オープンソースを利用したNMS構築

2002/12/17

イー・アクセス株式会社
矢萩茂樹

index

オープンソースの定義

- オープンソースソフトウェアプログラムとは、
  - どんな用途にも使える、
  - 誰でも修正できる、
  - オリジナルも修正版も自由に再配布できる、
- というライセンスを持つプログラムである。

- これは opensource.orgの規定規定する The Open Source Definitionにより規定される。

The Open Source Definition Version 1.9

(http://www.opensource.org/docs/definition_plain.html)

- Introduction
  - Open source doesn't just mean access to the source code. The distribution terms of open-source software must comply with the following criteria:

1. Free Redistribution
2. Source Code
3. Derived Works
4. Integrity of The Author's Source Code
5. No Discrimination Against Persons or Groups
6. No Discrimination Against Fields of Endeavor
7. Distribution of License
8. License Must Not Be Specific to a Product
9. The License Must Not Restrict Other Software
10. No provision of the license may be predicated on any individual technology or style of interface.

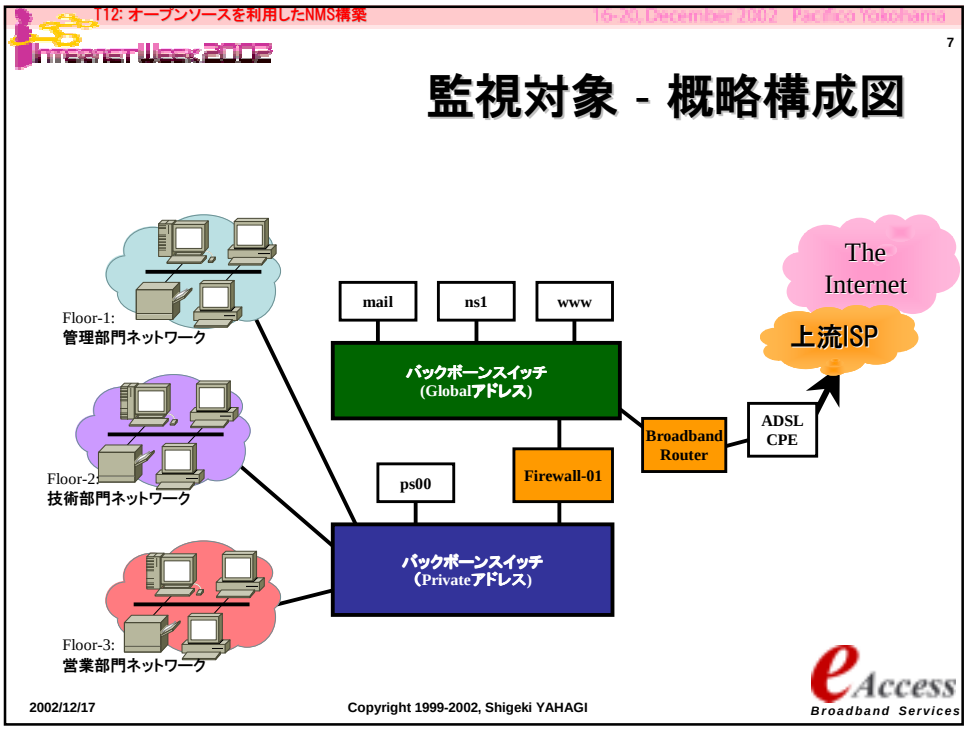
- Origins: Bruce Perens wrote the first draft of this document as "The Debian Free Software Guidelines", and refined it using the comments of the Debian developers in a month-long e-mail conference in June, 1997. He removed the Debian-specific references from the document to create the "Open Source Definition."
- Copyright c 2002 by the Open Source Initiative

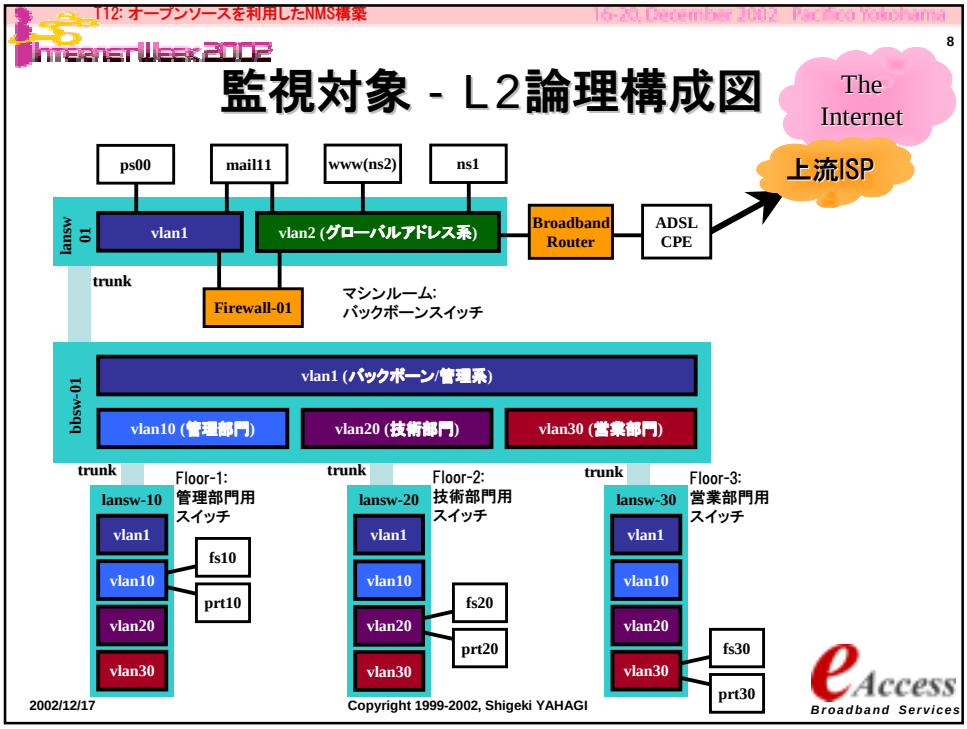
本セッションの目的

- 本チュートリアルでは、エンタープライズネットワークを仮定し、そのためのオープンソースソフトウェアベース監視システムを構築するというシナリオシュミレーションをする中で、監視システム構築にかかわる様々な事柄を検討する
- 紹介するのは以下のソフト
  - Big Brother + extensions
    - BBについてはThe Open Source Definitionからはずれると思われるが、自由に使えるという意味で取り上げる。
  - Net-SNMP
  - MRTG

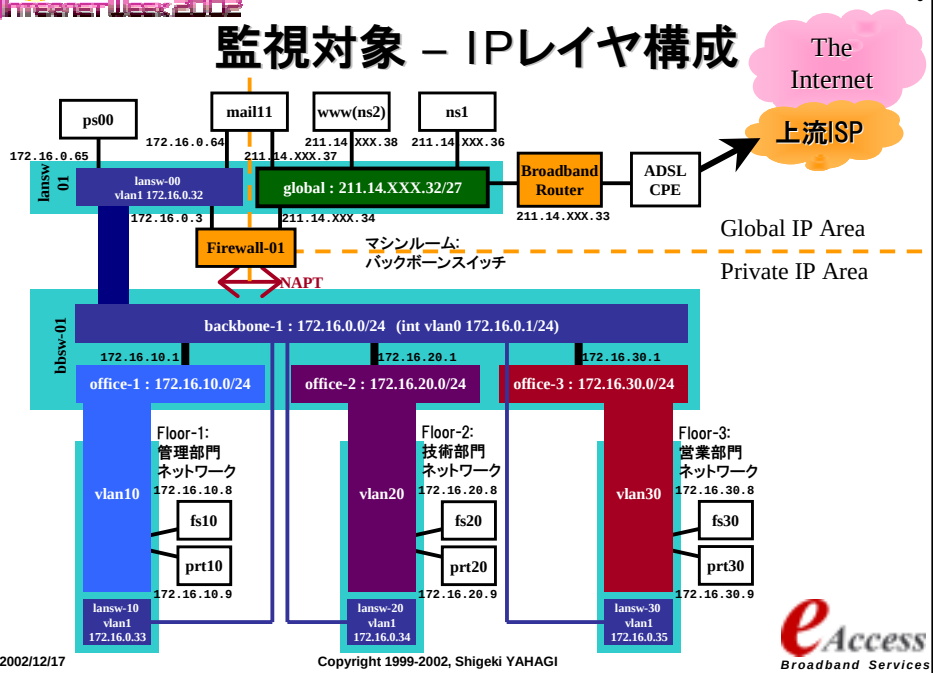
監視対象 - 概要1

- 監視ネットワーク概要
  - 中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。
  - ISPとの接続はADSLを使用。ADSLモデムはブリッジモードとして使用。ブロードバンドルータからPPPoEにてリンクレイヤ(L2)接続を行う
  - マルチホームは行っておらず、上流ISPよりSub Allocation Block(/27)の割当を受ける。
  - Firewallを導入しており、社内からInternetへの接続はすべてFirewall経由となる。
  - Firewall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。
- 詳細説明(対象解析)は後章で実施します。


T12: オープンソースを利用したNMS構築
InternetWeek2002
16-20 December 2002 Pacifico Yokohama
7
監視対象 - 概略構成図
Floor-1:
管理部門ネットワーク
Floor-2:
技術部門ネットワーク
Floor-3:
営業部門ネットワーク
mail
ns1
www
バックボーンスイッチ
(Globalアドレス)
ps00
Firewall-01
バックボーンスイッチ
(Privateアドレス)
Broadband
Router
ADSL
CPE
The
Internet
上流ISP
2002/12/17
Copyright 1999-2002, Shigeki YAHAGI
eAccess
Broadband Services


T12: オープンソースを利用したNMS構築
InternetWeek2002
16-20 December 2002 Pacifico Yokohama
8
監視対象 - L2論理構成図
The
Internet
上流ISP
ps00
mail11
www(ns2)
ns1
lansw
01
vlan1
vlan2 (グローバルアドレス系)
Broadband
Router
ADSL
CPE
trunk
Firewall-01
マシンルーム:
バックボーンスイッチ
bbsw-01
vlan1 (バックボーン/管理系)
vlan10 (管理部門)
vlan20 (技術部門)
vlan30 (営業部門)
trunk
trunk
trunk
Floor-1:
管理部門用
スイッチ
Floor-2:
技術部門用
スイッチ
Floor-3:
営業部門用
スイッチ
lansw-10
lansw-20
lansw-30
vlan1
vlan10
vlan20
vlan30
fs10
prt10
fs20
prt20
fs30
prt30
2002/12/17
Copyright 1999-2002, Shigeki YAHAGI
eAccess
Broadband Services

監視対象 – IPレイヤ構成



index

要件定義 – 概要1

- 監視機能
  - システム稼動を把握するための必要十分な監視を行うこと
  - ネットワーク全体の稼動状況を簡潔に/速やかに把握可能とするインタフェースを備えること
- 通知機能
  - 障害検知にて、適切な通知が適切なエスカレーション箇所になされること
  - 障害イベントに応じて、適切な通知先の自動選択し、通知がなされること
- 障害履歴管理
  - システム稼動状況の履歴追跡機能を備えること

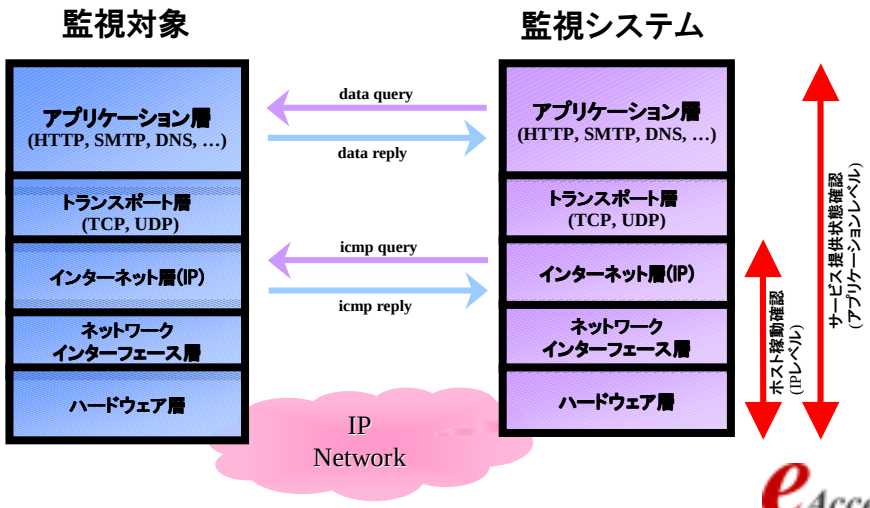
要件定義 – 概要2

- 他システムへの影響
  - 監視処理を行うことによりネットワークおよびその提供サービスに対して影響を与えないこと。
- セキュリティー
  - 監視情報について許可されたユーザにのみ情報を提供し、意図しないアクセスに対して無闇に情報を流さないような機構を持つこと
  - 外部からの稼動妨害行為に対して適切な防御機構を持ち、妨害によりシステム稼動に影響を受けることがないこと
- システムの稼動安定
  - 十分な稼動安定度をもち、誤報／検知ミスなどができる限り発生しないこと

要件定義 - 監視機能1

- 監視機能1
  - ホスト稼動確認
    - 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
    - サービスが問題なく稼動していることを確認する
  - プロセス監視
    - プロセスが正常に起動していることを確認する。
    - また、不必要なプロセスが起動していないことを確認する
  - リソース監視
    - 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

