JPNIC・JPCERT/CC
セキュリティセミナー 2005

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 理事
有限責任中間法人JPCERTコーディネーションセンター 代表理事
株式会社インターネットイニシアティブ 特別研究員

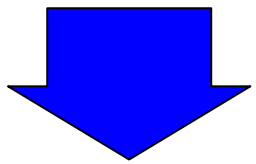
歌代　和正

JPNIC・JPCERT/CC Security Seminar 2005
JPNIC・JPCERT/CC Security Seminar 2005
JPNIC・JPCERT/CC Security Seminar 2005

テーマ
サーバアプリケーションセキュリティ

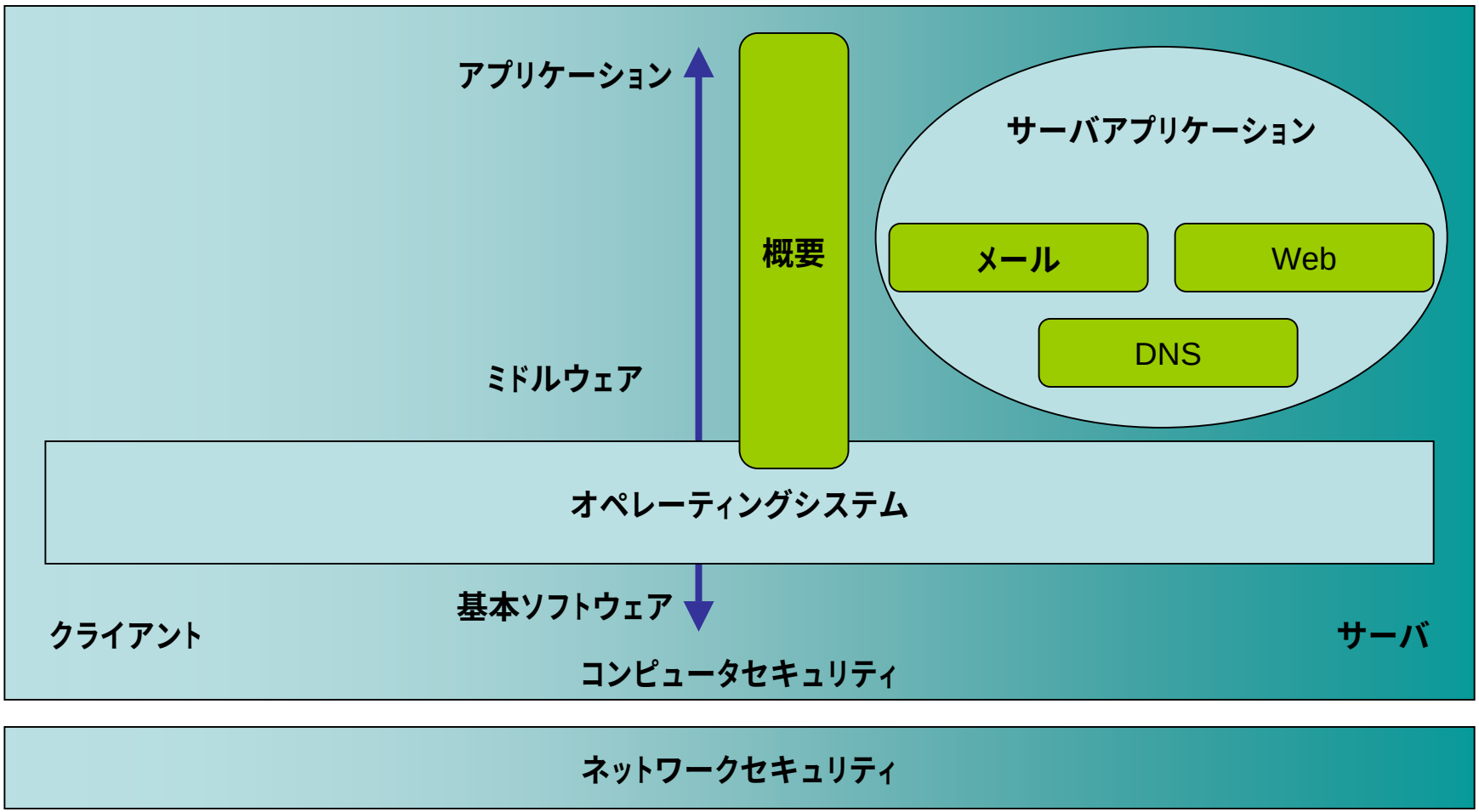
JPNIC・JPCERT/CC セキュリティセミナー2005
サーバアプリケーションセキュリティ

ネットワークのセキュリティやサーバ自身のセキュリティだけではなく、「サーバのアプリケーション」のセキュリティに目を配る事も重要



サーバアプリケーションにおけるセキュリティにスポットをあて、UNIXとWindowsにおけるDNSサーバ・メールサーバ・Webサーバの実践的なセキュリティ設計とその効果について、ご紹介します。

サーバアプリケーションセキュリティ



1日目：UNIX Day

- Unix系サーバのセキュリティ概要
  - 富士通株式会社 城崎 徹様
- DNS (BIND, djbdns)
  - 株式会社日本レジストリサービス 民田 雅人様
- メールサーバとセキュリティ(迷惑メール対策)
  - 株式会社インターネットイニシアティブ　山本 功司様
- Webのセキュリティ
  - セコム株式会社 新井 幹也様
  - セコム株式会社　金岡 晃様
  - JPNIC 木村 泰司様
  - JPNIC 岡田 雅之様

2日目：Windows Day

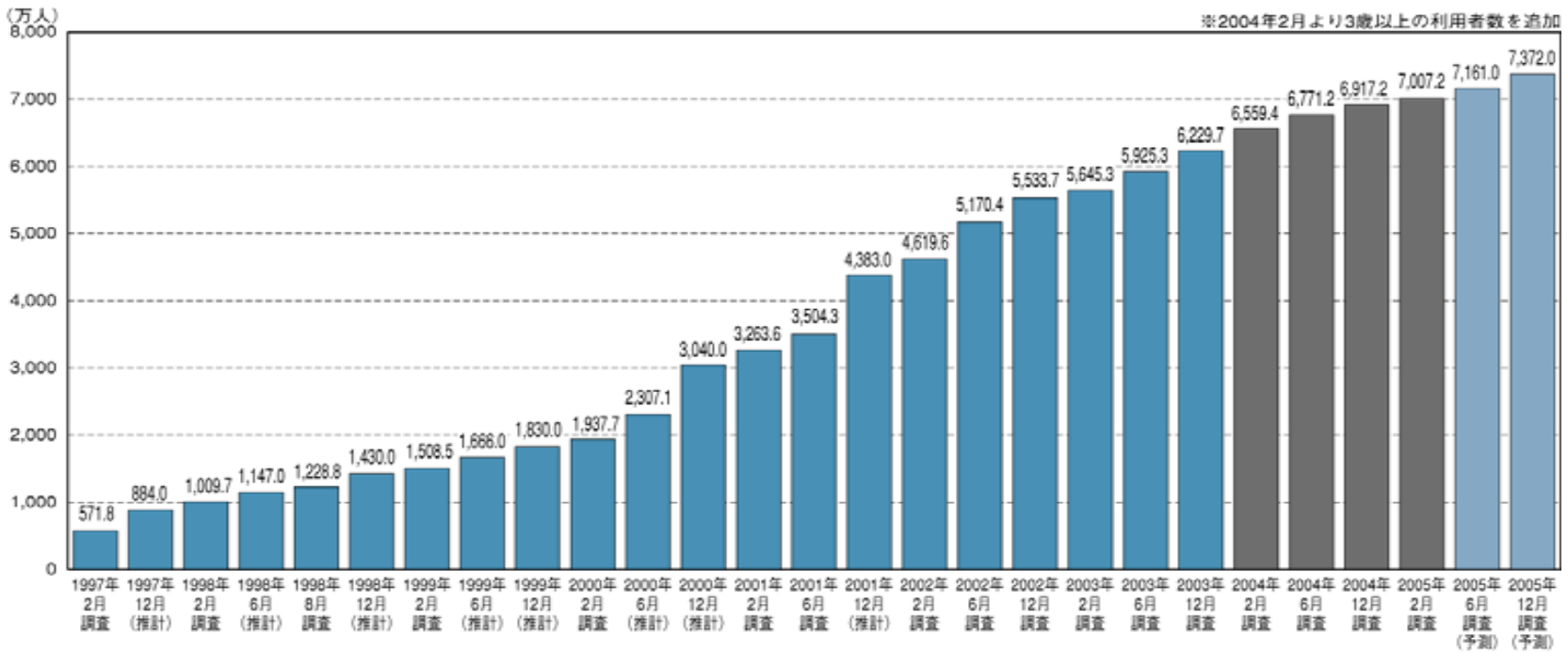
- 基調講演 「このパッチあてても大丈夫？」
  - 株式会社ラック　三輪 信雄様
- Windows Server のセキュリティ概要
  - マイクロソフト株式会社 小野寺 匠様
- Windows DNS と ActiveDirectory
  - マイクロソフト株式会社 山本 明広様
- RADIUSで実現する認証サーバ
  - 株式会社アクセンス・テクノロジー 納村 康司様
- Web (IIS, Apache)
  - インターネットセキュリティシステムズ株式会社 守屋 英一様

