

コンピュータネットワーク障害解析エキスパートシステム EXNETS の設計概念

山平 拓也 桐葉 佳明 阪田 史郎
日本電気（株） C & C システム研究所

コンピュータネットワーク障害解析エキスパートシステム EXNETS (EXpert system for NEtwork TroubleShooting)は、AI 手法を用いてコンピュータネットワークで発生する障害の検出、診断、復旧を行なうシステムである。本稿では、統合ネットワーク管理システムにおける障害管理を実現する EXNETS の設計概念、システム構成、解析機能、OSI 管理に基づく分散管理形態について述べる。

EXNETS の設計に当り、専門家から障害事例やその診断方法を調査し、その手法を診断方式、知識ベースの構築に反映させた。障害解析機構を、ネットワークの機器や構成に依存しない共通的な形式で診断を行う部分と、機器や構成に固有の情報を解析する部分に分けたことにより、EXNETS の狙いであるネットワークの複雑、多様化への対処、管理システムの可搬性を実現している。

EXNETS のネットワーク管理機能は、OSI 管理に準拠した当社の C & C - DINA プロトコルに基づき、マルチベンダー対応の分散管理形態への拡張を可能にしている。

Design Principles on Network Troubleshooting Expert System EXNETS

Takauya YAMAHIRA, Yoshiaki KIRIHA and Shiro SAKATA

C&C Systems Research Laboratories, NEC Corporation

4-1-1 Miyazaki, Miyamae-ku, Kawasaki, Kanagawa, 213 Japan

This paper describes the processing configuration of EXNETS (EXpert system for NEtwork TroubleShooting), a network fault management expert system used to detect, diagnose, and recover from computer network malfunctions.

Artificial intelligence techniques are used to implement appropriate network fault analyses and to invoke proper recovery procedures. The inference mechanism comprises two modules: a Supervisor, which generates a hypothesis using hardware-independent information, and an Executor, which checks error conditions using hardware-dependent information according to Supervisor's instructions. Separating the inference mechanism into two function modules allows EXNETS to deal with a diversity of network configurations which include various types of computers and terminals.

Network management mechanisms of EXNETS, which are based on OSI management protocols, enable to manage faults in a distributed network environment.

1. はじめに

ネットワークの広域分散化、大規模化に伴い、障害が発生した場合その損失は増加し、同時にネットワーク運用、保守の複雑化がからみ、そのコストも増大する傾向にある。そのため、ネットワークを柔軟に管理するシステムの必要性が高まっている。本稿では、コンピュータネットワークを主対象とする障害解析エキスパートシステムEXNETS(EXpert system for NEtwork TroubleShooting)の設計概念、解析機構、OSI管理に基づく分散管理形態について述べる。

コンピュータネットワークを対象とするネットワーク管理としては、ISOがOSI管理として障害管理、性能管理、構成および名前の管理などの5つの機能を定義し、管理モデル、機能構成、通信プロトコルなどの国際標準化の活動を行っている[1]。EXNETSも、当社のOSI対応のC&C-DINAプロトコルに準拠し、マルチベンダー対応の分散管理形態への拡張を想定している。

コンピュータネットワーク管理システムの研究としては、IBMがホスト集中型ネットワーク管理システムNetViewと、マルチベンダー資源にも適用できNetViewとの連係機能を備えたシステムNetView/PCを構築している[2]。また伝送／交換系においては、AT&Tによるネットワーク管理アーキテクチャUNMA[3]の発表や、CCITTのTMN[4]の検討などが代表的である。

一方、AI手法を利用した故障診断の研究やシステム構築は、伝送／交換系においては最近徐々に発表されている[5]。しかし、コンピュータ系の障害をAIを利用して解析するシステムで本格的に実用に供しているものは未だ例を見ない。これは、コンピュータ系のネットワーク構成がより多様であり、ソフトウェアに関係した論理的な障害も多く含むなど障害解析に幅広い知識を必要とし、システムの実装が複雑になるなどの理由が挙げられる。この多岐にわたる障害を効率的に解析するためには、実際のネットワーク運用、管理者の診断知識を利用することが重要である。

