ネットワーク監視
～ 考え方と
オープンソースソフトウェアによる実践 ～

2002/12/4

イー・アクセス株式会社　矢萩茂樹
(yahagi@eaccess.net)

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.

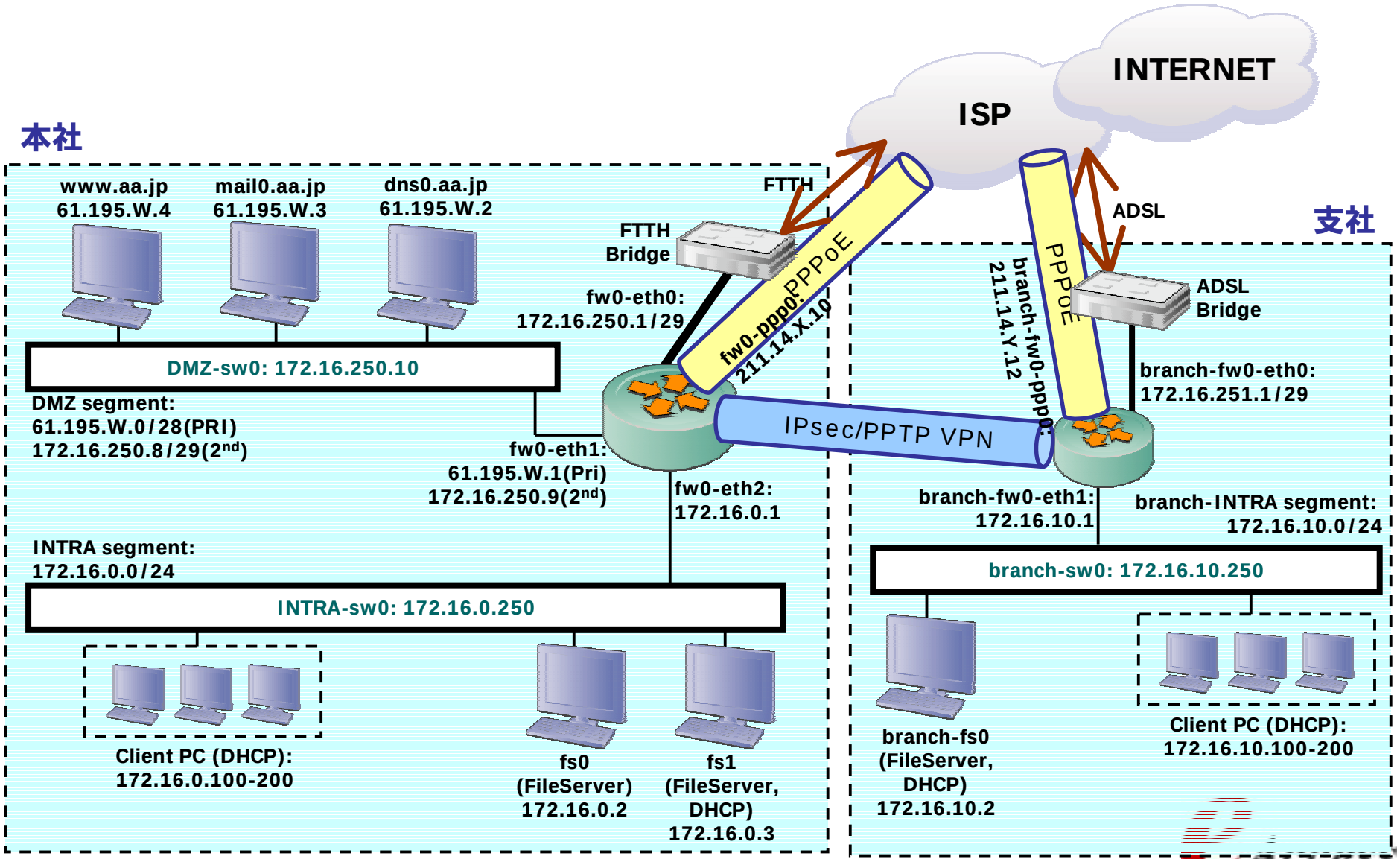
- Origins: Bruce Perens wrote the first draft of this document as "The Debian Free Software Guidelines", and refined it using the comments of the Debian developers in a month-long e-mail conference in June, 1997. He removed the Debian-specific references from the document to create the "Open Source Definition."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

- 取り上げるのは以下のツール
  - 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
  - syslogd
  - MRTG

監視対象:aa.jp – ネットワーク構成



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

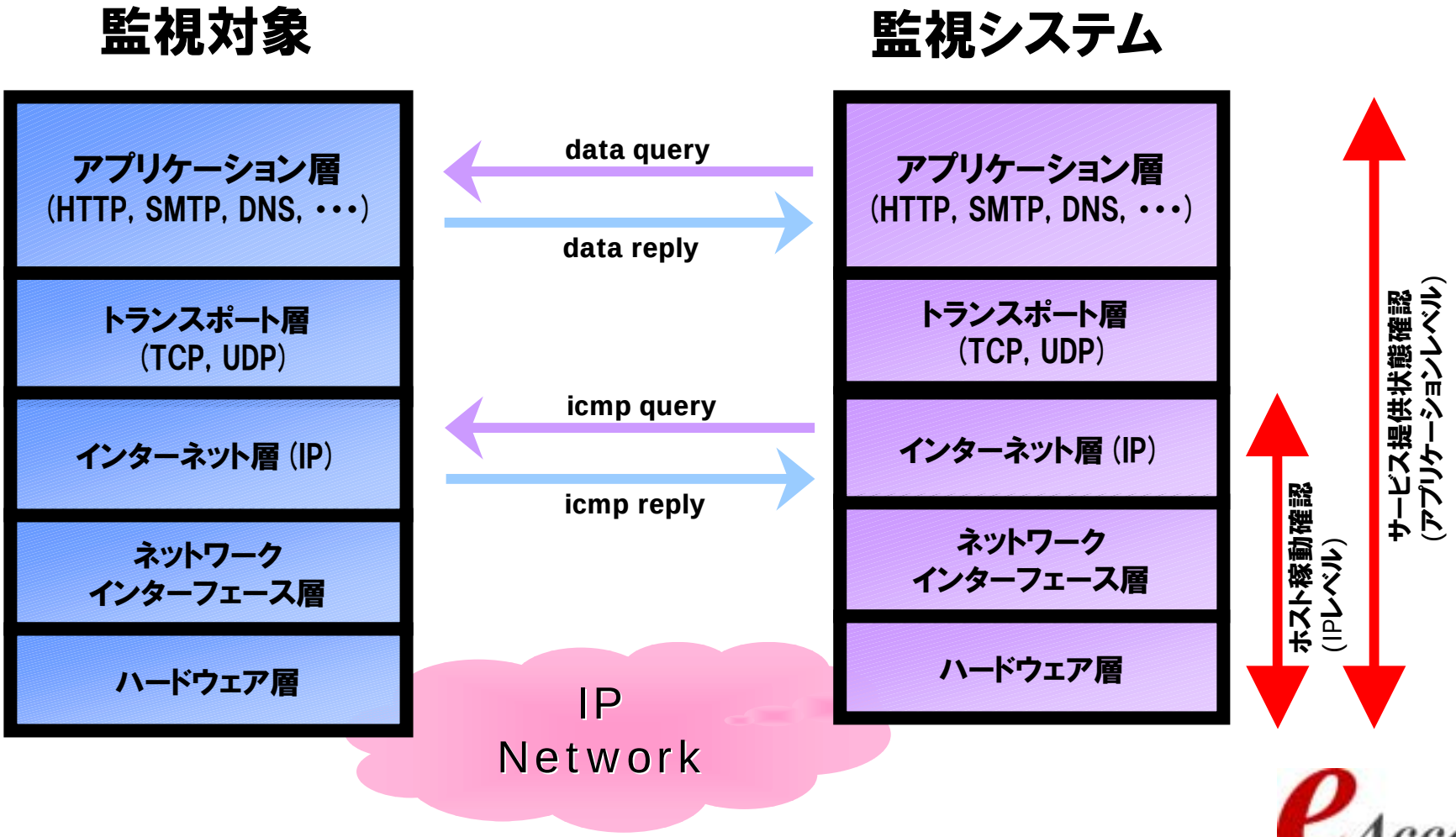
要件定義 – 概要2

- 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

- 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
    - VPN部分を含む
- 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

- 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アクセスでネットワーク側対応とする

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

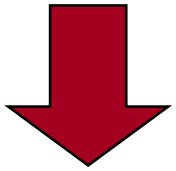
- 障害履歴管理
  - 監視サーバにて、発生した障害の履歴管理機能を行う
  - 障害発生／復旧時間を記録し、過去に遡って障害履歴を追跡可能とする
  - 障害履歴を日間・週間・月間・年間の各スパンにてチェック可能とすることで、障害の発生頻度／発生傾向の追跡解析をサポートする機能が欲しい。
    - MRTGでのDaily/Weekly/Monthly/Yearly表示のような経過サマリー画面

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、将来案件とする

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

用件定義 – オープンソースでどこまでできるか

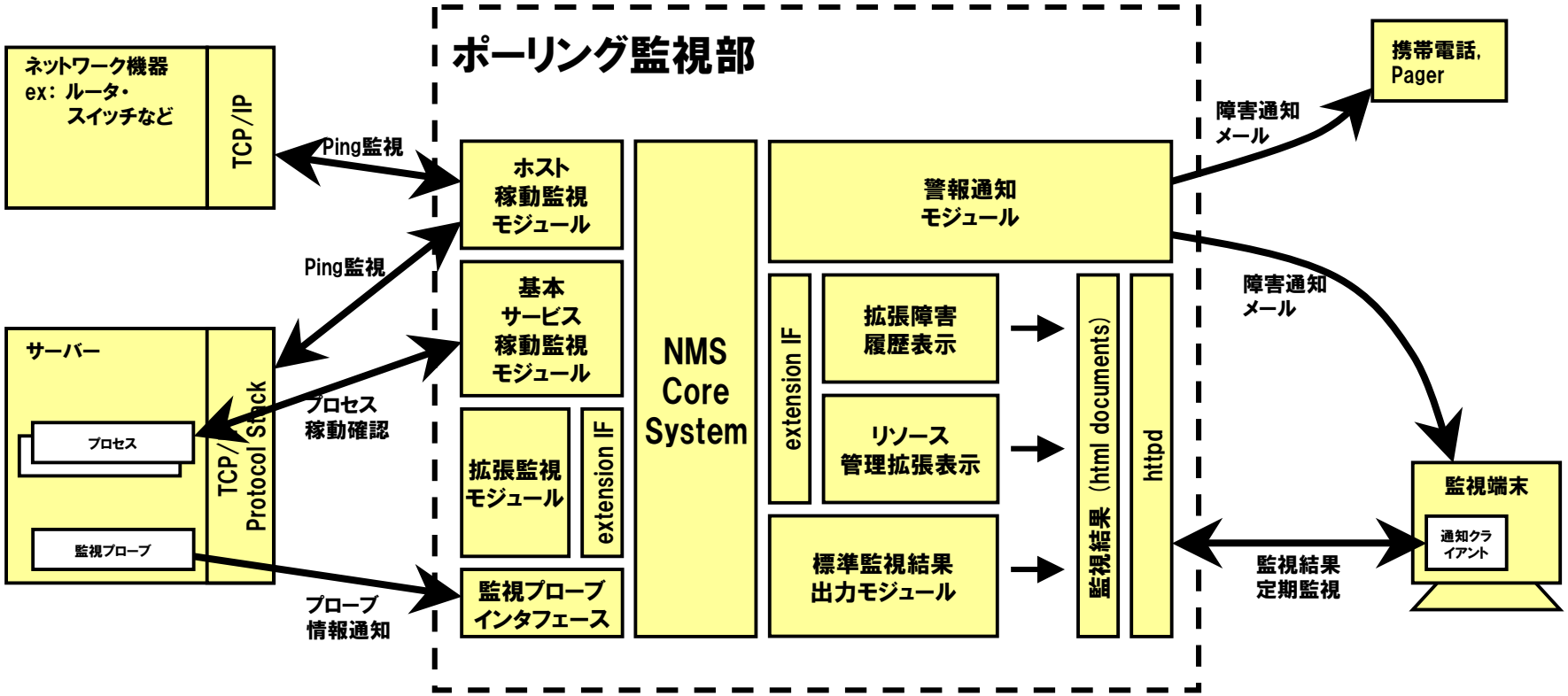
- 本チュートリアルでは、エンタープライズネットワークを仮想設定し、それをオープンソースソフトウェアベースの監視システムにて構築することを目的とする

