大規模ネットワークシステムにおけるシステム管理/ネットワーク管理の現状

Trend of System Management and Network Management System on Large-Scale Network System

金　子　　勲，高　野　　勉

要　約　従来のネットワーク管理では，接続形態の構成図表示やイベントの表示，さらに性能値のグラフ表示やしきい値監視など，SNMP（Simple Network Management Protocol）ベースの管理を主たる対象要件としてきた．またシステム管理ではサーバの資源管理，ソフトウェア配布，ジョブ制御などの利用者要件に応えられる製品が広く普及してきた．しかし最近ではネットワーク環境や管理要件の変化から，管理範囲や管理情報の内容に変化が見られる．本稿では，特にSLA（Service Level Agreement）の視点からの基本管理機能，ポリシーネットワーキング，インターネット環境での管理などシステム管理とネットワーク管理の現況と今後の動向について述べる．

Abstract　The conventional network management has mainly targeted the SNMP (Simple Network Management Protocol) based management, which provides graphical presentation of the network configurations, the state transition of network events, and the measures of network characteristics, as well as the monitoring of network thresholds. On the other hand, products able to meet the user requirements, such as resources management on servers, software distribution, and job control etc., have diffused widely in the field of systems management.

However, recent changes in network environment and/or the management requirements have lead a large effect on the scope of management and details of management information involved.

This paper describes the current state and future trends of the systems management and network management, including the basic management function especially at the viewpoint of SLA (Service Level Agreement), policy networking, and management activities in the Internet environment.

1. はじめに

近年の大規模ネットワーク管理では，管理の対象は増える一方であり，Web環境で多様なサーバやネットワーク機器があふれ，システムダウンがますます許されない状況になっている．システムダウンの影響は他社や取引先に広がり，ついには顧客の信用を失う．ネットワークの安定運用に欠かせないのが，ネットワーク管理とシステム管理である．

従来のネットワーク管理では，接続形態の構成図表示，障害個所の特定，イベント表示，ネットワーク機器やトラフィックの過負荷などのリアルタイム監視，グラフ表示，しきい値監視，SNMP/MIB/RMONなどの技術を用いた一元管理の製品が使われてきた．システム管理ではサーバリソースのハードウェア/ソフトウェア監視，配布，タスク自動制御，プロセス管理，バックアップなどの管理要求があり，それに応える製品が広く普及している．

一方最近は，ベンダからの運用設計コンサルテーションやハードウェア/ソフトウェアの導入・構築サービス，さらにはMSP（Management Service Provider）やIDC（Internet Data Center）によるアウトソースビジネスなど，管理方法の選択肢も増えてきている．さらに，ビジネスの視点からの，スピーディかつプロアクティブな管理・監視が求められている．ユーザ・業務サービスから見た影響を即時に把握するビジネスサービスビューやサービスグラフィカル構成マップの提供，影響されるサービスの検出とポリシーの自動展開により，短時間で的確な結果を導く．さらに問題の予兆・発生を検知したときは，通常より詳細な情報を自動収集して，状況に応じたプロアクティブな対応を図る．また複合した条件設定やイベントの相関関係設定により，問題解決の糸口を提供したり，原因追求の自動化を図るなど，管理者能力を補完する高度な技術の提供が進んでいる．

本稿では特に，ネットワーク管理のトレンドであるSLAの視点からの基本管理機能，QOS（Quality of Service）ポリシーネットワーキング，インターネット環境での管理，およびBtoBやIDC環境の複合ネットワークの管理など，現在の管理システムの状況と今後の技術動向について述べる．

2. 管理の環境変化と課題

2.1 ネットワークシステム管理環境の変化

ビジネスにとってネットワークが不可欠になったが，その様相は大きく変化している．オープン化やマルチベンダ，マルチプラットフォームは勿論，ESシリーズ[*1]やCSシリーズ[*2]などの高性能サーバの出現や，サーバコンソリデーションの流れがある．またネットワーク自身も拠点の拡大や国内外への広域化，大規模化，ブロードバンド対応機器や負荷分散装置の利用，およびインターネットでの場の広がりなど，イ

