システムソフトウェアと
オペレーティング・システム　64－4
マルチメディア通信と分散処理　65－4
（１９９４．　５．　１９）

インターネットにおける障害管理の総合的な支援システムについて

上水流 由香 †　　浅羽 登志也‡　　小野 諭†

†NTT ソフトウェア研究所　‡(株) インターネットイニシアティブ

計算機の利用環境として一般的になってきたインターネットは、今後も地球規模の情報基盤として拡大していくと考えられる。そこで今後は現在よりも更に安定したネットワークを提供することが求められ、組織的に管理作業を行っていくことも必要になると考えられる。障害管理作業は一刻も早く運用状態に戻すための作業と、簡単に解決できない問題を根本的に解決するための作業という２つの段階に分けて考えることができる。本稿では、現在の障害管理作業の全体の流れを分析し、目的の違いから作業の流れを２つに分け、それぞれの作業の特徴を考えた上で、障害管理作業全体としてどのような支援を行っていくべきなのかということについて考察していく。

System Requirements for Supporting Internet Fault Management

Yuka Kamizuru†　Toshiya Asaba‡　Satoshi Ono†

†NTT Software Laboratories　‡Internet Initiative Japan Inc.

As the Internet grows, fault management has become a key issue to provide a stable network service to the people utilize it as a basis for their daily activities. Some computer systems are necessary to support administrators to manage troubles.

This paper breaks down the job flow of fault management typically taken on the Internet. There are 2 roles in managing network troubles. One is for keeping the availability of the network, and the other is for improving the robustness of the network. Requirements for systems supporting administrators job are pointed out with the consideration for those 2 roles.

1 背景

計算機ネットワークを相互接続したインターネットは、計算機を利用する上で必要欠くべからざるものとなっている。最近では遠隔地の計算機を利用するというだけでなく、電子メールや情報提供サーバへのアクセスなどといった情報交換のための地球規模のネットワークとして社会的にも注目されはじめている。

現在、我々の身の周りで利用されいているインターネットの多くは大学や研究機関などを結ぶ実験的なネットワークが発展してきたものが多い。そのため、他の仕事の傍らでボランティアでネットワーク管理も行っているという場合が多く見られる。また、広く一般的な社会生活においてインターネットに依存する部分がまだ少ないため、仮にネットワークに何らかの障害が発生したとしても、社会的に与える影響はまださほど大きくない。しかし、今後(今でも一部ではそうであるのかもしれないが)一般社会の基盤としてインターネットが重要な役割を果たすようになれば、常に安定したネットワークの運用が強く求められる。

障害管理作業は、インターネットに関する広汎な知識と経験を必要とするため、現在は各管理者の専門的な知識と経験に大きく依存している。しかし今後は、多くの人がネットワークの運営を行っていくことが必要であり、また、ネットワークの専門家はより専門的な知識を活かして効率的にネットワークの管理を行っていく必要がある。

そこで、今後さらにインターネットが大規模化し、地球規模の情報基盤として常に安定したサービスを提供していくためには、障害管理作業を総合的に支援するようなシステムが必要不可欠となる。作業支援を行うためには、現在管理者により行われている障害管理作業の全体について分析することが必要であり、また実際の作業においてそれを利用する人にとって本当に役だつものでなくてはならない。また、現存する管理システムについても、その有効性や不足している点などについて明らかにする必要がある。

本稿では、まず現在の障害管理作業の流れを分析し、どのような方向で支援を行っていくべきなのか、また現在の作業の中で行われいていることの意義は何なのか、ということについて考察していく。そして、作業支援の方向性を考慮した上で、現在の障害管理作業において不十分な点はどこなのかを指摘していく。そして、今後、障害管理を総合的に支援するために必要な支援システムへの要件を指摘する。最後にそのような支援システムが利用される条件を考慮しながら、実際にシステム構築の際に注意すべき点について述べる。

2 ネットワーク管理

障害管理の支援を考えるために、現在のネットワークの障害管理作業の流れを分析していく。

2.1 ネットワーク管理作業の目的

障害管理の目的として大きく以下の2つが挙げられる。

- 一刻も早い障害からの復旧
- 障害の原因の究明と根本的な改善

ネットワークの障害の原因として、すぐに根本的な解決策が発見できる場合もあれば、それが分からない場合もある。しかし、実際のネットワークの運用では、ともかく利用可能な状態にもどすことが優先される場合がある。

