WIDE バックボーンにおける
ネットワーク監視システムの構築

関谷　勇司 (sekiya@wide.ad.jp)

1.　ネットワークの障害と監視

WIDE 内におけるネットワークバックボーンは拡大しており、それにともなって拠点となる NOC やルータの数も増加している。また、IPv4 と IPv6 のマルチプロトコルにて定常的に運用される拠点や回線が増えたため、経路障害などの場合、どちらのプロトコルにて発生しているのかを判別する必要がある。

ネットワークの障害には、大きく分けて以下のものが考えられる

- ソフトウェアのバグ等による Layer 3 経路障害
- ソフトウェアのバグ等による Layer 2 経路障害
- 回線障害
- 機器障害
- トラフィック増加による回線もしくは CPU の飽和
- 人為的な設定ミス

上記の障害のうち、人為的な設定ミス以外は突発的に発生する可能性のある障害である。従って、常時監視を行っていない限り、発生を即時に検知することは難しく、検知して修復を行うまでに多くの時間を費やしてしまう場合が多い。そこで、WIDE バックボーンにおいて、ネットワークの常時監視を行うためのシステムを構築した。

2.　監視システムの概要

本システムは、リモートから定常的にネットワークの状態を監視し、異常を検知した場合に報告するためのシステムである。本 draft では、このシステムの概要について述べる。WIDE バックボーン監視システムに求められる要求として、以下の点があげられる。

- ルータもしくはホストまで、ネットワーク到達性があるか判定する
- ルータもしくはホストが ping に応答するか判定する

- ホストにて行われているサービスが正常に応答するか判定する
- ルータもしくはホストからの SNMP trap を受け、異常を検知する
- 異常を検知した場合、何らかの手段にて適切な管理者に通知する
- 異常が回復した場合、何らかの手段にて適切な管理者に通知する
- 複数の地点から監視する

以上の要求を実現するため、nagios と呼ばれるオープンソースソフトウェアを利用してシステムを構築した。nagios はサーバとして UNIX 上にて動作する監視ツールであり、ping による到達性のみならず、様々なサービスの監視を行うことが可能である。また、監視のためのプラグインを、C 言語や Perl を用いて簡単に作成することができるため、監視するサービスを容易にカスタマイズすることが可能となる。nagios は http://www.nagios.org/ から取得することが可能である。2004 年 2 月現在、最新版はバージョン 1.2 であり、本システムも nagios 1.2 を用いて監視を行っている。

異常を検知した場合には、電子メールにて障害箇所の通知を行う。また、障害から回復した場合にも、電子メールにて通知を行う。障害通知メールの例を図 1 に示す。

```
***** Nagios  *****

Notification Type: PROBLEM
Host: nspixp.sfc.wide.ad.jp
State: DOWN
Address: 203.178.142.154
Info: CRITICAL - Plugin timed out after 10 seconds

Date/Time: Fri Jan 30 08:42:55 JST 2004
```

図 1 : 障害通知メールの例

本例は、DIX-IE(NSPIXP) の情報を載せている Web サーバに到達性異常が発

生し、それを検知した際のメールである。

3. 監視ネットワークの概要

本システムを運用するにあたって、図 2 に示すトポロジにおいて監視を行った。2004 年 2 月現在、監視対象となっているルータもしくはホストは、図 2 に示されているものである。また、監視は WIDE バックボーンと接続している組織である、東京大学内にあるホストから監視を行った。これは、WIDE バックボーンに異常が合った場合の通知が電子メールにて行われるため、電子メールの到達性が WIDE バックボーンに依存しない場所から監視を行う方が都合が良いからである。従って、異常検知の電子メール送信先も、WIDE バックボーン内にあるメールサーバ以外のメールサーバが望ましい。現在は、ほとんどの障害に対して、携帯電話のメールアドレスに対して通知を行っている。

