報道関係者各位

2005 年 11 月 7 日
有限責任中間法人 JPCERT コーディネーションセンター

インターネットセキュリティに対する JPCERT/CC 2005 年第 3 四半期活動報告
（2005 年第 3 四半期 2005 年 7 月～9 月）

有限責任中間法人 JPCERT コーディネーションセンター 東京都千代田区、代表理事 歌代 和正、略称 JPCERT/CC）は本日、2005 年 7 月 1 日から9 月 30 日までに確認したコンピュータセキュリティインシデントについて、以下の通り発表いたします。

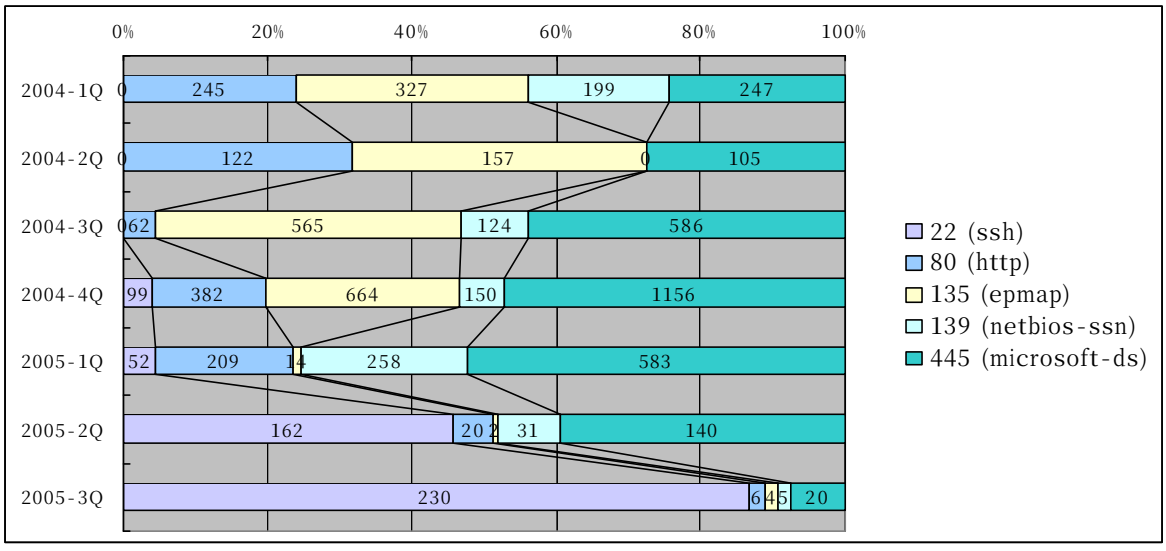
① インシデント報告件数

2005 年 7 月 1 日から2005 年 9 月 30 日までの間に JPCERT/CC が受けたコンピュータセキュリティインシデントに関する報告件数は 667 件でした。インシデント発生元に対する通知件数の対前期比は 21.8%と増加しています。

SSH サービスに対するブルートフォースアタックが増加

今期間の特徴として TCP22 番ポートに関するインシデント報告が増加していることが挙げられ、その要因はリモート管理などに用いられる SSH サービスに対するブルートフォースアタックが増加しているためと推測されます。ブルートフォースアタックとは、ログイン名パスワードの組み合わせに対する総あたり攻撃を行うことです。さらに、日本語辞書を用いたブルートフォースアタックが確認されているため、SSH サービスの提供は、類推しにくいパスワードと公開鍵認証などを組み合わせて実施することが推奨されます。