その場合、障害は一旦は取り除かれるが、根本的な原因が解決されずに残されているため、同じ障害が繰り返されるおそれがある。根本的な原因の究明や解決策の検討は、運用への回復と別の流れで行われる。

障害管理作業は、このように、2つのフェーズに分けて考えることができる。

2.2 ネットワーク管理作業の流れ

ネットワークの管理作業の流れを大まかに捉えると**障害の検知、問題の特定、原因の究明、復旧**である。しかし、前節で挙げた障害管理の目的にもあるように、障害の原因を解決するより先に**応急的な復旧**を行う場合もある。また、同様の障害が何度も発生するような場合には、その障害に至る根本的な問題があると考えられるため、その原因を究明し根本的な解決(復旧)を行う必要がある。障害管理作業の流れは図1のように表される。

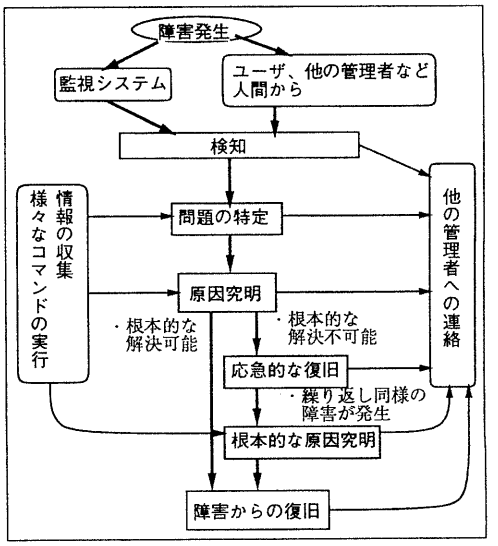

図 1: 障害管理作業の流れ

- **障害の検知**
  障害の発生が管理者に認識され問題への対処が開始される。障害の検知として以下の2つのケースがある。
  - システムによる検知
  - ユーザなど人による検知

システムによる検知としては、SNMP のトラップメッセージによるものや他の機器からの定期的なポーリングによる試験などがある。人による検知は実際にネットワークを利用するユーザが、特定のサービスを受けられなかった等の申告を管理者に対して行うような場合である。

システムによる検知は、ネットワーク管理システムなどが管理者に対して何らかの形で警告メッセージを出す事により行われる。例えば、ネットワーク図上で障害箇所を正常な場合とは異なる色で表示して見せる、管理者へ電子メールを送る、ポケットベルを鳴らすなどの方法 [2] が現在用いられている。人からの場合には電子メール、電話、などの方法がある。

障害の発生は早く確実に必要な管理者に伝えるべきであるが、ユーザによる検知に頼っている部分が大きい。電子メールを用いる場合には、例えばメーリングリストなどの場合、担当者を特定できなくても伝えられる可能性が高い。また障害の状況を文章の形で柔軟に伝えることができ、管理者が計算機を利用している時間帯であれば即座に伝えることができる。一方、流れる情報量や含まれるメンバーが多くなってきた場合、受けとる人にとって冗長な情報が多くなり必要なものまで見落とされる可能性もでてくる。また後から受けとった情報を探す場合にも、メールの形では効率的な検索は難しい。現在多く利用されている電子メールには、利用されているだけの利点もあるが管理対象の増加に従って問題点多くなってきている。

- **問題の特定**
  問題を特定するためには、管理者はできるだけ早くネットワークの状況を把握しようとする。即座に問題の個所やその原因が分かる場合もあれば、短時間で問題を特定できない。様々なコマンドの実行結果、機器の設定状態やその時のネットワークの利用状況など、様々な情報を総合的に用いて判断していく。

- **原因究明**
  問題の特定同様、様々な情報を用いながら状態を把握し、原因を究明する。比較的単純な原因による障害であれば、根本的な原因を明らかにし、即座に復旧作業にうつることができる。もし、そうでなければ障害による影響を最小限にとどめながらネットワークの運用を再開する方法を検討し、応急的な復旧を行う。

