



フリーソフトウェアによる ネットワーク監視

矢萩 茂樹
イー・アクセス株式会社
2000/12/19

2000.12.19

Copyright 2000, eAccess Ltd, Shigeki YAHAGI



T10 : フリーソフトウェアによるネットワーク監視

2

本チュートリアル の 進行

- ⌘ 第1部 ネットワーク管理の基礎知識
☑ 9:30 - 10:00
- ⌘ 第2部 フリーソフトウェアによるネットワーク監視
☑ 10:00 - 11:40
- ⌘ 第3部 ネットワーク管理に関するTIPS
☑ 11:40 - 12:20
- ⌘ 質疑応答
☑ 12:20 - 12:30

2000.12.19

Copyright 2000, eAccess Ltd, Shigeki YAHAGI





第1部：ネットワーク管理 の基礎知識



ネットワークとは

⌘ ネットワークは
様々な中継装置の複合接続により、通信機能を持つ機器を遠隔接続し、多対多のコミュニケーションを実現するシステム

☑ 様々な機器による複雑系

☑ ネットワークは生き物。状況は刻々と変化する。状況把握はなかなか困難

☑ 多岐にわたる構成機器・関連機器：

☑ PC、ルーター、スイッチ、WDM伝送装置、ATM交換機、多重化装置、サーバー、DSU、メディアコンバーター、ケーブル、電源冷却装置、...



監視業務の必要性1

※ ミッションクリティカル

- ☑ E-mail/DNS/WEBは既に企業活動上、必須の通信手段となった
- ☑ E-mail/DNS/WEBが止まる = 業務が止まる！

※ 多岐にわたる構成機器と複雑になる障害要因

- ☑ 全機器の稼動状況を把握するのは困難な作業
- ☑ 障害は必ず起こる
 - ☑ とはいえ、泣き言はいってられない

※ 止まらないネットワークは実現困難

- ☑ 金をかければ冗長構成をとれるが...、バックアップされただけ
 - ☑ 結局復旧作業は必要
- ☑ 止めないようにする努力と止まったときに復旧する努力
 - ☑ こける前にささえるのが一番被害が少ない。けど...
 - ☑ こけてしまったら、なんとかはやく直さないと...



監視業務の必要性2

※ ネットワークをこけさせないためには

- ☑ 障害の予兆をつかんで、予防保全

※ こけたものをできるだけ早く立て直すには

- ☑ 障害発生を速やかに検知し、
- ☑ 原因をできるだけ早く確定する

※ これらの実現には、定常的な監視とサポートする監視システムの構築が必要


18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10 : フリーソフトウェアによるネットワーク監視 7

監視処理とは

- ⌘ 監視ポイントを設定し、
- ⌘ 閾値を設けて、
- ⌘ それを超えているか判断し、
- ⌘ 通知すること
- ⌘ このフローの繰り返しとなる
- ⌘ 通知が障害と判断された後、障害対処に分岐

2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI



18-21, December 2000 Grand Cube Osaka Internet Week 2000

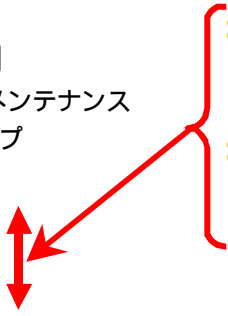
T10 : フリーソフトウェアによるネットワーク監視 8

監視のワークフロー


1. 定常運用
 1. 稼動状況確認
 2. 障害検知
2. 非定常運用
 1. システムメンテナンス
 2. ラインアップ
3. 障害対応
 1. 障害検知
 2. 状況把握
 3. 原因確定
 4. 復旧処理

⌘ 3.1障害検知から 3.3 原因確定区間をシステム化により情報整理を行い、

⌘ オペレータが復旧処理にできるだけ早くかけられるようにしたい



2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI





T10: フリーソフトウェアによるネットワーク監視

速やかな原因確定を 実現するワークフローとは

- ⌘ 的確な参照情報が盛り込まれたアラーム通知が重要
- ⌘ 必要なのは 必要十分情報と障害サマリー画面へのURLリンク
 - ☑ 障害発生時刻
 - ☑ 障害発生個所・機器
 - ☑ 障害状況
 - ☑ 障害サマリーページへのURL情報
 - ☑ 障害システムのみがまとめられたサマリー画面
- ⌘ この情報をアラームメッセージに乗せることで、速やかな障害サマリーページへのアクセスを実現
- ⌘ ハイパーリンクによるワークフローの確立

2000.12.19

Copyright 2000, eAccess Ltd, Shigeki YAHAGI



T10: フリーソフトウェアによるネットワーク監視

10

監視ポイントの設定

⌘ 監視基点と監視経路

- ☑ In-Bound Management (帯域内管理)
- ☑ Out-Bound Management (帯域外管理)



2000.12.19

Copyright 2000, eAccess Ltd, Shigeki YAHAGI



通知について考える

⌘ 監視通知の方法

- ☑ アラームメッセージ
- ☑ グラフィカル (画面、アイコンの点滅)
- ☑ アラーム音
- ☑ メール
- ☑ ポケベル・携帯電話にリモートメール
 - ☑ ポケベルもほとんど絶命寸前。クリティカルな通知には*-Modeは使いもんにならんし、なにかいいものないだろうか？



監視における切り口 - 現状と経過

- ⌘ 現状監視 - 今を見る : Polling
 - ☑ 現在のシステム状態を監視する
- ⌘ 現状検知 - 今を検知する : Event Trap
 - ☑ システムからの自律アラームをとらえる
- ⌘ 経過監視 - これまでを見る : Traffic Analysis
 - ☑ トラフィックの推移を監視。トレンドを把握する
- ⌘ これらは密接にからんだ独立事象
 - ☑ どれがぬけても片手落ち



監視する手段 - Polling

⌘ ICMP Polling

- ☑ ICMP echo(ping)による監視。必要最低限どんなノードでもサポートしているために、最低限の監視に使用可能

⌘ TCP/UDP Port Polling

- ☑ 各サービスポートを直接監視する方法。実際に稼動しているかを直接判断できるので、サーバプロセスの監視には有効

⌘ SNMP Polling

- ☑ SNMP(Simple Network Management Protocol)を用いて、ネットワーク機器のより詳細なデータを取得・監視を行う



ポーリング - ICMP / ping

⌘ ICMP echo/replyによりIP的動作確認をする

- ☑ 付帯情報: RTT : Round Trip Time
Packet Loss : パケット到達率

⌘ ホストの動作確認するもっとも簡単な手段

⌘ RTT/Packet lossは、時系列に整理すると回線品質を測る上で重要な情報として利用できる

```
$ multiping -t -c 10 www.apple.com www.bose.com
PING www.apple.com (17.254.0.91) (17.254.0.91): 56 data bytes
PING bose.com (146.115.60.42) (146.115.60.42): 56 data bytes
64 bytes from 17.254.0.91: icmp_seq=0 ttl=224 time=144 ms
64 bytes from 146.115.60.42: icmp_seq=0 ttl=237 time=207 ms
~省略~
64 bytes from 17.254.0.91: icmp_seq=9 ttl=224 time=151 ms
64 bytes from 146.115.60.42: icmp_seq=9 ttl=237 time=208 ms
```

```
-- -- PING statistics -- --
```

Remote Site	Number of Packets				Round Trip Time		
	Sent	Rcvd	Rptd	Lost	Min	Avg	Max
www.apple.com (17.254.0.91)	10	10	0	0%	143	144	151
bose.com (146.115.60.42)	10	10	0	0%	206	206	208
TOTALS	20	20	0	0%	143	175	20


```
$
```

18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10 : フリーソフトウェアによるネットワーク監視 15

ポーリング – ICMP/ping

- ⌘ pingにまつわるパラメータ
 - ☑ パケットサイズ
 - ☑ 送出回数
 - ☑ 送出間隔
 - ☑ タイムアウト
 - ☑ (送出内容)
- ⌘ SLA的な確認を行うためには、短時間に適正なタイムアウトを設定したping試験を行いたい
 - ☑ 特に 送出間隔・タイムアウト をきめ細かく制御したい


2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI 

18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10 : フリーソフトウェアによるネットワーク監視 16

ICMP/ping - ツール1

- ⌘ fping
 - ☑ <http://www.stanford.edu/~schemers/docs/fping/fping.html>
 - ☑ icmp echoについて特化。複数のホストを一気にチェックすることが可能
 - ☑ 送出間隔・タイムアウトが調整可能など、かなりの項目をきめ細くチューニングが可能
- ⌘ NOCOL multiping
 - ☑ <http://freshmeat.net/projects/nocol/homepage/>
 - ☑ ネットワーク監視ツールであるNOCOL (NOC OnLine) のサポートツールとして付属。multipingだけでも十分利用価値がある
 - ☑ 複数のホストにまとめて試験を行い、測定結果の表形式サマリーとして出力可能

2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI 


18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10 : フリーソフトウェアによるネットワーク監視 17

ICMP/ping - ツール2

- ⌘ sing
 - ☑ sing - Send ICMP Nasty Garbage packets to network hosts
 - ☑ <http://sourceforge.net/projects/sing>
 - ☑ ICMPパケットジェネレータ
 - ☑ ICMPパケットを自在にカスタマイズして、送出することに特化したツール
 - ☑ ICMP redirect, unreachableなどのパケットを自在に作成、送出できる

2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI



18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10 : フリーソフトウェアによるネットワーク監視 18

監視する手段 - TCP/UDP Port Polling


- ⌘ 各サービスポートを直接監視する方法。実際に稼動しているかを直接判断できるので、サーバプロセスの監視には有効
- ⌘ 各サービス用のクライアントを使ってチェックを行うものが多い
 - ☑ DNS : nslookup
 - ☑ radius : radping(dti-radius), radpwtst(merit)
 - ☑ http: lynx, w3m
 - ☑ telnetでたたくチェック

```

$ telnet www.eaccess.net 80 http(80)でアクセスしてみる
Trying 211.14.194.242...
Connected to www.eaccess.net.
Escape character is '^J'.          session確立
get /                               GET request送信
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<HTML><HEAD>
<TITLE>501 Method Not Implemented</TITLE>
</HEAD><BODY>
<H1>Method Not Implemented</H1>
get to /index.html not supported.<P>
Invalid method in request get /<P>
<HR>
<ADDRESS>Apache/1.3.12 Server at www.eaccess.net Port 80</ADDRESS>
</BODY></HTML>
Connection closed by foreign host.
$      結果が返ってきているのでOK! Serviceの起動確認

```

2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI




18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10 : フリーソフトウェアによるネットワーク監視 19

監視する手段 – SNMP Polling

- ⌘ 標準プロトコルベースでの管理方法
- ⌘ サーバー・クライアント型プロトコル
 - ☒ サーバー : SNMPマネージャー
 - ☒ クライアント : ネットワーク機器(エージェント)
- ⌘ ベンダーに依存せず、様々な機器において各種トラフィック・運用状況の監視が可能
- ⌘ ルーターやインテリジェントスイッチから詳細情報を得るにはもっとも一般的
- ⌘ アプリケーションサーバーでは個別にSNMP daemonを追加しなければならない場合が多い
 - ☒ 商用製品が多い。例 : HP OpenView


2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI 

18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10 : フリーソフトウェアによるネットワーク監視 20

SNMP : Simple Network Management Protocol

- ⌘ SNMP: Simple Network Management Protocol
 - ☒ UDP : polling port 161, trap port 162
- ⌘ マルチベンダーを実現するための2つのフレームワーク
 - ☒ 情報取得のための簡潔なプロトコル
 - ☒ 取得情報を標準化するMIB(Message Information Base)
- ⌘ 情報伝達の2つのモード
 - ☒ ポーリング
 - ☒ マネージャからエージェントに情報を要求する
 - ☒ トラップ
 - ☒ エージェントからマネージャに対してイベントを転送する

2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI 

18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10 : フリーソフトウェアによるネットワーク監視 21

SNMP Messages

- ⌘ GetRequest : manager agent
 - ☑ マネージャが更新情報を要求する
- ⌘ GetNextRequest : manager agent
 - ☑ マネージャがテーブルの次のエントリを要求する
- ⌘ GetResponse : manager agent
 - ☑ エージェントがマネージャからの要求に応答する
- ⌘ SetRequest : manager agent
 - ☑ マネージャが管理対象機器装置のデータを修正する
- ⌘ Trap : manager agent
 - ☑ エージェントがマネージャにイベントを通知する

2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI 

18-21, December 2000 Grand Cube Osaka Internet Week 2000


T10 : フリーソフトウェアによるネットワーク監視 22

SNMP Message Handling

```

    graph LR
      Manager[SNMP Server (Manager)] -- "GetRequest  
GetNextRequest" --> Agent[ネットワーク機器 (Agent)]
      Agent -- "GetResponse" --> Manager
      Manager -- "SetRequest" --> Agent
      Agent -- "Trap" --> Manager
  
```

The diagram illustrates the communication between an SNMP Server (Manager) and a Network Device (Agent). The Manager sends GetRequest and GetNextRequest messages to the Agent. The Agent responds with GetResponse messages to the Manager. The Manager sends SetRequest messages to the Agent. The Agent sends Trap messages to the Manager.