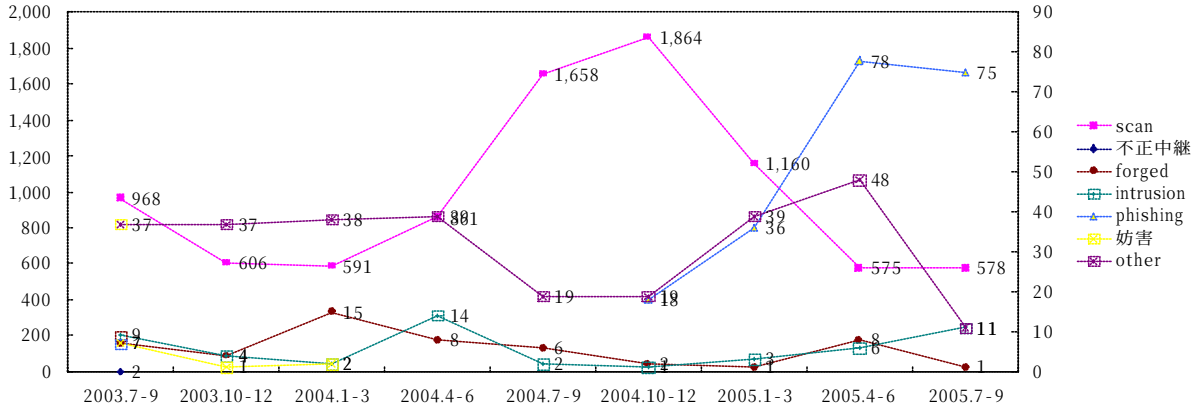
資料 1:インシデントレポートポート別グラフ



フィッシングに関する報告件数が高水準を維持

JPCERT/CC が 2005 年 7 月 1 日から2005 年 9 月 30 日までの間に受けたインシデントの種類別では、Web 偽装詐欺などフィッシング（Phishing）に関する報告が 75 件と、報告件数が倍増した前期（2005 年 4 月～6 月）と比べてほぼ横ばいの数値となり、フィッシング行為に関する活動が活発なまま推移している現状がうかがえる結果となりました。特に、7 月末には邦銀のフィッシングサイトが発見されるなど、今後は日本の利用者を標的にしたフィッシング行為に対しても注意する必要があると考えられます。

資料 2 ：インシデント種類別報告件数



Scan （※1） ：スキャン、プローブ、その他不審なアクセス
Forged ：送信ヘッダを詐称した電子メールの配信
Intrusion ：システムへの侵入
Phishing ：認証情報等の不正取得
Other ：その他

＊1： Scan とは、自動化ツールを用いて広範囲にわたる任意のホストに対して行なわれます。セキュリティ上の弱点を放置していると、弱点の存在を検出され、ホストへの侵入等さまざまなアタックを受ける可能性があります。

②中国をアクセス元とするスキャンが増加

2005 年 7 月 1 日から2005 年 9 月 30 日までのインターネット定点観測システム（ISDAS）観測では、アクセス先ポートとして、TCP1433 番ポートへの突発的なスキャン増加が観測され、大半は中国からのものでした。一方、TCP135 番および 445 番ポートへのスキャンは減少傾向が見られます。
アクセス元地域別に関しては、2005 年 6 月頃より日本国内からのスキャンは減少し、中国からのスキャンが増加傾向にあります。