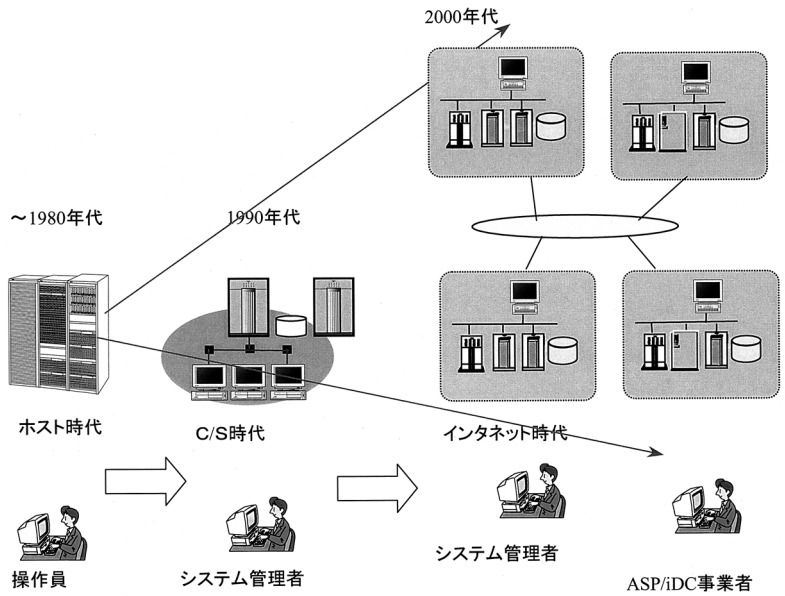

図 1 ネットワークの拡大

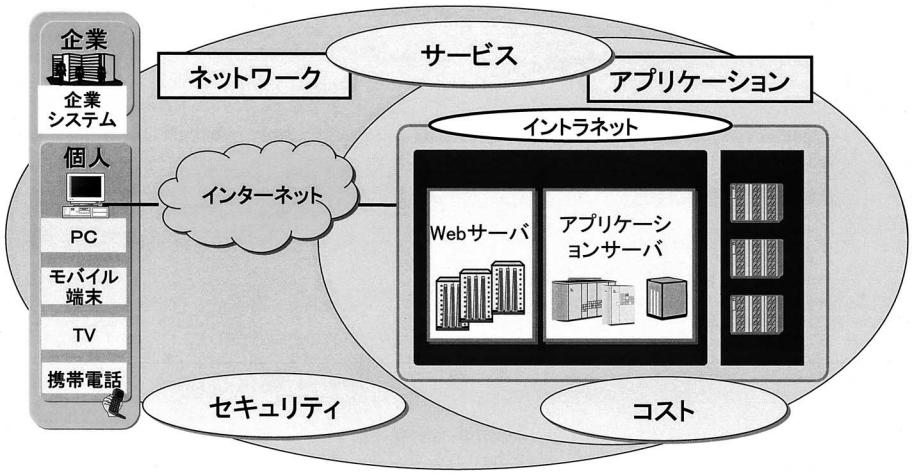

図 2　インターネットによる接続ネットワークモデル例

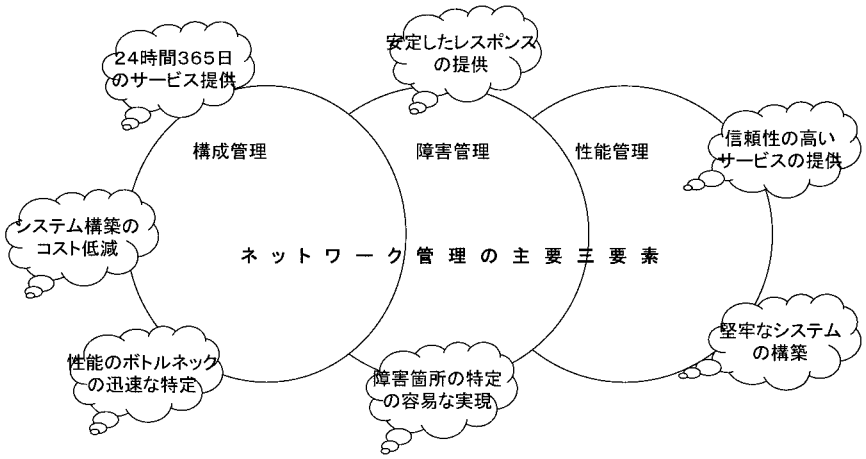

図 3　管理の課題

ンフラの多様化が目立っている（図 1，2，3）．

2.2　管理に対する意識変化

2.2.1　企業側の事情

企業にとってネットワーク・システムの維持管理はコスト以外の何者でもない．サーバやクライアントの運用維持，設定変更，および保守コストが年々増加する．加えて，管理ツールはより高度化し，専門性をもった要員の不足に悩んでいる．管理ツールは，障害を検知し識別してアラーム通知は提供する．しかしながら，定型の対応を超えた複雑な事象に対しては，業務や管理システムに精通した臨機応変な対応が必須であり，一般の保守要員や操作員ではエスカレーションするしか打つ手がない．結局，管理教育や体制の充実からくるコスト増が課題となる．まして年中無休の常時監視では重荷である．従って管理費用を削減すべく，運用管理をアウトソースしてサービス保証を得る道を選択することとなる．これは企業の本来の業務へのパワーシフトともなり意味がある．

2.2.2 ベンダ，SIer 側の事情

ベンダ，SIer は従来からのハウジング・ホスティングサービスや，ASP（Application Service Provider），ISP（Internet Service Provider）などのサービスビジネスを加速している．特に，管理のスケールメリットと，技術力の蓄積・向上も兼ねたアウトソーサとして MSP が台頭してきた．また，Web コンテンツやレスポンスのコンサルテーション・診断サービスや，ストレージ管理サービスも急速に伸びているなか，管理製品とサービスを組み合わせたビジネスで収益を拡大させたい意向がベンダ，SIer 側に存在する．

3. 管理方法の変化に対する対策

3.1 管理コンセプトの変化

多くのベンダがシステム管理とネットワーク管理のコンセプトとして，サービス品質，コスト低減，およびセキュリティ維持を挙げている．サービス品質を数値化し保証するため，運用の簡素化や自動化を目的としたツールを提供したり，ビジネス戦略・情報維持の面からセキュリティ対策を施すことが柱となっている．

サービス品質 SLA 契約には，IDC，ISP，MSP のようなサービスプロバイダと企業との間や，社内の情情システム部門と他部署との間もあり，より客観的な評価が普及しつつある．いずれもその内容は，障害対応時間，応答時間，システム可用性，エラー率など非常に分かりやすい指標である．目標を達成できない場合は一般的にペナルティが課せられる．特に障害管理と性能管理の側面で適用されている．

コスト削減の省力化には，ジョブ起動・連携の運用の自動化やソフトウェア配布・導入，さらには PC などの IT 資産の一元管理やライセンス管理などの効率向上が挙げられる．

セキュリティでは，外部からの不正アクセスの検知・防御など安全で信頼されるセキュアなシステムの実現がある．データへのアクセス制御や機密情報の漏洩防止策，コンテンツのアクセス管理など，強固な情報管理の要求があり，要求を満たす運用管理製品が数多く利用されている．

3.2 サービスレベル管理へのシフトおよび基本管理機能のサービスレベルマッピング

3 大基本管理機能である障害，性能，および構成管理をサービスレベル管理と対応づけするとおよそ表 1 の通りとなる．

表 1 サービスレベルマッピング

障害管理	サービスが使用可能な時間割合や障害からの回復時間など
性能管理	応答時間，ネットワークトラフィックなど
構成管理	ネットワーク構成、インベントリ、障害箇所の特定など

プロバイダはこれらの結果レポートをユーザが Web により参照することができるようなサービスを提供する．さらにレポートのカレンダ制御，時系列加工のサービスなども提供する．これらのサービスレベル管理機能を SLM（Service Level Management）サーバに集約するアプローチもとられ，サーバ自体の障害対策や自動運転も実現されてきている．

3.2.1 障害管理サービスの SLA

1) 障害管理からみたサービスレベル管理

障害管理の SLA には，ネットワークの IP の稼働管理，ネットワーク機器の異常監視がある．管理者は SLA で決められた障害復旧時間内に問題を解決すべく，障害機器の特定，障害の切り分け，ベンダへの修復依頼，回復手順指示等，迅速な対応を求められる．障害対応手順は通常，障害検知，アラーム通知，資料採取，解析，原因追求，問題の除去，ハードウェア交換，修復，代替機器への切り替え，モジュール修正，入れ替え，報告となる．

