# アプリケーションに対するネットワーク情報提供手法の考察

3U－1

金子　正和　齋藤　武夫　Glenn Mansfield　木下　哲男　白鳥　則郎
東北大学電気通信研究所/情報科学研究科

## 1.はじめに

インターネットの普及とその利用者層の拡大に伴い、ネットワーク上で運用されるアプリケーションは多様化の一途をたどっている。

しかし、現在のインターネット環境ではネットワークの通信品質を保証することが困難であるため、あるアプリケーションがなんらかのサービス品質(QoS)を満たさなければいけない場合、自らネットワークの情報を収集し、状況を予測しながら動的にQoSの制御を行う必要がある。

我々は、この様なアプリケーションを支援するためにネットワーク情報を収集提供するシステム(APOS)の構築を試みている[1]。

APOSが収集するネットワーク情報には個人や組織に関するプライバシー情報が含まれる可能性がある。そこで本稿では、プライバシーの保護を図りながらより精度の高い情報を提供する手法の考察を行い、そのモデルを提案する。

## 2.アプリケーション運用支援システム(APOS)

アプリケーションの効率的な運用・管理のためには、以下に例を挙げるようなネットワーク情報の収集と分析が必要である。

(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)　これらネットワーク情報の履歴

そこでAPOSは図1に示すように、ネットワーク情報の収集・分析・蓄積・加工を行ない、アプリケーションの要求に基づき高度な情報を提供する機能を持つ。

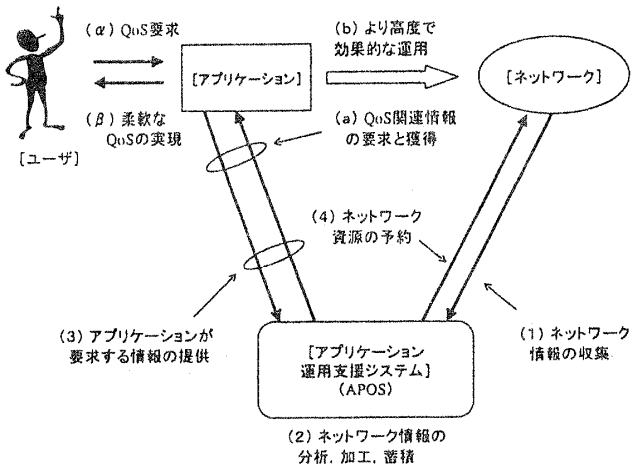


図1　APOSのシステムモデル

## 3.プライバシーに関する情報

ネットワーク上のトラフィックには、パスワードやクレジットカード番号など、セキュリティやプライバシーに関わる情報が含まれている。また、APOS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ーに関わる情報が含まれる可能性がある(図2)。情報提供時には通信者のプライバシー保護について考慮する必要がある。

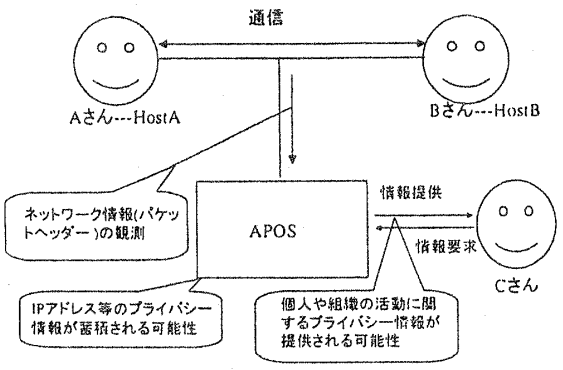


図2　プライバシー情報の存在

我々はこれらプライバシーに関する情報を保護するために、データウェアハウスの概念を導入する。機密性の高いデータをあらかじめ生のデータから削除し、残りのデータをデータウェ

---

A method to provide Network Information to the Applications
Masakazu Kaneko, Takeo Saito, Glenn Mansfield, Tetsuo Kinoshita and Norio Shiratori
Research Institute of Electrical Communication / Graduate School of Information Sciences, Tohoku University