要件定義 - 監視機能2



要件定義 - 監視機能3

- 監視機能2
  - 異常メッセージ検知
    - システム稼動ログを集中管理する
    - syslogによるリモートロギング機能
    - SNMP trap ロギング機能
      - システムリブート検知
      - LINK UP/DOWN検知

要件定義 - 監視機能3

- 監視情報表示
  - 集中監視・一斉通知
  - 監視画面は各自の手元で実施できること
    - 通知後の確認はWEB画面でリモート監視・リモート確認
- 外部ネットワークからの状況確認要件
  - 自宅からでもリモート対応可能としたいが、本要件はセキュリティー要件と相反する。
  - 監視システム側での対応ではなく、VPNアクセスなどネットワーク側での対応とする。

要件定義 - 通知機能

- 障害通知
  - 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
    - メールによる障害発生通知
    - 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
  - 通知には以下の情報を含める
    - 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
      - 障害情報のみがまとめられたサマリー画面
  - 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。
    - 適切な担当者への迅速な通知
    - 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

要件定義 - 障害履歴管理

- 障害履歴管理
  - 監視サーバにて、発生した障害の履歴管理機能を行う
  - 障害発生／復旧時間を記録し、過去に遡って障害履歴を追跡可能とする
  - 障害履歴を日間・週間・月間・年間の各スパンにてチェック可能とすることで、障害の発生頻度／発生傾向の追跡解析をサポートする機能が欲しい。
    - MRTGでのDaily/Weekly/Monthly/Yearly表示のような解析画面

要件定義 - トラフィック監視

- トラフィック監視
  - 通信ノードにおいて以下のトラフィックデータを定期観測し、トラフィックグラフを作成／管理する。
    - 通信トラフィック監視
      - bps, pps
    - 品質関連トラフィック監視
      - packet discards, interface errors
    - システムパフォーマンス関連データ監視
      - CPU Load
    - ノード間品質監視トラフィック
      - Packet Loss, Round Trip Time
  - トラフィック監視における問題検出はパターン分析がロジック上難しいことから、今回のシステムでは取り扱わず、将来案件とします。

要件定義 - セキュリティー

- セキュリティー対策要件（再掲）
  - 監視情報について許可されたユーザにのみ情報を提供し、意図しないアクセスに対して無闇に情報を流さないような機構を持つこと
  - 外部からの稼動妨害行為に対して適切な防御機構を持ち、妨害によりシステム稼動に影響を受けることがないこと

- セキュリティー対策：実装方式
  - 監視システムの機能分担／ネットワーク配置構成などを適正化することにより、セキュリティーを確保する
    - ログサーバーなどについて検討が必要

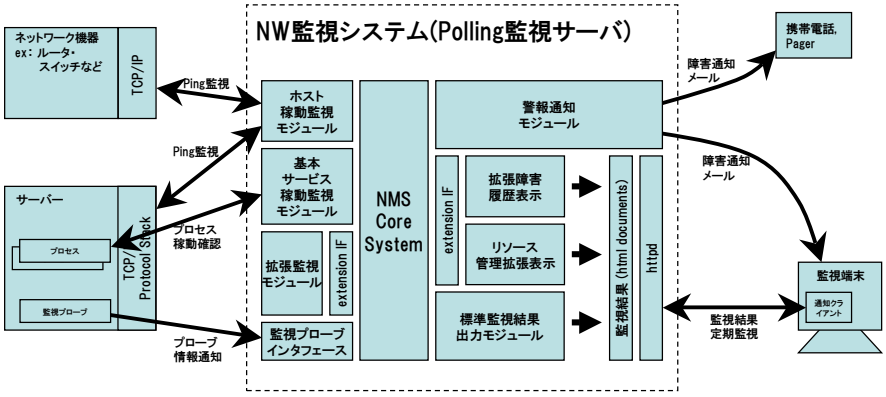
要件定義 - オープンソースでどこまでできるか

- 本チュートリアルでは、エンタープライズネットワークを仮想設定し、それをオープンソースソフトウェアベースの監視システムにて構築することを目的とする
- これらの要件をみたすNMSを、以下のオープンソースソフトにて構築する
  - Big Brother + extensions
    - larrd + RRDTools
    - bb-hist.pl
    - BBtray
  - snmptrapd(Net-SNMP)
  - MRTG

用件定義 – 構築方針

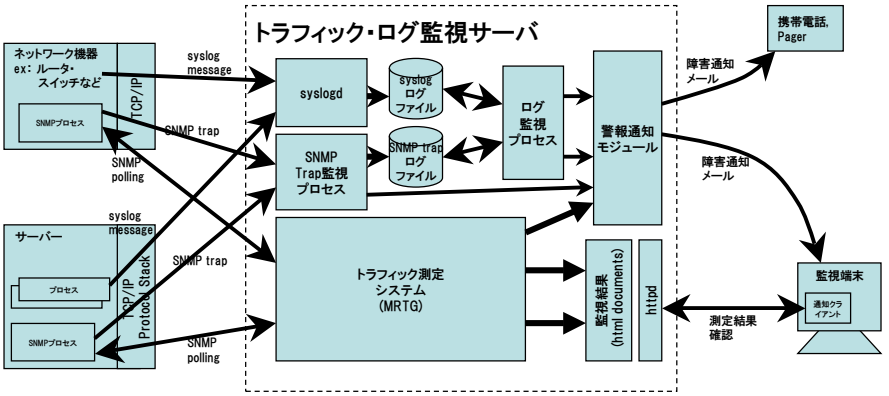
- セキュリティー・機能・能力を検討し、サーバーを二つに機能分割する
  - Polling監視サーバー
    - ホスト稼動確認・サービス提供状態確認・プロセス監視・リソース監視などの主要監視業務を分担する
  - トラフィック・ログサーバー
    - トラフィック測定・syslog/SNMP trapなどのログ管理を分担する

監視システムのモデル - Polling監視サーバ



eAccess Broadband Services

監視システムのモデル - トラフィック・ログ監視サーバ



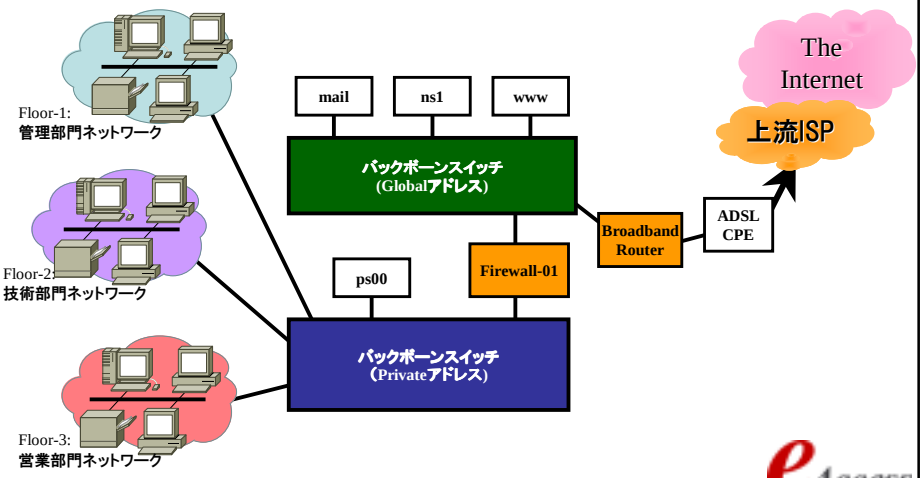
eAccess Broadband Services

Index

監視対象分析 - 概要1

- 監視ネットワーク概要
  - 中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。
  - ISPとの接続はADSLを使用。ADSLモデムはブリッジモードとして使用。ブロードバンドルータからPPPoEにてリンクレイヤ接続を行う
  - マルチホームは行っておらず、上流ISPよりSub Allocation Block(/27)の割当を受ける。
  - Firewallを導入しており、社内からInternetへの接続はすべてFirewall経由となる。
  - Firewall配下のネットワークはPrivateアドレスを使用し、Firewallにて NAPTしている。

監視対象 - 概略構成図



監視対象分析 - 概要2

- 監視ネットワーク概要 - ロケーション
  - 会社は一つのテナントビルにおさまっている。
  - 組織は管理　技術　営業の3部門に別れており、それぞれ別のフロアに分散している。
  - それぞれの部門用にファイルサーバを配置している。
  - プリンタサーバは全社共通となっている。

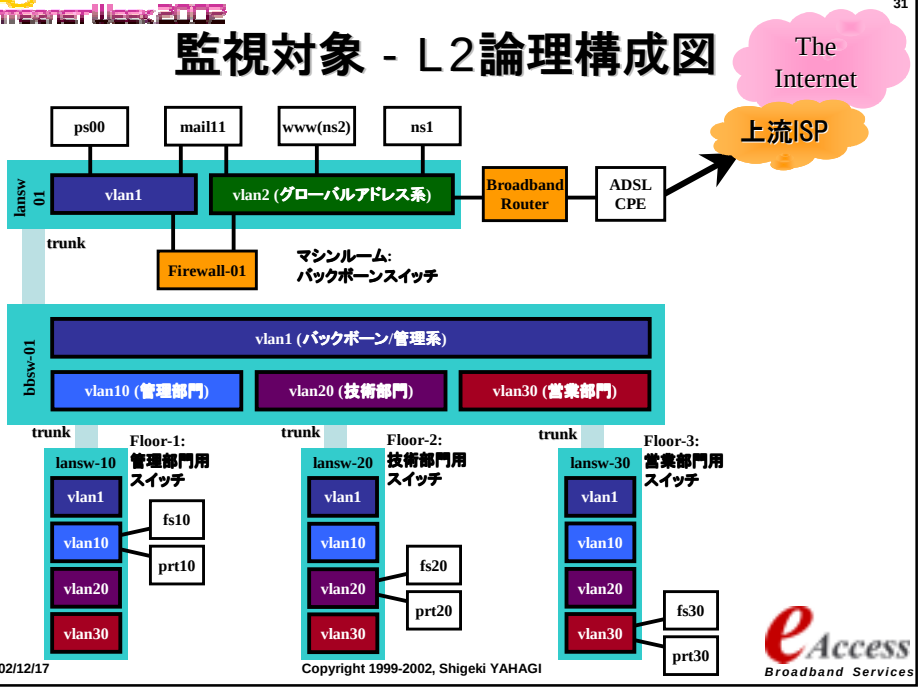
監視対象分析 - 提供サービス1

- ネットワーク提供サービス
  - 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も社外向けには開いていない
    - inetdは使用しない
    - 社外へはポートはあけておらず、IPsec 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: ns1.hogehoge.com
    - Secondary: ns2(www).hogehoge.com
  - メール設定
    - Primary: mail1.hogehoge.com
    - Secondary: ns1.hogehoge.com
  - 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

監視対象 - L2論理構成図



監視対象分析 - L2論理構成1

- L2論理構成1
  - Layer-3 8-Port GbEスイッチであるbbsw01を中心にネットワークを構築。
  - 各部門毎にVLANを独立させている。
  - 各部門には張り出し用のL2エッジスイッチ(lanswXX: 2GbE, 48FE)を設置。この装置を部門ネットワークの分解点とする。
  - バックボーンスイッチとエッジスイッチの間はL2 trunk接続となっている。
  - GlobalセグメントおよびNOC内監視サーバ類は管理系エッジスイッチであるlunsw01を経由して接続する
  - エッジスイッチのVLAN識別はポートごとの固定とする(ポートVLAN使用)
  - IPルーティングはバックボーンスイッチ(bbsw01)にて行う

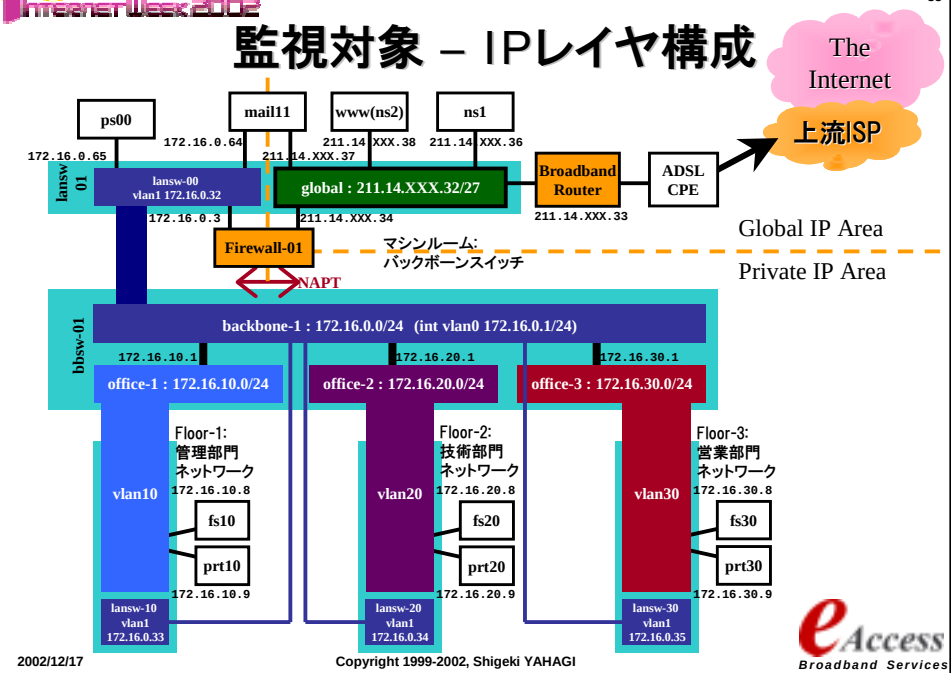
監視対象分析 – vlan/address割当

割付アドレスブロック	VLAN-ID	用途
211.14.XXX.32/27	vlan2	グローバルセグメント
172.16.0.0/24	vlan1	バックボーン1セグメント/ 管理用セグメント
172.16.10.0/24	vlan10	オフィスセグメント1(管理部門用)
172.16.20.0/24	vlan20	オフィスセグメント2(技術部門用)
172.16.30.0.24	vlan30	オフィスセグメント3(営業部門用)
172.31.0.0/24	---	ループバックセグメント