- **応急的な復旧**
  障害管理では、根本的な解決方法が分からない場合も、まずネットワークの動作を復旧させることが障害発生時に優先される。もちろん、根本的な解決も必要だが、ネットワークが停止しているといった場合には、とりあえず応急的な復旧をした後に障害発生の根本的な原因を追及することになる。

  しかし、ネットワーク運用を再開させることにより、障害の状況を詳しく調査する事が難しくなる場合等、応急処置のまま運用を続けざるを得ないこともある。

- **根本的な原因究明**
  複雑な原因による障害が発生し、例え応急的な対処によって運用可能になったとしても、長期的な視野にたって、その根本的な原因を発見し対処する必要がある。障害が一時的なもので、応急処置を施すことにより同じ障害が二度と発生しないような場合もあるが、同様の障害が繰り返し発生する場合もある。後者の場合には、障害発生と応急処置による対処を繰り返しながら徐々に障害発生時のネットワークの状態や障害発生への過程などの様々な情報を収集し、それをもとにした状況の分析を行い、時間をかけて根本的な解決をはかって行く事になる。

- **障害からの復旧**
  ネットワークの障害の原因をとり除き、正しく動作するようにする。地理的に離れた場所に目的とする機器がある場合には、他の人にその作業を依頼して作業を行う。

3 ネットワーク管理支援システムへの要求条件

前章からわかるように、ネットワークの障害管理作業は大きく2つの流れに分けて考えることができる。

3.1 障害管理作業のタイプ

管理作業はその過程において2つの段階に分けられる。

1. 運用状態を維持するための障害管理
2. 運用状態を長期的に改善するための障害管理

比較的単純な障害であれば根本的な障害原因がすぐに分かるため、運用状態に戻すのと同時に根本的な問題も解決される。しかし、複雑な問題であればまず1の応急的な回復を行い、その後で2の根本的な解決にあたることになる。

つまり、1の作業は比較的単純な問題の解決もしくは応急的な対策、2の作業は複雑な問題への対処または長期的な改善ということになる。

今後、障害管理の対象となるネットワークが増加すると考えられるため、現在より組織的に管理作業を行っていく必要がある。その場合に、この2つの管理作業はある程度分担して行われるべきである。つまり、1の単純な障害回復および応急的な復旧については、ある程度定型的な業務として行われ、2の複雑な問題への対処は、専門的な知識をもった管理者が柔軟な対処を行っていく。

そこで、障害管理作業の支援を考える場合も、全てに対して同じアプローチをとるのではなく、異なる特性をもつ作業として分けて考えるべきである。双方の作業に必要な支援の項目についてここで挙げる。

1. 単純な問題および応急的復旧
   - 定型的な作業の指示
   - 作業に必要な情報を分かり易く提供
   - 管理範囲以外の機器やソフトウェア、および、他のネットワークの状況の把握

2. 複雑な問題の根本的原因究明

- 発生した障害についての情報の記録 (人が残す)
- 障害発生時のネットワークの記録 (ネットワークの監視によって得られる)
- 様々なコマンドの実行などによって得られる情報を効果的な提示

1の定型的な作業の指示は、2の作業の過程で得られる様々な障害発生の過程についての知識が活かされる。また、2で障害の根本的な原因を究明するするためには、1の管理作業の中で得られるネットワークの状況などの報告が利用される。このように、2つの作業の間では互いに別の作業で得られる情報を利用する。

また、2つの作業は双方ともネットワークに関する情報が必要になるが、それぞれで必要となる情報の質が異なる。たとえば、1の作業にでは障害の発生情報や定型的に必要となる情報など、システムがそのデータの意味を解釈したような情報を必要とする。一方、2の複雑な障害を解決するための作業では、障害発生時の状況を正確に把握するためには障害が発生した前後のネットワークの状態を示す詳しいデータが必要となる。この場合、システムがデータをある程度解釈して管理者に示すのではなく、必要な情報を落とさない為にも、生のデータを内容を変更する事無くしかも管理者がそのデータを解釈するために有効な形式、例えば数値の変化などはグラフ化して把握が容易な形、にして提供する等が望まれる。

