JPCERT CC®

報道関係者各位

2006 年 7 月 20 日

有限責任中間法人 JPCERT コーディネーションセンター

JPCERT/CC、コンピュータセキュリティインシデントに対する 2006 年度事業方針を発表

CSIRT 構築支援、ボットネット対応策の推進、JVN コンテンツの拡充、国際連携などの活動を強化

2005 年 1 月 1 日から 2006 年 6 月 30 日までの活動報告を発表

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、以下 JPCERT/CC）は本日、①企業等の組織内においてコンピュータセキュリティインシデントに対応する専門チームである組織内 CSIRT（Computer Security Incident Response Team）の構築支援、②ボットおよびボットネットの実態把握と対応策の推進を含むコンピュータセキュリティ早期警戒体制の強化、③国内の情報システムに影響を及ぼす可能性のあるソフトウェア等の脆弱性及びその対策に関する情報を公開する JP Vendor Status Notes（略称、JVN）の Web サイトの充実を含む、脆弱性情報流通事業の一層の定着、および④海外関係機関との連携強化の 4 分野を柱とした 2006 年度の事業方針を発表しました。また、2005 年 2005 年 1 月 1 日から 2006 年 6 月 30 日までの JPCERT/CC 活動内容も発表しました。

(1)組織内 CSIRT 構築支援の強化

企業等の組織がコンピュータセキュリティインシデントの脅威にさらされた際に組織内においてレスポンス活動や予防、再発防止等の対策を行う専門チームである組織内 CSIRT の構築支援を強化します。

昨今のコンピュータセキュリティインシデントは、かつての不特定多数のコンピュータを狙った愉快犯的な攻撃から、特定の組織や企業等を狙った攻撃へと推移しつつあります。また、インターネットはすでに社会生活において不可欠なインフラとなっており、そのサービスの停止は組織や企業活動のみならず、社会に重大な影響を及ぼす可能性があります。また、各組織のシステムには、固有の資産価値を持つ情報が蓄積されており、各組織が他の組織とは異なった固有の脅威にさらされていることから、各組織は独自に適切な対応を行えることが必要になってきているといえます。

そこで、JPCERT/CC では、各企業等の組織内 CSIRT の構築を支援するとともに、各組織内 CSIRT が他の組織内 CSIRT や関連組織との連携により、より効果的な対策・対応を可能とする環境構築を進めます。

(2) コンピュータセキュリティ早期警戒体制の強化

（内閣官房情報セキュリティ政策会議が決定した、セキュア・ジャパン2006第2章第3節④をご参照ください）

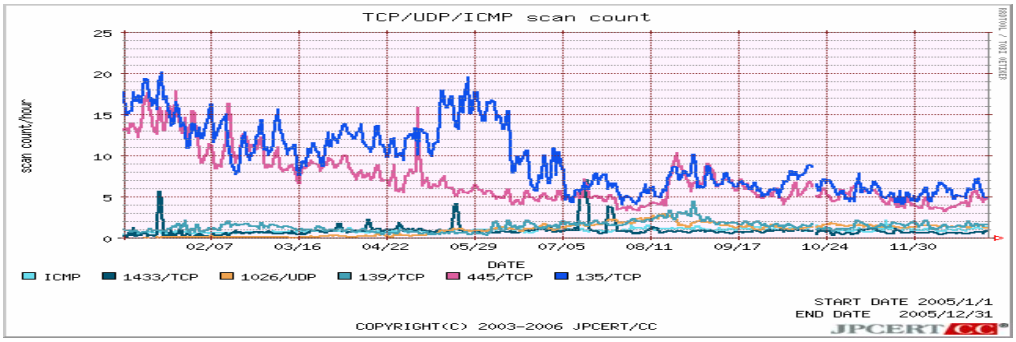
ボットおよびボットネット対策の推進

JPCERT/CC は、昨年度、インターネット セキュリティ システムズ株式会社等と共同で、ボットおよびボットネットの実態や今後想定される脅威の把握を目的とした研究を実施しました。その結果について、本日、「ボットネットの概要」を公開し、今後は脅威の認知向上に向けた言葉の定義と統一、ボットネットの実態研究結果、および対策などを順次公開していく予定です。

インターネット定点観測システムの改良

JPCERT/CC では、インターネット上で発生する攻撃に関する、より精度の高い観測データの提供を目的として 2006 年 3 月 27 日から、定点観測システム(ISDAS: Internet Scan Data Acquisition System)で、一部センサーの特異な観測結果を全体の観測結果に反映しないよう機能改善が施された新しいシステムへと移行しました。また、1週間、1 ヶ月、3 ヶ月であった観測結果の公開グラフの表示期間を 3 ヶ月および 1 年に変更し、より長期のスキャン傾向の把握が可能となりました。

