ポートスキャンログ分析からみたインターネットセキュリティの一考察

常時接続におけるネットワークセキュリティの脅威

ソフトウェアコンサルタント
鈴木裕信
Hironobu@h2np.net

主旨

- H2NP.NETサイトにおける外部からのポートスキャンのログを解析することにより、アタックのトレンドを考察する
- セキュリティログをPretty Printするツール clscanの紹介
- Clscanをベースに拡張した広域におけるポートスキャン解析システムの提案

バックグラウンド

- **ダイアルアップから常時接続へ**
  - CATV**や**xDSL**の普及**
- 24hours in a day / 7 days in a week
- **本格的なインターネット環境へ**
  - **～**1993：**先端的研究部門への普及**
  - **～**1995: **大企業への普及**
  - **～**2000: **ビジネスの現場への普及**
  - 2000**～**: **小規模サイト・小中学校・家庭へ普及へ**

問題点

- 常時接続環境においては大企業のサイトも一般家庭のサイトも規模は違えど本質的には何も変わらない
  - まったく同じ問題を抱えている
    - ソフトウェアの脆弱性
    - ネットワークサービスのセットアップミス
    - 不十分な管理
    - 無防備なシステム

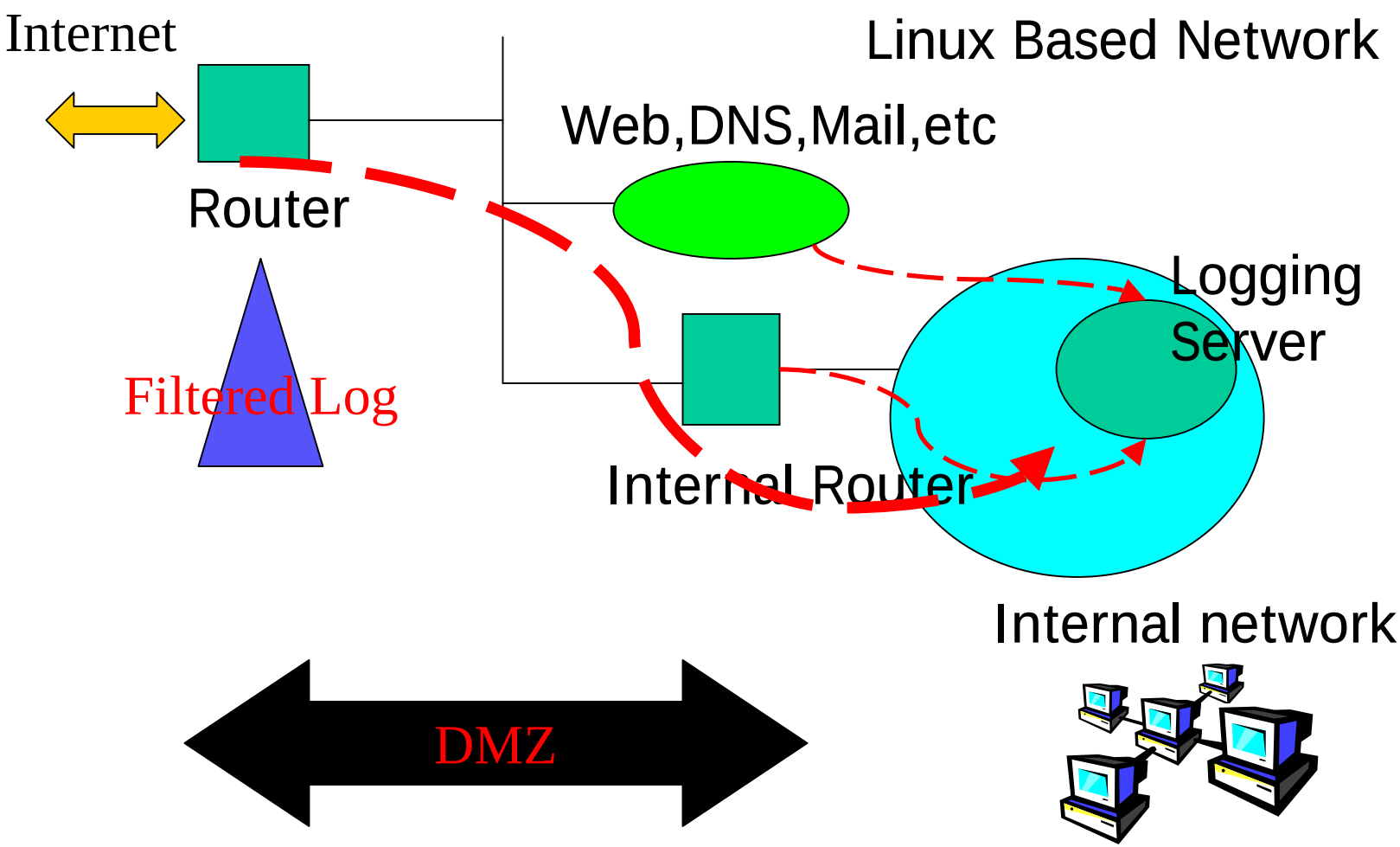
その結果...