このように、障害管理おけるシステムからの支援は、その作業段階によって異なる方向性での支援になることを前提に検討していく必要がある。

4 現在のネットワーク管理における問題

現在の障害管理作業においての問題点について述べる。

- **障害検知のためのネットワークの監視**
  ネットワークの障害検知のためのネットワークの監視が不十分である。IP層での通信の確認など、ネットワークが動作する上で基本的な部分は常に確認する必要がある。

- **管理している機器やネットワークの情報の把握**
  ネットワークの状態を把握するためには様々なコマンドを利用し、またネットワークを構成する機器の情報といった設定情報などをそれぞれ別の操作を用いなければ取り出すことができない。単純な作業への定型的な対応の場合の情報収集は自動化が可能である。

  また、SNMP[1] によって遠隔地の計算機の情報を得られるようになったが、それでもSNMPだけでは得る事のできない情報も扱わなければらないため、作業が繁雑である。

- **原因追及のためのネットワークの監視**
  ネットワークの障害検知と、障害発生時の状況を把握するために必要な、定常的なネットワークの監視が不十分である。

- **障害発生時の記録**
  現在、発生した障害に関する記録が不十分である。障害への定型的な対処を明らかにするために、過去の障害への対処記録は役立つ。また、根本的な原因が解決されない場合には、同じ障害が繰り返される場合も多く、根本的な問題の解決のためにも過去の障害事例の蓄積はは有効である。また障害の記録は、当該ネットワークの管理者間や、また、別のネットワークの管理者同士の間で共有するための方法を提供する事が重要である。

- **情報の伝達**
  ネットワークの障害には、できるだけ短い時間で対応することが望まれるため、様々な場面で必要な情報を的確に伝える必要がある。しかし、状況に応じて的確な情報伝達の手段が利用されているとは言えない。警告情報の伝達のために現在多く用いられている電子メールは、手軽に使えるという利点もあるが確実さに欠ける。

  また、他のネットワークに関する情報を把握するための良い手段が提供されていない。現在、メーリングリストによって相互接続されたネットワークの管理者間で障害情報をやりとりしている場合が多いが、情報量がある程度多くなった場合には、必要でない情報が多くなり本当に必要な情報を得るのが困難になってくる。

5 ネットワーク管理の支援

ここではネットワークの障害管理に必要な支援項目について述べ、このような支援が実現された場合の管理作業の流れを示す。

5.1 障害検知のために必要な支援項目

- **障害検知のためのネットワーク監視**
  ネットワークの障害を検知するために、ネットワークの状態を常時監視し、障害発生と判断される状態の変化によって何らかの警告を出す必要がある。ネットワークの動作の基本的な部分を支える部分について、障害の発生頻度や、全体に与える影響などに基づいて得られる重要度に応じた監視を行う。

- **管理範囲の障害に関する情報の獲得**
  障害の種類によって必要とされる情報は異なるが、障害が発生した部分を構成する機器やソフトウェアの設定に関する情報の中から、発生した障害のパタンに応じて定型的に必要とされる情報は、障害発生と同時に管理者に提示する事ができる。

  定型的な業務として管理作業にあたる人に対しては、単純なデータを示すのではなく、発生した障害に応じてシステムがある程度情報を解釈し、障害を解消するために必要な作業を示唆する必要がある。

  一方、障害を細かく分析し長期的な解決にあたる管理者に対しては、障害発生時の状況を分析するために必要となるさまざまな情報を容易に収集できるようなインター

フェースを提供する必要がある。集められた情報をシステムが必要以上に解釈し、加工された情報として示すのではなく、むしろ、システムを利用する管理者が、集められた情報を整理し解釈する作業を支援する事に重点を置くべきである。

- **障害分析のためのネットワーク監視**
  ネットワークの障害原因を追及する為には、障害発生の前後のネットワークの動作状況を詳しく調査する必要がある。障害に至った状況を再現するといった方法による調査も可能だが、それではネットワークの運用に支障をきたしてしまう。

  ネットワークの運用に影響を与えずに障害の原因究明を行うためには、常にネットワークの状態を監視したデータを記録し、障害原因究明の際には必要なデータを後から参照できるような機能が要求される。