監視対象分析 - L2論理構成2

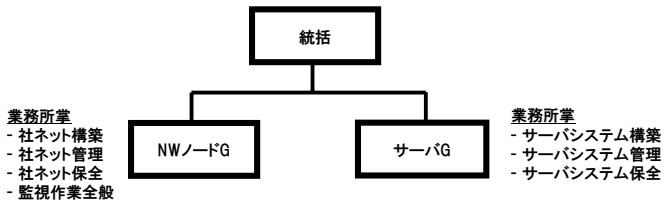
- L2論理構成2
  - 管理系としてVLAN1(default)を使用し、エッジスイッチの管理インタフェースはこのVLANに所属させる
  - 各部門セグメントには最低限 部門用ファイルサーバとネットワークプリンタが接続される
  - The Internetへのサービスは全てDMZ(非武装地帯)に置かれたサーバからのみ行われる

監視対象 – IPレイヤ構成



監視対象分析 – 監視体制とエスカレーション

- 全システムの管理は技術部門 情報システム部で行う。
- 管理はサーバGとNWノードGの2グループ体制となっており、監視はNWノードGにて行っている。
- 24時間常駐はしておらず、通常勤務時間外についてはシステムからの自動警報通知にてリモート対応とする。
- 重要ノードの障害については担当に通知するとともに統括責任者にもエスカレーション通知がなされる

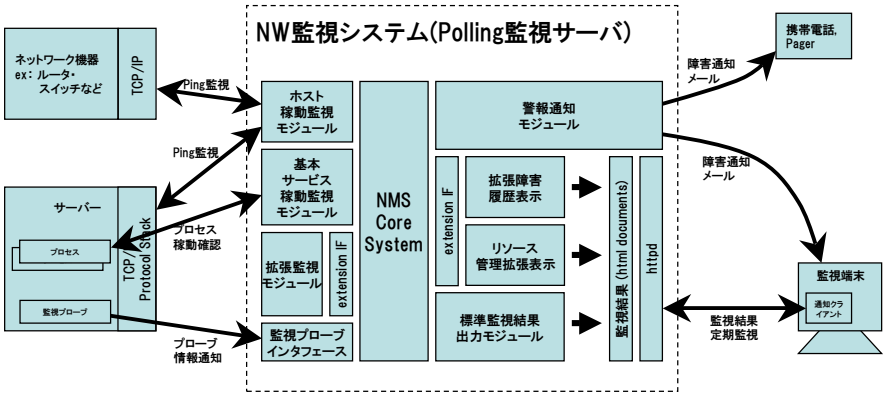


業務所掌
- 社ネット構築
- 社ネット管理
- 社ネット保全
- 監視作業全般

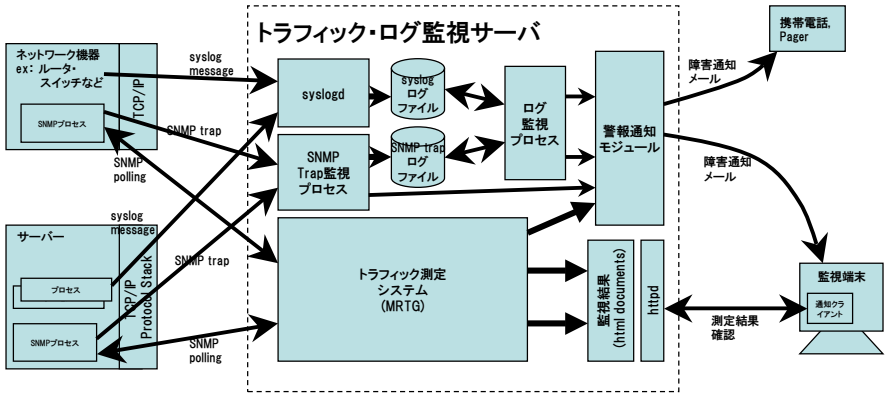
業務所掌
- サーバシステム構築
- サーバシステム管理
- サーバシステム保全

index

監視システムのモデル - Polling監視サーバ



監視システムのモデル - トラフィック・ログ監視サーバ



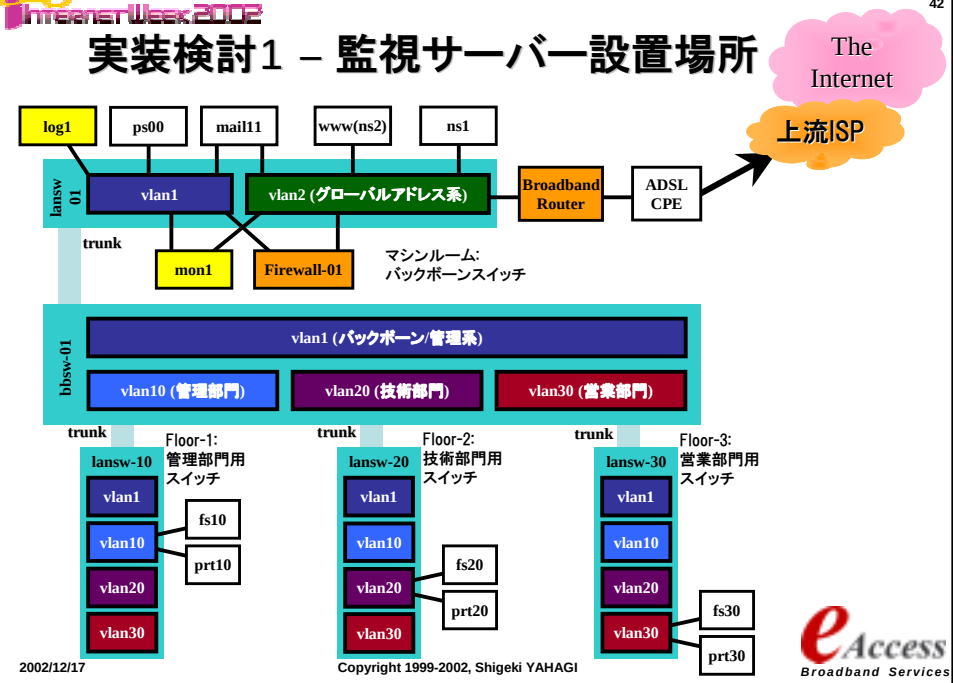
実装検討1 – 監視サーバの設置ポイント

- Polling監視サーバー(mon1)
  - ホスト稼動確認・サービス提供状態確認・プロセス監視・リソース監視などの主要監視業務を分担する
  - 監視項目としてIPアドレスの生存性確認があり、Private/Globalそれぞれの確認が必要となる。
  - Firewall・スイッチの障害でも、その他のノードの監視が妨げられない場所に設置する。
  - 設置場所:
    - Global : lansw01 vlan2(global vlan) IP=211.14.XXX.39/27
    - Private : lansw01 vlan1(backbone1 vlan) IP=172.16.0.66/24

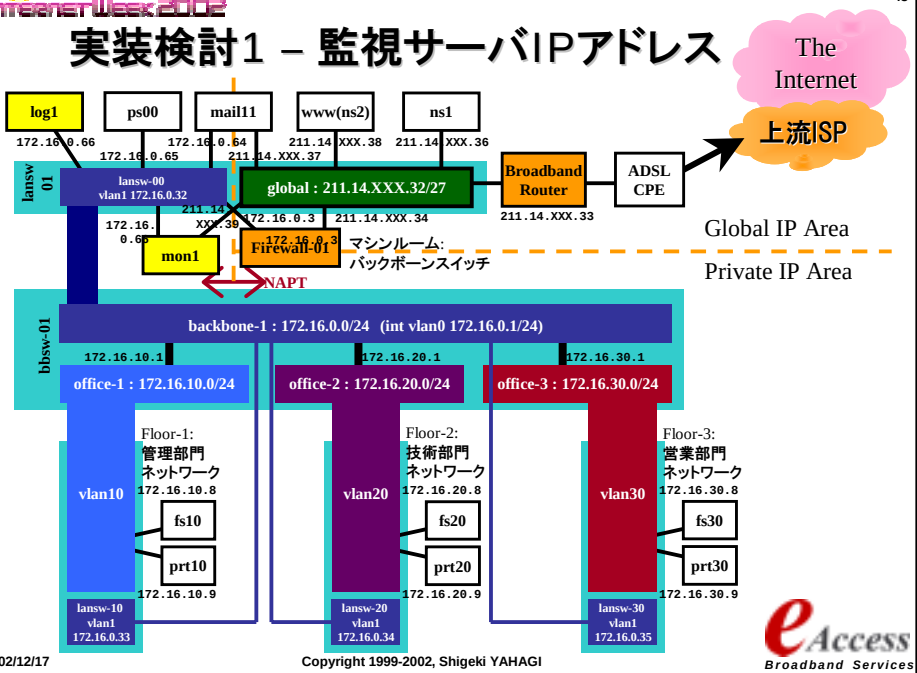
実装検討1 – 監視サーバの設置ポイント

- トラフィック・ログサーバー(log1)
  - トラフィック測定・syslog/SNMP trapなどのログ管理を分担する
  - 処理対象は社内ネットワークの装置に限られており、外部に情報を発信する必要性がないことから、Privateブロックに設置する
    - 逆に必要性がないのであるならば、Global Segmentに設置すべきでない。Global Segmentに設置した場合、syslogd/snmptrapdに対してDoSアタックされる可能性がある。
    - Private Segmentにおくことで、論理構成的にこれらの妨害から防御可能となる
  - 設置場所:
    - Private : lansw01 vlan1(backbone1 vlan) IP=172.16.0.67/24

実装検討1 – 監視サーバー設置場所



実装検討1 – 監視サーバIPアドレス



eAccess Broadband Services

実装検討1 - 時間同期

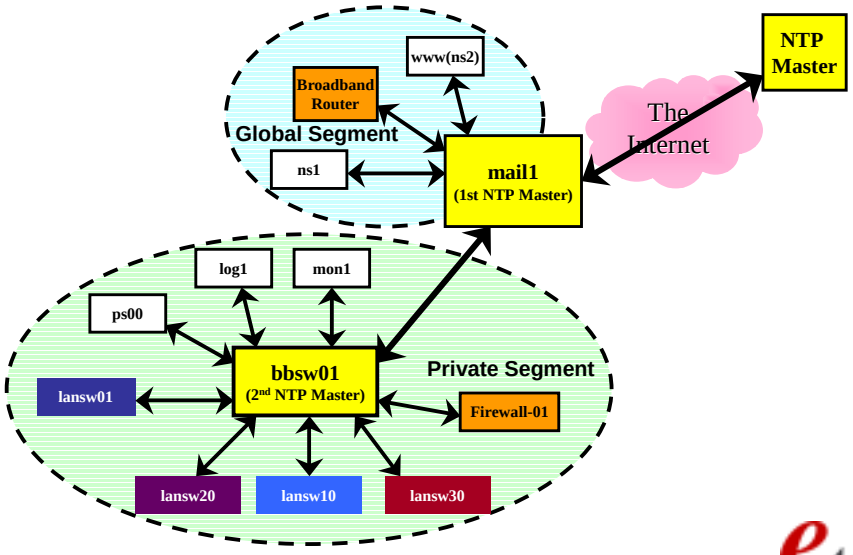
- 時間同期環境整備
  - 絶対基準のひとつは当然、時間
    - 障害原因追跡の絶対基準
  - NTPでサーバーと監視機器の時間を同期させる
    - Timezoneの同期も必要。JST-9 or UTC
  - hogehoge.com導入のFWはNTPクライアント機能しかないため、独自にNTP環境が必要。
  - Global/Privateの両方に接続しているノードがNTPサーバーになっていることが望ましく、Globalに接続されていることが条件のサーバで稼動させる。

↓

  - mail1.hogehoge.comを社内NTPマスターサーバーとして、NTPリンクを構築する

eAccess Broadband Services

実装検討1 – 時間同期



index

実装検討1 - 状態監視ツール - Big Brother

- http://bb4.com/
- WEB Baseの監視システム
  - ソースが公開されているが、オープンソースではない
  - 今年からFreeware version 1.9c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/WindowsNT系/NetWare/Macintoshの監視用プローブがあり、複合OS統合監視が可能

実装検討1 – 状態監視ツール - Big Brother 続き

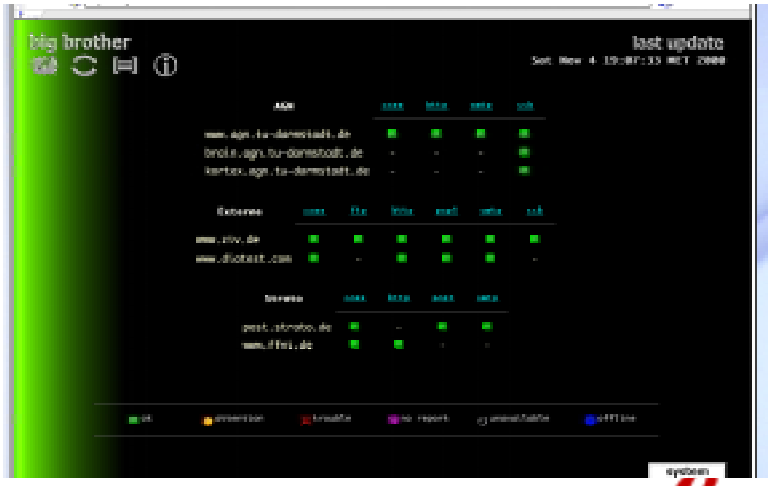
- 監視対象のグループ化機能
- 監視画面の階層化機能(2段階)
- 柔軟なアラーム通知機能
  - E-mailによりアラームを通知する。
  - ホスト単位にシステムの停止時間を設定。自動で監視対象から除外可能
  - ホスト単位で障害通知先を変更可能
  - アラームの検出されている機器のみサマリーした画面を標準で生成。
  - アラームメッセージに障害情報ページのURLが引用されており、迅速に障害情報に到達可能