インターネット環境の変化

日本国内のインターネット利用者数推移

3歳以上のインターネット利用者は7,000万人を突破

資料1-3-1　日本国内のインターネット利用者数推移（1997年－2005年）

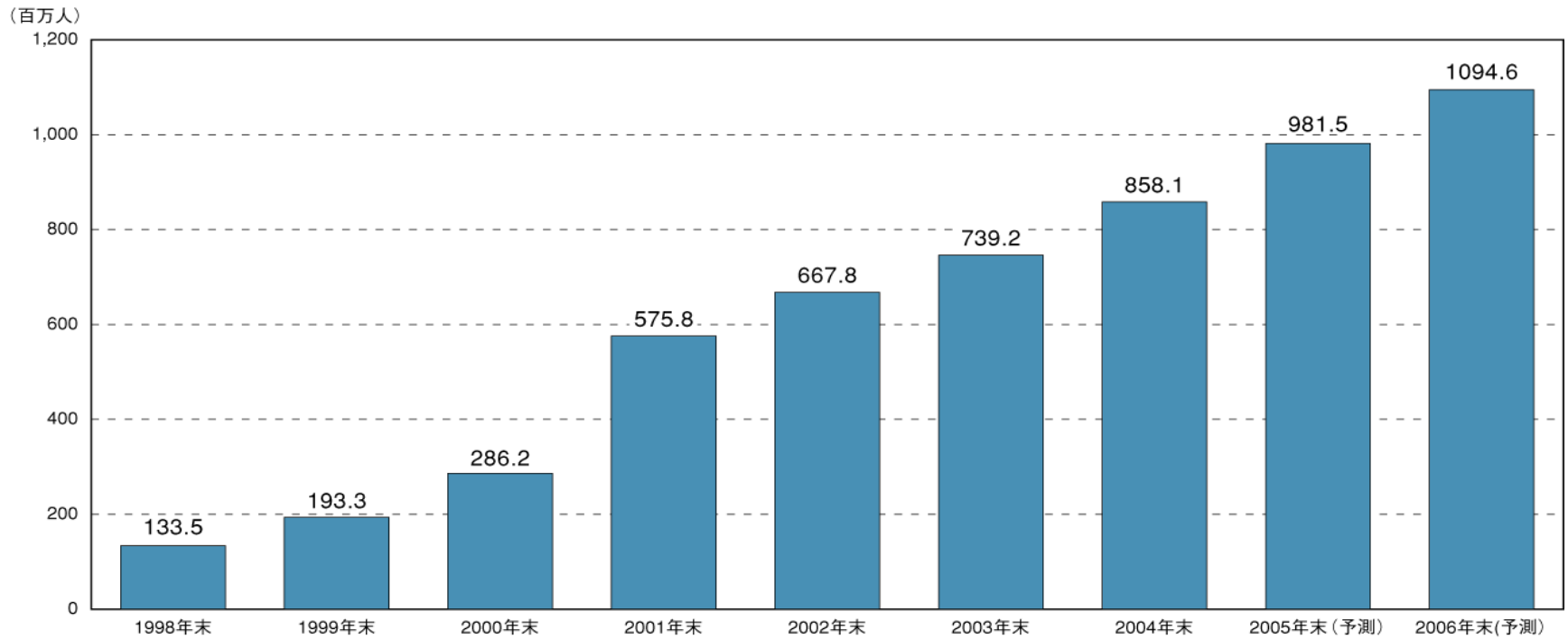


インターネット白書2005　©Access Media/impress,2005

世界全体のインターネット利用者数推移と予測

2005年末には9億8,150万人に達する見込み

資料7-1-1　世界全体のインターネット利用者数推移と予測（1998年－2006年）

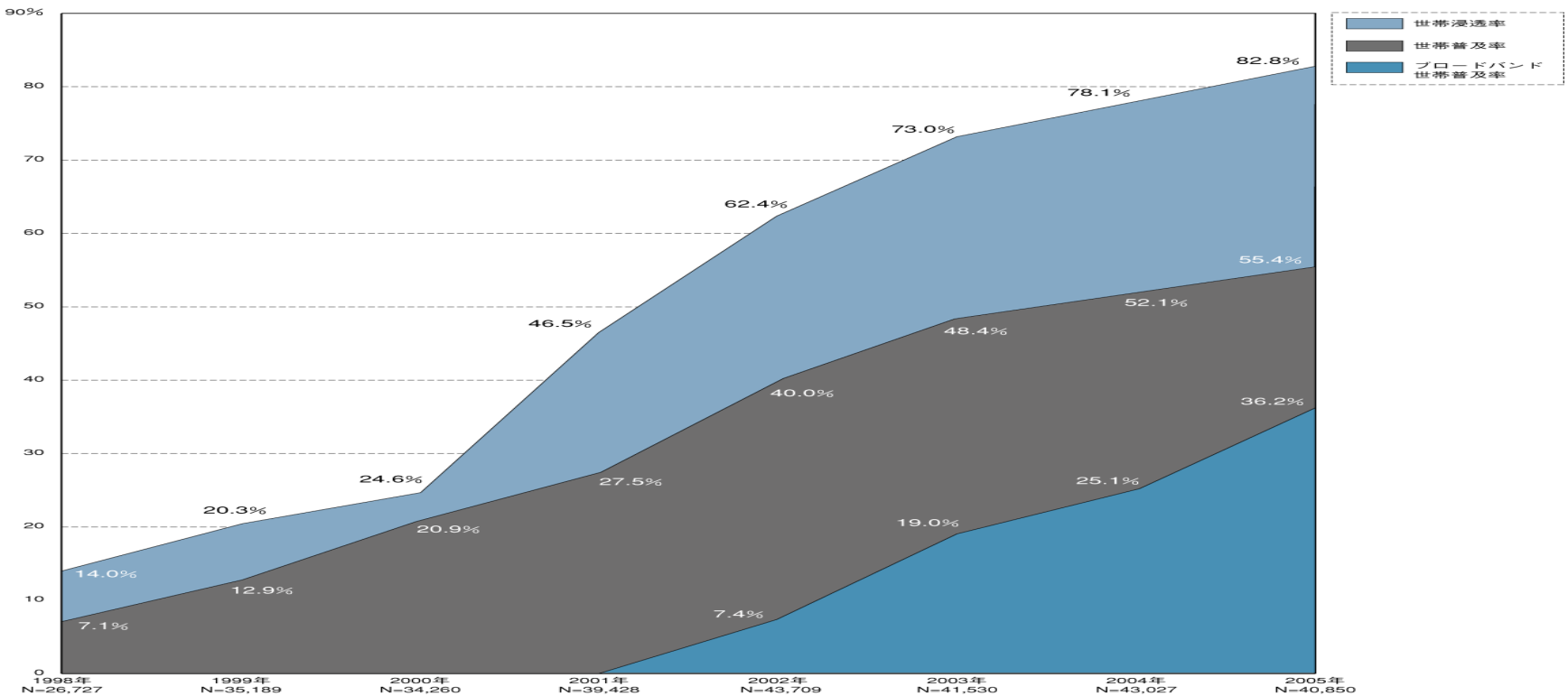


インターネット白書2005　©Access Media International,2005

インターネット世帯浸透率と世帯普及率の推移

2001年以降はADSLの普及により、世帯普及率と家庭内でのインターネット利用者が増加

資料1-1-5　インターネット世帯浸透率と世帯普及率、ブロードバンド世帯普及率の推移（1998年－2005年）

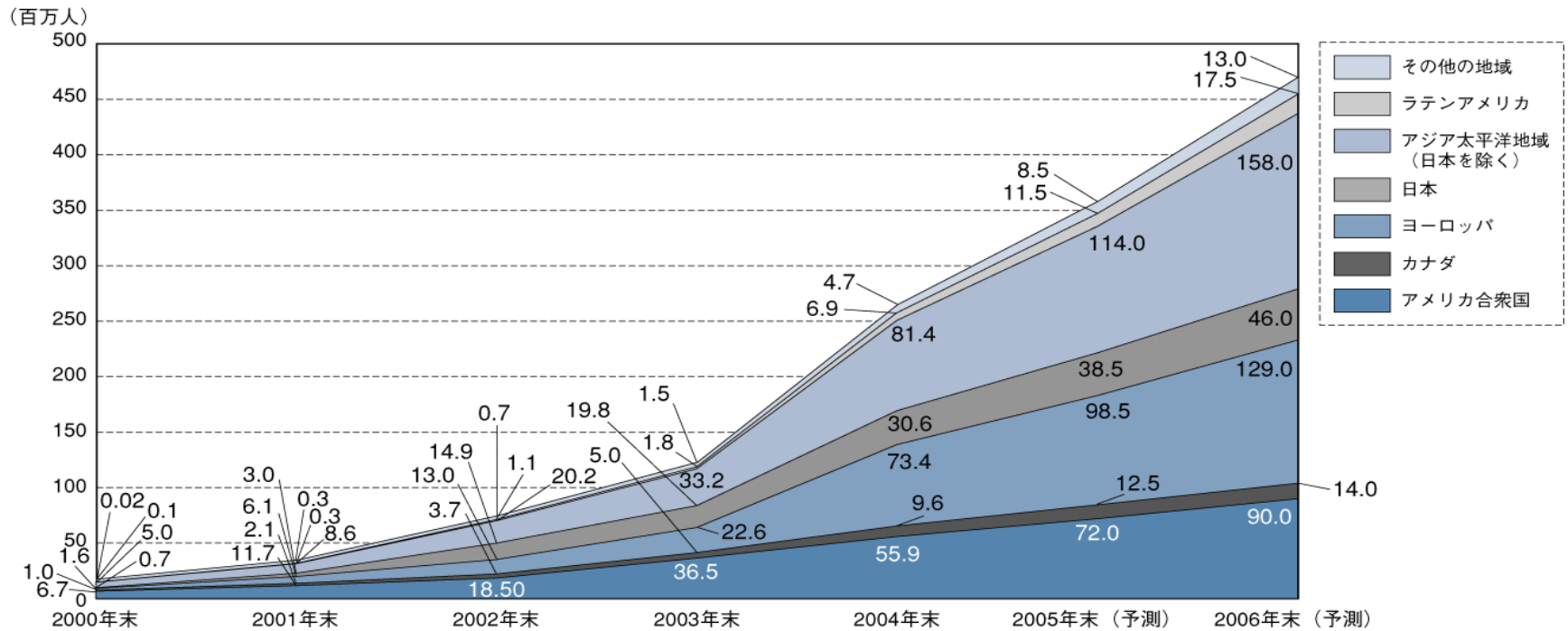