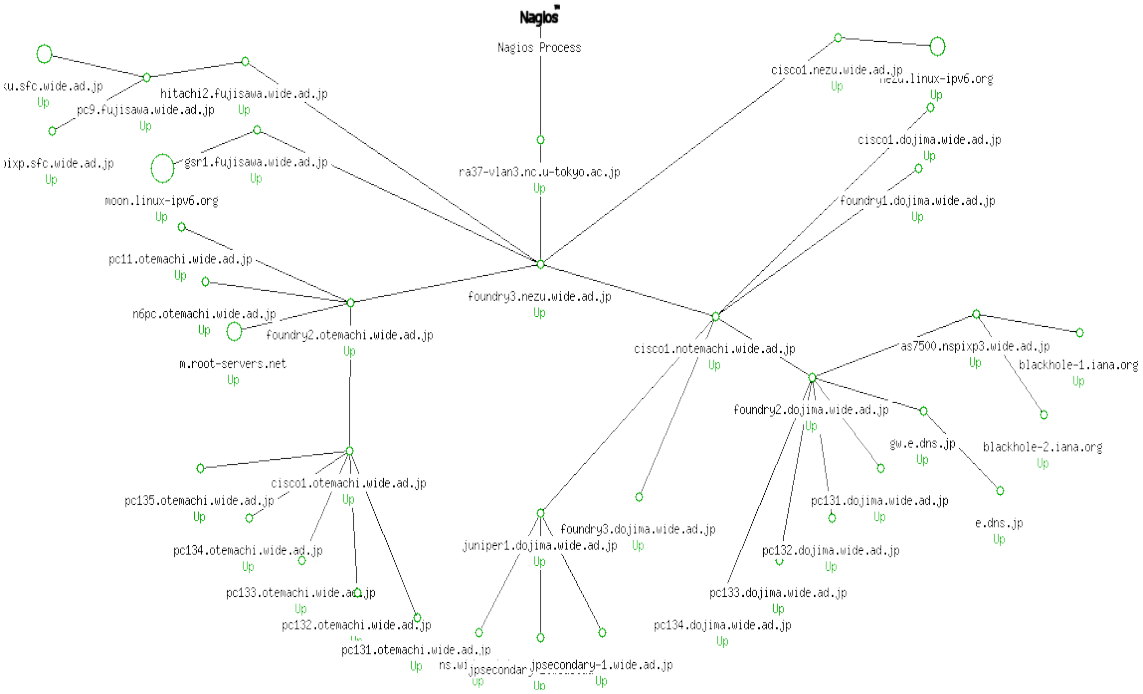

図 2 : 監視ネットワークトポロジ

4. 監視状況

本監視システムによる、監視状況例を図 3 に示す。各ルータやホストのサービスに対する、監視状況の一覧を表示することができる。また、各ルータやホスト

のサービスに対する、障害履歴を表示することも可能である。

図 3 : 監視サービス状態一覧

5. 監視記録

本システムは、1 日単位で監視記録を保存しており、過去の記録を表示させることが可能である。図 4 に、2004 年 2 月 3 日の監視記録を示す。本監視記録では、cisco1.notemachi.wide.ad.jp と foundry1.dojima.wide.ad.jp を結ぶ回線に障害が発生し、一時的に jpsecondary-1.wide.ad.jp の DNS サービスへの到達性が失われたことを示している。

