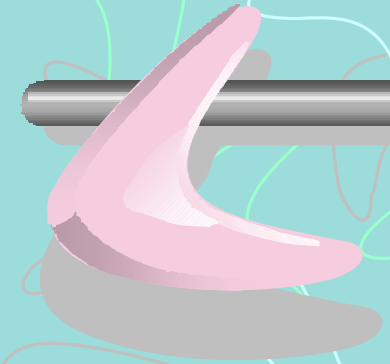
セキュリティインシデントの現状とネットワーク環境におけるセキュリティ保全



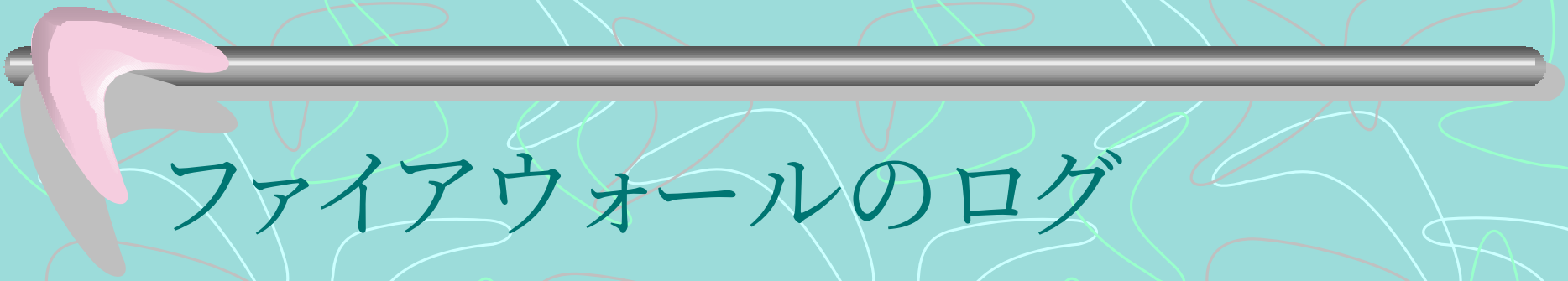
すずきひろのぶ

hironobu@h2np.net

本プレゼンテーションは
Linux Conference 2001にて
使用されたものです

内容

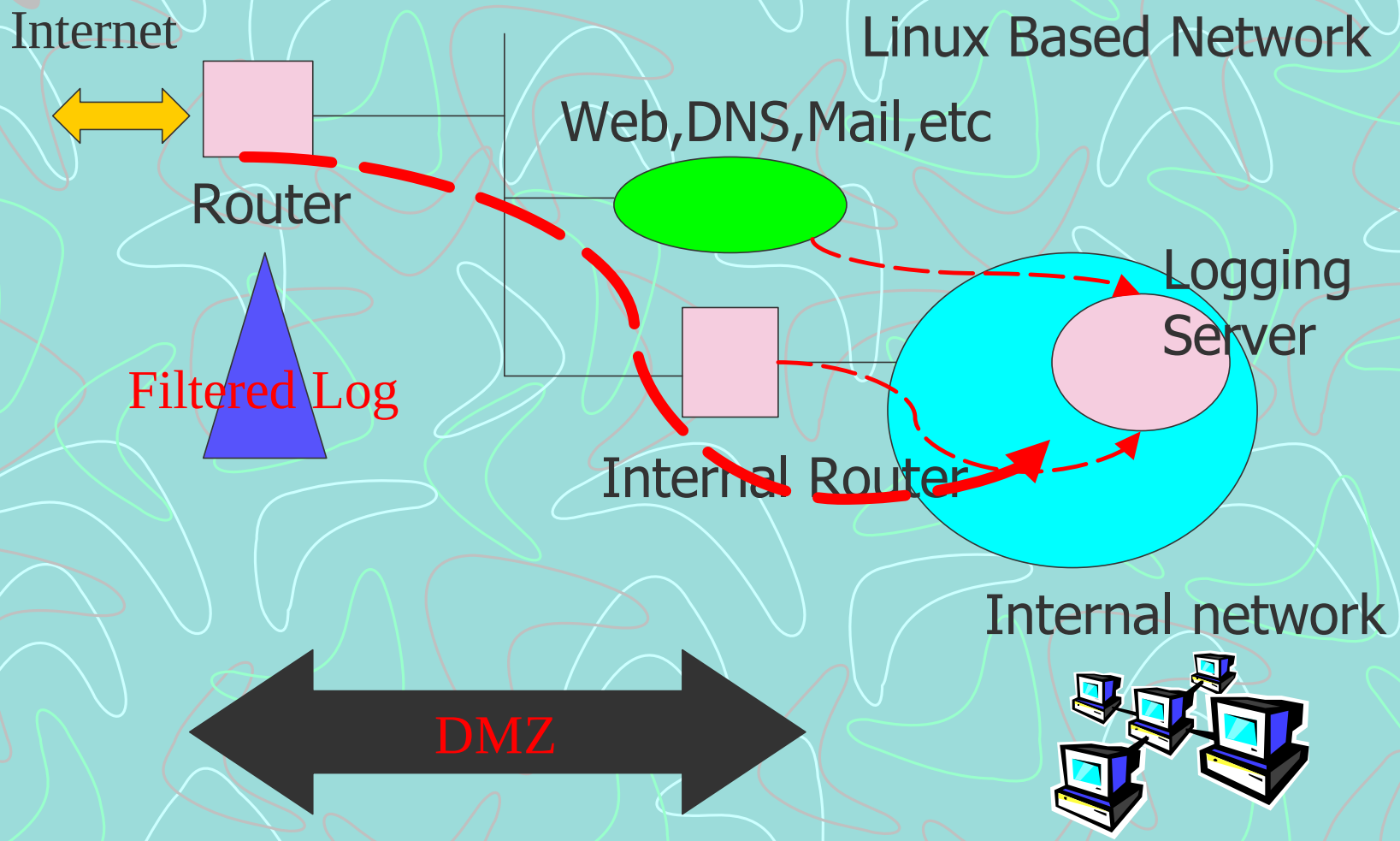
- セキュリティインシデントの現状分析
  - ネットワーク構成
  - 過去12ヶ月の分析から
  - CLSCANの紹介
  - WCLSCANの提案
- ネットワーク環境におけるセキュリティ保全



