# セキュリティ対策の実際

名古屋大学情報連携基盤センター
大規模計算支援環境研究部門
長谷川　明生

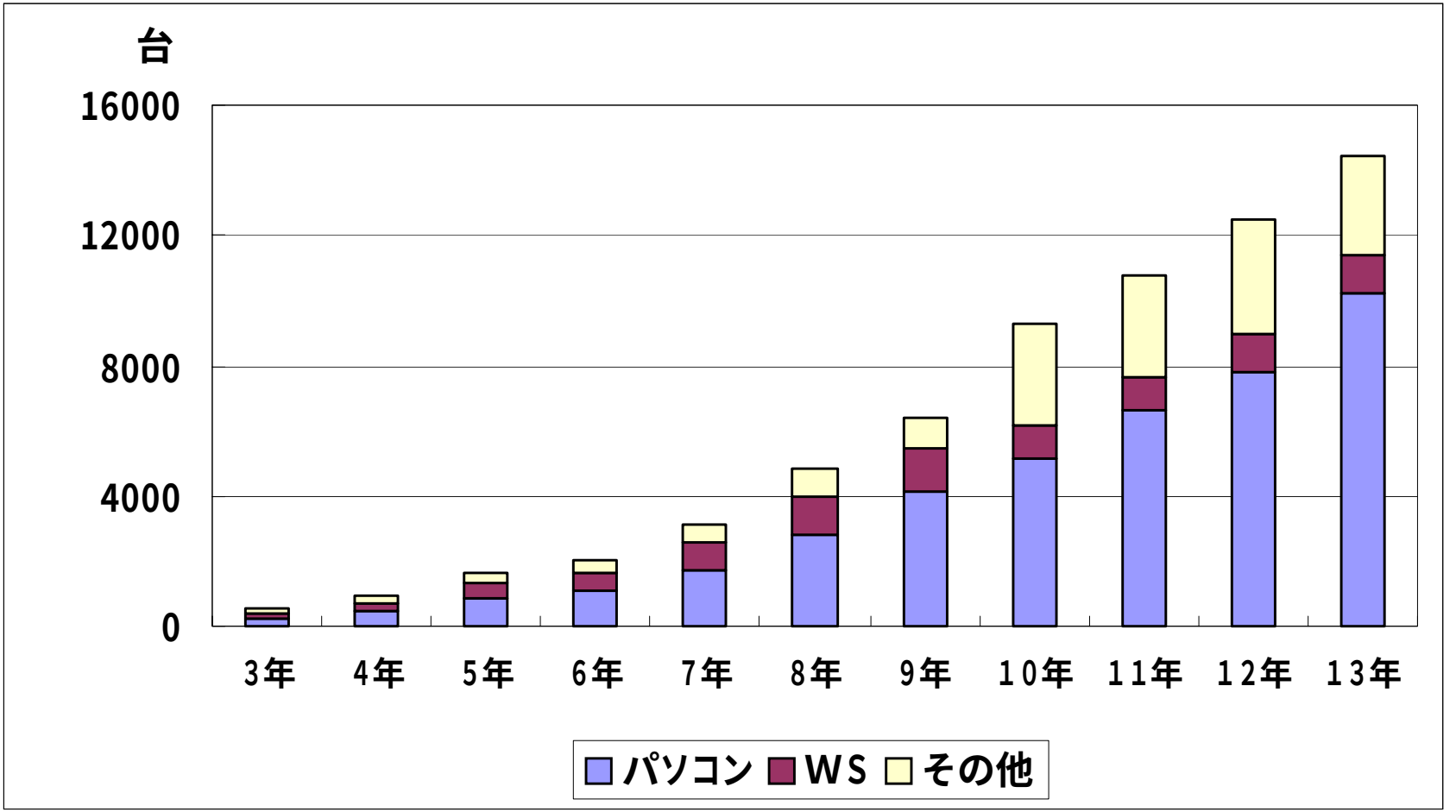
# 今日の話題