EXNETS[6,~11]の開発にあたっては、事前にネットワーク関係者から障害とその対処の事例をアンケートにより収集し、その手法をシステム設計に反映させた。障害解析機構を、ネットワークの機器や構成に依存しない共通する形式で診断を行う部分と、機器や構成に固有の情報を解析する部分に分けることにより、EXNETSの狙いであるネットワークの複雑、多様化への対処、管理システムの可搬性の向上を実現する。

2. 設計概念

EXNETSは、AI手法を用いてコンピュータネットワークにおいて生じる障害の検出、診断、復旧を支援するシステムである。

EXNETSの特徴を以下に挙げる。

①複雑／多様化するネットワークへの対応

—— 機種独立性

機種の増加、構成の多様化、網種の違いなどにより複雑化するネットワークの障害解析を行うため、個々のネットワークに対し新しく診断機能を追加することは、今後一層困難になる。EXNETSにおいては、障害解析の中核である診断機能をネットワークに共通する基本的な診断戦略を行う部分と、ネットワーク内の機器や構成に固有の情報を基づいて解析する部分に分け、各部分における処理と相互の情報のやり取りにより、ネットワークの多様性に対処する。

図-1にEXNETSの機能構成を示す。Supervisorが基本的な診断を行い、ExecutorがSupervisorの指示に従い各資源の情報を収集し解析を行う。Supervisorがネットワークの機器や構成に依存しない形で処理を実行するように設計されているので、ネットワークの機器や構成を更新する際、Executorの知識だけを変更すればよく、また分散管理への拡張、他のネットワーク管理システムへの移植も容易になっている。

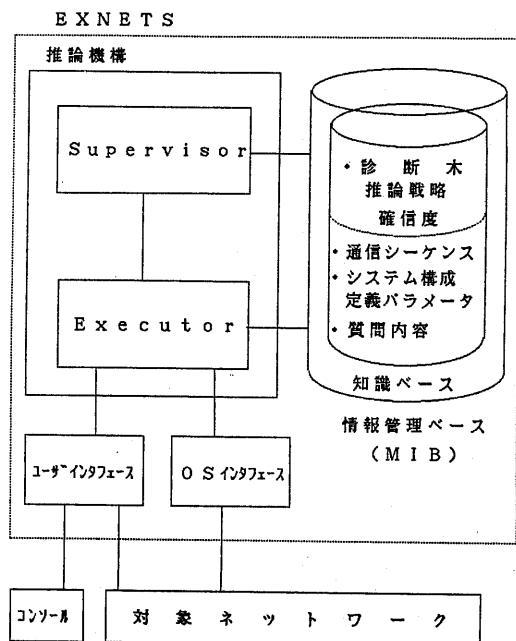


図-1 EXNETS の機能構成

②ネットワーク運用／保守専門家の知識の活用

—— A I 手法の導入

複雑、多様化するネットワークを管理するシステムには、専門家の知識を診断処理に盛り込むことが不可欠である。EXNETSでは、専門家の知識を診断木に置き換えて障害解析に利用している。診断に利用する知識は、ネットワークシステムの保守、設計などの関係者を対象とした約500件のアンケートから収集した。特に、専門家が障害発生時に採る原因究明方法や復旧方法などを調査し、診断知識に反映させている。

③標準化への対応 —— O S I 管理との整合

分散、大規模化したネットワークや、特にマルチベンダー機器を含んだネットワークを統一的に管理するためには、標準プロトコルと整合をとることが不可欠である。EXNETSはO S I 管理に基づく当社のアーキテクチャC & C - D I N Aプロトコルに準拠している。

SupervisorとExecutor間は、O S I 管理の共通管理情報サービスであるC M I Sと、そのプロトコルであるC M I Pを利用して情報交換を行い、それぞれが利用する知識は管理情報ベースM I B[1]に格納される。

EXNETSは、現在単一ホストによって管理されるネットワークを対象としているが、複数台のホストコンピュータが稼働しているネットワーク障害への対処や、マルチベンダー環境下における分散管理形態にも適用を計っている（図-2）。

