# ロギングに基づくネットワークサービス管理

2K－3

藤崎 智宏　犬束 敏信　浜田 雅樹

NTT ソフトウェア研究所 広域コンピューティング研究部

## 1　はじめに

ここ数年のコンピュータネットワークの発展には目覚ましいものがあり，数多くの組織，多くのネットワークの相互接続が全世界的に行われている．利用の形態も変化しており，従来の電子メールや電子ニュースといったアプリケーションに加え，遠隔教育，電子商取引などの高度なアプリケーションが増加しており，コンピュータネットワークの重要性は増大の一途である．このような状況で，コンピュータネットワークを運用する側にはこれまで以上に安定したネットワークの管理・運用が求められているが，現状ではネットワークの運用は一部のエキスパートといった人的資源に負うところが非常に大きい．インタネットを例に取って見ても，組織におけるネットワークの運用・管理を円滑に行うにはかなりのスキルを有した担当者が必要であり，トラブルへの対応などは担当者の経験に頼る場面が多い．しかしながら，従来のネットワーク機器の監視のみでなく，電子メール，ネットニュース，WWW システムといったネットワークサービス管理の必要性の増大により，少数のエキスパートがネットワーク全体を管理することは困難になってきている．

本稿では，ネットワーク管理の一環としてネットワークサービスを管理を，サービスプログラムが出力する各種のロギング情報を元に行うフレームワークについて提案する．ロギング情報を適切に利用することにより，ネットワークサービスの日常監視，障害の発見・対策立案を容易に行うことが可能である．

## 2　ネットワークサービス

### 2.1　ネットワークサービスの定義

本稿ではネットワークサービスを，「ネットワーク中のホスト上で動作するサービス提供プログラム（サーバプログラム）が連携し，ユーザに提供されるサービス」と定義する．ネットワークサービスの例としては，電子メールシステム，ネットニュースシステム，WWW システム，ネットワークプリンタシステムなどが挙げられる．

### 2.2　ネットワークサービスの動作

ネットワークサービスを構成するプログラムは，主に UNIX や Windows NT といった OS 上で実行されている．これらのプログラムは，図1で示すような構造を持つものがほとんどである．

例えば，UNIX で広く使われている電子メール配送プログラムである sendmail は，sendmail.cf その他の設定ファイルを読み込み動作し，動作中にロギング情報（サービス履歴やエラーなどの記録）を出力する．

出力されたロギング情報は，一般ホスト上の特定のファイルに追記される．

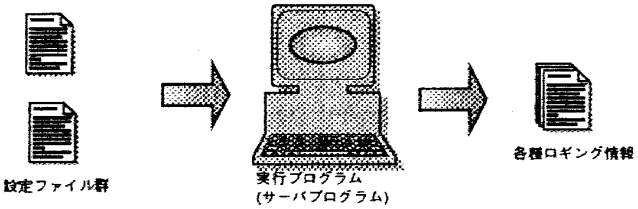


図 1: ネットワークサービスプログラムの動作

### 2.3　ネットワークサービスの管理

ネットワークサービスの維持管理には，従来のネットワーク型でないサービス（特定のホスト内に閉じたサービス）と同等の

1. サービス設定ファイル
2. 実行されるサービスプログラム
3. サービスプログラムが動作中に使用する資源

といった管理に加え，サービスを構成する他のプログラムとの関連を管理しなければならない．さらに，ネットワークサービスによっては他のネットワークサービスとの関連を管理する必要がある．

例えば，ネットニュースシステムの管理では，

1. ユーザアクセス制御，古い記事削除の制御，ニュースグループの種類設定といった単一ホスト上でのネットニュースシステムの動作を設定するファイル群の管理
2. ユーザに購読サービスを提供するプログラム，古い記事を削除するプログラムの正常動作の管理
3. 記事を貯めておくディスクの容量管理

などが必要であり，更に他のホスト上で動作するネットニュースプログラムとの配送関連の管理が必要である．

また，電子メールシステムにおいては，インタネットでの名前サービスシステムである DNS サービスシステムと深い関連を持っている場合が多いため，DNS サービスシステムの設定，動作状況も管理する必要がある．

以上述べた管理は，OSI の管理体系における構成管理と障害に属するものである．この他，性能管理，課金管理，セキュリティ管理なども状況に応じて必要となる．

## 3　ロギングに基づいたサービス管理フレームワーク

ネットワークサービスの日常監視，障害の検知・復旧には，ロギング情報が用いられることが多い．しかしながら，その手法は管理者ごとにまちまちであり，複数の

---

Network service management using the logged information.

Tomohiro FUJISAKI(fujisaki@slab.ntt.co.jp),
Toshinobu INUZUKA(inuzuka@slab.ntt.co.jp),
Masaki HAMADA(hamada@slab.ntt.co.jp),
NTT Software Laboratories.