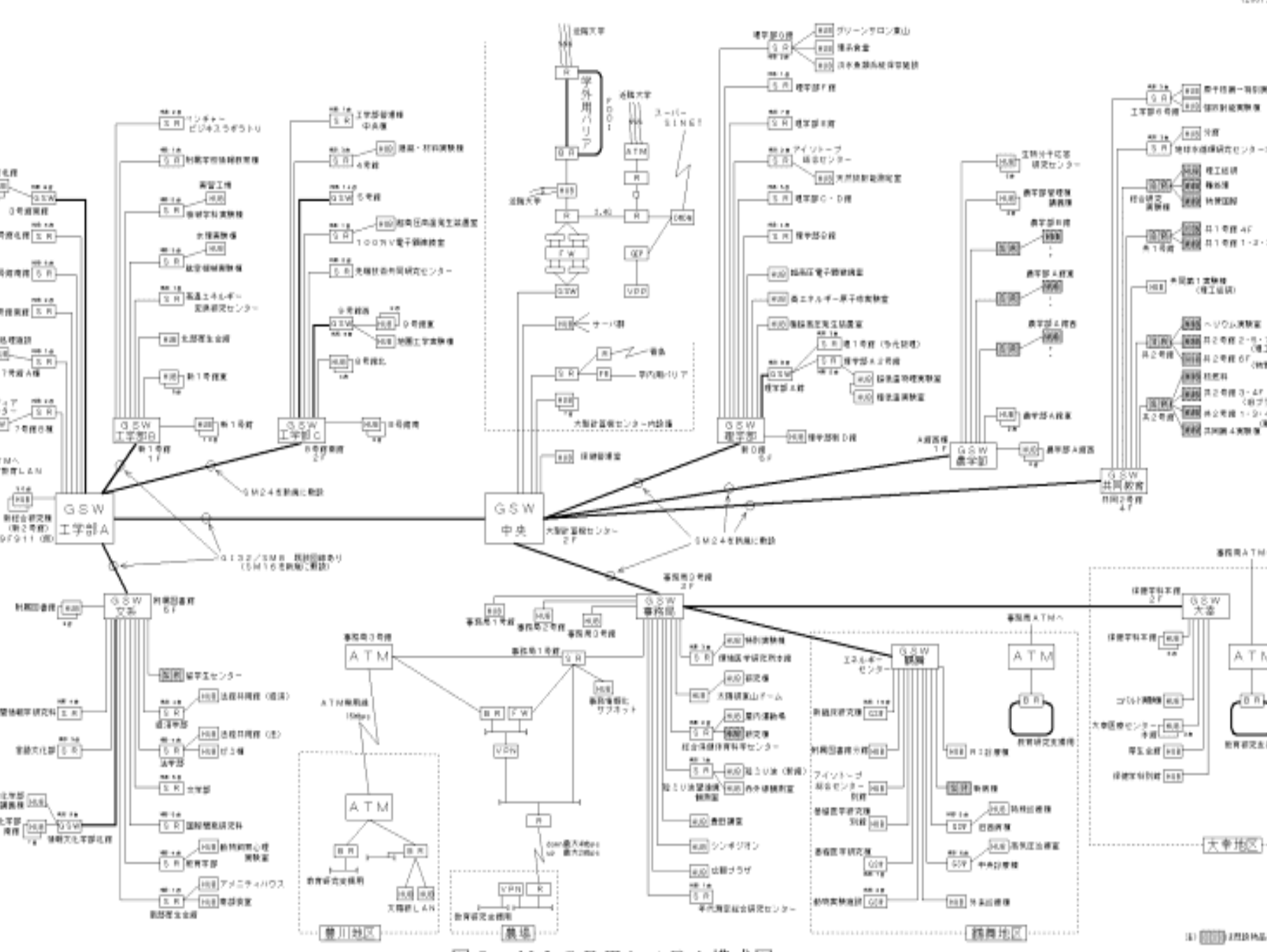
- 学内LANの現状紹介
- IDSのログに見る脅威の分析
- IDSやファイアウォールの設計と問題
- 運用上の問題点
- 問題点の解決のために
  - セキュリティポリシや管理体制
- まとめ

