障害情報を利用したネットワーク故障診断エキスパートシステムの知識獲得*

2C－9

三浦 郁夫，　Glenn MANSFIELD，　木村 行男†

AIC ‡

1　はじめに

近年の情報社会において通信ネットワークは重要な役割を果たしており，必要不可欠なものとなっている．このため大規模，複雑化となり，ネットワーク管理，特に障害管理においては，熟練した管理者が必要である．

現在我々はこの様な状況に対処するため，知的ネットワーク管理システム AIMS(AIC's Internet Management System) [1] を研究開発中であり，その機能の一つに障害診断エキスパートシステム [2] がある．このシステムは，障害診断の自動化を目指したものであるが，多種多様な障害に対して的確な原因の提示を行なうために，多くの知識を蓄積しなければならない問題がある．

本稿では，この知識をトラブルチケットシステム [3] より得て蓄積し，故障診断に利用する方式の検討結果を報告するものである．

2　故障診断システム構成

本システムの構成を図1に示す．

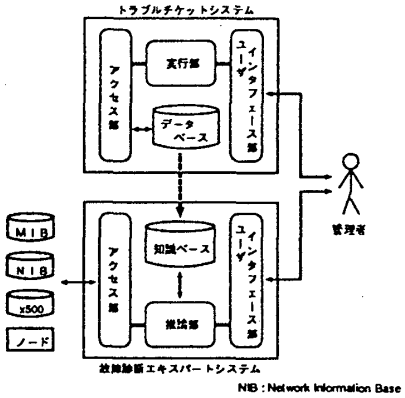

図 1: 故障診断システム構成

2.1　トラブルチケットシステム

トラブルチケットシステムはユーザインタフェース部，過去の障害情報を蓄積しているデータベースにアクセスを行なうアクセス部，及び実行部から構成されている．

以下に，ユーザインタフェース部に管理者が障害情報を入力する項目を示す．

1. 番号：トラブルチケットの管理上の番号
2. 発生日時：障害が発生した日時
3. 場所：障害が発生した箇所または区間
4. 現象：障害の現象
5. 原因：障害が発生した原因
6. 調査：原因究明調査の内容
7. 対処：復旧対処方法
8. 復旧日時：障害が復旧した日時
9. 記入者：情報を入力した人の名前
10. 備考：関連，その他の事項

2.2　故障診断エキスパートシステム

故障診断エキスパートシステムはユーザインタフェース部，情報収集や診断対象に操作を行なうアクセス部及び，このアクセス部で収集した情報を，知識ベースに記載されているルールにより解析を行なう推論部から構成されている．

本方式は，これら2つのシステムのデータベースと知識ベースをリンクさせるものである．

3　障害情報からの故障診断の実現方法

3.1　トラブルチケットシステムからの知識獲得方法

障害が発生すると管理者は，トラブルチケットシステムにその時の障害情報を入力する．この時幾つかある項目の中で，調査の項目には障害原因が究明されるまでの調査内容を入力する．すなわち，原因究明で調査した一つ一つの内容と，それぞれの結果が入力される．
これら一連の調査した一つ一つの内容と究明された障害原因とを対応させ，知識ベース化を容易にするためにマトリックスで表現する方法を採用した．

この様にマトリックスで表現する事で障害事例が障害診断のルールとなり，知識ベースに蓄積される．

入力方法は，データベース化のために選択式とする．調査の項目には，"ping" 等のコマンド投入やファイルエントリ等となる．調査結果は成功か失敗か，有るか無いかを"1","0" で入力する．
なおマトリックス表において，調査しなかった項目に対しての結果は"*" が入力され，この場合は"1"，または"0" となる．

*Knowledge acquisition for an expert fault diagnosis system using fault information

†Ikuo MIURA, Glenn MANSFIELD, Yukio KIMURA

‡Advanced Intelligent Communication Systems Lab.

