人に関連するリソースに適したアクセス制御機構の提案†

3M－6

菅野博靖，大谷浩司，光岡円，神田陽治
(株)富士通研究所

1. はじめに

電子メール等の通信サービスはインターネットの黎明期からその発展を支える主要な軸であった．情報蓄積提供型アプリケーションが発展した現在においても，その重要性はさらに高まっている．例えば，ICQ[1]をはじめとしたバディリストは，親しい人々の簡易なアウェアネスを提供し，ネットワークを通した「つながり」を意識させることによって，急速に普及した．しかし一方で，現在の我々はネットワークコミュニケーションやプライバシーに関わる新たな課題に直面することになる．

この論文では，ネットワークを介した対人コミュニケーションにおけるアクセス制御やプライバシー情報の公開制御について考察し，人に関連するリソースへのインタラクションを制御する新たなアクセス制御機構を提案する．

2. オンラインインタラクションにおけるアクセス制御

ネットワークを介したコミュニケーション要求を相手の端末やエージェントに送る，あるいは相手のアウェアネス情報の取得を要求する，これらの場合，受け手から見たアクセス・公開制御はどうあるべきか．我々はこの問題を「オンラインインタラクションのためのアクセス制御」の問題と定義し，統一的な解決策を与えることを検討する．

2.1. オンラインインタラクションの課題

オンラインインタラクションとは，(a) ネットワークを介したインタラクティブなアクセスを伴なうものであり，(b) 基本的に双方の背後に人間がいることを前提とする，ものと考える．典型的な例としてバディリスト／インスタントメッセージやインターネット電話が挙げられるが，WWW などを通して個人情報を公開・提供する場合も含まれる．これらをアクセス制御の観点から見ると，以下のような課題が現れてくる．

(1) アクセス要求者の信頼性
仮にディジタル ID のようなもので要求者の身元が明らかにされたとしても，アクセス対象者の視点から信頼できるかどうかは不明である．

(2) プライバシー
各要求者に対して公開したい情報は異なるはずである．また何を公開したいかも動的に変化しうる．

(3) アクセス対象者の状態や都合
特にコミュニケーション要求などは，アクセス対象者の都合によって処理を変えたい場合がある．

しかし現状のアクセス制御への取り組みを見ると，先の例で示したアプリケーションにおいても各々固有の ACL (Access Control List)が利用されているのみで，先の課題が直接検討されているわけではない．ACL は従来 OS レベルのリソース管理やディレクトリサービス等で利用されてきた基本的なアクセス制御機構で，柔軟性等の問題がある．ACL の弱点を克服するためにセキュリティ関連分野ではいくつかの試みがなされているものの（たとえば[2]），オンラインインタラクションにおける先述の課題を解決するために我々は新たな視点を必要とする．

2.2. WWW ベースのトラスト管理の枠組み

WWW を基盤としたネットワーク社会におけるインタラクティブな情報取得の枠組みに信頼性の観点から注目すべき２つの試みがある．これらはコンテンツ選択とプライバシーの分野で以下のような成果を示しつつある．

(1) REFEREE [3]　W3C で検討されている WWW のためのトラスト管理機構であり，コンテンツ選択の枠組みである PICS[4]等での利用が想定されている．PICS が提供するのは，コンテンツに対する評価ラベル，コンテンツ提供者，評価者等のメタデータからコンテンツを受け入れるかどうか判断する枠組みであり，同時にインターネットにおける信頼性の枠組みである．判断のためのポリシー設定言語として

---

† A New Access Control Mechanism for Online Interaction
Hiroyasu Sugano, Koji Otani, Madoka Mitsuoka, Youji Kohda
Fujitsu Laboratories Ltd.
64, Nishiwaki, Ohkubo-cho, Akashi 674-8555, Japan

Profiles-0.92 や PICSRules が検討されている.

(2) P3P のプライバシー管理機構

P3P (Platform for Privacy Preference Project) は Web ベースのサービス利用時に，利用者の個人情報を取得することを求めるサービス提供者と利用者の間のネゴシエーションプロトコルを規定する W3C の活動である．取得した情報の利用種別宣言や同意に基づく情報提供などに特徴を持つ.