アハウスのシェルで囲むことによって、データに対して多様なレベルでのアクセスを実現するアクセス制御を行う。図 3 にそのフレームワークを示す。

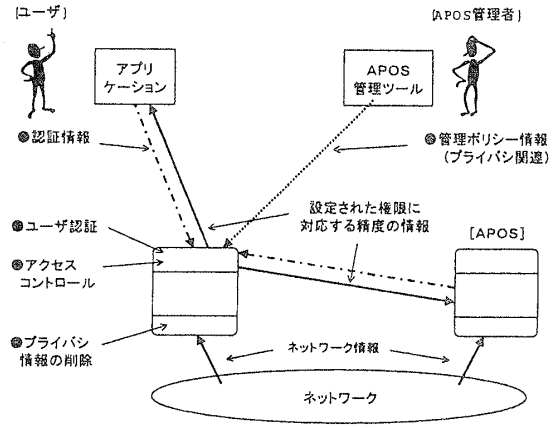


図 3　プライバシー保護のためのアクセス制御

## 4.プライバシーを考慮した情報提供手法

アプリケーションに提供される情報は以下の概念式により定義される。

[アプリケーションに提供する情報]
≡F(アプリケーションから要求された情報，
　P(ユーザー情報))

関数 P はユーザ、プライバシー情報、アクセス特権レベルに関するリスト(APOS 管理者が設定したアクセスポリシー(表 1))を保持し、与えられたユーザ情報から、個々のプライバシー情報に関するアクセス特権レベルのリストを作成する。

関数 F はそのリストと、一度加工生成された、アプリケーションの要求に沿った情報から、P(アクセスポリシー)を考慮した実際にアプリケーションに提供する情報を生成する。

表 1　情報アクセス特権レベルリストの例

プライバシー情報

| ユーザー | IP アドレス | Port 番号 | ------- |
|---|---|---|---|
| ユーザー A | L(IPadd)4 | L(Po)4 | --- |
| ユーザー B | L(IPadd)2 | L(Po)3 | --- |
| ------- | --- | --- | --- |
| APOS の管理者 | L(IPadd)5 | L(Po)4 | --- |
| ------- | --- | --- | --- |
| AS1 の管理者 | L(IPadd)3 | L(Po)3 | --- |
| 一般ユーザー | L(IPadd)1 | L(Po)2 | --- |

※L(k)n ---- k に関する情報アクセス特権レベルのレベル値 n

APOS を利用するアプリケーションの情報アクセス特権レベル(Information Access Privilege Level (=IAPL))は、APOS の管理者によって、その運用ポリシーに合わせて表 1 に示すようにユーザ毎(APOS 管理者、APOS が運用されているネットワークの管理者、他の APOS の管理者、一般の利用者 etc.)に、そして提供する情報毎(IP アドレス、ポート番号 etc.)に設定される。

図 4 に、IP アドレス情報の提供の場合の、管理ポリシーに基づく、プライバシーに関わる情報の情報アクセス特権レベルの設定例を示す。IAPL が L1 から L5 に上がるに連れて、アプリケーションに提供される IP アドレスに関する情報の精度は増大していくことを示している。

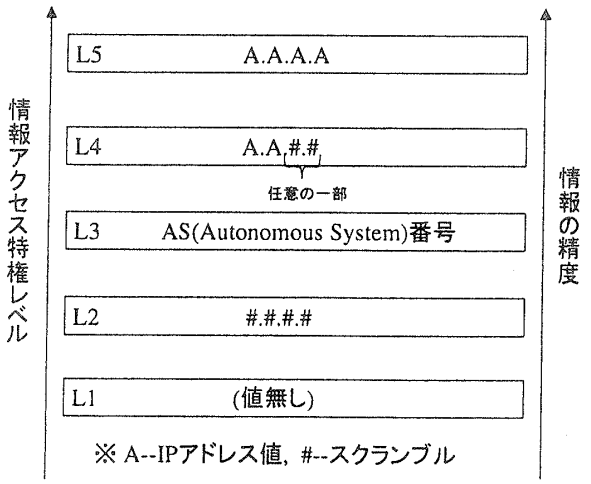


図4　IPアドレスに対する情報アクセス特権レベルの例

## 5.まとめ

本稿では、アプリケーション運用支援システムにおけるプライバシーを考慮したアクセス特権レベルと、それに基づく情報提供の枠組みの提案を行なった。現在は、このフレームを実現するための、ネットワーク情報データウェアハウジングクエリー言語(NDWQL) の設計を行っている。

## 参考文献

[1]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, pp.149-154, 1999