- 無防備なシステムは自動的にスキャンされ、攻撃を受けることになる
  - rpc.statd (111)
    - NFSに使うデーモン
  - LPRng(515)
    - 新しいlpd
  - 911 Worm(137,138,139)
    - Windowsを狙って増殖
  - smurf, land (ICMP)
    - ICMP Echoなどの設定ミス

ファイアウォール

- **本論文での定義**
  - **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**
- **ファイアウォールとして最初にすること**
  - **インターネットと直接接続するルータでのIPパケットフィルタリング**
    - **マシン側でアクセス制御する方法もある**
      - TCPWAPPER
      - BlackIce

利用環境


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

IPフィルタログの分析

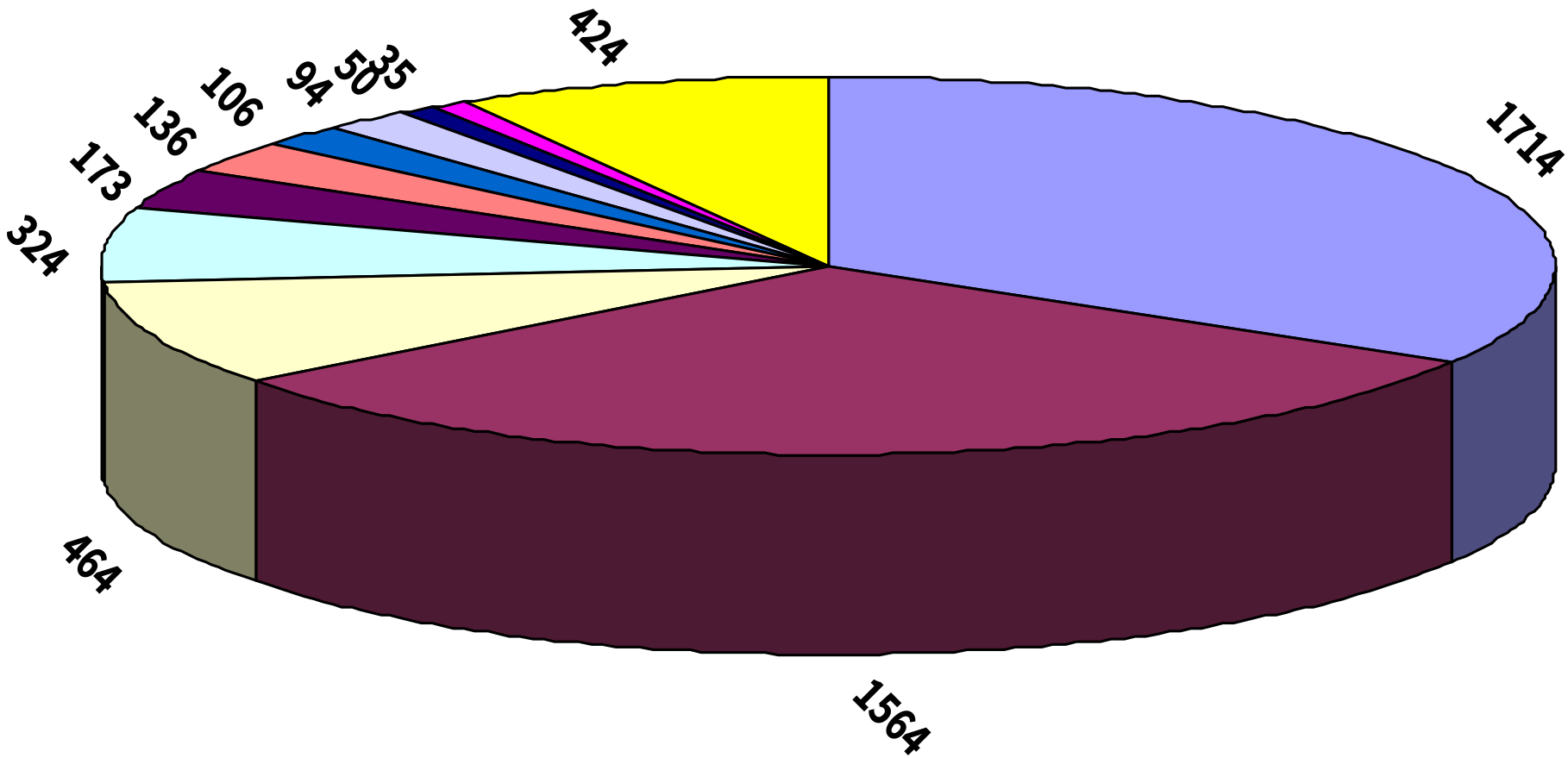
- 期間
  - 2000年7月1日～2001年1月31
- 記録数
  - 6714
    - syslogに記録されたルータのIPフィルタ設定で破棄された記録)
- ポートスキャンとして扱う対象
  - 26種類
- ポートスキャン数
  - 4898

