して IT セキュリティ予防接種を実施し、IT 予防接種の運用手法の検証を進めています。

3.IPv6 脆弱性に関する調査

JPCERT/CC では、平成 19 年度において、IPv6 プロトコルと IPv6 を使用したサービスに関し、実際にユーザが利用する上でセキュリティ上問題となる事項がないか調査を行いました。この調査結果より、IPv6 に関する複数のセキュリティ上の問題点が見つかりました。
JPCERT/CC では、現在、これらの問題について、外部有識者を交えた委員会を設置し、対策の検討を行っています。今後、IPv6 製品を開発する企業に対し、問題点と対策(案)についての情報共有を行い、IPv6 の脆弱性をねらった攻撃の未然防止を目指していきます。

§4. 早期警戒－CSIRT 構築支援活動関連－

国内の組織・団体・企業などに対し、サイバー演習の実施支援等を通じた CSIRT 構築支援及び脅威情報（早期警戒情報など）の共有等のコミュニケーション活動を行っています。

I. 国内 CSIRT 構築支援活動

CSIRT あるいはその機能の構築を検討している企業、組織及び団体に対し、調査、構築支援、機能強化を目的に、CSIRT マテリアル等の資料提供、訪問による打ち合わせ、講師依頼対応などの支援活動を行いました。

特に、今期は、組織等において実施されたサイバー演習の実施支援を通じて、CSIRT 機能として必要な既存のインシデントレスポンス能力等の検証及び改善活動に関わるなど、より具体的な施策に関与させていただく形で構築支援を行いました。

II. 日本シーサート協議会への参画

日本国内の CSIRT の集まりである日本コンピュータセキュリティインシデント対応チーム協議会(日本シーサート協議会：NCA)に、JPCERT/CC の職員が運営委員会のメンバとして参画するとともに、同協議会の事務局を担当しています。

(1)2008 年 8 月 22 日　日本シーサート協議会　総会及び年次会合

東京で開催された日本シーサート協議会総会及び年次会合において、事務局を担当するとともに、日本シーサート協議会に参加している各国内 CSIRT メンバと意見交換を行い、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。

日本シーサート協議会の詳細： http://www.nca.gr.jp/

§5. 脆弱性情報流通

JPCERT/CC では、脆弱性関連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関連情報取扱基準」(以下「本基準」といいます。)により、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関連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

2008 年 7 月 1 日から 2008 年 9 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 43 件 (総計 674 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。