資料 1: 公開グラフ (アクセス先ポートグラフ: 1 年グラフ)



2005 年度および 2006 年度上半期の ISDAS 観測動向

2006 年 4 月から 6 月の観測傾向

2006 年 4 月から 6 月における ISDAS における影響の高いインシデントの観測としては 2006 年 5 月 17 日に注意喚起を公開した RealVNC の脆弱性を狙った攻撃に関するスキャン増加の観測があげられます。本ポートへのスキャンは探索ツールも公開されており、現在でも 5900/TCP へのスキャンは継続して観測されています。(添付資料 1-1 を参照)

2005 年 12 月 7 日 1025/TCP 番ポートへのスキャン増加を観測

2005 年 10 月 12 日に Microsoft 社から公開された MS05-051 の脆弱性を狙った攻撃と思われるスキャン増加を確認、2005 年 12 月 12 日注意喚起を発行しました。本スキャンに新種のワームによる感染の試みである可能性も考えられます。本スキャンに関しては 2005 年 12 月 27 日頃に終息したことを確認しました。
(添付資料 1-2 を参照)

2005 年 7 月 12 日 1433/TCP 番ポートへのスキャン増加を観測

Microsoft SQL Server で使用されている 1433/TCP 番ポートを狙った攻撃と思われるスキャン増加を観測したため、2006 年 7 月 15 日に注意喚起を発行しました。本スキャンの増加と同時期に SQL インジェクションなどによる SQL Server 向けの攻撃が活発に行われており、その影響を観測した可能性が高いと考えられます。本スキャン増加に関しては 2005 年 7 月 29 日頃には終息したことを確認いたしました。
(添付資料 1-3 を参照)

2005 年 6 月 26 日 10000/TCP 番ポートへのスキャン増加を観測

2005 年 6 月 22 日に公開された VERITAS Backup Exec の脆弱性を狙った攻撃と思われるスキャン増加を観測したため、2006 年 6 月 28 日に注意喚起を発行しました。本スキャン増加に関しては 2005 年 7 月 10

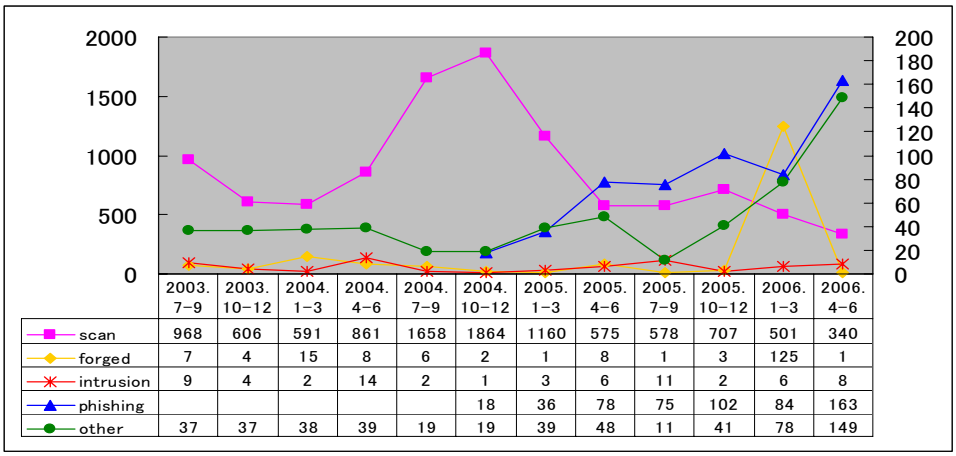
日頃には終息したことを確認しました。
（添付資料 1-4 を参照）

2005 年度および 2006 年度上半期に JPCERT/CC が受領した、インターネットセキュリティインシデントに関する報告の推移

当該期間中に受領したインターネットセキュリティインシデントの報告のうち、フィッシング（Phishing）に関する報告は、依然増加傾向にあります。また、サービス運用妨害、コンピュータウィルスや SPAM メールの受信などに関する報告件数も増加傾向にあります。Scan の報告件数は減少していますが、リモートから SSH（＊1）を使用してログインする際に使用される 22 番ポートへの Scan 報告数の割合が高く、22 番ポートを使用する場合は十分なセキュリティ対策が必要です。

