マルチメディア通信と分散処理 64−18
（1994. 3. 4）

インターネットでの障害管理と トラブルチケットシステムについて

上水流 由香† 浅羽登志也‡ 砂原秀樹*

†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

* 電気通信大学情報工学科

現在の大規模広域分散ネットワークでは、複数のサイトの管理者が協調して管理を行っている。これらの管理者同士が協調作業をおこなう際に不可欠となる情報交換を支援するものとして、いくつかのトラブルチケットシステムが考案され実装されている。

本論文では、実際にネットワークでの障害発時に管理者のメーリングリストに残された障害に関する記録をもとに、障害に関する情報交換の必要性について考察した。そして、トラブルチケットシステムの概念を紹介し、既に実装されているシステムでの問題点を指摘する。最後にそれらの問題を解決したシスステムを構築していくための今後の方針を述べていく。

Fault Management on the Internet and Trouble Ticket Systems

Yuka Kamizuru† Toshiya Asaba‡ Hideki Sunahara*

†NTT Software Laboratories ‡Internet Initiative Japan Inc.

* Dept. of Computer Science, The University of Electro-Communications

Network managers in different locations usually have to cooperate with each other to solve a problem by the nature of distributed administration of today's computer network. Information related to failures should be shared among managers efficiently to achieve quick recovery and to minimize the impact on the human activities caused by those failures.

This paper breaks down the types of information exchanged by electric mail among network managers on occasion of network failures into several categories. Then the current framework of the Trouble Ticket System (TTS) is examined as a candidate for more effective method for information sharing among managers in distributed sites. Finally, plan for improvement is presented.

[0]†本研究は著者が電気通信大学大学院に在籍中に行った研究を主にまとめたものである

1 はじめに

現在、TCP/IP による計算機のネットワーク環境は必要欠くべからざるものとなっている。また、ネットワークはある組織内にとどまらず、様々な組織のネットワークを相互接続するインターネットも広く利用されている。そのため、常に安定したネットワークの運用が求められており、例え障害が発生しても一刻も早く正常な状態に復旧し、できるかぎり障害の発生を未然に防ぐ必要がある。

安定してネットワークを運営していくための作業は一般に**ネットワーク管理**と呼ばれ、それは、構成管理、アカウントの管理、障害管理、セキュリティ管理、性能管理に分けられる [1]。本稿では、これらのうち**障害管理**について議論をすすめる。

ネットワークの障害という言葉にはネットワークに関わる様々な問題が含まれる。例えば、通常使えるネットワークアプリケーションが動作しない場合、その原因としてはアプリケーションの問題、ネットワークプロトコルの動作の不良、物理的な回線の不良、他からの影響によってネットワークが非常に混雑している、など非常に多くの原因が考えられる。殊にインターネットではある 2 点間の通信であってもそれは非常に多くの要素に支えられて動作しているため、それらのどの部分が原因となっているかを判断し問題を解決するためには広汎な知識と経験を必要とする。また、完全にネットワーク上のアプリケーションが使えないといった以外にも、アプリケーションは一応動作するが非常にその反応が遅いといった場合、ネットワークを利用した作業には支障をきたすことになる。ここでは、ネットワークが通常と異なる状態になっている場合をネットワークの障害と呼ぶこととする。

障害管理の作業は、障害の**検知**、**原因の特定**、**復旧**という 3 段階に分けかれる。何か異常な状況が検知されると、ネットワークの状態を示す様々な情報を総合して原因を特定し、復旧作業を行う。これらの作業のためには、ネットワークの状態を示す様々な情報が必要となるが、以降ではこのような情報を**管理情報**と呼ぶこととする。インターネットのようなネットワークが相互接続された大規模なネットワークでは、各ネットワークの部分を担当する管理者が把握している情報を、お互いに交換していくことも必要となる。

次章以降では、まず実際にインターネットで生じた障害の例を紹介し、ネットワークの管理作業行われている情報交換について考察する。さらに、障害管理に必要である情報交換の形を示す。次に障害情報を扱うシステムとして**トラブルチケットシステム**紹介し、障害管理をどのように扱っているかを整理する。最後に我々のネットワークでこのシステムを構築する際の方針について説明する。

インターネットは複数の組織のネットワークが相互接続されたて作られるネットワークである。本稿では両者において利用されるトラブルチケットシステムについて考えていくため、特に違いを説明する場合以外は両方を"ネットワーク"という言葉で表す。

