さまざまなアクセス手段を備えたルータ運用支援機構

辻元 孝博　　大野浩之
東京工業大学大学院 情報理工学研究科

概要

計算機ネットワークの急速な普及が進み、今日ではさまざまな機器によりネットワークが構成されている。しかし、それに伴い管理作業も増加し、ネットワーク管理者に大きな負担を与えている。その要因として、構成機器の多様化という点と管理手段が限定されているという点があげられる。本論文では、さまざまなアクセス手段からネットワークの運用ポリシを記述することで、これらの要因を改善し、管理作業の負荷を軽減するシステムを提案する。運用例としてルータの重要な機能の一つであるパケットフィルタリングに対して、このシステムが有効であることを示す。

Supporting router management using various access methods

Takahiro Tujimoto　　Hiroyuki Ohno
Department of Information Science, Tokyo Institute of Technology

abstract

Recently, a network became complex caused by the development of the computer network, and the load of the computer network management work is on the increase. In this paper, we propose the system which reduces the load of the management work by describing management policy of the computer network from various access methods such as the telephone, WWW, and so on. This system reflect management policy on the computer network precisely, and provide a wide management style for the network manager. As an example, show that this system is effective on computer network management of access control on the network (packet filtering) which is one of the important function of router.

1　はじめに

計算機ネットワークの急速な普及が進み、今日ではさまざまな機器によりネットワークが構成されている。しかし、それに伴い管理作業も増加し、ネットワーク管理者に負担を与えている。

ネットワークの管理が管理者に与える負荷の主な要因は、次の 2 つであると著者らは考える。1 つの要因は、ネットワーク構成機器が多様化し、管理対象が増えたため、ネットワーク管理に幅広い知識が求められることであり、もう 1 つの要因はネットワーク管理のための手段が限られることである。そこで著者らは、この 2 つの問題点を改善するためのシステムを提案し、NIIS システムと名付けた。

本論文では、この NIIS システムの設計と実装、およびその利点について述べる。第 2 章では計算機ネットワークを管理する上での問題点を指摘し、これを解決する方法について述べる。第 3 章では、NIIS システムの概要および構成について述べ、第 4 章で NIIS システムの運用例として、ルータのアクセス制御に関する運用例について述べる。第 5 章では、考察を述べ、第 6 章で課題および今後の展望について述べる。

2　ネットワーク管理

計算機ネットワークの発展に伴い、さまざまなシステムがネットワークに接続され、ネットワーク環境が複雑になっている。そしてネットワーク管理者にかかる管理作業の負担も増加している。

本章ではネットワーク管理者にとってネットワー

ク管理の負荷を増加させる要因について述べ、この問題を解決するためのネットワーク管理システムを提案する。

2.1 ネットワーク管理の問題点

ネットワーク管理者の負荷が増加した主な要因として以下の 2 つをあげる。

第 1 に、ネットワークにつながれるコンピュータが増加し、ネットワークを構成する機器や、そこで使われる管理ツールなどが多種多様になったということである。それらの操作法、設定法が機種ごとに違うために、管理者には豊富な知識と経験が必要とされる。特に、大学の研究室や学科などの組織では、ネットワーク管理は本業ではなく、システムに詳しい人が副業として行うことが多く、それらの人が副業として管理作業を行なうことが難しくなってきている。

第 2 には、ネットワーク管理の手段が少ないことである。現在のネットワーク管理機構のほとんどが、「ネットワーク管理をネットワーク経由」で行うことを前提としている。つまり、ほとんどの場合、コンソールからシステムの設定を行うことになる。ネットワークが正常に機能していて、管理者や管理プログラムが管理対象の計算機に到達できるときには設計どおりの能力を発揮するが、何らかの原因によりネットワークに障害が発生した場合、目的の計算機に到達できない状況に陥り、ネットワーク管理機構が機能しなくなる。例えば、多くの構成機器や管理ツールではネットワークを介して設定をするので、ネットワークが寸断された状況では、簡単な設定変更すらできない。