実装検討1 – 状態監視ツール - Big Brother 続き

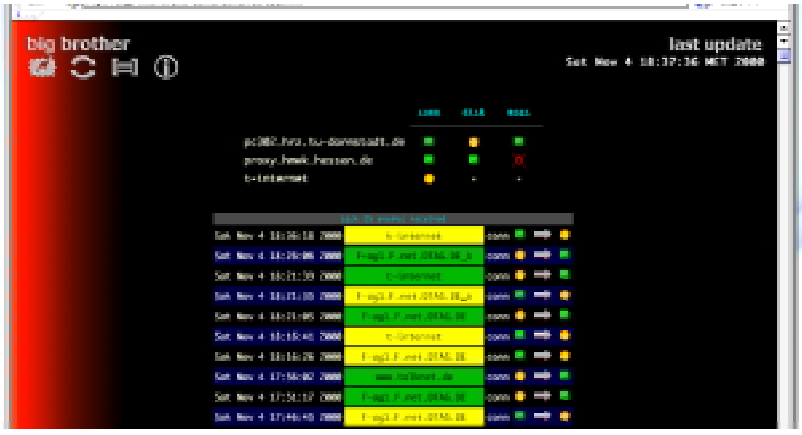
- 障害履歴機能
- システム稼動状況レポート作成機能
- 拡張インタフェースが公開されており、多彩な拡張監視モジュールが存在する(後述)
  - オープンソースの利点を生かし、BB基本ソフトをそのまま置換する機能拡張版ソフトも存在する
  - 拡張監視モジュール: DBMS, ファイルサーバ, プリンタサーバ, …
  - 他ソフトとの連係: MRTG, RRDTools, snort, tripwire, …
  - BBTray : Big Brother監視ツール on Windows
- マニュアルがかなり整っている。
  - 各モジュールの構成にまで踏み込んだ解説付き
- 適用範囲: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

実装検討1 – BB - 監視画面 (TOP)

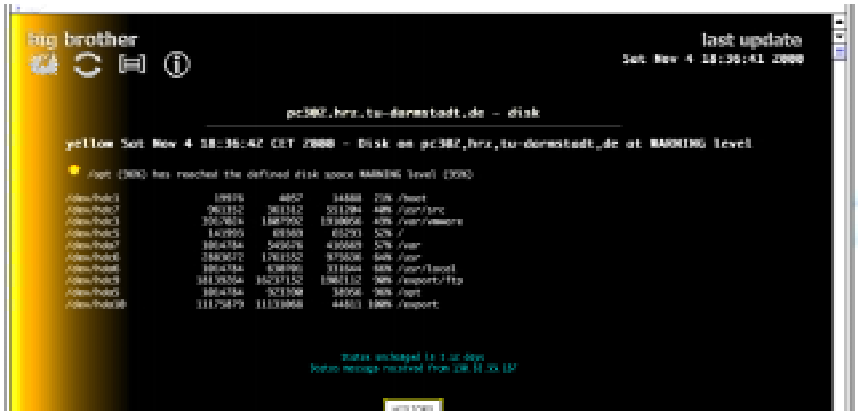
実装検討1 – BB - 監視画面 (sub)



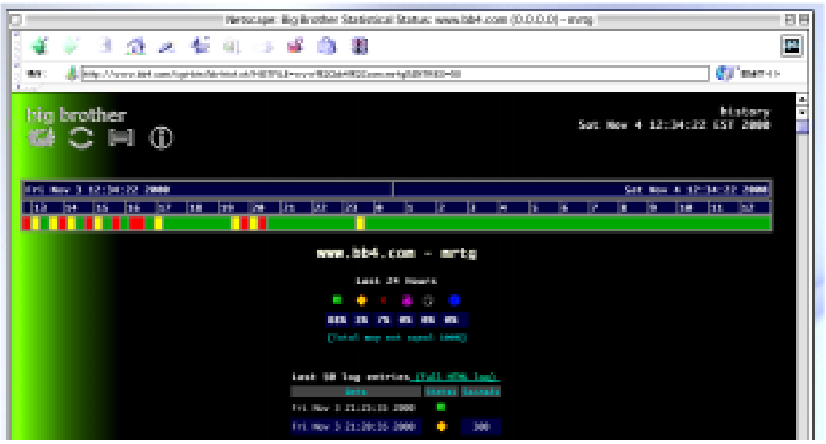
実装検討1 – BB - アラートサマリ



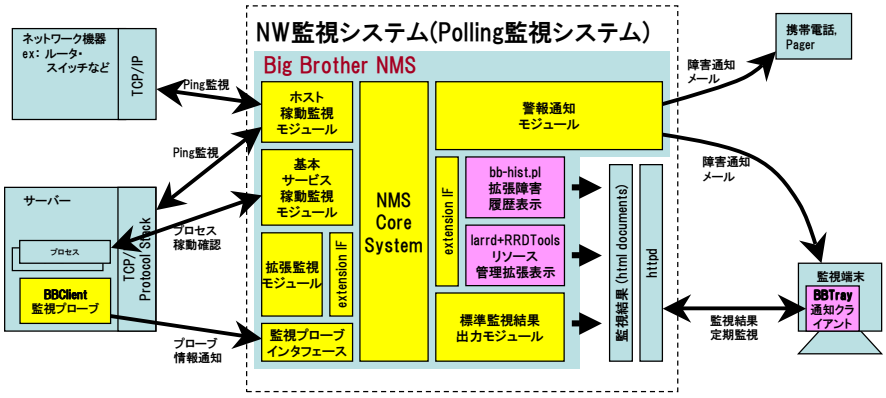
実装検討1 – BB - イベント情報画面



実装検討1 – BB - ヒストリ画面



監視システムのモデル - Polling監視システム



機能実装1 – Big Brother 監視サーバー設定ファイル

- Big Brother監視ソフトのセットアップは以下のファイルの設定による。
  - $BBHOME/etc/bb-hosts: 監視対象定義ファイル
  - $BBHOME/etc/bb-warnrule.cfg: 障害通知定義ファイル
  - $BBHOME/etc/bbdef.sh: システム監視定義ファイル
  - $BBHOME/etc/security

機能実装1 – 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
  - 非提供サービス確認

ホスト名	Interface	IPアドレス	監視サーバ監視項目名称	サービス提供状況確認							
				Ping	telnet	ssh	DNS	WWW	sendmail	pop	ftp	finger
ns1(mail2)	eth0	211.14.XXX.36	ns1	O	X	O	O	X	O	---	X	X
mail1	eth0	211.14.XXX.37	mail1.external	O	X	X	O	X	O	X	X	X
	eth1	172.16.0.64	mail1.internal	O	X	O	O	X	O	O	X	X
www(ns2)	eth0	211.14.XXX.38	www	O	X	O	O	O	X	---	O	X
log1	eth0	172.16.0.66	log1	O	X	O	---	O	X	---	X	X
mon1	eth0	211.14.XXX.39	mon1.external	O	X	X	---	X	X	---	X	X
	eth1	172.16.0.67	mon1.internal	O	X	O	---	O	X	---	X	X
ps00	eth0	172.16.0.65	ps00	O	---	---	---	---	---	---	---	---
fs10	eth0	172.16.10.9	fs10	O	---	---	---	---	---	---	---	---
fs20	eth0	172.16.20.9	fs20	O	---	---	---	---	---	---	---	---
fs30	eth0	172.16.30.9	fs30	O	---	---	---	---	---	---	---	---

ホスト名	Interface	IPアドレス	監視サーバ監視項目名称	サービス提供状況確認							
				Ping	telnet	ssh	DNS	WWW	sendmail	pop	ftp	finger
bbsw01	vlan1	172.16.0.1	bbsw01.vlan1	O	---	---	---	---	---	---	---	---
	vlan10	172.16.10.1	bbsw01.vlan10	O	---	---	---	---	---	---	---	---
	vlan20	172.16.20.1	bbsw01.vlan20	O	---	---	---	---	---	---	---	---
	vlan30	172.16.30.1	bbsw01.vlan30	O	---	---	---	---	---	---	---	---
lansw01	vlan1	172.16.0.32	lansw01	O	---	---	---	---	---	---	---	---
lansw10	vlan1	172.16.0.33	lansw10	O	---	---	---	---	---	---	---	---
lansw20	vlan1	172.16.0.34	lansw20	O	---	---	---	---	---	---	---	---
lansw30	vlan1	172.16.0.35	lansw30	O	---	---	---	---	---	---	---	---
prt10	eth0	172.16.10.10	prt10	O	---	---	---	---	---	---	---	---
prt20	eth0	172.16.20.10	prt20	O	---	---	---	---	---	---	---	---
prt30	eth0	172.16.30.10	prt30	O	---	---	---	---	---	---	---	---
firewall01	wan0	211.14.XXX.34	firewall01.wan0	O	---	---	---	---	---	---	---	---
	lan0	172.16.0.3	firewall01.lan0	O	---	---	---	---	---	---	---	---
extgw01	wan0	a.b.c.d	extgw01.wan0	O	---	---	---	---	---	---	---	---
	lan1	211.14.XXX.33	extgw01.lan0	O	---	---	---	---	---	---	---	---

機能実装1 - 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。

実装検討1 - 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.hogehoge.com # BBPAGER BBNET BBDISPLAY http://kansi1/

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

# router interface entry
page Router-IF “Router Intereface”
group-compress <H3><I>Router1 Interfaces</I></H3>
192.168.0.1  gw1.hogehoge.com
192.168.0.50 gw2.hogehoge.com
group-compress <H3><I>Router2 Interfaces</I></H3>
192.168.1.2  tok-yok-ma30.wan.hogehoge.com
192.168.1.6  tok-osa-dr15.wan.hogehoge.com
$2
```


実装検討1 - 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.hogehoge.com/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

実装検討1 - 監視対象定義
etc/bb-hosts - 3

- 特殊設定項目: `dialup modem-bank`
  - DHCP/ダイア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
- 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
    - 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
    - <page title>にはhtmlタグが使用可能

実装検討1 – mon1設定
etc/bb-hosts

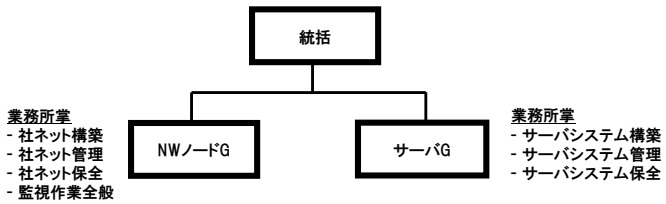
```
##################################################################
# BIG BROTHER bb-hosts --- monitoring hosts definitions
##################################################################
######
# hogehoge.com - Servers
######
group-compress <H3><B>Servers </B></H3>
211.14.XXX.36 ns1 # !telnet ssh dns smtp !ftp !finger
211.14.XXX.37 mail1.external # !telnet !ssh dns smtp !pop3 !ftp !finger
172.16.0.64   mail1 # !telnet !ssh dns smtp  pop3 !ftp !finger
211.14.XXX.38 www # !telnet !ssh dns http://www.hogehoge.com/ smtp !ftp !finger
172.16.0.66   log1 # !telnet ssh !smtp !ftp !finger
211.14.XXX.39 mon1.external # !telnet !ssh !http://211.14.XXX.39/ !smtp !ftp !finger
172.16.0.67   mon1 # BBPAGER BBNET BBDISPLAY !telnet ssh http://172.16.0.67/ !smtp !ftp !finger
172.16.0.65   ps00
172.16.10.9   fs10
172.16.20.9   fs20
172.16.30.9   fs30

######
# hogehoge.com - Network Node
######
group-compress <H3><B>Network Nodes</B></H3>
172.16.0.1    bbsw01.vlan1
172.16.10.1   bbsw01.vlan10
172.16.20.1   bbsw01.vlan20
172.16.30.1   bbsw01.vlan30
172.16.0.32   lansw01
172.16.0.33   lansw10
172.16.0.34   lansw20
172.16.0.35   lansw30
172.16.10.10  prt10
172.16.20.10  prt20
172.16.30.10  prt30
211.14.XXX.34 firewall01.wan0
172.16.0.3    firewall01.lan0
a.b.c.d       extgw01.wan0
211.14.XXX.33 extgw01.lan0