- 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
  - syslogd
  - MRTG

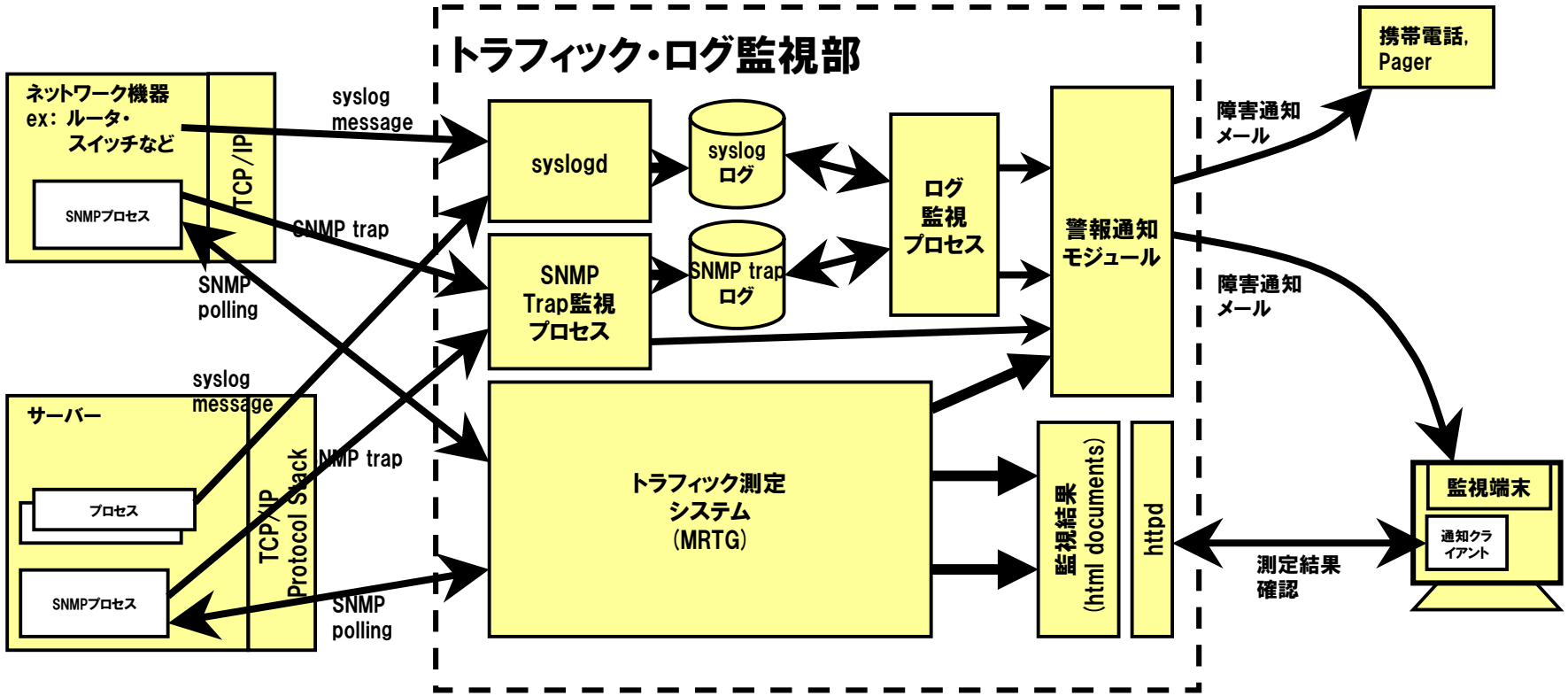
用件定義 – 構築方針

- 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
  - ポーリング監視
    - 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・ログ管理
    - 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 – ポーリング監視

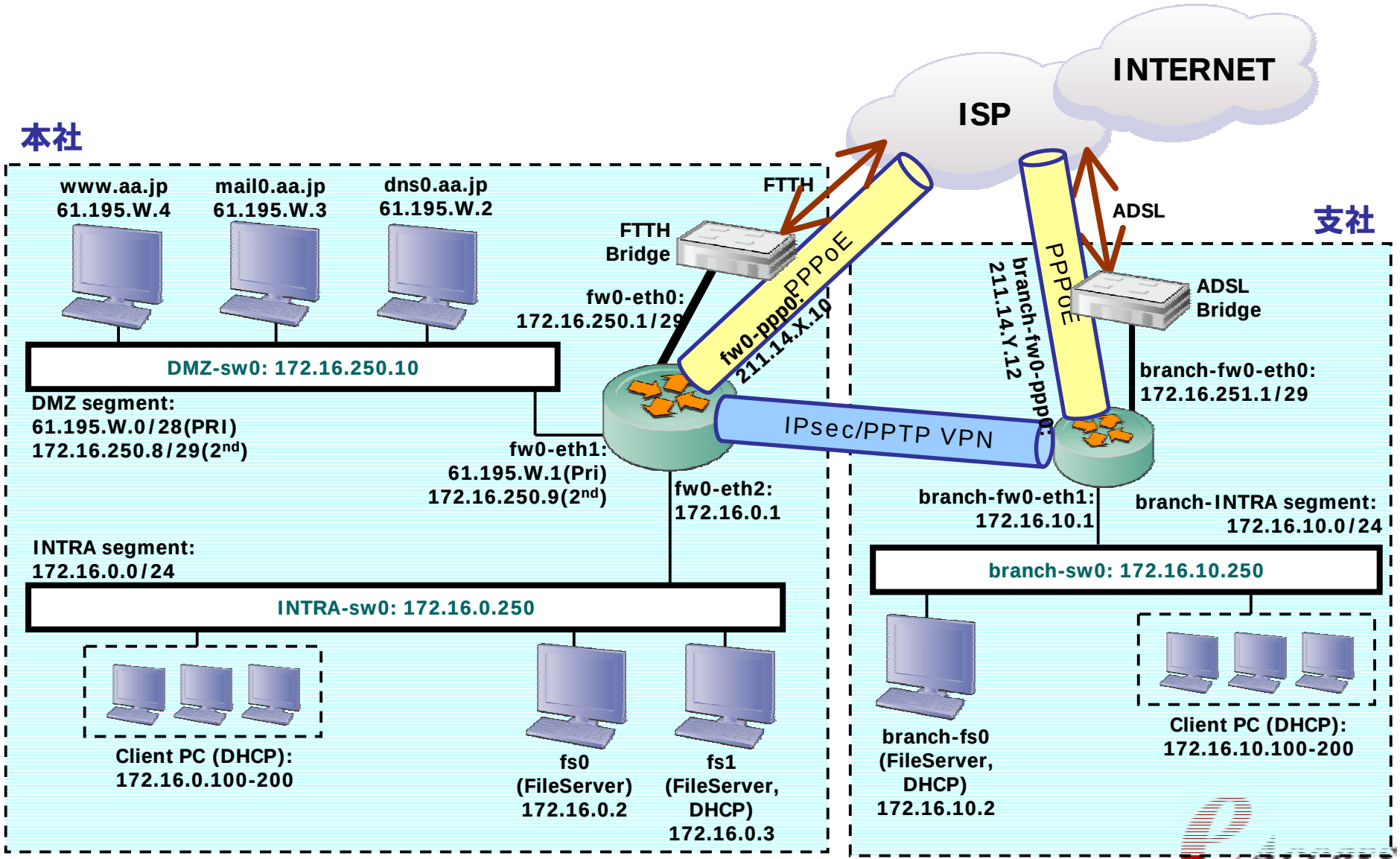


監視システムのモデル – トラフィック・ログ監視



Index

監視対象:aa.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・支社とも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ファイヤーウォールを経由する
- ISPとの接続は本社はFTTH、支社はADSLを使用。モデムはブリッジモードとして使用。ファイヤーウォールからPPPoEにてリンクレイヤ(L2)接続を行う
- 本社支社ともWANアドレスは固定アドレス(/32)をISPより割当。本社はこのほかにSub Allocation Block（61.195.W.0/28）の割当を受ける

監視対象 - 概要2

- 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
- 本社と支社間はファイヤーウォールにてIPsec VPNで接続をしている
- 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
- 本社ー支社間はVPN経路を選択。その他のインターネット接続はここの回線の上流ISP経路を選択

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	61.195.W.0/28	ISP割当グローバル
	172.16.250.8/29	DMZ管理用
本社イントラセグメント	172.16.0.0/24	イントラ向けプライベート
本社WANセグメント	172.16.250.0/29	WAN機器チェック用プライベート
	211.14.X.10/32	ISP割当グローバル
支社WANセグメント	172.16.251.0/29	WAN機器チェック用プライベート
	211.14.Y.12/32	ISP割当グローバル
支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

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
    - inetdは使用しない
    - 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: dns0.aa.jp（61.195.W.2）
    - Secondary: mail0.aa.jp（61.195.W.3）
  - メール設定
    - Primary: mail0.aa.jp
    - Secondary: dns0.aa.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

