分散システム運用技術研究グループ資料
資料番号 DSM-9505035

管理情報を自動的に収集・分析するネットワーク管理支援系の設計と実装

中嶋 良彰
(東京工業大学大学院情報理工学研究科)

大野 浩之
(東京工業大学 Titanet 運用センター)

1995年5月17日

社団法人 情報処理学会
東京都港区芝浦三丁目16-20
芝浦前川ビル7階

Abstract

計算機やネットワークの管理作業は管理者の知識や経験に依存する上に、作業のほとんどを管理者の人手に頼っている。本研究では管理者が管理に用いる道具相互の関係を記述することによって、管理者の知識を表現し、管理情報の収集・分析の自動化を行なった。

1 はじめに

本報告では、管理作業の自動化を目指して筆者らが開発している magP system[1] の現状と課題について述べる。magP system はあらかじめ記述された管理者の知識に従って自動的に管理情報の収集・分析を行なうシステムである。また、分析結果を電子メール、ページャなどで管理者に報告する手段も提供する。magP system を使うことによって、管理者の作業量を軽減できるとともに、熟練していない管理者でも管理作業を行なことができるようになると考えている。

magP system は、既存のオペレーティングシステムで構築されるシステムにおける管理作業の自動化を目的として開発されている。既存のオペレーティングシステムではなく、より管理しやすいオペレーティングシステムを設計し利用することも、管理者の作業量を軽減する方法の 1 つである。ただし、そのためには、「管理の容易なオペレーティングシステムを設計・実装し、現存する多数の管理の難しいシステムのすべてをこれに移行させることの労力」と、「現存するシステムの管理作業を援助する枠組を提案し実装する労力」の双方を見極め、どちらがより良い解決法であるかを決定する必要がある。そこで、筆者らは現状ではこの問題に対する明確な解答を得ることが困難であるため、後者すなわち現存するシステムの管理を自動化すること目標とした。

2 管理作業の問題点

現在、計算機や計算機ネットワークの管理作業は、大部分管理者の人手によってなされているのが実状である。それは、管理者個人の知識や経験に頼る部分が多い複雑で時間のかかる作業である。また、発生した障害の内容やその調査結果に対して作業内容がはっきりと決定しているとは限らず、管理者は情報を整理し、状況に応じて作業しなければならない。管理者の「勘」に頼る部分も多い。その上、管理に用いる「道具」の数も多く、これによって管理対象から得られる情報の形態も多様である。それらすべてを把握し、効率よく管理を行なうためには、複雑な知識や経験が必要である。このように、現在の管理作業には

> 「道具は存在するが、複雑な知識や豊富な経験が必要とされるため、多大な労力を必要とする」

という問題がある。しかも、計算機やネットワークが普及し、その規模も拡大している現在、この問題はますます深刻化しつつある。この研究の目的は、熟練した管理者にとっては管理作業が軽減され、熟練していない管理者にもある程度管理作業が可能になるような、なんらかの手段を提供することである。

本報告ではオペレーティングシステムとして UNIX を仮定し、UNIX を用いたシステムの管理作業について述べている。しかし、管理作業の自動化のもととなるモデルの設計は、他のオペレーティングシステムにも応用可能であると考えている。

3 magP system

magP system についてその設計方針、概要、管理者の知識の表現方法などについて述べる。

3.1 設計方針

magP system の開発にあたって、まず図 1のように一般の管理作業のモデル化を行なった。今回は、このモデルの情報収集・分析・報告 (図 1中の破線で囲まれた部分) の部分を中心に自動化を行なった。将来的には対策部分も含めたモデル全体の自動化が必要であると考えている。情報収集・分析・報告を自動化するためには、収集する情報の内容・情報の収集方法・情報の分析方法を決定するための知識、すなわち管理作業に関する知識の表現方法が大きな問題となる。今回の実装では、管理者が情報収集に用いる道具それぞれに対して、情報の収集・分析のための規則を記述することによって、管理者の知識を表現している。このような方法で記述された管理者の知識は、管理知識データベースに登録され、magP system はこの管理知識

---

[1] magP は magpie(かささぎ) をもとにしている。これは、黒白の羽毛で鳴き声がやかましく、様々な小さなもの (管理情報?) を巣に集めてくる鳥である。

