# セキュリティインシデントの現状とネットワーク環境におけるセキュリティ保全

すずきひろのぶ
hironobu@h2np.net



## 内容

- セキュリティインシデントの現状分析
  - ネットワーク構成
  - 過去１２ヶ月の分析から
  - CLSCANの紹介
  - WCLSCANの提案
- ネットワーク環境におけるセキュリティ保全

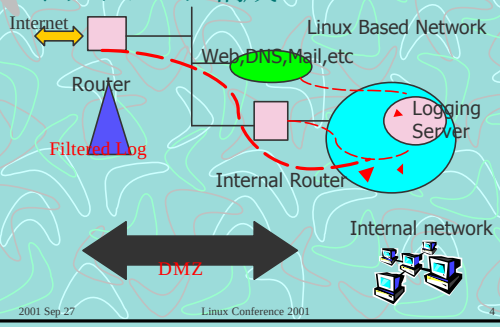


## ファイアウォールのログ

- インターネットとDMZを区切るルータによるIPフィルタリングのログ
- IPフィルタリングは最小のコストで最大の防御ができる
- ネットワーク空間を分割する役割を果たす



## ネットワーク構成



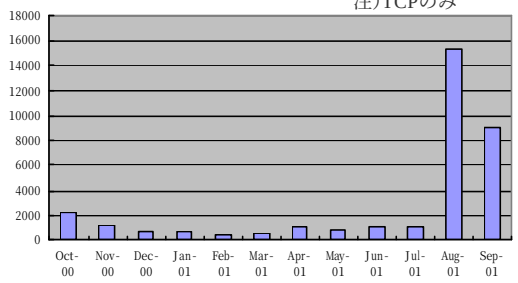
## 過去12ヶ月の記録

- 2000.10.9〜2001.9.23
- リジェクトされた接続
  - 210.145.219.248/29
  - 68ポート（TCPのみ）
  - 35106エントリ（TCPのみ）



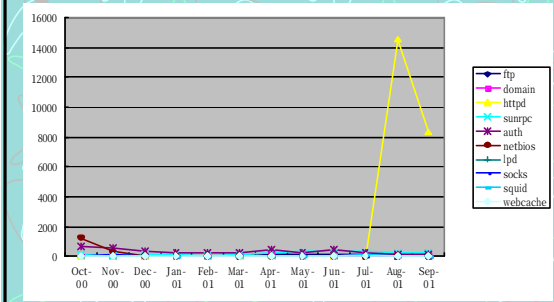
## 過去12ヶ月

注）TCPのみ



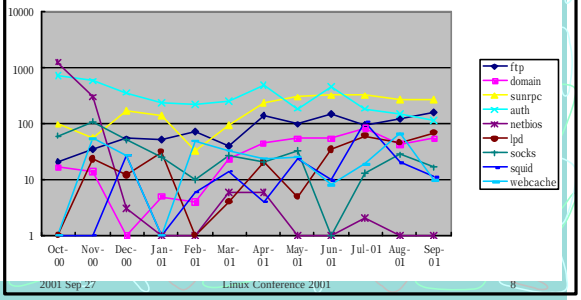



## トップ10

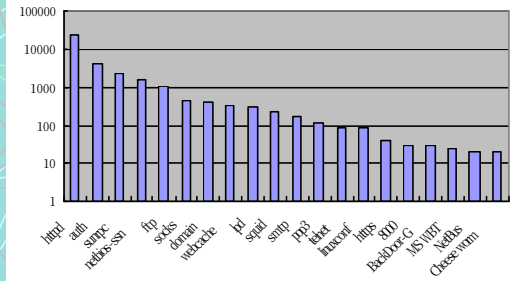





## トップ9

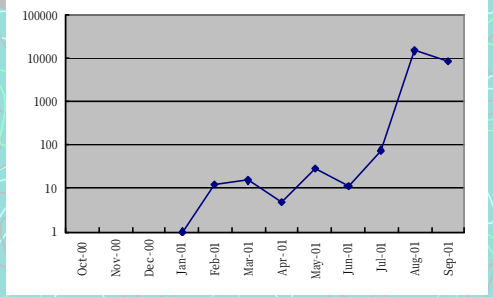


## トップ20






## Port 80

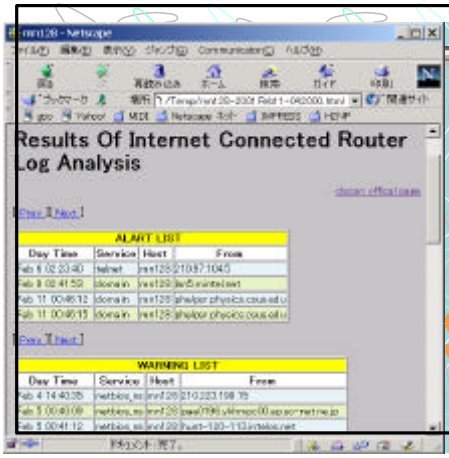





## CLSCAN

- Common Log SCAN
  - 既にsyslogに記録される数々のセキュリティ情報は存在しているが人間が簡単に読める形ではない
  - セキュリティログのプリティプリント
    - HTML, Text
  - 簡単な統計情報
  - 各種SOHO向けルータ、TCPWAPPER、IP filterなどのログに対応
  - http://h2np.net/clscan

