トラブルシュートを想定したネットワーク監視
～オープンソースソフトウェアによる実践～

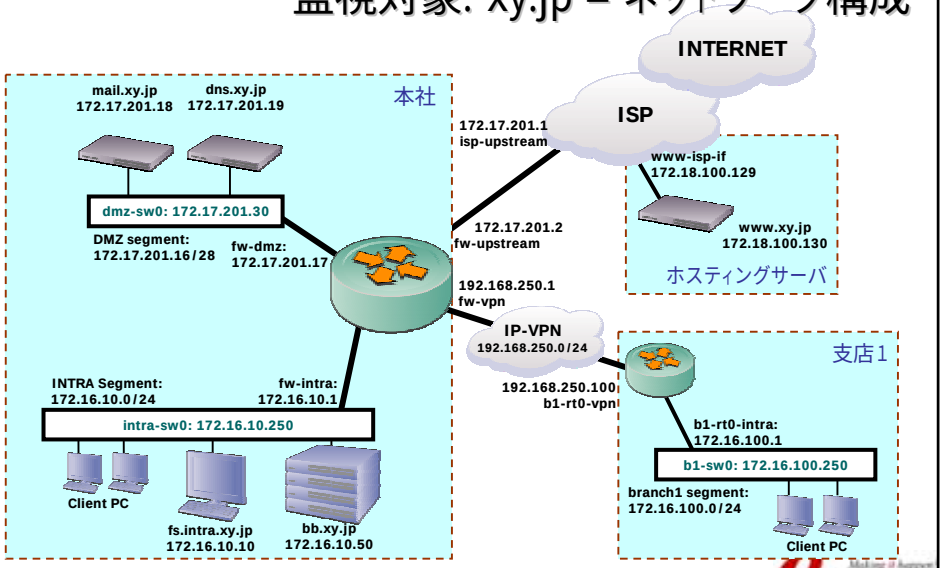
2004/12/1
イー・アクセス株式会社
矢萩茂樹
(yahagi@eaccess.net)

本セッションの目的

- 本チュートリアルでは、ネットワーク監視と障害発生時のフローに着目し、効率的なネットワーク監視について考察する。
- 小規模ネットワークを仮想し、そのネットワークを監視するオープンソースベースツールの設定を元に、どのように監視を行えばトラブルシュートが行いやすくなるかを検討する。

- 取り上げるのは以下のツール
  - Big Brother + 機能拡張スクリプト
    - bbgen, larrd, bbmrtg.pl, maint.pl, bbtray
  - MRTG

監視対象: xy.jp – ネットワーク構成

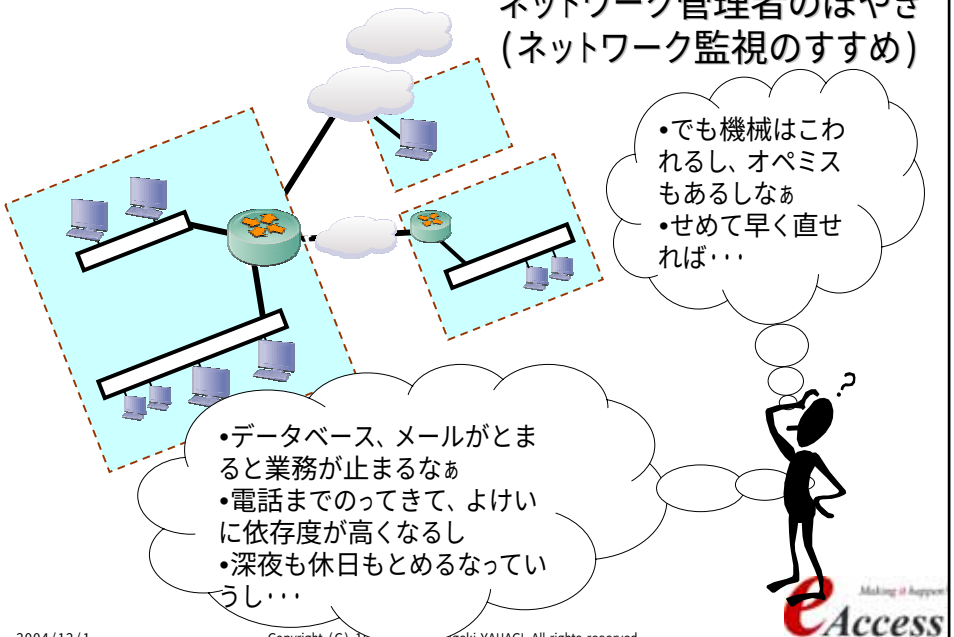


INDEX

I. ネットワーク監視とトラブルシュート概論
II. 監視サーバからの監視
III. プローブクライアントによるリソース監視
IV. トラフィックリソース監視

ネットワーク管理者への文句

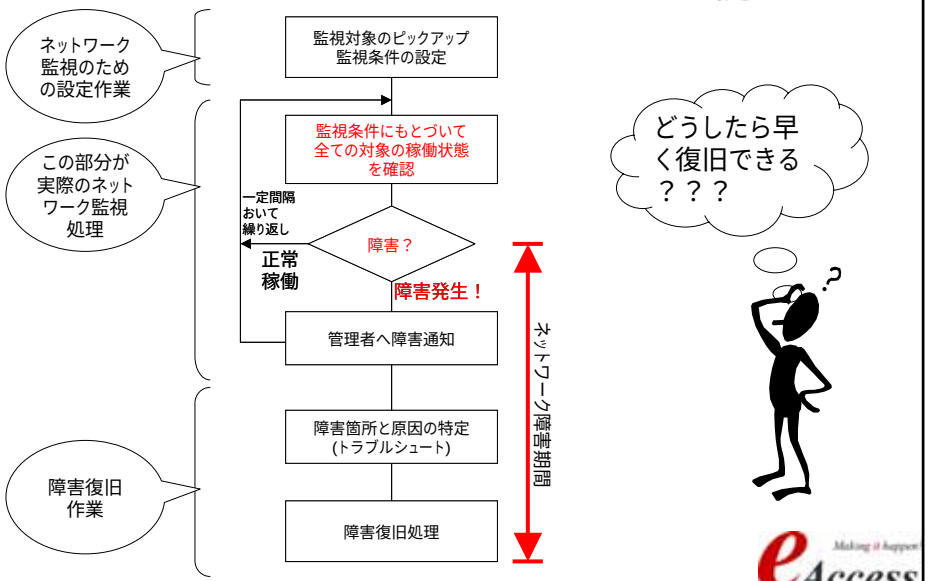
ネットワーク管理者のぼやき(ネットワーク監視のすすめ)



ネットワーク監視とは

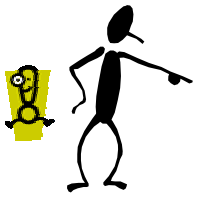
- ネットワークの稼働状態を監視する業務
  - 障害を的確に検知し、迅速な障害復旧を行うために行う
- フローを文章化すると
  - 監視すべきノードをピックアップし、
  - 監視条件を設定し、
  - 全ての監視対象を漏れなく定期的に稼働監視し、
  - 問題があったら障害を管理者に通知する。
- ネットワーク監視の後には障害復旧処理が続く
  - 障害原因を特定(トラブルシュート)し、
  - 障害ノードの復旧を行う

ネットワーク監視のフロー

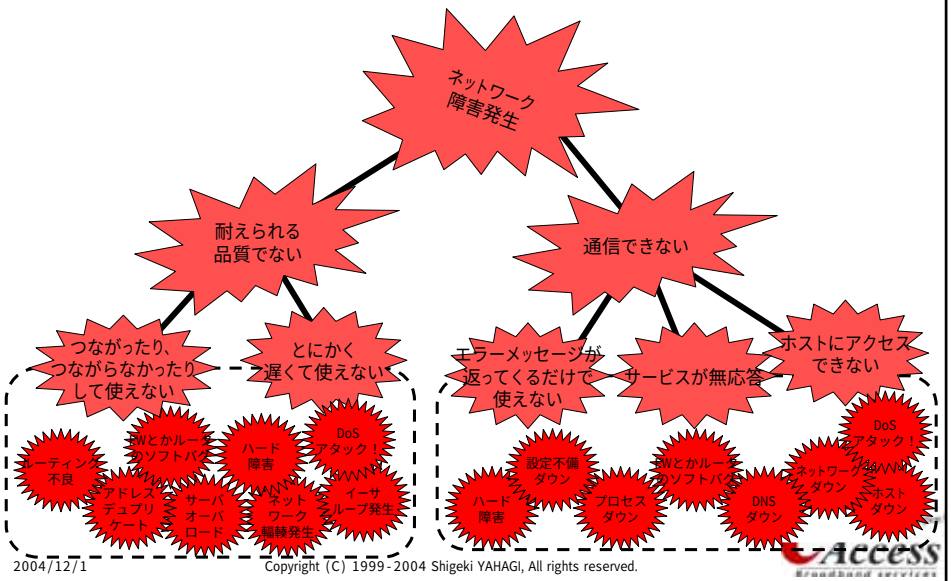


ネットワーク障害を早期復旧させるには

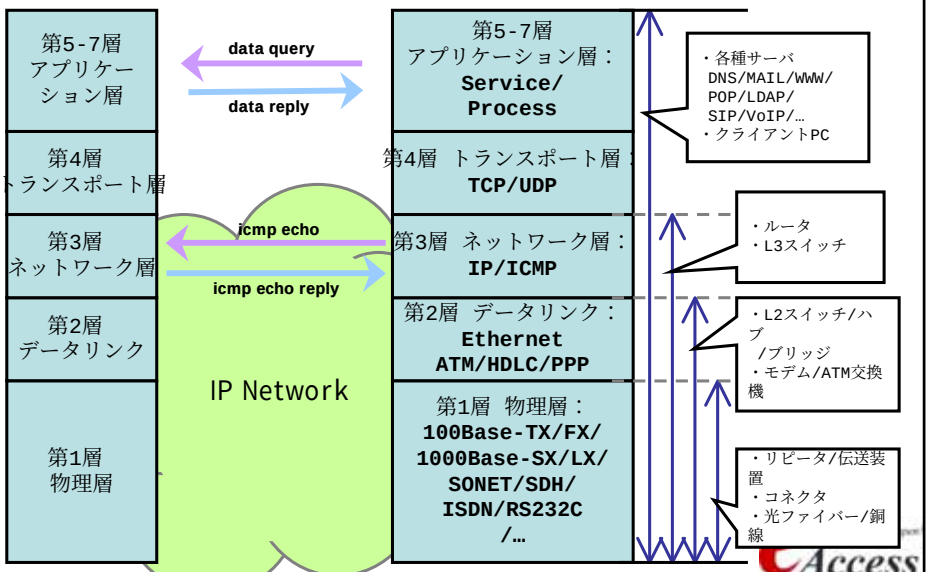
- 漏れのない稼働状態確認
- 的確な障害通知
- 迅速な障害原因調査開始
- 迅速な障害原因の特定
- 障害復旧のための準備



様々なネットワーク障害の例

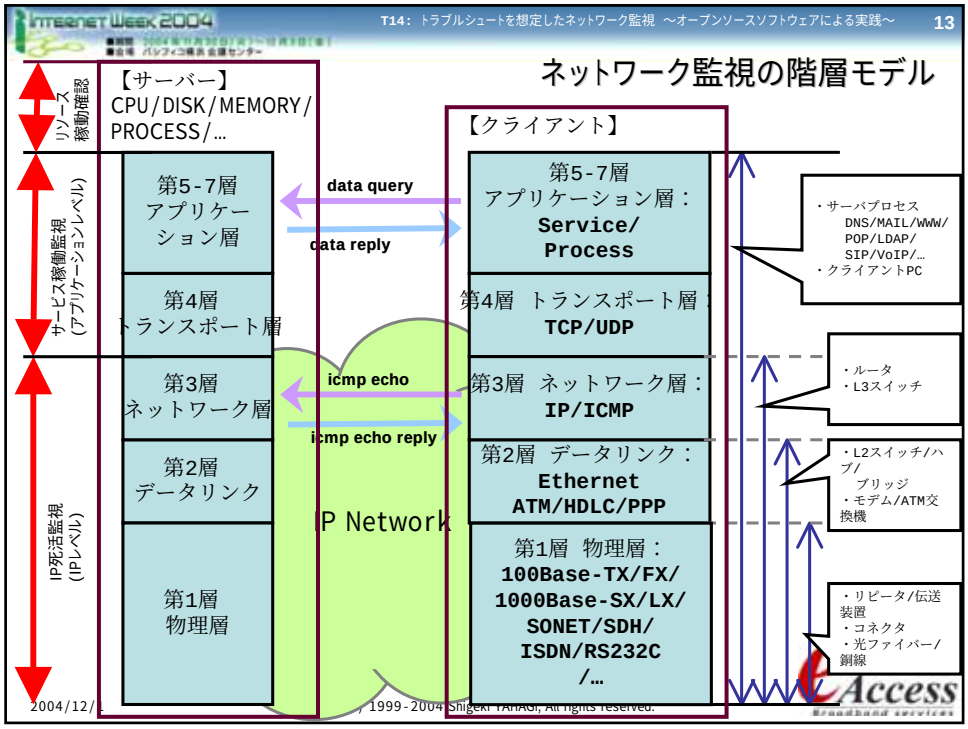


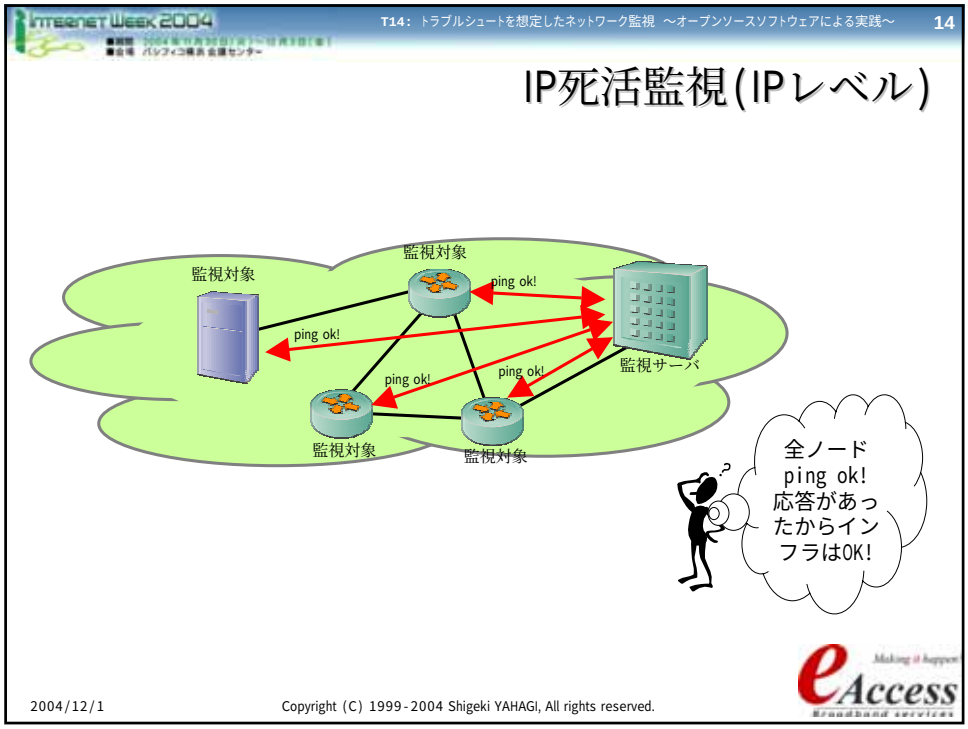
ネットワーク監視対象



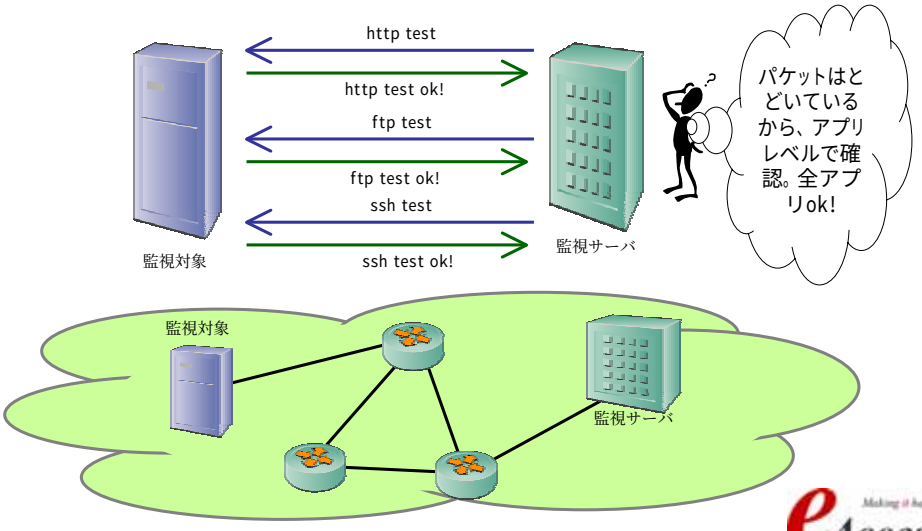
プロトコルスタックに準じたネットワーク監視の種類

- IP死活監視：IP基盤確認
  - 監視対象がIP的に生存していることを確認する
- サービス提供状態監視：提供サービス確認
  - サービスが問題なく稼動していることを確認する
- リソース監視：システム稼働状態確認
  - プロセスが正常に起動していることを確認する。
  - 十分なリソースが確保されていることを確認する
    - CPU/DISK/MEMORY/PROCESS

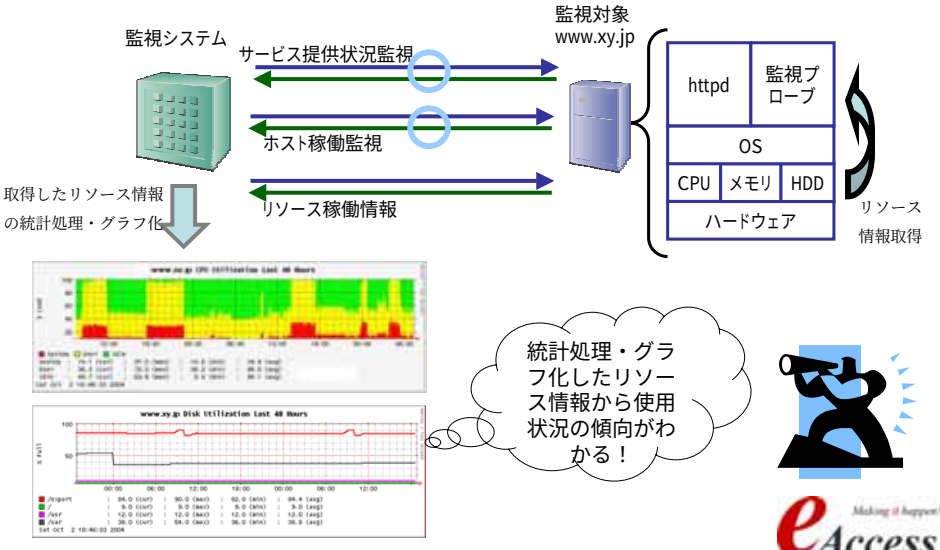

T14: トラブルシュートを想定したネットワーク監視 ～オープンソースソフトウェアによる実践～ 13
ネットワーク監視の階層モデル
【サーバー】
CPU/DISK/MEMORY/
PROCESS/…
【クライアント】
リソース稼動確認
サービス稼働監視(アプリケーションレベル)
IP死活監視(IPレベル)
第5-7層 アプリケーション層
第4層 トランスポート層
第3層 ネットワーク層
第2層 データリンク
第1層 物理層
data query
data reply
icmp echo
icmp echo reply
IP Network
第5-7層 アプリケーション層：Service/Process
第4層 トランスポート層：TCP/UDP
第3層 ネットワーク層：IP/ICMP
第2層 データリンク：Ethernet ATM/HDLC/PPP
第1層 物理層：100Base-TX/FX/1000Base-SX/LX/SONET/SDH/ISDN/RS232C/…
・サーバプロセス DNS/MAIL/WWW/POP/LDAP/SIP/VoIP/…
・クライアントPC
・ルータ
・L3スイッチ
・L2スイッチ/ハブ/ブリッジ
・モデム/ATM交換機
・リピータ/伝送装置
・コネクタ
・光ファイバー/銅線
2004/12/1
Copyright (C) 1999-2004 Shigeki YAHAGI, All rights reserved.


T14: トラブルシュートを想定したネットワーク監視 ～オープンソースソフトウェアによる実践～ 14
IP死活監視(IPレベル)
監視対象
監視対象
監視対象
監視対象
監視サーバ
ping ok!
ping ok!
ping ok!
ping ok!
全ノード ping ok! 応答があったからインフラはOK!
2004/12/1
Copyright (C) 1999-2004 Shigeki YAHAGI, All rights reserved.