トラブル・障害の未然防止の SLA を満たすものとして，稼働率報告やアラーム通知がある．回線使用率，CPU 使用率およびディスク使用率などの表示はもとより，事前設定値との比較や，過去データとの比較による通知などが行われる．ユーザは障害発生前にシステム低下やダウンなどの異常事態を予測検知して，トラブルを未然防止する．故障原因の関連付けにより，障害個所の特定のスピードアップを図り，ユーザとの SLA 契約を守ることができる．メールでの通知やリモコン画面での状況把握により，場所を問わず，障害の詳細や原因を探る手段を提供できる．イベント関連付けや通知内容の条件選択，対応メッセージ変更などの機能が，多くの管理ツールにインテリジェントサービス機能として組み込まれ，プロアクティブ監視を実現している．

2) イベント相関処理機能による効果的な障害管理および迅速な検知

問題解析は，個人の経験からくるスキルや既知の問題の情報を蓄積して，共有することが近道である．イベント相関処理機能 ECS（Event Correlation Service）はシステム的に原因追求スピードアップを図る一例である．管理システムに通知されるイベントは，ネットワーク構成図上に反映され，機器のシンボルの色で認識できるし，障害情報はテキストでも表示される．しかし大量のイベントが発生した場合，管理者が重要なイベントを見逃す可能性があるため，イベント相関処理機能によりイベントに対して関連付けを設定しておき不要な表示は省略する．障害時の情報をピンポイント化する事で，問題の早期解決および効率的な監視運用が可能となる．表 2 に相関定義の例を示す．

表 2　相関定義例

コネクタ停止相関定義	ネットワーク・デバイスの物理的障害とコネクタ・デバイスの障害（ルータ等）により発生した障害を区別し，マップとアラーム・ブラウザに表示する．
計画保守相関定義	メンテナンス中の機器からのイベントを一定期間だけ無視する．
繰り返しイベント相関定義	あるイベントに付随した複数のイベントを 1 つに纏めてブラウザ上に表示する．（例）装置入れ替えによる MAC アドレス変更．
ペア・イベント相関定義	あるイベントがアラームブラウザ中の関連するイベントを削除または受諾する．

3) 障害管理対象の変化・高度化

管理ツールは統合一元管理を目指している一方，末端に配置するエージェントが益々インテリジェント化して自立し，中央の負荷軽減に一役買っている．特にサーバやネットワーク機器のハードウェア監視や，リソース監視・制御を司るツ

ールが各機器ベンダから出ている．知識エージェントを配置して，電源，ファン等のハードウェア障害を検知したり，性能値の自動チェックやパラメータの変更などを行う． ESシリーズで提供されるES System Managerの例を表3に示す．ネットワーク機器の管理にはCiscoWorks 2000JP 1/LAN element Managerのような機器ベンダ固有の管理アプリケーションがある．機器のバックパネルの画面を管理システムで表示できる．機器固有の診断やステータスが表示でき，障害箇所の特定がスムーズに行なえる．また，管理システムに通知されるイベントログを蓄積し，過去の履歴から障害傾向を分析して，障害予防に役立てる．

表 3　ES System Manager 機器管理項目

ess3.0		機　能
System Manager	Consolidated View	個々の ES シリーズサーバのパォーマンス情報や構成情報などを Web ブラウザや MMC から監視することができる.
	System Definition	ES シリーズサーバに関係付けられた MIB オブジェクトを定義する.
	System Manager World View または System Manager Interface for HP OpenView NNM	ネットワーク上に配置されたESシリーズサーバを監視する. HP OpenView NNM(または JP1/Cm2 NNM) 上でネットワーク上に配置されたESシリーズサーバを監視する.
AdminTools	Analysis Manager	システムやアプリケーション障害が発生した時の解析に必要な資料を採取するツール.
	Event Log Manager	イベントログの情報を調べ，新しいイベントの記録を監視したり，記録内容を集める.
	Power Manager	システムの電源オン・オフをスケジュールする. ES5000 シリーズでのみ使用可能(ES7000 では，APSC を，使用する).
	Restart Manager	プロセスの実行が正常かどうかを監視し，必要に応じてシステムを再起動する.
	Service Manager	Windows サービスの障害を検出し，それに対するアクションを設定する.
	Threshold Manager	パフォーマンスカウンタに関するしきい値を設定し，それに対して特定のイベントを起動する.

3.2.2　性能管理サービスの SLA

1)　ネットワークトラフィックのサービスレベル管理

性能管理の SLA には，パケット流量，利用率，センタとユーザが接続するアクセスポイント間のレスポンス監視，ダイヤルアップルータのビジー率監視，などがある．それを日，週，月，年毎に報告し，定常的な状況把握や傾向分析にあてる．キャパシティプランニングの材料ともなる．

2)　性能予測

システム構成情報，ネットワークの負荷情報，サーバの利用状況などから，将来的にサービスレベルが保証できるかを予想する．設備増強などの拡張計画を支援する．またソフトウェアの使用状況を収集し，評価やレポートを提供する．

各種サーバの性能情報の収集から，目的別のデータ評価，単体データの増減傾向分析や，一歩進んで，複数の性能管理ソースとデータ項目を関連付けて条件と結果を解析するなど色々な予測方法がとられている．

ネットワークトラフィックに関しても常時データを収集・蓄積し，データの傾向分析に役立てる．一方，管理対象であるエージェント側には蓄積されたデータ

を分析するのみならず，将来の予測や，構成変更，追加した場合のシミュレーションを行い，拡張計画の検証を行う．

3) Web トランザクションのサービスレベル管理

SLA の要件の一つにエンドユーザからみた性能評価尺度がある．Web サイトの利用者からみたレスポンス性能評価により最適な Web サイトの運営を支援する．また各種インターネットプロトコル毎のサービス品質を維持する．さらには管理者のみならず経営やマーケティングサイドからも SLA の達成度や性能の傾向分析などの要求が起きている．

これらのサービス管理を実現するものとして HP（ヒューレットパッカード）社および日立製作所では，Web Transaction Observer（WTO）や Internet Services（IS），さらに Vantage Point Reporter の提供を開始した．

