第 9 部

トラブルチケットシステム

第 1 章

はじめに

現在では、異機種で小型かつ高性能な複数の計算機を相互接続してネットワークを構築し、様々な計算機資源を共有する分散環境が一般的になってきている。WIDE インターネットには 80 以上の組織が接続されており、世界中で IP 接続されている計算機も 100 万台以上になる。

インターネットを介した大規模広域な分散環境では通信の遅延が比較的大きくなるため、利用されるサービスもローカルでの分散環境に比べて限られる。しかし、最近では高速の専用回線も利用されており、ローカルエリアネットワーク内で利用されているサービスと同様のサービスがインターネットを介して利用され始めている。また、高速の回線が利用できることに伴って、大量のデータのやり取りを必要とする高度なサービスも開発されている。

回線の高速化、利用されるサービスの多様化、インターネットへ参加する組織の急増などに伴ない、交換される情報量も増加し、広域分散環境実現の基盤となるネットワークの信頼性への要求もますます大きくなってきている。

このように大規模化かつ複雑化してきたネットワークを利用していくためには、ネットワークを構築しているハードウェアならびにソフトウェアの整備や保守が必要である。ネットワークを運営していくための一連の作業は**ネットワーク管理**という言葉で表現されているが、その作業は多岐に渡っており、計算機ならびにネットワーク技術全般の知識を必要とする。これまで、ネットワーク管理の作業内容としては、構成管理、アカウントの管理、障害管理、セキュリティ管理、性能管理などが挙げられおり [78] それぞれが議論の対象となっている。本稿では、これらのうち障害管理に関する問題点を中心に述べていく。

これまでにネットワーク管理の為に提案された枠組の代表的なものとして、ネットワークを構成する機器やソフトウェアの情報をネットワークを介して交換するプロトコルである SNMP[79]、SNMP で扱われる情報を定義した MIB[80] などが挙げられる。ただし、これらは先に挙げたような様々なネットワーク管理作業で利用される情報を提供するが、ネットワーク管理そのものについて新たな考えを提供しているわけではない。

障害管理に関しては、SNMP によりネットワークを構成している機器の状況をある程度把握することも可能になった。しかし現実に障害が発生した場合の原因究明や復旧には、ネットワークの技術に詳しい人間の経験則と知識、そして比較的単純なツールを用いて対応していることが多い。また、障害の影響により SNMP による通信が利用できな

くなり、障害発生時に必要な情報が得られない可能性もある。

インターネットで発生する障害では、あるネットワークが原因となってその他の多くのネットワークにも影響を与え得る。そこで、独立して管理されている様々な組織のネットワークの相互接続によって構成されているインターネットでは、各ネットワークの管理者が情報交換を行いながら協調して障害管理を行う必要がある。

そこで、インターネットでの障害管理を行う上で必要となる情報に着目し、ネットワーク管理者が情報を扱う方法について述べていく。

本稿では、まず、本稿で用いる用語の定義を行い、次にネットワークならびにインターネットを管理する際に管理者間で障害に関する情報交換がどのように行われているかについて述べる。その後、実際に発生している障害の例を紹介する。そして、障害情報の交換として現在利用、または提案されている方法を紹介し、それらの問題点をあげ、最後にそれら問題点の解決方法について提案する。

第 2 章

ネットワーク管理

この章では、まずネットワークならびにインターネットという言葉の定義を行う。そして、インターネットでの管理体制ならびに、管理のための情報について述べる。

2.1 ネットワークとインターネット

ここでは、本稿で用いる言葉の定義を行う。

2.1.1 ネットワーク

最も単純なネットワークは、それぞれのネットワークインターフェースを介して複数の計算機を Ethernet や FDDI といった物理媒体に接続することによって構築される。 一つの物理媒体からなるネットワークは、ブリッジ、ルータなどの様々な接続機器を用いて延長することができる。

異なるベンダの計算機の様々な物理媒体を介した相互接続は、**プロトコル**と呼ばれる規約に従うことによって実現されている。プロトコルは、通信の手順や交換するデータのフォーマットの規定である。本論文で対象とするネットワークのプロコトルは、ある特定のベンダが用いているものではなく、詳しい仕様が公開されているため様々なベンダによって実装されているものである。そのため、様々な種類の計算機がこのネットワークのプロコトルを利用して相互接続されている。

ネットワークのうち、大学のキャンパスやあるビルの中など比較的狭い範囲のネットワークは**ローカルエリアネットワーク** と呼ばれる。ローカルエリアネットワークは、単一の組織内で構築されていることが多く、その組織全体での合意の上で管理運営される。

以降で**ネットワーク**という言葉は、ある組織によって管理されているローカルエリアネットワークを表すこととする。

2.1.2 インターネット

一般に、多くのネットワークを相互接続したネットワークをインターネットと呼ぶ。 インターネットを実現するための、現在最も一般的に用いられているプトロコルは、1970 年代にアメリカの DARPA(国防省高等研究計画庁) で開発されたネットワークプロトコ

ル [19] であり、これは一般に TCP/IP(Transmission Control Protocol/Internet Protocol) と呼ばれている。TCP/IP は、ネットワーク間の相互接続ための規約のみならず、あるネットワーク内での通信規約も含んでいる。 TCP/IP については後ほど詳しく説明する。

ネットワークとネットワークの間は、ルータ (またはインターネットルータ) と呼ばれる計算機を介して接続される。ルータはパケットの行き先を示す識別子によって一方のネットワークから他方にパケットを転送する、経路制御を行う。ルータ間は公衆回線や専用回線によって point-point 接続されており、現在用いられている回線の速度は数 k〜数百 kbps であり、Ethernet などに比べて遅いことが多い。

TCP/IP によるインターネットはアメリカを中心に発展し、現在は世界中に広まり、日本でもその一部となるインターネットが構築されている。以降では**インターネット**は TCP/IP プロトコル体系によるインターネットを表す。

2.2 ネットワーク管理の機能による分類

ネットワークを安定して運用していくための作業全般を総称して**ネットワーク管理**と呼ぶのが一般的である。

OSI ではネットワーク管理を機能的には次の 5 つに分類している [78]。

障害管理 ネットワーク上で発生する問題への対処

構成管理 ネットワークの接続や設定など構成に関する管理。

性能管理 ネットワークの性能を向上させるための管理

アカウント管理 ネットワークの利用に関する管理

安全管理 ネットワークへ不法にアクセスされないための監視や対策

このように管理作業には、ネットワークの動作に関係する機器の保守や整備、ソフトウェアの設定や整備、ネットワークの性能のチェックなど、様々な作業が含まれる。ネットワーク管理の担当者は**ネットワーク管理者**または単に**管理者**と呼ばれる。 計算機をネットワークに接続するためには、ネットワークを構成する各機器それぞれに責任をもって保守管理していく管理者が必要である。何故なら、各計算機で動作しているソフトウェアはネットワークというシステムを構成する一部であり、一部の誤動作はシステム全体にも影響を与えるからである。

例えば、ネットワークの規模拡大に伴いネットワークの構成が変更された場合それに伴ない種々なソフトウェアの設定変更が必要になる。また、計算機ネットワークの技術は現在発達段階であり、ネットワーク全体で新しい技術を導入するためには、ハードウェアの変更や新たに開発されたソフトウェアを導入するなどの作業が必要になる。このように、ネットワークシステム全体を安定して運用していくためには、システムの細部を構成する各要素を常に監視し、気を配っていく必要がある。

2.3　ネットワーク管理体制

インターネットはここ数年で急速に発達した技術である。ネットワークの規模の拡大に伴い管理対象も拡大してきたが、現実には管理者の数はネットワークの規模拡大に対して十分であるとはいえない。また、ネットワークは数多くの計算機で動作している複数のプログラムが協調して動作するシステムであるため、相互接続される計算機の増加に従いシステム全体は複雑になりその管理も困難になりつつある。

したがって、計算機利用環境としてのネットワークが必要不可欠になる一方で、ネットワーク管理者への負担は増加し続けている。実際は、この急速なネットワークまたはインターネットの拡大に応じて、管理組織は自然発生的に組織されてきた部分も多く、規模が拡大してきた現在ではその体制にいくつかの問題もかかえている。そこでまず以降では、現在のネットワークならびにインターネットの管理体制について考察していく。

2.3.1　ローカルエリアネットワークでの管理体制

一つの組織内で構築されたローカルエリアネットワークは、複数のセグメントが相互接続されてネットワーク全体が構成されている場合が多い。ネットワーク管理の作業は計算機のシステム管理と重なる部分も大きいため、ネットワーク全体を一ヶ所で管理するのではなく、セグメントを単位としてネットワーク全体をいくつかに分けて管理に関する作業が行われる場合が多い。したがって、各計算機のネットワークに関する設定や動作のチェックなどの作業は管理部分ごとに行われる。しかし、ある計算機で設定に不備があった場合は、ネットワークの他の部分にも多大な影響を与え得るためそれぞれの計算機での管理作業は重要である。

各管理部分が相互接続されてネットワークを構築するためには、各計算機での設定のいくつかはネットワーク全体で協調して行う必要がある。また、相互接続をどうやって実現するかということは、各部分で合意して行わなければ実現できない。そこで、各管理部分の管理者をまとめる**全体の管理者**が必要となる。全体の管理者は、物理的には各ネットワークの接続部分の機器を管理する必要がある。 また論理的には、相互接続を実現するために各ネットワークで必要な情報を把握し、各部分の管理者間が協調するためにその情報を提供する必要がある。

実際のネットワーク内部での相互接続は相互接続を提供するためのバックボーンネットワークを構築し、そこにルータとなる計算機を接続することによって実現される場合が多い。そのため、全体の管理者は各ネットワークのネットワーク管理作業を取りまとめるだけでなく、それらの相互接続を提供するルータやネットワークの物理媒体についての管理作業も担当する。

あるセグメントの管理者にとって、物理的な管理対象は接続される計算機とそれが接続している物理媒体である。しかし、そのセグメントが他のセグメントと接続されるためには通信のためのソフトウェアの設定などが必要である。協調が必要とされる事柄については全体の管理者によって、または各管理者の協議によってある方針を決め、それ

に従って設定する。

協調が必要な典型的な例としては以下のようなものが挙げられる。

- IP アドレスの設定
- 経路制御プログラムの設定
- DNS の設定

このように、ネットワーク管理は作業は複数の管理部分に分かれるがそれらが協調して行われなければならない。

このように、組織内部のネットワークの管理体制としては、ネットワークの接続構成や組織構成を反映して階層的に管理責任の範囲を分割して行う**階層型管理体制**をとられることが多く、またこれは有益だと考えられる。

例として、大学のローカルエリアネットワークがサブネットで分割されている場合を考える。ネットワークはサブネットがゲートウェイによって相互接続されることにより構築されている。ネットワーク内のパケットの配送はサブネットごとに行われ、また DNS でのゾーンはサブネットを単位として定義される場合が多い。ネットワーク全体で協調が必要な設定は、大学全体のネットワークの管理に責任を持つ管理担当者の指示に従って行われる。そこでこの場合は、サブネットを単位とした管理部分の分割が自然であると考えられる。

また、大学に複数のキャンパスがあり、それぞれのキャンパスのネットワークを相互接続して大学全体のネットワークを構築している場合には、管理構造の階層はもう一つ深くなり、各サブネットの管理者群、各キャンパスでのサブネットの管理者群をまとめる管理者、各キャンパスの管理者群をまとめる大学全体のネットワークを管理する管理者というような構造の管理組織をもつ必要がある。

ローカルエリアネットワークでの管理区分の例を図 2.1に示す。

2.3.2 インターネットでの管理体制

バックボーンネットワークに複数のネットワークが接続されて構築されているインターネットの管理は、バックボーンネットワークを構築する組織の管理者を中心として行われるのが一般的である。

インターネットでは、あるバックボーンネットワークにより複数のネットワークの間接続が実現されており、バックボーンネットワークの管理者はローカルエリアネットワークでの管理の場合での管理部分をまとめる全体の管理者と同様な役割を果たす。インターネットの場合、物理的にはバックボーンネットワーク自体とバックボーンと各ネットワークとの接続を提供する機器を管理し、論理的には相互接続を実現するためのソフトウェアの設定を管理する。

インターネットの場合にローカルエリアエネットワークと異なる点として相互接続されるネットワーク構成要素が、一つのネットワークという規模の大きなものになるということである。

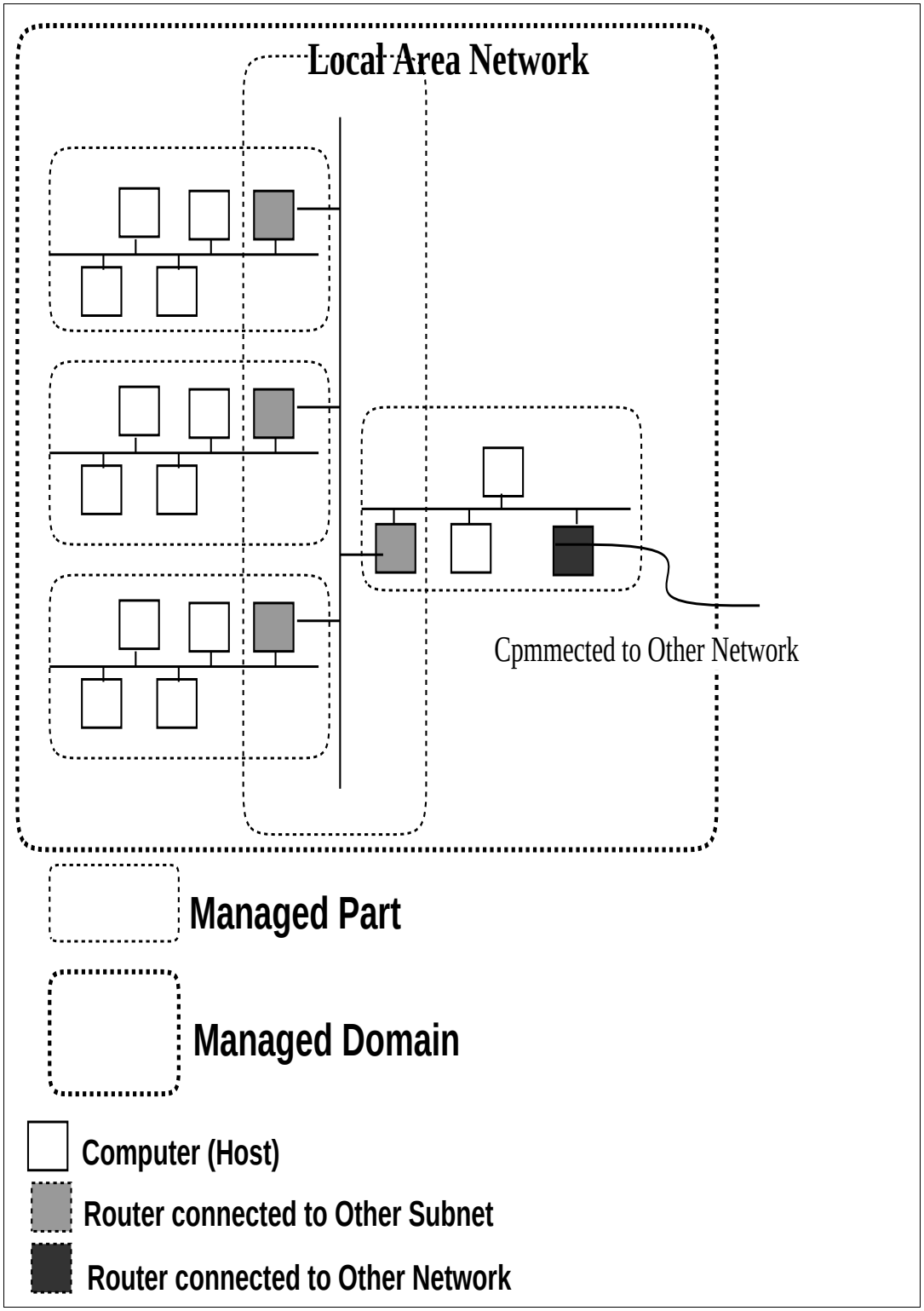

図 2.1: ローカルエリアネットワークでの管理部分

インターネットの相互接続に必要で、各ネットワークが情報を相互に参照しながら動作するソフトウェアの例として、以下がが挙げられる。

- IP のネットワークアドレスの設定
- 経路情報交換プログラム
- DNS の設定

これらはネットワーク内部の設定の場合はそのネットワークの各管理部分の協調で行われたが、インターネットの場合は各管理部分にあたるのがローカルエリアネットワークである。アドレスはネットワークごとに割りあてられ、経路制御もネットワークアドレスを用いたものが対象であり、インターネット全体に承認されるような名前をネットワークごとに割りあてる。

