

ネットワーク管理の実態と OSI管理への期待

平成元年 3 月

(財)日本情報処理開発協会
産業情報化推進センター

本資料は、日本自転車振興会から競輪収益の一部である機械工業振興資金の補助を受けて、昭和63年度に実施した「産業界における情報・通信システム高度化に係わるユーザー問題調査」の一環としてとりまとめたものであります。

はじめに

近年、企業内および企業間のコンピュータネットワークの新規構築あるいは更新が盛んになってきています。

この理由として、産業界において経営効率化のための情報化の要請が高まる中、デジタル通信、コンピュータネットワーク等の新技術の進歩やISDN等の新サービスの提供など、ネットワーク環境が大きく変化していることが上げられます。

このような背景のもとで、情報通信ネットワークは大規模化・複雑化し、かつ利用範囲の広がりとともに、その障害による影響が従来に比べ格段に大きくなって来ています。

このことからユーザー企業では、ネットワークシステムに対する高信頼性、機密保全性、保守管理の容易さ等「ネットワーク管理」への要求が高まり、特に異機種ネットワーク、マルチメディア間の結合のためにその標準化が強く望まれております。

当協会産業情報化推進センターに設置の「OSIユーザー懇談会」では、このようなユーザーニーズを踏まえ、活動の一環として「ネットワーク管理」の調査・分析を行いました。

本資料はその調査結果について取りまとめたものであり、メーカー側に対してはネットワーク管理を支援する各種製品の考え方、ユーザー側については、現在、運用中のネットワーク管理上の問題点と要望等を調査・分析し、同時にOSIにおけるネットワーク管理の標準化範囲、内容等を整理しております。

従って本資料が、ネットワーク管理に対するユーザーの理解の促進と今後の標準化・製品化へ役立つことを期待するとともに、調査に協力をいただいた関係各位に深く謝意を表します。

平成元年 3 月

OS I ユーザー懇談会 ネットワーク管理WG

(順不同)

主 査	梶 亨	(株)日興システムセンター 総務部企画調査課課長代理
〃	伊藤 一彦	日本航空(株) 情報システム本部企画部調査技術G課長補佐
〃	下郷 昌夫	日本電気(株) V A N 技術本部 システム課長
委 員	中村 功	日産自動車(株) 情報システム部 システム技術課
〃	八十田 純	伊藤忠商事(株) 情報システム部 システム技術チーム課長補
〃	今田 泰寛	新日鉄情報通信システム(株)
		関東支社東京システムセンター第3室
〃	川島 真	日本たばこ産業(株) 情報システム部情報管理室
〃	三宅 信正	ソニー(株) 情報システム運用部テクニカルサポート課係長
〃	得居 信也	日本情報サービス(株)
		技術開発部 D B / D C 課ハーベストチーム
〃	増田 勉	日立ソフトウェアエンジニアリング(株) システム事業部
		金融システム本部第一保険証券システム部課長
〃	竹内 良信	沖電気工業(株) ソフトウェア開発第3部開発第3課主任
〃	津野 浩一	住友電気工業(株)
		情報電子技術研究所通信システム研究部主任

目 次

第1章 ネットワーク管理とは	1
1.1 概説	1
1.1.1 ネットワーク管理とOSI管理の背景	1
1.1.2 ネットワーク管理の目的	3
1.2 ホストコンピュータを中心としたネットワーク管理	4
1.2.1 富士通のネットワーク管理の考え方	4
1.2.2 日本アイ・ビー・エムのネットワーク管理の考え方	12
1.2.3 日立製作所のネットワーク管理の考え方	28
1.2.4 日本電気のネットワーク管理の考え方	39
1.3 LANやワークステーション環境を中心としたネットワーク管理	50
1.3.1 LANやワークステーションにおけるネットワーク管理の位置づけ...	50
1.3.2 種々の管理アーキテクチャの検討例	52
1.3.3 管理領域と検討例	58
1.3.4 LANにおけるOSI管理について	66
1.4 回線環境を中心としたネットワーク管理	71
1.4.1 通信網管理の概要	71
1.4.2 オペレーションシステムの事例	76
第2章 ネットワーク管理のユーザ実態	87
2.1 ユーザのネットワーク管理事例	87
2.1.1 ネットワーク集中管理システム	87
2.1.2 AIによるネットワーク管理	91
2.1.3 マルチメディア環境におけるネットワーク管理	97
2.2 ユーザの課題とニーズ	102
2.2.1 ネットワーク管理に関する各種環境面からの要請	102

2.2.2	マルチベンダー環境下におけるネットワーク管理の問題	103
2.2.3	ネットワーク管理システム, 製品機能上の問題	106
2.2.4	運用面の問題	107
2.2.5	情報管理における問題	108
第3章	OSI 管理の範囲と考え方	111
3.1	OSI 管理の範囲と考え方	111
3.2	OSI 管理の概要と動向	116
3.2.1	OSI 上の位置づけ	116
3.2.2	OSI 管理の管理モデル	117
3.2.3	システム管理	118
3.2.4	システム管理プロトコル	122
3.3	OSI 管理の仕様概要	125
3.3.1	文書体系	125
3.3.2	共通管理情報サービス	129
3.3.3	構成管理サービス	137
3.3.4	障害管理サービス	148
3.3.5	管理情報構造	157
3.4	OSI 管理プロフィール	165
第4章	ネットワーク管理に関するアンケート調査結果	167
(参考)	ネットワーク管理に関するアンケート調査表	193

第 1 章 ネットワーク管理とは

第1章 ネットワーク管理とは

1.1 概 説

1.1.1 「ネットワーク管理」と「OSI管理」の背景

大規模オンラインシステムの増大、分散処理の進展などに伴い、情報通信処理ネットワークは大規模化し複雑化している。また、今まで音声、データ通信と分離されていたネットワークが、デジタルネットワークに統合化され経済的なネットワークが提供されつつある。その結果、ネットワークシステムの利用者および利用範囲が格段に広がる状況にある。

従って、ネットワーク障害によるビジネス上の損失や社会的影響は膨大なものとなることが予想され、障害発生時の迅速な処置が必要とされる。そのみならず障害が発生する前に異常兆候のある機器装置の摘出や過負荷箇所の設備増強を行う予防保守も要求される。

他方、大規模で複雑なネットワークシステムを効率的に運転し、問題発生時に的確な処置のできる高スキルな専門家を養うことは非常に困難であり、運用の自動化、省力化が強く求められてもいる。

ネットワーク管理システムはこれら問題点を解決し、ネットワークシステムを安全、効率的に運用するための支援機能である。現在においても、各情報処理機器メーカーおよび通信機器メーカーより製品が提供されている。

しかるに、ネットワークシステム環境は通信の自由化によるマルチキャリア（通信事業者）化とともに、多様なメディアの機器がネットワークに接続されるマルチベンダ、マルチメディア環境になっている。残念ながら各社のネットワーク管理製品は個々バラバラに機能し、統一性のないのが現状である。

OSI管理は、マルチキャリア、マルチメディア環境において統一性のとれたネットワーク管理システムを実現するための、概念および管理の規約を技術的に体系化するものである。

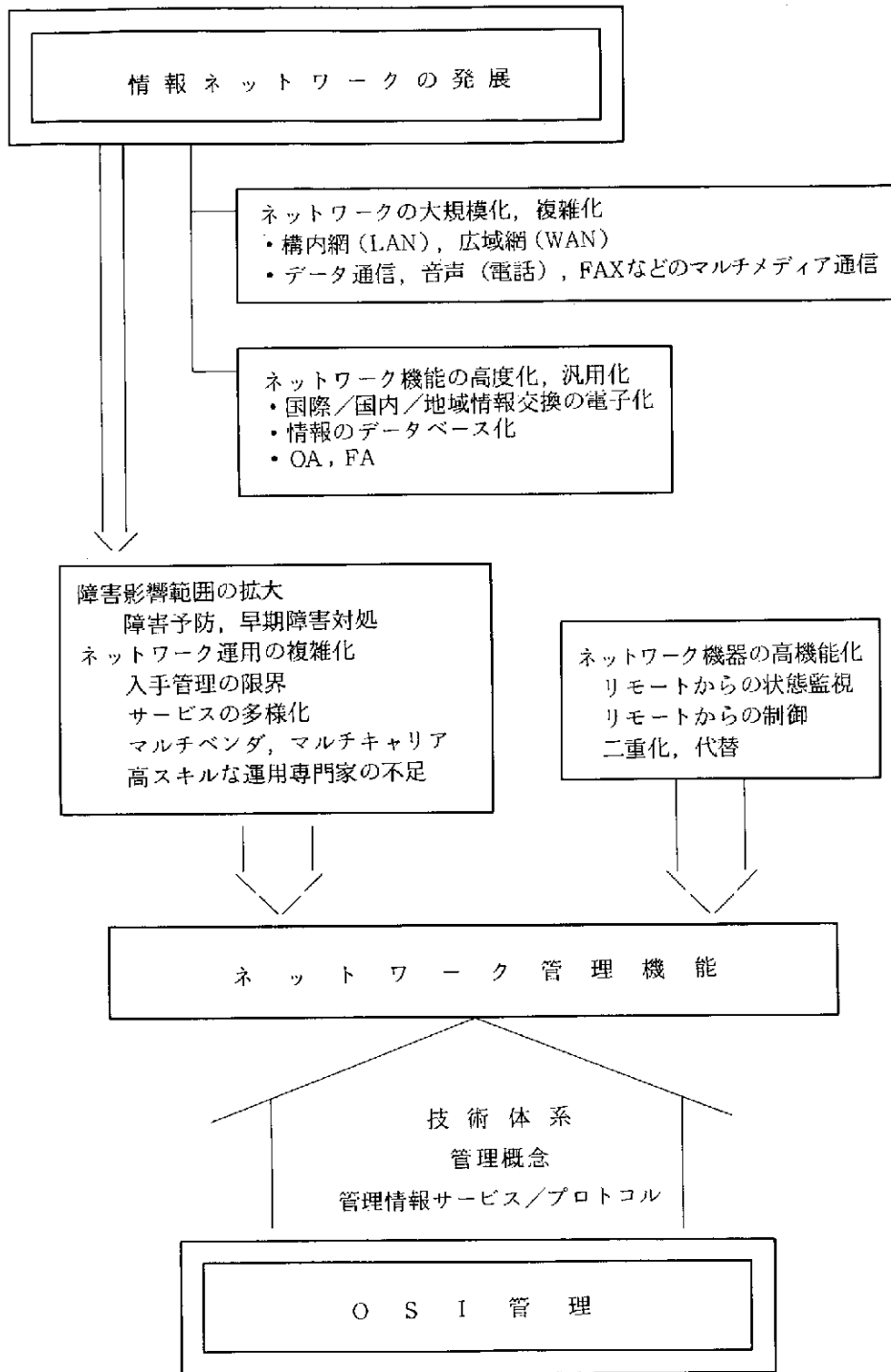


図 1.1 ネットワーク管理と OSI 管理の背景

1.1.2 ネットワーク管理の目的

ネットワーク管理は、ネットワークシステム管理者に対して以下のサービスを提供するものである。

(1) 利用者へのサービス品質の維持

ネットワークの異常状態を早期に発見し、代替ルートまたは代替装置への切り替え、接続規制を行い、通信断および伝送品質悪化または高負荷によるサービス品質低下を防止する。また、障害発生に対する迅速、的確な試験、診断および修復を行い、サービス中断を最少限度にとどめる。さらにはネットワークを構成する機器の異常兆候を検出し、問題発生の未然防止を図る。

(2) 運用・保守の省力化

システムサイドに応じた集中、分散管理により、ネットワークシステムの運用・保守要員の削減を図る。高度な運用スキルのない人でも運用できるとともに、遠隔地から専門家が効率的に保守を行うことができる。また、ネットワークシステム全体の運用管理を自動化することもできる。

課金情報を集中処理することにより、利用者に対する一括した料金請求書の発行ができる。また統計情報の集中化により、全体的な統計、トラフィック解析処理をすることができる。さらにそれら処理の自動化を図ることができる。

(3) 拡張・更新計画に対する的確な情報提供

データベース化された加入者情報および設備情報とネットワーク上のトラフィック情報とを統計処理して、将来の拡張計画を提示する。

(4) ユーザフレンドリ機能の提供

システム内部の管理情報に制約されずに、略称などによる覚え易いアプリケーション操作、管理操作を提供する。また、複雑な構成関係を条件に応じて分かりやすく提示する。

次節では、このようなネットワーク管理の考え方、ポイントについて、幾つかの局面から見てみることにする。

1.2 ホストコンピュータを中心としたネットワーク管理

1.2.1 富士通のネットワーク管理の考え方

近年、情報化社会の進展に伴ってコンピュータネットワークは大規模／複雑化の傾向をたどっている。このような状況を背景にネットワークシステムを管理するネットワーク管理者の役割は重要性を増すと同時にネットワーク管理システムに対する期待も高まってきている。

従来は情報処理を司るホストシステムと、通信を司る通信機器とは別個に管理されていた。しかし、ネットワークシステムの大規模化に伴ってネットワークを構成する多様な通信機器とホストシステムを統合した形で一元的に管理する必要が生じている。

富士通では、情報処理・通信の両分野にまたがる多様なネットワークに対応するネットワーク管理システムを実現することをねらいとした統合ネットワーク管理システムCOMS(CORporated network Management System)を提供している。COMSは通信系の基盤ネットワーク管理システムと、ホスト／端末群の管理システムが連携・融合することによって、信頼性の高い、より確かなネットワーク運用を実現する機能を提供している。以下にCOMSの特徴、並びに構成を述べる。

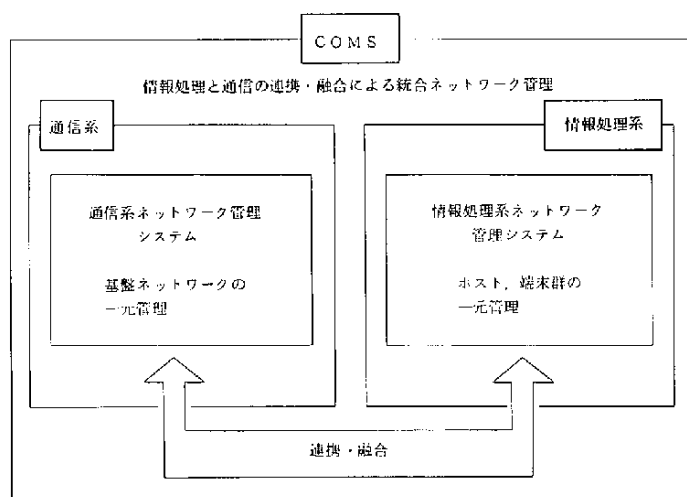


図 1.2 COMSの考え方

(1) COMSの特徴

多様な管理形態への対応

ネットワークの規模やユーザの組織形態等の要件によって構築されるネットワークの管理形態は多種多様である。このような多様なネットワーク管理形態に柔軟に対応するため、COMSでは、NSP (Network Service Processor) による通信機器の個別管理、COMS-C (COMS of Communication subsystem) による通信系の基盤ネットワークの一元管理、COMS-I (COMS of Information processing subsystem) によるホスト・端末系の一元管理といった各分野別の個別管理は勿論のこと、これらの連携と融合により、ネットワーク全体を統合管理するシステムを提供する。

以下に、各形態別のネットワーク管理の方法について説明する。

① 機器個別ネットワークの管理

モデム網ネットワーク、マルチメディア多重化装置網ネットワーク、デジタル電子交換機網ネットワークのような同一ネットワーク機器で構成される、小規模なネットワークや機器個別ネットワークの管理形態に対しては、NSPにより一元管理機能を提供する。

② 基盤ネットワークの管理

VAN業者のVANユーザの関係のような、基盤ネットワークを管理する組織がホスト／端末群を管理する組織と異なるネットワーク管理形態に対しては、COMS-Cにより、基盤ネットワークを構成するマルチメディア多重化装置、デジタル電子交換機等の複数種類のネットワーク機器を一元的に管理する。

③ ネットワーク全体の統合管理

一企業、同一組織でネットワーク全体を管理するような形態の場合には、

ホスト／端末群を一元的に管理するCOMS-Iと通信機器を管理するCOMS-Cの連携により、ホスト／端末群のデータネットワークと基盤ネットワーク機器群のネットワーク全体を一元的に管理することができる。

このようにCOMSでは各形態別のネットワーク管理の方法を提供しているが、さらに第一ステップでNSPによる管理、第二ステップでCOMS-Cによる管理、最終的にはCOMS-IとCOMS-Cでの統合ネットワーク管理といった段階的適用も可能となる。

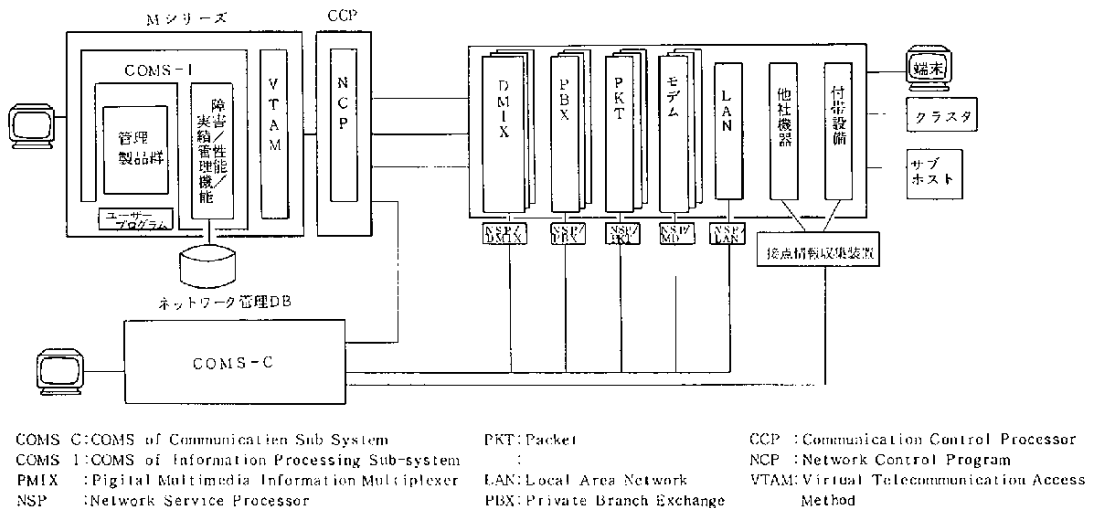


図 1.3 COMS の概念図

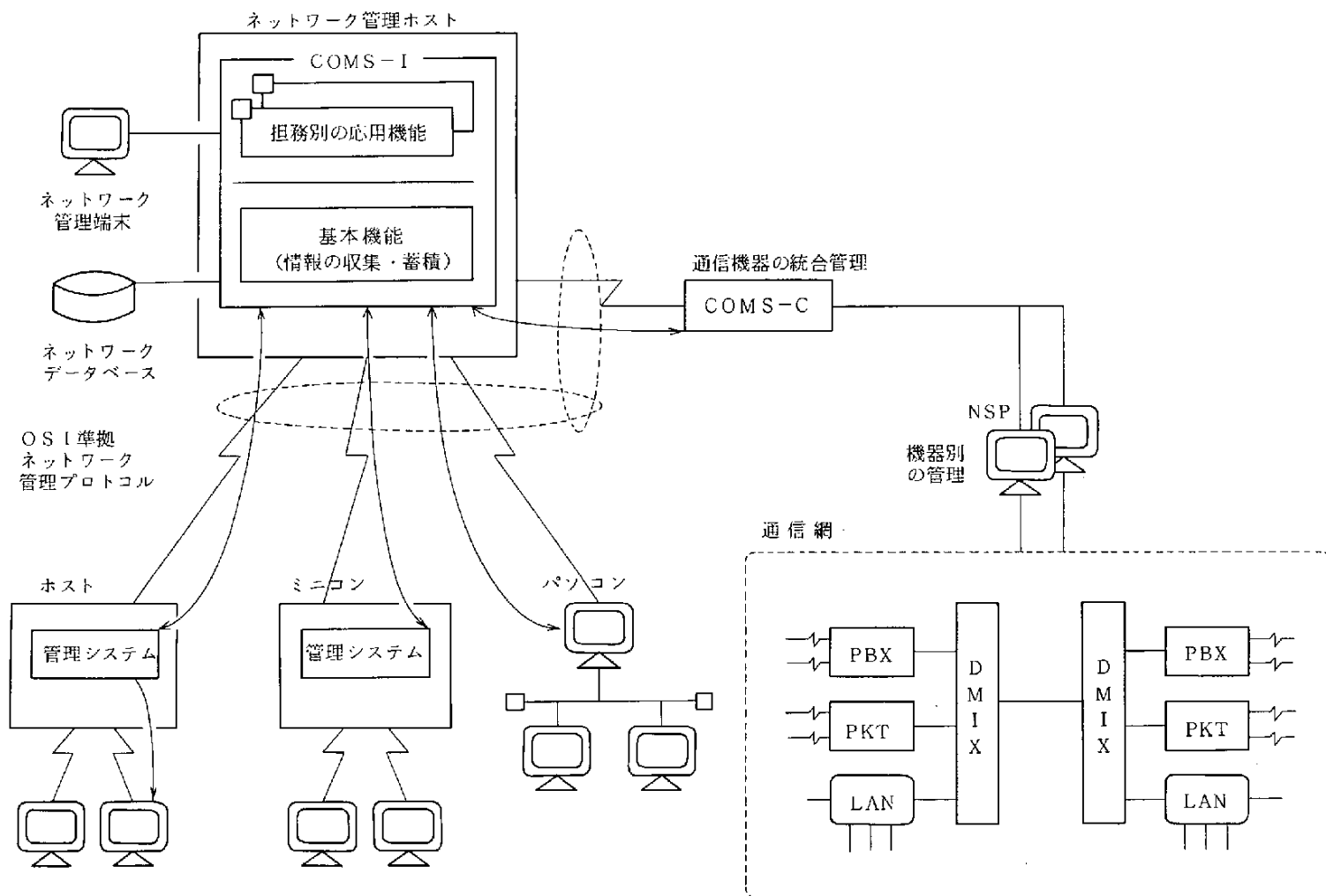


図1.4 COMSの構成

開放的なアーキテクチャに基づくネットワーク管理

ネットワークを構成する機器は多様化しており、様々なメーカーの機器によって構築される。COMSは富士通のネットワーク機器だけでなく、富士通以外のネットワーク機器を含めたオープンなネットワーク管理をねらいとして、OSIに基づくネットワーク管理機能体系を採用している。同時にOSIに準拠した接続インタフェース、ネットワーク管理プロトコルを採用している。

豊富な管理対象と管理機能

上記で示した多様な管理形態への対応や、オープンなネットワーク管理を実現するために、富士通と富士通以外のネットワーク機器を含めた豊富な機器を管理対象としている。また、管理業務の効率化を図るために、自動化、簡易化を追求する豊富な管理機能も提供している。

使いやすいマンマシンインタフェース

ネットワーク管理の運用効率の向上をねらいとして、ネットワーク障害のグラフィック画面表示等の使いやすいマンマシンインタフェースを追求している。

(2) COMSの構成

COMSは以下に示す3種類のネットワーク管理システムより構成されている。

- ① 各機器個別ネットワークを一元管理する機能提供すると共に、収集した情報をCOMS-Cに渡すNSP。
- ② 各NSPから渡された情報を一元化し、基盤ネットワーク管理を一元管理する機能を提供すると共に、必要な情報をCOMS-Iに渡すCOMS-C。

- ③ ホスト／端末群を一元管理する機能を提供すると共に、COMS-Cより渡された情報を基に、ネットワーク全体の一元管理を行うCOMS-I。

さらに、COMSではシステム構成の基本的な考え方に、ネットワークの管理側（マネージャ）と、被管理側（エージェント）からなる管理モデルを適用している。

エージェントはデータ収集等の標準機構であり、マネージャはエージェントから転送される情報の蓄積等の基本機能と、計画管理や技術サポート、運用サポート等の担務別の応用機能を持つ。COMSの概略構成を図1.3に示す。

(3) COMSの機能概要

以上述べてきた考え方に基づいてCOMSは各管理機能を提供している。以下に各管理機能の概要について述べる。

① 障害管理

障害管理とは、過去の障害履歴データや、ネットワーク資源のテストなどの手段で収集したデータを基に、障害の原因等について解析し、問題解決に必要な情報をネットワーク管理者に提供する機能である。

COMSでは、障害時の迅速な対応を可能とすることをねらいとして、以下の障害管理機能を提供している。

- ・ ネットワークの一元的な状態監視
- ・ 障害箇所、影響範囲、それに対する連絡先の表示
- ・ 障害の予防保守、障害原因調査のための障害情報収集
- ・ ネットワーク障害診断支援エキスパートシステム

② 性能管理

性能管理とは、ネットワークの性能に関する情報の収集、記録、解除を行

い、性能低下の原因や能力未使用のネットワーク資源など、ネットワークのチューニングに有効な情報をネットワーク管理者に提供することにより、ネットワークのサービス品質改善を可能とする機能である。

COMSでは、最適なネットワークの構築を可能とすることをねらいとして、以下に示す性能管理データを収集し、ネットワーク性能データベースを構築する機能機能提供している。

- ・ レスポンスタイム（端末側／ホスト側の両方で採取）の収集
- ・ ネットワーク機器負荷率（CCP、回線、端末）の収集
- ・ 送受信データ量の収集

③ 会計管理

会計管理とは、各ネットワークユーザが使用したネットワーク資源のコストに関する情報収集、記録、解析を行い、ネットワーク管理者に報告する機能である。

COMSではネットワークの使用量に応じた料金請求、費用分配を可能とすることをねらいとして、以下に示すネットワーク機器において、ネットワーク使用料金産出データの収集、蓄積、編集機能を提供している。

- ・ デジタル電子交換機システム
- ・ パケット交換機システム

④ 機密管理

機密管理とは、ネットワーク資源にアクセス可能なユーザと、そのアクセスタイプなどの管理や、暗号化のための鍵管理などの手段をネットワーク管理者に提供する機能である。

COMSでは、資源保護を可能とすることをねらいとして、以下に示すネットワークへのアクセス時の資源のチェック機能を提供している。

- ・ ネットワーク管理者用端末の利用者制限

- ・ 利用者属性による表示／出力情報，制御コマンドの制限
- ・ ネットワーク交換網に対する閉域の登録／解除機能

⑤ 構成管理

構成管理とは，ネットワークの柔軟かつ効率よい運用を可能とするために，各ネットワークシステムの開始，終了時に予め定義したネットワーク資源の活性化，非活性化を行う手段や，各ネットワークシステム開始後，ネットワーク資源を必要により動的に活性化，非活性化する手段をネットワーク管理者に提供する機能である。

COMSでは，ネットワークを構成する各種資源の属性，接続関係を一元管理することをねらいとして，以下の構成管理機能を提供している。

- ・ 大規模／複雑なネットワークの状況を一目で把握するためのネットワーク構成 機器，回線の集約表示
- ・ 管理者が必要とする情報のみを表示，出力するためのネットワーク切り出し
- ・ ネットワーク構成の容易な登録，表示，出力を可能とするネットワーク定義言語の提供
- ・ データベースによる構成情報データの一元管理
- ・ ネットワークを停止することなく，ネットワーク構成の変更を可能とするリソース再構成機能

⑥ その他の機能

COMSではネットワーク管理者の自動化／省力化を図ることをねらいとして，以下の機能を提供している。

- ・ ネットワークの一元化／自動化機構
- ・ ホスト，サブホスト，クラスタ等の遠隔操作
- ・ 通信機器，回線の稼働状況の一元監視

- ・ 作業計画の管理

- 増設，変更，保守に伴う通信機器の停止と実際の障害の識別
- 増設，変更，保守の作業計画の登録，及び実績レポートの出力

(4) 今後の展開

以上述べたように大規模／多様化するネットワークを柔軟に管理する機能をCOMSは提供している。今後はさらに基本機能の充実を図るとともに，ユーザニーズを踏まえた高度の応用機能の拡充を行う。具体的には以下の点である。

- ・ 管理対象機器の拡大
- ・ 各種カスタマイズ機能の提供
- ・ より洗練されたユーザインタフェースの提供
- ・ 性能データに基づくネットワークの自動設計機能 等

1.2.2 日本アイ・ビー・エムのネットワーク管理の考え方

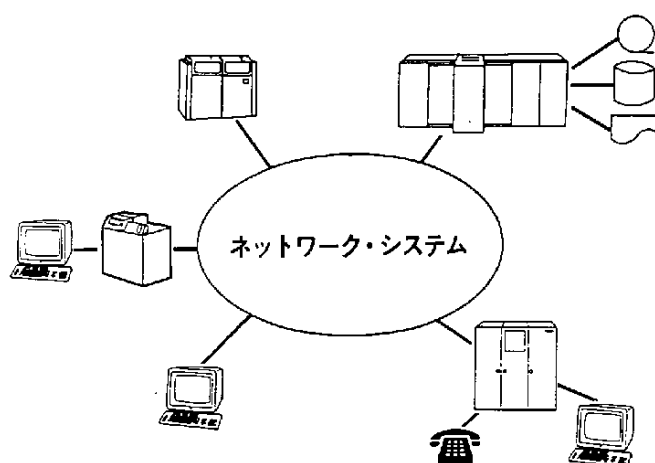
従来のオンライン情報処理の時代から，現在では機能統合による情報通信ネットワークの時代に入っていると言われている。最初にネットワークとは何かを定義するとともに，ネットワークの現状，問題点，ネットワーク管理の役割と範囲，必要な機能について触れ，最後にIBMのネットワーク管理の方式について述べることにする。

(1) ネットワークとは何か

従来のホスト・コンピュータ中心のオンライン情報処理の時代から，現在では通信ネットワークを中心とした情報通信ネットワークの時代に変わりつつある。この情報通信ネットワークには，各種のオンライン適用業務を処理するホスト・コンピュータやデータベース・システム，分散処理システム，多数の汎用ワークステーションや業務専用端末機などが接続されており，さらにデジタル回線や構内交換設備を通して電話機やファクシミリ，それに画像や映像端

末機も接続されている。このように情報通信ネットワークには、各種・多数の処理装置と端末装置が参加し、その中を各種の情報が流れる共通伝送媒体として使われている。

ネットワーク構成要素には通信回線の他にいろいろなものが含まれており、ハードウェアでは大きなもので通信制御装置、TDM装置やデジタルPBXがあり、小さなものではモデムや直流分岐装置などがある。これらはノードと呼ばれている。コンピュータ・システムや端末装置もノードと見ることができる。またソフトウェアの主なものでは通信アクセス方式やネットワーク制御プログラム、データベース・サブシステムなどがある。



ネットワーク資源により、ネットワーク・システムは構成されています。

〈ネットワーク資源〉

- | | |
|----------------|-----------------|
| • コンピューター | • TDM |
| • 端末/ワークステーション | • PBX |
| • モデム | • プログラム |
| • 回線 | • DB etc. |

図 1.5 ネットワークシステムの構成

このようにさまざまなノードや多くの通信回線と各種のソフトウェアから成るネットワークは、その規模と構成がますます複雑化する傾向にあり、機能と伝送メディアを統合化した複雑なネットワークを管理運営するには、コンピュータ・システムの利用するのが有利である。情報通信ネットワークは企業や組織のインフラストラクチャとして重要な位置を占めており、ネットワークになんらかの問題があってそれがうまく機能しない場合には、業務活動に少なからず影響を与えることになる。端末装置を使用するエンドユーザにとって、業務に支障を与えるすべての事象はネットワーク障害として映り、したがってネットワーク管理は単に回線障害のみを対象とするものであってはならない。

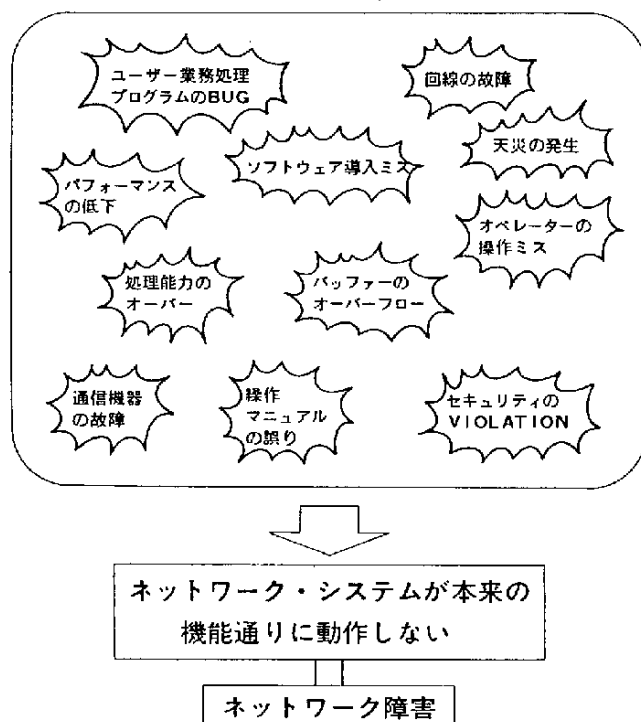


図 1.6 ネットワークの障害

(2) ネットワークの問題点

ネットワーク・システム化の問題を眺めて見ると、開発、運用・管理要員の不足とネットワーク管理費用の増大が大きく取り上げられている。

さらにそれらの問題をネットワーク管理の現場から見ると、たとえば次のような点が挙げられる。

- * ネットワーク・システム操作の煩雑さ
 - －複数の操作員の介入が必要
 - －メッセージ処理操作の負荷が大きい
 - 付随処理への対応が煩雑
- * ネットワーク・システム全体の状況把握が難しい
 - －利用者からの連絡で障害を知る
 - －事前対応ができない
 - －対応時間の遅れ
 - －復旧に時間がかかる
 - －利用者からの問い合わせが集中し対処しきれない
 - －代替処理手段がない
- * 物理的ネットワークと論理的ネットワークの一元管理ができない
 - －物理的ネットワーク管理（管理用ミニコン）
 - －回線障害や機器障害
 - －論理的ネットワーク管理（ホスト・コンピュータ）
 - －L U / P U、セッション、応対時間
- * ネットワーク・システム変更時の処理が複雑で影響が大
 - －システム停止頻度とその時間
 - －変更に伴う障害発生の危険性

(3) ネットワーク管理の役割と範囲

ネットワーク管理は、処理サービス提供者（D P 部門）にとっては、現在の運用を円滑に遂行し将来計画（拡張）に備えるとともに、ネットワーク投資効果を最適化することである。また利用者（エンドユーザ）にとっては、ネットワーク・システムが常に一定環境のもとで求められている機能要件通りに作動する仕組みを確保することである。

情報通信ネットワークの運用状況は時間とともに変化し、一時として一定であることはなく、それは永い時間経過とともに、また月単位、週単位で、さらに一日の内でも変化する。それらの変化は定常的である程度予期できるものから、システムの変更や拡張、障害による切り替えなどに伴う予期しない変化までである。

それらの変化に対応してシステムの運用管理を円滑に行い、利用者にとって常に効率良いしかも高信頼性サービスを提供するには、確固としたネットワーク管理システムの設計思想が必要である。

理想的なネットワーク管理システムは、第一にシステム環境・業務環境に応じてネットワーク資源が制御可能でなければならない。

これは有限な資源を最大限利用し、また業務の重要性和緊急性に応じてネットワークの制御を行い、各業務のサービス・レベルを維持するために必要である。

次に全ネットワーク資源は集中的に制御可能でなければならない。これは物理的、論理的なネットワーク構成要素を含めて資源の稼働状況を常に監視し、状況が的確に判断でき、必要に応じて装置やシステム構成の指定変更、停止、切り替えなどの操作制御ができることを意味する。その中には障害や異常状態の予知や検知ネットワークと資源に関する情報の収集と蓄積、さらに運用操作の自動化などが含まれる。それぞれのネットワーク資源は自身が管理対象となれる機能を持っていなければならない。そのためには、本来の情報伝達機能に加えてネットワーク管理機能をもつネットワーク資源（ハードウェアとソフトウェア）を採用する必要がある。

さらにネットワーク管理システム自体は体系化されており、将来の拡張と発展（網間接続、対外接続や国際ネットワーク）に対応し得なければならない。

① ネットワーク管理支援ツール

ネットワーク管理を行う支援ツールとしては最初にネットワーク管理用ユ

ーザ・アプリケーションがあり、企業なり組織の必要に応じてカスタマイズされたものが必要である。これによって管理の目的と範囲に応じてどんなデータをどのように利用するかが決まる。

次に、データを収集しそれを有効利用するためのデータベース・システムとサブタスク／サブプログラムがある。これは報告書や統計を作成し、また見易いかたちでデータを表示する。

ネットワーク管理基本プログラム（たとえばNet View）は、管理対象となるそれぞれの分野に応じて、データを集め、基本加工し、それをネットワーク管理者や運用者に提供する。最後に、通信アクセス方式とネットワーク制御プログラムはネットワーク適応業務を通す一方、ネットワーク管理機能を支援する機能を組み込んだものである必要がある。

② ネットワーク管理の対象分野

ネットワーク管理の対象分野には、次に挙げる6つの分野が含まれる。

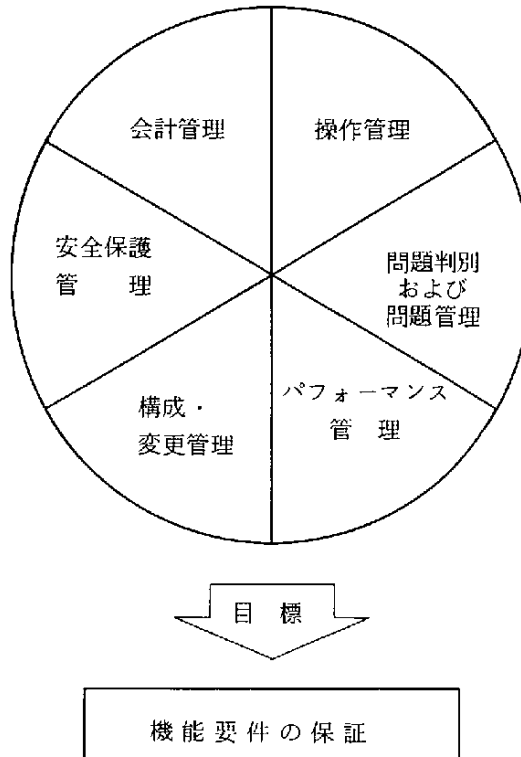


図1.7 管理支援ツールCNMの管理分野

運用支援

障害管理

パフォーマンス管理

問題・変更・構成管理

安全保護管理

課金管理

これらの対象分野は互いに連動して、ネットワーク・システムの必要な機能要件を確保するために管理されなければならない。

(4) ネットワーク管理の機能

ネットワーク管理の機能要件は、たとえば次のような項目を挙げることができる。

- ・ 予期し得る障害に対して未然防止策の作成ができるのが理想的で、このためには、障害が起きない仕組みを作ることと、事前保守と兆候管理が必要。
- ・ 次に不幸にして障害が発生した場合には、迅速な問題判別と対応策の実行が望まれ、このためには問題箇所の切分けを適切に行なうため、システムが問題判別をし、問題対応処理と波及処理を確実に行う自動化処理が必要。
- ・ 問題再発防止策の検討と立案の仕組みが確立されるべきである。このためには、問題の真の原因追求と対策立案に数字データの裏付けが必要であり、事象の分析や統計が約に立つ。

従ってネットワーク・システムおよびその環境に対する状況が常に把握できる仕組みと、さらにネットワーク・システム及びその環境の変化の経緯が把握できる仕組みが確立されていなければならない。

- ・ ネットワーク・システムの運用を少ない操作員で容易に行うために、運用操作の自動化・簡素化・確実化が必要。

- ・ システムのオーバー・フローを事前に察知し予防するとともに、決定的なシステムダウンは避けなければならない。

更に複雑なネットワークにおいて、処理システムのセキュリティと機密保護は確保される必要がある。

- ・ 課金管理は重要な課題である。部門別に経費を賦課するために、処理サービスの原価計算のために、また情報提供サービスの料金算定の基礎として、いろいろな角度からネットワーク・システム利用状況とトラフィック量などの基礎データの収集が求められる。統合通信ネットワークでは、データ通信のみならず電話の課金管理も含まれる。

以上はネットワーク管理要件の一部であるが、その他にもいろいろな項目を挙げることができる。

(5) IBMのネットワーク管理方式

効果的にネットワーク管理を行うために、IBMのシステム・ネットワーク体系のなかには、CNM（通信ネットワーク管理）と呼ばれる機能が組み込まれている。前にも述べたようにネットワーク・システムを構成するハードウェア要素は多数であり、それらの機器にCNM機能が分散されていることにより、ハードとソフトを含むネットワーク全体の稼働状況が一元的に把握でき、問題判別が総合的に行えることになる。

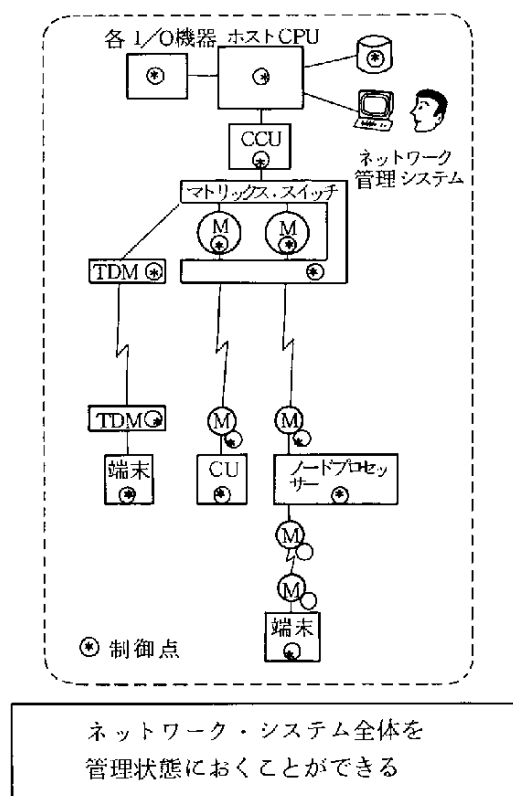


図 1.8 理想的なネットワーク管理システム

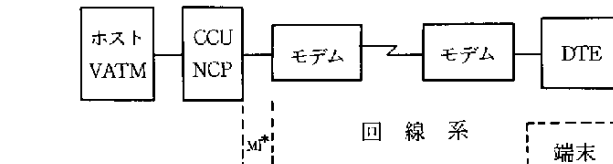
CNMには警報を生成して知らせる機能があり、たとえば装置、回線やモデムなどの機器が障害を起こしたり、パフォーマンスがあらかじめ設定された限界値を越えると、ネットワーク管理システムは警報を作成して操作員に自動的に知らせる。これにより、端末利用者が機器の異常や操作の支障を感じる前にネットワーク管理センター側では障害箇所を知ることができる。したがって運用状況を常に監視し問題を即座に検知して解決への迅速な対応がとれる。

たとえば、ネットワーク障害の分野に例をとっても、IBMモデムの中には内蔵したマイクロプロセッサを中心として各種の監視と検知の機能がある。これは回線の品質と通信状況、送受信の信号レベル、モデム自体と接続機器のピンの状態、データの再送回数などをホストの問題判別プログラムと連動して把握できる。さちに必要に応じてホスト側からの指令により、伝送速度の変更受信レベルの変更、専用線から公衆網へのバックアップ切り替え（自動ダイヤル）などの操作を行うことができる。

LPDA（リンク問題判別支援）機能

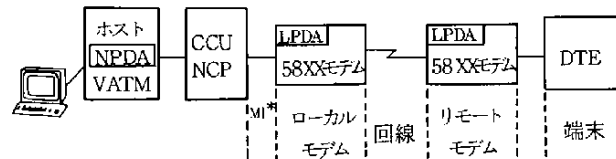
MI* : モデム・インターフェース
DTE : DATA TERMINAL
EQUIPMENT

(1) LPDAが無い場合の問題の切分け



⇒ 回線系に問題が発生した場合、ホスト側での原因究明は非常に困難

(2) LPDAが有る場合の問題の切分け



⇒ 回線系の問題判別が非常に容易

LPDAとNPDAの連携によりコンソールに情報を提供します

図 1.9 SNA モデム

このようなC NM機能は、モデムのみならずあらゆるIBMの物理装置内に内蔵されており、それぞれの装置と隣接機器の状況把握と制御に関与する。前に述べたネットワーク管理の6つの分野をカバーするために、管理支援機能を備えた各種のソフトウェア・ツールが容易されている。それらの中にはネットワーク管理プログラム（NCCF）、ネットワーク問題判別プログラム（NLDM）などが含まれ、さらに操作、構成／変更、パフォーマンス、機密保護、課金を取り扱うためにその他各種のソフトウェア（NPM、RMF、RTM、TAF、SMF、TPNS、INFO/MGT、RACF、DSX、HCF、TARA、SAMON）がある。

① NetView

総合ネットワーク管理プログラム（NetView）は、従来からあったネットワーク管理の個々のプログラムの基本機能を統合して、運用監視と構成の状

況把握，集中制御，障害からの自動化回復のための機能を持ついくつかのソフトウェア群から成る。

さらにNetViewには，それらの機能を支えるために，コマンド機能，ハードウェア監視，ソフトウェア監視，セッション監視，状況監視，ヘルプ機能，カスタマイゼーション機能，及びソフトウェア群導入を容易にする支援機能が含まれている（図1.10～1.12参照）

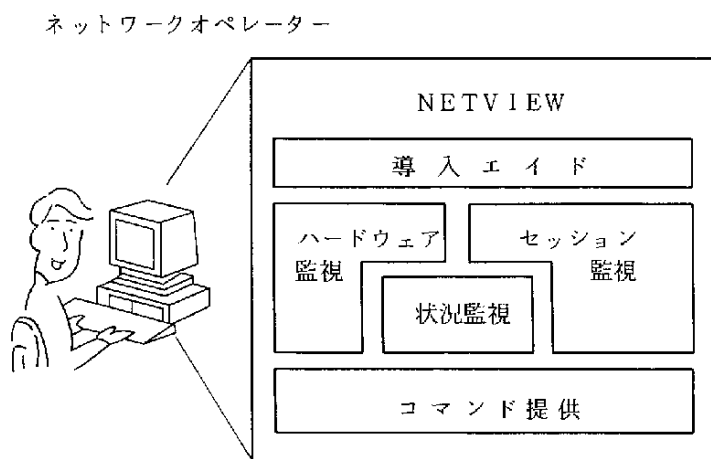


図1.10 NETVIEW(ネットビュー)：統合ネットワーク管理プログラム

問題警告
 問題判別, データ収集表示
 解決策提示



NPDA (ネットワーク問題判別プログラム)

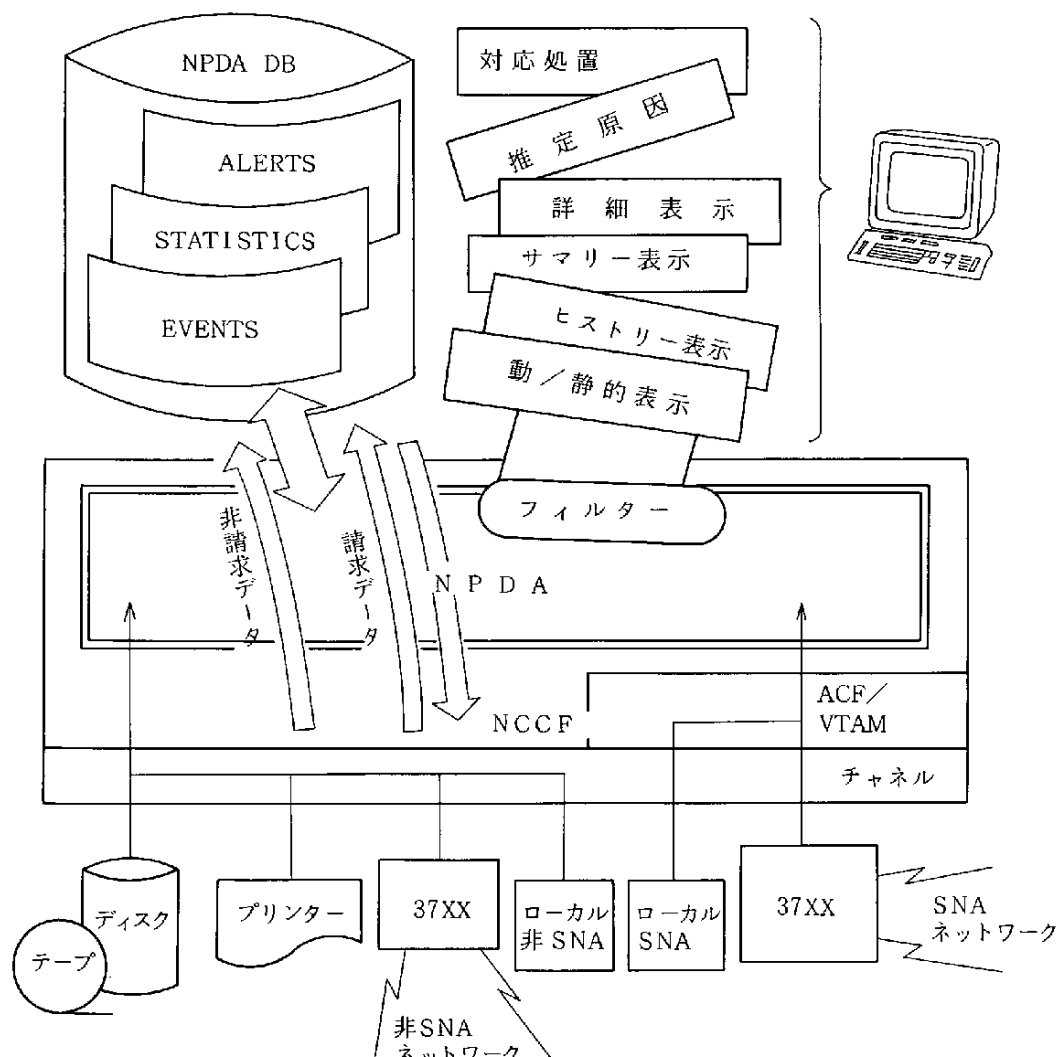


図 1.11 ハードウェア監視機能

応答時間監視

セッション状況監視



NLDM (ネットワーク論理データ管理プログラム)