ISP やアウトソーサにとって，エンドユーザがどのようなサービスを体験しているかを把握することは不可欠になってきている．ISP は，ユーザの満足できるレベルで IT サービスを提供できているか，測定を基本としたパフォーマンス管理を通してサービスの改善を図るものである．ネットワーク上にプローブを配置して，Web，メール，FTP，DNS など多様なサービスプロトコルをユーザサイトから監視測定しリアルタイムに表示するもので，クライアントへのソフトウェア導入が不要なことが特徴である．リアルタイムレポートは問題解析に，中長期のレポートはトレンド分析に活用できる．また Web ビジネスに特化した測定ツールである WTO はクライアントに直接アプレットをダウンロードして，トランザクションの動き，集中度合い，滞留時間，アクセス中断や失敗回数など体感情報を収集する．サービス統計は管理部門，ビジネス推進・マーケティング部門で利用可能であり，分析・改善に利用できる．従来の管理者の目からの定量的なパフォーマンスデータの把握や障害検知から，ユーザに視点を変えた，ビジネス指向管理の一例である．

4) ログ

イントラネット環境だけでなく，BtoB 環境や DMZ（非武装ゾーン）に存在するサーバから出力されるイベントログ，システムログ，SNMP トラップなどのログファイルを集中監視する．

複数拠点に存在するログを夜間などに集約・分析することも通常行われている．

3.2.3 構成管理サービスの SLA

1) 図面管理

構成管理の SLA にはハードウェア/ソフトウェアの資産管理やネットワークの接続状況管理，さらには電源，ケーブル，ラック，およびビルなどの設備・図面管理などがある．

管理システムが持つネットワーク構成図は論理上の構成を表しており，ネットワークセグメント毎に自動作成される．このため，物理的にフロアや部屋が分かれていてもセグメントが同じであれば構成図上は同じ場所となる．障害が構成図上で検知できたとしても機器がどこにあるのか判別できなくては迅速な対応はで

きない．カスタマイズして物理的な配置に構成図を手動で追加作成可能であるが手間とコストが掛かる．このような場合，管理システムの構成図を取り込んであらかじめ作成しておいたフロアレイアウト図に機器を配置できる製品が多く提供されている．LAN ケーブル配線やハブのどこのポートにどの機器が接続されているかも表示する．ラックマウント状況の機器配置や写真を取り込めるので極めて直感的に認識できることになる．例を図 4 に示す．

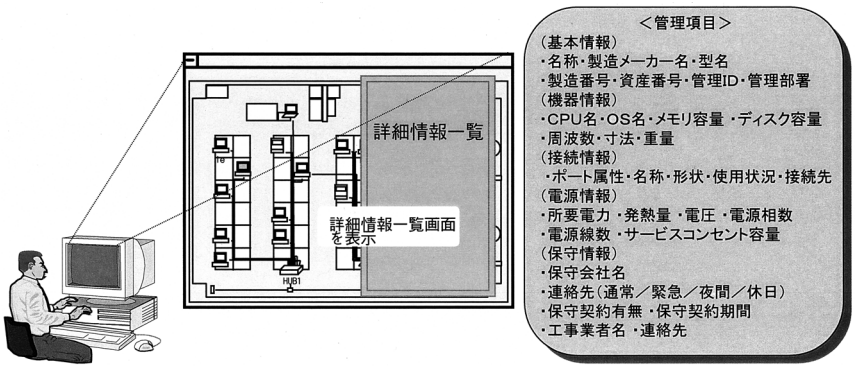

図 4　図面/資産管理

3.3　管理要件の多様化への対応

3.3.1　複合ネットワークの管理

1）　SNMP Gateway 概要

インターネットに接続されたネットワークでは，セキュリティ確保のため Firewall で社内の LAN との接続を分断したり，グローバル IP アドレス不足のためローカル IP アドレスを割当てている．これらの環境を管理するには，NAT（ネットワークアドレス変換）による IP アドレス変換を使用するが，ping による機器の生死監視はできても SNMP パケットまでは NAT でもアドレス変換が行われず，管理に不備があった．特に iDC のような複数のユーザのサーバを管理したり，リモート監視センターなどの場合は，IP アドレスが重複するといった問題もある．監視マネージャも，ローカルネットワークの管理対象を意識できるようアドレス対応づけする機能と，SNMP パケット内の MIB（Management Information Base）のローカルアドレスなどデータ変換機能が必要である．JP 1 ではこのための製品として Internet SNMP Gateway を追加した．

製品の特徴を表 4 に示す．

2）　SNMP Gateway のアドレス変換の仕組み

SNMP アドレス変換は，被管理側の Internet SNMP Gateway でアドレスを変換する構成と，管理側の Internet SNMP Gateway で変換する構成の 2 種類がとれる．管理側で変換すれば，一元管理・保守が容易になるが，性能は落ちる．逆にアドレス変換効率を上げるため，被管理側で変換すると，アドレス管理が分散し，管理・保守性が落ちることになる．どちらを重視するかで選択が分かれる．

表 4　JP 1/Cm 2/Internet SNMP Gateway の特長

特徴	概要/特徴
アドレスが競合する複数のプライベートネットワークを統合マネージャで管理	監視マップ上でネットワーク管理用の管理用アドレスを割り当て、アドレス変換によりアドレスの競合を解決して管理する.
NAT で割り当てたグローバルアドレスを使用した管理	スタティック NAT 環境においては，スタティックに割り当てられているグローバルアドレスを使用してネットワーク管理が可能.
ダイナミック NAT への適用	監視対象のグローバルアドレスが NAT によって動的に割り当てられているような場合でも管理が可能．この場合は，管理用アドレスとして仮想的なアドレスを割り当てて管理する.
グローバルアドレスを持たないローカルノードの管理	プライベートネットワーク内の実際には外部と接続していないローカルノードについても管理可能．この場合も管理用のアドレスとして仮想的なアドレスを割り当てて管理する.

被管理側でアドレスを変換する場合を例に，仕組みと流れを説明する．ここでは SNMP 要求・応答の流れを図 5 に示す． トラップも向き以外は同じ処理となる.