##################################################################
# BIG BROTHER bb-hosts --- end of lie
##################################################################
```

実装検討1 - 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

監視体制とエスカレーション(再掲)

- 全システムの管理は技術部門 情報システム部で行う。
- 管理はサーバGとNWノードGの2グループ体制となっており、監視はNWノードGにて行っている。
- 24時間常駐はしておらず、通常勤務時間外についてはシステムからの自動警報通知にてリモート対応とする。
- 重要ノードの障害については担当に通知するとともに統括責任者にもエスカレーション通知がなされる



業務所掌
- 社ネット構築
- 社ネット管理
- 社ネット保全
- 監視作業全般

業務所掌
- サーバシステム構築
- サーバシステム管理
- サーバシステム保全

実装検討1 – 警報通知定義

ホスト名	Interface	IPアドレス	監視サーバ 監視項目名称	通知先	管理G	通知時間	備考
ns1(mail2)	eth0	211.14.XXX.36	ns1	svr-alert,crit-alert	SVR-G	24h/7d	
mail1	eth0	211.14.XXX.37	mail1.external	svr-alert,crit-alert	SVR-G	24h/7d	
	eth1	172.16.0.64	mail1.internal	svr-alert,crit-alert	SVR-G	24h/7d	
www(ns2)	eth0	211.14.XXX.38	www	svr-alert,crit-alert	SVR-G	24h/7d	
log1	eth0	172.16.0.66	log1	svr-alert	SVR-G	24h/7d	
mon1	eth0	211.14.XXX.39	mon1.external	svr-alert	SVR-G	24h/7d	
	eth1	172.16.0.67	mon1.internal	svr-alert	SVR-G	24h/7d	
ps00	eth0	172.16.0.65	ps00	svr-alert	SVR-G	週日 8:00-21:00	監視対応時間内対応のみ
fs10	eth0	172.16.10.9	fs10	svr-alert	SVR-G	0:00-2:59 6:00-23:59	定期バックアップ時間 3:00-6:00
fs20	eth0	172.16.20.9	fs20	svr-alert	SVR-G	0:00-2:59 6:00-23:59	定期バックアップ時間 3:00-6:00
fs30	eth0	172.16.30.9	fs30	svr-alert	SVR-G	0:00-2:59 6:00-23:59	定期バックアップ時間 3:00-6:00
bbsw01	vlan1	172.16.0.1	bbsw01.vlan1	nwt-alert, crit-alert	NWT-G	24h/7d	
	vlan10	172.16.10.1	bbsw01.vlan10	nwt-alert, crit-alert	NWT-G	24h/7d	
	vlan20	172.16.20.1	bbsw01.vlan20	nwt-alert, crit-alert	NWT-G	24h/7d	
	vlan30	172.16.30.1	bbsw01.vlan30	nwt-alert, crit-alert	NWT-G	24h/7d	
lansw01	vlan1	172.16.0.32	lansw01	nwt-alert, crit-alert	NWT-G	24h/7d	
lansw10	vlan1	172.16.0.33	lansw10	nwt-alert	NWT-G	24h/7d	
lansw20	vlan1	172.16.0.34	lansw20	nwt-alert	NWT-G	24h/7d	
lansw30	vlan1	172.16.0.35	lansw30	nwt-alert	NWT-G	24h/7d	
prt10	eth0	172.16.10.10	prt10	nwt-alert	NWT-G	週日 8:00-21:00	監視対応時間内対応のみ
prt20	eth0	172.16.20.10	prt20	nwt-alert	NWT-G	週日 8:00-21:00	監視対応時間内対応のみ
prt30	eth0	172.16.30.10	prt30	nwt-alert	NWT-G	週日 8:00-21:00	監視対応時間内対応のみ
firewall01	wan0	211.14.XXX.34	firewall01.wan0	nwt-alert, crit-alert	NWT-G	24h/7d	
	lan0	172.16.0.3	firewall01.lan0	nwt-alert, crit-alert	NWT-G	24h/7d	
extgw01	wan0	a.b.c.d	extgw01.wan0	nwt-alert, crit-alert	NWT-G	24h/7d	
	lan1	211.14.XXX.33	extgw01.lan0	nwt-alert, crit-alert	NWT-G	24h/7d	

実装検討1 - 警報通知定義
etc/bbwarnrules.cfg

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

ns1.* mail1.* www.*;;*;;*;*;svr-alert@hogehoge.com crit-alert@hogehoge.com
## ns1.*, mail1.* www.*については24H/7Dの監視を行い、
## 障害時はsvr-alert, crit-alertに通知する

log1.* mon1.*;;*;;*;*;svr-alert@hogehoge.com
## log1.* mon1.*については24H/7Dの監視を行い、障害時はsvr-alertに通知する

fs*;;*;*;0-6;0000-0259 0600-2359;svr-alert@hogehoge.com
## fs*(fs10.* fs20.* fs30.*にマッチする)は、障害時はsvr-alertに通知する
## ただし、AM3:00-AM5:59までの間は監視対象外とする

ps00.* prt10.* prt20.* prt30.*;;*;;1-5;0800-2100;intra-nwt-alert@hogehoge.com
## ps00.* prt10.* prt20.* prt30.*は月曜日から金曜日のAM8:00-PM9:00まで全て
## のサービス監視を行い、障害時はsvr-alertに通知する

bbsw01* lansw01.* firewall01* extgw01.*;;*;;*;*;svr-alert@foo.co.j
## 主要ネットワークノードであるbbsw01* lansw01.* firewall01* extgw01.*の各
## 監視項目についてはについては24H/7Dの監視を行い、障害時はnwt-alert, crit-alertに通知する

*;;*;;*;*;nwt-alert@hogehoge.com
## 上記以外のホスト(lansw10/lansw20/lansw30)の障害検知については
## nwt-alert@hogehoge.com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
$
```

実装検討1 - 監視システム定義 etc/bbdef.sh - 1

- Big Brotherシステム定義ファイル
- 稼動に必要な環境変数の定義を設定。監視閾値・挙動指定をし、外部拡張監視(Plug-in)の登録もこのファイルに行う
- 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%)
  - サーバー全体に関する設定であり、パ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動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)

実装検討1 - 監視システム定義 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
    - PAGEMSMS - 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"
    - Red = critical level
    - Purple = target no response
- 外部機能拡張登録: BBMKBBEXT, BBMKBB2EXT, BBEXT
  - 外部機能拡張(plug-in)の登録を行う。詳細は後述

実装検討1 - 監視システム定義 etc/bbdef.sh設定

```
$cat bbdef.sh
#!/bin/sh
# bbdef.sh
【省略】
# LOCAL CLIENT MONITORING CONFIGURATION FOR bb-local.sh
#   WARNING AND PANIC LEVELS FOR LOCAL SYSTEM INFOMRAION
#   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 snmpd !inetd !popd !sendmail snmptrapd syslogd"  #(YELLOW)WARN IF NOT RUNNING
PAGEPROC="cron sshd httpd" # (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
PAGEMSG="NOTICE"                        # (RED) PAGE IF WE SEE THIS MESSAGE
IGNMSGS=""              # List of messages to ignore if string(s) matches line
【省略 - 続く】
```


実装検討1 - 監視システム定義 etc/bbdef.sh設定 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
BBMKBBEXT=" "
BBMKBB2EXT="eventlog.sh"
export BBMKBBEXT BBMKBB2EXT
【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】
$
```

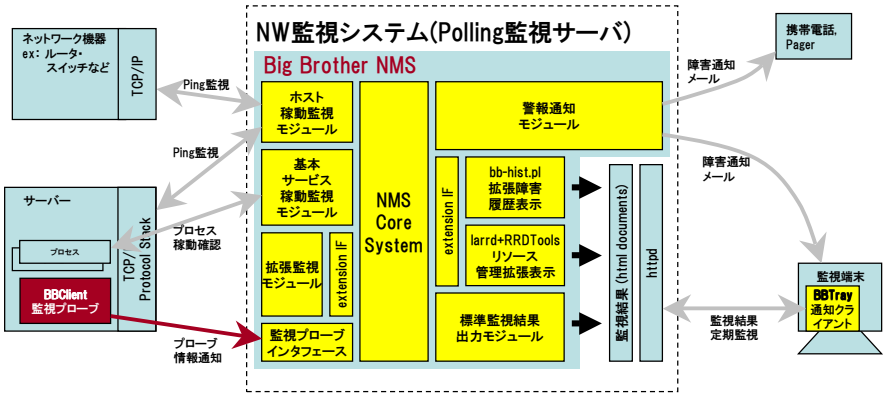
実装検討1 - process監視

- 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と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
```


実装検討1 - process監視

実装検討1 – 監視プローブの設定



実装検討1 – 監視プローブの設定

- Big Brother監視サーバーのみの設定では、各監視対象のIP疎通・ポート監視は可能であるが、CPUプロセス監視やディスク容量監視などといったリソース監視はできない
- これらを可能とするものとして、監視対象にbbclient(監視プローブ)をインストールする。
  - 可能となるリモート監視:
    - CPUロード監視
    - プロセス監視
    - メッセージ監視
    - ディスク容量監視

実装検討1 – 監視プローブの設定

- インストール方法
  - Big Brother NMSのインストールと基本的には同じ手順を行う。
  - BB Serverインストール後、$BBHME/install/bbclientスクリプトにて bbclient tar archiveを作成し、各サーバにftpで転送する
  - 設定はbbdef.shの該当変数部分のみ。
    - ディスク監視:DFWARN, DFPANIC
    - CPU ロード監視:CPUWARN, CPUPANIC
    - プロセス監視:PROCS, PAGEPROCS
    - メッセージ監視:MSGS, PAGEMSGS
  - プロセス監視以外はほとんど共通となる。
  - プロセス監視は各サーバ毎の機能に応じてアレンジが必要。

実装検討1 – 監視プローブの設定 プロセス監視部分

ホスト名	Interface	IPアドレス	監視サーバ 監視項目名称	プロセス確認									
				inetd	sshd	named	httpd	cron	syslogd	sendmail	popd	snmpd	snmptrapd
ns1(mail2)	eth0	211.14.XXX.36	ns1	×	○	○	×	○	○	○	×	○	×
mail1	eth0	211.14.XXX.37	mail1.external	---	---	---	---	---	---	---	---	---	---
	eth1	172.16.0.64	mail1.internal	×	○	×	×	○	○	○	○	○	×
www(ns2)	eth0	211.14.XXX.38	www	×	○	○	○	○	○	×	×	○	×
log1	eth0	172.16.0.66	log1	×	○	×	×	○	○	×	×	○	○

【ns1 - $BBHOME/etc/bbdef.sh該当部分】
```
PROCS="bbrun snmpd !inetd syslogd !httpd !popd"
PAGEPROC="cron named sshd sendmail"
```

【mail1.internal - $BBHOME/etc/bbdef.sh該当部分】
```
PROCS="bbrun snmpd !inetd syslogd !httpd"
PAGEPROC="cron sshd sendmail popd"
```

【www - $BBHOME/etc/bbdef.sh該当部分】
```
PROCS="bbrun snmpd !inetd syslogd !httpd !popd !sendmail"
PAGEPROC="cron named sshd"
```

【log1 - $BBHOME/etc/bbdef.sh該当部分】
```
PROCS="bbrun snmpd !inetd !httpd !popd !sendmail"
PAGEPROC="cron sshd syslogd snmptrapd"
```

BB - extensions

- 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/
  - 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

BB - Extension Archive

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, postgress, 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

実装検討1 - 拡張ヒストリー

- ftp://ftp.deadcat.net/pub/BB/bb-hist-2.6.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

実装検討1 - 拡張ヒストリー画面

実装検討1 - システムリソース管理
BB-RRDTool連係:larrd

- larrd: loadavg rrdtool -> latest v 0.42
- 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
- 反面、設定は簡単であり、以下の設定だけで動作する
  - 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/bbdef.shへの登録
    - $BBEXT変数へのエントリー追加
  - BigBrother再起動

実装検討1 - 監視システム定義
BB-RRDTool連携:larrd設定

- $BBHOME/etc/bbdef.shにて以下の部分にlarrdを追加する。
  - ここではlarrdのデフォルトインストールディレクトリを /usr/local/larrd とし、/usr/local/bb/ext/larrdのシンボリックリンクがはられている場合の変更場所を示す

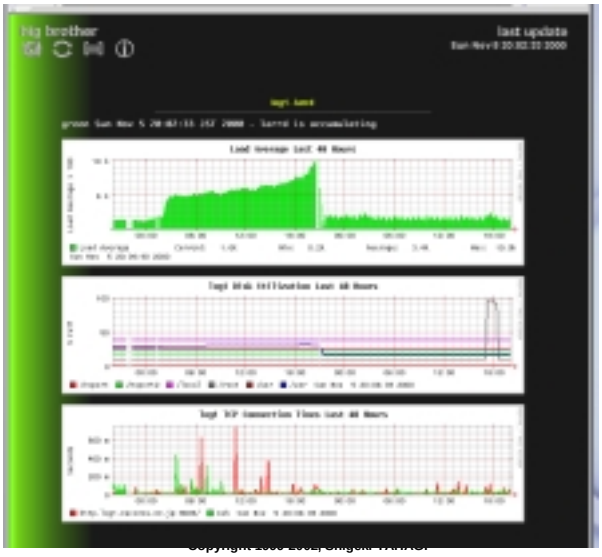
- 【 $BBHOME/etc/bbdef.sh 変更箇所】

```
# 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
```

【 $BBHOME/etc/bbdef.sh 変更箇所 終わり】

-

実装検討1 - システムリソース管理
BB-RRDTool連係:larrd画面



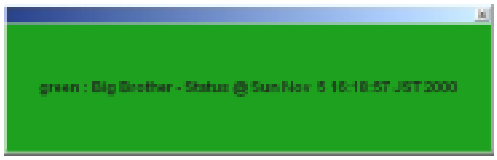
85

実装検討1 - 監視クライアント連係
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
- ftp://ftp.deadcat.net/pub/BB/BBtray-0.8.3.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

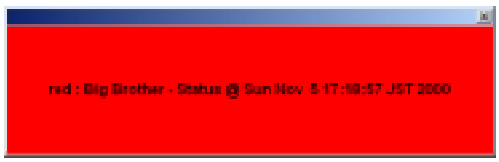
86

実装検討1 - 監視クライアント連係
BBTray - 続き



Green Window
- this is normal status

Yellow Window
- this is warning status.