注) domainやsmtpなどは存在していないアドレスへのアクセス

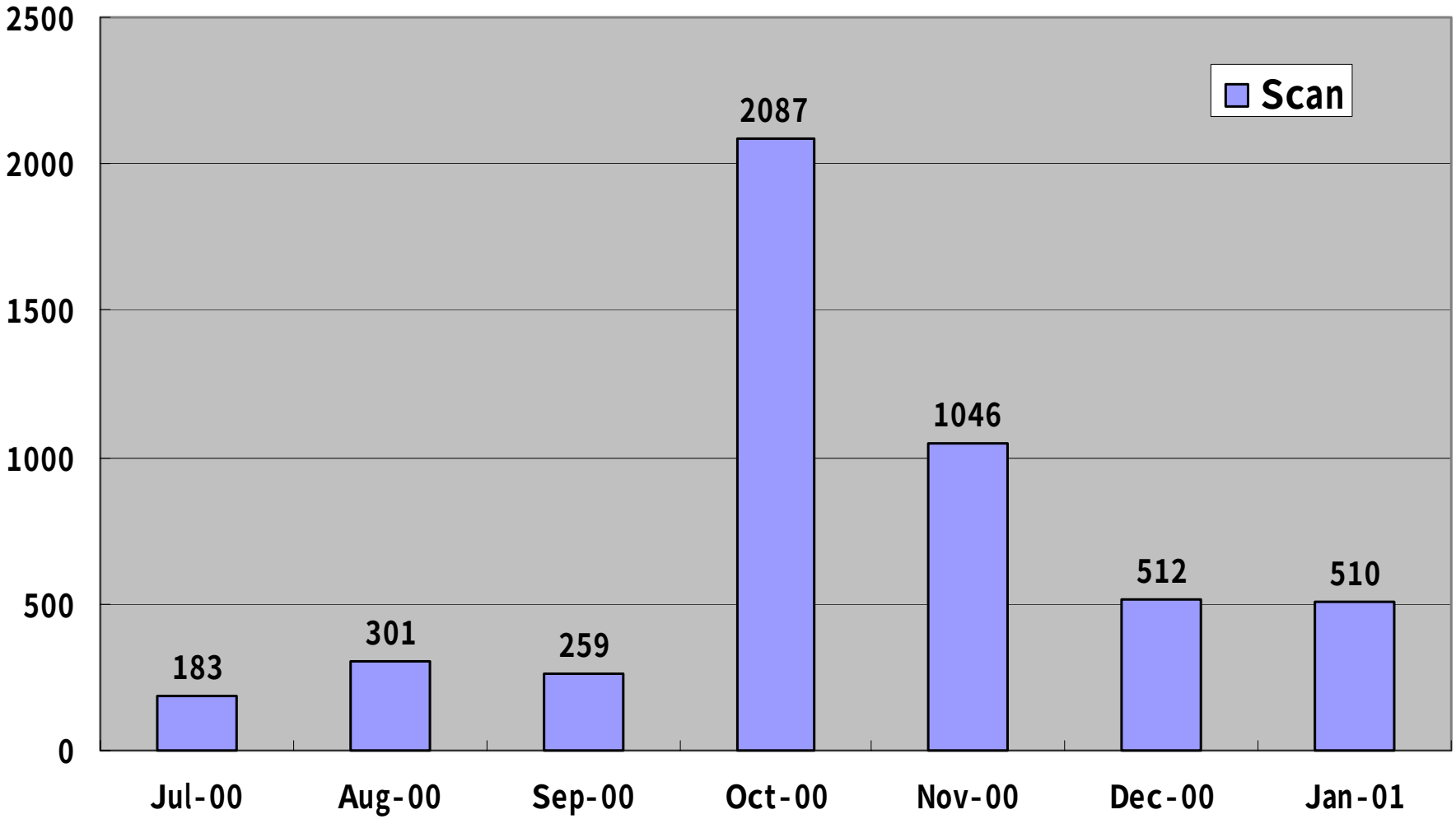
対象ポート

ftp(21/tcp), telnet(23/tcp), smtp(25/tcp),
domain(53/tcp), httpd(80/tcp), linuxconf(98/tcp),
pop2(109/tcp), pop3(110/tcp), sunrpc(111/tcp),
netbios_ns(137/tcp), netbios_ns(137/udp),
netbios_dgm(138/tcp), netbios_dgm(138/udp),
netbios(139/tcp), netbios_ssn(139/udp),
imap(143/tcp),
printer(515/tcp), linux_mountd(635/tcp),
socks(1080/tcp),
Sub7(1243/tcp), MS_SQL_S(1433/tcp),
ingreslock(1524/tcp),
squid(3128/tcp), pcanywheredata(5631/tcp),
wwwproxy(8080/tcp), NetBus(12345/tcp),
BackDoor_G(27374/tcp),
 Hackatack(31789/udp), rpcbind(32773/tcp)