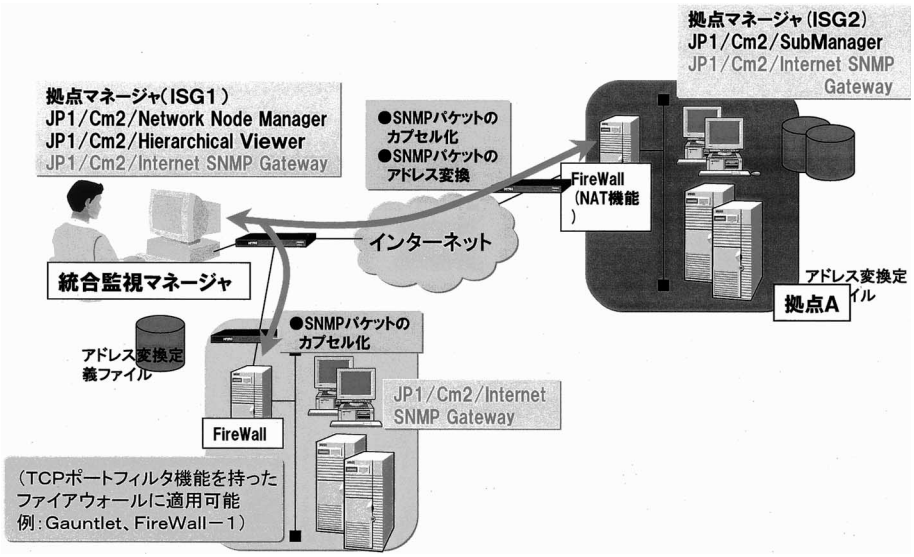

図 5　被管理側でアドレスを変換する場合の SNMP 要求発行と応答

① 管理側の ISG 1 は，同一ノード上の NNM（Network Node Manager）から管理用アドレスの SNMP 要求を受け取る.

② SNMP 要求応答定義ファイルに従って，被管理側の ISG 2 へ通知.

③ 被管理側の ISG 2 は，通知された SNMP 要求中のアドレス情報について，アドレス変換定義ファイル, 変換対象 MIB 定義ファイル, 変換対象文字列 MIB 値定義ファイルに従ってアドレスを変換し，実アドレスの SNMP 要求を生成する.

④ 生成した実アドレスの SNMP 要求をエージェントへ発行する.

⑤ エージェントからの SNMP 応答は被管理側 ISG 2 が受け取る.

⑥ 被管理側 ISG 2 は，受け取った実アドレスの SNMP 応答をアドレス変換定

義ファイル，変換対象 MIB 定義ファイル，変換対象文字列 MIB 値定義ファイルに従ってアドレスを変換し，管理用アドレスの SNMP 応答を生成する．

⑦　被管理側 ISG 2 は，管理用アドレスの SNMP 応答を管理側 ISG 1 に送信する．

⑧　管理側 ISG 1 は NNM へ SNMP 応答を返す．

3）　Firewall 越え

セキュリティ強化には通常 Firewall を挟むが，管理マネージャのなりすましによるエージェントへの設定変更も考えられるため，Firewall で全ての SNMP パケットを通すのは危険である．従って，管理マネージャの IP アドレスをもつ Ping/SNMP パケットのみを通すよう設定すべきである．更に，SNMP のパスワードであるコミュニティ名には，ディフォルトとして広く知られている public や private は使用せず，独自の設定を施して不正侵入を防ぐべきである．一方，管理システムを階層化して，Firewall 配下にサブマネージャを配置することにより，外部からの ping/SNMP パケットを遮断する方法もある．しかし，ポートは遮断したいがサブマネージャなどの大掛かりな階層構造までは採りたくないケースが大半である．このような場合のためにも，SNMP　Gateway がある．この製品は SNMP パケットをカプセル化して TCP パケットに変換する機能を提供することで，サブマネージャを使わず，かつ well-known port を遮断しても Firewall を越えることができる構成を実現している．

4）　サーバ

アプリケーション間の分断や，ユーザアクセス制御，および不正検知システムの採用なども考慮しなければならない．

3.3.2　ビジネス指向の管理

企業内ではすべての管理対象を統合して管理することに主眼が置かれてきた．統合オペレーションや統合マネージャと呼ばれている．しかし，IDC やプロバイダなどの複合ネットワーク環境では全体の監視・管理とともに，個々の独立したネットワーク・システム管理も求められる．すなわちユーザ向けに各種の情報を提供することが望まれる．例えば，サービスプロバイダのユーザ向けポータル Web サイトを動的に作成する．ユーザ毎の IT インフラを定義することで，ユーザ毎のサービス状況を表示する．ユーザ毎の SLA レポート機能．さらにサービス契約状況や，広告などもユーザ毎に提示する．これらの企業別ポータルサービスが，ビジネスプロセス管理とともに，ビジネス指向管理の一つの流れになっている．

3.3.3　ポリシーマネージメント

ユーザ・会員単位での論理的な帯域要求に対して最適なルートを選択し，効率的なネットワーク運用を実現する．その一つの解決策としてポリシーベースネットワーキングが普及し始めている

1）　ポリシーベースネットワーキングの動向

システムの運用に関する様々な対象や局面に対してポリシー（方針）を作成することが多くなってきた．すなわち判断の基準を設けることを考え始めている．しかし対象や状況が多種多様であり，一様に基準を設定しあらかじめデータベー

ス化して自動化を図ることは非常に難しい．そこでネットワーク機器やソフトウェアについて特に資源管理と処置を自動化することを目指すアプローチが採られている．特定の性能・資源条件を規定し，それに該当した場合のアクションを取り決めて，規則集を作る．これをもとに色々な場面での効率的な振る舞いを導き出すことを，ポリシーベースのネットワーキングと呼ぶ．

より業務・ビジネスにとって重要な基幹系のデータ通信をメールなどのOA系通信より優先したり，特定ユーザのみネットワークへのアクセスを許したりすることがそれに当たる．ネットワーク資源の有効活用や利用者へのサービス向上を，さらには管理コストの低減を目的にしている．ポリシーベースネットワーキングを実現するためには，ポリシーサーバとして，ルールを格納するポリシーリポジトリと制御コントローラ，およびGUIやAPIを提供するポリシーツール群が提供される．リポジトリはディレクトリ形態が一般的となっている．一方被制御側はポリシーに従って機器を制御するモジュールを搭載する．