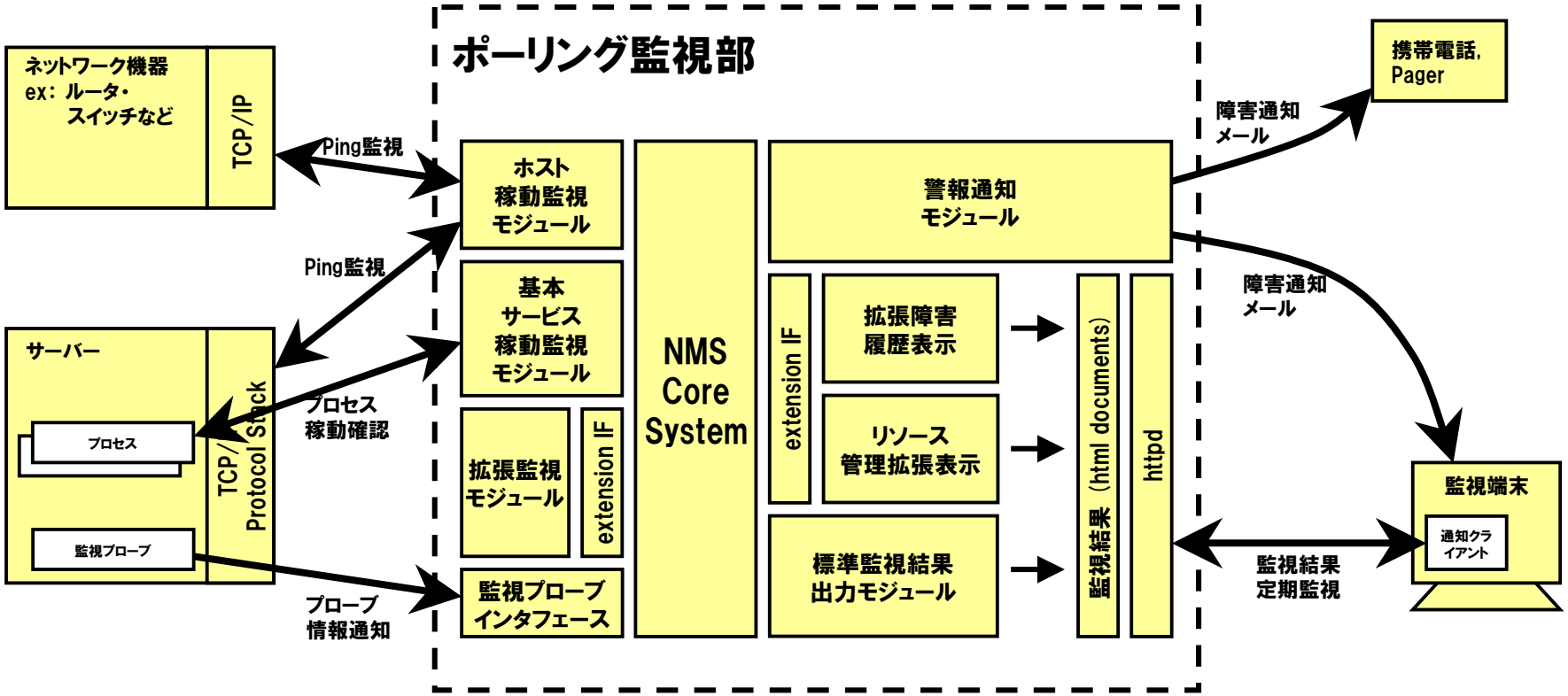
セグメント	IP address	ホスト名称	URL	提供サービス
本社DMZセグメント (61.195.W.0/28) (172.16.250.8/29)	61.195.W.1	fw0-eth1	---	firewall
	61.195.W.2	dns0.aa.jp	dns0.aa.jp	dns, smtp, ssh
	61.195.W.3	mail0.aa.jp	mail0.aa.jp	dns, smtp, pop, ssh
	61.195.W.4	www.aa.jp	www.aa.jp	http, ftp, ssh
	172.16.250.9	fw0-eth1-2	---	firewall
	172.16.250.10	dmz-sw0	---	switch
本社イントラセグメント (172.16.0.0/24)	172.16.0.1	fw0-eth2	---	firewall
	172.16.0.2	fs0	fs0.hq.aa.jp	FileServer
	172.16.0.3	fs1	fs1.hq.aa.jp	FileServer, DHCP
	172.16.0.250	intra-sw0	---	switch
本社WANセグメント (172.16.250.0/28) (211.14.X.10/32)	172.16.250.1	fw0-eth0	---	firewall
	211.14.X.10	fw0-ppp0	---	firewall
支社WANセグメント (172.16.250.16/28) (211.14.Y.12/32)	172.16.250.17	branch-fw0-eth0	---	firewall
	211.14.Y.12	branch-fw0-ppp0	---	firewall
支社イントラセグメント (172.16.10.0/24)	172.16.10.1	branch-fw0-eth0	---	firewall
	172.16.10.2	branch-fs0	fs0.branch.aa.jp	FileServer, DHCP
	172.16.10.250	branch-sw0	---	switch

監視対象分析 – 監視時間と通知先

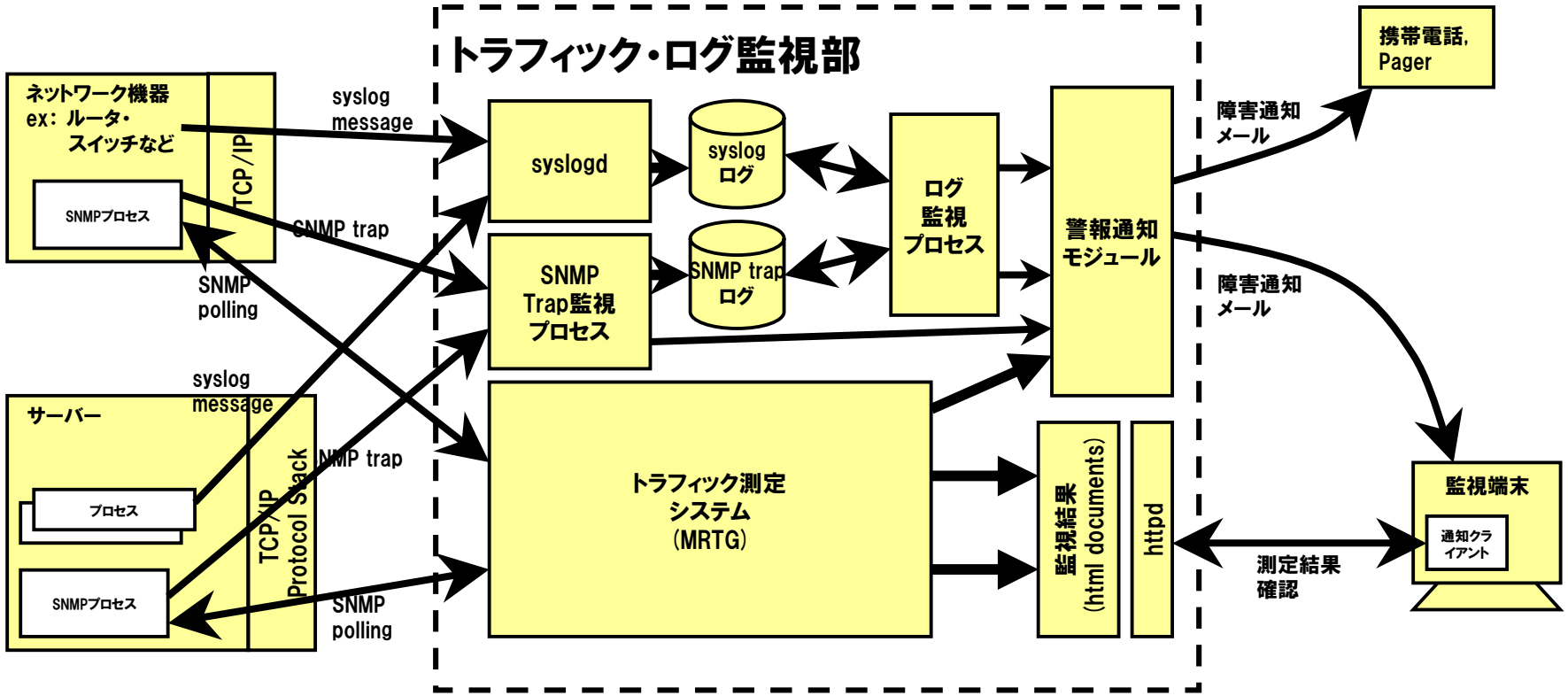
- 全ての機器の障害情報は障害受付窓口であるalert@aa.jpに通知
- 独自のイントラ系と支社ネットワークの部分については以下の監視・障害通知ポリシーを適用
  - 本社ファイルサーバ fs0, fs1 ：
    - 毎日午前4時から6時の間でデイリーバッチ処理が走り、高負荷となることから監視を停止。監視省力化
    - この機械の障害時には担当窓口：intra@aa.jpにも通知
  - 支社のファイルサーバ branch-fs0：
    - 監視業務の省力化のために 平日の7時から24時までの時間帯のみ障害通知を行う
    - この機械の障害時には担当窓口：intra@aa.jp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.aa.jpへの通知を追加

index

監視システムのモデル – ポーリング監視



監視システムのモデル – トラフィック・ログ監視



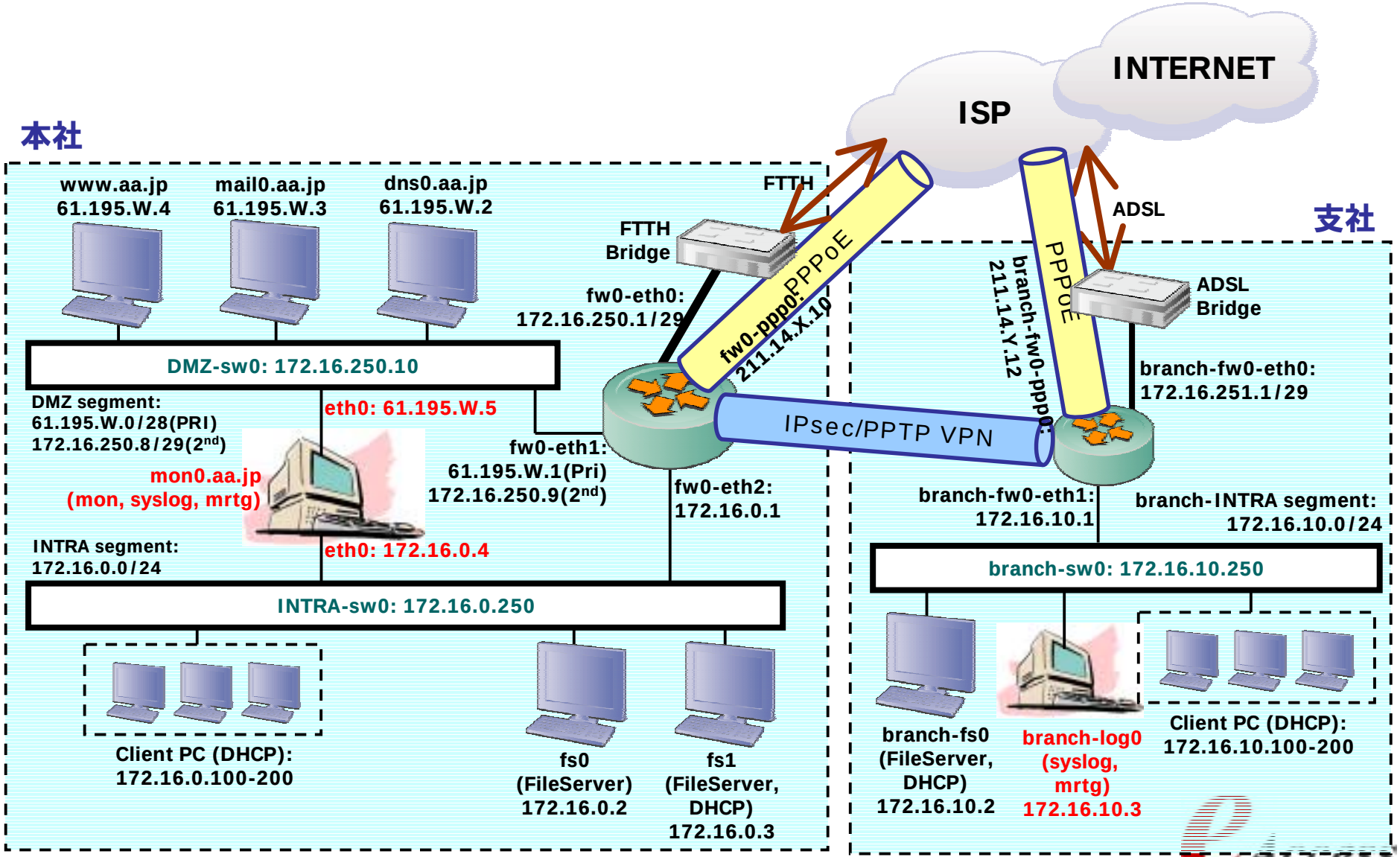
実装検討1 – 監視サーバの設置ポイント

- ポーリング監視部
  - 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
    - DMZとイントラに直接接続する
    - セキュリティーホールになる可能性がある。外部から直接たたけるとまずいことから、ファイヤーウォール越えの監視はDMZ経由ではなく、イントラセグメントのプライベートアドレス経由で行う
      - よって、このサーバのデフォルトはイントラの足経由
  - 設置場所：
    - 本社DMZセグメント：IP=61.195.W.5/28
    - 本社イントラセグメント： IP=172.16.0.4/24

実装検討1 – 監視サーバの設置ポイント

- トラフィック・ログ管理部
  - 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、プライベートブロックに設置する
    - 逆に必要性がなければ、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
    - プライベートセグメントに設置することで、論理構成的にこれらの妨害から防御可能となる
    - ログサーバは機器障害時のログを取得するために設置する。よって外部影響を受けずらい直近に設置することがのぞましい。
      - 支社セグメントにも設置する
  - 設置場所：
    - 本社イントラセグメント：IP=172.16.0.4/24
    - 支社イントラセグメント：IP=172.16.10.3/24