インターネットの管理では、ローカルエリアネットワークという抽象的なネットワーク構成要素をバックボーンネットワークによって接続したネットワークの管理であると考える。各ネットワークの接続の設定の方針は、バックボーンネットワークの管理者によって、もしくは各ネットワークを代表する管理者の協議によって決められる。

組織内部のネットワークでは、階層的な管理体制によりある程度全体の方針が決められた上で各部分はそれに従って管理される。一方、異なる組織のネットワークが多数接続されたインターネット全体の管理は、各組織内部のネットワークと同様な階層型管理体制にのものとで、全体としての管理方針を決めそれに従って行うのは難しく、むしろそれぞれの組織が独立した意思を持ちながら、全体の安定を考慮し協調して行われるものと考えることができる。

そこで、インターネットの管理を考える上でバクボーンネットワークに接続される各ネットワークを一つのまとまりをもった管理部分と考え、**管理ド メイン**という言葉で表すこととする。

インターネットの管理では、管理ド メン間のを代表する管理者とインターネットバックボーンの管理者が協調して行う必要がある。

各管理ド メインを代表する管理者の役割は以下のようにまとめられる。

- インターネットとネットワークを接続する機器の管理
- ネットワークの内部の情報のうち外に必要なものをネットワークの外へ対して伝える。
- ネットワーク内部のインターネット利用者に対して必要な情報を伝える。

まず、ネットワークとインターネットとの接続部分は通常専用回線などの通信媒体とルータがある。これら物理的な接続部分については管理する必要がある。

また、論理的にはインターネットとの接続で必要とされる設定がネットワーク内部で正しく行われているかどうかについて責任を負うことになり、インターネット側に対して必要なネットワーク内部の管理に関する情報を提供するインターフェースとなる。この

場合、ネットワークの管理者はネットワークの外部で必要とされる形に情報の抽象化を行っているといえる。

インターネット全体は、論理的には次の図 2.2のような構造として捉えられる。

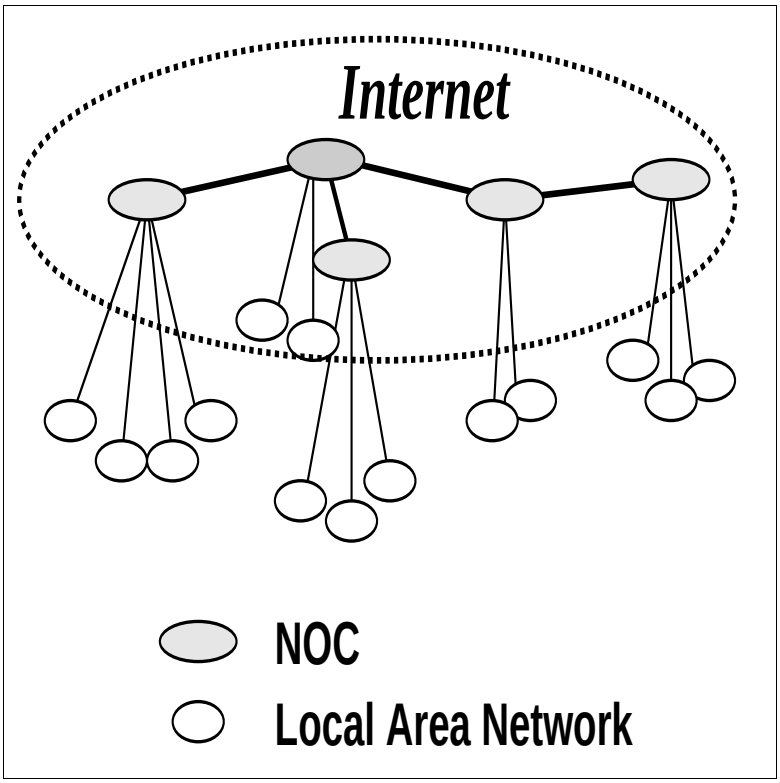

図 2.2: インターネットの論理的な接続

また逆に、ネットワーク内部に対してもインターネットの管理に関する情報のうち伝える必要のある情報を伝える。例えば、インターネットに接続されているあるネットワークとの通信が不可能になった場合には、ネットワーク内部の利用者に知らせる必要がある。

なぜなら、図 2.3に示されるように、ネットワーク内の利用者はサービスを利用することが重要であり、インターネットの構造について知る必要は必ずしもない。

各管理ドメインの管理者は、実際の作業だけでなくネットワークの管理のため必要とされる情報を伝えるインターフェースの役割も行っている。

また、バックボーンの各 NOC は多くの場合地理的に離れて配置されており、バックボーンネットワークが正しく安定して運用されていくためには、各NOCごとに管理を行いそれぞれが協調して作業を行っていく必要がある。そこで、バックボーンネットワークの管理では各 NOCが管理部分となり、バックボーンネットワーク全体が一つの管理ドメインと考えることができる。

また、バックボーンでの接続は NOC によって実現さてりいるため、各 NOC の管理者は、その NOC に接続されているネットワークに関して他の NOC に必要とされる管理に関する情報を伝える役割を果たす。

つまり、NOC の管理者として次のような役割が挙げられる。

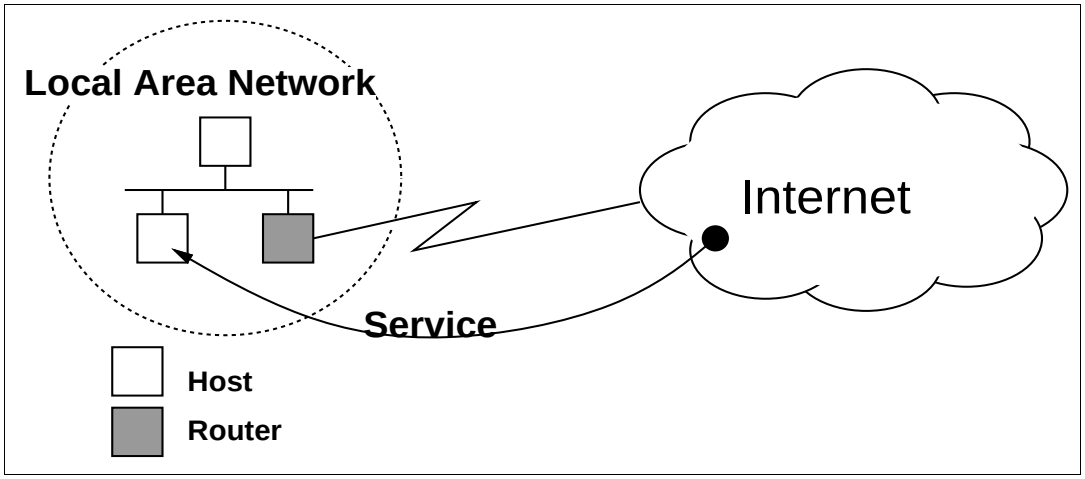

図 2.3: 利用者にとってのインターネット

- 各 NOC の接続機器とそれを接続する物理媒体の管理
- NOC 間の接続について管理に関する情報を交換する。
- その NOC に接続されているネットワークについて管理上必要な情報を他の NOC の管理者に伝える。
- NOC に接続されるネットワークに対してインターネットの管理に関してそのネットワークが必要とする情報を伝える。

インターネット全体の管理体制を把握するために、その全体の構造を次の図 2.4に示す。

2.4 インターネットでの管理情報

ローカルエリアネットワークの場合同じ組織の内部では、ネットワークの構造やホストに関する情報が比較的簡単に得られる。しかし、インターネットの場合、接続される各ネットワークはネットワークの内部構造やホストの情報など公開が望まれない場合が多く、外部からは情報を得ることが比較的困難な場合が多い。

ネットワーク管理の為に必要な情報を得る方法として、ネットワークを構成する機器 (ネットワーク構成要素) に関する情報をネットワークを介してやりとりするためのプロコトルである SNMP が現在標準として広く認められている。

SNMP での管理モデルは、ネットワーク管理を行う Network Management Station(NMS) と、管理される対象である Managed System (MS または ネットワーク構成要素) で構成される。(図 2.5参照。)

NMS として動作するプログラムはマネージャと呼ばれ、Managed System 上で Manager と情報交換するプログラムはエージェントと呼ばれる。SNMP では、マネージャからエー

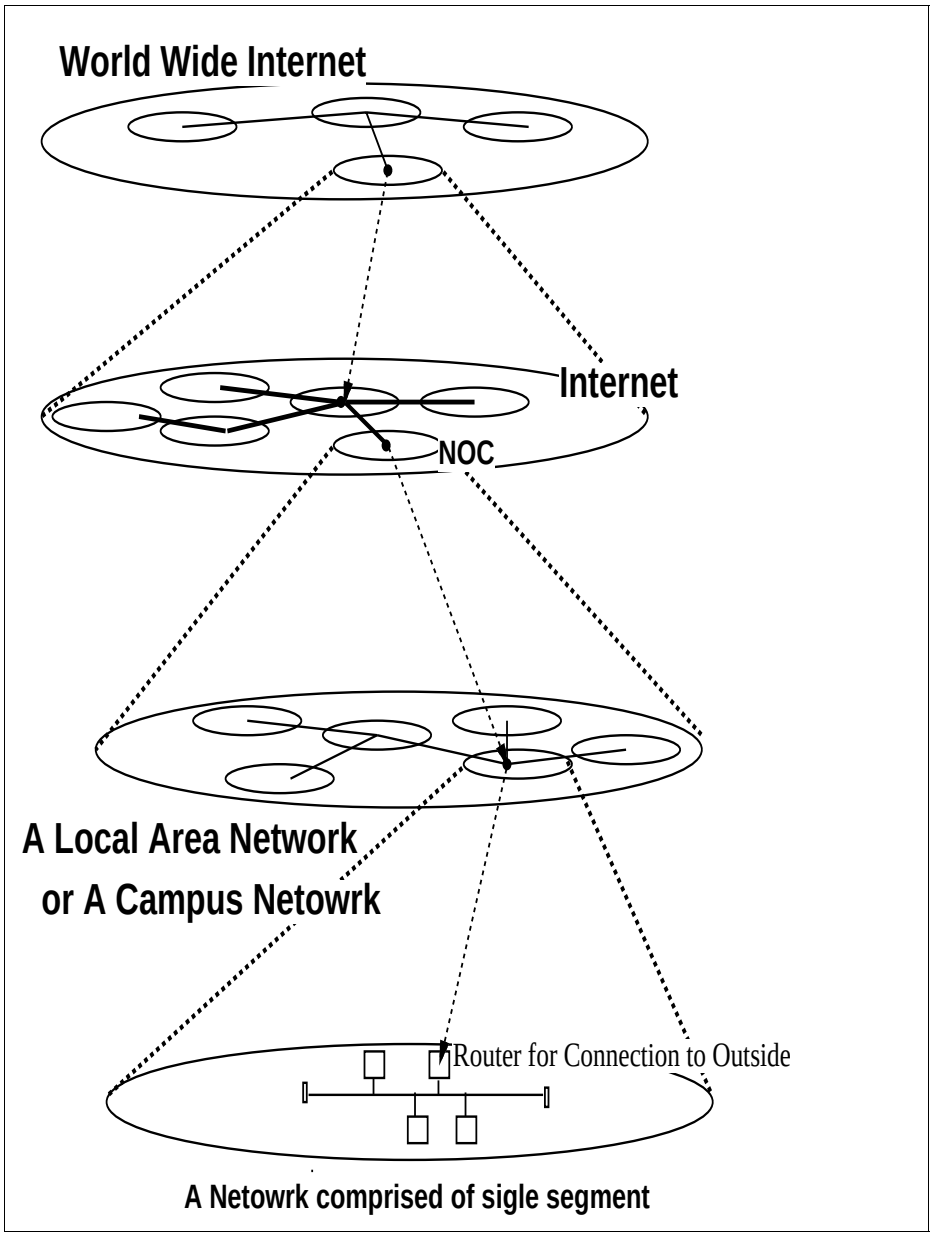

図 2.4: インターネットの階層構造

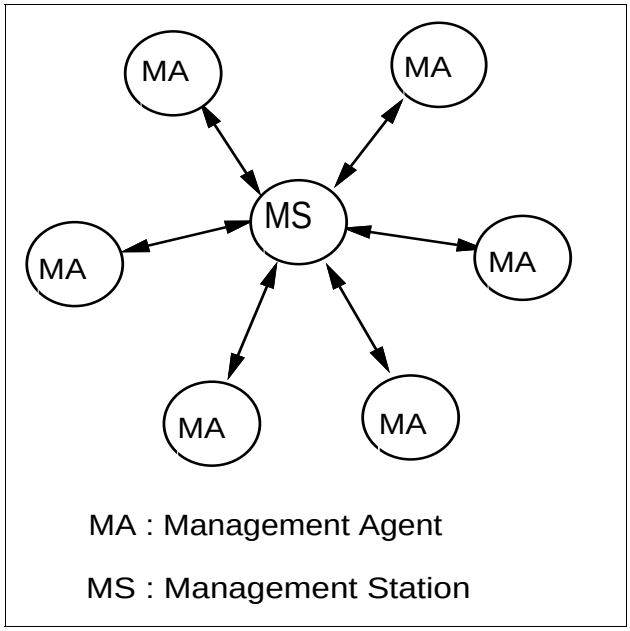

図 2.5: SNMP での管理モデル

ジェントへの情報の問い合わせにエージェントが応える、マーネジャがエージェントにある値を設定する、エージェントがイベントの発生を非同期にマネージャに知らせる、という操作が定義されている。これらの操作は、UDP を用いて行う。情報の特定は MIB というネットワーク構成要素を示すオブジェクトの識別子を用いて行われる。そのため SNMP によって扱うためにはその対象をマネージャとエージェントで合意された MIB として定義しなければならない。