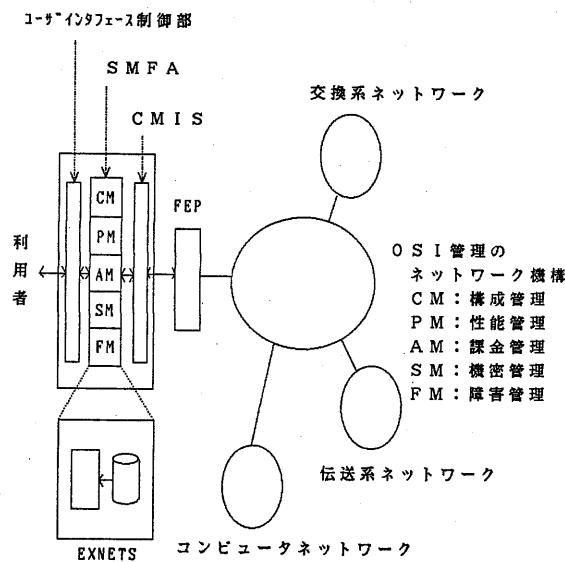


図-2 EXNETS の位置付けを示す概念図

3. システム概要

3.1 障害対象

EXNETSの解析対象を決定し、適切な障害解析機能を設計するため、ネットワーク障害の実態調査を行った。障害の症状、原因、検査方法、復旧方法、発生頻度、重要度を一応の回答項目とし、さらに備考欄、あるいはインタビューにより情報を入手した。

アンケート結果から、コンピュータネットワーク障害の原因は以下の様に分類できる。

- ①ハードウェア障害
- ②システム構成定義のパラメータの不整合
- ③オペレータの操作ミス
- ④ユーザのアプリケーションプログラムのエラー
- ⑤システムプログラムのエラー

現状では、障害のうち約80%は、1から3の原因のタイプに帰着され、EXNETSは当面これらを診断対象とする。

3.2 システム環境

本障害解析機能で対象とするシステム範囲を図-3に示す。EXNETSは、多くのネットワーク資源（ホストコンピュータ、F E P、L A N／回線、モデム、ユーザ端末など）を管理する。

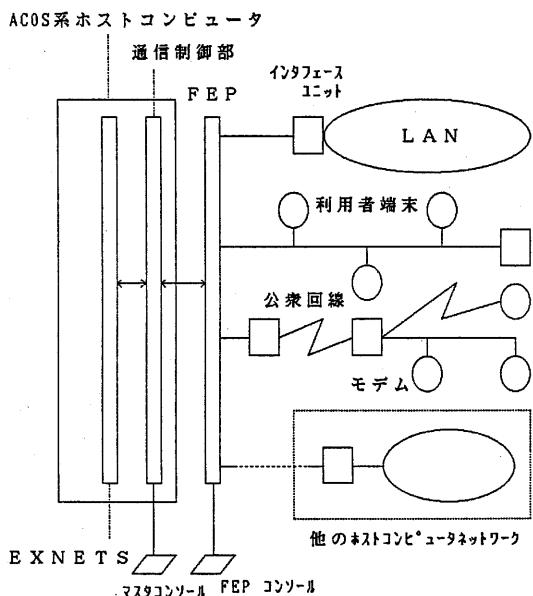


図-3 EXNETS の対象領域

EXNETS は、当社の統合ネットワーク管理システム VISION-NMS [12] の障害解析機能に組み込み、分散環境下での稼働を計る。

3.3 ユーザインタフェース

障害解析は、システムとオペレータの間でインタラクティブに行われる。EXNETS は、通常、障害に気付いたユーザやオペレータからの診断要求によって解析を開始する場合と、コンピュータシステムが自動的に障害を発見して処理を開始する場合がある。特に後者の場合は、その旨は、障害メッセージの表示とともに、自動的に EXNETS に送られる。

EXNETS は、オペレータが入力した障害状況に関する情報と、ネットワーク資源の状態や動作履歴などの自動的にネットワーク機器や記憶装置から収集した情報を利用して、障害解析を行なう。EXNETS とオペレータの間でやり取りされる情報や指示を表-1 に示す。