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

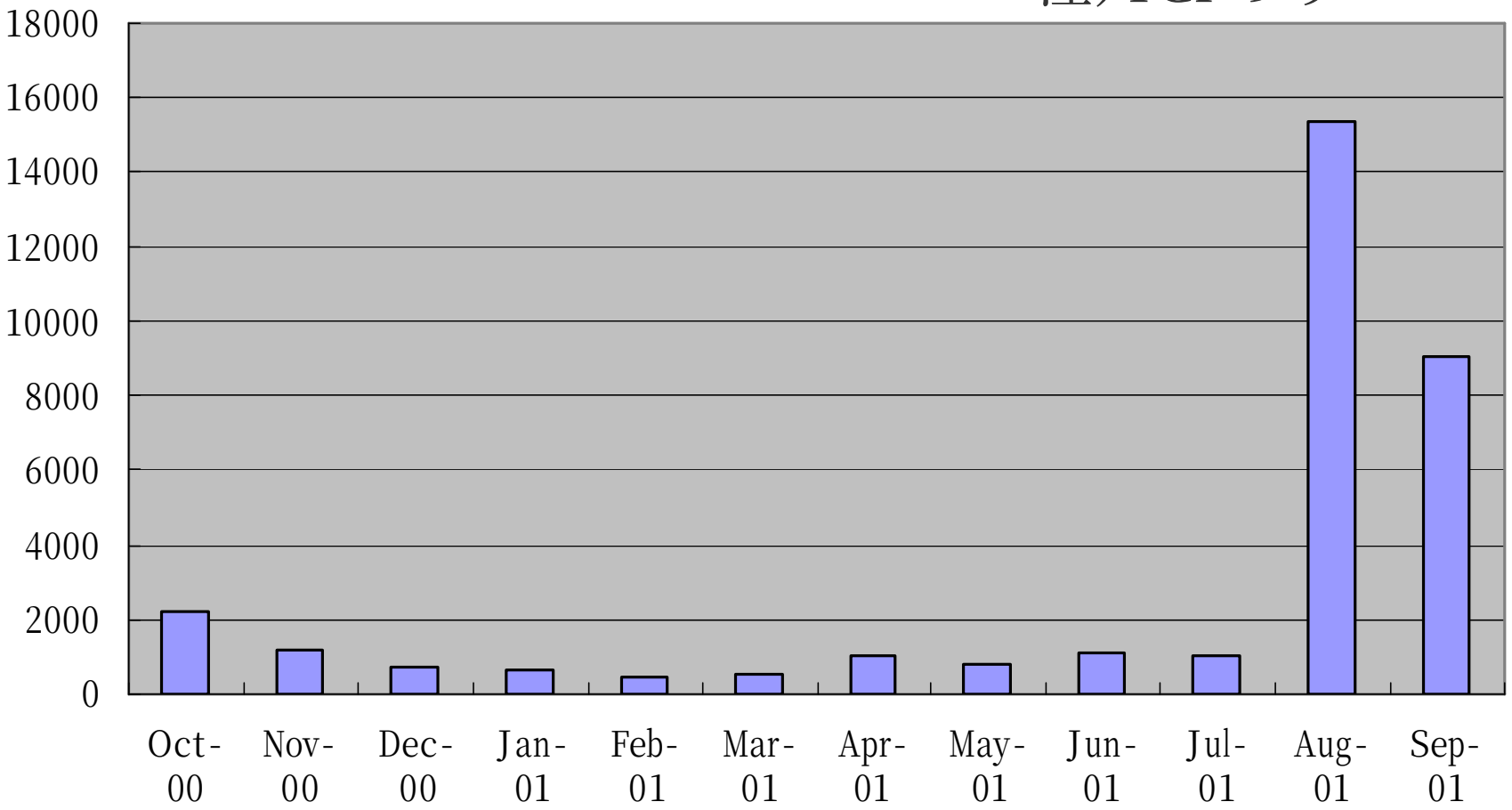

Internet
Linux Based Network
Web,DNS,Mail,etc
Router
Logging
Server
Filtered Log
Internal Router
Internal network
DMZ

