2R-01 ネットワーク情報ウェアハウスシステムの構築とその応用

齋藤 武夫, Ahmed Ashir, Glenn Mansfield, 白鳥 則郎
東北大学電気通信研究所/大学院情報科学研究科

1 はじめに

アプリケーションの効率的な運用・管理のためには，高度なネットワーク情報が要求される．たとえば，(1) ノード間のトラフィックフロー情報，(2) ネットワーク構成情報，(3) 輻輳情報，(4) 資源予約情報，(5) アプリケーションのスケジュール予約情報，(6) これらネットワーク情報の履歴，などの情報が得られれば，(2) をもとに (1),(3) の分析をうことにより，アプリケーションの利用する通信路の通信品質情報を得ることが可能であり，また，(2), (4), (5) をもとに，(1), (3) 等の履歴情報を含めて分析を行うことにより，ネットワーク資源の利用状況を予測することが可能となる [1][2]. そこで我々は，この様なネットワーク情報をもとにより高度なネットワーク情報をアプリケーションに提供する，アプリケーション運用支援システム (APOS) を提案している．(図 1)[3].

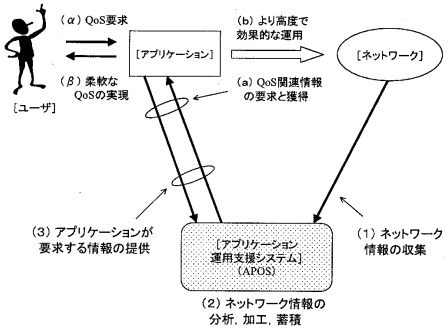

図 1: アプリケーション運用支援システム (APOS)

本稿では，このモデルに基づき，インターネットにおける高度なネットワーク情報の提供を目的とした，ネットワーク情報ウェアハウス (NIWH) の構築と応用について述べる．

2 ネットワーク情報ウェアハウス

高度なネットワーク情報を生成するためには，ネットワーク情報の収集と分析が必要となる．図 2 に示す様なインターネット環境において，通信アプリケーションに関わる高度なネットワーク情報を得るためには，サブネットワーク N1, N7 間の経路の特定と，その経路上におけるネットワーク情報の分析を行なう必要がある．

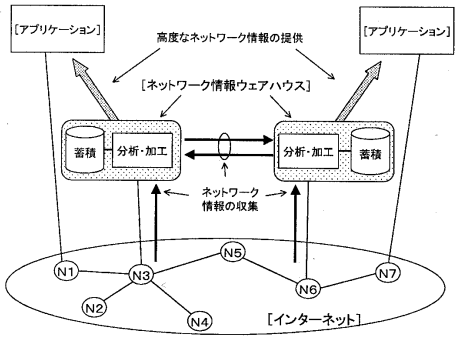

図 2: ネットワーク情報ウェアハウス

NIWH はインターネット上に分散した形で運用され，SNMP ポーリング等のアクティブ型とトラフィックモニタリングを基本としたパッシブ型のネットワーク情報収集機能を持つ．また，情報の分析，加工機能をもち，さらに，収集された情報や生成された高度な情報を蓄積，利用する機能を持つ．収集された情報が蓄積される際には，収集された時刻が付加される．

アプリケーションや NIWH が，ある NIWH に対してネットワーク情報の収集や高度なネットワーク情報の生成を要求するためには，Network Information Configuration and Query Language (NICQL) を用いてその要求を記述する．NICQL は手続き型の言語で，以下に挙げる機能を持つ．

(1) フィルタ機能

(2) テーブル操作機能

(3) データベース操作機能

(4) ネットワーク情報収集制御機能

  (a) パッシブ型: トラフィック・プローブの制御

  (b) アクティブ型: SNMP, ping, traceroute 等

(1) の記述は SRL(the Simple Ruleset Language)[4] を基本としており，これにデータ構造としてのテーブ

Design of a Network Information WareHouse System and its Applications
Takeo SAITOH, Ahmed ASHIR, Glenn MANSFIELD, and Norio SHIRATORI
Research of Institute of Electrical Communication/
Graduate School of Information Siences, Tohoku University