インターネット白書2005　©Access Media/impress,2005

世界の地域別ブロードバンド利用者数推移と予測

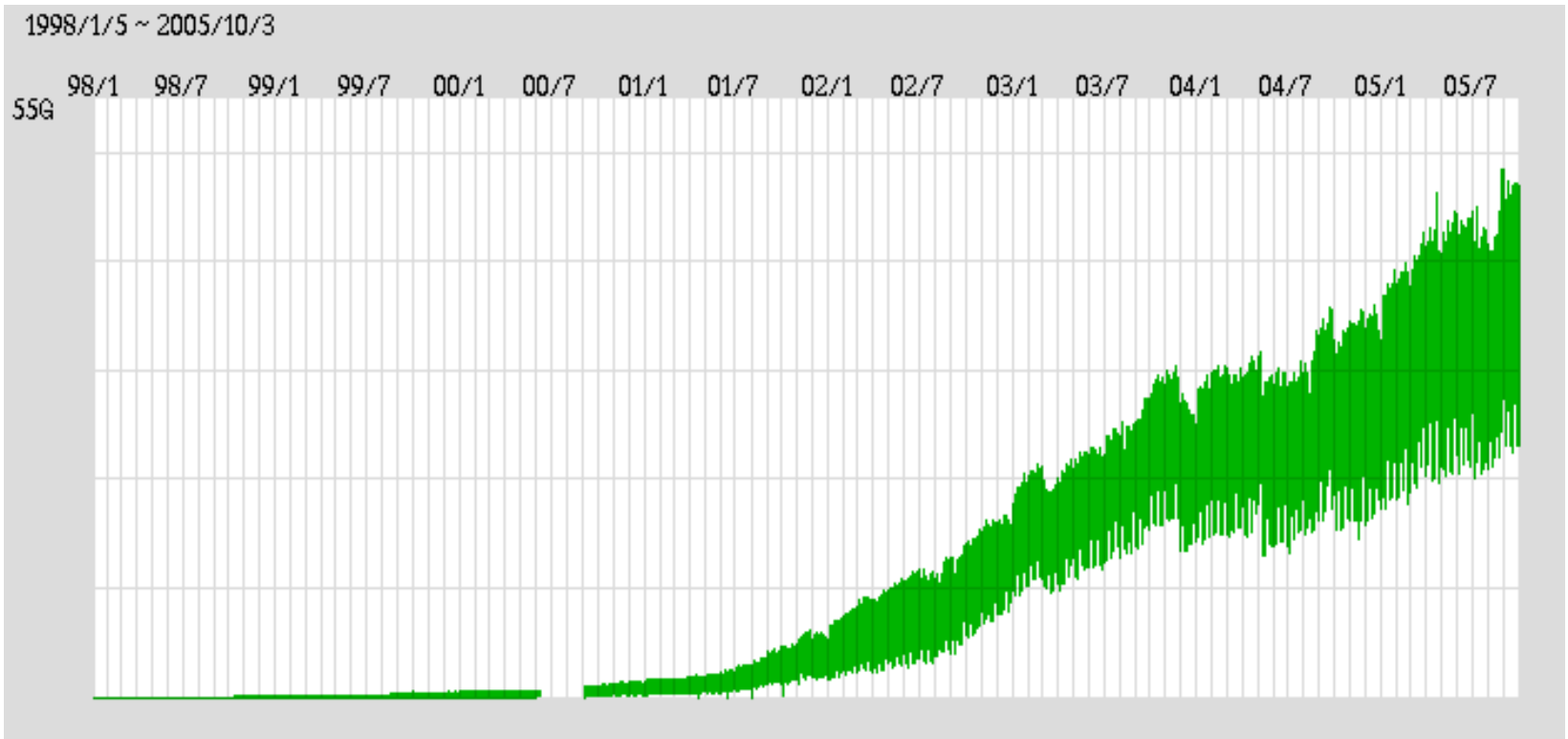
2004年末にアジア太平洋地域で3億を突破

資料7-1-7　世界の地域別　ブロードバンド利用者数推移と予測（2000年－2006年）



インターネット白書2005　©Access Media International,2005

JPIX Backplane Max/Min トラフィックボリューム



出所：JPIX

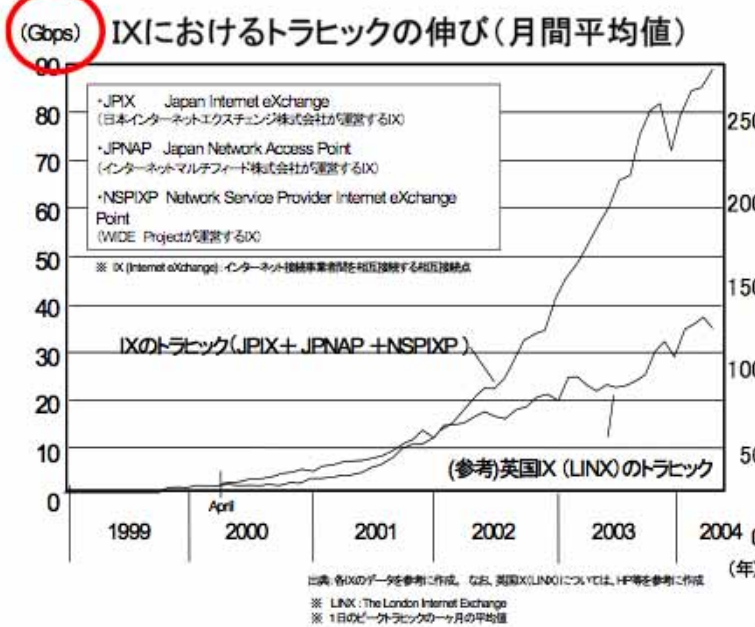
1．現時点で把握できているトラヒック情報

MIC

(1) インターネットについては、**把握可能なトラヒック情報が極端に少ない**のが実情（インターネットはまさにweb＜クモ＞の中の世界）。

(2) 現時点で継続的に把握することができるのは、主要なIXにおけるトラヒック情報のみ。

(3) 次世代IPインフラ研究会の**第一次報告書で把握することができたのも**、「トラヒックそのもの」ではなく、トラヒック交換のために用意されている回線の「容量」（ISP14社ベース）。



