オープンシステム環境での監視の取り組み
～省力化と可用性向上に向けて～

ヤマトシステム開発（株）

■ 執筆者Ｐｒｏｆｉｌｅ ■

山　崎　英　樹

1992 年　ヤマトシステム開発（株）入社
　　運用技術部配属
2002 年　現在，運用技術部ネットワーク運用課所属

日名田　　圭

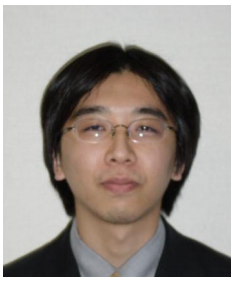
1997 年　ヤマトシステム開発（株）入社
　　運用技術部配属
2002 年　現在，運用技術部運用技術課所属

館　山　浩　武

1998 年　ヤマトシステム開発（株）入社
　　技術開発部配属
2001 年　運用技術部オープンシステム運用課転属
2002 年　現在，運用技術部オープンシステム運用課所属

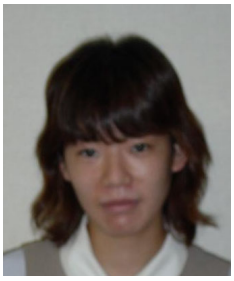
佐　藤　和　裕

1991 年　ヤマトシステム開発（株）入社
　　総務部企画課配属
1998 年　社長室経営企画課転属
1999 年　運用技術部運用技術課転属
2002 年　現在，運用技術部運用技術課所属



飯　塚　真　吾

2000 年　ヤマトシステム開発（株）入社
　　運用技術部配属
2002 年　現在，運用技術部オープンシステム運用課所属



勝　田　真　由

2001 年　ヤマトシステム開発（株）入社
　　運用技術部ネットワーク運用課配属
2002 年　現在，運用技術部ネットワーク運用課所属

■ 論文要旨 ■

近年，汎用機などで行ってきた処理が TCP/IP をベースとした分散型オープンシステムへ移行しており，システムを構成する機器も大型集中型から小型分散化へ移行している．また，システム障害が直接消費者へ影響を与え機会損失と企業イメージを損なうことになる．

そのような背景の中，障害原因が機器の死活的な障害から性能低下による障害に移行しており，監視対象及び障害要素が急速に増加している状況にあった．また，サポート員のスキルの向上と障害時の対応方法を統一することは困難でありシステムの拡大と複雑化に比例して増員してゆかなければならないという問題を抱えていた．

これらを解決するために，弊社では性能監視，回線帯域監視などを含めた統合監視ツールを導入することによって複雑な複数の運用と監視対象を一元的に監視することが可能となり，障害時の迅速な影響範囲の把握と監視業務の省力化を行なうことが可能となった．

■ 論文目次 ■

■ 図表一覧 ■

１．はじめに

１．１　当社概要

当社は，1973 年１月にヤマト運輸の電算機部門より独立した，ヤマトグループの情報処理会社であり，宅急便をはじめとするヤマト運輸の業務を約３割，ヤマト運輸以外の一般顧客の業務約７割を行っている．

ヤマト運輸の業務では，宅急便の全国ネットワークの構築，運用を行っており，年間９億個以上の宅急便の情報を処理し，荷物追跡等のサーバ運用管理や新商品への対応を一手に行っている．また，宅急便のコンピュータシステムも汎用機から荷主のシステムに柔軟に対応，より柔軟な貨物情報の提供ができるよう大型 UNIX サーバを導入して基幹システムの抜本的な更新に着手している．

ヤマト運輸以外の一般企業へ向けては「情報処理業」のほかに「情報通信業」として通信コストを削減するネットワークサービスの提供を開始し，わが国で最初の民間 VAN 事業登録者（1982 年 11 月）や，一般第二種電気通信事業者（1985 年４月），システムインテグレータ認定（1988 年 12 月）の届出を行った．こうして培ったノウハウでモノの効率的な流れを創造するべく「情報＋通信＋物流」を一体化した独自のソリューション「Logisis」として，ロジスティクスサービス，アウトソーシングサービス，システムインテグレーションサービス，EC サイトの構築・運用，データセンタ業務などを多数の企業へ提供している．