# 学内LANの現状

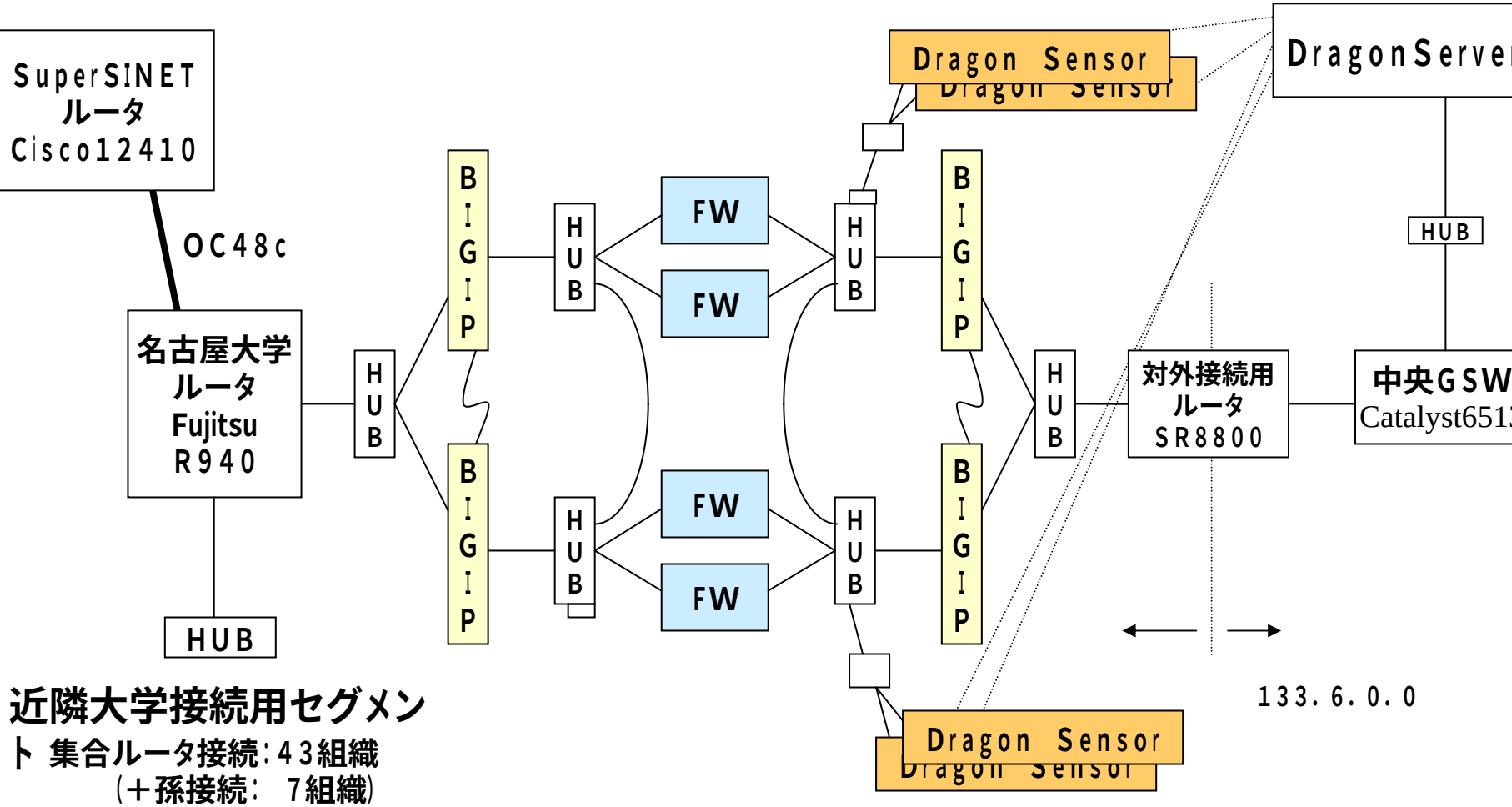
- **端末数　約17，000**
- NICE　III　（10GbE，GbE,FastEther）
- **セキュリティ関連**
  - FireWall-1＋Big-IP
  - Dragon　IDS