3.2 本方式の知識ベースを用いた故障診断方法

故障診断エキスパートシステムは障害が発生すると，故障ホスト等の状況をユーザに対し質問する．この回答より，マトリックス表に対応する調査全項目について調査する．
その結果とマトリックス表の結果との比較を行ない，一致したら，その障害原因が究明したい原因と判断する．

4 知識獲得と診断方法の具体例

ここで，ホストA(発信ホスト)が"telnet"でホストB(受信ホスト)にloginしようとしたが，"unknown host"というエラーメッセージが出力されて通信出来ない障害を例として，以下に，知識獲得と診断の方法について述べる．

1. 知識獲得方法
   障害が発生し，管理者は復旧対処のための原因調査を行なった．

   (a) 発信ホストのNISドメイン名は正しいか?
   → 正しい(1)

   (b) 発信ホストでypbindが起動しているか?
   → 起動している(1)

   (c) 発信ホストのNISサーバ名は正しいか?
   → 正しい(1)

   (d) 発信ホストの/etc/hostsに受信ホストが登録されているか?
   → 登録されていない(0)

   (e) NISマップのhostsに受信ホストが登録されているか?
   → 登録されている(1)

   (f) NISサーバの/etc/hostsに受信ホストが登録されているか?
   → 登録されていない(0)

   これらより管理者は障害原因が"NISマップの未更新"と判断した．

   上記の内容を管理者がトラブルチケットシステムの調査項目に入力する事より，マトリックス表現でデータベース化される．
   データベース化された内容を表1に示す．

2. 診断方法
   障害が発生し，図1の調査全項目を行なうと，以下の調査結果が得られる．

   {0,1,1,1,0,1,0}

   このビット内容とマトリックス表の調査結果値とを比較する．
   これより一致する障害原因は"NISマップの未更新"となる．
   ここで，マトリックス表『発信ホストへのping』項目の結果は"*"であるので，実際の調査結果が"1"，"0"のどちらでもかまわない．

   この様に，過去の障害事例から判断すると，障害原因は"NISマップの未更新"と考えられる．

調査＼障害	受信ホスト未登録	NISマップの未更新
発信ホストへping	0	*
発信ホストのNISドメイン名	0	1
発信ホストでypbindの起動	*	1
発信ホストのNISサーバ名	*	1
発信ホストの/etc/hostsに受信ホストの登録	0	0
NISマップのhostsに受信ホストの登録	*	1
NISサーバの/etc/hostsに受信ホストの登録	*	0

調査結果値
1:OK
0:NG
*:OK/NG

表1: マトリックス表

5 結論

本処理を導入する事で，以下の効果が考えられる．

1. 知識ベースをマトリックスで表現するので，知識の修正や追加を行なう事が容易である．
2. 過去の障害事例を診断のルールとして有効活用出来る．

しかし，課題も幾つか残されている．

1. 事例情報をマトリックス表現にするために，調査内容を選択し，管理者に選んで入力してもらう事を考えている．このため，数多くある調査内容の項目化を体系化する必要である．
2. 調査結果には"シロ","クロ"ではかならずしも言い表せない数量的なものもある．
   これらをどの様に表現し，そして一致して認識させるのかの方法について検討する必要がある．
3. 診断時に全調査項目に関して調査を行ってしまうので，必要でない調査までもしてしまう．このため効率の良い調査方法について検討する必要がある．

6 おわりに

本稿は，過去の障害情報を収集蓄積するトラブルチッケットシステムから，故障診断エキスパートシステムへの知識として獲得方法，及びこれによる故障診断の方法についての検討報告を行なった．

今後の実現に当たり，幾つかの課題の検討をする予定である．

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] 佐々木ほか"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"，情報処理学会第46回全国大会論文(1),pp.145-146,1992.
[3] 三浦ほか"障害情報管理データベースシステムによる障害復旧の対処"，情報処理学会第47回全国大会論文(1),pp.289-290,1993.