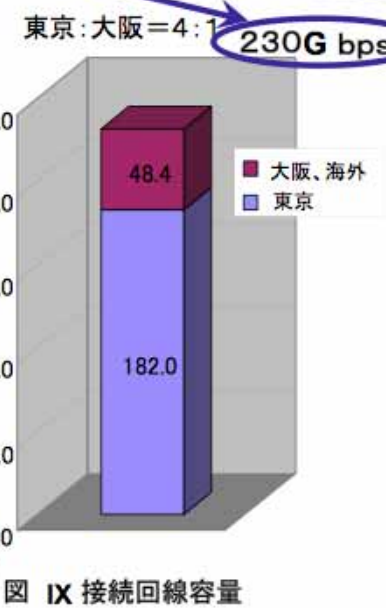


図 IX 接続回線容量

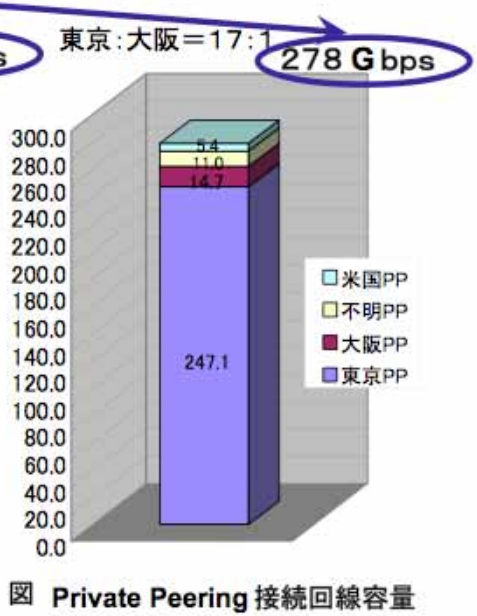
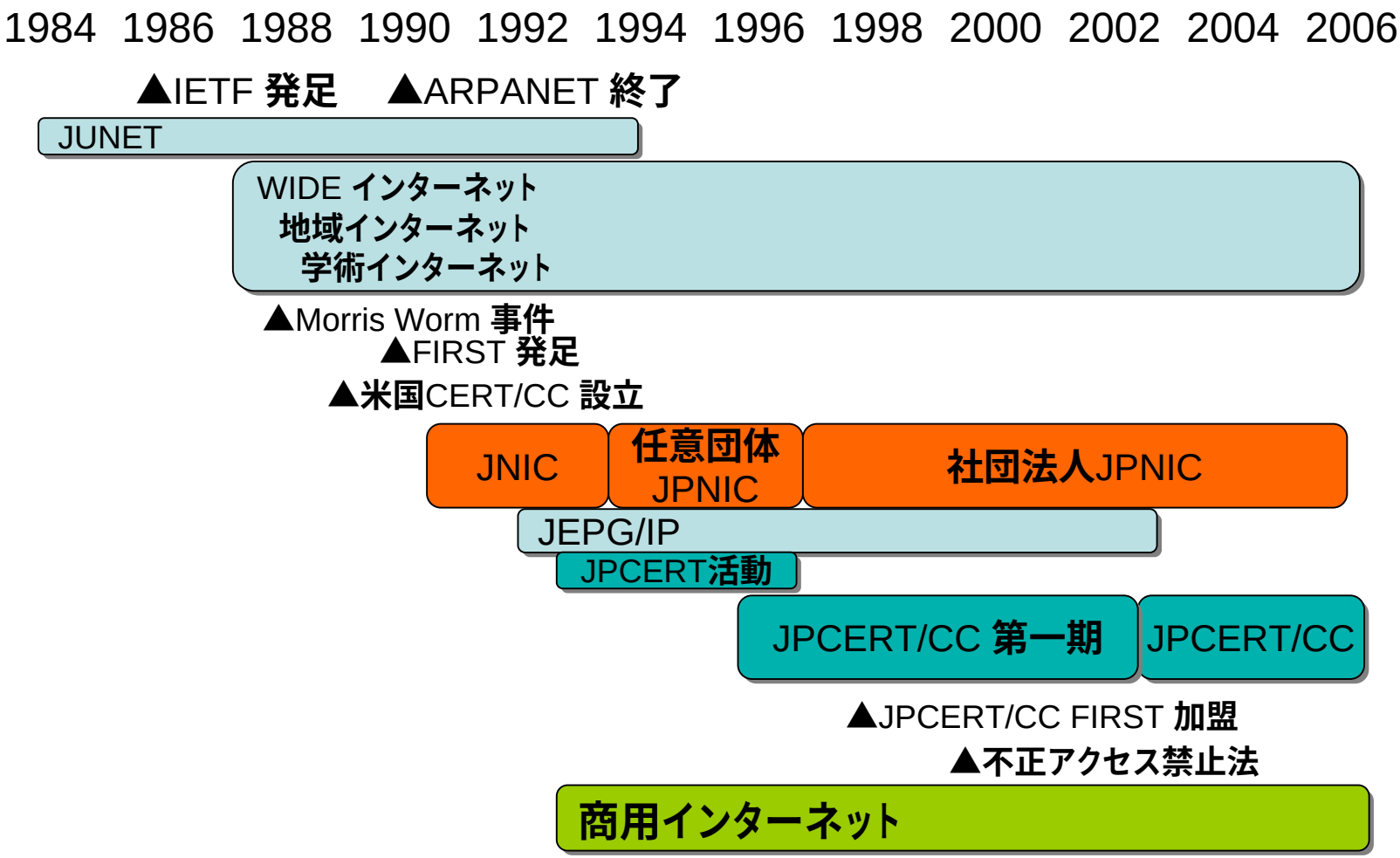


図 Private Peering 接続回線容量

peering：ＩＳＰ間でお互いに相手方ＩＳＰ宛てのトラヒックを交換し合うこと。一般的には無償接続。IXで行われるpeeringをpublic peering、IXを介さないpeeringをprivate peeringという。

JP・NIC & JPCERT/CC


1984 1986 1988 1990 1992 1994 1996 1998 2000 2002 2004 2006
▲IETF 発足
▲ARPANET 終了
JUNET
WIDE インターネット
地域インターネット
学術インターネット
▲Morris Worm 事件
▲FIRST 発足
▲米国CERT/CC 設立
JNIC
任意団体 JPNIC
社団法人JPNIC
JEPG/IP
JPCERT活動
JPCERT/CC 第一期
JPCERT/CC
▲JPCERT/CC FIRST 加盟
▲不正アクセス禁止法
商用インターネット

JPNIC

- 正式名称
  - 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
- 何をしているところ？
  - ネットワーク資源の管理業務、インターネットに係わる各種の調査・研究や教育・啓発活動など

JPNIC発足の経緯

1980年代	有志によるボランタリーな努力
1991年	JPNIC の前身となる JNIC 発足
1993年	任意団体 日本ネットワークインフォメーションセンター（JPNIC)設立
1997年	インターネットの急速な普及を底辺から支える活動を4年継続後、科学技術庁、文部省、通商産業省、郵政省の共管により社団法人となる
2001年	総務省、文部科学省、経済産業省の共管
2002年	JPドメイン名登録管理業務を（株）日本レジストリサービス(JPRS)へ移管

事業内容

JPNICは2つの事業を柱としています

IPアドレス事業

・IPアドレス資源管理

・ルール作り

IPアドレス事業を行うと共に、レジストリとしてインターネットの基盤整備に関わる事業(インターネットの普及啓発を目的としたセミナーやシンポジウムの 開催・インターネットセキュリティの普及啓発・インターネットセキュリティの調査研究・DNS及びその利用技術の調査研究等)を行っています。