表-1 EXNETS とオペレータ間の情報

情報の方向	情報の内容
Operator → EXNETS	障害発生通知と診断要求 障害状況 障害前の操作内容など
EXNETS → Operator	障害状況の質問 診断内容 原因と復旧方法

これらの情報を利用して、本解析機構は原因領域を次第にしづらり、最終的に原因に対応した適切な復旧手順を選択する。EXNETS は、オペレータへ障害の原因に関する内容を報告し、可能ならば復旧手順をアドバイスする。たとえ正確な原因が検出できなくても、解析の中間結果を復旧の参考として提供する。

4. 実現方式

図-4 に EXNETS の診断手順を示す。診断手順は、初期問診、原因究明、復旧からなる。

初期問診では、EXNETS は次に示す情報を収集し、これらを利用して障害を症状のタイプに分類する。

- ① 障害メッセージ。
- ② 障害状況。発生の間欠／固定、症状の変化状況など。
- ③ 障害発生前のユーザの操作や機器構成の変更、SG 変更の有無など。

図-5 に初期問診の画面例を示す。

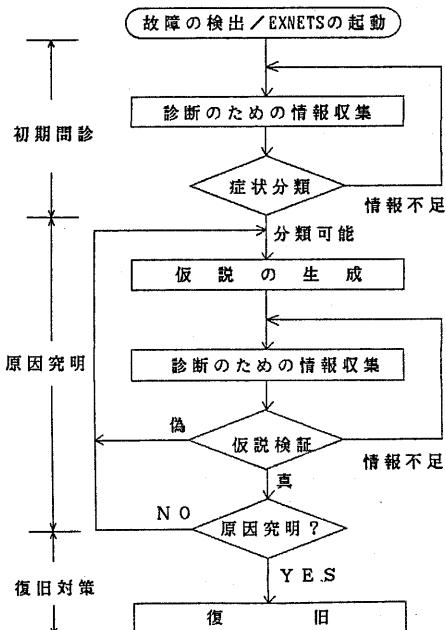


図-4 EXNETS の診断手順

EXNETS	
*** 初期問診 ***	
1. 障害症状 -----	コネクト不可
2. 障害発生状況 -----	突然に発生
3. 障害発生環境 -----	S 5. 障害再現性の選択 H 固定的 変時々
4. 操作による現象変化 -----	変 次画面 前画面
5. 障害再現性 -----	WHY
6. 端末アドレス番号 -----	

図-5 初期問診画面例

Executor は初期問診で収集した情報を、Supervisor によって処理できるように変換する。例えば、障害メッセージなどは個々の機器に依存した形式で表現されているため、EXNETS はそれらを各機器に共通した表現に置き換える。Supervisor は、Executor からの情報を利用し、初期問診後、原因究明を開始する。

原因究明では、Supervisor は知識を利用し、“ある障害状態が生起している”という仮説を立て、その仮説を裏付ける条件検査を Executor に指示する。

Supervisor によって利用される知識ベースの内容を次に示す。

①初期問診情報と症状のタイプを結びつける関係

②障害と原因を関係づける診断木

- ・仮説を検証する優先度
- ・仮説検証のための検査項目
- ・症状タイプとプロトコルレイヤの関係
- ・システム構成定義の構成
- ・確信度を算出するための方法
- ・原因と復旧手段の関係

診断木の構成や確信度算出方法は、ネットワーク関係者の経験、障害の統計的要素、障害の重要性に基づいたアンケート結果に従って定義されている。

Executorは、Supervisorの指示に従い、知識を利用して個々の検査を行う。例えば、ネットワーク情報（通信シーケンスとSGパラメータなど）を収集したり、ユーザやオペレータに質問を行って得られたデータを解析する。

SupervisorとExecutorの間でやり取りされる情報を、表-2に示す。

表-2 SupervisorとExecutor間の情報

Supervisor→Executor	Executor→Supervisor
初期問診／質問 プロトコルレイヤ SG属性の種類 検査結果の質問 原因／復旧対策	初期問診／質問の答 検査の正否