各ポートの機能について

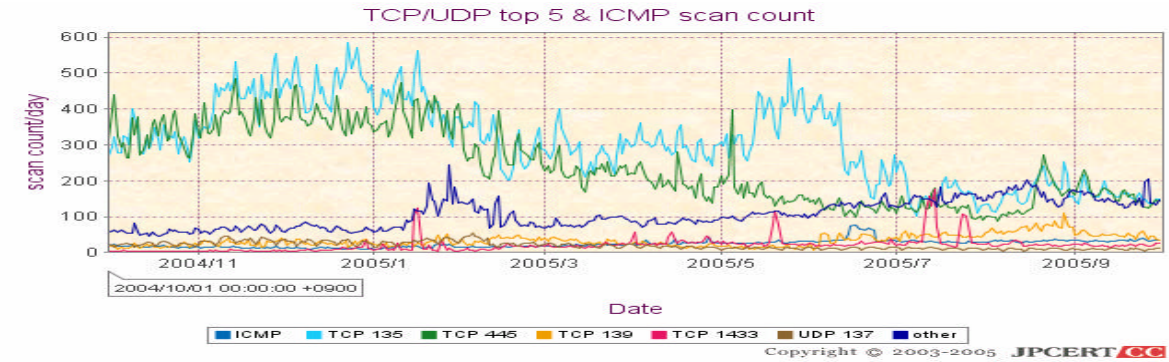
TCP1433 ：Microsoft SQL Server

TCP135 ：DCE end point resolution

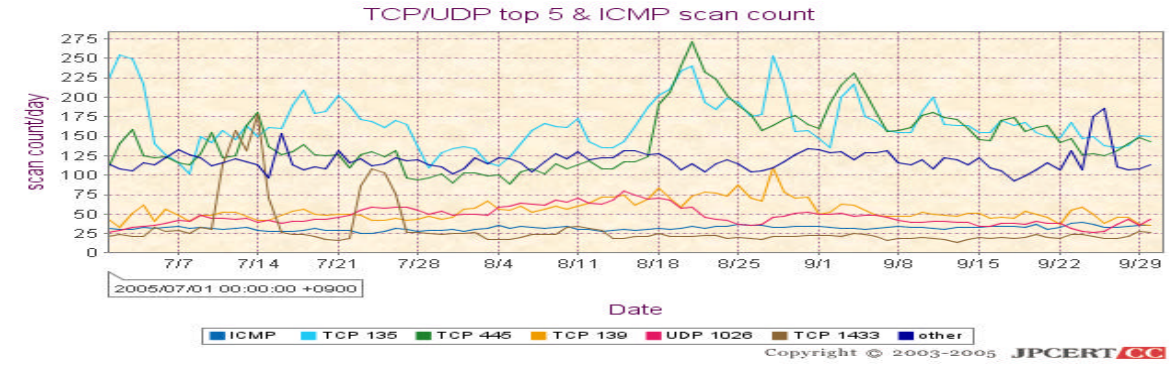
TCP445 ：Microsoft Directory Service

TCP22 ：SSH

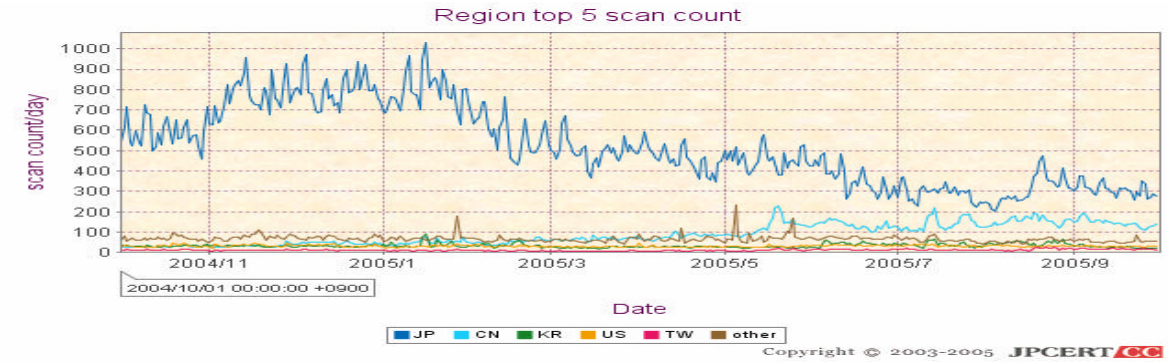
資料 3 :アクセス先ポートグラフ（1 年グラフ 2004/10/1～2005/9/30）