2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI 

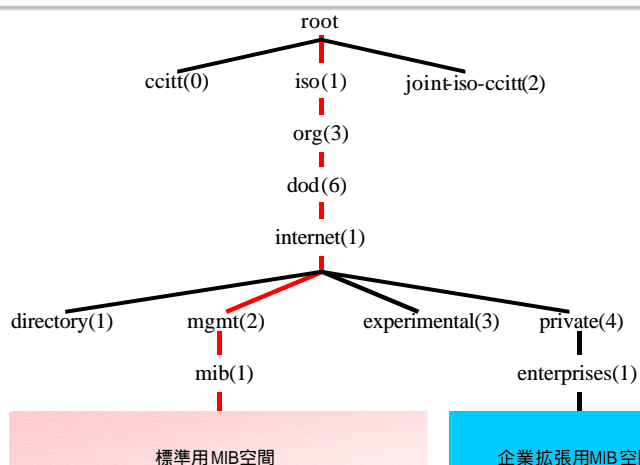


MIB (Message Information Base)

- ⌘ RFC-1213 インターネット標準 MIBv2
- ⌘ 階層的な命名体系で管理オブジェクトを定義
- ⌘ オブジェクト識別子(OID: Object ID)とMIB Symbol
- ⌘ 標準勧告部分 (MIBv2) と企業特有部分(Enterprise MIB)に分かれる



MIB Tree



18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10 : フリーソフトウェアによるネットワーク監視 25


MIB OID

※ 表記法 :

```
iso(1).org(3).dod(6).internet(1).mgmnt(2).mib(1).
```

1: system	システムグループ
2: interfaces	インタフェースグループ
3: at	アドレス変換グループ
4: ip	IPグループ
5: icmp	ICMPグループ
6: tcp	TCPグループ
7: udp	UDPグループ
11: snmp	SNMPグループ

2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI



18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10 : フリーソフトウェアによるネットワーク監視 26

監視する手段 - Event Trap

※ Local Event Trap

- ☑ システム状態監視(CPU,disk,process)
- ☑ Process個別処理状況監視
- ☑ Log file監視

※ Remote Event Trap

- ☑ syslog によるメッセージ伝達
- ☑ SNMP trap

2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI



18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10 : フリーソフトウェアによるネットワーク監視 27

監視する手段 – Event Trap: SNMP

- ⌘ SNMP trap
 - ☑ Pollingを待たずにSNMPエージェントからマネージャに情報を送る
 - ☑ トラップを利用してエージェントがマネージャに異常イベントの発生を知らせる
 - ☑ ポーリングの制御権は、マネージャが保持
 - ☑ SNMPのトラップ情報はUDPポート162に送られる

 - ☑ 詳細は第2部にてのべる


2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI 

18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10 : フリーソフトウェアによるネットワーク監視 28

第一部まとめ

- ⌘ IP通信はミッションクリティカルなインフラとなった
 - ☑ 通信を良好に維持するためには、定常的な監視が必要
 - ☑ こけさせないためには 予兆をつかむ
 - ☑ こけたら 障害発生を速やかに検知し、原因を早急に特定し、回復させる
- ⌘ 監視における切り口
 - ☑ 現状監視
 - ☑ 現状検知
 - ☑ 経過監視
- ⌘ これらは密接にからんだ独立事象
 - ☑ 3つの監視をもれなく行うことで、通信を安定維持させる

2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI 



第2部：フリーソフトウェアによる ネットワーク監視



何故フリーソフトを使用するか

- ⌘ 小規模なLANでも、手軽にネットワーク監視
- ⌘ 必要は発明の母
 - ☑ 必要だから作った。みんなの必要が集約
 - ☑ 実際に管理している人のノウハウが反映
- ⌘ アレンジ可能
 - ☑ さらに自分の必要を加えることができる
 - ☑ ソースに手を加えることが可能
 - ☑ 商用NMSですぐに対応できないところに適応する



フリーソフト導入の問題

- ⌘ 保証無し。全て自分の責任で
- ⌘ マニュアルが完備しているとは限らない
 - ☒ 最後はコードを読めというのかい
- ⌘ サポートがあるかどうか不明確
 - ☒ バグも結構あります。だれに相談する??
 - ☒ けど、作者が開発を止めているものもある
- ⌘ 高機能なものはインストール自体が大変
 - ☒ 他のフリーソフトへの依存度が高い

- ⌘ 結局は不明確というのが最大障壁か



フリーソフト導入の問題 - ならば

- ⌘ 不明確の整理。せめての一言をうめてみる
 - ☒ マニュアルがそろっていないよ
 - ☒ 不自由しない程度に完備しているツールを選べばよらしい
 - ☒ サポートはどこ?
 - ☒ 活発な公式MLがあるツール。作者のやる気も大事!
 - 活発ということはユーザが多いということ。迅速なバグ対処も期待できる
 - ☒ インストールが大変
 - ☒ Ports/Packageで逃げる
 - メジャーなツールならPorts/Packageになっているはず
 - ☒ インストールマニュアルがしっかり書いてあるツールを選ぶ



フリーソフトで作る監視システム

- ⌘ 全てを一つで満足することはできない
 - ☑ 満足するものに作り上げるための努力は無視できない
 - ☑ なんでも(そこそこに)できるは何もできないの法則
- ⌘ なら、適材適所の組み合わせで簡単に作る！

- ⌘ 監視システムを構成する3つのアイテム
 - ☑ 状態監視
 - ☑ 状態検知
 - ☑ トラフィック監視
- ⌘ システムへの統合はWEBで



監視における切り口 - 現状と経過 (再び)

- ⌘ 現状監視 - 今を見る : Polling
 - ☑ 現在のシステム状態を監視する
- ⌘ 現状検知 - 今を検知する : Event Trap
 - ☑ システムからの自律アラームをとらえる
- ⌘ 経過監視 - これまでを見る : Traffic Analysis
 - ☑ トラフィックの推移を監視。トレンドを把握する

- ⌘ これらは密接にからんだ独立事象
 - ☑ どれがぬけても片手落ち



監視システムへの要件1

- ☑ 集中監視・一斉通知
 - ☑ 人は分散できない・できるだけしたくない
 - ☑ 監視は1カ所で。通知はそこから一斉に

- ☑ 監視画面は各自の手元で
 - ☑ ...でも、自分の机で自分のPCでみたい



監視システムへの要件2


- ☑ 出先でも状態確認
 - ☑ リモートで対応するために遠隔で情報取得したい
 - ☑ 他人のPCでも状況確認できないと...
 - だれでも持っているソフト Web Browser
 - 状態確認に専用クライアントが必要なシステムは、いざというときには使い物にならない
 - X-Window, tcl/tkも同様
 - JavaもVM相性があるから結構苦しい

18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10 : フリーソフトウェアによるネットワーク監視 37

監視システムへの要件3 - 結論

- ⌘ WEB画面でリモート監視・リモート確認
- ⌘ E-mailで通知(まずは携帯へPager Call ? !)
- ⌘ WEB画面でトラフィック監視

2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI 

18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10 : フリーソフトウェアによるネットワーク監視 38

監視の切り口と使えるツール

- ⌘ 今を見る Polling Base状態監視
 - ☑ Big Brother, NOCOL, SPONG, mon, NetSaint, Scotty,...
- ⌘ 今を検知する Trap Base状態検知
 - ☑ Syslog + log監視ツール(SWATCH,LogSurfer,...)
 - ☑ Snmptrapd(UCD, CMU),...
- ⌘ これまでを見る トラフィック監視
 - ☑ MRTG+RRDTools, Seafelt, Shepherd, RRDTools+Frontends(Remstat,Cricket,ORCA,NRG), ...

2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI 

18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10 : フリーソフトウェアによるネットワーク監視 39

監視システムのモデル

equipment polling traffic monitor event trap alarm notification

Basic IF Traffic Grabber SNMP pkg log mon warning notifier

extension IF / Plug-ins

Network Monitor Base System

2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI **eAccess**

18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10 : フリーソフトウェアによるネットワーク監視

フリーソフトウェアによる ネットワーク監視

Big Brother Network Monitor

eAccess

2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI



Polling base 状態監視ツール

⌘ 去年は以下のものを紹介していました

- ☑ Big Brother
- ☑ SPONG
- ☑ NOCOL
- ☑ Mon
- ☑ Angel monitor

⌘ 今年はBig Brother 一本で勝負！

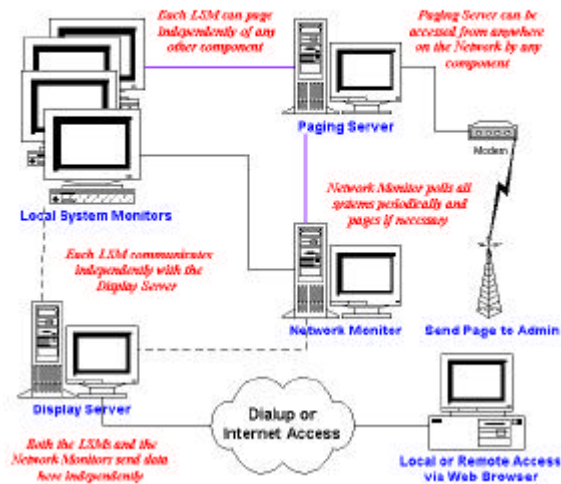


状態監視ツール - Big Brother

- ⌘ <http://bb4.com/>
- ⌘ WEB Baseの監視システム
 - ☑ オープンソースであるが、フリーソフトではない
 - ☑ 通常使用においては費用は発生しない
- ⌘ 監視・表示・通知機能をモジュール分割しており、それぞれを別サーバに分散することで、大規模ネットワークまで適用可能
- ⌘ ICMP/TCPポーリングによる監視を行う
 - ☑ 監視可能サービス: ping, smtp, http, pop3, dns, ftp, telnet, ssh, imap
 - ☑ サーバー個別監視: CPU, disk, processes, logs
- ⌘ 各種Unix/NT/NetWare/Macintoshの監視用プローブがあり、複合OS統合監視が可能



Big Brotherサーバー構成



2000.12.19

Copyright 2000, eAccess Ltd, Shigeki YAHAGI



状態監視ツール - Big Brother 続き

- ⌘ 監視対象のグループ化機能
- ⌘ 監視画面の階層化機能(2段階)
- ⌘ 柔軟なアラーム通知機能
 - ☑ E-mailによりアラームを通知する。snmptrapによる通知も可能
 - ☑ ホスト単位にシステムの停止時間を設定。自動で監視対象から除外可能
 - ☑ ホスト単位で障害通知先を変更可能
 - ☑ アラームの検出されている機器のみサマリーした画面を標準で生成。便利!
 - ☑ アラームメッセージに障害情報ページのURLが引用されており、迅速に障害情報に到達できる!

2000.12.19

Copyright 2000, eAccess Ltd, Shigeki YAHAGI


18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10 : フリーソフトウェアによるネットワーク監視 45

状態監視ツール - Big Brother 続き

- ⌘ 障害履歴機能
- ⌘ システム稼動状況レポート作成機能(v1.5より追加)
- ⌘ 拡張インターフェースが公開されており、非常に多彩な拡張監視モジュールが存在する(後述)
 - ☑ オープンソースの利点を生かし、BB基本ソフトをそのまま置換する機能拡張版ソフトも存在する
 - ☑ 他ソフトとの連係：例えばMRTG、RRDTool
 - ☑ BBTray : Big Brother監視ツール on Windows
- ⌘ マニュアルがかなり整っている。:-)
 - ☑ 各モジュールの構成にまで踏み込んだ解説付き
- ⌘ 適用範囲：ネットワーク監視、気象情報監視
株価監視(?!),...

2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI



18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10 : フリーソフトウェアによるネットワーク監視 46

BB - 監視画面 (TOP)



big brother last update Sat Nov 4 14:17:15 MET 2000

Big Brother	SMTP	SNMP	HTTP	TELNET	POP3	IMAP	IRC	SSH
pci79.hrz.tu-drestadt.de	ok	ok	ok	ok	ok	ok	ok	ok
wandl.hrz.tu-darmstadt.de	ok	ok	ok	ok	ok	ok	ok	ok
dbt.hrz.tu-darmstadt.de	ok	ok	ok	ok	ok	ok	ok	ok

Pages Wasted Locally

- MAMM und E-NIM ●
- MMN (FH Wiesbaden, H3 und HMN) ■
- HRZ-Rechner ●
- Roaming-Partner am ISM/Medapool ●
- Verschiedenes ●

● ok
 ● attention
 ■ trouble
 ■ no report
 ■ unavailable
 ■ offline

2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI



18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10 : フリーソフトウェアによるネットワーク監視 47

BB - 監視画面 (sub)

2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI

eAccess

18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10 : フリーソフトウェアによるネットワーク監視 48

BB- アラートサマリ

2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI

eAccess

18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10 : フリーソフトウェアによるネットワーク監視 49

BB - イベント情報画面

The screenshot displays the 'big brother' interface with the following content:

```

big brother
last update
Sat Nov 4 18:36:41 2000

pc302.hrz.tu-darmstadt.de - disk

yellow Sat Nov 4 18:36:42 CET 2000 - Disk on pc302.hrz.tu-darmstadt.de at WARNING level

/opt (94%) has reached the defined disk space WARNING level (95%)

/ow/hdc1      29978      4857      24888      21% /boot
/ow/hdc2      761252     261512     522984     68% /usr/src
/ow/hdc3      3517824    1887952    2598856    65% /usr/wmware
/ow/hdc5      343993     69369     65293      2% /
/ow/hdc7      3824784    563016    4286600    57% /usr
/ow/hdc8      2443457    1761552    976608     64% /usr
/ow/hdc6      3824784    638783    113644     6% /usr/local
/ow/hdc9      18139264   16237152   2962112    98% /export/ftp
/ow/hdc5      3824784    623708    18968     6% /opt
/ow/hdc10     11175879   11131808   44811      100% /export
  
```

2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI

18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10 : フリーソフトウェアによるネットワーク監視 50

BB - ヒストリ画面

The screenshot displays the 'big brother' interface with the following content:

```

big brother
history
Sat Nov 4 12:34:22 EST 2000

Fri Nov 3 12:34:22 2000 Sat Nov 4 12:34:22 2000
[Timeline showing disk usage bars for various directories]

www.bb4.com - mrtg

Last 24 Hours
[Colorful bar chart showing network usage]
[Legend: 100% 75% 50% 25% 0%]

Last 30 log entries (Full HTML log)
[Log entries showing dates and times]
  
```

2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI

18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10 : フリーソフトウェアによるネットワーク監視 51

BB - 稼動レポート作成



2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI



18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10 : フリーソフトウェアによるネットワーク監視 52

BB - 稼動リポート(top)



2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI



18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10 : フリーソフトウェアによるネットワーク監視 53

BB - 稼動リポート(sub)

The screenshot shows the 'big brother' availability report for the period Jan 1 2000 - Oct 1 2000. It displays a table with columns for 'AGN', 'Externs', and 'Strata'. Each row lists a domain and its corresponding status metrics (Load, Stop, Up, etc.). A legend at the bottom indicates status levels: 100% available (green), over 5% (yellow), less than 5% (red), and no data for period (grey).