2) QOSでの利用

インターネットの普及に伴い，IP通信の品質保証が求めれれている．ルータにもRSVP(Resource Reservation Protocol)やDiffserv(Differentiated Services)などの標準技術が追加されてきた．ネットワーク全体にルールを配布し一貫したポリシー制御を可能にしている．RSVPはリソース要求パケットをルータに送りあらかじめ帯域を確保する仕組みであり,動的な制御が可能であるが,反面RSVPパケットが大量に出ると負荷が大きくなる．一方Diffservは，パケットの先頭のIP TOSフィールドを再定義して6ビットのDSコードポイントを設け，そこに優先度や帯域の相対的なクラスを設定し，QOSを実現する手法である．集約されたフロー間で転送サービスを差別化する．RFC 2474[*3]とRFC 2475[*4]に規定されている．クラスにパターン分類するため比較的実装はしやすいが，ドメイン内の全ルータにおいてクラスを統一しておくことが前提となる．これらの基本仕様と合せてポリシーベースネットワーキングのフレームワーク概要やモデル，およびCOPS (Common Open Policy Service) 制御プロトコルやPIB (Policy Information Base)，さらにCIM（Common Information Model）への組み込みなどもIETF[*5]で検討されている．

図6にCOPS-DSのモデルを示す．

これらの技術をもつネットワーク機器や制御ソフトウェアが製品化され，漸く研究段階から実用化段階に移ってきた．当社ではHP社OpenViewおよび日立製作所JP1から共同開発のQOS Policy Xpertを提供している．ミッションクリティカルなアプリケーションや音声アプリケーションの帯域をDiffservで実現している．多数の通信トラフィックを少数のグループに集約するので，従来のコネクション単位のQOS制御に比べてルータや管理サーバにかかる負荷が小さくシステムに無理なく適用できる．

サーバやクライアント内のエンドホストエージェントに次のような情報を与えてマシンからの通信データを識別する．エージェントの種類を表5，ポリシー設定項目を表6に，システム構成を図7に示す．

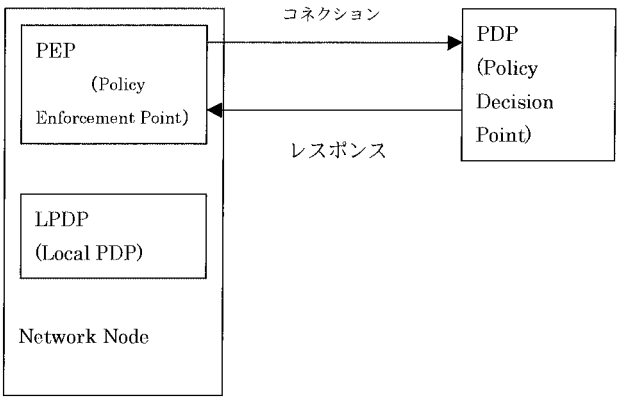

図 6 COPS-DS

表 5 Policy Xpert 管理対象機器

	GR2000 プロキシ エージェント	Ciscoルータ プロキシエージェント	PacketShaper プロキシエージェント	エンドホスト エージェント
対象機器	GR2000-2S,4S, 6H,10H,20H	Cisco 2500,2600, 3600,4000,7200,7500	PacketShaper 1500, 2500,4500	クライアント、 サーバ
稼動環境	WindowsNT/2000	WindowsNT/2000	WindowsNT/2000	WindowsNT/2000

表 6 ポリシー設定項目（条件と動作）

ポリシー	項目	概要
条件	IPｱﾄﾞﾚｽ指定	宛先及び発信元IPアドレスによるデータの識別
	ﾎﾟｰﾄ番号指定	TCP及びUDPのポート番号によるデータの識別
	ﾌﾟﾛﾄｺﾙ種別指定	TCP/UDPのプロトコル種別によるデータの識別
	日時,曜日指定	日付，時間，曜日による条件付け
	URL指定	WebのURLによるデータの識別
	データ転送速度	データ転送速度のしきい値による条件付け
	DSCP指定	DiffServのサービス識別子によるデータの識別
動作	優先度	データ転送優先度(使用する優先度キュー)の選択
	帯域制御	データ転送速度の上限値を設定
	DSCP値設定	DiffServのサービス識別子を設定

3) 管理マネージャとの連携

JP 1 Policy Xpert を例にとると，この製品は JP 1/Cm 2/NNM と連携し，ポリシーサーバの障害表示, マップへの反映, イベントアラームブラウザへの通知・記録などの機能も提供する．管理対象機器を表 7 に示す．ルータ側にはクラスファイア（フロー識別），マーカ（IP ヘッダへの DSCP 値書き込み），UPC（ユーザ契約帯域監視），シェーパ（送信帯域制御）などの機能が必要である．

しかし実際にはネットワークや業務全体にわたり，非常に定義が複雑となる．このため JP 1 では Policy Xpert のさらに上位の製品として IPRM（IP リソースマネージメントサーバ）を提供している．テンプレートの提供や QOS ポリシー

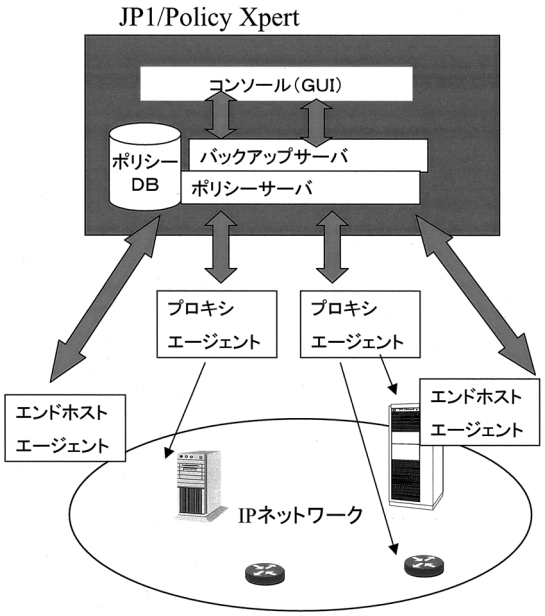

図 7　Policy Xpert 構成図

の抽象化により複雑な QOS 制御システムをより簡単に実現できる．サービス要求単位で QOS の設定や追加変更が可能である．例えば適用するサービスの種類・クラスのサービス要求は表 7 のように指定できる．適用イメージには，NNM からのルータトポロジ情報などの管理ネットワーク定義，サービスクラス・DS ドメイン設定などの QOS 初期設定，および個々の条件・帯域情報チェックなどのサービス要求の，3 段階操作からなる．またネットワーク管理者は帯域の割り当て状況を容易に表やグラフでビジュアルに把握できる．