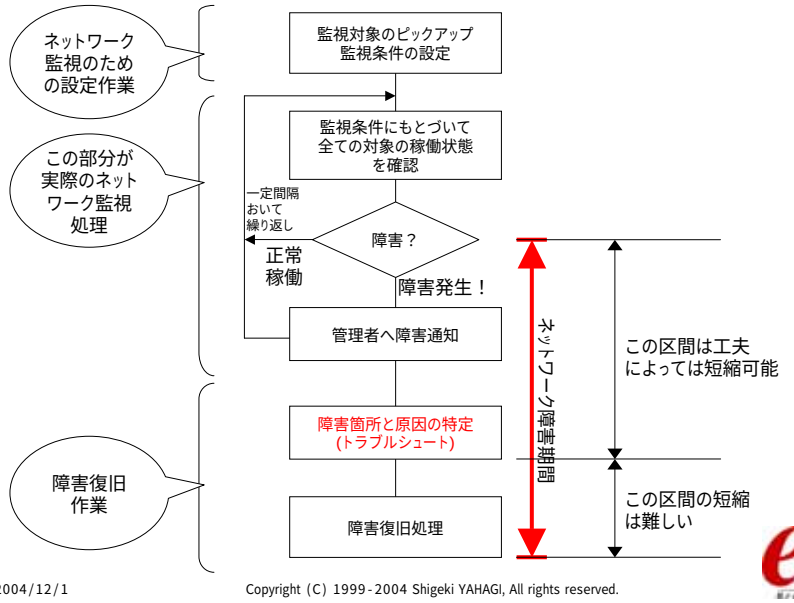
サービス稼働監視(アプリケーションレベル)



リソース監視 (システムレベル)



ネットワーク監視のフロー



ネットワーク障害の分類

- ネットワーク監視では”単体障害”・”複数障害”で対応がわかれる
- 単独ホスト障害は切り分けは見ての通りでわかりやすい
- 複数ホスト障害の場合にはトラブルシュートによる原因追求が必要
  - tracerouteによる障害ポイントの把握
  - ネットワーク接続図と障害ホストのマッピングによる障害ポイントの絞込み
- 絞込みの条件
  - 単独？:
    - 対象確定！
  - 複数？:
    - 同一ルータ？, 同一ネットワーク？. 同一セグメント？, 同一スイッチ？, …

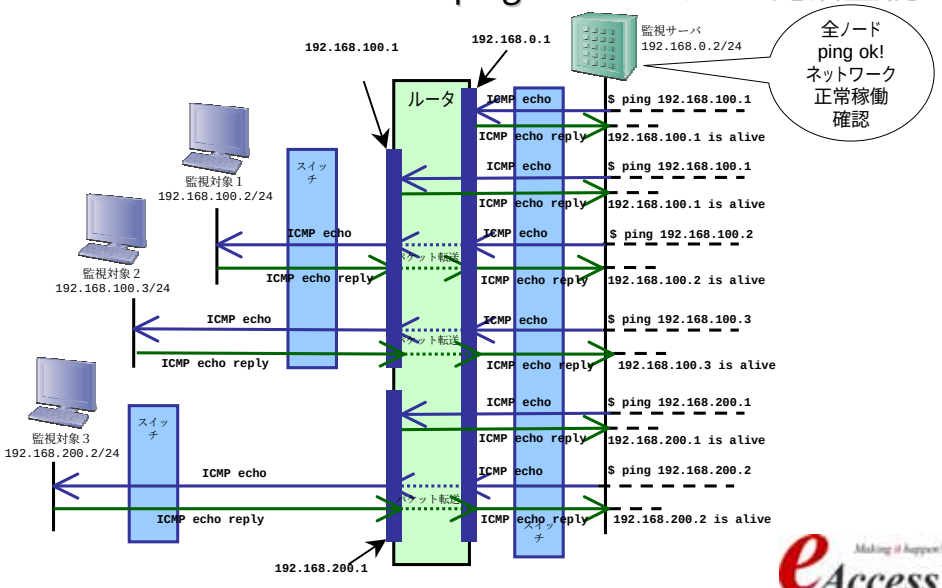
迅速なトラブルシュートのための準備

- 時間がかかるのは複数障害の切り分け作業
  - トラブルシュートの手順は基本的に同一
    - tracerouteによる障害ポイントの把握
    - ネットワーク接続図と障害ホストのマッピングによる障害ポイントの絞込み
  - この情報整理が整っているかどうかが、早期解決のわかれめ
    - これらの情報はネットワーク構築時確定している
    - トラブルにあってから調べるのでは遅い

  - 整理した情報をそのままネットワーク監視システムにトポロジーごと設定するのが肝！

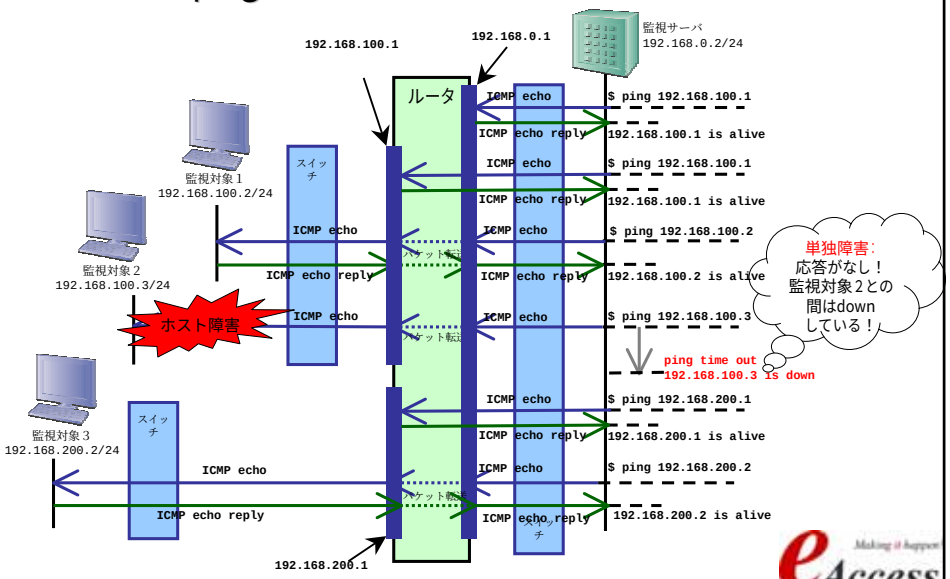
2004/12/1

pingコマンドによるIP死活監視

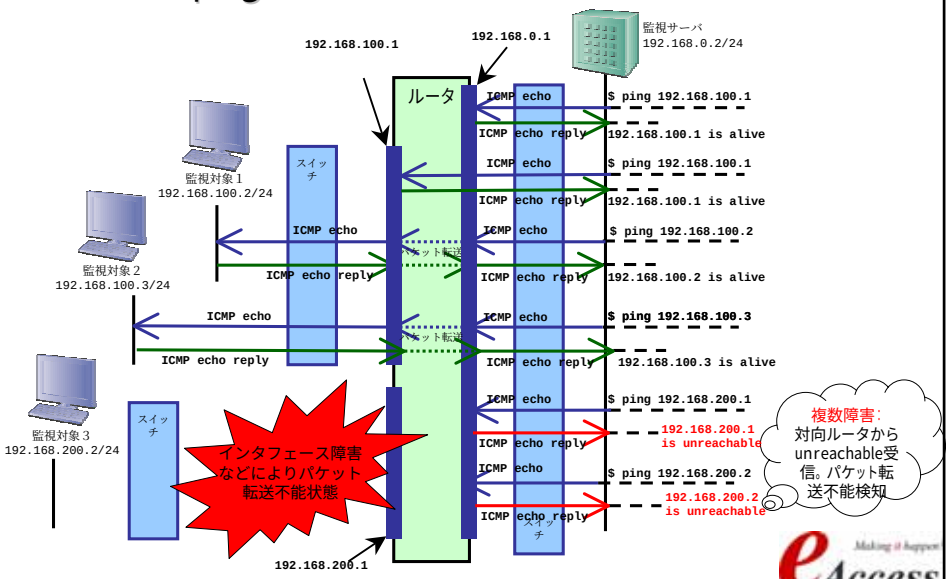


2004/12/1

pingコマンドによるIP死活監視（単独障害検知）



pingコマンドによるIP死活監視（複数障害検知）



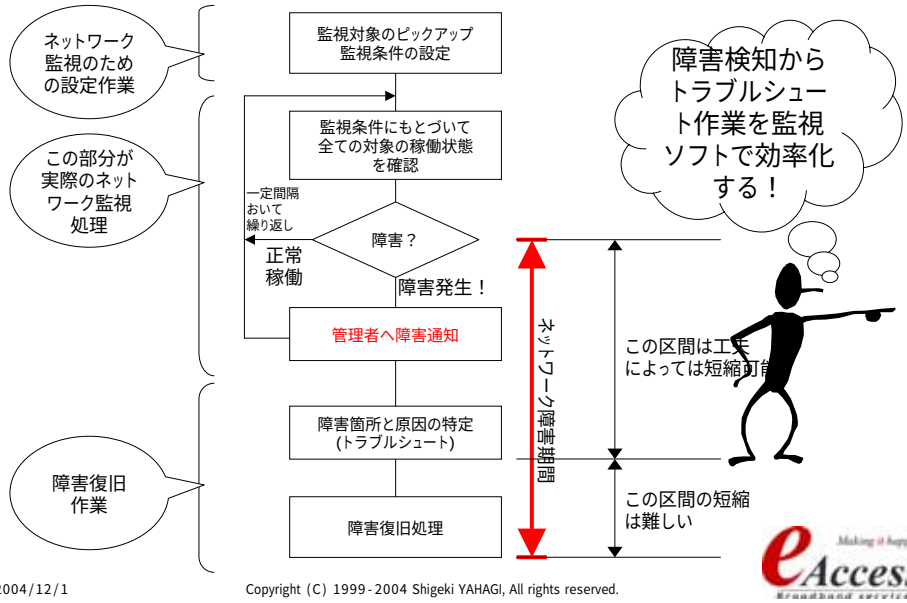
サービス稼働監視・リソース監視とIP死活監視の複合障害の関係

		IP死活監視		
		警報無し	単独ノード警報	複数ノード警報
サービス稼働監視	単独サービス警報	単独ホスト障害	単独ホスト障害	ネットワーク障害
	複数サービス警報	単独ホスト障害	単独ホスト障害	ネットワーク障害
	単独ノード警報	単独ホスト障害	単独ホスト障害	ネットワーク障害
	複数ノード警報	ネットワーク障害の可能性	サービス関係処理障害	ネットワーク障害
リソース監視	単独サービス警報	単独ホスト障害	単独ホスト障害	ネットワーク障害
	複数サービス警報	単独ホスト障害	単独ホスト障害	ネットワーク障害
	単独ノード警報	単独ホスト障害	単独ホスト障害	ネットワーク障害
	複数ノード警報	ネットワーク障害の可能性	サービス関係処理障害	ネットワーク障害

障害通知について考える

- 適切な障害通知ポイントの設定と確実な通知方法
- 障害検知後、管理者に対して速やかにイベントの報告を行う
  - 障害システム／イベント／時間により障害通知先を判断し、通知を行う。
    - 確実に届いて反応するエスカレーション体制が一番重要
    - 通知されても対処開始が遅れればその分だけ障害が重大化していく！
  - 定期メンテナンスやエスカレーション対象外の通知を抑制
    - 計画停止を障害検知しない仕組みは対応速度や精度を上げるためにも重要！
- メールによる障害発生通知
  - 通知には以下の情報を含めると迅速な対応が可能となる
    - 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
- 監視クライアントからの自動通知
  - 音、POPUP WINDOWなどによる通知

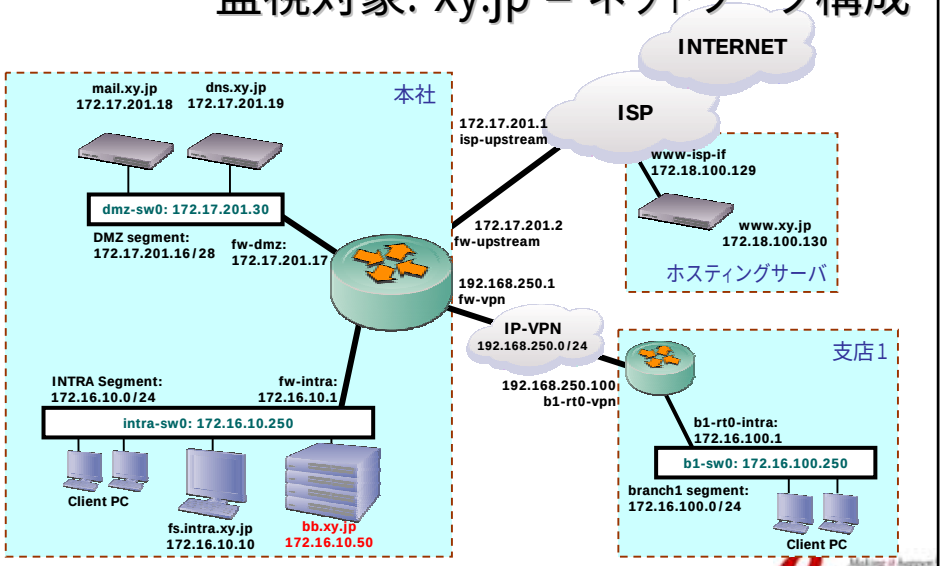
ネットワーク監視のフロー



INDEX

I. ネットワーク監視とトラブルシュート概論
II. 監視対象分析
III. 監視サーバからの監視
IV. プローブクライアントによるリソース監視
V. トラフィックリソース監視

監視対象: xy.jp – ネットワーク構成



監視対象 – 概要1

- 小規模企業のエンタープライズネットワークを想定。
- 仮想ネットワークはGlobal Address/Domainを取得／管理しており、ISPを経由してThe Internetとの接続を行っている。
- 本社側にファイヤーウォールを導入しており、社内からインターネットへの接続はすべて本社ファイヤーウォールを経由する
- ISPとの接続は本社FWからFTTH経由で接続
- 本社ー支社間はIP-VPN経由で接続
- 本社はこのほかにSub Allocation Block（172.17.201.16/28）の割当を受ける
- グローバルアドレスが振られるサーバはすべて本社ファイヤーウォールのDMZ配下に配置
- www.xy.jp(172.18.100.130)はISPのサーバホスティングを使用し、ISPデータセンターに設置
- ファイヤーウォール配下のネットワークはPrivateアドレスを使用し、FirewallにてNAPT(Network Address/Port Translation)している

監視対象分析 – IPアドレスブロック割当

セグメント	アドレスブロック	用　途
本社DMZセグメント	172.17.201.16/28	ISP割当グローバル
www.xy.jpセグメント	172.18.100.128/30	www.xy.jpホスティンググローバル
本社イントラセグメント	172.16.10.0/24	イントラ向けプライベート
本社WANセグメント	172.17.201.0/30	ISP割当グローバル
本社ー支社間セグメント	192.168.250.0/24	WAN機器チェック用プライベート
支社イントラセグメント	172.16.100.0/24	イントラ向けプライベート

監視対象分析 - 提供サービス1

- ネットワーク提供サービス
  - 社外向けサービス
    - DNS/MAIL(SMTP)/WWW
  - 社内向けサービス
    - DNS/MAIL(SMTP/POP)/WWW(Intra)
    - DHCP
    - File Server/Print Server
  - 共通ポート
    - メンテナンスはTELNETは使用せず、SSHのみ。
    - FTPサービスも社外向けには開いていない
    - SMTPサービスは必要なサーバのみに限定
    - 社外へはポートはあけておらず、IPsec/PPTP VPN経由で内部からのみLOGIN可能とする

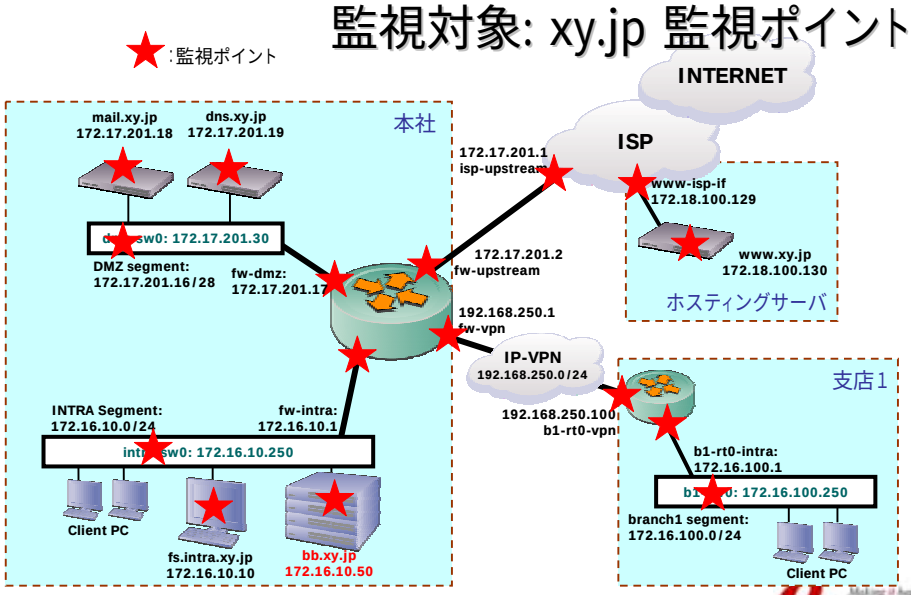
監視対象分析 - 提供サービス1

- ネットワーク提供サービス2
  - DNS設定
    - Primary: dns.xy.jp（172.17.201.18）
    - Secondary: mail.xy.jp（172.17.201.19）
  - メール設定
    - Primary: mail.xy.jp
    - Secondary: dns.xy.jp
  - POPは社内のみに制限。
  - 社外からのアクセスはVPNを経由してのみ可能

監視ポイントの割り出し

- 監視ポイントは以下の設備を対象とする
  - 共用サービスを提供している設備：各種サーバ
  - ネットワーク設備：ルータ・スイッチ・ファイアウォール
    - イーサネット区間は障害となると切り分けが難しいことから、基幹部分のスイッチはSNMP対応のインテリジェントスイッチ導入が好ましい
    - ファイアウォールはデフォルトではICMPには答えない。監視するためには返答するようなポリシー適用が必要
- 監視対象外の設備
  - クライアントPCやオンラインと関係のない開発サーバなどは対象外
  - 稼働時間が規定されるノードの設定には注意が必要
- 該当するノードと提供サービスを漏れなく、ピックアップすることが重要
  - ぬけていては管理されていないのと同じ

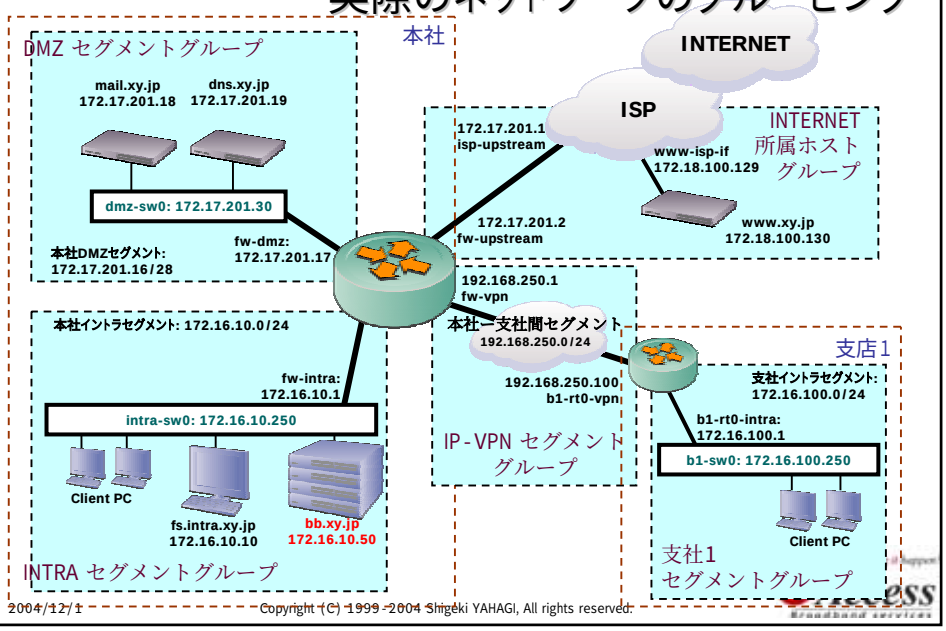
監視対象: xy.jp 監視ポイント



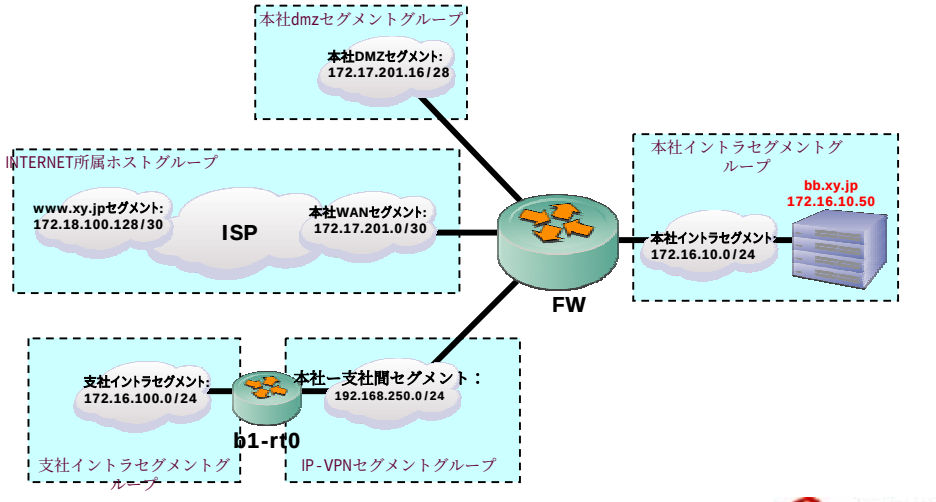
監視ポイントのグルーピング

- ネットワーク監視を効率的に行う上で整理整頓が非常に重要
- 障害発生時のフローは以下の手順が基本
  - IP死活監視が失敗！
  - 失敗したノードの物理トポロジーに基づいて、直前のポイントまでからのping確認を実施。詳細の切り分けを行う
- IPネットワークの依存関係はあくまでもサブネットセグメントとそれをつなぐルータの木構造
- セグメント毎にグルーピングし、監視サーバをトップノードとしたセグメントツリーを作る