２．ネットワークの規模，運用体制

２．１　概略

現在，弊社（以下 YSD という）が運用しているネットワークの規模と運用体制の概略を示す．（**図１**参照）

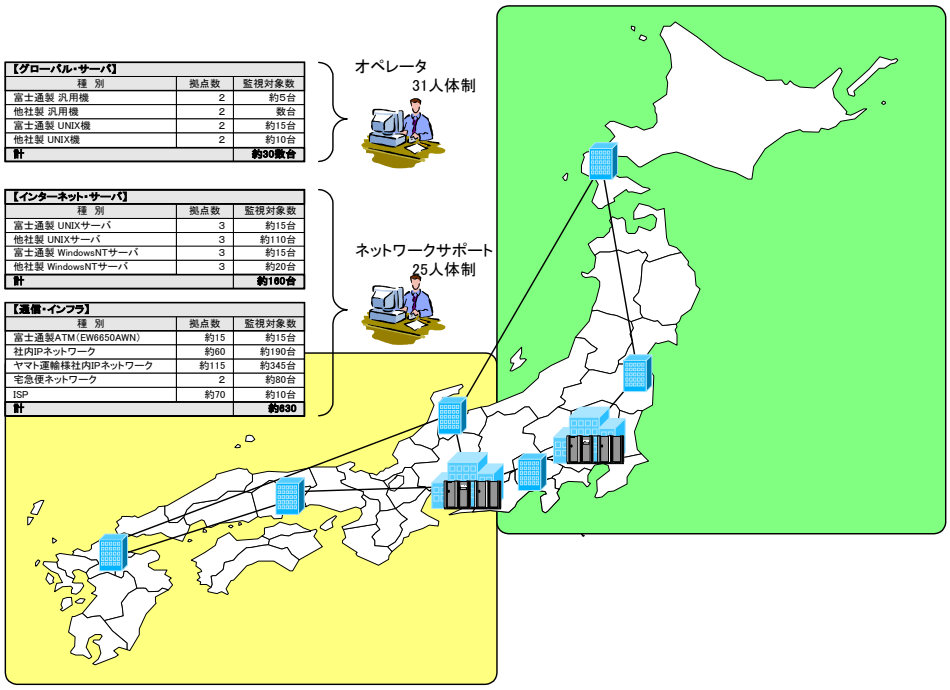


図１　運用規模概要図

２．２　グローバルサーバ

GS8900 を中心とした大規模なコンピュータセンタを東京・大阪（以下東阪という）の二拠点に構えている，特に宅急便コンピュータシステムでは通常 東京センタが東日本の営業所で発生したデータを，大阪センタは西日本の営業所で発生したデータの処理を行ない，東阪のシステム間でデータの同期を行なっている．東阪の両センタは，互いにバックアップを行なう処理能力を有しており地域災害などのセンタ障害の際には全店からのデータを受信し処理を行なうことが可能である．

これは過去の世田谷ケーブル火災を教訓として，地域災害により建物設備が影響を受けた場合，システムトラブルの発生によってセンタ運用の継続が不可能になった場合を考慮している．いざという時の人的およびシステム的運用の実効性をチェックするために，毎月訓練も兼ねて“片センタ運用”を実施している．

現在，両センタにて常時 四人体制で 24 時間 365 日のシステムの監視とオペレーションを行なっている．

オペレーション体制は下記のとおりである．

・各センタ，24 時間，常時二人体制で監視・オペレーション
・年数回のオペレータ教育
・月一回の TV 会議システムを利用した東阪でのオペレータ定例会
・毎日 朝夕 TV 会議システムを利用した引き継ぎ会議
・グループウェアによる過去障害情報の共有

監視対象は，下記の OS 単位にハードウェア障害，ソフトウェア障害，システム資源の枯渇，アプリケーションのエラーなどの情報を監視用コンソールに出力することで，オペレータへの通知を行なっている．（**表１**参照）

表１　グローバルサーバ監視対象一覧表

（監視対象:2002/06/01 現在）

機種名	台数	稼働 OS 数
富士通製 汎用機	約５台	約 10
他社製 汎用機	数台	約５
富士通製 UNIX 機	約 15 台	約 15
他社製 UNIX 機	約 10 台	約 10

２．３　インターネットサーバ

1997 年から [1]二次プロバイダとして ISP サービスを展開し始めた YSD であるが，運用規模の拡大に伴い 2001 年 10 月に東阪のインターネット回線を含めた ISP 設備の冗長化が可能な [2]マルチホーム環境に移行した．冗長性のあるネットワーク下で各種接続サービスはもとより，東阪のセンタにて [3]ハウジング，[4]ホスティングなど各種サービスにて顧客サーバを預かり，保守・運用を行っている．また，ISP 運用の要となる [5]DNS サーバやメールサーバなど ISP 設備を加えた監視対象サーバ数は**表２**のとおりである．

1 インターネットバックボーンに直接接続する 1 次プロバイダに接続して，インターネットへの接続サービスを提供するプロバイダ
2 冗長性確保のため，上位プロバイダへの接続を複数持つ環境のこと
3 Internet プロバイダが，高速な接続環境を提供するために直接顧客サーバの設置を請け負うサービス
4 サーバのディスクの一部とアプリケーションをセットにして，仮想サーバを提供するサービス
5 TCP/IP ネットワークで，ホストネームと IP アドレスの紐付けを持ち，名前解決のサービスを提供するシステム

表２　インターネットサーバ監視対象一覧表

種別	拠点数	監視対象数
富士通製 UNIX サーバ	3	約 15
他社製 UNIX サーバ	3	約 110
富士通製 WindowsNT サーバ	3	約 15
他社製 WiudowsNT サーバ	3	約 20
計		約 160

ただし，一台のサーバには DNS サーバ，メールサーバ，Web サーバなどといった複数のアプリケーションが稼働しているので，運用を構成しているアプリケーションの監視を行なう場合，監視対象は増加する．監視対象の増加推移は**図２**のとおりである．

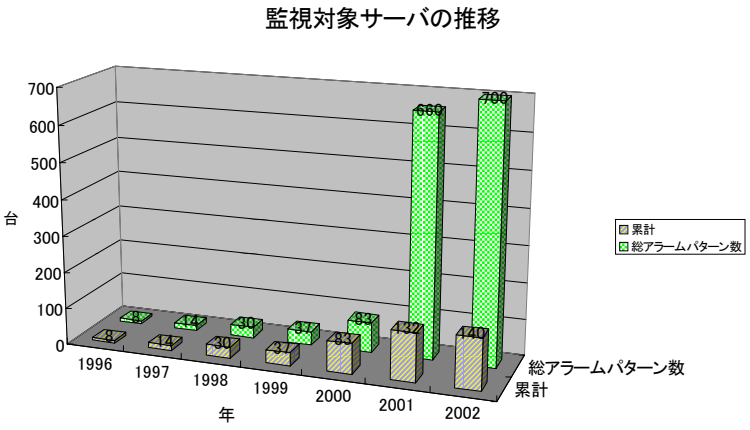


図２　監視対象サーバの推移

また，ホスティングサービスにおいては一台のハードウェアで仮想的に複数の Web サーバを立ち上げており，約 280 もの仮想 Web サーバを運用している．

また，最近は電子店舗，EC サイト，グループウェアの ASP サービスなどより付加価値の高いサービスも展開しており，複数のアプリケーションから構成されているため運用の観点から監視を行なう場合，複雑なものとなる．

２．４　通信インフラ

YSD はヤマト運輸を含め顧客の基幹ネットワークを請け負っており，全国規模のネットワークの運用・監視を行なっている．

YSD のネットワーク構成は，[6]ATM ネットワークをバックボーンに，パケットネットワーク・[7]TDM ネットワーク・IP ネットワークと分類される．このうち，主な監視対象機器は**表３**に示すとおりである．