データベースを用いながら動作を行なう(図2)。magP system は、管理者によって管理知識を指定され動作を始めると、管理知識に記述された情報や規則をもとに自動的に作業を行なう。また、オペレーティングシステムが用意している既存の管理コマンドを利用することによって、複数の異なるオペレーティングシステムでの利用を比較的容易にする。

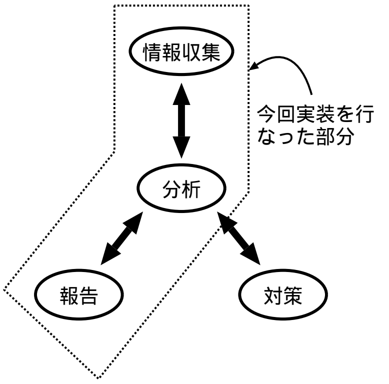

図 1: 管理作業のモデル

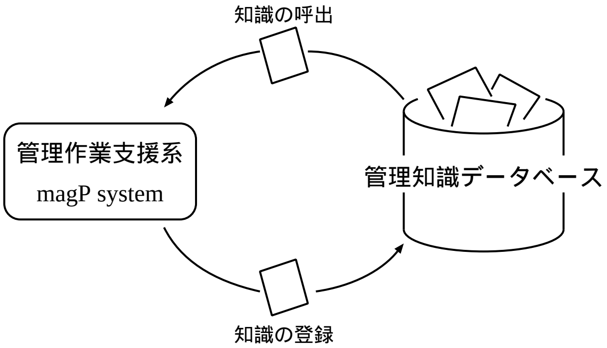

図 2: 管理作業支援系と管理知識データベース

3.2 magP system の構成

magP system は次の 3 つのプログラムによって構成されている。

1. magpp: magP system のユーザインタフェースである。magpd に管理者の要求を伝える。要求には、「管理知識を実行」「管理知識の追加、削除、変更」「管理知識の実行スケジュールの制御」「magP system の動作状況の取得」などがある。
2. magp: magpd によって実行される。管理知識名を 1 つ指定されることによって動作を開始する。管理知識データベース内の管理知識に従って自動的に管理情報の収集・分析を行ない、必要に応じて報告を行なう。
3. magpd: magpp による管理者の操作の受け付け、電子メールによる操作および、magp の実行を受け付けるサーバプログラム。また、管理知識データベースへの知識の追加、削除などを行なう。

これらのプログラムの関係を図3に示す。通常は管理ホスト上にmagpd が常駐する。管理者はmagpp を用いてmagpd に要求を伝える。magpd は要求を受理すると、それに従って作業を行なう。このとき、管理知識の実行を要求された場合、magpd は管理知識名を指定してmagp を呼び出す。magp は指定された管理知識に従って、コマンドの実行・分析を行ない結果の報告を行なう。報告には電子メールやページャーなどを用いる。また、magpd へ要求を伝えるために、電子メールを用いることも出来るため、管理ホストにログインができない場合にも magP system の操作が可能になっている。

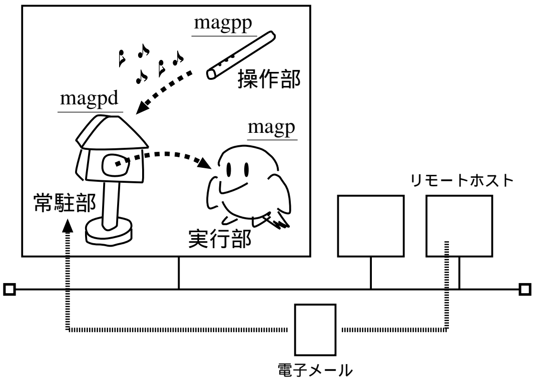

図 3: magP system

3.3 管理知識データベース

通常、管理者が行なう作業は複数の道具(コマンド)によって構成され、その道具はシステムの状況に応じて選ばれる。また、得られた実行結果の分析に従って再び適当な道具が選び出され、同様の作業を繰り返す。この時、一塊の管理作業を道具(コマンド)によっ