(*1)SSH： 遠隔から暗号化してリーモートログインするためのプロトコル

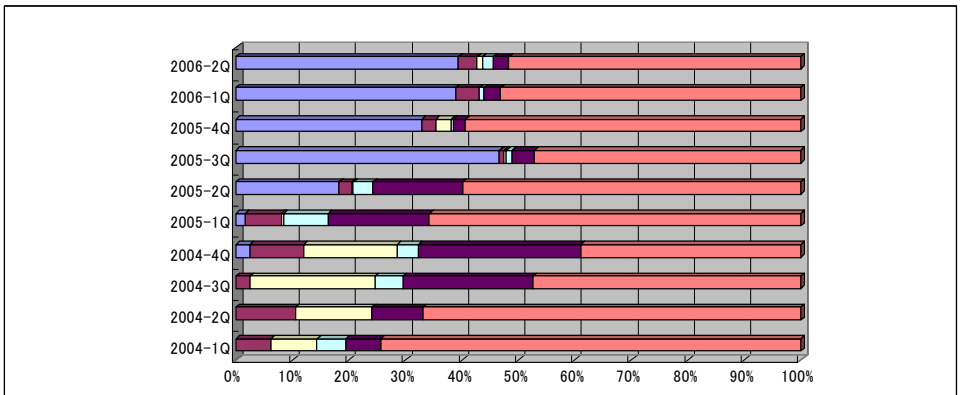
資料 2:インシデント種類別グラフ



	2003. 7-9	2003. 10-12	2004. 1-3	2004. 4-6	2004. 7-9	2004. 10-12	2005. 1-3	2005. 4-6	2005. 7-9	2005. 10-12	2006. 1-3	2006. 4-6
scan	968	606	591	861	1658	1864	1160	575	578	707	501	340
forged	7	4	15	8	6	2	1	8	1	3	125	1
intrusion	9	4	2	14	2	1	3	6	11	2	6	8
phishing						18	36	78	75	102	84	163
other	37	37	38	39	19	19	39	48	11	41	78	149

Scan　　：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　　：サービス運用妨害(DoS)、コンピュータウィルスや SPAM メールの受信など

資料 3: インシデントレポートポート別グラフ



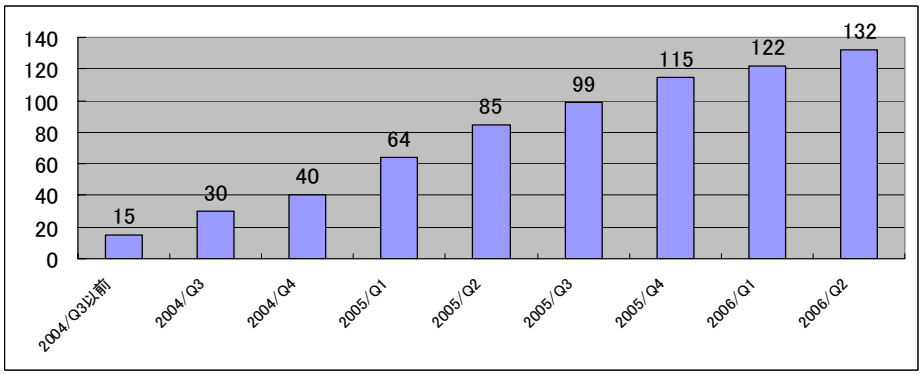
	2004-1Q	2004-2Q	2004-3Q	2004-4Q	2005-1Q	2005-2Q	2005-3Q	2005-4Q	2006-1Q	2006-2Q
other	2950	774	1205	1561	2142	529	228	343	198	110
TCP 445 (microsoft-ds)	247	105	586	1156	583	140	19	12	11	6
TCP 139 (netbios-ssn)	199	0	124	150	258	31	5	3	3	4
TCP 135 (epmap)	327	157	565	664	14	2	2	15	0	2
TCP 80 (http)	245	122	62	382	209	20	4	15	16	7
TCP 22 (ssh)	0	0	0	99	52	162	226	190	145	84