インターネット基盤事業

・技術開発

・イベント・講演会の実施

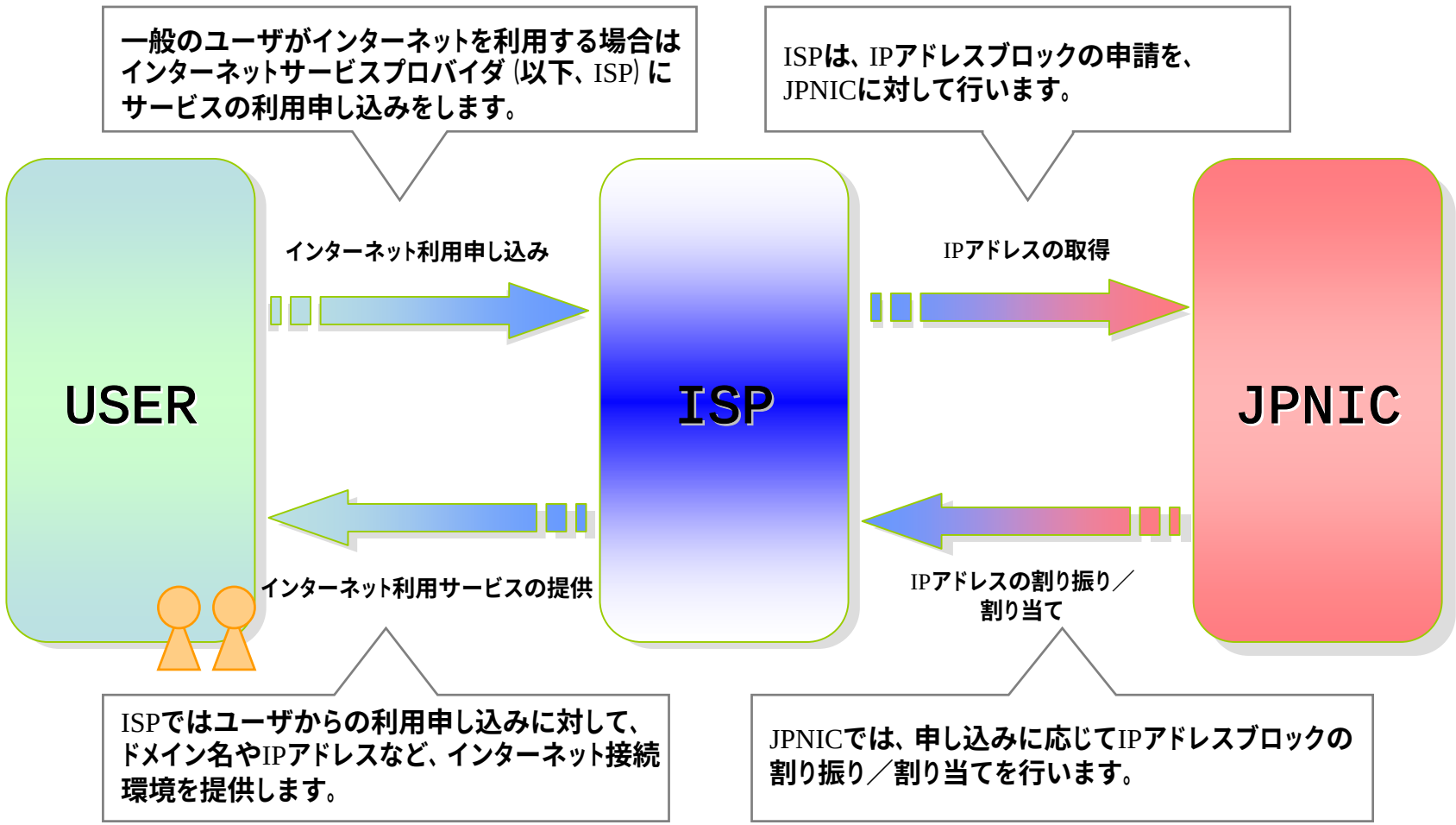
・会報誌発行

・情報収集・提供

・国際活動

・JPドメイン名のポリシ提案

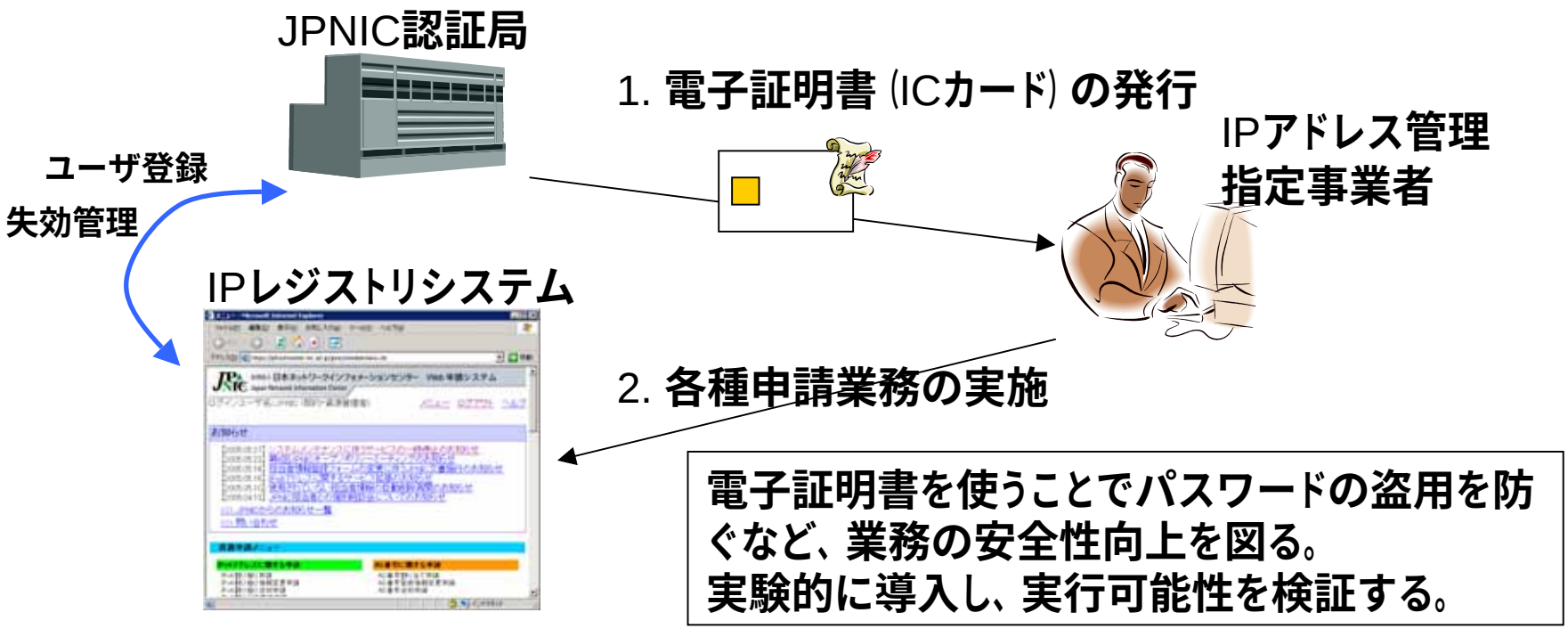
ユーザから見たJPNIC・ISPとのかかわり



インターネットセキュリティの普及・啓発

- JPNIC・JPCERT/CCセキュリティセミナー開催
  - 有限責任中間法人ＪＰＣＥＲＴコーディネーションセンターとの共催で、2003年度から開始。今年3年目
  - 安定したインターネットオペレーションの維持を目的に
  - ネットワークオペレータを対象に
  - ネットワークセキュリティに関するニッチな内容のセミナー
  - 今年の工夫
    - 地方開催版を行うこととした
  - プログラム
    - サーバアプリケーションセキュリティ(10月開催)
    - 知っておくべき不正アクセス対策　in 大阪(10月開催予定)
    - 知っておくべき不正アクセス対策　in 札幌(11月開催予定)
  - http://www.nic.ad.jp/security-seminar/

セキュリティに関する調査研究(1)
IPアドレス認証局の運用



電子証明書を使うことでパスワードの盗用を防ぐなど、業務の安全性向上を図る。
実験的に導入し、実行可能性を検証する。

セキュリティに関する調査研究(2)
インターネットレジストリのセキュリティに関する調査研究

- ルーティングのセキュリティ
  - ISPなどのネットワーク同士を世界規模で繋ぐ為、ルータと呼ばれる機器を使って行われている「経路情報の交換」のセキュリティに関する調査研究です。
    JPIRRで登録された情報を元に（ISPなどに）ネットワークの運用をしてもらうことで間違いを防ぐ仕組みや、ルーティングで使われる通信技術の中で電子的な認証を行う仕組みなどについて、調査研究を行っています。
  - JPIRRとは
    - 経路情報の登録サービスで、インターネットの経路の管理に使われる。
      JPIRRは、JPNICで運用されているInternet Routing Registryの意味。
    - ルーティングにおける電子認証の実施によって、インターネットからプロバイダごと切り離すようなテロ行為を難しくできる。（認証強化）

セキュリティに関する調査研究(3)
認証技術に関する調査研究

- **電子認証フレームワークに関する調査研究**
  - 2005**年度から始まった経済産業省からの受託調査研究**
- **電子証明書の技術**PKI (Public-Key Infrastructure) **を利用するための実用的な方法は、まだ解明されていないことが多い。**JPNIC**における**IP**アドレス認証局の調査研究活動を生かし、電子認証の実用面のドキュメント化を進めるための調査研究。**

DNSの運用技術の蓄積

- DNSの運用技術に関する調査・研究
  - DNSの安定的な運用のための技術開発
    （DNS運用健全化タスクフォース：DNSQC-TF）
    http://www.nic.ad.jp/ja/newsletter/No24/063.html
- DNSの運用技術の蓄積
  - DNSに関する新しい利用技術の調査・研究
  - ENUM(ENUM研究グループ・ENUM Trial JAPAN)
  - デイレクトリ技術
- その他インターネットの基盤整備
  - VoIP/SIPの相互接続(VoIP/SIP相互接続タスクフォース)

JPNIC · JPCERT/CC Security Seminar 2005
JPNIC · JPCERT/CC Security Seminar 2005
JPNIC · JPCERT/CC Security Seminar 2005

JPCERT/CC

CSIRT の分類
http://www.cert.org/csirts/csirt_faq.html

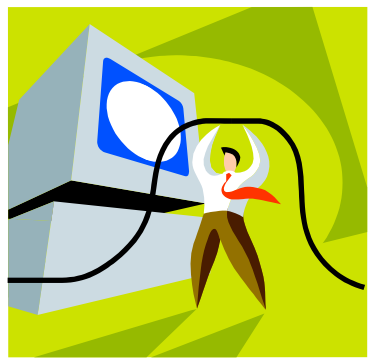
- constituencyと呼ばれるサービス対象によって分類
  - Internal CSIRTs
    - 自組織や顧客が関わるインシデントに対応
  - National CSIRTs
    - national = 地域のコンタクトポイント
  - Coordination Centers
  - Analysis Centers
  - Vendor Teams
    - 自社製品の脆弱性について対応
  - Incident Response Providers
    - いわゆる「セキュリティベンダ」