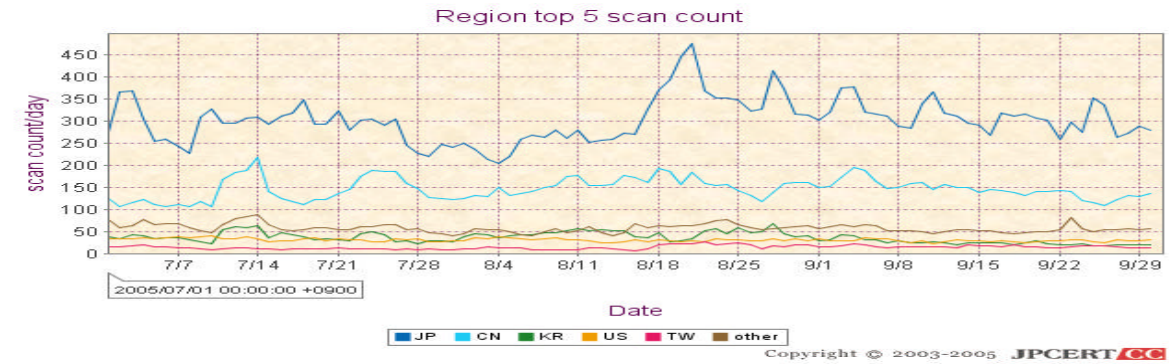
資料 4 :アクセス先ポートグラフ（2005/7/1～2005/9/30 グラフ）



資料 5 :アクセス元地域別グラフ（1 年グラフ 2004/10/1～2005/9/30）



資料 6 :アクセス元地域別グラフ（2005/7/1～2005/9/30 グラフ）



③ 脆弱性情報流通

国際的な脆弱性関連情報コーディネーションの増加

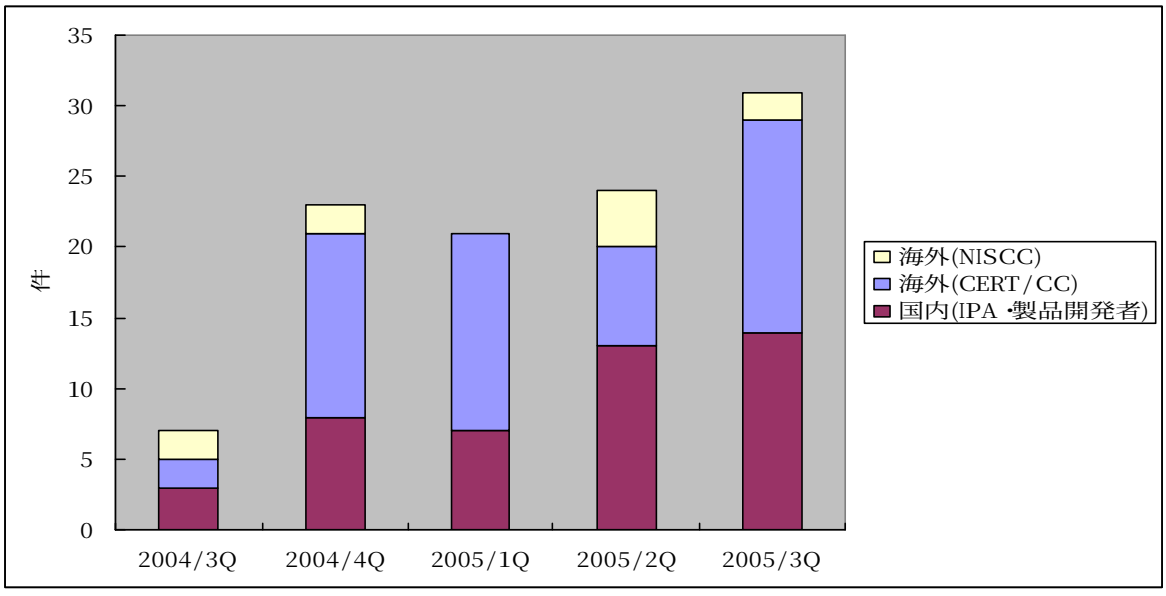
2005 年 7 月 1 日から 2005 年 9 月 30 日までの間に、JPCERT/CC が日本国内の製品開発者や海外の調整機関などの関連組織とのコーディネーションを行ない、公開した脆弱性情報は 31 件です。このうち、経済産業省告示「ソフトウェア等脆弱性関連情報取扱基準」に基づいて、独立行政法人情報処理推進機構（IPA)および国内製品開発者からの連絡により、コーディネーションを行い、公開した脆弱性情報は 14 件です。また、海外の調整機関（米国 CERT/CC、英国 NISCC）とのパートナーシップに基づいて、コーディネーションを行い、公開した脆弱性情報は 17 件です。国内の届出に基づき、公開した脆弱性 14 件のうち、6 件は海外 CSIRT 組織を通じて国際的なコーディネーションを実施しており、国際的なコーディネーションを必要とする事例が増加しています。JPCERT/CC が今期間に行ったコーディネーションに関する詳細な情報は、添付参考資料をご参照下さい。