Red Window
- this is critical status!!

実装検討1 - 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://172.16.0.66:5963/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!
```


実装検討1 - security確保1

- BBサーバへのアクセス規制
  - デフォルトではBBのポート規制がかかっていないため，BBサーバへの語情報を送り込むことが可能
  - このため、BBであクライアント受付範囲を規制するネットワークリストを設定可能となっている。
    - $BBHOME/etc/security

```
$ cat $BBHOME/etc/security
# THE SECUIRTY FILE DETERMINES WHO CAN CONNECT TO A BIG BROTHER SERVER.
# NO SECURITY FILE MEANS ANYONE CAN CONNECT, OTHERWISE ONLY THE IP ADDRS
# AND NETWORKS LISTED HERE CAN CONNECT.
#
# mon1.hogehoge.com accept network lists
# -----------------

211.14.xxx.32/255.255.255.224
172.16.0.0/255.240.0.0

# end of security list
$
```

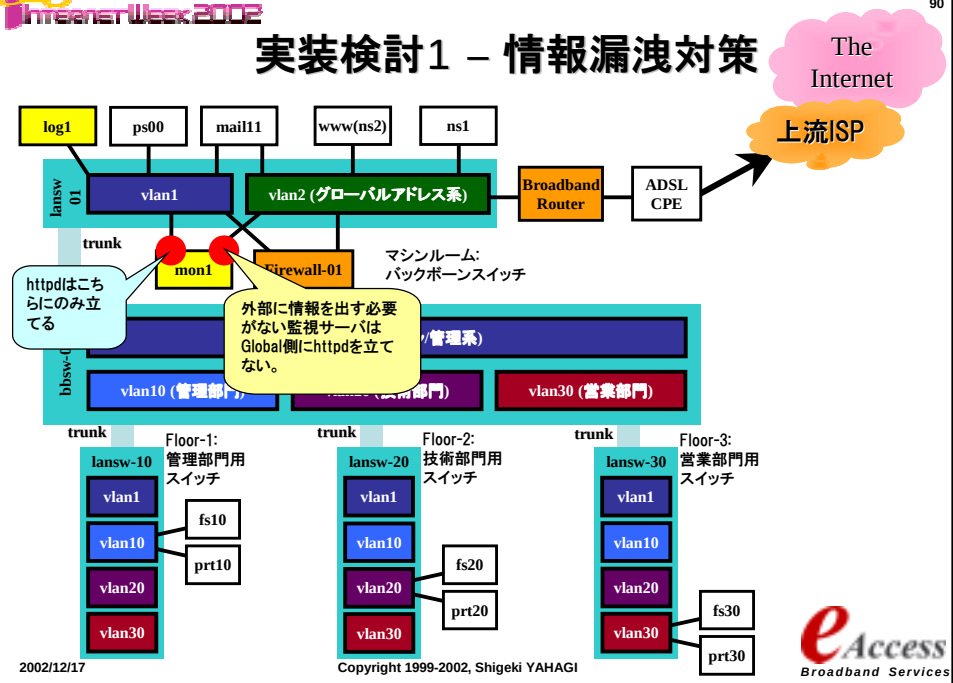
実装検討1 - security確保2

- 監視サーバーの画面は外に公開するものか？
  - 業務要件上必要がないのであれば、Globalセグメントにhttpdを立てない。
  - 外に公開しないのでればhttp portもRFC標準である必要はない
    - http portを変更する (http port != 80)
    - Ex: http://mon1.hogehoge.com:5963/bb/

【apache httpd.confの抜粋】

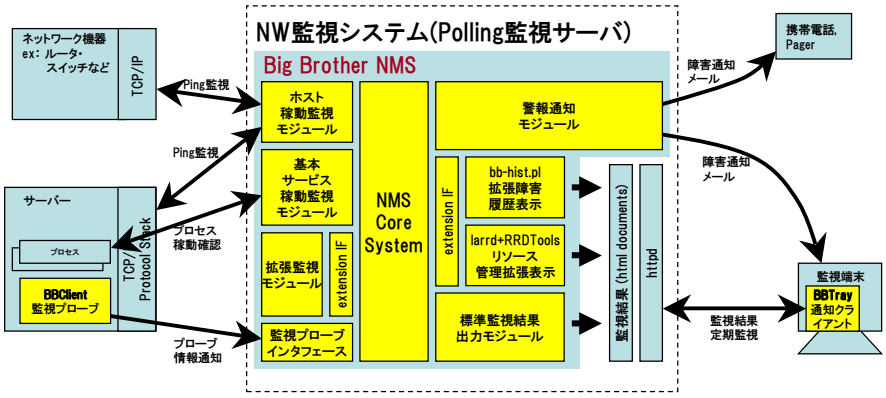
```
# Listen: Allows you to bind Apache to specific IP addresses and/or
# ports, in addition to the default. See also the <VirtualHost>
# directive.
#
Listen 172.16.0.67:5963

# Port: The port to which the standalone server listens. For
# ports < 1023, you will need httpd to be run as root initially.
#
Port 5963
```


実装検討1 – 情報漏洩対策



91

監視システムのモデル - Polling監視システム



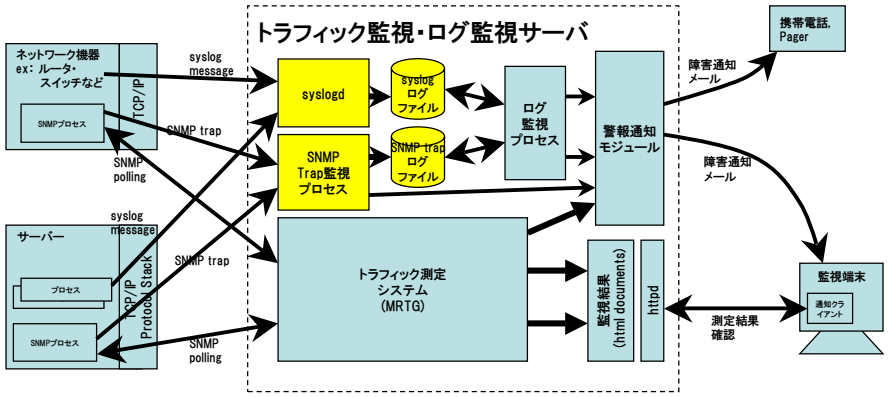
eAccess Broadband Services

92

index

eAccess Broadband Services

監視システムのモデル - トラフィック・ログ監視サーバ



実装検討2 – syslog1

- ログの集中管理を行う。
- ハードディスクのような固定的な記憶媒体を持たないネットワーク機器はリブートしてしまうと、障害にいたるまでの経過が把握できない。
- syslog機能により、ログサーバに対してログメッセージをネットワーク経由で記録する。

- メッセージファシリティーとメッセージプライオリティ
  - ファシリティー：メッセージの送り先チャネルの指定
  - プライオリティー：メッセージの重要度の指定

実装検討1 – syslog2

- メッセージファシリティーとメッセージプライオリティ
  - ファシリティー:メッセージの送り先チャネルの指定
    - 例:kern -> kernel message, mail -> mail system message,
      auth -> authorization system message,
      security -> security subsystem message
    - ユーザが独自に使用できるのは local0からlocal7までの8ファシリティとなる
  - プライオリティー:メッセージの重要度の指定
    - 8種類のプライオリティー
      - EMERG PANICメッセージ。全ユーザに通知される
        ALERT システムDBが壊れているような直ちに対処が必要な重要障害警告
        CRIT ハードウェアのデバイスエラーのような危急状態の警告
        ERR その他のエラーメッセージ
        WARN 警告メッセージ
        NOTICE エラーではないが、注意が必要なメッセージ
        INFO 参考情報メッセージ
        DEBUG デバッグメッセージ
  - メッセージの指定例
    - ex: kern.debug, local2.crit, mail.err

実装検討2 – syslog3

- syslogにて情報を取得する対象を以下のように分類
  - バックボーンスイッチ: local0
    - 対象:bbsw01, lansw01, extge01
  - エッジスイッチ: local1
    - 対象:lansw10, lansw20, lansw30
  - ファイヤーウォール(firewall01):local2
  - ネットワークプリンタ:local3
    - 対象:prt10, prt20, prt30
- 各装置からはINFO以上のメッセージのみを送信する
- 保存場所は以下のとおりとする
  - バックボーンスイッチ:/var/log/bbsw.log
  - エッジスイッチ:/var/log/edgesw.log
  - ファイヤーウォール:/var/log/firewall.log
  - ネットワークプリンタ:/var/log/nprt.log
    - #注意 これらのファイルは事前に作成しないと記録が始まらない。

実装検討2 – syslog4 /etc/syslog.conf

- log1のsyslogdに以下の設定を追加投入する。
  - 【/etc/syslog.conf追加設定】

```
local0.info     /var/log/bbsw.log
local1.info     /var/log/edgesw.log
local2.info     /var/log/firewall.log
local3.info     /var/log/nprt.log
```

  - ＃注意 ファシリティと記録ファイルの間はスペースではなくタブ(TAB)で区切ることを注意

実装検討2 – syslog5 L3スイッチでの設定

- ネットワーク装置側からは
- CISCO IOSでの設定例
  - logging trap info
  - logging facility local1
  - logging 172.16.0.67

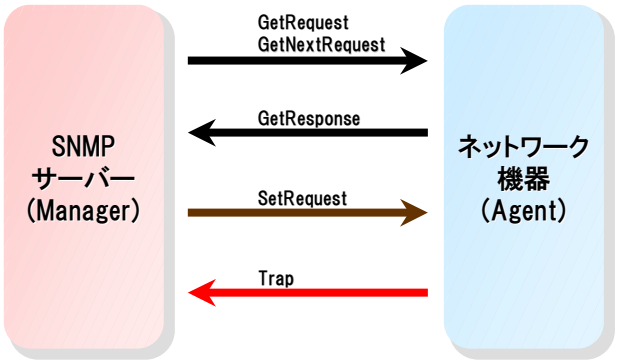
実装検討2 – snmptrapd1 Net-SNMP Package

- http://net-snmp.sourceforge.net/
- 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, snmptest, snmpusm, snmpcheck, snmpgetnext, snmpstatus, snmptranslate, snmpwalk, snmpdelta, snmpnetstat, snmptable, snmptrap

実装検討2 – snmptrapd2 NET-SNMP

- 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….>

SNMP Message Hundling



実装検討2 - snmptrapd.conf

```
# SNMP Trap : Cold Start
traphandle .1.3.6.1.6.3.1.1.5.1 /usr/bin/mail -s "coldStart Trap" nwt-alert@hogehoge.com
# SNMP Trap : Warm Start
traphandle .1.3.6.1.6.3.1.1.5.2 /usr/bin/mail -s "warmStart Trap" nwt-alert@hogehoge.com
# SNMP Trap : Link Down
traphandle .1.3.6.1.6.3.1.1.5.3 /usr/bin/mail -s "linkDown Trap" nwt-alert@hogehoge.com
# SNMP Trap : Link Up
traphandle .1.3.6.1.6.3.1.1.5.4 /usr/bin/mail -s "linkUp Trap" nwt-alert@hogehoge.com
# SNMP Trap : Authentication Failure
traphandle .1.3.6.1.6.3.1.1.5.5 /usr/bin/mail -s "authFail Trap" nwt-alert@hogehoge.com
# SNMP Trap : Other
traphandle   default  /usr/bin/mail -s "Other Traps" yahagi@hogehoge.com
```

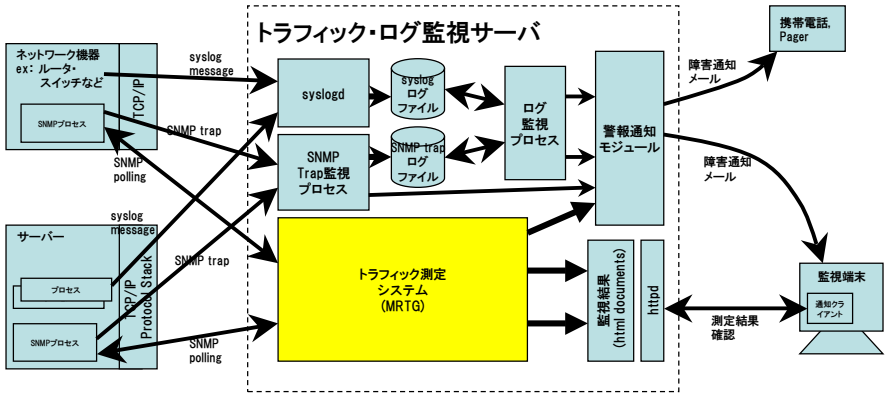
実装検討2 - snmptrapd - CISCOルータでのsnmp関連config

- CISCOルータでのSNMPv2設定例
  - access-list 30 permit 172.16.0.66
  - access-list 30 permit 172.16.0.67
  - snmp-server contact nwt-alert@hogehoge.com
  - snmp-server location YOKOHAMA-IW2002
  - snmp-server community himitsu RO 30
  - snmp-server enable traps config
  - snmp-server host 172.16.0.66 NAISHO tty config envmon snmp

実装検討2 - snmptrapd - 通知結果

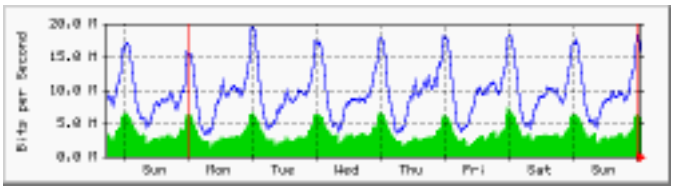
- From: log-admin <root@log.hogehoge.com>
- To: nwt-alert@hogehoge.com
- Date: Thu, 1 Nov 2001 22:01:49 +0900 (JST)
- Subject: linkDown Trap
- nspixp2-gw.hogehoge.com
- 192.168.244.21
- system.sysUpTime 24:10:03:09.12
- .iso.org.dod.internet.snmpV2.snmpModules.snmpMIB.snmpMIBObjects.snmpTrap.snmpTrapOID .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

実装検討2 – トラフィック監視



実装検討2 – トラフィック監視
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



107

実装検討2 – トラフィック監視 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

108

実装検討2 – トラフィック監視 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

109

実装検討2 – トラフィック監視
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.hogehoge.com > 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

110

実装検討2 – トラフィック監視
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 Addres`
  - `--ifref=eth ... by Ethernet Number`
  - `--ifref=descr ... by Interface Description`
  - `--ifref=name ... by Interface Name`
  - `--ifref=type ... by Interface Type`

実装検討2 – トラフィック監視
MRTG - cfgmaker の出力結果

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

######################################################################
# Description: Cisco Internetwork Operating System Software IOS (tm)
#     Contact: nwt-alert@hogehoge.com
# System Name: ix-gw.hogehoge.com
#    Location: PA, CA, US
#.....................................................................…

Target[ix-fddi.hogehoge.com]: 1:himitsu@192.168.98.133
MaxBytes[ix-fddi.hogehoge.com]: 12500000
Title[ix-fddi.hogehoge.com]: ix-gw.hogehoge.com (ix-fddi.hogehoge.com): Fddi1/0/0
PageTop[ix-fddi.hogehoge.com]: <H1>Traffic Analysis for Fddi1/0/0
 </H1>
 <TABLE>
   <TR><TD>System:</TD><TD>ix-gw.hogehoge.com 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.hogehoge.com (172.16.0.2)</TD></TR>
   <TR><TD>Max Speed:</TD>
       <TD>12.5 MBytes/s (fddi)</TD></TR>
  </TABLE>
```