統計分析データ

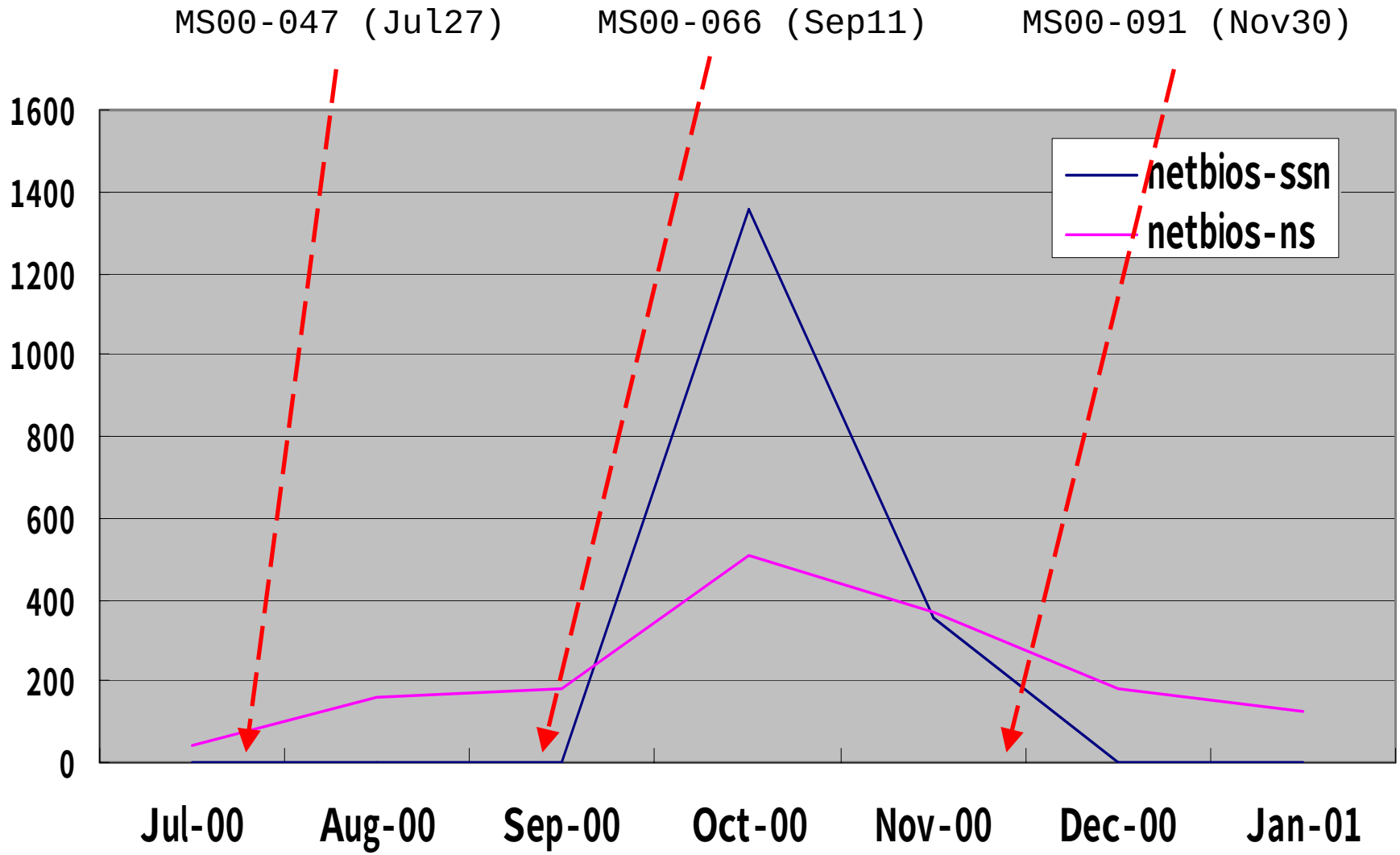

1714
1564
464
324
173
136
106
94
50
35
424
netbios-ssn
netbios-ns
sunrpc
socks
smtp
http proxy
linuxconf
ftp
printer
domain
other

月別変化


2500
2000
1500
1000
500
0
Scan
183
301
259
2087
1046
512
510
Jul-00
Aug-00
Sep-00
Oct-00
Nov-00
Dec-00
Jan-01

NetBIOS編

月別変化



NetBios編　用語説明

- Netbios-ssn
  - **ポート番号**139
    - Windows**のポートサービス**
- Netbiso-ns
  - **ポート番号**137
    - Windows**のネームサーバ**