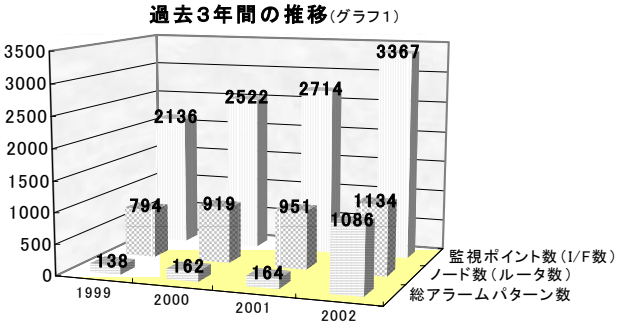


図３　監視対象インフラ機器の推移

6 異なる種類のデータを 53bytes の固定長のセルに分割して伝送する通信方式
7 複数のデータを一定の時間で切り替えて伝送することを可能にした装置

表３　インフラ機器監視対象一覧表

ネットワーク名	機器台数		回線数
ATM ネットワーク	ATM 交換機	約 15 台	約 20 回線
パケット（X.25）ネットワーク	パケット交換機	約 5 台	約 45 回線
	PAD	約 50 台	
TDM ネットワーク	ITDM 装置	約 21 台	約 19 回線
IP ネットワーク	ルータ	約 210 台	約 150 回線
	RAS	約 30 台	
	HUB	約 405 台	

TCP/IP を利用したネットワークの増加と共にネットワーク機器の形態も大型・集中型からルータやハブをはじめとした小型・分散化が主となったことにより監視対象が増加し，監視形態も基幹ネットワークの監視から運用毎の監視に移行し監視対象も広範囲なものとなっている．（**図３**参照）

３．ネットワーク監視の問題点と利用監視ソフトウェア

ここではホストコンピュータを含めたグローバルサーバ，インターネットサーバ，通信インフラのそれぞれの運用に伴う監視上の問題点と具体的な対策を述べていきたい．

３．１　グローバルサーバ

富士通製を主とした汎用機は，ヤマト運輸の宅急便の取り扱い増大とともに増強を続けてきた．近年ではホットスタンバイ構成となり，オンライン区画と待機系の区画が増えた．平行して，新しいシステムの構築が行なわれ，今までと根本的に異なる UNIX で構築することとなった．

移行のために平行運用が始まると，オペレータにとっては一時的に監視対象が増加することとなる．これには本体のみならずストレージをはじめとする補助記憶装置群も含まれている．

稼動している業務は変わらず，一時的に監視対象が追加となることはオペレータの負担と比例する．ましてや今までの汎用機文化に UNIX が加わったのである． 監視コンソールの追加によって，異常検知の見落としを含んだ監視精度の低下を防がなければならなかった．

また，多数のシステムは複雑なネットワークで結ばれ，障害が発生した際に，システム，ネットワーク，業務アプリケーションのどの部分が障害なのか原因究明が困難となる．

ハードウェアの障害時は，汎用機と同様にメーカのサポートセンタへ自動通報することとし，富士通 UNIX 機においては，サポートセンタから障害発生時に遠隔でログインして，原因調査・ログの収集が可能である．

UNIX 機の運用・監視にはベンダソフトの [8]SystemWalker や [9]Tivoli が導入された．汎用機の重要なメッセージは，赤色の高輝度メッセージでオペレータに通知している．汎用機から UNIX へのオペレーションのスムーズな移行を行なうために，同様に高輝度メッセージの概念を用いて，違和感のないオペレーション環境を構築することにした．システムテスト期間中に発生したハードやアプリケーション，そしてネットワークに至る様々な障害のログを元にオペレータが発見すべきメッセージを絞り込み，クリティカルメッセージとして

8 富士通製運用監視及び管理ソフトウェア
9 IBM 製運用監視及び管理ソフトウェア

汎用機と同様の赤色で表示させた．しかし，オペレータは磁気テープやプリンタのハンドリング作業も行なうため，コンソール上に赤色のメッセージを表示するだけでは見落とす原因となり発見が遅れることがあった．

高輝度メッセージを気付かせるためには，画面表示以外の工夫が必要となった．過去に同じ問題が発生し，他社製の汎用機ではパトランプを導入し解決していた．UNIX 機でもパトランプを導入してこれを解決した．（**図４**参照）