# 端末接続数の変化


台
16000
12000
8000
4000
0
3年
4年
5年
6年
7年
8年
9年
10年
11年
12年
13年
パソコン
WS
その他


学外用バリア
スーパーSINET
GSW 工学部A
GSW 工学部B
GSW 工学部C
GSW 中央
GSW 理学部
GSW 農学部
GSW 共同教育
GSW 文系
GSW 事務局
GSW 講義
GSW 大幸
ATM
SM24を新規に敷設
G132/SM8 既設回線あり (SM16を新規に敷設)
富山地区
奥田地区
大幸地区
農場

# 名古屋大学対外接続の構成



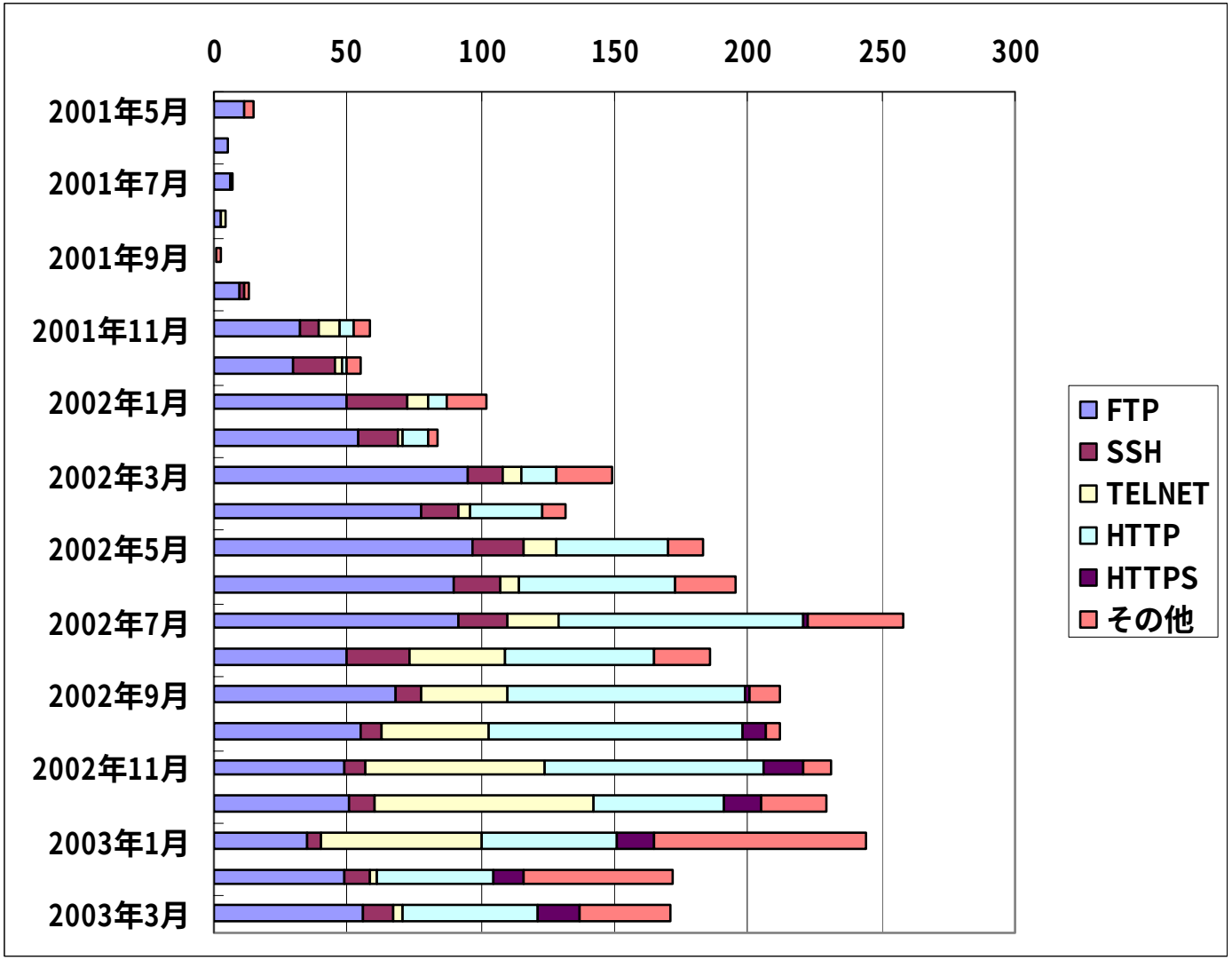

近隣大学接続用セグメント
集合ルータ接続: 43組織
(＋孫接続: 7組織)
ルータ持ち込み: 5組織

# 負荷分散装置（BIG－IP）

# ファイアウォール

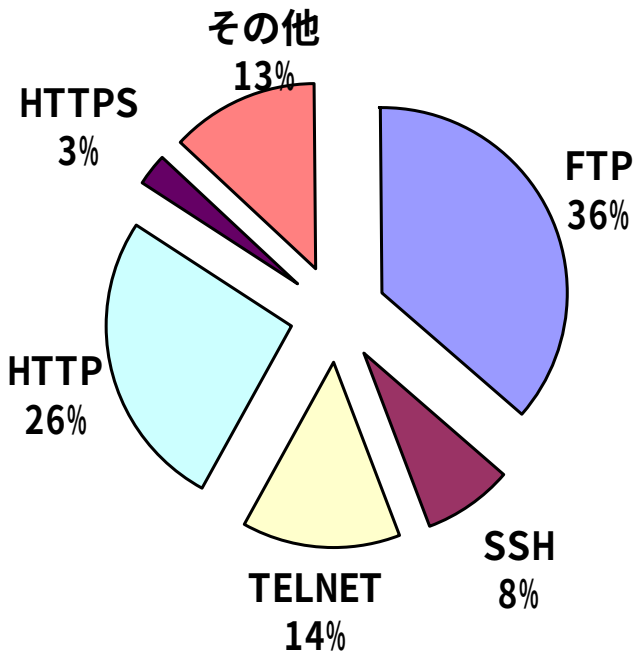