SNMP では、MS としてネットワークを構成する物理的な構成要素を想定してて設計された。基本的には、IP アドレスによってネットワーク構成要素を指定し、MIB によってその構成要素に含まれる特定の情報が指定される。例えば、標準的な MIB である MIB-II[80] の項目としては、その計算機持つネットワークインターフェースの数、特定のネットワークインターフェースをを通過したパケット数の累積値、そのインターフェースに接続されている物理媒体の速度、などがある。SNMP では MIB の 1 つの項目ごとに一つの UDP のデータグラムを出して問い合わせ、それに対する応えのデータグラムを必要とする。そのため、大量の情報を得るためには少なくとも MIB の項目の数の 2 倍以上、UDP のパケットがマネージャとエージェントの間で交換される。

SNMP によって、計算機を直接利用せずに必要なデータだけをネットワークを介して扱うことができるようになった。そのため、複数のネットワーク構成要素を遠隔地からある程度管理することが可能になった。しかし、ひとつの管理ドメインに属するネットワークのように比較的狭い範囲で、しかもある程度自由に情報を得ることができるような場合には有効であるが、異なる管理ドメインが相互接続され比較的広い範囲での情報交換が必要な場合には、SNMP は必ずしも適さない。

管理対象の規模が大きい場合に SNMP を利用した欠点として次のものが挙げられる。

- IP アドレスと MIB の項目によって問い合わせを行うため管理対象の拡大に比例して SNMP によるトラフィックが増大する。

- ネットワーク構成要素それぞれを IP アドレスによって指定する方法であるため、ネットワークの構造を知っている必要があり、また管理対象となるネットワーク全体の把握は難しい。

- インターネットの場合複数の管理ドメインが相互接続されており、別の組織からなる管理ドメイン内の詳しい情報へのアクセスは許されていない場合が多い。そのため、各機器を指定する SNMP での問い合わせは困難になる。

このような SNMP の問題点をある程度解決し、階層化した管理体制になっている規模の大きなネットワークで管理情報を扱うためには、各管理部分または管理ドメインをネットワーク構成要階素としてとらえる管理情報の抽象化が考えられる。そこで、このようなネットワークの管理情報を扱う仮想エージェントを用いた SNMP が新たに提案されている [81][82]。仮想エージェントの実装方法とは、ブジッリやモデムのような IP アドレスが割り当てられていない機器に代わってその管理情報を扱う Proxy(**代理**) **エージェント**を利用する。

SNMP を利用する場合、得られる情報の定義である MIB が重要となる。ここ数年の間に様々なネットワーク機器に関して MIB の定義が行われてきたが、SNMP では MIB に定義された情報しか利用することはできず、また必要な情報が MIB でどのように定義されているか知る必要がある。

数多くの MIB が定義されたとしても、ネットワーク管理で必要な情報は SNMP による MIB に定義された情報だけで充分とは言えない。何故なら、ネットワークの管理を行うためには、前に挙げたように管理者の間での情報交換が重要になるからである。現在、他のネットワークの管理者との情報交換には、主に電子メールや電話などが用いられている。メールの利用方法として特定の管理部分の管理者をメンバーとするメーリングリストが多く用いられている。インターネットの管理の場合には、バックボーンネットワークの管理者と各接続組織の代表者が含まれている。このメーリングリストでは、各設定に関する合意や問題が発生した場合の報告、障害への対処の依頼などのメールが交換される。

情報交換を行う管理ドメインが少ない場合はこれで充分であったが、インターネットの接続組織の数が増えるに従い、やりとりされるべき情報量も増えメーリングリストを用いた情報交換は必ずしも有効であるとは言えなくなった。また、インターネットに障害が発生した場合はインターネットのサービスを用いた連絡は困難になるという重大な欠点がある。

そこで、次章以降ではインターネットの管理、特にインターネットに発生した問題点を複数の管理ドメインが協調して解決していくための管理に利用する情報と、その交換方法について新たに提案していく。

第 3 章

インターネットでの障害管理

この章では、インターネットでの障害管理について述べる。
まず始めに、ネットワークの障害を定義し、実際に広く行われている障害管理の方法や用いられているツールやプロコトルについての分析を行う。

3.1 インターネットの障害

ここでは、まずネットワークの障害について定義を行う。その後、障害への対処方法とそこで利用されるツールやプロコトルについて説明する。最後に、インターネットの管理者の間で交換されたメールの記録をもとに実際にインターネットでどよのうな障害が発生しているか、障害を解決するためにはどのような情報が必要か、障害によって通信にどのような影響が与えられるか、ということについて考察する。

3.1.1 ネットワークの障害

計算機のネットワークは、様々な機器とソフトウェアの集合が協調して動作するシステムである。
そのため、一部分に問題があった場合でも、全体として正常に動作しているとは言えない。そこで、ネットワーク全体の中の一部分にネットワークの利用上の問題が発生し、その原因がネットワークを構成する要素にあるならばそれを**ネットワークの障害**とする。ネットワークは様々な要素から構成されているため、障害にも様々な場合がある。
ネットワークを利用する立場からは、ネットワークのサービスが完全に利用できない場合は明らかに障害と見倣すことができるが、例えばネットワークの混雑のため円滑な通信が行われない場合などはそれが障害であるか単に利用者が多いためなのか判断することができない。この場合、利用状況から当然予測されるネットワークの混雑が原因でネットワークが円滑に利用できない場合は障害ではないとする。しかし、ネッワークを構成する機器やソフトウェアに何らかの不備があってネットワークが混雑している場合はネットワークの障害である。また、保守のための予定されたネットワーク機器の停止も障害には含まれない。
インターネット場合もネットワークの障害の定義と同様に、その一部でも問題が生じた場合を障害と考える。

インターネットで発生する障害については、この章の最後に実例を挙げながら詳しく述べる。

3.2　障害管理作業

ネットワークの障害への対処には大きく分けて次の 3 つの段階がある。

検知 障害が起きたことを発見する。ネットワークを利用しようとした際に不具合に気付く場合と、ネットワーク監視システムによって自動的に検知される場合などがある。障害の原因がとなった部分がそこに含まれる管理ドメインではなく、その他の管理ドメインによって検知される場合もある。

原因の特定 障害の原因を特定する。障害の原因を追及する場合は、ネットワークの状況を知るために様々なソフトウェアなどを利用して、正常な部分と異常な部分を切り分け徐々にその原因を特定していく。しかし、障害原因を簡単には特定できない場合も多い。

特にその原因が管理ドメイン内にないと考えられる場合には、直接その部分を確認することができない場合が多いため、原因があると考えられる部分の管理者に連絡する必要がある。

復旧 障害の原因となっている部分を修復する。ネットワークを利用して遠隔地より作業可能な場合と、原因となった個所で作業を行わなければならない場合がある。

その部分を担当する管理者のみ作業を行うことができる。

また、障害が発生したとは言いきれないが、障害の前兆となるような状況が検知される場合もある。その場合は、ネットワークの状態に注意して監視し、事前に解決できる場合は早急に作業を行うべきである。

3.3　障害管理で用いられるツールやプロトコル

ここでは、ネットワークまたはインターネットでの障害管理で用いられるツールやプロトコルのいくつかを説明する。

障害管理のうちの、検知、原因の特定、復旧の 3 つの段階のどこで利用できるかについても説明する。

ping IP 層での到着可能性の確認のために最も利用されるツールである。目的とする計算機に ICMP の echo_request を送ると受けとった計算機は ICMP echo_reply を返すことを利用している。もし、目的とする計算機まで ICMP のメッセージが到達してない、またはその計算機がそれを処理できない状態ならば、echo_reply が返され

ない。そこで、ping を実行することによって目的とする計算機が動作し、IP パケットがその計算機まで到達可能であることを確認することができる。

ping では 1 秒に 1 個の icmp のデータグラムを送出し、そのデータグラムの大きさはデフォルトでは 64 バイトだが、最大 4000 バイトまで指定できる。実装されている ping の多くは各データグラムが往復に要した時間 (Round Trip Time(RTT)) をミリ秒で表示し、最後に全部のパケットの RTT の最少値、平均値、最大値を表示する。これによって、目的の計算機までのネットワークの負荷を調べることができる。

障害検知の段階としては、例えば、ルータに対して一定の時間間隔で ping を実行しそれが失敗すると担当の管理者へ警告を送るプログラムを実行することによって、そのルータが動作しているかどうかを監視することができる。警告を送る方法としては、電子メールを送る、ポケットベルを鳴らすなどいくつかの方法が考えられるが、ping に失敗してしまうルータを介した通信は当然行うことができないということを考慮する必要がある。

実際に障害の検知に利用されている例として、WIDE インターネットの NOC の一つである wnoc-tyo では 6 分間隔で各ルータに ping を実行し、それが失敗するとその機器の管理担当者のポケットベル (自由文が表示可能なもの) に対してあらかじめ設定されている警告メッセージを送る、というプログラムが実行されている。

障害の原因を特定する段階としては、ある計算機まで到達不可能になったと考えられる場合、管理者の多くはまず IP 層での接続が可能かどうかを ping を用いて確認する。ping の失敗によって通信の端点である 2 つの計算機の間に問題があることは確認できるが、原因個所を特定することはできない。管理者は自分の管理範囲内にその原因がないか (例えば、外への接続ポイントまでの通信が可能か。) という確認までしかできないため、そこで問題点が発見できなければ、問題があると考えられる部分の管理者にその情報を伝え対処を依頼する。

障害の復旧の段階としては、問題点を解決するような作業を行った後に IP 層での通信可能性の確認として利用される。

traceroute ping と同様、IP 層の通信可能性を確認することができる。ただし、目的ホストに至る経路上の各ルータの名前もしくは IP アドレスと始点からそのルータまでの往復の遅延時間も表示できる。

目的とする計算機 (IP アドレス) への到達は、特定のサービスに割り当てられていないポート番号である 33435 を指定したパケットを送ることにより、もしその計算機がパケットを受けとれば ICMP PORT_UNREACHABEL が返されることを利用して確認される。途中の経路の表示は、通常 30 くらいに設定されている IP パケットの Time_To_Live の値を 1 から 1 つずつ増やしながら設定し、目的の計算機へパケットを送り出すと経路の途中のルータから ICMP の TIME_EXCEED のパケットが返されることを利用して行われている。これを用いて IP 層の経路制御の状態を確認することができる。

障害検知の段階では、2 点間の IP 層の通信可能性の確認は通常 ping によるポーリングが利用されるため、traceroute はあまり利用されていない。

障害の原因を特定する段階としては、ping が失敗した後に、目的とする計算機へ至る経路のどこまで到達可能かを調べるために利用される。また、-g オプションで途中の経路となるルータを指定することにより、そのルータでの経路制御がどのように行われいているかを知ることができる。

障害の復旧の段階としては、問題点を解決した後の IP 層の通信確認に利用される。

snmp Simple Network Management Protocol(SNMP) は、ネットワークを構成する要素に関する情報を、ネットワークを介して交換するためのプロトコルである。SNMP で扱う情報は MIB(Management Information Base) に定義されているオブジェクト識別子によって指定される。SNMP では情報交換のための 5 種類のメッセージ (GetRequest,GetNextRequest, SetRequest, GetResponse, Trap) が

定義されており、メッセージの交換には信頼性の保証されない UDP が用いられる。管理モデルとしては、ネットワーク管理を行う Network Management Station(NMS) と、管理される対象である Managed System (または ネットワーク構成要素) の間で情報交換を行う。NMS として動作するプログラムはマネージャと呼ばれ、Managed System 上で Manager と情報交換するプログラムはエージェントと呼ばれる。マネージャからエージェントへ特定のオブジェクト識別子を指定して情報を要求する場合は GetRequest、ある MIB のオプジェクト識別子の辞書順で次にくるオブジェクトを指定する場合は GetNextRequest を用いられてる。エージェントはそれに対して GetResponse メッセージで応答を返す。マネージャがエージェントの管理情報の設定をする場合には、SetRequset が用いられる。また、エージェントは予め設定されたイベントの発生を Trap メッセージによりマネージャへ非同期に送る。

SNMP の実装によって、ネットワークを構成する機器の MIB に定義された情報をネットワークを介して得ることができるようになり、ネットワーク管理の為の画期的な方法として注目されている。しかし、SNMP の実装によってネットワーク管理の問題を全て解決できるわけではなく、逆にいくつかの問題も挙げられている。

SNMP は分散されたネットワーク構成要素の NMS による集中管理を実現するが、NMS が集中的に管理できる範囲には限界がある。マネージャが SNMP を用いて情報を得る為には、MIB に定義されたオブジェクト 1 つにつき、request のパケットとそれに対する responce のパケットを最低 1 つずつネットワーク上でやりとりするため、頻繁に多くの管理情報をやり取りしようとするとその分ネットワークのトラフィックが増加してしまう。また様々なネットワーク構成要素を扱うために数多くの MIB が定義されたため、それらから必要な MIB のオブジェクトの識別子を探すのは困難である。

このように SNMP では、参照できる情報とそれを交換するための機構が提供されただけであり、実際に管理を行う際にその情報をどう解釈し、管理作業に役立ていく

かということは、それを利用する管理者の判断に任されている。

障害検知の段階としては、一定間隔であるオブジェクトの値を問い合わせ、その値の変化により警告を出す方法や、管理者が trap メッセージを受けるなどといった方法で利用される。

障害の原因を特定する段階としては、様々なネットワーク構成要素の状態を知るために利用される。

障害の復旧の段階としては、復旧作業の後でネットワーク構成要素の状態を確認するのに利用される。また、SetRequest を利用して、ネットワーク構成要素の変更を遠隔地から行うこともできる。

netstat ネットワークのためのソフトウェアが動作するために計算機が内部的に持っている各種カウンタの値を表示する。これを用いて、ネットワークの状態をある程度知ることができる。以下のようないくつかのオプションがある。

-i ネットワークインターフェースの状況を示す。計算機のブート時にカーネルに読みこまれたインターフェースについての値が表示される。各インターフェースごとに表示される項目は以下の通り。

Nmae	インターフェースの名前
Mtu	Maximum Transmission Unit(MTU) 一回で転送可能なパケットの最大の大きさ
Network/Dest	そのインターフェースの接続されているネットワークアドレス
Address	そのインターフェースに割り当てられた IP アドレス、またはその名前
Ipkts	受信したパケット数の累積値
Ierrs	受信時のエラーの数の累積値
Opkts	送信したパケット数の累積値
Oerrs	送信時のエラー数の累積値
Coll	コリジョン (衝突) の数の累積値

-r その時点での経路テーブルの内容を表示する。送り先のアドレスごとに以下のような項目が表示される。

Destination	送り先のホストアドレス、またはネットワークアドレス
Gateway	Destionation へ至るためのに次の送り先になるルータ
Flags	その項目の経路の性質を示すフラグ
Refcont	その項目を参照しているコネクション数
Use	その経由したパケット数
Interface	その経路へ至るためのインターフェース