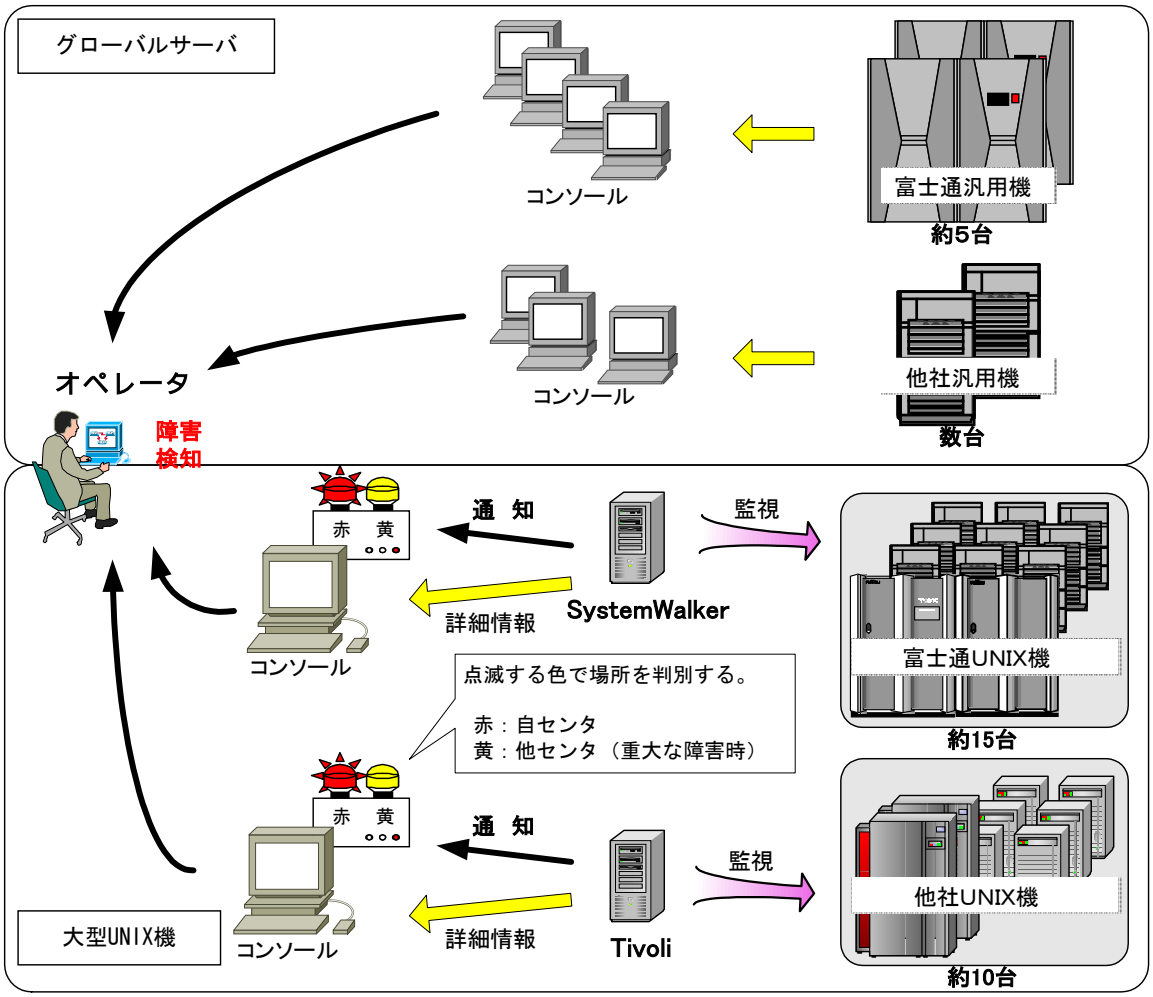


図４　グローバルサーバ及び大型 UNIX 機 監視概要図

３．２　インターネットサーバ

３．２．１　監視に求められるものの変化

導入当初は重要な運用も稼動することなく実験的意味合いも強かったインターネットサーバの監視は[10]Ping による死活監視のみを行ない，ダウンしてからの対応で十分であった．しかしクリティカルな運用に適用されダウンすることが許されない立場となった今，ダウンタイムをできるだけ短くするためのアプリケーション監視や，無理無駄のない運用のためのリソース監視などを行なう必要が出てきた．

３．２．２　アプリケーションの死活監視

インターネットサーバの一例として，一台のサーバで DNS サーバ，メールサーバ，Web サ

10 TCP/IP ネットワークにおいて，IP パケットが通信先まで届いているかを調べるためのコマンド

ーバといった複数のアプリケーションを稼動させているサーバが存在する．このようなサーバにおいては，サーバ自体は稼動しているが，特定のアプリケーションのみダウンしているといったケースを発見する仕組みを設けなければならない．従来の Ping による死活監視ではこのような障害には発見することはできないため，死活監視と併せて新たにアプリケーションの監視を行なう[11]iMark という製品を導入してこの課題を解決した．

iMark は，擬似的にクライアントと同様の動作を行ない各アプリケーションに適した監視を行なうことができる．

YSD ではこの iMark を，上位プロバイダとの接続個所直下に設置し，極力 インターネットから接続してくるユーザに近い環境から監視を行なっている．これにより，ユーザの立場に立ったアプリケーションの死活監視を行なうことが可能である．

３．２．３　リソース監視

前述したリソースの監視もインターネットサーバの信頼性を高めるために必須の課題となってきた．YSD においてはこの課題をクリアするために[12]SunMicroSystems（以下 Sun という）社プラットフォームの UNIX サーバ（富士通の OEM 製品も含む）へは SunManagementCenter（以下 SMC という）ツールを，IBM・WindowsNT サーバ・一部の Sun サーバへは[13]PATROL という製品を導入して，きめ細かなリソース情報収集の体制を整えるに至った．（**図５**参照）

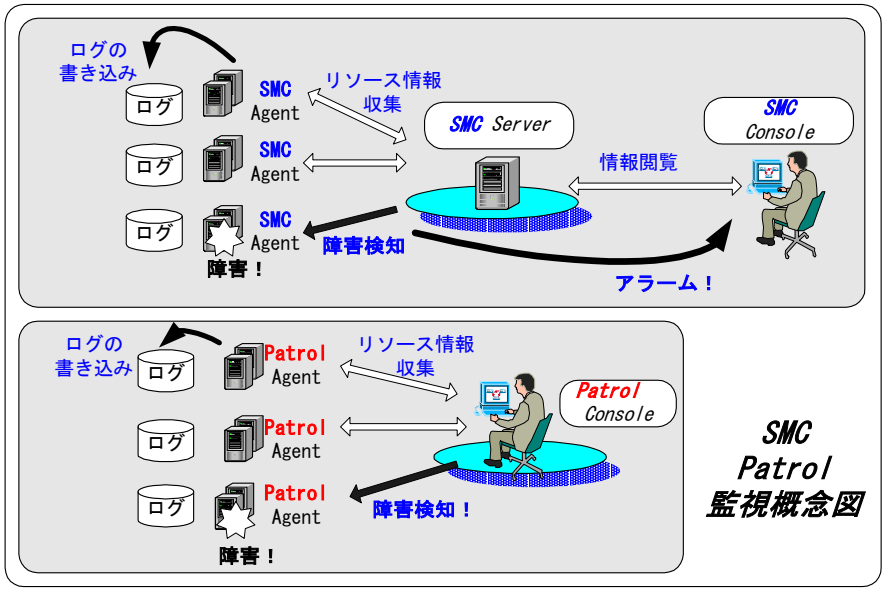


図５　SMC，PATROL 監視概要図

SMC は Sun 社が提供する監視ツールで，監視項目にしきい値を設け，取得した値がしきい値を超えるなどした場合にアラームを発生させてネットワークサポートに知らせることができる．また SMC は基本パッケージが無償であるため，富士通製 UNIX 機も含め，Sun プラットフォームのものがインターネットサーバの大部分を占める YSD では大きなコストメリットが見込める．しかし無償であるがゆえにままならない機能も多い．数ある監視可能項目の中から CPU，メモリ，スワップ領域，プロセス待ち時間という項目を選び，リソースに特化した監視を行っているが，重要なリソース項目であるファイルシステムのスライス使