今期間の脆弱性の特徴として、国内届出においては、オープンソースソフトウェア、Web を利用したアプリケーションに関する脆弱性が多くなっており、脆弱性の種別でもクロスサイトスクリプティング（※2）やクロスサイトリクエストフォージェリ（※3）といった Web アプリケーションに関する脆弱性が増加傾向にあります。海外 CSIRT 組織から連絡を受けた脆弱性に関しては、システム管理、特にバックアップ製品に関する脆弱性が複数発見されています。脆弱性の種別としては、バッファオーバフローや認証機構に関する脆弱性が増加傾向にあります。

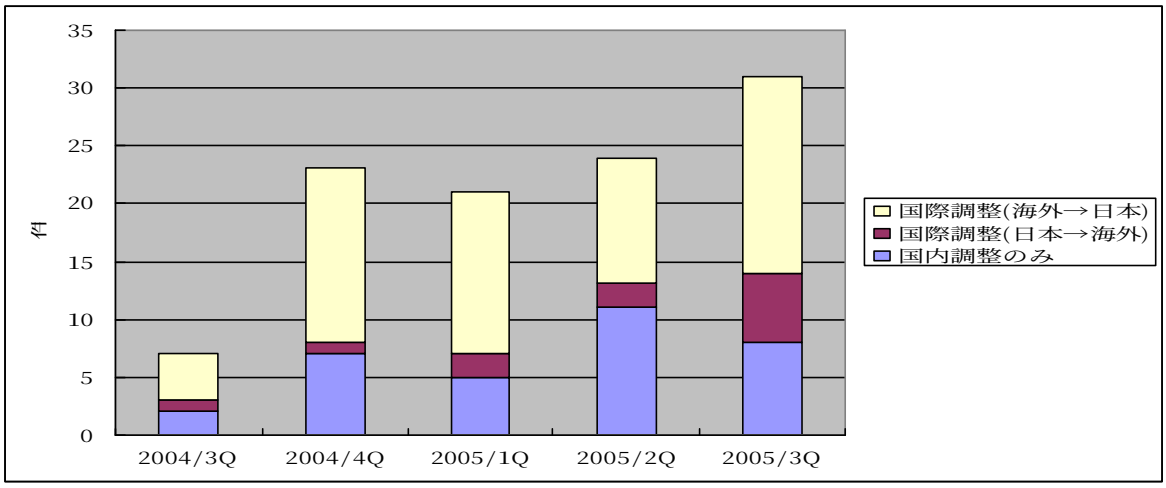
＊2： クロスサイトスクリプティング　　ソフトウェアのセキュリティホールの一つで、Web サイトの訪問者の入力をそのまま画面に表示する掲示板などのプログラムが、悪意のあるコードを訪問者のブラウザに送ってしまう脆弱性のこと。（Incept Inc. IT 用語辞典 e-Words より引用）

＊3： クロスサイトリクエストフォージェリ　　悪意のある Web サイトに仕組まれたスクリプトや自動転送(HTTP リダイレクト）によって、閲覧者が意図せず別の Web サイト上で何らかの操作を行なわされてしまう攻撃手法。（Incept Inc. IT 用語辞典 e-Words より引用）