これによってその計算機の経路制御がどのように行われているか確認することができる。

-s TCP/UDP/IP/ICMP の各層の各ステータスを表示する。各プロトコルごとに送受信したデータグラム、パケット、エラーなどの累積値が表示される。これら

のうち、ip や udp や tcp のチェックサムエラー、受けとった ICMP メッセージの数などには注目するべきである。

オプションなし 各ポートの利用状況を示す。その時に使用されているコネクションの数、ポートの状態などが示される。

障害検知の段階としては、一定時間間隔でこれらの値の変化を検査することによって、いくつかの障害の可能性を知ることができる。例えば -s オプションで表示される ICMP の数の変化に注目し、それが通常の変化に比べ非常に大きければ何らかの問題点があると考えるべきである。また他の例として、-r オプションによって経路情報の変化を監視し、動的に経路情報を交換するプログラムに問題が発生したことを検知することができる。

障害の原因を特定する段階としては、ルーティングのエラーの発見やインターフェースの不備の発見に利用される。

障害の復旧の段階としては、経路情報については確認に利用される。

nslookup DNS の様々な資源に関する問い合わせを会話的に行う。BIND の設定のチェックや、ユーザが IP アドレスのドメイン名への変換や、その逆の変換をする場合に利用される。BIND の設定ミスによって起きる障害は比較的よく発生しており、また DNS はインターネット全体が協調した設定を特に必要とするため、ネットワークの管理のための重要なツールの 1 つである。

障害の原因を特定する段階としては、ドメイン名とアドレスとの変換が正しく行われているかの確認に利用される。また、メールの配送が正しく行われない場合にはメールアドレスに対する MX レコードが正しく設定されていない場合が考えられるため、この確認にも用いられる。nslookup では、ローカルな設定の不備だけでなく、他のドメインのゾーンファイルが正しいかどうか調べることができる。

障害の復旧の段階としては、他のドメインのゾーンファイルを修正した結果が正しくリモートからも参照できるかどうかの確認に利用される。

etherfind 計算機が接続されている Ethernet 上を流れるパケットをモニタする。表示するパケットの種類は条件により指定することができる。条件は、ソースとデスティネーションの ホストアドレス、ネットワークアドレス、ポート番号、プロトコルの種類、パケットの長さなどが指定できる。

特定の種類のパケットを調べたい場合に役だつ。-x オプションを用いることにより、パケットそのものの 16 進数でのダンプを表示するため、パケットのヘッダを直接調べることもできる。

障害検知の段階としては、障害の原因を特定する段階としては、例えば異常にネットワークのトラフィックが増加した場合にどのプロトコルで利用されるパケットが多いかを調べることができる。この場合に、-x オプションを用いて急増しているパ

ケットのヘッダ部分の情報を調べることによって、その原因を特定することもできる。また、特定のホストからのパケットが来ているかどうかをの確認やそれに対する応答が正しく行われているかを確認に利用される。

障害の復旧の段階としては、障害に対処している過程で、通信できるようになったかどうか、通常のトラフィックの状態に戻ったかどうかを確認することができる。

tcpdump ネットワークインターフェースが接続されているネットワーク上のトラフィックをモニタする。etherfind と同様に様々な条件を用いて特定のパケットに限って表示することができる。表示されるのは各パケットのプロトコルごとのヘッダの情報。

- Ethernet フレームタイプ
- Ethernet アドレス
- IP アドレス
- IP ポートのタイプ
- プロコトルのタイプ
- パケット長

などである。実際の表示は以下のようになる。

```
18:51:04.91 simon.cs.uec.ac.jp.e4d42 > grover.cs.uec.ac.jp.nfs: 40 null
18:51:04.91 grover.cs.uec.ac.jp.nfs > simon.cs.uec.ac.jp.e4d42: reply ok 24
18:51:04.91 penelope.cs.uec.ac.jp.nfs > simon.cs.uec.ac.jp.e4d52: reply ok 24
18:51:05.08 bigbird.cs.uec.ac.jp.4720 > twoheaded.cs.uec.ac.jp.1032: udp 92
18:51:05.08 twoheaded.cs.uec.ac.jp.1032 > bigbird.cs.uec.ac.jp.4720: udp 88
18:51:05.08 twoheaded.cs.uec.ac.jp.1032 > bigbird.cs.uec.ac.jp.4720: udp 88
```

障害検知の段階としては、あまり用いらていないが、Ethernet を流れるパケットのモニタとして、各プロトコルのトラフィクの異常、経路制御のエラーによる不当なトラフィックの発生などを検知することが可能である。

障害の原因を特定する段階としては、上の etherfind とほぼ同様に利用される。ただし、tcpdump では特定のアプリケーションプロコトルに関してアプリケーション層のデータまでモニターできるため、アプリケーション層の障害を特定するために利用できる。

障害の復旧の段階としては、復旧作業を行った後に、ネットワークの状態が正常に戻ったかどうかの確認に利用される。

nnstat インターネットのトラフィックの統計情報を収集するためのツールである。ネットワーク管理の上で、長期的な統計情報を集めたい場合に用いられる。ネットワークインターフェースごとに、そのインターフェースが直接接続されているネットワークを流れるパケットの情報を取ることができる。これが”statspy” というプロセスに

よって行われる。statspy によってモニタ可能なネットワークの情報を集めるのが、collect というプロセスである。統計は、指定した時間間隔ごとに、パケットの種類 (ip/icmp/UDP/TCP などのプロコトル) と、さらにそれらを種類 (ポート) によって分け、それぞれネットワーク、サブネット、ホスト などの source、destination の組ごとにパケットの数を得ることができる。

ethernet モニタ Sniffer などの製品がある。Ethernet を流れるパケットの量をモニタする。特定のパケットが来るとアラームを出したり、通常のトラフィックの値を取るなどの機能があるものもある。

障害検知の段階としては、トラフィック量や、不当なパケットを指定しアラームを発生することにより検知に利用することができる。

障害の原因を特定する段階としては、パケットのヘッダの情報を解析することにより、障害の特定に利用することができる。etherfind と同様に利用できる。

障害の復旧の段階としては、復旧した後の確認に利用する。etherfind や tcpdump と同様に Ethernet を流れるパケットをモニタすることにより確認する。

telnet TELNET プロコトルを用いて他のホストと通信するためのユーザーインターフェース。他の計算機のアドレスだけを指定すると、telnet 用のポートを用いてその端末にログインしたように操作できる。ポート番号を指定することもできるため、特定のポートを指定することにより、指定したポートでサービスを受けられるかを確認することができる。

障害管理では主にネットワークソフトウェアのデバッグに利用される。

障害の原因を特定する段階としては、あるアプリケーションが利用できない場合に、telnet によってそのサービスを提供するポートに接続し、そのプロコトルの手順を管理者が手で入力することにより、そのサービスが正常に利用可能であるかどうか確認する。

障害の復旧の段階としては、作業終了後の確認に利用される。

ICMP(Internet Control Message Protocol) ルータで IP パケットの配送に関して何らかのエラーが発生した時にそのエラーやコントロールメセージをそのパケットの送り元のホストに送るためのプロトコル。ICMP のメッセージは IP データグラムのデータ部分として作られる。ICMP のメッセージは、上に述べた traceroute や ping のような IP ネットワークでの到達確認に用いられている。

しかし、実際ネットワーク管理の場面で netstat などで、icmp のパケット数の累積値の変化を監視する程度の利用しかされていない。ICMP は TCP/IP プロトコル体系にもともと含まれているプロトコルであり、snmp のように問い合わせのパケットとそれに対する応答パケットを必要としないため、ネットワーク上を流れる icmp を監視することによってネットワークの障害を検知するという研究も行われている [83]。

障害管理に利用するためには、Ehterfind、tcpdump などといったネットワークを流れるパケットをモニタするツールを利用することによって、どのような種類の ICMP が、どのホスト間で流れているかを調べる必要がある。

障害検知の段階としては、Destination Unreach や Source quench などのパケットを受けとっていないかを監視することによって、障害の検知を行うことができる。

障害の原因を特定する段階としては、どの 2 つの計算機の間で ICMP のパケットが流れているかを調べることにより、障害の発生している個所や原因の特定に利用することができる。

以上のツールで得られる情報は、TCP/IP プロトコル体系での各層に対応づけることができる。上に挙げたツールがプロトコルの階層のどこに対応しているかを図 3.1 に示す。

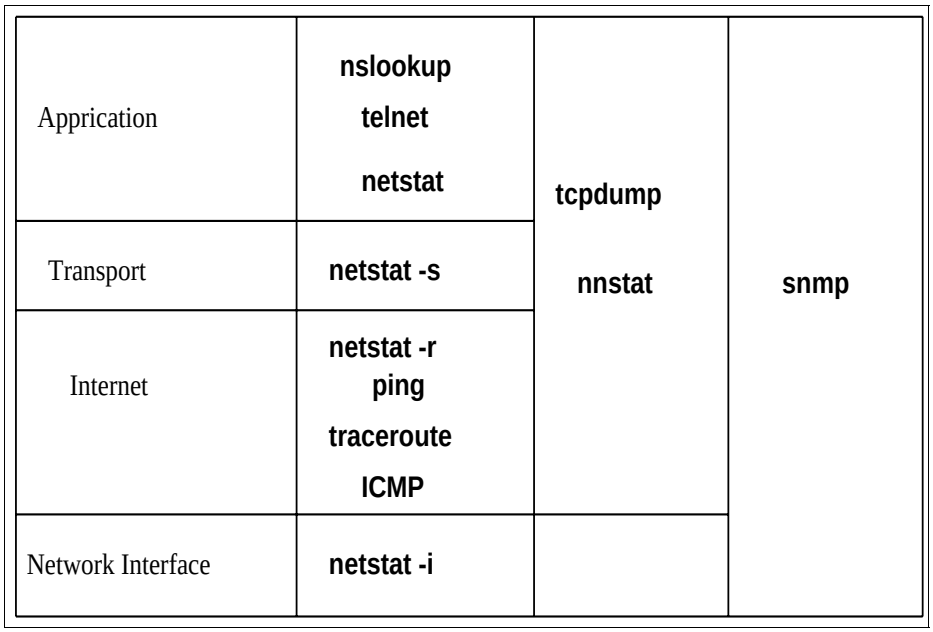

図 3.1: ネットワークの障害管理に用いるツールと対応するプロコルの階層

3.4 インターネットで発生した障害の例と分析

障害管理を考えるために、ここでは実際に WIDE インターネットで発生した障害を例にとり障害の分析を行う。

3.4.1 WIDE インターネットで発生した障害の例

WIDE インターネットは広域分散環境の実現を目的とした WIDE プロジェクトの実験環境となるネットワークである。運用と管理は WIDE プロジェクトのメンバーによって行われている。通常 WIDE プロジェクトのメンバー間はメーリングリストによる情報交

換が行われており、ネットワークの障害に関する情報交換も同じメーリングリストを用いて行われている。

このWIDEプロジェクトのメーリングリストでのやりとりの中から、WIDEインターネットでの障害に関するものを分類し、実際にインターネットで発生した障害例を分析するために利用した。

このメーリングリストによる障害の記録には発生した障害の全てについての記録が残されているわけではない。一人の管理者だけで解決された障害、メーリングリストを利用せずに特定の管理者の間の情報交換で解決された障害、障害の影響でメールが利用できず電話などメール以外の方法で連絡を取り解決されたものなどについてはここには記録が残されていない場合が多い。このメーリングリストによる情報交換は障害に関する情報を残すのが目的ではなく、ネットワークの運用上必要な情報交換に利用されているだけであるため、障害が最終的にどのように解決されたのか分からない場合も多く含まれている。

1991 年 1 月 11 日から 10 月 10 日までのメールのうちネットワークの障害に関係する情報が書かれたものが 288 通あった。(ただしこの中には、ネットワークの保守のために予定されたネットワークの停止のアナウンスなどは含まれない。) これらのうち障害の原因の数としては 94 件があった。つまり 1 つの原因につき平均 3 回のメールが交換されたことになる。メールの内容としては以下のようなものが代表的である。

- 比較的原因のはっきりした障害について復旧作業の依頼。
- 原因の分からない障害について問題点の究明の依頼。
- 障害への対処についてアドバイス。
- 障害の原因は分かっているが復旧まで時間がかかるものについての連絡。
- 障害が復旧したという連絡。

97 件の原因のうち、メールの記録からははっきりと原因が理解できないものが 27 件あった。これらは、障害の検知についてのメールはあったが最終的な解決方法についてのメールが残されていなかったためである。

70 件の障害の原因ごとの分類は以下の通りである。

原因	件数
メールのソフトウェア関係	9
ニュースのソフトウェア関係	2
DNS のソフトウェア関係	8
経路情報交換ソフトウェア関係	5
ルータの問題	30
モデムの問題	4
ブリッジの問題	4
DSU の問題	3
専用回線	3
その他	4

ここで用いた記録では、ルータの問題がメールで交換される障害の原因として多いことがわかる。ただし、全ての障害について記録されていないため、これはインターネットで発生する障害の頻度を反映しているとは言えない。また、メールで記録された問題は管理者間で情報交換が必要とされたものであり、かつメールによる情報交換が利用可能な状況であった場合のみが含まれていると考えられる。

次にこれらの障害のいくつかの内容を、障害の原因となった部分を TCP/IP プロトコル体系での層ごとに分類しながら例を挙げて説明する。

3.4.1.1 物理層の問題

ハードウェアの故障 (回線、モデム、ルータなど) インターネットを構成するハードウェア機器としては、ルータ、計算機、Ethernet などの物理媒体、専用回線、モデムなどが挙げられる。これらの機器が物理的に壊れてしまった場合、当然通信は行われなくなる。しかし、インターネットを介して障害の原因を追及する場合に、それが機器の物理的な問題によるのか、動作しているソフトウェアによるのか判断がつきかねる。なぜなら、ハードウェアの問題はそこで動作しているソフトウェアを利用して調べることができないからである。

実際に起きたネットワーク構成機器の故障例としては、

- 突然事故により停電が起きた。
- ルータの計算機のコネクタがゆるくなって、接触不良になっていた。
- ルータとして動作している計算機のディスクが壊れた。
- ルータとして動作している計算機の電源が抜けそうになっていた。
- ブリッジの故障。

- DSU が壊れた。DSU のスイッチが事情を知らない人によってリセットされた。
- モデムの故障。
- あるネットワーク内でのネットワークの物理媒体が切れた。
- 専用回線に問題が生じた。

予想以上に多いのが、ネットワークを構成している計算機 (ルータや各ネットワークを構成するソフトウェアが動作している計算機) のハードディスクのクラッシュを原因とする障害である。常にディスクの状態を監視していない場合は、その計算機を介した通信によって初めて検知される。