実際のネットワークのグルーピング



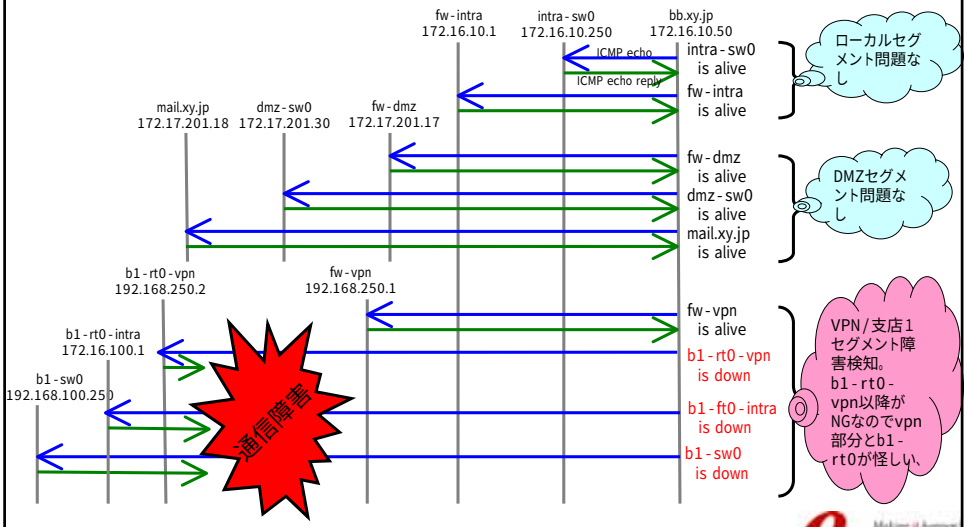
各グループのトポロジー整理



監視対象分析 – 監視ホスト一覧

セグメント	IP address	ホスト名称	URL	提供サービス
本社イントラセグメント (172.16.10.0/24)	172.16.10.1	fw-intra	- - -	firewall
	172.16.10.10	fs.intra.xy.jp	- - -	FileServer
	172.16.10.50	bb.xy.jp	bb.xy.jp	http, ssh
	172.16.10.250	intra-sw0	- - -	switch
本社DMZセグメント (172.17.201.0/28)	172.17.201.17	fw-dmz	- - -	firewall
	172.17.201.18	mail.xy.jp	mail.xy.jp	dns, smtp, pop, ssh
	172.17.201.19	dns.xy.jp	dns.xy.jp	dns, smtp, ssh
	172.17.201.30	dmz-sw0	- - -	switch
本社WANセグメント (172.17.201.0/30)	172.17.201.1	isp-upstream	- - -	ISP-Router
	172.17.201.2	fw-upstream	- - -	firewall
www.xy.jpセグメント (172.18.100.128/30)	172.18.100.130	www.xy.jp	www.xy.jp	http, ftp, ssh
	172.18.100.129	www-isp-if	- - -	ISP-Router
本社ー支社間セグメント (192.168.250.0/24)	192.168.250.1	fw-vpn	- - -	firewall
	192.168.250.2	b1-rt0-vpn	- - -	router
支社イントラセグメント (172.16.100.0/24)	172.16.100.1	b1-rt0-intra	- - -	firewall
	172.16.100.250	b1-sw0	- - -	switch

セグメントグルーピングによる障害点の把握



監視対象分析 – 監視時間と通知先

- 全ての機器の障害情報は障害受付窓口であるalert@xy.jpに通知
- 独自のイントラ系と支社ネットワークの部分については以下の監視･障害通知ポリシーを適用
  - 本社ファイルサーバ fs0.intra.xy.jp ：
    - 毎日午前4時から6時の間でデイリーバッチ処理が走り、高負荷となることから監視を停止。監視省力化
    - この機械の障害時には担当窓口：intra@xy.jpにも通知
  - 支社機器の障害対応は現地の担当に任せることが多いためにalert@branch.xy.jpへの通知を追加

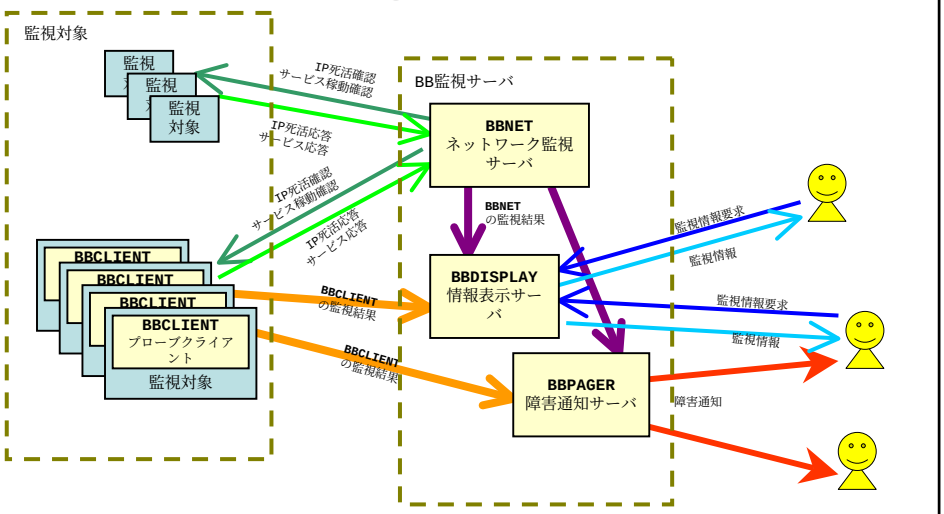
INDEX

I. ネットワーク監視とトラブルシュート概論
II. 監視対象分析
III. 監視サーバからの監視
IV. プローブクライアントによるリソース監視
V. トラフィックリソース監視

状態監視ツール - Big Brother

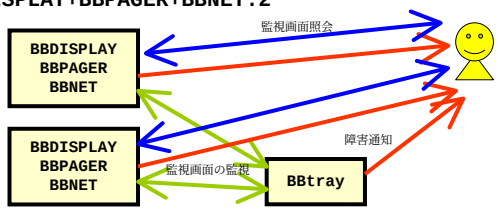
- **http://www.bb4.org/**
- WEB Baseの監視システム
  - 2002年からオープンソース版 と製品版に分かれる
  - 通常使用においては費用は発生しない
- 監視･表示･通知機能をモジュール分割しており、それぞれを別サーバに分散することで、大規模ネットワークまで適用可能
- ICMP/TCPポーリングによる監視を行う
  - 監視可能サービス:
    - **ping,smtp,http､https,pop3,dns,ftp,telnet,ssh,imap,nntp, ･･･**
  - サーバー個別監視:
    - **CPU,disk,processes,logs**
- 各種Unix/Windows NT系/NetWare/Macintoshの監視用プローブがあり、複合OS統合監視が可能

BigBrother監視システムの機能概要

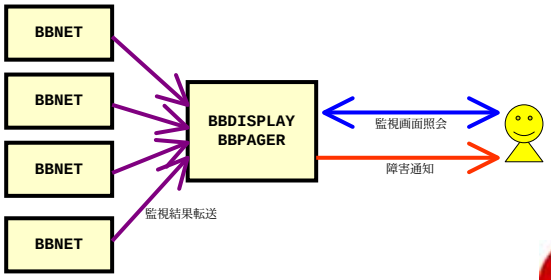


BigBrother 分散構成例

分散構成１：**BBDISPLAY+BBPAGER+BBNET:2**



分散構成２：**BBDISPLAY+BBPAGER:1, BBNET:n**



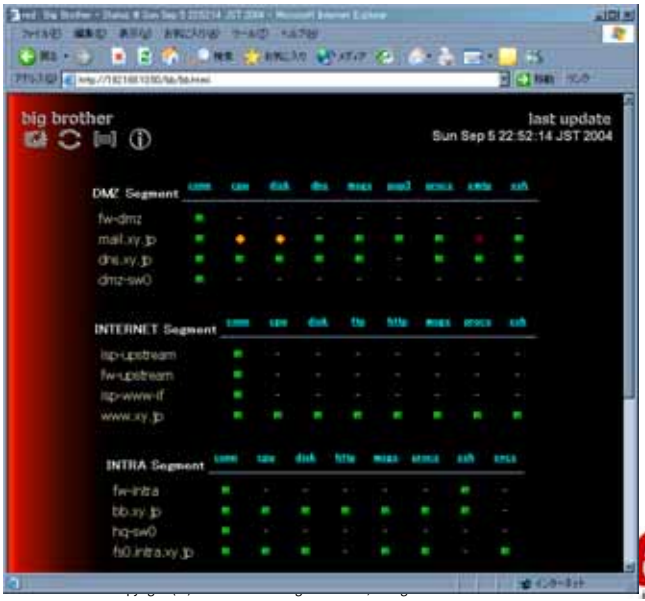
状態監視ツール - BigBrother

- 監視対象のグループ化機能
- 監視画面の階層化機能(３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
  - 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
  - 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可能

状態監視ツール - BigBrother

- 障害履歴機能
- システム稼動状況レポート作成機能
- 拡張インタフェースが公開されており、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
  - 拡張監視モジュール：DBMS, ファイルサーバ, プリンタサーバ, ・・・
  - 他ソフトとの連係：MRTG, RRDTools, Snort, tripwire, ・・・
  - 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、IDS Front-end、気象情報監視、株価監視(?!),・・・

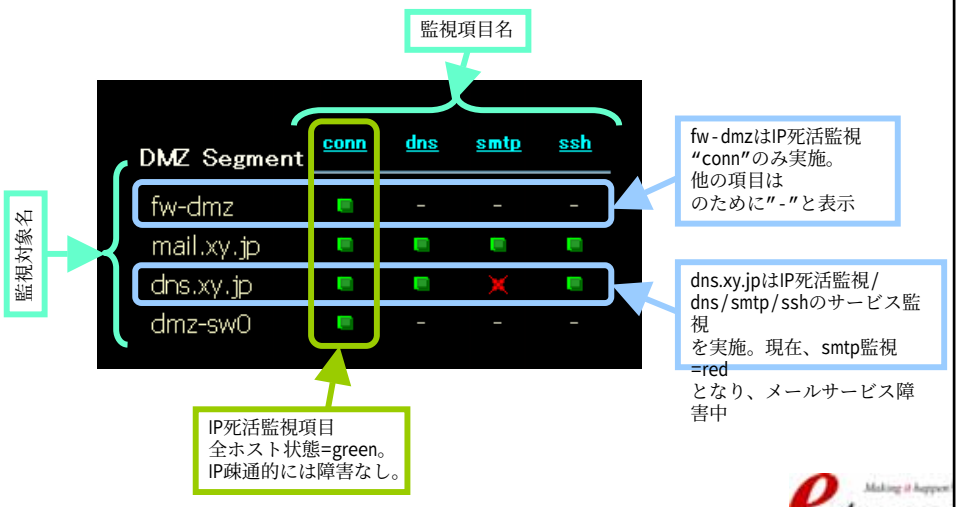
BB：監視画面(TOP)



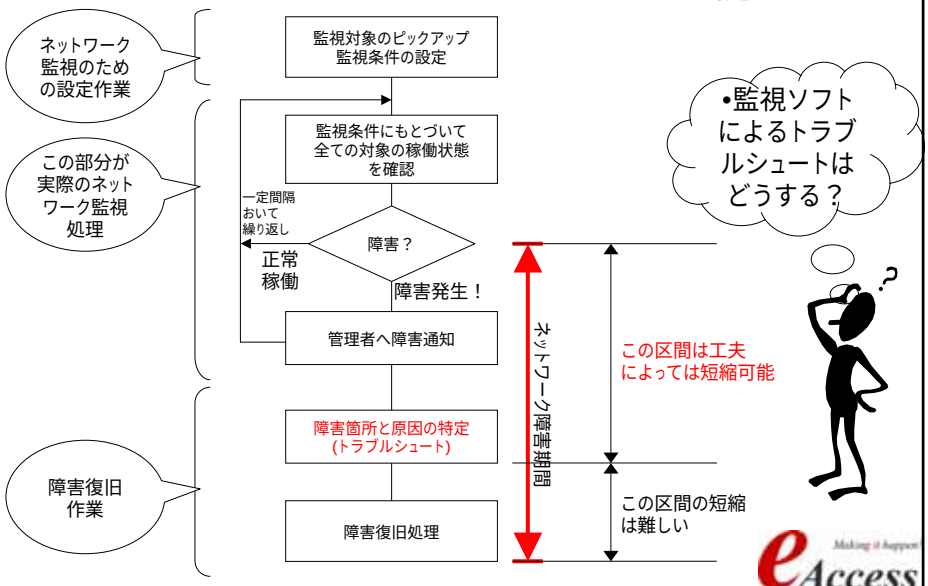
稼働状態アイコン

ok	“緑”,”green”：ホストの稼働状態問題なし
attention	“黄”,”yellow”: 軽微な障害あり。注意が必要
trouble	“赤”,”red”：障害発生中。
no report	“紫”,”purple”: ホスト無反応状態。監視履歴が存在するが、情報更新なし。システムチェックが必要。

監視状態表示

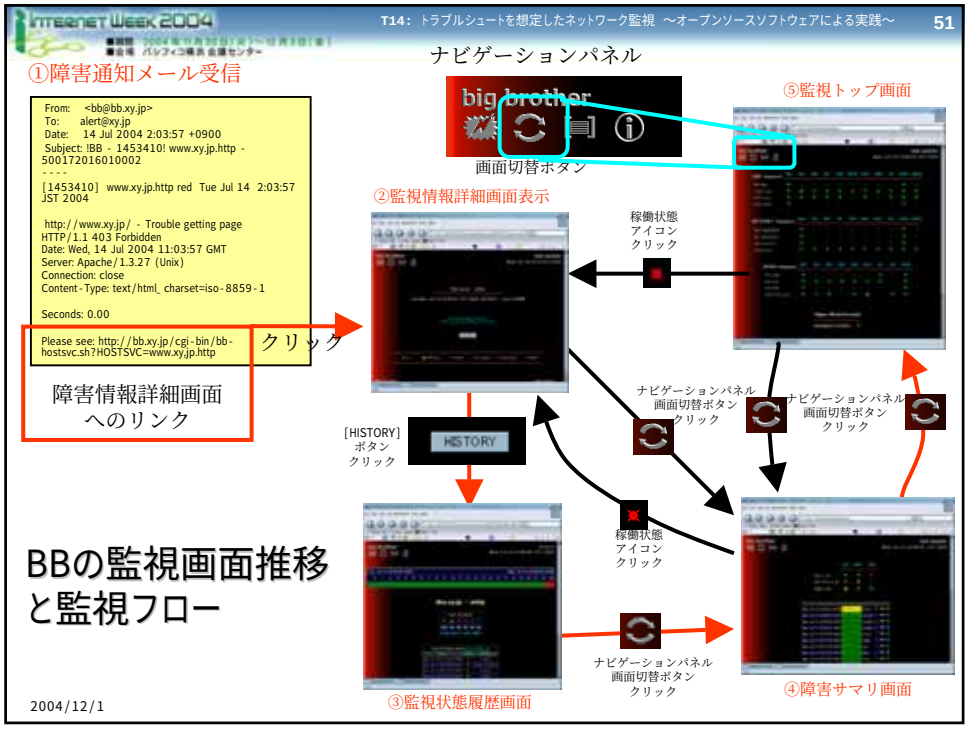


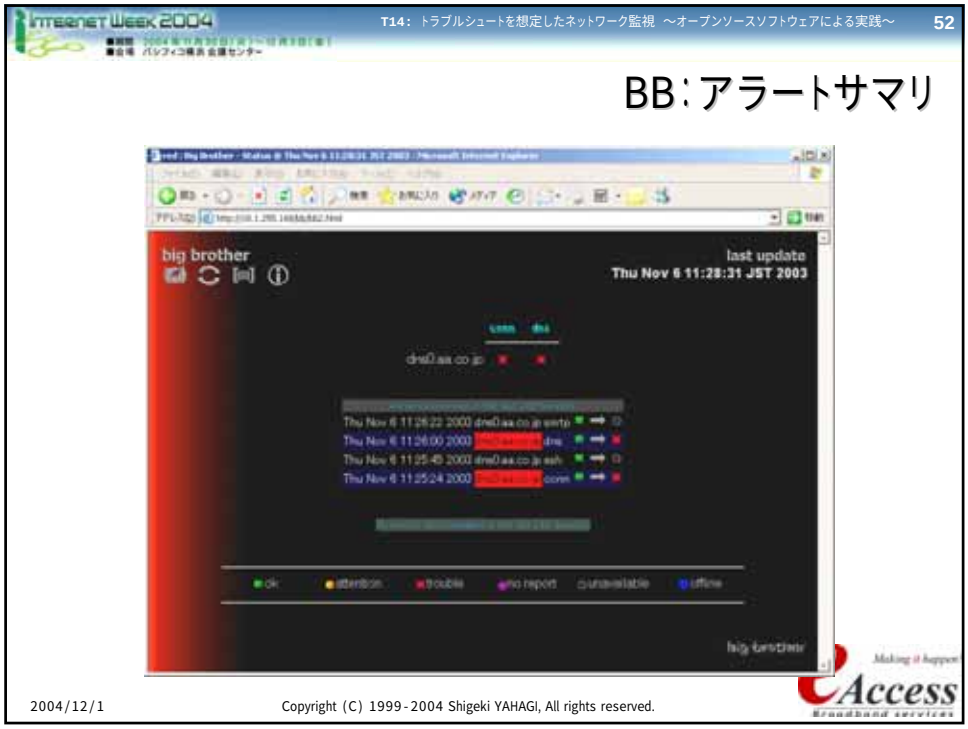
ネットワーク監視のフロー



BBを使った障害トラブルシューティングフロー

① 障害通知を受信
② 障害情報詳細画面にて状況を確認
③ いつから障害が発生しているかを確認
④ 他の障害を確認
⑤ 障害を全体から把握


T14: トラブルシュートを想定したネットワーク監視 ～オープンソースソフトウェアによる実践～ 51
①障害通知メール受信
From: <bb@bb.xy.jp>
To: alert@xy.jp
Date: 14 Jul 2004 2:03:57 +0900
Subject: !BB - 1453410! www.xy.jp.http - 500172016010002
[1453410] www.xy.jp.http red Tue Jul 14 2:03:57 JST 2004
http://www.xy.jp/ - Trouble getting page
HTTP/1.1 403 Forbidden
Date: Wed, 14 Jul 2004 11:03:57 GMT
Server: Apache/1.3.27 (Unix)
Connection: close
Content-Type: text/html_ charset=iso-8859-1
Seconds: 0.00
Please see: http://bb.xy.jp/cgi-bin/bb-hostsvc.sh?HOSTSVC=www.xy.jp.http
クリック
障害情報詳細画面へのリンク
ナビゲーションパネル
big brother
画面切替ボタン
⑤監視トップ画面
②監視情報詳細画面表示
稼働状態アイコンクリック
[HISTORY]ボタンクリック
HISTORY
ナビゲーションパネル画面切替ボタンクリック
③監視状態履歴画面
④障害サマリ画面
BBの監視画面推移と監視フロー
2004/12/1


T14: トラブルシュートを想定したネットワーク監視 ～オープンソースソフトウェアによる実践～ 52
BB：アラートサマリ
big brother
last update
Thu Nov 6 11:28:31 JST 2003
2004/12/1
Copyright (C) 1999-2004 Shigeki YAHAGI, All rights reserved.