て構成されるため、それらの道具がどのような関係にあるのかを明確にすることによって、管理作業を表現することができる (図 4)。たとえば、ローカルホストとリモートホストとの通信状況を調査する場合、作業を構成するコマンドの関係は図 5のようになる。この場合、作業は 6 つのコマンドによって構成されている。そこで、magP system ではそれら 6 つのコマンドそれぞれについて管理知識を記述し、それらの相互呼び出しによって管理作業が実現される。例えば、図 5に示される作業は、ping コマンドに関する知識を呼び出すことによって開始される。この知識が呼ばれると、ping の実行結果と「アドレスが引けるかの確認」と「インタフェースを調べる」のそれぞれの知識で表現される作業の結果をもとに分析が行なわれ、次の作業 (新しい知識を呼び出すや報告するなど) に移っていく。「アドレスが引けるかの確認」や「インタフェースを調べる」も、同様にコマンドごとに記述される。

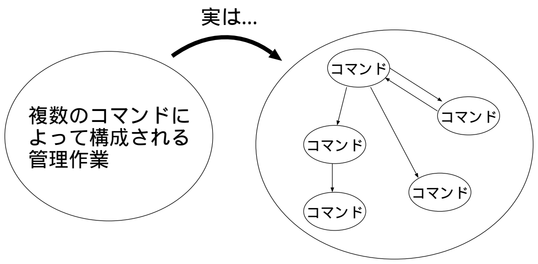

図 4: 管理作業を構成するコマンドの関係を明確にする

以上のようにして、magP system ではコマンドごとに管理者の知識を記述し、これを管理知識データベースに蓄積・管理する。また、管理知識の記述には管理知識記述言語を用いる。

また、管理情報の取得には UNIX のコマンドによる以外にも SNMP [2, 6, 7, 9] を用いることができ、magP system では SNMP で取得する管理情報をもとに管理知識を記述することも出来る。

3.4 管理知識記述言語

3.3節で述べた通り、管理知識は管理知識記述言語によって記述する。図 8や図 10が管理知識の記述例である。管理知識を構成する要素は、基本的にはラベルに続いてその定義を記述する。主な構成要素は次の通りである (ただし括弧内はラベル名)。

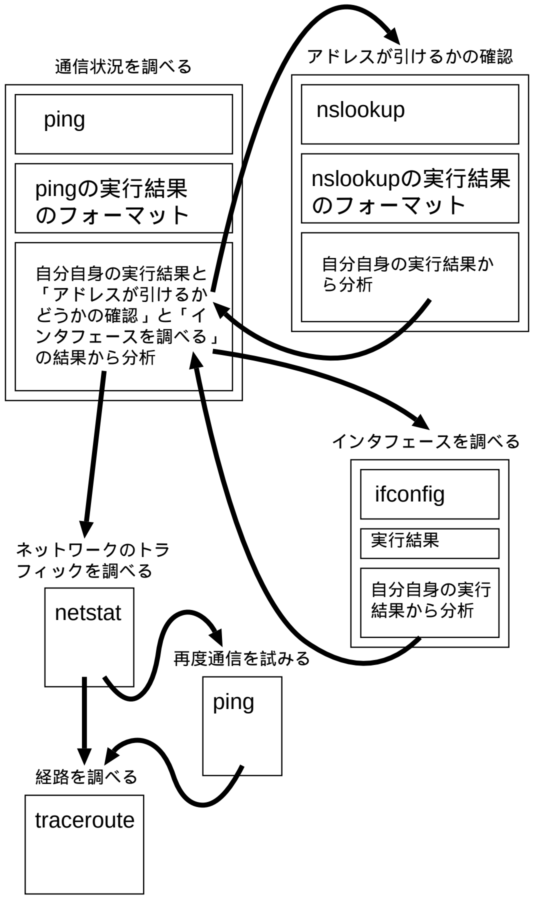

図 5: リモートホストとの通信状況の調査

1. 管理知識名 (IDENT): この例では「disk_free_space」。
2. コマンドに関する定義 (TYPE,COMMAND): 図 8では「df -t 4.3」。他に実行制限時間[2] などを定義できる。
3. 実行結果の定義 (DATA_TYPE,FIELD_NAME): 実行結果の形式を定義する。図 8では、空白を区切りとして単語 (これをフィールドと呼ぶ) に分け、一部のフィールドを正規表現によって定義している。たとえば、図 6 はdf コマンドの実行例であるが、これを図 8の知識にしたがってフィールドに分割すると図 7のようになる。また、フィールドの値を参照するために名前をつける。図 8 中の記述「capacity * 4」は、左から 5 列目[3] の全ての値を参照するための定義である。この場合、リストのように扱われることになる。