ハードウェアの故障による障害の影響としては、その原因となる個所を通るような通信が全くできないということがある。

3.4.1.2　インターネット層の問題

ルータのハングアップ　ルータの計算機がハングアップした場合、通信は行われなくなる。復旧するためには、そのルータ (計算機) をリブートする必要がある。

この場合、IP 的に接続が切れるため ping などを用いて IP 的に到達可能かを調べることによって、ある程度原因が特定される。

多くの場合そのネットワークの利用者がインターネットを利用しようとして、IP 接続が切れていることに気付く場合が多い。ネットワークと NOC の point-to-point 接続では、NOC 側とネットワーク側の 2 台のルータの間を専用回線などで接続している。そのため、接続されているネットワーク側からは、ローカルネットワーク側のルータは通常近くにあるため容易に確認できるが、NOC 側のルータの多くは遠くに設置されているため、その状態をすぐに確認するのは困難である。そのため、気付いた管理者は早急に NOC の管理担当者に連絡を取る必要がある。

ルーティング情報の欠落　ルータが誤った経路情報に従っているならば、正しい経路制御は行われない。

経路情報を静的に設定している場合には、その記述に誤りがある場合が考えられる。また、ルータの計算機がハングアップしてしまい、それを立ち上げ直した場合に正常に経路のアナウンスが行われない場合もある。

経路情報の欠落による障害の例

例 1 モデムを用いて NOC に point-to-point で接続されているあるネットワークの経路情報 (ネットワークアドレス) は、通常 NOC 側のルータから他のネットワークに対してアナウンスされていた。

NOC 側のルータを立ち上げ直した際に、設定の不良により接続されているネットワーク側のルータのホストアドレスのみがアナウンスされ、ネットワークアドレス

がアナウンスされなかった。そのため、そのネットワークが接続されているルータまでは到達できるが、ネットワーク内部の計算機にはどれにも到達できなかった。NOC 側の管理者は、ローカルネットワーク側のルータまでの到達可能性のみを確認して作業を終えたため、設定の不良に気付かずそのネットワークを利用している人によってまず検知された。

例 2 通常静的に経路を設定していたが、設定されるべき項目が消えてしまっていた。

誤った経路情報による障害の例

デフォルト経路 通常、インターネットに接続されいてるルータからデフォルトの経路を無闇にアナウンスしてはならない。しかし、あるネットワークのルータが、gated.conf の設定ミスにより誤った経路へのデフォルト経路をアナウンスしてしまった。そのため、本来のデフォルト経路と重複してしまいパケットがピンポンしてしまい、ネットワークの負荷が非常に大きくなってしまった。

経路情報の欠如は、実際にその経路を利用しなければ RIP のアナウンスの不備が検知されないことが多い。正しい経路情報がアナウンスされているかどうかを知るためには、netstat -r などを用いてルータが持っている経路テーブルの内容を確認することによって行われる。netstat -r による比較は通常の経路テーブルの状態を知っていなければ異常かどうかを判定することはできない。しかし、通常の経路情報がないのは、そのネットワークのルータが落ちて rip が送られない場合も考えられるため、一概に RIP のアナウンスの不備であるとも言いきれない。

インターネットの経路の到達可能性は、ping や traceroute によって調べられる。

ルータの設定ミス ルータの周りの装置の設定を変えようとした時にルータが立ち上がらなくなった。その際に設定を始めからやり直した際に、ルーティングの設定がおかしくなった。障害の検知は、経路情報がアナウンスされなくなってしまったネットワークの利用者だった。

デフォルト経路 各ネットワークのデフォルト経路はネットワークの外に対してアナウンスしてはいけない。あるネットワーク内にとってのデフォルト経路 (つまりバックボーンに接続してるルータへの経路) を、ネットワークの外に対してもアナウンスしてしまったため、そのデフォルトに従ったパケットがそのネットワークのインターネットルータへ向けて配送された。また、インターネットバックボーンで通常設定されている正しいデフォルト経路の情報との両方が混在しルータの経路制御が混乱した。

3.4.1.3 アプリケーション層の問題

ドメイン名システムに関する障害 インターネットを介したサービスを利用する場合、通常は計算機の名前を用いて目的とするホストを指定する。ホスト名を用いる場合にはネー

ムサーバにその名前に対するアドレスを問い合わせる必要がある。この時名前からアドレスが引けなければ目的とする計算機を指定することができないため、通信することはできない。

ネームサーバのシステムである BIND の不良によるネットワークの障害は比較的頻繁に発生している。

例えば、あるゾーンがプライマリサーバのみを設定してセカンダリサーバの設定をしていなかった場合、プライマリサーバが落ちている場合にはそのゾーンのネームサーバへの問い合わせが失敗するため、そのゾーンに属する計算機への通信ができない。また、問い合わせのリトライが発生するためトラフィックが増えネットワークに負荷をかける。

また、named の設定ミスや設定の手違いにより 2 つの計算機の間で互いに問い合わせをフォワードしてしまい、大量の domain パケットが発生し、ネットワークに非常に負荷をかけてしまうという障害もみられる。

named の障害の場合、大量のドメインのパケットの流出がネットワークに非常に大きな負荷をかける場合が多いが、通信ができないなどの致命的な障害として現れないため検知されるまでに時間がかかる。また、あるネットワークの外部とのインターフェースでのトラフィックを監視していたとしても、全体のトラフィックの増加が、直ちに Domain のパケットの増加が原因であるとも言いきれない。snmp の標準 MIB では、インターフェースを通るパケットの数の累積数が定義してあるため、特定のインターフェースのトラフィックの変化を知ることはできるが、どのような種類のパケットが多いか、またはどの計算機との間のパケットが多く流れているのか、などということを知ることはできない。

Domain のパケットであることを調べるためには、パケットの種類をモニタする etherfind で調べるか、または nnstat 、tcodump などのネットワークのトラフィックの統計を取るためのツールを用いる必要がある。

ネームサーバが原因として発生した障害として以下の例が挙げられる。

サーバーの設定がされていなかった　ネットワーク A がネットワーク B に UUCP によって接続される予定になっていた。ネットワーク A のセカンダリサーバ は設定されていたが、プライマリサーバが B に設定される前に、ネットワーク A の利用が開始されてしまった。そこで、ネットワーク A の名前の問い合わせのあった secondary server は primary に設定される予定のホストに問い合わせを送り、primary sever になる予定のホスト B は、forwarder に問い合わせを送ってしまった。そこで、primary server になる予定の B と、B の forwarder との間で大量の domain の問い合わせのパケット (通常の数十倍) が流れてしまい、インターネットに大きな負荷を掛けてしまった。この場合、ネットワークの負荷が非常に大きかったためインターネットを介してインタラクティブな操作を行うサービス (telnet) を利用した人によって異常が検知された。しかしインターネットが完全に利用できなくなる訳ではなく、また通常でも FTP などのサービスを同時に利用しているユーザが多い場合もネットワークの負荷が非常に大きくなるため、実際に障害が発生からそれが障害であると認識されるまで、半日以上が経過した。

登録されるデータの入力ミス named のデータベースを書き間違えたため、例 1 と同じように大量の Domain パケットが流れてしまった。

あるネットワークで、誤って存在しないゾーンに対して NS レコードを書いてしまった。さらに、存在しないゾーンに対する NS レコードに他のドメインのサーバを指定してしまった。そのため、その設定に従って大量の query が飛んでしまった。この場合もネットワークの非常に大きくなったため検知された。

タイプミス DNS の資源のデータベースの設定で “wide.ad.jp” と書くべき部分を誤って、“wide.ac.jp” と書いた。

ypserv のプロセス あるローカルネット内の計算機で、ypserv のプロセスが沢山 fork してしまったために、大量に domain の問い合わせのパケットが出てしまった。

named の設定 named の MX の設定を忘れた。設定すべきエントリがゾーンデータとして書かれていなかった。

3.4.2 各種設定ミス

設定ミスによる障害は、多く見受けられる。単純ですぐに見付かる場合もあるが、その原因となる設定ミスが表面化するのが難しい場合もある。設定ミスの例をいくつか挙げる。

サブネットの設定 あるローカルエリアネットワーク内でサブネットの設定がされている部分と、されていない部分がルータで接続され混在していた。そのため、デフォルトルートの間でピンポン してしまった。

3.4.2.1 その他

インターネットを構成する機器の保守のため、一時的なルータの停止や回線の切断が予定される場合がある。その予定のアナウンスは、実施のしばらく前に行われるため、管理者が予定されているものを障害と勘違いしてしまう場合がある。このような予定されたネットワークの停止は、管理者が常に確認できる状態にある必要がある。

3.5 障害による影響

インターネット上に何らかの問題がある場合でも、全ての通信が不可能になる訳ではない。ここでは前の節と反対に、障害によってインターネットに与えられる影響ごとに、考えられる障害原因の例を挙げる。

- 特定のアプリケーションが利用できないが、IP 層での通信は可能である。

  目的とする計算機に対してホスト名を指定してパケットが送られることが確認できれば、アプリケーションプログラムの原因である可能性が大きい。目的とする計算機でアプリケーションプログラムが動作していない場合、そのアプリケーションを受けつけるポートが利用できない場合などが考えられる。

  メールの配送に失敗してる場合には、メールのスプールをしているディスクの容量に余裕がない場合も考えられる 。

  また、メールの配送では DNS による名前からアドレスの変換が行われないため、通信に失敗している場合もある。この場合 nslookup を利用して DNS の設定を確認することにより DNS が原因であるかどうか知ることができる。

- ホスト名を指定した通信が不可能である。アドレスを指定すると IP 層の通信が可能なことが確認できるが名前を指定すると不可能になる (ping による確認) ならば、DNS に問題がある場合が考えられる。この場合、nslookup によって DNS が利用可能かどうか確認することができる。DNS の動作不良による障害は多くみられ、管理者の協調が必要とされる典型的なシステムの一つである。

  DNS が正しく動作していない場合として以下の場合が考えられる。

  – DNS のソフトウェアが動作していない場合、
  – DNS のデータが正しく設定されていない場合、
  – DNS のサーバとなっている計算機との間で通信が不可能な場合

  がある。この場合、名前と IP アドレスの対応が付けられないことのみが問題であるため、アドレスを指定する方法が利用できれば通信することができる。ただし、必ず名前により相手を指定するアプリケーションプログラム (例えばメールの配送) の場合 DNS が正しく動作しなければ、アプリケーションの利用はできない。

- 目的とする計算機との間で IP 層での通信が不可能である

  IP 層の通信ができない場合その原因として様々な場合がある。以下のような原因が考えられる。

  – 経路制御が正しく行われない場合

    traceroute で目的とするアドレスまでの経路を確認することができる。そこで、正常状態の経路を把握しているならば正常状態の経路と比較して、どのルータでの経路制御が正しくないかを判断することができる。その場合、経路指定オプションによって正しい経路を通るような指定をした traceroute を実行することにより目的とするアドレスに到達できるならば、そのルータでの経路制御のプログラムまたは経路情報の伝達の部分に問題があると考えられる。ある計算機での経路制御の状況は、そこで netstat -r コマンドを実行することによって確認することができる。

– 経路の途中の機器に問題がある場合

途中まで正しい経路を通っているにも関わらず、そのアドレスまで到達できない場合はその途中の機器に問題が発生した可能性が高い。しかし、途中の機器がソフトウェアの問題により動作しないのかハードウェアの問題により動作できないのかは、ソフトウェアを利用しては確認できない。その機器の管理担当者が直接その機器の様子を確認するなどの作業が必要な場合が多い。この場合、その機器を介した通信は不可能なためもし通常は経由していないがインターネットとして迂回経路が存在すれば、その部分を経由する経路を指定することによって通信を可能にすることもできる。

このように、障害が検知されてもその原因には様々な場合がある。しかし、障害の影響として全ての通信が不可能になる訳ではなく、その一部が利用できないためアプリケーションプログラムの利用に支障をきたす場合も多い。そのような場合、利用できる部分を巧みに利用して情報交換を行い、早急に障害の原因を解決することが必要である。

第 4 章

障害に関する情報の交換

前章では、インターネット上で実際にどのような障害が発生し、その際にどのような対処が行われてきたかということについて考察した。その結果、インターネットの障害管理では、各管理ドメインの間の情報交換が必要不可欠であることが分かった。

通常、インターネットを介した情報交換には電子メール多く用いられているが、障害が発生した場合には電子メールが使用不可能になる可能性がある。この時に電話など計算機を用いない方法では、計算機上に記録が残らないため後からそれを利用することができない。

本章では、管理ドメインの間でインターネットの障害に関する情報交換を行う方法について検討していく。

4.1 現在の障害情報の交換の手段

インターネットの障害は広範囲に影響を与え、障害を解決するためには異なる管理ドメインの管理者間の情報交換が必要となる。

障害に関する情報を伝える場合には、障害発生時にはそれを知らせるための情報は早急に伝えられるべきである。また、ネットワークの異常を検知した複数の管理者が、原因追及のためにネットワークの状態を確認するためのコマンドをむやみに実行しネットワーク上のパケットを増加させるといった事態を避けなければならない。

以下では実際に行われている情報交換の手段について考察を行う。

4.1.1 電子メールを用いた情報交換

これまで、WIDE インターネットでの障害発生時には電子メールが使用可能な場合はメールで、不可能な場合は電話などのインターネットを利用しない方法で情報交換を行ってきた。電子メールでは主に、各管理ドメインの管理者をメンバーとするメーリングリストが主に利用されている。

メーリングリストを用いた障害情報の交換には以下のような特徴がある。

- 利点

- 情報を伝えるべき相手が電子メールの到着に注意を払ってるような場合ならば、迅速にその情報を伝えることができる。
- 電子メールはインターネットの利用者にとって最も一般的な情報交換の手段であるため、アドレスだけ把握していれば連絡を取ることができる。
- 受けとった電子メールを消去しなければ、後から参照することも不可能ではない。
- メーリングリストの場合受けとった管理者が直接その障害に関係しない場合も、送られてくる電子メールの内容から障害への処理方法を学ぶことができ、その後に同様な障害が発生した場合にはその知識が生かされる可能性がある。
- 電子メールは自由に文章を書くことが可能であり、コマンドの実行結果などを含めた詳しい説明を自由に書くことができる。

• 欠点

- 伝えるべき相手がその時に電子メールに注意を払っていなければ、緊急に伝えるべき情報もすぐには伝えらない。
- 発生した障害の影響によりメールが利用できなくなる可能性がある。
- 障害情報のメールも通常のメールと同じように送られるため、障害情報だけを区別するのが難しく、ある情報が必要になった場合それを検索するのは困難である。
- メーリングリストの場合、その情報を必要としない管理者にもメールが送られる場合がある。

現在、WIDE インターネットではネットワークの管理がボランティアのスタッフによって行わているため、専任のスタッフが常にインターネットの状態を監視する状態ではない。また、NOC の機器などの障害管理作業を行うことができる管理者は数が限られる。そこで、常にネットワーク機器を監視する専門の管理者が居ないという状況でも、障害発生時など緊急な連絡が必要な場合には必要な情報を確実に伝える方法を考えなくてはならない。

4.1.2 電子メールを用いた障害情報の交換での問題点

上にあげたように、現在の主に電子メールによる障害に関する情報の交換方法は多くの問題を含んでいる。そこで、電子メールを利用した方法の欠点について詳しく述べる。

• 確実に即座に情報を伝達できない。

電子メールは、情報を受ける側が情報獲得の努力をするのではなく、伝える側が受ける側に対して積極的に情報を送り付けるシステムである。しかし、電子メールを受ける側が受けとった電子メールを読まれなければ情