BB：ヒストリ画面

BB：監視画面(sub)

BigBrother 監視サーバー 設定ファイル

- Big Brother監視サーバー設定は以下のファイルに行う

- $BBHOME/etc/bb-hosts: 監視対象定義ファイル
- $BBHOME/etc/bb-warnrules.cfg: 障害通知定義ファイル

監視対象定義 etc/bb-hosts - 1

- 監視対象の定義ファイル
- 記述方法は/etc/hosts の拡張版に類似
- 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。

監視対象定義 etc/bb-hosts - 設定例

```
$ cat bb-hosts
#
# THE BIG BROTHER HOSTS FILE
#
192.168.0.10 kansi1.aa.jp # BBPAGER BBNET BBDISPLAY http://kansi1.aa.jp/bb

group-compress <H3><I>aa.jp Servers</I></H3>
192.168.0.2  ns1.aa.jp  # dns ssh !telnet
192.168.0.3  mail0.aa.jp # dns smtp pop3 ssh !telnet
192.168.0.5  www.aa.jp  # telnet ssh ftp http://www.aa.jp/

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


監視対象定義 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が動いていることを指示
    - **BBNET**：ネットワーク監視サーバ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.xy.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。
        ただし、**dns/http/https**での**”!”**指定は不可
      - **~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

監視対象定義 etc/bb-hosts - 3

- 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
    - <group name>にはhtmlタグが使用可能
  - サブページ指定: page/subpage
    - page <page name> <page title>
    - subpage <subpage name> <subpage 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
    - <page title>にはhtmlタグが使用可能

bb-hosts監視指定タグ一覧

監視指定	監視指定タグ	タグの意味
BBサーバ機能指定	BBDISPLAY	BB監視画面サーバ稼動指定
	BBPAGER	BB監視通知サーバ稼動指定
	BBNET	BBネットワーク監視サーバ稼動指定
PING監視指定	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
監視サービス指定	ftp	ftpサービスの監視実行
	smtp	smtpサービスの監視実行
	pop3	pop3サービスの監視実行
	telnet	telnetサービスの監視実行
	ssh	sshサービスの監視実行
	nntp	nntpサービスの監視実行
	http://URL	URLに指定されたhttp実行サービスの監視
	https://URL	URLに指定されたhttpsサービスの監視実行。(lynxが必要)
	dns	dnsサービスの監視実行
	dig	dnsサービスの監視実行。digコマンドが使用可能なら同コマンドにて実施
	bbd	BBDISPLAY/BBPAGERの監視実行

監視設定

- ネットワークノードの全IPアドレスに対してPing試験を実施
- サーバについてはサービスポートの確認を行う。
  - 提供サービス確認/規制サービス確認

セグメント	IP address	ホスト名称	提供サービス	規制サービス
本社イントラセグメント (172.16.10.0/24)	172.16.10.1	fw-intra	firewall	
	172.16.10.10	fs.intra.xy.jp	FileServer	telnet smtp
	172.16.10.50	bb.xy.jp	http ssh bbd	telnet smtp
	172.16.10.250	intra-sw0	switch	
本社DMZセグメント (172.17.201.0/28)	172.17.201.17	fw-dmz	firewall	
	172.17.201.18	mail.xy.jp	dns smtp pop ssh	telnet
	172.17.201.19	dns.xy.jp	dns smtp ssh	telnet
	172.17.201.30	dmz-sw0	switch	
本社WANセグメント (17217201.0/30)	172.17.201.1	isp-upstream	ISP-Router	
	172.17.201.2	fw-upstream	firewall	
www.xy.jpセグメント (172.18.100.128/30)	172.18.100.130	www.xy.jp	http ftp ssh	telnet smtp
	172.18.100.129	www-isp-if	ISP-Router	
本社ー支社間セグメント (192.168.250.0/24)	192.168.250.1	fw-vpn	firewall	
	192.168.250.2	b1-rt0-vpn	router	
支社イントラセグメント (172.16.100.0/24)	172.16.100.1	b1-rt0-intra	firewall	
	172.16.100.250	b1-sw0	switch	

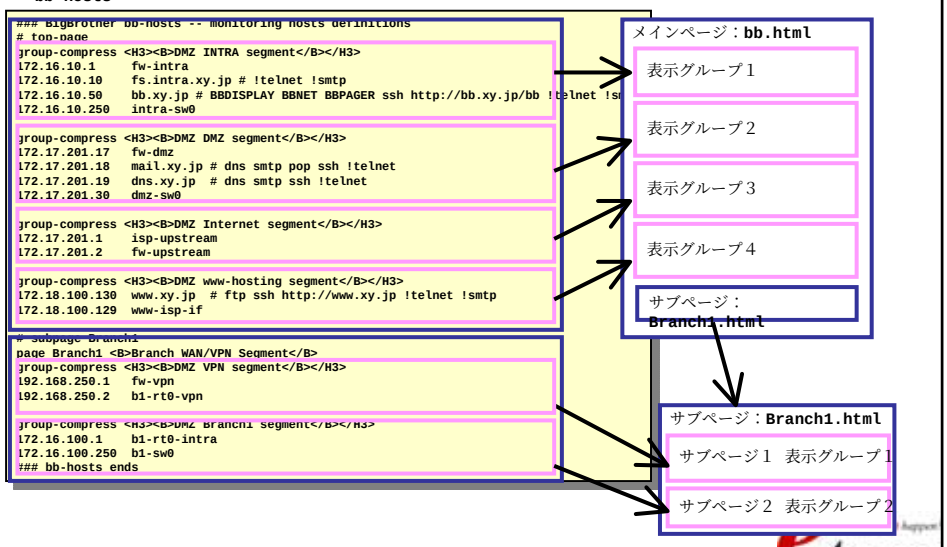
監視ノードの整理表

所属ページ	所属group	IP address	ホスト名称	BBServer	提供サービス	提供サービス(http)	規制サービス
top-page	INTRA segment	172.16.10.1	fw-intra				
		172.16.10.10	fs.intra.xy.jp				telnet smtp
		172.16.10.50	bb.xy.jp	BBDISPLAY BBNET BBPAGER	ssh	http://bb.xy.jp/bb	telnet smtp
		172.16.10.250	intra-sw0				
	DMZ segment	172.17.201.17	fw-dmz				
		172.17.201.18	mail.xy.jp		dns smtp pop ssh		telnet
		172.17.201.19	dns.xy.jp		dns smtp ssh		telnet
		172.17.201.30	dmz-sw0				
	Internet segment	172.17.201.1	isp-upstream				
		172.17.201.2	fw-upstream				
	www-hosting segment	172.18.100.130	www.xy.jp		ftp ssh	http://www.xy.jp	telnet smtp
		172.18.100.129	www-isp-if				
sub-page Branch1	VPN segment	192.168.250.1	fw-vpn				
		192.168.250.2	b1-rt0-vpn				
	Branch1 segment	172.16.100.1	b1-rt0-intra				
		172.16.100.250	b1-sw0				

bb.xy.jp設定 etc/bb-hosts

```
### BigBrother bb-hosts -- monitoring hosts definitions
# top-page
group-compress <H3><B>INTRA segment</B></H3>
172.16.10.1     fw-intra
172.16.10.10    fs.intra.xy.jp # !telnet !smtp
172.16.10.50    bb.xy.jp       # BBDISPLAY BBNET BBPAGER ssh http://bb.xy.jp/bb !telnet !smtp
172.16.10.250   intra-sw0

group-compress <H3><B>DMZ segment</B></H3>
172.17.201.17   fw-dmz
172.17.201.18   mail.xy.jp # dns smtp pop ssh !telnet
172.17.201.19   dns.xy.jp  # dns smtp ssh !telnet
172.17.201.30   dmz-sw0

group-compress <H3><B>Internet segment</B></H3>
172.17.201.1    isp-upstream
172.17.201.2    fw-upstream

group-compress <H3><B>www-hosting segment</B></H3>
172.18.100.130  www.xy.jp   # ftp ssh http://www.xy.jp !telnet !smtp
172.18.100.129  www-isp-if

# subpage Branch1
page Branch1 <B>Branch WAN/VPN Segment</B>
group-compress <H3><B>VPN segment</B></H3>
192.168.250.1   fw-vpn
192.168.250.2   b1-rt0-vpn

group-compress <H3><B>Branch1 segment</B></H3>
172.16.100.1    b1-rt0-intra
172.16.100.250  b1-sw0
### bb-hosts ends
```


bb-hostsの設定とページ構成



警報通知定義 etc/bbwarnrules.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

監視対象分析 – 監視時間と通知先

- 全ての機器の障害情報は障害受付窓口であるalert@xy.jpに通知
- 独自のイントラ系と支社ネットワークの部分については以下の監視･障害通知ポリシーを適用
  - 本社ファイルサーバ fs.intra.xy.jp :
    - 毎日午前4時から6時の間でデイリーバッチ処理が走り、高負荷となることから監視を停止。監視省力化
    - この機械の障害時には担当窓口:intra@xy.jpにも通知
  - 支社機器の障害対応は現地の担当に任せることが多いためにalert@branch.xy.jpへの通知を追加

警報通知定義

セグメント	IP address	ホスト名称	提供サービス	通知先	通知時間
本社イントラセグメント	172.16.10.1	fw-intra	firewall	alert@xy.jp	24/7D
(172.16.10.0/24)	172.16.10.10	fs.intra.xy.jp	FileServer	alert@xy.jp	24/7D, 午前4-5時台は除外
	172.16.10.50	bb.xy.jp	http ssh	alert@xy.jp	24/7D
	172.16.10.250	intra-sw0	switch	alert@xy.jp	24/7D
本社DMZセグメント	172.17.201.17	fw-dmz	firewall	alert@xy.jp	24/7D
(172.17.201.0/28)	172.17.201.18	mail.xy.jp	dns smtp pop ssh	alert@xy.jp	24/7D
	172.17.201.19	dns.xy.jp	dns smtp ssh	alert@xy.jp	24/7D
	172.17.201.30	dmz-sw0	switch	alert@xy.jp	24/7D
本社WANセグメント	172.17.201.1	isp-upstream	ISP-Router	alert@xy.jp	24/7D
(17217201.0/30)	172.17.201.2	fw-upstream	firewall	alert@xy.jp	24/7D
www.xy.jpセグメント	172.18.100.130	www.xy.jp	http ftp ssh	alert@xy.jp	24/7D
(172.18.100.128/30)	172.18.100.129	www-isp-if	ISP-Router	alert@xy.jp	24/7D
本社ー支社間セグメント	192.168.250.1	fw-vpn	firewall	alert@xy.jp	24/7D
(192.168.250.0/24)	192.168.250.2	b1-rt0-vpn	router	alert@xy.jp alert@branch.xy.jp	24/7D
支社イントラセグメント	172.16.100.1	b1-rt0-intra	firewall	alert@xy.jp alert@branch.xy.jp	24/7D
(172.16.100.0/24)	172.16.100.250	b1-sw0	switch	alert@xy.jp alert@branch.xy.jp	24/7D

警報通知定義 etc/bbwarnrules.cfg

```
$ cat bbwarnrules.cfg
### bbwarnrules.cfg

fs*;;*;;*;0000-0359 0600-2359;alert@xy.jp
## fs*(fs.intra.xy.jpにマッチ)については24H/7Dの監視を行い、
## 障害時はaltert@xy.jpとintra@xy.jpに通知する
## ただし、AM4:00-AM5:59までの間は通知対象外とする

b1-*;;*;;*;*;alert@xy.jp alert@branch.xy.jp
## b1-*(支社の装置)については24H/7Dの監視を行い、
## 障害時はaltert@xy.jpとintra@xy.jpに通知

*;;*;;*;*;alert@xy.jp
## 上記以外のホストの障害検知については
## alert@xy.jpに通知する。

unmatched-*;;*;;*;*;bb@xy.jp
## bb-hosts定義外のイベント(unmatched-*)検知についてはbb@xy.jpに通知する

### end of bbwarnrules.cfg
$
```

障害通知例

障害検知通知: **dns.xy.jp - conn**

```
---------------------- Original Message ----------------------
 From:    <bb@bb.xy.jp>
 To:      alert@xy.jp
 Date:    6 Nov 2004 11:33:28 +0900
 Subject: !BB - 8393010! dns.xy.jp.conn - 500192168001002
----

[8393010]  dns.xy.jp.conn red Thu Nov  6 11:33:26 JST 2004 ERROR: Can't connect to
172.17.201.19
PING 172.17.201.19 (172.17.201.19): 56 data bytes

--- 172.17.201.19 ping statistics ---
1 packets transmitted, 0 packets received, 100% packet loss

Please see: http://bb.xy.jp/bb/html/dns.xy.jp.conn.html
-------------------- Original Message Ends --------------------
```

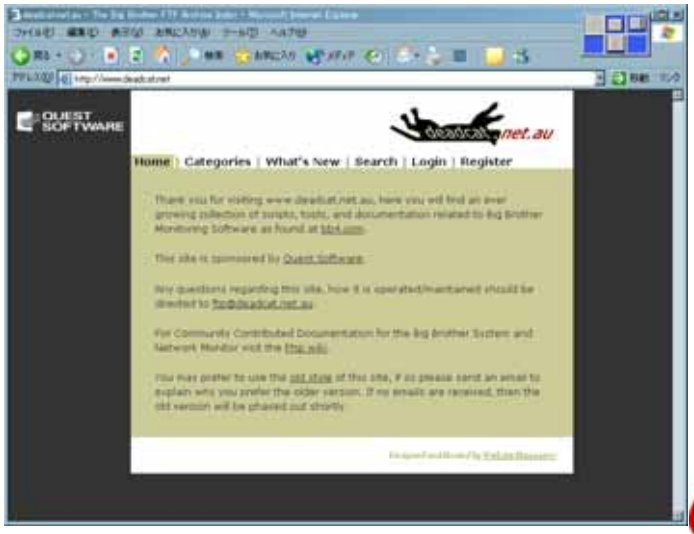
障害回復通知: **dns.xy.jp - conn**

```
---------------------- Original Message ----------------------
 From:    <bb@bb.xy.jp>
 To:      alert@xy.jp
 Date:    6 Nov 2004 12:48:15 +0900
 Subject: !BB - 0000000! dns.xy.jp.conn - 500192168001002
----

[0000000]  dns.xy.jp.conn recovered Thu Nov  6 12:48:15 2004 Problem has been resolved after
4971 seconds

Please see: http://bb.xy.jp/bb/html/dns.xy.jp.conn.html
-------------------- Original Message Ends --------------------
```


BigBrother機能拡張スクリプト

- 拡張インタフェースが公開されており、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/
  - モジュールごと拡張版への置換
  - 外部拡張スクリプトによる機能追加
- 実現されるもの
  - サービス稼働監視拡張:
    - radius, ntp, ldap, smb, mqueue, ・・・
    - RDBS (ORACLE, PostgreSQL, MySQL, ・・・)
    - 他システム監視: RAS, UPS, RAID, Printer, ・・・
  - 他ソフトとの連係: 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 http://www.deadcat.net



BB機能拡張スクリプト maint.pl

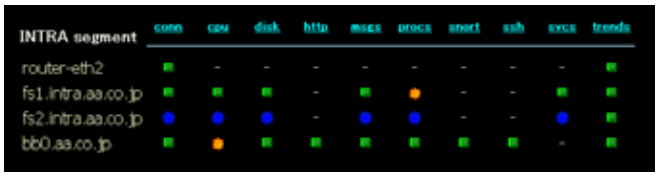
- 監視対象の保守停止といったメンテナンスの際に、一時的に対象を監視対象外にする拡張スクリプト
- GUIを使って簡単に監視の一時停止・開始が可能
- atコマンドと連携して、事前に監視停止・再開スケジュールを登録可能
  - maint.plのインストールのほか、BBのシステム設定ファイル $BBHOME/etc/bbdef-server.shに以下の設定追加が必要
    - RUNOPTS="ENABLE_DISABLE"

maint.pl画面

監視停止状態表示パネル

監視停止制御パネル

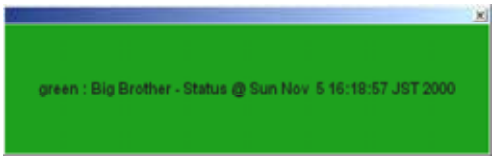
maint.pl 青アイコン(fs2監視停止中)



BB機能拡張スクリプト
BBTray - 監視サポートツール

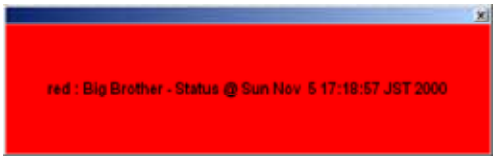
- Big Brother Display Serverを常時監視するサポートツール
  - `http://www.deadcat.net/cgi-bin/download.pl?section=4&file=BBtray.zip`
  - Windows9x/NT/2000/XPで動作
  - BBを監視し、状態が変化すると音とPopup Windowにて通知
  - Windowをクリックすることで、障害サマリー画面に直接とべるので、即時に現状把握可能
    - BBサーバーとIP通信ができれば、どこでも現状が分かる
  - 類似品にtkBB(Tk-Perl版)あり

BB機能拡張スクリプト
BBTray - 監視サポートツール



Green Window
- this is normal status

Yellow Window
- this is warning status.



Red Window
- this is critical status!!

機能拡張スクリプト BBtrayのコンフィグ

```
; BBTRAY.INI - BBtray Configuration File
;   This file must be in the same directory as the BBTRAY.EXE.
;   Changes will only take effect on restart of BBtray
;---------------------------------------------------------------------------
; Default options

[General]
DisplayURL=http://bb.xy.jp/bb/bb2.html
SoundsPath=C:¥Program Files¥BBtray¥Sounds¥
IconsPath=C:Program Files¥¥BBtray¥Icons¥
;ProxyName=192.168.0.200:3128
PollFrequency=15
PageDelay=900
PopupLevels=r,p,y,g

; String for tray icon's hint and pop-up window. Can include the following
; fields identifiers:
;   %U   BBDISPLAY URL
;   %T   BBDISPLAY title
;   %c   color letter (ex: 'g' for 'green')
;   %C   color string
;   ¥n   NewLine
; For the old URLOnHint format, use HintString=%C: %U
; OBS: Max HintString size is 63 chars.
HintString=My Servers: %T
PopupString=My Servers: %U¥n%T