JPCERT/CC**業務内容**

Japan Computer Emergency Response Team Coordination Center

ジェーピーサートコーディネーションセンター

- **インターネットを介して発生する侵入やサービス妨害等の**
- **コンピュータセキュリティインシデント*に関する以下のサービスを**
- **技術的な立場から行っている組織です。**
  - **インシデント関連情報の窓口対応および対応支援**
    - **インシデントハンドリング**
    - **脆弱性情報ハンドリング**
  - **国内向け技術情報の配信**
    - **注意喚起、調査結果、その他**
    - **インターネット定点観測システム** (ISDAS)
  - **セキュリティインシデント対応体制の強化**
    - **国内外の関連組織との連携および協業**



*** コンピュータセキュリティに関係する人為的事象で、意図的及び偶発的なもの**

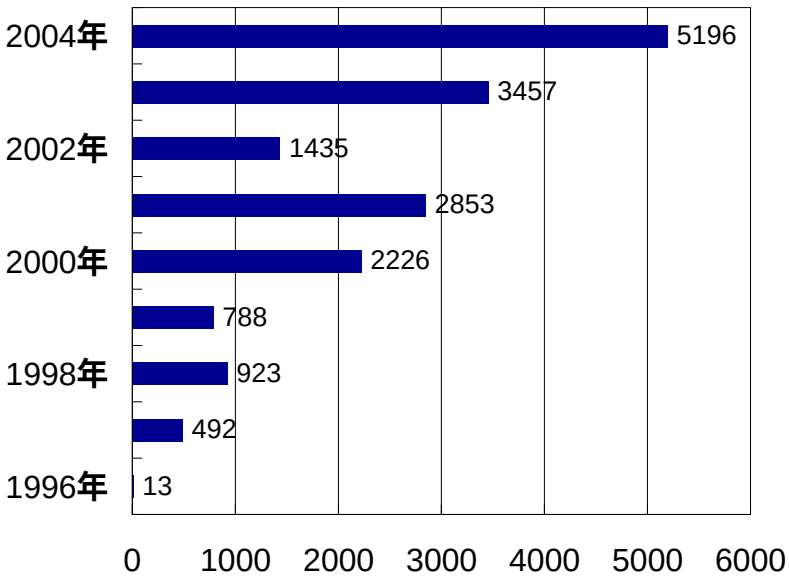
インシデントハンドリング

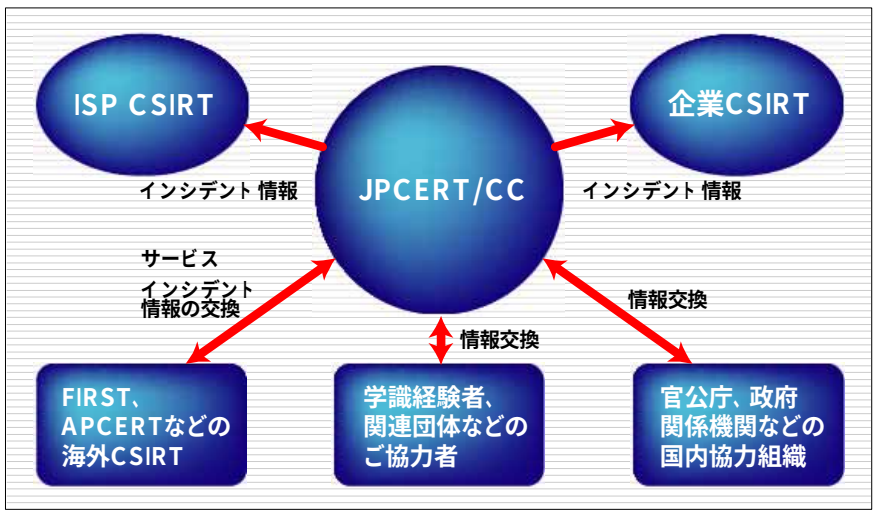
「CSIRT of CSIRTs」

CSIRT (Computer Security Incident Response Team) 間の連携をコーディネート

1. インシデントレスポンスの時間短縮による被害最小化
2. 再発防止に向けた関係各機関の情報交換および情報共有

インシデント報告件数の推移



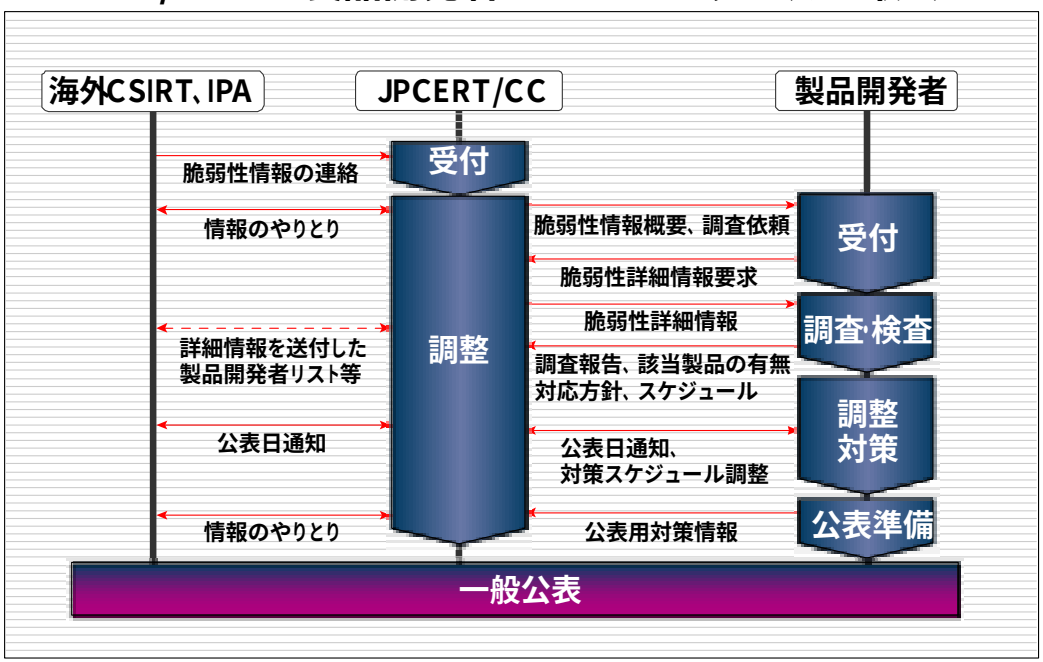


脆弱性情報ハンドリング

「ソフトウェア等脆弱性関連情報取扱い基準」(2004年7月経産省公告) 認定調整機関
対応支援と情報公開業務

1. 登録開発ベンダ向けに、脆弱性関連情報を提供し対応依頼
2. 国際的に情報公開日を調整

JPCERT/CCとの製品開発者のハンドリング　(やり取り) フロー図



情報提供サイト
JVN (JP Vendor Status Notes)