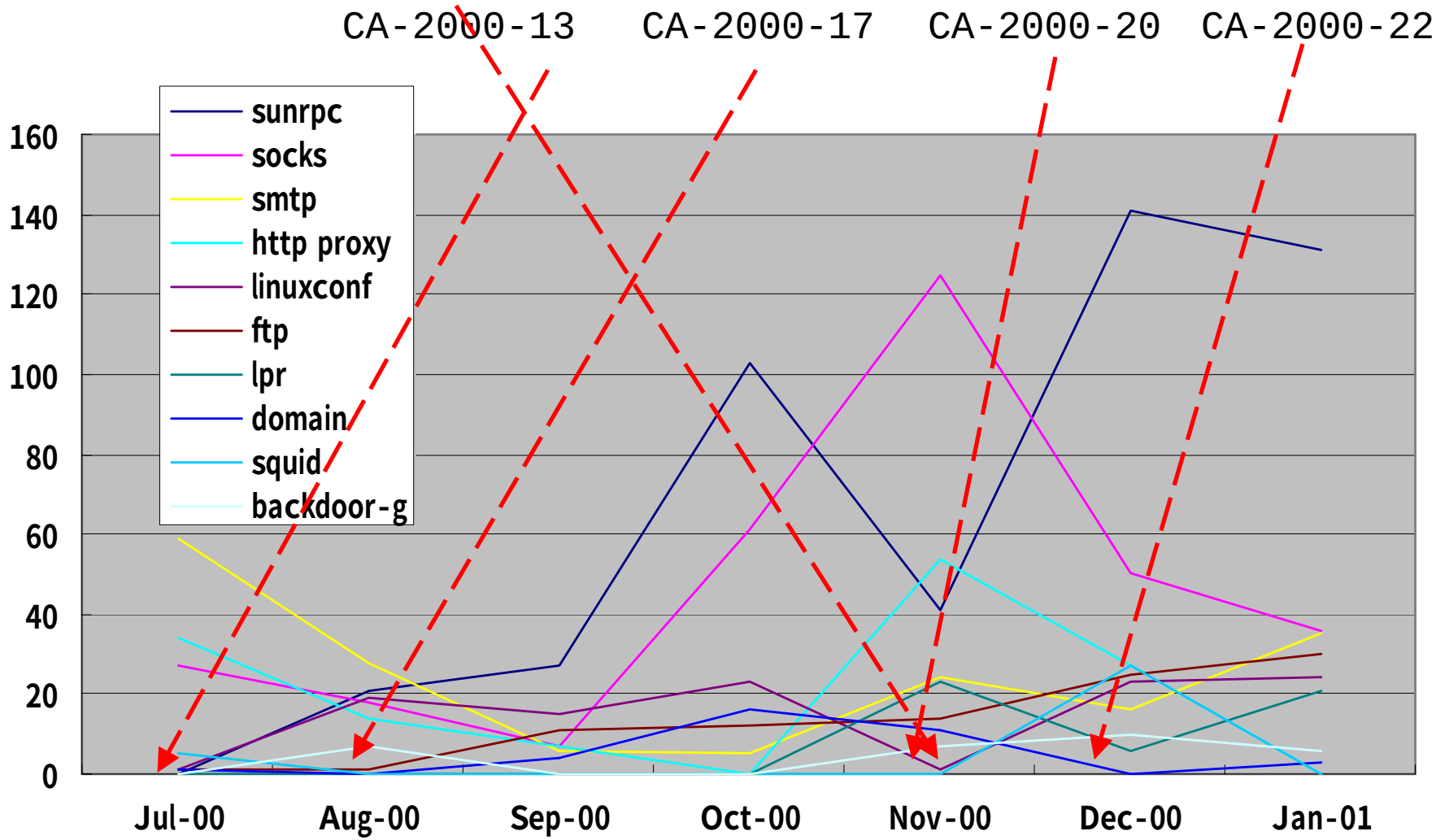
www.microsoft.com

- MS00-047
  - NetBIOS Name Server Protocol Spoofing Vulnerability (NT4.0 W2K)
- MS00-066
  - Malformed RPC Packet Vulnerability(W2K)
- MS00-091
  - Incomplete TCP/IP Packet Vulnerability(NT4.0 95 98 Me 98s)

BugTraq Nov15
Socks remote
exploit code posted

月別変化

ベスト10 (netbiosを除く)