表 7　サービス要求

ポリシー	指定項目	GR2000	Cisco ルータ	PacketShaper	エンドホスト
条件	IP アドレス	○	○	○	○
	ポート番号	○	○	○	○
	プロトコル種別	○	○	○	○
	日時，曜日	○	○	○	○
	URL	×	×	○	○
	DSCP	○	○	×	○
動作	優先度	○	○	○	○
	帯域制御	○	○	○	○
	DiffServ	○	○	×	○

3.3.4　システム管理対象の多様化

1)　ストレージ管理

システム管理面ではサーバの資源管理が中心であったが，アプリケーション中心の上位レイヤ管理にシフトしている．SAP や OAS（Oracle Application Server）などの ERP 管理などであるが，やはり主流はまだサービスのプロセスやアプリケーションの障害管理の域を出ない．

一方，顧客情報，商品情報などから，トランザクションデータやWebコンテンツ情報などまで，データベース管理が急激に増加している．eビジネスの普及やIDCの出現によりデータを保護する要件が高まり，高速で大容量のストレージも必要となっている．システムの主要要素としてこのストレージが占める割合が急激に拡大したため，IDCやMSPではストレージの運用管理サービスが大きな柱になった．従来のネットワーク管理にNAS（ネットワーク接続型ストレージ）管理やSAN（ストレージエリアネットワーク）管理を追加している．これらに対しては表8のような管理項目があり，SNMP　MIB化もIETFで行われている．

表 8　ストレージ管理項目

SAN 内のスイッチやストレージ装置の障害・性能管理	・ ディスク，データベース容量不足 ・ テープマウント情報や運用状況 ・ バックアップ状況や結果の監視
ディスクアレイ管理	・ SAN 構成の把握，論理パスの設定，診断など

ストレージ管理のサービス例を示す．

・ハードディスクのデータストレージ・サービス
・データ・バックアップ・リストア・サービス
・リアルタイム・データ・レプリケーション・サービス
・データの正確さや情報の信頼性の保証
・顧客のサービス利用状況の報告，データ容量やアカウンティング情報のレポート

2）リモートコントロール

監視ルーム以外からの状況確認や指示のため，あるいは災害対策からの予備監視形態などを可能にするための遠隔監視，リモートコントロールが多く採用されている．複数拠点に存在する運用管理サーバを集中化して複数コンソールをセンター1個所で統合管理するスケーラブルな運用管理形態など柔軟性も増している．リモート監視もWebベースの浸透に伴い，モバイルや携帯電話からも可能になった．リモートへアクセスが可能である反面セキュリティには注意が必要である．衛星経由での情報配信や監視も実現している．

3）モバイルデバイス

モバイルデバイス自身の設定が不要に成り，通信機器側からの遠隔操作で，各種のサポートやアップデートが行えるようになった．モバイルデバイスを管理する国際標準も近く制定される見とおしである．

3.3.5　管理システムの信頼性向上

1）監視の二重化

24時間365日運用サービスに向けてネットワークの信頼性を向上させるため，ネットワーク機器や電源供給装置の二重化を図る．ネットワーク機器ベンダではHSRP（HotStanby Router Protocol）やVRRP（Virtual Router Redundancy Pro-

tocol）を使用した切り替え機能を提供している．お互いの機器をハートビートにより監視し，無応答になった場合は障害とみなし，自動で切換える．これらに加えて WAN 回線の障害対策としてバックアップ回線の確保も必要となる．専用回線が障害時，ISDN 回線に自動または手動で切換えられるよう配慮する．

また一般的に重要な業務サーバでは障害に備えてクラスタリング技術により信頼性を向上させている．データを引継ぐためディスク装置は共用させ，かつ RAID（Redundant Arrays of Inexpensive Disks）構成を採る．

LAN ボードの二重化，無停電電源装置の採用，あるいはバックアップ監視センターなど，要求に応じてガードを強化する．

使用者，経営者層にとっては障害により切換えが起きたとしても，業務に支障がなければ問題視する必要がないが，管理者にはどちらに障害が起きたかを知る必要がある．二重化構成を取るサーバや機器は，業務アプリケーションが障害時の切換えを意識せずに済むように，IP アドレスを引継ぐ機能を持つ．この場合，仮想 IP アドレスを使用する場合が多い．管理システムがこの仮想 IP アドレスを管理すると常に正常である可能性が高いため，管理者が切換えを知るには，実 IP アドレスで管理する必要がある．

業務サーバと管理サーバを共に二重化した場合の監視では次の点に留意することが必要である．

・管理マネージャ，管理 DB，管理構成ファイルを両監視サーバに準備する．
・業務サーバは本番・待機系の実アドレスで監視する．
・管理収集データは共用ディスクに採取保存する．管理サーバの障害切替え時に共用ディスクから従系のマネージャにリストアした後で従系を起動する．
・業務サーバからのトラップの宛先は両管理サーバ共通の仮想アドレスを使う．管理サーバがフェールオーバしても宛先はそのまま使用できる．JP 1/Cm 2 の場合は NNM からエージェント側のトラップ設定が行える．
・業務サーバでのプロセスや性能管理エージェントは両方とも稼動させ，どちらの情報も常時取得する．
・ログファイルの採取は共用ディスクのマウントと監視の停止・切替え・再起動が必要．

2）　ナレッジエージェント

また管理マネージャに対応するナレッジモジュールを被管理サーバやネットワーク機器に組み込むことで，それぞれの管理項目を統一した方式で管理することが一般化している．条件や動作をカスタマイズするための API やスクリプトが各管理製品で提供されている．ES シリーズのスクリプトの例を示す．例では使用可能なメモリバイト数をメッセージボックスに表示する．

```
'**********************************************************************
' GetAvailableMemory.vbs
'
' This script demonstrates using the CurrentValue property of a
' counter by displaying the amount of available memory in a message box.
'
Option Explicit
Dim objThreshold
Set objThreshold = CreateObject("Unisys.esThreshold")

objThreshold.Pathname = "¥Memory¥Available Bytes"
MsgBox "The system currently has " & objThreshold.CurrentValue &_
        " bytes of available memory"
```