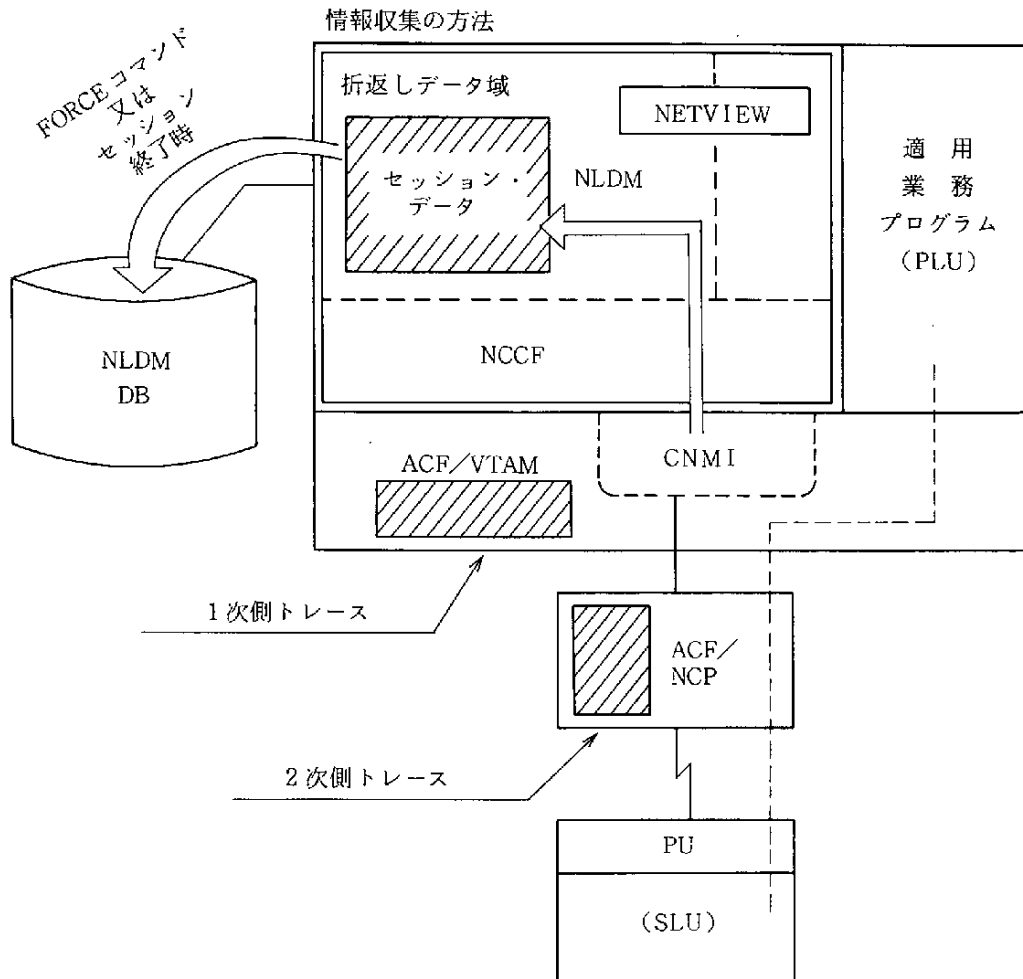


図 1.12 セッション監視機能

② NetView/PC

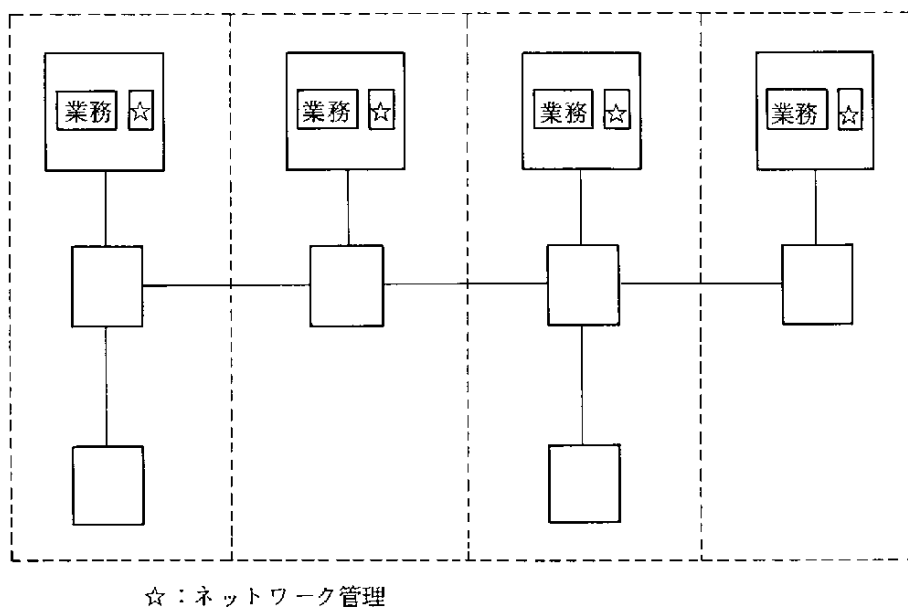
NetView/PCは、ユーザーのネットワーク状況に合わせてネットワーク管理を拡張します。これはIBMトークン・リング・ネットワークやTDM、音声ネットワークをネットワーク管理対象に含める場合や、マルチベンダー環境のもとで他社の通信製品も含めて管理する場合に使用出来る。

NetView/PCはNetViewと通信する機能がありますので、NetViewが理解できる形式と規則でPCを介して管理データを送ることにより、他社製品も含めて多様な構成要素から成る通信ネットワークを一元的に管理することができる。これはIBMのコミュニケーション体系の公開の方針に沿って、それを具体化するものの一つである。

③ ネットワーク管理構成

ネットワーク管理を論じる際に、IBMはネットワーク管理構成(CMC)を避けて通るわけにはいかない。一元的なネットワーク管理と網間接続に対してこの方式は有効な手段を提供する。共通伝送資源としての通信ネットワークと適用業務処理を独立させるために、ネットワーク資源を管理する通信管理ホストを業務処理ホストと別に設けるのがこの方式である。

MSNF : 複数CPU ネットワーキング



CMC : ネットワーク資源の管理を一元化する為のネットワーク構成

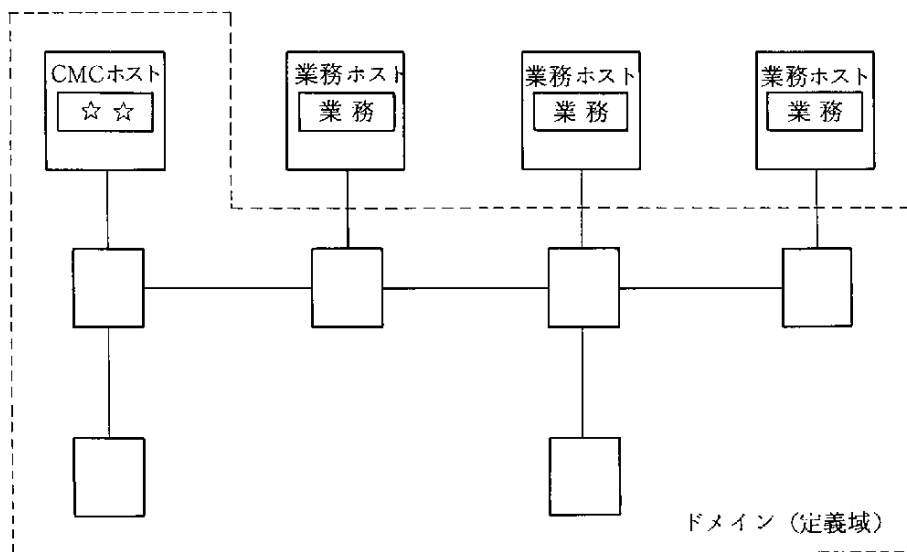


図 1.13 CMC : Communication Management Configuration

通信管理専用ホストにはネットワークに参加するあらゆる資源の定義を蓄え、CNMのためのソフトウェア群を装備し、これによって業務ホストは本来の目的である業務処理に専念できるようになる。さらにネットワーク管理と業務処理の相互干渉を無くすることにより、ネットワークの拡張や変更は容易に行える。

CMCの利点

— ネットワークを業務から独立

- ・ 相互依存がなくなることによりシステム全体の拡張性が向上
- ・ ネットワークの構成の再編成／最適化が容易に
- ・ 高度なスキルを最適配置
- ・ 問題／影響／干渉を絶縁

— ネットワークを一元管理

- ・ ネットワーク利用可能度の向上
- ・ ネットワーク生産性の向上
- ・ 利用者サービスの質向上

IBMのSNAに基づく通信ネットワークは汎用伝送媒体として各種の情報を運ぶ。ネットワーク管理の見地からその管理領域は、地域または業務組織上の理由から最適な管理規模に分割するのが有利な場合があるが、このような場合に複数のネットワークを相互接続し、適用業務資源、端末装置の増設、ネットワーク利用者やそのパスワードなどの管理をネットワーク毎に独立させることができる。もちろん、ネットワーク間の接続と統合的なネットワーク管理情報の交換はゲートウェイを通して行われる。

1.2.3 日立製作所のネットワーク管理の考え方

コンピュータや通信網から成る情報ネットワークの管理は、ネットワークサービスへのユーザニーズの高まり、高速、広域公衆網の普及による広域化によってますます重要性が高まってきている。このようなネットワークを運用するには、ネットワークを構成する要素をあるまとまりで個別に管理し、更に中央からシステムの運行状況をネットワークワイドに把握できることが必要となってきた。

以下では、ネットワーク管理の目的と、それに対応して日立製作所が提供するネットワーク管理システムの考え方を説明する。また、ネットワーク管理システムを構成するNETM/OP (Network Management/Operation assist), NETM/DS (Network Management/Distributed Systems assist) の機能概要についても説明を行う。

(1) ネットワーク管理の目的

ネットワークシステムの基本は、「良好なサービスを、利用者が使いたいときに、いつでも受けられること」にある。これを実現するためには、まず第一にネットワークシステム自体をユーザーのニーズに合った構成とする必要がある。すなわち、対象メディア、トラフィック量およびレスポンスを考慮し、信頼性、安全性を加味した最適網構成の設計を行い、更に、将来の拡張性、機能追加の柔軟性を持たせた、経済的かつ安全なネットワーク管理を構築することである。

第二に、ネットワークシステムの全体構成が把握できるようになっていることが必要であり全体の稼働状況がネットワーク管理者に容易に把握できなくてはならない。

第三に、ネットワークシステムの障害時の対応が迅速に行えることが必要である。これは、システムを監視しておき、障害発生時に詳細情報を調査することによって、ネットワークシステムの運用者が迅速に適切な処置がとれるよう

にしておくこと。また、原因究明が迅速に行え、できるだけ短時間で正常状態に復旧させ、更に、異常の発生を予知して、それが起こるのを防ぐことも重要となる。

第四に、ネットワークのトラフィック量、レスポンスの状態を監視しておき、性能の異常を早期にキャッチすること、公衆網、海外ネットワークとの接続で今後ますます重要になるアクセス資格のチェックなどのセキュリティ対策やネットワーク利用者に対する課金処理などネットワークを運用していくための管理業務を支援することもある。

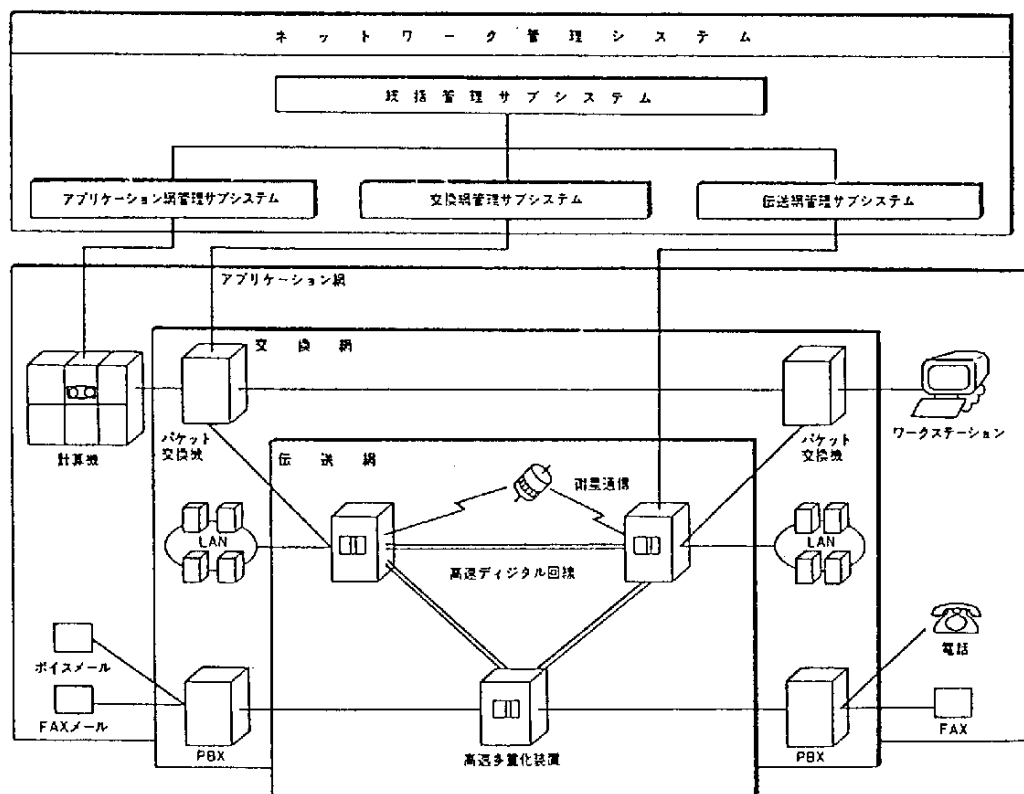
ネットワーク管理とは、以上のことをネットワークシステムの運用者が適切に把握し、ネットワークシステムの安定した運用を行うための支援をするものである。また、ネットワーク管理システムは、ネットワーク管理者がこれを円滑に行うための各種支援機能を提供するものである。このようなネットワーク管理システムの機能を表 1.1 に示す。

表 1.1 ネットワーク管理の機能

本論文で述べる分散・統括形のネットワーク管理システムは、運用支援機能、保守支援機能を実現する。

種 別	機 能 項 目
構築支援機能	・導入計画、構築支援機能 ・増設計画機能
運用支援機能	・稼働監視、遠隔操作機能 ・ネットワークの構成情報、属性情報管理 ・ネットワークの操作に関する資格管理機能 ・性能の監視と性能情報の管理 ・操作支援機能 ・分散システムの資源の管理と保守機能 ・課金情報の収集と管理機能
保守支援機能	・障害の検知機能 ・障害部位の切分け機能 ・障害データの収集と解析支援機能 ・障害部位の切離し（再構成）支援機能 ・ネットワーク資源のテスト機能

上記で述べた機能を実現するため、ネットワーク管理システムは、図 1.14 に示すような分散統括形の管理を行う。この理由は以下の通りである。



注：略語説明 FAX（ファクシミリ）

ネットワークシステムを構成する機器を、三つに分類して管理している。

図1.14 ネットワーク管理システムの構造

- ① ネットワークの構成は多様であり、さまざまな組合せのネットワークに対して管理を行うためには、機能の分散化、モジュール化が必要。
- ② ネットワークワイドな管理を顧客の運用形態に対応して実施するには、統括形の管理も必要となり、図1.14に示す四つの管理サブシステムは、それぞれ独立したサブシステムとして実現され各々が単独で管理機能を実行する。

ここで、対象ネットワークを伝送網、交換網、アプリケーション網の三つに階層化しているが、それぞれは、次の意味を持つ。

伝 送 網

多重化装置など O S I (Open Systems Interconnection) の 7 階層モデルでレイヤ 1 の機能を提供する機器の構成されるネットワーク

交 換 機

P B X (Private Branch Exchange), パケット交換網など O S I の 7 階層モデルでレイヤ 1 ～ 3 の機能を実現する機器から構成されるネットワーク

アプリケーション網

計算機, 端末などの O S I の 7 階層モデルでレイヤ 1 ～ 7 の機能を実現する機器から構成されるネットワーク

(2) D P O S N E T M / O P

① 概 要

D P O S N E T M / O P (ネットワーク管理/操作支援) は, 分散されている分散機 (D P O S) をホスト (V O S 3) から集中的に操作できる機能を提供することによって, ホストからの分散処理システムの統一的な運用管理を実現することを目的とするプログラムである。

D P O S N E T M / O P は, V O S 3 N E T M / O P と接続し, ホストのネットワーク管理用操作支援端末又はホストのコンソール装置からの D P O S コマンド操作機能, 及び D P O S で発生するメッセージをホストの操作支援端末又は, コンソール装置に表示する機能を持つ。

② システムの構成

D P O S N E T M / O P は, N E T M / D S などの, 他のネットワーク管理機能とともに 1 個のパーティション上で動作し, T A C F / O T L

(Telecommunication Access Control Facility/O S I Transport Layer support), 及び L N C F (Line Control Facility) を使用してホストと通信する。

NETM/OP はまた、他のネットワーク管理機能に対し、ホスト側の対応するネットワーク管理機能との間の通信機能を提供している。

図 1.15 にシステムの構成を示す。

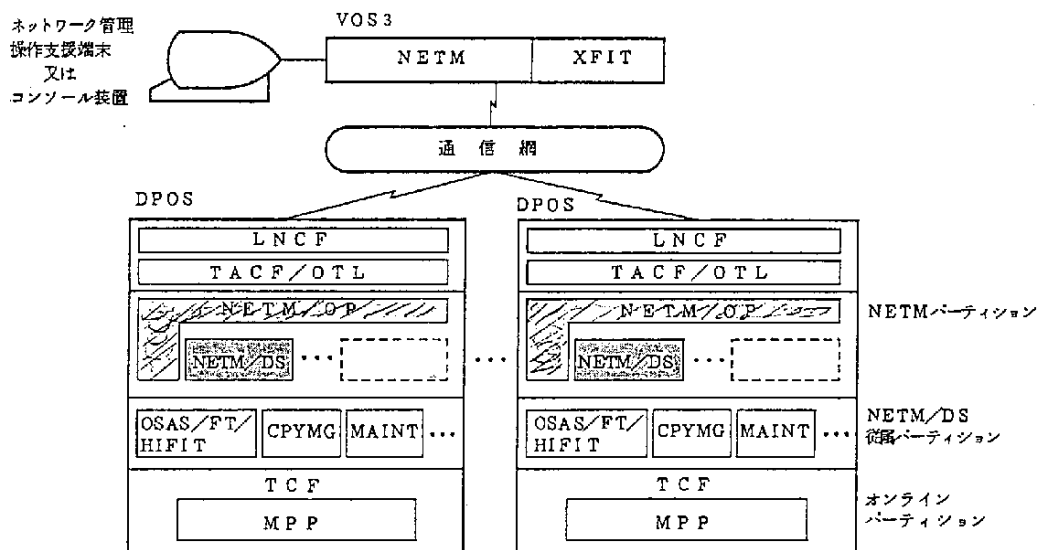


図 1.15 システムの構成

③ 機能概要

分散機操作機能

ホストの操作支援端末又はコンソール装置から投入した DPOS コマンドを、ホストの NETM/OP から受信して DPOS 側で実行し、コマンド処理結果メッセージをホストの NETM/OP に送信し、コマンド投入装置に表示ひる機能である。分散機のホストからの操作の流れを図 1.16 に示す。

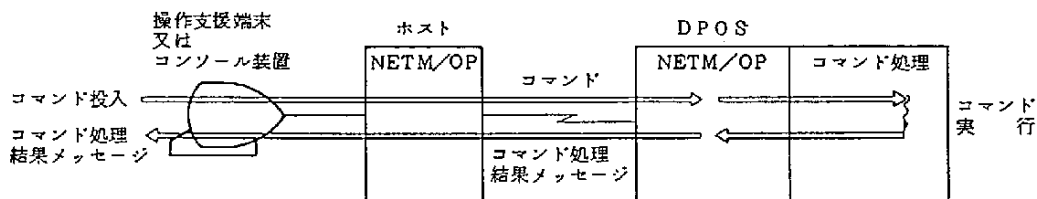


図 1.16 ホストからの分散機操作の流れ

分散機状態監視機能

DPOSで発生した重要障害メッセージなどのメッセージをホストに送信し、ホストの操作支援端末又はコンソール装置に表示することによって、ホストで分散機の状態を集中監視できるようにする機能である。

DPOSでSYSLOGへのメッセージが発生すると、NETM/OPは標準およびユーザ定義のメッセージ定義フェーズの指定に従って、そのメッセージをホストに送信するかどうかの決定、および送信する場合には重要メッセージか一般メッセージかの属性の付加をしてホストに送信する。

図 1.17にDPOSの状態監視の概念を示す。

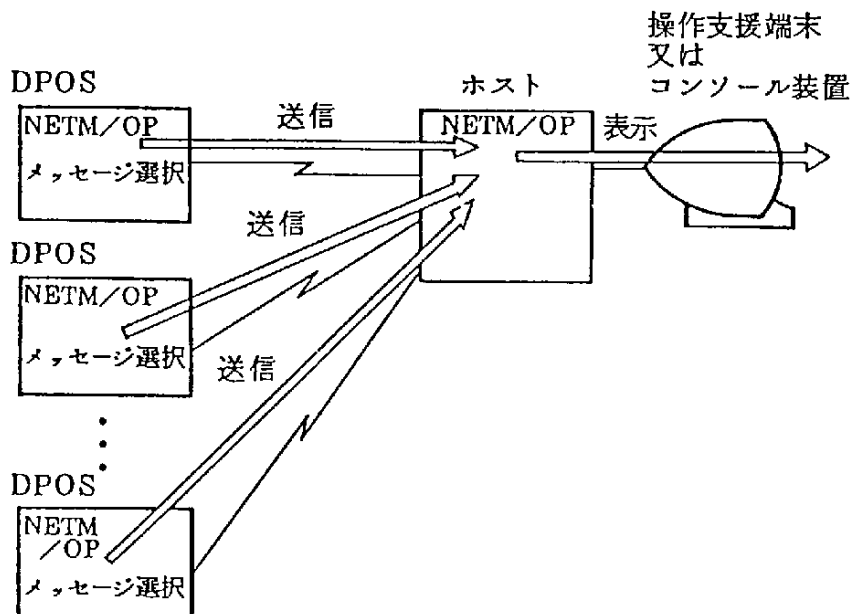


図 1.17 DPOS の状態監視の概念

a. 応答用メッセージに対する応答投入

DPOSで発生し、ホストの操作支援端末又はコンソール装置に出力したメッセージはDPOSのSYSLOGにも出力されている。ホストに送信したメッセージのうちオペレータの応答が必要なメッセージに対する応答は、ホスト又はDPOSのどちらからでも入力できる。どちらか一方から応答を投入すればそのメッセージは応答済みとなり、もう一方の側に出力されている応答要メッセージは応答要ではなくなる。

b. ホスト送信メッセージ選択機能

NETM/OPは、DPOSで発生したSYSLOGメッセージをNETM/OPのメッセージ選択機能によって選択し、送信対象となったメッセージをホストに送信する。図1.18にメッセージ選択の概念を示す。

DPOSでSYSLOGメッセージが発生した時、NETM/OPはNETM/OP構成定義ファイル、ユーザーメッセージ定義フェーズ、及び標準メッセージ定義フェーズの3種類のデータの内容を参照して、それらの中に定義された指定に従って、発生したメッセージを送信するかどうか、送信するメッセージについては重要メッセージとするかどうかの決定をする。

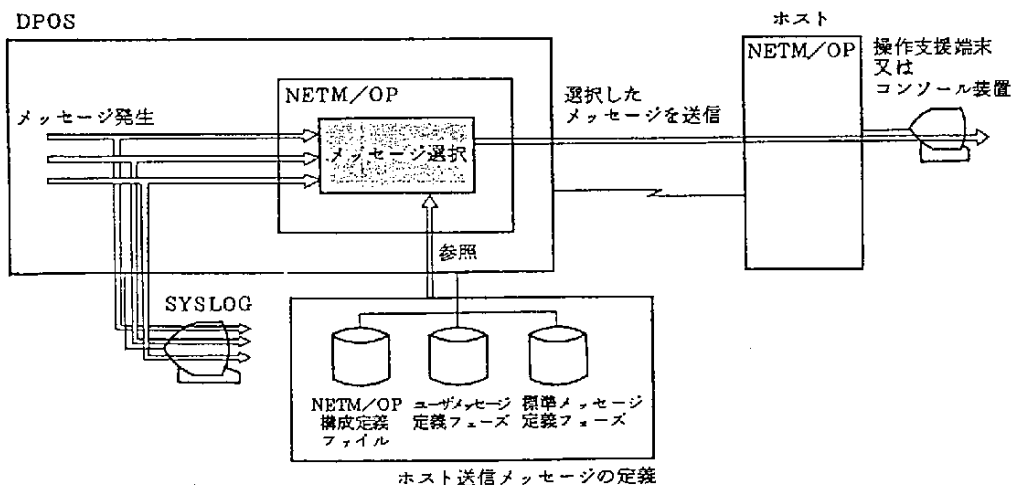


図1.18 メッセージ選択の概念

(2) DPOS NETM/DS

① 概 要

DPOS NETM/DS (ネットワーク管理/分散システム支援)は、分散配置されている分散機(DPOS)のファイル、ライブラリなどのソフトウェア資源の配布、収集をホスト(VOS3)から集中的に伝える機能を提供することによってホストからの分散処理システム資源の統一的な管理を実現することを目的とするプログラムである。

DPOS NETM/DSはVOS3 NETM/DSと接続し、ホストからの指令に従ってDPOSのファイル、ライブラリの送受信、ジョブの実行などの機能を実行する。

② システムの構成

DPOS NETM/DSは、NETM/OPなどの、他のネットワーク管理機能とともに1個のパーティション上で動作し、NETM/OP、TACF/OTL (Telecommunication Access Control Facility / OS I Transport Layer Support), およびLNCF (Line Control Facility)を使用してホストと通信する。

ホストとのファイル転送には、OSAS/FT/HIFIT (OS I Application Support Common Facility / File Transfer Access and Management / High level File Transmission Program)を、NETM/DS従属パーティションと呼ぶ別パーティションで起動してファイル転送を実行する。OSAS/FT/HIFITはホストのVOS3 XFIT (Extended File Transmission Program)との間でファイル転送を行う。

NETM/DS従属パーティションでは、OSAS/FT/HIFITの他に、CPYMG (Copy and Merge), MAINT (Library Maintenance)などのプログラムをNETM/DSが起動して実行する。

T C F (T r a n s a c t i o n C o n t r o l F a c i l i t y) 下 の M P P (M e s s a g e P r o c e s s i n g P r o g r a m) のオンライン中のモジュール替えをホスト指示によって行う場合には、N E T M / D S から T C F に対して M P P メモリロード要求を行う。(図 1.15 参照)

③ 機能概要

ファイル送受信機能

ホストの N E T M / D S からの指示に従って、指定されたファイルをホスト-D P O S 間で送受信、又は削除する。ファイル転送は D P O S 側ではファイル転送プログラム O S A S / F T / H I F I T を起動することによって行う。図 1.19 にファイル送受信機能の概念を示す。

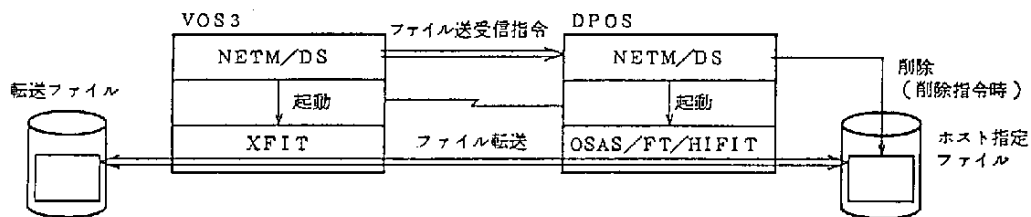


図 1.19 ファイル送受信処理の概念

ライブラリ送受信機能

ホストの N E T M / D S からの指示に従って、指定されたライブラリをホスト-D P O S 間で送受信、又は削除する。指定ライブラリからのメンバの取出し、指定ライブラリへのメンバーの追加、置換は C P Y M G を起動することによって行い、ホストとのファイル転送には O S A S / F T / H I F I T を起動することによって行う。指定ライブラリのメンバーの削除は、M A I N T を起動することによって行う。ここで言うメンバーとは次のものである。

- ・ 原始文ライブラリ中のブック

- ・ 相対形式ライブラリ中のモジュール
- ・ 実行形式ライブラリ中のフェーズ
- ・ プロシジャライブラリ中のプロシジャ
- ・ メッセージライブラリ中のメッセージ

ジョブ実行機能

ホストのCNETM/DSからの指令に従って、DPOS用JCLを受信し、DPOSで実行する。図1.20にジョブ実行機能の概念を示す。

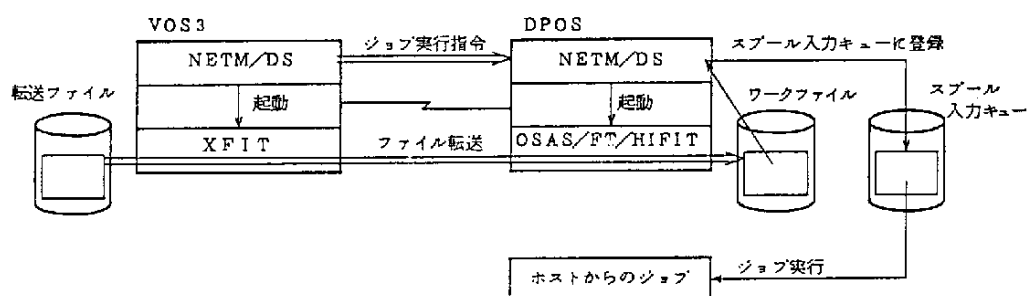


図1.20 ジョブ実行機能の概念

ダンプファイル送信機能

ホストからの指令に従って、DPOSのシステムダンプファイル（SYSDMP）又はパーティションダンプファイル（SYSPDM）の全体は一部をホストに送信する。

ホストから指定されたダンプ領域を取出すのには、NETM/DSのダンプ変換プログラムを従属パーティションに起動することによって行う。

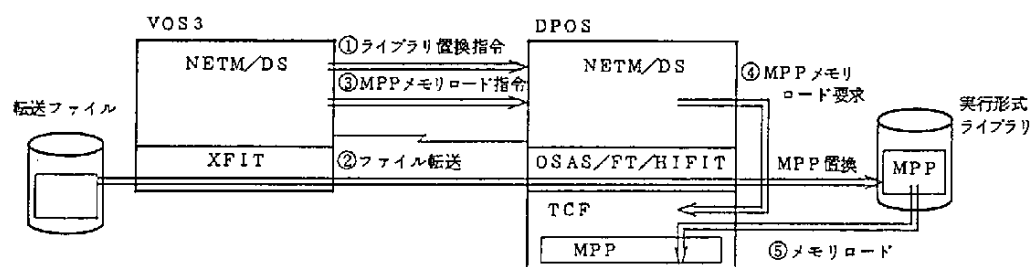
ホストではDPOSから収集したダンプファイルをCDEDT（Cross Dump Editor）を使用して編集出力できる。

メッセージ出力機能

ホストからの指令に従って、ホストからメッセージを受信し、DPOSのSYSLOGに出力する。

MPPメモリーロード機能

ホストからの指令に従って、TCFに対しホストから指定されたMPPのメモリーロードを要求する。図1.21にMPPメモリーロード機能の概念を示す。



- ①② ライブラリ置換指令により、ホストからDPOS実行形式ライブラリにMPPフェーズを送信する。
- ③④ MPPメモリーロード指令により、DPOS NETM/DSはTCFに対してMPPフェーズのメモリーロードを要求する。
- ⑤ TCFはNETM/DSから指定されたMPPフェーズを、そのMPPに制御を渡すときにメモリーロードする。

図1.21 MPPメモリーロード機能の概念

1.2.4 日本電気のネットワーク管理の考え方

世の中、ここ数年前より企業情報ネットワークが、地域的ネットワークから国内・国際的ネットワークへと広域化、大規模化、高度化、複雑化してきている。その背景には、通信環境の変化、技術の発展に伴い各企業が自由自在に最適なネットワークシステムを構築できる時代となり、更に企業自体の変革により地域から国内・国際へとビジネスの活動範囲が拡大してきている。

このように企業情報ネットワークの広域化、大規模化、高度化、複雑化が進むことによりネットワークの安全性、信頼性を維持することが更に重要となってきた。また、ネットワークの広域化、大規模化に伴いネットワークの運用経費、人手は増大の傾向にあり、ネットワークの運用経費の削減、効率的運用、管理の自動化など経済性が重要となっている。

従来のネットワーク管理システムは、コンピュータ系、伝送系、交換系など、それぞれ個別に独立して配置されてきたが、ネットワークの広域化、大規模化が進むにつれて、それらを統合化して一元管理のできるネットワーク管理の要求が高まっている。

(1) VISION-NMSのねらい

日本電気では、企業情報ネットワークを構成する情報処理機器、通信機器を一元的に統合管理する統合ネットワーク管理システムVISION-NMS (Network Management System) を提供している。

VISION-NMSは、コンピュータシステム、伝送系ネットワーク、交換系ネットワークおよび無線系ネットワークなど総合的に管理するシステムでネットワークの運用経費の削減、運用の効率化、保守の迅速化、管理の精度向上を目的としている。更には、企業情報ネットワークのマルチベンダ環境、マルチキャリア環境を考慮し、またネットワークの国際化へ対応するためにネットワークの国際標準化が進められているOSI管理を積極的に採用し、国際的なネットワーク管理システムを狙いとしている。如何にVISION-NMSの特徴、論理構造およびシステム構成について述べる。

(2) VISION-NMSの特徴

VISION-NMSは、ネットワークの各種資源を効率的、且つ効果的に管理するために個別機器管理、サブネットワーク管理、統合ネットワーク管理の3階層構造に体系化している。VISION-NMSの階層構造を図1.22に示す。

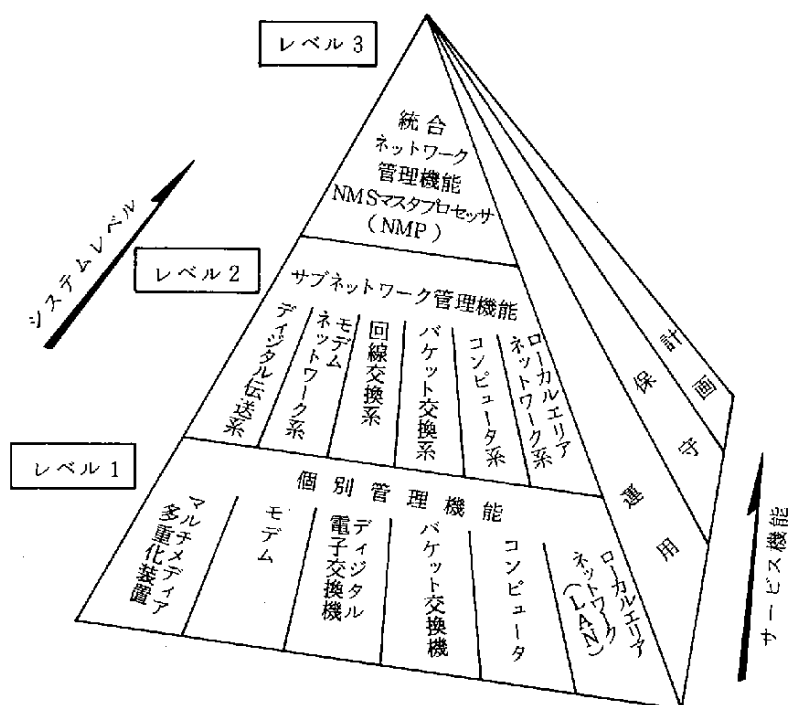


図1.22 VISION-NMSの階層構造

分散統括管理方式

① レベル1：個別管理機能

個々の装置を個別に管理するための管理機能である。各装置に実装される R A S (Reliability, Availability, Serviceability) 機能, すなわち障害検出機能, 動的ルーティング機能, 試験・診断機能など広義のフォールトトレラント機能および運用管理のために必要な機能により装置自身の管理と隣接した装置と連携した管理を実行する機能である。

② レベル2：サブネットワーク管理機能

コンピュータネットワーク, デジタル伝送系, 回線交換系, パケット交換系などをそれぞれサブネットワークとし, そのサブネットワークごとの集中管理を行うサブネットワーク管理機能である。サブネットワーク管理は, レベル1の個別管理とインタフェースをもち, サブネットワーク内で完全に閉鎖された環境での運用管理機能である。このサブネットワーク管理システムは, 上位の管理システムが存在しない場合でもサブネットワークに関する全ての運用管理機能を完全に満足するものである。

③ レベル3：統合ネットワーク管理機能

ネットワーク全体を統合的に管理する統合管理機能であり, サブネットワーク管理レベルを介して下位レベルのネットワーク各資源の管理を行う。統合ネットワーク管理システムは, 下位のサブネットワーク管理システムを各装置の集線ノード的位置付けとし横断的にネットワーク全体の把握を可能とするとともに統合的ネットワーク管理を実現する。

このように V I S I O N - N M S の管理方式は, 分散統括管理方式を採用することにより, 各装置, ベンダごとに異なるインタフェースをそれぞれサブネットワーク管理システムで吸収し, 標準インタフェースにより上位と接続する

ことにより容易に統合ネットワークシステムを構成することができマルチベンダ環境でのネットワーク管理も可能とする。

管理サービス機能

V I S I O N - N M S のサービスは、ネットワーク管理システムの利用者の形態に応じた運用・保守・計画機能に分類し各々豊富な管理サービス機能を提供している。

① 運用機能

ネットワークの各種資源の状態を常時監視し、各装置の稼働状態および負荷状態に関する情報を収集し、ネットワーク資源の効率的運用や安全性を維持する。更に性能情報、負荷情報は、統計データベース化し、これらの情報分析することによりネットワーク最適化の検証およびネットワーク拡張計画を容易に行うことができる。

② 保守機能

ネットワークの信頼性、安全性を確保するために予防保守として実施する定期試験あるいは障害が発生した場合に障害箇所の特定化を行うために実施する試験・診断であり、遠隔保守、障害診断などの機能がある。

③ 計画機能

ネットワークを構成する各装置、回線などの物理的構成情報、資源使用状況、性能情報などを管理し、必要な統計情報および履歴情報を提供する機能及び課金処理機能がある。

(3) VISION-NMSの論理構造

VISION-NMSの論理構造は、OSI管理論理モデルをベースにしている。論理構造モデルを図1.23に示す。OSI管理の標準化への対応は、論理構造のNMPE (Network Management Protocol Entity) の拡張として順次OSI管理標準を導入していく。NMPEへのOSI管理の取り込みは、ネットワーク管理サービスアプリケーションに影響しないようにNMUP (Network Management User Process)の移行性を保証する。

・NMUP (ユーザプロセス)

ネットワーク管理を行う利用者プログラム群であり、運用・保守・計画機能ごとに目的別に構築される。アプリケーションプログラムは、NMMP (Network Management Managing Process) の提供するネットワーク管理ファシリティ、マンマシンインタフェースおよびデータベースインタフェースを用いて種々の機能を実現するとともに、これらのインタフェースを開放することによりユーザアプリケーションをカスタマイズ可能とする。

・NMMP (マネージングプロセス)

NMMPは、ネットワーク管理プログラムに必要なネットワーク管理ファシリティを提供するエンティティであり、エージェントプロセスとのアソシエーションの管理、管理情報の転送のための制御および蓄積を行う。NMMPは、OSI管理のSMFA (Specific Management Function Area: 特定管理機能領域) の管理サービス要素と同一の位置付けとしている。

・NMPE (プロトコルエンティティ)

プロトコルエンティティは、マネージャおよびエージェントともに実装され、マネージャとエージェント間のネットワーク管理プロトコルによる接続性を保証する。本エンティティは、管理情報転送プロトコルを実現するエンティティ

であり、各種プロトコルをどのように制御するかはNMMPおよびNMAP (network Management Agent Process)に任せられる。

NMPEは、OSI管理のCMISE (Common Management Information Service Element: 共通管理情報サービス要素), ROSE (Remote Operation Service Element: リモートオペレーション・サービス要素) およびACSE (Association Control Service Element: アソシエーション制御サービス要素) を基本ソフトウェアとして提供する。

・NMAP (エージェントプロセス)

ネットワーク管理プロトコルによって転送されたネットワーク管理情報に応じて、管理対象装置を管理・制御する。

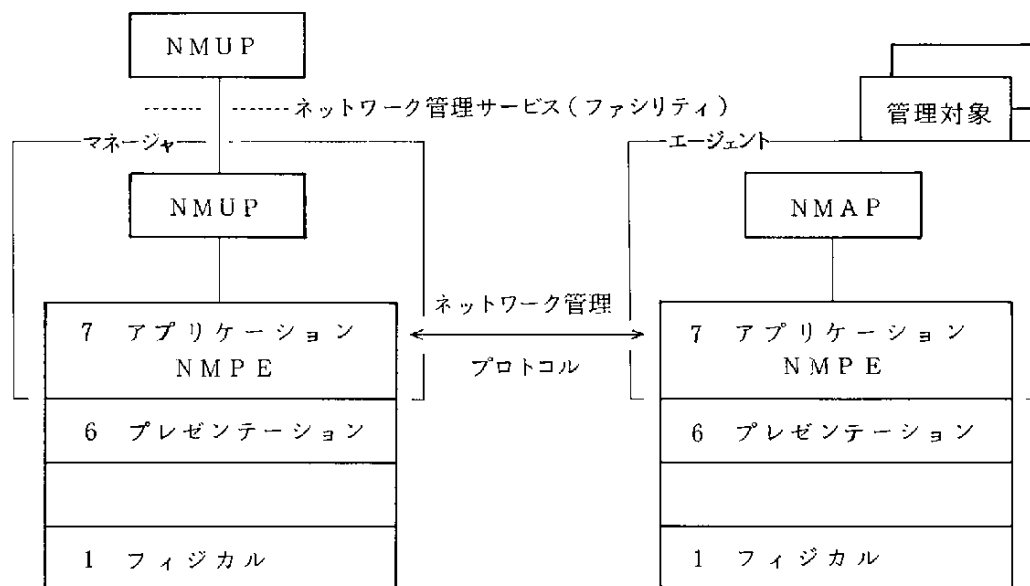


図1.23 VISION-NMS論理構造モデル

V I S I O N - N M S の 具 体 的 イ メ ー ジ

以上、O S I 管理論理モデルをベースにしたV I S I O N - N M S の 論 理 構 造 を 述 べ て き た が、以 下 に V I S I O N - N M S の 具 体 的 な イ メ ー ジ 構 成 の 概 要 について述べる。具体的なイメージを図 1.24 に示す。

V I S I O N - N M S は、以下のサブネットワーク管理システムの組合せにより構成される。

- ・ コンピュータ／端末サブネットワーク管理システム
- ・ 伝送サブネットワーク管理システム
- ・ 交換サブネットワーク管理システム
- ・ ゲートウェイサブネットワーク管理システム

各サブネットワーク管理システムは、それぞれエージェントと呼ばれる集中管理機構の下でサブネットワークに閉じたネットワーク管理を行う。

N M S マスタプロセス内のマネージャは、これらのサブネットワークをエージェントを介して統合管理する。

各サブネットワーク内では、必要に応じてさらに階層構造をとることができる。ただし、この内部構造は他のサブネットワークを意識しないことを原則としている。V I S I O N - N M S は、また以下の外部システムと連携して機能することが可能である。

- ・ 保守支援システム
- ・ 環境保全システム
- ・ 他のネットワーク管理システム

保守支援システムは、V I S I O N - N M S に対し専門的な立場から各種診断、障害解析、ソフトウェア更新などの支援を行う。環境保全システムは、オフィスファクトリ環境を管理するものとしてネットワークシステムの置かれている環境すなわち局舎、付帯設備の管理を行う。

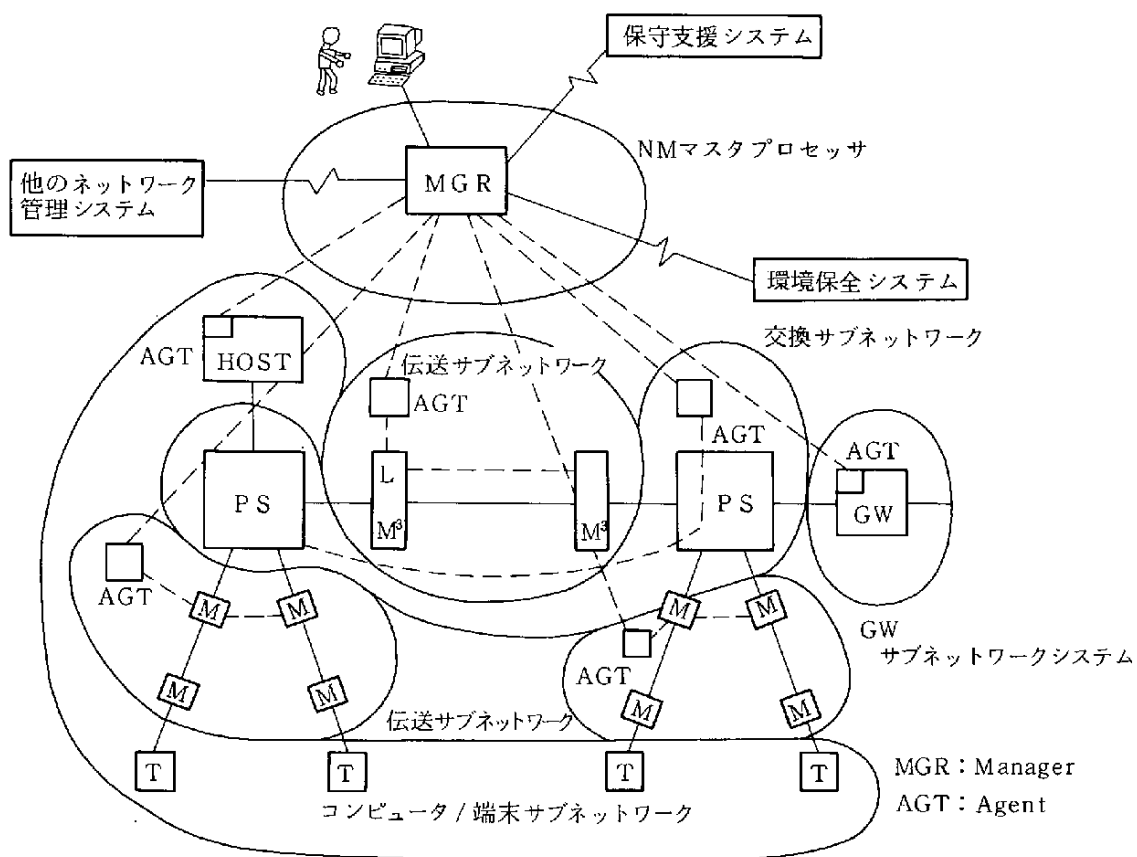


図1.24 VISION-NMSの具体的イメージ

(4) システム構成

VISION-NMSとサブネットワーク管理システムおよび管理対象装置との構成イメージを図1.25に示す。

VISION-NMSの核となるNMSマスタプロセッサは、ミニコンピュータMSシリーズあるいは大型汎用機のACOSシリーズからネットワーク規模および適用管理サービス機能により選定できる。

NMSマスタプロセッサには、監視用コンソールと制御用コンソールが接続され、監視の一元化、制御の一元化を可能とする。

VISION-NMSは、ネットワークの各種資源の稼働状態を常時監視し、管理対象装置からの障害情報を受け取ると監視コンソールへ表示、ブザー鳴動するとともに履歴情報としてログファイルへ登録する。これにより障害の迅速な対応を可能とし、制御コンソールを使用し障害の特定化、復旧作業を可能とする。

監視画面は、グラフィック表示を用いて運用者に対するネットワーク全体の稼働状態を容易に認識できるように視認性の高いマンマシンインタフェースを提供する。更に監視画面は、ネットワーク全体／ローカル地域などユーザの管理体制に合わせた画面を用意し、それらを階層構成で表示し、地域から装置単位、パッケージ実装単位までの監視を容易に行うことができ、同様に大型ディスプレイに表示できる。ネットワーク構成の監視画面は、ユーザごとにカスタマイズすることを可能とし、更に障害種別の表示色を変えることにより、より一層のビジュアル表現を高めている。

- ・ 緊急障害 (Major)
- ・ 準緊急障害 (Minor)
- ・ 注 意 (Caution)
- ・ 単なる通知 (Information)
- ・ 介入要求 (Intervention Required)

制御コンソールは、ネットワークの制御および保守用として使用し、運用モードの変更、障害の特定化、ネットワークの資源の試験・診断あるいはネットワークの再構成などを行う。コンソールは、運用形態に合わせて複数台設置することが可能であり、また遠隔によりネットワークの監視・制御できる。

アラーム接点情報装置は、信号レベルによる物理的な障害検出を装置の外部からアラーム接点情報の収集を可能とし、また局舎の付帯設備、電源装置あるいは他ベンダ機器からアラーム接点情報が取り出せる場合にはこれらの情報をこのアラーム接点情報装置で収集しネットワーク管理センタにて集中監視することも可能である。

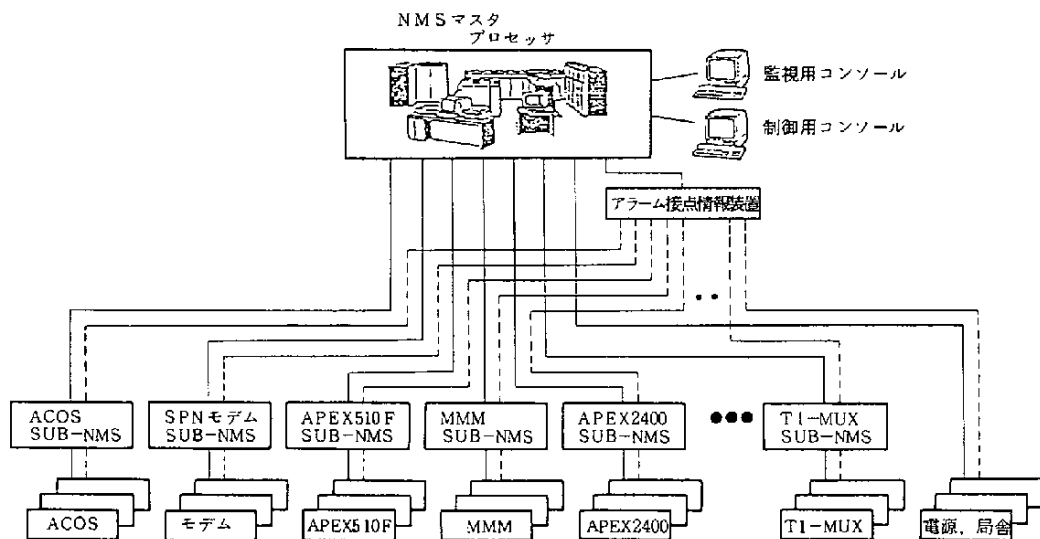


図 1.25 V I S I O N - N M S システム構成

(5) 今後の展開

開放的ネットワーク管理システム

ネットワーク管理システムは、企業情報ネットワークの信頼性、安全性を維持するために、ますます重要性を増していく。

今後、ISDN、衛星通信を利用することによりネットワークのグローバル化といった、ますます広域化、複雑化、国際化していく企業情報ネットワークに対するネットワーク管理システムの期待は大きい。またネットワーク構成機器のマルチベンダ化が進むなかで、早期のネットワーク管理の国際標準化が重要な課題となる。日本電気の提供するVISION-NMSの目的は、OSIネットワーク管理システムの標準動向を見つめながら開放的ネットワーク管理システムを製品化し将来を展望した企業戦略ツールとして提供していくことにある。