2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI

18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10 : フリーソフトウェアによるネットワーク監視 54

BB - 稼動リポート(text出力)

```

* Availability Report
Oct 17 2000 - Nov 1 2000

dev01.lab.eaccess.net - cpu
Availability: 95.52%

Red      Yellow Green Purple Clear Blue
4.48%   2.11% 93.41% 0.00% 0.00% 0.00%

Event logs for the given period

Event Start      Event End      Status Seconds Cause
Mon Oct 30 20:13:42 2000      Mon Oct 30 20:18:42 2000      yellow 300      up: 12 days, 2 users, 48 procs, load=703
Mon Oct 30 05:38:43 2000      Mon Oct 30 05:43:43 2000      yellow 300      up: 11 days, 2 users, 48 procs, load=708
Sun Oct 29 15:03:44 2000      Sun Oct 29 15:08:44 2000      yellow 300      up: 10 days, 3 users, 51 procs, load=725
Sun Oct 29 10:53:45 2000      Sun Oct 29 10:58:45 2000      yellow 300      up: 10 days, 3 users, 51 procs, load=702
Sun Oct 29 08:03:49 2000      Sun Oct 29 08:08:46 2000      yellow 297      up: 10 days, 3 users, 51 procs, load=708
Sun Oct 29 00:28:46 2000      Sun Oct 29 00:33:46 2000      yellow 300      up: 10 days, 3 users, 51 procs, load=773
Sat Oct 28 20:23:47 2000      Sat Oct 28 20:28:47 2000      yellow 300      up: 10 days, 3 users, 51 procs, load=710
Sat Oct 28 09:53:47 2000      Sat Oct 28 09:58:48 2000      yellow 301      up: 9 days, 4 users, 56 procs, load=715
Sat Oct 28 06:18:48 2000      Sat Oct 28 06:23:47 2000      yellow 299      up: 9 days, 4 users, 66 procs, load=713
Sat Oct 28 03:33:48 2000      Sat Oct 28 03:43:47 2000      yellow 599      up: 9 days, 4 users, 90 procs, load=806
Sat Oct 28 02:03:46 2000      Sat Oct 28 02:08:46 2000      yellow 300      up: 9 days, 4 users, 75 procs, load=713
Wed Oct 18 12:41:25 2000      Wed Oct 18 21:21:35 2000      yellow 31210     up: 4 days, 2 users, 43 procs, load=415
Tue Oct 17 16:06:23 2000      Wed Oct 18 12:41:25 2000      red      74102      up: 3 days, 1 users, 64 procs, load=464

Time Critical/Offline: 20 hours 35 mins 2 secs
Time Non-Critical: 9 hours 40 mins 6 secs

```


2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI

18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10 : フリーソフトウェアによるネットワーク監視 55

BB - 設定ファイル

- ⌘ etc/bb-hosts:
 - ☑ 監視対象定義ファイル
- ⌘ etc/bb-warnrule.cfg:
 - ☑ 障害通知定義ファイル
- ⌘ etc/bbdef.sh:
 - ☑ システム監視定義ファイル
- ⌘ その他
 - ☑ etc/security.INFO


2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI 

18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10 : フリーソフトウェアによるネットワーク監視 56

BB - etc/bb-hosts - 1

- ⌘ 監視対象の定義ファイル
- ⌘ 記述方法は/etc/hosts の拡張版に近い
- ⌘ 監視対象の記述 :
 - ☑ `<IP Address> <Host Name> [# <Service> {<Service>}]`
 - IP Address: 監視対象のIP Address
 - Host Name: 監視対象のホスト名
 - Service: サーバー機能及び監視サービス。

2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI 



Big Brotherの設定例 - bb-hosts

```
% $ cat bb-hosts
#
# THE BIG BROTHER HOSTS FILE
#
192.168.0.10 kansil.foo.co.jp # BBPAGER BBNET BBDISPLAY http://kansil/

group-compress <H3><I>foo.co.jp Servers</I></H3>
192.168.0.2 ns1.foo.co.jp # dns ssh !telnet
192.168.0.3 mail.foo.co.jp # dns smtp pop3 ssh !telnet
192.168.0.5 www.foo.co.jp # telnet ssh ftp http://www.foo.co.jp/

# router interface entry
page Router-IF "Router Intereface"
group-compress <H3><I>Router1 Interfaces</I></H3>
192.168.0.1 gw1.foo.co.jp
192.168.0.50 gw2.foo.co.jp
group-compress <H3><I>Router2 Interfaces</I></H3>
192.168.1.2 tok-yok-ma30.wan.foo.co.jp
192.168.1.6 tok-osa-dr15.wan.foo.co.jp
$
```



BB - etc/bb-hosts - 2


- ※ Serviceには以下のものを記述可能。
 - ☑ サーバー機能 : BBNET, BBPAGER, BBDISPLAY
 - ☑ BBDISPLAY: ネットワーク監視画面サーバーが動いていることを指示
 - ☑ BBPAGER: ネットワーク警報通知サーバーが動いていることを指示
 - ☑ BBNET: ネットワーク監視サーバーが動いていることを指示
 - ☑ ping監視はデフォルトで行われる。以下のアレンジも可能
 - ☑ noping: ping監視を行わない。監視対象外の表示はする
 - ☑ noconn: ping監視を行わない。表示自体も消す
 - ☑ dialup: ping監視結果:NGにて、アラームをあげない
 - ☑ 監視サービス : smtp, http, pop3, dns, ftp, telnet, ssh, imap
 - ☑ httpはURL指定する。例: http://www.foo.co.jp/top.shtml
 - ☑ 以下のアレンジが可能。
 - !telnet : telnet portが開いている際に警告を行う。
 - ~telnet : 試験は通常通りに行い、逆の結果を返す。
 - 例: 試験OK:赤、試験NG:緑

18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10 : フリーソフトウェアによるネットワーク監視 59

BB – etc/bb-hosts - 3

- ※ 特殊設定項目: `dialup modem-bank`
 - ☒ DHCP/ダイヤルアップのアドレスプールの使用状況を確認する
 - ☒ 例: `dialup modem-bank 192.168.0.92 16`
 - 計測時間がかかるので、あまり多くのプール監視はむかないと思う
- ※ 画面修飾関係の設定
 - ☒ 表示グループ指定: `group, group-compress`
 - ☒ `group(-compress) <group name>`
 - ☒ この指定以下の計測対象をひとつの表示サブグループとして固めて表示する
 - `group`: すべての計測項目を表示する
 - `group-compress`: サブグループ内にて計測される項目のみ表示する
 - ☒ サブページ指定: `page`
 - ☒ `page <page name> <page title>`
 - ☒ この項目以下の計測対象をサブページにまとめる
 - ☒ 画面上は<page name>の項目にまとめて表示される。状態表示アイコンからサブページにリンクがはられる




2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI

18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10 : フリーソフトウェアによるネットワーク監視 60

BB - etc/bbwarnrule.cfg

- ※ 警告通知に対するルールを記述する
- ※ 記述方法:
 - ☒ `hosts;exhosts;services;exservices;day;time;recipients`
 - ☒ `hosts`: 一致するホスト ("*"はワイルドカード)
 - ☒ `exhosts`: 除外するホスト
 - ☒ `services`: 一致するサービス ("*"はワイルドカード)
 - ☒ `exservices`: 除外するサービス
 - ☒ `day`: 0-6 (日曜日-土曜日)
 - ☒ `time`: 0000-2359
 - ☒ `recipients`: メールアドレス
 - ☒ `hosts, services`についてはワイルドカード指定可能



2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI

18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10: フリーソフトウェアによるネットワーク監視 61

Big Brotherの設定例 – bbwarnrule.cfg

```

% $ cat bbwarnrules.cfg
# bbwarnrules.cfg
ns1.* mail.*;*;*;*;server-admin@foo.co.jp
## ns1.*, mail1.*については24H/7Dの監視を行い、障害時はserver-adminに通知する
www.*;http;*;*;web-admin@foo.co.jp yahagi
## www.*についてはhttpのみ24H/7Dの監視を行い、
## 障害時はweb-adminとyahagiに通知する
strage.*;*;conn;0-6;0000-0259 0500-2359;strage-admin@foo.co.jp
## strage.*はping以外の監視を行い、障害時はstrage-adminに通知する
## ただし、AM3:00-AM4:59までの間は監視対象外とする
intra.*;*;1-5;0800-2000;intra-admin@foo.co.jp
## intra.*は月曜日から金曜日のAM8:00-PM8:00まで全てのサービス監視を行い、
## 障害時はintra-adminに通知する
*;*;*;*;admin@foo.co.jp
## 上記以外のホストの障害検知についてはadmin@foo.co.jpに通知する。
unmatched-*;*;*;*;bb@localhost
## bb-hosts定義外のイベント (unmatched-*)検知についてはbb@localhostに通知する
# end of bbwarnrules.cfg
$

```

2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI



18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10: フリーソフトウェアによるネットワーク監視 62


etc/bbdef.sh - 1

- ※ Big Brotherが発生した状況への反応定義を行う
- ※ また、外部拡張監視(plugin)の登録も行う

- ※ ディスク容量テスト設定:DFWARN, DFPANIC
 - ☒ ディスク容量テストの閾値を%レベルで表記する
 - ☒ DFWARN - warning設定値 (default:90%)
 - ☒ DFPANIC - panic設定値 (default:95%)
 - ☒ サーバ全体に関する設定であり、パーティションごとに閾値を設定・管理したい場合にはetc/bb-dftabファイルに詳細設定を行う

- ※ CPU load averageテスト設定:CPUWARN, CPUPANIC
 - ☒ load averageを元にシステムプロセス稼働状況監視のための設定
 - ☒ 設定値 = load average(uptimeからの値) * 100
 - ☒ CPUWARN - warning設定値 (default:150)
 - ☒ CPUPANIC - panic設定値 (default:300)

2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI




18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10 : フリーソフトウェアによるネットワーク監視 63

etc/bbdef.sh - 2

- ※ プロセス監視設定:PROCS, PAGEPROCS
 - ☑ 起動確認したいプロセスを定義する。後述
- ※ メッセージ監視設定:MSGs, PAGEMSGs, IGNMSGs
 - ☑ システムログでエラーメッセージを監視したい場合に利用する
 - ☑ MSGs - warning対象キーワード
 - ☑ PAGEMSGs - panic対象キーワード
 - ☑ IGNMSGs - 識別対象外キーワード
 - ☑ それぞれの変数には":"をデリミタとすることで、複数のキーワードを設定可能
- ※ 警報レベル設定: PAGELEVELS
 - ☑ 警報を行うイベントレベルを設定する。デフォルトは"red purple"
- ※ 外部機能拡張登録: BBMKBBEXT, BBMKBB2EXT, BBEXT
 - ☑ 外部機能拡張(plugin)の登録を行う。詳細は後述

2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI



18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10 : フリーソフトウェアによるネットワーク監視 64


設定例 - bbdef.sh

```

※ $cat bbdef.sh
#! /bin/sh
# bbdef.sh
【省略】
# LOCAL CLIENT MONITORING CONFIGURATION FOR bb-local.sh
# WARNING AND PANIC LEVELS FOR LOCAL SYSTEM INFORMATION
# YOU CAN SET VALUES ON A SPECIFIC FILESYSTEM BY USING
# THE etc/bb-dftab FILE
DFWARN=85 # (YELLOW) DISK % TO WARN
DFPANIC=95 # (RED) DISK % TO PANIC
export DFWARN DFPANIC
# CPU LEVELS ARE THE 5 MINUTE LOAD AVERAGE x 100
CPUWARN=3000 # (YELLOW) WARN AT LOAD AVG OF 30 (default:1.5)
CPUPANIC=6000 # (RED) PANIC AT LOAD AVG OF 60 (default:3)
export CPUPANIC CPUWARN
# PROCESS MONITORING
# THESE VALUES ARE OVERRIDDEN BY THE etc/bb-proctab FILE
PROCS="bbrun smptrapd httpd inetd" # (YELLOW) WARN IF NOT RUNNING
PAGEPROC="cron radiusd sshd syslogd" # (RED) PAGE IF NOT RUNNING
export PROCS PAGEPROC
# MESSAGE FILE MONITORING (/var/adm/messages or similar)
CHKMSGLEN="TRUE" # MAKE SURE MSG FILE IS NON-ZERO LEN
MSGs="NOTICE WARNING" # (YELLOW) MESSAGES TO WATCH FOR
AGEMSG="NOTICE" # (RED) PAGE IF WE SEE THIS MESSAGE
IGNMSGs="" # List of messages to ignore if string(s) matches line
【省略 - 続く】

```

2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI



18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10 : フリーソフトウェアによるネットワーク監視 65

設定例 - bbdef.sh 続き

```

* 【省略 - 続き】
# Default colors to send notification messages on
PAGELEVELS="red purple" # Default red purple
export PAGELEVELS
# Specify scripts to execute while running mkbb.sh/mkbb2.sh
# Echo from them will be displayed on the generated web page
BMKBBEXT="bbradius.sh"
BMKBB2EXT="eventlog.sh"
export BMKBBEXT BMKBB2EXT
【省略】
# EXECUTE LOCAL SCRIPTS FROM HERE...
# SCRIPTS SHOULD LIVE IN $BBHOME/ext DIRECTORY
# BBEXT CONTAINS THE FILENAMES TO EXECUTE
# SEPERATE THE SCRIPTS WITH A SPACE: BBEXT="ext1.sh ext2.sh"
BBEXT="larrd/larrd.pl larrd/bf-larrd.sh"
export BBEXT
【省略】
$

```

2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI



18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10 : フリーソフトウェアによるネットワーク監視 66

etc/bbdef.sh - プロセス監視定義


- * プロセス監視設定:PROCS, PAGEPROCS
 - ☑ 起動確認したいプロセスを定義する
 - ☑ PROCS - warning対象プロセス
 - ☑ PAGEPROCS - panic対象プロセス
- * 非起動確認についてもサポートしており、その際にはプロセス名の前に"!"を付加設定する
- * セキュリティー上あがっているまずいプロセスの監視につかえる
 - ☑ ex: !inetd, !sendmail, ...
 - ☑ 設定例


```

# PROCESS MONITORING
# THESE VALUES ARE OVERRIDDEN BY THE etc/bb-proctab FILE
PROCS="bbrun snmptrapd httpd !inetd" # (YELLOW) WARN IF NOT RUNNING
PAGEPROC="cron radiusd sshd syslogd" # (RED) PAGE IF NOT RUNNING
export PROCS PAGEPROC

```

2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI



18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10 : フリーソフトウェアによるネットワーク監視 67

procs監視の話



2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI

eAccess

18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10 : フリーソフトウェアによるネットワーク監視 68

BB - extensions

- ⌘ 拡張インターフェースが公開されており、非常に多彩な拡張監視モジュールが存在する
 - ☑ オープンソースの利点を生かし、BB基本ソフトをそのまま置換する機能拡張版ソフトも存在する
 - ☑ <http://www.deadcat.net/>
 - ☑ Enhancement script to BB
 - ☑ モジュールごと拡張版への置換
 - ☑ External plug-in script for BB
 - ☑ 外部拡張スクリプトによる機能追加

2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI

eAccess



BB – extensions & plug-ins

⌘ 実現されるもの

- ☑ さらなるアプリケーションの監視 :
 - ☑ radius, ntp, ldap, smb, mqueue, ...
 - ☑ RDBS (oracle, infomix, sybase, postgres, MySQL, ...)
 - ☑ 他システム監視 : RAS, UPS, RAID, Printer, ...
- ☑ 他ソフトとの関係 : 例えば MRTG, RRDTOOLS
- ☑ モジュールへの入れ替えによる高速化
- ☑ BBTray : Big Brother監視ツール on Windows



BB - Extension Archive

Date	FTP	HTTP	Enhancements scripts to BB
20/4/2000	bb-silversta.sh	bb-silversta.W	CGI script to display "all" the events that have occurred. Track various events about a UPS.
20/10/1999	bb-stpcheck.sh	bb-stpcheck.sh	If you have more than 2 DBSERVER's then this script run from cron will send a status of any DBSERVER to 2 other DBSERVER's. It will send file to up to dbserver1/dbserver2. This check will turn purple when machine/cron is down.
5/6/2000	bb-rrdcheck.tar.gz	bb-rrdcheck.tar.gz	No description currently available
20/10/1999	bb-ftp-ofshoppers.tar	bb-ftp-ofshoppers.tar	A replacement for the standard bb-host.sh which shows uptime percentages for disks, walls, memory and ports and also it will send e-mails to the whoever is in charge.
20/9/2000	bb-host-1.5.tar.gz	bb-host-1.5.tar.gz	Alternate images for BB. New versions of green, yellow, red, and purple gif files. These images were originally created to make it easier for colour blind browsers to see status levels. This set uses different shapes for each color: green - rounded square (like default BB icons), yellow - triangle, red - diamond, purple - square.
20/10/1999	bb-images-alt-arr81.sh	bb-images-alt-arr81.sh	Alternate images for BB. New versions of green, yellow, red, and purple gif files. These images were originally created to make it easier for colour blind browsers to see status levels. This set uses different shapes for each color: green - check mark, yellow - rolling circle (CC), red - large cross (X), purple - question mark (?)
20/10/1999	bb-images-alt-arr82.sh	bb-images-alt-arr82.sh	Alternate images for BB. New versions of green, yellow, red, and purple gif files. These images were originally created to make it easier for colour blind browsers to see status levels. This set uses different shapes for each color: green - check mark, yellow - rolling circle (CC), red - large cross (X), purple - question mark (?)
20/10/1999	bb-infomix.sh	bb-infomix.sh	A script which can be called from so-local to ensure that infomix database is running.