  しかし、あらゆる項目について同じようにモニタし記録を残すのではなく、障害発生時の直前の状態については、全てのプリミティブなネットワーク構成要素に対して比較的短い時間間隔でモニタしたデータを記録しておき、時間が遡るに連れて、それらのデータをある程度集計したもののみを記録しておくというアプローチが必要であると思われる。これらのデータは、障害を細かく分析する際に利用される可能性があるものであり、ネットワークの構成に応じて、その収集の仕方は、容易に設定可能である必要がある。また、管理者が障害を分析し把握するために必要な情報を、繁雑な手続きなしに提示できるようなインターフェースが要求される。

- **障害の記録**
  障害が発生した場合、それがどのように検知され、どういった症状を示し、結局どのような原因によって起きたのか、といった障害の事例は、同じネットワークや類似した構成を持つ他のネットワークで、後に同様の障害が起きた場合に非常に有効である。そのため、ネットワークの障害対処の記録は残すべきである。記録が増えた場合には、さらにそれをデータベースのような情報を共有できるシステムを利用し、必要に応じて他の管理者や、他のネットワークからも参照できるようにする。

- **管理者間の情報交換**同じ管理範囲を複数の管理者が共同で管理している場合には、お互いに密な情報交換が必要である。また、インターネットでは異なるネットワークにより運営されるさまざまな機器やソフトウェアが相互に依存しながら動作しているので、異なる管理範囲の管理者同士でも、他の管理範囲で起こった障害をある程度把握する必要がある。

  密な情報交換のためには、作業記録のようなものを共同管理する管理者間で共有する。そのために、現在多く利用されているメーリングリストように、ある決まったメンバー全てに対して情報を送りつける方法もあるが、情報が多くなるに従い情報の欠如、冗長な情報が増えるなどの問題がでてくる。ある程度大量になった場合には、必要に応じて検索して情報を得られる、データベースのようなシステムで情報を共有するといった方法が良い。

  しかし、障害発生時の作業に関わる連絡では、確実に一刻も早く連絡する必要がある。そこで、受け取る管理者の注意を促すような警告情報の伝達手段を準備する。

  また、直接管理に関わっていない他のネットワークについての情報も、他での状況をある程度把握するためにも、データベースのような形で皆が参照できるシステムで提供されるべきである。

5.2 支援システムのある障害管理作業の流れ

障害の検知から復旧までの作業の理想的な流れとして、次のようなものが考えられる。(図 2)

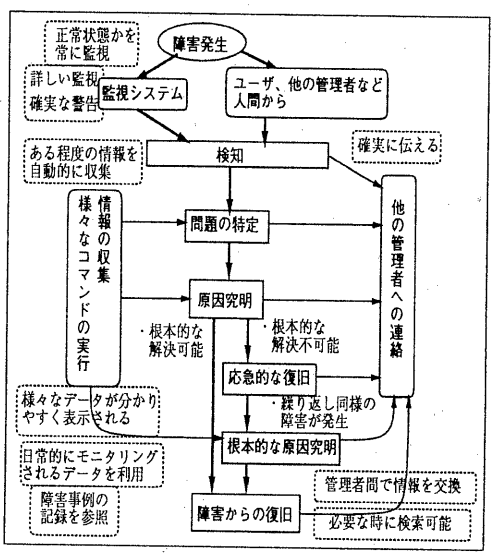

図 2: 理想的な障害管理作業の流れ

- **障害の検知**
  多くの障害はネットワーク監視システムからの警告メッセージによって知ることができる。ネットワーク監視システムによって認識されず、ユーザや他の管理者からの連絡によって発見された障害についても、警告メッセージとして管理者の注意を促す形で送られる。

- **問題の発見**
  障害管理システムによって検知された障害についてはある程度の状況を把握するためのコマンドがシステムによって実行され、管理者はその結果を参照する。また問題が発生した部分についてのネットワークの構成に関する情報、接続先を担当する連絡先など、障害に対処するために必要となる可能性のある情報は容易に参照できるようにする。

- **原因の究明**
  ある程度自動的に収集された情報や、コマンドの実行結果を用いながら調査する。比較的単純な原因による障害であり、短期間で根本的な対応ができるような場合には、即座に復旧作業を行う。コマンド実行結果などのを含めて作業を記録し、他の管理者へ作業の進行状況などを連絡する。