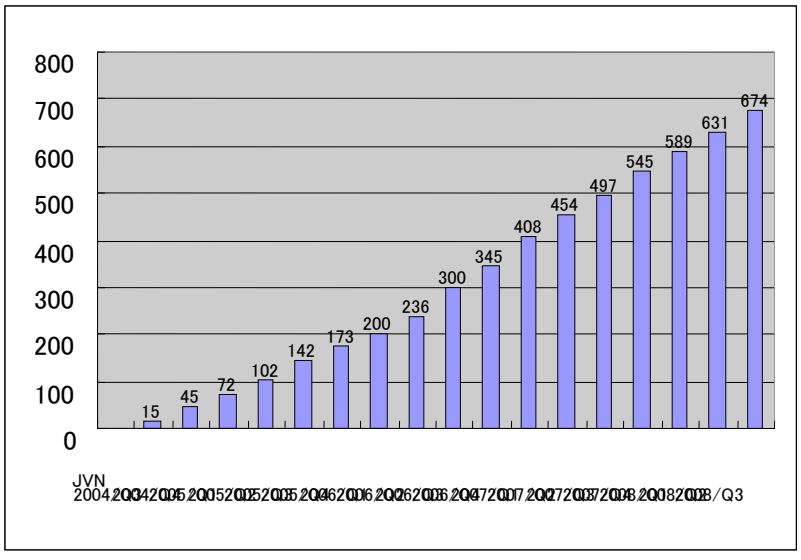

図 3-1: 累計 JVN 公表件数

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 25 件(累計 299 件)[図 3-2]でした。

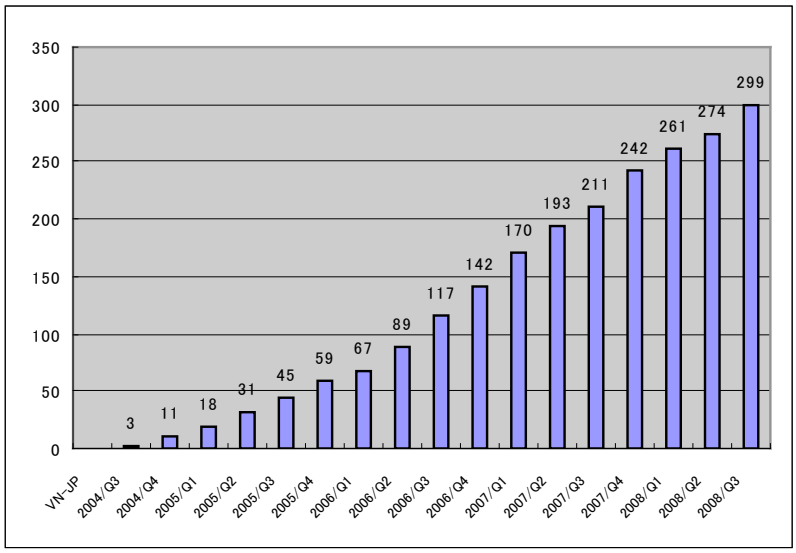

図 3-2: 累計 VN-JP 公表件数

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 18 件(累計 353 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 22 件)[図 3-4]でした。

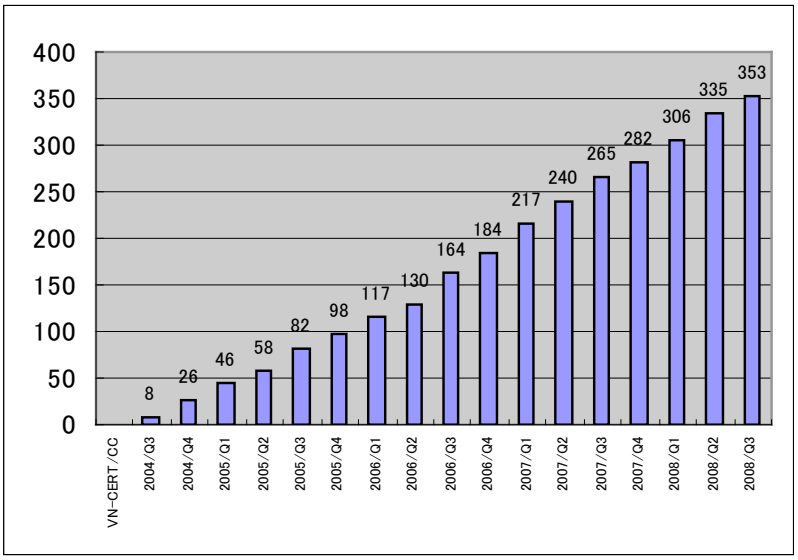

図 3-3: 累計 VN-CERT/CC 公表件数

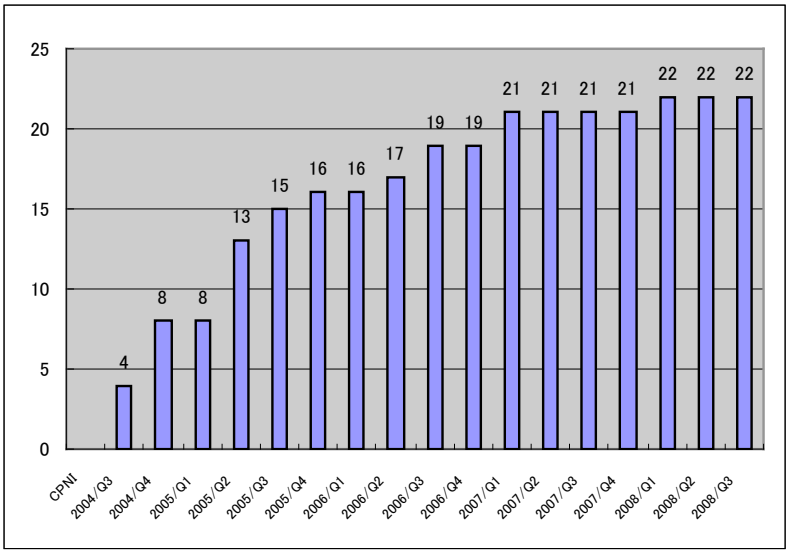

図 3-4: 累計 VN-CPNI 公表件数

II. 海外 CSIRT との脆弱性関連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 など海外 CSIRT と、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、公開までの情報を共有し活動を行っています。