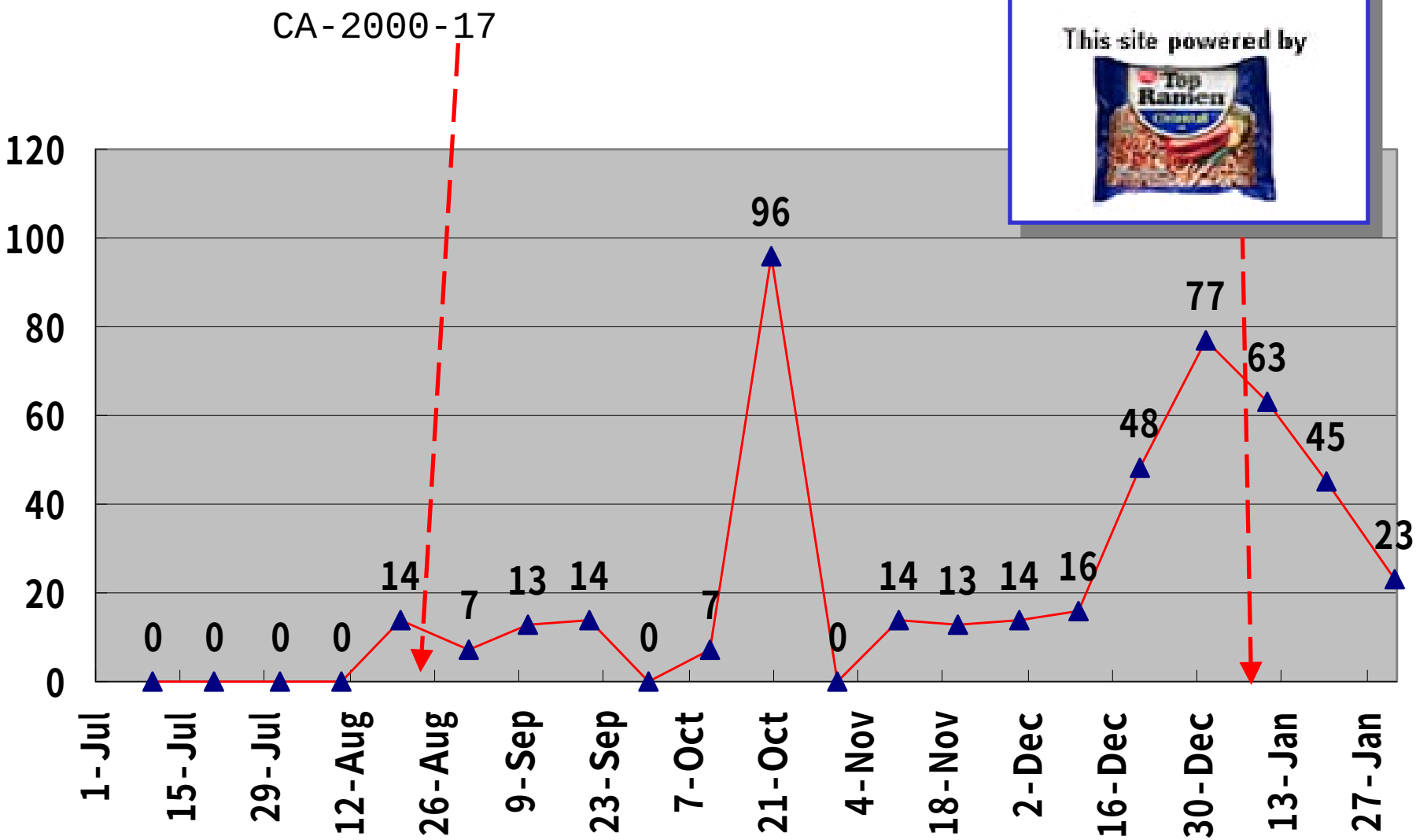
ベスト10 用語説明

- CA-2000-13
  - Two input Validation problems in FTPD
- CA-2000-17
  - Input Validation Problem in rpc.statd
- CA-2000-20
  - Multiple Denial-of-Service Vulnerability in ISC BIND
- CA-2000-22
  - Input Validation Problem in LPRng

www.cert.org

sunrpc

月別変化


CA-2000-17
120
100
80
60
40
20
0
0
0
0
0
14
7
13
14
0
7
96
0
14
13
14
16
48
77
63
45
23
1-Jul
15-Jul
29-Jul
12-Aug
26-Aug
9-Sep
23-Sep
7-Oct
21-Oct
4-Nov
18-Nov
2-Dec
16-Dec
30-Dec
13-Jan
27-Jan