- **応急的な復旧**
  障害とその原因との因果関係がすぐには解明できない場合や、根本的な対処を行うためには、比較的長期間のネットワーク停止を伴うような場合には、応急的にネットワークの根本的な原因が分からなかった場合には、根本的な原因究明を専門家に依頼する。

- **根本的な原因の究明**
  専門知識のある管理者が根本的な障害原因の究明を行う。障害発生時の状況を把握するために、障害発生の前後一定期間のネットワークの状態を監視した記録を参考にし、様々なコマンドからの情報も効率的に扱えるような状態で、調査を行う。また、過去の障害発生事例なども参照する。

- **復旧**
  必要な復旧作業を行う。他の担当者へ作業を依頼する場合でも、確実な連絡が必要である。また、作業の記録を残し、他の管理者へ対しても障害から復旧したという情報を提供する。

6 支援システム実現のために考慮すべき点と今後の課題

前章で支援システムに必要とされる項目を挙げたが、これらを実現するためにはそれぞれの作業の流れや、作業を担当する人の条件なども考慮しなければならない。

- **障害検知のためのネットワーク監視**
  ネットワークの障害検知に有効な監視ポイントの特定は容易ではない。また、ある値が正常なのか異常なのかということは、対象となるネットワークによって異なる。そのため、有効な監視を実際に行っていくためには試行錯誤が必要となる。はじめは、ある典型的な例での監視を行い、障害発生のどのくらいを認識できるのか、ということを考察し、より的確な監視ポイントを設定していく。このためには、障害の記録や専門的な知識のある人の意見なども重要である。

- **障害分析のためのネットワーク監視**
  障害発生時のネットワークの詳しい状況を把握するための監視ポイントはそれを使う管理者が柔軟に指定できるようにするべきである。また、得られたデータはそれを用いる人が把握しやすいように(例えばグラフ化するなどして)見せる工夫が必要である。また、知識があればデータから簡単に分かるような事実をシステム側から示唆するといったようなことも必要ない。

- **障害発生の記録**
  人が記録を残すためには、その人に大きな負担をかけることになる。そこで、極力システムからの出力結果を用いるようにする。また、後に検索しやすいようにキーワードを設定したり、他の障害事例との関係付を定義したりする作業が容易に行えるようなインターフェースも提供する必要がある。

- **管理者間の情報の交換**
  現在、障害の記録や障害に関する情報交換として利用されている電子メールは、自由に記述することが可能であり、計算機ネットワークを日常的に利用している人にとって気軽に利用できるシステムである。このメールでの現在の情報交換の様子も参考にするべきである。

作業を支援するためのシステムは、利用者の実際の作業量や、それを利用する各利用者にとって、どれだけの利益になるかということが、そのシステムが利用されるために重要である[3]。そのため、これを利用する人の特性や利用状況を詳しく検討した上で本当に作業が支援されるようなシステムになるよう検討しなければならない。

今後は、ここに挙げた障害管理支援に必要な各項目それぞれについて、具体的にどのようなことが必要になるのかを詳しく分析し、実装に結びつけていく。

7 まとめ

今後のインターネットでの障害管理作業を支援するシステムを構築していくために、現在の障害管理の作業の流れを分析した。それにより、障害管理作業には一刻も早く運用を再開するための作業と、長期的に見て根本的な解決をするための作業の2つの流れがあり、支援システムとしてもそれぞれに対応して異なるアプローチが必要であることがわかった。そして、それらの作業の流れを有効に支援するために、それぞれの管理作業に応じてネットワークに関する情報の提供を行うための要求項目について説明した。

参考文献

[1] Case, J., Fedor, M., Schoffstall, M., and J. Davin, "A Simple Network Management Protocol (SNMP)", RFC 1157, SNMP Research, Performance Systems International and MIT Laboratory for Computer Science, May 1990.

[2] WIDE プロジェクト, "1992 年度 WIDE プロジェクト研究報告書 (第 16 部 WIDE/PhoneShell pp.595-561)", 1993.

[3] Jonasan Grudin,"Ehight Challenges for Developers", Communications of the ACM, Vol.37,No.1, January 1994.