11 シリウス社のサーバ監視ソフトウェア
12 SunMicrosystems 社の UNIX マシン監視ソフトウェア
13 BMC Software 社のサーバ監視ソフトウェア

用率は SMC では監視できない．そのため独自にスクリプトを組み cron[14] により実行させる監視を行っている．ログの蓄積については，SMC の機能によりグラフ表示させるためのログは監視対象サーバの物理メモリ上に確保されるため，サーバへの負荷を考慮して，テキストベースでディスクに保存する方式を選択して異常時にはいち早く解析が行なえるように備えている．

PATROL は有料ツールであるが，SMC と同様にリソースの監視，ログの蓄積ができるほか，DB，グループウェアなどアプリケーションの詳細が監視できるのが大きな特徴である．システムの用途により例えば Oracle のセッション数にしきい値を張り監視を行なうといったことが可能である．YSD では SMC と同様に基本リソースの監視のほか，サーバの用途により一部アプリケーションには特化した項目にしきい値を設けて監視を行っている．また，ログの解析機能として，PATROL は GUI からグラフの呼び出しを容易に行なうことができ，サーバ管理者以外のネットワークサポートがリソース情報に安全にアクセスできるのも特徴である．SMC・PATROL にて取得できる情報は**表４**のとおりである．

こうして新たな監視ポリシーとツールの導入によりインターネットサーバに対して新たな監視体制が整い，死活監視から一歩も二歩も踏み込んだ監視が行なえるようになってきた．障害にこそ至らないが常に負荷の高いサーバを特定できるなど，リソース監視ツール導入の効果は大きい．

表４　SMC・PATROL による取得情報

監視項目	SMC	PATROL	監視内容
CPU	○	○	CPU ユーザ利用率・CPU システム利用率 全体利用率
メモリ	○	○	空きメモリ容量・ページフォルトの回数 ページをスキャンした回・SWAP 空間の利用率
ディスク	×	○	物理ディスク領域の利用率・ディスク I/O 率 論理ディスク利用率
インタフェース	○	○	パケットの入出力量 ネットワーク上でのコリジョン発生率
プロセス	×	○	起動しているプロセス
アプリケーション	×	○	Oracle・MS SQL Server・Lotus Domino

３．３　通信インフラ

３．３．１　性能監視の必要性

汎用機を中心にシステムを構築していた時，ネットワークの基本構成は一回線（ネットワーク）に対して一端末を接続している形態が主であったが TCP/IP の普及により複数の端末や運用が一つのネットワーク上で稼働するようになった．

TCP/IP ネットワーク構築初期は端末数や運用も少なく，基本的な監視である死活監視で充分であり障害が発生してから対処する方法で十分と思われた．現在では予期できない回線帯域不足やルータやハブなどの通信機器の処理能力不足による性能低下が障害の要因となっている．また，運用やアプリケーションの充実に併せてこのような障害はアプリケーションエラーやリカバリ処理などを必要とする二次障害を誘発することとなる．

現在，ネットワークの性能障害に対して早期発見と履歴を残すことが困難なため改善を施すには調査から対策立案まで一週間から一ヶ月程度 要すこととなり運用管理に多大な

14 指定した日時にプログラムを起動できる，UNIX のタイマー機能デーモン

労力を必要とすることとなる．また，ネットワークの拡大に比例して労力も増大するためネットワークの性能監視を行なうシステムを構築することとなった．

３．３．２　SNMP の利点

IP に対応したインテリジェント型と称される機器は[15]SNMP 機能が搭載されており，CPU 負荷率や帯域使用率など機器の性能に関する情報が MIB というデータベースに格納されている．（**図６**参照）機器が標準で備えている一般的な[16]MIB だけでも取得可能情報は約 1,000 種類にも及ぶ．その他にも，現在約 3,000 社がメーカ独自の MIB を公開しており，監視に必要と思われる情報はすべて取得可能である．更に，SNMP エージェントと MIB はライセンスフリーであり，機器の増加による監視コスト増を抑えることが可能である．

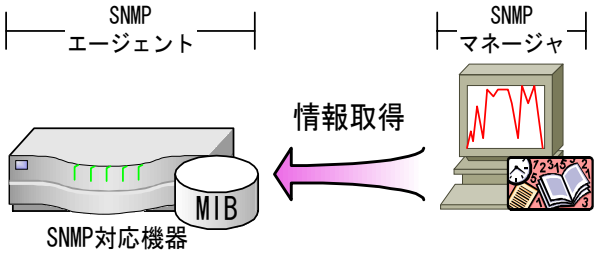


図６　SNMP 概要図

幅広い情報を取得できる SNMP に着目した YSD では，[17]InfoVista というツールを導入した．SNMP を利用したツールは他にも存在するが，InfoVista はライセンス形態で有利でありシステム構築におけるカスタマイズ性にも優れており汎用性が高い．主な機能は定期的に機器から複数項目の MIB 情報を取得し，計算と時系列のグラフ作成・レポート作成を行なうことである．また，計算やグラフ作成のカスタマイズ性が高いため通信機器以外にも無停電電源装置など SNMP 機能を有している機器であれば監視が可能である．YSD にて監視している主な機器と監視項目を下記に示す．（**表５**参照）

表５　YSD におけるオリジナルレポートによる取得 MIB 情報

監視項目	監視内容
ルータ	CPU 負荷率・メモリ使用率・システム稼動時間・各インタフェース情報
LAN インタフェース	帯域使用率・エラーパケット数・破棄パケット数・コリジョン発生率・ブロードキャストパケット数・プロトコル分布
WAN インタフェース	帯域使用率・エラーパケット数・破棄パケット数 PING レスポンスタイム・プロトコル分布
UPS	電圧・周波数・負荷率・バッテリ電圧・バックアップ可能時間 バックアップ経過時間
RAS	アクセスユーザ数