18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10 : フリーソフトウェアによるネットワーク監視 71

BB enhancement - Japanese Help

2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI

eAccess

18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10 : フリーソフトウェアによるネットワーク監視 72

BB extensions - Japanese Help

- ⌘ マニュアルの日本語化されたもの
 - ☑ 作者不明??
- ⌘ ちょっと古くてver 1.4ぐらいの内容
- ⌘ <http://www.deadcat.net/BB/japanese-help.tar.gz>
- ⌘ www/help以下をこれに入れ替えるだけですべてのマニュアルが日本語化される
 - ☑ 硬い日本語であるが、かなり助かります

2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI

eAccess

18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10 : フリーソフトウェアによるネットワーク監視 73

Big Brother - extensions

2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI

eAccess

18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10 : フリーソフトウェアによるネットワーク監視 74

拡張ヒストリー

- ※ <http://www.deadcat.net/BB/bb-hist-2.5.tar.gz>
- ※ /cgi-bin/bb-hist.shの置換プログラム
- ※ イベントヒストリ解析を拡張し、日間・週間・月間・年間のイベント状況を棒グラフにて表示する
 - ☑ MRTG的イベント解析
 - ☑ 長期トレンドにてシステムの稼動状況をみることができ、障害間隔などの状況も把握しやすいことから、かなり重宝する
- ※ bb-hist.plとして提供されており、これを/cgi-binのbb-hist.shと置換することで、追加を行う

2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI

eAccess

18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10 : フリーソフトウェアによるネットワーク監視

75

BBTray - Big Brother監視サポートツール

⌘ Big Brother Display Serverを常時監視するサポートツール

- ☑ <http://www.deadcat.net/BB/BBtray-0.5-1.zip>
- ☑ Windows9x/NT/2000で動作
- ☑ BBを監視し、状態が変化するとPopup Windowにて通知
 - ☑ 派手な警報音付き！
- ☑ Windowをクリックすることで、障害サマリー画面に直接とべるので、即時に現状把握可能
 - ☑ BBサーバーとIP通信ができれば、どこでも現状が分かる
 - 客先で鳴ると非常に恥ずかしい！☹
- ☑ 類似品にtkBB(Tk-Perl版)あり

2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI

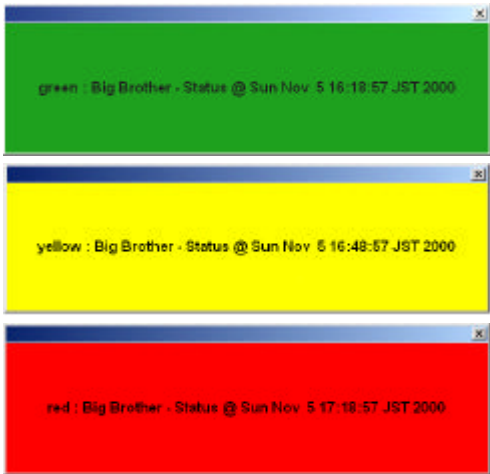


18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10 : フリーソフトウェアによるネットワーク監視


76

BBTray - 続き



- Green Window
- this is normal status
- Yellow Window
- this is warning status.
- Red Window
- this is critical status!!

2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI



18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10 : フリーソフトウェアによるネットワーク監視



フリーソフトウェアによる ネットワーク監視

UCD-SNMP(Net-SNMP) snmptrapd

2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI



18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10 : フリーソフトウェアによるネットワーク監視 78



UCD-SNMP(Net-SNMP) Package

- ⌘ <http://sourceforge.net/projects/net-snmp>
- ☑ OLD SITE = <http://ucd-snmp.ucdavis.edu/>
- ⌘ さまざまなUnixプラットフォームで稼動するSNMP Package
- ⌘ 以下のコマンドを提供
 - ☑ snmpd, snmptrapd, snmpbulkwalk, snmpget, snmpset, snmpstat, snmptranslate, snmpwalk, snmpdelta, snmpnetstat, snmptranslate, snmptrap

2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI





UCD-SNMP snmptrapd

- ⌘ 外部からのSNMP trap eventを監視するdaemon
- ⌘ trap eventごとに処理を規定することが可能
- ⌘ Trap受信後、以下の処理を行う
 - ☑ 外部コマンドがアクションとして規定されている際には、アクションである外部コマンドの標準入力に受信したTrap eventを渡し、コマンドを起動する
- ⌘ Trap受信によりアラートなどの通知を行うことが可能
- ⌘ Snmptrapd.confの記述
 - ☑ traphandle <OID> <action> <parameters...>
 - ☑ traphandle default <action> <parameters...>



snmptrapd.confの例

```

⌘ # SNMP Trap : Cold Start
⌘ traphandle .1.3.6.1.6.3.1.1.5.1 /usr/bin/mail -s "coldStart Trap"
  admin@foo.co.jp
⌘ # SNMP Trap : Warm Start
⌘ traphandle .1.3.6.1.6.3.1.1.5.2 /usr/bin/mail -s "warmStart Trap"
  admin@foo.co.jp
⌘ # SNMP Trap : Link Down
⌘ traphandle .1.3.6.1.6.3.1.1.5.3 /usr/bin/mail -s "linkDown Trap"
  admin@foo.co.jp
⌘ # SNMP Trap : Link Up
⌘ traphandle .1.3.6.1.6.3.1.1.5.4 /usr/bin/mail -s "linkUp Trap"
  admin@foo.co.jp
⌘ # SNMP Trap : Authentication Failure
⌘ traphandle .1.3.6.1.6.3.1.1.5.5 /usr/bin/mail -s "authFail Trap"
  admin@foo.co.jp
⌘ # SNMP Trap : Other
⌘ traphandle default /usr/bin/mail -s "Other Traps" yahagi@foo.co.jp

```




snmptrapd - ciscoでのsnmp関連config例

```
% access-list 30 permit 192.168.100.1

% snmp-server contact admin@foo.co.jp
% snmp-server location YOKOHAMA-IW99
% snmp-server community himitsu RO 30
% snmp-server enable traps config
% snmp-server host 192.168.100.1 NAISHO tty config envmon snmp
```



snmptrapd - 通知結果

```
% From: log-admin <root@log.foo.co.jp>
% To: admin@foo.co.jp
% Date: Mon, 1 Nov 1999 22:01:49 +0900 (JST)
% Subject: linkDown Trap

% nspix2-gw.foo.co.jp
% 192.168.244.21
% system.sysUpTime 24:10:03:09.12
% .iso.org.dod.internet.snmpV2.snmpModules.snmpMIB.snmpMIBObjects.snmpTrap.snmpTrapOID
% .iso.org.dod.internet.snmpV2.snmpModules.snmpMIB.snmpMIBObjects.snmpTraps.linkDown
% interfaces.ifTable.ifEntry.ifIndex.1 1
% interfaces.ifTable.ifEntry.ifDescr.1 "Fddi1/0/0"
% interfaces.ifTable.ifEntry.ifType.1 Fddi
% enterprises.9.2.2.1.1.20.6 "administratively down"
% .iso.org.dod.internet.snmpV2.snmpModules.snmpMIB.snmpMIBObjects.snmpTrap.snmpTrapEnterprise
% enterprises.9.1.48
```



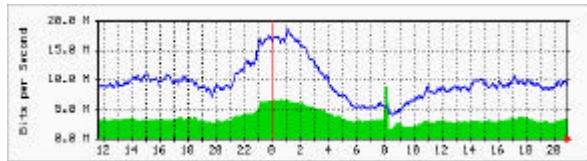
フリーソフトウェアによる ネットワーク監視

MRTG (Multi Router Traffic Grapher)

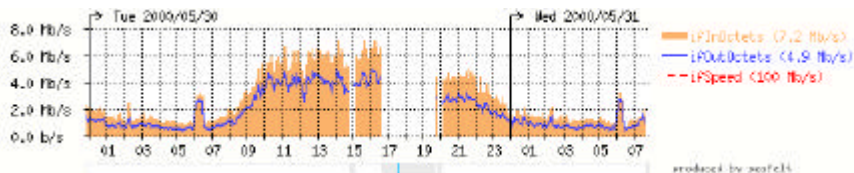


これまでを見る監視ツール

⌘ MRTG (Multi Router Traffic Grapher)



⌘ Seafelt




18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10 : フリーソフトウェアによるネットワーク監視 85

seafelt

- ⌘ URL: <http://seafelt.unicity.com.au/>
- ⌘ MRTGと同様のことはほとんど可能な上、高速
 - ☑ RDBをバックエンドにした高速エンジン
 - ☑ 要求に応じてグラフを作成
- ⌘ seafelt health barというステータスバーがグラフ下部に表示されており、以下の装置ステータスを表示可能
 - ☑ Interface Reset
 - ☑ System Reboot/Downtime
 - ☑ データ未取得時間
- ⌘ 機器にインタフェースを追加した際、自動的にそのインタフェースを追加して計測を開始可能
- ⌘ 必要なもの :
 - ☑ mySQL, gd, libpng, python,, libz, ucd-snmp, POSIX messag
 - ☑ かなり他のソフトに依存しているので、インストールは面倒

2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI

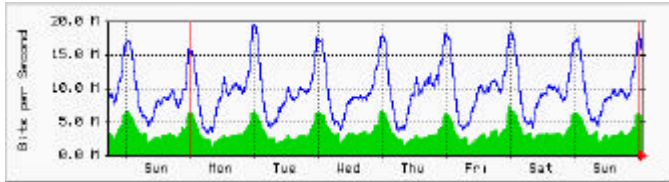


18-21, December 2000 Grand Cube Osaka Internet Week 2000


T10 : フリーソフトウェアによるネットワーク監視 86

MRTGとは

- ⌘ <http://ee-staff.ethz.ch/~oetiker/webtools/mrtg/mrtg.html>
- ⌘ <http://www.ceres.dti.ne.jp/~riocat/webtools/mrtg/>
(日本語翻訳サイト)
- ⌘ MRTG : Multi Router Traffic Grapher
- ⌘ 2系列のデータを基に集計を行い、短期・中期・長期トレンドグラフを生成するツール



2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI





MRTGの特徴

- ⌘ ほとんどのUnixプラットフォームとWindowsNT上で稼動
- ⌘ 独自にSNMPを実装。外部のSNMP Packageは不要
- ⌘ 定期的にログをサマリーするデータ管理を行っており、ログファイルのサイズが大きくなるしない
- ⌘ 半自動のコンフィグ作成ツールが付属
- ⌘ 日・週・月・年ごとにデータを集計したWEBページを結果として生成する
 - ☑ 便利！便利！便利！
- ⌘ コンフィグからindexを簡単に生成するツールが付属



MRTGの新機能 - 1

- ⌘ v 2.9より以下の機能が追加
 - ☑ Daemon化指定: RunAsDaemon: , Interval:
 - ☑ MRTGのPerl ProcessをDaemonにすることにより、Perl起動にかかるFork処理をなくし、高速化する。計測周期はIntervalにより指定する
 - ☑ 並列照会: Forks:
 - ☑ 照会処理の並列化度を指定する。このオプション指定により、無応答の照会処理がボトルネックとなって、プロセスの完了時間が延びることを防ぐことが可能となる
 - ☑ Unixプラットフォームでのみサポート
 - ☑ Target[]への新たな指定方法追加
 - ☑ 以下のInterface属性をキーに、当該インタフェースを特定する
 - MAC address指定
 - Description指定
 - Interface Name指定
 - Interface Type指定



MRTGの新機能 - 2

※ v 2.9より以下の機能が追加(続き)

☒ RRDTOOLSとの統合 : LogFormat: rrdtool

- ☒ logの管理をRRDToolを使用することにより、劇的な高速化を実現するこれまでのlogについては本オプション指定により自動的にデータ移行がなされる
- ☒ このオプション指定することで、グラフの作成は測定時はなされず、付属の14all.cgiによりon the flyで(要求のたびに)作成をする
- ☒ 10倍以上高速になることも



MRTG - cfgmaker - 1

※ mrtg付属の簡易設定ツール

- ☒ `cfgmaker { <option> } <community>@<target>`
- ☒ `<community> : snmp community string`
- ☒ `<target> : target address or hostname`
- ☒ 例: `$ cfgmaker himitsu@ix-gw.foo.co.jp > ix-gw.cfg`

※ communityとtargetを指定するだけで機器に存在するインタフェースをサーチし、ifInOctets/ ifOutOctetsを測定する設定の大部分を作成する

- ☒ syscontact/locationなどの情報からコメントも自動作成
- ☒ 保守停止しているインタフェースについてはコメントとして作成
- ☒ 追加設定は WorkDir: だけでほぼ動く

18-21, December 2000 Grand Cube Osaka Internet Week 2000


T10 : フリーソフトウェアによるネットワーク監視 91

MRTG – cfgmaker - 2

⌘ v2.9から--ifref optionが追加され、以下のTarget指定のコンフィグを作成可能

- ☒ --ifref=nr ... interface references by Interface Number(default)
- ☒ --ifref=ip ... by Ip Address
- ☒ --ifref=eth ... by Ethernet Number
- ☒ --ifref=descr ... by Interface Description
- ☒ --ifref=name ... by Interface Name
- ☒ --ifref=type ... by Interface Type

2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI



18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10 : フリーソフトウェアによるネットワーク監視 92

MRTG - cfgmaker の出力結果

```


⌘ # Add a WorkDir: /some/path line to this file

#####
# Description: Cisco Internetwork Operating System Software IOS (tm) GS ...
# Contact: admin@foo.co.jp
# System Name: ix-gw.foo.co.jp
# Location: PA, CA, US
#.....

Target[ix-fddi.foo.co.jp]: 1:himitsu@192.168.98.133
MaxBytes[ix-fddi.foo.co.jp]: 1250000
Title[ix-fddi.foo.co.jp]: ix-gw.foo.co.jp (ix-fddi.foo.co.jp): Fddi1/0/0
PageTop[ix-fddi.foo.co.jp]: <H1>Traffic Analysis for Fddi1/0/0
</H1>
<TABLE>
  <TR><TD>System:</TD><TD>ix-gw.foo.co.jp in Otemachi 5F</TD></TR>
  <TR><TD>Maintainer:</TD><TD></TD></TR>
  <TR><TD>Interface:</TD><TD>Fddi1/0 (1)</TD></TR>
  <TR><TD>IP:</TD><TD>ix-fddi.foo.co.jp (172.16.0.2)</TD></TR>
  <TR><TD>Max Speed:</TD>
    <TD>12.5 MBytes/s (fddi)</TD></TR>
</TABLE>

```

2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI



18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10 : フリーソフトウェアによるネットワーク監視 93

