コンピュータセキュリティ　1－6
（1998．5．29）

ディレクトリーサービスに対する プライバシーを考慮した個人情報管理方式の提案

山崎重一郎*、須賀祐治*、村上美幸、荒木啓二郎*,**
*(財)九州システム情報技術研究所(ISIT), ** 九州大学

概要

本稿では、プライバシー権を考慮したディレクトリーサービスへの個人情報へのアクセス制御方式について提案する。プライバシー権にはいくつかの側面があるが、我々は「自分に関する情報は自分で管理できる権利で」という観点に着目する。

本稿で提案するアクセス制御モデルは、次のように構成される。(1) 既存のX.500ディレクトリのアクセス制御の上位レイヤとしてプライバシー管理のレイヤを設ける。(2) そのレイヤに本人の代理として情報へのアクセスを監視するエージェントを常駐させる。(3)エージェントを利用して情報要求者のデジタル証明書及びそのディレクトリーのエントリーに格納された信用情報に応じて自律的に情報へのアクセスの可否を判断する。

A Privacy Enhanced Access Control Model for Directory Service

Shigeichiro YAMASAKI*,Yuji SUGA*,Miyuki MURAKAMI ,Keijiro ARAKI**
* Institute of Systems & Information Technologies/Kyushu (ISIT), * * Kyushu University

abstract

We propose a privacy enhanced access control model for X.500 directory service.

The notion of privacy has various aspects. In this paper, we focused on a notion of a privacy as a right to control own information. Our model is constructed as follows. (1) We provade a new privacy control layer over the X.500 Directory access control. (2) An ACA (access contorol agent) which observe the requests for access to privacy information in the privacy control layer. (3) The ACA access judge the adviability about the access of privacy information from the trust information of the requester from the directory.

1. はじめに

我々は、社会基盤としての公開鍵認証基盤の研究開発を進めている[1]。これまで、複数の認証ドメインを統合的な相互認証を目的とした「認証システムの3権威分立モデル」の提案と実験を行ってきた[8]。

我々の認証基盤モデルでは、LDAPによるX.500ディレクトリーサービス[3]を証明書のリポジトリとして利用している。X.500ディレクトリーサービスは、人に関する情報を扱う情報サービスであり、我々の認証システムのディレクトリーサービスでも、デジタル証明書だけでなく様々な個人情報が登録されている。

個人情報を情報システムで管理しようとするときにまず問題になるのは、国民総背番号制への批判と同じように、あらゆる個人情報を特定の機関に管理されてしまうのではないかという不安である。この問題は、求人求職、行政情報、教育、医療など、個人情報を扱うアプリケーションでは必ず問題となる共通課題である。

また、プライバシー権を侵害するのは、人間だけではなく今後はシステムによるプライバシー権の侵害についても考慮が必要である。

近年 WWW サーバーなどでSSLによるクライアント認証が普及しはじめているが、クライアント認証を安全に行うには、クライアントのデジタル証明書を管理するシステムとの連携が必要である。このような証明書リポジトリとして現在有望なのがLDAPを使ったディレクトリサービスである。しかしWWWサーバーがディレクトリーの情報を濫用した場合の被害は、個人によるものよりも深刻であろう。

このような問題意識に基づいて、本稿では、プライバシー権を考慮したディレクトリーサービスへのアクセス制御方式について提案する。

ため，本稿で述べる方式は、情報の所有権を持つ個人の代理となるエージェントを使い、情報アクセス者のデジタル証明書と信用情報に応じて情報へのアクセスの可否を判断するものである。この判断の基準を作るために、ディレクトリーの中に信用情報を登録する認証基盤システムを作る。また、信用情報を元にする判断の方法についても述べる。

2. プライバシー権について

プライバシー権にはいくつかの側面があるが、我々は「自分に関する情報は自分で管理できる権利で」という観点のみに着目する[15][16]。

X.500ディレクトリーで定義されているアクセス制御モデルでは、ディレクトリーの管理者がアクセス権の管理を行うことになっているが、個人の情報をシステム管理者が管理するのは、このプライバシー権の考え方に反している。またシステム管理者の側から見ても、個人情報の公開範囲の判断という過大な責任を負うことになる。