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。

脆弱性関連情報取扱体制
http://www.meti.go.jp/policy/netsecurity/vulhandlingG.html
脆弱性関連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 脆弱性関連情報取り扱いガイドライン
http://www.jpcert.or.jp/vh/guideline.pdf

主な活動は以下の通りです。

(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。2008 年 9 月 30 日現在で 259 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。

登録の詳細については、http://www.jpcert.or.jp/vh/agreement.pdf をご参照ください。

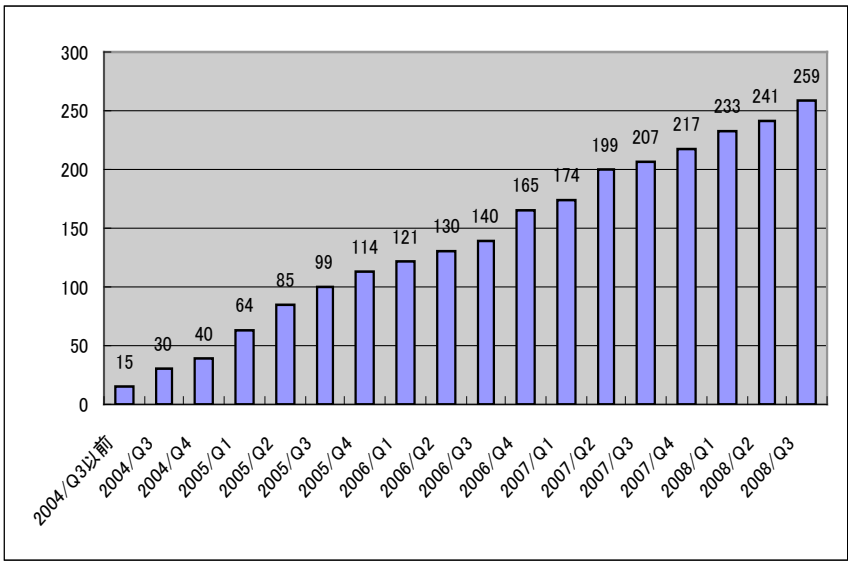

図 3-5: 累計製品開発者登録数

(3) 脆弱性情報ハンドリングワークショップの開催

「JPCERT/CC 製品開発者リスト」に登録いただいている国内ベンダの連絡担当者にお集まりいただき、7 月 30 日に脆弱性関連情報ハンドリングワークショップを開催しました。脆弱性関連情報に関する関連活動や最新状況を紹介するとともに、ベンダ連絡担当者との意見交換を行ないました。

(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

JPCERT/CC では、今期、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企業向け個別セミナーを 3 社に対して行いました。

各組織にコース内容を調整し、より現場に沿った内容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。個別セミナー開催に興味を持たれた組織のご担当者様は、seminar-secure@jpcert.or.jp までご連絡ください。

(5) C/C++ セキュアコーディング トワイライトセミナーの継続開催

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、問題を回避することを目的とした C/C++ セキュアコーディング トワイライトセミナーを開催しました。多くのプログラム開発関係者の方に参加いただき、2008 年 7 月 2 日「文字列」、8 月 6 日「動的メモリ管理」、9 月 3 日「ファイル入出力 Part1」を開催しました。各回ともにセキュアコーディング作法や最新状況を紹介するとともに意見交換を行ないました。

§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。

1. ボット対策事業の活動実績（月次）及び平成 19 年度の活動報告の公開

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。また、平成 19 年度の活動の成果等をとりまとめた「平成 19 年度サイバークリーンセンター活動報告」も公開しました。

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/
2008 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/200807/0807monthly.html
2008 年 08 月度 サイバークリーンセンター活動実績
https://www.ccc.go.jp/report/200808/0808monthly.html
平成 19 年度サイバークリーンセンター活動報告
https://www.ccc.go.jp/report/h19ccc_report.pdf

§7. 国際連携活動関連

I. 海外連携強化等

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に関する取り組みの実施状況に関する情報収集を目的とした活動や個別の協議等を行いました。

(1)2008 年 9 月 1-5 日　2008 APISC Security Training Course 参加

韓国のソウルで開催された 2008 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。

(2) 2008 年 9 月 16-18 日　GOVCERT.NL Symposium 2008 参加

オランダのロッテルダムで開催された GOVCERT.NL Symposium 2008 に出席し、インターネットセキュリティの維持に関して参加者と意見交換を行い、JPCERT/CC との間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。