MRTGの使い方

- ※ 独立コマンドとして作成されており、通常はcronにて定期的に起動する。(default : 5分間隔)
 - ☒ # crontab -l
0-59/5 * * * /usr/local/sbin/mrtg /usr/local/etc/ix-foo.cfg
#
- ※ RunAsDaemonしている際には以下のような設定をコンフィグに投入し、コマンドを投入
 - ☒ RunAsDaemon:Yes
Interval:5
 - ☒ \$ mrtg --user=mrtg_user --group=mrtg_group mrtg.cfg
- ※ データ収集指定はconfigファイルのTargetレコードにて指定

2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI 

18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10 : フリーソフトウェアによるネットワーク監視 94

MRTG - Targetの指定法

- ※ Keyword: Target - データ収集項目を指定
 - ☒ 例:
 - ☒ Target[gw1-3]: 3:himitsu@gw1.foo.co.jp
 - ☒ Target[gw1-err-3]:
ifInErrors.3&ifOutErrors.3:himitsu@gw1.foo.co.jp
 - ☒ Target[gw1-if-1]: -/10.0.0.101:himitsu@gw1.foo.co.jp
 - ☒ Target[gw1-pingloss]: ` /usr/local/bin/check_loss.sh gw1`
- ※ SNMPデータの収集
- ※ 外部コマンド結果の埋め込み収集

2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI 



MRTG - Targetの指定法:SNMP 1

⌘ SNMPデータの収集

☒ Target[<target name>]:
 <target kind>:<community>@<address>

- ☒ <target name> : 測定機器の名称
- ☒ <target kind> : 測定項目
- ☒ <community> : 測定機器に設定している
community string
- ☒ <address> : 測定機器のアドレス・ホスト名



MRTG - Targetの指定法:SNMP 2

⌘ SNMPデータ収集指定方法

- ☒ Port指定(ifIndex指定)
- ☒ SNMP OID指定 / SNMP MIB symbol指定
- ☒ Interface Address指定
- ☒ 組み合わせ指定
- ☒ 新規追加の指定方法
 - ☒ MAC address指定
 - ☒ Description指定
 - ☒ Interface Name指定

18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10 : フリーソフトウェアによるネットワーク監視 97

MRTG - Targetの指定法:SNMP 3

- ⌘ Port指定(ifIndex指定)
 - ☑ SNMP Client側で管理しているPort番号(ifIndex)を使ってデータ照会する。
 - ☑ ifInOctetsとifOutOctetsを測定
- ⌘ 例1: Target[gw1-3]: 3:himitsu@gw1.foo.co.jp
 - ☑ gw1.foo.co.jpに収容されているifIndex=3のInterfaceに関してifInOctets/ifOutOctetsを測定
- ⌘ 例2: Target[gw1-3]: -3:himitsu@gw1.foo.co.jp
 - ☑ 例1のIn/Outを逆にしてデータ収集する


2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI 

18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10 : フリーソフトウェアによるネットワーク監視 98

MRTG - Targetの指定法:SNMP 4

- ⌘ SNMP OID指定 / SNMP MIB symbol指定
 - ☑ SNMP OID(Object ID)またはMIB symbolを指定し、データ照会する。
 - ☑ 変数1、変数2は"&"で連結指定する
- ⌘ 例3: Target[gw1-err-3]: ifInErrors.3&ifOutErrors.3:himitsu@gw1.foo.co.jp
 - ☑ gw1.foo.co.jpに収容されているifIndex=3のInterfaceに関してifInErrors/ifOutErrorsを測定
- ⌘ 例4: Target[gw1-err-3]: 1.3.6.1.2.1.2.2.1.14.3&1.3.6.1.2.1.2.2.1.20.3:himitsu@gw1.foo.co.jp
 - ☑ 上の例のOID指定

2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI 

18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10 : フリーソフトウェアによるネットワーク監視


ちよつと脇道 - 99

よく使うSNMP OID/MIB Symbols

※ [interfaces.ifTable.ifEntry] group

- ☒ 1.3.6.1.2.1.2.2.1.1 : ifIndex
- ☒ 1.3.6.1.2.1.2.2.1.2 : ifDescr
- ☒ 1.3.6.1.2.1.2.2.1.3 : ifType
- ☒ 1.3.6.1.2.1.2.2.1.7 : ifAdminStatus
- ☒ 1.3.6.1.2.1.2.2.1.8 : ifOperStatus
- ☒ 1.3.6.1.2.1.2.2.1.10 : ifInOctets
- ☒ 1.3.6.1.2.1.2.2.1.16 : ifOutOctets
- ☒ 1.3.6.1.2.1.2.2.1.11 : ifInUcastPkts
- ☒ 1.3.6.1.2.1.2.2.1.17 : ifOutUcastPkts
- ☒ 1.3.6.1.2.1.2.2.1.13 : ifInDiscards
- ☒ 1.3.6.1.2.1.2.2.1.19 : ifOutDiscards
- ☒ 1.3.6.1.2.1.2.2.1.14 : ifInErrors
- ☒ 1.3.6.1.2.1.2.2.1.20 : IfOutErrors

2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI



18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10 : フリーソフトウェアによるネットワーク監視

100

MRTG - Targetの指定法:SNMP 5

※ Interface Address指定1

- ☒ パッケージタイプのルーター・スイッチはインタフェースの増減設によりPort番号(ifIndex)が変化する
- ☒ loopbackやtunnel Interfaceのような仮想インタフェースもSNMP上では一つのポート番号をもつ
 - ☒ ifIndexの割付が変化する可能性がある
- ☒ 機器の構成変更の度に設定変更をさけるためにインタフェースに割り振られたアドレスをキーにしてデータ照会を行う
 - ☒ numberedで使われていることが前提!
- ☒ デフォルトではifInOctetsとifOutOctetsを測定

2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI



18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10 : フリーソフトウェアによるネットワーク監視 101

MRTG - Targetの指定法:SNMP 6

- ⌘ Interface Address指定2
- ⌘ 例5: Target[gw1-if-1]:
/10.0.0.101:himitsu@gw1.foo.co.jp
 - ☑ gw1.foo.co.jpに收容されている10.0.0.101のInterfaceに
関してifInOctets/ifOutOctetsを測定
- ⌘ 例6: Target[gw1-if-1]:
-/10.0.0.101:himitsu@gw1.foo.co.jp
 - ☑ 例5のIn/Outを逆にしてデータ収集する


2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI 

18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10 : フリーソフトウェアによるネットワーク監視 102

MRTG - Targetの指定法:SNMP 7

- ⌘ 組み合わせ指定
 - ☑ Interface address指定とOID/MIB symbol指定を組み合わせる
- ⌘ 例7: Target[gw1-if-1-disc]: ifInDiscards/10.0.0.101&
ifOutDiscards/10.0.0.101:himitsu@gw1.foo.co.jp
 - ☑ gw1.foo.co.jpに收容されている10.0.0.101のInterfaceに関し
てifInDiscards/ifOutDiscardsを測定
- ⌘ 例8: Target[gw1-if-1-disc]:
1.3.6.1.2.1.2.2.1.13/10.0.0.101&
1.3.6.1.2.1.2.2.1.19/10.0.1.101:himitsu@gw1.foo.co.jp
 - ☑ 例7のOIDパターン

2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI 



MRTG - Targetの指定法:SNMP 8

※ Interface Name指定

- ☑ Interface Address指定はIP Addressをキーにしているために、switching hubのようにポートごとにアドレスをもたないものには適用できない。
- ☑ この状況に適応するためにInterfaceに割り振られたInterface名前をキーにしてデータ照会を行う
- ☑ デフォルトではifInOctetsとifOutOctetsを測定

※ 例9:

- ☑ Target[sw1-2-11]: #2/11:himitsu@sw1.foo.co.jp
 - ☑ Target[sw-2-11]: -#2/11:himitsu@sw1.foo.co.jp
 - ☑ Target[sw-3-7]:
 - 1.3.6.1.2.1.2.2.1.14#3/7&1.3.6.1.2.1.2.2.1.20#3/7:himitsu@sw1.foo.co.jp
 - ☑ Target[sw-3-7]:
 - ifInErrors#3/7&ifOutErrors#3/7:himitsu@sw1.foo.co.jp



MRTG - Targetの指定法:SNMP 9

※ Interface Description指定

- ☑ Interface Address指定では、故障時にポートの入れ替えなどが発生した際に、MRTG側の設定を修正しなければならない
- ☑ サーバー側で対応するよりも収容変更先の装置の設定情報を元に変更できたほうが適応範囲が広いことから、これらのキーとしてInterfaceに割り振られるDescriptionをキーにデータ照会を行う
- ☑ デフォルトではifInOctetsとifOutOctetsを測定

※ 例9:

- ☑ Target[sw1-2-11]: ¥to_web1:himitsu@sw1.foo.co.jp
 - ☑ Target[sw-2-11]: -¥to_web1:himitsu@sw1.foo.co.jp
 - ☑ Target[sw-3-7]:
 - 1.3.6.1.2.1.2.2.1.14¥to_web1&1.3.6.1.2.1.2.2.1.20¥to_web1:himitsu@sw1.foo.co.jp
 - ☑ Target[sw-3-7]:
 - ifInErrors¥to_web1&ifOutErrors¥to_web1:himitsu@sw1.foo.co.jp

18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10: フリーソフトウェアによるネットワーク監視

MRTG - ¹⁰⁵

Targetの指定法:コマンド埋め込み

⌘ コマンド埋め込み指定

- ☒ Target[<target name>]: `<command>`
 - ☒ <target name> : 測定機器の名称
 - ☒ <command> : 測定コマンド
 - ``: バックシングルコーテーションでくくるのがミソ
- ☒ コマンドの結果として4行の値が必要
 - ☒ 1行目: 第1変数、通常 incoming bytes数
 - ☒ 2行目: 第2変数、通常 outgoing bytes数
 - ☒ 3行目: 文字列 targetのuptime
 - ☒ 4行目: 文字列 targetの名称

2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI



18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10: フリーソフトウェアによるネットワーク監視

MRTGによる品質計測 ¹⁰⁶

⌘ 埋め込みコマンドによりSNMPでは計測が難しい品質測定なども可能となる


⌘ 例: 特定の2点間のpacket lossの定常監視

- ☒ 一定間隔でpingによる定期監視を実施
 - ☒ # ping -i 0.02 -c 100 ftp.foo.co.jp


```

PING ftp.foo.co.jp (192.168.101.238): 56 data bytes
.
--- ftp.foo.co.jp ping statistics ---
100 packets transmitted, 95 packets received, 5% packet loss
round-trip min/avg/max/stddev = 0.161/0.164/0.221/0.006 ms
#
          
```
 - ☒ -i 0.02 : supervisor only option.
FreeBSDのpingにおける指定。送出間隔を20ms。
ネットワークに高負荷を強いいることから取り扱い注意

2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI



18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10: フリーソフトウェアによるネットワーク監視 107


MRTGによる品質計測 - check_loss.sh

⌘ pingの出力結果からpacket lossのデータを抽出

☑ 100 packets transmitted, 95 packets received, 5% packet loss

```
# cat /usr/local/bin/check_loss.sh
#!/bin/sh
/sbin/ping -f -c 100 $1 | /usr/bin/sed 's%/g' | /usr/bin/awk '
  /packet loss/ { printf("%d\n%d\n", $7, $7)
  }'
echo 0 ; echo $*
# /usr/local/bin/check_loss2.sh ftp.foo.co.jp
5
5
0
/usr/local/bin/check_loss.sh ftp.foo.co.jp
#
```

2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI



18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10: フリーソフトウェアによるネットワーク監視 108


MRTGによる品質計測 - ping-loss.cfg

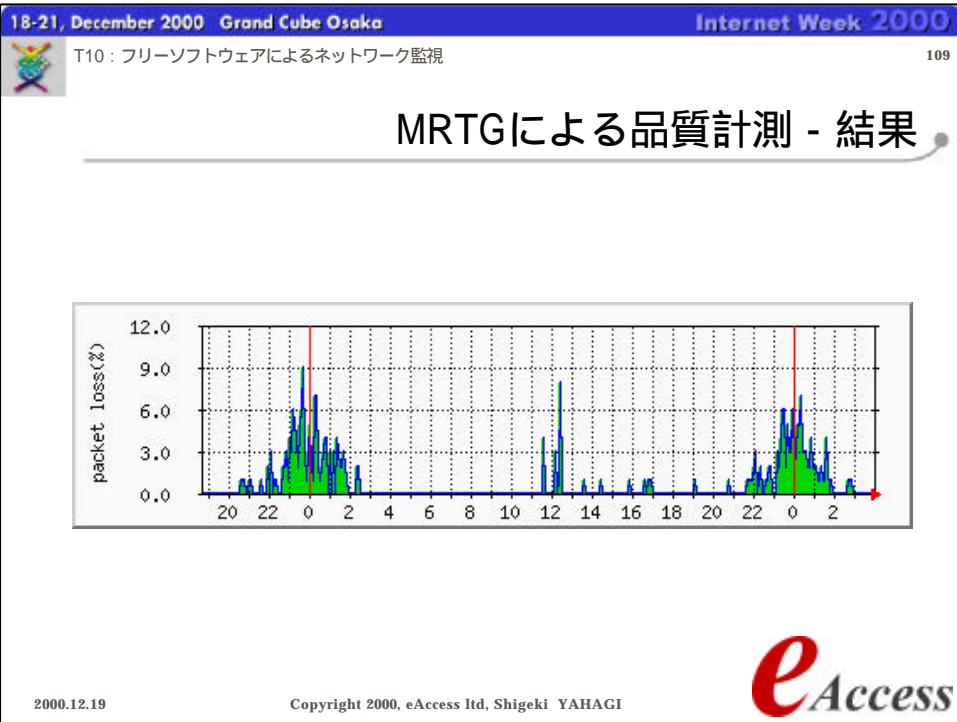
⌘ # cat ping-loss.cfg

```
WorkDir: /usr/local/etc/www/mrtg/ping-loss

Target[pingloss-ftp]: `/usr/local/bin/check_loss.sh ftp.foo.co.jp`
Title[pingloss-ftp]: ftp.foo.co.jp - pingloss
MaxBytes[pingloss-ftp]: 100
PageTop[pingloss-ftp]: <H1> ftp.foo.co.jp - pingloss </H1>
YLegend[pingloss-ftp]: packet loss(%)
ShortLegend[pingloss-ftp]: %
LegendI[pingloss-ftp]: &nbsp;loss:
LegendO[pingloss-ftp]: &nbsp;loss:
Legend1[pingloss-ftp]: packet loss
Legend2[pingloss-ftp]: packet loss
Legend3[pingloss-ftp]: Maximal 5 Minute packet loss
Legend4[pingloss-ftp]: Maximal 5 Minute packet loss
Options[pingloss-ftp]: noinfo, growright, gauge, nopercen
t
#
```