1.3 LANやワークステーション環境を中心としたネットワーク管理について

I S O (国際標準化機構)でのO S I (開放型システム間相互接続)の考え方が普及する一方で、エンドユーザに近いLANやワークステーション環境においては、広域網における以上に、数多くの各社固有のネットワーク・アーキテクチャが存在している。このため、ネットワーク管理も、それらに応じた特有の方式がとられているのが実情である。本文では、まず、LANやワークステーション環境を中心としたネットワーク管理の位置付けについての一般的な考え方を記述する。そして、研究段階のものを中心にして、LANや分散システムにおけるネットワーク管理を実現する上での種々の考え方、課題、あるいは実現例を、1988年に開催された国際ワークスショップI F I P T C 6 / W 6.4 Aの予稿集の中から、LANや分散システムにおけるネットワーク管理についての論文を調査することなどから紹介する。さらに、I E E E 8 0 2 委員会で検討されているようなLANに、O S I 管理を適用する場合の考え方についても言及する。

1.3.1 LANやワークステーションにおけるネットワーク管理の位置付け

(1) 管理領域と管理主体

図1.26にX.25パケット網やI S D NなどのWAN (Wide Area Network; 広域網) およびLANから構成される一般的なネットワークの階層構成を示す。すなわち、ワークステーション等のエンドシステムは通信用インタフェースを介してC S M A / C D やトークンリングなどのアクセスプロトコルを持つ中低速の、フロアレベルに相当する支線LANに結合される。いくつかの支線LANは、ブリッジを介してF D D I (Fiber Distributed Data Interface)やT D M A - L A N などの高速の幹線LANに結合される。そして、この幹線LANが、ゲートウェイを介してWANに結合されるというのが一般的な構成と考えられる。このモデルに従えば、各レベルまたは領域の管理は表1.2に示すような管理領域とそれらに対応する管理主体との組み合わせで区分することが

できる。

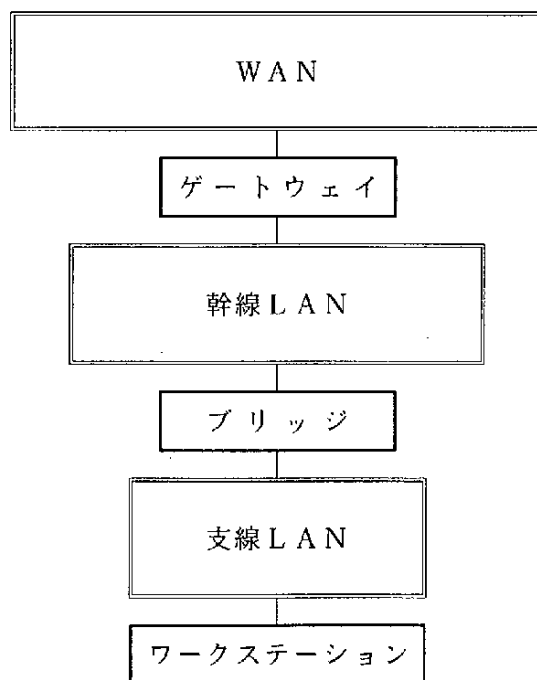


図 1.26 一般的なWANおよびLANの階層構成

表 1.2 一般的な管理領域と管理主体

管 理 領 域	管 理 主 体
WAN	WANマネージャ
ゲートウェイ	WANマネージャまたはゲートウェイ
幹線LAN	幹線LANマネージャまたはゲートウェイ
ブリッジ	幹線LANマネージャまたはブリッジ
支線LAN	支線LANマネージャまたはブリッジ
ワークステーション	ホストOSまたはホスト管理機能
通信用インタフェース	インタフェース内局管理機能

(2) LANの管理

LANにおける管理対象としては、メディアや物理層でのリピータ、データ

リンク層でのブリッジ、ネットワーク層でのルータトランスポート層以上でのゲートウェイ等の中継装置、さらに通信用インタフェース内のモデムやプロトコルマシンなどが挙げられる。各管理対象には管理情報があり、たとえば、メディアには断線チェック情報、モデムには送受信機動作チェック情報等の情報が管理される。プロトコルマシンでは、プロトコル固有のカウント情報等のほか、構成管理情報としての各ノードのアドレスが管理される。

(3) ワークステーション環境の管理

ワークステーション環境における管理対象としては、ワークステーションそのもののほか、ファイル、プログラム、また外部メモリ装置、プリンタ、イメージスキャナ等の周辺装置などがある。ワークステーションそのものは、固有名およびアドレスにより管理され、たとえば、UNIXの4.3BSDの環境では指定領域あるいはドメイン内の資源の固有名を管理するネームサーバ、ネームサーバに対するクライアントであるネームレゾルバが実装される。また、ファイルの管理においては、同じくUNIX環境でNFS(Network File System)とよばれる異なるワークステーション内の階層的に構成されたファイルシステム内のディレクトリを互いにリンクすることにより、ファイルの共有を可能にするような管理機能などが実用されている。さらに、ワークステーションの電源が不用意に切られ、他のエンドシステムからのアクセスが不能になったときの遠隔立ち上げ方法などのネットワーク運用管理上の問題も重要である。

1.3.2 種々の管理アーキテクチャの検討例

(1) サービスタイプによる管理 (Imperial College, UK)⁽¹⁾

分散システムでは個々のサービスが互いに他のサービスを利用してそれぞれの機能を実現していると考えられる。そのサービス構造を表現するのに、仮オブジェクトとしてのサービスタイプと、そこから生成される実体であるサーバ

という概念を用いる。管理は、サービスを維持し拡張させることを可能にするための機能であり、管理情報を構成要素から集め判断し、乖離オペレーションを実行する管理エージェントをサービスタイプ内部に含めることにより図1.23のようにモデル化できる。主な管理機能としては、構成管理、名前管理、監視、故障処理、性能最適化、保険管理、課金などがあるが、これらの管理機能は互いに関連し合っており、それぞれをサービスタイプと考える整理することができる。また、管理領域は階層状の構造を持つのが通常で、地域、組織、機密管理上の境界に基づくまとまりであるドメインの概念を各階層での管理単位として導入することにより管理の構造が記述できる。

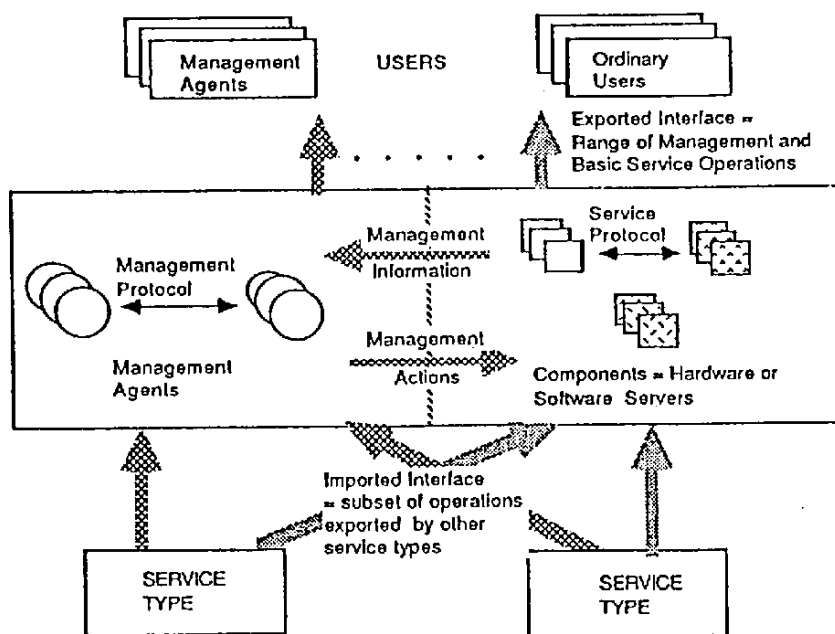


図 1.27 サービスタイプ情報の流れ

(2) データディクショナリによる管理
(University of London Computer Center, UK)⁽²⁾

ネットワーク管理における5つの機能的管理分野—障害、構成、性能、機密、および会計—の管理機能は、図1.28に示すように相互に関連し合っている。これらの管理情報を効率的に処理するために広域分散システムをサポートする技術を開発するためのプロジェクトであるADMIRALでは、従来の、情報を

一括して中央に蓄積する方法を修正し、単に、どこにデータがあるかが分かるように、データ・ディクショナリを用いる分散的な方法を実現した。これは Recnik と呼ばれる仮想データベースに基づく情報管理方法であり、図1.29に示すように、データ・ディクショナリ、ルータ、トランスレータ、およびノーティファイアから構成される。このとき各管理エンティティはRecnik をコールすることで情報の獲得や編集が行える。

(3) LAN相互接続における管理 (University College London, UK) ⁽³⁾

LAN間を相互接続する装置として、MAC (メディアアクセス制御) 副層で中継するMACブリッジとネットワーク層で中継するルータが存在する。この2つの装置に関して、以下の6つの観点から比較している。

- ① プロトコルの透過性：ブリッジはいかなる上位層もサポートできる。
- ② ホスト、ブリッジ、およびルータのアドレッシング：ブリッジを使用する場合は、ホストはアドレッシングに関し何らプロトコルを持つ必要はないが、ルータを使用する場合はアドレスレゾリューションプロトコルがホストとルータ双方に必要である。
- ③ 障害の分離とトラフィックの限界：ブリッジもルータも障害の分離を容易にし、システムが許容するトラフィックの限界を向上させる。
- ④ ルーティングとループの防止：ブリッジは、ルーティング時のループ防止のプロトコルはないが、ルータには存在する。
- ⑤ アクセス制御：ブリッジにとってのアクセスは物理アドレスに基づいており、ルータにとってのアクセスはネットワークIDに基づいている。したがって、ルータの方が扱う情報としては少ない。
- ⑥ 遠隔管理：ルータに関しては多くの遠隔管理プロトコルが存在するが、ブリッジにはない。

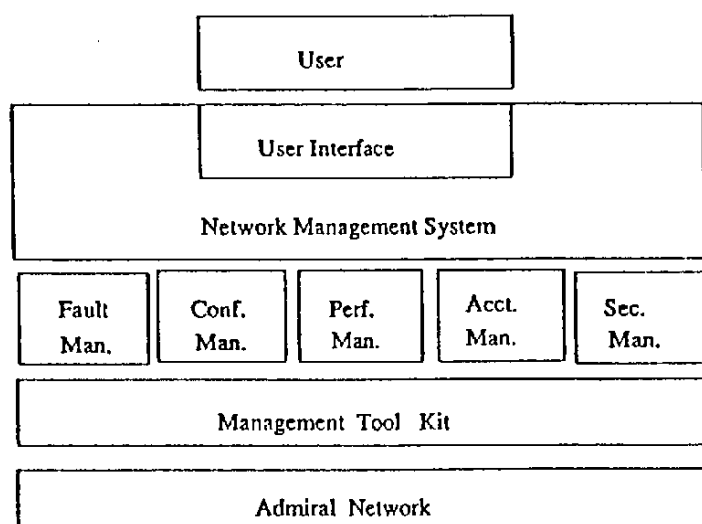


図 1.28 管理フレームワーク

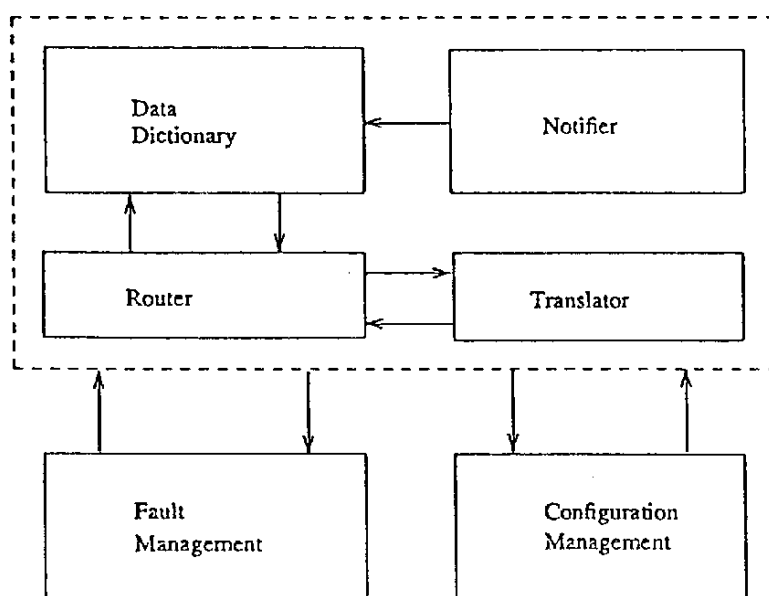


図 1.29 Recnik の内部構造

(4) オブジェクト指向ポートによる管理
(Bulgarian Academy of Sciences, Bulgaria) ⁽⁴⁾

完全に分散化されたオペレーティング環境を構築・管理する1つのアプローチを紹介する。このオペレーティング環境は、カーネル、ネットサーバ、およびファイル転送など種々のアプリケーション・プロセス群からなり、カーネルがマルチタスク制御とオブジェクト指向型のプロセス生成をサポートする一方、ネットサーバが複数プロセス間の統一的な通信手段を提供する。図1.30に示すように、通信はオブジェクトとして定義されている何種類かのポートを介して行われる。プロセス生成時にネットサーバとの通信用のポートが作られ、プロセスはこれを通じて他のプロセスからのメッセージを受け取るためのポートを任意に生成、制御、および削除をする。ネットサーバはこれらのポート操作に合わせて、自ノードおよび他ノード上のアドレステーブルを管理し、透過的なプロセス間の通信を実現する。

(5) 分散システム・カーネルによる管理
(University of Mining and Metallurgy, Poland) ⁽⁵⁾

UMMLANプロジェクトは、大学内LAN上に構築された分散コンピュータ・システムの開発を目的にしている。この研究では、UMMLANネットワークで行っている管理のアプローチが述べられている。ここでは、オペレーティングシステムや上位層からのアクセスを容易にするために、ネットワーク上のノードのオペレーティング・システム内に、トランスポート・サービスを入れている。これは、図1.31に示すように、各ノードが持つ分散システム・カーネルを採用することにより可能になった。この方法は異種のマイクロコンピュータ間の結合を強くし、トランスポート層のオペレーションの管理を簡単にするという利点がある。ここでは、この分散システム・カーネルのプリミティブの定義と、のプリミティブにより構成される代表的な相互プロセス通信メカニズムとして、プリントサーバとプリント・ユーティリティの実例が述べられている。TSB (Transport Station Board) は、CPUとイーサネット・

コントローラとからなり、トランスポート層まで実装しており、ホストとは共有メモリとシステム・バスでつながっている。なお、図1.32ではカーネルの管理構造を示す。

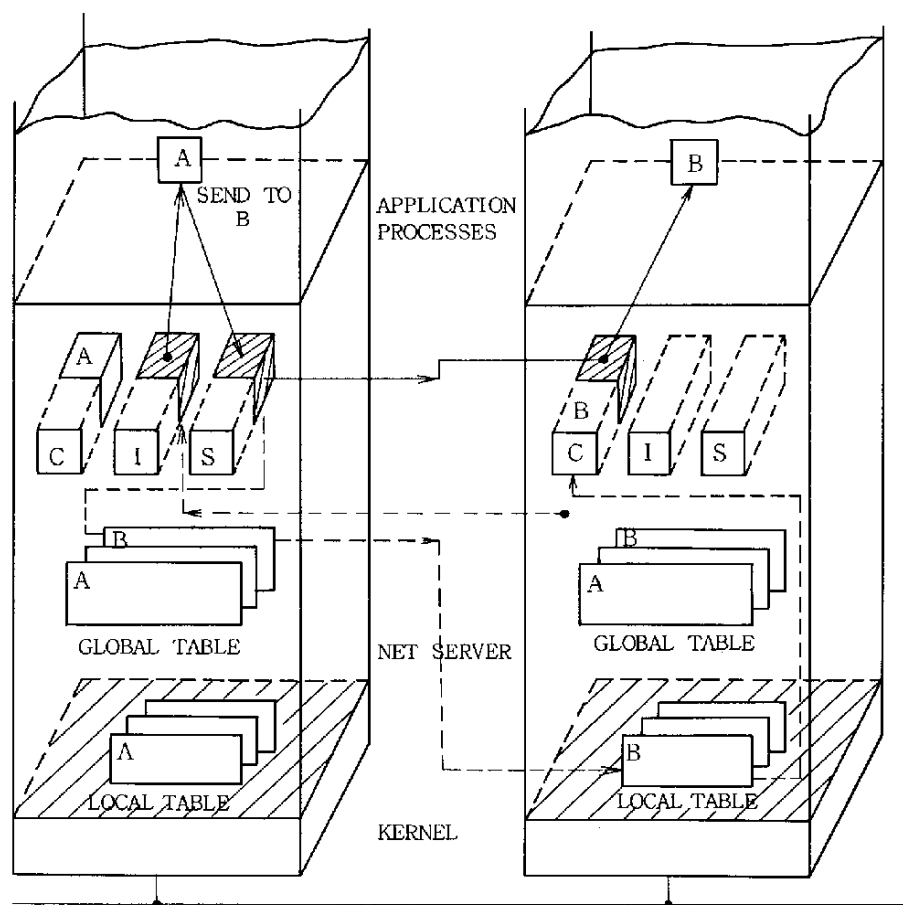


図 1.30 通信ポートを通るメッセージの転送

1.3.3 管理領域と検討例

(1) 障害管理

(a) 光LANにおける自己診断機能など⁽¹³⁾

32Mbpsのトークンリング方式光LANである住友電工製 SUMINET-3300での実現例について紹介する。

① 自己診断機能／切り離し機能

ノードには電源投入リセット時にデバイスを自己診断する機能を実装している。また、運用中、本来の通信の合間に自己診断パケットをリングに送出し、自身の送受信機能をたえずチェックする機能を持っている。もし、ノード自身あるいは伝送路のリングに異常が発生した場合、光ファイバコンセントレータでは、障害の箇所によってバイパス、ループバックにより障害部分をネットワークから切り離し、予備系の光ファイバを用いて、リングを再構成する。(図1.29参照)。

② ネットワークモニタ機能

NSM(ネットワーク・サービス・モニタ)の端末から、ネットワークの監視や利用状況を照会することができる。異常の発生したノードを診断パケットによって調査するコマンドやリング上の順列をモニタする機能がある。なお、広域網を利用した遠隔保守機能サービスも提供している。

(2) 構成管理

(a) 光LANにおけるプログラム・ダウンロード機能など⁽¹³⁾

同じくSUMINET-3300における具体例を紹介する。

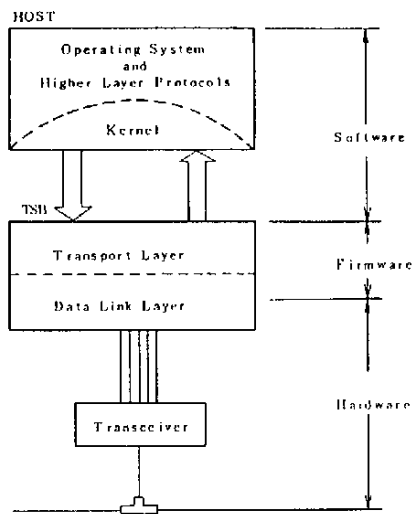


図 1.31 UMMLAN ノード

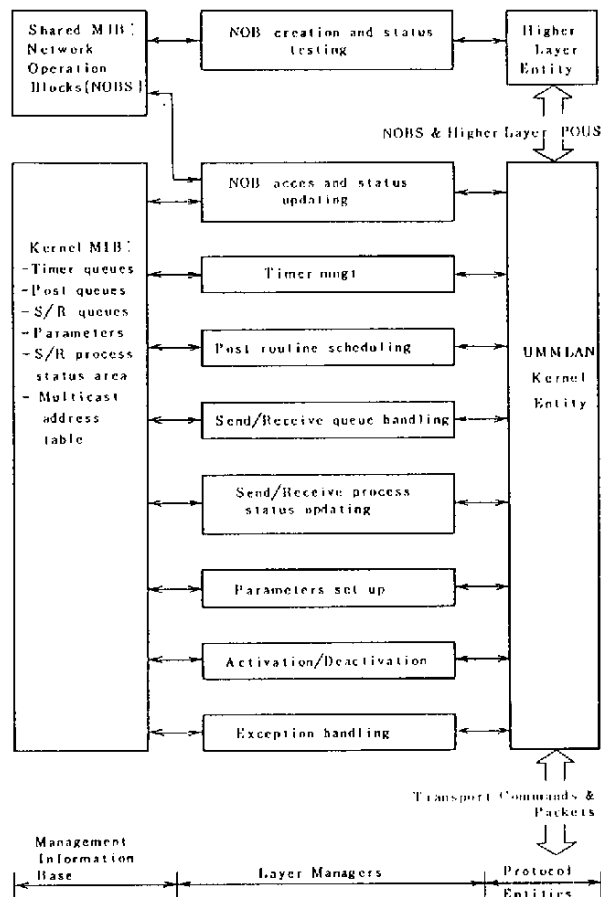


図 1.32 カーネル管理機能

① プログラム・ダウンロード機能

ノードのプロトコルは種類が多く、機能追加やノードごとのパラメタの設定など、ソフトウェア構成の変更が要求されることがある。そのため、ノードは最低限のプログラムをファームウェアとしてROMに実装し、その他のプロトコルはNSMのディスクに格納してあり、各ノードの電源投入により自動的にダウンロードされる。この場合、ダウンロード・プロトコルは次の通りである。電源がリセットされたノードは自己診断した後、自分のノードアドレスを付けてダウンロード要求パケットを一斉に同報する。NSMでは同パケットを受信すると、そのノードとのプロトコル・ソフトウェアをディスクから取り出し、アドレスを付けて送信する。要求ノードでは送られてくるプロトコル・ソフトウェアをRAMに配置し、ノードとして稼働を開始する。

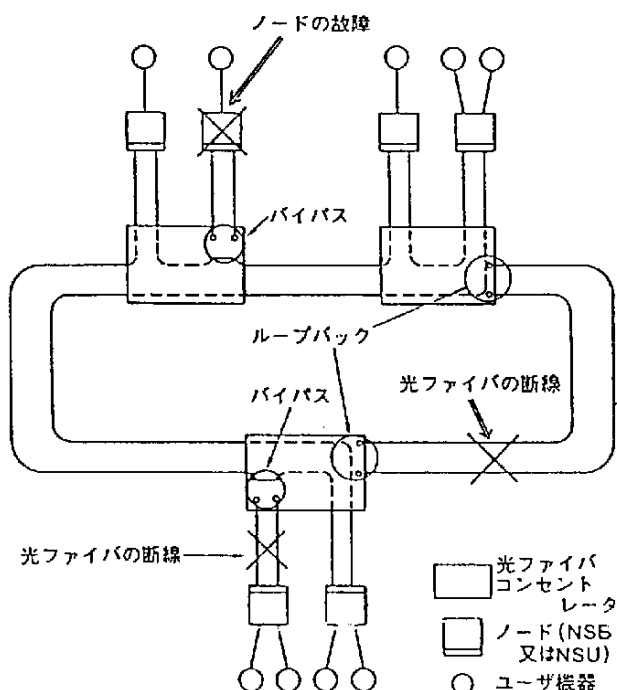


図 1.33 光ファイバコンセントレータによるバイパス／ループバック

② ノード・コンフィギュレーション機能

NSMに格納してあるノードのプロトコル・ソフトウェアをCRT端末を用いて編集する機能である。編集項目として、ノードタイプに応じた基本プログラムの選択、愛称の設定などがある。

(b) 相互接続ネットワークのための分散管理 (IEI-CNR, Pisa, Italy)⁽⁶⁾

LANやWANにおける、広範囲勝つ広帯域で、より高度なサービスの結合を考えるとときに、問題になる帯域幅の管理に対し簡単なアルゴリズムを提案する。この提案は、相互接続ネットワークの大規模システムを対象にし、パケットのオーバーヘッドが軽く、ハードウェアが複雑にならないという特徴がある。アルゴリズムは以下のようにになっている。各局はトラフィック測定器を持ち、パケットの伝送レートの平均値が観測できる。ホストがコネクション時に使う経路に沿って宛先ホストに送る。このパケットは、コネクションに必要な帯域についての情報を持つ。経路に沿う各ノードは、その帯域要求が可能となきのみ中継し、不可能なときはそのパケットを捨てる。宛先ホストからACKパケットが返ってきたら当該経路にて要求帯域が確保されたとし、通信を始める(図1.34および図1.35参照)。その他、サイレンスの状態でも、新たなコネクションが張られるのを阻止するための、帯域保持パケットなども考えられている。

(c) サービス統合型ネットワークにおけるチャンネルの割り当て (Face-RC, Italy)⁽⁷⁾

超広帯域コヒーレント光通信ネットワーク上での複数のチャンネルに周波数を分割して用いる方法が取り扱われている。ネットワークの構造に影響を与えるOSIの下位3層のうち物理層では、複数のチャンネルごとの光インタフェースを持っている(図1.36参照)。物理層管理は、これらの光インタフェースへの周波数の割り当てを行う。データリンク層は、非同期のバースト的なサービスを提供するMACと長時間の大容量のサービスを提供するMACと異なったサービスを提供する複数のLLC(ロジカルリンク制御)から構成される。データ

リンク層管理エンティティは、これらのサービスのトラフィックを管理するための管理情報ベースとして各種のマップを作成する。たとえば、ネットワーク層では、ネットワーク層管理エンティティが管理する各局の周波数割り当ての要求待ちマップを用いて情報のルーティングを行う。基本的には、OSI管理に準拠したものであり、管理情報の交換にはトークンバス方式の別建てのバスを用いている。

```
select route for connection
send allocate-band packet
if (positive ACK received)
    then start regular transmission
else < retry or give up as appropriate >
endif
```

図 1.34 ホスト向けのコネクション開始プロトコル

```
if (request < internetwork capacity - monitored traffic figure)
    then { forward packet;
          monitored traffic figure =
              monitored traffic figure - request }
else { drop packet;
      [send NACK] /* optional */}
endif
```

図 1.35 ノードからの帯域割り当てパケットの処理

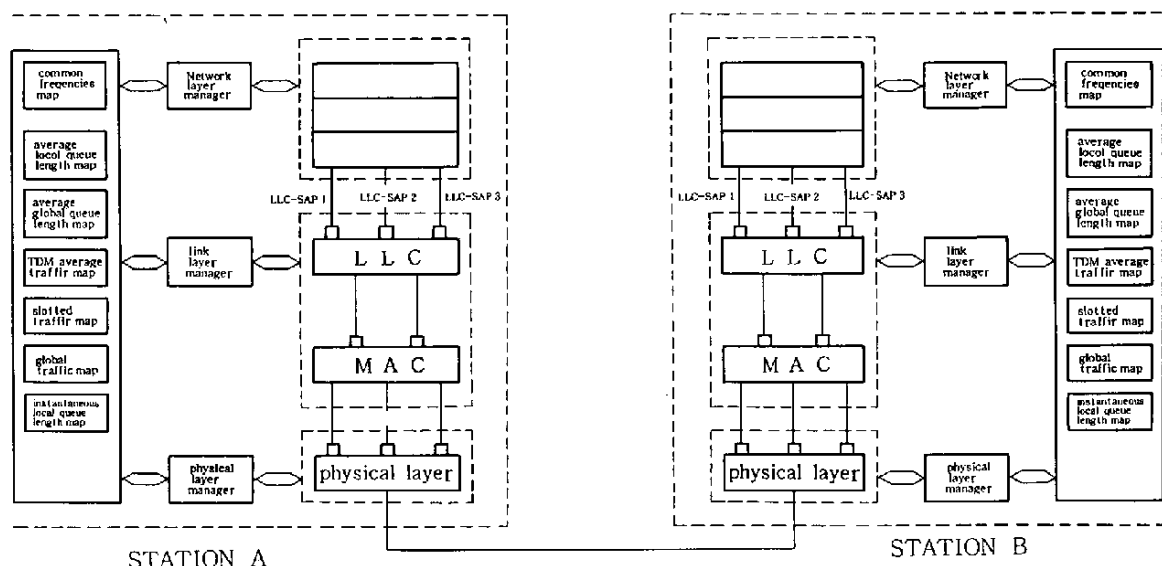


図 1.36 局間相互接続アーキテクチャ

(d) 位置情報やアベイラビリティ情報の管理
(University College London, UK) ⁽⁸⁾

ネットワークの構成管理は、構成情報を収集しネットワーク資源の構成を制御して、サービスの質を維持することを目的とする。構成情報には、名前、アドレス、および経路などの位置情報、アベイラビリティやリーチャビリティ情報がある。リーチャビリティはネットワークの階層別マップで簡潔に表現できる。構成管理情報には、これらの構成の変化をユーザやモニタからの情報で知り、データベースを更新するとともに経路制御機構と協調して経路テーブルを更新する機能が必要である（図1.37参照）。また、必要に応じて障害管理など他の管理機構を起動することが要求される。例えば、ここのLANでは、構成管理はシステム管理者による名前・アドレスの管理と、その結果を配布する機能で構成されている。分散された相互監視、再構成を行う自動的な構成管理機能を持つシステムもある。

(3) 性能管理

(a) LAN-WANゲートウェイにおけるネットワーク性能管理 (Hatfield Polytechnic, UK)⁽⁹⁾

LANの出現により、資源の最適分配を実現する分散OSの技術が発展してきている。LANがWANを介して接続され始め、LAN上で培った分散OSの技術をそのままそこでも適用しようとする研究がなされてきた。ここでCOST 11 ter MANDISシステムで実装されているLAN-WANゲートウェイの管理機能を例にとりて考察する。これはOSI参照モデルとは違ったアーキテクチャを持つものであり、ここでの分散システムはクライアント・サーバ間でのコネクションレス型プロセス間通信に基づく(図1.38参照)。また、ゲートウェイはリモートに位置するものと通信しようとしているローカルのサーバあるいはクライアントに対してそれぞれクライアント、あるいはサーバとして機能する。ゲートウェイは、アクセス制御、課金、モニタ、障害管理、性能最適化等の管理機能も持たせている。たとえば、性能最適化に関していえば、LAN上のプロトコルでの短い再送タイマのタイムアウト値に起因するLAN側からの数多くの再送を、ゲートウェイは適度にフィルタするものである。このように、WANを介しての分散システムにおいてはOSI参照モデルで規定している機能上のものとしては、たとえば前述のようなインテリジェントなゲートウェイが必要であることが示された。

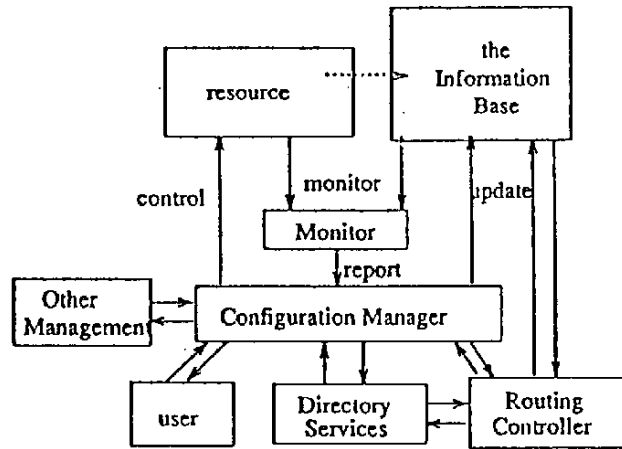


図 1.37 構成管理の要素

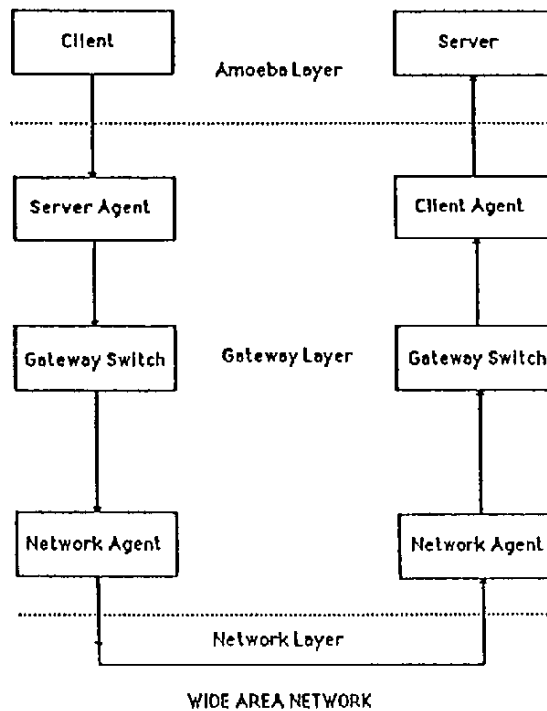


図 1.38 ゲートウェイとWANを介するクライアント・サーバ間の相互利用

(4) 機密管理

(a) LAN-WANゲートウェイにおけるネットワーク機密管理 (University of Kent, UK)⁽¹⁰⁾

ケント大学とケンブリッジリングをつなぐゲートウェイの管理においてはハッカーに対する対策が重要である。そこで、16段階のアクセスレベルと16段階のプライオリティを各ホストとユーザに付け、またユーザ名とパスワードを1台のコンピュータで管理している。

1.3.4 LANにおけるOSI管理について

LANにおける標準化はIEEE 802委員会の下の802.3 (CSMA/CD方式), 4 (トークンバス方式), および5 (トークンリング方式), 各ワーキンググループを中心に標準化が進められている。これらの標準は, ANSIの承認を経て, ISOにおいて国際標準となる。このとき, それぞれはISO 8802-3, 4, および5と呼ばれる。OSIモデルにおける物理層およびMAC副層は, 図1.39に示すように, ISO 8802-2 (IEEE 802-2) で規定されるLLC副層の下位に位置付けられている。したがって, 管理オブジェクト (MO: Managed Object)の包含関係を示すトリーは図1.40のように書かれる。

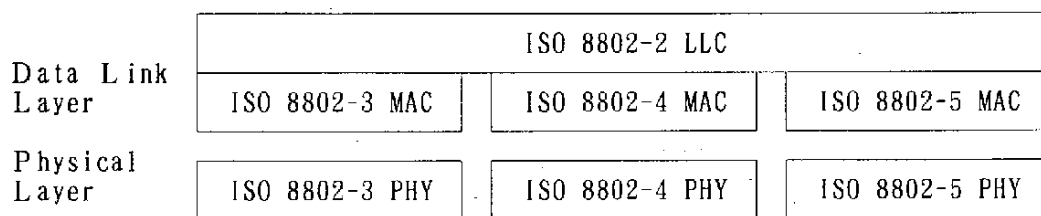


図 1.39 ISO 8802 関連の層構造

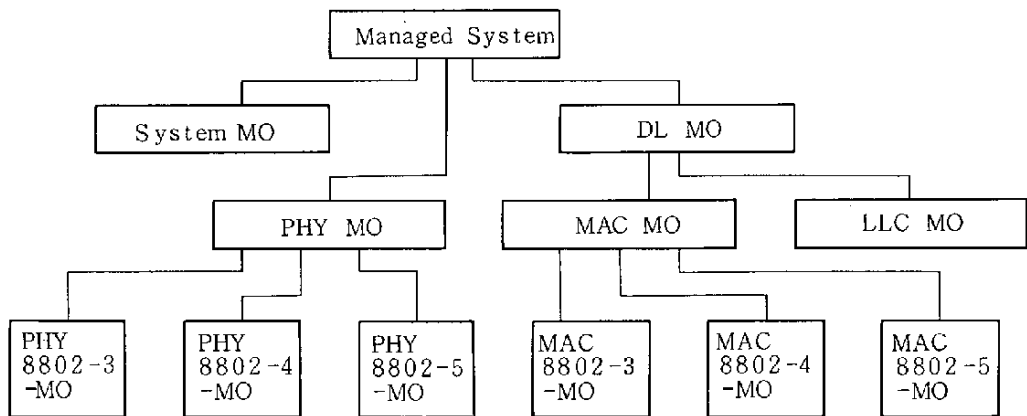


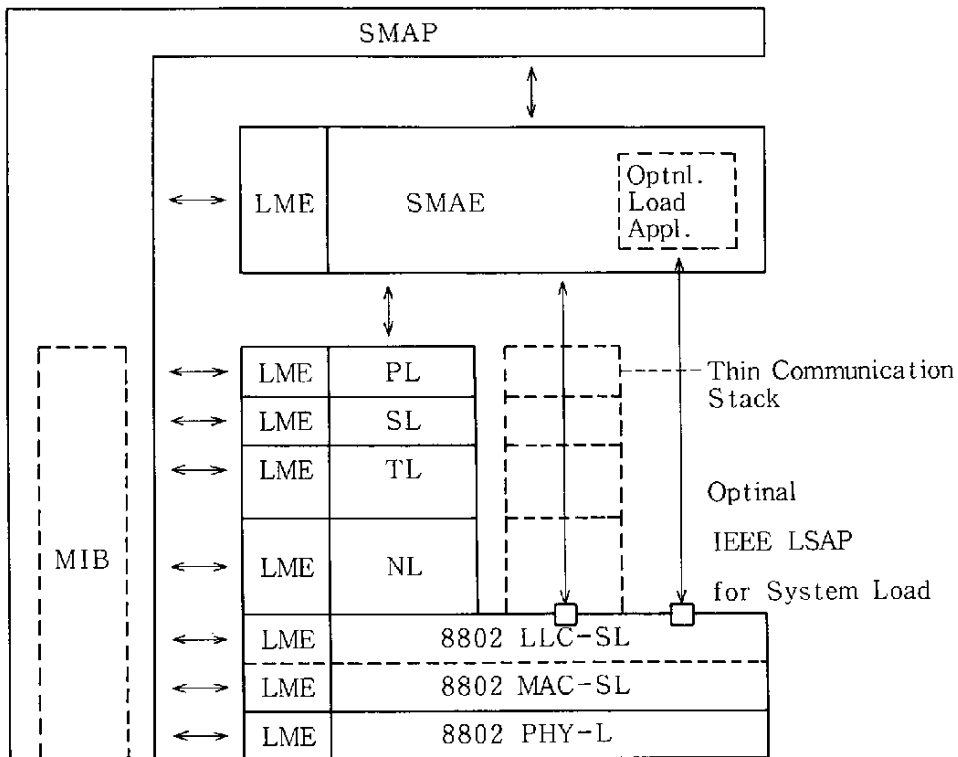
図 1.40 ISO 8802 包含木の構造

図 1.41 に OSI 管理アーキテクチャにおける ISO 8802 層管理の位置付けを示す。SMAE (システム管理アプリケーション・エンティティ) はプレゼンテーション・サービスを用いることもできるが、いわゆる、Thin Communication Stack を通して、直接、データリンク・タイプ 1 (コネクションレス型) のサービスを用いることもできる。また、システムプログラムのローディングをサポートするため、データリンク層のサービスを用いることをオプションとしている。ローカルシステムの層管理は実装者に任されるロヒカルマスターであるが、少なくともリモートシステムの層管理は、各層の LME (層管理エンティティ) と

SMAP (システム管理アプリケーション・プロセス) との間で各層または各プロトコルにおける管理情報が交換されることにより行われる。

IEEE 802 委員会では、IEEE 802.3 ワーキング・グループが、ISO での OSI 管理標準化の動きに協調しながら、ネットワーク管理に関するフレームワークをほぼ終えた段階である⁽¹¹⁾。また、個々のアクセス・プロトコルに対する管理情報は個別の標準内に列挙されている。実装規約レベルでは、IEEE 802.4 トークンバス方式を採用している MAP (Manufacturing Automation Protocol) バージョン 3.0 におけるネットワーク管理実装仕様が最も先行しており、上記の考え方に基づくものとして雛形的存在となっている

(12)。



LME : Layer Management Entity
 LSAP : LLC Service Access Point
 MIB : Management Information Base
 SMAE : System Management Application Entity
 SMAP : System Management Application Process

図 1.41 OSI管理アーキテクチャにおける
IEEE802層管理

ISOにおけるOSI管理標準においては管理情報を交換するときのプロトコルや管理情報とその記述方法については標準化していこうとしているものの、個々の管理情報の利用方法や制御方法については標準化の範囲外としている。たとえば、ルールベースでLANやワークステーション環境上の障害の把握から原因を追求し復旧策を案出するような、AIを適用した障害管理システムも開発されている。言い換えれば、ネットワーク管理者とネットワークシステム間の応用プロセスのレベルこそが、ネットワークシステムの機能性を決定する

と同時に、ネットワーク管理製品相互の差別化のポイントになると考えられる。

SUMINETは住友電工の登録商標である。

UNIXはAT&Tの登録商標である。

NFSはSun Microsystemsの登録商標である。

<参考文献>

- [1] M.Sloman, "Distributed Systems Management."
- [2] D.Sirovica, et al, "Recnik: A Virtual Database for Coordination of Distributed Network Services."
- [3] J.Crowcroft, et al, "Managing the Interconnection of LANs."
- [4] L.Manassiev, et al, "Object Oriented and Port Based Distributed Operating Medium."
- [5] P.Magra-Witkowski, et al, "Distributed Systems Kernel and Interprocess Communication in LAN Environment."
- [6] F.Grandoni, et al, "An Algorithm for Distributed Management of Traffic on Interconnected Networks."
- [7] A.Fioretti, et al, "Design Issues of OSI Layers in Integrated Services Multichannel Metropolitan and Regional Area Networks."
- [8] Y.Murayama, et al, "The Scope of Network Configuration Management."
- [9] J.Hall, et al, "Gateways and Management in an Internet Environment."
- [10] I.Dallas, "Operational Experiences in Managing a LAN/WAN Gateway."

以上は, "Issues in LAN Management," "Proceedings of the IFIP TC6/WG6.4A Workshop, North-Holland, 1988 から。

- [11] Draft IEEE Standard 802.1(Part A)-Overview, Interworking and Systems Management - Supplement B: Systems Management - Trial Use Standard.
- [12] Manufacturing Automation Protocol Specification Version 3.0, Implementation Release.
- [12] 橋本他, 「高速光ローカルエリアネットワーク UMINET-3300 の開発」, 住友電機, No.129, 1986.