2.2 解決法

前節の問題点を解決し、管理者の負担を軽減するためには、次のような解決法が考えられる。

第 1 の問題点を解決するためには、管理作業などがある程度自動化されることが必要不可欠である。そのために必要なことは” システムをどのように運用していくか” という運用ポリシを明確にすることである。そのため運用ポリシの記述法を定める必要がある。

そして運用ポリシから具体的な管理作業への変換機構が必要である。これにより、機種間の設定法の違いなどを埋めることができる。管理者には異なる機器間における設定方法の違いが隠蔽されるため、設定方法の違いを意識しなくてよい。

第 2 の問題点を解決するためには、ネットワーク構成機器やネットワーク管理支援ツールの設定変更、設定内容の入手をコンソールからに限らず、さまざまなアクセス手段を用いて、行なえることが必要である。

3 システム構成

本章では、NIIS システムの設計と実装について述べる。NIIS システムは前章で述べた問題点を解決することを目的として設計、実装されたネットワーク管理システムである。

3.1 システムの概要

NIIS システムは、運用ポリシを与えることで、それに基づいてルータの設定を変更することができる。また、運用ポリシを記述するさまざまな手段を提供する。

NIIS システムは図 1 のようなクライアント-サーバモデルに基づいたシステムである。ネットワークに接続された複数の機器はサーバで一元的に管理される。管理作業を自動化するために、システムの運用ポリシの記述法があらかじめ決められている。管理者は運用ポリシ記述法に従い、NIIS クライアントからシステムの運用ポリシを記述し、それをサーバに渡す。運用ポリシに従ってサーバはさまざまな機器の設定を変更する。このため、ユーザからはシステムを構成するさまざまな機器や管理ツールの設定の詳細などが隠蔽される。

サーバ-クライアント間の通信は NIIS プロトコルに従う。このため、新たなクライアントの拡張は、NIIS プロトコルに従った仕様にすることで容易に行なえる。

3.2 NIIS サーバ

NIIS サーバ内では、NIIS クライアントから受け取った運用ポリシを設定ファイル作成部に送る (図

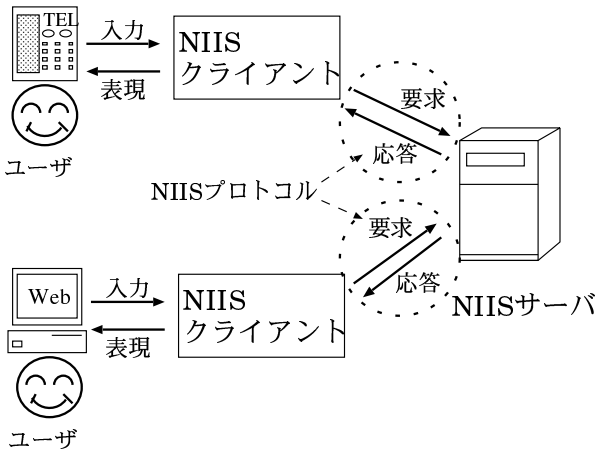

図 1: システム構成図

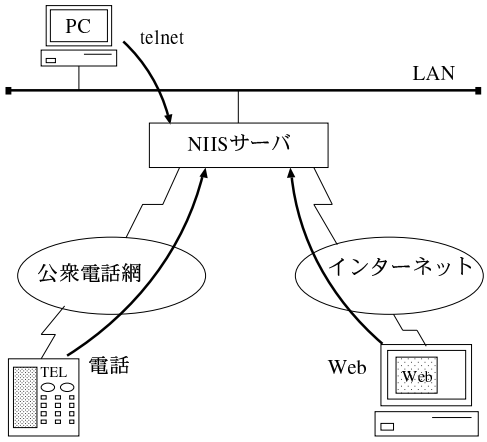

図 3: NIIS サーバへのアクセス手段

2)。設定ファイル作成部では、運用ポリシをもとにサーバの管理している機器や管理ツールの設定ファイルを生成する。設定ファイルは expect [4] というスクリプト言語の形式である。設定ファイルを実行することで、設定の変更や、管理情報の入手を行なう。expect を用いることで、対話的に行なってきた設定を自動的に処理することができる。