過去12ヶ月の記録

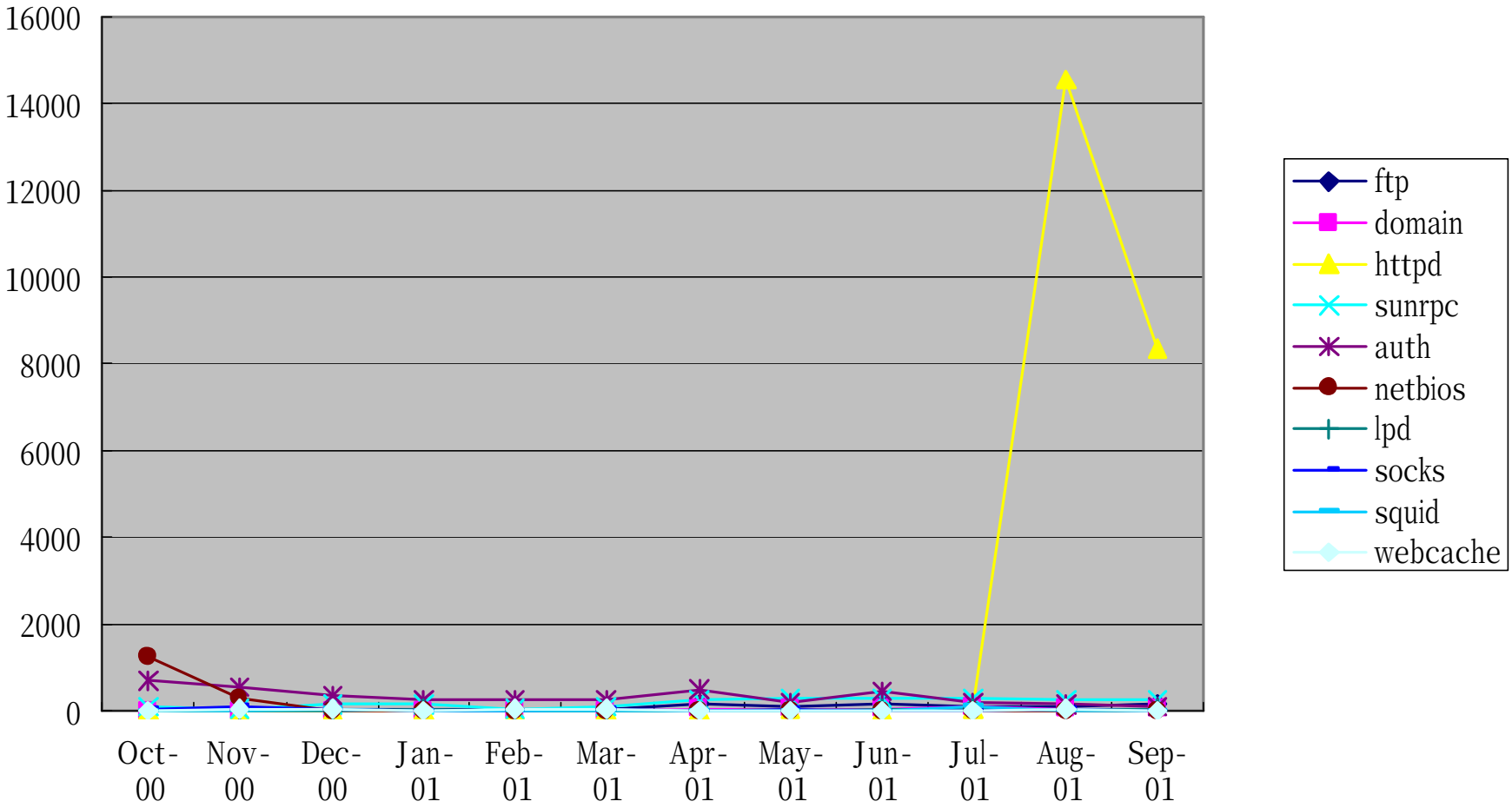
- 2000.10.9～2001.9.23
- リジェクトされた接続
  - 210.145.219.248/29
  - 68ポート（TCPのみ）
  - 35106エントリ（TCPのみ）