This site powered by
Top Ramen

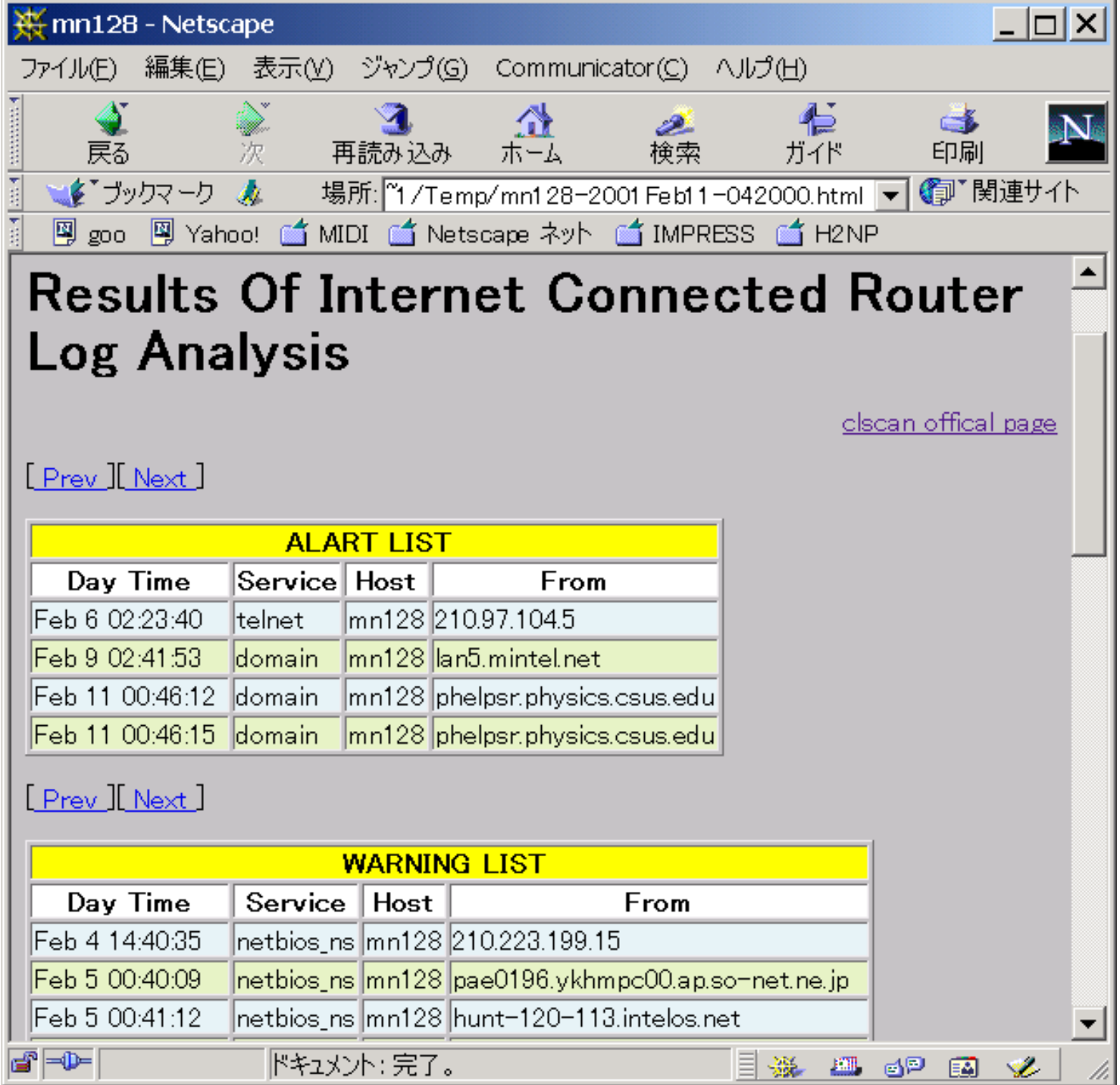
Sunrpc 用語説明

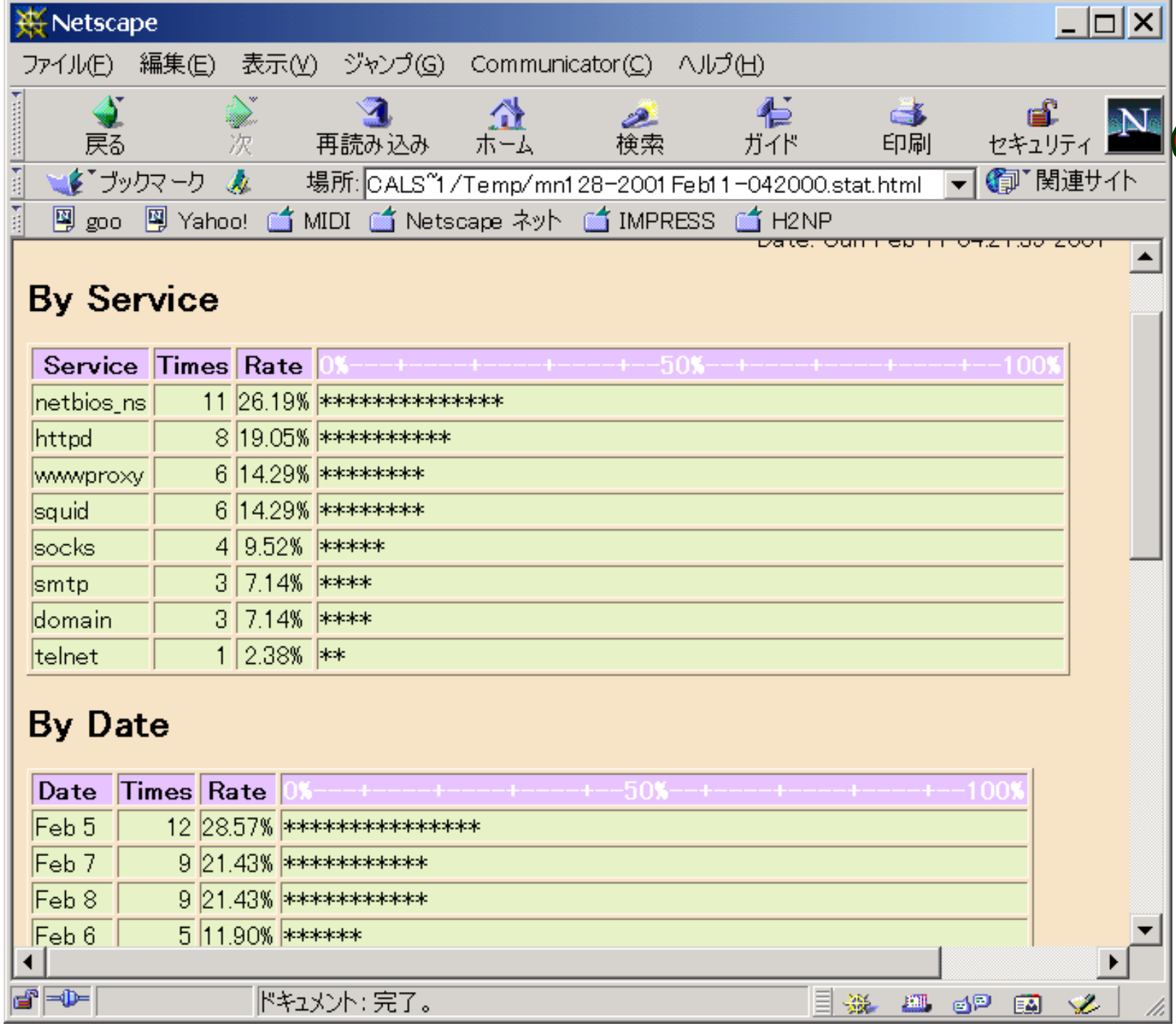
- CA-2000-17: Aug 18
  - Input Validation Problem in rpc.statd
- IN-2001-01: Jan 18
  - Ramen Worm toolkit