また、NIIS サーバでは、管理作業に関する管理者への報告、ログなどが自動的に行なわれる。

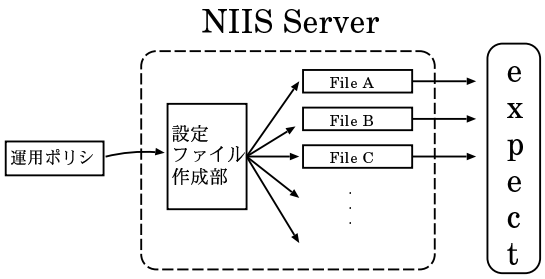

図 2: NIIS サーバ

3.3 NIIS クライアント

NIIS システムでは、アクセス手段ごとに NIIS クライアントが用意される。ここでは、WWW、電話、端末インターフェイスを用いた NIIS クライアントについて述べる。

3.3.1 WWW クライアント

CGI[1] を利用して、WWW クライアントの実装を行なった。フォームにデータを入力することにより、運用ポリシを記述し、サーバにデータを送る。

3.3.2 電話クライアント

遠隔地からアクセスするための手段として、電話を用いて運用ポリシを入力する NIIS クライアントを作成した。これを電話クライアントと呼ぶ。この電話クライアントを用いることで、ネットワークの外部から電話網を介して、NIIS サーバにアクセスできる。これにより、ネットワークが分断した状態でも利用可能な補助的な通信手段を確保することがでる。

電話クライアントではユーザからの入力は DTMF 信号[2] を用い、ユーザへの出力に音声を用いる。電話クライアントの内部では、ユーザからの DTMF 信号による入力を NIIS プロトコルに変換し、NIIS サーバへ送る。また NIIS サーバからの応答は音声に変換して、ユーザに送る。電話クライアントの実装には WIDE/PhoneShell [1] システムを利用した。

[1] Common Gateway Interface
[2] 公衆電話をかけるときに聞こえてくる音は DTMF(Dual Tone Multi Frequency) 信号といわれる。

3.3.3 端末クライアント

telnet を使用して、NIIS サーバを利用することができる。この場合、端末から直接 NIIS プロトコルを入力する。端末クライアントを使うことにより、NIIS サーバとの実際のやりとりを知ることができるので、NIIS クライアントを開発するときなどには参考になる。

この他にも、NIIS クライアントとして FAX やページャ、電子メールの利用などが考えられる。これら、さまざまなアクセス手段の利用により、管理作業の負担の軽減が期待できる。

4 NIIS システムを用いたルータの運用事例

この章では、NIIS システムが実際にどのようにルータを制御するかについて事例を述べる。ルータの重要な機能のひとつに、アクセス制御（以下パケットフィルタリング）がある。この章では、パケットフィルタリングの運用ポリシの記述法、NIIS システムの利用例について述べる。

4.1 フィルタ運用ポリシ

クライアントは、パケットフィルタリングの運用ポリシとして、以下の項目をサーバに渡す。NIIS システムではこれをフィルタ運用ポリシ (図 4) と呼ぶ。*の 6 項目は必ず記述する必要がある。

*	始点 IP アドレス
*	終点 IP アドレス
*	プロトコル
*	始点ポート番号
*	終点ポート番号
*	許可または拒否
	始点サブネットマスクアドレス
	終点サブネットマスクアドレス
	フィルタ設定に関する注釈

図 4: フィルタ運用ポリシ

クライアントからサーバに、このフィルタ運用ポリシが渡され、サーバで解析されて、システムに反映される。次に、各クライアントがどのようにフィルタ運用ポリシを記述するかを示す。

4.2 WWW クライアント

図 5 に WWW クライアントを示す。WWW のフォームにしたがって、運用ポリシを入力する。入力が終了した後、左下の”Submit Registration”と書かれたボタンを押すと、NIIS サーバにフィルタ運用ポリシが送られ、処理される。