---

[2] 実行したコマンドが永久に動作し続けることを防ぐために設定する。この他にも設定可能な要素がいくつかあるが、図 8では省略時の値を用いている。

[3] 数字は 0 から始まるため 5 列目は 4 で表される。「*」は任意の数を表す。

4. 分析規則の定義 (`IF`~`THEN`~`ELSE`~`ENDIF` など): 分析規則を記述する。図8では「使用率が90%以上」か「前回調査に対する使用率の変化率が10%以上」である場合に、警告のためメールを`root` に対して送るように定義されている。
5. 報告書の定義: 報告書の定義を記述する。この定義をもとに報告書が生成される。

3.5 分析結果の報告

分析結果の報告手段には、電子メールの他に、WIDE/PhoneShell [8] を用いてページャ、FAX などの利用が可能である。特に、遠隔地から電子メールによって magP system を操作し、その後処理が終り次第、結果をページャによって受信することが可能であるため、携帯端末の普及に従って magP system の有用性が高まると考えられる。

4 magP system の実行例

ここでは、magP system の簡単な実行例として「ファイルシステムの使用率の監視」「通信状況の調査」「電子メールによるオペレーション」について述べる。

4.1 ファイルシステムの使用率の監視

magP system でファイルシステムの使用率の監視を行なう。この作業では`df` コマンドを用いる。図8が、この作業で用いる管理知識の記述例である。また、この管理知識の記述に従って、magP system が動作し、ファイルシステムの使用率に異常を発見した場合に管理者へ送られる電子メールの例が図9である。このように、magP system では実行結果が一定の形態で統一されていれば、容易に分析規則を記述することができ、作業を自動化することができる。

```
% df -t 4.3
Filesystem  kbytes    used   avail capacity  Mounted on
/dev/sd00a   22129   11552    8364    58%    /
/dev/sd01c 1961710 1626134  139404    92%    /home
/dev/sd00d  141405   19211  108053    15%    /tmp
/dev/sd00e  141099   84566   42422    67%    /var
/dev/sd00h  758404  514381  168182    75%    /usr
%
```

図 6: df コマンドの実行例

	0	1	2	3	4	5
0	Filesystem	kbytes	used	avail	ca..	Mo..
1	/dev/sd00a	22129	11552	8364	58	/
2	/dev/sd01c	1961710	1626134	139404	92	/home
3	/dev/sd00d	141405	19211	108053	15	/tmp
4	/dev/sd00e	141099	84566	42422	67	/var
5	/dev/sd00h	758404	514381	168182	75	/usr

図 7: df コマンドの出力をフィールドに分割

4.2 通信状況の調査

システムの運用中にネットワーク上の他のホストと通信ができない状態になることがある。この例では、このようなときに管理者が行なう原因の分析と同様の作業を magP system によって行なう。まず、一般にネットワーク上のリモートホストと通信ができない場合に考えられる原因を整理する。そのために、原因の所在を「ローカルホスト」「ネットワーク上」「通信対象のホスト」に分け、以下のように考える。

- ping によって、ホスト A からホスト B と通信できないことが分かった。そこで、以下のような問題点を考えながら分析を行なう。
  1. ホスト A の問題
     (a) ホスト B の IP アドレスが引けていない
     (b) ローカルホストのネットワークインタフェースに異常がある
  2. ネットワークの問題
     (a) ネットワークの負荷が高い
     (b) 経路情報が誤っている
     (c) 中継ホストの障害
  3. ホスト B の問題
     (a) ホスト B の負荷が高い
     (b) ホスト B のネットワークインタフェースに異常がある