監視対象:aa.jp – 監視サーバの配置

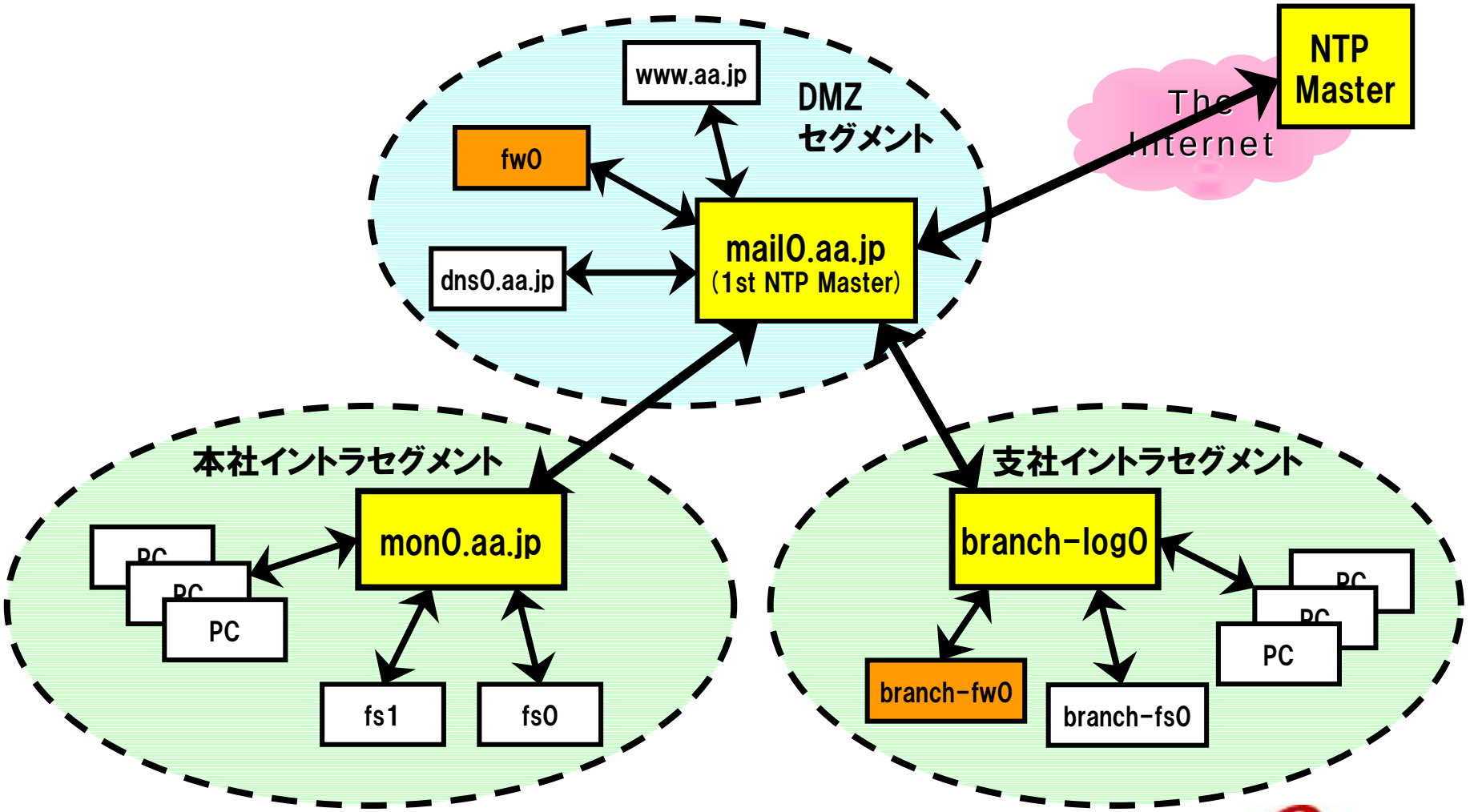


実装検討1 - 時間同期

- 絶対基準は時間
  - 全ての機器にて時間同期していることが必要
    - 問題解決をするためには、正確なイベントの発生順番追跡が必須。

    → システム時間の同期が必要となる
  - 基準時刻とタイムゾーンの設定が必要
  - 日本ゾーンは表記：JSTで、国際基準時間：UTCに対して9時間先行
- 時間同期の手段：NTP (Network Time Protocol) サーバを基準にネットワーク機器を同期させる
  - 対象装置：ルータ・スイッチ・サーバなど、全ての機器
  - NTPマスターはGlobalに接続されていることが条件
    - ルータ・スイッチ・FWでNTPサーバ機能持つものがある場合にはまかせるのが一番、楽。
    - しかし、高価な装置に偏る
  - イントラセグメントではGlobal/Privateの両方に接続しているノードがNTPサーバー
  - 今回はmail0.aa.jpを社内NTPマスターサーバーとして、監視サーバを経由するNTPリンクにて検討する

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
  - 2002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/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

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

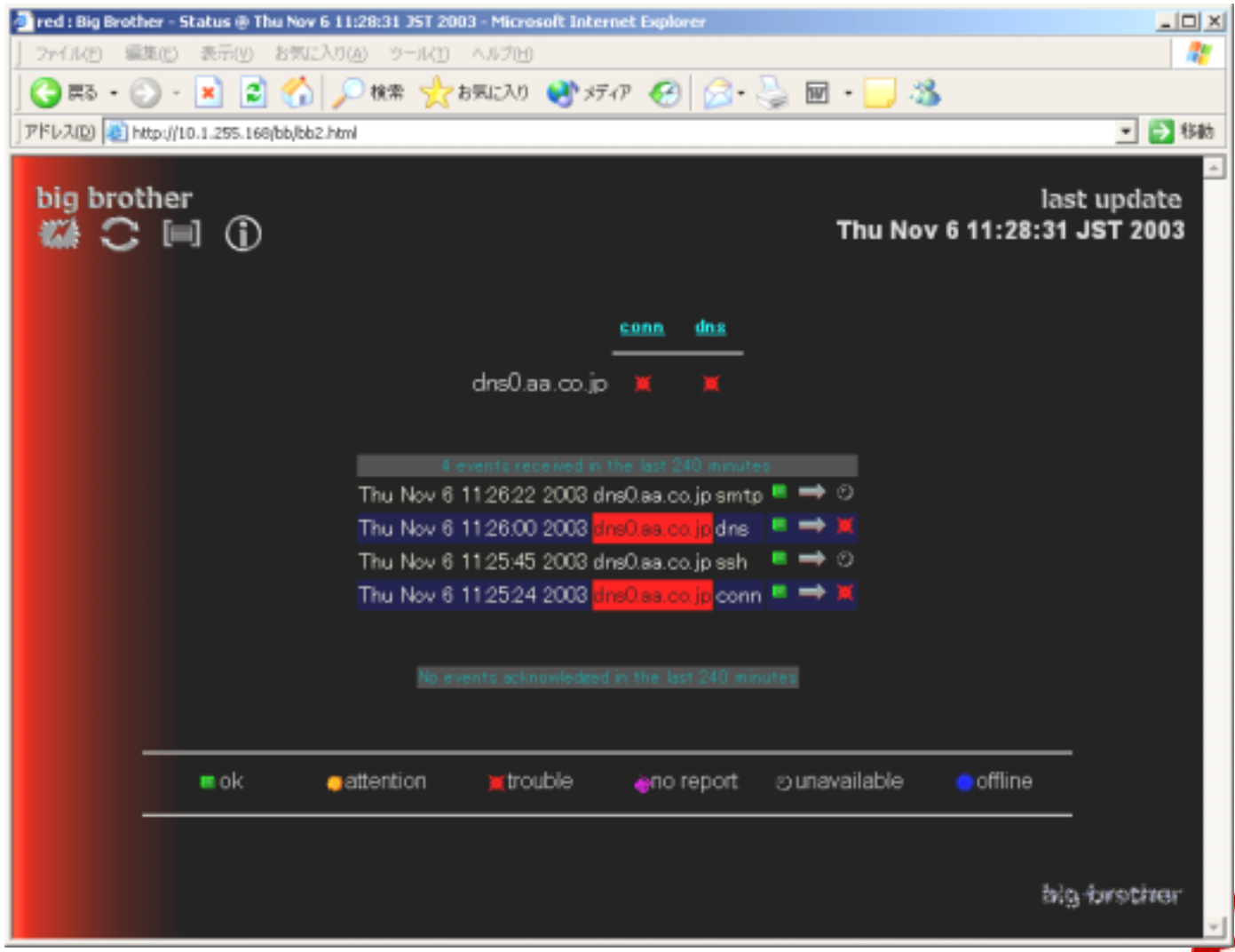
実装検討1 – 状態監視ツール - Big Brother 続き

- 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（?!）,・・・

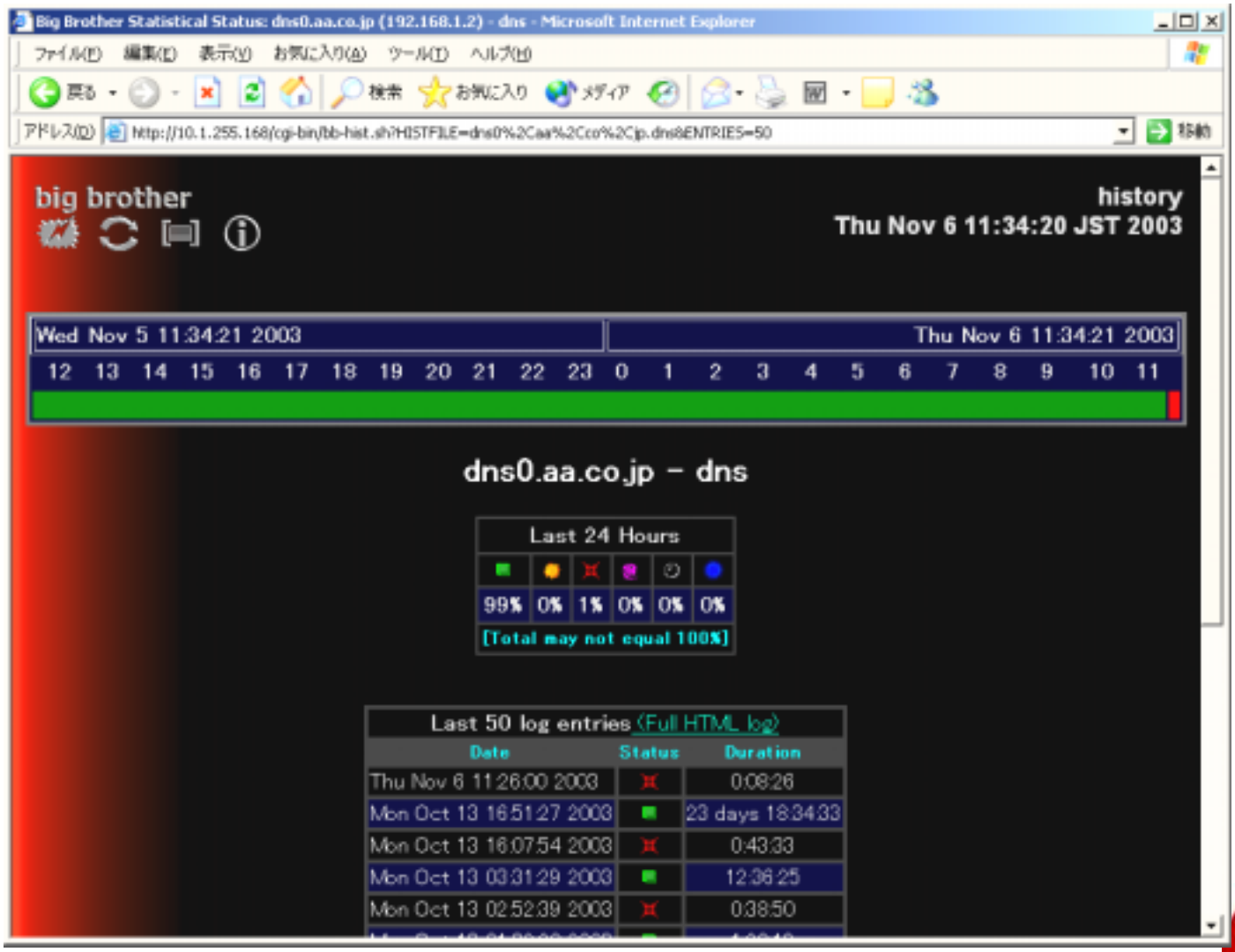
実装検討1 – BB：監視画面（TOP）

実装検討1 – BB:監視画面 (sub)