3. アクセス制御モデル

3.1 従来のアクセス制御モデル

アクセス制御モデルとして、代表的なものにDAC（Discretionary Access Control model)と、MAC :(Mandatory Access Control model) がある[5]。

DACは、は通常 UNIX などで利用されているアクセス制御モデルである。このモデルでは、ユーザーがディレクトリーやファイルなどの情報の所有者となり、グループや他者に対して、読み、書き、実行などのアクセス権限の管理を行うものである。

MACは、アクセス制御のための束順序関係が定義されたラベルを情報やアクセス者に付け、この順序構造に従って不適当な情報の流れが無いように管理するものである。

またこれらとは別の観点から構成されたRBAC (Role Based Access Contorol model) というモデルがある[10]。RGAC ではアクセス権限の管理方法そのものを対象にしており、「ロール」と呼ばれる中間的な識別子を使って、ユーザーとアクセス権限割り当ての定義を抽象化している。

ロールには、2つの観点がある。一つはアクセス権限(permittion)の集まりに付けられた名前という見方で、例えば「社長」というロールは、その組織の中で社長という役割を持つ人に与えられているアクセス権限定義の集まりに付けられた名前である。もう一つは、ユーザー管理のためのグループに対応する概念で、例えば「新製品開発者」というロールを持つグループのメンバーには、個別にアクセス権限を定義する代わりにロールを定義することによって、組織変更などによるアクセス権管理を簡略化できる。

3.2 X.500ディレクトリアクセス制御モデル

X.500ディレクトリシステムのディレクトリアクセスプロトコルは、ユーザーのプロセスを意味するDUA(Directory User Agent) とサーバーのプロセスを意味するDSA(Directory Service Agent) から構成されている。

ディレクトリの情報は DIT (Directoru Information Tree) と呼ばれる階層的な名前構造のノードとして管理される。情報が格納されるノードをエントリーを呼ぶ。

X.500ディレクトリーは分散協調型のデーターベースなので、ディレクトリーへのアクセス制御には、DUA-DSA間のものとDSA-DSA間のものがある。本稿では、DUA-DSA 間のもののみに注目する。

X.500の1993年の勧告によるアクセス管理モデルでは、DIT をACSA (Access Control Specific Area) という領域に分割して、それぞれを SA (Security Authority)と呼ばれる機関によって管理し、さらにACSA をACIA (Access Contorol Inner Area)と呼ばれる複数の部分領域に分割して管理する方法をとっている。

エントリへのアクセス制御は、そのエントリ自身が持っているアクセス制御定義だけでなく、その上位にある管理領域が定義しているアクセス制御を総合したものになる。

このようにX.500ディレクトリーのアクセス制御モデルは、基本的にシステム管理者による管理を前提にしている。

3.3 プライバシー制御のためのアクセス制御の要件

2章に述べたプライバシー権の観点から見て、個人情報を扱うシステムには次の2つの条件を満たす

ことが要求される。

(1) 情報の所属範囲（情報の所有権）を明確化できること。

(2) 情報の所有権を持つ本人が、自分の意志に基づいて自分の情報の公開範囲を決定すること。

この要件は、3.2節で述べたX.500ディレクトリーのアクセス制御モデルの範囲を越えているので、何らかのシステムの追加が必要となる。

4. 信用情報に基づくアクセス制御

4.1 アクセス許可の判断情報の問題

3.3節の(2)で挙げた、本人の意志によって公開範囲を決めるという要件を満たすためには、そのような判断の手段や情報が必要になる。

自分の情報の公開範囲を決める判断は、アクセスしてきた相手によって動的に変化するために相手の信頼度を計る手段が必要である。

例えば、自分の住所はプライバシーに関わる情報であるが、通信販売で商品を発送してもらうには商店に自分の住所を知らせなければならない。このようなサービスを利用するときにディレクトリーサービスは便利だが、その商店が必ずしも信頼できるとは限らないので、商店にディレクトリ情報の自分の住所へのアクセス権限を与えるかどうかという判断に利用できる情報が必要になる。