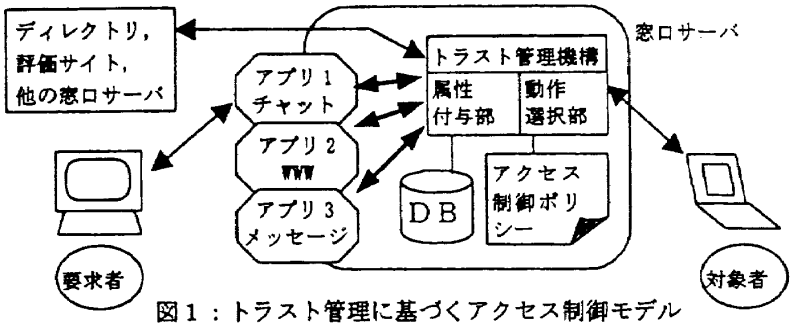

図 1 ：トラスト管理に基づくアクセス制御モデル

3. 新しいアクセス制御機構の提案

上述した既存アプローチを踏まえ，オンラインインタラクションに適したアクセス制御モデルを提案する.

3.1. トラスト管理に基づくアクセス制御モデル

オンラインインタラクションには PICS や P3P に類似したトラスト管理機構が必要だと考え，トラスト管理に基づくアクセス制御機構を提案する（図 1）．これは，インターネット上でユーザのコンタクトポイントを提供する「窓口サーバ」で動作し，ユーザへのインタラクション要求に対して適切な処理を選択させる．このモデルの特徴は以下の通りである.

(1) アクセス要求に対する信頼度制御

アクセス要求者の信頼度が十分でない場合，必要な補助的情報を本人，あるいは第 3 者（サイト）から情報を取得することで判断の補助とする．ディジタル署名や証明書を利用することで信頼度を向上させることができる.

(2) アクセス対象者の状態に基づく要求処理

アクセス要求に対して対象者の状態を反映した要求処理を可能にする枠組みを提供する．在不在や忙しさの程度によって適切な処理を選択できる．また，必要な場合には対象者や関連ユーザに最終的な判断を問い合わせることができる.

3.2. モデルの構成

以上の特徴を実現する上でこのモデルは以下のような構成を取る．(a) ユーザデータベースとの統合．要求者・対象者を含めたユーザの多様なデータを管理する DB を持つ．(b) アクセス要求，要求者属性などの情報から要求に対して動的に属性付与を行う属性付与部を持つ．(c) 付与された属性と対象者の状態等の情報からアプリケーションがとるべき処理を選択する動作選択部を持つ．アクセス制御のためのポリシーは，(b)と(c)に対応して「属性ポリシー」と「動作ポリシー」を持つ．属性付与は，役割ベースアクセス制御[2]の役割(Role)付与と，分散ファイルシステム AFS (Andrew File System)のユーザ定義可能なプロテクショングループ双方に関連する特徴を持つ．動作選択部は，付与された属性からアプリケーションが取るべき動作を認可(Authorize)する役割を持つ.

このような構成をとることの利点は以下の通りである．(1)アプリケーション独立．オンラインインタラクションを提供する複数のアプリケーション(WWW，チャット，メッセージ等）に対して共通のデータを用いたアクセス制御機構を提供することが可能となる．アプリケーション依存の処理は，動作ポリシーに記述される．(2) 記述の柔軟性と管理の容易さ．アクセス制御ポリシーを分離することで，動作ポリシーのみを変更することによって利用者が柔軟なアクセス制御の設定を行える．また，ポリシーの再利用・継承を可能にすることで，管理者，利用者双方の立場から設定を容易にすることができる.

4. おわりに

ネットワーク社会におけるオンラインインタラクションに適したアクセス制御について考察し，トラスト管理に基づくアクセス制御の仕組みを提案した．これは要求者に対する動的な属性付与と，アクセス対象者に関するデータの双方に基づく柔軟なインタラクション制御を可能にする．現在このモデルに基づくアクセス制御機構を実装中であり，チャットや WWW での利用を通して提案したアクセス制御モデルの効果について検証・評価を行う予定である.

参考文献

[1] Mirabilis 社ホームページ
http://www.mirabilis.com/
[2] D.F.Ferraiolo, J.A.Cugini, D.R.Kuhn "Role-Based Access Control (RBAC): Features and Motivations" Computer Security Application Conference, 1995
http://hissa.ncsl.nist.gov/rbac/newpaper/rbac.ps
[3] Yang-hua Chu "Trust Management for the World Wide Web" http://www.w3.org/1997/Theses/YanghuaChu/
[4] Platform for Internet Contents Selection
http://www.w3.org/PICS/