報は伝わらない。ワークステーションなどでは電子メールの到着を知らせるアプリケーションが利用されている場合もあるが、伝えるべき相手が必ずしも計算機を利用しているとも限らない。緊急を要する情報の伝達が必要な場合には、電子メールが有効であるとは言えない。

- インターネットに障害が発生した場合に情報交換ができなくなる可能性がある。

  IP 層での接続ができなくなった場合はもちろん、メールの配送を行うために必要なソフトウェア (例えば DNS など) が利用できないような状況では、メールの配送が不可能になる。

  もし仮に、管理者が別のネットワークにアカウント持っており、かつその計算機にモデムと公衆回線などを用いた臨時の経路を作るという、インターネットを介さない方法を利用できるならば、その計算機にログインして障害についての電子メールを出すことも可能である。しかし、これはあくまでもその場限りの方法であり、全ての管理者が確実に利用できるシステムとして提供されているわけではない。

- 必要な情報を効率的に獲得できない。

  ネットワークを構成する機器などの保守のため、インターネットから接続されなくなる予定がある場合の連絡も、メールによって行われている。そのため、通常通りインターネットが利用できなかった場合に障害が発生したと管理者が勘違いしてしまうということが、時おりみられる。(実際に WIDE インターネットでも、予定された障害であることに気付かずに、予定されていない障害として連絡するメールが見られる。)

- 冗長な情報交換が行われる。

  メーリングリストは、特定のメールアドレスに電子メールを出すと、あらかじめそのメールアドレスに登録されていた複数のアドレスに対してそのメールの内容のコピーが送られるというシステムである。そのため、必ずしも全ての電子メールの内容がメーリングリストに登録された全員に関係ある情報ではないため、メールを受ける側にとって情報の冗長性が大きい。多くのネットワークの管理者がインターネットのある部分で発生した障害の状況を把握したり、障害対処の過程で多くの管理者の知識を集めてその問題に対処する良い方法を考えることができる、という利点もある。しかし、冗長な情報交換が多いため必要な情報まで見落とす可能性も考えられるため、効果的に必要な情報交換を行う方法を利用するべきである。

- 情報交換の記録を後から履歴として利用するのが困難である。

  障害発生には様々な場合があるため、単純な規則に従って対処できるというわけではない。ネットワークの管理者は、ネットワークの構成やその

動作原理を知ると共に、実際に起きる障害についてはある程度の経験を積むことによって対処できる場合も多い。しかし、ネットワークが一般的なものとなり管理されるべきネットワークが増えてくるにつれ多くの管理者が障害への対処方法を効率良く学ぶ必要がある。

通常の電子メールでの障害に関する情報交換では電子メールを受け取った個人で整理するなどの作業をしない限り、電子メールの内容となる情報の関係を示すものがないため過去の履歴として参考にするのは難しい。また、電子メールに残された障害に関する情報はあくまでも管理作業上必要な情報交換の手段として利用されたものであり、障害管理作業の記録としては不十分な内容である場合が多い。

- 記録として残されたものの形式が統一されていない。

  電子メールでの障害の記録では、伝える側が必要と思われる内容のみが記入されるため、その形式が統一されていない。そこに情報として含まれる内容も統一されていないためその情報を整理し、後で利用するのが困難である。

4.2 トラブルチケットシステム

アメリカのインターネットの中心となっているバックボーンネットワークである NSFNET は Merit Inc. によって管理されている。Merit では、24 時間体制でスタッフが交代しながら NSF のネットワークを監視し、管理作業にあたっている。

管理作業の担当者が交代する際の作業の引きつぎを円滑に行うため、行われた作業を記録し、複数の管理者間で情報を共有するための**トラブルチケットシステム** [84] が考案された。トラブルチケットとは、ネットワーク上で障害が起きた時、障害に関する情報を記録しネットワークの管理に関係する人々が参照するための一種のデータベースシステムである。

スタッフはネットワークの状況や作業の進行状況をチケットシステムに記録し、交代するスタッフはネットワークの状況をそのシステムを参照することによって把握することができる。また、チケットに残された記録からネットワークに発生した事柄に関する統計を出すことも可能である。

一つの例して、あるユーザがサービスを実行しようとしてそれが失敗してしまった場合、その症状 (状況) を書き入れたトラブルチケットを発行する。ネットワークの管理者はそのトラブルチケットを見ることによって、障害の状況を知る。管理者が作業を行った時には、その作業の記録をトラブルチケットに残す。作業の記録を残した本人だけでなく交代して作業にあたる他の管理者も、チケットに残されている記録を見て状況を把握することができる。

1992 年 1 月には、トラブルチケットシステムについての RFC1297 の “NOC Internal Integrated Trouble Ticket System Functional Specification Wishlist (NOC TT REQUIRE-

MENTS)([85])" が作られ、トラブルチケットに求められる機能やその利点、今後求められる拡張などが述べられている。

また、IETF の UCP WG(User Connectivity Problem working group [1]) も、トラブルチケットについて議論している。

以下では、RFC1297 に述べられているトラブルチケットシステムの内容、ならびに実際に作られたトラブルチケットシステムについてその特徴や実装方法などを紹介する。

4.2.1 RFC1271

この RFC では、トラブルチケットの目的やチケットに必須とされる情報、さらにシステムをどのように拡張していくことが望まれるか、などが述べられている。以下に、この RFC の内容の概略を説明する。

4.2.1.1 概要

ネットワークでのトラブルを処理する過程で問題点を記録しておくようなシステムが必要とされる。 もともと考えられたトラブルチケットシステムは、複数の人がある問題に対処するための、例えると病院のカルテのようなシステムである。

ネットワーク障害の処理を効果的に行うために、トラブルチケットシステムには様々な拡張が考えられる。チケットに残された記録は、障害に関する統計値を出すためにも用いることもできる。また ネットワークの警告システムから、自動的にチケットを発行することも考えられる。また、警告システムをトラブルチケットの状況を監視するために用いることもできる。そして、ネットワークの" 健康状態" を複数の NOC 間、電話会社などの間でやりとりする為に用いることもできるだろう。

4.2.1.2 NOC Trouble Ticket System の目的

" 良い" トラブルチケットシステムは、以下に挙げたような目的を果たすべきである。

1. 覚え書きとして複数の人の参照を可能にする
   NOC では複数のオペレータが交代で勤務しており、障害への対処はオペレータが交代しても引きつがれなければならない。そこで、トラブルチケットを病院のカルテのように利用して、オペレータが今までに起こった事や、それへの対処などを簡単に把握することができる。

2. 勤務のスケジュールリングと人員配置のための利用
   その時点での障害の一覧を表示できる。さらにその内容によって重要度の順に表示することも可能である。把握した状況に応じて、効果的な人員配置をすることも可能である。

[1] TheUser Connectivity working group will study the problem of how to solve network users' end-to-end connectivity problems.

3. 担当者を示すことにより迅速な対応を可能にする
   障害に応じて、適任者をトラブルチケットに指定できる。適任者への委託により、迅速な対応が可能になる。

4. アラーム
   トラブルチケットが発行される時に、問題の重要度などに応じてある間隔でタイムアウトを設定してアラームを発生させ、管理者の注意を促すことができる。

5. 技術者や顧客であるサイトの代表者が監視に利用する
   NOC が複数のサイトを管理している場合、それぞれのサイトの代表者に関係する過去のトラブルチケットの記録をまとめて報告に利用することができる。くわしい情報は、チケットの番号を知らせて該当するものを参照してもらう。

6. 統計的な分析
   トラブルチケットに記入することが必須である値や障害発生間隔時間などを統計的に分析することができる。

7. 現在の警告情報のフィルタリング
   トラブルチケットの情報をフィルタリングし、そのいくつかを条件に従って警告システムに表示できる。トラブルチケットから出される警告情報をさらにエキスパートシステムに渡し分析に用いることもできる。

8. 利用者への説明
   利用者の不満をチケットに記録し、通常のトラブルと同じように 対処する。また、その時点でのチケットを見せることによって、問題発生時に管理者が対処している状況を示して、利用者の不満を抑えることができる。

以下では、現在幾つかのネットワークで利用されているトラブルチケットシステムについて考察する。

4.2.2 Merit のトラブルチケットシステム

Merit は アメリカの学術インターネットのバックボーンとなっている NSFNET の管理をしている組織である。ネットワークを監視するスタッフは常に Network Operation Center に配置され、それぞれ交代で勤務しいる。そのため、ネットワークの状況や、作業の進行状況をチケットシステムに記録し、スタッフの交代時にはチケットシステムに残された記録を見ることによって仕事の引き継ぎをする。また、チケットに残された記録によって発生した障害などを記録できるため、後で発生した事件について統計を出すことも可能である。この Merit のトラブルチケットシステムの目的としては次の 7 つ挙げられている。

- スタッフの覚え書きとその情報交換

- スケジューリングと仕事の割りふり
- 作業を委任して迅速な対処をする
- アラームの設定 (警告を出す)
- 技術者の状況把握
- 統計の分析
- ユーザへの説明

チケットへの登録は、オペレータの名前、チケットに記入した日時などの決められた欄への記入と、自由な欄での詳しい説明書きをする。

4.2.3 JvNCnet の TROUBLE TICKETING SYSTEM (NETLOG)

JvNCnet では “NETLOG[86]” という名前の トラブルチケットシテムが作られている。NETLOG は特定のデータベースに依存せず UNIX 上で標準的に提供されているツールのみで実装されている。全て記録は ASCII text のファイルで残し、ファイルの長さに制限はない。UNIX のツールを用いて設計されているので、チケットにアクセスする時のパフォーマンスは grep の性能に依存する。NETLOG への入力としては次の 4 つが準備されている。

1. OPEN
   問題が発生した時にチケットを新たに発行する。チケットには自動的に新しく一意に決まるチケット番号が割り振られる。

2. UPDATE
   OPEN されたチケットに何か情報を付加する時、OPEN されたチケットから該当するものを探して情報を付け加える。

3. CLOSE
   チケットが OPEN されていた問題が解決されると、チケットを CLOSE してリストから外す。その時に、発生した問題を短くまとめて、後で報告するときに利用できるようにする。

4. INFORMATIONAL
   情報とする目的のためだけの全てチケットの入力指す。ユニークなチケット番号は自動的に割り付けられる。

NETLOG コマンドのオプションは 次の 6 種類。

1. Create Entry
   WRITE-GROUPS に入っている人だけが、チケットを生成できる。時刻 (何時何分) を入れ、デフォルトでは vi を用いて文章を入力する。 入力が終わると、メールでチケットを送る宛先を尋ねられる。入力がうまく記録をアップデートできなかった時は、エラーのメールがユーザや管理者に送られ、エラーの内容は subject に書かれる。

2. Edit Log
   記録されているデータを編集する。

3. Read Log
   記録されている情報を参照する。

4. Index
   管理者がインデックスファイルを保守に用いる。

5. List open tickets
   オープンされているチケットの一覧を表示するときに用いる。

6. Search logs
   正規表現を用いて、記録を検索する。このコマンドは”grep” を用いた記録の検索を用いている。この検索にはオプションが 2 つあって、一つは全ての記録ファイルの検索をする、もう一つはもう少し狭い範囲のファイルを検索する。

7. Process tickets
   登録された情報はチケット番号の順番に保存されるのではなく、入力された日付の順番で保存されている。このオプションは、日付けの順番での特定の (またはある範囲の) チケットをある指定された出力 (標準出力、プリンタ、ファイルなど) に出力する。

このトラブルチケットシステムは、RFC1297 が出される以前に作られており RFC の指針に沿って作られていない。

4.2.4 ConcertNet Trouble Tickt System

ConcertNet Trouble Tickt System[87] は ConcetrNet で作られたトラブルチケットシステムである。データベースとしては postgres[88] を用いており、実際のチケットの操作の部分はシェルスクリプトで記述され、インターフェースには shellform[89] と Tk[90] が用いられている。

次の 7 つの操作が用意されている。(たらし、そのうち 1 つは実装されていない。)

Create New Ticket 新しいチケットを発行する

Display Ticket 入力した条件に合うチケットを表示する

Update Ticket チケットを選んで情報を追加する

Close Ticket チケットを選び、Close する

Cancel Ticket チケットを選び、無効にする

Handoff Ticket (まだ実装されてない)

List Open Tickets open されている ticket 全てのリストを示す

チケットを新たに発行した時に入力する必須の項目は

- Site 問題が起きたサイト名。41 のサイト名が登録してあった。(これは ConcertNet の環境のため)
- Types "planned" "unplanned" から選択
- Source 問題を発見した手段。 email, phone, monitor, other, self の中から選択する。
- Priority 優先度として high, normal, low の 3 つから選択。
- Scope 問題の及ぶ範囲。campas, host, internet, network, other, subnet 6 つの侯補から選択する。
- Problem 問題の説明を文章で入力
- Action どのような対処をしたかを文章で入力

任意で入力する項目は

- Problem Start 障害が発生した時刻
- Next Alarm 次のアラームを設定するまでの期間
- Site Contact このチケットの内容についての問い合わせ先

自動的に入力されるのは

Status チケットが open された時には open と入力される。(他に、close, cancelled が用意されている。)

Owner チケットをオープンした人のログイン名

Ticket Number チケットに割りふられた番号 (チケットの発行順に 1 つづつ大きくした整数を割り振る)

Ticket Opened オープンした日時が表示される

Create 以外のコマンドを用いるときには、選択肢が用意されていた入力項目のうち、一つ以上の項目での選択肢を条件として指定することにより、その条件に該当する全てのチケットを表示し、さらにその中から目的とするチケットを選び出して操作を行う。

Update の時には、 新たに”additional info” という欄が作られ、そこでファイル名を指定することができる。後でそのチケットを参照する時に、その additional info に指定したファイルを表示することができる。

List Open Tickets ではオープンされているチケットの一覧を表示する。表示される項目は、Ticket Number、Site, Priority, Popend(日時) のみである。

4.2.5 既存のトラブルチケットシステムの利点

障害に関する情報を扱うためにトラブルチケットを利用する利点として以下が挙げられる。

- 効率的に情報を扱うことが可能。
  障害情報がデータベースに記録されるため、電子メールの記録などに比べて効率良く必要な情報を検索して利用することができる。記録した人だけでなく、アクセス権をもつ複数の人間がその情報を利用することができる。

- 障害管理作業の記録が残される。
  チケットシステムの記録から障害への対処作業の経過を辿ることができるため、効率的に障害管理作業を行うことができる。また、その作業の記録を後で障害対処の作業の履歴として利用することが可能である。

4.2.6 既存のトラブルチケットシステムの問題点

トラブルチケットシステムには上に挙げたような利点があるが、インターネットでの障害管理で利用されるためには十分であるとはいえない。なぜなら以上挙げたシステムでは単一の管理ドメイン内部での利用が前提となって設計されたものだからである。ここで既存のトラブルチケットシステムをインターネットの管理に利用する場合の問題点を挙げ、インターネットの管理にも利用できるような拡張を考えていく。