;---------------------------------------------------------------------------
; These are the messages displayed by BBtray
[Messages]
VERIFY=Verifying...
NOCONN=It was not possible to connect to the monitoring system!
INVSTATUS=Invalid status received!
```

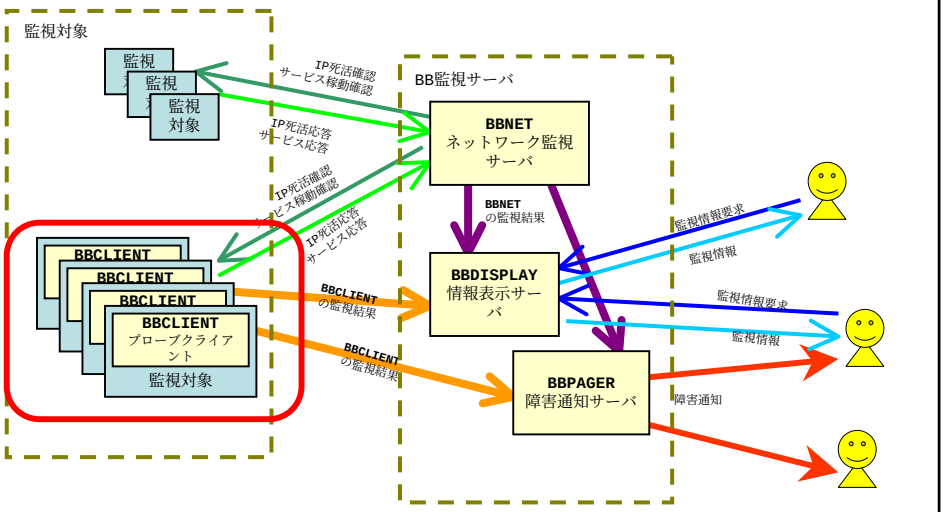

INDEX

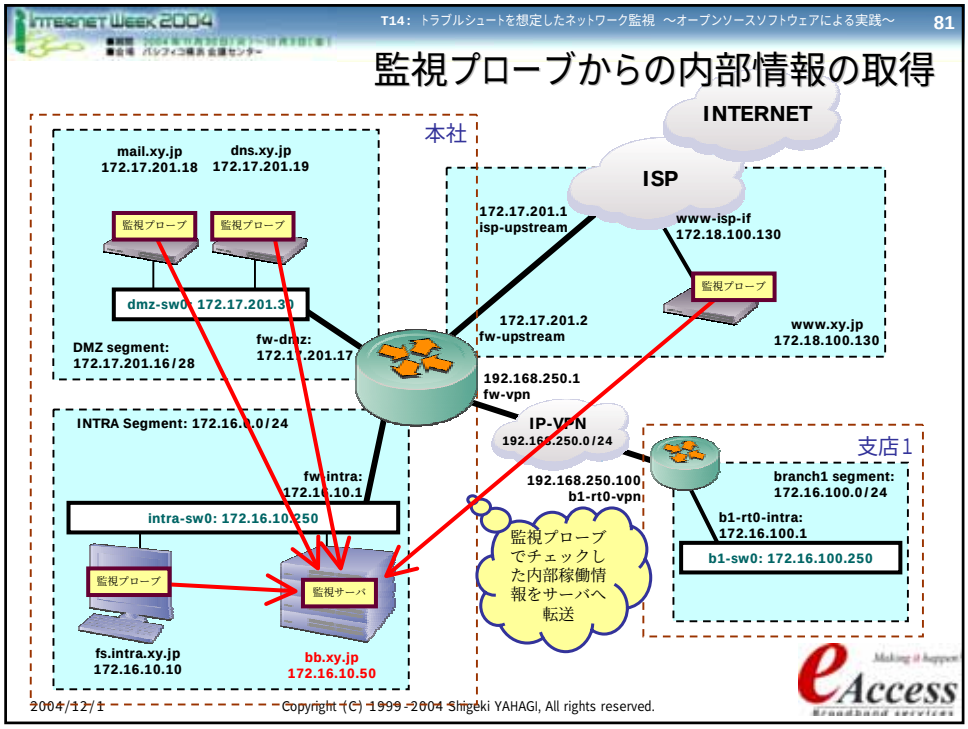
I. ネットワーク監視とトラブルシュート概論
II. 監視対象分析
III. 監視サーバからの監視
IV. プローブクライアントによるリソース監視
V. トラフィックリソース監視

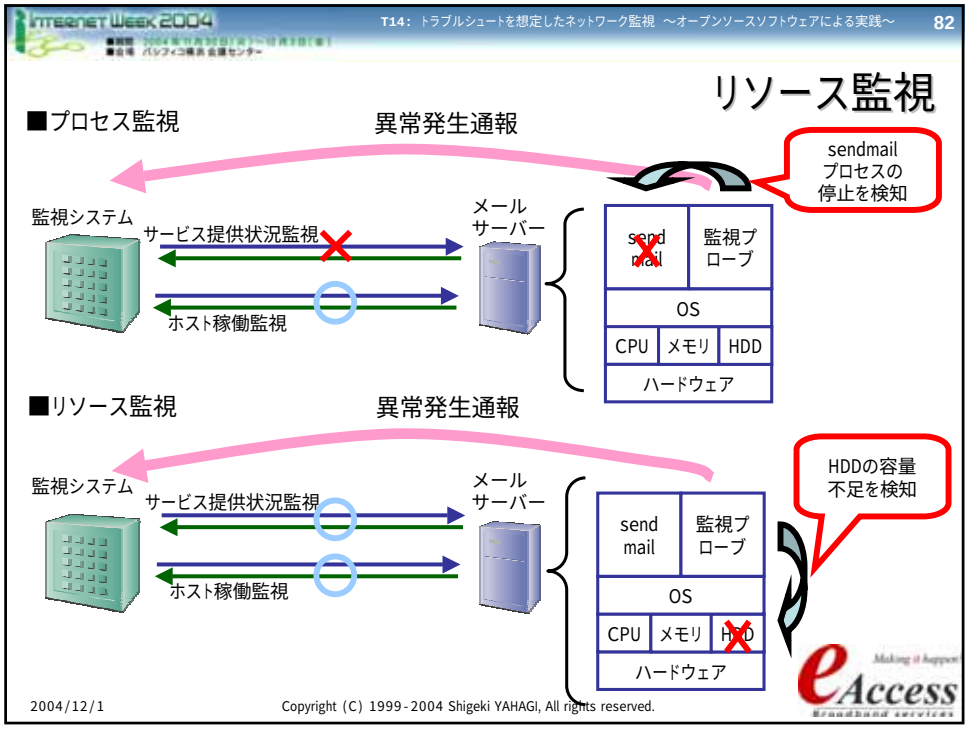
監視プローブによるリソース監視

- Big Brother監視サーバー単体では、各監視対象のIP死活監視とサービス稼働監視のみとなる
- より詳細に監視対象の稼働状態を把握するためには、監視対象にて自身のリソースをチェックする監視プローブのインストールが必要となる
- 監視プローブで可能となるリソース監視：
  - CPU使用率監視
  - プロセス稼働監視
  - ディスク容量監視
  - 自律メッセージ監視

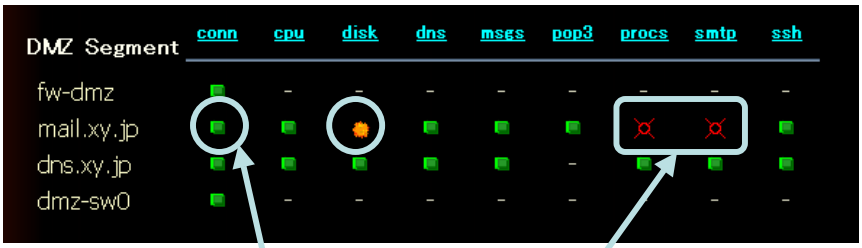
監視プローブによるリソース監視




INTERNET
ISP
本社
mail.xy.jp
172.17.201.18
dns.xy.jp
172.17.201.19
監視プローブ
監視プローブ
dmz-sw0: 172.17.201.30
DMZ segment:
172.17.201.16/28
fw-dmz:
172.17.201.17
172.17.201.1
isp-upstream
www-isp-if
172.18.100.130
監視プローブ
172.17.201.2
fw-upstream
www.xy.jp
172.18.100.130
192.168.250.1
fw-vpn
IP-VPN
192.168.250.0/24
192.168.250.100
b1-rt0-vpn
支店1
branch1 segment:
172.16.100.0/24
b1-rt0-intra:
172.16.100.1
b1-sw0: 172.16.100.250
INTRA Segment: 172.16.10.0/24
fw-intra:
172.16.10.1
intra-sw0: 172.16.10.250
監視プローブ
監視サーバ
監視プローブでチェックした内部稼働情報をサーバへ転送
fs.intra.xy.jp
172.16.10.10
bb.xy.jp
172.16.10.50
T14: トラブルシュートを想定したネットワーク監視 ～オープンソースソフトウェアによる実践～
81
監視プローブからの内部情報の取得
2004/12/1
Copyright (C) 1999-2004 Shigeki YAHAGI, All rights reserved.

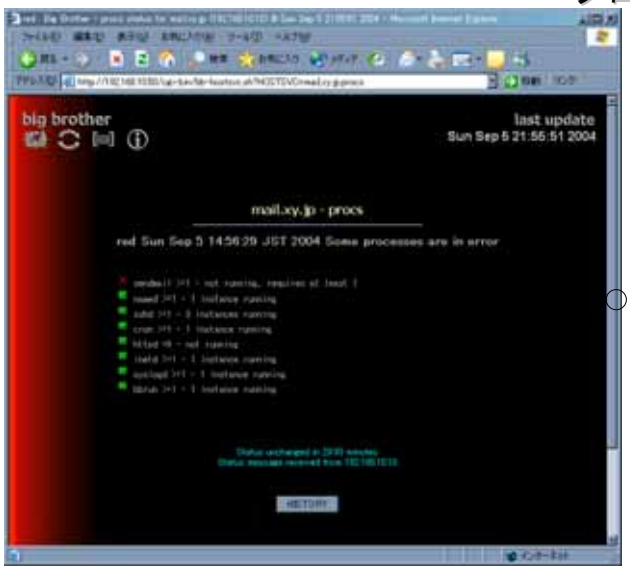

T14: トラブルシュートを想定したネットワーク監視 ～オープンソースソフトウェアによる実践～
82
リソース監視
■プロセス監視
異常発生通報
sendmail
プロセスの
停止を検知
監視システム
サービス提供状況監視
ホスト稼働監視
メール
サーバー
send
mail
監視プ
ローブ
OS
CPU
メモリ
HDD
ハードウェア
■リソース監視
異常発生通報
HDDの容量
不足を検知
2004/12/1
Copyright (C) 1999-2004 Shigeki YAHAGI, All rights reserved.

BBCLIENTを追加したときの監視項目



- mail.xy.jpで障害発生。IP死活監視はOK。
- サービス監視でSMTPのみ障害でプロセス監視でも障害がでている他のサービスでは警告があがってないので、SMTP回りの障害と判断
- DISK使用率監視で注意がでているが、注意レベルなので後回しにして、まずはプロセス監視の詳細情報チェックする！

プロセス監視画面

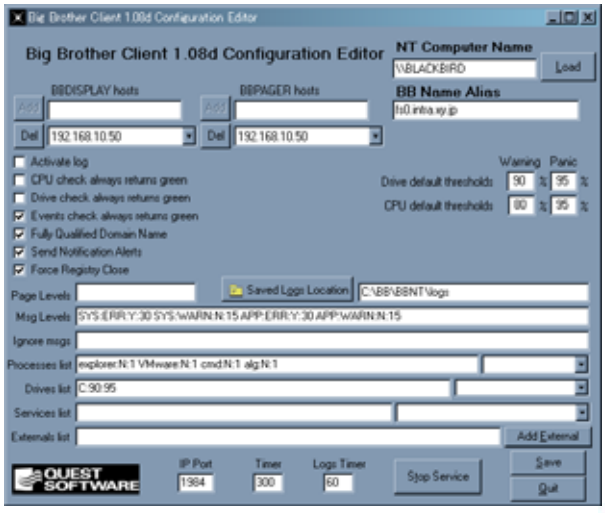


sendmailがなぜか落ちている！これが原因らしい。

監視プローブの設定

- 設定ファイル
  - CPU使用率監視：$BBHOME/etc/bb-cputab
  - 自律メッセージ監視：$BBHOME/etc/bb-msgstab
  - プロセス監視：$BBHOME/etc/bb-proctab
  - ディスク使用率監視：$BBHOME/etc/bb-dftab

Windows版BBCLIENT



監視プローブ設定 - CPU使用率監視 $BBHOME/etc/bb-cputab

- load averageを元にCPU使用率を監視
- レコードフォーマット:
  - <ホスト名>: <未設定> : <CPUWARN値> : <CPUPANIC値>
- 起動確認したいプロセスを定義する
  - <ホスト名> : レコードの対象となるホストの名称を指定
    - <ホスト名>には"localhost"の設定もあり、全ホストに適用可能なデフォルト設定として使用可能
  - <CPUWARN値> - Load average warningレベル設定値
  - <CPUPANIC値> - Load average panicレベル設定値
- 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)
  - デフォルトの値は最近のサーバでは小さすぎるので、5-10倍の値を設定

```
### bb-cputab
localhost : : 1500 : 2000
www.aa.co.jp : : 2000 : 3000
### bb-cputab end
```

2004/12/1

監視プローブ設定 - 自律メッセージ監視 $BBHOME/etc/bb-msgstab

- load averageを元にCPU使用率を監視
- レコードフォーマット:
  - <ホスト名>:<ログファイル>: <未設定> :<注意テキスト>:<警告テキスト>:<識別対象外テキスト>
- 起動確認したいプロセスを定義する
  - <ホスト名> : レコードの対象となるホストの名称を指定
    - <ホスト名>には"localhost"の設定もあり、全ホストに適用可能なデフォルト設定として使用可能
  - <ログファイル> : 検索対象となるログファイル名を絶対パス指定
  - <注意テキスト> : 注意イベント対象となる文字列パターンを列挙する
  - <警告テキスト> : 警告イベント対象となる文字列パターンを列挙する
  - <識別対象外テキスト> : 識別対象外の文字列パターンを列挙する

```
### bb-msgtabs
localhost:/var/log/messages::WARNING:NOTICE:
localhost:/var/log/maillog:: refused.*from;failed connection : error;ERROR : from localhost
www.aa.co.jp:/var/adm/messages::WARNING:NOTICE:
### bb-msgtabs end
```

2004/12/1

監視プローブ設定 - プロセス監視 $BBHOME/etc/bb-proctab

- 監視対象のプロセスの存在を監視する
- レコードフォーマット：
  - <ホスト名>: <PROC値>：<PAGEPROC値>
  - <ホスト名>：レコードの対象となるホストの名称を指定
    - <ホスト名>には”localhost”の設定もあり、全ホストに適用可能なデフォルト設定として使用可能
  - <PROC値>：warning対象プロセス名を列挙する
  - <PAGEPROCS値>：panic対象プロセス名を列挙する
    - 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とまずいプロセスの監視に使用
      - ex: !inetd, !sendmail, ・・・

監視プローブ設定 - プロセス監視

監視プローブ設定 - プロセス監視 $BBHOME/etc/bb-proctab

監視対象	プロセス確認									
	inetd	bbrun	sshd	named	httpd	cron	xntpd	syslogd	sendmail	popd
dns.xy.jp	×	○	🔴	🔴	- - -	🔴	○	○	🔴	- - -
mail.xy.jp	×	○	🔴	🔴	- - -	🔴	○	○	🔴	🔴
www.xy.jp	×	○	🔴	- - -	🔴	🔴	○	○	×	- - -
bb.xy.jp	×	○	🔴	- - -	🔴	🔴	○	○	×	- - -

記号	説　明
🔴	警告レベルでの存在確認プロセス
○	注意レベルでの存在確認プロセス
×	注意レベルでの非存在確認プロセス
- - -	設定対象外

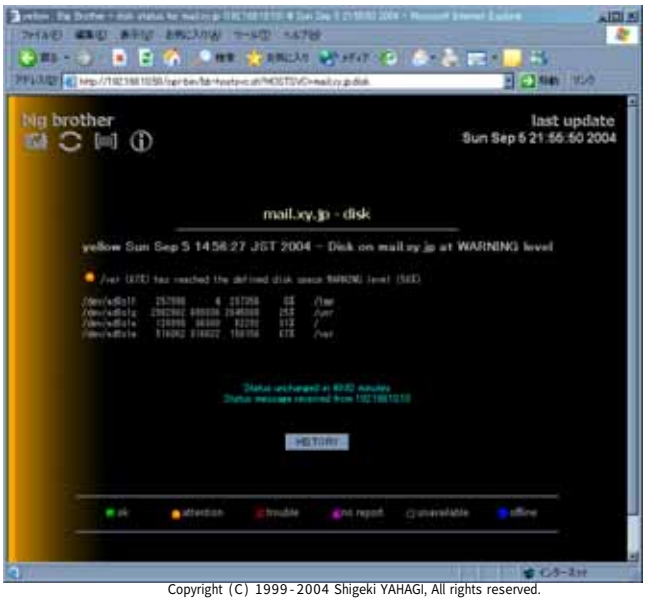
```
### bb-proctab
dns.xy.jp  : !inetd bbrun xntpd syslogd : sshd named cron sendmail
mail.xy.jp : !inetd bbrun xntpd syslogd : sshd named cron sendmail popd
www.xy.jp  : !inetd bbrun xntpd syslogd !sendmail : sshd httpd cron
bb.xy.jp   : !inetd bbrun xntpd syslogd !sendmail : sshd httpd cron ntpd
### bb-proctab end
```


監視プローブ設定 - ディスク使用率監視 $BBHOME/etc/bb-dftab

- パティションごとのディスク使用率を指定する
  - レコードフォーマット1: デフォルト設定
    <partition>：<DFWARN値>：<DFPANIC値>
  - レコードフォーマット2: ホスト別設定
    <ホスト名>: <partition>：<DFWARN値>：<DFPANIC値>
    - <ホスト名>：レコードの対象となるホストの名称を指定
      - <ホスト名>には”localhost”の設定もあり、全ホストに適用可能なデフォルト設定として使用可能
    - <DFWARN値> - warning設定値（default: 90%）
    - <DFPANIC値> - panic設定値（default: 95%）