ルと制御構造の拡張，情報の蓄積と再利用のためのデータベース操作機能，トラフィック・プローブポートの制御，SNMP を用いた通信機能の付加を行なっている．

3 プライバシ情報の保護

ネットワーク情報の収集に際して，トラフィックデータ (パケット) 等を収集し分析する場合，IP アドレスやユーザデータ等のプライバシ情報の保護について十分考慮しなければならない．また，NIWH により分析提供される高度なネットワーク情報にも，人や組織のアクティビティなどプライバシに関わる情報が含まれる可能性もある．

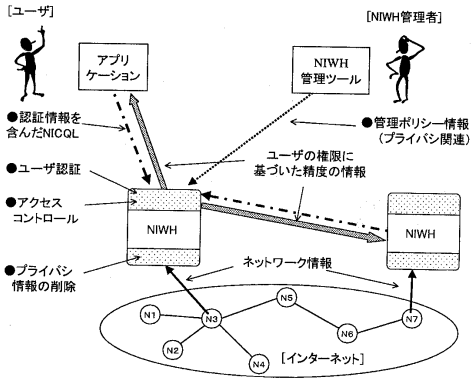

図 3: プライバシ情報保護のためのフレームワーク

ネットワーク情報の収集や提供に関わるプライバシ保護のポリシーは NIWH が運用される組織により異なるため，以下に挙げる機能を NIWH に持たせることにより，ポリシーを実現するためのプライバシ・フレームワークを実現する (図 3).

(1) 収集，蓄積時におけるプライバシ情報のフィルタ

(2) プライバシレベルに対応したネットワーク情報のカテゴライズ

(3) ユーザの権限レベル

(4) (1),(2) のマッピング

NIWH の管理者は，組織のポリシーを基に情報収集機能における (1) の設定を行なう．また，管理者は，ネットワーク情報毎に (2),(3) を定義し，(4) を設定することで，情報提供に際したプライバシ保護ポリシーの反映を行なう．(2) の例として IP アドレスを取り上げてみると，(i)IP アドレス (無制限)，(ii) ネットワークアドレス部のみ，(iii)IP アドレスが属する AS 番号，(iv)IP アドレスのスクランブル，(v) 情報無し，などのレベル分けが出来る．

この様なプライバシ・フレームワークを提供することで，NIWH は，サイトのポリシーに応じて収集・蓄積情報のフィルタリングを行なったり，ユーザの権限に応じて蓄積された情報のアクセス制限や提供する情報の精度の制御を行なうことで，プライバシ情報の保護を行なう．

4 現状と今後

現在 SNMPv3 フレームワークを基にして NIWH の実装を進めており，複数の NIWH による TCP retransmission 情報を基にした輻輳部分の特定 [2] や，RTP トラフィックのパケット内情報を基にしたジッタ情報の生成 [5] を試みながら，NICQL の設計の詳細化と実装評価を進めている．

プライバシ・フレームワークに関しては，現在はパケットのユーザデータの削除と IP ヘッダのスクランブルのみを実装しているに留まっている．様々なネットワーク情報に対するカテゴライズと，組織のポリシーに関する検討は今後の課題である．

参考文献

[1] Ahmed Ashir, Glenn Mansfield, Norio Shiratori, "Estimation of Network Characteristics and Its Use in Improving Performance of Network Applications," IEICE Transactions, Vol.E82-D No.4, pp.747-pp.755, 1999.

[2] Takeo Saitoh, Glenn Mansfield, Norio Shiratori, "Network Congestion Monitoring and detection using the IMI infrastructure," Proceedings of the 1999 International Conference on Parallel Processing, pp.462-pp.469, 1999.

[3] 齋藤 武夫, Glenn Mansfield, 木下 哲男, 白鳥 則郎, "分散環境におけるアプリケーション運用支援システム," 情処研報 DPS-94-27, pp.149-pp.154, 1999.

[4] N. Brownlee, "SRL: A Language for Describing Traffic Flows and Specifying Actions for Flow Groups," RFC2723, Oct.1999.

[5] 六藤 雄一, 齋藤 武夫, Glenn Mansfield, 白鳥 則郎, "RTP トラヒックの分析によるネットワーク通信品質の解析方法," 信学技報 IN99-46, pp.27-pp.32, 1999.