３．３．３　InfoVista 導入効果

MIB 情報は様々な情報を収集することが可能なため，YSD の用途に合った独自にカスタマイズし監視を行なっている．（**図７**参照）

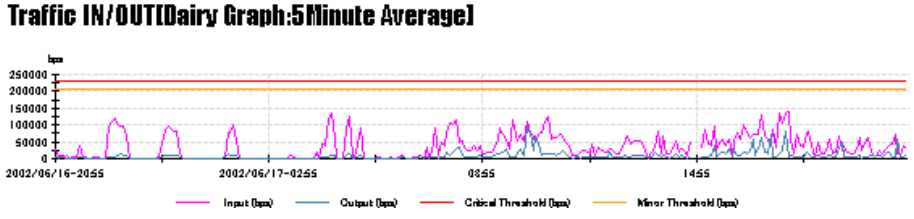


図７　InfoVista グラフ出力例

15 標準化されたTCP/IPネットワーク環境での管理プロトコル
16 SNMP によって管理される，マシンの状態を保持する変数
17 InfoVista 社のマシンの性能監視ソフトウェア

特に早急な見直しが必要となる回線帯域の圧迫や [18]RAS での回線不足が発生した際には，しきい値の設定により後述する統合監視装置へアラームを上げることが可能である．下記に回線帯域監視でのしきい値設定の一例を示す．（**表６**参照）

表６　しきい値の最適値設定

アラーム重度	しきい値設定
マイナーアラーム	トラフィック　＞　回線帯域＊80%
クリティカルアラーム	トラフィック　＞　回線帯域＊90%

SNMP と InfoVista を利用したネットワーク監視体制を整えることによりネットワークの性能低下を迅速に把握することが可能となり，運用へ影響が出る前にトラフィックの抑止を行なうことが可能となった．また，傾向を分析することにより障害の予知と無駄のない設備投資を行なうことが可能となった．

ネットワークサポートにおいてはルータやハブなどの操作方法に熟知していなくても障害を発見することが可能であり，詳細な状態を確認することが可能となった．

４．ネットワーク監視環境の統合

４．１　監視環境の問題点と統合後の構成

インターネットサーバ環境とネットワーク環境において監視範囲を「設備的な監視を行なう死活監視」から「アプリケーションや資源の監視を行なう性能監視」に移行したことにより運用が停止する致命的な障害は減少したが，発生するアラームは非常にシステムよりで高度な内容となりスキルを必要とする．特にインターネットサーバに関してはメッセージ内容の判断に管理者レベルのスキルを要求され，アラームに気が付かない可能性もある．また，運用（ネットワーク）毎に増加していく監視装置を常に視野に入れておくことは不可能であり監視体制もチェックシートによる定期的な目視確認となってしまう．

また，2002 年４月に UNIX 環境へ移行したグローバルサーバとネットワークの監視環境の統合は柔軟な人的対応フローなどの運用体制を検討する必要があるため統合化は行なわれていない．

上記 問題点を解決するに当たり監視環境の統合も行なうため，統合監視装置である BMC Software 社の PATROL Enterprise Manager（以下 PEM という）を導入した．監視装置は様々なメーカで構成され，監視する機器も様々である．今回，統合監視装置を導入するに当たりメーカに依存しない技術で統合監視装置と接続することが可能であり，カスタマイズと拡張が可能なことであった．YSD での監視装置との接続環境は全て SNMP の仕組みを含めメーカに依存しないオープンで標準化されている技術で構成されている．