```
### bb-dftab
/:80:90
/tmp:50:70
/var:70:80
/usr:80:90
www.xy.jp:/var:50:70
mail.xy.jp:/var:50:60
### end of bb-dftab
```

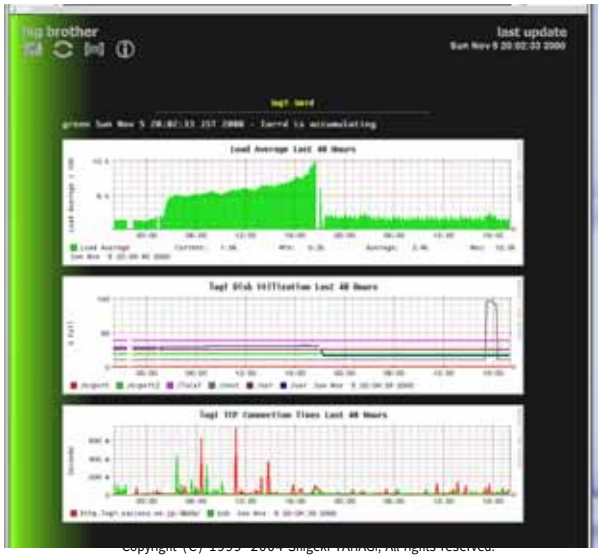
ディスク使用率監視画面



リソース監視 機能拡張 larrd(load average rrdtool)

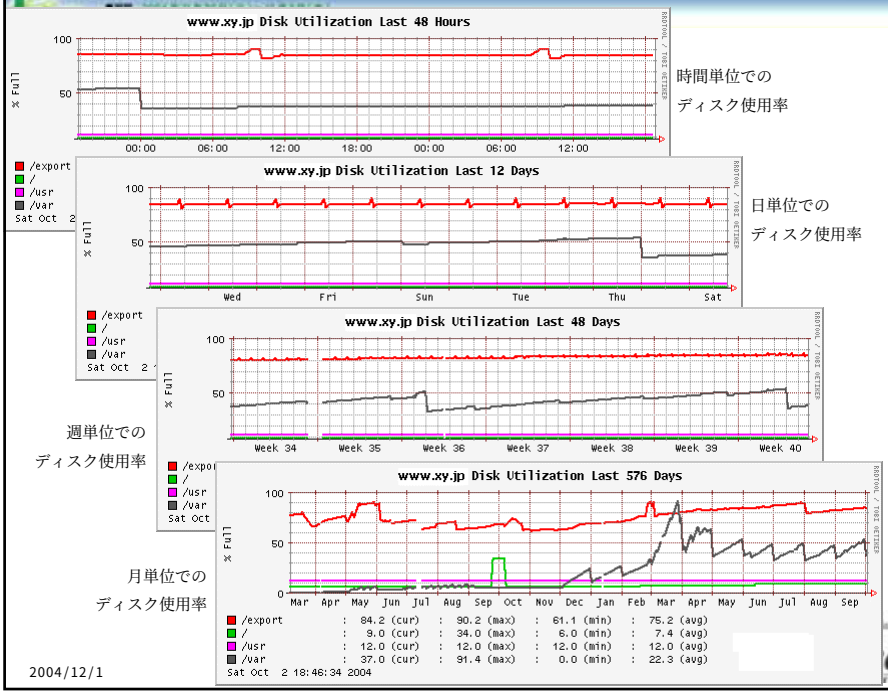
- **http://larrd.packetpushers.com/**
- Big Brother Clientが各監視対象から取得したデータをRRDToolによりグラフ化する
  - 対象データ：load average, Disk Usage, Memory, SWAP, bind, TCP Connection Time, (Memory Usage, CPU idle,)...
- グラフ作成のみに特化しており、larrdは閾値を設定したトラフィックアラーム監視は行わない
- 以下のインストール手順だけすれば、ほかの設定は必要なし
  - RRDToolsのインストール
  - 指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/bb-bbexttabへの登録
  - BigBrother再起動

システムリソース管理
BB-RRDTool連係：larrd画面



2004/12/1

disk使用率の経過監視の例



2004/12/1

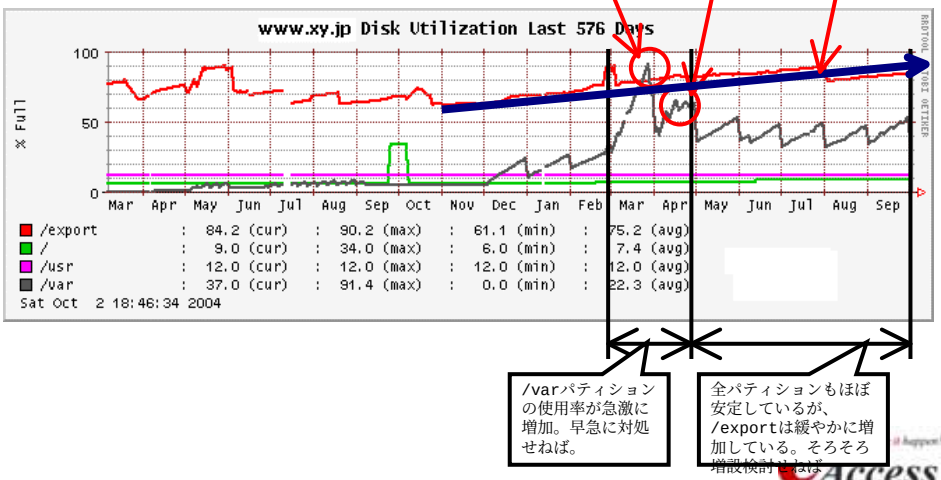
disk使用率の経過監視の例

急激なディスク使用率増加対処
ファイル配置の最適化と圧縮

ディスク増設
による本対処

緩やかな
増加傾向

図1-d 月単位でのディスク使用率



/varパティションの使用率が急激に増加。早急に対処せねば。

全パティションもほぼ安定しているが、/exportは緩やかに増加している。そろそろ増設検討すべき

2004/12/1

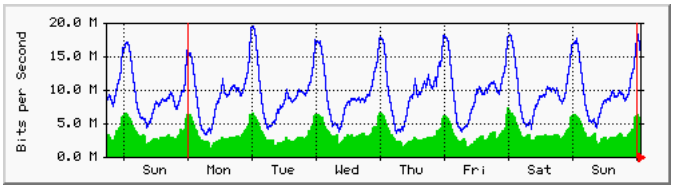
INDEX

I. ネットワーク監視とトラブルシュート概論
II. 監視対象分析
III. 監視サーバからの監視
IV. プローブクライアントによるリソース監視
V. トラフィックリソース監視

2004/12/1

トラフィックリソース監視
MRTG(Multi Router Traffic Grapher)

- MRTG : Multi Router Traffic Grapher
  - http://ee-staff.ethz.ch/~oetiker/webtools/mrtg/mrtg.html
- 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
- ネットワーク・トラフィック監視をする上での定番ツール



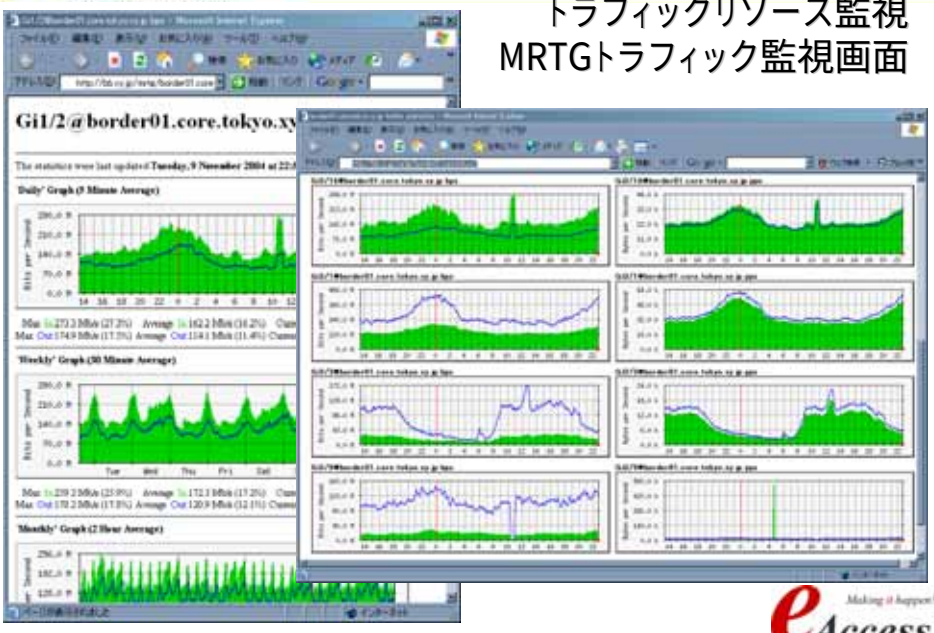
トラフィックリソース監視
MRTGの特徴1

- ほとんどのUnixプラットフォームとWindowsNT/2k/XP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らない
- 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
- コンフィグからindexを簡単に生成するツールが付属
- デフォルトはcronによる定期起動だが、Daemon化することも可能
- Unixプラットフォームでは並列照会による高速化をサポート

トラフィックリソース監視 MRTGの特徴2

- 多様性に富んだ測定対象の指定方法
  - 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
- 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
  - データは本オプション指定により自動的にRRD形式にデータ移行される
  - グラフの作成は測定時しない。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
- 最新版(2.10)でのトピック
  - IPv6対応
  - ConversionCode: Perlの外部サブルーチン関数を埋め込み可能

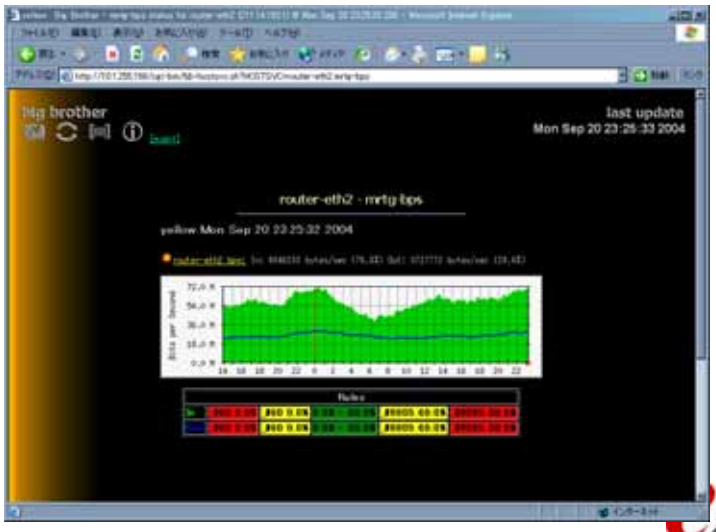
トラフィックリソース監視 MRTGトラフィック監視画面



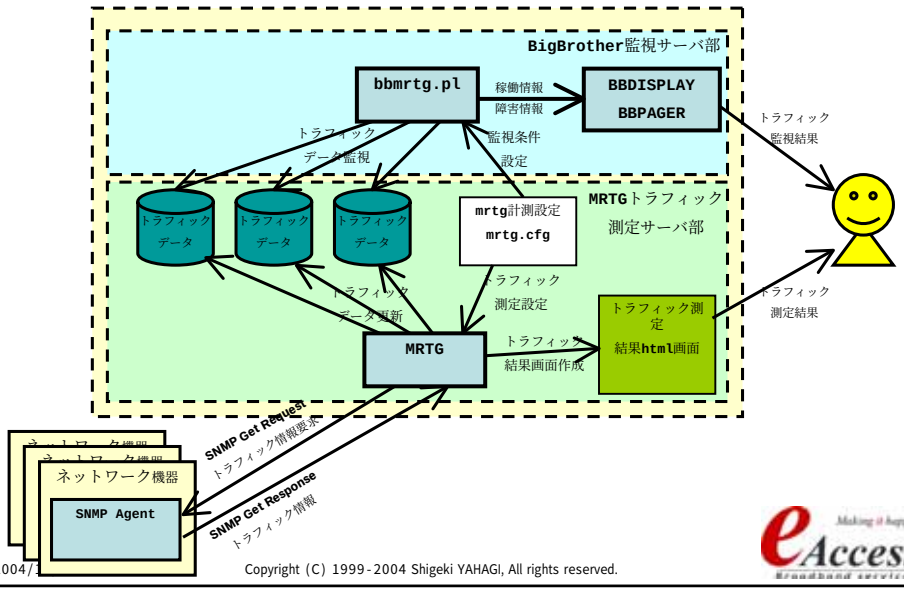
トラフィックリソース監視
BBとMRTGの連携：bbmrtg.pl

- MRTGと連携するBigBrother機能拡張
  - bbmrtg.pl ver 1.41：
    http://www.deadcat.net/viewfile.php?fileid=753
  - bbmrtg-craigs_ver.pl ver 1.5 ：
    http://www.deadcat.net/viewfile.php?fileid=58
- MRTGで計測しているトラフィックデータの監視を行う
- MRTGの計測設定ファイルの各測定項目にしきい値を設定
- 監視はMRTGの計測ファイル単位で行う。MRTG設定ファイルに定義されている計測項目を監視する

トラフィックリソース監視
BBとMRTGの連携：bbmrtg.pl



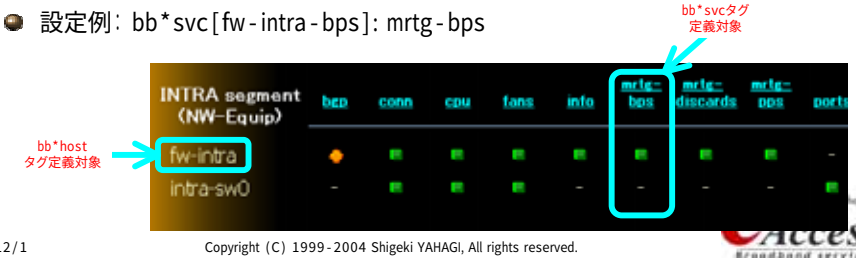
bbmrtg.plプロセス関係図



トラフィックリソース監視 bbmrtg.pl 指定タグ - 1

① 監視ホスト名称タグ (必須項目)
- 'bb*host[<測定項目>]: <監視ホスト名>'
- <測定項目>が属するホスト名を<監視ホスト名称>に設定する。<監視ホスト名>はbb-hostsに登録されている名前と一致している必要がある。
- 設定例: bb*host[fw-intra-bps]: fw-intra

② 監視テスト項目タグ (必須項目)
- 'bb*svc[<測定項目>]: <テスト項目名>'
- <測定項目>で行われているトラフィック監視のテスト名称を設定する。<監視ホスト名>のエントリーの中で<テスト項目名>として表示される。
- 設定例: bb*svc[fw-intra-bps]: mrtg-bps



トラフィックリソース監視 bbmrtg.pl 指定タグ - 2

- 監視しきい値タグ（必須項目）
  - 'bb*yellow[<測定項目>]: <上限閾値>‘
  - 'bb*red[<測定項目>]: <上限閾値>‘
  - <測定項目>のトラフィック監視の注意・警報レベルの閾値を設定する。bb*yellowが注意レベル、bb*redが警報レベルの指定になる。値の設定方法は測定値とパーセント値の二つが設定でき、パーセント指定の場合には<測定項目>で設定されるMaxByte[<測定項目>]: での値を100%とした比率で計算される。
- 監視計測単位タグ（オプション項目）
  - bb*unit[<測定項目>]: <表示単位>
  - <測定項目>で行われているトラフィック監視の測定単位を設定する。
  - 設定例：bb*unit[fw-intra-cpu]: "CPU ulitilization“
- データ種別設定タグ（オプション項目）
  - bb*in[<測定項目>]: <第1系列データ種別>
  - bb*out[<測定項目>]: <第2系列データ種別>
  - 2種類のデータ系列の種別を設定する。
  - 設定例：bb*in[fw-intra-cpu]: "in 1min“
bb*out[fw-intra-cpu]: "in 5min"

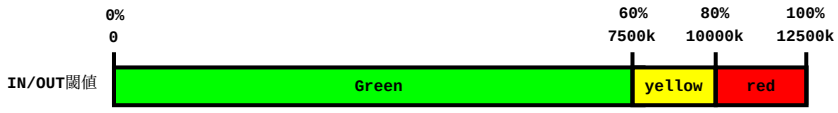
トラフィックリソース監視 bbmrtg.pl 閾値設定 - 1

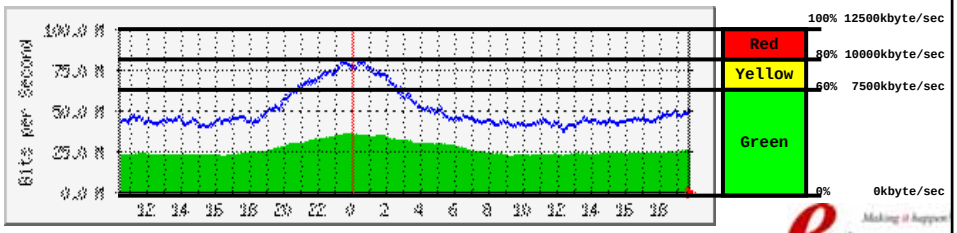
(1) 上限値指定 （測定値指定）

```
MaxByte[fw-intra-bps]: 12500000
bb*yellow[fw-intra-bps]: 7500000
bb*red[fw-intra-bps]: 10000000
```

(1’)上限値指定 （パーセント指定）

```
MaxByte[fw-intra-bps]: 12500000
bb*yellow[fw-intra-bps]: 60%
bb*red[fw-intra-bps]: 80%
```





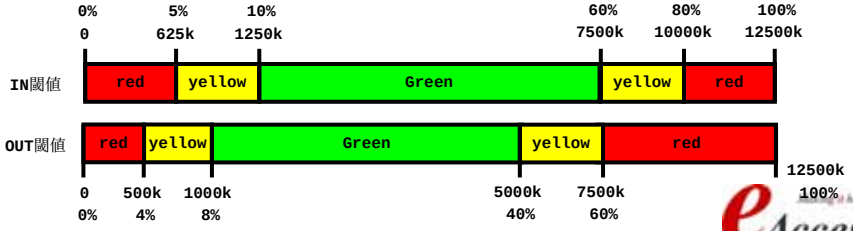
トラフィックリソース監視 bbmrtg.pl 閾値設定 - 2

(2) 上限下限値指定 （IN/OUT同値指定、測定値指定）

```
MaxByte[fw-intra-bps]: 12500000
bb*yellow[fw-intra-bps]: 1250000:7500000
bb*red[fw-intra-bps]: 625000:10000000
```

(3) 上限下限値指定 （IN/OUT個別指定、測定値指定）

```
MaxByte[fw-intra-bps]: 12500000
bb*yellow[fw-intra-bps]: 1250000:7500000:1000000:5000000
bb*red[fw-intra-bps]: 625000:10000000:500000:7500000
```



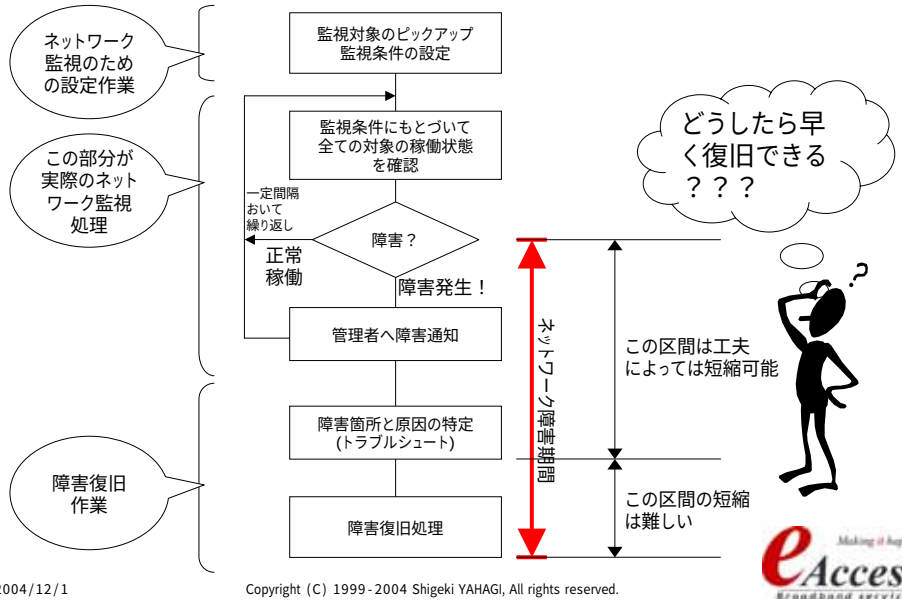
2004/12/1

fw-intra MRTG設定 bbmrtg.pl版

```
Target[fw-intra-bps]: #Fa2:myReadCom@router
MaxBytes[fw-intra-bps]: 12500000
Title[fw-intra-bps]: fw-intra bps
PageTop[fw-intra-bps]: <H1>fw-intra bps</H1>
Options[fw-intra-bps]: growright, bits
bb*host[fw-intra-bps]: fw-intra
bb*svc[fw-intra-bps]: mrtg-bps
bb*yellow[fw-intra-bps]: 60%
bb*red[fw-intra-bps]: 80%
bb*unit[fw-intra-bps]: bytes/sec

Target[fw-intra-pps]: ifInUcastPkts#Fa2&ifOutUcastPkts#Fa2:myReadCom@router
MaxBytes[fw-intra-pps]: 30000
Title[fw-intra-pps]: fw-intra pps
PageTop[fw-intra-pps]: <H1>fw-intra pps</H1>
YLegend[fw-intra-pps]: packet/sec
ShortLegend[fw-intra-pps]: pps
Options[fw-intra-pps]: growright
bb*host[fw-intra-pps]: fw-intra
bb*svc[fw-intra-pps]: mrtg-pps
bb*yellow[fw-intra-pps]: 10000
bb*red[fw-intra-pps]: 20000