- 迅速な情報伝達の方法が提供されていない
  トラブルチケットシステムはデータベースを基本としているため、利用者が検索を行って初めて情報が伝達され、システム側から管理者へ情報を積極的に送り伝える機能は作られていない。アラームの設定が可能なものもあるが、これはあるチケットに記録されたことに対して一定時間経過しても対処されていない場合に出される警告である。迅速に伝えるべきイベントの発生を、担当する管理者に確実に伝える方法は提供されていない。

- インターネットを介したアクセスを前提としていない
  ひとつの管理ドメインの内部でのみ利用する場合には、インターネットを介さずローカルエリアネットワークの内部でチケットシステムを利用することができる。しかし、管理ドメイン間の情報交換に用るためにはインターネットを介して他の管理ドメインの管理者に必要な情報を提供する機能が必要がある。上に挙げたシステムは単体で用いるもためのものであり、複数のドメインによるチケットシステムの関連を前提とされていない[2]。

- 他のシステムとの連動を前提とされていない
  SNMP などを用いてネットワークの状況を監視するシステムは徐々に利用されはじめている。多くのネットワークの監視システムでは監視している部分の値がある閾値を越えると何らかの方法でアラームを発生させて管理者の注意をうながすことが多い。この時、障害情報のひとつとして監視システムからトラブルチケットにその記録を残すことも重要である。それによってその障害の検知というインベントを記録にすることも考えられる。

  現在のシステムでは、自動的な (人間以外による) チケット記入などの方法は提供されていない。

- チケット相互の関連性
  既存のトラブルチケットシステムでは、現在オープンされているチケットを検索して、関係があると判断されるチケットがオープンされていればそれに引き続いたチケットへの記録を付加していくという方法をとっている。管理ドメン間での情報交換を可能にするには、複数のチケットシステムの持つ情報の関係付けが必要とされる。

- 入力方法
  既存の Ticket System の実装では、Curses、Shellform、X などのインターフェースが用いられている。たとえば必ず記入しなければならないフォーマットの決まった欄には、いくつかの入力侯補が挙げられており、その中から 1 つを選んで入力するという形式になっている。ネットワーク管理を行っている人は、日常的に計算機を利用しており、必ずしも X のインターフェースが使い易いとも限らない。そこで、利用者によって入力方法をカスタマイズ可能なように入力方法を切り分けられるような拡張性を持たせる必要がある。

4.3　インターネットの障害管理に必要とされる情報の伝達

ネットワークもしくはインーターネットを管理する場合、管理に関する情報を複数の管理ドメインの間で交換する必要がある。ここでは、インターネットの障害管理で必要とされる情報の伝達について述べる。

[2]CONCERT Trouble Ticket では、操作項目の中に”Handoff to another NOC” というメニューは作られているが、まだ実装されていない

4.3.1 障害に関する情報の交換

一般にインターネットの管理では情報交換が重要であることは前に述べた通りである。特に障害については、協調して動作しているシステムの間の情報交換が大変重要になる。

情報交換が必要な障害に関する情報は大きく次の 2 つに分けられる。

- 障害発生などの通知 (警告)
- 障害についての詳しい情報

前者は、担当の管理者に確実に知らされなければならない場合で、一刻も早い対処が必要である場合などがある。後者は障害解決の作業を行うために必要となる情報であり、障害管理の作業の過程で利用できなければならない。また、障害についての情報を知らせるという場合である。

この 2 つはその目的に的した情報伝達の方法を用いるべきであり、現在一般に用いられている電子メールもしくはメーリングリストを用いる方法はどちらの情報伝達にとっても中途半端な役割しか提供しない。

前者は伝える側が積極的に情報を送りつける必要があり、後者は情報を受ける側が必要に応じて情報を得られるようにするべきである。そこで以降ではこの 2 つの情報伝達の方法を、**警告**と**問い合わせ型**という言葉で表していく。警告型とは、知らせるべき相手に対して伝える側から情報を送り付けて伝える場合であり、問い合わせ型は情報を受ける側が必要とする時に情報が伝えられる場合である。

ネットワークの障害管理での情報交換をこの 2 つに大きく分け、それぞれどのような場合どのような方法で情報を伝達していくかということについて、検討していく。

4.3.1.1 警告型

目的とする相手に必ず情報が伝達されなければならない場合であり、以下のような例が挙げられる。

- 比較的原因のはっきりした障害について復旧作業の依頼 (ルータのリセットが典型的)
- 原因があると思われる部分の管理者に障害原因の究明の依頼
- 現在発生している障害に関係する情報の提供依頼

障害が発生した場合には、それがネットワークに与える被害を最小限にするためにも、できる限り早急に原因を特定し復旧作業を行わなければらない。この場合、早急にかつ確実に担当する管理者に伝わり認識されることが重要である。そのために、情報を伝える側から必要な相手に対して情報を通知する必要がある。認識されるために伝えられる情報は、管理者の注意を向けるための必要最小限の情報で十分であり、一度通知した後は別の方法を用いて詳しい情報を獲得できればよい。

警告型の情報としては、必ずしも緊急に伝えられる必要があるものばかりとは限らず、特定の管理者によって認識されていなければならないこと、例えばその管理ドメインが

直接接続されている NOC のゲートウェイの保守のための停止の予定など、についても警告型によって知らされるべき情報として考えるべきである。

障害に関する情報の伝達の場合に考慮慮するべきことは、障害発生時にはその影響によってネットワークが利用できない可能性が大きいということと、管理者が必ずしもインターネットアクセスが可能な場所にいるわけではないということである。この場合にも、何らかの手段をによって情報を伝える必要がある。

現在広く用いられている電子メールによる情報伝達は、問い合わせをしなくとも情報が送られてくるため警告型の情報の伝達の一つの方法といえる。そかし、メールによる情報伝達には様々な欠点があり障害情報の伝達に適しているとは言い難い。

警告型の情報の伝達によって伝えられた情報は、管理者がそれを忘れないように何らかの覚え書きを残すべきである。これは作業を確実に行うこと、また作業の記録を確実に残すという意味で必要である。そのため、警告型で伝えられた情報は後から参照可能な形、つまりこの後で述べる問い合わせ型の情報として利用可能な形で残すべきである。

4.3.1.2　問い合わせ型

問い合わせに応じて、情報を提供するような場合の情報伝達方式である。この場合として、以下のような例が挙げられる。

- 発生した障害の詳しい状況の説明
- 対処の必要がない管理者に対しての障害が発生の連絡
- 障害が復旧したという連絡
- 保守のための予定されたネットワークの停止の連絡

障害発生によってネットワークが利用不可能になった場合も、その影響を大きく受けない管理ドメインにとっては、その障害に関する情報を必要としない場合が多い。同様に、保守のための予定された障害 (ネットワークの停止) は大きく影響を受けるネットワークのの管理者には伝えられるべきであるが、それ以外の管理者にとっては必要となった時にその情報が得られる状態にすることが必要である。

さらに、一般のユーザが直接そのような障害情報を知るための方法が提供されていないため、障害についての情報を得るためにはそのユーザの所属するネットワークの管理者に問い合わせるという間接的な方法を用いなくてはならない。一般のユーザにとっても、インターネットを介した何らかのサービスが利用不可能である場合、それが予定されたネットワークの停止のためなのか、予定していない事故としての障害によのか、さらにその障害がいつ復旧するのか、などの情報が得られた方が良い場合も多い。

そこで、ユーザからの問い合わせに対して効率的に情報を提供するシステムが必要である。これを実現するものの一つとして前に挙げたトラブルチケットシステムがある。

問い合わせ型の場合には、ユーザが必要とする情報を効果的に検索できるかどうかが重要である。

4.4 障害の影響下での情報交換

障害に関する情報交換をする場合に、障害の影響によってネットワークが利用できない状況になることが考えられる。そこで、障害の影響をできる限り回避して情報伝達を実現する手段について検討する。

4.4.1 警告型の情報伝達

必要とされる人に情報を送り付ける警告型の情報伝達の手段としては、現在以下の方法が利用されている。

- 電子メール
- ポケットベル
- 電話

電子メールの場合、相手が到着したメールを読もうとしなければ送られた情報も伝わらない。情報を伝えるべき相手が到着する電子メールを即座に読んでいるという状態が保証されるならば電子メールでも十分であるといえるが、通常はそのような状況とは限らない。また、相手がメールを即座に読んでいる状況でも、障害の影響によってメールの配送に失敗する場合も多い。そこで、電子メールより確実に相手に認識され、障害の影響を受けない方法を用いて伝えられるべきである。

インターネットを利用しない伝達方法としては、電話、ポケットベルなどがある。電話は現在、電子メールが利用できない場合に最も一般的に利用されている。ただし、電話の場合必要とする相手の電話番号を知っている必要があり、また相手がその電話を取ることのできる状況でなければならない。しかし障害の復旧作業をする場合の連絡には電話による状況報告をしながら作業を行う場面はよく見られる。電話で情報交換する場合は、特定の 2 人の間でしか情報の交換が行われず、それ以外の管理者には情報が伝えられないためこれも障害に関する記録として参照できる形に残すべきであるが、問題点が解決された時点でその事後報告を残すという作業は面倒であるため、管理者が書くという方法では実際には記録を残すのは難しいと考えられる。

電話やポケットベルは、通常人が直接操して用いられるが、WIDE プロジェクトでは計算機からポケットベルへメッセージを送るシステム [91] が実装されている。現在は、計算機から自動的に電話をかけ自由文型ポケットベルに電子メールの日本語を含むメッセージ (32 文字まで) を表示することが可能である。これは、あらかじめ各ポケットベルに対応する電子メールのアドレスが設定されており、あるメールアドレスに対してメッセージを送り、それを受けとる計算機は、電子メールのメッセージをポケットベルが文字を表示できるような電話の信号に変換し、指定されたポケットベルの番号に自動的に電話をかけ信号を送る。計算機からポケットベルへのメッセージの送出が可能であるため、他のシステムがある条件で自動的にポケットベルへメッセージを送ることも可能で

ある。また、問い合わせ型の情報としてポケットベルへ送られたメッセージを残すことも容易である。

しかし、現時点ではポケットベルで伝えることのできる情報量は少なく、また実験段階であるため広く一般的に用いられいる訳ではない。警告型の場合、伝えられる情報量よりも迅速に確実に最低限の情報を伝えることが重要であり、詳しい情報については別の方法で獲得する必要がある。

ポケットベルによる警告を伝える現在の方法の欠点としては、ポケットベルをによって相手に確実に情報が伝えられたかどうかが確認できないという点である。ポケットベルが鳴らない場所に相手がいる場合もそれが確認できない。しかし、ポケットベルのメッセージを受けとった場所で受けとり確認のメッセージを送るなどの方法を実現するべきである。この時に現在実験段階であるが、電話のプッシュホンによる計算機の遠隔地からの利用などの利用も考えられる。

また、ポケットベルへの信号を出すシステムまでメールが到達できないような障害が発生した場合にはポケットベルへ信号を送り出すことができない。そこでインターネット全体で利用する場合には各管理ドメインポケットベルへメッセージを送るシステムを置くなど、ある程度起き得る障害を考慮してシステウを配置することが必要である。

現在利用可能な警告型のシステムのでは、ポケットベルにようる方法は相手がどこに居ても、どういう状況でもほとんどの場合に情報の伝達が可能であり、計算機からの操作するなどといった理由で、最も効果的な方法であるといえる。

4.4.2　問い合わせ型の情報伝達を実現する手段

管理者が障害の通知を受けた後、その障害に対処するためには障害に関する詳しい情報が必要になる。この場合、必要とされる情報は管理者の側から要求する問い合わせ型となる。

問い合わせ型のシステムの例としては、前に紹介したトラブルチケットシステムがある。ただし、インターネットでの障害管理の場合必要になる情報は管理ドメイン内部のものだけでなく、他の管理ドメインの情報も必要になる。そのため、インターネットを介して他の管理ドメインの情報も参照可能なトラブルチケットシステムが必要である。

インターネットが正常に利用できる場合には、通常のインターネットでの通信の方法を利用することにより、他の管理ドメインのシステムへのリモートアクセスを実現することも可能である。

しかし、障害の発生によって通常インターネットで利用可能な通信が不可能になる可能性もある。そこで、可能性のある障害をあるていど考慮し、障害発生時には特別な手段を構じることによってインターネットを利用可能にする方法を、障害の原因を挙げながら考えていく。

4.4.2.1 ホスト名を指定した通信のみが不可能な場合

DNS が正常に動作しない場合には計算機の名前を指定することによる通信は不可能になる。しかし、この場合には直接 IP アドレスを指定することによって通信可能になる。目的とする計算機を名前で指定することを前提としたアプリケーションプログラムのいくつかは、たとえ IP アドレスを知ていても利用することはできない。(例えば電子メールなど)

そのため、障害情報を提供するシステムでは DNS が利用できないことを考慮し IP アドレスによる利用を可能にするべきである。

4.4.2.2 IP 層の通信ができない場合

この場合、通常の通信は利用できないが、障害を解決するためには通常の TCP/IP での通信手順やインターネットの運用方針を無視したいくつかの方法が考えられる。ここでは、IP パケットの配送を可能にするいくつかの方法を挙げる。

- あるルータでの経路制御の不良が原因となっている場合

  IP パケットの経路制御オプションを指定することにより、経路制御に問題のあるルータでの経路制御の影響を受けずに、目的とする計算機まで IP パケットの配送を可能にする。

- 途中の経路が断たれている場合

  – 通常、経路制御は動的に交換される経路情報に従って効率の良い経路を用いて行われる。 もし目的とするアドレスまで利用可能な迂回経路があるならば、その経路を IP の経路制御オプションで指定することにより目的とするアドレスまで到達することができる。

    日本のインターネット環境で、例えば WIDE インターネットから他の経路を利用する方法として以下の例がある。日本の場合 WIDE インーターネット以外に、TISN[3]、JAIN[4]などの複数のインターネットが存在する。インターネットへの参加組織は 1 つのインターネットだけに接続しているとは限らず、同時に複数のインターネットに参加している場合もある。各ネットワークの内部では参加しているそれら複数のインターネットの利用についての制御が行われている。そこで、複数のインターネットに接続されているネットワークは 2 つの複数のバックボーンネットワークの相互接続を実現していることになる。そこで、あるインターネットのバックボーンでで障害が起きた場合にバックボーンを相互接続しているネットワークを介して障害が発生した部分を迂回し、 目的とする計算機まで到達可能にすることができる場合もある。しかし、この場合通常と異な

[3] Todai International Science Network
[4] Japan Academic Inter-university Network

る経路制御をする必要があるため、インターネット相互で代替経路として利用することについての合意が行われていなければならない。

– 代替経路が全く考えられない場合には、通常のインターネットの経路と別に、特別に臨時の経路として、ISDN の回線や普通の電話回線とモデムを利用してある計算機までの経路を作り、その経路を介して目的とする計算機まで到達することができる。

通常は、インターネットのプロトコルを無視したこのような方法での通信は行うべきではないが、緊急の情報を伝えることによって正常な状態に早く復旧できるならば、必要最小限の障害に関する情報の伝達にこのような方法を用いることは、インターネットの管理にとって有益であると考えられる。