www.cert.org

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


mn128 - Netscape
ファイル(F) 編集(E) 表示(V) ジャンプ(G) Communicator(C) ヘルプ(H)
戻る 次 再読み込み ホーム 検索 ガイド 印刷
ブックマーク 場所: ~1/Temp/mn128-2001Feb11-042000.html 関連サイト
goo Yahoo! MIDI Netscape ネット IMPRESS H2NP
Results Of Internet Connected Router Log Analysis
clscan offical page
[Prev][Next]
ALART LIST
Day Time | Service | Host | From
Feb 6 02:23:40 | telnet | mn128 | 210.97.104.5
Feb 9 02:41:53 | domain | mn128 | lan5.mintel.net
Feb 11 00:46:12 | domain | mn128 | phelpsr.physics.csus.edu
Feb 11 00:46:15 | domain | mn128 | phelpsr.physics.csus.edu
[Prev][Next]
WARNING LIST
Day Time | Service | Host | From
Feb 4 14:40:35 | netbios_ns | mn128 | 210.223.199.15
Feb 5 00:40:09 | netbios_ns | mn128 | pae0196.ykhmpc00.ap.so-net.ne.jp
Feb 5 00:41:12 | netbios_ns | mn128 | hunt-120-113.intelos.net
ドキュメント: 完了。

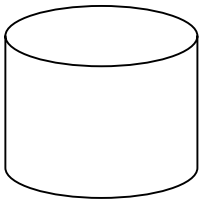

Netscape
ファイル(F) 編集(E) 表示(V) ジャンプ(G) Communicator(C) ヘルプ(H)
戻る 次 再読み込み ホーム 検索 ガイド 印刷 セキュリティ
ブックマーク 場所: CALS~1/Temp/mn128-2001Feb11-042000.stat.html 関連サイト
goo Yahoo! MIDI Netscape ネット IMPRESS H2NP
By Service
Service Times Rate 0%---+---+---+---+--50%--+---+---+---+--100%
netbios_ns 11 26.19% **********
httpd 8 19.05% *******
wwwproxy 6 14.29% ******
squid 6 14.29% ******
socks 4 9.52% ****
smtp 3 7.14% ***
domain 3 7.14% ***
telnet 1 2.38% *
By Date
Date Times Rate 0%---+---+---+---+--50%--+---+---+---+--100%
Feb 5 12 28.57% **********
Feb 7 9 21.43% *******
Feb 8 9 21.43% *******
Feb 6 5 11.90% ****
ドキュメント: 完了。

CLSCANをより広域へ

- 現在のCLSCANは個々のサイトのログを統計処理しているだけ
  - なんとなくトレンドはわかる
    - しかし統計的には偏りが大きいはずである
  - もっと広域の情報を集めれば、さらにトレンドがはっきりする？
    - ポートスキャンとアタックの関係をもっとフィールドワークする必要がある

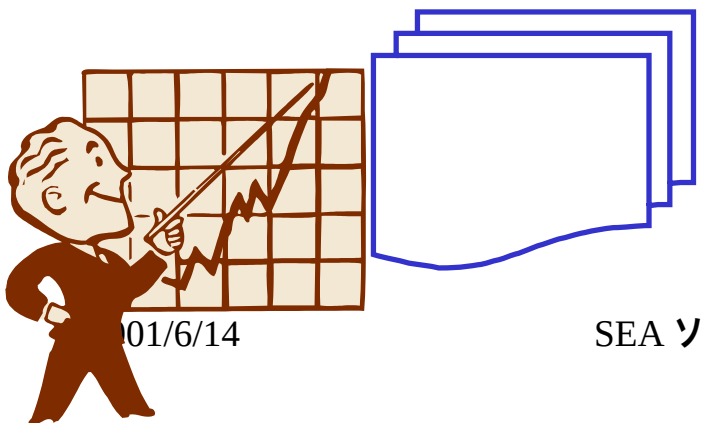
WCLSCAN

Database



Secure Message

Statistics Processing



Pre-processing by clscan library

誰か一緒にやりませんか？

WCLSCANは広域の情報を集めるツールであって、それは手段である。その集めた情報から何が見えてくるのか、これが筆者の興味であり、目的である。まだ誰も広域データの分析をしたことがない。誰も知らないことを知りたいと思いませんか？

まとめ

- SOHOレベルでもたくさんのポートスキャンがある
- システムへの侵入を前提としたポートスキャンであると強く示唆するものもある
- ブロードバンド時代では一般家庭レベルでも問題になるだろう
- さらに今後も観察を続ける必要がある
- １サイトのログだけではなく、広域のデータを集めることができれば、さらに新しい発見が可能かも知れない