Target[fw-intra-discards]: ifInDiscards#Fa2&ifOutDiscards#Fa2:myReadCom@router
MaxBytes[fw-intra-discards]: 10000
Title[fw-intra-discards]: fw-intra discards
PageTop[fw-intra-discards]: <H1>fw-intra discards</H1>
YLegend[fw-intra-discards]: Discards
ShortLegend[fw-intra-discards]: Discards
Options[fw-intra-discards]: growright
bb*host[fw-intra-discards]: fw-intra
bb*svc[fw-intra-discards]: mrtg-discards
bb*yellow[fw-intra-discards]: 1
bb*red[fw-intra-discards]: 5
```

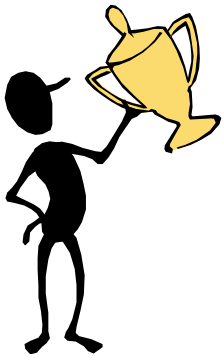
2004/12/1

まとめ：ネットワーク監視のフロー



まとめ：ネットワーク障害を早期復旧させるには

- 漏れのない稼働状態確認
- 的確な障害通知
- 迅速な障害原因調査開始
- 迅速な障害原因の特定
- 障害復旧のための準備



Making it happen!
eAccess
Broadband services

追加資料1：
BigBrother監視サーバ補足資料

BigBrother 機能拡張 bbgen

- BTF版BBをベースにプログラムへパッチ当てし、大幅な速度向上・機能拡張を行う
- ほとんどの主要プログラムにパッチがあたっているために、BTFライセンスサポート外となるが、それを補ってあまるほどの機能拡張がなされる
- BigBrother BTF版 ver 1.9cとver 1.9eに対応
- 他の機能拡張との互換性があり、ほとんどのスクリプトの共存可能

監視状態表示サーバ(BBDISPLAY)の拡張

a. bb-hosts定義以外の監視画面作成機能
b. 3階層以上のサブページサポート
c. 特定アラート専用ページの作成
d. 障害履歴ページの拡張。過去にさかのぼった障害履歴の参照機能
e. manドキュメントの充実
f. 稼働率・SLAレポート作成機能の追加
g. 多くのWEBページの機能拡張

ネットワーク監視サーバ(BBNET)の拡張

a. fpingによる高速IP死活監視機能
b. サービス監視の並列処理による高速監視機能
c. より詳細なhttps監視設定機能
d. proxy経由でのhttp監視機能
e. LDAPサービス監視機能
f. CGI稼働確認機能
g. コンテンツ確認機能
h. 監視設定ファイルの分割管理機能
i. その他多数の機能拡張

BigBrother 機能拡張 bbgen 拡張タグー1

機能名	タグ用途	使用方法
外部ファイル挿入	外部設定ファイル挿入	include <filename>
	外部BBDISPLAY設定ファイル挿入	dispinclude <filename>
	外部BBNET設定ファイル挿入	netinclude <filename>
BBDISPLAY bb-hosts拡張	多階層サブページ指定	subparent <parentpage> <newpage> [<Page-title>]
	タイトルテキスト挿入	title <title_text>
	表示ホスト名変更	A.B.C.D HOST # NAME:<hostname>
	BBCLIENTエイリアス名指定	A.B.C.D HOST # CLIENT:<hostname>
	ホストコメント表示	A.B.C.D HOST # COMMENT:<host_comment>
	ホスト説明設定	A.B.C.D HOST # DESCR:<HostType>:<Description>
	bb.html非表示設定	A.B.C.D HOST # nodisp
	障害サマリ画面非表示設定	A.B.C.D HOST # nobb2
	複数ホスト定義時優先指定	A.B.C.D HOST # perfer
	IPレンジでのIP死活監視	dialup <hostname> <startIP> <count>
	LARRDグラフ表示設定	A.B.C.D HOST # LARRD:[*,][![<larrdgraph>….]]
NK機能拡張	NK監視指定	A.B.C.D HOST # NK:testname[,<testname>]
	NK対象時間指定	A.B.C.D HOST # NKTIME=<day>:<starttime>:<endtime>[,<day>:<starttime>:<endtime>]
WAP機能拡張	WMLページ設定	A.B.C.D HOST # WML:[+|-]<testname>[,[+|-]<testname>]
状態広報オプション	状態広報規制設定(RED)	A.B.C.D HOST # NOPROPRED:[+|-]<testname>[,[+|-]<testname>]
	状態広報規制設定(YELLOW)	A.B.C.D HOST # NOPROPYELLOW:[+|-]<testname>[,[+|-]<testname>]
	状態広報規制設定(PURPLE)	A.B.C.D HOST # NOPROPPURPLE:[+|-]<testname>[,[+|-]<testname>]
	状態広報規制設定(ACK)	A.B.C.D HOST # NOPROPACK:[+|-]<testname>[,[+|-]<testname>]
稼働率レポート指定	稼働率レポート対象時間指定	A.B.C.D HOST # REPORTTIME=<day>:<starttime>:<endtime>[,<day>:<starttime>:<endtime>]
	稼働率レポートしきい値指定	A.B.C.D HOST # WARNPCT:<percentage>

BigBrother 機能拡張 bbgen 拡張タグー2

機能名	タグ用途	使用方法
BBTEST-NET bb-hosts拡張サービス監視	監視対象ネットワーク指定	A.B.C.D HOST # NET:<location>
	SSL認証対象外指定	A.B.C.D HOST # nosslcert
	SSL認証有効期限設定	A.B.C.D HOST # ssldays=<WARNDAYS>:<ALARMDAYS>
	非監視時間指定	A.B.C.D HOST # DOWNTIME=<day>:<starttime>:<endtime>[,<day>:<starttime>:<endtime>]
	SLAレポート対象時間指定	A.B.C.D HOST # SLA=<day>:<starttime>:<endtime>[,<day>:<starttime>:<endtime>]
	監視テスト依存設定	A.B.C.D HOST # depends=(<testA>:<host1>/<test1>,<host2>/<test2>),(<test8>:<host3>/<test3>),[...]
	障害判定回数設定	A.B.C.D HOST # badTEST[-<weekdays>-<starttime>-<endtime>]:<x>:<y>:<z>
	dns監視拡張指定1	A.B.C.D HOST # dns[=<hostname>]
	dns監視拡張指定2	A.B.C.D HOST # dns=<TYPE>:<lookup>[,<TYPE>:<lookup>...]
	dns監視拡張指定(dig使用)	A.B.C.D HOST # dig
	ntp監視	A.B.C.D HOST # ntp
	ldap監視指定1	A.B.C.D HOST # ldap
	ldap監視指定2	A.B.C.D HOST # ldap://<hostname>/dn[?<attrs>[?<scope>[?<filter>[?<exts>]]]]
	ldap ssl監視指定1	A.B.C.D HOST # ldaps
	ldap ssl監視指定2	A.B.C.D HOST # ldaps://<hostname>/dn[?<attrs>[?<scope>[?<filter>[?<exts>]]]]
	ldap login ID指定	A.B.C.D HOST # ldaplogin=<username>:<password>
	ldap障害ステータス変更指定	A.B.C.D HOST # ldapyellowfail
	RPCサービス監視指定	A.B.C.D HOST # rpc[=rpcservice1,rpcservice2,...]
BBTEST-NET bb-hosts拡張IP死活監視	IP死活監視指定	A.B.C.D HOST # conn
	IP死活監視拡張指定	A.B.C.D HOST # conn={best,|worst,}IP1[,IP2...]
	IP死活監視非実施指定	A.B.C.D HOST # badconn[-weekdays-starttime-endtime]:x:y:z
	IPルーティング監視指定１	A.B.C.D HOST # route:router1,router2,....
	IPルーティング監視指定2	A.B.C.D HOST # route_LOCATION:router1,router2,...
	traceroute確認指定	A.B.C.D HOST # trace
	traceroute非確認指定	A.B.C.D HOST # notrace

BigBrother 機能拡張 bbgen 拡張タグー3

機能名	タグ用途	使用方法
BBTEST-NET HTTP拡張監視	BASIC認証	A.B.C.D HOST # http://USERNAME:PASSWORD@www.sample.com/
	ssl client認証	A.B.C.D HOST # http://CERT:FILENAME@www.sample.com/
	http ver指定	A.B.C.D HOST # http10://www.sample.com/ : use HTTP 1.0
		A.B.C.D HOST # http11://www.sample.com/ : use HTTP 1.1
	ssl ver指定	A.B.C.D HOST # https2://www.sample.com/ : use only SSLv2
		A.B.C.D HOST # https3://www.sample.com/ : use only SSLv3
		A.B.C.D HOST # httpsm://www.sample.com/ : use only 128-bit ciphers
		A.B.C.D HOST # httpsm://www.sample.com/ : use only 128-bit ciphers
	IPアドレス指定	A.B.C.D HOST # http://www.sample.com=1.2.3.4/index.html
		A.B.C.D HOST # http://www.sample.com:3128=1.2.3.4/index.html
	proxy経由	A.B.C.D HOST # http://webproxy.sample.com:3128/http://bb4.com/
		A.B.C.D HOST # http://fred:Wilma1@webproxy.sample.com:3128/http://bb4.com/
BBTEST-NET コンテンツチェック	コンテンツチェック	A.B.C.D HOST # cont[=COLUMN];URL;[expected_data_regexp|A.B.C.D HOST #digesttype:digest]
		A.B.C.D HOST # content=URL
	CGIチェック	A.B.C.D HOST # post[=COLUMN];URL;form-data;[expected_data_regexp|A.B.C.D HOST #digesttype:digest]
	コンテンツ不稼働チェック	A.B.C.D HOST # nocont[=COLUMN];URL;forbidden_data_regexp
	CGI不稼働チェック	A.B.C.D HOST # nopost[=COLUMN];URL;form-data;expected_data_regexp
	content-typeチェック	A.B.C.D HOST # type[=COLUMN];URL;expected_content_type

BigBrother 機能拡張
bbgen監視設定情報画面

Hostname: BB SVR1 (bb.xy.jp)
IP: 172.16.0.10
Page/subpage: Top page

Host type: FreeBSD48
Description: "BigBrotherServer1"

NK alerts: None

Network tests use: Hostname
Checked with ping: Yes

URL checks: http://bb.xy.jp/bb/

E-mail/SMS alerting:

Services	Ex.Services	Weekdays	Time	Recipients
All		All days	0000-2359	yahagi bb
Exceptions				
All		All days	1610-1625	yahagi@eaccess.net

Default time between each alert: 15 minutes

BigBrother 機能拡張
bbgen拡張ヒストリー

BigBrother 機能拡張
bbgen拡張ヒストリー 過去のイベント表示

2004/12/1

TIPS - BB編1

- 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
- Big Brotherサーバのシステム監査ログには注意が必要
  - BBの基本はshell scriptとなっており必要な機能は外部コマンドで実現されている。よって一回の監視フェーズにおいて数十のプログラムが起動される
  - Accountingログが短時間に巨大になる
  - ログ領域の拡大。細かなメンテナンス
  - もしくはアカウンティングを停止
    - # accton

2004/12/1

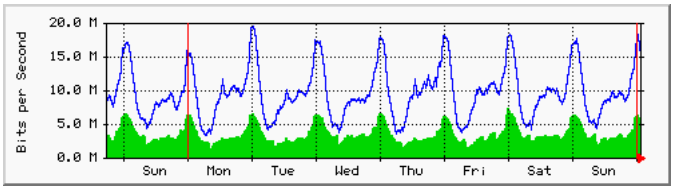
TIPS - BB編2

- Longer than Sleeptime XXXがでたら環境限界の印
  - BBのシステムログは$BBHOME/BBOUT。これをチェック！
  - Longer than Sleeptimeメッセージは監視間隔以内に監視が終わらないというシステムメッセージ
    - `Thu Nov 1 06:12:07 JST 2001 bbrun: (/usr/local/bb/ext/fping.sh) Runtime 517 longer than Sleeptime 300`
    - `Thu Nov 1 06:13:21 JST 2001 bbrun: (/usr/local/bb/bin/bb-network.sh) Runtime 346 longer than Sleeptime 300`
  - マシンスペックのグレードアップ･監視サーバ分割を視野にいれた、システム環境･チューニングを含めた見直しが必要

追加資料2：
MRTGによるトラフィック計測

MRTGとは

- MRTG：Multi Router Traffic Grapher
- http://ee-staff.ethz.ch/~oetiker/webtools/mrtg/mrtg.html
- 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



MRTGの特徴1

- ほとんどのUnixプラットフォームとWindowsNT/2k/XP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らない
- 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
- コンフィグからindexを簡単に生成するツールが付属
- デフォルトはcronによる定期起動だが、Daemon化することも可能
- Unixプラットフォームでは並列照会による高速化をサポート

MRTGの特徴2

- 多様性に富んだ測定対象の指定方法
  - 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
- 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
  - データは本オプション指定により自動的にRRD形式にデータ移行される
  - グラフの作成は測定時しない。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
- 最新版(2.10)でのトピック
  - IPv6対応
  - ConversionCode: Perlの外部サブルーチン関数を埋め込み可能

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.xy.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
  - pps/packet discardsなどの他の項目測定については、cfgmakerの結果を元に作成していくのが、普通のやり方
    - 各測定項目のスケルトンパターンを持つのが一番有効ではあるが...
- 以下のキー指定可能

```
--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
```

MRTG - cfgmaker の出力結果例

```
$cfgmaker  --ifref=name  himitsu@192.168.0.1

～初期設定処理表示:省略～

# Created by
# /usr/local/bin/cfgmaker --ifref=name himitsu@192.168.0.1

### Global Config Options

#  for UNIX
# WorkDir: /home/http/mrtg

#  or for NT
# WorkDir: c:¥mrtgdata

### Global Defaults

#  to get bits instead of bytes and graphs growing to the right
# Options[_]: growright, bits

######################################################################
# System: router1
# Description: Cisco Internetwork Operating System Software
# Contact:
# Location:
######################################################################

### Interface 1 >> Descr: 'ATM2/0' | Name: 'AT2/0' | Ip: '' | Eth: ''
###
### The following interface is commented out because:
### * it is operationally DOWN
#
# Target[192.168.0.1_AT2_0]: #AT2/0:himitsu@192.168.0.1:
# SetEnv[192.168.0.1_AT2_0]: MRTG_INT_IP="" MRTG_INT_DESCR="ATM2/0"
# MaxBytes[192.168.0.1_AT2_0]: 10720000
# Title[192.168.0.1_AT2_0]: Traffic Analysis for AT2/0 -- router1
# PageTop[192.168.0.1_AT2_0]: <H1>Traffic Analysis for AT2/0 --
router1</H1>
#  <TABLE>
#    <TR><TD>System:</TD>     <TD>router1 in </TD></TR>
#    <TR><TD>Maintainer:</TD> <TD></TD></TR>
#    <TR><TD>Description:</TD><TD>ATM2/0  </TD></TR>
#    <TR><TD>ifType:</TD>     <TD>sonet (39)</TD></TR>
#    <TR><TD>ifName:</TD>     <TD>AT2/0</TD></TR>
#    <TR><TD>Max Speed:</TD>  <TD>18.7 MBytes/s</TD></TR>
#  </TABLE>


### Interface 2 >> Descr: 'FastEthernet0/0' | Name: 'Fa0/0' | Ip:
'192.168.0.1' | Eth: '00-05-01-a0-7c-00' ###

Target[192.168.0.1_Fa0_0]: #Fa0/0:himitsu@192.168.0.1:
SetEnv[192.168.0.1_Fa0_0]: MRTG_INT_IP="192.168.0.1"
MRTG_INT_DESCR="FastEthernet0/0"
MaxBytes[192.168.0.1_Fa0_0]: 12500000
Title[192.168.0.1_Fa0_0]: Traffic Analysis for Fa0/0 -- router1
PageTop[192.168.0.1_Fa0_0]: <H1>Traffic Analysis for Fa0/0 --
router1</H1>
 <TABLE>
   <TR><TD>System:</TD>     <TD>router1 in </TD></TR>
   <TR><TD>Maintainer:</TD> <TD></TD></TR>
   <TR><TD>Description:</TD><TD>FastEthernet0/0  </TD></TR>
   <TR><TD>ifType:</TD>     <TD>ethernetCsmacd (6)</TD></TR>
   <TR><TD>ifName:</TD>     <TD>Fa0/0</TD></TR>
   <TR><TD>Max Speed:</TD>  <TD>12.5 MBytes/s</TD></TR>
   <TR><TD>Ip:</TD>         <TD>192.168.0.1 ()</TD></TR>
 </TABLE>


### Interface 3 >> Descr: 'Ethernet1/0' | Name: 'Et1/0' | Ip: '' |
Eth: '00-05-01-a0-7c-1c' ###
### The following interface is commented out because:
### * it is operationally DOWN
#
# Target[192.168.0.1_Et1_0]: #Et1/0:himitsu@192.168.0.1:
# SetEnv[192.168.0.1_Et1_0]: MRTG_INT_IP=""
MRTG_INT_DESCR="Ethernet1/0"
# MaxBytes[192.168.0.1_Et1_0]: 1250000
# Title[192.168.0.1_Et1_0]: Traffic Analysis for Et1/0 -- router1
# PageTop[192.168.0.1_Et1_0]: <H1>Traffic Analysis for Et1/0 --
router1</H1>

後､省略
```


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

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.xy.jp`
    - `Target[gw1-err-3]: ifInErrors.3&ifOutErrors.3:himitsu@gw1.xy.jp`
    - `Target[gw1-if-1]: -/10.0.0.101:himitsu@gw1.xy.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

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

測定項目

- 各ネットワークノードのポートにおいて以下の項目を測定する
  - トラフィック
    - bps(incoming/outgoing)
    - pps(incomfing/outgoing)
  - エラー関係
    - packet discards (incoming/outgoing)
    - interface errors (incoming/outgoing)

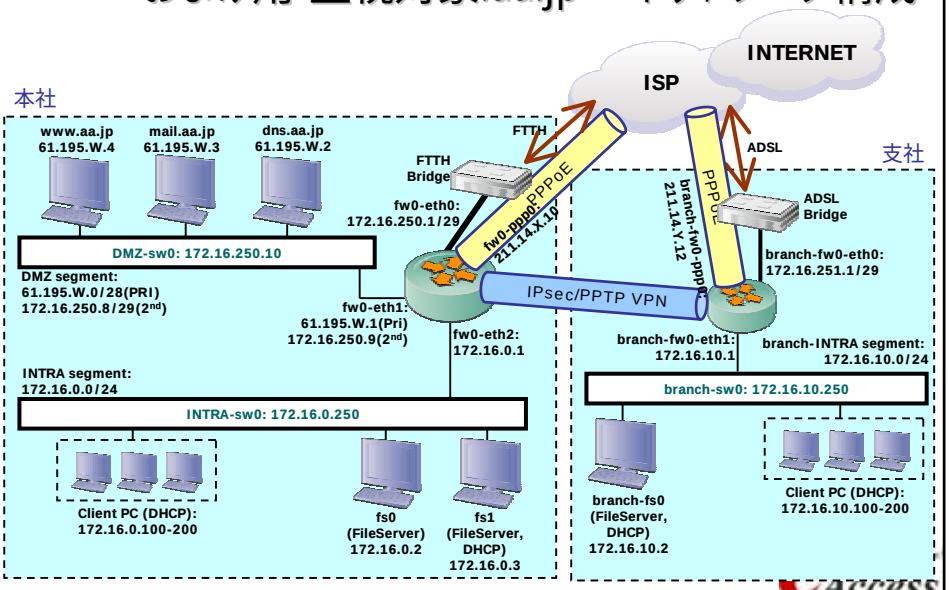
トラフィック監視 使用するSNMP OID/MIB Symbols

- **[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**

mrtg configの作り方

- 測定項目はひとつの対象に対して以下の4項目
  - bps, pps, packet discards, interface err
  - これらは独立したコンフィグとしてまとめるのがやりやすいが、indexmakerを使ってindex.htmlを作ることを考えると、正常トラフィック(bps, pps)とエラー系トラフィック(discards, error)にまとめるのが使いやすい。
  - 測定結果ディレクトリはマシンごとにまとめる
- Target指定のキー項目
  - ifIndex指定が一番素直だが、indexとインタフェースの関連を人がとらなければならない。リブートするとifIndexの対応表は変わってしまうことがある
  - IPアドレス指定はルータのように全インタフェースにアドレスがある場合には有効 ⇒ だが、アドレスのないスイッチのポートには適用できない
  - Interface Description指定もしくはInterface Name指定にて作成するのが簡単

おまけ用 監視対象:aa.jp – ネットワーク構成



MRTGディレクトリ構成

- /usr/local/mrtgのディレクトリ構成
  - **/usr/local/mrtg**
    /usr/local/mrtg/bin
    /usr/local/mrtg/lib
    /usr/local/mrtg/conf
    /usr/local/mrtg/data/fw0/
    /usr/local/mrtg/data/branch-fw0/
    /usr/local/mrtg/data/dmz-sw0/
    /usr/local/mrtg/data/intra-sw0/
    /usr/local/mrtg/data/branch-sw0/
- 測定コンフィグファイル構成

測定対象	データディレクトリ	測定分類	測定項目	コンフィグファイル名
fw0	/usr/local/mrtg/data/fw0/	トラフィック測定	bps, pps	fw0.cfg
		エラー測定	Discards, Errors	fw0-err.cfg
branch-fw0	/usr/local/mrtg/data/branch-fw0/	トラフィック測定	bps, pps	branch-fw0.cfg
		エラー測定	Discards, Errors	branch-fw0-err.cfg
dmz-sw0	/usr/local/mrtg/data/dmz-sw0/	トラフィック測定	bps, pps	dmz-sw0.cfg
		エラー測定	Discards, Errors	dmz-sw0-err.cfg
intra-sw0	/usr/local/mrtg/data/intra-sw0/	トラフィック測定	bps, pps	intra-sw0.cfg
		エラー測定	Discards, Errors	intra-sw0-err.cfg
branch-sw0	/usr/local/mrtg/data/branch-sw0/	トラフィック測定	bps, pps	branch-sw0.cfg
		エラー測定	Discards, Errors	branch-sw0-err.cfg

mrtg configの作り方（続き）

- bps項目についてはGigabit Ethernetの測定にて注意が必要
  - ifInOctets/ifOutOctes は32bit正数
  - 5分間隔の測定をした場合、114Mbps付近でカウンターがゼロリセットされてしまう。
  - 対処方法:
    - MRTG ver 2.9以上にてSNMPv2c 64bit counter MIBを使用する
      - **Target[192.168.0.1_gi_0_1]: 2:himitsu@router1:::::2**
    - 測定周期をDefault=5分以下の間隔にて測定を行う
      - **0-59/3 * * * /usr/local/sbin/mrtg ./ix-foo.cfg**
      - とはいってもこの設定では5分/3分=166%。いうことで増分66%(=190Mbps)を超えるとやはりカウンターがゼロリセットされる･･･
    - カウンターリセットしないEnterprise MIBを使用する
      - Cisco Enterprise MIB : **locIfInBitsSec = .1.3.6.1.4.1.9.2.2.1.1.6**
      - Cisco Enterprise MIB : **locIfOutBitsSec = .1.3.6.1.4.1.9.2.2.1.1.8**

MRTG config file: bps/pps: fw0.cfg

```
#####
# fw0 bps/pps config – fw0.cfg
###
WorkDir: /usr/local/mrtg/data/fw0/
IconDir: /mrtg-icons/
Forks: 4

Target[fw0-e1-bps]: ¥ethernet1:himitsu@172.16.0.1
MaxBytes[fw0-e1-bps]: 100000000
Title[fw0-e1-bps]: fw0: ethernet1 bps
PageTop[fw0-e1-bps]: <H1>fw0: ethernet1 bps</H1>
Options[fw0-e1-bps]: gauge,growright

Target[fw0-e1-pps]: ifInUcastPkts¥ethernet1&ifOutUcastPkts¥ethernet1:himitsu@172.16.0.1
MaxBytes[fw0-e1-pps]: 500000
Title[fw0-e1-pps]: fw0: ethernet1 pps
PageTop[fw0-e1-pps]: <H1>fw0: ethernet1 pps</H1>
Options[fw0-e1-pps]: growright

[中略]

Target[fw0-e8-bps]: ¥ethernet8:himitsu@172.16.0.1
MaxBytes[fw0-e8-bps]: 100000000
Title[fw0-e8-bps]: fw0: ethernet8 bps
PageTop[fw0-e8-bps]: <H1>fw0: ethernet8 bps</H1>
Options[fw0-e8-bps]: gauge,growright

Target[fw0-e8-pps]: ifInUcastPkts¥ethernet8&ifOutUcastPkts¥ethernet8:himitsu@172.16.0.1
MaxBytes[fw0-e8-pps]: 500000
Title[fw0-e8-pps]: fw0: ethernet8 pps
PageTop[fw0-e8-pps]: <H1>fw0: ethernet8 pps</H1>
Options[fw0-e8-pps]: growright
#####
# fw0 bps/pps config – fw0.cfg end
###
```


MRTG config file: discards/errors: fw0-err.cfg

```
#####
# fw0 discards/errors config - fw0-err.cfg
###
WorkDir: /usr/local/mrtg/data/fw0/
IconDir: /mrtg-icons/
Forks: 4

Target[fw0-e1-discards]: ifInDiscards¥ethernet1&ifOutDiscards¥ethernet1:himitsu@172.16.0.1
MaxBytes[fw0-e1-discards]: 500000
Title[fw0-e1-discards]: fw0: ethernet1 discards
PageTop[fw0-e1-discards]: <H1>fw0: ethernet1 discards</H1>
Options[fw0-e1-discards]: gauge,growright

Target[fw0-e1-errors]: ifInErrors¥FastEthernet0/1&ifOutErrors¥FastEthernet0/1:himitsu@172.16.0.1
MaxBytes[fw0-e1-errors]: 500000
Title[fw0-e1-errors]: fw0:  ethernet1 errors
PageTop[fw0-e1-errors]: <H1>fw0:  ethernet1 errors</H1>
Options[fw0-e1-errors]: growright

[中略]

Target[fw0-e8-discards]: ifInDiscards¥ethernet8&ifOutDiscards¥ethernet8:himitsu@172.16.0.1
MaxBytes[fw0-e8-discards]: 500000
Title[fw0-e8-discards]: fw0: ethernet8 discard
PageTop[fw0-e8-discards]: <H1>fw0: ethernet8 discards</H1>
Options[fw0-e8-discards]: gauge,growright