この作業の際に用いられる道具 (コマンド) の関係を表したものが図5である。4.1節の例と同様に、それぞれのコマンドについて知識を記述する。そのうち、この作業で最初に呼び出される知識 (図5の左上の ping に関する知識) は図10のように記述される。分析条件は`ping` の結果と、知識「`CheckName`」「`CheckIF`」に従って行なわれる作業の結果にを用いて記述されている。知識「`CheckName`」はホスト名から IP アドレスを求めることに成功しているかの調査に用いられ、知識「`CheckIF`」はネットワークインタフェースの調査に用いれる。図10中の分析規則では、通信不能で、正常に IP アドレスが得られ、ネットワークインタフェースが

```
IDENT:
          disk_free_space
TYPE:
          shell
COMMAND:
          df -kt ufs
DATA_TYPE:
          f * "(Mounted .*)"
          f * "([0-9]*)%" f
          *
          .
FIELD_NAME:
          capacity      * 4
          .
IF:
          (( $capacity[1..*] > 90 ) \
          || (&percentage($capacity[1..*]) >= 10 ))
          .
THEN:
          INFO: MAIL,root,WARNING_MAIL
          .
ENDIF:

WARNING_MAIL:
Subject: Check Filesystems
  ファイルシステムの使用率に異常が発見されました
  ので報告します

  各ファイルシステムの使用率は以下の通りです。
  %filesystem[1..*]: %capacity[1..*] %

  各ファイルシステムの使用率の前回調査時と比較し
  た変化率は以下の通りです。
  %filesystem[1..*]: %history(&capacity[1..*]) %
.
END:
```

図 8: ファイルシステムの使用率の監視作業を表す管理知識

正常である場合、次の作業のために知識 「`CheckNet`」が呼ばれる。

4.3 電子メールによるオペレーション

magP system では電子メールによる管理操作を受理することにより、遠隔地からの操作を可能にしている。電子メールによって可能な操作には次のものが用意されている。

1. 管理知識の追加・削除・変更
2. 管理知識の呼出し
3. 動作状況の取得

```
Subject: Check Filesystems
From: root (magP)
To: root
Date: Fri, 3 Feb 1995 07:27:36 0900 +

  ファイルシステムの使用率に異常が発見されました
  ので報告します

  各ファイルシステムの使用率は以下の通りです。
  /dev/wd0a: 80 %
  /dev/sd0e: 14 %
  /dev/sd0g: 76 %
  /dev/sd0h: 70 %
  /dev/wd0h: 25 %

  各ファイルシステムの使用率の前回調査時と比較し
  た変化率は以下の通りです。
  /dev/wd0a: 0 %
  /dev/sd0e: 53 %
  /dev/sd0g: 0 %
  /dev/sd0h: 0 %
  /dev/wd0h: 0 %
--
magP system
```

図 9: ファイルシステムの使用率に異常が発見された場合に報告される電子メールの例

ここでは、この電子メールによる操作を用いた例を示す。例えば、電子メールによって管理知識データベースに知識を登録する場合、図 11のようなメールをあらかじめ magP system に登録された管理者宛に出す。magP system は登録されている管理者のメールスプールを監視し、到着した magP system へのリクエストメールを処理する。この作業を行なうプログラムは前述した magpd である。リクエストメールは、電子メールの先頭行に文字列 「`#HELLOMAGP`」が存在すること、管理者が magP system に登録されていることによって判別される。また、登録済の管理知識を呼び出し、その知識に従って magP system に作業を行なわせるためには、図 12のような電子メールを送る。図 10の知識が登録されている状態で、この電子メールが受理されると、管理ホストとホスト nsc との通信状況の調査を行なう。また、その結果ページャに送られる報告メッセージの例が図 13である。

このように、magP system は電子メールによって操作を行なうことが可能であるが、現在は実験段階の機能である。この機能を安全に用いるためには、PEM [1, 3–5] などを用いて電子メールのセキュリティを確保しなければならないと考えている。

```
IDENT:
          check_connection
TYPE:
          shell
COMMAND:
          ping $argv[1] 64 1
DATA_TYPE:
          f *
          f * "([^\t ]+):" f *
          *
          .
FIELD_NAME:
          targethost 1 3
          .
IF:
      (("$targethost" eq "") \
      && (&call(CheckName, "$argv[1]") eq "OK")
      && (&call(CheckIF, "$argv[1] en0") eq "OK"))
      .
THEN:
      EXEC: CheckNet $argv[1] en0
      .
ENDIF:
END:
```