4.2 3権威分立モデルによる信用情報の管理

我々は、認証基盤の一部として、安全なディレクトリによる証明書リポジトリを提案している。また、「認証局の3権威分立モデル」という認証基盤のモデルを提案しており、認証局の機能を「本人確認」「与信」「利用ポリシー定義」の3つに分割する方法についてシステムを試作し運用実験を行っている。

我々のこの認証モデルでは、各エンティティの信用情報は、証明書の中ではなく、ディレクトリーに格納する方針をとっている。このために常にアクセスして来たユーザーの信用情報を入手可能であるということを前提にすることができる。

4.3 信用情報の扱い方

我々は、「信用」という抽象的な概念を「信用のためのシンボル」＋「保証契約」という２つの情報の対として管理する。この二つについて少し説明する。

信用のためのシンボル：シンボルとは、象徴のことである。「日本銀行」や「情報処理学会」などはシンボルの例である。あるデーターに「日本銀行」が適切な手段でデジタル署名をしていた場合、保証内容と関係なくそれだけで一定の信用を持つことになる。

保証契約：与信者が契約として保証する内容であり、もし事故が発生した場合に与信機関が支払う代償や保証の範囲などが明確に定義されている。

我々は、「与信」や「信用」という用語を経済的な意味以外でも使用しているということに注意されたい。例えば、「本人は医師である」というような情報を国立病院が保証するというような場合も、国立病院が「与信」しているというような用語法を用いる。

ディレクトリには、エンティティの属性情報として信用情報のリストが定義されるようになっている。各エントリーに定義される信用情報は、与信機関のシンボルと保証契約へのポインタに与信者のデジタル署名がタイムスタンプと有効期限付きで登録される。

4.4 与信者と信頼者の関係の相対性

自分の病気に関する情報はプライバシーに関わるが、遠隔医療を受ける場合には医師にそれを開示しなければならない。

しかし、相手が本当に医師であるのかどうか確認する手段が必要である。この手段として信用情報が利用されるが、信用情報とは結局与信機関の「シンボル」としての意味を情報の情報管理主体が認めるかどうかにかかっている。場合によっては、遠隔地の国立病院よりも近くの個人病院の方が与信能力が高い場合もあり得る。

我々のアクセス制御モデルは、このような信頼度の相対性を扱えるようにしている。

5. 提案するモデル

我々は、既存のX.500ディレクトリーの標準仕様や実装例との連続性や応答性能なども考慮した現実的なプライバシーアクセス制御のモデルを提案する。

5.1 プライバシー管理レイヤの追加

我々の意味でのプライバシー権を守るシステムには、DAC的な情報の所有権管理とアクセス権限の本人確認が不可欠である。一方、既存システムとの整合性も重要なので、両方の連続的な結合のために、従来のX.500ディレクトリのアクセス制御システムの上位レイヤとしてプライバシー管理のレイヤを設ける構成をとることを提案する。

この新しいレイヤは、プロキシーサーバーとして実現する。ディレクトリーユーザーエージェントは、このプロキシーを介してディレクトリーサーバ

ーへアクセスする。プロキシーによる変換によって、ディレクトリーサーバーでは、通常のX.500ディレクトリーアクセス制御モデルの元で動作する。

5.2 ロールの導入

プライバシー管理レイヤとX.500ディレクトリの連携の管理を整理するために、RBACで用いられているロールの概念を導入する。

我々はロールを「役割のシンボル」＋「アクセス権の集合」として定義する。また、RBACにおけるユーザーに対応するのは、情報の要求者になるが、ユーザーに対するロールの割り当ては、信用判断そのものになる。

5.3 アクセス管理エージェント

情報アクセス者に対するアクセス可否の判断を本人が行うとして、常に本人がネットワークに接続した状態で判断を行うことはできない。このため、本人の代理としてそのような判断を行うエージェントをプライバシー管理レイヤに常駐させることを考える。このエージェントを ACA (Access Control Agent) と呼ぶことにする。