過去12ヶ月

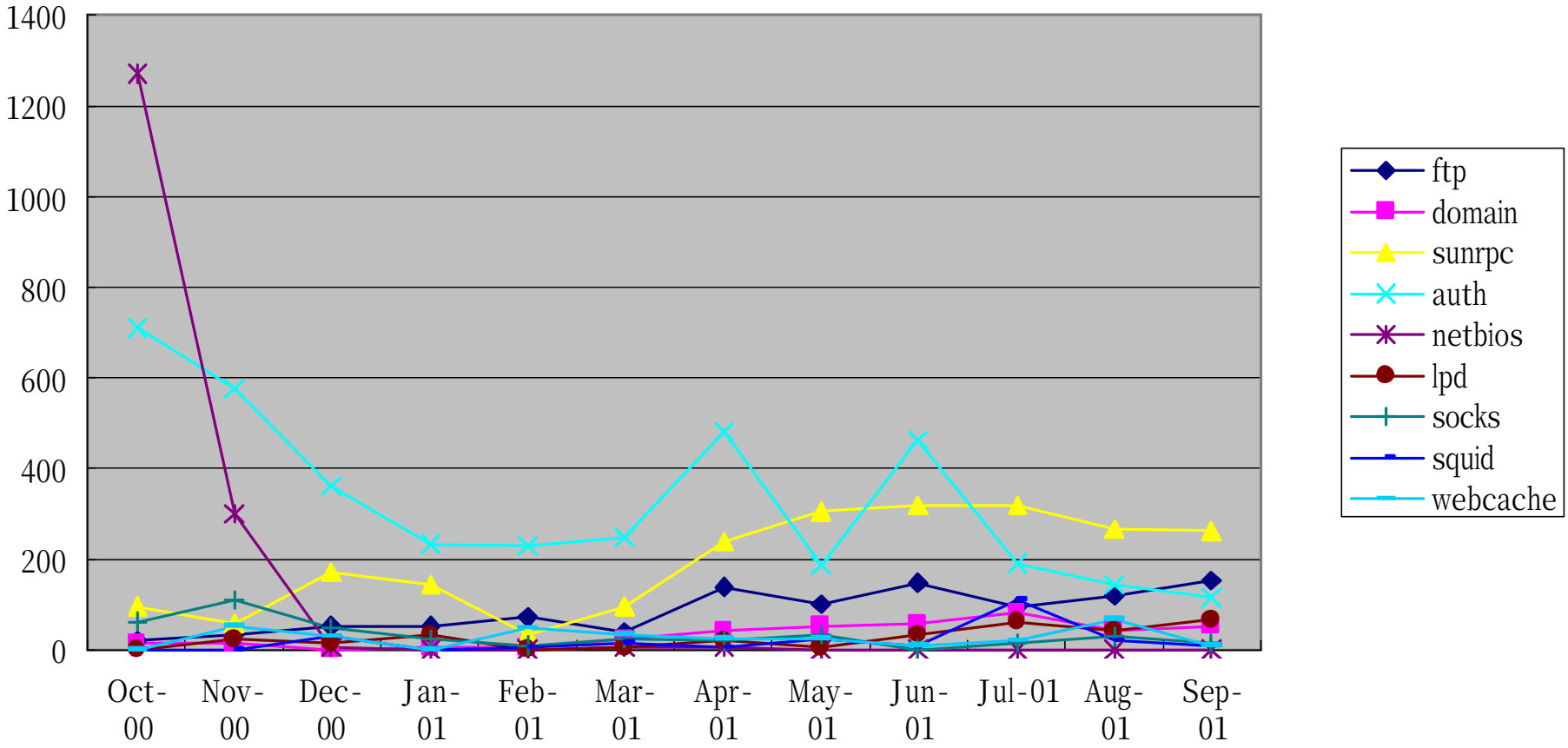
注)TCPのみ



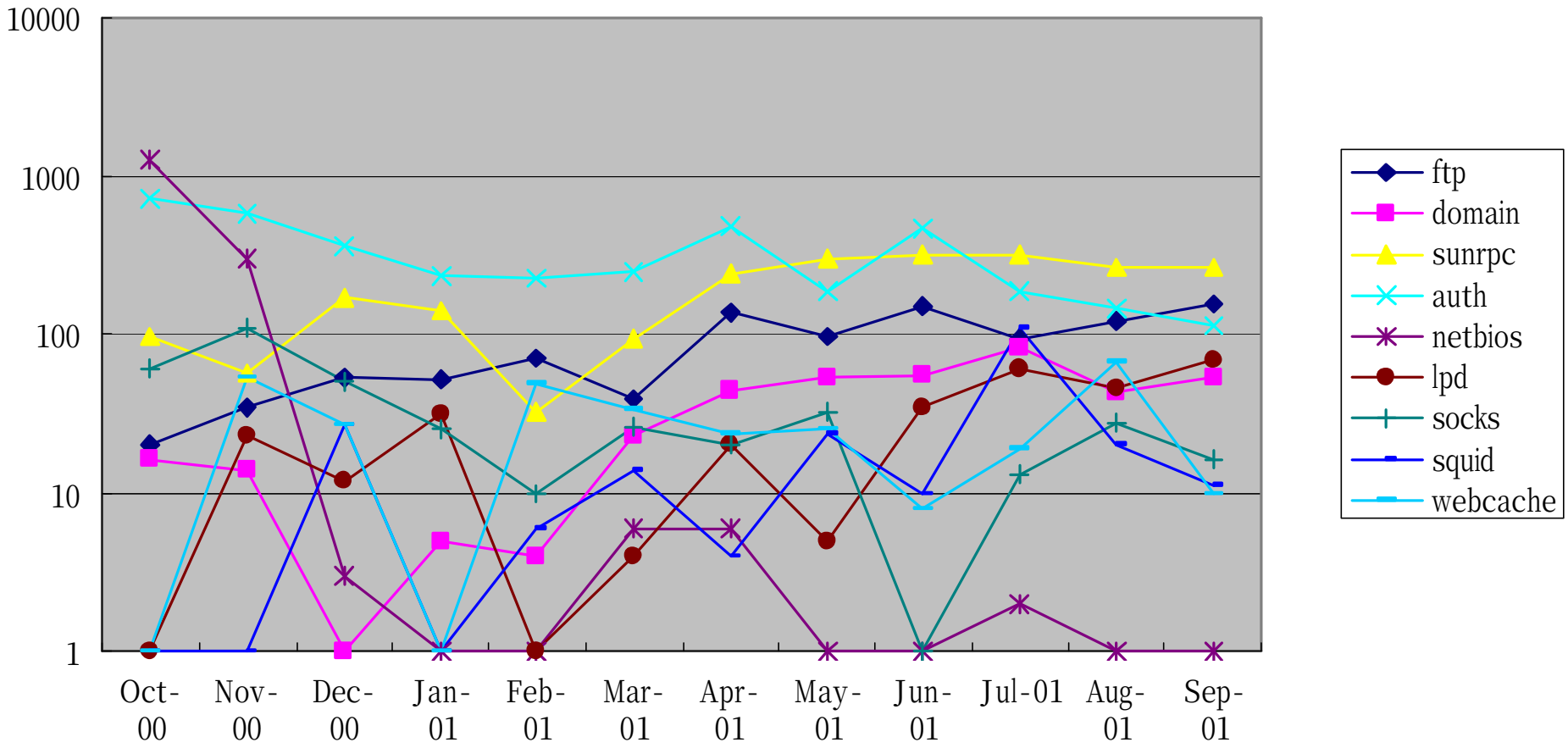
トップ10


16000
14000
12000
10000
8000
6000
4000
2000
0
Oct-00
Nov-00
Dec-00
Jan-01
Feb-01
Mar-01
Apr-01
May-01
Jun-01
Jul-01
Aug-01
Sep-01
ftp
domain
httpd
sunrpc
auth
netbios
lpd
socks
squid
webcache