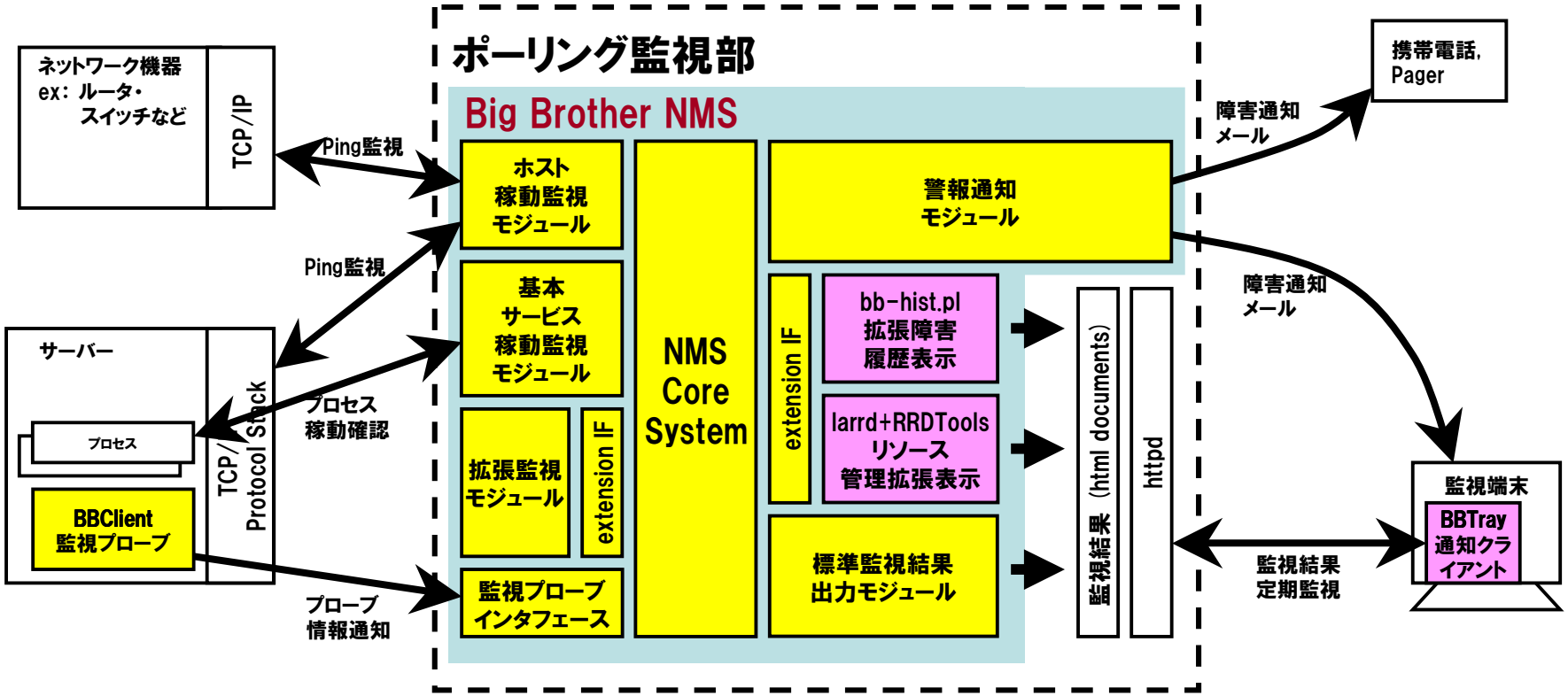
実装検討1 – BB:アラートサマリ



実装検討1 – BB:ヒストリ画面



監視システムのモデル － ポーリング監視部



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-warnsetup.cfg： 障害通知動作定義ファイル
  - $BBHOME/etc/bb-warnrules.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： BBサーバアクセス規制設定ファイル

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
  - 規制サービス確認

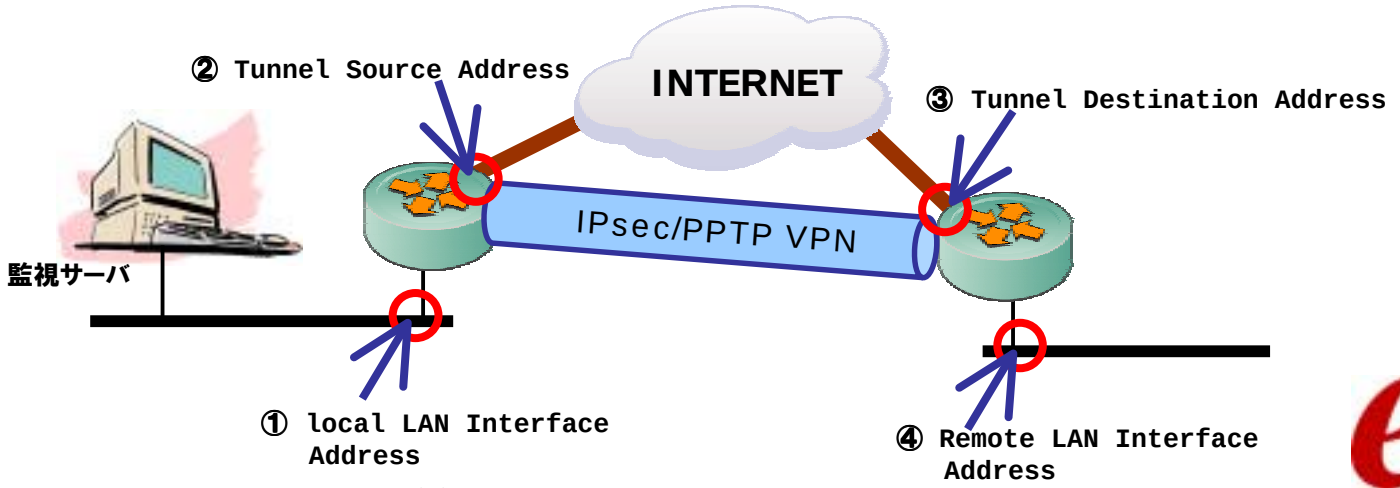
セグメント	IP address	監視名称	URL	提供サービス	規制サービス
本社DMZセグメント (61.195.W.0/28) (172.16.250.8/29)	61.195.W.1	fw0-eth1	---	firewall	
	61.195.W.2	dns0.aa.jp	dns0.aa.jp	dns, smtp, ssh	telnet
	61.195.W.3	mail0.aa.jp	mail0.aa.jp	dns, smtp, pop, ssh	telnet
	61.195.W.4	www.aa.jp	www.aa.jp	http, ftp, ssh	telnet, smtp
	61.195.W.5	mon0-2.aa.jp	---	なし	telnet, smtp
	172.16.250.9	fw0-eth1-2	---	firewall	
	172.16.250.10	dmz-sw0	---	switch	
本社イントラセグメント (172.16.0.0/24)	172.16.0.1	fw0-eth2	---	firewall	
	172.16.0.2	fs0	fs0.hq.aa.jp	FileServer	telnet, smtp
	172.16.0.3	fs1	fs1.hq.aa.jp	FileServer, DHCP	telnet, smtp
	172.16.0.4	mon0.aa.jp	mon0.aa.jp	BB, http, ssh	telnet, smtp
	172.16.0.250	intra-sw0	---	switch	
本社WANセグメント (172.16.250.0/28) (211.14.X.10/32)	172.16.250.1	fw0-eth0	---	firewall	
	211.14.X.10	fw0-ppp0	---	firewall	
支社WANセグメント (172.16.250.16/28) (211.14.Y.12/32)	172.16.250.17	branch-fw0-eth0	---	firewall	
	211.14.Y.12	branch-fw0-ppp0	---	firewall	
支社イントラセグメント (172.16.10.0/24)	172.16.10.1	branch-fw0-eth0	---	firewall	
	172.16.10.2	branch-fs0	fs0.branch.aa.jp	FileServer, DHCP	telnet, smtp
	172.16.10.3	branch-log0	log0.branch.aa.jp	http, ssh	telnet, smtp
	172.16.10.250	branch-sw0	---	switch	

機能実装1 – 監視設定
VPN監視について

- 監視ポイントの設定
  - 以下のポイントをもれなく監視

① Local LAN Interface Address
② Tunnel Source Address
③ Tunnel Destination Address
④ Remote LAN Interface Address

- 注意点
  - ファイヤーウォールはデフォルトでICMPに応答しない
    - ICMP応答可能なネットワークレンジを設定し、監視する



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.aa.jp # BBPAGER BBNET BBDISPLAY http://kansi1/

group-compress <H3><I>aa.jp Servers</I></H3>
192.168.0.2  ns1.aa.jp  # dns ssh !telnet
192.168.0.3  mail.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 Intereface”
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
$
```

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.aa.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

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
## Head Quarters
group-compress <H3><B>DMZ Segment</B></H3>
61.195.W.1    fw0-eth1
61.195.W.2    dns0.aa.jp      # dns smtp ssh !telnet
61.195.W.3    mail0.aa.jp     # dns smtp pop ssh !telnet
61.195.W.4    www.aa.jp       # http://www.aa.jp ftp ssh !telnet !smtp
61.195.W.5    mon0-2.aa.jp    # !telnet !smtp
172.16.250.9  fw0-eth1-2
172.16.250.10 dmz-sw0

group-compress <H3><B>INTRA Segment</B></H3>
172.16.0.1    fw0-eth2
172.16.0.2    fs0             # !telnet !smtp
172.16.0.3    fs1             # !telnet !smtp
172.16.0.4    mon0.aa.jp      # BBDISPLAY BBNET BBPAGER http://mon0.aa.jp/bb/ ssh !telnet !smtp
172.16.0.250  intra-sw0

group-compress <H3><B>WAN Segment</B></H3>
172.16.250.1  fw0-eth0
211.14.X.10   fw0-ppp0

## Branch Office-1
page BRANCH-1 <B>BRANCH-1</B>
group-compress <H3><B>BRANCH WAN/VPN Segment</B></H3>
172.16.250.17 branch-fw0-eth0
211.14.Y.12   branch-fw0-ppp0

group-compress <H3><B>BRANCH INTRA Segment</B></H3>
172.16.10.1    branch-fw0-eth0
172.16.10.2    branch-fs0    # !telnet !smtp
172.16.10.3    branch-log0   # http://log0.branch.aa.jp ssh !telnet !smtp
172.16.10.250  branch-sw0
### end of bb-hosts
```

実装検討1 – 障害通知システム設定
etc/bbwarnsetup.cfg - 1

- Big Brother障害通知システム設定ファイル
  - 障害通知処理のタイミング、通知頻度、タイマーなどの設定を記述
  - ほとんどの設定はデフォルトで良いが、以下の2つについては変更したほうが好ましい

- 障害復旧時の通知設定：pagerecovered
  - 障害復旧時の通知設定。デフォルトはFALSEで行わない
  - 回復時の通知を行う場合には以下のように変更する。
    pagerecovered: TRUE

実装検討1 – 障害通知システム設定
etc/bbwarnsetup.cfg - 2

- 障害通知タイプ設定：pagetype
  - 障害検知時の通知タイプを設定。設定可能な通知形式は以下の4種類
  - 例
    pagetype: HOST

- RCPT ：障害通知受信者単位（デフォルト）
  - 監視期間内にて障害が発生した場合、障害通知先毎に一通の障害通知を行う
  - 複数の障害が発生していても一番先に検出した障害のみ通知
  - 通知件数は，最も少ないが他の障害は通知されないため、必ず他障害の発生確認が必要
- EVENT：障害発生イベント単位
  - 全ホストの全監視項目全てのイベントを個別に通知
  - 通知頻度が最も多いが、メールにて確実に障害検知可能
- HOST ：障害発生ホスト単位
  - 障害が発生したホスト単位で通知
  - 障害ホストにて複数の障害イベントを検知していても、一通だけ通知
- GROUP：bb-hostsのgroup/group-compress単位
  - bb-hostsにて設定されたgroup単位に通知
  - group内で複数の障害が発生していても一通しか通知しないため、必ず他障害の発生確認が必要