# IDSシステム

# ホストスキャン件数の推移



# プロトコル別割合

## プロトコル別割合（2001年5月～2003年3月）



# ワームの動向

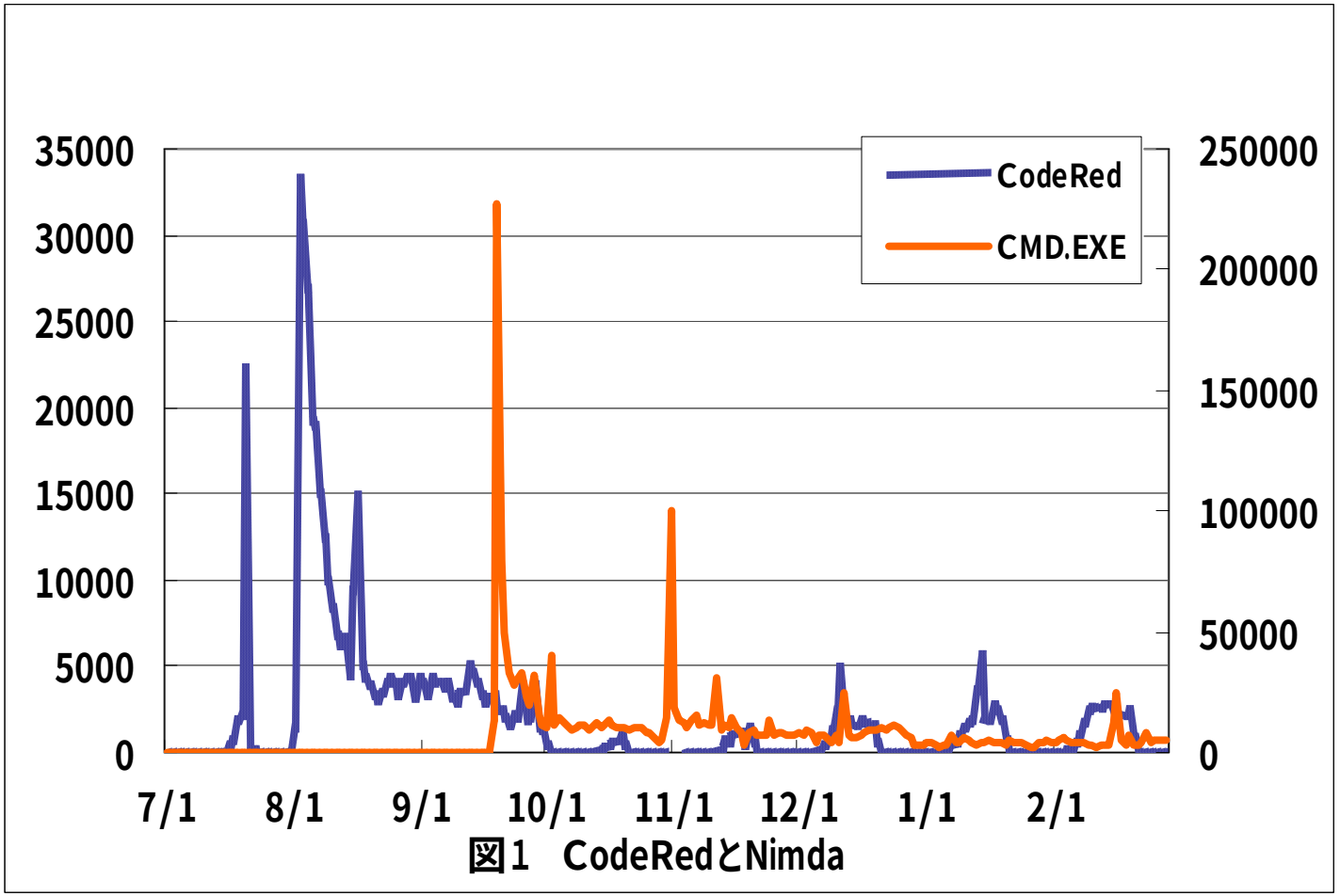



図1　CodeRedとNimda

# クラッキングの発生例

- CGIスクリプトによるパスワードファイル取得
- FTPサーバの不備によるルート権限奪取
- statdのバッファオーバーフロー (Solrais)
- IISのバグによるWebの改ざん、不正侵入
- OpenSSHのCRCコードのバッファオーバーフロー
- OpenSSLのバッファオーバーフロー
- telnetdオプションのバッファオーバーフロー
- Windows　SQLサーバのバグ攻撃
- Windowsのバグによるウィルス感染 (Nimda等)

# IDSからわかること

- 攻撃には，流行がある。古典的なものは常に存在する．
- スキャンと攻撃件数は比例しない．
  - ピンポイントの攻撃が増加している．購入直後の侵入の増加
- 攻撃ツールのネットを通した急速な拡散
- ステルスが増加している．
- ADSLやCATV常時接続が踏み台の温床

# ホストスキャン、攻撃の傾向

- ホストスキャン件数の増加
- SSLへの攻撃が急増
- スキャンと攻撃ホストの分散化
- 見慣れないポートへのスキャン
  - （例　17300/TCP)
- DDoSツール、SPAMツールの普及
- rootkitの普及
- Warezの増加
- ネットプリンタや無線アクセスポイントのWeb設定

# IDSからわかる問題

1. OSの保守がなされていない.
   - パッチの不足
2. 利用しないサービスの起動
3. だれでもアクセスできるアカウントが放置されている.
4. アクセス制限がない（Web設定、無線LAN）
5. セキュリティ情報に無頓着.
6. 問題サイトへのアクセスに無頓着.
7. 管理者が明確になっていない.