(3) 脆弱性情報流通事業

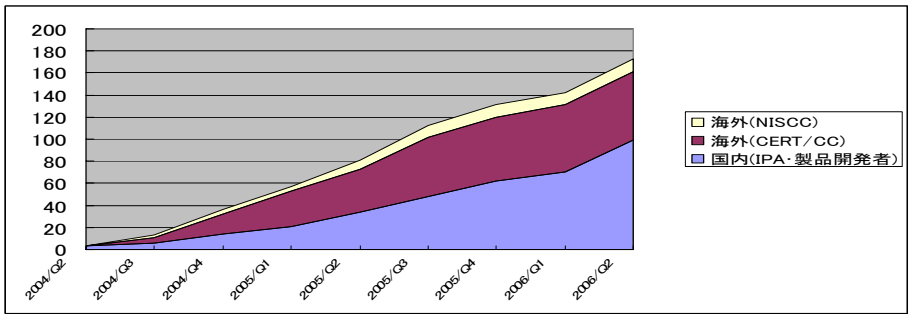
JPCERT/CC は、製品開発者との迅速かつ強固な連携による脆弱性ハンドリング、ならびにオープンソースおよびフリーソフトウエアの脆弱性情報流通活動の強化を行います。また、脆弱性への対応が必要なシステム管理者等に対策情報を適切に提供し、より迅速に対応を講じていただけるよう JVN（http://jvn.jp/）をより利用しやすいものにしていくための情報の拡充を図ります。JVN は、IPA（独立行政法人 情報処理推進機構）と共同で運営しています。

現在の脆弱性情報流通事業における開発ベンダー登録数は 132 社と拡大し、前年同期比で 35%の増加となりました。製品開発者との迅速かつ強固な連携によって、脆弱性情報流通パートナーシップが社会基盤を守る役割を担えるようになってきました。また、その脆弱性情報流通事業は国内だけにとどまらず、海外ベンダーとの調整業務も拡大しています。登録製品開発者の詳細、ならびに日本国内の情報システムに影響を及ぼす脆弱性に関する情報については、JVN の Web サイトをご確認下さい。

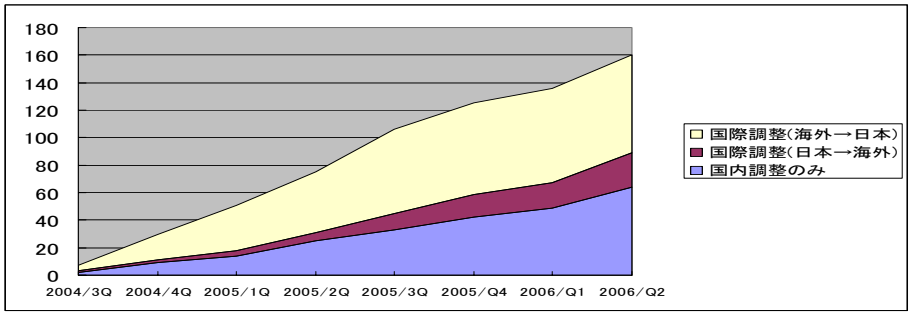
資料 4：POC(Point of Contact)登録社数



資料 5: 四半期毎の脆弱性関連情報の公開件数(報告元別)



資料 6: 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)



2005 年度および 2006 年上半期における脆弱性の動向

当該期間の脆弱性の特徴は、国内届出においては、オープンソフトウエア、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)の脆弱性が増加しています。海外 CSIRT 組織から連絡を受けた脆弱性に関しては、世界的に広く利用され、かつ影響度の高いメール配信プロトコルや Web ブラウザ製品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: Web サイトにアクセスしたビジターが入力した情報を、そのまま画面に表示させる掲示板などのプログラムが、悪意あるコードをサイトのビジターのブラウザに送る脆弱性。

(4)国際連携事業

(内閣官房情報セキュリティ政策会議が決定した、セキュア・ジャパン2006第3章第3節②をご参照ください)

アジア太平洋地域における海外CSIRTの構築を支援し、同地域におけるCSIRTの集合であるAPCERT(アジア太平洋コンピュータ緊急対応チーム*3)とも連携をとりながら、JPCERT/CCにおけるインシデント運用技術や蓄積された経験を同地域の関係諸機関と共有し、これらの機関の能力向上を図ります。

また、FIRST (Forum of Incident Response and Security Teams *4)の活動については、当センター職員が理事として組織運営に参画しています。2006 年 6 月に米国ボルチモアで開催された FIRST 年次会合には、全世界から 400 名近くの情報セキュリティ対策等に携わるメンバーが参加し、それぞれのミッションや機能、地域、経済、文化、法の壁を越えた会議を実施しました。本年度の会合では、世界的規模で発生しているサイバー犯罪に対応するための法執行機関と CSIRT の連携のあり方に関する議論が注目されました。また、日立グループの CSIRT 組織である HIRT や、NTTグループの CSIRT 組織であるNTT-CERTなど、国内外 5 組織の FIRST 加盟の支援を行いました。

さらに、APCERT においても、理事メンバーとして事務局機能を担い、APEC TEL(APEC 情報通信委員会)、ASEANなどの会議ではインシデント、また脅威情報ハンドリングを行うオペレーション CSIRT の立場から、現