1. 4 回線環境を中心としたネットワーク管理

電気通信網はアナログ設備を主体とした通信網からデジタル設備を主体とした通信網へと発展してきた。このような通信網のデジタル化により、多彩なサービスを提供するサービス総合化へ向けて通信網は急速な変貌を遂げつつある。また、電気通信サービスに対するユーザのニーズが多様化・高度化するに従って、経済的で良質なサービスを提供することが必要となる。このため、通信品質の維持・向上、保全サービスの向上、及び通信網の効率的な運営を目的とした通信網管理システムを実現する必要がある。本システムの対象となる通信網管理業務には、通信網設備を状態を常時モニタし、故障発生時に試験や制御を行う故障管理業務、顧客毎の住所や機器構成情報などの収集・活用を行う顧客管理業務、通信網設備の計画・設計・建設管理を行う設備・建設管理業務等様々なものがある。未報告では上記の通信網管理業務のうち、通信網設備の運用・保守業務を中心にN T Tの通信網管理システムの概要を紹介する。

1. 4. 1 通信網管理の概要

(1) 通信網管理機能

通信網設備の運用・保守に関連した通信網の管理項目は、表 1. 3 に示すように網の構成管理、性能管理及び障害管理の 3 つの項目に分類される。

表 1.3 通信網管理機能

管 理 項 目	管 理 の 内 容	動 作
〔網構成の管理〕 需要や運用状況に即した、必要十分な網構成になっているか？	・通信網設備の導入計画立案，導入の実施，稼働状況の把握，必要時の設備の変更（対需要変動，障害時や試験実行時の構成変更等）など	・設備計画設計 ・設備 ・装置の接続，切換えや切離し ・回線の開通，切換え切離し ・予備切換え，切戻しなど
〔網の性能管理〕 網の目標性能は，発揮されているか？ サービス品質は？	・回線の伝送品質，交換機の接続品質，その他個々のサービスで，顧客に明らかにした通信サービスの品質の把握と品質維持の対策	・トラヒックデータの測定 ・伝送誤りの測定 ・サービス品質への換算と評価 ・網構成への反映など
〔網の障害管理〕 網の障害管理個所と修理状況は？	・各装置，設備からの警報をみて障害を発見し正常状態への復旧を図る	・警報の収集 ・警報の解析 ・装置診断 ・切分け試験 ・修理手配 ・復旧確認など

(2) 通信網管理技術の発達過程⁽¹⁾

通信網管理業務は次のような3段階に分けることができる。

① 人手依存の時代（1970年以前）

本時期は人手依存による通信網管理が主体であり，管理の対象範囲も限られていた。

② 集約化の時代（1970～1980年代）

本時期には網管理業務の省力化，保守精度の向上を目的としてアナログ通信網を主体に個々の装置対応，サービス対応に相互に独立したネット

ワーク管理システム（オペレーションシステム）が開発され、現在はその拡充段階にあると言える。

また、この時期にはオペレーションと通信網設備あるいはオペレーションシステム相互間を標準インタフェースを用いて接続するためのTMN（電気通信管理網）のアーキテクチャの研究が進展した。

*Telecommunications Management Network

③ 統合化の時代（1990年代）

前期で個々に開発されたオペレーションシステムの統合が進むと共に、AI技術の導入等により、より迅速・正確・高度な統合オペレーションシステムが実現されよう。

表 1.4 通信プロトコル

TMNの種類 OSIレイヤ		ローカル情報 転送網	汎用情報転送網		WSとの通信用	
OSI参照モデル	応用層	データ形式の規定	OSIプロトコル	NO.7 信号方式 プロトコル	OSIプロトコル *	
	プレゼンテーション層	NULL				
	セッション層					
	トランスポート層					
	ネットワーク層		パケットプロトコル		パケットプロトコル	•電話網
	データリンク層	•LAPB •LANプロトコル •その他	•LAPB •ISDN プロトコル		•LAPB •SDNプロトコル	JUST-PC 手順
物理層						
通信網種別		•LAN •インハウス専用線	•パケット網 •ISDN •専用回線	•共通線 信号網	•インハウス専用線 •パケット網 •専用回線 •LAN	•電話網

NULL：プロコルトの実装不要

*：WSの処理能力に応じて一部のプロコルト

(1) 統合オペレーションシステムの構成と標準化

① 統合オペレーションシステム

従来のオペレーションシステムは、前述したように個々に開発されたため、通信サービスの複合化、サービス要求の高度化・多様化に応えるためには融通性が不足しており、発展性も乏しい。このため、NTTでは各種の通信網管理機能要素を整理し、これらの機能要素を組み合わせる通信網管理業務を実現する統合オペレーションシステムの開発を進めている。

② システム構成

統合オペレーションシステムは以下の要素より構成されており、各構成要素間のインタフェースについて現在標準化を進めている。

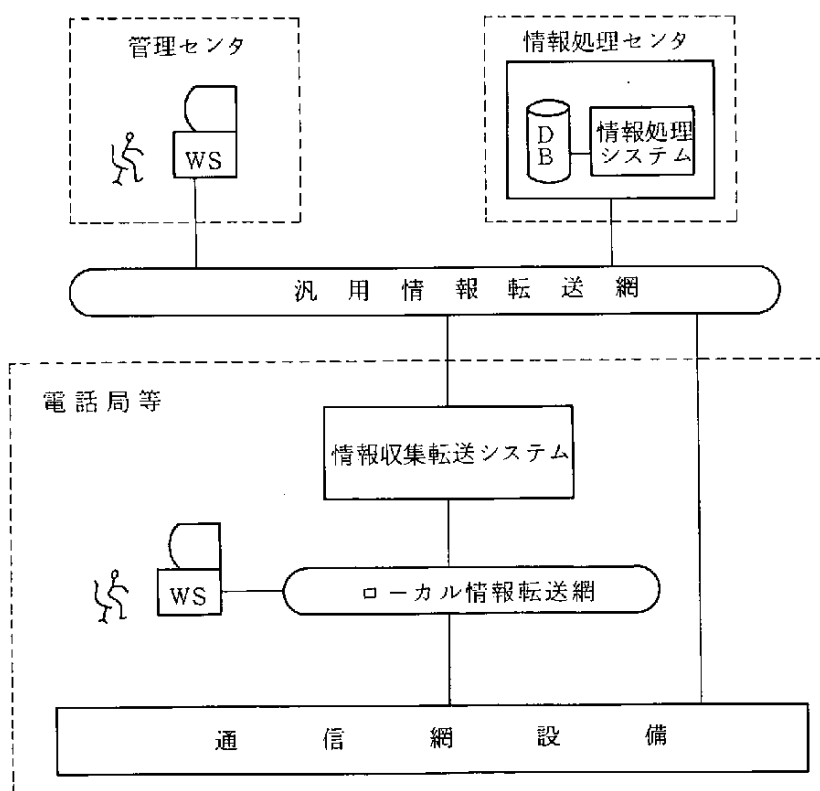


図 1.42 統合オペレーションシステムの基本的な構成

通信網設備

電気通信網の構成要素である交換機，伝送路，電力設備等の各種装置類であり通信網管理の対象となる。

オペレーションの処理系

通信網管理用の各種データベースを保有し，通信網管理用アプリケーションを実現する情報処理センタ，保守・運用者の作業場所であり，オペレーションシステムとの接点となるワークステーション（WS）が設置される管理センターから構成される。

情報転送網

情報転送網には，以下の２種類がある。

(a) ローカル情報転送網

通信網設備とはオペレーションシステム処理系を接続するための転送網であり，通信網設備の電気的特性，物理的特性に合わせて個々に構築される。

(b) 汎用情報転送網

主として情報処理センタ間を接続するための転送網であり，本転送網を利用する通信コードは，地理的・機能的な制約をうけずに相手コードとの通信が可能である。

情報収集転送システム

通信網設備と情報処理センタ間の情報の授受を効率的に行うための集線，プロコルト変換等の機能をもつ中継システムであり，本システムで監視・試験等のオペレーション処理を行うこともある。

③ 通信プロトコルの標準化

前記した情報転送網はTMNと呼ばれ、現在CCITTを中心に網アーキテクチャ、通信プロトコルの標準化が進められている。NTTでも上記TMNに準拠した情報転送網の標準化を進めており、今後開発されるオペレーションシステムに順次適用していく予定である。現在TMN用の標準プロトコルとしてNTTで規定している通信プロトコルの概要を表1.4に示す。

1.4.2 オペレーションシステムの事例

現在、NTTで開発済あるいは開発中のオペレーションシステムについて以下に紹介する。

(1) 伝走路網運用保守システム⁽³⁾

① システムの目的

伝送路網は、端局装置や中継伝送設備といった個々の構成要素に該当する「装置」と、各ハイアラキー対応の多重伝送バスや専用線等のサービスバスといった「回線」により構成されている。このため、故障の形態によっては、各所で発生している警報を1ヶ所に集めて網的に分析しなければ故障原因の分析、及び適切な回復措置を取ることが困難である。

本システムは上記問題に対処することにより、故障時間の短縮とユーザ対応のサービスの充実を目的として開発が進められている。

② システムの構成

本システムは、伝送装置本体からの警報を概ねビル単位に集約するDSV、保守エリア内のDSVからの警報を収集・処理するTOMS、及び各TOMSで処理した警報を全国的に処理するNOS等階層的に構成されている。更に、保守業務に必要な情報を出力するためのワークステーションであるWS

1 , 及びユーザ対応業務に必要な情報を出力するためのWS 2等の装置により構成されている。

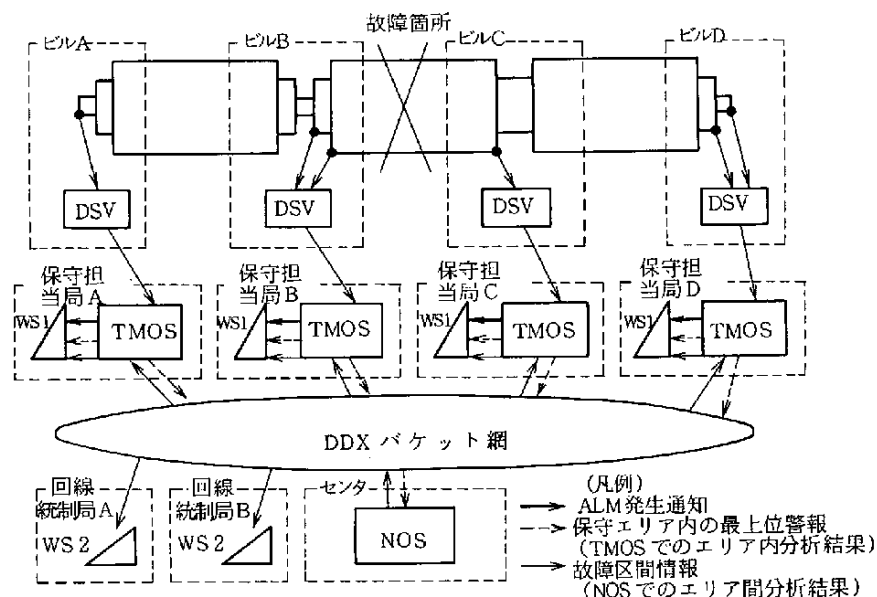


図 1.43 伝送路網運用保守システム

③ システムの概要

警報の収集

本システムは専用線の監視を目的としたものであり、従来からの1秒以上故障が継続した場合の警報に加え、瞬時に発生・回復する警報もすべて捕捉し、自動記録している。これにより、高速デジタル専用線のように短時間の瞬断がサービスに影響を与える回線の保守精度の向上を図っている。

回線警報の自動処理

伝送路が故障した場合、高次群の警報は下位次群に対し両面に波及し、多数の保守担当局の装置に波及警報を発生させるため、保守担当局のオペレータは故障区間の特定が困難であった。このため本システムで各保守担当局で自動判定された最上位警報をセンタに集めて故障区間を特定し、各特定担当局並びに回線統制局オペレータに通知する。この時、回線統制局オペレータには、警報と共に故障している統制回線名についても自動出力している。

(2) 交換機総合保守システム⁽⁴⁾

① システムの目的

従来、SPC交換機*の保守・運用は機種対応に行なわれていたため、同じ目的の作業でもその手順が異なっており、保守者は、多種多様な対応を要求されていた。本システムはアナログ／デジタルSPC交換機保守支援システムの統合・一元化、保守支援機能の強化、マンマシンインタフェースの統一・高度化を目的として、現在開発が進められている。

* S t o r e d P r o g r a m C o n t r o l (蓄積プログラム制御方式)

② システムの構成

本システムは異種複数の交換機を収容して、交換機より発生する警報を監視、転送及び交換機の制御情報の転送を行う交換局用装置 (STM, STTF)、交換機保守システムの統合、マンマシンインタフェースの統一・高度化を実現するための交換機保守支援サブシステム (EOS) 並びにWS等より構成されている。

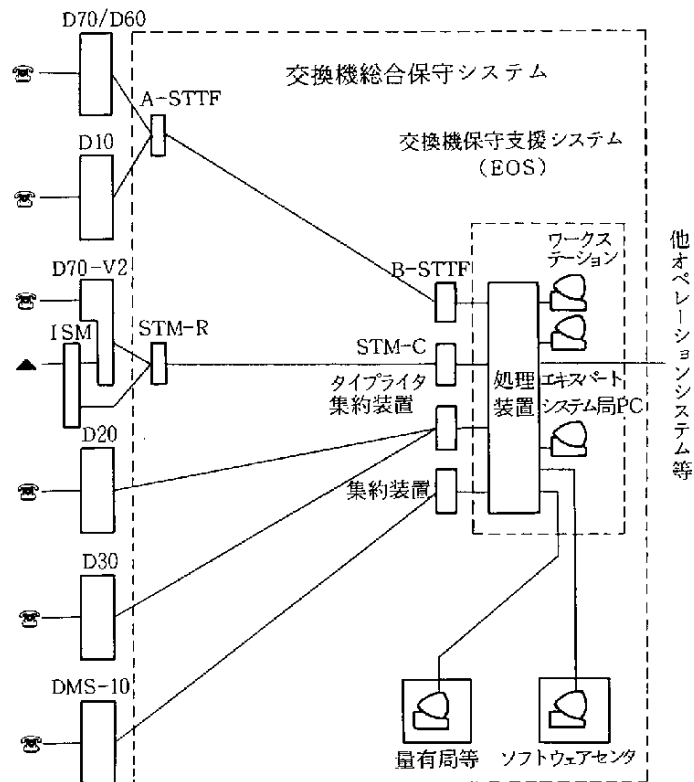


図 1.44 交換機総合保守システム

③システムの概要

交換機の監視・制御

従来、交換機で発生する警報やメッセージは交換機の警報表示盤、システム状態表示盤及び監視試験席等色々な個所に表示されていた。本システムでは上記情報をWSに一元的に表示することにより、保守エリア内に点在する交換機を1ヶ所から効率的に遠隔監視すると共に、故障装置の閉塞、自動試験、自動IPL等をWSから行うことができる。

保守業務の効率化・高度化

本システムでは交換機のシステム構成に関する局データの変更を遠隔地から行う機能、各地に点在する交換機より送られてくる警報、メッセージをジャーナルとして一元的に蓄積・検索する機能、ソフトウェアセンタ内のWSからパケット網を経由してパッチデータを受信し、遠隔地にある交換機に人手を介さずにパッチデータを投入する機能等保守業務の効率化・高度化を図っている。

(3) DDX網試験システム⁽⁵⁾

① システムの目的

従来、DDX回線の保守は手作業をベースに行っていたため、広域的な広がりをもつ回線故障時の切分け試験を1つの局で一元的に行うことが困難であった。また、アナログ回線では問題とならなかったノイズ、時々断等のデジタル特有の故障がDDX回線では問題となる。本システムは、これらの問題に対処するため開発されたものである。

② システム構成

本システムはDDXの交換局、集線局に設置され、各種試験を実行する遠隔試験装置類(RTS)、全国で1ヶ所に設置され、システム全体を管理・制御するセンタ装置(MAC)、並びに交換機、集線装置、加入者線及び中継線の各接続点に挿入され、本システムへ回線の引込みを行う回線アクセス装置(AF)等から構成されている。

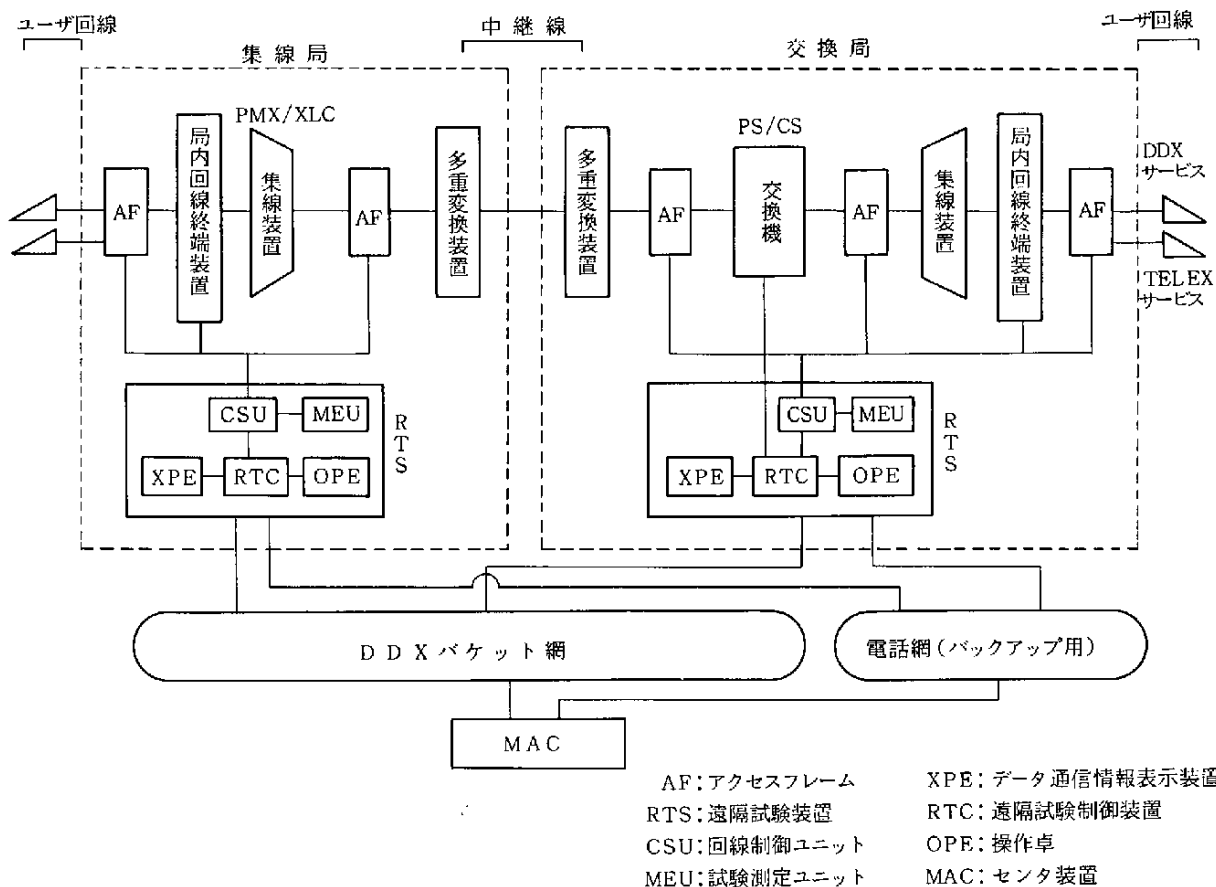


図 1.45 DDX網試験システム

③ システム概要

試験の遠隔実施

故障受付局から全国の回線試験を遠隔で実施可能である。これにより、全国にまたがったユーザシステムのどの端末、回線試験も即時に、かつ一元的に実施できる。

試験の自動化

加入者線の電気・物理特性の測定、デジタル伝送特性の測定等の試験を自動化することにより、従来の人手により単体測定器を使って行っていた方法に比べて試験時間の短縮が可能となるばかりでなく、特殊技術を用いずに

試験の実施が可能となった。

試験機能の高度化

時々断、プロコルト誤り等のデジタル特有の故障に対応するため、ユーザが実際に通信している状態でDDX網の複数ポイントにおいてモニタできる機能を実現し、区間切り分け等の解析を容易にしている。

情報の一元化

全国の回線に関するユーザ情報、故障履歴等をデータベース化し、随時に検索可能である。また、各種故障及び設備状況の統計処理を自動的に行うことにより、従来手作業で行っていた業務の省力化を図っている。

(4) 市外電話網トラヒック管理システム⁽⁶⁾

① システムの目的

本システムは、従来人手を介してサンプル調査により行っていたトラヒック測定業務を機械化し、全国の市外交換機のトラヒックデータを365日、24時間自動測定・収集し、ネットワークの呼の疎通状況、設備の使用状況やその変動状況を定量的に把握・管理し、網の設備設計、輻輳管理等に資することを目的としている。

② システム構成

本システムは市外交換機からトラヒック原始データを収集する観測装置（DET, OBS）それを統一インタフェースに変換するインタフェース装置（IE）、網管理のためのトラヒックデータを収集し、表示処理を行う集約処理系装置（CE, RPE, CPE）と、設備・サービス管理のためのトラヒック情報の一元的管理を行うトラヒック情報処理センタ（TIC）から

構成される。

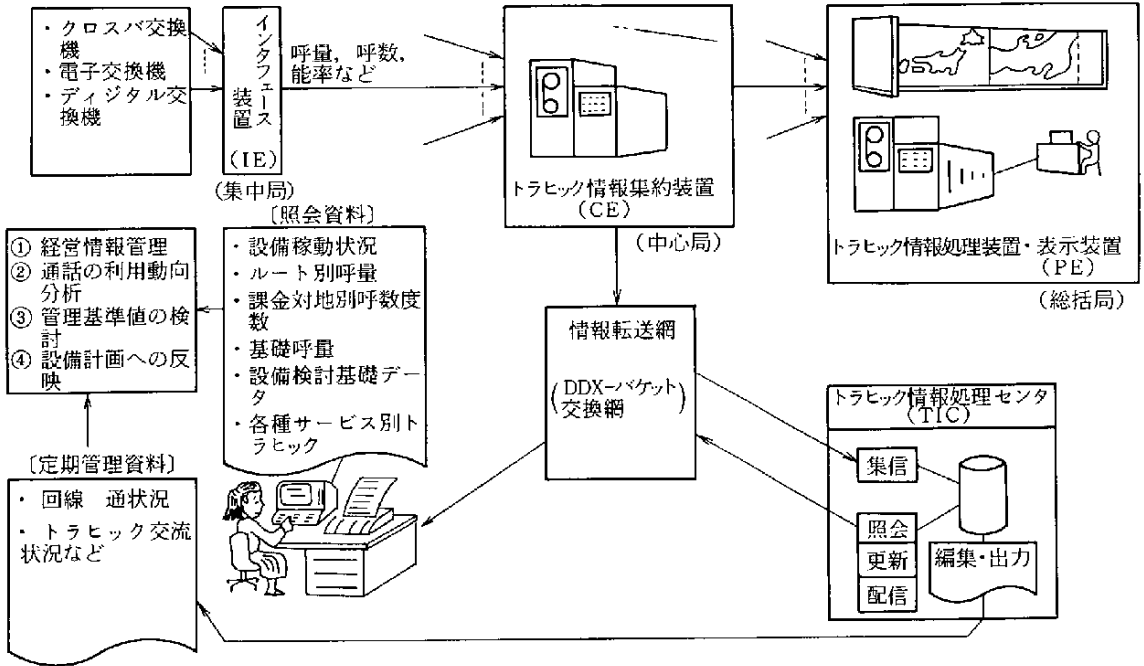


図 1.46 市外電話網トラヒック管理システム

③ システムの概要

トラヒック情報の表示

トラヒックデータとしては、共通機器使用可能率、ルート別呼量、各種呼数等を一定周期で収集する。収集されたトラヒックデータは、集的・表示系装置で網管理用情報として集中局エリア（DA）、総括局エリア（RA）、等の網の局階位単位でまとめてCRTディスプレイに表示している。

トラヒック情報の照会

トラヒックデータは、集約・表示装置で設備管理用情報として、最繁時トラヒックと一時間毎の毎時トラヒックにまとめられた後、トラヒック情報処理センタに転送され、一元的に管理される。これらのトラヒックデータはトラヒック管理実施局等に設備された端末から随時オンラインで参照できる。

(5) ガス圧遠隔監視システム⁽⁷⁾

① システムの目的

電気通信として不可欠な通信ケーブルは、大部分が地下に設置されており、浸水を防ぐために高い圧力の乾燥空気が封入されている。本システムは、ガス保守を行っているケーブルに浸水の危険があるか否かを常時監視し、ケーブル故障の予防保全を図ることを目的として開発された。

② システム構成

本システムはガス圧力、流量等の常時監視や各種警報判定を行うME、無人局エリアの監視を行うRMU、夜間監視用のALD、既存装置とのインタフェースをもつIFE、保守者との接点となるWS等の装置類とケーブル内のガス圧力を精度よく測定する圧力発振器、ケーブルを流れる流量値を測定するケーブル流量発振器等の各種発振器から構成される。

③ システムの概要

ガス圧力の監視

本システムでは、ケーブルの接続点に設置した圧力発振器からの情報に基づいてガス圧力分布図を作成し、CRT画面上で自動的に漏洩点の推定を行うことができる。また精度のよい推定を実現するために高精度な圧力発振器を使用すると共に、大気圧の変化によって送出圧力の変動の影響を受けない乾燥空気供給装置を使用している。

ガス流量の監視

ガス流量の監視は、圧力だけでは把握しにくい送端近傍の漏洩点の発見、漏洩規模の推定、何らかの原因で圧力監視が不能となった場合のバックアップ用として必要であり、従来行っていた目視点検を遠隔で行うことが可能で

あり、とくに無人局の保守に大きな効果がある。

N₂ ボンベ残存時間の推定

N₂ ボンベは、乾燥空気供給装置の予備として用いられており、トータル流量発振器で測定した総流量とN₂ ボンベの圧力により、その残存時間の推定が遠隔のWSから可能である。これにより、N₂ ボンベのポンプの取り替え時期を事前に把握できる他、正常時においても自然漏洩による圧力低下を遠隔で察知することが可能である。

通信網設備の運用・保守業務を中心にN T Tの通信網管理の概要を紹介した。今後は、個別に開発されたシステムの機能の拡充を図ると共に、個別システムを有機的に結合あるいは統合してより高度な柔軟性のある通信網管理システムを開発していく予定である。

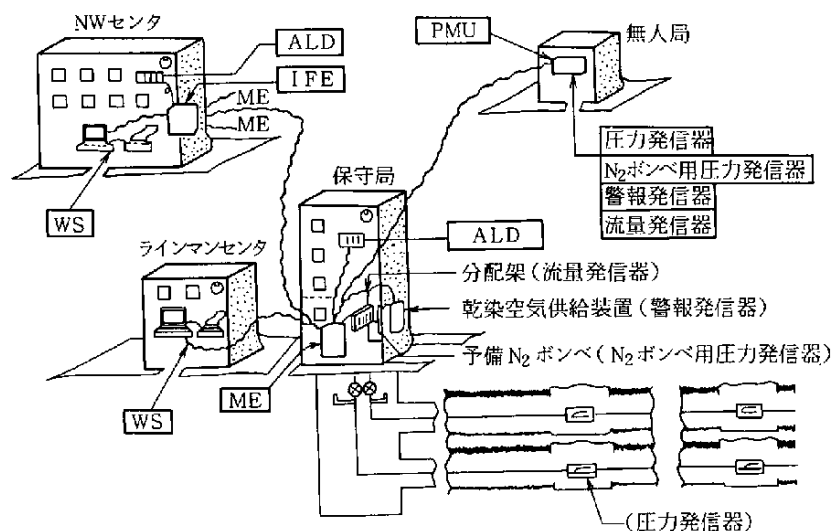


図 1.47 ガス圧遠隔監視システム

< 参考文献 >

- (1) 武内, 本間他: “通信網管理技術の動向”, 信学誌, 72, 1, P82 (1989)
- (2) 吉田: “情報ネットワークのオペレーションシステム”, 信学誌, 情報通信網の安全性, 信頼性時限研究専門委員会報告,
- (3) 今泉, 瓜本, : “伝送路網運用保守システム(COSMICS)の概要”, 施設 39, 9(1987)
- (4) 吉岡, 加瀬他, : “高度化される保守支援システム”, 施設, 40, 7, (1988)
- (5) N T T: “ D D X 網試験システム”, OSC REPORT, (1988)
- (6) 情報通信技術ハンドブック, PP84~86, オーム社(1987)
- (7) 高橋, 森林他, : “新ガス圧遠隔監視システムの導入開始”, 40, 1(1988)

第 2 章 ネットワーク管理のユーザ実態

第2章 ネットワーク管理のユーザの状態

2.1 ユーザのネットワーク管理事例

2.1.1 ネットワーク集中監視システム

(1) システム概要

本ネットワークにおけるネットワーク集中監視システムは、富士通製のマクロ監視システム（COMS）および以下に示す各装置のNSPにより構成されている。

- ・ DMIX-NSP（マルチメディア多重化装置）
- ・ FETEX-NSP（パケット交換機）
- ・ MDMS-NSP（モデム）
- ・ F2880-NSP（光データハイウェイ）

このシステムでは、マクロ監視装置を頂点として配下に各装置のNSPを設置し、ネットワークの監視・運用をセンター集中でおこなうことができる。各装置の接点情報は、各拠点のCOMS伝送装置にて収集し、高速デジタル回線を介してセンターに伝送される。なお回線障害時のバックアップとして公衆回線を使用し、常時監視できるようにしている。

監視範囲は、ホスト／端末系を除くネットワーク装置、通信回線をカバーしている。

各装置の接点情報（障害情報）は、マクロ監視システムにより、センターのグラフィックパネルに障害地区／装置として表示される。その表示により該当装置のNSPで詳細情報の収集を行う。また、各装置の診断機能を利用して、障害時の一次切り分けを行い、障害個所を特定することにより、障害の早期発見、早期復旧をめざしている。

システム概要仕様

局数 21 自営パケット網

回線数 高速デジタル回線 21, 専用回線 300, DDX-C 88。

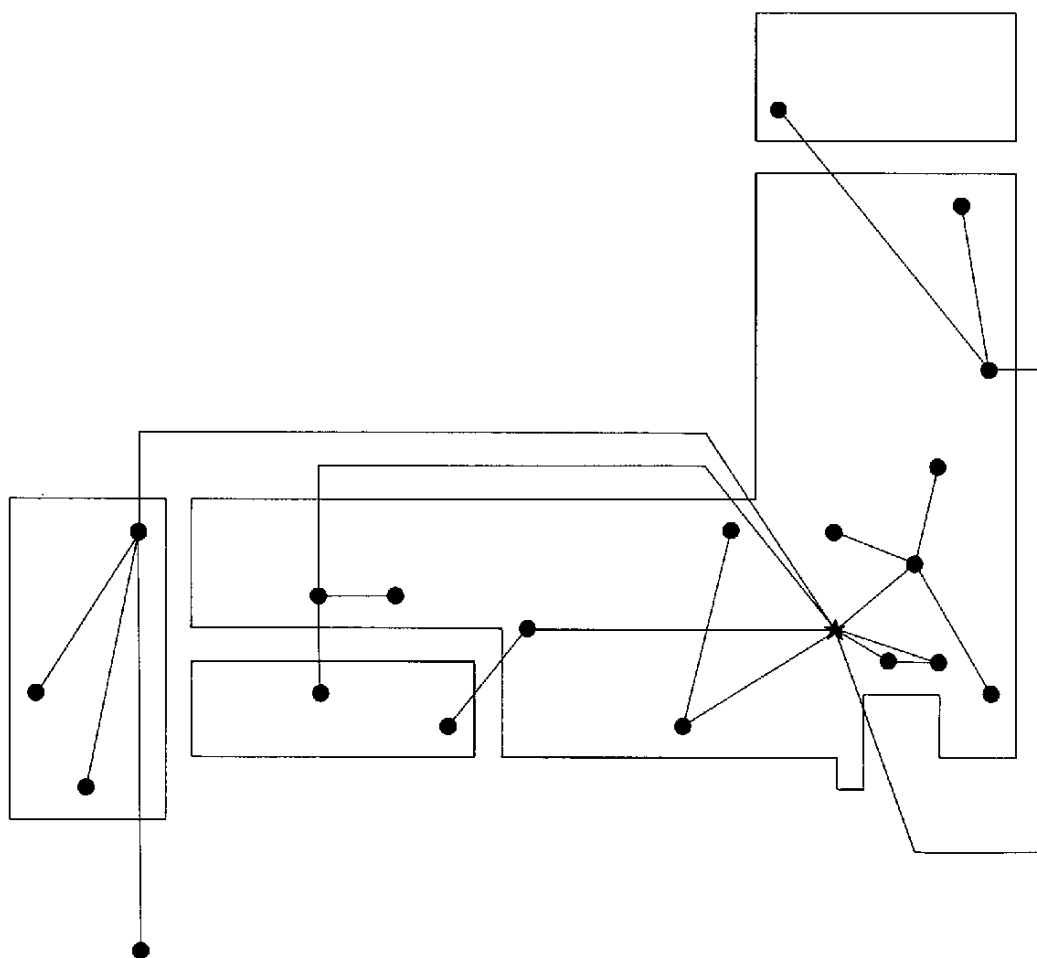


図 2.1 ネットワーク構成図

(2) 運用方法

運用は、センター運用と各地方支店に大別される。

・ センター運用

センターには専任のネットワーク管理者を設置し、本システムの管理・運用を行う。主な作業としては以下のとおりである。

- ・ ネットワークの監視，運用
- ・ 障害時の切り分け，連絡
- ・ ネットワーク作業の調整，連絡

- ・ 統計情報の収集，管理，分析
- ・ ネットワークの管理

各地方には，専任のネットワーク管理者を配置せず，ネットワーク運用に関してはセンターからのリモート運用を図った。ただし，機器の管理およびセンターなどの対応窓口は設けている。

ネットワーク監視のフローを図2.2に示し，以下にフローの概略を記す。

- ① マクロ監視システムのアラーム表示器のブザーおよびグラフィックパネルのランプ点燈によりネットワーク監視者に障害発生を知らせる。
- ② グラフィックパネルのランプにより，障害地区，装置を確認する。
- ③ 高速ディジタル回線ランプ点燈の場合，N T Tへ連絡。
- ④ ②で限定された装置に対して，各N S Pを用い障害情報を収集する。ただしモデムの場合は回線モニター機能により回線の状態を確認し，回線障害の場合はN T Tへ連絡する。
- ⑤ 各装置の診断機能を活用して，データの折り返しを設定し，障害の一次切り分けを行う。
- ⑥ 障害情報および一次切り分けの情報の結果をメーカーに連絡し，復旧を待つ。
- ⑦ メーカーより復旧完了の連絡後に各地に稼働可能を連絡する。

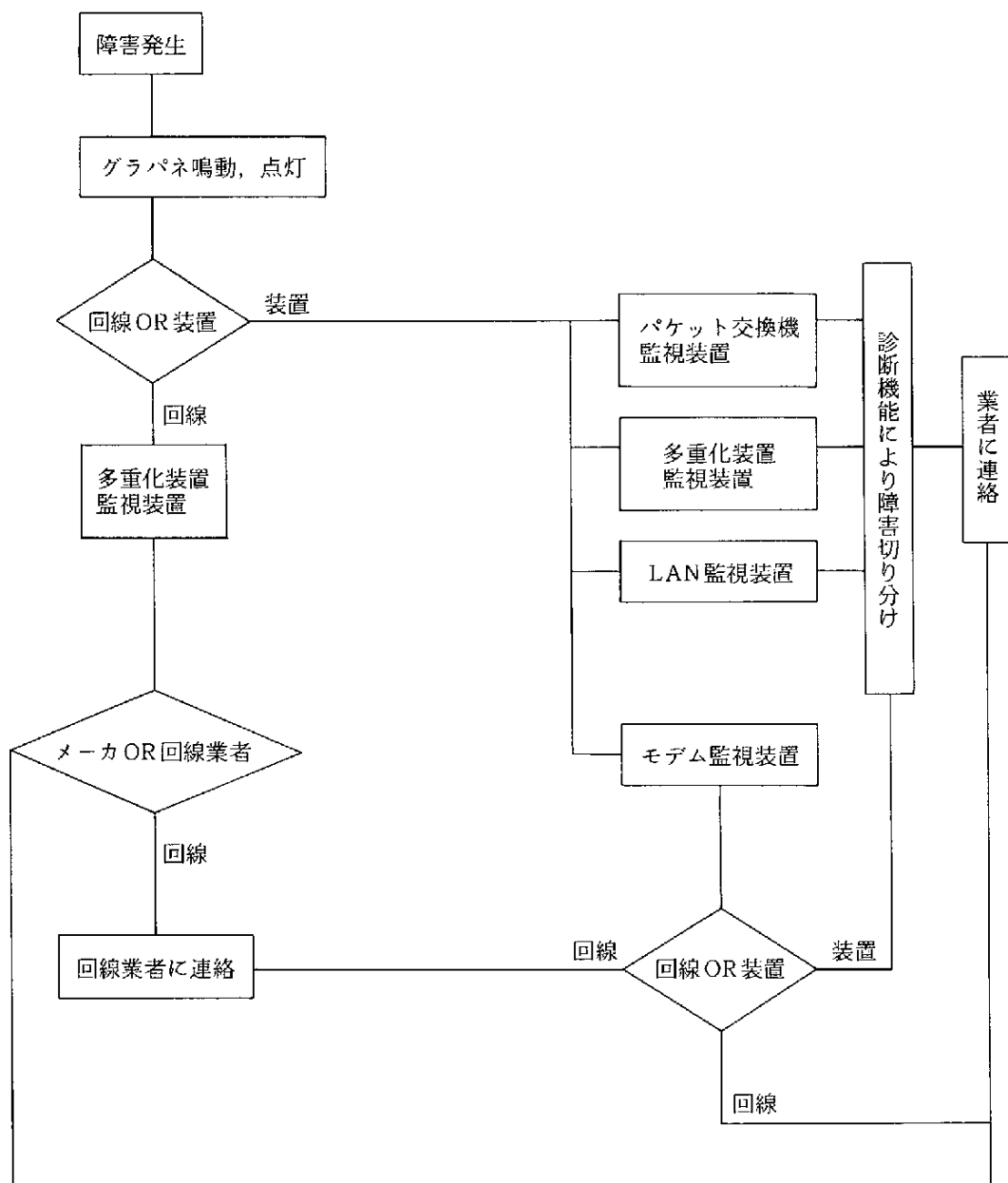


図 2.2 障害切り分けフロー

2.1.2 AIによるネットワーク管理

(1) SPARKプロジェクトの狙い

住友金属工業(株)では、ネットワーク管理の高度化を推進するため、日本アイ・ビー・エムと共同でSPARKプロジェクトを発足させ、その成果として「システムネットワーク運用自動化支援ツール」（略称：SANOASサノアス）を製品発表している。

このSPARKプロジェクトの発足にあたっては図2.3のような背景をもとに、AIの積極的活用を図った。

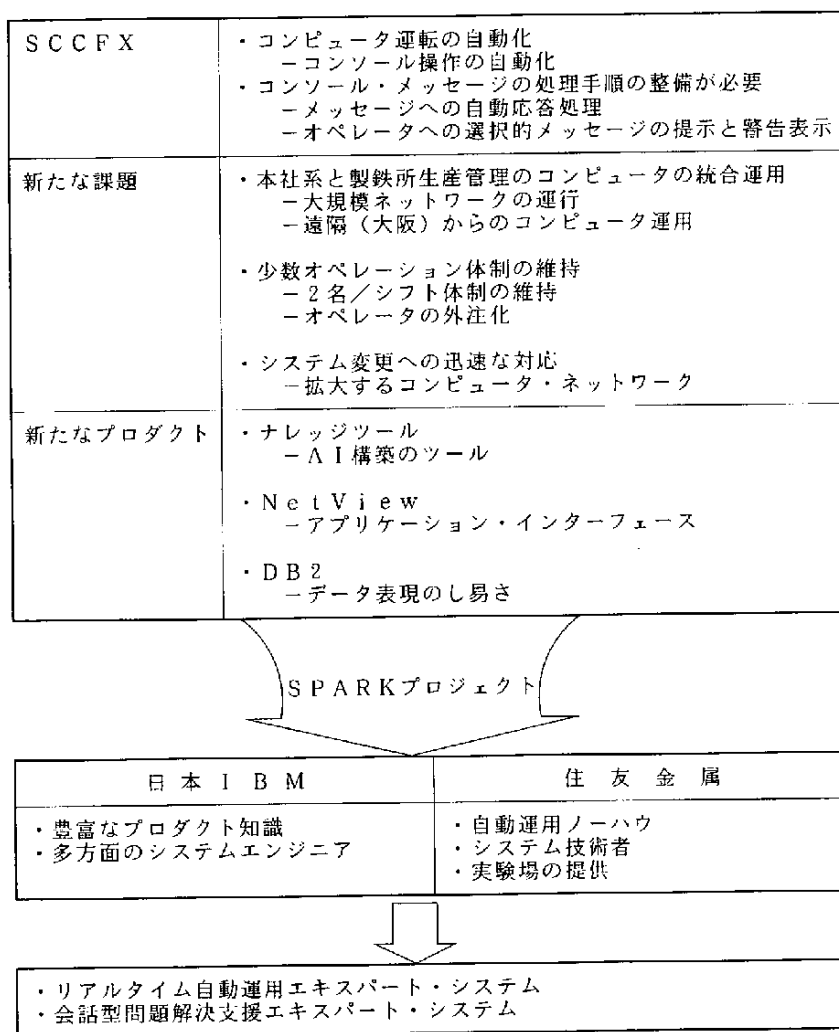


図2.3 SPARKプロジェクトの背景

(2) システム概要

① 特徴

SANOASは次のような特徴が挙げられる。

- ・ コンソール・オペレーションの自動化ツール
- ・ AIテクノロジーの採用
 - － 熟練オペレーターの知識を容易にシステム化可能
 - － 開発・保守・管理が容易
- ・ リアルタイムに動作する本格的なAIアプリケーション
- ・ 24時間 365日稼働のシステム・ネットワークに対応が可能
- ・ DB 2 上に運用ルールを構築することにより開発・保守・管理が容易
- ・ リージョンごとに機能を分割するマルチ・リージョンの設計により柔軟な機能拡張が可能

② 自動化の対象

コンピュータの運用の自動化対象は主に以下の5項目に分類される。この中で最も効率化に影響を及ぼすのはコンソール・オペレーションである。

SANOASはこの最も困難で、しかも最も効果の高い次のようなコンソール・オペレーションの自動化を促進するためのツールである。

- ・ コンソール・オペレーション
- ・ テープ及びプリンター操作
- ・ バッチ・ジョブ運行管理端末操作
- ・ ハードウェア操作（3090のスイッチ操作等）
- ・ 設備の操作（空調の操作等）

③ SANOASの機能

SANOASはNet ViewのアプリケーションでNet Viewが持つ自動化タスク機能を強化し、複雑な運用システムを構築するための運用支援ツールである。

基本的な機能として運用環境の立上げ、停止及び障害の管理／発見／原因の切分け／回復処理を持つ。さらにSANOASが使用するデータベースを管理・保守するためのユーティリティが用意されている。

注意) SANOASが持つネットワーク障害の管理対象はPUのみ。

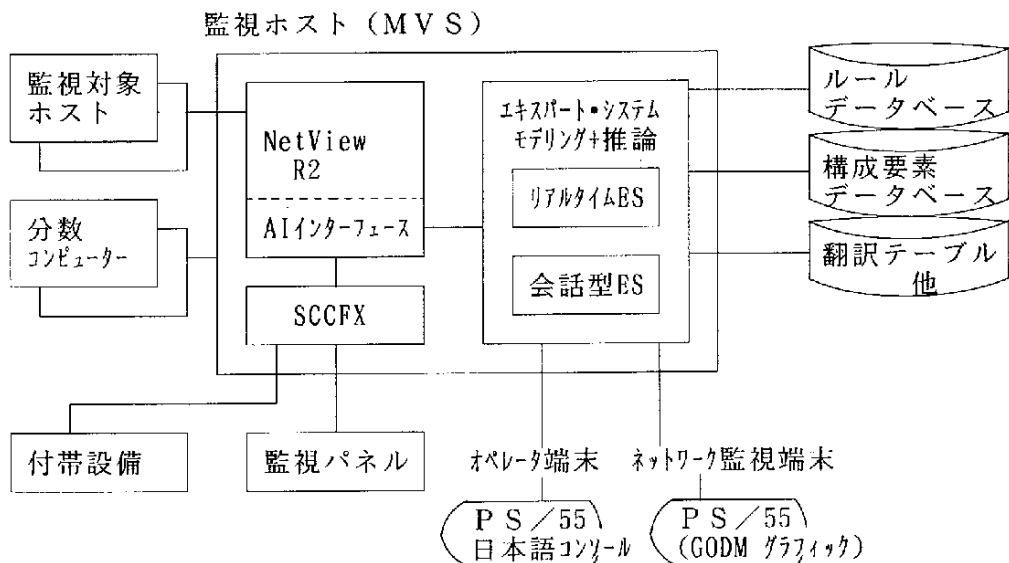


図 2.4 AIによるコンピュータ自動運用管理システム

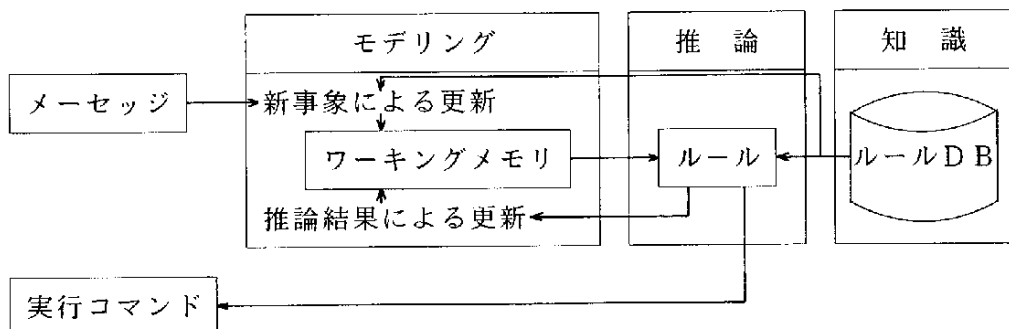


図 2.5 システムの動き

④ SANOAS システム構成図

SANOAS は次のように 1 つのモジュールが 1 つのアドレス・スペースを占有しメッセージ交換プログラムを介して連携をとる構成になっている。

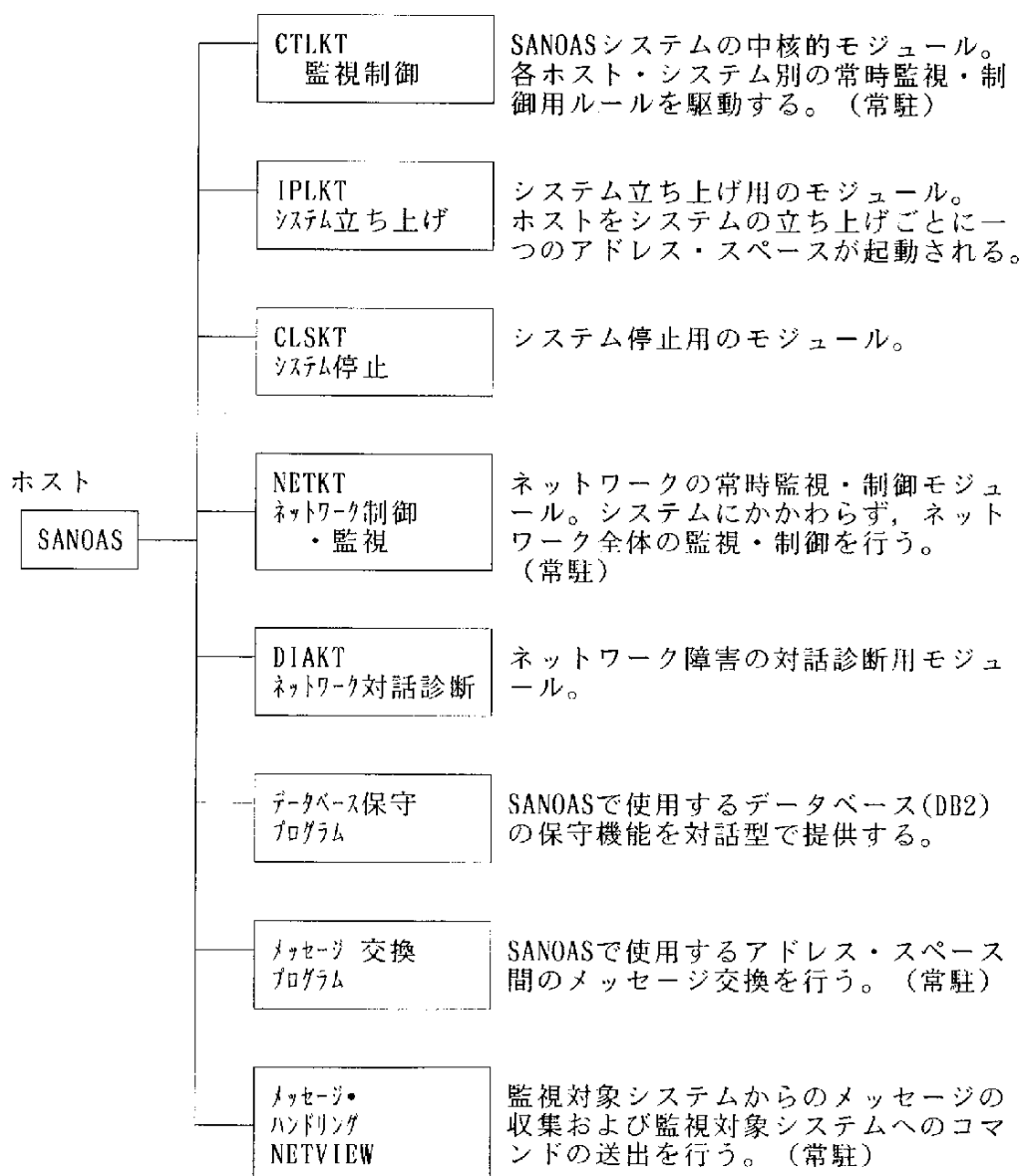


図 2.6 SANOAS システム

⑤ テクノロジー

SANOAS最大の特長はAI技術の採用により制御のレベルを高度にし、開発・保守の期間を従来の手法による場合に比べ大幅に短縮していることである。AIの機能を実現するために自動運用エキスパート・システムのベースとして育まれてきた「IBMナレッジツール」を採用している。

また開発・保守の効率を高めるために運用のルールをデータベース化し、マルチ・リージョンにまたがるモジュール構成を採用して機能追加を容易にするなど設計においてもIBMが持つ技術を最大限に活用している。

⑥ SANOASの効果

SANOASの使用によって得られる効果には以下のものが挙げられる。

- オペレータの生産性向上による運用コストの削減
- 人的ミスによる障害の防止
- メッセージ着過による障害の防止
- オペレーションの標準化
- 障害防止コンソール・オペレーションの短縮による信頼性、可
用度の向上
- 遠隔地コンピュータのオペレーション

⑦ 自動運行システムのカバー領域

SANOASはシステム環境の設定及び停止、障害の管理（発見／切分け／回復／通知）といったコンソール・オペレーションの自動化を対象としており他の運用自動化製品を補完する製品。

Net Viewには自動化タスクの機能があるが、複雑な制御、大規模なシステムの制御あるいは変更・保守の柔軟かつ迅速な対応が必要な場合にはSANOASは効果を発揮する。

(3) 構築目標と現状

本ネットワーク集中監視システムの導入にあたっては、以下のとおりの主な目的を達成するために構築された。

- ① 通信運用コスト削減
- ② 障害対応サービスの向上
- ③ ネットワークシステムの必要性

以上が導入の大きな要因である。

①の通信の運用コストの削減については、通信業務に携わる要員の削減を図ることが大きな効果を得る。と考え、集中で監視し障害対応ができることを徹底した。

②の障害対応サービスの向上については、大規模ネットワークシステムにおいては一部の障害であっても全体の稼働に影響を及ぼすことがあり、このことをすみやかに判定し、正確な状況をインフォメーションすること。また、監視システムを導入することによって障害の切り分け時間の短縮を図り、復旧作業のアクションを即時に起こせるようにした。

③については、大規模で複雑なネットワークシステムにおいて障害管理、構成管理を分散でおこなうことが不可能になった。これは全体にたいする影響を判断するためには、全体を管理する必要があるからである。

現状において構築当時の目的は達成されたと考えるが、次のような課題がある。

- ① 監視システムを運用する要員の教育
- ② 集中監視を維持しつつ、システムの拡張、変更を行うこと
- ③ 構成管理が質、量ともに多くなり管理システムの導入を必要とすること
- ④ 通信機器、電算機、回線などのハードおよびソフトにわたる複合障害対応
- ⑤ マルチメディア化にともなう運用体制のあり方

2.1.3 マルチメディア環境におけるネットワーク管理

(1) ネットワーク概要

回線網

本ネットワークのイメージを図 2.7 に示す。

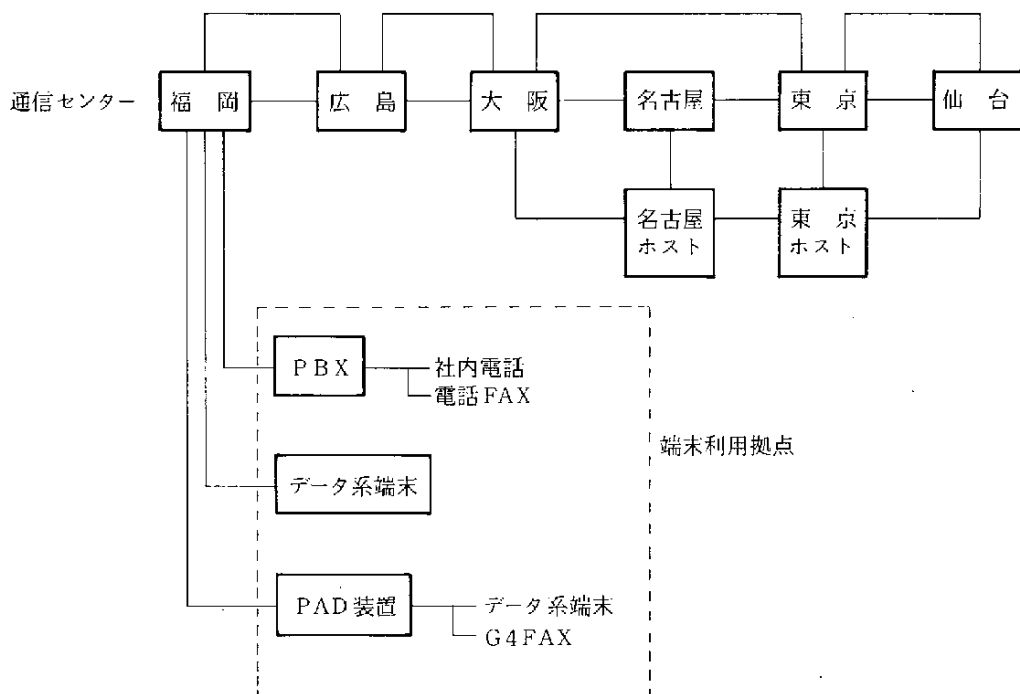


図 2.7 ネットワークイメージ図

図で示すように、全国の6地点に通信センターを設けており、各センター間は192K～6Mの高速デジタル回線で接続されている。事故対策として重要な業務については必ず2系統の情報経路を設けている。実際に端末を利用する拠点は、全国に100ヶ所あまり存在し、各拠点はそれぞれ最も近い通信センターと64K以上の回線で接続されている。

各通信センターには、マルチメディア多重化装置と共にパケット交換機を設置し、自営パケット網を構築している。自営パケット網のバックアップ回線としてはDDX-C回線を利用している。

ホストコンピュータセンターは東京・名古屋に存在し、コンピュータセンター間、及び通信センターと大容量の高速デジタル回線で接続されている。

伝送データ

本ネットワークでは以下の3種類のデータを扱っている。

- ① コンピュータデータ
- ② 音声データ ⇒ 全社の内線電話化
- ③ FAXデータ ⇒ 全社のG4FAX網

これらのデータの内、①の一部と③のデータについてはパケット化して伝送している。

マルチベンダー化の現状

本ネットワークは以下に示すように、多くのベンダーの機器によって構成されている。

- ・ ホストコンピュータ …………… IBM／富士通
- ・ マルチメディア多重化装置 …………… 富士通
- ・ パケット交換機 …………… 日本電気
- ・ データ系端末 …………… 富士通／IBM等
- ・ G4FAX …………… 松下電送
- ・ 回線 …………… NTT／第二電電／日本テレコム
／日本高速通信等
- ・ モデム …………… 富士通／日本電気等

また端末側で使用している通信手順も様々であり、パケット化を行うために、PAD装置を利用して吸収している。

- ・ SDLC ・ HDLC (ARM) ・ X25
- ・ BSC ・ HDLC (NRM)

(2) ネットワーク管理概要

東京のコンピュータセンター内には「ネットワークセンター」を設置し、日常のネットワーク運用を行なうと共に、ユーザからの障害連絡等の受付窓口としている。各種の情報はネットワークセンターに集中させ、一元的な運用を実現している。