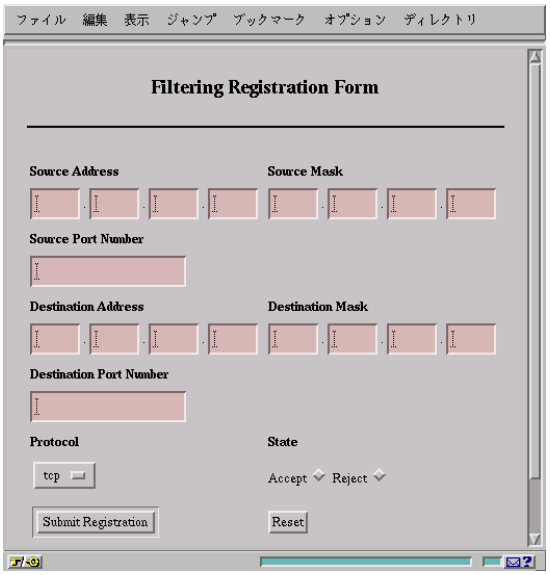

図 5: Web クライアント

4.3 電話クライアント

図 6 に電話クライアントを用いた時の、システムの動作を示す。

ユーザが、電話をかけると WIDE/PhoneShell が電話クライアントを起動する。電話クライアントは NIIS サーバに接続し、サービスが開始される。

電話クライアントからの音声ガイダンス指示に従って、ユーザが DTMF 信号を入力すると、WIDE/PhoneShell は DTMF 信号が入力されたことを電話クライアントに通知する。電話クライアントは入力された信号列を NIIS プロトコルに変換して NIIS サーバに送る。NIIS サーバは電話クライアントからの要求を処理し、電話クライアントに応答

する。電話クライアントは、NIIS サーバからの応答を音声に変換してユーザに送る。この繰り返しにより、ユーザは対話的にサービスを受け、フィルタ運用ポリシを記述して行く。

ユーザが電話を切ると、WIDE/PhoneShell は電話クライアントに対して、終了の指示をする。指示を受けた電話クライアントは、NIIS サーバとの接続を切断したのちに処理を終了する。

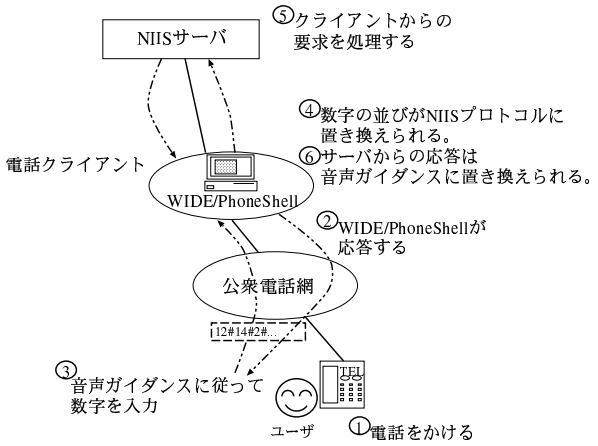

図 6: 電話クライアント概要図

5 考察

さまざまなアクセス手段により、運用ポリシを記述することができるため、以下のような利点が生まれる。

電話クライアントによる利点

- 電話は広く普及しているので、利用が容易である。
- 停電の影響を受けにくい。
- コンピュータ、PDA 等の特別な機材を必要としないのでこれらの機器を持ち歩かなくてもよい。
- 携帯電話があれば、外出先などからも管理作業ができる。仮に携帯電話がない場合でも高終電話を利用すればよい。