ACAは、各個人情報の所有者に対応して存在する。各ACA の所有者を「ACAの所有者」あるいは単に「所有者」と呼ぶことにする。ACAは、その所有者との接続によって、アクセスに関する判断基準の定義を保持する。

5.4 エージェントによる所有権の管理

プライバシー権を主張するには、個人情報を持つ本人が所有している情報の範囲を厳密に定義する必要がある。

ACAはディレクトリシステム側から見るとアクセス管理権限を持ったACIAの管理者としての権限を持つ必要がある。ACIA は、DIT のサブツリーとして定義されるので、個人が管理するエントリーをサブツリーACIA と定義することになる。したがって、結局このACIAが所有権が与えられている個人情報の範囲となる。

5.5 エージェントによる信用判断

ACAは、情報要求者が提示するデジタル証明書のDNを使ってディレクトリーからそのエンティティに定義されている信用情報のリストを得ることができる。

また、ACA はその所有者から信用してよい信用シンボルと、その信用判断の結果割り当てられるロールの定義が与えられる。

6. 信用判断の論理

ACA による信用判断の論理について簡単にふれる。

6.1 直観主義論理による信用判断

我々は、ACAによる信用情報の判断を直観主義論理に基づく型判断を利用して実現する[17]。

つまり、ACAの所有者のよって与えられた信用のシンボルを型と解釈して計算を行う。

例.

A を「信用シンボル」＝型　と解釈

B を「ロールシンボル」＝型　と解釈

a をエンティティ

a:A エンティティへの型割り当てを「a はAとして保証されている」と解釈する。

$$\frac{c:(\Pi x:A)B \quad a:A}{c(a):B(a\,|\,x)}$$

という式は、上式の左側は「何らかのAという機関から信頼されているエンティティx があれば、それにBというロールを持つことができるものとして信用を与える」というエージェントへの指示を意味し、上式の右側は「アクセスして来たエンティティaがA によって保証されている」ときに、下式は、「aの内部的なエンティティ c(a) はB というロールをa に適合させたものとして保証を与える」と解釈する。

この論理判断によって、信用シンボルからロールシンボルへの割り当ての可否が計算される。

6.2 信用情報に基づく直接分類

6.1で挙げた例は、信用する機関のシンボルを直接的に定義し、ロールを直接的に割り当てる判断を行っている。つまり、アクセス者をACAの所有者が定義したシンボルに基づいて直接的に分類している。この方法に基づく場合、信頼を許可する信頼シンボルの全て列挙する必要がある。

6.3 信用情報に基づく間接分類

現実のアクセス権管理では、信頼する組織を全て列挙することはあまり実用的でない。例えば決済が可能な金融機関とか、配達を許可する運送会社とかを全て列挙するのは難しいであろう。

この代わりに、与信機関の与信機関というような存在があると便利になる。クレジットカード会社は、まさにそのような立場にある。このような与信機関の与信機関によるエンティティの分類を間接分

類と呼ぶことにする。

経済活動だけでなく、求人のドメインは、教育のドメインや、医療のドメインなどの与信機関の与信機関利用すると、ACAの定義は非常に簡単になる。したがって、このような間接分類の機構は非常に有用であると考えている。

7. システム構成

X.500のアクセス制御の認証には、X.509を使った公開鍵暗号による認証を含んでいる。

我々の実装では、LDAPをSSL上で使用するが、SSLは認証にX.509に基づいたデジタル証明書を使用しているので、DSAやDUAのx.500ディレクトリーのエントリーへのアクセスは同じ名前空間を利用して実現できる。

7.1 アクセス制御のレイヤ構成

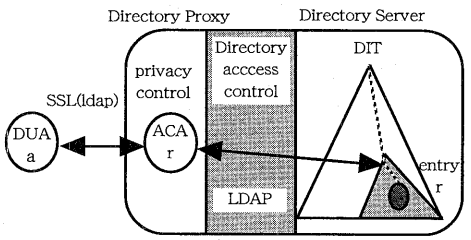

図1. プライバシー管理レイヤとACA

システムの全体的な構成は、図1のようになる。DUAは、ディレクトリーにアクセスするユーザーである。DUAとディレクトリシステムの間はSSLに基づいたクライアント認証を行う。また、DUAが直接アクセスできるのは、ディレクトリーシステム本体ではなく、そのプロキシーにあるエージェントである。