JVN JP Vendor Status Notes

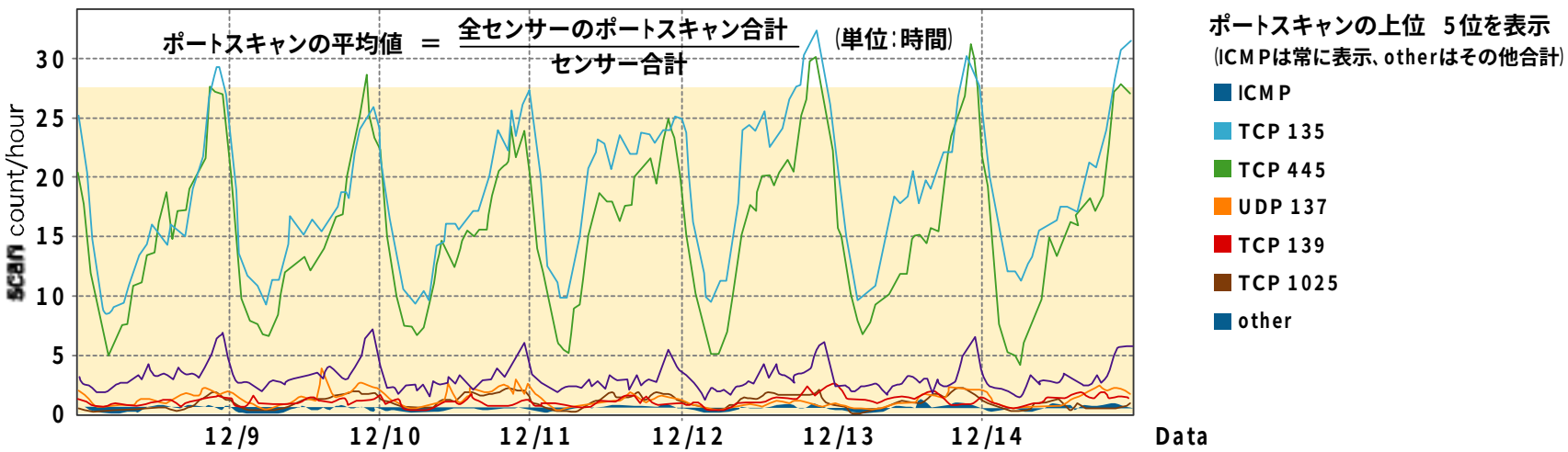
http://jvn.jp/

インターネット定点観測システムの運用

ISDAS：Internet Scan Data Acquisition System（http://www.jpcert.or.jp/isdas/）

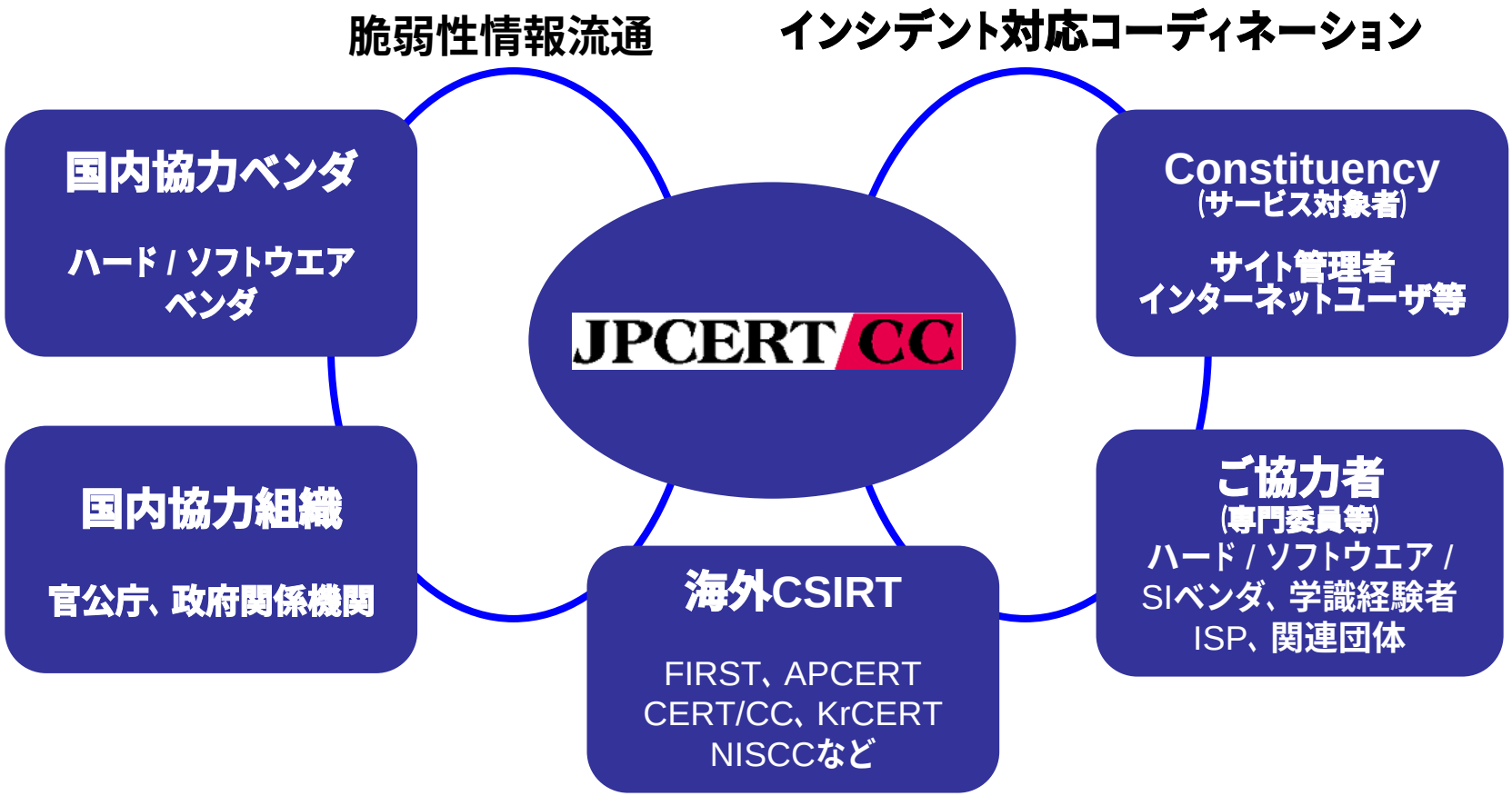
インシデントの早期把握のための観測および情報提供

1. **定期的なセキュリティ予防情報の提供**
2. **異なる監視・観測アプローチをとる定点観測および広域モニタリング間での情報共有により精度の高い情報共有**
   （IPA、Telecom-ISAC、@police、WCLSCANなど）



国内外の関連組織との連携

CSIRTとして日本で最初にFIRST (Forum of Incident Response and Security Teams) に加盟
重層的な協力関係の拡充による、最新技術動向の共有と、経営層に対する啓蒙活動



JPCERTの今後の事業展開

インシデント予防専門の社内組織「早期警戒グループ」発足
事後対応の継続と、未然防止の強化

	1996～	2003～	2004～	2005～
インシデント発生前の予防				**早期警戒** 情報配信サービス セキュリティ演習
リアルタイム状況把握			**脆弱性情報ハンドリング** プライオリティの仕様作成	
			定点観測 新観測システム（JPCERT/Telecom-ISAC）	
インシデント発生後		**インシデントハンドリング**		

NISC
重要インフラ事業者
(通信、電気、鉄道、空港)

@Police
WCLSCAN
Telecom-ISAC Japan
北陸先端科学大学院大学 (JAIST)
2地域間個別連携
オーストラリア、韓国、中国
SOC事業者連携・連絡会

Abuse**担当連携** (ISP、XSP)
Who is DB (JPNIC、JPRS)
ボットネット対応
(Telecom-ISAC、AVV、SOC事業者)

製品開発ベンダ (仮登録XX社)
オープンソースコミュニティ
情報共有スキーム
(1) 早期警戒パートナーシップ (IPA)
(2) 国際パートナーシップ
(NISCC、CERT/CC)

FIRST (*)
APCERT (*)
eCSIRT (*)
2地域間個別協定
米国 (CERT/CC)
韓国 (Kr CERT)
中国 (CN CERT)

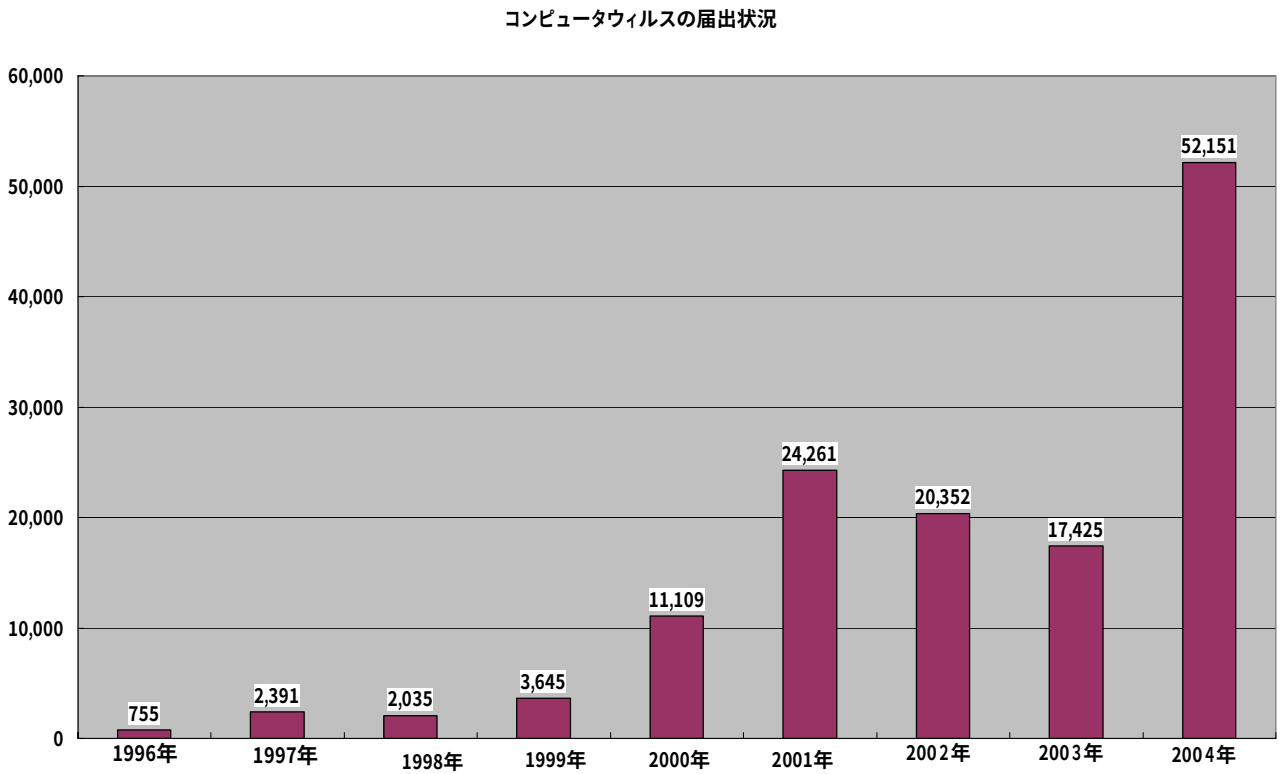
JPCERT/CCとインターネット動向の10年

	1996年	2002年	2005年
JPCERT/CC社員数	5人	13人	26人
JPCERT/CCオフィス面積	50坪	50坪	110坪
JPCERT/CC業務内容	インシデント対応 国際連携	インシデント対応 国際連携 定点観測・分析	インシデント対応 国際連携 定点観測・分析 脆弱性情報対応(2004年) 早期警戒対応
インターネット利用者数（日本）	571.8万人(1997年2月)	4,619.6万人(2002年2月)	7,007.2万人(2005年2月)
インターネット利用者数（US）	6470万人(1998年末)	16,500万人(2002年末)	19,050万人(2005年末予測)
ブロードバンド伸び率（日本）	—	1,300万人(2002年末)	3,850万人(2005年末予測)
ブロードバンド伸び率（US）	—	1,850万人(2002年末)	7,200万人(2005年末予測)
コンピュータウィルスの届出	755件	20,352件	52,151件（2004年）
IX Backplane Max/Min トラフィックボリューム			