2 ネットワークで発生する障害と情報交換

TCP/IP による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に動作するシステムである。 2 つの計算機の間で通信をする際にも、その間には多くの機器やソフトウェアが介在しているため、障害の原因を特定するのは難しい。また、その障害の原因がある管理者の管理範囲内で完結したものであでば一人の作業で問題の解決が可能だが、複数のネットワークが接続されているネットワークでは、各部分の管理担当者間の協調と連携が必要になる。たとえば、ある遠隔地の計算機まで到達できず、traceroute などによって通常と経路の異常が確認できたとしても、それが管理範囲の外であれば問題部分を担当する管理者にその情報を伝えることしかできない。また、ある管理者の担当部分での障害がその人の担当する範囲外にも影響を及ぼすならば、その旨伝える必要がある。

現在、このようなネットワーク管理の連絡には主にメーリングリストが利用されている。ここで、実際に WIDE インターネットで発生した障害の例をメーリングリストでのやりとりの記録から示す。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。運用と管理は専任の担当者ではなく WIDE プロジェクトに参加している人々のボランティアで行われている。障害が発生しメンバーに対して何らかの連絡が必要になると、通常メンバーの議論に用いられているメーリングリストが利用される。ここで例に挙げるのは 1991 年 1 月 11 日から同年 10 月 10 日までと数年前の古い記録になるため、現在の状況と多少異なると思われる。ただし、メールでの連絡なしで解決したものや、メール以外の電話などを介して情報交換したものについては含まれないため、メーリングリストでの記録が全ての障害を含むわけではない。

上記の期間中、WIDE のメーリングリストでのメールのやりとりから障害に関するものを取り出すと、障害に関するメールが 288 通あった。そして、これらのメールで議論された障害の原因の数としては 94 件が数えられた。つまり、1 つの原因について平均 3 回のメールがやりとりされたことになる。

メールの内容としては以下のものが代表的であった。

- 比較的原因のはっきりした障害の復旧作業の依頼
- 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見込みの連絡
- 障害の復旧の連絡

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

この中で、特徴的な点を障害の原因の具体的内容は以下のように挙げられる。

ハードウェア (回線、モデム、ルータなど) が原因 ルータとして動作している計算機のハードディスクの不良、電源コンセントの緩み、専用回線の不良などがある。このようなハードウェアの障害では、その部分を通る通信が全くできなくなる。

インターネット層の問題 ルータのハングアップ、経路情報の欠落などが。例えば遠隔地のルータ間が専用線での直接接続になっている場合、一方から到達不可能が確認されても、ネットワークが利用できないためメールを使った連絡が不可能になる。このように、障害の原因がある程度明らかだが、機器が遠隔地にあるため直接操作できないためそれが出来る担当者に依頼するという必要がある。

アプリケーションン層の問題 アプリケーションソフトウェアの設定ミスなど。ドメイン名システムの設定ミスによる障害が多くあり、設定ファイル作成時の単純なタイプミスによる障害もあった。この場合、IP のパケットは到達できるが大量の Domain パケットにより回線が非常に混雑して通常の利用ができないという場合もあるため、完全にネットワークが使えなくなるわけではない。この場合、担当者に早く伝える必要がある。

ネットワークの障害により、障害修復を依頼する連絡が取れなくなる場合、通常利用しているネットワークと別に緊急連絡の手段が必要である。

また、今回メーリングリストにより明らかになった障害の事例では、ネットワークが利用できる状態の人が、他の人に何らかの情報を得るためや、他の人に作業を依頼するなどといったような必然性のある場合が多いと思われる。

3 障害管理のための情報交換

前に示したようなメールによる情報伝達の場合、過去の障害関係のメールにおいて、以下のことが特徴的であった。

管理者の設定ミスなどによる障害が多い 単純な設定ミスによる場合、担当の管理者より先に他の部分の管理者が、迅速な対応によって復旧可能である。

情報がうまく把握されていない 障害には含まれないが、停電などによる予定されたネットワークの停止もあり、これは事前に停止予定がメーリングリストによって連絡される。しかし、通常のメールの形式では後からの検索が難しいため、障害と勘違し障害報告のメールを出されているところが見られた。事前に情報が知らされることも必要ではあるが、調べたい時に手軽にいつでも参照可能な状態にするべきである。

障害報告の中に有効な情報が多く含まれている ネットワークの障害には非常に多くの事例があり、障

害管理の為にはネットワークに関する広汎な知識と経験が必要になる。そこで、障害に関するこのようなメールはネットワークの障害の事例として有効な情報が多く含まれている。また、同じ障害がそのサイトで再発する場合も見られる。管理担当者が把握している限りは問題ないが、管理範囲が大きくなる、もしくは管理担当の交代など、複数の人が関わる場合には、過去の情報を引きだしやすくすることは円滑なネットワーク管理に役立つと思われる。メールの保存では、後から利用することが考慮されていないためそれらの情報を効果的に利用することができない。また、現在メールでやりとりされているのは、発生した問題の解決が目的であるため、最終的にどう解決されたか、どのような状況だったか、などの細かい状況がわからない。