機能実装 – トラフィック監視
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

実装検討2 – トラフィック監視 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.hogehoge.com`
  - `Target[gw1-err-3]: ifInErrors.3&ifOutErrors.3:himitsu@gw1.hogehoge.com`
  - `Target[gw1-if-1]: -/10.0.0.101:himitsu@gw1.hogehoge.com`
  - `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

実装検討2 – トラフィック監視 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

115

実装検討2 – トラフィック監視 測定対象

- 各ネットワークノード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)

ホスト名	Interface	bps	pps	packet discards	IF error
bbsw01	GigabitEthernet 1	○	○	○	○
	GigabitEthernet 2	○	○	○	○
	GigabitEthernet 3	○	○	○	○
	GigabitEthernet 4	○	○	○	○
	GigabitEthernet 5	○	○	○	○
	GigabitEthernet 6	○	○	○	○
	GigabitEthernet 7	○	○	○	○
	GigabitEthernet 8	○	○	○	○
lansw01	FastEthernet 0/1 - 0/48	○	○	○	○
	GigabitEthernet 0/1	○	○	○	○
	GigabitEthernet 0/2	○	○	○	○
lansw10	FastEthernet 0/1 - 0/48	○	○	○	○
	GigabitEthernet 0/1	○	○	○	○
	GigabitEthernet 0/2	○	○	○	○
lansw20	FastEthernet 0/1 - 0/48	○	○	○	○
	GigabitEthernet 0/1	○	○	○	○
	GigabitEthernet 0/2	○	○	○	○
lansw30	FastEthernet 0/1 - 0/48	○	○	○	○
	GigabitEthernet 0/1	○	○	○	○
	GigabitEthernet 0/2	○	○	○	○
extgw01	wan0	○	○	○	○
	lan0	○	○	○	○
firewall01	wan0	○	○	○	○
	lan0	○	○	○	○

116

実装検討2 – 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

117

実装検討2 – トラフィック監視 mrtg configの作り方

- 導入している装置にはモジュラータイプのものがないために、インタフェースは全て事前に把握可能
  - Interface Description指定にて作成するのが簡単
- 測定対象はひとつの装置に対して以下の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

118

実装検討2 – トラフィック監視 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/bbsw01/
/usr/local/mrtg/data/lansw01/
/usr/local/mrtg/data/lansw10/
/usr/local/mrtg/data/lansw20/
/usr/local/mrtg/data/lansw30/
/usr/local/mrtg/data/extge01/
/usr/local/mrtg/data/fw01/
```

実装検討2 – トラフィック監視
mrtg configの作り方 (続き)

- bps項目についてはGigabitEthernet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 2.9系列にてSNMPv2c 64bit counter MIBを使用する
    - 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`
    - カウンターリセットしないEnterprise MIBにてを使用する
  - ここではCISCOエンタープライズMIBでの例をあげる。
    - 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

実装検討2 – トラフィック監視
config file – bps/pps

```
#####
# lansw01 bps/pps config – lansw01-if.cfg
###
WorkDir: /usr/local/mrtg/data/lansw01/
IconDir: /mrtg-icons/
Withpeak[_]: wmy

Forks: 4

Target[fa0-1-bps]: ¥FastEthernet0/1:himitsu@172.16.0.32
MaxBytes[fa0-1-bps]: 100000000
Title[fa0-1-bps]: lansw01:  FastEthernet0/1 bps
PageTop[fa0-1-bps]: <H1>lansw01:  FastEthernet0/1 bps</H1>
Options[gi0-1-bps]: bits,growright

Target[fa0-1-pps]: ifInUcastPkts¥FastEthernet0/1&ifOutUcastPkts¥FastEthernet0/1:himitsu@172.16.0.32
MaxBytes[fa0-1-pps]: 500000
Title[fa0-1-pps]: lansw01:  FastEthernet0/1 pps
PageTop[fa0-1-pps]: <H1>lansw01:  FastEthernet0/1 pps</H1>
Options[fa0-1-pps]: growright

【中略】

Target[gi0-1-bps]: 1.3.6.1.4.1.9.2.2.1.1.6¥GigabitEthernet0/1&1.3.6.1.4.1.9.2.2.1.1.8¥GigabitEthernet0/1:himitsu@172.16.0.32
MaxBytes[gi0-1-bps]: 193750000
Title[gi0-1-bps]: lansw01:  GigabitEthernet0/1 bps
PageTop[gi0-1-bps]: <H1>lansw01:  GigabitEthernet0/1 bps</H1>
Options[gi0-1-bps]: gauge,growright

Target[gi0-1-pps]: ifInUcastPkts¥FastEthernet0/1&ifOutUcastPkts¥FastEthernet0/1:himitsu@172.16.0.32
MaxBytes[gi0-1-pps]: 5000000
Title[gi0-1-pps]: lansw01:  GigabitEthernet0/1 pps
PageTop[gi0-1-pps]: <H1>lansw01:  GigabitEthernet0/1 pps</H1>
Options[gi0-1-pps]: growright
```

実装検討2 – トラフィック監視
config file – bps/pps (続き)

```
Target[gi0-2-bps]: 1.3.6.1.4.1.9.2.2.1.1.6¥GigabitEthernet0/2&1.3.6.1.4.1.9.2.2.1.1.8¥GigabitEthernet0/2:himitsu@172.16.0.32
MaxBytes[gi0-2-bps]: 193750000
Title[gi0-2-bps]: lansw01:  GigabitEthernet0/2 bps
PageTop[gi0-2-bps]: <H1>lansw01:  GigabitEthernet0/2 bps</H1>
Options[gi0-2-bps]: gauge,growright

Target[gi0-2-pps]: ifInUcastPkts¥FastEthernet0/2&ifOutUcastPkts¥FastEthernet0/2:himitsu@172.16.0.32
MaxBytes[gi0-2-pps]: 5000000
Title[gi0-2-pps]: lansw01:  GigabitEthernet0/2 pps
PageTop[gi0-2-pps]: <H1>lansw01:  GigabitEthernet0/2 pps</H1>
Options[gi0-2-pps]: growright

#####
# lansw01 bps/pps config – lansw01-if.cfg end
###
```


機能実装 – トラフィック監視
config file – discards/errors

```
#####
# lansw01 discards/errors config - lansw01-err.cfg
###
WorkDir: /usr/local/mrtg/data/lansw01/
IconDir: /mrtg-icons/
Withpeak[_]: wmy

Forks: 4

Target[fa0-1-discards]: ifInDiscards¥FastEthernet0/1&ifOutDiscards¥FastEthernet0/1FastEthernet0/1:himitsu@172.16.0.32
MaxBytes[fa0-1-discards]:  500000
Title[fa0-1-discards]: lansw01:  FastEthernet0/1 discards
PageTop[fa0-1-discards]: <H1>lansw01:  FastEthernet0/1 discards</H1>
Options[gi0-1-discards]: gauge,growright

Target[fa0-1-errors]: ifInErrors¥FastEthernet0/1&ifOutErrors¥FastEthernet0/1:himitsu@172.16.0.32
MaxBytes[fa0-1-errors]: 500000
Title[fa0-1-errors]: lansw01:  FastEthernet0/1 errors
PageTop[fa0-1-errors]: <H1>lansw01:  FastEthernet0/1 errors</H1>
Options[fa0-1-errors]: growright

【中略】

Target[gi0-1-discards]: ifInDiscards¥GigabitEthernet0/1&ifOutDiscards¥GigabitEthernet0/1:himitsu@172.16.0.32
MaxBytes[gi0-1-discards]: 5000000
Title[gi0-1-discards]: lansw01:  GigabitEthernet0/1 discards
PageTop[gi0-1-discards]: <H1>lansw01:  GigabitEthernet0/1 discards</H1>
Options[gi0-1-discards]: gauge,growright

Target[gi0-1-errors]: ifInErrors¥FastEthernet0/1&ifOutErrors¥FastEthernet0/1:himitsu@172.16.0.32
MaxBytes[gi0-1-errors]: 5000000
Title[gi0-1-errors]: lansw01:  GigabitEthernet0/1 errors
PageTop[gi0-1-errors]: <H1>lansw01:  GigabitEthernet0/1 errors</H1>
Options[gi0-1-errors]: growright
```

実装検討2 – トラフィック監視
config file – discards/errors (続き)

```
Target[gi0-2-discards]: ifInDiscards¥GigabitEthernet0/2&ifOutDiscards¥GigabitEthernet0/2:himitsu@172.16.0.32
MaxBytes[gi0-2-discards]: 5000000
Title[gi0-2-discards]: lansw01:  GigabitEthernet0/2 discards
PageTop[gi0-2-discards]: <H1>lansw01:  GigabitEthernet0/2 discards</H1>
Options[gi0-2-discards]: gauge,growright

Target[gi0-2-errors]: ifInErrors¥FastEthernet0/2&ifOutErrors¥FastEthernet0/2:himitsu@172.16.0.32
MaxBytes[gi0-2-errors]: 5000000
Title[gi0-2-errors]: lansw01:  GigabitEthernet0/2 errors
PageTop[gi0-2-errors]: <H1>lansw01:  GigabitEthernet0/2 errors</H1>
Options[gi0-2-errors]: growright

#####
# lansw01 discards/errors config - lansw01-err.cfg end
###
```

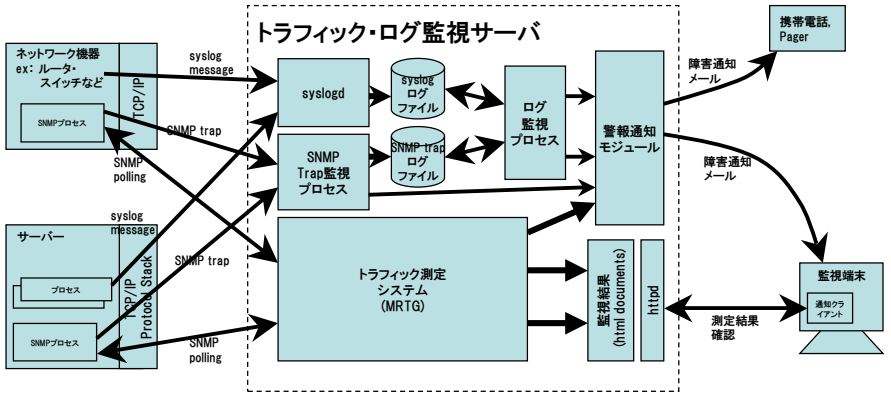

実装検討2 – トラフィック監視
パフォーマンス調整のTIPS

- 測定項目数
  - (bbsw01(8GbE)+lanswXX(48FE+2GbE)*4+FW(2FE)+extgw(2FE))*4 = 212 * 4 = 848項目!
  - すべての計測を同時に実施した場合、オーバーロードとなる可能性が高い
- 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。
  - 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

実装検討2 – トラフィック監視
crontab – mon1

```
####
# crontab mrtg@log1
##

# bbsw01 mrtg
0-59/5 * * * * /usr/local/mrtg/bin/mrtg /usr/local/mrtg/conf/bbsw01-if.cfg > /dev/null 2>&1
2-59/5 * * * * /usr/local/mrtg/bin/mrtg /usr/local/mrtg/conf/bbsw01-err.cfg > /dev/null 2>&1

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

# extgw01 mrtg
2-59/5 * * * * /usr/local/mrtg/bin/mrtg /usr/local/mrtg/conf/extgw01-if.cfg > /dev/null 2>&1
4-59/5 * * * * /usr/local/mrtg/bin/mrtg /usr/local/mrtg/conf/extgw01-err.cfg > /dev/null 2>&1