Executorにより得られた条件の検査結果は、Supervisorに送られる。検査結果は、指示された範囲の通信プロトコルの異常や、ネットワークノード間のシステム構成定義の不整合の有無などを示す真偽(true/false)で与えられる。Supervisorは、Executorで得られた検査結果を基に確信度を算出し、その仮説の正しさを検証する。

Executorが利用する知識の内容を以下に示す。

①通信プロトコルの状態遷移図

②各機器のシステム構成定義の構造とパラメータ値

③収集情報を機種独立の情報に変換する表

④復旧戦略を各機器に対応した手順に変換する表

仮説の生成と検証を繰り返し実行し、原因を究明する。

Supervisorは、Executorに原因と復旧戦略を提示し、Executorは該当装置に対応した復旧手順に変換し、オペレータに示す。障害によっては、EXNETSから障害機器に情報を直接提供し、自動的に復旧を行う。

図-6にEXNETSにより求まった原因と復旧対策の表示例を示す。

図-7に本障害解析処理の機能コンポーネント間のインタラクションを示す。ここでSupervisorとExecutorは、それぞれOSI管理モデルにおけるManagerとAgentに対応させることができる。

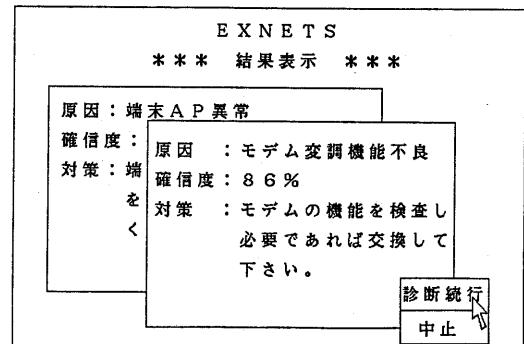


図-6 原因と復旧対策の表示例

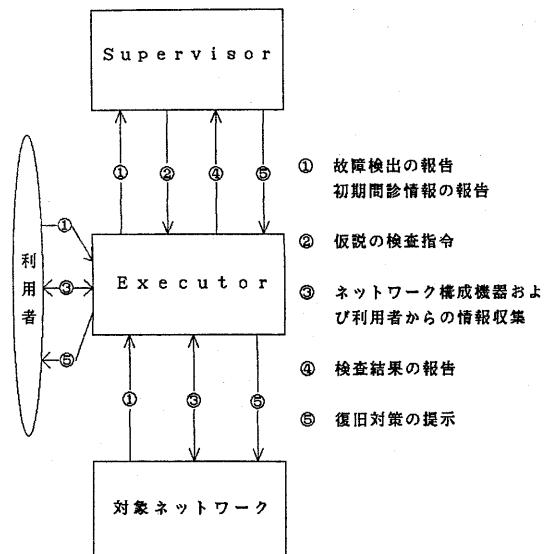


図-7 機能間のインタラクション

5. 解析機能

5.1 Supervisor

診断木は、図-8に示すように、重み付き有向グラフで記述される。診断木の各ノードはオブジェクトであり、症状の詳細度に従って階層的に構成される。

診断木のルートノード（最上部）は、診断の開始にあたり初期問診の結果に従って症状のタイプを割り出

す。ルートノードの直下のノードは症状のタイプに対応し、初期問診で収集された情報を利用して分類される。中間ノードは、それぞれネットワークの障害状態に対応し、推論を行う上での仮説として利用される。中間ノードには、その仮説を検証するための条件群と、条件の検査結果から確信度を算出するための方法が記述されている。確信度は、仮説の確からしさを示す。最下部のノードは障害の原因を示し、個々の原因に対応する復旧戦略に関係づけられる。

Supervisorは診断木に従い、下位ノードのプライオリティの順（図-8のアーケに付加）に検証を開始する。仮説検証のための個々の条件をExecutorが検査し、その結果からノードの確信度を求める。検証した複数の仮説の中で最も高い確信度が得られた仮説を選択し、その対応するノードに進み推論を続ける[10]。