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@aa.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, fs1 ：
    - 毎日午前4時から6時の間で日次バッチ処理が走り、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@aa.jpにも通知
  - 支社のファイルサーバ branch-fs0：
    - 監視業務の省力化のために 平日の7時から24時までの時間帯のみ障害通知を行う
    - この機械の障害時には担当窓口：intra@aa.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.aa.jpへの通知を追加

実装検討1 – 警報通知定義

セグメント	IP address	監視名称	URL	通知先	通知時間
本社DMZセグメント (61.195.W.0/28) (172.16.250.8/29)	61.195.W.1	fw0-eth1	---	alert@aa.jp	24H/7D
	61.195.W.2	dns0.aa.jp	dns0.aa.jp	alert@aa.jp	24H/7D
	61.195.W.3	mail0.aa.jp	mail0.aa.jp	alert@aa.jp	24H/7D
	61.195.W.4	www.aa.jp	www.aa.jp	alert@aa.jp	24H/7D
	61.195.W.5	mon0-2.aa.jp	---	alert@aa.jp	24H/7D
	172.16.250.9	fw0-eth1-2	---	alert@aa.jp	24H/7D
	172.16.250.10	dmz-sw0	---	alert@aa.jp	24H/7D
本社イントラセグメント (172.16.0.0/24)	172.16.0.1	fw0-eth2	---	alert@aa.jp	24H/7D
	172.16.0.2	fs0	fs0.hq.aa.jp	alert@aa.jp, intra@aa.jp	22H/7D, 午前4-5時台は除外
	172.16.0.3	fs1	fs1.hq.aa.jp	alert@aa.jp, intra@aa.jp	22H/7D, 午前4-5時台は除外
	172.16.0.4	mon0.aa.jp	mon0.aa.jp	alert@aa.jp	24H/7D
	172.16.0.250	intra-sw0	---	alert@aa.jp	24H/7D
本社WANセグメント (172.16.250.0/28) (211.14.X.10/32)	172.16.250.1	fw0-eth0	---	alert@aa.jp, alert@branch.aa.jp	24H/7D
	211.14.X.10	fw0-ppp0	---	alert@aa.jp, alert@branch.aa.jp	24H/7D
支社WANセグメント (172.16.250.16/28) (211.14.Y.12/32)	172.16.250.17	branch-fw0-eth0	---	alert@aa.jp, alert@branch.aa.jp	24H/7D
	211.14.Y.12	branch-fw0-ppp0	---	alert@aa.jp, alert@branch.aa.jp	24H/7D
支社イントラセグメント (172.16.10.0/24)	172.16.10.1	branch-fw0-eth0	---	alert@aa.jp, alert@branch.aa.jp	24H/7D
	172.16.10.2	branch-fs0	fs0.branch.aa.jp	alert@aa.jp, alert@branch.aa.jp, intra@aa.jp	週日、午前0-7時台は除外
	172.16.10.3	branch-log0	log0.branch.aa.jp	alert@aa.jp, alert@branch.aa.jp	24H/7D
	172.16.10.250	branch-sw0	---	alert@aa.jp, alert@branch.aa.jp	24H/7D

実装検討1 - 警報通知定義
etc/bbwarnrules.cfg

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

fs*;;*;;*;0000-0359 0600-2359;alert@aa.jp intra@aa.jp
## fs*(fs0 fs1にマッチ)については24H/7Dの監視を行い、
## 障害時はaltert@aa.jpとintra@aa.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

branch-fs*;;*;;1-5;0700-2359;alert@aa.jp intra@aa.jp alert@branch.aa.jp
## branch-fs0については月曜日から金曜日の週日に監視を行い、
## 障害時はaltert@aa.jpとintra@aa.jpとalert@branch.aa.jpに通知する
## ただし、AM0:00-AM6:59までの間は通知対象外とする

branch-*;branch-fs0;*;;*;*;alert@aa.jp alert@branch.aa.jp
## branch-*(支社のfw0インタフェース)については24H/7Dの監視を行い、
## 障害時はaltert@aa.jpとintra@aa.jpに通知

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

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

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

実装検討1 – 障害通知例

障害検知通知: dns0.aa.jp - conn

```
---------------------- Original Message ----------------------
 From:    <bb@mon0.aa.jp>
 To:      alert@aa.jp
 Date:    6 Nov 2003 11:33:28 +0900
 Subject: !BB - 8393010! dns0.aa.jp.conn - 500192168001002
----

[8393010]  dns0.aa.jp.conn red Thu Nov  6 11:33:26 JST 2003 ERROR: Can't connect to 61.195.W.2
PING 61.195.W.2 (61.195.W.2): 56 data bytes

--- 61.195.W.2 ping statistics ---
1 packets transmitted, 0 packets received, 100% packet loss

Please see: http://mon0.aa.jp/bb/html/dns0.aa.jp.conn.html
--------------------- Original Message Ends -------------------
```

障害回復通知: dns0.aa.jp - conn

```
---------------------- Original Message ----------------------
 From:    <bb@mon0.aa.jp>
 To:      alert@aa.jp
 Date:    6 Nov 2003 12:48:15 +0900
 Subject: !BB - 0000000! dns0.aa.jp.conn - 500192168001002
----

[0000000]  dns0.aa.jp.conn recovered Thu Nov  6 12:48:15 2003 Problem has been resolved after
4971 seconds

Please see: http://mon0.aa.jp/bb/html/dns0.aa.jp.conn.html
--------------------- Original Message Ends -------------------
```

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)
  - 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