II. 海外 CSIRT コミュニケーション、トレーニング等

アジア太平洋地域における CSIRT 構築支援およびトレーニングを行っています。

(1) CamCERT 構築支援活動　2008 年 9 月 25 日～

今期においては、カンボジア王国のナショナル CSIRT である CamCERT に対して ICT 管理能力向上などを目的とした CSIRT 構築支援活動を開始しました。

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

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。

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

FIRST Steering Committee のメンバとして、JPCERT/CC の職員が FIRST の運営に協力しています。

V. 第 21 回 FIRST Conference 京都

第 21 回目となる FIRST Annual Conference 2009 (FIRST 年次会合)が、来年(2009 年)、京都において開催されます。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 CSIRT メンバや関係機関の協力を得ながら、開催準備を進めています。

開催テーマ:「余波:インシデント復旧の技術と教訓」
開催日程：2009 年 6 月 28 日～7 月 3 日（詳細プログラム未定）
開催場所：京都　ホテルグランヴィア

プログラム、講演申込み、参加申込みなど詳しくは、以下 URL をご参照ください。
http://www.first.org/

§8. 講演活動一覧

(1) 業務統括　伊藤　友里恵
「変化し続ける情報セキュリティ上の脅威への対応」
JAIPA 沖縄 ICT フォーラム 2008/2008 年 7 月 11 日

(2) 常務理事　早貸　淳子
「ＥＣサイトにおけるセキュリティ上の脅威の動向と対策」および
「EC サイトの包括的セキュリティ向上策と迷惑メールの対策」パネルディスカッション
JAIPA 沖縄 ICT フォーラム 2008/2008 年 7 月 12 日

(3) 早期警戒グループ　小宮山　功一朗
「コミュニケーションの変化がもたらす光と影　～人が主役の情報セキュリティ～」
高エネルギー加速器研究機構/2008 年 7 月 16 日

(4) 理事　真鍋　敬士
「CSIRT の役割とインシデント情報共有」
IT-Keys /2008 年 7 月 18 日

(5) 情報流通対策グループ　久保　正樹
「セキュアプログラミング(C/C++編)」
IT-Keys /2008 年 7 月 18 日

(6) 早期警戒グループ　グループマネージャ　鎌田　敬介
「インターネットセキュリティ最新動向」
「情報セキュリティの技術的な基礎論」
「情報の分類と保管」
平成 20 年度法務局・地方法務局職員情報セキュリティ研修　法務省民事局
2008 年 8 月 5、6 日

(7) 早期警戒グループ　リーダ　名和　利男
「組織内におけるインシデント対応」

平成 20 年度法務局・地方法務局職員情報セキュリティ研修　法務省民事局
2008 年 8 月 6 日

(8)　業務統括　伊藤　友里恵
「Vulnerability in Control System Handling and Disclosure Policy」
Process Control System Industry Conference/2008 年 8 月 26 日

(9)　業務統括　伊藤　友里恵
「制御系システムセキュリティとサイバーセキュリティ」
Manufacturing Open Forum 2008/2008 年 9 月 12 日

§9. 掲載記事一覧

(1)　早期警戒グループ　リーダ　名和　利男
日経コミュニケーション from CSIRT フォーラム　CSIRT 構築日誌
第4回 情報収集に欠かせない「棚卸し」
日経 BP 社日経コミュニケーション/2008 年 7 月 15 日号 Page80

(2)　早期警戒グループ　グループマネージャ　鎌田　敬介
「JPCERT/CC 情報発信の取り組みについて」
NISC 重要インフラニュースレター（評価版）/2008 年 8 月 6 日

(3)　早期警戒グループ　リーダ　名和　利男
日経コミュニケーション from CSIRT フォーラム　CSIRT 構築日誌
第5回 VRDAで対策の意思決定を迅速に
日経 BP 社日経コミュニケーション/2008 年 8 月 15 日号 Page80

(4)　早期警戒グループ　リーダ　名和　利男
日経コミュニケーション from CSIRT フォーラム　CSIRT 構築日誌
第6回 KENGINEでぜい弱性分析に一貫性を
日経 BP 社日経コミュニケーション/2008 年 9 月 1 日号 Page80

(5)　早期警戒グループ　グループマネージャ　鎌田　敬介
「標的型メール攻撃対策 /「予防接種」」
NISC 重要インフラニュースレター（評価版）/2008 年 9 月 17 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 ：
BA F4 D9 FA B8 FB F0 73 57 EE 3C 2B 13 F0 48 B8

☐ インシデント報告様式

http://www.jpcert.or.jp/form/