出所：Access Media/impress2005、AccessMedia International,2005、IPA「ウィルス届出状況」

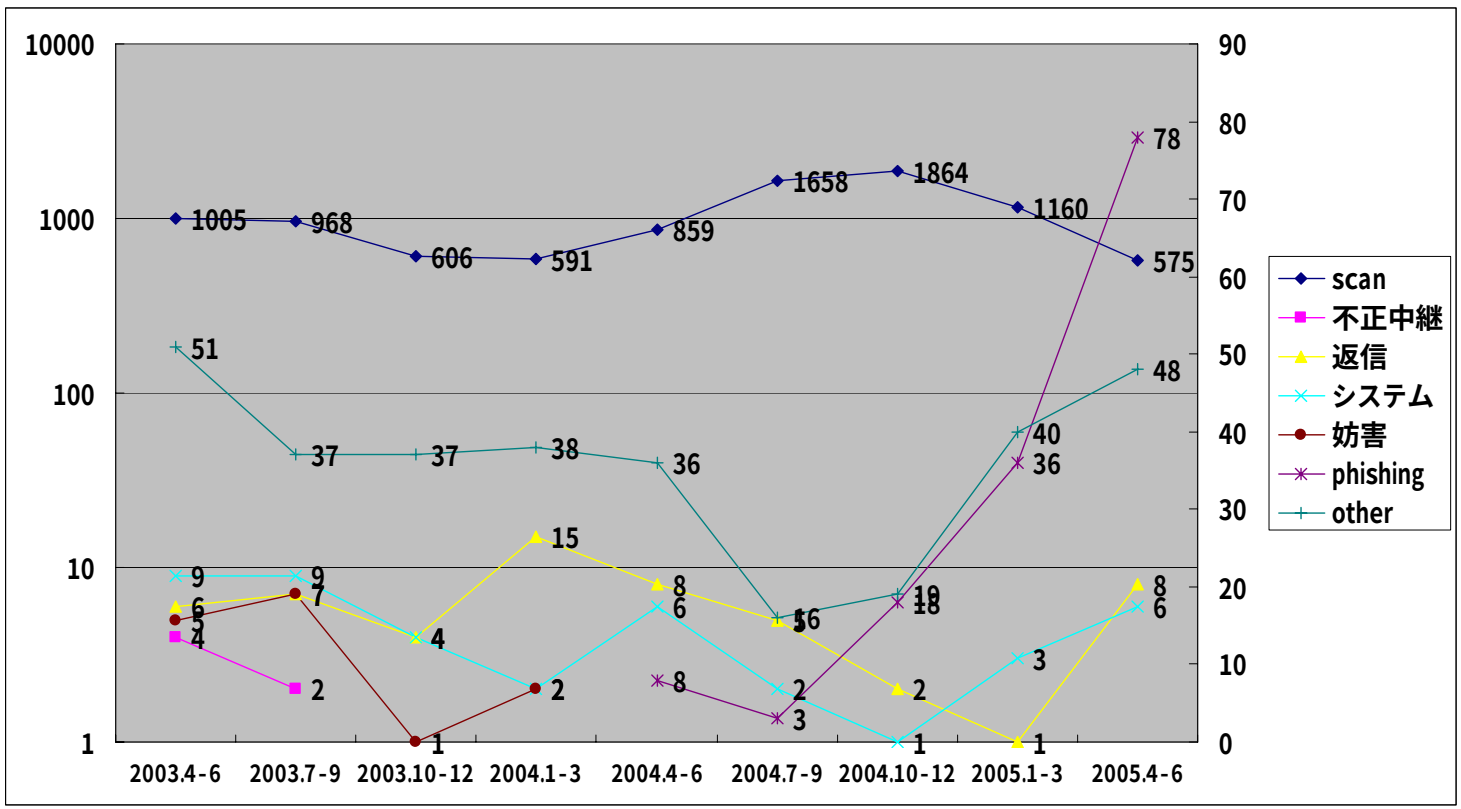
セキュリティ状況の変化

コンピュータウィルスの届出状況

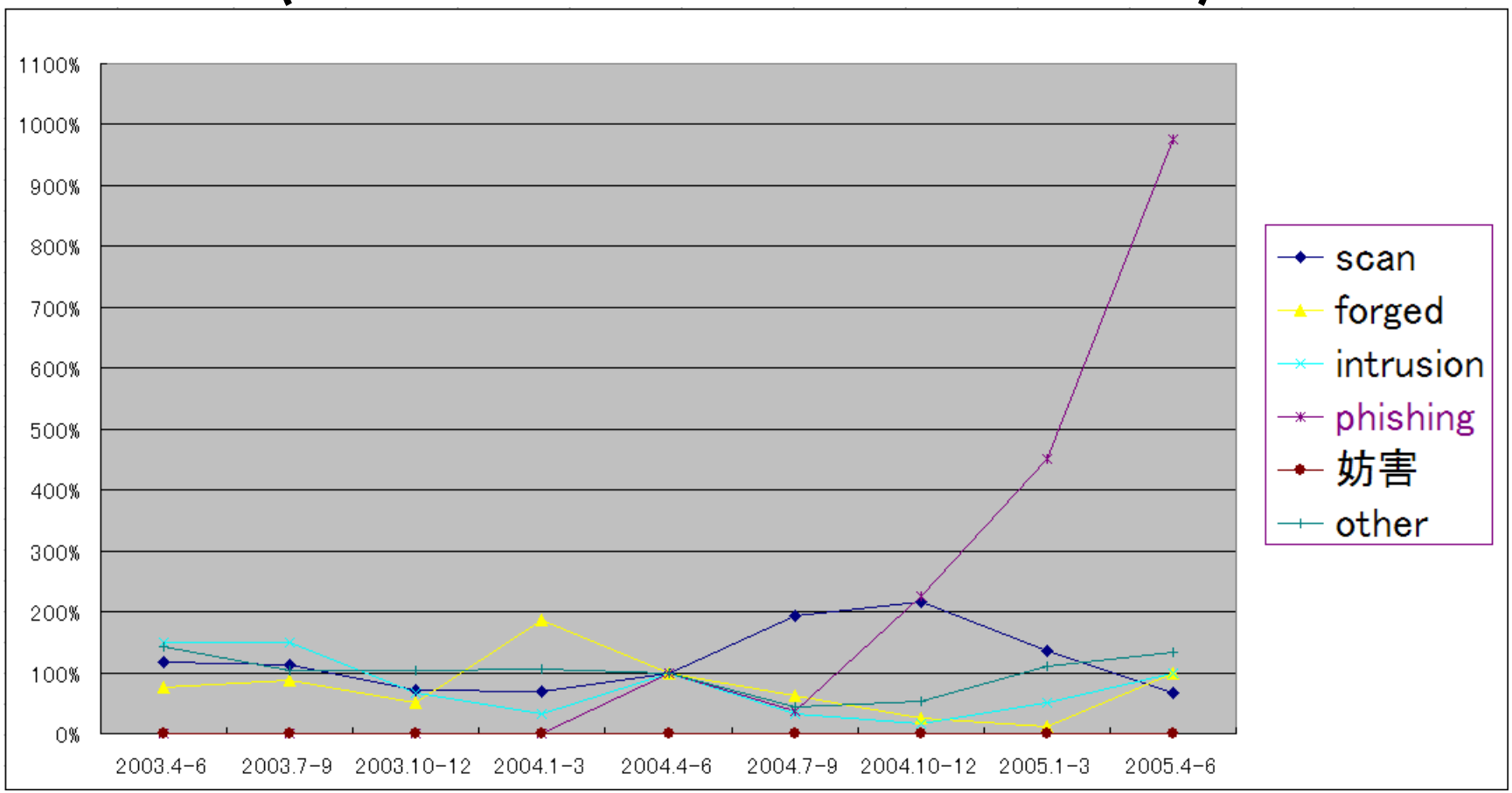


出所 IPA[2004年]ウィルス届出状況

インシデント報告件数の推移
(件数)



インシデント報告件数の推移
(2004年4-6月を100%とした変化率)



JPNIC · JPCERT/CC Security Seminar 2005
JPNIC · JPCERT/CC Security Seminar 2005
JPNIC · JPCERT/CC Security Seminar 2005

Thank you