ネットワーク管理システムAIMSのエキスパート障害管理機能 *

1N−6

佐々木 修二, 村田 眞人, Glenn Mansfield, 樋口 謙一 †
(株)高度通信システム研究所 ‡

1 はじめに

我々は，インターネットを対象としたネットワーク管理システムAIMS(AICs Internet Management System)の研究開発を行なっている[1].

AIMSにおける障害管理機能としては，熟練したネットワーク管理者や，管理マニュアルに記述されている管理知識を知識ベース化したエキスパートシステム(以下ES)により，障害の検出や診断作業をできるだけ自動化することを目的として，次の2つのシステムを検討している.

1. 障害検出ES
   SNMP(Simple Network Management Protocol)のMIB(Management Information Base)情報から障害の検出を行なうES[4].
2. 障害診断ES
   障害を検出した後，症状や各種のテストにより診断を行ない，障害の原因を特定し復旧を行なうES.

本稿では，後者の障害診断ESについて述べる.

2 AIMSの障害管理機能

2.1 障害診断エキスパートシステムの構成

障害診断ESの構成を図1に示す．障害診断ESには，情報収集や管理対象の操作を行なうアクセス機能部と，ルールで表現された管理知識とデータから解析などを行なう推論実行部がある.

アクセス機能部が持つ機能について以下に示す.

- MIBアクセス機能部
  SNMPエージェントからMIB情報を収集する.
- NIBアクセス機能部
  各SNMPエージェントから収集したMIB履歴情報を持つNIB (Network Information Base) から必要な情報を検索する.
- 停止予定DBアクセス機能部
  ネットワーク停止予定DB[2]からネットワークあるいはネットワーク機器の停止予定情報を検索する.
- 構成DBアクセス機能部
  X.500ディレクトリ上に構築されたネットワーク構成DB[3]から，ネットワーク機器の情報(メーカやOS名など)やネットワークの接続構成に関する情報を検索する.
- コマンド実行機能
  MIBに登録されていない情報の収集や，機器に対するテスト(例えばICMP Echo Requestを発行するpingコマンドを実行するなど)を行なう.

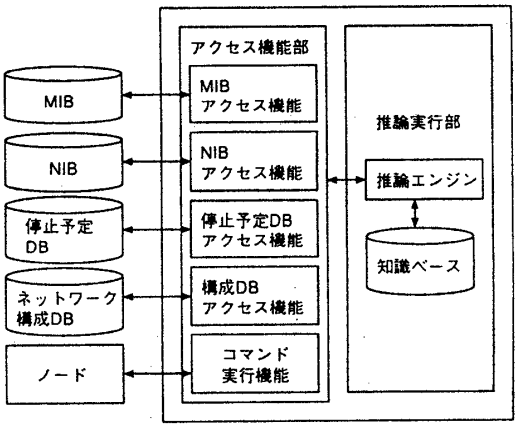

図1: 障害診断エキスパートの構成

推論実行部では，上記のアクセス機能を用いて収集されたデータと知識ベースに記述されたルールから推論を行ない，診断を実行する.

2.2 診断の処理の流れ

障害検出ESやユーザが障害を検出した後，障害診断ESは起動される．診断は次に示す4つのフェーズで行なわれる.

1. 症状入力
   障害診断ESを起動すると，システムは障害の種類や症状，障害が発生した時の状況ついての質問をユーザに行なう．例えば，発信したホスト名や受信するホスト名，その時の使用アプリケーションなどである．次に，システムは，ネットワーク構成DBにアクセスし，入力された情報から，接続構成やホストの機種やOSのバージョンといったネットワーク固有の情報を検索する．また，エラーメッセージがあった場合には，エラーメッセージの一覧を表示し，ユーザに選択入力してもらう.

*Expert fault diagnosis functions in the network management system AIMS

†Shuji SASAKI,Makoto MURATA,Glenn MANSFIELD,Ken'ichi HIGUCHI

‡AIC System Laboratories.