今回 行なった監視体制と既存の監視装置の統合構成を下記 **図８**に示す．

18 リモート・アクセスを行うためのネットワーク機器

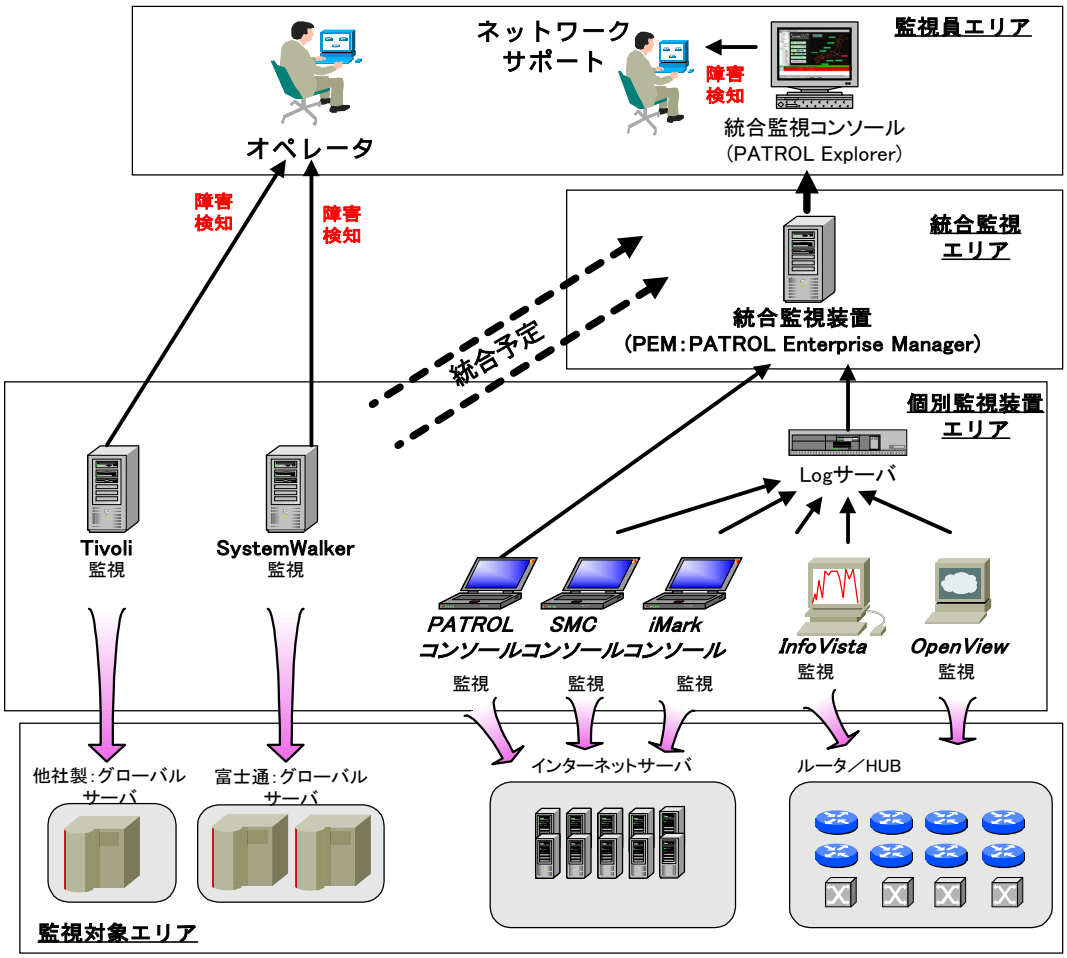


図８　統合監視相関図

４．２　目的

４．２．１　監視規模に比例する監視要員

常時監視を行なう場合，監視対象・監視装置の増加と監視内容によって監視要員を増加させていかなければならない．また，すべての監視装置を監視要員の視野に入るよう監視装置を設置することは環境的に不可能であったが，統合監装置を導入することによって少数の監視要員で常時監視環境を構築することが可能となった．（**図９**参照）

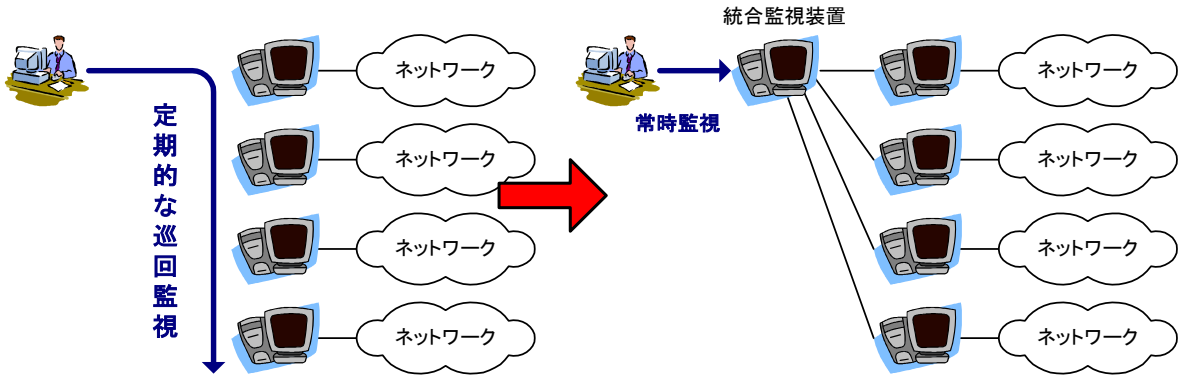


図９　監視フロー１

４．２．２　システムごとに要求される高度なスキル

各システム（技術）に特化した監視装置は監視の方法から障害の通知内容まで非常に詳細で技術的な内容を通知してくるものである．構築された様々なシステムにおいても監視装置のメーカ，ソフトウェア，操作方法が統一されていることが理想的であるが，マルチベンダ環境で低コストなシステムを構築している YSD にとっては不可能なことである．また，近年においてはセキュリティ製品であるファイアウォールや侵入検知ツールなどの監視装置も設置されている．このような環境下において監視要員のスキルを均一にすることは困難であり，最悪の場合 障害を見逃す危険性もある．統合監視装置では技術的な障害メッセージを監視要員向けに変換することが可能であり，即時に障害内容を把握することが可能である．特に夜間の障害においては担当者との電話連絡が主になるため，障害内容の伝達を迅速かつ正確に行なうことができる．（**図 10** 参照）

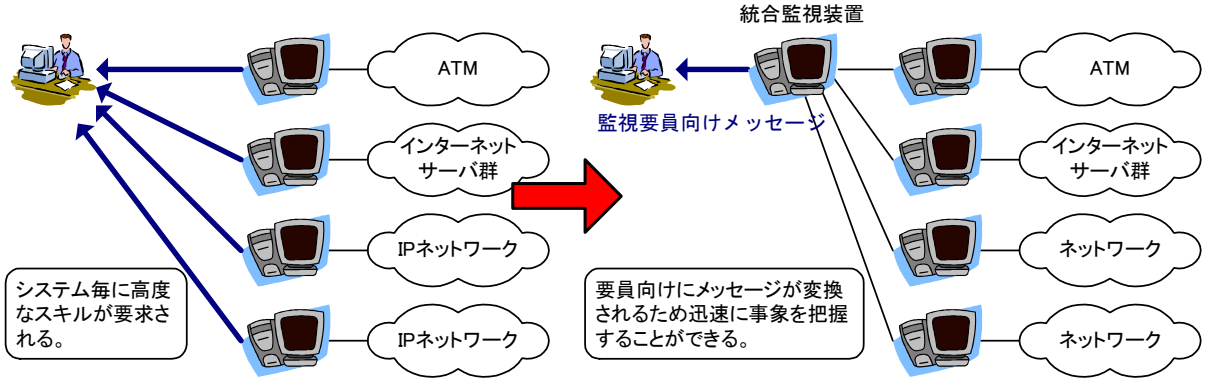


図 10　監視フロー２

４．２．３　影響範囲の迅速な把握

下位層にてアラームが発生した場合，上位にて稼働しているネットワーク及びサーバなどの監視装置から多数のアラームが誘発される．統合監視装置を導入することによって複数のアラームから迅速に原因箇所の把握と影響範囲を把握することができる．特に拠点での停電時は，拠点に設置されている多数のネットワーク（監視装置）からアラームが発生するがアラームを統合的に監視することによって停電やシステムダウンを予想し対応することができる．（**図 11** 参照）