以下に当センターの役割について簡単に記述する。

障害監視

現在ネットワークの障害監視は以下のようなネットワーク機器毎の監視システムを導入し、実施している。

- ① ホストコンピュータのネットワーク監視コンソール（例，Netview）
- ② マルチメディア多重化装置の監視コンソール
- ③ パケット交換機の監視コンソール

障害対応

障害発生時はネットワークセンターが中心となって、以下の作業を実施する。

- ① 障害原因の一時切り分け
- ② 適切な業者（メーカー／回線業者）のコール
- ③ ユーザ部門への連絡
- ④ 運用上の応急対策 ⇒ ・予備回線への切り替え指示
・通信制御装置の予備機への切り替え等

障害切り分けのためには前述の監視コンソールを利用（例、パケット交換機監視コンソールによるトレース情報の取得）する他、以下のような情報を収集して利用している。

- ① モデム／D S Uのランプ状態
- ② P A D装置のランプ状態
- ③ 端末の状態

これらの内、運用側では把握できない情報（例、ユーザ側モデム／端末のランプ状態等）に関してはネットワークセンターがユーザに依頼し、情報収集を行っている。

また個別端末レベルで再現性のある障害に関しては、必要に応じてプロトコルアナライザを利用して詳細な情報を取得し、分析している。

ネットワーク構成の変更

端末の増設・端末利用拠点の移設等の、ネットワーク構成の変更に係わる情報は、全てネットワークセンターに集中し、業者・ユーザと調整する。ホストコンピュータ側のパラメータ変更はコンピュータ運用管理者が行うが、その他のネットワーク機器のパラメータ変更等についてはネットワークセンターが管理し、業者に作業依頼をしている。

また特に社外ユーザの端末新設に関しては、現地でモデム設定等を確認し、初期の接続確認を実施している。

ネットワーク構成・障害履歴の管理

ネットワークセンターにはUNIXベースのワークステーションを設置し、DBソフトを用いてネットワーク構成の管理に利用している。現在の所、以下のような情報をDB化し管理している。

- ① 各ネットワーク機器のリソース台帳
- ② 各端末の機種・ユーザ・連絡先
- ③ 回線原簿（回線番号・品目・起点・終点・開通日等）
- ④ 各ネットワーク機器の接続情報

また障害履歴に関してもデータを登録しており下記の統計資料の作成、及び類似障害の検索等に利用している。

統計資料の収集・作成・分析

下記の統計資料について、定例的に実施している。

- ① 障害発生状況
- ② パケットトラフィック量

(3) ネットワーク管理に関する期待、及び今後の課題

以上当社におけるネットワーク管理について簡単に記述したが、現在は運用開始からほぼ 2.5 年を経過したこともあり、ほぼ順調に運用している。今後のネットワーク拡大への対応・より効率的な運用のためには、以下のよう
な点について考慮していきたい。

① 各種監視装置の統合

⇒ ① 機器毎のコンソールを統合し、1つのコンソールで各種
ネットワーク機器の監視・操作

② 大型パネル等を用いた一元的な監視

② 監視レベルの向上

例) パフォーマンス監視 ⇒ ① 障害の未然防止

② 性能データを蓄積し機器増設
の判断基準

③ 運用管理システムのマンマシンインタフェースの向上

⇒ 現在でもパケットトレースの解析・トラフィック量計算等の
ために、パソコンを利用して部分的に実施している。

④ ネットワーク運用管理要員の教育・育成

この内、特に①についてはマルチベンダー環境下で運用を行っている当社
としては、現在検討が進んでいる OSI のネットワーク管理に期待する所が
大である。

2.2 ユーザの課題とニーズ

2.2.1 ネットワーク管理に関する各種の環境面からの要請

各企業におけるオンライン業務の拡大・通信技術の進展・法的規制の緩和等が絡み合い、ここ数年でネットワークは大きな変貌を遂げた。以下に具体的な事項と、その変化がネットワーク運用に及ぼす影響・問題点について、簡単に記述する。

(1) ネットワーク規模の拡大

各種のオンライン処理が一般化すると共に、ネットワークに接続される端末数は飛躍的に増大しており、その利用者もコンピュータとかネットワークを意識しない一般のエンドユーザが、大多数を占めるようになっている。

また業務の拡大・国際化に伴い、異企業間のネットワーク接続・国際ネットワーク接続といった形態も極めて多くなっている。

- ⇒ ① ネットワーク機器に対する監視・リモート操作の必要性
② ネットワークの変更（端末の増設・移設等）頻度の増大
③ 障害発生頻度の増大
④ ネットワーク運用要員の増大
⑤ 機密管理の必要性

(2) ネットワーク形態の多様化

分散処理の発展に伴いネットワークの形態も、従来のホストコンピュータを中心とした「スター型」の結合（垂直型通信）から、WSやインテリジェント端末による水平型通信・LANの結合など、より複雑な形態が一般化してきた。

またデータの内容も高速デジタル回線が普及するにつれて、従来のコンピュータデータに加え音声・画像等のデータが統合されるようになり、PBX・FAX端末・電話器等も同一のネットワークに結合されるようになった。

- ⇒ ① 管理対象範囲の拡大
- ② 要員教育の困難さ
- ③ ネットワーク管理組織の必要性

(3) ネットワーク資源の戦略的活用

「情報」は「人・物・金」と同様に企業にとって基本的な資源と捉えられる。その処理・伝達機能を果たすネットワークは企業の「インフラストラクチャー」と考えられ、その利用方法は直接企業戦略に結びつくと言われるほど、ネットワークの重要性は極めて高いものとなっている。

またネットワークに関する投資額も大変大きくなり、その利用方法・経済的効果については企業経営上の重大な関心事となっている。

- ⇒ ① ネットワーク障害の与える影響の大きさ
- ② ネットワーク計画（使用状況・投資効果の把握）の重要性

(4) マルチベンダー環境の進展

ネットワークに接続される資源の増大・多様化に伴い、それらの機器をシングルベンダーで統一することは、事実上不可能なこととなっている。また回線キャリアも複雑存在し、それらのネットワーク内における混在も通常のこととなっている。

- ⇒ ① 運用業務の複雑化
- ② 障害切り分けの困難さ

以上のような背景から「ネットワーク管理」に対するユーザ側の関心は、近年極めて高いものとなっている。

2.2.2 マルチベンダー環境下におけるネットワーク管理の問題

(1) 異機種ネットワークアーキテクチャ間の問題

① 要員増大／作業負担の増大

マルチベンダー環境下では、複数の管理システム・ツールを共有するこ

とは出来ず、個々にユーザ自信が管理ツールを独自に開発する必要があり、作業負担を少なくし、また教育・訓練に多くの時間を必要とする。

② 互換性

各ベンダーのネットワークアーキテクチャ (SNA, FNA, MMA, BNA etc) 間には互換性はなく直接ネットワークどうしを各メーカーの保証のもとで接続することは出来ない。

また各ベンダーのネットワーク管理ツールにも互換性がなく全体的な管理が出来ない。

③ 運用業務の複雑化

マルチベンダ環境下では各ベンダーのネットワーク管理ツールにも互換性がなくネットワーク管理の方法が異なる為、そのネットワークを管理運用するためのコンソールを別々に設置し、管理しなければならず複雑になっている。

④ ソフトウェアの更改

異機種間結合をなんらかの方法で行った場合、双方のソフトウェアの更改を行う時は、その整合性に関してお互いに責任の対象外となり、ユーザが充分なる検証をする必要がある。

⑤ 障害時切り分け

双方のネットワーク上にエラーが生じた場合、障害切り分けのための責任分解点等、責任分担がはっきりしていないケースがあり障害解決上、問題となりうる。

(2) マルチ構成間の問題

① 通信回線キャリア上のネットワーク管理

H O S Tから端末までのネットワークを考えた場合、H O S T機器、通信制御装置、多重装置、モデム、回線、端末とネットワーク構成要素がマルチベンダーとなっていた場合障害切り分けの責任分解点が複雑化し障害解決に時間がかかる。

(3) LANにおける問題

LANの場合、資源の有効活用や異機種接続の要請からマルチベンダ環境が通常となってきたが、ネットワーク管理の観点からは、以下の問題がある。

① LAN間接続時の問題

(検証作業の煩雑さ)

一つのLANに複数のプロトコルがのっている場合、接続時の動作検証はプロトコル毎に行なわれているのが現状である。

(検証機能の差)

端末機器が持っている接続検証機能はメーカーにより差があり、すべてのプロトコルについて同レベルの検証を行うことが難しい。また、機器によりユーザ・インタフェースが異なる。

(ルータ)

リモートで異機種接続を行う場合、マルチプロトコルルータの利用が望まれるが、プロトコル毎のバージョンアップ時の対応が懸念される。

(接続性の問題)

LAN同士をローカルな要請に基づき特定のプロトコルのルータで接続しながら成長してきた広域LANの場合、トランスポート層以下の接続は全体的になされているが、ネットワーク層以上ではローカルにしか接続されていない場合がある。

このような場合、LAN間の接続性についてエンドユーザに周知する必要がある。

② 端末機器接続時の問題

(構成管理)

端末の増設や切り放し等の構成変更を行う際のユーザ（ネットワーク管理者）側の必要作業がプロトコル毎に異なり、構成変更時の作業が標準化しにくい。

2.2.3 ネットワーク管理システム、製品機能上の問題

(1) 低いマン・マシン・インターフェイス

機器毎の管理システムにおいては、例えば障害対応業務等における作業フローと画面遷移や操作手順が一致しないために一連の作業が複雑化してしまう。これは統合管理システムでも同様にシステム間の運用業務にそれらが一致していないものが多い。またコマンドなどの登録作業手順等の運用においてもマンマシンインターフェイスが低いものがある。

(2) 機能不足や能力不足

監視やリモートコントロール機能がない機器がある。このことは多種多様化しているネットワークシステムなかに機能の混在を生み管理をより複雑化する。またネットワークの構成変更作業を無停止で実施できないことやシステムの拡張をするとレスポンスが悪くなるなどの管理機能の能力や不足や機能のシステムに対する柔軟性が乏しい。

(3) 管理システム、ツールに互換性がない

各管理システム、ツールにインターフェイスが無いために個別管理しかできず、統合管理ができないことや管理範囲に漏れが生じる。

(4) 管理システム導入による作業の増加

課金情報等の収集方法が機種ごとに異なっているなど、システム導入により全体の作業量を増加させるケースがある。また管理ツールを独自に開発せざるを得ない状況もあるので作業がかえって増加する場合がある。

(5) 管理システムは高価格で導入できない

管理機器やツール自体が高価であり、また管理システムや管理ツールのユーザ要求に対する開発が高額であり導入しにくい。特に機密管理の関係は高い。

(6) 統一基準にもとづく機器が提供されていない

回線障害などの障害認定において各キャリアとの間に機器の測定結果に認識のずれが生じる場合が多くあり障害対応時間の短縮を阻害している要因の

一つとなっている。このことに関しては障害診断関係の基準に統一規格を作成し認識の統一を図ることが必要である。

2.2.4 運用面の問題点

(1) 運用工数の増大

益々拡大し、複雑化するネットワークに対応するためには、オペレーションの強化が重要である。しかし、専門知識が必要で人員の養成には時間がかかってしまうネットワークオペレーションの強化は非常に難しい問題である。そこで、AI等を利用したオペレーションの機械化による省力化の推進が必要になってきている。障害の検出と障害箇所の診断、およびバックアップリカバリは、最も要求される自動オペレーションの一つであり、また、障害箇所の判定のためには、ネットワークの構成情報を把握しておくことも大切で、ネットワーク構成情報管理システムの構築が必要となる。

ネットワークの拡大複雑化で問題なのは、オペレーション工数の増大だけではなく、端末追加、移動、削除などのネットワーク構成変更時の工数増大である。このためには、構成変更の簡略化、接続テストの簡略化、オンライン稼働時の構成変更が必要となる。また、ここでもネットワークの構成情報を把握しておくことは大切であり、ネットワーク構成情報管理システムの構築が必要となる。

(2) ノンストップ オペレーションへの対応

最近、企業間のオンライン取引が進み、取引が何時でもできるようにノンストップ・オペレーションが必要になってきている。また、国際化の進んだネットワークでは時差の関係で、ノンストップ・オペレーションが必須となる。このため、オンライン稼働中のネットワーク構成変更が必要であり、また、その変更情報は、ユーザに即時に周知徹底される必要がある。

(3) 課金情報の取得

通信費用削減も重要項目の一つである。高速デジタルサービスの開始や多

重化装置等の通信技術の発展と法的規制緩和は、自営ネットワークの企業内の共同利用を可能し、大いに通信費用削減に貢献してきている。しかし、共同利用がゆえに、費用の平等負担のためデータ伝送ボリューム等の課金情報の把握が必要となる。

(4) ネットワーク管理システムの運用

ネットワーク管理システムとて、他のシステムと同様に省資源、省エネルギーである必要がある。また、ネットワークの管理情報は膨大な量となり、ペーパーレスは勿論、光ディスク等の大容量の記憶媒体を使用したシステムが必要となる。

2.2.5 情報管理における問題

1. 管理情報の項目の増加

システムの拡大や複雑化にともない管理する項目が増加し、障害対応など各々の運用業務に欠かせない状況になってきているのに、必要項目の整理等がなされていない。

また、項目数の増加が運用要員のスキルと同期がとれない。

2. 言葉の標準化

構成要素が増加しているネットワークにおいて、各社が各々の言葉で同一現象を表現しているケースが多く、ユーザの要員教育が妨げている。

3. 管理情報の動的取得

管理情報のメンテナンスに大変な手間が掛かり、運用業務に負荷をかけているので、もっと動的に（E. X. ジェネレーションと同時に登録されるシステム）管理情報の変更を行える様にしてほしい。

4. LANのディレクトリ差とセキュリティ

LAN上の端末の増移設を行なった際、ネットワーク上の位置に関わらず、同一のサービスが受けられることが望まれるが、そのためにはディレクトリサービスツールが必要になる。さらに、アクセスが容易になることからセキ

セキュリティが問題になり、機密管理ツールも同時に必要になる。LANが複数の上位プロトコルで構成されている場合には、管理作業の簡素化・標準化のため、全プロトコルをサポートする管理ツールが望まれる。

第 3 章 O S I 管理の範囲と考え方

第3章 O S I 管理の範囲と考え方

3.1 O S I 管理の範囲

「O S I 管理」で規定される範囲と、規定範囲外でネットワーク管理システムを提供するメーカーが独自に決めるべきものとを説明します。理解し易くするために簡単なネットワークシステムモデルを例に採って説明します。

3.1.1 ネットワークシステムモデル

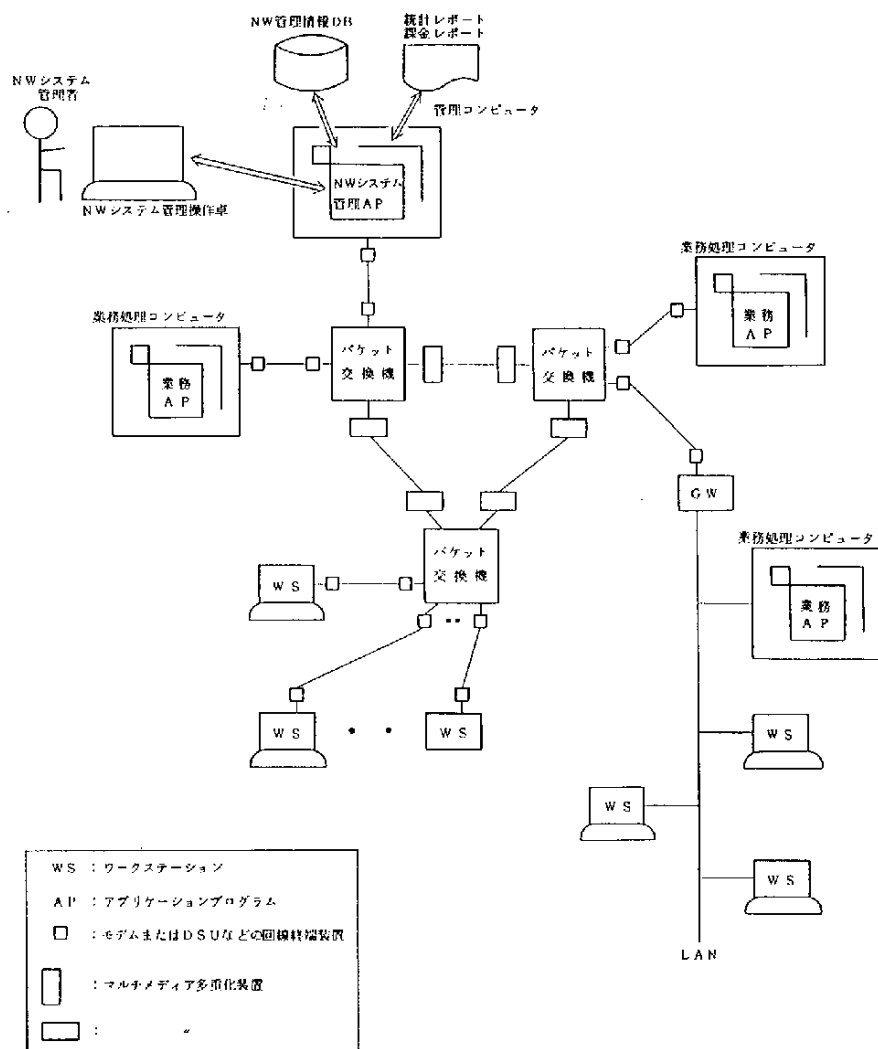


図 3.1 ネットワークシステムモデル

3.1.1 ネットワークシステムの一般的な管理

ネットワークシステム管理者は、管理コンピュータ内のネットワークシステム管理A P（群）に対して以下のような管理操作を行い、ネットワークシステム全体を一元管理します。

(1) システムの監視

ネットワークシステムを構成する機器、回線の正常状態を監視する。

(2) システムの運転

ネットワークシステムを構成する機器、回線を起動ないしは停止させる。または自律的に起動、停止する機器については起動ないしは停止の通知を受ける。

(3) システム構成の追加変更

端末、回線の追加に伴う制御属性値の設定や、ソフトウェアの配送を行う。

また、ネットワークシステムを構成する機器の変更通知を受ける。

(4) 統計、会計情報収集

C P U 負荷や送受信データ数、またはエラー率などの各種統計情報および会計情報を収集する。

それら収集情報を統計処理したレポートを出力したり、課金請求書を出力する。

(5) 試験、診断

障害検出後の試験、診断を行う。また、予防保守のために（定期的に）試験を行う。

3.1.3 O S I 管理の観点からの論理化

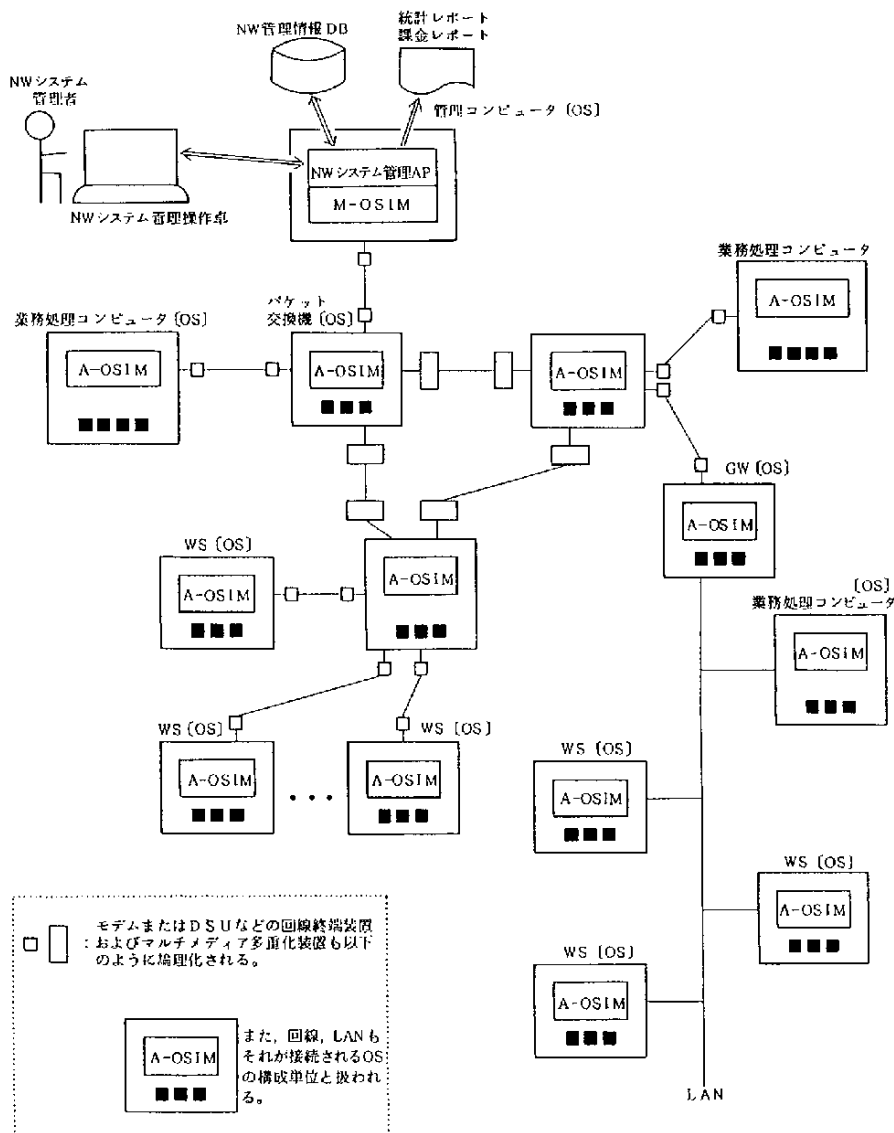
図3.1のモデルシステムをO S I 管理の観点から論理化すると図3.2のようになる。管理コンピュータ、業務コンピュータ、W S（ワークステーション）、マルチメディア多重化装置およびモデムも論理的には個々のオープンシステムとなる。管理コンピュータ上にネットワークシステム管理者による管理操作に従って動作するネットワークシステム管理アプリケーションプログラム（NW

システム管理AP)が存在する。そしてそのNWシステム管理APに対して、管理側としてのOSI管理機能を提供する機能体(M-OSIM)が存在する。

一方、M-OSIMと管理情報を交換することによって、管理される側としてのOSI管理機能を提供する機能体(A-OSIM)が、管理される各オープンシステムに存在する。そしてこのA-OSIMが実際の管理対象物とローカルなインタフェースをとることにより、ネットワークシステム管理者が個々の機器の装置や機能体を管理することとなる。

OSI管理の規定範囲は以下になる。

- ① M-OSIMとA-OSIMとの間の管理情報交換プロトコル
- ② M-OSIMがネットワークシステム管理APに、またA-OSIMが管理対象側システム管理APにOSI管理機能を提供するサービス仕様
- ③ ネットワークシステム管理APと管理対象との間で交換される管理情報の内容(コーディング規則と意味付け)



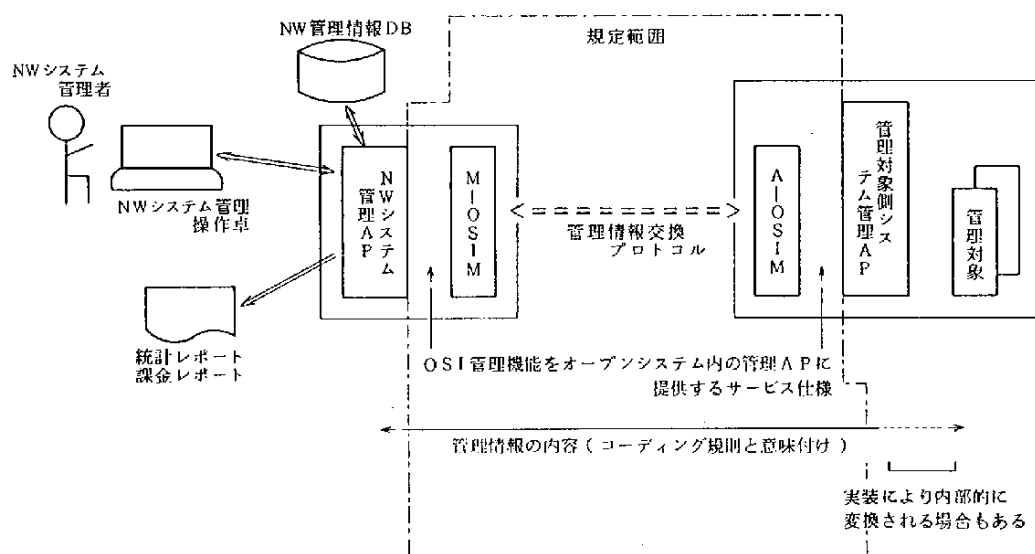
- M-OSIM: 管理側としてOSI管理の機能を実現する機能単位
 (詳細は後述)
 A-OSIM: 管理側される側としてOSI管理の機能を実現する機
 能単位 (詳細は後述)
 OS: オープンシステム
 ■: ネットワークシステム管理者により直接的ないしは間
 接的に管理される具体的な管理対象

図 3.2 OSI 管理の観点からの論理図

従って、以下の項目はネットワーク管理システムを提供するメーカー、ないしは各ネットワークシステム毎に決めるべきものである。

- ① ネットワークシステム管理者とのコマンドなどのマンマシンインタフェース仕様
- ② ネットワークシステム管理操作卓の画面形式
- ③ ネットワークシステム管理情報データベース内の具体的情報
- ④ 統計レポート、課金レポートの具体的内容

OSI管理で規定される範囲と規定されない部分を簡単に示すと図3.3のようになる。



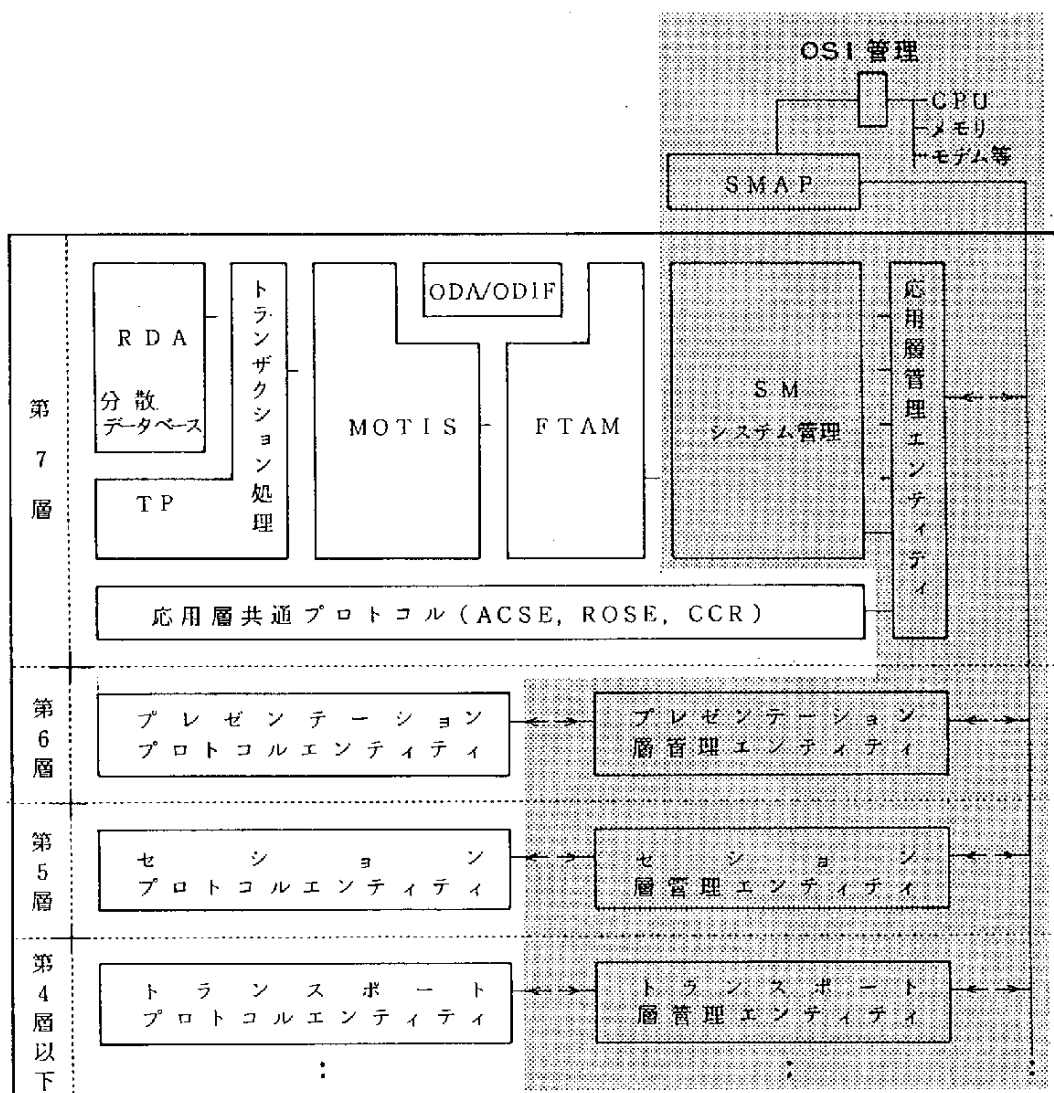
注：OSI管理のサービス機能仕様としては、M-OSIM用とかA-OSIM用とかの区別はなく一律な規定となっている。

図3.3 OSI管理の規定範囲

3.2 OSI 管理の概要と動向

3.2.1 OSI 上の位置づけ

OSI 管理は、OSI 基本参照モデルの第7層（応用編）内のシステム管理（SMAE：システム管理応用エンティティ）と、管理対象のモデル化に従って動作するSMAP（システム管理応用プロセス）および層管理の集合である。



■：ISO 7498-4「OSI 基本参照モデルPart4 管理フレームワーク」で導入された「OSI 管理」の概念

図 3.4 OSI 上の位置づけ

3.2.3 システム管理

システム管理は、OSI環境中の資源の監視 (monitoring) , 制御(control), 調整 (cordination)のためのメカニズムと, それら資源に関わる情報を伝送するためのOSIプロトコル標準を規定している。

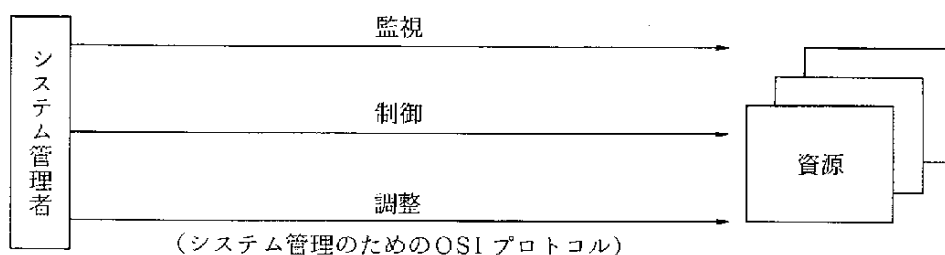


図 3.7 システム管理プロトコルの目的

OSI環境上の資源に対する管理オペレーションを表現するために, それら資源は, 固有特性を定義した管理対象として見る。

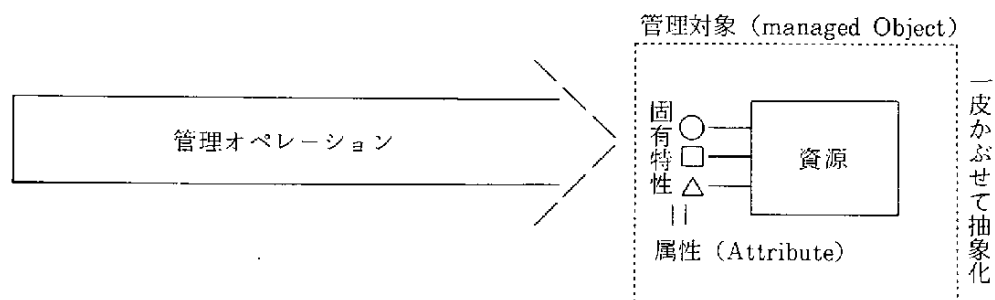


図 3.8 資源を抽象化

ある開放型システムでシステム管理の目的で要求される情報は、ローカルな入力によって得られるかもしれないし、システム管理（応用層）通信によって、または、下位層プロトコル交換の結果として、他の開放型システムからの入力から得られるかもしれない。

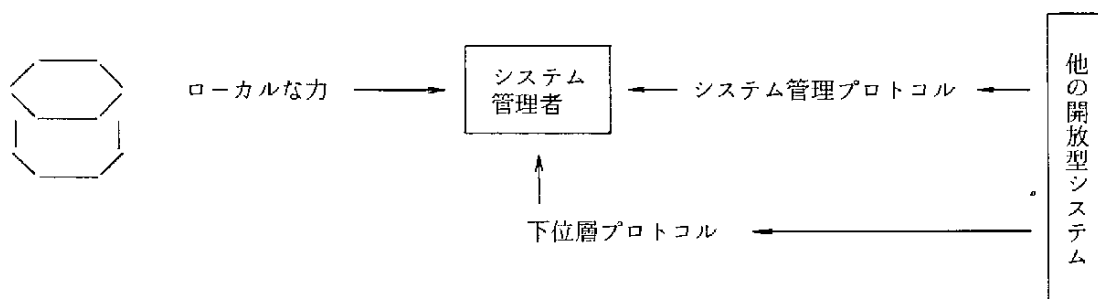


図 3.9 システム管理活動の情報の流れ

システム管理は、分散処理と通信環境の広い範囲に適用される。

その環境とは、

- ・ ローカルネットワーク上にインプリメントされた小さく局所化されたシステムから
- ・ 企業や国営ネットワークで大規模に結ばれたシステムまで及ぶ。

（例え、通常は自律的な管理ドメインにあるものさえ、この同じ標準とコンセプトを適用する。）

システム管理活動に要求される機能要件は、以下の5つの管理領域にグループ化できる。

① 障害管理 (fault management)

- ・ エラー発生のお知らせとエラー情報の読み取り
- ・ テストの実行と結果のお知らせ

接続性テスト：2つのプロトコルエンティティ間でコネクションが確立できるか否かを検証する。
 プロトコル整合性テスト：2プロトコルデータ単位（PDU）の転送順序の正当性を検証する。
 機能テスト：特定の層またはシステムの特定の機能が正しく作動することを検証する。
 診断テスト：診断情報によりどの構成要素に障害が起こっているかを検出する。
 性能テスト：管理対象の性能を測定する。

② 構成管理 (configuration management)

- ・ 管理対象の生成，削除を管理する。
- ・ 状態を変更する，状態を通知する。
- ・ 関係情報の生成，変更を管理する。
- ・ ソフトウェアの配布，初期化等を管理する。

③ 会計管理 (accounting management)

- ・ 課金単位の定義
- ・ 課金情報の読み出し
- ・ 課金限度の設定・変更・読み取りと，限度超過の報告
- ・ 課金記録の読み出し

④ 性能管理 (performance management)

- ・ 性能の監視
- ・ 性能の制御と調整
- ・ 性能の分析
- ・ 性能の情報の収集

⑤ 機密管理 (security management)

- ・ アクセス権の設定，変更を管理する。
- ・ アクセスについてパスワードを検査する。

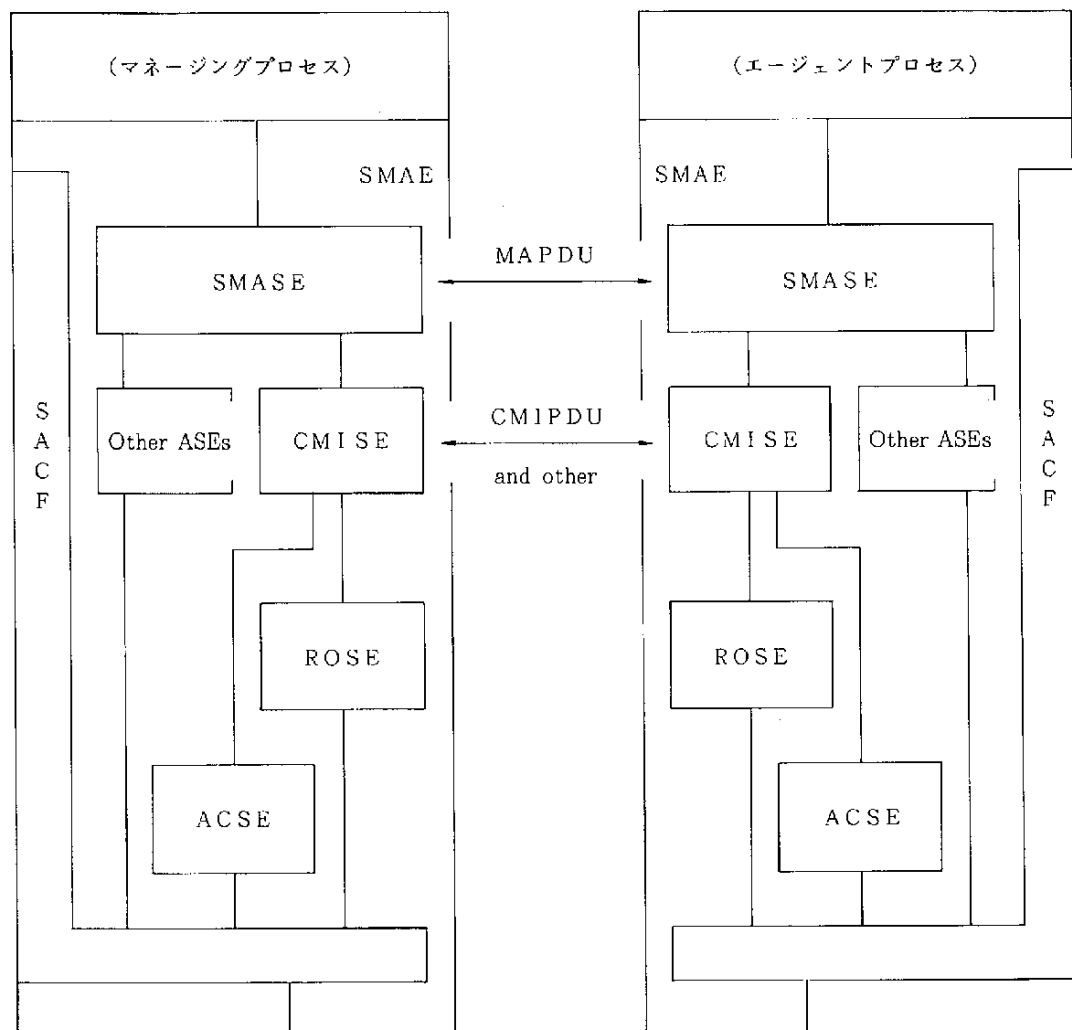
- ・アクセス権の違反について報告する。
- ・アクセスに関する記録の収集と読み取り。

情報の多くの項目と、それに関係付けられているオペレーションや通信プロトコルは、複数の領域で共通するものである。従って、システム管理者はある方針に基づいた管理を達成するために複数の管理機能を組合わせて使用し、管理活動を実現する。

3.2.4 システム管理プロトコル

マネージングプロセスとエージェントプロセス間の会話は、管理情報の交換によって実現され、この通信は、OSIプロトコルを使用して達成される。

図3.10は、システム管理プロトコルを実現する応用エンティティであるSMAE（システム管理応用エンティティ）の論理構造を示している。



注：この図は、システム管理による応用層の使用の例である。応用層コンポーネントの正確な構成を図示している訳ではない。

図3.10 システム管理応用エンティティ

・ S M A S E (システム管理応用サービス要素)

上位の管理プロセス (S M A P : マネージングプロセスまたはエージェントプロセス) に対して, S M F A (特定管理機能領域: F M, C M, A M, P M, S M の機能要件) を多対多で満たすシステム管理機能 (オブジェクト管理機能, 関係管理機能, 状態管理機能, エラー報告と情報検索機能, 管理サービス制御機能, 信頼性と試験診断機能, ログ制御機能, 等) のサービスを提供する A S E。

・ M A P D U (管理応用プロトコルデータ単位)

O S I 管理に関係して転送される情報のセマンティックスと抽象構文を定義する。具体的には, A C T I O N, E V E N T, A T T R I B U T E テンプレートで定義される抽象構文と, それに加えて, O B J E C T, N A M E, G R O U P A T T R I B U T E, S U P P L E M E N T A R Y P A C K A G E, B E H A V I O R テンプレートで定義されるセマンティックスである。

・ C M I S E (共通管理情報サービス要素)

共通管理情報プロトコルデータ単位 (C M I P D U s) の転送のためのサービスと手続きを規定している。つまり, 管理の目的で情報とコマンドを共通の方法で交換するための手段を提供する。主に, 管理対象を, クラスとインスタンスで捉え, そのインスタンスの識別に, I S O / I E C 9594 (The Directory) で定義される識別名 (Distinguished Name) を使用することを定義している。

・ C M I P D U (共通管理情報プロトコルデータ単位)

R O S (リモートオペレーションサービス, I S O 9072) で定義されている O P E R A T I O N マクロ, E R R O R マクロを使用して定義される。

m - E v e n t R e p o r t オペレーション

m - E v e n t R e p o r t - C o n f i r m e d オペレーション

m - L i n k e d - R e p l y オペレーション

m-Get オペレーション

m-Set オペレーション

m-Set-Confirmed オペレーション

m-Action オペレーション

m-Action-Confirmed オペレーション

m-Create オペレーション

m-Delete オペレーション

のセマンティックスと抽象構文を定義する。

このうち、GDM1は、層に関係なく各層で保持すべき管理情報（接続／切断数等）の内容を規定し、層特有な管理情報は、各層管理（トランスポート層のISO/IEC JTC1/SC6/WG4 T.19（東京会議）やネットワーク層のSC6/WG2 A2, 33（ゲイサスバーグ会議）などの仕様）で規定される。

なお、最近の動向として、標準化が重要視されてきた管理対象／管理情報の規定方法を体系化するため文書体系が以下のように日本からISOへ寄書（SC21/WG4 N628）が作成された。他に、米案（N655）、CCITT案（N697）が提案されておりシドニー会議で審議される。

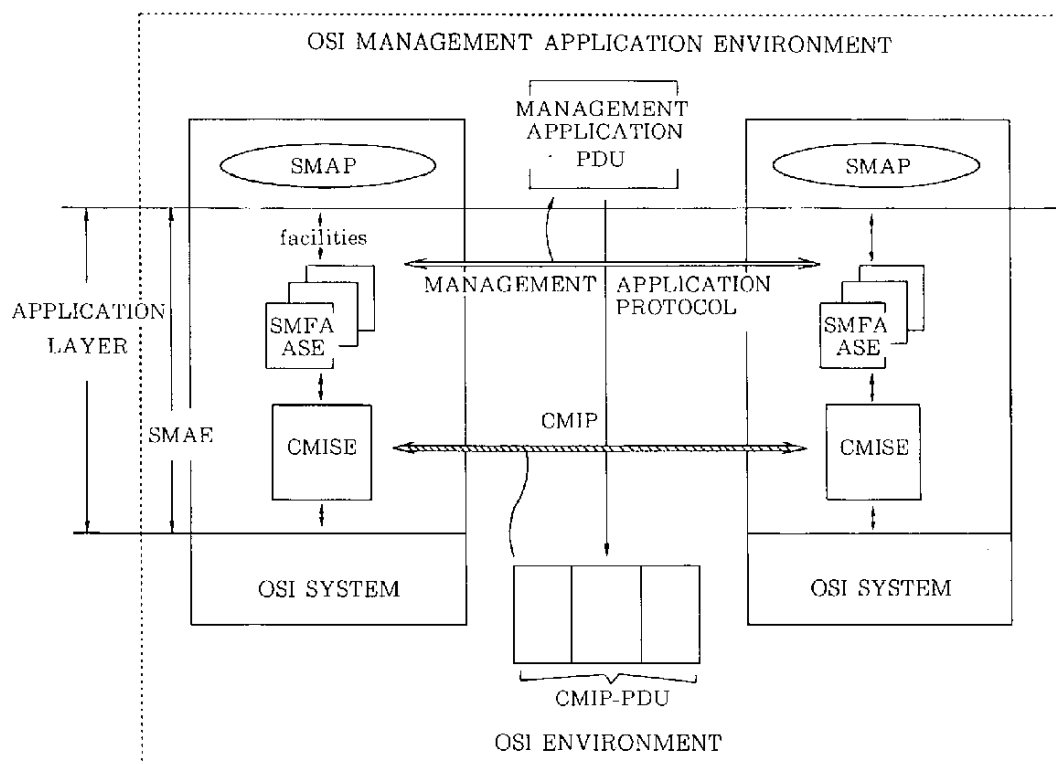
管理の枠組みと、そのAddendum 7498-4, 7498-4/Ad 1			
特定管理機能領域（SMFA）			
特定管理機能領域概要	10AAA-1	管理情報 構造(SMI)	10BBB
障害管理(FM)	-2	一般的な管理対象クラス、属性、 事象および動作の定義	10CCC
構成管理(CM)	-3		
性能管理(PM)	-4		
会計管理(AM)	-5		
機密管理(SM)	-6		
共通管理情報サービス定義（CMIS）		9595	
共通管理情報プロトコル仕様（CMIP）		9596	

図 3.12 提案された標準化文書の新体系

(2) O S I 管理の規定概要

管理フレームワーク（7498-4）の規約では、主に以下のことを規定している。

- ・ 「O S I 管理環境」内の開放型資は，
 - ① 開放型システムは自律的な管理が行えること。
 - ② 情報交換により管理活動の協調を行うため、他の開放型システムと協調できること。という管理責任がある。
- ・ O S I 管理は、管理データの情報通信 a n d / o r ローカルな操作で効果が現れ、以下の 5 つのファシリティで情報通信をサポートする。
 - 障害管理（F M）
 - 会計管理（A M）
 - 構成管理（C M）
 - 性能管理（P M）
 - 機密管理（S M）
- ・ O S I 管理は、3 つの管理によって達成される。
 - システム管理－複数層／複数システムの管理を行うメカニズムを提供する。
 - システム管理間の通信を提供するのが S M A E が実行する応用層プロトゴルである。
 - 層管理－層（P E：プロトコルエンティティ）内の通信活動を管理するメカニズムを提供する。
 - 層管理（L M E：層管理エンティティ）同士はシステム管理プロトコルまたは層管理プロトコルで通信する。
 - 層オペレーション－1 つの通信インスタンス（P M）を管理するメカニズムを提供する。



Higher level procedures will make use of specific facilities which, in turn, consist of procedures and information required to accomplish some OSI management functions falling within the scope of the particular SMFA.

fault management
 configuration management
 accounting management
 performance management
 security management

図 3.13 機能モデル

3.3.2 共通管理情報サービス

(1) 位置づけ

管理のための共通的な機能を提供するもので、応用層プロトコルの1つである。

(2) サービスの概要

現ドキュメントに定義されたサービス要素を以下に示す。ここで「管理対象」(Managed object)は管理の対象(例 X.25エンティティ, H/Wユニット, 回線)を示す。

表 3.1 サービス要素

サービス要素	概要
EVENT REPORT	管理対象に関して事象が発生してことを報告する。
GET	管理対象の属性を読み出す。
SET	管理対象の属性を指定した値に設定する。
ACTION	管理対象に対して動作を指示する。
CREATE	管理対象を生成する。
DELETE	管理対象を削除する。

(3) 共通的なパラメータ

Managed Object Class

管理対象の種別を示す。

Managed Object Instance

特定の管理対象を識別するための名前。

Attribute

管理対象の持つ各種の属性情報で、typeとvalueからなる。

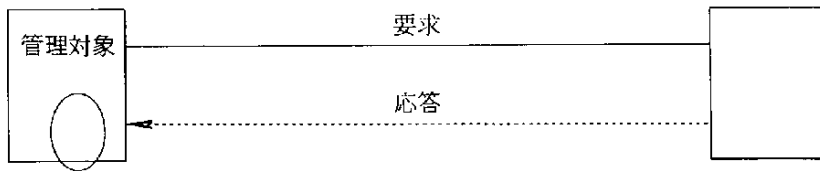
例.

type	パケット数カウンタ	回線速度	Errors
value	100	9600bps	エラー応答時のエラーコード

(4) 各サービスの内容

① Event Report

管理対象に関して何らかの事象（障害等）が発生したことを通知する。



要求のパラメータ

Managed Object Class	前述
Managed Object Instance	〃
Mode	応答を要求するか否かの指定。
Event Type	発生した事象の種別を示す。
Event Time	事象の発生した時刻を示す。
Event Argument	その事象に関連する付加的な情報を示す。

応答のパラメータ

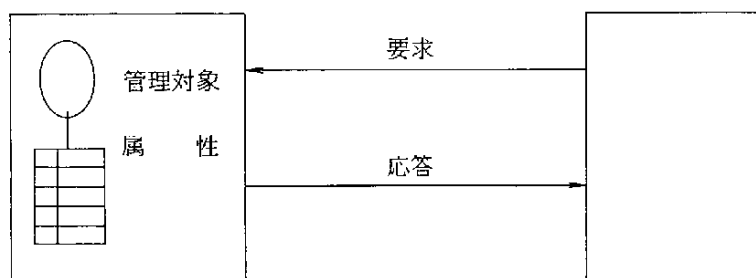
Managed Object Class	前述
Managed Object Instance	〃
Event Type	〃
Current Time	応答を送信した時刻
Event Result	結果

例.

Managed Object Class	x.25コネクション
Managed Object Instance	ノード4 - 論理チャネル1 (?)
Event Type	コネクション異常切断
Event Argument	結果

② Get

管理対象の属性を読み取る。



要求のパラメータ

Base Managed Object Class	後述
Base Managed Object Instance	"
Scope, Filter	"
Attribute identifier list	読み取るAttribute の名前のリスト

応答のパラメータ

Managed Object Class	前述
Managed Object Instance	"
Attribute list	読み取られたAttribute のリスト

Ex.