2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI





18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10 : フリーソフトウェアによるネットワーク監視

フリーソフトウェアによる ネットワーク監視

ツール間関係 -
Big Brother/MRTG/RRDTool

2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI

eAccess



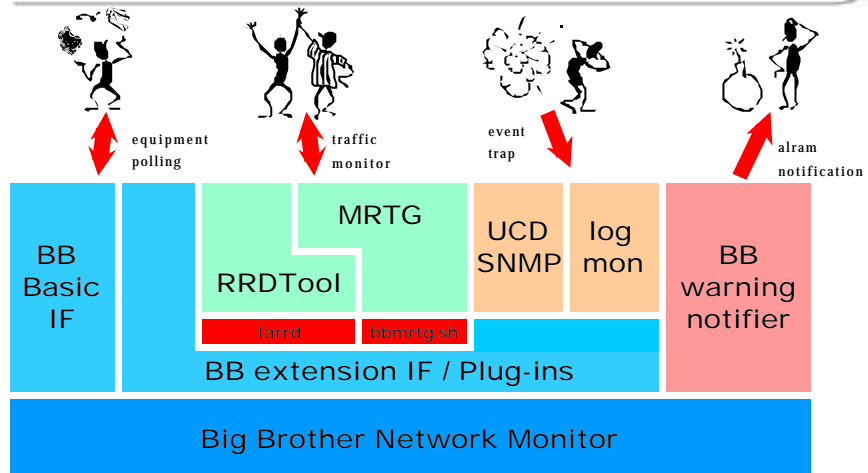
BB-MRTG/RRDToolの統合

- ⌘ 現状監視と経過監視はともに必要
- ⌘ 経過監視し、その傾向によりアラームを自発的に通知したい
- ⌘ System稼動状況をグラフ化する
- ⌘ トラフィックに閾値を設けて監視したい

- ⌘ Big Brotherのextensionにより統合を行う
 - ☑ larrd - RRDToolsとの連携
 - ☑ bbmrtg.sh - MRTGとの連携



フリーソフトによる統合監視システム



18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10 : フリーソフトウェアによるネットワーク監視 113

RRDToolとの関係: larrd

- ⌘ larrd: loadavg rrdtool -> latest v 0.41
- ⌘ <http://larrd.packetpushers.com/>
- ⌘ Big Brother Clientが各監視対象から取得したデータをRRDToolによりグラフ化する
 - ☑ 対象データ : load average, Disk Usage, TCP Connection Time, (Memory Usage, CPU idle,) ...
- ⌘ グラフ作成のみに特化しており、larrdは閾値を設定したトラフィックアラーム監視は行わない
- ⌘ 反面、設定は簡単であり、以下の設定だけで動作する
 - ☑ 指定ディレクトリへの展開
 - ☑ シンボリックリンクの作成
 - ☑ \$BBHOME/etc/bbdef.shへの登録
 - ☑ \$BBEXT変数へのエントリー追加

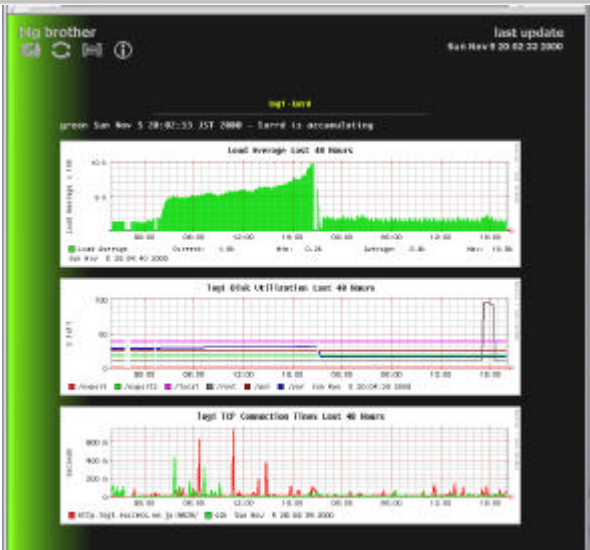
2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI



18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10 : フリーソフトウェアによるネットワーク監視 114


larrd - 画面



The screenshot displays the larrd monitoring interface. At the top, it shows the 'big brother' logo and 'list update' status. Below, there are three main graphs:

- Load Average LAST 48 hours:** A line graph showing load average over time, with a peak around 18:00.
- Top 5 disk I/O last 48 hours:** A line graph showing disk I/O for the top 5 disks, with a significant spike for the top disk around 18:00.
- Top 10 TCP Connection Times Last 48 hours:** A line graph showing TCP connection times for the top 10 connections, with several spikes.

2000.12.19




18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10 : フリーソフトウェアによるネットワーク監視 115

bbmrtg.sh

- ⌘ MRTGとの連携を図るPlug-in
- ⌘ <http://www.deadcat.net/BB/ext/bbmrtg.sh>
- ⌘ MRTGが動いているサーバーもしくはMRTGのlogファイルにアクセスできるBB監視サーバー上で稼動
- ⌘ データの取得はMRTGが行い、このPlug-inはMRTGが生成したlogファイルのチェックを行う。
- ⌘ 閾値を設定して、それを超えたらアラームをあげることが可能。

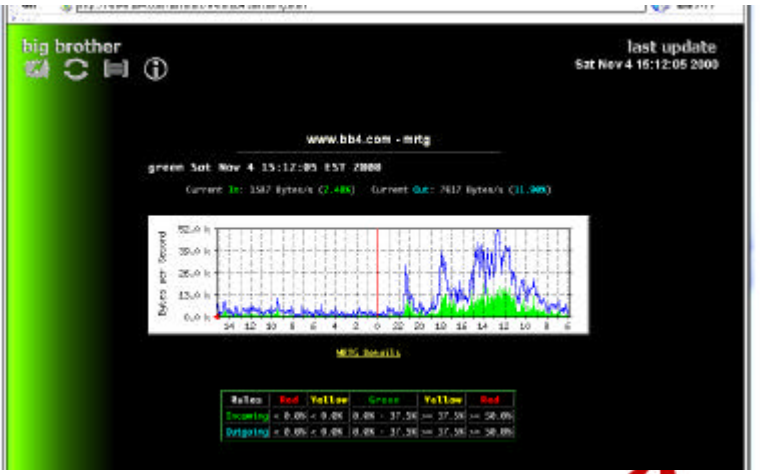
2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI



18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10 : フリーソフトウェアによるネットワーク監視 116

bbmrtg.sh



big brother

last update
Sat Nov 4 16:12:05 2000

www.bb4.com - mrtg


green Sat Nov 4 15:12:05 EST 2000
Current In: 352 Bytes/s (2.4%) Current Out: 747 Bytes/s (31.9%)

Bytes per Second

MIB2_results

Alert	Red	Yellow	Green	Yellow	Red
Ingoing	< 0.0%	0.0%	0.0% - 37.5%	37.5%	> 50.0%
Outgoing	< 0.0%	0.0%	0.0% - 37.5%	37.5%	> 50.0%

2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI



18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10 : フリーソフトウェアによるネットワーク監視 117

設定例 - bbmrtg.sh


- ※ 閾値の設定はbbmrtg.shの中に埋め込まれている
- ※ 新規追加、閾値の変更の際にはPlug-in自体を直接変更しなければならない
 - ☑ 運用上はあまり良い作りではない。改良する必要ありかと思う
 - ☑ とはいえ、トラフィックアラームをあげてくれるのはかなり助かる
 - ☑ 有効なツールとしてあげたい

```

BBMRTGCFG="Y
# MRTG device      BB Host      svc  Yellow      Red          Max  Unit
www.maclawran.ca   www.login.sh mrtg 24000      32000        64000 Bytes/s In Out
www.maclawran.ca   www.login.sh mrtg 750:24000   500:32000    64000 Bytes/s In Out
www.maclawran.ca   www.login.sh mrtg 750:24000:700:24500 500:32000:550:32500 64000 Bytes/s In Out
www.maclawran.ca   www.login.sh mrtg 50%        75%          64000 Bytes/s In Out

```

2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI




18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10 : フリーソフトウェアによるネットワーク監視 118

第2部のまとめ


- ※ フリーソフトウェアはみんなのニーズが集約された成果物
 - ☑ 現場のノウハウが集約 使わない手はない
- ※ 全てをひとつで補うことはできないが、適材適所の組み合わせで簡単にシステム化可能
- ※ 要はやる気と根気。
- ※ それとちょっとしたコツさえつかめれば、かなりの部分まではフリーソフトで幸せになれる

2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI




18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10 : フリーソフトウェアによるネットワーク監視



第3部 : ネットワーク管理に関するTIPS

2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI



18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10 : フリーソフトウェアによるネットワーク監視 120



TIPS - まずは

- ⌘ ツールの挙動確認はまずオフラインで
 - ☑ 監視・測定ツールでネットワークに障害を与えることができる
- ⌘ 時間を合わせましょう
 - ☑ 絶対基準のひとつは当然、時刻
 - ☑ NTPでサーバーと監視機器の時間を同期させる
 - ☑ Timezoneも一致させないとわからなくなる
 - ☑ UTC or JST-9

2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI



18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10 : フリーソフトウェアによるネットワーク監視 121

TIPS – 最近再確認したこと

- ⌘ SwitchのAuto Negotiationは信じない!
 - ☑ これは基本中の基本
 - ☑ 今、no errorだからといって、明日、no errorが続くとは限らない
 - ☑ 突然、duplexが full <-> half と変わってしまうことがある

2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI




18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10 : フリーソフトウェアによるネットワーク監視 122

TIPS - ping編1

- ⌘ ping checkの間隔に注意
 - ☑ ルーター/スイッチは以外にflood pingに弱い
 - ☑ 下手すると内部からのDoS Attackになりかねない
- ⌘ 広域で遠隔監視するにはチューニングが必要
 - ☑ 手早く数をこなすためには、送出間隔とタイムアウトとリトライ回数のバランスが必要
 - ☑ ローカルと違い、単純に一発落ちたからといって死んでいるわけではない。
 - ☑ リトライをうまく使い 対応する
- ⌘ #バージョンと機器毎の仕様の確認が必要だが#
 - ☑ 2ndary Addressへのpingは通らないかもしれない(cisco)?
 - ☑ ciscoはprimary addressをソースに返事をするものがある

2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI




18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10 : フリーソフトウェアによるネットワーク監視 123

TIPS – ping編2

- ※ ショートパケットが通ったからといって安心できない。開通確認はロングパケットで
 - ☑ トラフィックが多くなってくるとパケットが落ちるところも多々ある
 - ☑ ATM Megalink回線では必須。シェーピングレートの設定が失敗しているといきなり品質劣化して、通信障害となる
 - ☑ 私はpaket size=1500byte, count=1000以上、送出Interval=40msとかで試験してるかな
 - ☑ スイッチのduplexミスマッチもこれならはっきり検知できます

2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI




18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10 : フリーソフトウェアによるネットワーク監視 124

TIPS – traceroute編1

- ※ tracerouteは絶対ではない
 - ☑ 行きと帰りは非対称。同じ道を通るとは限らない
 - ☑ ソースルートオプションは絶対ではない
 - ☑ tracerouteの結果にのるRTTは結構あやしい
 - ☑ RouterのICMP処理の優先度はかなり低い
- ※ looking glass/traceroute siteを使えば外から確認できる
 - ☑ <http://www.traceroute.org/>
 - ☑ <http://nitrous.digex.net/>
 - ☑ <http://neptune.dti.ad.jp/>
 - ☑ <http://www.geektools.com/traceroute.html>

2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI





ちょっと関連- traceroute編2

⌘ 便利なツール: VisualRoute

- ☑ <http://www.visualroute.com>
- ☑ sharewareです。それだけの価値はあると思う



TIPS - 監視サーバー編1

⌘ 監視サーバの置き場所には注意

- ☑ より詳細な監視をするためには最もコアになる装置のそばに置く

⌘ 監視サーバーの画面は外に公開するものか？

- ☑ .htaccess規制もやっておきましょう
- ☑ Proxyに注意。
 - ☑ 「.htaccess」で規制していても、proxyが中にいてopenな状態だと意味がない。
 - ☑ ACLでno-cacheにしましょう

⌘ http portを変更する (http port != 80)


18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10 : フリーソフトウェアによるネットワーク監視 127

TIPS - 監視サーバー編2

- ⌘ 監視対象拡大に伴う問題
 - ☑ 規模が大きくなると、NMSがポーリングして統計処理を行う時間も増加する
 - ☑ 監視対象機器を適正な数に抑えないと...
 - ☑ 次のポーリングタイミングまで計測が終らない
 - ☑ 適正範囲に分割が必要
 - ☑ 規模拡大時に見落としやすいので注意

2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI




18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10 : フリーソフトウェアによるネットワーク監視 128

TIPS - SNMP編1: アクセス規制

- ⌘ SNMPに関する規制
 - ☑ SNMPは便利。しかし便利なものには必ず穴がある
 - ☑ セキュリティーホールになりやすい
 - ☑ SNMPでネットワークを落とすことも可能!
- ⌘ Default communityはつかわない
 - ☑ Read only community != `public`
 - ☑ Write community != "private"
- ⌘ 不要なrw rwaはできるだけ使えないように設定する

2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI




18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10 : フリーソフトウェアによるネットワーク監視 129

TIPS - SNMP編2: アクセス範囲の限定

- ⌘ SNMPクライアントにはアクセス規制が必須
 - ☑ 意外に狙われているルーター・スイッチ・www server
- ⌘ SNMP package
 - ☑ libwrapをlink, hosts.allow/hosts.denyでアクセス規制する
- ⌘ Cisco
 - ☑ SNMPアクセス規制用access-listの設定
- ⌘ そんな機能のない装置は...
 - ☑ Private address blockにいれてしまう
 - ☑ ガードの低い装置をルーティング的にInternetから隔離する (例:Switching Hub, ...)