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】
$
```

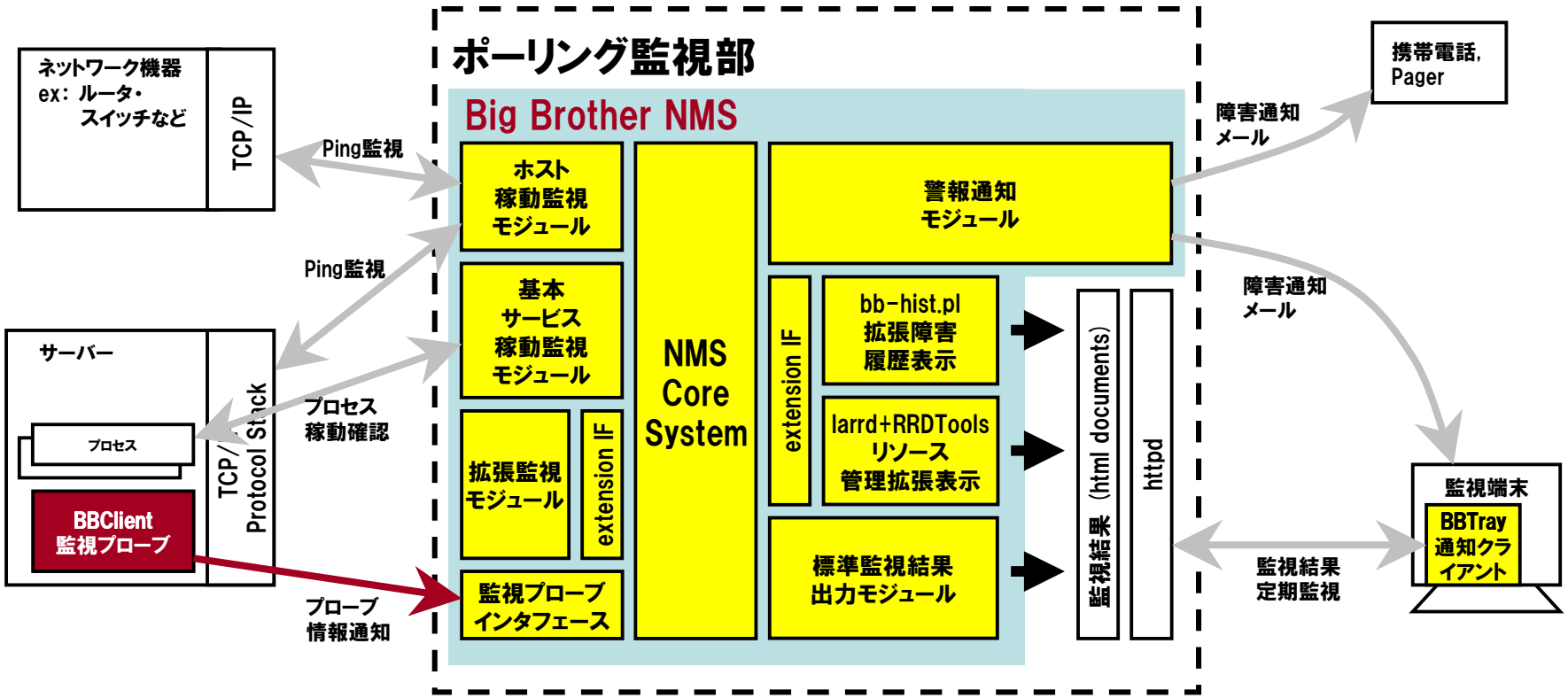
実装検討1 - process監視

- 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



eAccess Broadband Services

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

監視名称	URL	プロセス確認										
		inetd	bbrun	sshd	named	httpd	cron	ntpd	syslogd	sendmail	popd	snmptrapd
dns0.aa.jp	dns0.aa.jp	×	○	○	○	×	○	○	○	○	---	---
mail0.aa.jp	mail0.aa.jp	×	○	○	○	×	○	○	○	○	○	---
www.aa.jp	www.aa.jp	×	○	○	---	○	○	○	○	×	---	---
mon0.aa.jp	mon0.aa.jp	×	○	○	---	○	○	○	○	×	---	○
branch-log0	log0.branch.aa.jp	×	○	○	---	○	○	○	○	×	---	○

【dns0.aa.jp - $BBHOME/etc/bbdef.sh該当部分】
```
PROCS="!inetd bbrun !httpd ntpd syslogd"
PAGEPROC="sshd named cron sendmail"
```

【mail0.aa.jp - $BBHOME/etc/bbdef.sh該当部分】
```
PROCS="!inetd bbrun !httpd syslogd"
PAGEPROC="sshd named cron ntpd sendmail popd"
```

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

【mon0.aa.jp - $BBHOME/etc/bbdef.sh該当部分】
```
PROCS="!inetd bbrun syslogd !sendmail"
PAGEPROC="sshd httpd cron ntpd snmptrapd"
```

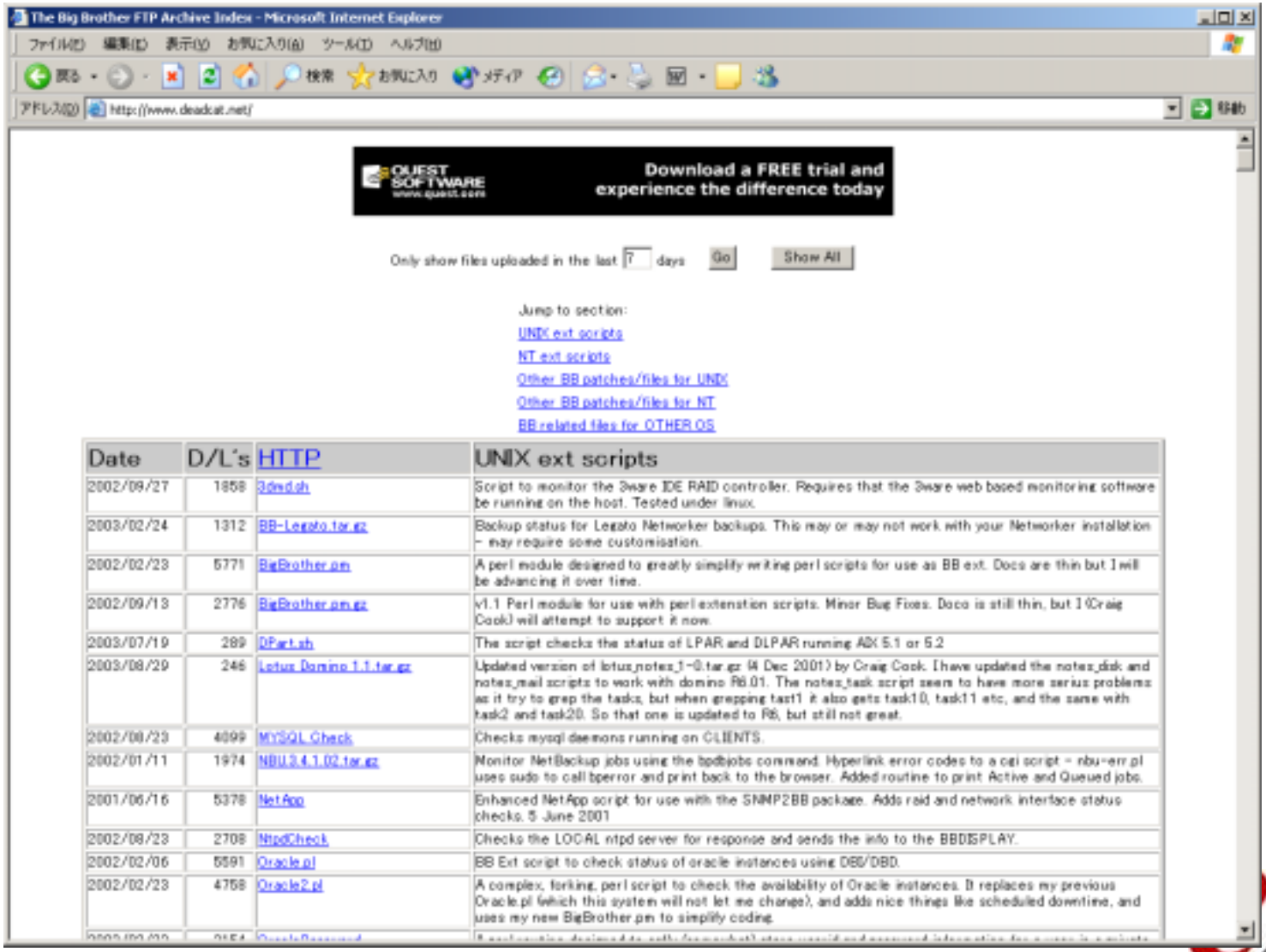
【branch-log0 - $BBHOME/etc/bbdef.sh該当部分】
```
PROCS="!inetd bbrun syslogd !sendmail"
PAGEPROC="sshd httpd cron ntpd snmptrapd"
```

記号	説　明
○	PAGEPROCSでの存在確認プロセス
○	PROCSでの存在確認プロセス
×	PROCSでの非存在確認プロセス
---	設定対象外

BB - extensions

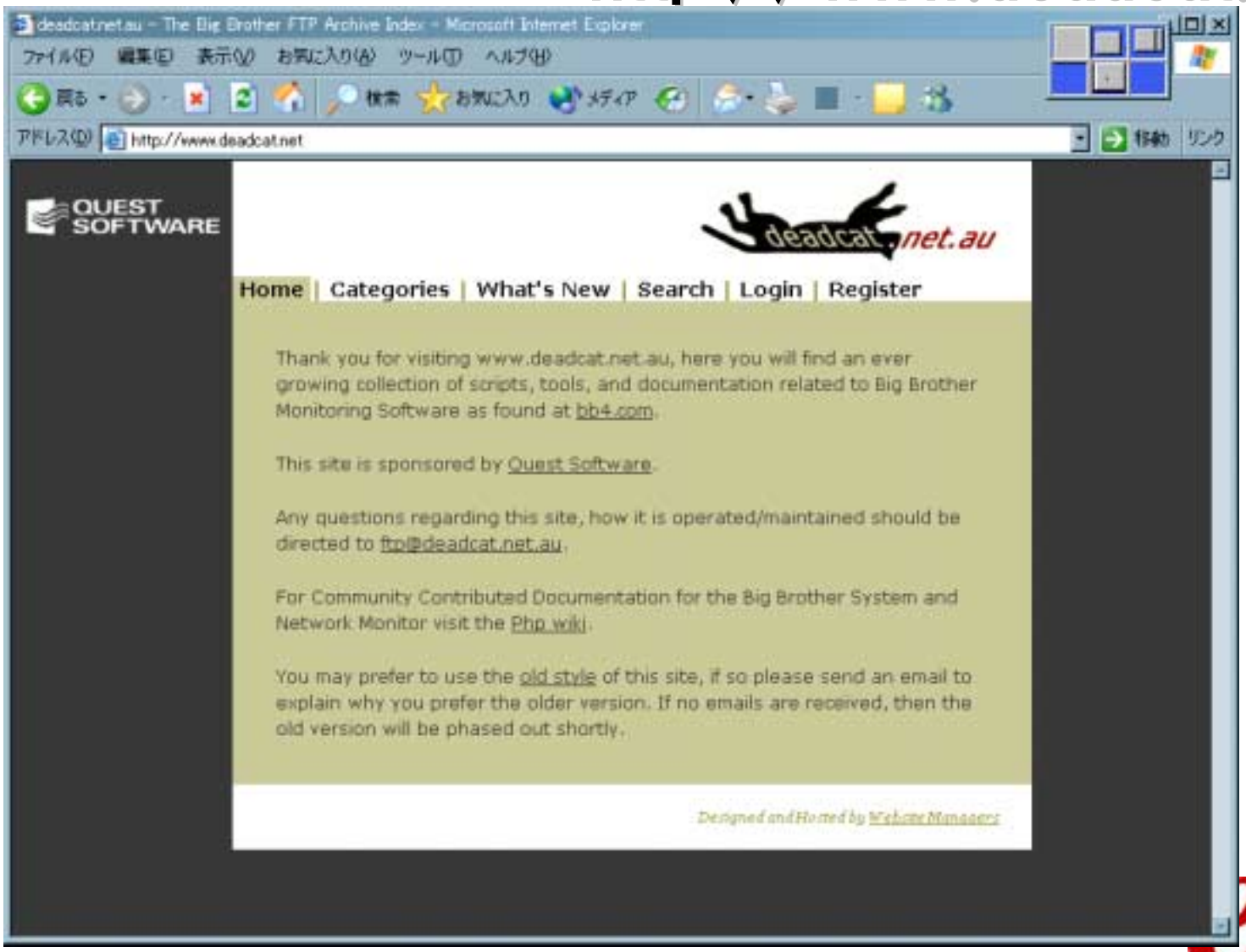
- 拡張インタフェースが公開されており、多彩な拡張監視モジュールが存在する
  - オープンソースの利点を生かし、BB基本ソフトをそのまま置換する機能拡張版ソフトも存在する
    - http://www.deadcat.net/
  - Enhancement script to BB
    - モジュールごと拡張版への置換
  - External plug-in script for BB
    - 外部拡張スクリプトによる機能追加

BB - Extension Archive
http://www.deadcat.net

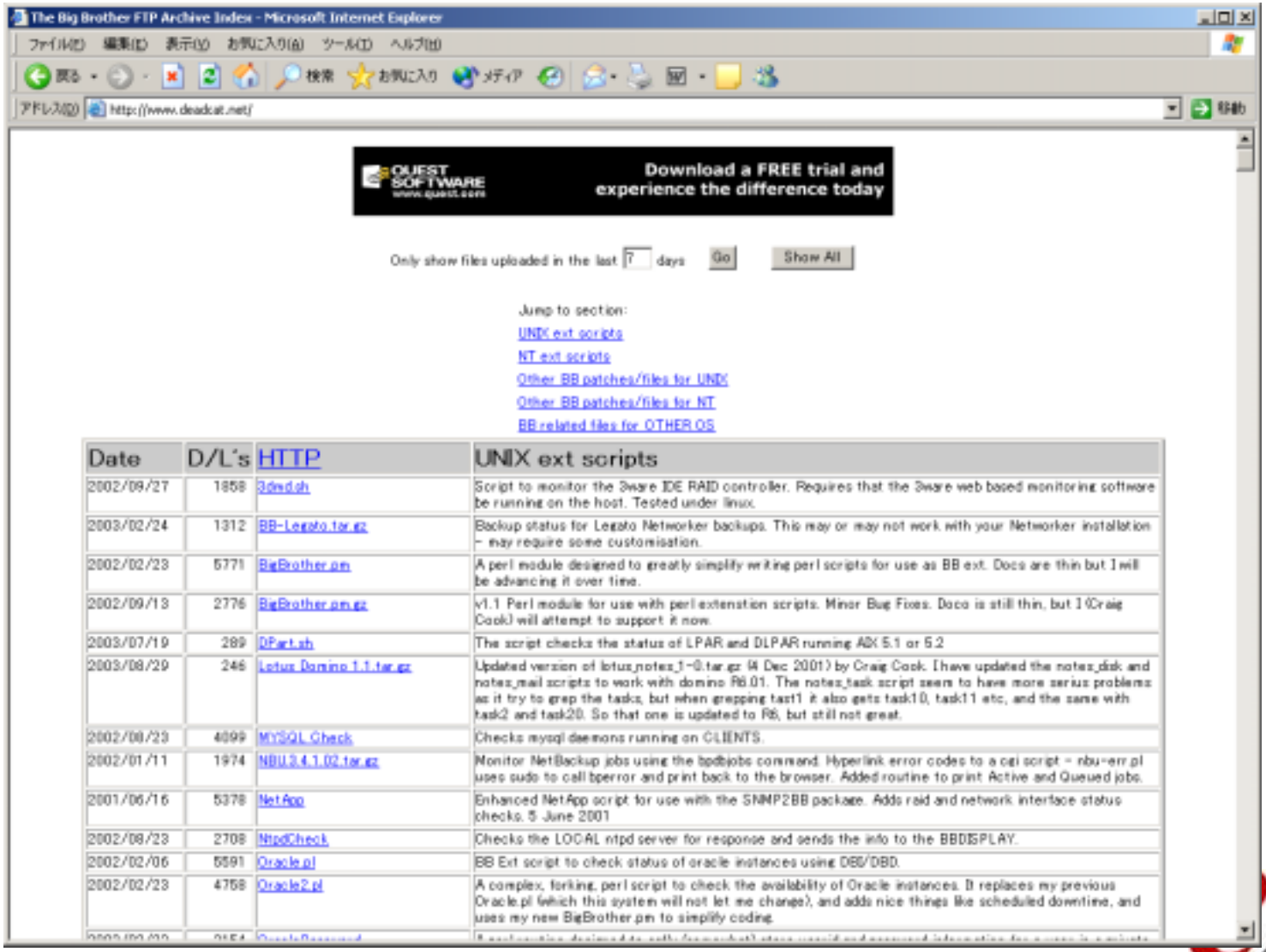


Date	D/L's	HTTP	UNIX ext scripts
2002/09/27	1858	3dwdsh	Script to monitor the 3ware IDE RAID controller. Requires that the 3ware web based monitoring software be running on the host. Tested under linux.
2003/02/24	1312	BB-Legato.tar.gz	Backup status for Legato Networker backups. This may or may not work with your Networker installation - may require some customisation.
2002/02/23	5771	BigBrother.pm	A perl module designed to greatly simplify writing perl scripts for use as BB ext. Docs are thin but I will be advancing it over time.
2002/09/13	2776	BigBrother.pm.gz	v1.1 Perl module for use with perl extenstion scripts. Minor Bug Fixes. Docs is still thin, but I (Craig Cook) will attempt to support it now.
2003/07/19	289	DPart.sh	The script checks the status of LPAR and DLPAR running AIX 5.1 or 5.2
2003/08/29	246	Lotus_Domino_1.1.tar.gz	Updated version of lotus_notes_1-0.tar.gz (4 Dec 2001) by Craig Cook. I have updated the notes_disk and notes_mail scripts to work with domino R6.01. The notes_task script seem to have more serius problems as it try to grep the tasks, but when grepping task1 it also gets task10, task11 etc, and the same with task2 and task20. So that one is updated to R6, but still not great.
2002/08/23	4099	MYSQL Check	Checks mysql daemons running on CLIENTS.
2002/01/11	1974	NBU.3.4.1.02.tar.gz	Monitor NetBackup jobs using the bpdbjobs command. Hyperlink error codes to a cgi script - nbu-err.pl uses sudo to call bperror and print back to the browser. Added routine to print Active and Queued jobs.
2001/06/16	5378	NetApp	Enhanced NetApp script for use with the SNMP2BB package. Adds raid and network interface status checks. 5 June 2001
2002/08/23	2708	NtpdCheck	Checks the LOCAL ntpd server for response and sends the info to the BBDISPLAY.
2002/02/06	5591	Oracle.pl	BB Ext script to check status of oracle instances using DBI/DBD.
2002/02/23	4758	Oracle2.pl	A complex, forking, perl script to check the availability of Oracle instances. It replaces my previous Oracle.pl (which this system will not let me change), and adds nice things like scheduled downtime, and uses my new BigBrother.pm to simplify coding.