要求

Base Managed Object Class	x.25エンティティ
Base Managed Object Instance	...
Attribute identifier list	DTパケット数, RRパケット数

応答

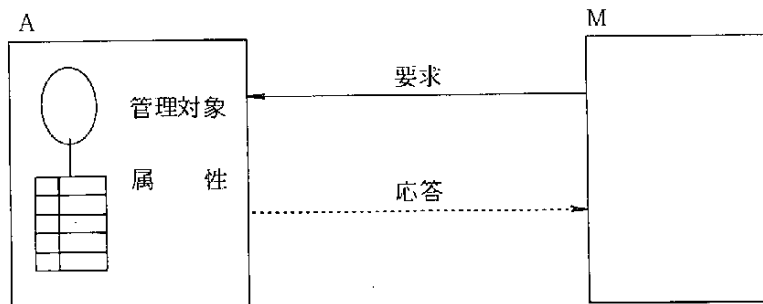
Managed Object Class 要求に同じ

Managed Object Instance ”

Attribute list D T パケット数=200, R R パケット数=100

③ S e t

管理対象の属性を指定された値に設定する。



要求のパラメータ

Base Managed Object Class 後述

Base Managed Object Instance ”

Scope, Filter ”

Mode 前述

Attribute list 設定されるAttribute のリスト

応答のパラメータ

Managed Object Class 前述

Managed Object Instance ”

Attribute list 設定されたAttribute のリスト

Ex.

要求

Base Managed Object Class x.25エンティティ

Base Managed Object Instance . . .

Attribute list H T C = 50, H O C = 75

応答

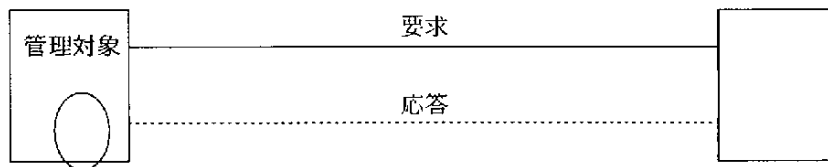
Managed Object Class 要求に同じ

Managed Object Instance "

Attribute list "

④ A c t i o n

管理対象に対して何らかの動作（試験の実行等）を指示する。



要求のパラメータ

Base Managed Object Class 後述

Base Managed Object Instance "

Scope, Filter "

Hode 前述

Action Type 指示する動作の種別を示す。

Action Argument その動作に関連する付加的な情報を示す。

応答のパラメータ

Managed Object Class 前述

Managed Object Instance "

Action Type

Current Time 応答を送信した時刻

Action Result 動作の結果

Ex.

要求

Base Managed Object Class 通信制御装置

Base Managed Object Instance

Action Type バックアップ回線への切り替え

Action Argument 切り替え先回線

応答のパラメータ

Managed Object Class 要求に同じ

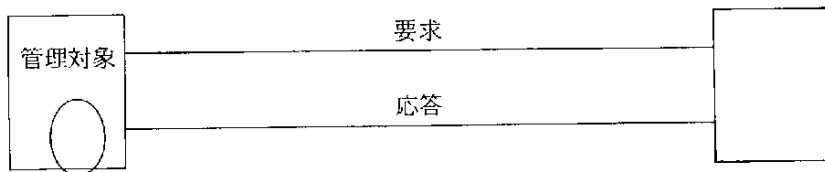
Managed Object Instance "

Action Type "

Action Result 実際に切り替えられた回線

⑤ Create

管理対象を生成する。



要求のパラメータ

Managed Object Class 前述

Managed Object Instance "

Reference Object Instance Attributeの初期値としてここで指定されたObjectの Attribute値をコピーする。(下記で指定されない時)

Attribute list Attributeの初期値を指定する。

応答のパラメータ

Managed Object Class 前述
 Managed Object Instance "
 Attribute list 実際のAttribute 値
 Current Time 応答を送信した時刻

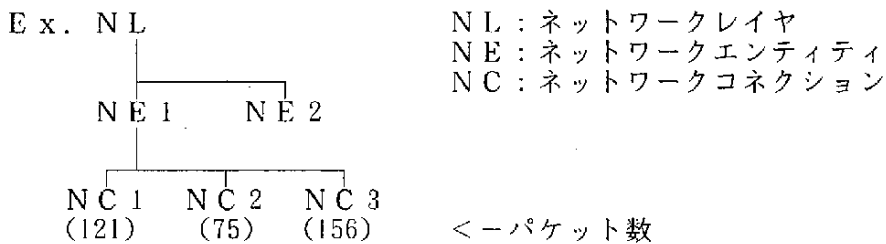
⑥ Delete

管理対象を削除する。

(5) その他の機能

FilterとScope

FilterとScope は複数の管理対象の指定を可能とする。各管理対象はMIT (Mangement Information Tree=Naming Tree) によって規定される「包含」の関係を持つ。



Scope は以下の値をとる。(指定なきときは0)

- O : Base Managed Object 自身
 - n : Base Managed Object のnレベル下位のObject群
 - 1 : Base Managed Object とそのすべての下位Object群
- 上記の例でBase Managed Object = NE 1, Scope = 1 とすると (NC 1,

N C 2, N C 3) が指定出来る。

FilterはAttribute 値が特定の値より大きい, 小さい, 等しいなどの条件を指定出来る。さらに複数の条件をAND, ORで連結することが出来る。

E x.

G e t 要求

Base Managed Object Class ネットワークエンティティ

Base Managed Object Instance N E 1

Scope 1

Filter パケット数>100

Attribute identifier list パケット数

応答 1

Managed Object Class ネットワークコネクション

Managed Object Instance N C 1

Attribute list パケット数=121

応答 2

Managed Object Class ネットワークコネクション

Managed Object Instance N C 3

Attribute list パケット数=156

3.3.3 構成管理サービス

(1) 構成管理とは

定常操作を左右する開放型通信ファシリティの特性を制御・監視する機能の集合である。

その機能とは：

- ・ 開放型システムのパラメタの設定
- ・ 管理オブジェクトの初期化および閉塞処理
- ・ 開放型システムに付与されたデータの収集
- ・ 開放型システム構成の変更
- ・ 管理オブジェクトとその名前の関連付け

〔具体的には次のような機能を果たすことになる。〕

- ・ 新たな管理オブジェクトを導入し、定義すること
- ・ 管理オブジェクトの名前づけ及び割り当てた名前を管理すること
- ・ 管理オブジェクト間の関係を生成、削除、変更すること
- ・ 操作特性の設定と変更
- ・ 可変属性の初期ネットワークを割り当てること
- ・ 種々の運用レベルで設定される管理オブジェクトの管理状態を変更すること
- ・ 管理オブジェクトの識別子、クラスや関係の報告とそれらを要求すること
- ・ 管理オブジェクトの存在や操作状態における重要な変化を報告すること
- ・ 管理オブジェクトを削除すること

(2) 構成管理モデル

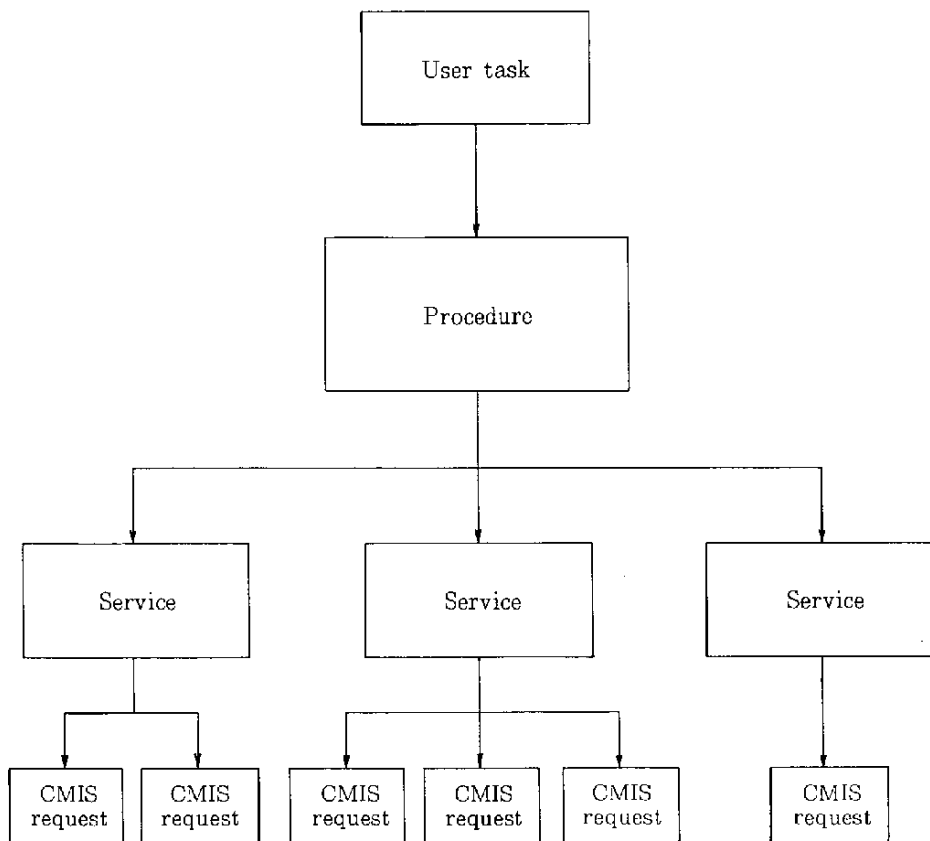


図 3.14 操作モデル

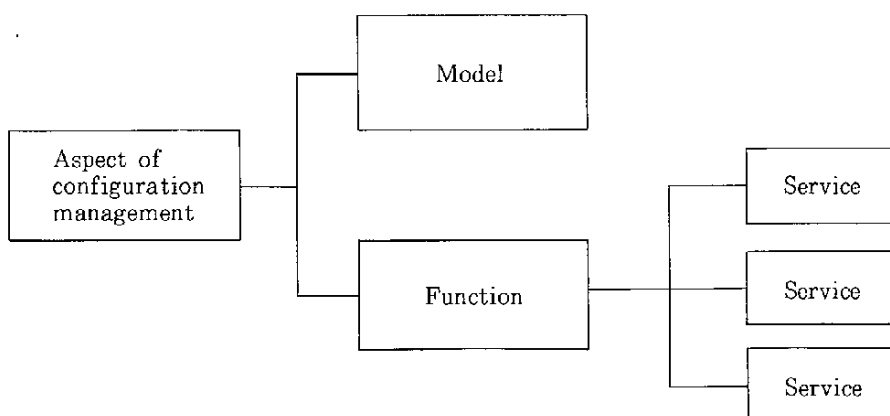


図 3.15 機能モデル

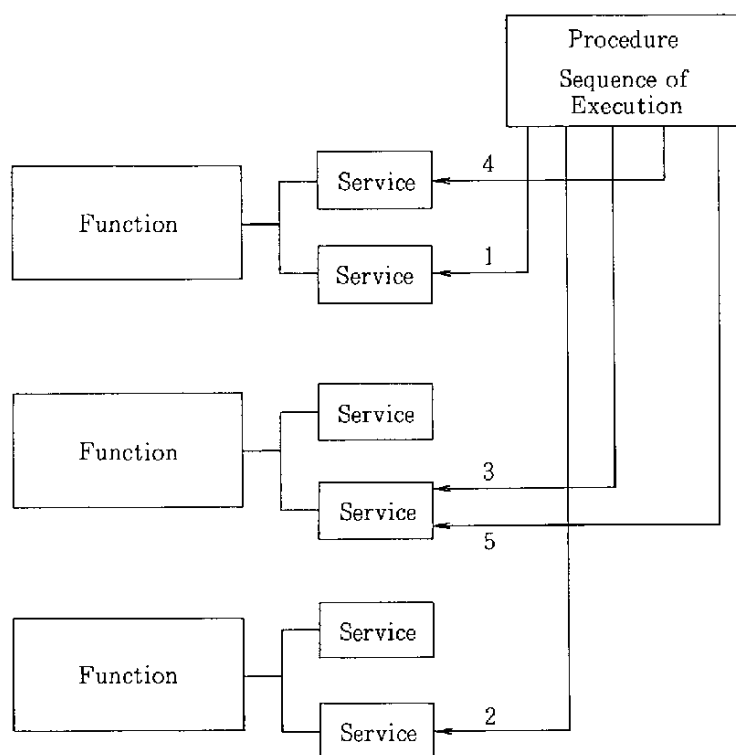


図 3.16 操作モデルと機能モデルの関係

(3) オブジェクト管理

① モデル

[管理対象]

構成管理で取り扱うシステムの部分は、管理対象のインスタンスで表現される。管理対象は、特定のクラスを持つ。クラスとは、同じ性質を持ち、同様の目的を満たす同種の管理対象の集合を分類するものである。

[属性]

管理対象の幾つかの性質を記述する管理情報項目である。例：操作特性、操作条件、現状態、ステータスなど、属性は、識別子と値を持つ。

② サービス機能

- ・ CREATE-OBJECT : 管理対象のインスタンスの作成を依頼する。
- ・ DELETE-OBJECT : 管理対象のインスタンスの削除を依頼する。
- ・ RENAME-OBJECT : 管理対象のインスタンス名の変更を依頼する。
- ・ ENROL-OBJECT : 新しい管理対象インスタンスが作成されたことを報告する。
- ・ DEENROL-OBJECT : 管理対象インスタンスが削除されたことを報告する。
- ・ REENROL-OBJECT : 管理対象インスタンスの名前が変更されたことを報告する。
- ・ GET-OBJECT-NAMES : 管理対象の名前を要求する。
- ・ DISPLAY-ATTRIBUTES : 管理対象インスタンスが持つ属性値を要求する。
- ・ CHANGE-ATTRIBUTES : 管理対象インスタンスが持つ属性値を変更する。
- ・ REPORT-ATTRIBUTE-CHANGE : 管理対象インスタンスの属性値を変更を通知する。

[CMISとの関係]

CREATE-OBJECT	← M-CREME
DELETE-OBJECT	← M-DELETE
RENAME-OBJECT, CHANGE-ATTRIBUTES	← M-SET
ENROL-OBJECT, DEENROL-OBJECT, REENROL-OBJECT,	
REPORT-ATTRISUTE-CHANGE	← M-EVENT-REPORT
GET-OBJECT-NAMES, DISPLAY-ATTRIBUTES	← M-GET

(4) 状態管理

① モデル

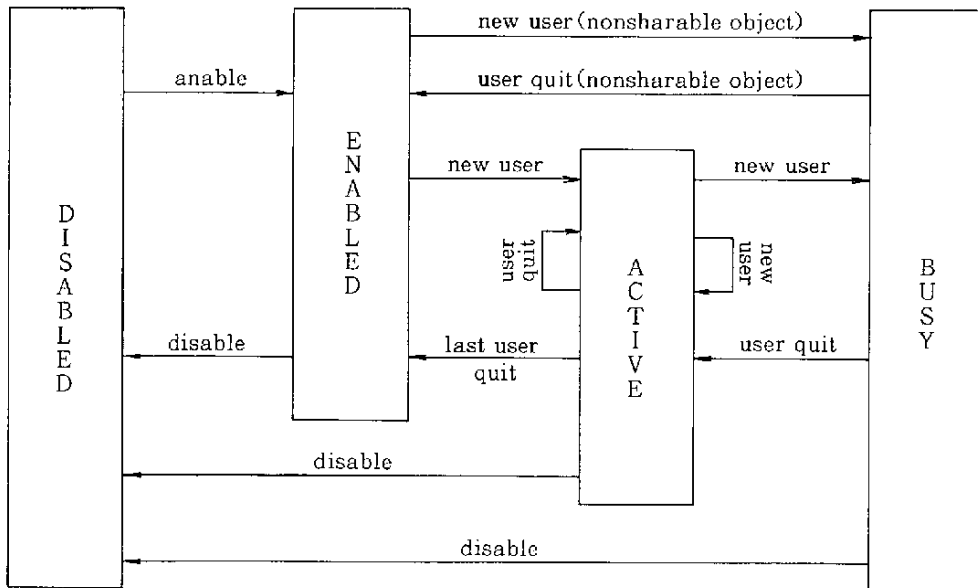


図 3.17 操作状態

- (0) Disabled : 管理対象が実装されていない, 不完全などの理由 で操作不可, 又はこれに関連する資源でないので操作不可。
- (1) Enabled : 管理対象は, 操作可能であるが, 現在使用されていない状態
- (2) Active : 管理対象は, 操作可能で現在使用されている。まだ, 使用できる余裕がある。
- (3) Busy : 管理対象は, 操作可能で使用されている。この管理対象は他にサービスする余裕はない。

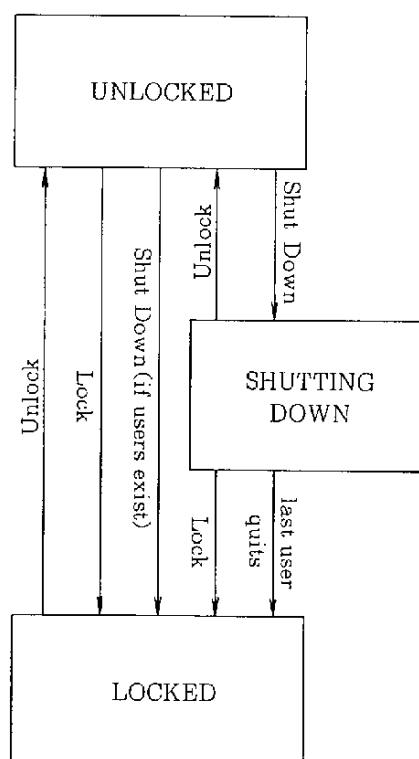


図 3.18 運用管理状態

- Locked : 運用管理的に管理対象の使用が禁止されている状態 (0)
- Shutting Down : 管理対象は, それを現在使用している利用者のみ使用可能な状態 (2)
- Unlocked : 管理対象が, 使用可能である状態 (1)

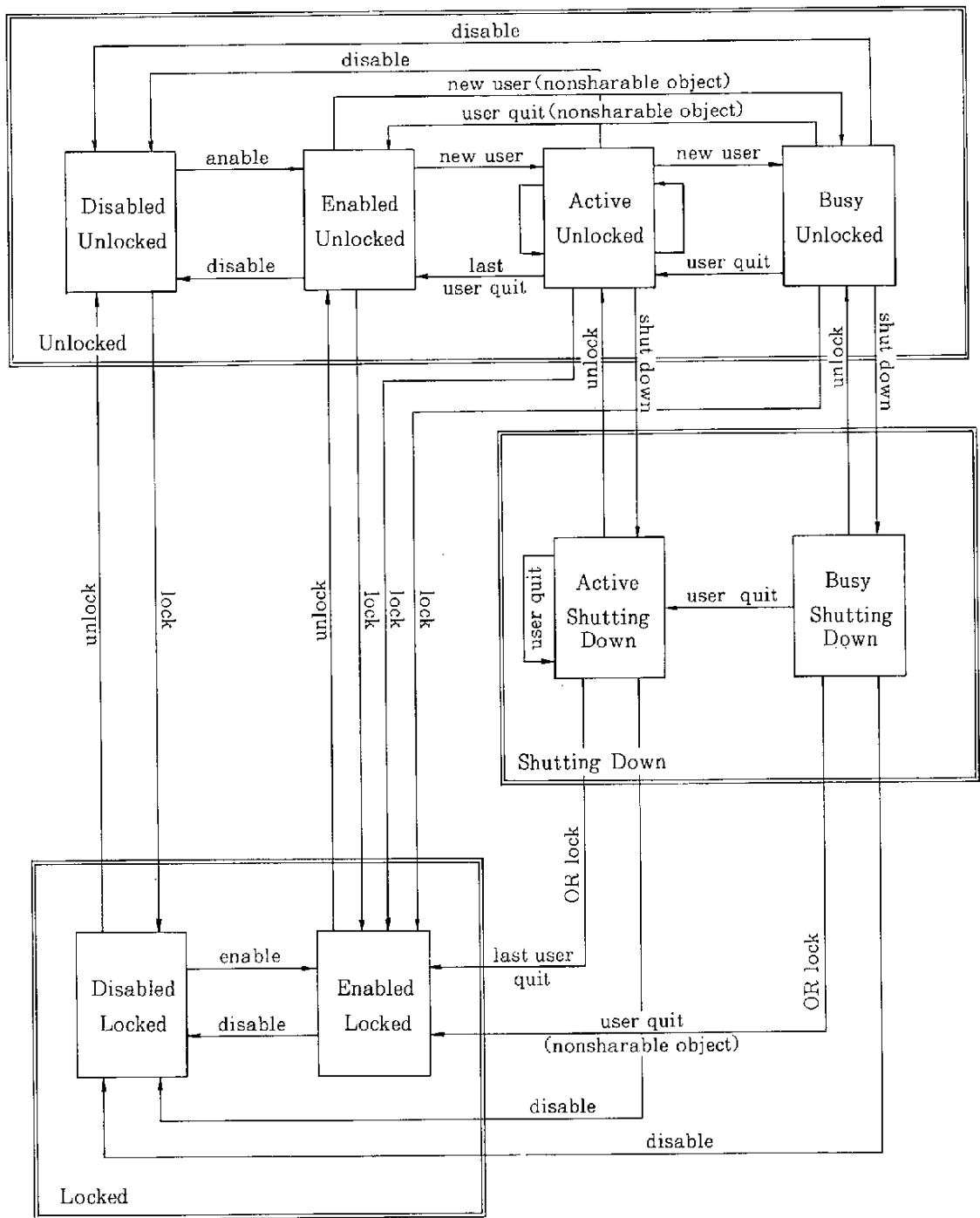


図 3.19 状態管理モデル

表 3. 2 状態マトリックス

	DISARLED	ENABLED	ACTIVE	BUSY
LOCKED	Disabled Locked ①	Enabled Locked ②	_____	_____
SHUTTING DOWN	自動的に ①に遷移	自動的に ②に遷移	Active Shutting down.	Busy Shutting down.
UNLOCKED	Disabled Unlocked	Enabled Unlocked	Active Unlocked	Busy Unlocked

Disabled Locked : 管理対象は、運用が禁止されており、何らかの原因で操作不能である。使用できるようにするためには、アンロック操作と修復が必要である。

Enabled Locked : 管理対象は、運用が禁止されているが、操作可能である。使用できるようにするためには、アンロック操作が必要である。

Active Shutting down: 管理対象は、操作可能であり、使用中である。しかし、運用が制限されている。再度利用可能にするためにはアンロック操作が必要である。

Busy Shutting down: 管理対象は、操作可能であり、使用中である。しかし、運用は制限されている。利用者に対して余力はない。他の利用者にアクセス可能にするためには、現利用者の終了を待ち、アンロック操作を行う必要がある。

Disabled Unlocked : 管理対象は、運用が禁止されている訳ではない。しかし、何らかの原因で操作不能である。使用するためには、修復が必要である。

Enabled Unlocked: 管理対象は、操作可能であり、利用者がアクセス可能である。しかし、実際には使用されていない。

Active Unlocked : 管理対象は、操作可能であり、使用中である。また、利用者に対する十分な余力がある。

Busy Unlocked : 管理対象は、操作可能であり、使用中である。利用者に対して余力がない。他の利用者が使用可能となるためには、現利用者が終了しなければならない。

② サービス機能

- GET-STATE : 構成状態の値を要求する。
- SET-STATE : 構成状態の値を変更する。
- REPORT-STATE-CHANGE : 状態が変わったことを報告する。

[CMISとの関係]

GET-STATE	← M-GET
SET-STATE	← M-GET
REPORT-STATE-CHANGE	← M-EVENT-REPORT

(5) 関係管理

① モデル

a. 直接関係と間接関係

直接関係 : ある管理対象に関連する管理情報が他の管理対象を識別するような場合の関係

間接関係 : 2 つ以上の直接関係の連結から引き出される関係

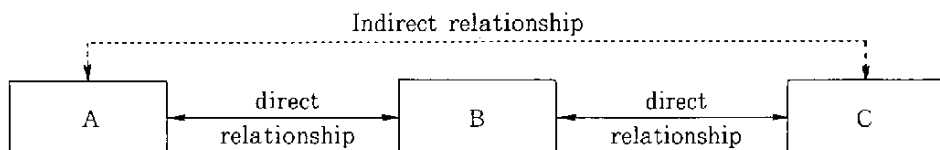


図 3.20 直接関係と間接関係

また、関係には対称な関係と非対称な関係の 2 種類がある。

b. 暗黙な関係と明白な関係

暗黙の関係： 所有したり，管理したりする管理対象の名前で決まる
関係

明白な関係： 関係属性によって関係付けられる関係

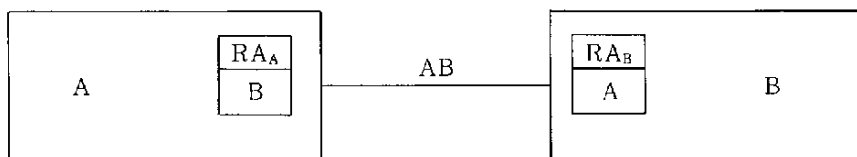


図 3.21 明白な関係

② 関係の種類

- ・ サービス関係： サービス提供者の関係。
- ・ 対等関係： 二つの管理対象の関係が対等な関係。
- ・ バックアップ関係： 現用と予備の関係。故障時にバックアップされる。
- ・ グループ関係： グループ対象とそのメンバーオブジェクトの関係。
- ・ トポロジカル関係： 二つの管理対象の間が空間的またはトポロジカル結合で定義される関係。

③ サービス機能

- ・ CREATE-RELATIONSHIP： 明白な関係の作成の要求
- ・ DELETE-RELATIONSHIP： 明白な関係の削除の要求
- ・ CHANGE-RELATIONSHIP： 関係属性値の変更要求
- ・ DISPLAY-RELATIONSHIP： 関係属性値の取り出し要求
- ・ REPORT-RELATIONSHIP-CREATION： 関係属性が生成されたことの報告

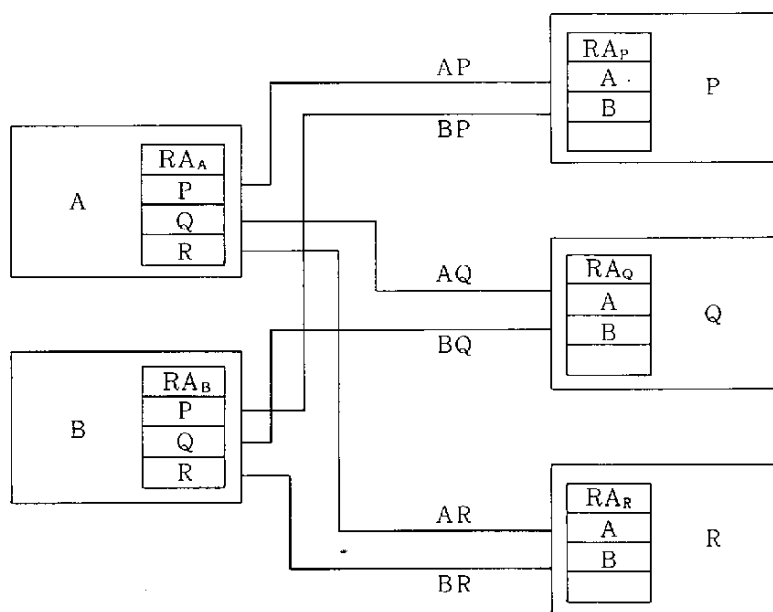


図 3.22 多数対多数の明白な関係

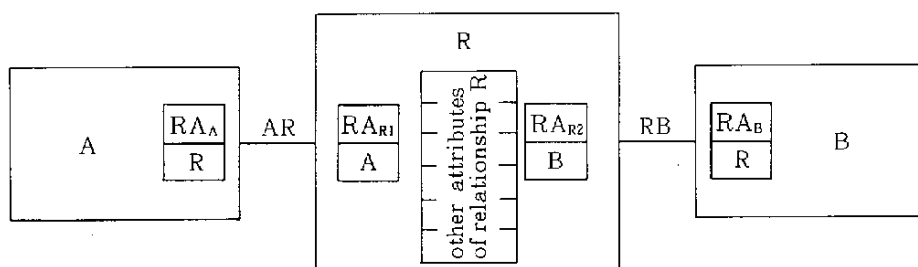


図 3.23 非対称の関係を表す管理オブジェクト

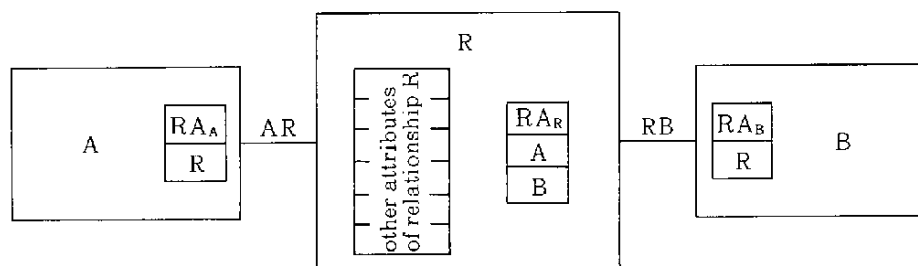


図 3.24 対称の関係を表す管理オブジェクト

- ・ REPORT-RELATIONSHIP-DELETION : 関係属性が削除されたことの報告
 - ・ REPORT-RELATIONSHIP-CHANGE : 関係属性が変更されたことの報告
- [CMISとの関係]

CREATE-RELATIONSHIP, DELETE-RELATIONSHIP,	
CHANGE-RELATIONSHIP	← M-SET
DISPLAY-RELATIONSHIP	← M-GET
REPORTY-RELATIONSHIP-CREATION,	
REPORT-RELATIONSHIP-DELETION	← M-EVENT-REPORT
REPORT-RELATIONSHIP-CHANGE	← M-EVENT-REPORT

3.3.4 障害管理サービス

ISO/IEC JTC1/SC21/WG4 N587 August. 1988 6thWD

(1) 障害管理で規定する機能

① エラー報告と情報検索機能

エラー報告

閾値超過報告

カウンタ, ゲージ, 閾値情報の取得

② 信頼性と診断試験

管理対象に対する試験の実行を指示する機能

試験結果報告

試験の取り消し

試験結果の取得

③ 管理サービス制御

障害報告のみならず, 事象報告すべてに対する制御機能を規定

管理対象の振る舞いを制御 (事象報告やログをするのかしないのか等)

(2) エラー報告と情報検索機能

要件

- ① 障害の発生と関連情報を標準的な形式で報告すること
- ② 障害検知の機構を提供すること
- ③ 障害発生に関する統計情報を計算し、引き続きそのような統計情報を要求できること

障害のモデル

- ① エラータイプ（と、推測原因）

OBJECT IDENTIFIER

通信障害（INTEGER 0）

（信号の紛失，フレーム誤り，伝送誤り，呼設定失敗，等）

サービス品質障害（INTEGER 1）

（応答時間オーバー，キューサイズオーバー，帯域減少，再送比率オーバー，等）

処理障害（INTEGER 2）

（データ改ざん，バージョン不一致，メモリ不足，等）

装置エラー（INTEGER 3）

（電源，クロック，プロセッサ，回線カード，等）

- ② 重度（Severity）

INTEGER

- | | | |
|---|--------------|---|
| 1 | 固 定 | 構成管理で規定するDisable 状態に遷移し，それ以後，利用者による使用を禁止する。 |
| | Permanent | この重度のために“Backup状態”がある。 |
| 2 | 間 欠 | 電源の瞬断など障害に陥ったが処理が継続されている。 |
| | Intermittent | この重度のために“閾値”の機構がある。 |

- 3 過 渡 少数パケットの紛失に対する再送などサービスレベルは低下したが正常終了した。

Transient この重度のために“ゲージ”の機構がある。

③ 傾向暗示 (B O O L E A N)

病状が悪化したかどうか。

④ 診断情報 (A N Y)

障害時のカウンタ値, 閾値, 構成情報。

⑤ B a c k u p 状態 (B O O L E A N)

故障した管理対象が二重系に切り替わったかどうか。

⑥ 提案修復動作 (A N Y)

障害が発生したシステムで示唆できる解決方法。

⑦ 他の情報 (A N Y)

呼び出し先, 通信相手など。

エラー報告サービス

パラメータ → C M I S

↓

M - E V E N T - R E P O R T

エラータイプ → Event Type

推測原因コード ...

重度

傾向暗示

診断情報

→ Event Info

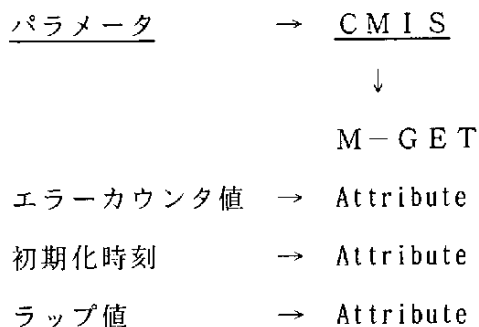
Backup状態

提案修復動作

閾値情報

他の情報 ...

エラー情報検索サービス



(3) 信頼性と診断試験機能

要件

① 接続性試験

P E間の接続性の検証を行う能力を提供する。

② プロトコル完全性試験

特定の P D U N O 転送順序を指定し，応答を監視する能力を提供する。

③ 機能試験

ある層のあるシステムにおける特定の機能が正常に動作していることの検証を行う能力を提供する。

④ 診断試験

兆候情報に基づいて，どの要素が不良かを決定する能力を提供する。

⑤ 性能試験

管理対象の性能を測定する能力を提供する。データ飽和／接続飽和／
応答時間試験等

試験機能のモデル

① 環境

試験指示者 (T e s t C o n d u c t o r)

試験実行者 (T e s t P e r f o r m e r)

第一次試験実行者に対して第二次試験実行者がいて接続性の試験を

行う。試験実行者は“試験対象”と呼ばれる。

② 試験状態

- (a) アイドル
- (b) 開始
- (c) 試験中
- (d) 報告中
- (e) 終了

③ 試験識別

試験クラス

試験指示者

試験インスタンス

④ 試験対象識別

試験指示者は試験中に試験実行者を識別する必要がある。

⑤ 試験の開始

開始要求のパラメータ

- (a) 第二次試験実行者の識別
- (b) 試験クラス固有のパラメータ

⑥ 返却機構

- (a) 暗黙の報告と終了の合体
- (b) 暗黙の報告と暗黙の終了
- (c) 暗黙の報告と隅の終了
- (d) 隅の報告と暗黙の終了
- (e) 隅の報告と隅の終了
 - ・ 暗黙の報告：定義済事象発生時に報告
 - ・ 隅の報告：試験指示者からの要求直後に報告
 - ・ 暗黙の終了：定義済事象発生時に終了
 - ・ 隅の終了：試験指示者からの要求直後に終了

⑦ 試験の報告

隅の報告時，必要なパラメータ

- (a) ユニークな試験識別

⑧ 試験の終了

隅の終了時，必要なパラメータ

- (a) ユニークな試験識別
(b) 報告を終了させるか否かの論理値

⑨ 試験テンプレート

すべての試験に共通な特性

試験対象としての管理対象の定義に含まれるもの

- (a) 試験状態属性

試験クラスの定義には以下のものを含む

- (b) 試験の目的
(c) 試験クラス識別子
(d) 使用する返却機構の型
(e) 暗黙の報告／終了の定義済事象
(f) その試験固有のパラメータ
(g) 試験実行者間の関係と，それらの間の相互動作
(h) 報告の内容

⑩ 混合試験

各クラスの試験を混合して使用することもできる。

試験サービス

接続性試験	→	M-ACTION
データ完全性試験	→	M-ACTION
プロトコル完全性試験	→	M-ACTION
データ飽和試験	→	M-ACTION

接続飽和試験	→ M-ACTION
応答時間試験	→ M-ACTION
仮想折り返し試験	→ M-ACTION
機能試験	→ M-ACTION
診断試験	→ M-ACTION

(4) 管理サービス制御機能

要件

- ① 事象報告を選択可能にする
事象報告ディスクリミネータ
- ② 事象報告の宛先（管理システム，ログ等）
- ③ 特定の管理システムや管理対象に有効なサービスを規定した
サービスアクセスディスクリミネータ
- ④ 事象報告による幅輻を防止する機構
- ⑤ 事象ログの確立と管理
- ⑥ 事象報告ディスクリミネータやサービスアクセスディスクリミネータ
の基準を外部システムから変更する能力

管理サービス制御モデル

- ① 管理サービス制御ディスクリミネータ
 - ・ ディスクリミネータに関連するサービス利用者の識別子
 - ・ 操作／通知が有効な基幹の開始時刻と終了時刻
 - ・ 各ディスクリミネータに固有のもの
- ② 事象報告ディスクリミネータ
 - ・ このディスクリミネータがactive/inactive
 - ・ 管理対象名
 - ・ 事象タイプ
 - ・ 事象に固有の属性（重度, Backup, 原因, 診断, 等）

③ サービスアクセスディスクリミネータ

- ・ このディスクリミネータがactive/inactive
- ・ 管理対象名
- ・ 許される管理操作の集合
- ・ アクションタイプ
- ・ アクセス制御パラメータ

管理サービス制御サービス

① 管理サービス制御開始サービス → M-CREATE

パラメータ

ディスクリミネータ対象

ディスクリミネータ構成

管理利用者識別子

ディスクリミネータ状態

開始時刻 (Generalized Time)

終了時刻

② 管理サービス制御終了サービス → M-DELETE

パラメータ

ディスクリミネータ対象

③ 管理サービス制御中断サービス → M-SET

パラメータ

ディスクリミネータ対象

ディスクリミネータ状態属性 → inactive

④ 管理サービス制御再開サービス → M-SET

パラメータ

ディスクリミネータ対象

ディスクリミネータ状態属性 → active

- ⑤ ログ取得開始 → M-CREATE
- パラメータ
- 管理対象=ログ
- ログID
- ディスクリミネータ構成
- 生成時刻
- 開始時刻
- 終了時刻
- ⑥ ログ取得終了 → M-DELETE
- パラメータ
- 管理対象=ログ
- ⑦ ログ取得中断／再開
- f u r t h e r s t u d y
- ⑧ ログ属性の変更 → M-SET
- パラメータ
- 管理対象=ログ
- ⑨ ログ属性の検索 → M-GET
- パラメータ
- 管理対象=ログ
- ⑩ ログに関する事象報告
- f u r t h e r s t u d y

3.3.5 管理情報構造

OSI管理では、管理情報を取得・変更することにより、管理対象を監視・制御する。これに対してSMI (P14 10BBB)では個々の管理情報の定義と、管理情報に対する種々操作方法に対する共通の原則を規定

→ 「管理情報タイプ」

(1) 管理情報タイプ

- ① 状態
- ② 設定不可カウンタ
- ③ 設定可能カウンタ
- ④ ゲージ
- ⑤ タイドマーク
- ⑥ カウンタ閾値
- ⑦ ゲージ閾値
- ⑧ 定義済み事象
- ⑨ レポート制御
- ⑩ ログ制御
- ⑪ ログ

(2) 管理情報 (例)

- ◎ データリンク層 (LLC)
 - ・ 最大LLC情報領域サイズ
 - ・ 送／受信XIDコマンド数
 - ・ 送／受信XID応答数
 - ・ 送／受信試験コマンド数
 - ・ 送／受信試験応答数
 - ・ 活性中コネクション数
 - ・ 全コネクション数

- ・ 送／受信 I, FRMR, RRRNR, REJ, SAMEUA, DISC, DM, 数
- ・ e t c.

◎ ネットワーク層

(コネクションレス)

- ・ PDU生存時間
- ・ 最大NSDU長
- ・ 破棄PDU数
- ・ 送／受信PDU数
- ・ 送／受信PDUセグメント数

(パケット)

- ・ ウィンドウサイズ
- ・ 発／着呼チャネルに割当可能のLCN最大値／最小値
- ・ 最大パケット長
- ・ 送／受信REJ, リセット, リスタート数
- ・ e t c.

◎ トランスポート層

- ・ 不活性時間
- ・ ローカル再送時間
- ・ ローカルACK時間
- ・ 最大再送数
- ・ 輻輳拒否コネクション数
- ・ チェックサムエラーTPDU数
- ・ 最大TPDU長
- ・ 送／受信TPDU数
- ・ 再送TPDU数
- ・ 送受信TPDUオクテット数

- ・ 再送TPDUオクテット数
- ・ クラス, クレジット, 等
- ・ e t c .

Managed Object=Modem xyz	
state, E backup, user,	} Generic attributes
Alarm Report, Loop Back Test,	} Generic Actions & Events
baudrate, vendor, serial no.,	} object-class- specific attributes
dialback, begin- analogue - loopback- test	} object-class- specific Actions and Events

↑

↓

defined by
SMFA(GDML)

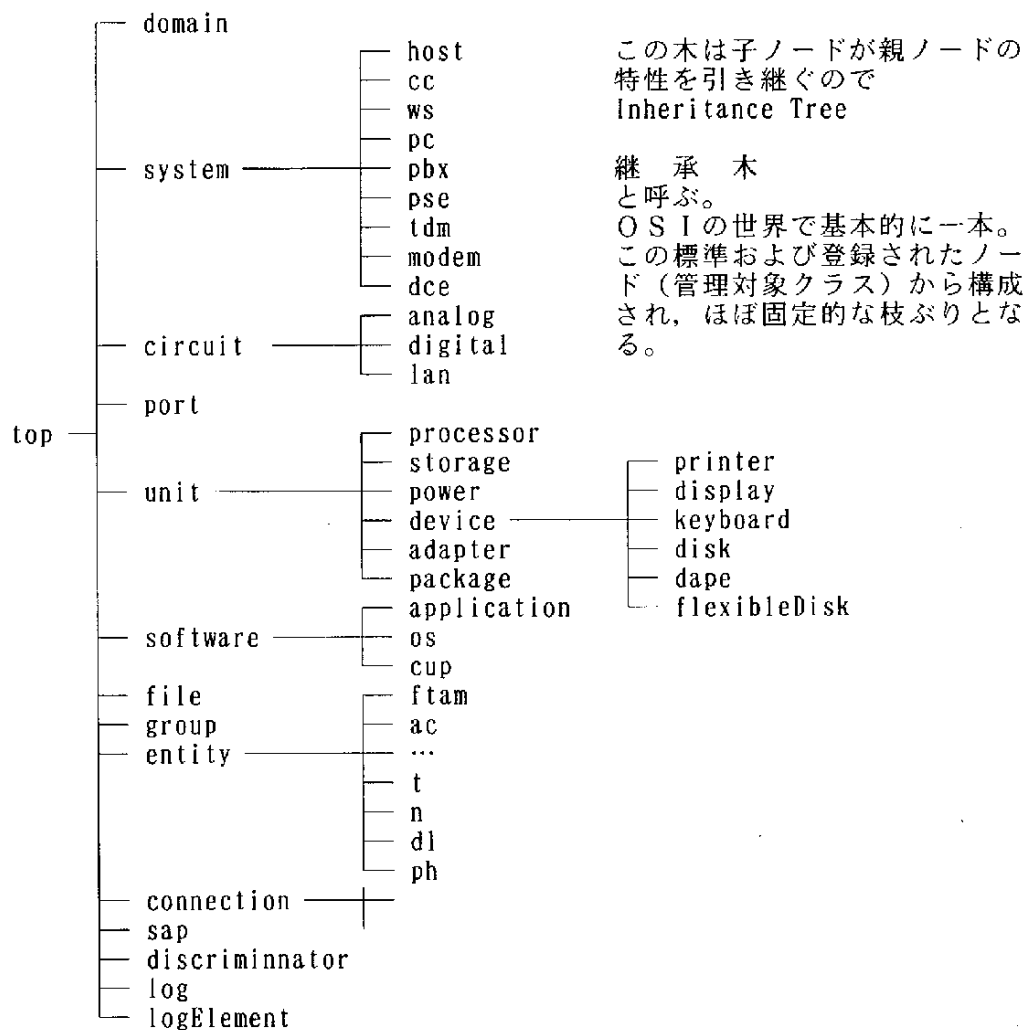
defined by
object-specifiers
(layer groups,
CCITT study
group)

図 3.25 Managed Object Class Template
as lodged with GDM1

(3) 一般定義

① 一般管理対象クラス

N612 : シドニー会議への日本からの寄書より



② 管理対象の体系

O S I 管理では、管理対象のインスタンスを指定する命令規則は、図 2. 4 で示す方法を取っている（現在の案であり決定ではない）。

例えばOBJECT-CLASSの定義として

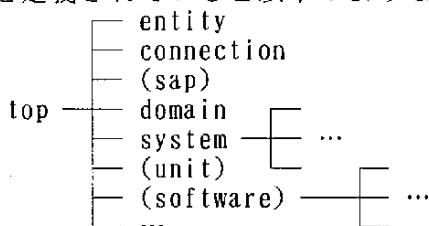
```
domlan OBJECT-CLASS
  SUBCLASS OF top
  POSSIBLE SUPERIORS (root, domain)
  NAMES                (domainID)
  ::=4

system OBJECT-CLASS
  SUBCLASS OF top
  POSSIBLE SUPERIORS (root, domain)
  NAMES                (systemID)
  ::=5

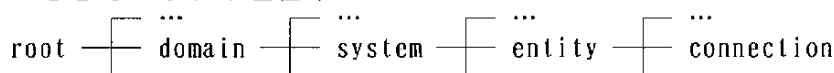
entity OBJECT-CLASS
  SUBCLASS OF top
  POSSIBLE SUPERIORS (system, entity)
  NAMES                (entityID)
  ::=1

connection OBJECT-CLASS
  SUBCLASS OF top
  POSSIBLE SUPERIORS (entity)
  NAMES                (connectionID)
  ::=2
```

と定義されていると以下のような継承木が定義されたことになる。



このとき考えられる包含木は



などがあり、あるセッションコネクションを識別するために管理対象クラス domain, system, entity, connectionそれぞれのインスタンスをOBJECT-CLASS マクロのNAMES で指定されたAttributeType の組で区分する。

((domainID, xxxx)), (systemID, yyyy)), ((entityID, session)), ((connectionID, zzzz)))

ISO 標準の場合は、この値を

```
ObjectInstance ::= CHOICE(
  distinguishedName [ 2 ] IMPLICIT DistinguishedName.
```

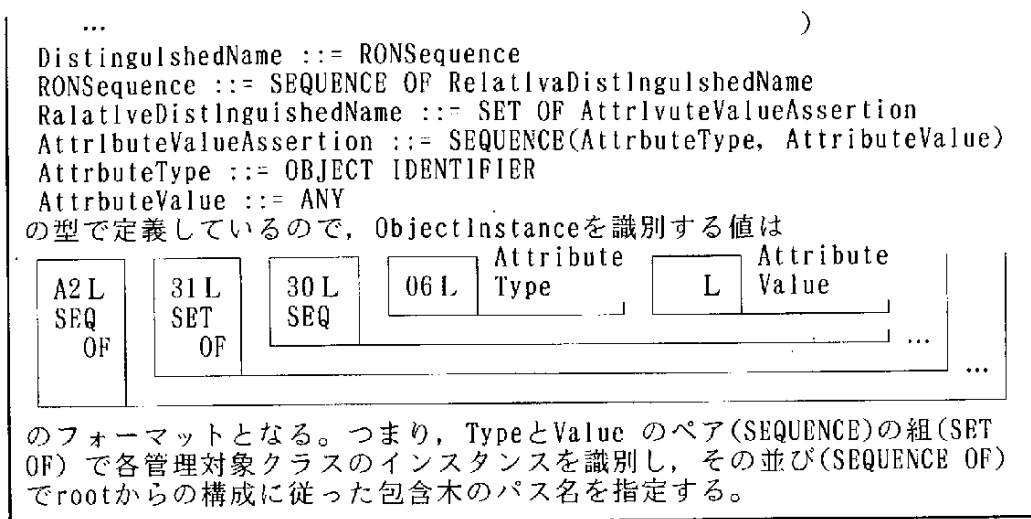


図 3.26 O S I 管理における管理対象インスタンス識別方法

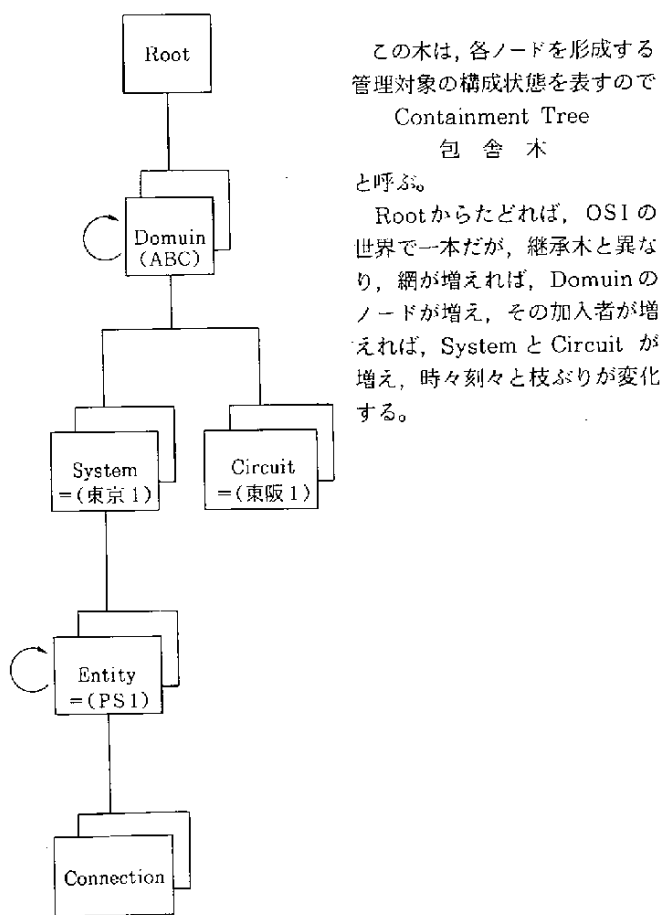


図 3.27 M I T - N a m e

② 一般事象

N613：シドニー会議への日本からの寄書より

<u>事象タイプ</u>	<u>パラメータ</u>
equipment Malfunction(装置異常)	重度 エラー情報 バックアップ 他の情報
software Error (ソフトエラー)	同上
operation Error(操作エラー)	同上
error Connection Rejection (拒否)	同上
error Disconnection(エラー切断)	同上
alarm(警告)	重度 閾値情報 バックアップ 他の情報
repaired (修復)	修復情報 他の情報

③ 一般属性

N614：シドニー会議への日本からの寄書より

<u>属性タイプ</u>	<u>構文</u>
objectClass(管理対象クラス)	OIS
entityID (エンティティ識別子)	CESS
connectionID (コネクション識別子)	CESS
userEntityID (利用者エンティティ識別子)	CESS
providerEntityID (提供者エンティティ識別子)	CESS

domainID (ドメイン識別子)	CESS
systemID (システム識別子)	CESS
circuitID(回線識別子)	CESS
portID (ポート識別子)	CESS
unitID (ユニット識別子)	CESS
componentID(コンポーネント識別子)	CESS
fileID (ファイル識別子)	CESS
groupID(グループ識別子)	CESS
discriminatorID(ディスクリミネータ識別子)	CESS
logID(ログ識別子)	CESS
eventID(事象識別子)	GTS
administrativeState(運用状態)	ASS
operationalState (操作状態)	OSS
outgoingConnectionEstablished(発呼)	CS
outgoingConnectionEstablishedThreshold (発呼閾値)	CTS
serviceUser(サービス利用者)	DNS