2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI 

18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10 : フリーソフトウェアによるネットワーク監視 130

TIPS - SNMP編3: Interface高速化に伴う問題

- ⌘ カウンター 一周問題
 - ☑ ifInOctets/ifOutOctets は32bit正数
 - ☑ 5分ごとに各数値を集計する場合、約114Mbpsを越えるトラフィックが生成されるネットワークではカウンターが一周する
 - ☑ MRTG 2.9系列にてSNMPv2 64bit counter MIBを使用する
 - ☑ それ以外だと測定周期の調整という方法が必要となる

2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI 



TIPS - SNMP編4: ifIndex問題

- ※ パッケージタイプのルーター・スイッチは以下の事象においてifIndexとinterfaceの割付が変わる可能性がある
 - ☒ パッケージ障害交換
 - ☒ パッケージの増減設
 - ☒ 仮想インタフェースの増減設
 - ☒ その他...
- ※ インタフェースの増減設が伴う際には監視ツールの設定を合わせて見直す



TIPS - SNMP編5: 使えるUCD-SNMPコマンド例(V 4.1.2)

- ※ `$ snmpwalk 10.0.0.1 himitsu 1`
- ※ `$ snmpwalk 10.0.0.1 himitsu 2`
- ※ `$ snmpwalk 10.0.0.1 himitsu ifDescr`
- ※ `$ snmpwalk 10.0.0.1 himitsu ifType`

- ※ `$ snmptranslate -IR ifInDiscards`
 - ☒ OIDを表示
- ※ `$ snmptranslate -Tdp -IR ifInDiscards`
 - ☒ OIDの他にMIB Tree及び詳細説明を表示
- ※ `$ snmptranslate -Tp 2`
 - ☒ Interface(2) MIB配下のMIB Treeを表示
- ※ `$ snmptranslate -On .1.3.6.1.2.1.2.2.1.1`
 - ☒ OIDをMIB Symbolに変換して表示
- ※ `$ snmptranslate -On -Tda .1.3.6.1.2.1.2.2.1.1`
 - ☒ 上のコマンドに詳細説明を追加



TIPS – MRTG編1

⌘ データの方向性に注意

- ☑ 対向している装置で同じポートを測定するとIn/Outが逆の結果がでる
- ☑ 対外線を出口として、ここを起点にデータが流れるように設定すると考えやすい

⌘ データの単位に注意

- ☑ ifInOctets/ifOutOctetsはOctet単位系
- ☑ 回線・物理接続速度はbps、つまりbit単位系
 - ☑ Options[hoge] bitsした上でMaxbytes[hoge]を8倍する

⌘ IP address/MAC address/Comment指定Targetを効果的に使う



TIPS – MRTG編2

⌘ Cronからのメッセージには気をつける！

- ☑ 必ずMRTGのエラーメッセージは取得できるようにする
 - ☑ /etc/aliases
 - ☑ /.forward

⌘ まずいいメッセージ

- ☑ Config Error
- ☑ No Response
- ☑ Lockfile found



TIPS – MRTG編3

⌘ 非常にまずいメッセージ

```

⌘ From: root@mrtg1.eaccess.ne.jp (Cron Daemon)
⌘ To: mrtg@mrtg1.eaccess.ne.jp
⌘ Date: Fri, 13 Oct 2000 02:03:16 +0900 (JST)
⌘ Subject: Cron <mrtg@mrtg1> /usr/local/mrtg/mrtg
        /usr/local/mrtg/conf/mrtg.cfg
⌘ --

⌘ ERROR: I guess another mrtg is running.
⌘ A lockfile (/usr/local/mrtg/conf/mrtg.cfg_1) aged 303 seconds is
        hanging around.
⌘ If you are sure that no other mrtg is running you can remove the
        lockfile

```



TIPS – MRTG編4

⌘ じゃ、逆手にとって、エラーメッセージによるネットワーク監視

- ☑ 5分に毎に起動されるSNMP health checkという観点もある
 - ☑ MRTGのエラーメッセージを/dev/nullにするのはもったいない
- ☑ 経験的予兆
 - ☑ 同じインタフェースのno responseエラーが続いて上がってきたら、該当インタフェース回線のダウンか故障の可能性がある
 - ☑ どっと、まとめてエラーが帰ってきたら、ルータやスイッチなどのネットワーク障害が発生している可能性が高い



TIPS – MRTG番外編: 限界への挑戦1

- ⌘ まずはメモリ追加
 - ☑ なってたってオンメモリ
- ⌘ Forks: 指定で並列Query
 - ☑ 測定対象がこけてだまったときにも保険になる。
- ⌘ 起動順番を調整する。スタート基準は1分間隔
 - ☑ 0,5分スタート組、1,6分スタート組、2,7分スタート組、3,8分スタート組、4,9分スタート組
- ⌘ ブロックサイズの変更による速度改善
 - ☑ defaultは少なすぎ。32kぐらいにしても問題ないんでは
 - ☑ FreeBSD4.1 1024byte, Solaris2.6 4096byte, ...
 - ☑ まちがってたらごめんなさい。
 - ☑ i-node数の減少には注意



TIPS – MRTG番外編: 限界への挑戦2

- ⌘ Softupdate + async modeは結構効く！
- ⌘ ひとつのconfigにできるだけつつこむ。
 - ☑ 作業ディレクトリ指定：directory[]: で複数の測定をひとつのconfigにまとめる。
 - ☑ あるディレクトリを基準に各測定項目ごとに違うdirectoryをworkdirに設定。複数のtargetを一つのファイルに記述可能となり、計測プロセスを減少させることが、高速化に貢献する
- ⌘ RunAsDaemon！
- ⌘ それでもだめなら “LogFormat: rrdtool” + 14all.cgi！



TIPS – MRTG番外編： ほんとの限界への挑戦

- ⌘ じゃ、どこまで耐えられるか。
- ⌘ 耐える基準： loadavg ?, Proc idle ??
 - ☑ loadavgはあくまでも起動プロセス数。数が多くてもかまわない。
 - ☑ proc idle=0。いそがしいのはいいことだ
- ⌘ 結局は時間内に処理が終われば良い
- ⌘ 経験的にいえるのは、loadavgが中期的に拡散方向にいかなければ良いと思う
 - ☑ P3 650MHz, 768M Mem, SCSI2ぐらいなら、loadavg=100なんて日常的！

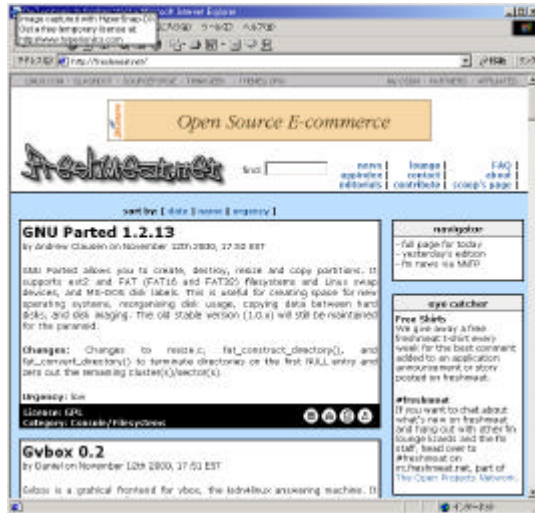


TIPS - Free Software探し方

- ⌘ ツール・ソフトをどうやって発掘するか
- ⌘ 一押しは <http://www.freashmeat.net/>
- ⌘ linux plathomeとしているが、他のOSでも稼動するものがそろっている
- ⌘ ツールの種類ごとの分類がしっかりしており、以下のような検索が可能
 - ☑ カテゴリー検索
 - ☑ ソフト名称検索
 - ☑ 関連検索



TIPS – freshmeat TopPage



2000.12.19

Copyright 2000, eAccess Ltd, Shigeki YAHAGI



TIPS – freshmeat 私の検索方法 一例

- ※ 課題: MRTGのようなツールを検索したい
 - ☑ トップで “MRTG” をキーにして検索
 - ☑ MRTGがConsole/Monitoringのカテゴリにあるので、advanced searchのoption categoryに “Console/Monitoring” を指定して検索
 - ☑ mrtg*以外にseafeltが見つかる。seafeltをみてる
 - ☑ home pageのhit数が2890ぐらいあるので、意外に使われていると判断して、Home Pageを見に行ってみる
 - ☑ よさげなので、使ってみる！

2000.12.19

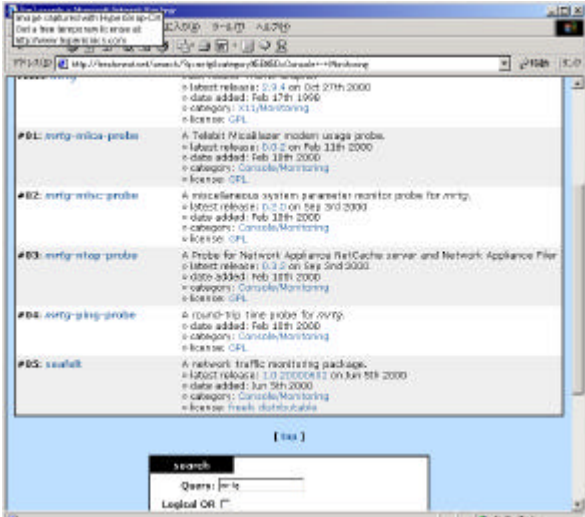
Copyright 2000, eAccess Ltd, Shigeki YAHAGI



18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10 : フリーソフトウェアによるネットワーク監視 143

TIPS – freshmeat – seafelt found !



The screenshot shows a web browser window displaying search results for 'seafelt' on the Freshmeat website. The results list several packages, with 'seafelt' at the bottom. The 'seafelt' entry includes the following details:


- Latest release: 1.0.20000611 on Jun 5th 2000
- Date added: Jun 5th 2000
- Category: Console/Monitoring
- License: fresh distributable

2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI eAccess

18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10 : フリーソフトウェアによるネットワーク監視 144

TIPS – freshmeat – seafelt page



The screenshot shows the project page for 'seafelt' on the Freshmeat website. The page includes a header with '6-gig MP3 Jukebox' and 'ThinkGeek' logos, and a navigation menu. The main content area features the following information:

seafelt
June 05th 2000, 15:44 EST

seafelt is a network monitoring package presenting a Web based graphical representation of network traffic, similar to the output of netstat. It has a highly scalable distributed state collection mechanism for monitoring larger networks and a database back-end for data archives and historical reviews.

urls

- Download: <http://seafelt.usncity.com.au/00/mbload/> (460KB)
- Homepage: <http://seafelt.usncity.com.au/> (2995 hits)

information

- Development Version: 1.0.20000611
- Author: Jim Crumpler <jim.crumpler@usncity.com.au>
- License: fresh distributable
- Category: Console/Monitoring


2000.12.19 eAccess

18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10 : フリーソフトウェアによるネットワーク監視 145

TIPS – freshmeat ゴミの判別

- ※ 判断基準： なにはともあれ、home pageのhit数！
 - ☑ 3000以上はメジャーソフト
 - ☑ 1500ぐらいいはまあ使えるレベル
 - ☑ 1000以下は...
 - ☑ ちなみに、apache 15120！ Big Brother 25180 !!, MRTG 43100 !!!
- ※ 更新頻度は重要なファクター
 - ☑ まだ開発が続いているものがうれしい
 - ☑ バグ対応もしてもらえし
 - ☑ 質問に答えてくれるかもしれない
 - ☑ 公式MLのあるツールにしましょう
- ※ まず落として使ってみる。あわせてMLに入って様子見しましょう
 - ☑ MRTG, Big BrotherのMLはかなりのthread量
 - ☑ 議論のないものはhome pageのヒットも少ない傾向あり


2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI 

18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10 : フリーソフトウェアによるネットワーク監視 146

おまけ

- ※ 今回、紹介しているBig Brother/MRTGについて Demoと稼働Configを公開(予定)。
 - ☑ 期間： 12/19 – 12/28
- ※ 参照URL:
 - ☑ <http://demo.iw2000.eaccess.net:2000/>
 - ☑ <http://demo.iw2000.eaccess.net:2000/bb/>
 - ☑ <http://demo.iw2000.eaccess.net:2000/mrtg/>
- ☑ まだ、トップページがないです。本日夕方にはupの予定にて気長にまってください。

2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI 



ご清聴ありがとうございました。

2000.12.19

Copyright 2000, eAccess Ltd, Shigeki YAHAGI

eAccess



おまけ 今後の期待

NetSaint

RRDTools + FrontEnds

2000.12.19

Copyright 2000, eAccess Ltd, Shigeki YAHAGI

eAccess



今後の期待 - NetSaint

- ※ <http://www.netsaint.org/>
- ※ WEB Baseの監視システム。現在 version 0.0.6
- ※ Web Baseでの管理・変更が可能
- ※ ICMP/TCPベースの監視を行う
 - ☑ 監視可能サービス
 - ☑ ping, smtp, http, pop3,dns,ftp.telnet,...
- ※ 詳細画面に操作用コントロールパネルがあり、監視停止などの動作が簡単に出来る。これはBBにはない機能
- ※ Plugin形式をとっており、外部拡張可能
 - ☑ MRTG plugin
 - ☑ remote server management plugin
 - ☑ ...



The screenshot displays the NetSaint web interface. At the top, it shows the current network status, including the last update time and the number of hosts and services monitored. Below this, there are several tables and controls for monitoring different host groups and services. The interface is designed for easy navigation and monitoring of network health.

18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10: フリーソフトウェアによるネットワーク監視

151

Current Network Status
 Last Update: Sun Nov 7 05:00:40 CST 1999
 Updated every 60 seconds
 NetSaint Network Monitor - successful
 No failed process is running

Host Status Totals

Up	Down	Warning	Change	Pending
21	0	0	0	0

Service Status Totals

OK	Warning	Unknown	Critical	Pending
16	2	0	1	0

Service Status Details For All Hosts

Host	Service	Status	Last Update	Alerts	Service Information
shiroki	SMTP	OK	Sun Nov 7 05:00:39 CST 1999	1/5	SMTPd - Process ID = 0x, PID = 0.70 m
shiroki	SMTP	OK	Sun Nov 7 05:01:09 CST 1999	1/5	SMTPd - Process ID = 0x, PID = 1.00 m
shiroki	SMTP	OK	Sun Nov 7 05:01:15 CST 1999	1/1	SMTPd - 4096 (512) Process /
shiroki	SMTP	OK	Sun Nov 7 05:01:18 CST 1999	1/1	User id - 0 connected
shiroki	SMTP	OK	Sun Nov 7 05:01:22 CST 1999	1/1	User id - up 67 days, 4:55, 1 min total 0.30
shiroki	SMTP	OK	Sun Nov 7 05:01:25 CST 1999	1/1	Process - 22 with 62702 status
shiroki	SMTP	OK	Sun Nov 7 05:01:33 CST 1999	1/1	Process - 0 with 2 status
shiroki	SMTP	OK	Sun Nov 7 05:01:29 CST 1999	1/5	UPS ac - Status=Idle Usage=125.0V Bat=100.0% Load=21.0% Temp=44.8
shiroki	SMTP	OK	Sun Nov 7 05:01:30 CST 1999	1/3	Printer id - (POWERSAVE 0x)
shiroki	SMTP	OK	Sun Nov 7 05:01:31 CST 1999	1/3	Printer id - (100 800V)
shiroki	SMTP	OK	Sun Nov 7 05:01:32 CST 1999	1/3	Printer id - (100 800V)
shiroki	SMTP	OK	Sun Nov 7 05:01:34 CST 1999	1/5	SMTPd - Process ID = 0x, PID = 2.50 m
shiroki	SMTP	OK	Sun Nov 7 05:01:44 CST 1999	1/5	FTP id - 8 second response time
shiroki	SMTP	OK	Sun Nov 7 05:01:47 CST 1999	1/3	Connection accepted at port 21 - 8 second response time
shiroki	SMTP	OK	Sun Nov 7 05:01:51 CST 1999	1/5	SMTPd - Process ID = 0x, PID = 0.00 m

2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI

18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10: フリーソフトウェアによるネットワーク監視

152

NetSaint - Object Map

The diagram illustrates a hierarchical network structure. At the top is a central host icon. Below it, several other host icons are connected, representing a network topology. Some icons are green, indicating they are online, while others are red with an 'N', indicating they are offline or unreachable. The structure shows a central hub with multiple branches leading to various devices and services.