BB - Extension Archive
http://www.deadcat.net



BB - Extension Archive
http://www.deadcat.net



Date	D/L's	HTTP	UNIX ext scripts
2002/09/27	1858	3dwdsh	Script to monitor the 3ware IDE RAID controller. Requires that the 3ware web based monitoring software be running on the host. Tested under linux.
2003/02/24	1312	BB-Legato.tar.gz	Backup status for Legato Networker backups. This may or may not work with your Networker installation - may require some customisation.
2002/02/23	5771	BigBrother.pm	A perl module designed to greatly simplify writing perl scripts for use as BB ext. Docs are thin but I will be advancing it over time.
2002/09/13	2776	BigBrother.pm.gz	v1.1 Perl module for use with perl extenstion scripts. Minor Bug Fixes. Docs is still thin, but I (Craig Cook) will attempt to support it now.
2003/07/19	289	DPart.sh	The script checks the status of LPAR and DLPAR running AIX 5.1 or 5.2
2003/08/29	246	Lotus_Domino_1.1.tar.gz	Updated version of lotus_notes_1-0.tar.gz (4 Dec 2001) by Craig Cook. I have updated the notes_disk and notes_mail scripts to work with domino R6.01. The notes_task script seem to have more serius problems as it try to grep the tasks, but when grepping task1 it also gets task10, task11 etc, and the same with task2 and task20. So that one is updated to R6, but still not great.
2002/08/23	4099	MYSQL Check	Checks mysql daemons running on CLIENTS.
2002/01/11	1974	NBU.3.4.1.02.tar.gz	Monitor NetBackup jobs using the bpdbjobs command. Hyperlink error codes to a cgi script - nbu-err.pl uses sudo to call bperror and print back to the browser. Added routine to print Active and Queued jobs.
2001/06/16	5378	NetApp	Enhanced NetApp script for use with the SNMP2BB package. Adds raid and network interface status checks. 5 June 2001
2002/08/23	2708	NtpdCheck	Checks the LOCAL ntpd server for response and sends the info to the BBDISPLAY.
2002/02/06	5591	Oracle.pl	BB Ext script to check status of oracle instances using DBI/DBD.
2002/02/23	4758	Oracle2.pl	A complex, forking, perl script to check the availability of Oracle instances. It replaces my previous Oracle.pl (which this system will not let me change), and adds nice things like scheduled downtime, and uses my new BigBrother.pm to simplify coding.

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

- /cgi-bin/bb-hist.shの置換プログラム
- http://www.deadcat.net/cgi-bin/download.pl?section=3&file=bb-hist-2.6.tar.gz
- 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

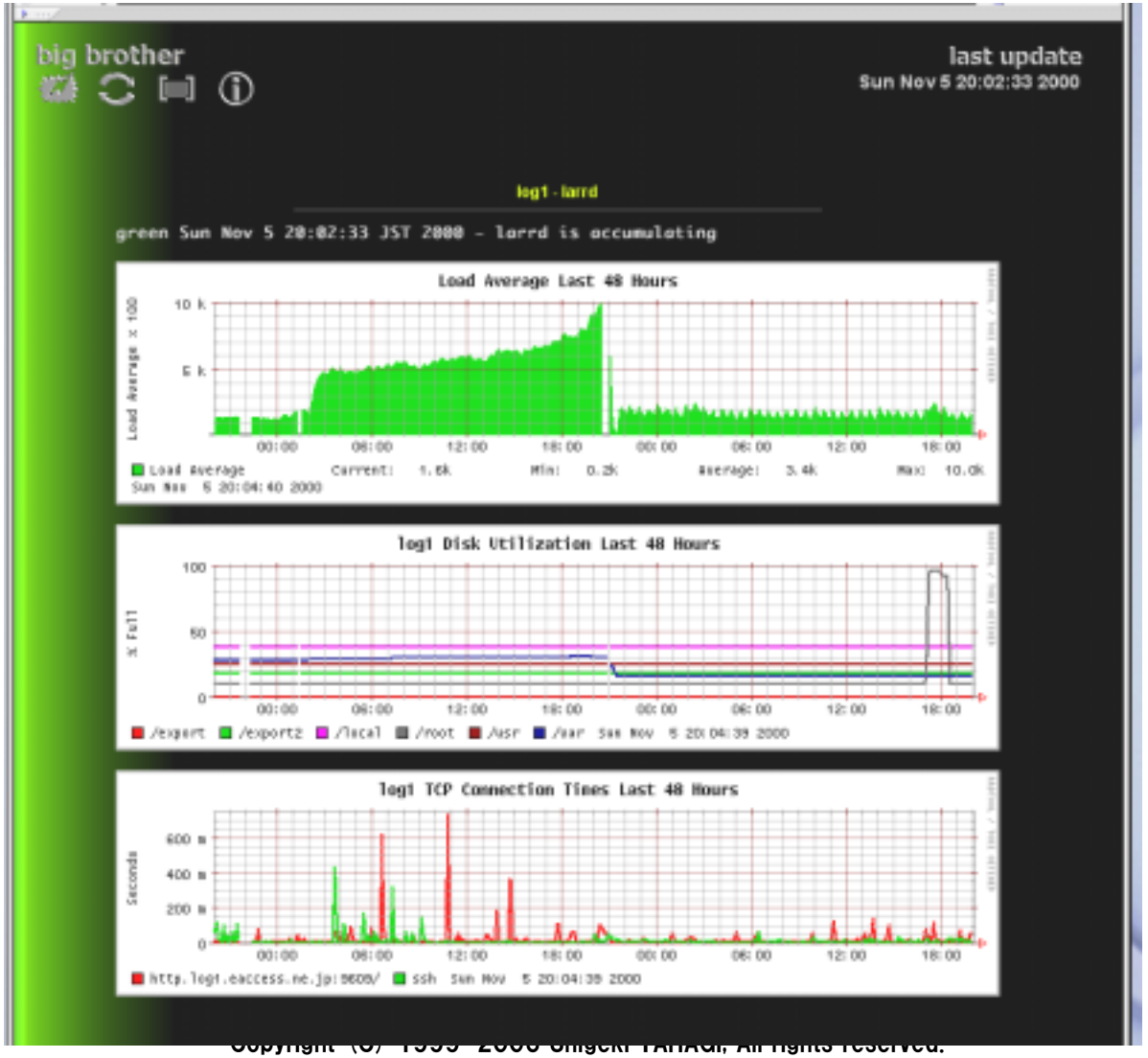
- larrd: loadavg rrdtool -> latest v 0.43c
- http://larrd.packetpushers.com/
- Big Brother Clientが各監視対象から取得したデータをRRDToolによりグラフ化する
  - 対象データ：load average, Disk Usage, Memory, SWAP, bind, TCP Connection Time, (Memory Usage, CPU idle,) ...
- グラフ作成のみに特化しており、larrdは閾値を設定したトラフィックアラーム監視は行わない
- 以下のインストール手順だけすれば、ほかの設定は必要なし
  - BBのコンパイル時、$BBHOME/src/Makefileに -DNOTAMP を付加して再コンパイル、再インストール
  - 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

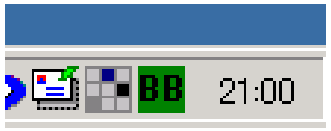
実装検討1 - 監視システム定義 BB-RRDTool連携：larrd設定

- $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

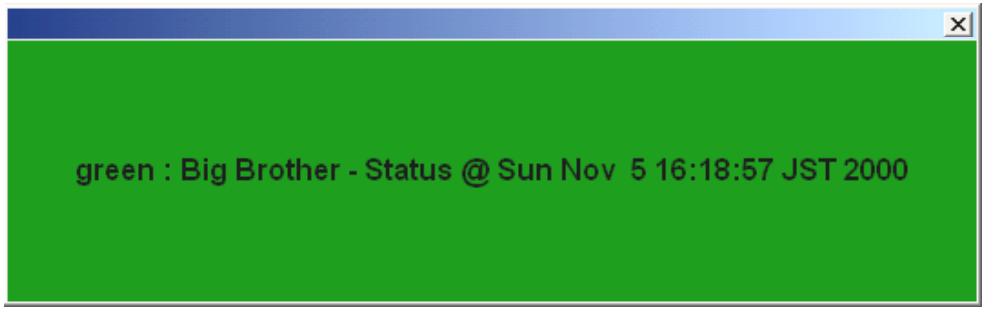




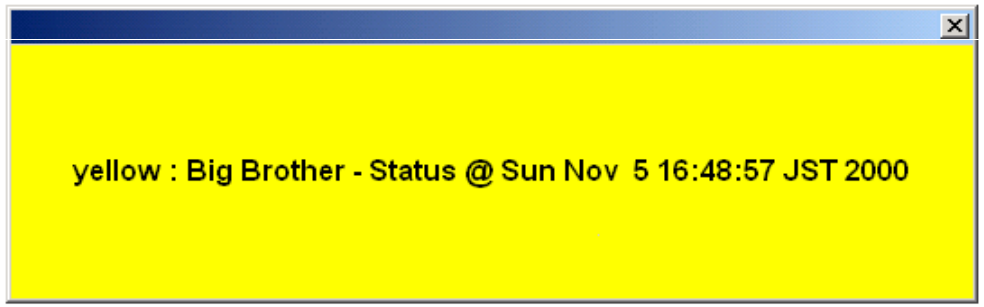
実装検討1 - 監視クライアント連係
BBTray - 監視サポートツール

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

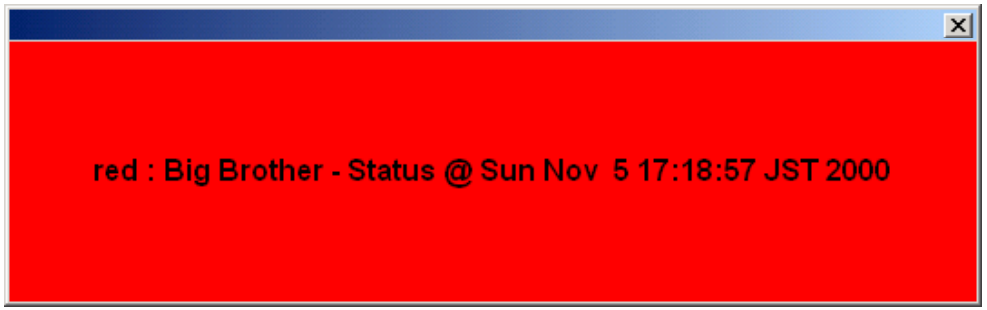
実装検討1 - 監視クライアント連係
BBTray - 続き



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://172.16.0.4/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(Port=1984)への誤情報を送り込むことが可能
  - このため、BBでは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.aa.jp 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://mon0.aa.jp: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 172.16.0.4:5963

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

監視システムのモデル － ポーリング監視システム