これらの方法は、障害情報について問い合わせ型の伝達を提供するシステムで利用可能にしなければならない。

4.4.2.3　IP の始点経路制御オプション

前に述べたように、IP 層のいくつかの問題は IP のオプションを利用することによって回避することができる。

このためには、IP のオプションの一つである**始点経路制御オプション**を利用する。始点経路制御とは、送信者にインターネットの経路を指定する方法を提供するもので、これはインターネットのシステムでの問題点を解決するために用いるものである。始点経路制御には、**厳密な始点経路制御** (strict source routing) と**厳密でない始点経路制御** (loose source routing) という 2 つの形式がある。

厳密な始点経路制御
: 指定される一連のアドレスが、終点に到達するまでの正確な経路を全て指定する。アドレスのリスト中の 2 つの連続したアドレスの間は一つのネットワークハードウェアから構成されていなければならない。ルータが指定されたアドレスに従うことができない場合にはエラーを返す。

厳密でない始点経路制御
: 一連の IP アドレスが含まれるが、リスト中のアドレスの間に複数のネットワークが存在していてもよい。

IP オプションは、IP ヘッダの最後に付けられる可変長のフィールドである。オプションの種類を示す 8 ビットの CODE フィールド、オプションの長さを示す 8 ビットの LENGTH フィールド、次に利用できるオプションフィールド中のオフセットを示す 8 ビットの POINTER フィールドそして経路として指定されるアドレスのリストが続く。両方の始点制御オプションとも、アドレスリスト中のアドレスがローカルアドレスになるようなルータで、リスト中のそのルータ自身のアドレスをルータのアドレスに書きかえる。つまり、データグラムが終点に到達した時には、通ってきた全てのアドレスがオプションのアドレスリストに含まれることになる。

IP オプションの始点経路制御を用いることによって、ルータが持つ経路テーブルを利用しない IP パケットの配送が可能になる。

4.4.3 障害を回避した通信を実現するための必要事項

障害発生時に上に挙げたような特別な方法を用いて通信を行うためには、情報交換を必要とするシステムはあらかじめ以下のようなことを確認し、準備しておく必要がある。

1. 他の管理ドメインのトラブルチケットシステムの IP アドレス
   通常、インターネットを介したサービスの利用は IP アドレスではなくホスト名を利用して行われる。そこで DNS を利用できないことを考慮して、ホスト名でなく IP アドレスで他の管理ドメインのトラブルチケットシステムにアクセスするためには、必要となる可能性があるシステムの IP アドレスをインターネットの障害の影響受けない場所に持っている必要がある。

2. 他の管理ドメイン内の情報を提供するシステムまでの代替経路
   障害を回避する代替経路を利用するためには、障害発生の状況をある程度想定し、障害に応じた代替経路を通常から把握しておく必要がある。しかし、ネットワークの構成の変化に応じて代替経路の情報を変更し保持していくのは手間がかかるため、ネットワークの構成の変更に伴って代替経路を更新する何らかの方法が必要である。

4.5 障害管理のための情報交換システム

ここまで述べたように、障害によりネットワークの通信に様々な影響を考慮し、目的に的した方法で障害情報の交換を実現するシステムが求められる。

警告型と問い合わせ型の情報伝達はどちらも障害管理にとって必要であり、この両方を利用して障害の原因となる問題点を解決していく。実際に障害に対処する作業の中で、2 つの情報伝達が用いられる例を挙げる。この例では、警告型としてポケットベルを、問い合わせ型としてトラブルチケットシステムを用いる。

1. ポケットベルによって、ルータのダウンが知らせられる。

2. 管理者はトラブルチケットに障害発生を記録する。

3. その障害による影響を受けた他のドメインの管理者は、トラブルチケットシステムにその障害に関する情報が記録されていないかどうかを調べる。

4. 障害から復旧したら、障害に対処した管理者はそれをトラブルチケットシステムに記録する。

これ以外にも、障害の原因を追及する場面で他のドメインの情報を調べるため、またユーザからの問い合わせにトラブルチケットシステムを利用する場合などがある。

現在利用可能な情報伝達の方法を考慮すると、警告型としてはポケットベルを、問い合わせ型としてはインターネットで利用可能なトラブルチケットシステムを利用することが求められているといえる。

そこで次の章では、インターネットでの障害に関する情報のうち、問い合わせ型のものを提供する、分散型のトラブルチケットシステムの設計を行う。

第 5 章

分散型トラブルチケットシステムの提案

この章では、インターネットで発生する障害情報を問い合わせ型として提供するための、分散型トラブルチケットシステムを提案し、今後このシステムを実現していくための課題を述べる。

5.1 分散型トラブルチケットシステム

既存のトラブルチケットシステムは、集中して障害に関する情報を登録するデータベースシステムである。そこで、インターネットでの障害情報を扱うために新たに分散型のトラブルチケットを提案する。

トラブルチケットシステムは障害情報を記録し、それを複数の管理者が参照するものである。インターネットを介した分散型として必要な機能として大きく以下の 2 つが挙げられる。

- 障害管理に必要な情報の記録
- 障害管理に必要な情報の交換

障害に関する情報の記録は、データベースに登録する。データベースは各管理ドメインで持ち、それらの複数のドメイン間での情報交換のためにインターネットを介したトラブルチケットシステムへのアクセスを提供する。

5.2 全体の構成

このシステムの機能の概念図を 5.1に示す。

データベースへは前に述べたトラブルチケットシステムと同様に、様々な障害に関する情報を格納する。ただしインターネットでの利用を考慮して管理ドメイン間で関係付けを行うための項目を加え、また管理者が直接チケットを発行する以外に管理システムや警告型として出された障害情報の記録など、他の計算機を利用したシステムからトラブルチケットシステムへの入力も実現する。また、将来的にはトラブルチケットへの登録と同時に、警告メッセージを出すといった他のシステムとも連携も実現する。情報を格

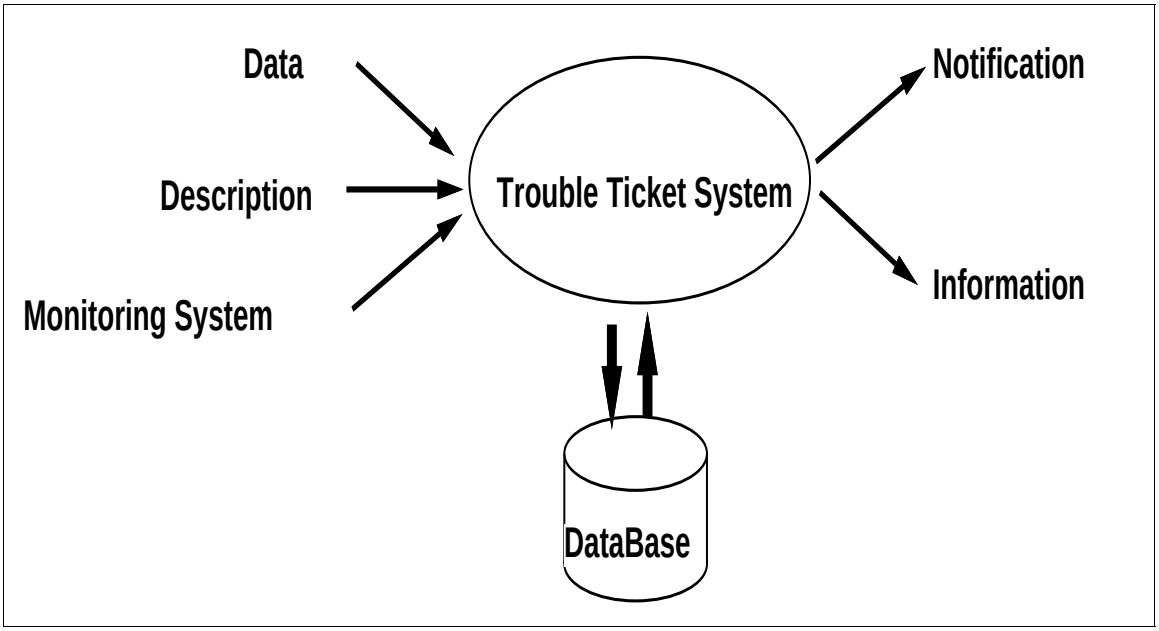

図 5.1: トラブルチケットシステムの提供する機能

納するデータベースは各管理ドメインごとに配置し、それらはインターネットを介して利用可能にする。ただしインターネットを介した利用では発生すると考えられる障害の影響を可能か限り回避してアクセスを可能とするような方法を実現する。

5.3　トラブルチケットシステムへの入力

従来のトラブルチケットシツエムでは、主に管理者の覚え書きとして残される記録としての役割のために用いられたため、記録の内容は管理者から直接入力されるものであった。

このチケットシステムでは以下のような入力を受け付けることとする。

- ネットワーク監視システムからの情報
  ネットワーク監視システムがネットワークの状態をモニタしている場合の多くは、ある条件が成立すると管理者に知らせる設定になっている。その時に、監視システムから得られるデータを自動的にチケットシステムの記録として残す。チケットシステムに残されたデータと、その時に発生している情報との因果関係を得ることができる。

- 管理者の作業の記録
  管理は自分の管理作業に関係した記録をチケットシステムに残す。残された記録から、行われた管理作業の履歴を得ることが可能である。記録は管理者が後から参照することを考え、登録される情報の関係を利用可能にする

- 各コマンドの実行結果
  ネットワークの状況を把握するために利用されるコマンドの実行結果は、障害管理

作業の上で重要である。そこで、障害に関する情報として各コマンドの実行結果を登録する。

5.3.1 チケットシステムが利用する障害情報データベースの形式

チケットシステムに記録する項目としては以下のようなものが考えられる。

識別子 チケットごとに固有の識別子

チケット登録の日時 記入した日時

登録者氏名 そのチケットの登録を行った人の名前

重要度 障害の重要度を示す

概要 障害の概要を示す

関連するチケットの識別子 その障害に関係するチケットの識別子

障害の内容説明 障害の内容

用いたコマンド 作業に用いたコマンドとその結果

対処 障害への対処

関係ある管理者 その障害に関係する管理者を示す

これらのうち、識別子はシステムが自動的に割り当てるが、複数のチケットシステムで情報交換をするとこを考慮し、インターネット全体で一意に決まるようなものを用いる。識別子によって、あるチケットの記録に関係ある他のチケットを指定する。概要、障害の内容、用いたコマンド、対処 については自由なフォーマットで記入されるが、それぞれでキーワードを取り出し登録する。キーワードは検索する場合のキーとして利用できる。

5.3.2 データベースの操作

データベースの操作としては、次の 3 つを用意する

- 新規登録
- 検索
- 変更

検索は、チケットの識別子、登録日時と、「概要」、「障害の内容」、「用いたコマンド」でのキーワードを用いる。

変更で重要なのは、関連するチケット識別子の登録である。障害管理の過程で関係する他のチケットを参照したならば、その識別子を記入する。

5.4　トラブルチケットシステムでの情報の交換

5.4.1　警告型の情報の伝達

障害の発生を検知し、その障害への対処に他の管理ドメインが関係するならば、その管理ドメインに対して障害が検知されたことを伝える必要がある。

チケットシステムの障害への対処に、あらがじめ設定で決まっている書式で記入することにより、チケットシステムはコマンドを実行する。例として、担当者のポケットベルへ電話をかける、またはメールとしてそのチケットの内容を伝える、など警告型で情報伝達を行うための操作を実行する。

このためには、前もって警告型の情報伝達が必要な場合を考慮し、必要な情報 (伝えるべき管理ドメインの指定方法) などを把握しておく必要がある。

5.4.2　問い合わせ型の情報の伝達

インーターネットの場合、ドメインごとに分かれている管理区分を反映して、ドメインごとに配置されているチケットシステムの間で通信を行い情報を伝達を行う。

5.4.2.1　障害発生時の問い合わせ型の情報伝達手段

何らかの障害が発生した場合には、前に述べたようないくつかの手段によって問題の部分を回避することが可能である。そこで、障害に関する情報を問い合わせによって得る場合にも障害を回避して通信を行う手段を提供する。

そのための方法としては以下の方法がある。

- IP の厳密でない経路制御オプションを利用する。
- 代替経路を臨時に設定する。

代替経路を用いた通信を行うために、他のドメインのチケットシステムにアクセスする場合は、目的とするチケットシステムに対してまずはじめに通信可能がどうかを確認する probe packet を送る。目的とするチケットシステムから確認応答を受けた後にチケットの操作を開始する。もし、最初の probe packet に対する確認応答を受けられなければ、代替経路として利用可能であると考えられる経路を指定し、再び probe packet を送る。このようにして、他のドメインのチケットシテウムへ問い合わせを行う場合には、その操作を行う人に対して明示的に通信可能性を示しながら操作を行う。

5.4.2.2　IP の始点経路制御を用いた経路制御

IP での問題を解決するために、厳密でない始点経路制御を利用する。指定する経路は、チケットシステムを利用する管理者によって直接指定する。しかし、障害の発生した場合に利用可能と考えられる代替経路については、あらじめ考慮したデータを用意しておき、代替経路を指定する場合にはそれを参照できるように準備しておく。

5.5 今後の課題

現在、この分散型トラブルチケットシステムのプロトタイプの実装をフリーのデータベースシステムである POSTGRES[88] を利用しながら行っている。また、厳密ではない始点経路制御を利用し、ネットワークを介した障害情報を交換を行うためのプロトコルを設計し、プロトタイプの実験を行っている。

今後、このシステムを実際のインターネット管理に利用するためには、以下のような課題を解決する必要がある。

- 他のネットワーク管理システムとの連携
  SNMP を用いたネットワーク監視システムなど、様々なネットワークに関する情報を得るためのシステムと、チケットシステムとの連携を行う。また、ネットワークモニタなどによってネットワークを監視して得られるデータをネットワーク管理情報として利用していく。

- 日本語の入力
  実際の我々が管理作業を行っていく中で用いるためには、日本語の入力を可能にする必要がある。

- 入力インターフェース
  実際の管理作業を考えると、管理者に負担をかけないインターフェースを提供する必要がある。ネットワークの管理者は日常的に計算機を利用している場合が多い。そこで、入力のためのインターフェースを個人で変更可能にし、いつかの入力方法を提供する必要がある。

  また、ネットワークの状態を説明するためにコマンドを実行しながら、その実行結果をエディタなどに入力して編集できるようなインターフェースが必要である。

- トラブルへ管理作業の分析
  本研究では、障害の分析をするために管理者間で交換されたメールを用いた。しかし、メールの記録は因果関係が捕めないものや不完全な情報が多く、記録されていない例も多い。トラブルチケットに残された記録から、ある障害が発生した場合の対処方法を分析し、ネットワークの障害管理に利用することができる。

これまでは、問い合わせ型としての管理情報を提供する部分を中心に考てきているが、警告型の情報の提供も合わせて、インターネットの管理に必要な情報を記録し伝達するためのシステムを構築する必要がある。

また、もっと広い目でインターネットというシステム全体を管理するために必要な情報を効果的に扱う方法について検討していく必要がある。