# 学生気質の変化による問題

- ハードウェアの損傷･盗難
  - キーボード、マウス、ディスク装置等
- ソフトウェアへのいたずら
  - .forwardに大量のアドレスを書く
  - 外部の掲示板やチャット荒し (高校生でも)
  - xxx.acドメイン取得によるwww.xxx.acを使ったイタズラWWWページ
- ネットワークの商業利用

# ネットワーク倫理問題

- 内外からの苦情の増加
  - メールマガジンへの無断登録
  - 架空名義による商品発注
  - インターネット・ダフ屋
  - チャットのトラブル
  - インターネット・ストーカー
  - 著作権無視（P2Pソフトウェアの普及）
- 内外からの個人攻撃
  - なりすましによるニセ投稿
  - インターネット・ストーカー
  - プライバシーの不当漏洩

# イントラネット神話の崩壊

- Nimdaは，あっさりファイアウォールを越えた．
  - メールやWWW閲覧に伴う問題は，完全には防御できないことを証明した．
- 内部に問題はないという前提は消えた．
  - ファイル共有や認証情報共有の問題
- よき隣人も幻想となった．
  - 問題メールは，知り合いから来る．

# セキュリティ対策とは

- セキュリティ対策はコンセンサス作り
  - コストと安全性
  - 利便性と安全性
- セキュリティポリシと組織体制
- 界面での対策＋個別セキュリティ

# 最低限のセキュリティ対策

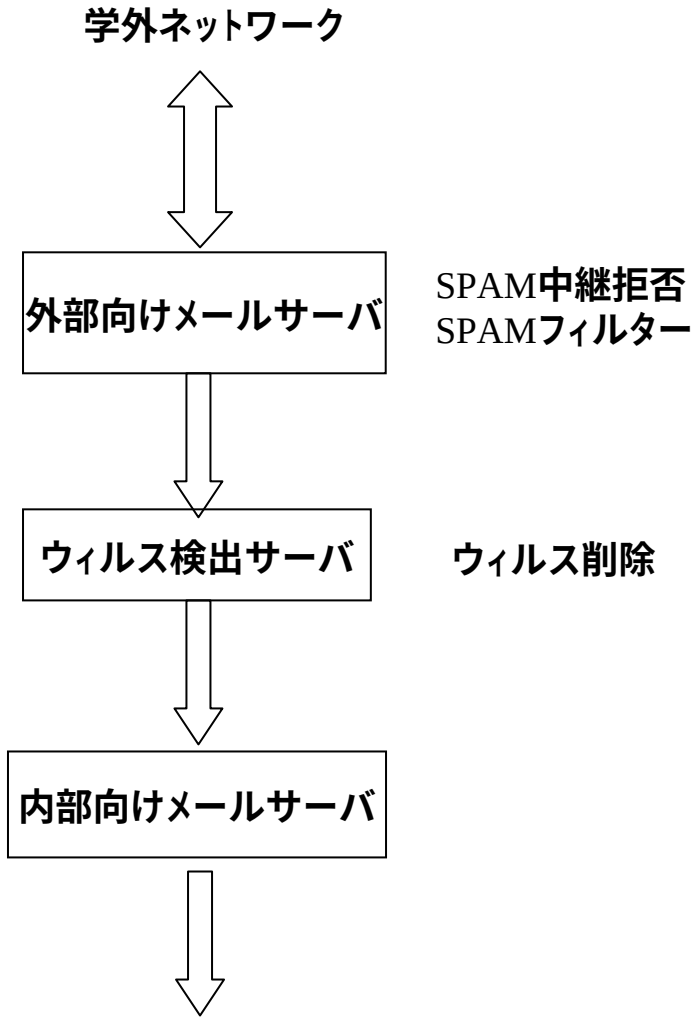
- 最低限の施錠は必要（建物の鍵と不法侵入監視）
  - ファイアウォール
  - 内外の監視＝IDS,MRTG
- ホストの日常管理（部屋の施錠）
  - 認証方式の監査
  - ソフトウェア監査
  - ログ監査
  - ファイルの統一性管理
  - ウィルスチェッカー、パーソナルファイアウォール
- 構成員の教育（防犯教育）

# ネットワークの問題

- 無認証のDHCP
- 無許可のバックドア
- 無許可もしくは信頼できないサイトとのVPN
- 無線LANの認証および暗号化
- 不適切なローカルアドレスの利用