2. 停止予定DB検索
   停止予定DBの検索を行ない，申告のあった時間にホスト間で予定された機器の停止がないか調べる．予定がある場合にはその情報をユーザに伝え処理は終了する．
3. 診断
   アクセス機能を用いて必要な情報を収集したり，コマンド実行機能を用いてテストを行ないながら，実際に診断を行ない，障害の原因を特定する．
4. 復旧
   特定された障害の原因から，復旧させるための案を作成する．ネットワーク構成DBから得られた情報に基づいて，障害が発生している機器やソフトウエアに応じた復旧案を作成し，可能なものに関しては復旧を行ない，それ以外のものに関してはユーザに提示する．

2.3 知識ベースの構成

障害診断知識ベースは大きく次のように分類される．

1. 通信レイヤ診断知識
   TCP/IPネットワークにおける各通信レイヤ毎の診断知識および診断を行なうべきレイヤを切り分ける知識．例えば障害が起きたホスト間でpingコマンドの応答があれば，IP層以下には障害がないことが分かるといった知識．
2. アプリケーション診断知識
   各種通信アプリケーション毎の知識と，ホストネームからIPアドレスへの変換といった通信の前段階で行なわれる処理に関しての知識．
3. ネットワーク機器診断知識
   “電源が入っていない”，“接触不良”程度のネットワーク機器のハードウェア的な知識．インタフェースボード内の不良箇所を特定するような詳細な知識ではない．
4. 過去の障害事例
   A社とB社のホストはNFSの相性が悪いとか，バージョンが異なると通信が不可能であるといった，過去に報告されている障害に関する知識．
5. その他知識
   ユーザの入力ミスといった，上記以外の知識．

知識は，先ず仮説をノードとした木構造で表現し，そこからプロダクションルールに変換して知識ベース化している．現在この作業は人手で行なっている．図2に木構造で表現した診断知識の例を示す．

3 診断の例

ここでは，“telnetによりloginしようとしたができない”という例を用いて診断の流れを示す．

1. 症状入力
   発信ホスト名としてホストAを，受信ホスト名としてホストBを入力し，さらに，使用アプリケーションがtelnetであり，そのときのエラーメッセージには“Connection refused”があったことを入力する．

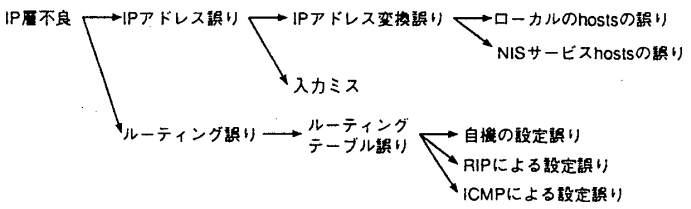

図 2: 診断知識の例

2. 停止予定DBの検索
   検索の結果，予定された停止はないことが分かる．
3. 診断
   (a) ホストAにおいてpingコマンドをホストBに対して行ない応答があるかを調べる．(rshを利用)
   →応答がある．
   (b) ホストBのinetdデーモンが起動中かを調べる．(rshを利用)
   →実行中である．
   (c) ホストBのinetd.confにtelnetのエントリがあるかを調べる．(rshを利用)
   →telnetのエントリがある．
   (d) ホストBのservicesにtelnetのエントリがあるかを調べる．(rshを利用)
   →telnetのエントリがある．
   (e) ホストBのinetdデーモン起動時にエラーメッセージがあるかを調べる．(rshを利用)
   →“inetd: telnet/tcp: unknown services”というエラーメッセージがある．

   診断の結果，ホストBのinetdが正常に起動されていなかったことが推定できる．
4. 復旧
   復旧案“ホストBのinetdの再起動”をユーザに提示する．

4 おわりに

AIMSにおけるネットワーク障害管理機能の一つであるネットワーク障害診断ESについて述べた．現在システムを開発中であり，“通信不可能”という障害を例として知識ベースの構築を行なっている．

参考文献

[1] 村田ほか，“SNMPを利用したエキスパートネットワーク管理システムAIMSの実現と利用”，情報処理学会92-DPS-54,pp.33-40,1992.
[2] 村田ほか，“電子メールを用いたデータ操作機能を持つネットワーク停止予定データベース”，情報処理学会第45回全国大会論文集(1),pp.117-118,1992.
[3] G.MANSFIELD et al., “CONFIGURATION MANAGEMENT USING THE DIRECTORY SERVICES”, 情報処理学会第45回全国大会論文集(1),pp.113-114,1992.
[4] K.JAYANTHI et al., “KNOWLEDGE BASES IN NETWORK MANAGEMENT”, Proceedings ICARCV'92,Sep,1992.