4. 実験的な試みの紹介

今まではなかった動きの例として情報処理相互運用技術協会（INTAP）のOSMIC（Open Systems Management Industry Collaboration）の活動を最後に紹介する（図8）．管理製品の相互接続を実現し，管理システムの共存を目指す動きである．

システム運用管理ツール市場において，システムモデル標準化は進んでいるものの，具体的な実装レベルは進んでいない．特にインターネット環境においてはマルチベンダ環境での運用が必須であり，ベンダの壁を越えた具体的な共通仕様と接続の確立が求められている．その実現のため，複数のシステム運用管理事業者が参加して，オープンプロセスで新たな共通仕様の策定や相互接続の実証を行っている．

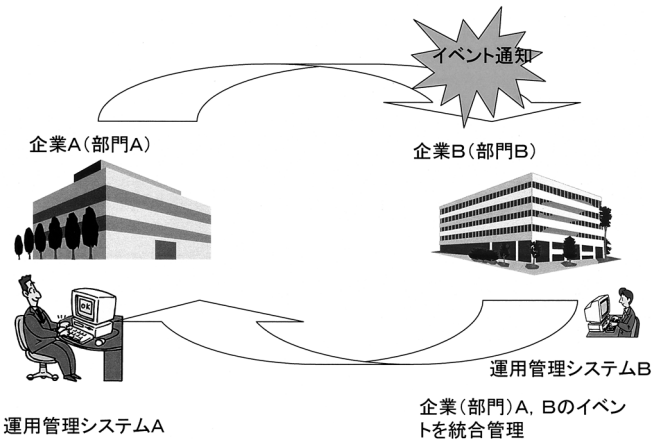

図 8　OSMICの概略

企業のインターネットへの接続が急速に増加して,インターネットを介しての BtoB システム連携が拡大した．このためそれぞれの企業で採用している異なるシステム運用管理ツールの連携が欠かせない要求となっている.システムの分散化やハウジング,ホスティングによりネットワークを介した遠隔地からのシステム運用もニーズも拡大している．

OSMIC では表 9 に示す「インターネット環境における運用管理システムの相互接続フレームワーク MAXI Version 1.0」を策定した．

表 9　MAXI 1.0 相互接続仕様（抜粋）

イベントレベルの XML へのマッピング	・イベント共通モデル，イベント形式を定義 ・イベントエンコードルールを定義,DMTF CIM 形式での記述(CIM/XML 2.0 準拠のクラス定義)，Event Common/Event Attribute Group，Event Attribute ・アラーム系共通イベントの XML 定義，CIM を XML にマッピングするためのスキーマ(CIM_DTD)の規約
Point to Point での伝送手順	・SMTP によるイベント伝送 ・DES CBC により暗号化

2001 年 4 月現在，当社を含む 25 社が参加している．2000 年から活動を開始して，MAXI を 9 月にリリース，各社実装の後，2001 年の 1 月と 3 月に異ツール間のイベント連携テストを実施した．JP 1（日立），SystemWalker（富士通），WebSAM（日本電気）などが実証評価に参加し，接続実験に成功した．接続実証や技術動向調査，プロモーションに加えて，今後は情報取得系の標準化を目指して，サービスレベルでの共通プロトコルの策定やよりタイトなオブジェクトレベルでの連携検討を予定している．

5. おわりに

運用管理は効率追求型からビジネスの道具として発展しつつある．従来のネットワーク管理はモニタリングを軸に障害の迅速な対応や，アクションの自動化を目指してきた．システム管理もジョブ管理，配布管理，バックアップなどの強化に努めてきた．ポイントソリューションは，フレームワーク上に管理製品を積むアーキテクチャをベースとしたトータルソリューションに発展し，遠隔の設定や監視制御を受け持つ自立エージェントとの連携も統合化へのシフトを加速した．これらの技術をもとに複合ネットワークの新たな要求に応える製品が逐次提供されている．

ご紹介したように環境変化とともに色々な製品やサービスが管理の方向を変えている．MSP や SSP（Storage Service Provider）に代表される運用管理サービスが始まり，管理を取り巻く世界が新たな方向に動いてきた．当社でも asaban 事業や電力マーケットプレイス，および金融共同センターなどで新たな技術をベースとした運用管理の検討・強化を進めている．今後もネットワークの変化やビジネスの変化に追随する管理ソリューションとサービスを順次提供する．例えば IPv 6 の拡大は家庭内機器の管理や非 IP までも管理対象とするかもしれない．今まで以上に複雑な管理ポリシ

ーや SLA が求められるであろう．管理の重要性が益々高まっている．

＊ 1　ユニシスの PC サーバ．ES 2000，ES 5000，ES 7000 シリーズがある．
＊ 2　ユニシスの次世代汎用機．
＊ 3　Definition of the Differentiated Services Field（DS Field）in the IPv 4 and IPv 6 Headers
＊ 4　An Architecture for Differentiated Service
＊ 5　Internet Engineering Task Force インタネットの標準化組織

参考文献

［1］「HP OpenView Product Brief」日本ヒューレットパッカード　2000 年 7 月
［2］「JP 1 V 6 I パートナ向け研修資料」日立製作所　2001 年
［3］「US e-Service Report」富士経済 USA 2001 年 2 月
［4］「HP OpenView セミナ資料」日本ヒューレットパッカード　2001 年 4 月
［5］「ネットワーク管理製品群戦略」シスコシステムズ　2001 年
［6］「INTAP ジャーナル NO 59」情報処理相互運用技術協会　2001 年 3 月

執筆者紹介

金　子　　勲（Isao Kaneko）
1976 年青山学院大学理工学部卒業．同年日本ユニシス（株）入社．金融オンラインパッケージ，PC 通信，電子メールシステム，OSI 製品などの開発，保守業務に従事．その後ネットワーク管理製品やセキュリティ製品の主管，構築業務などに従事し，現在ネットワークサービス部インテグレーションサービス室に所属．電信電話技術委員会委員．

高　野　　勉（Tsutomu Takano）
1971 年北豊島工業高校卒業．同年日本ユニシス（株）入社．シリーズ 90,80 のリアルタイムソフトウェアの保守業務に従事．その後ネットワーク管理製品である TNAS 1100 の日本語対応に従事，以降 SunNet　Manager，OpenView NNM,IT/O,JP/1　Cm 2 などのサポート業務に従事し，現在ネットワークサービス部インテグレーションサービス室に所属．