図-8は、'端末コネクト不可'と呼ばれる端末とホスト間の接続が不可能となる症状に対応する診断木の例である。個々のアーケに付加されている数値はプライオリティであり、ノードの検証の順序を示す。

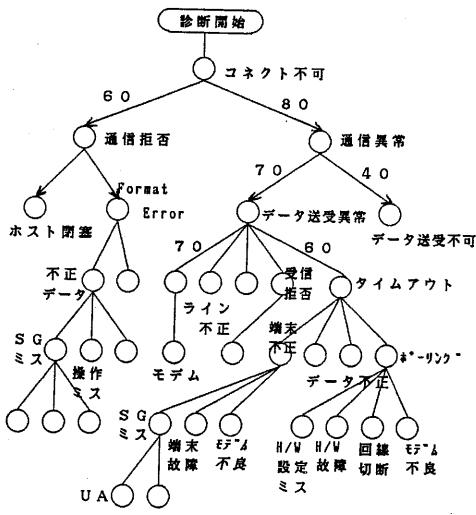


図-8 診断木の例

5.2 Executor

Executorの役割は以下の通りである。

- ①ネットワーク資源やユーザから受取った情報を共通化し、Supervisorにその情報を送る。
- ②Supervisorが指示した条件を検査し、その結果をSupervisorに送る。
- ③Supervisorの立てた復旧戦略を、対象機器に対応する復旧手順に変換し、オペレータに報告する。

以下に、仮説の検証のためにExecutorが行う解析の代表例について説明する。

(1) 通信シーケンス

通信プロトコルは、状態遷移図（システム内部では状態遷移表）により記述される。ネットワークノード間、例えばホストと端末間で通信されるコマンドとメッセージシーケンスは、状態遷移図を利用して解析される。この検査で検出される通信プロトコルの異常シーケンスは、原因究明の重要な手がかりとなる。

図-9は、仮説の検証に用いられる状態遷移図と対応する通信シーケンスの例であり、ホストコンピュータが通信データを受理できなくなった場合を示す。この状態遷移図上で通信コマンドに従って状態を遷移することによりエラー状態（図-9では、"Pビットカウントオーバーフロー"）を特定することができる。

状態遷移図には、各プロトコルの標準的な通信シーケンスに即した状態遷移に加え、実際に専門家が行なう熟練した解析手順や、特定の障害に固有の解析手順を盛り込み、よりきめ細かい原因の特定を可能にする。

(2) システム構成定義

現状では、コンピュータネットワークで発生する障害の原因で最も多いのが、システム構成定義（SG）のパラメータ値の不整合である。EXNETSにおいては、この重要なSGの解析処理を効率的に行なうため、ホストや端末などの各ネットワークノードのSGをその属性を要素とした木構造（SG-Tree）に表現し、知識として記憶している。SG-Treeのリーフノードは、各

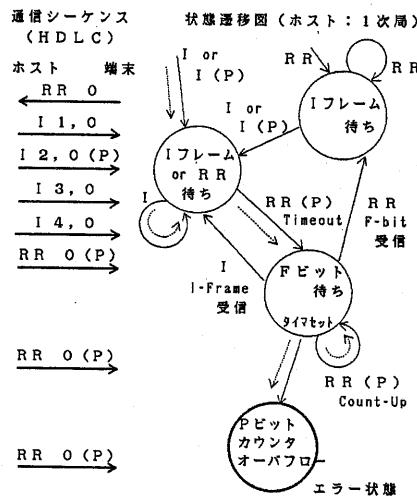


図-9 状態遷移図を用いた解析例

属性のパラメータ値が割り当てられる。

これらの知識は管理情報ベースMIBに格納されており、各ネットワークノードの情報はネットワーク構成定義を記述している管理情報木MITの構成要素に対応づけられる。

ホストコンピュータのSG-Treeは、Supervisorの利用する知識として、またホストコンピュータのSGのパラメータ値と各ネットワークノードのSG-Treeとのパラメータ値は、Executorの利用する知識として記憶されている。検査においては、それぞれのネットワークノードのSG-Treeの対応する部分を照合し、その整合性を判定する。