資料 7： 四半期毎の脆弱性関連情報の公開件数(報告元別)

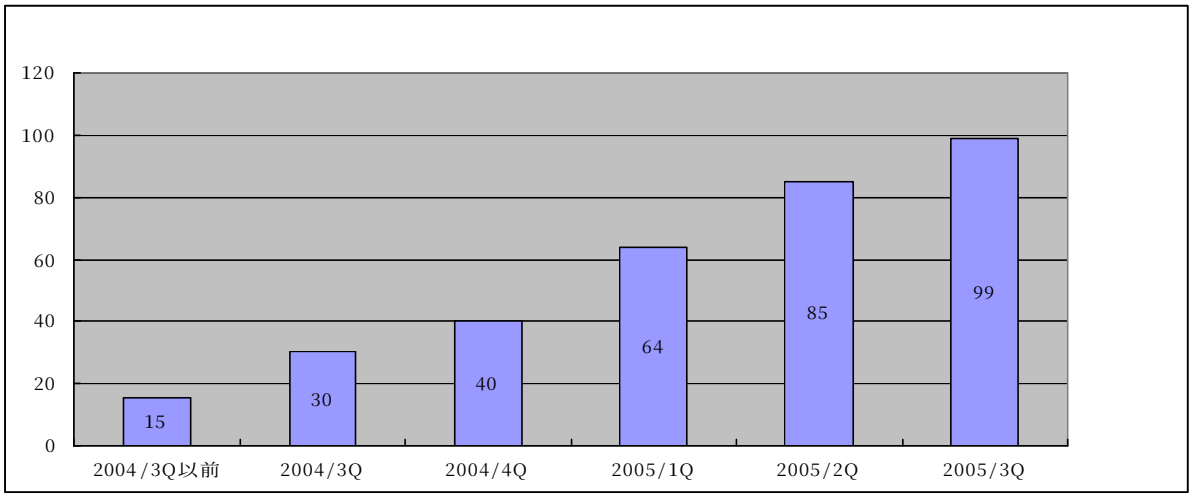


資料 8： 四半期毎の脆弱性関連情報の公開件数の内訳(国際調整の有無)



JPCERT/CC が実施している国内製品開発者の POC 登録については、2005年 9 月 30 日現在、登録件数は 99 件となりました。登録製品開発者の詳細は JPCERT/CC が IPA と共同運用している JP Vendor Status Notes(JVN)の Web サイト(http://jvn.jp/)をご参照ください。

資料 9： 四半期毎の POC 登録件数の推移



JVN では、2005 年 9 月 9 日より、JVNRSS という形式で、RSS 配信を開始しました。これにより Web サイトにアクセスしなくても、随時更新された最新脆弱性情報が配信されるため、従来に比べて容易に JVN が提供する脆弱性情報を入手することができるようになりました。JVNRSS では、Web ページ上で容易に JVNRSS を利用していただくために、JavaScript と Flash によるインタフェースも用意しています。JVN に関する詳細は JP Vendor Status Notes (JVN)の Web サイト (http://jvn.jp/)をご参照ください。

今後の脆弱性情報流通への対応としては、国際的な脆弱性の情報流通の重要性、拡大を踏まえ、より一層の海外 CSIRT 組織との連携強化を実施していくとともに、脆弱性への効果的な対応を実現するため、脆弱性が与えるインパクトや対応の優先度を評価する仕組みの構築を行う予定です。さらに、JVN に掲載されている情報を英語でも発信することを予定しています。

④ 早期警戒グループ　新規活動について

昨今、コンピュータセキュリティインシデントはその対象をインターネット全体から個人・個別組織に、またその目的も金銭の搾取といった内容に変化しています。このような変化に対応するためには、特定の企業、組織に直接アプローチし、その情報システムの保護を目的としたサービスが必要となります。このような背景から、JPCERT/CC では社会的に重要なシステムを運用する企業や組織のセキュリティリスクの軽減を目的に、2005 年 7 月より早期警戒グループの活動を開始いたしました。