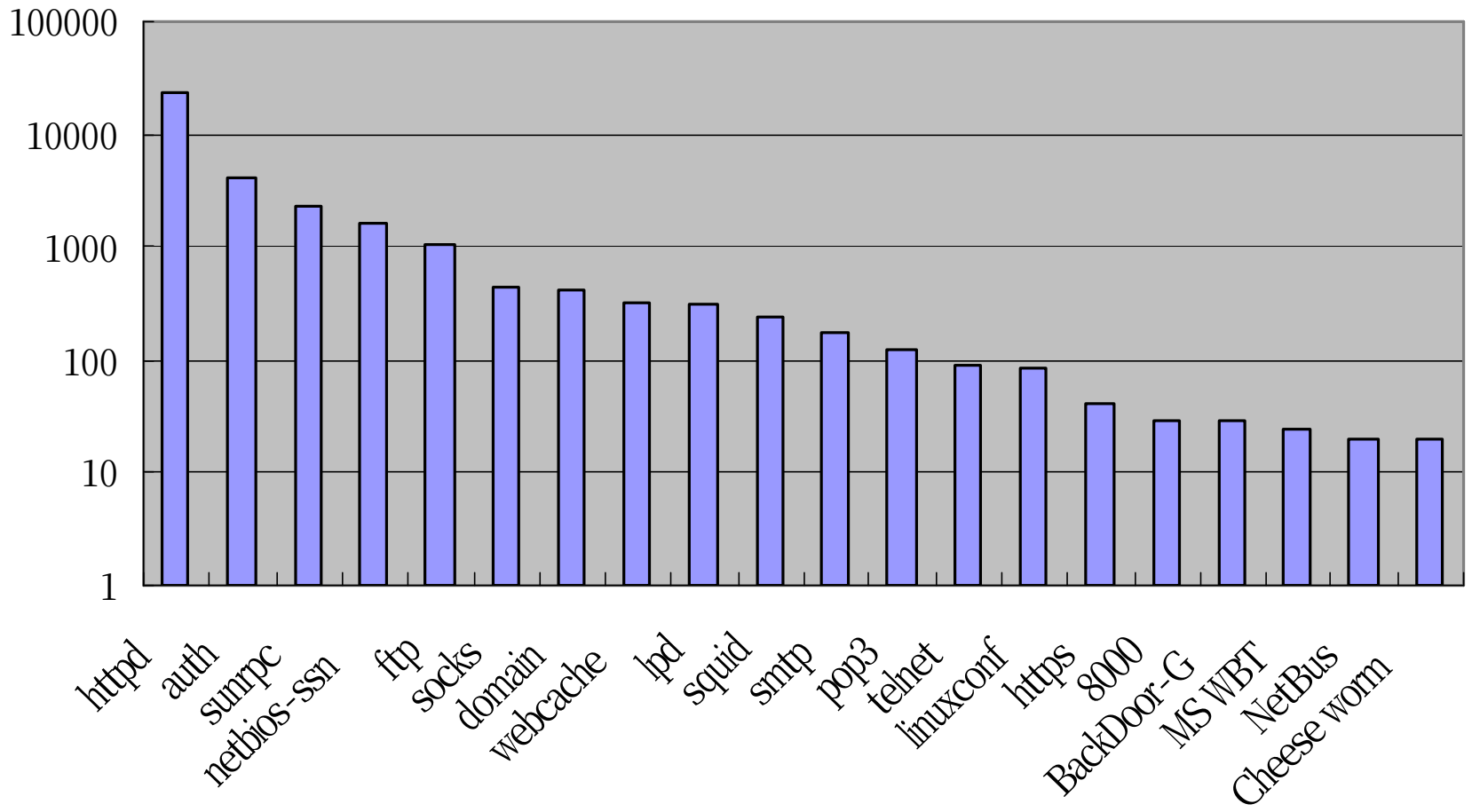
Httpdを除いたグラフ



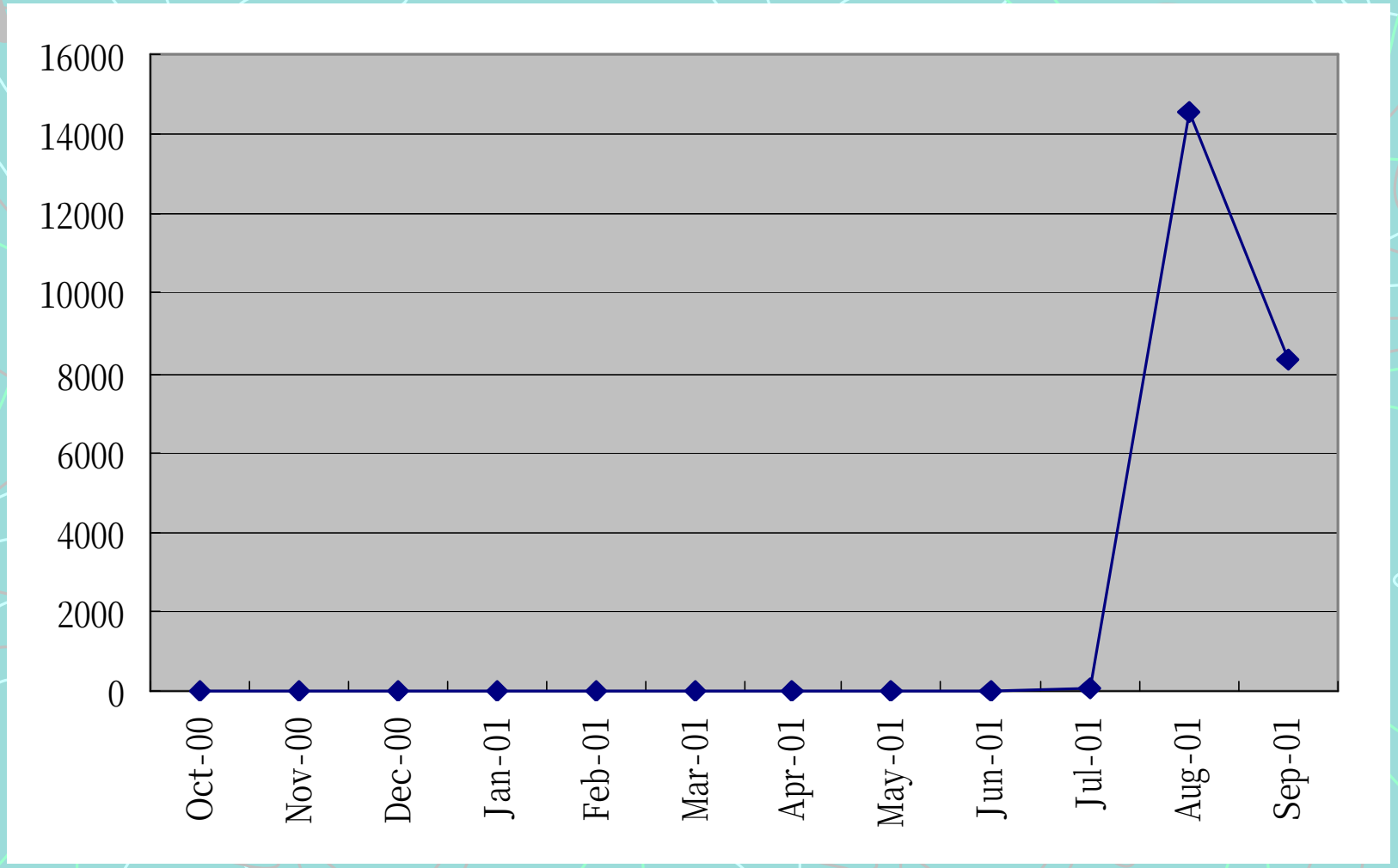
Httpdを除いたグラフ



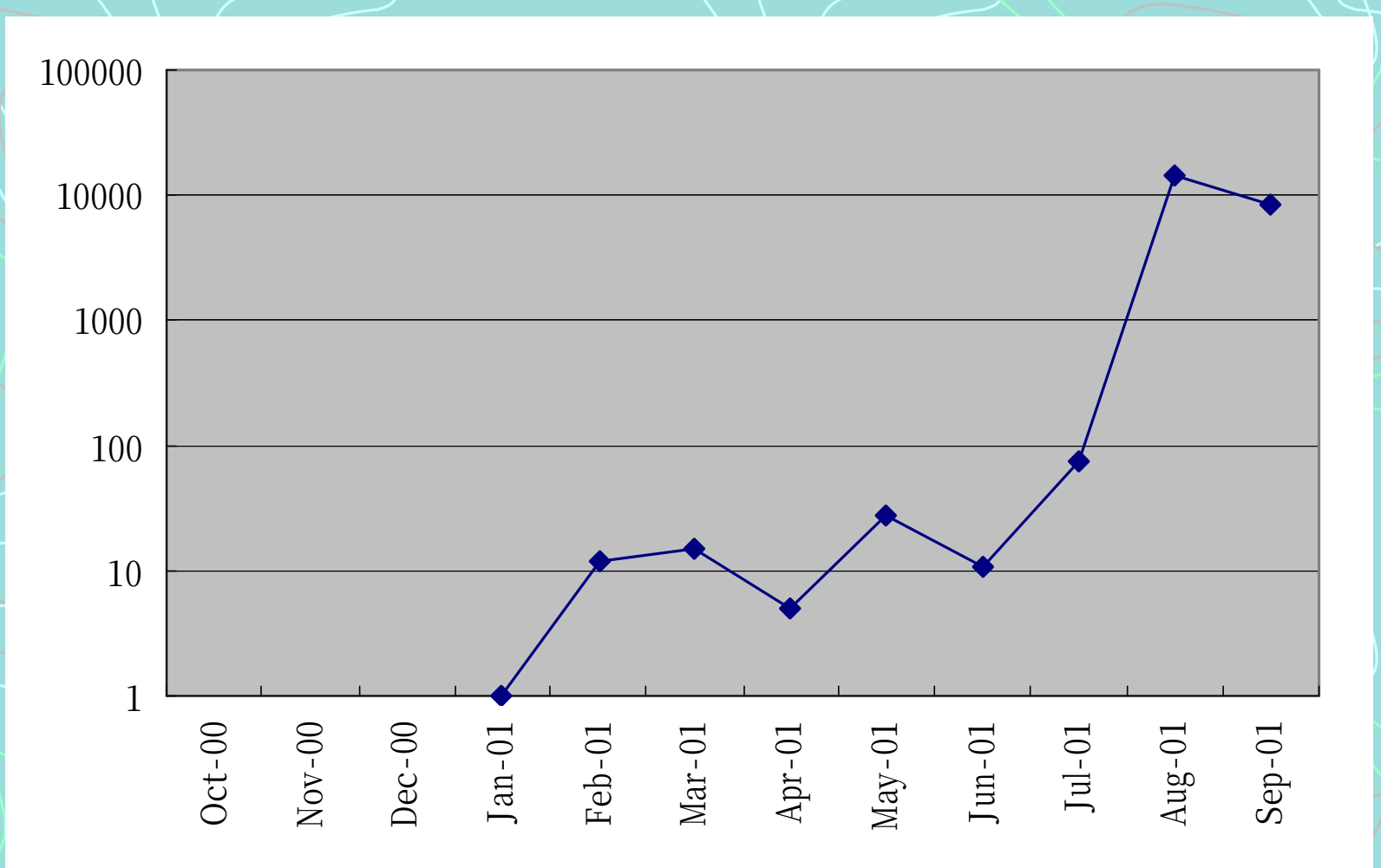
トップ20


100000
10000
1000
100
10
1
httpd
auth
sunrpc
netbios-ssn
ftp
socks
domain
webcache
lpd
squid
smtp
pop3
telnet
linuxconf
https
8000
BackDoor-G
MS WBT
NetBus
Cheese worm