障害が発生した場合、Supervisorは仮説の検証のため、検査項目である属性に対応するSG-Treeの部分木をExecutorに示す。実際には、その部分木のルートノードを示すことで、その関連するリーフノードまでのパラメータ値の検査を指示する。Executorは、指示された属性を、障害の発生していると考えられるネットワークノードのSG-Treeに写像し、その写像された部分に対応するSG情報を収集する。ネットワークノード間のパラメータ値を比較し、不整合が検出されればそのパラメータは障害の原因として考えられる。

6. 分散管理への拡張

今後、より柔軟でかつ大規模なネットワーク管理を可能にするため、次の2種の機能を実現する。

- ① SupervisorとExecutorの分割配置による管理
- ② EXNETSの分散、階層化による分散管理

(1)機能モジュールの分散化

SupervisorとExecutorは、機構上同一ホスト 컴퓨터に実装される必要はない。例えば、Supervisorをホストコンピュータに残し、Executorをインテリジェント端末のようなネットワークの情報を容易に収集できる装置に実装することができる。この場合、各インテリジェント端末に実装されているExecutorがその管理領域のネットワーク情報を収集、解析し、Supervisorが実装されている機器に結果を転送する。そのため、Executorがネットワーク情報を収集、解析するために要した負荷が、ホストコンピュータから軽減されるという利点が得られる。

(2)EXNETSの分散、階層化

現在EXNETSは、单一ホストによるネットワークを対象とするが、以下の方法で複数台のホストコンピュータにより稼働するネットワークへの拡張を可能にする。

個々のネットワーク領域の中心となる各ホストコンピュータにEXNETS(Slave EXNETS)を実装する。個々のSlave EXNETSは、そのホストコンピュータのネットワーク領域内の障害を診断する。Slave EXNETSの上位階層に、ネットワーク管理の中心となるEXNETS(Master EXNETS)があり、ネットワーク全体の障害管理と複数の管理領域にまたがる障害の解析を行う。

図-10に分散環境下におけるネットワーク管理概念を示す。Master EXNETSのExecutorは、管理領域の接続関係に関する情報を知識として有し、他のホストコンピュータ上のSlave EXNETSから、それぞれの管理情報と障害内容を収集する。収集した情報を利用し、Master EXNETSのSupervisorは、複数の管理領域にま

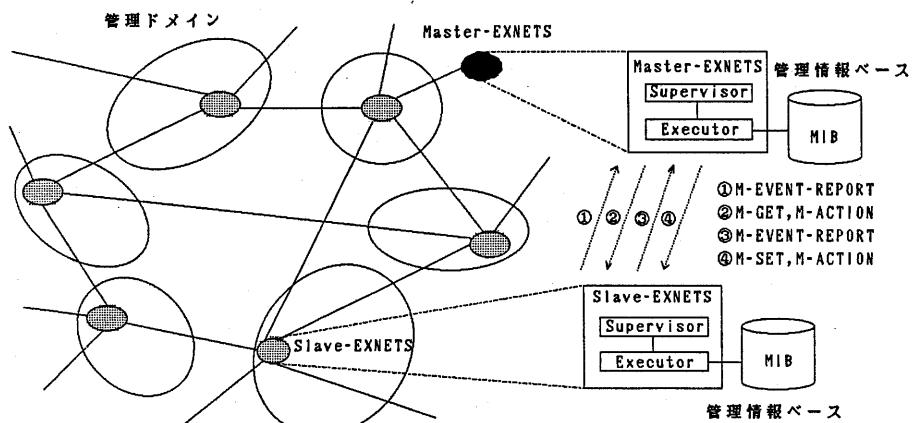


図-10 分散環境における診断動作例

たがる障害に関する知識を基に、個々の管理領域での障害状況を把握し、領域間で発生する障害の診断を行う。診断結果と復旧方法はそれぞれの関係するSlave EXNETSに報告される。