Target[fw0-e8-errors]: ifInErrors¥FastEthernet0/12&ifOutErrors¥FastEthernet0/12:himitsu@172.16.0.1
MaxBytes[fw0-e8-errors]: 500000
Title[fw0-e8-errors]: fw0: ethernet8 errors
PageTop[fw0-e8-errors]: <H1>fw0: ethernet8 errors</H1>
Options[fw0-e8-errors]: growrigh
#####
# fw0 discards/errors config - fw0-err.cfg end
###
```

MRTG
config file: bps/pps: dmz-sw0.cfg

```
#####
# dmz-sw0 bps/pps config – dmz-sw0.cfg
###
WorkDir: /usr/local/mrtg/data/dmz-sw0/
IconDir: /mrtg-icons/
Forks: 4

Target[dmzsw0-gi0-1-bps]: ¥GigabitEthernet0/1:himitsu@172.16.250.10:::::2
MaxBytes[dmzsw0-gi0-1-bps]: 1000000000
Title[dmzsw0-gi0-1-bps]: dmz-sw0: GigabitEthernet0/1 bps
PageTop[dmzsw0-gi0-1-bps]: <H1>dmz-sw0: GigabitEthernet0/1 bps</H1>
Options[dmzsw0-gi0-1-bps]: gauge,growright

Target[dmzsw0-gi0-1-pps]: ifInUcastPkts¥GigabitEthernet0/1&ifOutUcastPkts¥Gigabitthernet0/1:himitsu@172.16.250.10
MaxBytes[dmzsw0-gi0-1-pps]: 5000000
Title[dmzsw0-gi0-1-pps]: dmz-sw0: GigabitEthernet0/1 pps
PageTop[dmzsw0-gi0-1-pps]: <H1>dmz-sw0: GigabitEthernet0/1 pps</H1>
Options[dmzsw0-gi0-1-pps]: growright

【中略】

Target[dmzsw0-gi0-12-bps]: ¥GigabitEthernet0/12:himitsu@172.16.250.10:::::2
MaxBytes[dmzsw0-gi0-12-bps]: 1000000000
Title[dmzsw0-gi0-12-bps]: dmz-sw0: GigabitEthernet0/12 bps
PageTop[dmzsw0-gi0-12-bps]: <H1>dmz-sw0: GigabitEthernet0/12 bps</H1>
Options[dmzsw0-gi0-12-bps]: gauge,growright

Target[dmzsw0-gi0-12-pps]: ifInUcastPkts¥GigabitEthernet0/12&ifOutUcastPkts¥GigabitEthernet0/12:himitsu@172.16.250.10
MaxBytes[dmzsw0-gi0-12-pps]: 5000000
Title[dmzsw0-gi0-12-pps]: dmz-sw0: GigabitEthernet0/12 pps
PageTop[dmzsw0-gi0-12-pps]: <H1>dmz-sw0: GigabitEthernet0/12 pps</H1>
Options[dmzsw0-gi0-12-pps]: growright
#####
# dmz-sw0 bps/pps config – dmz-sw0-if.cfg end
###
```


MRTG
config file: discards/errors: dmz-sw0-err.cfg

```
#####
# dmz-sw0 discards/errors config - dmz-sw0-err.cfg
###
WorkDir: /usr/local/mrtg/data/dmz-sw0/
IconDir: /mrtg-icons/
Forks: 4

Target[dmzsw0-gi0-1-discards]: ifInDiscards¥GigabitEthernet0/1&ifOutDiscards¥GigabitEthernet0/1:himitsu@172.16.250.10
MaxBytes[dmzsw0-gi0-1-discards]: 500000
Title[dmzsw0-gi0-1-discards]: dmz-sw0: GigabitEthernet0/1 discards
PageTop[dmzsw0-gi0-1-discards]: <H1>dmz-sw0: GigabitEthernet0/1 discards</H1>
Options[dmzsw0-gi0-1-discards]: gauge,growright

Target[dmzsw0-gi0-1-errors]: ifInErrors¥GigabitEthernet0/1&ifOutErrors¥GigabitEthernet0/1:himitsu@172.16.250.10
MaxBytes[dmzsw0-gi0-1-errors]: 500000
Title[dmzsw0-gi0-1-errors]: dmz-sw0: GigabitEthernet0/1 errors
PageTop[dmzsw0-gi0-1-errors]: <H1>dmz-sw0: GigabitEthernet0/1 errors</H1>
Options[dmzsw0-gi0-1-errors]: growright

【中略】

Target[dmzsw0-gi0-12-discards]: ifInDiscards¥GigabitEthernet0/12&ifOutDiscards¥GigabitEthernet0/12:himitsu@172.16.250.10
MaxBytes[dmzsw0-gi0-12-discards]: 500000
Title[dmzsw0-gi0-12-discards]: dmz-sw0: GigabitEthernet0/12 discards
PageTop[dmzsw0-gi0-12-discards]: <H1>dmz-sw0: GigabitEthernet0/12 discards</H1>
Options[dmzsw0-gi0-12-discards]: gauge,growright

Target[dmzsw0-gi0-12-errors]: ifInErrors¥GigabitEthernet0/12&ifOutErrors¥GigabitEthernet0/12:himitsu@172.16.250.10
MaxBytes[dmzsw0-gi0-12-errors]: 500000
Title[dmzsw0-gi0-12-errors]: dmz-sw0: GigabitEthernet0/12 errors
PageTop[dmzsw0-gi0-12-errors]: <H1>dmz-sw0: GigabitEthernet0/12 errors</H1>
Options[dmzsw0-gi0-12-errors]: growright
#####
# dmz-sw0 discards/errors config - dmz-sw0-err.cfg end
###
```

MRTGトラフィック計測における パフォーマンス調整のTIPS

- 測定項目数
  - 以下のようにインタフェース数を仮定した場合：全測定項目は 232項目
    - fw0(8FE)
    - branch-fw0(2FE)
    - dmz-sw0(12GbE)
    - intra-sw0(24GbE)
    - branch-sw0(12GbE)

機器名称	インタフェース本数		各IF毎の測定項目数	測定項目数
	FE / E	GbE		
fw0	8	0	4	32
branch-fw0	2	0	4	8
dmz-sw0	0	12	4	48
intra-sw0	0	24	4	96
branch-sw0	0	12	4	48
合計				232

  - すべての計測を同時に実施した場合、[illegible]
- パフォーマンス改善のための対処：
  - Forks: 指定で並列Query
    - 測定対象が無応答状態となったときには、無応答Queryだけ保留され、他の計測に影響しないため動作の保険になる。
    - Forks: 4
  - 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

crontab – bb.xy.jp

```
####
# crontab mrtg@bb.xy.jp
##
# fw01 mrtg
0-59/5 * * * * /usr/local/mrtg/bin/mrtg /usr/local/mrtg/conf/fw0.cfg > /dev/null 2>&1
2-59/5 * * * * /usr/local/mrtg/bin/mrtg /usr/local/mrtg/conf/fw0-err.cfg > /dev/null 2>&1

# fw01 mrtg
1-59/5 * * * * /usr/local/mrtg/bin/mrtg /usr/local/mrtg/conf/branch-fw0.cfg > /dev/null 2>&1
3-59/5 * * * * /usr/local/mrtg/bin/mrtg /usr/local/mrtg/conf/branch-fw0-err.cfg > /dev/null 2>&1

# dmz-sw0 mrtg
2-59/5 * * * * /usr/local/mrtg/bin/mrtg /usr/local/mrtg/conf/dmz-sw0.cfg > /dev/null 2>&1
4-59/5 * * * * /usr/local/mrtg/bin/mrtg /usr/local/mrtg/conf/dmz-sw0-err.cfg > /dev/null 2>&1

# intra-sw0 mrtg
0-59/5 * * * * /usr/local/mrtg/bin/mrtg /usr/local/mrtg/conf/intra-sw0.cfg > /dev/null 2>&1
2-59/5 * * * * /usr/local/mrtg/bin/mrtg /usr/local/mrtg/conf/intra-sw0-err.cfg > /dev/null 2>&1

# branch-sw0 mrtg
1-59/5 * * * * /usr/local/mrtg/bin/mrtg /usr/local/mrtg/conf/branch-sw0.cfg > /dev/null 2>&1
3-59/5 * * * * /usr/local/mrtg/bin/mrtg /usr/local/mrtg/conf/branch-sw0-err.cfg > /dev/null 2>&1
####
# crontab mrtg@bb.xy.jp end
##
```

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注意
  - 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
- 深刻なメッセージ
  - Config Error
  - No Response
  - Lockfile found

TIPS – MRTG編3

- 非常に深刻なメッセージ

```
From: mrtg@bb.xy.jp (Cron Daemon)
To: alert@xy.jp.jp
Date: Fri, 13 Oct 2003 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_l) aged 303 seconds is hanging around.
If you are sure that no other mrtg is running you can remove the lockfile
```


追加資料3：
MRTGのTargetの指定方法

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.xy.jp`
    - `Target[gw1-err-3]: ifInErrors.3&ifOutErrors.3:himitsu@gw1.xy.jp`
    - `Target[gw1-if-1]: -/10.0.0.101:himitsu@gw1.xy.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

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

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.xy.jp`**
  - gw1.xy.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.xy.jp`**
  - 例1の**`In/Out`**を逆にしてデータ収集する

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.xy.jp`**
  - gw1.xy.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.xy.jp`**
  - 上の例のOID指定

MRTG – ifIndex指定の設定例

```
#------------------------------------------------------------------#
Target[ETHERNET11.0-BPS]: 8:himitsu@10.1.0.7
MaxBytes[ETHERNET11.0-BPS]: 155000000
Title[ETHERNET11.0-BPS]: router7: ETHERNET11.0 BPS
PageTop[ETHERNET11.0-BPS]: <H1>router7: ETHERNET11.0</H1>
Options[ETHERNET11.0-BPS]: bits,growright

#------------------------------------------------------------------#
Target[ETHERNET11.0-PPS]: ifInUcastPkts.8&ifOutUcastPkts.8:himitsu@10.1.0.7
MaxBytes[ETHERNET11.0-PPS]: 155000000
Title[ETHERNET11.0-PPS]: router7: ETHERNET11.0 PPS
PageTop[ETHERNET11.0-PPS]: <H1>router7: ETHERNET11.0 PPS</H1>
Options[ETHERNET11.0-PPS]: growright

#------------------------------------------------------------------#
```

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

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.xy.jp
  - gw1.xy.jpに収容されている**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.xy.jp
  - 例**5**の**In/Out**を逆にしてデータ収集する

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.xy.jp**
  - **gw1.xy.jp**に収容されている**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.xy.jp**
  - 例7の**OID**パターン

MRTG – Interface Address指定の設定例

```
#------------------------------------------------------------------#
Target[ETHERNET11.0-BPS]: /192.168.0.1:himitsu@10.1.0.2
MaxBytes[ETHERNET11.0-BPS]: 155000000
Title[ETHERNET11.0-BPS]: router2: ETHERNET11.0 BPS
PageTop[ETHERNET11.0-BPS]: <H1>router2: ETHERNET11.0</H1>
Options[ETHERNET11.0-BPS]: bits,growright

#------------------------------------------------------------------#
Target[ETHERNET11.0-PPS]:
ifInUcastPkts/192.168.0.1&ifOutUcastPkts/192.168.0.1:himitsu@10.1.0.2
MaxBytes[ETHERNET11.0-PPS]: 155000000
Title[ETHERNET11.0-PPS]: router2: ETHERNET11.0 PPS
PageTop[ETHERNET11.0-PPS]: <H1>router2: ETHERNET11.0 PPS</H1>
Options[ETHERNET11.0-PPS]: growright

#------------------------------------------------------------------#
```

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。
  - これ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.xy.jp**
    Target[sw-2-11]: -#2/11:himitsu@sw1.xy.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.x
    y.jp
    Target[sw-3-7]:
    ifInErrors#3/7&ifOutErrors#3/7:himitsu@sw1.xy.jp

MRTG – Interface Name指定の設定例

```
#------------------------------------------------------------------#
Target[gi1.1-bps]: #1/1:himitsu@10.1.0.2
MaxBytes[gi1.1-bps]: 1937500000
Title[gi1.1-bps]: switch1:  1/1 bps
PageTop[gi1.1-bps]: switch1:  1/1 bps
Options[gi1.1-bps]: bits,growright

#------------------------------------------------------------------#
Target[gi1.1-pps]: ifInUcastPkts#1/1&ifOutUcastPkts#1/1:himitsu@10.1.0.2
MaxBytes[gi1.1-pps]: 500000
Title[gi1.1-pps]: switch1:  1/1 pps
PageTop[gi1.1-pps]: switch1:  1/1 pps
Options[gi1.1-pps]: growright

#------------------------------------------------------------------#
```

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.xy.jp**
    Target[sw-2-11]: -¥to_web1:himitsu@sw1.xy.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.xy.jp
    Target[sw-3-7]:
    ifInErrors¥to_web1&ifOutErrors¥to_web1:himitsu@sw1.xy.jp

MRTG – Interface Description指定の設定例

```
#--------------------------------------------------------------------#
Target[gi1.1-bps]: ¥GigabitEthernet1/1:himitsu@10.1.0.1
MaxBytes[gi1.1-bps]: 1000000000
Title[gi1.1-bps]: router16:  GigabitEthernet1/1 bps
PageTop[gi1.1-bps]: <h1>router16:  GigabitEthernet1/1 bps</h1>
Options[gi1.1-bps]: bits,growright

#--------------------------------------------------------------------#
Target[gi1.1-pps]:
ifInUcastPkts¥GigabitEthernet1/1&ifOutUcastPkts¥GigabitEthernet1/1:himitsu@10.1.0.1
MaxBytes[gi1.1-pps]: 500000
Title[gi1.1-pps]: router16:  GigabitEthernet1/1 pps
PageTop[gi1.1-pps]: <h1>router16:  GigabitEthernet1/1 pps</h1>
Options[gi1.1-pps]: growright

#--------------------------------------------------------------------#
```

MRTG - 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

MRTGによる品質計測

- 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.xy.jp**

```
PING ftp.xy.jp (192.168.101.238): 56 data bytes
.
--- ftp.xy.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.**
      FeeBSD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ることから取り扱い注意

MRTGによる品質計測 - check_loss.sh

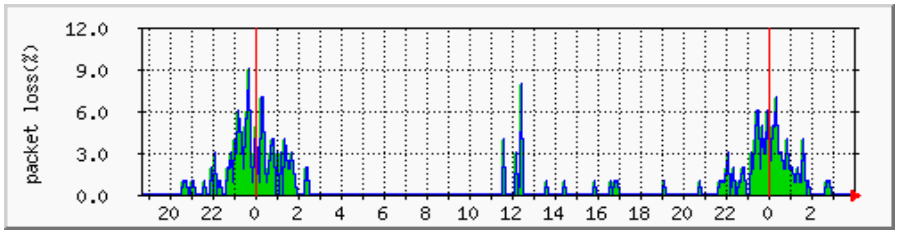
- pingの出力結果からpacket lossのデータを抽出
  - 100 packets transmitted, 95 packets received, 5% packet loss

```
# 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.xy.jp
5
5
0
/usr/local/bin/check_loss.sh ftp.xy.jp
#
```


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.xy.jp`
Title[pingloss-ftp]: ftp.xy.jp - pingloss
MaxBytes[pingloss-ftp]: 100
PageTop[pingloss-ftp]: <H1> ftp.xy.jp - pingloss </H1>
YLegend[pingloss-ftp]: packet loss(%)
ShortLegend[pingloss-ftp]: %
LegendI[pingloss-ftp]:  loss:
LegendO[pingloss-ftp]:  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, nopercent
#
```

MRTGによる品質計測 - 結果



参考資料:文献/URL

参考: 文献1

- “Big Brotherで快適ネットワークシステム管理”
  - Software Design 2003/9-2004/11
  - 矢萩茂樹@イーアクセス / 越川康則
    - 2003/10月号: 第 1回 BigBrother概説
    - 2003/11月号: 第 2回 BigBrotherを設定する
    - 2003/12月号: 第 3回 BigBrotherサーバの詳しい設定
    - 2004/01月号: 第 4回 bbclientと拡張スクリプト
    - 2004/02月号: 第 5回 BBの外部拡張 ①
    - 2004/03月号: 第 6回 BBでできるセキュリティ監視 (BBの外部拡張 ②)
    - 2004/04月号: 第 7回 最新バージョン1.9eの導入/バージョンアップ
    - 2004/05月号: 第 8回 独自エクステンションを導入する
    - 2004/06月号: 第 9回 BBのメンテナンス
    - 2004/07月号: 第10回 BBシステムのチューニング①
    - 2004/08月号: 第11回 複数BBサーバによる分散処理 (BBシステムのチューニング②)
    - 2004/09月号: 第12回 BBによるDBの監視
    - 2004/10月号: 第13回 BBによるSNMP監視①
    - 2004/11月号: 第14回 BBによるSNMP監視②
    - 2004/12月号: 第15回 BBによるSNMP監視③ そして 次のBB : bbgen

参考: 文献2

- ”丸ごとわかる「ネットワーク監視」の秘訣”
  - NetworkWorld 2004/10月号
  - 矢萩茂樹@イーアクセス / 河本卓司
- ”フリーソフトで始めるネットワーク監視”
  - 日経システム構築 2004/8-2005/1
  - 矢萩茂樹@イーアクセス

参考：Open Source / Free software link

- OSTG (Open Source Technology Group, 旧OSDN)
  - http://www.ostg.com/
- OSDN.jp
  - http://osdn.jp/
- SOURCE FORGE
  - http://sourceforge.net/
- SOURCE FORGE JAPAN
  - http://sourceforge.jp/
- Fresh Meat – Free Software Index
  - http://www.freshmeat.net/
- Solaris Freeware Project
  - http://sunsite.sut.ac.jp/sun/solbin/

ツールURL集1

- AWARE
  - http://www.elegant-software.com/software/aware/
- Big Brother
  - http://bb4.org/
  - Extensions Archive: http://www.deadcat.net/
- Big Sister
  - http://bigsister.sourceforge.net/
- Expect
  - http://expect.nist.gov/
- fping
  - http://www.fping.com/
- Ganglia
  - http://ganglia.sourceforge.net/
- hping
  - http://www.hping.org/
- IPTraf
  - http://cebu.mozcom.com/riker/iptraf/index.html

ツールURL集2

- Lire
  - http://www.logreport.org/
- LogSentry (Senty Tools)
  - http://sourceforge.net/projects/sentrytools
- MRTG
  - http://ee-staff.ethz.ch/~oetiker/webtools/mrtg/
- mon
  - http://www.kernel.org/software/mon
- monit
  - http://www.tildeslash.com/monit/
- moodss
  - http://moodss.sourceforge.net/
- Nagios (NetSaint)
  - http://www.nagios.org/
  - http://www.netsaint.org/
- NeTraMet
  - http://www2.auckland.ac.nz/net/NeTraMet/

ツールURL集3

- MTR
  - http://www.bitwizard.nl/mtr/
- NISCA
  - http://nisca.sourceforge.net/
- Net-SNMP (UCD-SNMP)
  - http://www.net-snmp.org/
- ngrep – Network grep
  - http://ngrep.sourceforge.net/
- nocol/multiping
  - http://www.netplex-tech.com/software/nocol
- nPULSE
  - http://www.horsburgh.com/h_npulse.html
- ntop
  - http://www.ntop.org/

ツールURL集4

- RRDTool
  - http://ee-staff.ethz.ch/~oetiker/webtools/rrdtool/
  - Frontend - Cacti
    - http://www.cacti.net/
  - Frontend - CRICKET
    - http://cricket.sourceforge.net/
  - Frontend - NRG
    - http://nrg.hep.wisc.edu/
  - Frontend - ORCA
    - http://www.orcaware.com/orca/
  - Frontend – RRDBrowse
    - http://www.rrdbrowse.org/
  - Frontend – SmokePing
    - http://people.ee.ethz.ch/~oetiker/webtools/smokeping/

ツールURL集5

- Scotty
  - http://wwwhome.cs.utwente.nl/~schoenw/scotty/
- shepherd
  - http://atrey.karlin.mff.cuni.cz/~clock/twibright/shepherd/
- sing
  - http://sourceforge.net/projects/sing
- snort
  - http://www.snort.org/
- ssh
  - http://www.ssh.com/
- statscout
  - http://www.statscout.com
- SWATCH
  - http://swatch.sourceforge.net/

ツールURL集6

- **syslog-ng**
  - **http://www.balabit.com/products/syslog_ng/**
- **php-syslog-ng**
  - **http://www.vermeer.org/syslog/**
- **SysOrb**
  - **http://www.evalesco.com**
- **visualroute**
  - **http://www.visualroute.com**
- **Zabbix**
  - **http://zabbix.sourceforge.net/**

参考：URL集1

- みっきーのネットワーク研究所
  - http://www.hawkeye.ac/micky/
- いちばん近道なLinuxマスター術
  - http://www.zdnet.co.jp/help/howto/linux/0007master/
  - 「第4回：システムログの読み方を理解しよう」
    - http://www.zdnet.co.jp/help/howto/linux/0007master/04/
  - 「第6回：SNMPによるネットワークモニタリング」
    - http://www.zdnet.co.jp/help/howto/linux/0007master/06/
- **SIMPLE WEB**
  - **http://www.simpleweb.org/**

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/
    - cflowd ,RRD ･･･etc