# 現在のファイアウォール

- 高速化への対応ー＞負荷分散
- IDSとの連携
- パケットトレース
- 法律的問題（構成員への周知）




ウィルス検出とSPAM対策の併設例

# ホスト管理者のジレンマ

- 利便性と安全性
- コストと安全性
- 侵入されたことは証明できても，侵入されていないことの証明は不可能

# ホストの問題

- 設定の済んでいない装置の接続
- 不要なサービスの起動
- アクセス制限
- ファイル共有
- パスワード問題
- 物理的問題 (盗難等)

# 最低限のホスト管理

- **情報漏洩の防止**
  - named,finger,rwho,whois,portmapper
- **遠隔管理やファイル共有システムの防御**
  - SGI**の**WEB
  - sadmind,NIS,NFS,Windows**ファイル共有**
- **アクセス制限** (tcpd)
- **タイムリーなパッチ作業**

# 侵入検出のためのツール一覧

| 名前 | 機能 | 起動タイミング | 備考 |
|---|---|---|---|
| tcpd | アクセス制限，記録 | inetdから起動 | フリー |
| snort | 攻撃やスキャンの検出 | ブート時起動 | フリー |
| logsurfer | 自動ログ監視 | ブート時起動 | フリー |
| swatch | 自動ログ監視 | ブート時起動 | フリー |
| tripwire | ファイルの整合性の検査 | cronにより定期的に起動する. | ASRは教育機関にかぎりフリー |
| snoop | パケットモニタ | コマンド | Solarisコマンド |
| tcpdump | パケットモニタ | コマンド | フリー |
| sps | プロセス状態確認 | コマンド | フリー |
| top | 負荷の重いプロセスの表示 | コマンド | フリー |
| lsof | 開かれているファイルやソケットとプロセスの関係の表示 | コマンド | フリー |
| ifstatus/cpm | ネットワークインターフェースの状態確認 | コマンド | Solaris用フリー |
| find_ddos | trin等のDDoSツール検出 | コマンド | フリー，Linux,Solaris用 |
| chkrootkit | rootkit検出 | コマンド | フリー，Linux,Solaris用 |
| truss | プロセスの動作トレース | コマンド | システムコマンド |

# 侵入が発見された場合

- 不必要な情報漏洩の防止
- ログの確保
- 侵入経路の確認と影響範囲の確認･連絡
- ネットワークからの切断
- ファイルバックアップ
- クリーンメディアからの再インストール
- 全IDとパスワードの変更
- ファイルの復元

# 侵入を発見した場合の対応

- 組織内への連絡･報告
  - 被害拡大の防止
  - セキュリティガイドラインを参考
- JPCERTやIPA等への報告
  - 被害拡大の防止
- 警察に被害を届けるかどうか？
  - 踏み台にされた場合には防衛的措置として考慮する.

# 管理体制の問題

- 24時間，365日面倒が見られるか？
- システム管理は，学生や一部教官のサービス
  - 権限と責任の所在があいまい
  - 技術レベルが平均していない
- 統一的ポリシがないー＞名古屋大学セキュリティポリシーとガイドラインの策定
- 対外窓口がない
  - 社会的問題（マスコミ，警察）
  - 法律的問題（損害賠償等々）

# その他のセキュリティ対策

- **Norton UntiVirus Corporate Ed.**
  - **4000ライセンス**
- Snort+Scram**によるサーバ監視**
- **tcpd＋ブービートラップ機能の利用**
  - **メールによる違反アクセスの監視**
- Macfee Interscan Virus Wall

# SPAM被害・加害対策

- Outlook等のフィルタ機能の活用
- SPAM対応ソフトウェアの導入
  - 例　bsfilter,bogofilter,spamassasin
- 侵入されない対策（加害防止）
  - タイムリーなパッチ
  - 異常検出やパーソナルファイアウォール

# セキュリティソフトウェア利用上の注意

- 重複インストールはトラブルのもと
  - 常駐型の同じような機能のセキュリティソフトウェアは、要注意
- 動かなくなるソフトウェアの存在
  - ファイル共有
  - サーバ・クライアント型ソフトウェア
- 可能ならログを保存

# まとめ

- ファイアウォールやIDSは補助対策
- 末端の端末管理が基本
  - アクセスの自由には，義務が付随している！
    （でも，すべての構成員がそうとは限らない．）