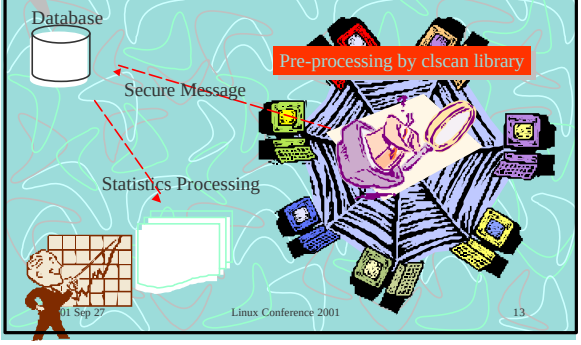





LIST

STAT

## WCLSCAN






## ネットワーク環境におけるセキュリティ保全

GNU/Linux環境における戦略



## フェイルセーフ

- 多重に防御する
  - 単体システムの機能のみに頼らない
- 問題をシンプルに切り分けることができる構成にする
  - All-In-Oneは避ける
  - 「何でもできる」は「何にもできない」と同じ



## いくつかの誤解

- ファイアウォールソフトを入れれば安全
  - パケット選別はルータレベルですべき
  - バッファオーバーフローには対応できない
- NATを使えば安全
  - 外部に接続する否かが問題
- 暗号化すればよい
  - 通信データ保全とシステム保全とは別問題

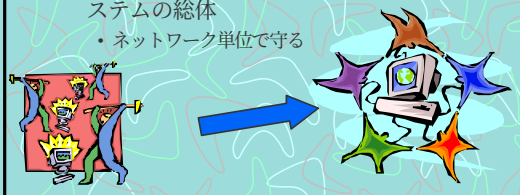
## いくつかの誤解

- LinuxはWindows NTより安全だ
  - ユーザがブラックボックスとして使う限り同じである
    - POP/IMAP, Telnetd, linuxconf, などなど事例にはことかかない
  - プラットフォーム数の違いである
    - ある規模になるとセキュアなアップデートが困難になる



## トータルな防御方法

- ファイアウォールの定義
  - 内部ネットワークを保護するプロテクションシステムの総体
    - ネットワーク単位で守る





## 5W1Hを明確にする

- WHAT: 何の情報を守るのか
- WHO: 誰から守るのか
- WHOM: 誰の情報を守るのか
- WHY: なぜその情報を守るのか
- WHERE: 守る情報はどこにあるのか
- HOW: どうやって守るのか



## GNU/Linuxのアドバンテージ

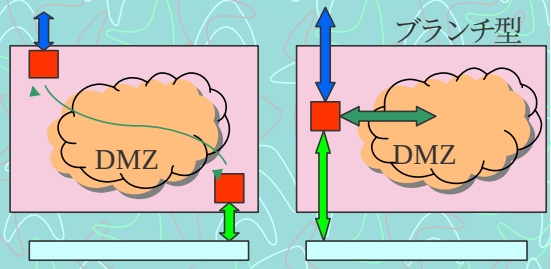
- 金銭的な負担が少ない
  - ×高額なソフトウェア
  - ×高価なハードウェア
- 目的別にマシンを用意する
  - 必要なソフトウェアのみで稼動させる
    - 問題の切り分けが明確になる
    - ブラックボックスとして使わない
  - Web DNS MAIL etc.

## ゾーン・ディフェンス

- サブネット化などをしてネットワーク的なゾーンを作る
- サーバが集中するゾーン
  - 境界ネットワーク（DMZ）
- 直接外部からアクセスされないゾーン
  - 通常のユーザが使う範囲
- インターネット側から遠いゾーンが必ずしも安全とは限らない
  - 内部からの攻撃・トロイの木馬・ウィルスetc



## スクリーンド・サブネット方式






## GNU/LinuxでIPフィルタリングBOX

- Linux BOXに複数NICカードをつければできあがり！
  - りぬくす工房の組込み向けSi-Linux
    - http://www.si-linux.com
- Iptables
  - Ipchain・ipfadmの後継
  - 強力なルールが適用できる



## 本質的な問題は…

- 適切なパケットフィルタリングのルールを作ることができるか？
  - ネットワークの論理設計ができる技量が必要だろう
  - 検証が難しい
    - 本格的に行うならばFormal Specification　形式的仕様記述）のアプローチが必要だろう

## 個別のマシンに関して

- TCP_WRAPPERによる制御
  - ゾーン（サブネット）単位でアクセスを管理
  - 個別のマシン毎にアクセスを管理
  - 外部からのアクセスをほぼシャットアウト
    - SSHを使ってのログインとポートフォワーディングのみ許す
- Iptabesを使って厳しくパケットをコントロールする
  - 最低限のサービスしかパケットを出さない
  - コンソールログイン以外許さない



## Libsafe

- バッファオーバーフローはパケットフィルタリングでは防げない
- 最新のGCCでプログラムをサイト毎に再コンパイルする
  - 不可能ではないが無理がある
- 多くのバッファオーバーフローはLibsafeで回避できる
  - http://www.gnu.org/directory/libsafe.html