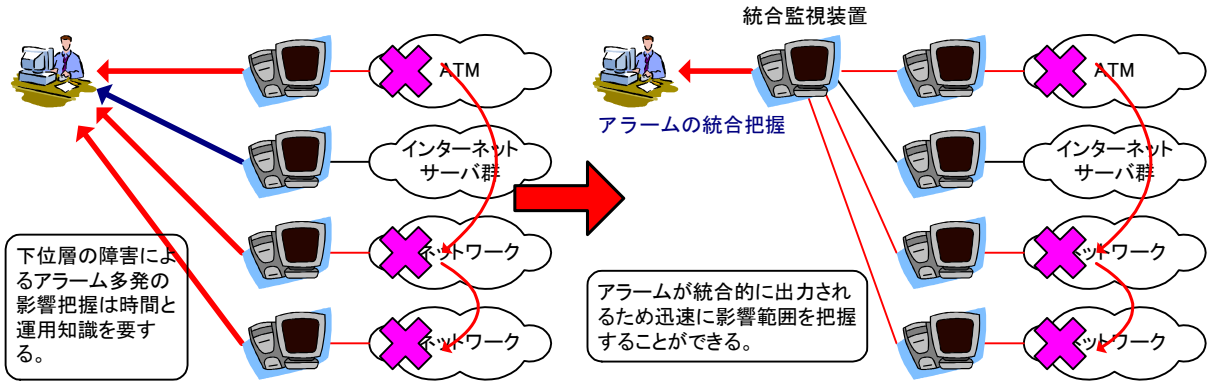


図 11　監視フロー３

４．３　統合監視導入の評価

統合監視装置を利用した監視環境を整備することによって監視業務における監視要員の業務効率アップとスキルの均一化を実施することができた．下記に統合監視装置を導入する前後で，障害の内容と対応内容の変化について述べる．

表７　統合監視導入効果対比表

対応内容	導入前	導入後
ネットワークサポートが第一発見元	185	223
統合監視装置が第一発見元	－	105
アプリケーション障害	12	6
機器の資源不足による障害	－	27
統合監視にて発見した資源不足	－	25

障害が増加しても監視要員は増員していない．

上記 **表７**から機器数の増加により障害件数も増加しているが，多くの障害は統合監視装置での発見及びPATROLやInfoVistaにて資源不足を発見し障害を未然に防いでいることがわかる．

また，今回のような監視体制を整えることによって定量的な効果としてとらえていない部分として障害対応における下記のような人件費の削減ができることが期待できる．

(1) 死活監視にて発生する急な機器ダウンに対する障害

急なシステム停止を伴う障害が発生した場合，障害の早期復旧のためにネットワーク担当者からサーバ管理者，アプリケーション開発者など複数の技術者が夜を徹して対応を行なうこととなるが，詳細な障害の予兆を収集することによって少ない人員で時間にゆとりを持って対応を行なうことが可能となり障害対応に関する人件費を必要最小限に留めることができる．

(2) 性能予測が可能となる

オープンシステム環境においては動作環境と条件が多岐に渡るためキャパシティ・プランニングは非常に困難なことである．現状での性能に関する傾向を分析することによって，無駄な処理及びトラフィックの発見とシステム拡張時の適切な設備投資を行なうことが可能である．

５．今後の課題

５．１　グローバルサーバとの監視の統合

SystemWalker，Tivoli で監視を行なっているグローバルサーバの場合，他のツールとの連携を柔軟に行なうことが可能なため容易にネットワーク監視へ統合が可能となる．

今後の課題としてこれまで統合されていないグローバルサーバのOSやアプリケーションの監視も今回 構築を行なった統合監視環境へ統合することである．障害時の影響範囲の大きいグローバルサーバからインターネットサーバ，ネットワークと統合的に障害を把握することが可能となり，多数の担当者が混乱することなくスムーズに障害対応と迅速な復旧作業を行なえる環境を構築することである．

５．２　セキュリティ監視の対応

システムダウンだけでなく社会的信用を失う要因としてファイアウォールなどのセキュリティ対策やウィルス対策も重要な監視項目となっており，侵入された場合 迅速に正しい知識を持って対応することが重要であり統合監視環境へ統合する必要がある．統合監視環境へ統合することによって迅速な発見と影響範囲を把握することができる．

５．３　データセンタ構築における監視環境の統合

2003 年４月に新しくデータセンタが竣工する予定であり，既設の東京センタ，大阪センタと合わせて３センタ体制となり，データセンタ開設により監視対象が増える予定である．

拠点が増える事により単純に人員増とならないよう，遠隔監視の仕組みを強化し，他拠点からの監視のバックアップ体制，拠点間の人員で作業補完し要員増を最小限に抑えられるような監視環境統合の仕組み作りが必要となる．

５．４　ノウハウ蓄積による障害原因の早期特定

監視体制の改善により障害の早期発見が可能となったが，日々高速化，複雑化し続けるハード構成やアプリケーションから原因を特定するのはより困難になってきているのが実情である．また，システムログやリソース情報を蓄積することから，詳細で大量の情報を得られるようになってきている．この情報の解析方法や，経験的な事例を積み重ねることにより，障害の原因特定，復旧までにかかる時間をできる限り短縮していく必要がある．

６．おわりに

監視の統合を進めていくにあたり，常に考えなければいけないのは，監視・対応を行なうのは機械ではなく人間であるということである．アプリケーションの機能・仕組みを使ってシステム監視を実現することにより，監視装置上からは，正常・異常がはっきりとわかるようになる．しかし実際のシステム監視には，監視要員全体のスキルレベル，連絡・対応といった体制，他の業務との絡み，各担当でのサポート範囲などの人的な不確定要素が多くあり，柔軟性を求められる仕組み，運用が必要である．

システム障害は機会損失と企業イメージを損なうことにつながるため，障害時はよりいっそうの早期復旧が行えるよう努めていく所存である．

今回の仕組みを構築するにあたり多くの問題点を抱えたが，解決に際し富士通をはじめとするメーカ・ベンダーの方々の多大なるサポートによるところが大きかった．この場をお借りして感謝の意を述べたい．