2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI

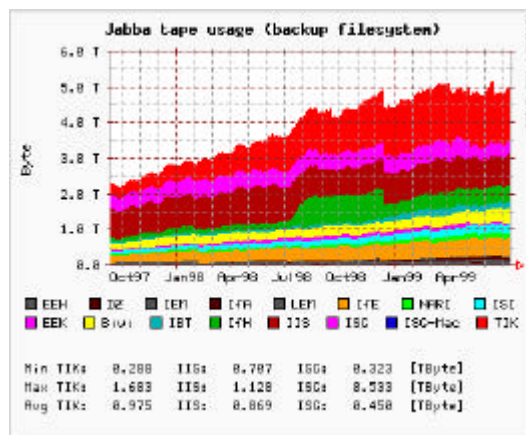


今後の期待 – RRDTools+Frontends

- ※ <http://ee-staff.ethz.ch/~oetiker/webtools/rrdtool/>
- ※ RRDTools :Round Robin Database Tools
- ※ MRTGの作者Tobi OetikerによるMRTGの後継プロジェクト
- ※ MRTGのログサイズが変わらないという利点を受け継ぎつつ、より柔軟に、より高速に、より多彩な表現ができるように、をコンセプトに開発
- ※ データベース管理、グラフ作成に特化
 - ☑ RRDToolsだけではMRTGのようなWEB画面はできない
 - ☑ FrontEnd Programが必要
 - ☑ MRTG/Big BrotherもFrontEndのひとつとなる
 - ☑ Remstat, ORCA, Cricket, NRG, ...
 - ☑ やはりひとつの画面で複数の関連情報を集約確認するにはこれしかない。うまく取り込めれば非常に強いツールとなる



RRDTools - 例1



18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10 : フリーソフトウェアによるネットワーク監視 155

RRDTools - 例2

Min TIK:	0.288	IIS:	0.787	ISC:	0.323	[TByte]
Max TIK:	1.683	IIS:	1.128	ISC:	0.533	[TByte]
Avg TIK:	0.975	IIS:	0.869	ISC:	0.458	[TByte]

2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI

18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10 : 711 156

NetScape: NoSuchSD to UWMadison

URL: http://www.usnet.net/~no/suchsd.html

Traffic Analysis for NoSuchSD to UWMadison

System: NoSuchSD-wsnet.net (Cisco 2502)
 Interface: Serial0 (PPP Instance 2)
 IP: NoSuchSD-30.000.usnet.net (149.189.164.70)
 Network: T1 (1.536 mbits/sec)

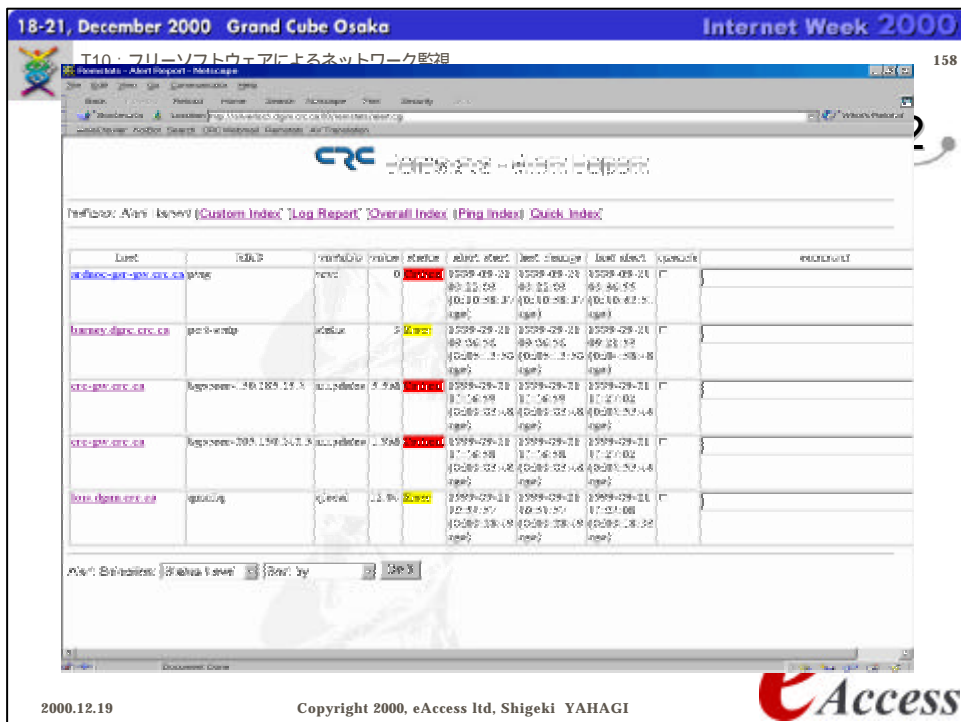
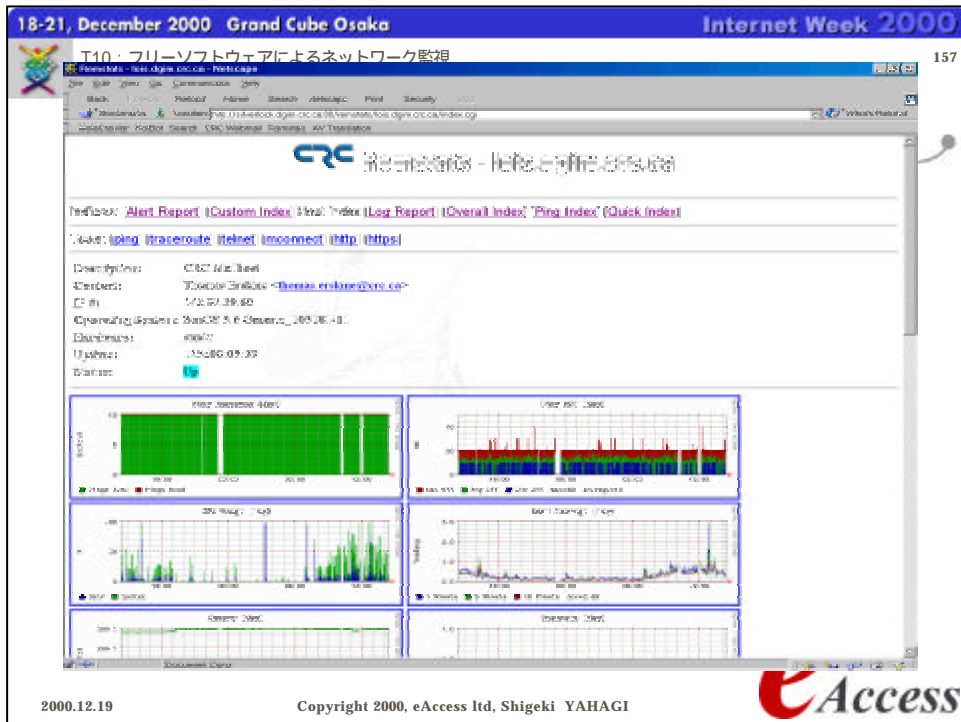
Last Four Hours

Input	365.27 kb/s	ave	1.09 Mb/s	max	867.88 kb/s	Test
Output	62.79 kb/s	ave	186.82 kb/s	max	122.68 kb/s	Test

Last Day


Input	250.13 kb/s	ave	1.09 Mb/s	max	867.58 kb/s	Test
Output	42.01 kb/s	ave	164.06 kb/s	max	122.68 kb/s	Test

2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI



18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10 : フリーソフトウェアによるネットワーク監視



参考資料:文献/URL

2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI



18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10 : フリーソフトウェアによるネットワーク監視 160



参考:書籍1

- ⌘ UNIX MAGAZINE
 - ☑ 連載「Unix Communication Notes」山口 英 1998.3~
 - ☑ 「倉敷芸術科学大学のネットワーク構築」小林和真 1997.12
- ⌘ OPEN DESIGN No.10
 - ☑ 「ネットワーク管理技術のすべて」
- ⌘ Software Design 1999.9
 - ☑ 「フリーソフトウェアでネットワークをチェック
trafshow, MRTG, ntopの導入」 田村吉章
- ⌘ Software Design 2000.7-10
 - ☑ 「FreeBSDサイト管理風雲録 - SNMPの話 その1 - 4」 工藤智行

2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI



18-21, December 2000 Grand Cube Osaka Internet Week 2000


T10 : フリーソフトウェアによるネットワーク監視 161

参考: 書籍2

⌘ SNMP

- ☒ "Snmp, Snmpv2, Snmpv3, and Rmon 1 and 2" -- William Stallings; 3rd edition (January 1999) Addison-Wesley Pub Co; ISBN: 0201485346 ;
- ☒ "Practical Guide to SNMPv3 and Network Management, A" -- David Zeltserman, Dave Zeltserman; (May 4, 1999) Prentice Hall; ISBN: 0130214531
- ☒ 「SNMPバイブル - インターネット管理への実践ガイド -」 William Stallings 著、大鐘久生、Addison-Wesley Publishing Company; ISBN-7952-9651-0

2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI



18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10 : フリーソフトウェアによるネットワーク監視 162

参考: 文献

⌘ "Yet Another network command/tool/system"

- ☒ 向阪 正彦 ファストネット株式会社
- ☒ http://www.janog.gr.jp/meeting/janog6/pdf/command/janog6_kosaka.pdf
- ☒ JANOG6 in 下丸子 2000/6/16

⌘ "Building Network Monitoring Systems with RRDtool"

- ☒ Tobias Oetiker, CAIDA
- ☒ <http://www.nanog.org/mtg-9910/tobi.html>
- ☒ NANOG17 in Montreal 1999/10/4

⌘ "Using Remstats for Network and Server Monitoring"


- ☒ Thomas Erskine, Communications Research Centre
- ☒ <http://www.nanog.org/mtg-9910/erskine.html>
- ☒ NANOG17 in Montreal 1999/10/4

2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI



18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10 : フリーソフトウェアによるネットワーク監視 163




参考：性能評価

- ⌘ Communication Traffic Project
 - ☒ <http://www.mmlab.tnl.ntt.co.jp/>
- ⌘ Distributed Benchmark System
 - ☒ <http://shika.aist-nara.ac.jp/member/yukio-m/dbs/index-j.html>

2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI 


18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10 : フリーソフトウェアによるネットワーク監視 164



Network Management

- ⌘ <http://wwwsnmp.cs.utwente.nl/Docs/software/pubdomain.html>
- ⌘ <http://netman.cit.buffalo.edu/index.html>
- ⌘ <http://www.nemoto.ecei.tohoku.ac.jp/~nitou/snmpdocs/tutorial1.html>

2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI 

18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10 : フリーソフトウェアによるネットワーク監視 165

ツールURL集1

- ※ Angel Network Monitor
 - ☒ <http://ibm-2.MPA-Garching.MPG.DE/angel/>
- ※ Big Brother
 - ☒ <http://bb4.com/>
 - ☒ Extensions Archive: <http://www.deadcat.net/>
- ※ Expect
 - ☒ <http://expect.nist.gov/>
- ※ fping
 - ☒ <http://www.stanford.edu/~schemers/docs/fping/fping.html>
- ※ IPTraf
 - ☒ <http://cebu.mozcom.com/riker/iptraf/index.html>
- ※ logsurfer
 - ☒ <http://www.cert.dfn.de/eng/logsurf/>

2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI



18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10 : フリーソフトウェアによるネットワーク監視 166

ツールURL集2

- ※ MRTG
 - ☒ <http://ee-staff.ethz.ch/~oetiker/webtools/mrtg/>
- ※ mon
 - ☒ <http://www.kernel.org/software/mon>
- ※ NeTraMet
 - ☒ <http://www.auckland.ac.nz/net/Accounting/ntm.Release.note.html>
- ※ MTR
 - ☒ <http://www.bitwizard.nl/mtr/>
- ※ NetSaint
 - ☒ <http://www.netsaint.org/>
- ※ nocol/multiping
 - ☒ <http://www.netplex-tech.com/software/nocol>
- ※ ntop
 - ☒ <http://www-serra.unipi.it/~ntop/>
- ※ NTTCP
 - ☒ <http://www.informatik.tu-muenchen.de/~bartel/nttcp/>

2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI



18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10 : フリーソフトウェアによるネットワーク監視 167

ツールURL集3

- ※ **RRDTool**
 - ☒ <http://ee-staff.ethz.ch/~oetiker/webtools/rrdtool/>
 - ☒ **Frontend - CRICKET**
 - ☒ <http://cricket.sourceforge.net/>
 - ☒ **Frontend - NRG**
 - ☒ <http://ee-staff.ethz.ch/~oetiker/webtools/rrdtool/frontends/nrg.html>
 - ☒ **Frontend - ORCA**
 - ☒ <http://www.gps.caltech.edu/~blair/>
 - ☒ **Frontend - Remstats**
 - ☒ : <http://remstats.crc.ca/remstats/release/>
- ※ **Scotty**
 - ☒ <http://wwwhome.cs.utwente.nl/~schoenw/scotty/>
- ※ **seafelt**
 - ☒ <http://seafelt.unicity.com.au/>

2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI



18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10 : フリーソフトウェアによるネットワーク監視 168

ツールURL集4

- ※ **shepherd**
 - ☒ <http://atrey.karlin.mff.cuni.cz/~clock/shepherd/>
- ※ **sing**
 - ☒ <http://sourceforge.net/projects/sing>
- ※ **SPONG**
 - ☒ <http://spong.sourceforge.net/>
- ※ **ssh**
 - ☒ <http://www.ssh.com/about/company/index.html>
- ※ **statscout**
 - ☒ <http://www.statscout.com>
- ※ **SWATCH**
 - ☒ <http://www.engr.ucsb.edu/~eta/swatch/>
- ※ **syslog-ng**
 - ☒ <http://www.balabit.hu/products/syslog-ng/>

2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI



18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10 : フリーソフトウェアによるネットワーク監視 169

ツールURL集5

- ※ Treno
 - ☒ <http://www.psc.edu/~pscnoc/treno.html>
 - ☒ Experimental TCP Implementations
<http://www.psc.edu/networking/tcp.html>
- ※ UCD-SNMP
 - ☒ <http://net-snmp.sourceforge.net/>
- ※ visualroute
 - ☒ <http://www.visualroute.com>

2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI



18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10 : フリーソフトウェアによるネットワーク監視 170

参考: URL集1

- ※ General network management portal
<http://netman.cit.buffalo.edu/index.html>
- ※ "The Simple Times"
<http://www.simple-times.org/>
- ※ SNMP FAQ
<http://www.cis.ohio-state.edu/hypertext/faq/usenet/snmp-faq/part1/faq.html>

2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI



18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10 : フリーソフトウェアによるネットワーク監視 171

参考: URL集2

- ※ Sample Cisco device security configs
http://www.cisco.com/warp/public/700/tech_configs.html#SECURITY
- ※ Cisco device SNMP configuration tips
<http://www.cisco.com/warp/public/490/index.shtml>

2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI



18-21, December 2000 Grand Cube Osaka Internet Week 2000

T10 : フリーソフトウェアによるネットワーク監視 172

参考: Free software link

- ※ Fresh Meat - Free Software Index
☒ <http://www.freshmeat.net/>
- ※ SOURCE FORGE
☒ <http://sourceforge.net/>
- ※ Solaris Freeware Project
☒ <http://sunsite.sut.ac.jp/sun/solbin/>

2000.12.19 Copyright 2000, eAccess Ltd, Shigeki YAHAGI





参考：組織

- ※ IETF <http://www.ietf.org/>
- ※ NANOG <http://www.nanog.org/>
- ※ JANOG <http://www.janog.gr.jp/>
- ※ CAIDA <http://www.caida.org/Tools/>
 - ☒ <http://www.caida.org/Tools/>
 - ☒ cflowd, RRDTool, ...etc
- ※ LBNL's Network Research Group
 - ☒ <http://ee.lbl.gov/>
 - ☒ tcpdump, libpcap, arpwatch, traceroute, pathchar