Port 80

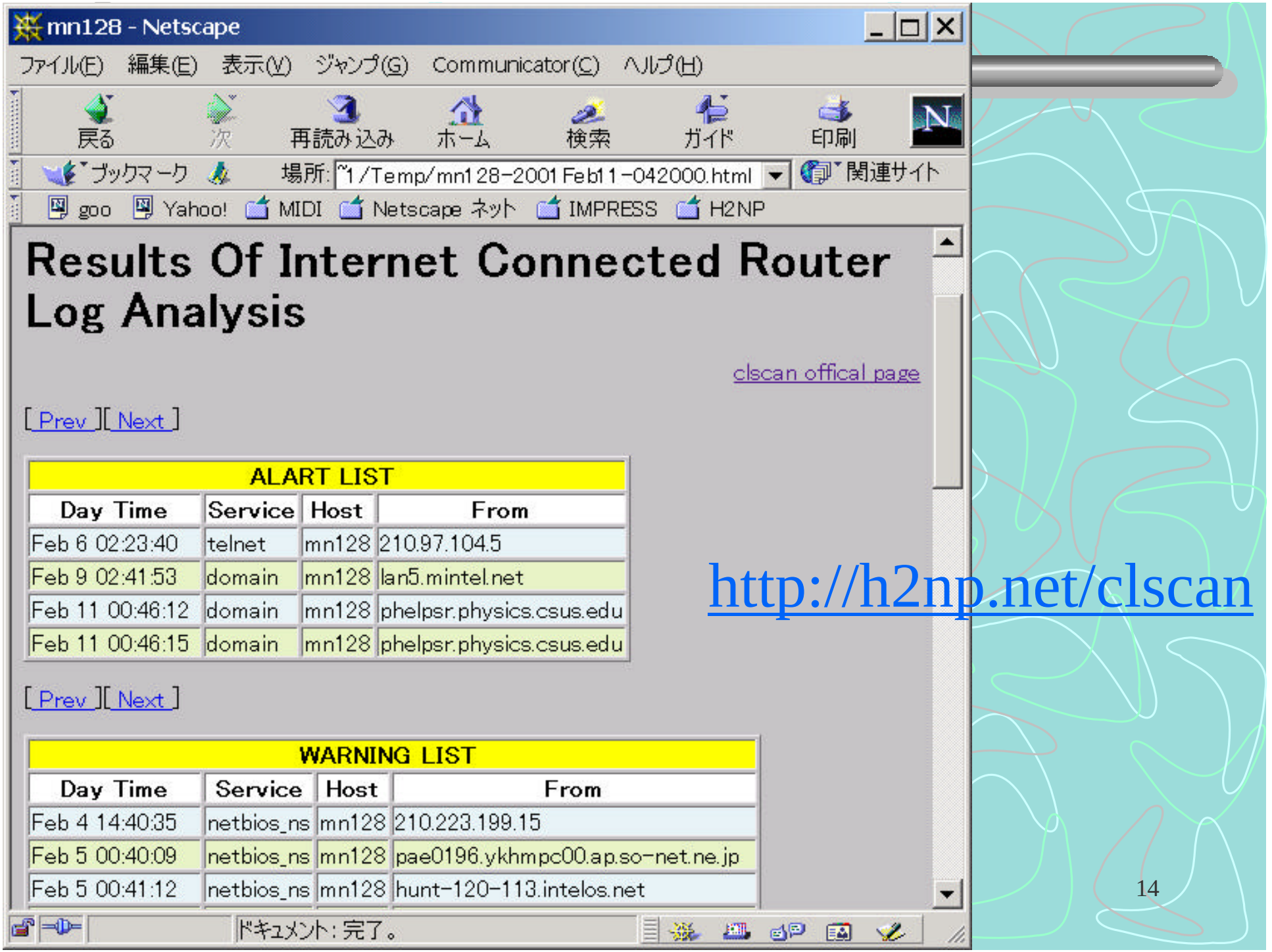

16000
14000
12000
10000
8000
6000
4000
2000
0
Oct-00
Nov-00
Dec-00
Jan-01
Feb-01
Mar-01
Apr-01
May-01
Jun-01
Jul-01
Aug-01
Sep-01

Port 80


100000
10000
1000
100
10
1
Oct-00
Nov-00
Dec-00
Jan-01
Feb-01
Mar-01
Apr-01
May-01
Jun-01
Jul-01
Aug-01
Sep-01

CLSCAN

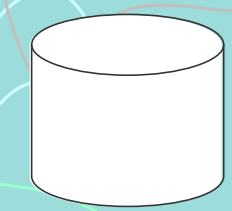
- Common Log SCAN
  - 既にsyslogに記録される数々のセキュリティ情報は存在しているが人間が簡単に読める形ではない
  - セキュリティログのプリティプリント
    - HTML, Text
  - 簡単な統計情報
  - 各種SOHO向けルータ、TCPWAPPER、IP filterなどのログに対応
  - http://h2np.net/clscan



http://h2np.net/clscan

WCLSCAN : 広域化したCLSCAN

Database



Secure Message

Statistics Processing

Pre-processing by clscan library