図 10: 「通信状況を調べる」で最初に呼ばれる知識

5 magP system の課題

magP system ではコマンドの実行結果が一定の形態で統一されていれば、大部分の情報について分析規則を記述できる。また、分析結果をもとに報告書を生成し適切な手段で報告するという部分についても、いくつかの実験を行ない期待した通りの結果を得た。しかし、管理知識記述言語や magP system の動作履歴の管理などについて問題点も多く残されており、引続き研究を進めていく必要がある。この節では、これらの問題点の改善も含めて今後の課題について述べる。

```
To: yoshiaki@is.titech.ac.jp
Subject: [MAGP] Add knowledge
From: Yoshiaki Nakajima <yoshiaki@is.titech.ac.jp>
Reply-To: yoshiaki@is.titech.ac.jp
----
#HELLOMAGP
#ADD_KNOWLEDGE
begin

                              :
      ここに登録したい管理知識の定義を記述する
                              :

end
```

図 11: 知識を登録するための電子メール

```
To: yoshiaki@is.titech.ac.jp
Subject: [MAGP] Exec knowledge
From: Yoshiaki Nakajima <yoshiaki@is.titech.ac.jp>
Reply-To: yoshiaki@is.titech.ac.jp
----
#HELLOMAGP
#EXEC_KNOWLEDGE check_connection nsc
```

図 12: 管理知識を呼び出しと実行を要求する電子メール

```
ｎｓｃまでのネッ
ワーク過負荷のた
め通信困難 (ｍａ
ｇＰ）
```

図 13: ページャーに表示されるメッセージの例

5.1 管理知識記述言語の改良

magP system は、あらかじめ管理知識記述言語によって必要な情報を記述することができれば、ある程度予想した通りに動作する。つまり、その能力の大部分を管理知識の記述に依存している。現在、管理知識記述言語に関する問題点は次のものが考えられる。

1. 分析結果を報告書の記述に反映できない
2. 出力形式が一定しないような管理コマンドは定義しにくい
3. 管理知識の記述が大きくなりやすい
4. 条件式で複数の値を意味するようにフィールド名を記述した場合の評価方法が 1 通りしかない

現在の管理知識記述言語では、分析規則部の評価結果を報告書で利用するような記述ができない。例えば、実用例で「ファイルシステムの使用率の監視」を行なったが、報告書の定義で問題があったファイルシステムのみ報告するような記述ができない。そのため、報告書の記述の自由度が制限されている。

管理知識を記述する場合、まず使用するコマンドを決定しなければならない。ここで特に問題となるのはコマンドの実行結果の形式である。例えば、df コマ

ンドのような出力結果が一定している場合は特に問題にはならないが、出力結果が一定しないようなコマンドは扱いにくい。そのため、扱える形式の範囲を広げることが課題の 1 つである。

条件式に複数の値を意味するようにフィールド名を記述した場合、現在は要素ごとに条件式の評価を行なう。例えば、条件式で 3 つの値を意味するようにフィールド名を記述した場合、まずの 1 つ目の値で条件式を評価し、同様にして 2 つ目、3 つ目の値で評価を行なう。そして、その結果、真になるものが 1 つでもあれば、その条件式は満たされているとしている。これは、4.1節の実用例のような場合には、条件式の記述が 1 つですむため非常に便利である。しかし、フィールド名が示す全ての値について条件式が真となる場合に、条件式が満たされているとするのように、他の評価方法も選択可能にすべきである。

5.2　作業履歴

現在の実装では収集した情報は履歴として保存されているが、管理知識の呼び出しや実行、分析の経過などのような magP system 自体の動作記録は残していない。通常の管理作業において過去の作業記録が非常に重要な情報源であると考えられることからも、magP system においても動作記録を管理し後の作業に利用する必要があると考えられる。特に、将来、管理知識を自動生成することを考えた場合、このような作業履歴の管理が重要な意味を持ってくる。