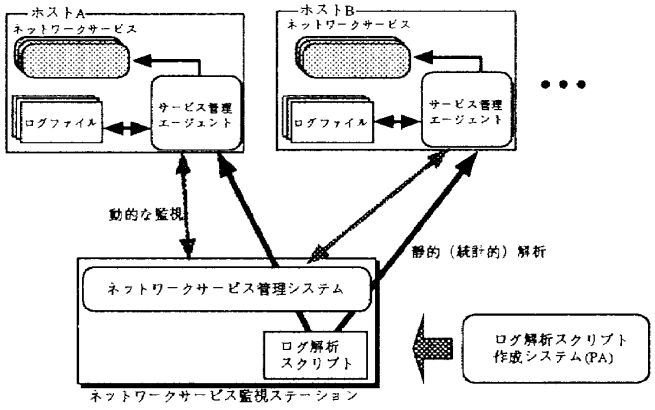


図 2: ネットワークサービス監視システムの概略

ホストに分散して動作するネットワークサービスを管理することは難しい.

本節では，分散環境においてネットワークサービスを効率よく監視するためのロギング情報に基づいた管理フレームワークを提案する.

## 3.1 ログ情報

ロギングされる情報はネットワークサービスごとに違うが，前節で述べたOSI管理項目に関連する内容を含んでいることが多い.

OSI管理項目とロギング情報の対応を以下に示す.

- 構成管理
  設定ファイルの有無，記述ミスなど
- 障害管理
  動作中に生じた障害，資源の不足など
- セキュリティ管理
  サービス利用者情報，アクセス違反など
- 課金管理
  ユーザごとのサービス利用状況，ネットワークサービスの提供履歴など
- 性能管理利用頻度，サービス時間など

更に，ロギング情報は，動的に利用する場合 (障害の発見，現在の利用者の特定を行う場合など)，静的に利用する場合 (日報を作成する場合や，月極で課金を行う場合など) がある.

ロギング情報の解析を目的に応じて行うことにより，ネットワークサービスの包括的な管理が可能である.

## 3.2 管理フレームワーク

ロギング情報を基にネットワークサービスの管理を行うには，ネットワーク中に分散したロギング情報を統括的に監視する必要がある. 図2に，ログ監視システムの概略を示す.

各ホスト上には，サービス管理エージェントを配置する. このエージェントは動的・静的管理を行う.

- 動的管理
  - ネットワークサービスを監視し，異常を管理システムに通知する.
  - ネットワークサービス監視システムから動的指示スクリプトを受け取り，実行する.
- 静的管理
  - ログファイル解析スクリプトをネットワークサービス管理システムから受け取り，実行し，実行結果を返却する.
  - 指定された日時に，指定されたスクリプトを動作させ，結果を管理システムに送る.

## 3.3 検討事項

上記システムを実現する際に検討しなければならないことについて述べる.

- ネットワークサービスの障害の検出
  管理者は，ネットワークサービスに障害が起った場合，その原因特定，対処のためにログデータを必要とする. それ以外の場合には，静的な統計解析のためにログデータを使用することが多い. ネットワークサービスの障害を検知し，障害が起こった時刻付近のログデータを管理者に提供することが出来れば，サービスの効率的な管理につながる.
- ログデータの効率的な収集方法
  ネットワーク上に分散したログデータをサービス管理システムに効率的に集める方法を検討する必要がある. すべてのログデータを集めると，収集のためのトラフィック，収集したデータの解析・保存が問題となる. このため，必要なデータを効率的に収集する方法が必要となる.
- セキュリティ
  ネットワーク管理を行うために，管理対象ホストにエージェントを配置するが，このエージェントは遠隔からの制御を可能とするため，セキュリティに配慮する必要がある.
- ログ解析スクリプト作成支援システムの構築
  静的，動的双方のログ解析を容易に行うために解析スクリプトの生成の支援をするシステムを検討している. 従来，Prefernce Analyzer(PA) によって静的なログ集計を容易に行うことを可能にしている. PA はデータフローダイアグラムを用いた視覚的プログラミング環境で，プログラム経験のない管理者が複雑なログ解析を行うことを可能にしている. これを動的監視にも使用できるように検討中である.

## 4 まとめ

本稿では，ロギング情報に基づいてネットワークサービスを管理するためのフレームワークについて提案した. ロギング情報を有効に利用することで，ネットワークサービス管理を効率的に行うことが可能となる. 今後は，個々の要素技術の検討を行い，フレームワークを実装する. 更に，ロギング情報以外の監視手法も取り込んでいく.

## 参考文献

[篠原 96] 篠原 他,“サービス管理に着目したネットワーク管理モデル”, 情報処理学会研究報告 96-DSM-3 pp7-12, 1996 年 9 月.

[犬束 97] 犬束 他, “利用者履歴解析支援システム Preference Analyser の実装及び評価”, 情報処理学会第 54 回全国大会論文集 (3), pp 313-134, 1997.