CESS ::= CHOICE {TeletexString, PrintableString}

CS ::= INTEGER

CTS ::= SEQUENCE {thresholdlevel [0] INTEGER,
 comparisonValue [1] INTEGER}

ASS ::= INTEGER {locked(0), unlocked(1), shuttingDown(2) }

OSS ::= INTEGER {disabled(0), enabled(1), active(2),
 busy(3)}

3.4 OSI管理プロフィール

OSI管理は、他のプロトコルとは異なり管理の意味合いが強い点を考慮すると、プロトコルと管理対象（管理情報）の2方向のプロフィール体系が必要となる。プロトコルプロフィールにおいては、システム管理機能が実現できる機能レベルにより体系化するのが妥当である。また、管理情報については、実際に仕様する網の種類などに応じて決定されるべきである。これらを考慮した結果、OSI管理プロフィール体系は、図3.28のようになるべきであろう。OSI管理実装時には、AP51とAP52の組合せでプロフィールを指定することになる。

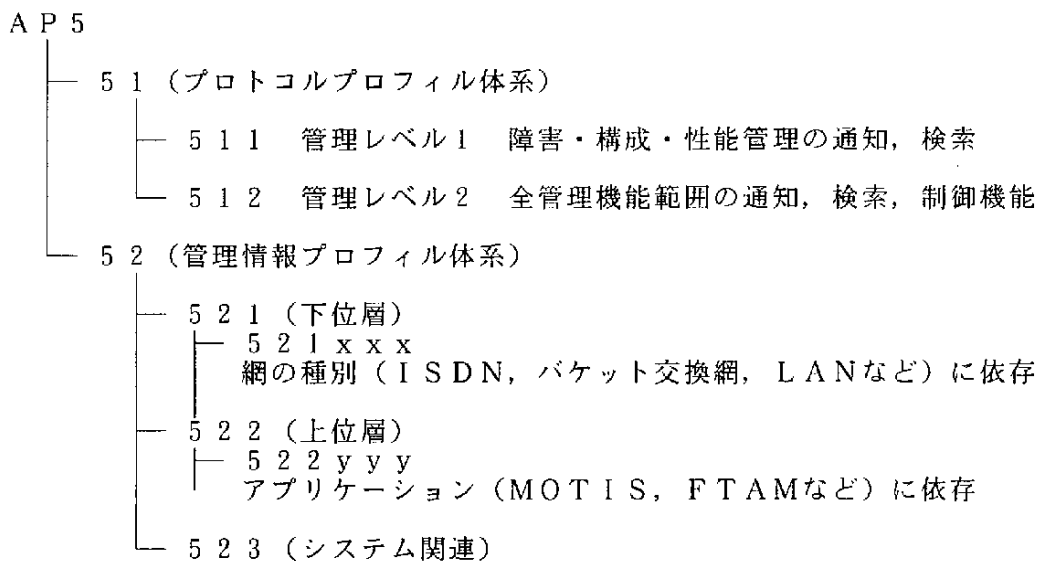


図3.28 理想的なOSI管理プロフィール体系

AP521yyyについては、下位4層（物理，データリンク，ネットワーク，トランスポート）を縦割りにした現実に仕様されているネットワーク形態ごとに管理オブジェクト／管理情報をプロフィール化する。また，AP522yyyについては，上位3層の各プロトコル単位（FTAM，MOTISなど）に管理オブジェクト／管理情報をプロフィール化する。

ただし管理レベルの分類については，レベル訳を含め利用者に分かりやすい分類（一つとなる場合も含め）を目指し今後検討していく予定である。

第 4 章 ネットワーク管理に関する

アンケート調査結果

第4章 ネットワーク管理に関するアンケート調査結果

ネットワーク管理に関するアンケート調査結果

本アンケート調査は、(財)日本情報処理開発協会産業情報化推進センター内に設置のOSIユーザー懇談会参加企業120社を対象に実施した。

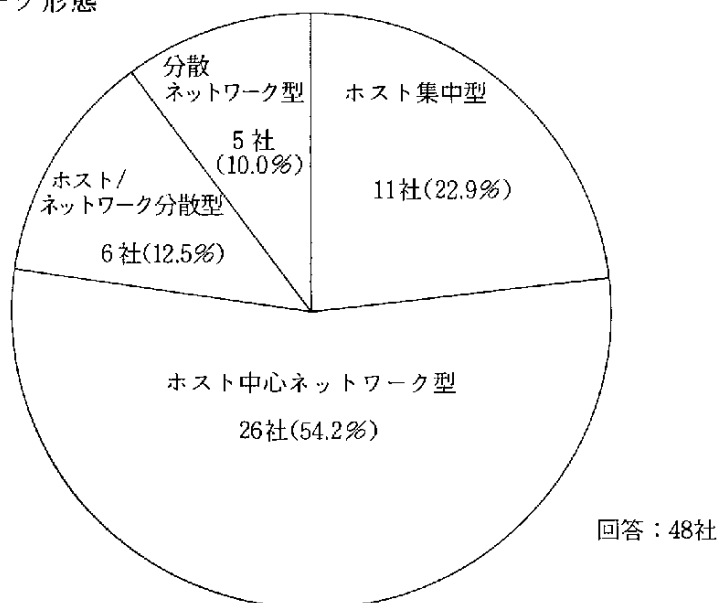
調査期間は、平成元年2月14日～3月3日、回答企業48社（回収率40％）の概要は以下の通りである。

業 種	回答社数		VANサービスの登録	社 数
建 設 業	2	→	① 特 別 第 2 種	2
製 造 業	16		② 一 般 第 2 種	15
商 業・流通業	6		③ 登録していない	31
金 融・保険業	3			
運 輸 業	1			
電力・ガス・水道業	3			
情報処理・情報通信業	12			
その他サービス業	3			
官公庁・団体	2			
計	48			

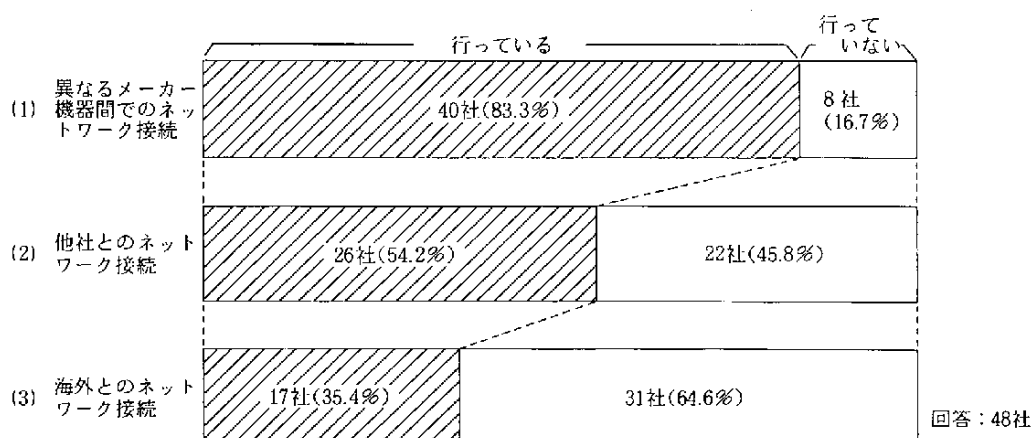
VAN事業の実施	社 数
① 行っている	7
② 関連会社に対してのみ行っている	8
③ 行っていない	2

ネットワークシステムの状況

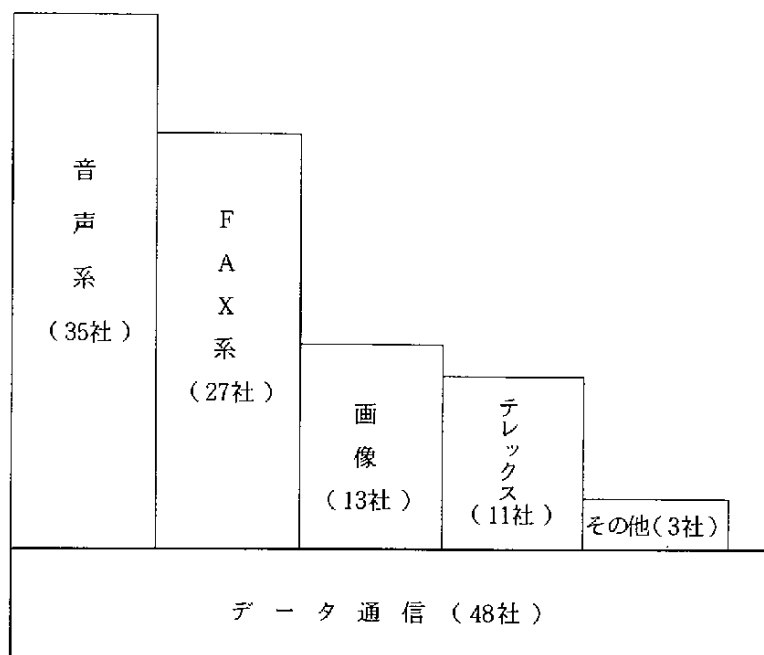
(a) ネットワーク形態



(b) 接続形態



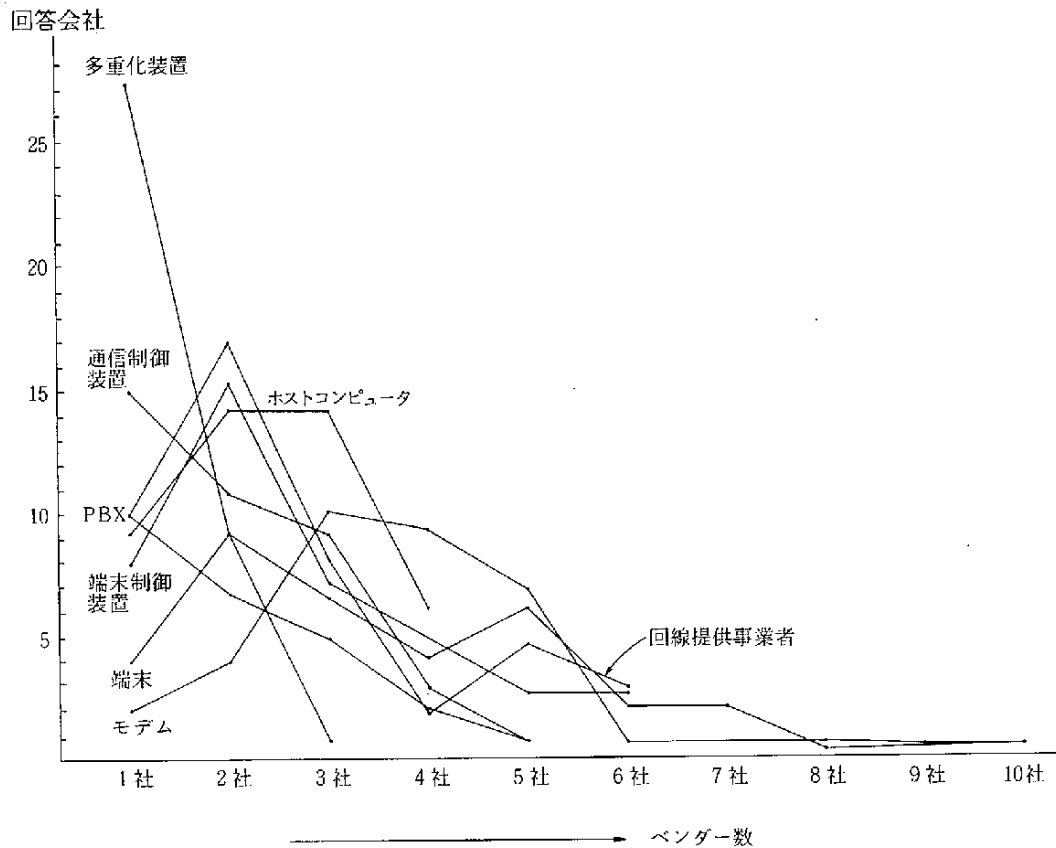
ネットワークの統合



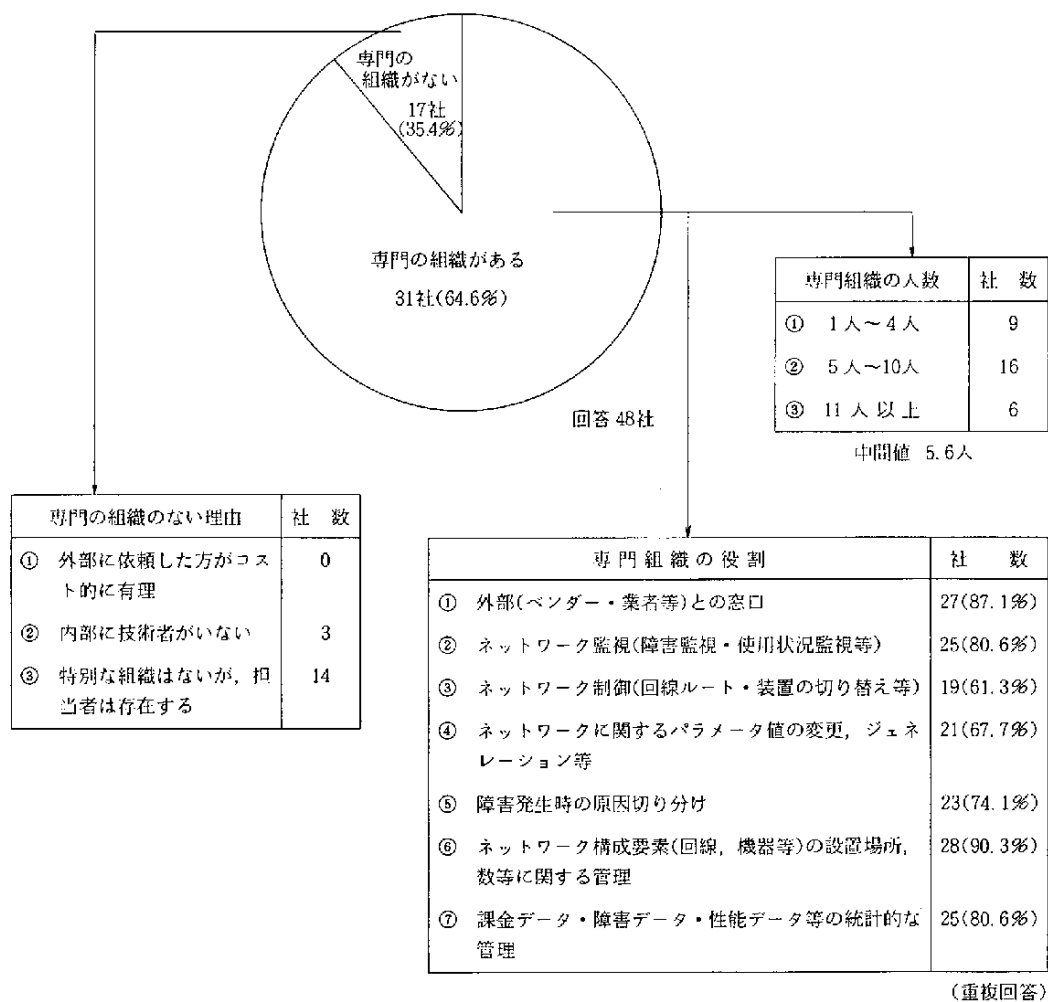
(注) 本図は、データ通信をベースに回答37社の統合しているものを個別にカウントしたもの。

従って、複数の統合の組合せを現わすものではない。

ネットワーク構成の異種性



ネットワーク運用管理のための専門組織

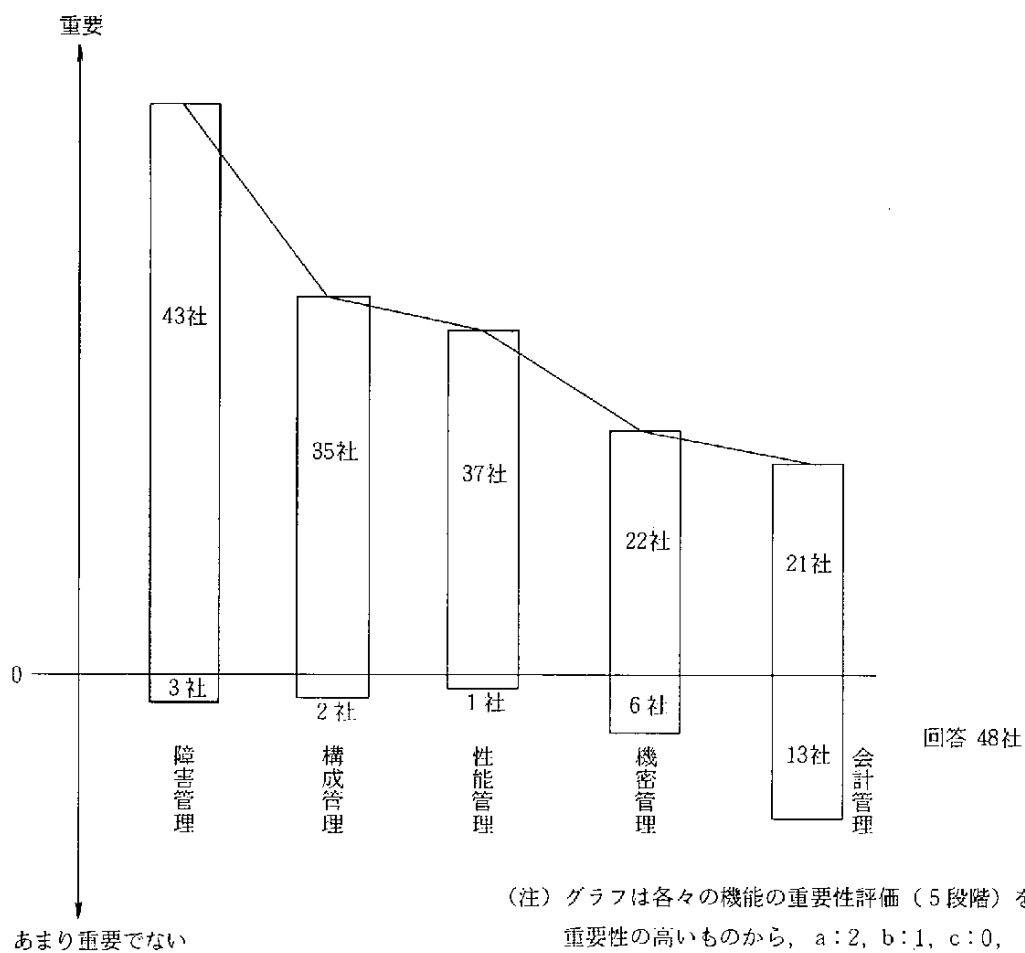


ネットワーク構成機器の管理主体

	情報処理部門 (ネットワーク運用 管理部門等)	非情報処理部門 (総務部門, ユーザー部門)	外部の業者 (メーカー, ベーター等)	
ホストコンピュータ	45 社	2 社	1 社	回答 48 社
通信制御装置	42 社	2 社	1 社	" 45 社
パケット交換機	14 社	5 社		" 19 社
多重化装置	34 社	4 社	3 社	" 41 社
モデム	46 社	2 社	1 社	" 46 社
P B X	16 社	20 社	3 社	" 39 社
回線(データ)	43 社	3 社	2 社	" 48 社
回線(音声)	22 社	20 社	2 社	" 44 社
構内回線	30 社	17 社	1 社	" 48 社
D A D	10 社	4 社	1 社	" 15 社
L A N	28 社	4 社		" 32 社
端末制御装置	39 社	5 社	2 社	" 46 社
端 末	37 社	7 社	2 社	" 46 社

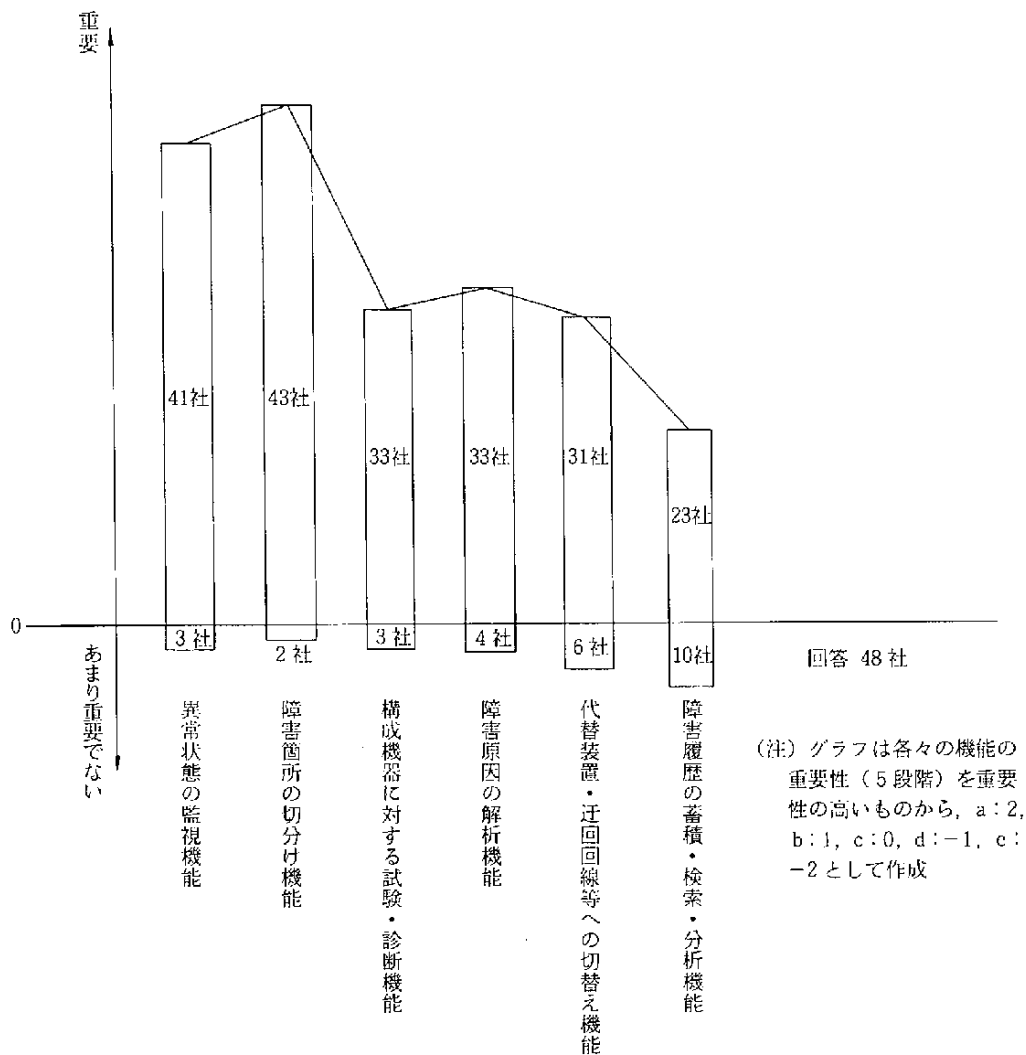
(注) 斜線は管理の主体が総務部門である
傾向が強いもの

ネットワーク管理機能の重要性



(注) グラフは各々の機能の重要性評価 (5段階) を
重要性の高いものから, a:2, b:1, c:0,
d:-1, e:-2として作成

障害管理における機能の重要性評価



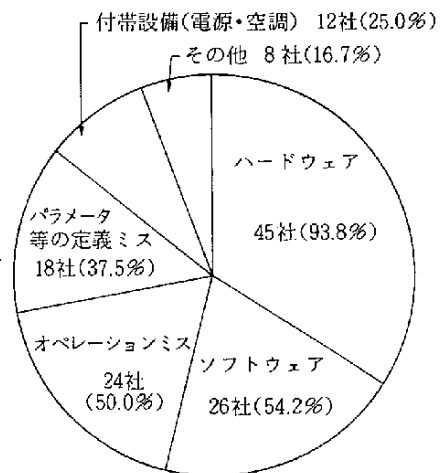
障害の現状

(障害発生が多いネットワーク構成機器)

ネットワーク構成要素	社 数
① ホストコンピュータ	17
② 通信制御装置	5
③ パケット交換機	2
④ 多重化装置	4
⑤ モデム	25
⑥ P B X	1
⑦ 高速デジタル回線	16
⑧ 回線 (⑦を除く)	35
⑨ 構内回線	4
⑩ L A N	3
⑪ 端末制御装置	9
⑫ 端 末	22

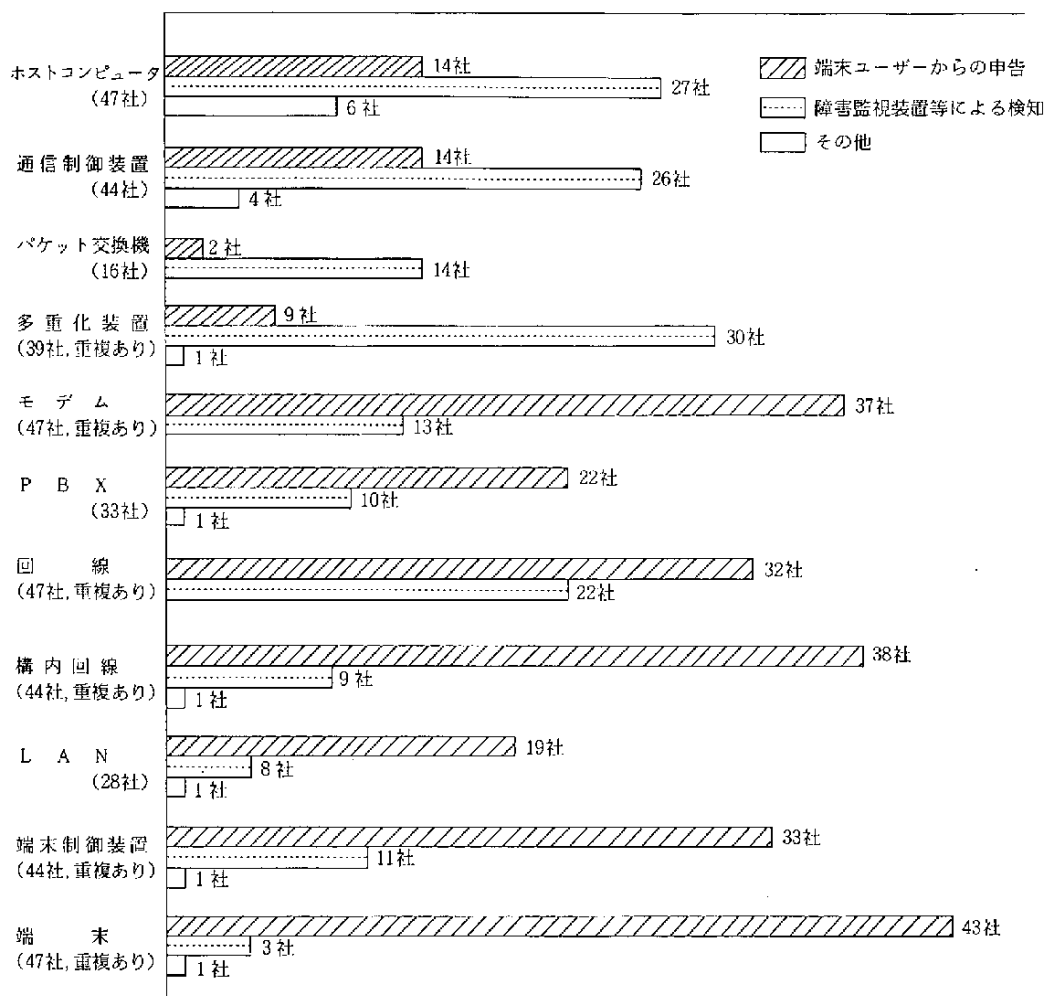
回答48社 (但し、3つの選択による重複回答)

(障害の主な原因)

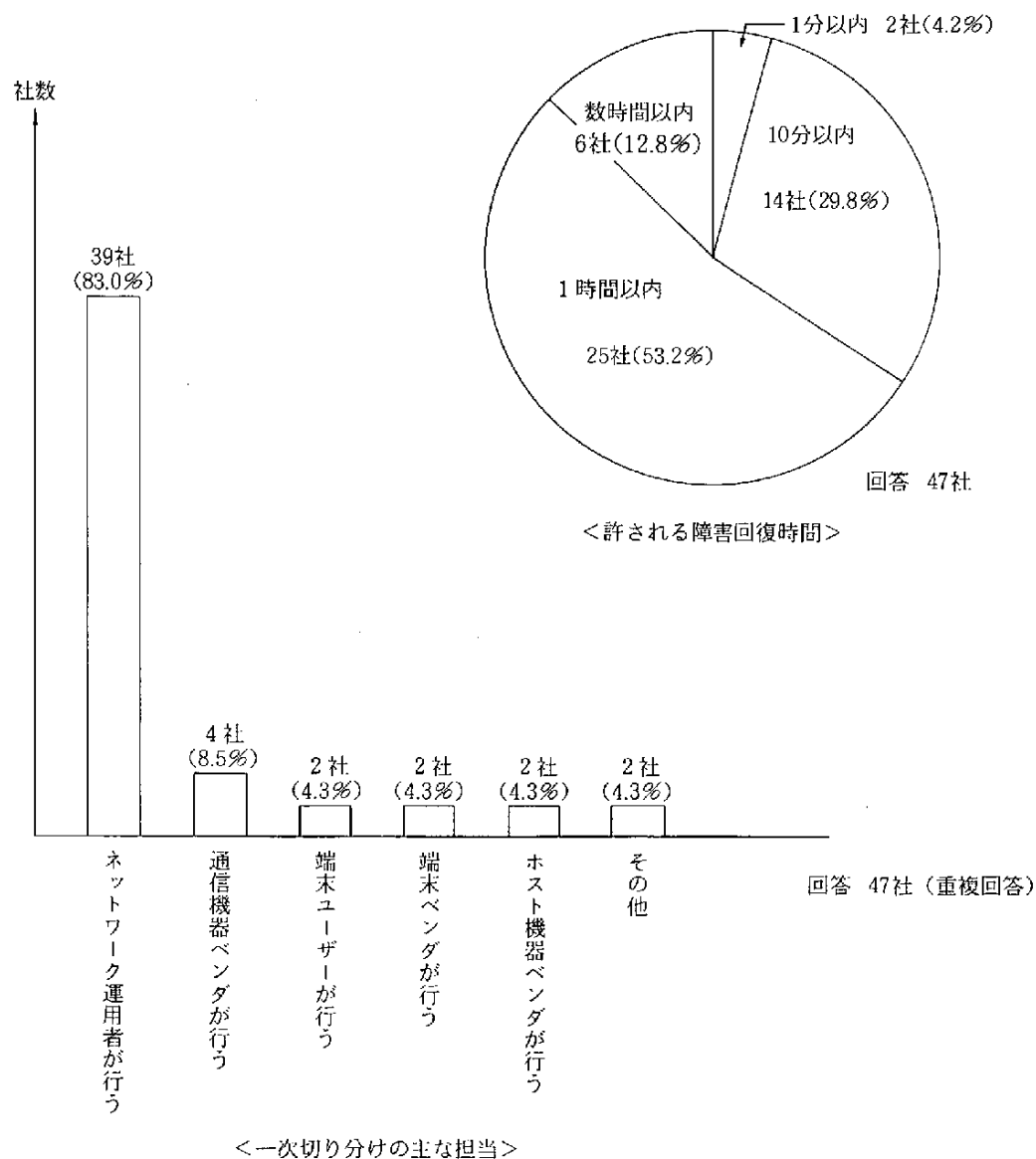


回答48社 重複回答

障害発生を検知

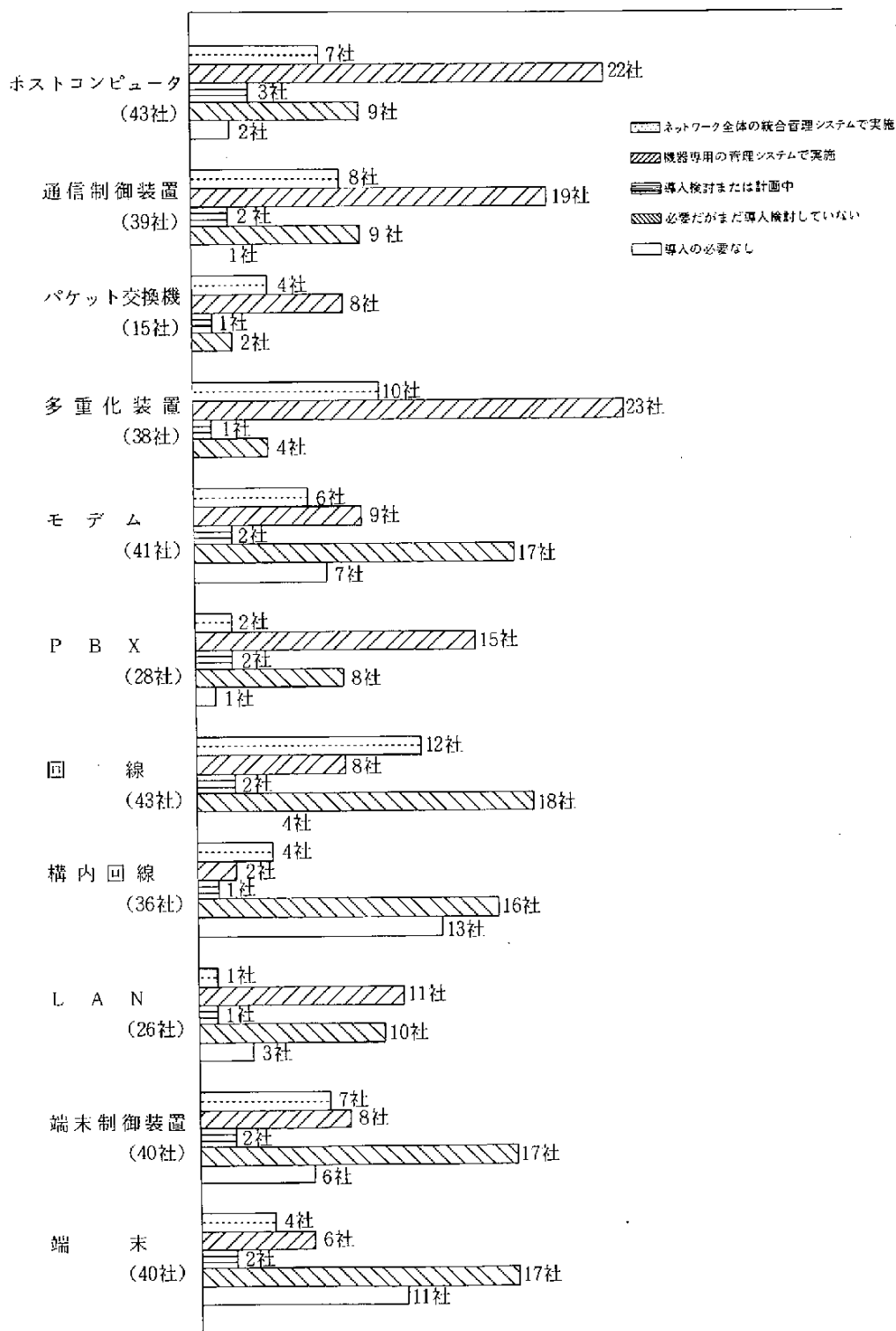


障害箇所判定のための一次切り分けと許される回復時間



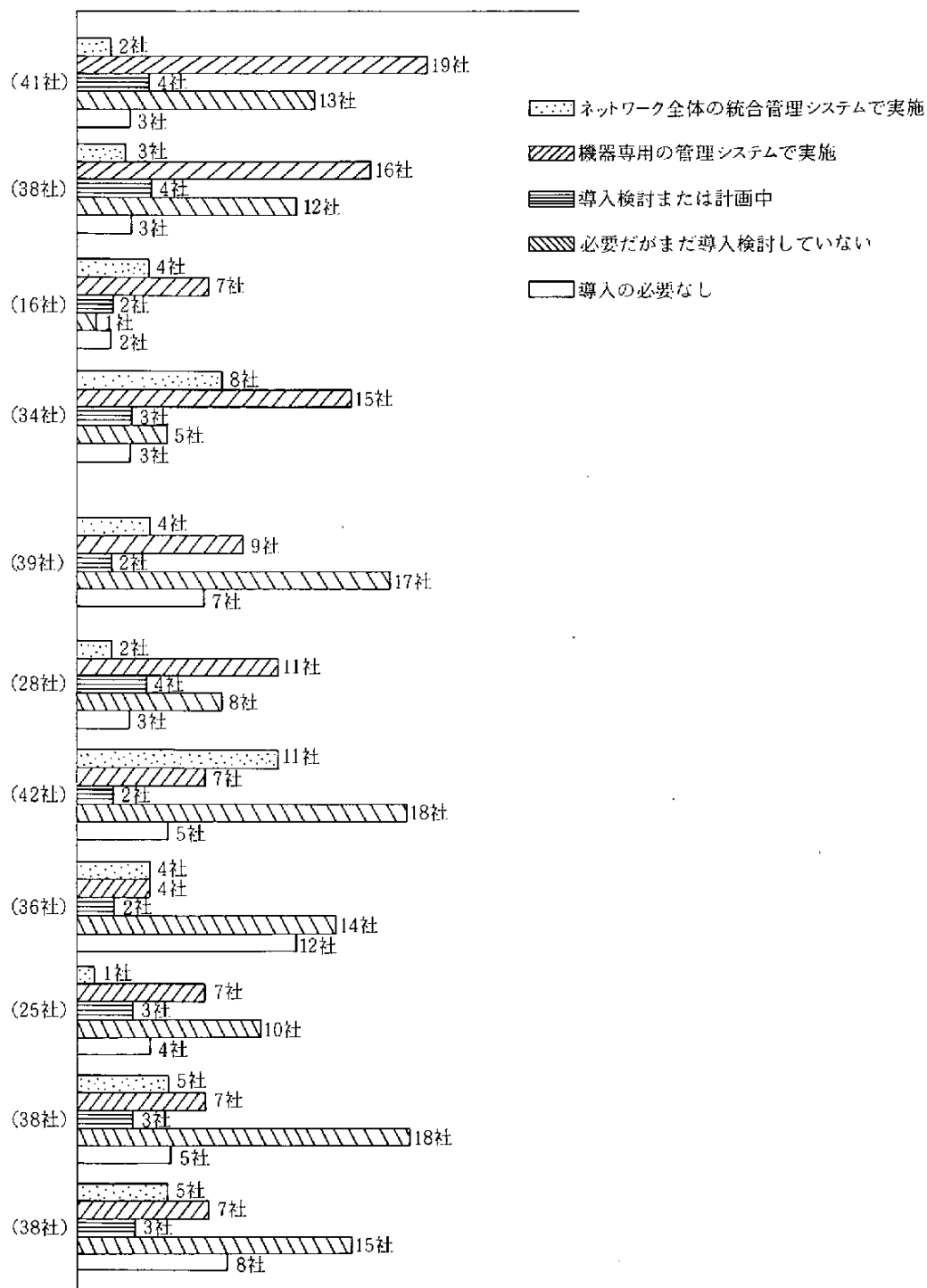
障害監視システムおよび障害診断システムの導入状況

<障害監視システム>

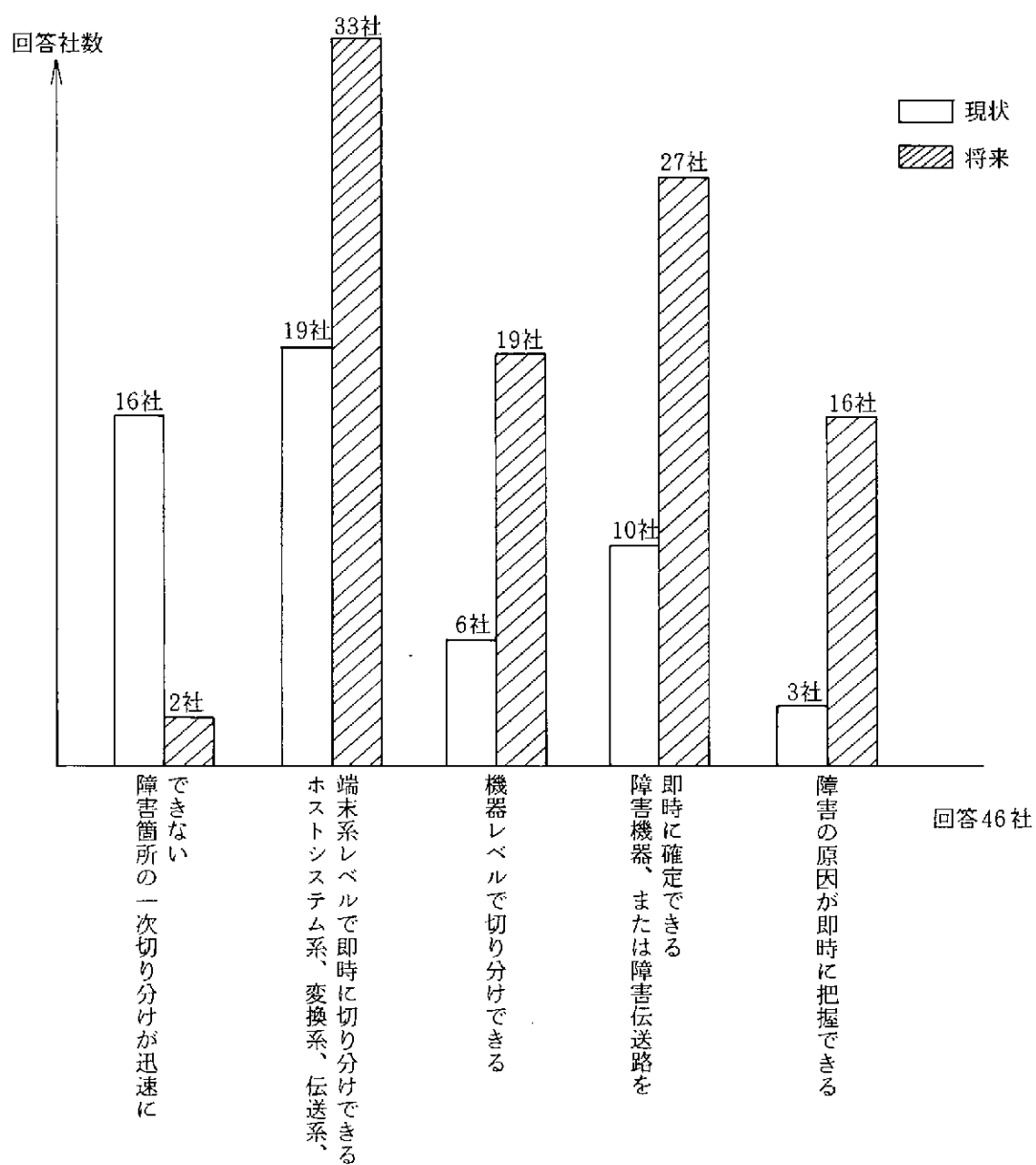


障害監視システムおよび障害診断システムの導入状況

<障害診断システム>



障害発生時、障害箇所判定のための一次切り分けのレベル



ネットワーク構成情報の管理状況

対象機器等 管理 対象となる情報	端 末 (回答47社)	端末制御 装置 (回答44社)	LAN (回答27社)	回 線 (回答44社)	モデム (回答44社)	センター 機器 (回答44社)	その他 構成情報 (回答30社)
1. 設置場所 ／ 住所	46 34 12(33)	41 35 6(29)	25 23 2(14)	42 34 8(28)	44 36 8(30)	42 35 7(28)	25 23 2(18)
2. 担当者 ／連絡先	42 36 6(27)	39 36 3(22)	27 25 2(13)	38 35 3(22)	38 34 4(24)	37 35 2(22)	24 24 0(16)
3. パー 提供者 ／連絡先	44 39 5(28)	42 38 4(26)	27 25 2(14)	40 35 5(26)	41 36 5(27)	41 37 4(26)	24 23 1(18)
4. 機種 ／モデル等	42 31 11(33)	40 32 8(33)	22 20 2(14)	33 27 6(23)	38 31 7(28)	41 34 7(29)	23 20 3(19)
5. ソフト 名称等	31 25 6(26)	31 28 3(21)	21 19 2(12)	21 19 2(15)	20 18 2(15)	33 28 5(24)	21 19 2(17)
6. 契約情報	38 29 9(27)	36 29 7(24)	22 19 3(12)	34 28 6(21)	33 28 5(19)	36 29 7(23)	20 17 3(16)
7. プロ等	40 32 8(28)	35 29 6(23)	23 18 5(15)	30 26 4(17)	29 23 6(20)	32 28 4(22)	23 20 3(18)
8. 回線種別	33 28 5(26)	37 33 4(24)	23 22 1(13)	44 38 6(29)	30 27 3(21)	30 27 3(22)	23 22 1(18)
9. 伝送経路	37 33 4(24)	32 30 2(23)	23 22 1(13)	37 34 3(24)	28 26 2(21)	29 26 2(21)	20 19 1(18)
10. 接続端末 ／システム	43 37 6(25)	34 31 3(23)	22 21 1(12)	31 29 2(22)	29 27 2(21)	29 25 4(22)	20 19 1(17)
11. 接続回線	38 34 4(24)	37 35 2(23)	24 23 1(13)	34 32 2(23)	31 29 2(23)	28 28 0(19)	21 20 1(17)
12. 保 守 ／作業日時	— —	— —	— —	— —	— —	— —	10 9 1(9)
13. 休 日 計画等	— —	— —	— —	— —	— —	— —	10 10 0(8)
14. 変 更 ／障害履歴	— —	— —	— —	— —	— —	— —	11 10 1(10)

注) 1.