5.3　作業量の軽減

現在の実装は実験不足のため、十分な評価を行なっていないため、管理者の作業量をどの程度軽減できるかがはっきりとしていない。そこで、実装を安定させるとともに、十分な実験を行なう必要がある。

5.4　課題のまとめ

今後の課題をまとめると次のようになる。

1. 管理知識記述言語の改良及び拡張
2. magP system の評価のための実験
3. 動作履歴の管理
4. 管理知識を記述するためのインタフェースの設計と実装
5. 管理知識の自動生成

1 ~ 3 についてすでに述べた。4 は GUI を用いて視覚的に管理知識を記述できるようにするなど、より容易に管理知識を記述可能にする手段を提供する。また、5 を実現するためには 3. の動作履歴の管理とその分析が特に重要になる。

システム管理はこれまで、人間である管理者がその経験や知識を用いて行ってきた作業である。そのため、管理作業を自動化する場合、人間の知能や知識の表現方法の決定が最も大きな問題である。そこで、今回は簡単な記述言語を用いて、分析部分の実装を試みた。しかし、この部分を汎用のエキスパートシステムを用いて実装するなどの方法も考えられ、さらに分析作業について研究を進めていく必要があると考えている。

また、現在の magP system はある 1 つの計算機を対象とした管理作業に向いている。しかし、magP system がネットワーク上の複数の計算機上で動作し、それぞれが互いに協調しながら管理作業を行なうようにすることも可能である。また、ネットワークワーム [11] が複数の計算機上を渡り歩きながら管理作業を行なう NMW-System [10] を用いることによってもこの目的を達成することができると考えている。

6　おわりに

現在の magP system は 5節でも述べた通りその能力の大部分を管理知識データベースに依存している。管理知識を記述する上では、これまでと同様に管理者の知識や経験を必要とする。しかし、一度記述してしまえば、その後は熟練していない管理者にも作業が可能になる。そこで、今後もインタフェースに提供や自動生成など管理知識の記述を中心に研究を進め、より完全な自動化を目指していきたい。

謝辞

様々な助言を頂いた東京工業大学大学院数理・計算科学専攻の木村泉教授、木村・大野研究室の皆さんに感謝致します。

参考文献

[1] D. Balenson. Privacy Enhancement for Internet Electronic Mail: Part III: Algorithms, Modes,

and Identifiers. Request for Comments 1423, Feb 1993.

[2] Jeffrey D. Case, Mark S. Fedor, Martin L. Schoffstall, and James R. Davin. A Simple Network Management Protocol (SNMP). Request for Comments 1157, May 1990.

[3] B. Kaliski. Privacy Enhancement for Internet Electronic Mail: Part IV: Key Certification and Related Services. Request for Comments 1424, Feb 1993.

[4] S. Kent. Privacy Enhancement for Internet Electronic Mail: Part II: Certificate-Based Key Management. Request for Comments 1422, Feb 1993.

[5] J. Linn. Privacy Enhancement for Internet Electronic Mail: Part I: Message Encryption and Authentication Procedures. Request for Comments 1421, Feb 1993.

[6] Keith McCloghrie and Marshall T. Rose. Management Information Base for Network Management of TCP/IP-based internets. Request for Comments 1156, May 1990.

[7] Keith McCloghrie and Marshall T. Rose. Management Information Base for Network Management of TCP/IP-based internets: MIB-II. Request for Comments 1213, March 1991.

[8] Hiroyuki Ohno. Improved Network Management using WIDE/PhoneShell. In *Proceedings of INET '93*, 1993.

[9] Marshall T. Rose. *The Simple Book*. Prentice-Hall, 1991.

[10] 清水亮博. 寄生プログラム（ネットワークワーム）を用いたコンピュータネットワークの管理方式. 平成４年度卒業論文, 東京工業大学理学部情報科学科, February 1993.

[11] E. H. Spafford, J. A. Rochlis, M. W. Eichin, D. Seeley, T.Eisenberg, D. Gries, J. Hartmanis, D. Holcomb, M. S. Lynn, and T. Santoro. 特集 ワーム・ストーリー — インターネット・ワーム事件の全容. *bit*, Vol. 21, No. 14, pp. 4–43, December 1989.