実のサイバー関連の脅威について状況報告を行い、政策策定を行う各国政府担当者に共通理解と問題提言を行い、各国セキュリティチームと政策担当者間の強固な連携促進を図りました。

(*3): APCERT とは、アジア太平洋地域の CSIRT で構成される組織で、現在 14 の経済地域から 18 チームが参加しています。

(*4): FIRST とは、アメリカ、アジア、欧州、オセアニアの世界 190 以上の企業、政府機関、大学など各種機関の CSIRT によって構成されるフォーラムで、コンピュータインシデントハンドリングを国際連携によって研究、分析、対応する組織です。

JPCERT/CC について

JPCERT コーディネーションセンターは、情報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。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 yoko.kohda@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 健太郎 kkanda@webershandwick.com

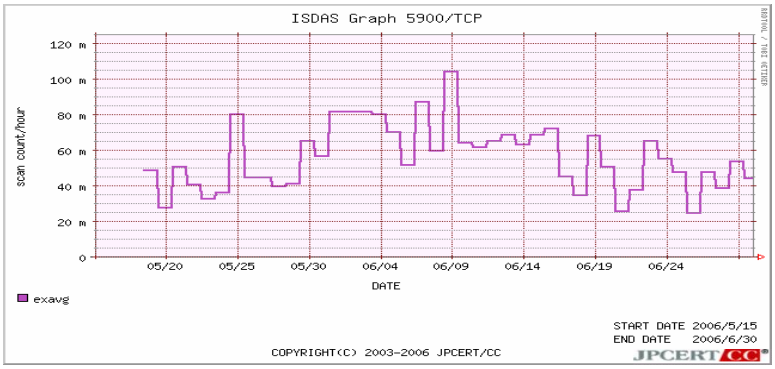
電話:03-5445-1272 FAX:03-5427-7327

JPCERT/CC ロゴは、有限責任中間法人 JPCERT コーディネーションセンターの登録商標です。その他すべての商標は、それぞれの権利帰属者の所有物です。

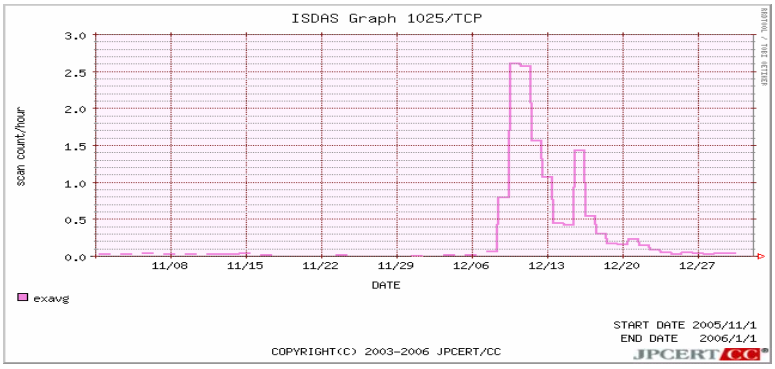
© 2006 JPCERT/CC

添付資料

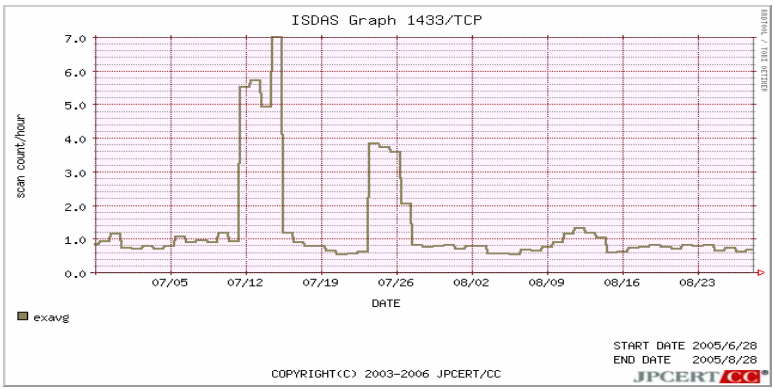
(添付資料 1-1)2006 年 5 月 17 日 5900/TCP 番ポートへのスキャン増加



(添付資料 1-2)2005 年 12 月 7 日 1025/TCP 番ポートへのスキャン増加



(添付資料 1-3)2005 年 7 月 12 日 1433/TCP 番ポートへのスキャン増加



(添付資料 1-4)2005 年 6 月 26 日 10000/TCP 番ポートへのスキャン増加