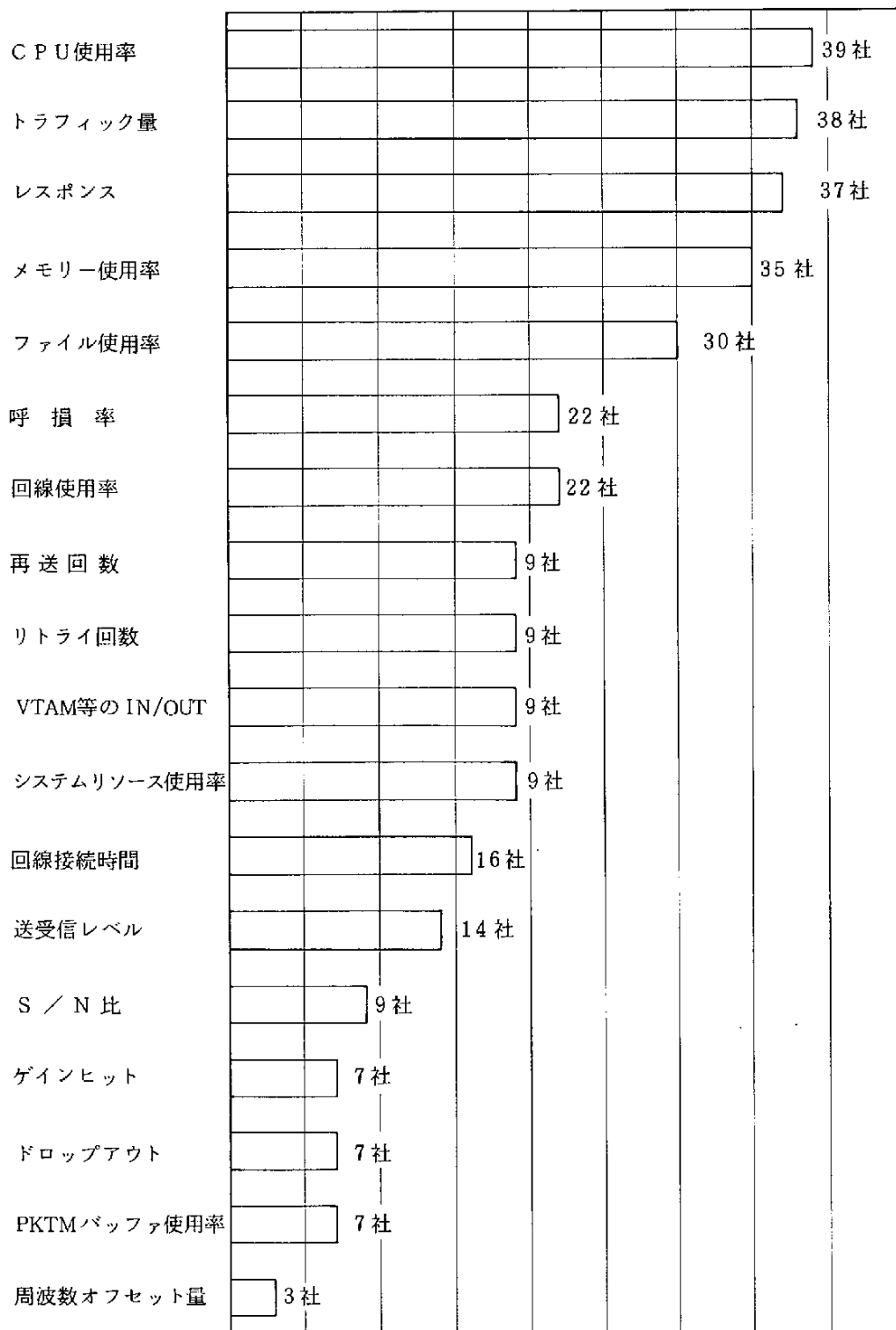


注) 2. () の数字は将来DB化して管理したいとする企業数

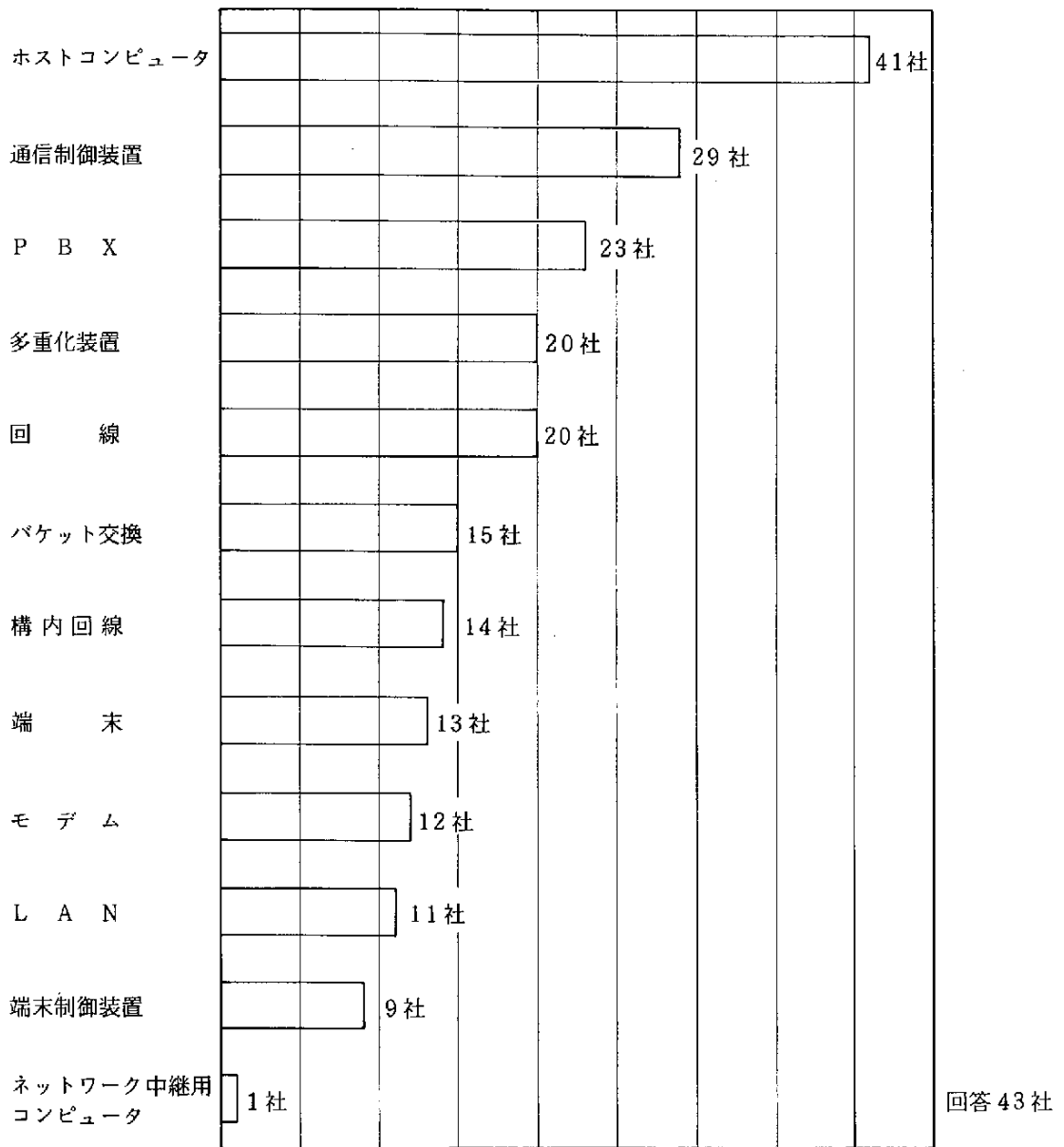
構成要素のバックアップ

	バックアップの必要性なし	重要部分二重化構造、手動切替え	重要部分二重化構造、隠患、自動検出、自動切替え	完全二重化構造、隠患、自動検出、自動切替え	その他	
ホストコンピュータ	12社(29.3%)	13社(31.7%)	6社(14.6%)	6社(14.6%)	3社(7.3%)	41社
通信制御装置	12社(29.3%)	12社(29.3%)	4社(9.7%)	7社(17.0%)	3社(7.3%)	41社
バケット交換	6社(33.3%)	3社(16.7%)	3社(16.7%)	6社(33.3%)		18社
多重化装置	11社(28.9%)	6社(15.8%)	12社(31.6%)	2社(5.3%)	4社(10.5%)	36社
モ デ ム	25社(61.0%)		8社(19.5%)	1社(2.4%)	6社(14.7%)	41社
P B X	14社(46.7%)	3社(10.0%)	8社(26.7%)	3社(10.0%)	2社(6.7%)	30社
回 線	18社(42.9%)	11社(26.2%)	3社(7.1%)	2社(4.8%)	3社(7.1%)	42社
構内回線	27社(71.1%)		4社(10.5%)	1社(2.6%)	5社(13.2%)	38社
L A N	17社(60.8%)		3社(10.7%)	3社(10.7%)	1社(3.6%)	28社
端末制御装置	25社(62.5%)		8社(20.0%)	1社(2.5%)	5社(12.5%)	40社
端 末	33社(80.5%)			4社(9.8%)	3社(7.3%)	41社

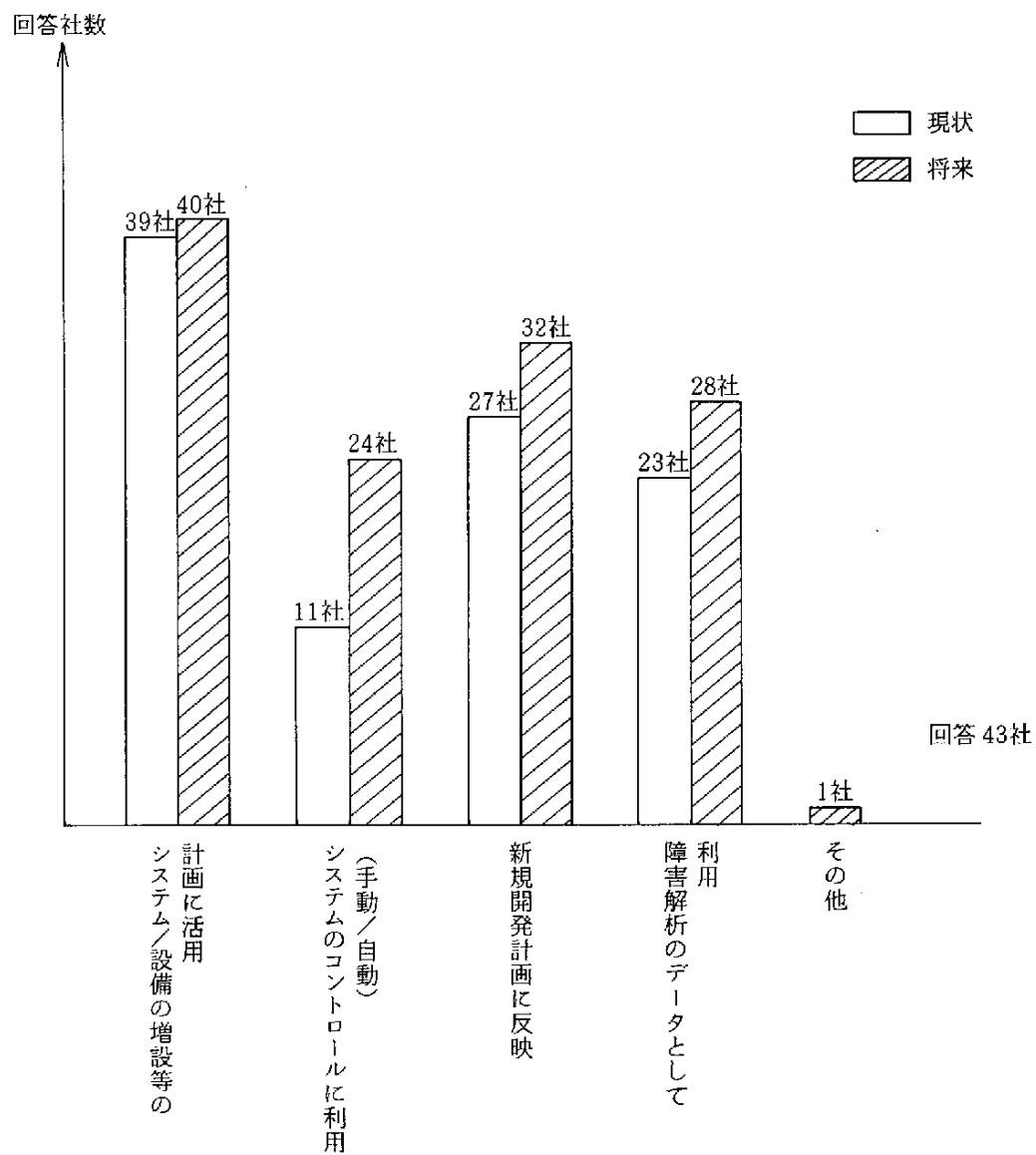
性能管理をおこなうための主な対象項目



性能管理をおこなっている対象機器



性能管理で収集・解析したデータの活用

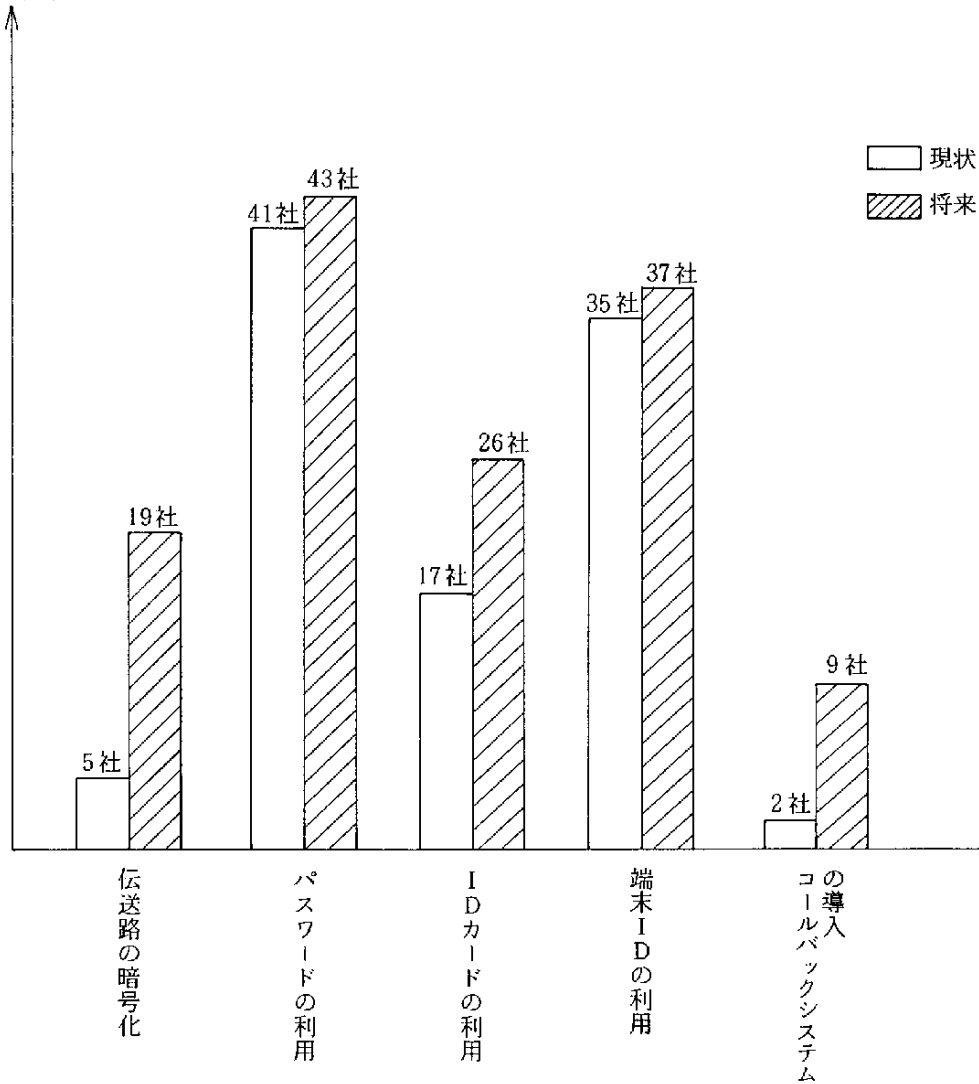


構成変更の方法

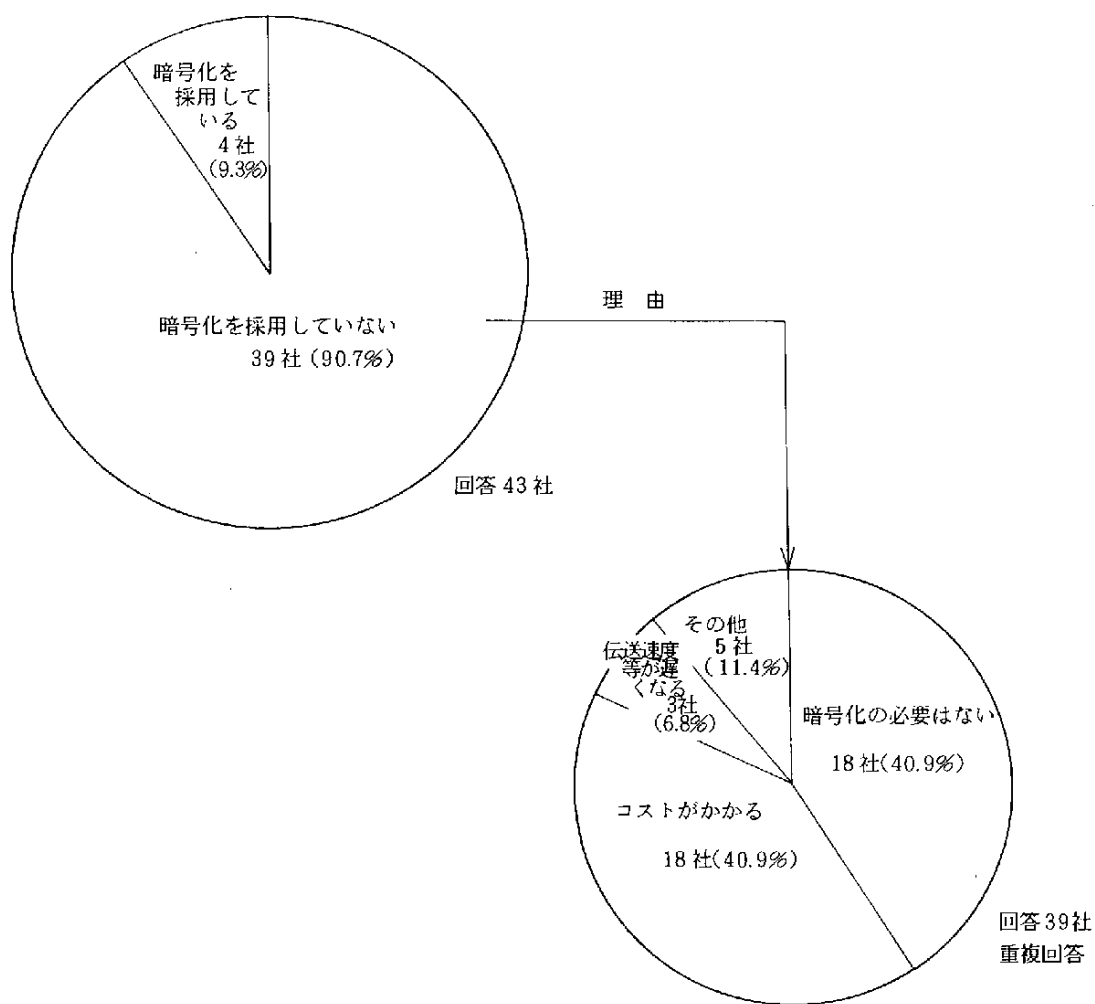


機密管理の方法

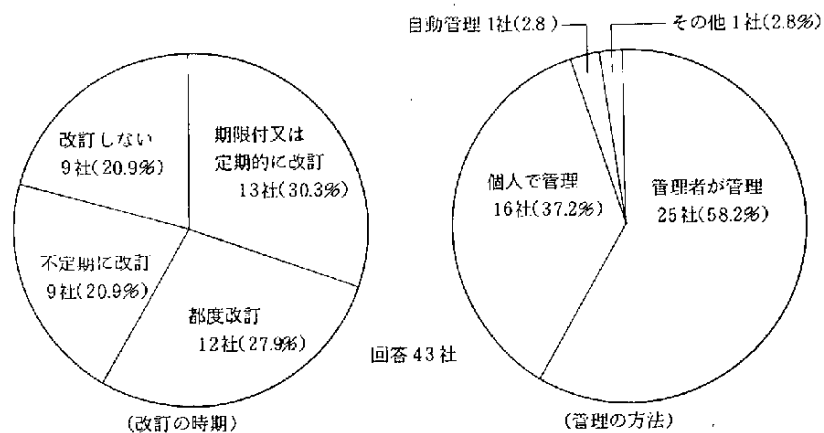
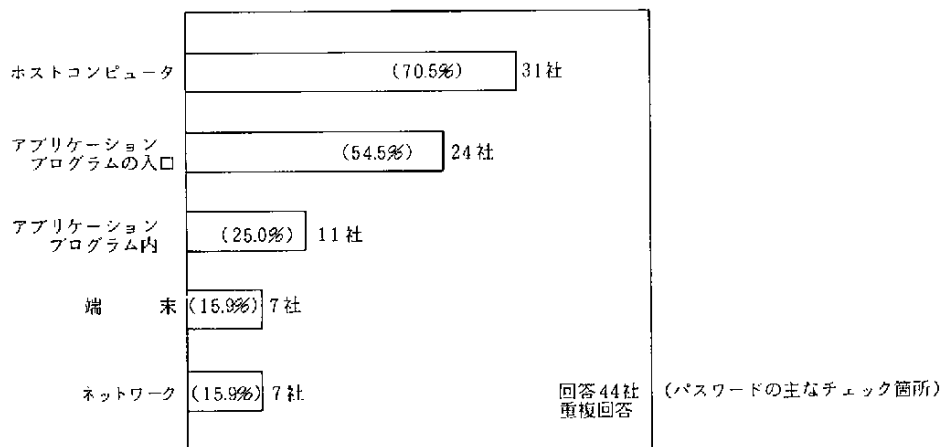
回答社数



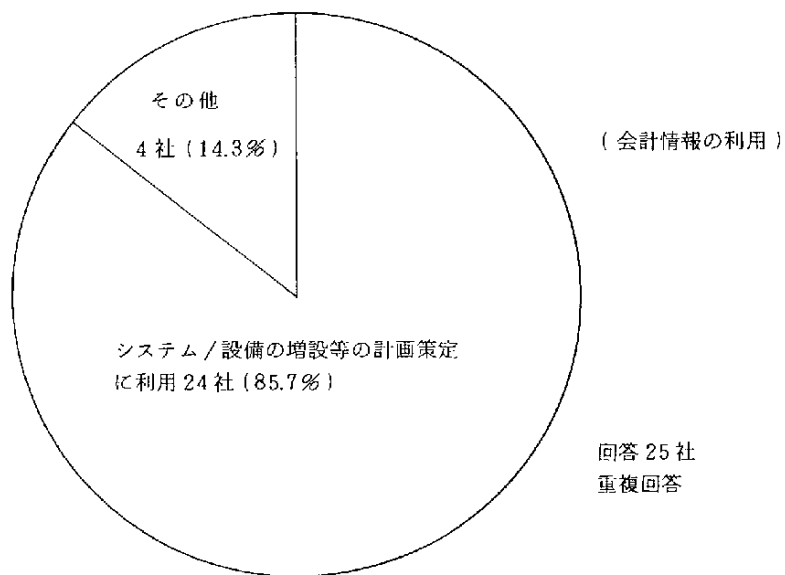
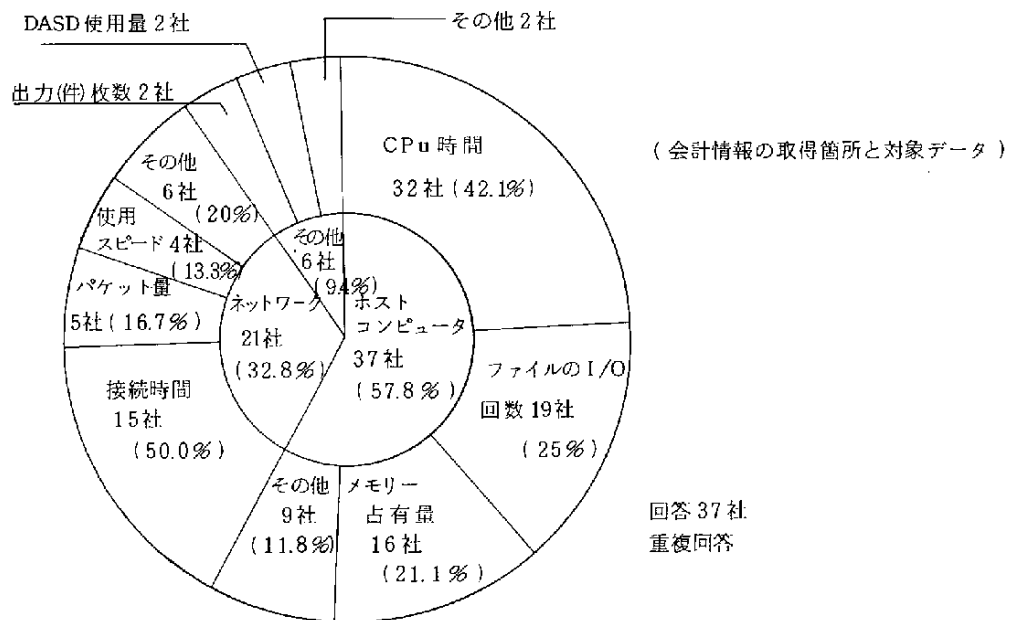
暗号化の採用状況



パスワードのチェック及び管理方法



会計情報の取得箇所とデータ利用

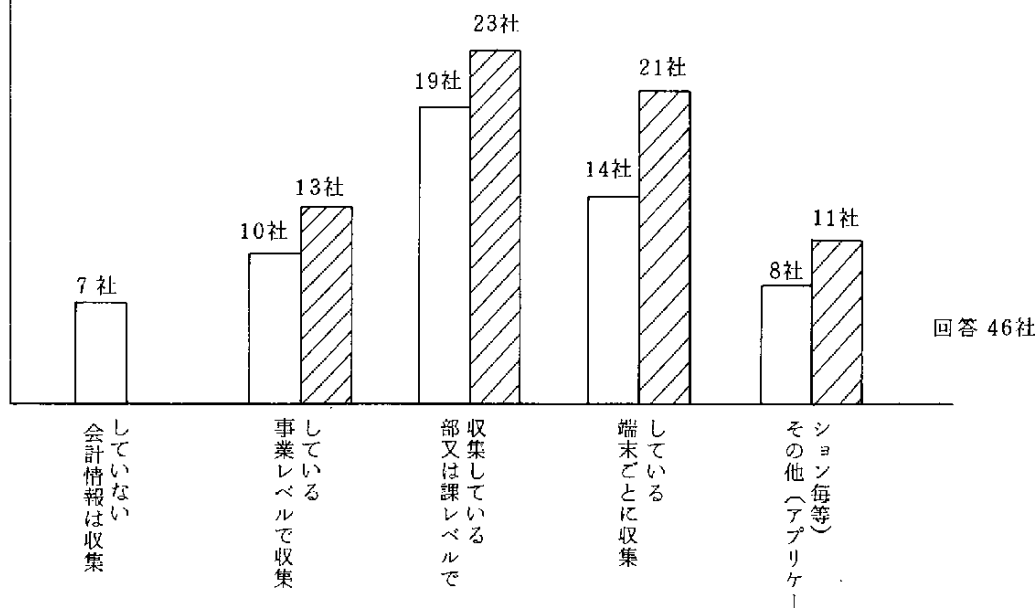


会計情報と課金の単位

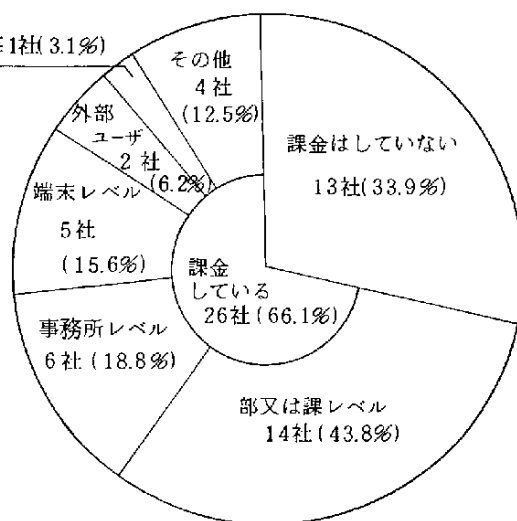
回答回数

(会計情報の収集単位)

□ 現状
▨ 将来



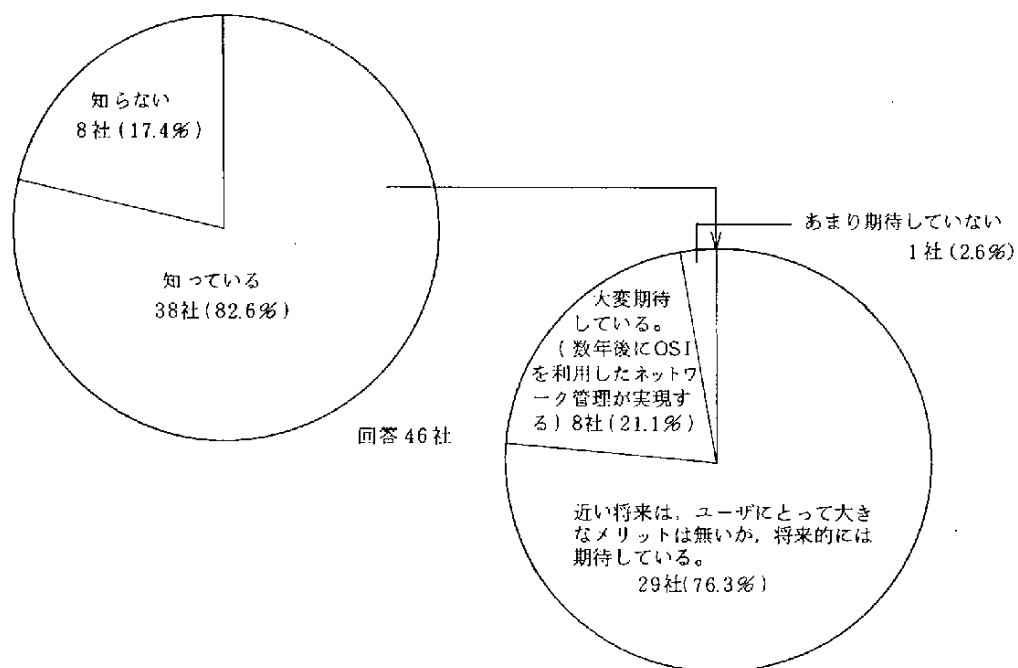
アプリケーション毎1社(3.1%)



回答 39 社
重複回答

(課金の単位)

OSI 管理の知名度とユーザの期待



(参 考) ネットワーク管理に関する

アンケート調査表

ネットワーク管理に関するアンケート

I. 貴社の概要についてご記入下さい

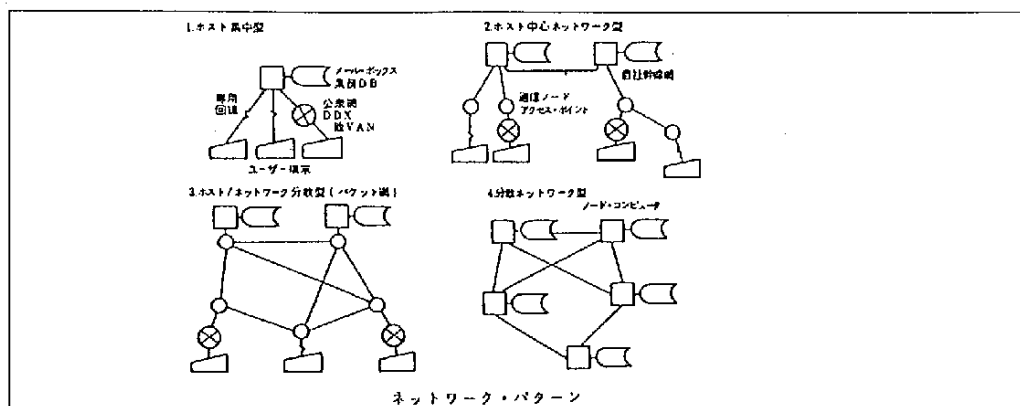
会社(団体)名			
業種	1. 農林水産業・鉱業 2. 建設業 3. 製造業 4. 商業・流通業 5. 金融・保険業 6. 運輸業 7. 電気・ガス・水道業 8. 情報処理・情報通信業 9. その他サービス業 10. 官公庁・団体		
資本金	百万円	年間売上高	百万円
従業員数	人	内情報システム部門	人
VANサービスの登録	1. 特別第2種 2. 一般第2種 3. 登録していない	実際にはVAN事業は	1. 行っている 2. 関連会社に対してのみ行っている 3. 行っていない

注) 情報通信部門が関連会社として独立しており、かつその関連会社における業務の多くの部分が独立前の会社のものである場合は、両社をあわせて一つの組織と考えて、以下の質問にご回答下さい。

II. 貴社のネットワークについて、ご記入下さい

1. 貴社のネットワークの形態は全社的に見た場合、下図の中でどのタイプにあてはまりますか。最も近い番号に○をつけて下さい。

1. ホスト集中型
2. ホスト中心ネットワーク型
3. ホスト/ネットワーク分散型(パケット網)
4. 分散ネットワーク型



2. 接続形態についてお答え下さい。

(1) 異なるメーカーの機器間で、ネットワーク接続を行っていますか。

1. 行っている
2. 行っていない

(2) 他社のネットワークと接続を行っていますか。

1. 行っている
2. 行っていない

(3) 海外のネットワークと接続を行っていますか。

1. 行っている
2. 行っていない

3. 貴社のネットワークではデータ通信の他に、どのようなものを統合していますか。
下記の中からいくつでも結構ですので、○をつけて下さい。

1. 音声系
2. FAX系
3. 画像
4. テレックス
5. その他 ()

4. 貴社で現在使用している国内の回線数を記入して下さい。

広 域 網								LAN ※ ₁	
常域品目		符号品目		高速デジタル		公衆データ通信		方式	数
種別	回線数	種別	回線数	種別	回線数	種別	回線数		
3.4KHZ	本	1,200bps	本	64Kbps	本	DDX-C	本	トークリング	
48 KHZ	本	2,400bps	本	192Kbps	本	DDX-P	本	トークバス	
200 KHZ	本	4,800bps	本	384Kbps	本	DDX-TP	本	CSMA/CD (イーサネット)	
		9,600bps	本	768Kbps	本	電話回線	本		
				1.5Mbps	本			その他	
				3 Mbps	本				
				6 Mbps	本				

※₁ LANについてはホストコンピュータ系のネットワークに接続されたもののみを対象として下さい。
またその数については

トークンリング→リングの数
トークンバス→論理的なリングの数
CSMA/CD→セグメントの数 } を記入して下さい。

5. 利用している回線提供事業者（NTT・NCC）、及びVAN業者の数をご記入下さい。

(1) 回線提供事業者 _____ 社

(2) VAN業者 _____ 社

6. 貴社のネットワークに接続されている下記の機器について、その接続数・ベンダー数をご記入下さい。

機 器	接続数	ベンダー数
ホストコンピュータ	台	社
通信制御装置	台	社
パケット交換機	台	社
多重化装置	台	社
モデム		社
PBX	台	社
PAD	台	社
端末制御装置		社
端末		社

7. 貴社のネットワークのサービス時間は、以下のいずれにあてはまりますか。最も近い番号に○をつけて下さい。

1. 原則として365日、24時間サービス
2. 月に何回かサービスを停止する
3. 週に何回かサービスを停止する
4. 毎日、何時間かサービスを停止する

8. ネットワーク管理は、一般に次のような管理機能から構成されていますが、貴社の現状にあわせて考えてみた場合、

各々の管理機能の重要性を5段階で評価して下さい。

	1 3 5
(1) 障害管理	あまり重要でない ----- 大変重要である
(2) 構成管理	-----
(3) 性能管理	-----
(4) 機密管理	-----
(5) 会計管理	-----

Ⅲ. 貴社のネットワーク管理体制についてご記入下さい

1. ネットワーク運用管理のための、専門の組織はありますか。

1. ある
2. ない

(1) 専門の組織がある場合、以下の質問にお答え下さい。

① その人数は何人ですか _____ 人

② その役割は何ですか。以下の中からいくつでも結構ですので、○をつけて下さい。

1. 外部（ベンダー・業者等）との窓口
2. ネットワーク監視（障害監視・使用状況監視等）
3. ネットワーク制御（回線ルート・装置の切り替え等）
4. ネットワークに関するパラメータ値の変更 ジェネレーション等
5. 障害発生時の原因切り分け
6. ネットワーク構成要素（回線・機器等）の設置場所・数等に関する管理
7. 課金データ・障害データ・性能データ等の統計的な管理

(2) 専門の組織がない場合、その理由は何ですか。最も大きな理由に○を付けて下さい。

1. 外部に依頼した方がコスト的に有利
2. 内部に技術者がいない
3. 特別な組織はないが、担当者は存在する
4. その他（ _____ ）

2. 次にあげる機器については、主としてどこで管理していますか。 下の番号の中から1つ選んで、表に記入して下さい。

1. ネットワーク運用管理の専門部署
2. その他の情報処理部門
3. ユーザ部門
4. その他の部門（例、総務部門）
5. メーカー・ベンダー
6. メーカー・ベンダー以外の専門業者

機 器	管理部門	機 器	管理部門
ホストコンピュータ		回線（データ）	
通信制御装置		回線（音声）	
パケット交換機		構内回線	
多重化装置		PAD	
モデム		LAN	
PBX		端末制御装置	
		端末	

IV. 障害管理に関して伺います。

1. 障害管理に関しては、以下のような機能が想定されています。

貴社の現状にあわせて考えてみた場合、各々の機能の重要性を5段階で評価して下さい。

(1) ネットワークの異常状態の監視機能	あまり重要でない	1	3	5	大変重要である
(2) 障害箇所の切り分け機能					
(3) ネットワーク構成機器に対する試験・診断機能					
(4) 障害原因の解析機能					
(5) 代替装置・迂回回線等への切り替え機能					
(6) 障害履歴の蓄積・検索・分析機能					

2. 貴社のネットワークにおける障害の現状についてお尋ねします。

(1) 貴社のネットワークでは、以下のネットワーク構成要素に分けたばあい障害発生が多いのは何ですか？

多い物から3つを選んでその番号をご記入下さい。

1. _____ 2. _____ 3. _____

ネットワーク構成要素の選択肢

- ① ホストコンピュータ ② 通信制御装置 ③ パケット交換機 ④ 多重化装置（デジタル回線用）
⑤ モデム（アナログ回線用、含TDM付） ⑥ PBX ⑦ 高速デジタル回線 ⑧ 回線（⑦を除く）
⑨ 構内回線 ⑩ LAN ⑪ 端末制御装置 ⑫ 端末 ⑬ その他（ ）

(2) またその原因は主として何ですか？

多いものから3つを選んでその番号をご記入下さい。

1. _____ 2. _____ 3. _____

選択肢

- ① ハードウェア ② ソフトウェア ③ オペレーションミス ④ パラメータ等の定義ミス
⑤ 付帯設備（電源、空調） ⑥ その他（ ）

3. 貴社のネットワークでは、障害の発生を主としてどのように検知していますか？構成要素ごとにその検知方法を選択肢の番号でご記入下さい。

構成要素	検知方法
ホストコンピュータ	
通信制御装置	
パケット交換機	
多重化装置	
モデム	
P B X	
回線	
構内回線	
L A N	
端末制御装置	
端末	

・検知方法の選択肢・

- ① 端末ユーザーからの申告
- ② 障害監視装置等による検出
- ③ その他（回答欄に具体的に記入して下さい）

4. 貴社ではネットワーク障害発生時、障害箇所判定のための一次切り分けは主として誰が行っていますか？

該当する番号に○を付けて下さい。

- ① 端末ユーザーが行う。
- ② ネットワーク運用者が行う。
- ③ 回線提供事業者が行う。
- ④ 端末ベンダが行う。
- ⑤ 通信機器ベンダが行う。
- ⑥ ホスト機器ベンダが行う。
- ⑦ その他（ ）

5. 貴社のネットワークの業務に与える影響を考えた場合、許される障害回復までの時間はどの程度ですか。

主要な業務についてお答え下さい。

- (1) 1分以内
- (2) 10分以内
- (3) 1時間以内
- (4) 数時間以内
- (5) 1日以内

6. 貴社では以下のネットワーク構成要素で障害監視システムおよび障害診断システムを導入していますか？

ネットワーク構成要素ごとに該当する番号を指定して下さい。

構成要素	障害監視システム	障害診断システム
ホストコンピュータ		
通信制御装置		
パケット交換機		
多重化装置		
モデム		
PBX		
回線		
構内回線		
LAN		
端末制御装置		
端末		

選択肢

- ① ネットワーク全体の統合的管理システムで実施
- ② 機器専用の管理システムで実施
- ③ 導入検討または計画中
- ④ 必要だがまだ導入検討していない
- ⑤ 導入の必要無し

7. 貴社ではネットワーク障害発生時、障害箇所判定のための一次切り分けはどのレベルまで可能ですか？ 該当する番号に○を付けて下さい。

現在 将来

- _____ ① 障害箇所の一次きりわけが迅速にできない。
- _____ ② ホストシステム系、交換系、伝送系、端末系レベルで即時に切り分けができる。
- _____ ③ 機器レベルで即時に切り分けができる。
- _____ ④ 障害機器、または障害伝送路を即時に確定できる。
- _____ ⑤ 障害の原因が即時に把握できる。

8. 貴社でネットワーク全体の統合的管理システムを導入している場合、そのシステム名をご記入下さい。

1. メーカー等の製品 (製品名: _____)
2. 独自で開発

9. 貴社では以下のネットワーク構成要素の障害時バックアップはどのようにしていますか？ 該当する番号を指定して下さい。

現在 将来

- _____ ① ホストコンピュータ
- _____ ② 通信制御装置
- _____ ③ パケット交換機
- _____ ④ 多重化装置 (デジタル回線用)
- _____ ⑤ モデム (アナログ回線用、含TDM付)
- _____ ⑥ PBX
- _____ ⑦ 回線
- _____ ⑧ 構内回線
- _____ ⑨ LAN
- _____ ⑩ 端末制御装置
- _____ ⑪ 端末

選択肢

- (1) バックアップは必要無し
- (2) 重要部分のみ二重化構造で、手動切替え
- (3) 重要部分のみ二重化構造で、障害自動検出自動切替え
- (4) 完全二重化構造で、手動切替え
- (5) 完全二重化構造で、障害自動検出自動切替え
- (6) その他 ()

10. 貴社では以下のネットワーク構成要素の定期点検、保守はどのようにしていますか？選択肢の中から最も近いものの番号を記入して下さい。（複数指定可能）

現在	将来		
_____	_____	① ホストコンピュータ	
_____	_____	② 通信制御装置	
_____	_____	③ パケット交換機	
_____	_____	④ 多重化装置（デジタル回線用）	
_____	_____	⑤ モデム（アナログ回線用、含TDM付）	
_____	_____	⑥ PBX	
_____	_____	⑦ 回線	
_____	_____	⑧ 構内回線	
_____	_____	⑨ LAN	
_____	_____	⑩ 端末制御装置	
_____	_____	⑪ 端末	

選択肢

(1) 保守契約無し

(2) 昼間、月～金曜日保守契約

(3) 24時間365日保守契約

(4) 定期点検保守契約

(5) リモート点検診断

11. 貴社では障害記録の保存・利用をどのように実施していますか。

以下の中から最も近いものに○をつけて下さい。

1. 特に何もしていない
2. 障害記録の保存を紙ベースで保存している
3. 障害記録を機械に入力し、統計をとっている
4. 障害記録を機械に入力し、統計をとると共に、障害発生時に原因分析のために利用している

12. 障害管理に関して要望事項、問題点等ございましたらお聞かせ下さい。

V. 構成管理に関して、お伺いいたします。

1. 貴社ネットワークで、下記ネットワーク構成要素の構成変更（追加・変更・削除）は、何時行いますか？該当する番号を指定して下さい。

現状	将来	
_____	_____	① ホストコンピュータ
_____	_____	② 通信制御装置
_____	_____	③ パケット交換機
_____	_____	④ 多重化装置（デジタル回線用）
_____	_____	⑤ モデム（アナログ回線用、含TDM付）
_____	_____	⑥ PBX
_____	_____	⑦ 回線
_____	_____	⑧ 構内回線
_____	_____	⑨ LAN
_____	_____	⑩ 端末制御装置
_____	_____	⑪ 端末

選択肢

- ① 毎月 ② 隔週 ③ 毎週
④ 毎日 ⑤ 随時 ⑥ その他（ ）

2. 貴社ネットワークで、下記ネットワーク構成要素の構成変更（追加・変更・削除）は、どのようにして行いますか？該当する番号を指定して下さい。

現状	将来	
_____	_____	① ホストコンピュータ
_____	_____	② 通信制御装置
_____	_____	③ パケット交換機
_____	_____	④ 多重化装置（デジタル回線用）
_____	_____	⑤ モデム（アナログ回線用、含TDM付）
_____	_____	⑥ PBX
_____	_____	⑦ 回線
_____	_____	⑧ 構内回線
_____	_____	⑨ LAN
_____	_____	⑩ 端末制御装置
_____	_____	⑪ 端末

選択肢

- ① システムの全体を停止して行う。
② システムの一部を停止して行う。
③ 該当装置の全体を停止して行う。
④ 該当装置の一部を停止して行う。
⑤ 通常の運用状態で行う。

3. ネットワーク管理においてネットワークを構成している機器の設置状況や設置状態等を管理することが必要ですが、貴社のネットワーク運用上構成情報として管理しているものは何ですか？

以下の記号を記して下さい。

例

・台帳等で管理しているものは、△ データベース化しているものは、○

・さらに将来データベース化したいものには、◎を該当欄に記入して下さい。

設置場所／住所	△	◎
---------	---	---

	端 末		端末制御装置		LAN		回 線		モデム		センター機器		その他構成管理情報	
	現状	将来	現状	将来	現状	将来	現状	将来	現状	将来	現状	将来	現状	将来
1. 設置場所／住所														
2. 担当者／連絡先														
3. マカ・提供者／連絡先														
4. 機種／モデル等														
5. ソフト名称等														
6. 契約情報														
7. アドレス等														
8. 回線種別														
9. 伝送経路														
10. 接続端末／システム														
11. 接続回線														
12. 保守／作業日時	——		——		——		——		——		——			
13. 休日計画等	——		——		——		——		——		——			
14. 変更／障害履歴	——		——		——		——		——		——			
15. その他 ()														
16. ()														
17. ()														
18. ()														

VI. 性能管理に関して伺います。

全社ネットワークの観点から、以下の質問にお答え下さい。

1. 貴社において性能管理をおこなっている対象機器について下記の該当欄に○を記入して下さい。

また今後性能管理の対象にしたいものは対象機器に○を記入して下さい。

該当する項目がない場合は⑫以降に記入願います。

(複数回答可)

	管理方法		収 集 手 段				収集タイミング				収集箇所		
	実績 管理	設計値 管理	メーカ ツール	ユーザ ツール	管理 システム	その他	常 時	定 期	随 時	都 度	セン サ	設置 場所	その他
①ホストコンピュータ													
②通信制御装置													
③パケット交換													
④多重化装置													
⑤モデム													
⑥PBX													
⑦回線													
⑧構内回線													
⑨LAN													
⑩端末制御装置													
⑪端末													
⑫													
⑬													
⑭													
⑮													
⑯													
⑰													
⑱													
⑲													
⑳													

2. 貴社において性能管理をおこなう対象項目について該当欄に○を記入して下さい。

(19以降は記載事項外の項目を記入して下さい。)
(複数回答可)

	管理方法		収 集 手 段				収集タイミング				収集箇所		
	実績 管理	設計値 管理	メーカ ツール	ユーザ ツール	管理 システム	その他	常 時	定 期	随 時	都 度	セン サ	設置 場所	その他
①トラフィック量													
②レスポンス													
③再送回数													
④リトライ回数													
⑤呼損率													
⑥送受信レベル													
⑦ゲインヒット													
⑧ドロップアウト													
⑨S/N比													
⑩周波数オフセット量													
⑪VTAM等のIN/OUT													
⑫回線使用率													
⑬CPU使用率													
⑭メモリー使用率													
⑮ファイル使用量													
⑯PKT/M/セグ使用率													
⑰システムリソース使用率													
⑱回線接続時間													
⑲													
⑳													
㉑													
㉒													

3. 貴社の性能管理で収集したデータや解析した結果などはどのように活用されていますか？

また今後どのようにしたいですか。該当する番号に○を付けて下さい。

現在 将来

- | | | |
|-------|-------|--------------------------------|
| _____ | _____ | (1) システム／設備の増設等の計画に活用している。 |
| _____ | _____ | (2) システムのコントロールに利用している。(手動／自動) |
| _____ | _____ | (3) 新規開発計画に反映する。 |
| _____ | _____ | (4) 障害解析のデータとして利用している。 |
| _____ | _____ | (5) その他 |

4. 性能管理に関して要望事項、問題点等ございましたらお聞かせ下さい。

VII. 機密管理についてお伺いいたします。

1. 貴社のネットワークの機密管理は、どのような方法で行っていますか？また、将来的にはどのような方法で行いたいと思っていますか？該当する番号に○を付けて下さい。（複数回答可）

現在	将来	
_____	_____	(1) 伝送路の暗号化
_____	_____	(2) パスワードの利用
_____	_____	(3) IDカードの利用
_____	_____	(4) 端末IDの利用
_____	_____	(5) コールバック・システムの導入
_____	_____	(6) その他（ _____ ）

2. 暗号化を採用されている方にお尋ねします。

- (1) 暗号化の対象となっているものは何ですか？該当する番号に○を付けて下さい。
（複数回答可）

- ① 回線データ
② ファイル
③ その他（ _____ ）

- (2) 暗号鍵の改訂の時期及び配布の方法はどのように行っていますか？
該当する番号に○を付けて下さい。

〈改訂の時期〉	〈配布の方法〉
① 期限付又は定期的に改訂する	① オンラインで配布する
② 不定期に改訂する	② その他（ _____ ）
③ 都度改訂する	
④ 改訂しない	
⑤ その他（ _____ ）	

3. 暗号化を採用していない方にお尋ねします。暗号化を採用していない理由は何ですか？
該当する番号に○を付けて下さい。

- ① 暗号化に時間がかかり伝送速度が遅くなるから
② 暗号化用の機器にコストがかかるから
③ 暗号化の必要はない
④ その他（ _____ ）

4. パスワードを採用されている方にお尋ねします。

(1) パスワードのチェックは、どこで行っていますか？該当する番号に○を付けて下さい。(複数回答可)

- ① 端末
- ② ネットワーク
- ③ ホストコンピュータ
- ④ アプリケーション・プログラムの入口
- ⑤ アプリケーション・プログラム内
- ⑥ その他()

(2) パスワードの改訂の時期及び管理の方法はどのように行っていますか？

該当する番号に○を付けて下さい。

〈改訂の時期〉

- ① 期限付又は定期的に改訂する
- ② 不定期に改訂する
- ③ 都度改訂する
- ④ 改訂しない
- ⑤ その他()

〈管理の方法〉

- ① 個人で管理
- ② 管理者が管理
- ③ 自動管理
- ④ その他()

5. 機密管理に関して要望事項 問題点等ございましたらお聞かせ下さい。

VII. 会計管理についてお伺いいたします。

1. 会計情報の収集の最小単位は、どのレベルですか？また、将来的にはどのレベルまで行いたいと思いますか？
該当する番号に○を付けて下さい。

現在	将来	
_____	_____	(1) 会計情報は収集していない。
_____	_____	(2) 事業所レベルで収集している。
_____	_____	(3) 部または課レベルで収集している。
_____	_____	(4) 端末ごとに収集している。
_____	_____	(5) その他 ()
_____	_____	(6) その他 ()

2. 会計情報を収集している場合、その取得箇所はどこですか？ 該当する番号に○を付けて下さい。
また、収集しているデータとしては、どのようなものがありますか？ 該当項目に○を付けて下さい。
(複数回答可)

(1) ホストコンピュータ	(① CPU時間	② メモリー占有量	③ ファイルのI/O回数
	④ その他 ()		))
(2) ネットワーク	(① 接続時間	② パケット量	③ 使用スピード
	④ その他 ()		))
(3) その他	()		)
(4) その他	()		)

3. 貴社では、ネットワークの会計情報をもとにどの単位で課金をしていますか？
該当する番号に○を付けて下さい。

(1) 課金はしていない。	
(2) 事務所レベルで課金している。	
(3) 部または課レベルで課金している。	
(4) 端末ごとに課金している。	
(5) その他 ()	)
(6) その他 ()	)

4. 貴社のネットワーク課金システムは、どのような方法で課金データを収集していますか？
該当する番号に○を付けて下さい。

- (1) 磁気テープで収集
- (2) オンラインで収集
- (3) 帳表で収集
- (4) その他 ()

5. 会計情報は、課金に使用するほか、どのようなことに利用していますか？
該当する番号に○を付けて下さい。

- (1) システム／設備の増設等の計画策定に利用している。
- (2) その他 ()

6. 会計管理に関して要望事項、問題点等ございましたらお聞かせ下さい。

IX 貴社のネットワーク管理に関して現在お困りの事、今後の課題等ございましたらなんでもお書き下さい。

X. OSIで検討している「OSIネットワーク管理」について、お答え下さい

1 現在、OSIの検討の一項目として「ネットワーク管理」があるのは御存知ですか。

- ① 知っている
- ② 知らない

2 「知っている」場合、「OSIネットワーク管理」に対するご意見に最も近いものに○をつけて下さい。

- ① 大変期待している（数年後にOSIを利用したネットワーク管理システムが実現する）
- ② 近い将来はユーザにとって大きなメリットは無いが、将来的には期待している
- ③ あまり期待していない

3 「あまり期待していない」と答えた場合、その理由は何ですか。

- ① 各ベンダーでOSI準拠の製品が主流とは思えない
- ② 現有の機器に対してまで、OSI準拠に変更することは考えられない
- ③ 将来的にも単一アーキテクチャを基本としているので、そのアーキテクチャに特化したネットワーク管理システムを考えている
- ④ その他 _____

以上で本アンケートに関する質問事項は終了です。
ご協力ありがとうございました。

——禁無断転載——

平成元年3月発行

発行所 財団法人 日本情報処理開発協会
東京都港区芝公園3丁目5番8号
機 機 振 興 会 館 内
TEL (432) 9384
印刷所 株式会社 正文社
東京都文京区本郷3丁目12番2号
TEL (815) 7271