このように、メーリングリストによる情報交換には問題点がみられる。ここで、メーリングリストによる連絡方法による利点と欠点をまとめる。

- 利点
  - 受けとった電子メールを消去しなければ、後から参照するもも不可能ではない。
  - メーリングリストで受けとった情報から新しい知識を得ること ができる。
  - 電子メールは自由に文章を書くことが可能であるため、コマ ンドの実行結果などを含め詳しい説明を書くことができる。
- 欠点
  - 緊急に伝えるべきことが必ずしもすぐに伝えられない。
  - 障害によりメールが利用できなくなる可能性がある。
  - 重要な障害の情報も一般のメールと同様に伝えられるため、特別に扱うことが難しい。
  - 後からある情報が必要になってもメールの形式ではそれを検索するのは困難である。
  - メーリングリストのメンバ全てに関係しない情報でも送られてくるため必要のない人まで冗長な連絡が行われる。

前に出したメールで交換されたものとして内容的に 2 種類の情報に分けられる。

警告型 障害発生などの通知 (警告)、復旧のための作業依頼など。緊急に伝えるべきものもある。確実に目的の相手に伝えることが重要である。これを

問い合わせ型 障害についての詳しい情報、停止予定、現在のネットワークの状態など情報が必要になった場合に、得ることができるようにする必要がある。

メールによる伝達では、これらの両方についても中途半端な役割しか果たしていない。情報を積極的に送りつけるという意味では警告型であるが、確実に即座に伝わる保証はない。また、保存してあるメールを検索することも可能ではあるが、効率的でなく、メールで全ての情報を受けとっていなければならない。

4 トラブルチケットシステム

トラブルチケットシステムとは、ネットワークを管理する組織において、ネットワークの障害に関する情報、たとえば発生した障害や復旧作業などの記録を残すためのシステムである。例えれば、 病院で患者の症状を記入するカルテのようなものであり、ネットワークで起きた障害の発見時刻やその時の状況、その原因や行われた処置などを一定のフォーマットに従って記録していくデータベースである。

このようなシステムの初期のものとしては、アメリカのインターネットのバックボーンとなっている NFS ネットの管理を担当する Merit.Inc で作られたものがある [4]。これは、交代で管理作業を行うスタッフの連絡として作られたが、その他にも障害の事例の記録として、また障害件数など統計情報を出すためなどにも利用された。

1992 年 1 月には、一般的にトラブルチケットシステムに対して求められる機能やその利点 、将来期待される拡張などについて述べられた RFC1297 “NOC Internal Integrated Trouble Ticket System Functional Specification Wishlist (NOC TT REQUIREMENTS)[3]” が作成されている。

RFC1297 では、トラブルチケットシステムの目的として以下のような事項が挙げられている。

- 覚え書きとして複数の人から参照可能にする
- 勤務のスケジュールリングと人員配置のために利用する

- 担当者を示すことにより迅速に問題へ対応させる
- 問題発生から一定時間経過するとアラームにより管理者の注意を促す
- 後で障害の記録を参照する
- 障害に関する統計的な分析可能にする
- 現在ある警告情報をエキスパートシステムを用いて原因などを分析できるようにする
- 障害の状況をネットワークの利用者へ説明することにより障害発生時の利用者の不安感を抑える。

また、Merit におけるトラブルチケットシステムの他にもいくつかの実装が行われている。現在、無料で利用できるソフトウェアとしては、NEARnet の Trouble Ticket System、JvNCnet の TROUBLE TICKETING SYSTEM (NETLOG)、ConcertNet の Trouble Ticket System[7] などがある。これらは機能的には類似しており、チケットのデータを格納するデータベースや、インターフェース部分が異なったりする。

ここで、ConcertNet の Trouble Ticket System を例として実際のトラブルチケットシステムの具体的内容について紹介する。データベースの部分としては

項目名	内容
Site	問題が起きたサイト名
Source	問題を発見した手段 email,pehon,monitor....
Priority	優先順位 high/normal/low
Scope	問題の及ぶ範囲
Problem	障害内容を文章で記す
Action	対処内容を文章で記す
Problem Start	問題が発生した時刻
Next Alarm	次のアラームまでの時間
Site Contact	問い合わせ先
Status	新規のものは open 他 close,cancelled など
Open	チケットを新規作成した人のログイン名
Ticket Number	チケットの ID 番号
TicketOpened	新規に作成した時刻

上の表の 3 つのカテゴリのうち一 1 番上は必須の項目、2 番目は任意、3 番目は自動的に記入される項目である。

チケットの操作としては以下のものがある。

Create New Ticket	新規作成
Display	入力した条件に会うチケットを表示
Update	入力した条件に会うチケットに追加
Close	チケットを選び、閉じる
Cancel	現在あるチケットを無効にする
List	現在 Open されている チケットのリスト
Handoff	(まだ実装されていない)