これらの管理形態において、各 Supervisor と Executor 間、および Master EXNETS と Slave EXNETS 間は、OSI 管理に準拠するよう C M I P を利用して情報交換を行う。例えば、Executor や Slave EXNETS からの障害の発生に関する報告は "M-EVENT-REPORT" により、Supervisor や Master EXNETS からのネットワーク状態の検査に関する指示や障害情報の収集は、それぞれ "M-ACTION"、"M-GET" により転送する。ここで Supervisor や Master EXNETS は、OSI 管理で定義されている Manager に、Executor や Slave EXNETS は Agent に対応している。この考え方は、交換／伝送系を含めた統合ネットワーク管理システムへの拡張においても有効と考える。

7. おわりに

統合ネットワーク管理システム構築に向けて開発を進めているコンピュータネットワーク障害解析エキスパートシステム EXNETSについて、その設計概念、解析機構、OSI 管理に基づく分散管理形態について述べた。EXNETS は、A I 手法を利用し、ネットワーク障害の検出、診断、復旧を行う。推論機構の中核部分を、機種独立な部分と從属な部分に分けることにより、EXNETS に可搬性を持たせ、ネットワークの多様性への対応を可能とした。EXNETS の機能要素間の情報交換は、OSI 管理に準拠するように設計しており、分散型の管理やリモート診断にも適用できる。

現在、以下の目標に対し、システムの拡張および機能強化を行っている。

①ネットワーク障害に対するより効果的な診断アルゴリズムの開発。特に、複合的な原因による障害に対してのアルゴリズム。

②OSI (C & C - D I N A) で検討されているネットワーク管理モデル、および障害管理プロトコルとの整合。

③構成管理や性能管理などの管理機能との連係、統一的運用。

④PBX を含む交換網や、高速モ뎀や LAN を含む高速伝送網などの他のネットワーク系を含めた統合ネットワーク管理 (VISION-NMS) への適用。

【謝辞】

本研究を進めるに当り、多大な御協力を頂いている当社 工藤、橋本、高村、森、中太、小黒、松岡、東、中島 各位に感謝致します。

【参考文献】

- [1] B. J. D. Carlos and Y. Kobayashi, "OSI System Management and SNA/Management Services," Proc. of 2nd International Symposium on Interoperable Information Systems, 1988.
- [2] D. Kanyuh, "An Integrated Network Management Product," ほか, IBM Systems Journal Vol 27, No 1, 1988.
- [3] J. G. Brinsfield, et al., "Unified Network Management Architecture-Putting It All Together," ほか, AT&T Technology Vol 3, No 2, 1988.
- [4] V. Sahin, et al., "Telecommunication Management Network (TMN) Architecture and Interworking Designs," IEEE Journal on selected areas in Communications, Vol.6, No.4, 1988.
- [5] R. N. Cronk, P. H. Callaban and L. Bernstein, "Rule-based Expert Systems for Network Management and Operations," IEEE Network, Vol. 2, No.5, 1988.
- [6] 鳩野、上田、阪田他, "コンピュータネットワークを対象とした故障診断エキスパートシステムの実現方式," 情処35回全大 5L-5, 1987.
- [7] 桐葉、山平、阪田他, "ネットワーク診断エキスパートシステムにおける論理誤り解析機構," 情処37回全大 3G-5, 1988.
- [8] 高村、橋本、小黒, "計算機運用・利用に関してジェネリークな3層推論機構による診断方式," 情処37回全大 5J-8, 1988.
- [9] T. Yamahira, Y. Kiriha, and S. Sakata, "Unified Fault Management Scheme for Network Troubleshooting Expert System," International Symposium on Integrated Network Management, IFIP WG6.6, May, 1989.
- [10] 中島、東他, "オブジェクト指向に基づくネットワーク診断方式," 情処38回全大, 1989.
- [11] 桐葉、山平、阪田、工藤, "統合ネットワーク管理を指向した障害解析方式," 情処38回全大, 1989.
- [12] 林、宗田、坂野、下郷、山本、工藤, "ネットワーク管理システム VISION-NMS," 情処、マルチメディア通信と分散処理研究会 35-6, PP41-47, 1987.