DTMF 信号と音声を用いて、運用ポリシを記述する電話クライアントは、扱える情報量が少ない。しかし、上で述べたような利点があるため、有用であるといえる。

WWW クライアントによる利点

- 視覚的に設定できるため、設定間違いが少なくなる。

端末クライアントによる利点

- 対話的に設定変更していくので、判りやすい。

ユーザはこれらのアクセス手段を状況に応じて選べるため、それぞれの NIIS クライアントが持つ利点を利用できる。

NIIS システム全体では以下のような利点が生まれた。

- 異なる種類のルータ間の設定方法の違いが隠蔽されるため、管理者は運用ポリシを記述するだけでよく、設定方法の違いを気にしなくてよい。
- 管理者への報告、ログなどが自動的に行なわれるため、システムの保守が容易になった。

NIIS サーバにルータ制御に関する新たな機能が追加された場合には、NIIS クライアントは NIIS プロトコルに従った実装を行なうことで、追加された機能を利用することができる。

6 今後の課題

今後、NIIS システムの実装、運用を行なう上で、次のような課題が考えられる。

NIIS クライアントの追加

今回は、電話クライアントと、端末クライアント、そして WWW クライアントを実装したが、今後さまざまなユーザインターフェイスに対応した NIIS クライアントを提供する必要がある。アクセス手段を多様化することにより、ネットワーク管理の手法

が増え、たとえネットワークが分断されていても最低限のネットワーク管理ができるようになる。

特に、すでにインフラストラクチャの整っているページャ、FAXなどを用いたNIISクライアントの開発を今後行い、システムの可用性を高める。

NIISシステムの運用

現段階は実験段階であり、管理者(ユーザ)の手間や単純な入力の間違いの数がどの程度減少するか、といった統計調査などは行なっていない。実際に運用を開始するには十分な実験を繰り返して定量的な評価を得る必要がある。

運用ポリシの抽象化

今後の展開を考えると、運用ポリシをあるレベルで抽象化することが重要である。しかし、あまり高いレベルで抽象化してもそれは管理者にとって理解しがたいものになるので、ある程度具体的な部分を残すことも必要であろう。適切なレベルの運用ポリシを記述するためには、管理のために必要な事項を体系化する必要がある。

RPSLの使用

現在の実装では、運用ポリシの記述法を独自に定めている。しかし、RPSL(Routing Policy Specification Language) [3]は、AS(Autonomous System)から個々のルータを制御するレベルまで、記述することができ拡張性も高いため、今後運用ポリシの記述法として、検討する必要がある。

7 まとめ

本論文では、電話やWWWなど、さまざまなアクセス手段を利用して、ネットワーク管理を支援するシステムを提案した。NIISシステムにより、種々の構成機器や管理ツールに関する設定方法を知らなくても、容易に運用を行うことができ、管理作業の軽減を実現することができた。

また、管理手法の幅が広がったことで、小人数の管理者によるシステム管理も、ある程度可能になったといえるだろう。とくに、電話など、ネットワークに依存しないアクセス手段は非常に有効であり、ユーザは、その時、その場所で最も都合の良いアクセス手段を利用し、その利点を受けることができる。

今後は、セキュリティの向上を含めた実装を行ない、システムの評価を行なっていく。また、このシステムの有用性を高めるために、ルータのアクセス制御以外に関するのさまざまなネットワーク管理支援サービスを用意し、より抽象度の高い運用ポリシでの運用ができるようにしていく。また、今後さまざまなNIISクライアントの開発などを行なう予定である。

参考文献

[1] Hiroyuki Ohno. Improved Network Management useing WIDE/PhoneShell. In *Proc. INET93*. Internet Society,August 1993.

[2] 大野浩之,“システム管理者が離散した状況下におけるシステム管理手法 “, 情報処理学会研究報告 97-DSM-6, Vol.97, No45,pp.13-18,1997.

[3] C.alaettinoglu, T.Bates, E.Gerich, D.karrenberg, D.meyer, M.Terpstra, and C.Villamizar. “Routing Policy Specificarion Language (RPSL)”. Technical report, Request for Comments 2280, January 1998.

[4] Don Libes. Exploring Expect: A Tcl-Based Toolkit for Automating Interactive Programs. O’Reilly & Associates,Inc, January 1995. ISBN1-56592-090-2.