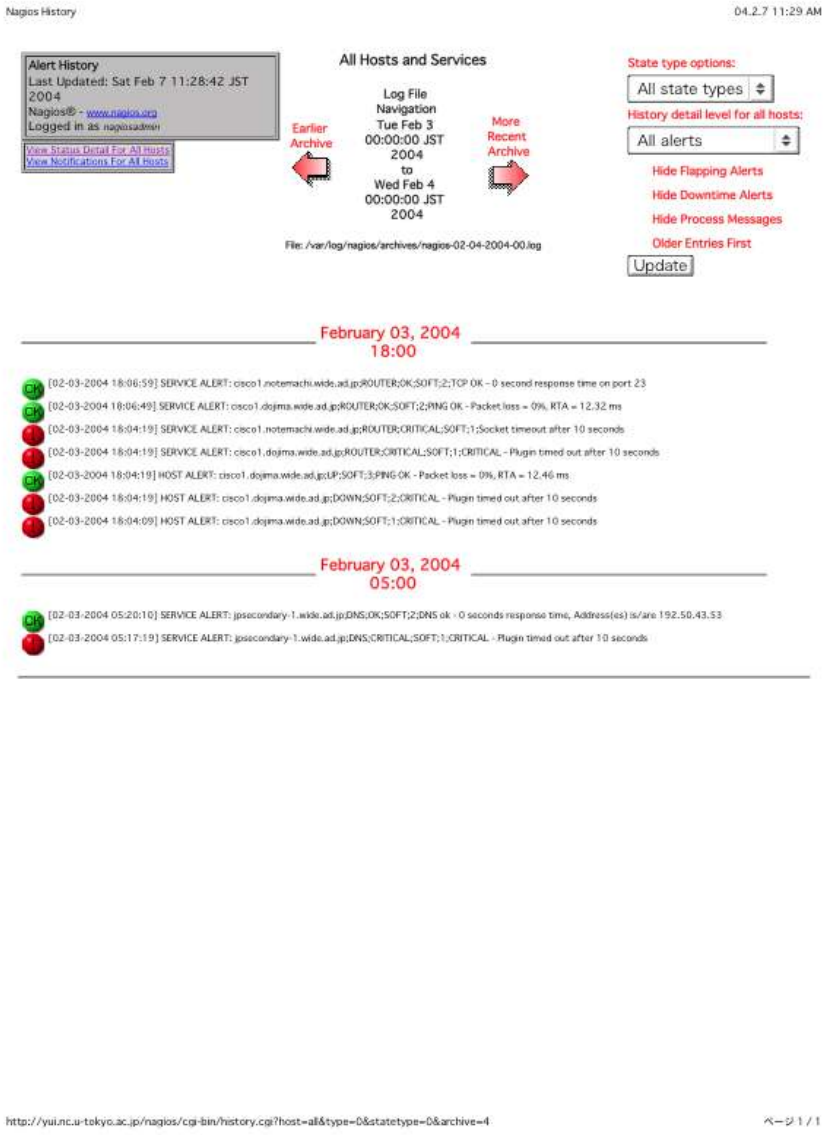

図 4 : 監視結果例

6. これからの課題

本監視システムによって、以下の要求は達成することができた。

- ルータもしくはホストまで、ネットワーク到達性があるか判定する
- ルータもしくはホストが ping に応答するか判定する
- ホストにて行われているサービスが正常に応答するか判定する
- 異常を検知した場合、何らかの手段にて適切な管理者に通知する
- 異常が回復した場合、何らかの手段にて適切な管理者に通知する

しかし、以下の要求はまだ達成されていない。

- ルータもしくはホストからの SNMP trap を受け、異常を検知する
- 複数の地点から監視する

SNMP trap に関しては、各ルータやホストにて SNMP trap に関する設定を追加し、nagios 実行ホストに対して SNMP trap メッセージを送信するよう設定することで、nagios にて一元管理する方法が存在する。今後各ルータやホストに設定を加え、インタフェースや経路制御デーモンの障害を瞬時に関知することも可能となる。

また、複数の地点からの分散監視は、nagios 用の分散監視クライアントが配布されている。これは、分散監視クライアントを立ち上げたホストからの、到達性やサービスの監視状況を、中央の nagios 監視ホストに送信し、集中監視を可能とする者である。これを WIDE バックボーン内の数カ所のホストにて設定することにより、複数地点からの監視結果を一カ所にて閲覧することが可能となる。現在、東京大学からの監視しか行っていないので、今後の課題として、関西方面、LosAngeles 方面等からの監視を加えたいと考えている。