1)早期警戒情報

JPCERT/CC には、インシデントハンドリング、インターネット定点観測システムの運用、脆弱性情報流通の各既存事業を通して得られる国内外の多くの脅威情報（インシデント情報、既知/未公開脆弱性情報、インターネット トラフィックモニタリング情報、攻撃情報等）が集約されます。早期警戒グループでは、これら脅威情報を総合的に分析し、重要システムの運用者等に対し早期警戒情報（※4）を発信します。

＊4： 早期警戒情報とは、JPCERT/CC が入手した情報の中で重要システムの運用者と共有する必要があると判断した脅威情報、及び対策情報を表します。

早期警戒情報の例として、

- 脅威度の高い未公開の脆弱性情報に関する、既知の回避策の共有
- 大規模な範囲を対象とした攻撃予告に関する、注意喚起と対策情報の共有
- 攻撃情報が一般に公開された脆弱性情報に関する、注意喚起と対策情報の共有

などが挙げられます。

早期警戒情報には必ず回避策をつけて提供すること、情報提供先とは直接やり取りをするといったルールを持つことで、安全で、適切な情報提供を行います。

2)サイバーセキュリティ演習

情報システムが社会的に重要なインフラを運営する組織のシステムにも浸透した結果、そのシステムをターゲットとしたサイバー攻撃が発生した場合の社会的影響が問題視されています。

JPCERT/CC では、重要システムの運営組織におけるインシデント発生時の組織内の情報共有・連絡体制、インシデント対応、復旧体制などの検証を目的とした「サイバーセキュリティ演習実施サービス」を行います。本演習サービスでは、演習の企画、計画、シナリオ作成から、演習の実施、結果のまとめまでの一連のサービスを提供します。また、外部のサイバー演習専門の機関と連携し、「過去の事例の活用」、「高度な演習技術」を利用したサービスを展開します。また、演習に使用するシナリオは、企業・組織の状況を個別ヒアリングし作成するため、各企業・組織が抱える問題点、課題をより鮮明に洗い出します。

3)脅威分析

「ボットネット」に代表されるように昨今のコンピュータセキュリティインシデントは、その性質の変化が激しく、また攻撃・影響範囲も局地化しています。このように急速に変化し、局地化するインシデントに対

応するためには、そこで使用されている技術について詳しく分析し、今後の動向を予測し、対策を開発することが重要です。JPCERT/CC では、脅威分析業務を通して、コンピュータセキュリティインシデントで使用される中心技術の分析を行い、今後の傾向の予測、有効な対策の開発を行います。今年度は、今日の重大な脅威の 1つである「ボットネット」を重点脅威として調査・分析を行います。

JPCERT/CC について

JPCERT コーディネーションセンターは、情報通信システムの円滑な運用の脅威となるコンピュータセキュリティインシデントに対応する組織（CSIRT：Computer Security Incident Response Team）です。任意団体設立時より、①コンピュータの不正利用などによるインシデントへの対応、②ワームの感染活動の観測をはじめとするインターネット定点観測システムの運用、③ソフトウェアの脆弱性に関する調整、④コンピュータセキュリティインシデントを未然に防ぐための早期警戒活動など、日本における情報セキュリティ対策活動のコーディネーションを行っています。さらに、国内における技術情報の配信やイベントを通じた啓発活動、およびアジア太平洋地域における CSIRT 間の情報交換網の構築や組織間の連携強化を主導しています。同社に関する詳細な情報は、Web サイト http://www.jpcert.or.jp/ でご覧いただけます。

<報道機関問い合わせ先>

有限責任中間法人 JPCERT コーディネーションセンター

広報 江田 佳領子

pr@jpcert.or.jp

電話 03-3518-4600

ウェーバー・シャンドウィック・ワールドワイド株式会社内

神田／清船

kkanda@webershandwick.com ikiyofune@webershandwick.com

電話 03-5445-1272 FAX 03-5427-7327

JPCERT CC™

参考資料

参考資料1：2005 年第 3 四半期にコーディネーションを行い、公開した脆弱性関連情報　(国内届出)