# lansw01 mrtg
0-59/5 * * * * /usr/local/mrtg/bin/mrtg /usr/local/mrtg/conf/lansw01-if.cfg > /dev/null 2>&1
2-59/5 * * * * /usr/local/mrtg/bin/mrtg /usr/local/mrtg/conf/lansw01-err.cfg > /dev/null 2>&1

# lansw10 mrtg
1-59/5 * * * * /usr/local/mrtg/bin/mrtg /usr/local/mrtg/conf/lansw10-if.cfg > /dev/null 2>&1
3-59/5 * * * * /usr/local/mrtg/bin/mrtg /usr/local/mrtg/conf/lansw10-err.cfg > /dev/null 2>&1

# lansw01 mrtg
2-59/5 * * * * /usr/local/mrtg/bin/mrtg /usr/local/mrtg/conf/lansw20-if.cfg > /dev/null 2>&1
4-59/5 * * * * /usr/local/mrtg/bin/mrtg /usr/local/mrtg/conf/lansw20-err.cfg > /dev/null 2>&1

# lansw01 mrtg
3-59/5 * * * * /usr/local/mrtg/bin/mrtg /usr/local/mrtg/conf/lansw30-if.cfg > /dev/null 2>&1
0-59/5 * * * * /usr/local/mrtg/bin/mrtg /usr/local/mrtg/conf/lansw30-err.cfg > /dev/null 2>&1

####
# crontab mrtg@log1 end
##
```


監視システムのモデル -
トラフィック・ログ監視サーバ



Index

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

TIPS – ping編

- 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い
  - 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packet size=1400byte, count=1000以上、送出Interval=40msの設定で試験しています
  - スイッチのDuplexミスマッチもこれなら検知可能
- Internet経由の監視は タイムアウト＞1000msec
  - 22時～26時ぐらいの最繁時間帯は特に揺らぎが大きいため、マージンをとらないと誤検出が増える

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

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

TIPS - BB編3

- Big Brotherの高速化：fping + fping.sh
  - `http://www.fping.org/`
  - `http://www.deadcat.net/cgi-bin/download.pl?section=1&file=fping.sh`
  - fpingによりping試験を高速化
    - bbdef.sh内にて“CONNTEST=FALSE”としてBBのping試験を停止する必要あり
- 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となっているために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
    - もしくは容量をアカウンティングを停止

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: 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_l) 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

- では、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にするのはちょっともったいない
  - 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

ご清聴ありがとうございました。

追加資料1：SNMP

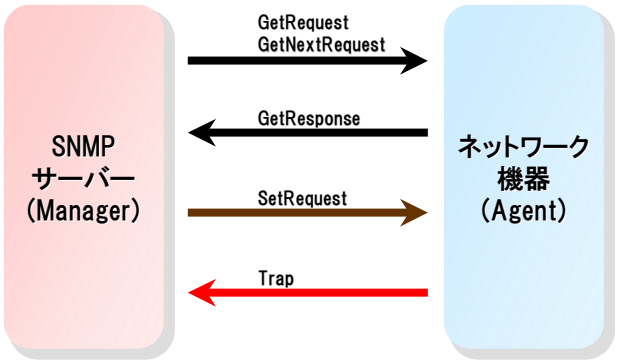
SNMP : Simple Network Management Protocol

- 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ーに対してイベントを転送する

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ーを要求する
- 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

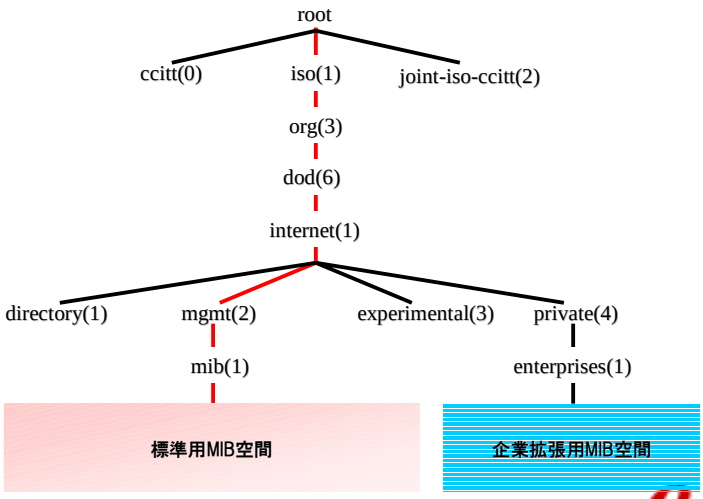
SNMP Message Hundling



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



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
```

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 : ifInUcastPktsa
  - 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

SNMP OID/MIB Symbols - CISCO Enterprise MIB

- CISCO Enterprise MIB
  - locIfInBitsSec = 1.3.6.1.4.1.9.2.2.1.1.6
  - locIfInPktsSec = 1.3.6.1.4.1.9.2.2.1.1.7
  - locIfOutBitsSec = 1.3.6.1.4.1.9.2.2.1.1.8
  - locIfOutPktsSec = 1.3.6.1.4.1.9.2.2.1.1.9
  - locIfInRunts = 1.3.6.1.4.1.9.2.2.1.1.10
  - locIfInGiants = 1.3.6.1.4.1.9.2.2.1.1.11
  - locIfInCRC = 1.3.6.1.4.1.9.2.2.1.1.12
  - locIfInFrame = 1.3.6.1.4.1.9.2.2.1.1.13
  - locIfInOverrun = 1.3.6.1.4.1.9.2.2.1.1.14
  - locIfInIgnored = 1.3.6.1.4.1.9.2.2.1.1.15
  - locIfInAbort = 1.3.6.1.4.1.9.2.2.1.1.16
  - locIfResets = 1.3.6.1.4.1.9.2.2.1.1.17
  - locIfRestarts = 1.3.6.1.4.1.9.2.2.1.1.18
  - locIfLoad = 1.3.6.1.4.1.9.2.2.1.1.24
    - OID/MIBを使用する際には、Interfaceに対して"bandwidth"定義が必要
  - locIfCollisions = 1.3.6.1.4.1.9.2.2.1.1.25
  - locIfInputQueueDrops = 1.3.6.1.4.1.9.2.2.1.1.26
  - locIfOutputQueueDrops = 1.3.6.1.4.1.9.2.2.1.1.27
  - avgBusy1 = 1.3.6.1.4.1.9.2.1.57 (CPU usage)
  - avgBusy5 = 1.3.6.1.4.1.9.2.1.58 (CPU usage)

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

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
    - ./configure –with-libwrap=…
- 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, …)

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Net-SNMPコマンド例(V 4.2.2)

- `$ 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

追加資料2：
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.hogehoge.com`
  - `Target[gw1-err-3]: ifInErrors.3&ifOutErrors.3:himitsu@gw1.hogehoge.com`
  - `Target[gw1-if-1]: -/10.0.0.101:himitsu@gw1.hogehoge.com`
  - `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.hogehoge.com
  - gw1.hogehoge.com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.hogehoge.com
  - 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.hogehoge.com
  - gw1.hogehoge.com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.hogehoge.com
  - 上の例のOID指定

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.hogehoge.com`
  - gw1.hogehoge.com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.hogehoge.com`
  - 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.hogehoge.com
  - gw1.hogehoge.com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.hogehoge.com
  - 例7のOIDパターン

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.hogehoge.com
    Target[sw-2-11]: -#2/11:himitsu@sw1.hogehoge.com
    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.hogehoge.com
    Target[sw-3-7]: ifInErrors#3/7&ifOutErrors#3/7:himitsu@sw1.hogehoge.com

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.hogehoge.com
Target[sw-2-11]: -¥to_web1:himitsu@sw1.hogehoge.com
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.h
ogehoge.com
Target[sw-3-7]:
ifInErrors¥to_web1&ifOutErrors¥to_web1:himitsu@sw1.hogehoge.com
```


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.hogehoge.com`
      `PING ftp.hogehoge.com (192.168.101.238): 56 data bytes`
      `.`
      `--- ftp.hogehoge.com 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

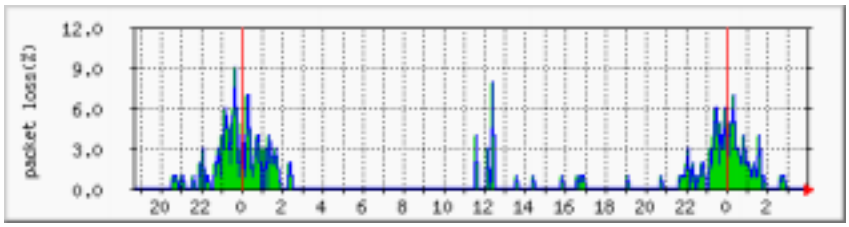
- pingの出力結果からpacket lossのデータを抽出
  - `100 packets transmitted, 95 packets received, 5% packet loss`

```
# 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.hogehoge.com
5
5
0
/usr/local/bin/check_loss.sh ftp.hogehoge.com
#
```

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.hogehoge.com`
Title[pingloss-ftp]: ftp.hogehoge.com - pingloss
MaxBytes[pingloss-ftp]: 100
PageTop[pingloss-ftp]: <H1> ftp.hogehoge.com - 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:Open Source/Free software link

- OSDN (Open Source Development Network)
  - http://www.osdn.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/

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

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

ツールURL集1

- AWARE
  - http://www.elegant-software.com/software/aware/
- Big Brother
  - http://bb4.com/
  - Extensions Archive: http://www.deadcat.net/
  - Big Sister(clone of BB):
    - http://bigsister.sourceforge.net/
- Demarc PureSecure
  - http://demarc.com/
- Expect
  - http://expect.nist.gov/
- fping
  - http://www.fping.com/
- Ganglia
  - http://ganglia.sourceforge.net/
- IPTraf
  - http://cebu.mozcom.com/riker/iptraf/index.html

ツールURL集2

- Lire
  - http://www.logreport.org/
- LogSentry
  - http://www.psionic.com/products/logsentry.html
- MRTG
  - http://ee-staff.ethz.ch/~oetiker/webtools/mrtg/
- mon
  - http://www.kernel.org/software/mon
- monit
  - http://www.tildeslash.com/monit/
- moodss
  - http://jfontain.free.fr/moodss/
- Nagios (NetSaint)
  - http://www.nagios.org/
  - http://www.netsaint.org/
- NeTraMet
  - http://www.auckland.ac.nz/net/Accounting/ntm.Release.note.html

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
- ntop
  - http://www-serra.unipi.it/~ntop/
- 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/
  - RRDTools翻訳Project
    - http://www.ofug.net/~gima/RRDtool/
  - Frontend - Cacti
    - http://www.raxnet.net/products/cacti/
  - Frontend - CRICKET
    - http://cricket.sourceforge.net/
  - Frontend - NRG
    - http://nrg.hep.wisc.edu/
  - Frontend - ORCA
    - http://www.orcaware.com/orca/
  - Frontend - Remstats
    - http://remstats.crc.ca/remstats/release/
  - Frontend – RRDBrowse
    - http://home.support.nl/~tommy/rrdbrowse/
  - Frontend – SmokePing
    - http://people.ee.ethz.ch/~oetiker/webtools/smokeping/

ツールURL集4

- RRDTool
  - http://ee-staff.ethz.ch/~oetiker/webtools/rrdtool/
  - RRDTools翻訳Project
    - http://www.ofug.net/~gima/RRDtool/
  - Frontend - Cacti
    - http://www.raxnet.net/products/cacti/
  - Frontend - CRICKET
    - http://cricket.sourceforge.net/
  - Frontend - NRG
    - http://nrg.hep.wisc.edu/
  - Frontend - ORCA
    - http://www.orcaware.com/orca/
  - Frontend - Remstats
    - http://remstats.crc.ca/remstats/release/
  - Frontend – RRDBrowse
    - http://home.support.nl/~tommy/rrdbrowse/
  - Frontend – SmokePing
    - http://people.ee.ethz.ch/~oetiker/webtools/smokeping/

ツールURL集5

- Scotty
  - http://wwwhome.cs.utwente.nl/~schoenw/scotty/
- seafelt
  - http://seafelt.unicity.com.au/
- shepherd
  - http://atrey.karlin.mff.cuni.cz/~clock/twibright/shepherd/
- sing
  - http://sourceforge.net/projects/sing
- snort
  - http://www.snort.org/
- SPONG
  - http://spong.sourceforge.net/
- ssh
  - http://www.ssh.com/
- statscout
  - http://www.statscout.com
- SWATCH
  - http://www.oit.ucsb.edu/~eta/swatch/

ツールURL集6

- syslog-ng
  - http://www.balabit.hu/products/syslog-ng/
  - php-syslog-ng
    - http://www.vermeer.org/syslog/
- SysOrb
  - http://www.sysorb.com
- Treno
  - http://www.psc.edu/~pscnoc/treno.html
  - Experimental TCP Implementations
    http://www.psc.edu/networking/tcp.html
- 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/
- EXP.（旧名：「働け!! linux!!」）
  - http://www.tujige.info/manage/index.html
- いちばん近道なLinuxマスター術
  - http://www.zdnet.co.jp/help/howto/linux/0007master/
  - 「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/

参考：URL集2

- 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

参考：URL集3

- Cisco FAQs
  - http://www.cisco.com/public/technotes/serv_tips.shtml
- Cisco device SNMP configuration tips
  - http://www.cisco.com/warp/public/477/SNMP/index.html

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
- LBNL's Network Research Group
  - http://ee.lbl.gov/
    - tcpdump, libpcap , arpwatch, traceroute, pathchar