ユーザインターフェスとしては、Shellform を利用した文字端末向けのものと、Tk を利用した X 端末用のものがある。また、このシステムは集中型であるためシステムを利用するためには、トラブルチケットシステムがインストールされた計算機にログインするなどといったことが必要になる。

このようなシステムにより、ネットワークの障害管理作業に関する情報を複数の担当者で共有することができ、また記録として残すことができる。しかし、現在、我々の周りでこのようなトブルチケットシステムの利用はあまり見られない。

利用されない大きな理由としては、**日本語が扱えないということと、現在のメールなどを介したやりとりである程度の連絡が可能である**という 2 つの点が挙げられる。しかし、例え日本語が利用できたとしても、実際にネットワーク管理作業でこのようなシステムを利用するためにはいくつかの問題点も挙げられる。

1. チケットシステムを書く作業の負担が大きい。(記録を残す人にとって有益でなければ、敢えて記録を残す作業はしないものである)
2. ひとつのシステム完結した集中型システムである。ネットワークを介してチケットシステムを利用することになると思うが、ネットワークの障害によりチケットシステムのまで到達不可能になる場合も考えらえる。
3. 検索型の情報の提供であり、警告型の情報伝達は考えられていない。
4. ネットワーク監視などの他のネットワーク管理システムとの連携が提供されていない。監視システムからの監視によるチケット発行も有効であると思われる。

5. 様々な事象の間の関連をチケットシステムで現せない。チケットを発行する際は、その時点でオープンされているチケットを見て、関係あるとおもわれるチケットがあればそれに続けて記録を残すことにより様々な事象の間の関連を出す。しかし別々に発行されたチケット相互の関連性後で示すのは難しい。

5 トラブルチケットシステムの設計

前節で紹介したトラブルチケットシステムをもとに、我々の環境でのネットワーク管理で利用することを目的としたトラブルチケットシステムを構築していく。システムは以下にあげる目標にしたがって段階的に発展させ、利用を確認しながら変更を行っていくこととする。

- 日本語の入力を可能にする
- チケット作成ができるだけ負担にならなインタフェースを提供する。利用者は、計算機の扱いに馴れた管理者であるため、全て統一された入力インタフェースよりも各自の馴れた入力系が利用可能な、カスタマイズが容易なものにする。
- 他のネットワーク管理システムとの連携をはかる。ネットワークの状態を調べる各種コマンドの実行結果がチケットの情報として残されるようにする。また、ネットワークを監視するシステムから自動的にチケットを発行することも考える。
- トラブルチケットシステムから警告型の情報伝達を可能にする。ネットワークを利用していない管理者に対して警告型の情報伝達をするためには、例えばポケットベルなどが利用可能である。
- 障害の発生によってネットワークが利用できなくなった場合に代替経路を利用してチケットシステムを利用できるようにする。

また、このシスム全体に関わることだが、入力するエントリーの項目や内容が、有効であるかどうか、十分検討するべきである。既存のチケットシステムの入力項目を比べた場合、特に大きな違いもなくほぼ同様の項目が設定されているため、まず既存のシステムに倣ったエントリを実装し、利用状況を見ながら検討と改良を行う。

また、インターネット全体の管理を考え、各ネットワーク間で情報交換が必要な情報をやりとりするために、チケットシステム間での情報交換のプロトコルを考えていく。

6 まとめ

ネットワークの障害管理を効果的に行うための情報交換について考えた。まず実際のネットワークで起きた障害例を障害管理に利用されたメールの記録から整理し、ネットワークの障害管理に必要とされる情報交換について検討した。そして、既に提案されているトラブルチケットシテムによる障害情報の扱いによる問題点を考慮し、今後のネットワーク管理に必要なトラブルチケットシステムについて検討した。

謝辞

本論文を書くにあたり様々な助言を下さいました、NTT ソフトウェア研究所ソフトウェア基礎技術研究部 小野諭主幹研究員ならびに Paul Francis 主任研究員に深く感謝致します。

参考文献

[1] ISO,"Information processing systems – Open Systems Interconnection – Basic Reference Model-Pert 4: OSI Management Freamwork",ISO7498,1984

[2] 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.

[3] D.Jonson,"NOC Internak Integrated Trouble Ticket System Functional Specification Wishlist (NOC TT REQUIREMENTS"),RFC 1297,Merit Network, Inc.,January 1992.

[4] Kraig R.MEYER, Dela S.JOHONSON,"Experience in Network Management : The Merit Network Operations Center", Integrated Network Management,II,1991

[5] Dela S.Jhonson,"Welcome to the NOC",Merit Network Operation Center.

[6] Vikas Aggarwal,"netlog reference manual",JvNCnet,May 1992.

[7] Tom Sandoski,"CONCERT Trouble Ticket System User's Guide", CONCERT Network,1992.