No.	項目	ソフトウェア種別
JVN#79314822	Tomcat におけるリクエスト処理に関する脆弱性	Web アプリケーション
JVN#76659792	WirelessIP5000 に複数の脆弱性	携帯電話
JVN#31226748	複数のウェブブラウザにおいてリクエスト分割攻撃が可能な脆弱性	Web ブラウザ
JVN#79925E6F	unicode 版 msearch におけるクロスサイトスクリプティングの脆弱性	検索システム
JVN#62914675	Ruby においてセーフレベル 4 がサンドボックスとして機能しない脆弱性	プログラミング言語
JVN#40940493	Webmin および Usermin における認証回避の脆弱性	システム管理
JVN#97422426	ハイパー日記システムにおけるクロスサイト・リクエスト・フォージェリの脆弱性	Web アプリケーション
JVN#42435855	FreeStyleWiki におけるコマンドインジェクション の脆弱性	Web アプリケーション
JVN#23727054	Pochy におけるサービス運用妨害 (DoS) の脆弱性	メールクライアント
JVN#8778A308	Common Management Agent 3.x における情報漏えいの脆弱性	システム管理
JVN#38138980	Hiki におけるクロスサイトスクリプティングの脆弱性	Web アプリケーション
JVN#29273468	QRcode Perl CGI & PHP scripts におけるサービス運用妨害の脆弱性	Web アプリケーション
JVN#60776919	tDiary におけるクロスサイト・リクエスト・フォージェリの脆弱性	Web アプリケーション
JVN#257C6F28	Internet Explorer コンポーネントを使用するアプリケーションにおけるセキュリティ ゾーンの扱いに関する脆弱性	Web ブラウザ

参考資料2：2005 年第 3 四半期にコーディネーションを行い、公開した脆弱性関連情報　(海外関係機関とのパートナーシップに基づく)

No.	項目	ソフトウェア種別
JVNVU#744929	mod_ssl にクライアン認証の回避が可能な脆弱性	Web サーバ
JVNVU#102441	X server に複数の整数バッファオーバーフロー の脆弱性	ネットワークサーバ
JVNVU#236045	Cisco IOS Firewall Authentication Proxy にバッファオーバーフロー の脆弱性	OS
JVNVU#139421	simpleproxy における書式文字列に関する脆弱性	ネットワークサーバ
JVNVU#778916	pam_ldap に認証回避が可能な脆弱性	システム管理
JVNVU#407641	EMC Legato NetWorker の database service の認証機構に脆弱性	ストレージ
JVNVU#801089	EMC Legato NetWorker の portmapper にリモートからの要求を実行する脆弱性	ストレージ
JVNVU#606857	EMC Legato NetWorker の認証機構に関する脆弱性	ストレージ
JVNVU#930892	Cisco IOS に IPv6 パケットの処理に関する脆弱性	OS
JVNVU#584505	VERITAS Backup Exec に遠隔からレジストリにアクセスされる脆弱性	ストレージ
JVNVU#352625	VERITAS Backup Exec Server Service にヒープオーバーフロー の脆弱性	ストレージ
JVNVU#259798	MIT Kerberos5 Key Distribution Center にメモリのヒープ領域が破壊される脆弱性	セキュリティ
JVNVU#623332	MIT Kerberos5 krb5_recvauth() におけるメモリ二重解放の脆弱性	セキュリティ
JVNVU#885830	MIT Kerberos5 Key Distribution Center にヒープオーバフロー の脆弱性	セキュリティ
JVNVU#680620	データ圧縮ライブラリ zlib におけるバッファーオーバーフロー の脆弱性	ライブラリ
NISCC-688910	HP Ignite-UX に様々な脆弱性	グループウェア
NISCC-356752	MindAlign 製品に複数の脆弱性	