アクセス制御は、プライバシー管理レイヤとディレクトリアクセス制御レイヤから構成され、これらを経てDITの中の個人のエントリーの情報へアクセスされる。

7.2 クライアントによるアクセス

まず、前提として、ACAには、Aという与信機関から保証されている人がアクセスしてきたらRというロールを割り当てなさい、という定義がなされているとする。この定義を簡略的にA →Rと書くことにする。

情報要求者がアクセスしてきたとき、そのクライアントのデジタル証明書のDNを使ってDITの中のクライアントのエントリを検索すると、そのクライアントの信用情報を得ることができる。この前提として、エージェントには、信用情報については全DITを検索する権限が与えられているものとする。

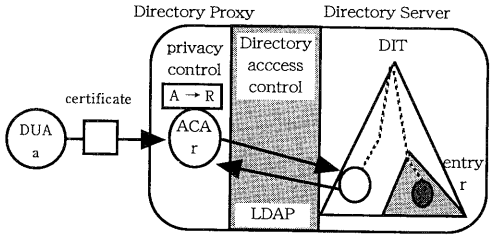

図2. アクセス要求と信用情報の検索

こうして得られた信用情報が、a:A つまり、アクセスして来たエンティティが与信機関Aによって保証されいるというものであった場合、情報要求者にはRというロールが割り当てられる。ロールとはアクセス権限（permittion)の集まりなので、これを元に、X.500 のアクセス制御に対してアクセス権限を定義できる。

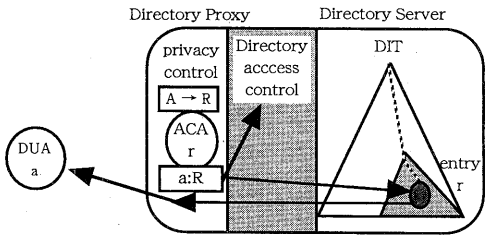

図3. アクセス権限の割り当てと情報アクセス

この結果、リクエストが評価され情報のアクセスが実行される。

8. 関連研究と議論

関連研究についてのべ、我々のモデルについて議論する。

8.1 目的 指向の アクセス制御

Tachikawaらは[11]、アクセス制御をオブジェクト指向の枠組みで定義された情報の流れと束論的な制御の関係として分析したうえで、間接的な操作の委譲について議論している。

我々はアクセス権限をロールという形でひとまとめにして議論したが、書き込みの可否などより詳細な情報の流れ方を定義するためには、このようなアプローチも必要かもしれない。

8.2 直観主義論理とBAN論理

認証プロトコルのための論理としては、BANロ

ジック[6]が良く利用される。BANロジックは、principal と呼ばれる通信の主体への動的な「知識」の移動を表現するのに適した内包論理である。暗号通信による情報の追加などを表現するにはこのような動的な知識の追加が必要である。しかし、内包論理をリアルタイムで計算するのは通常不可能である。

これに対して、我々のエージェントは、その所有者が与えた信用すべきシンボルは処理の過程で不変である。したがって内包論理を用いる必要は無い。また逆に、アクセス権限についての判断は常にリアルタイムで行わなければならないので、効率的な計算方法がわかっている型判断はこの用途に適していると考えられる。

8.3 エージェントのセキュリティ

エージェントへの攻撃には、トロイの木馬や仲介者攻撃などが考えられる。これらへの防御は、多岐にわたる。

しかし、ここではACAはセキュアなマシンで管理されるものとする。証明書リポジトリとしてのディレクトリは強く管理される必要があるので、アクセス管理エージェントが常駐しているサイトもセキュアであるということは仮定可能である。

ACAはサブツリーの上位のエントリへの権限をSAによって強く制限できるので、もしACAが攻撃を受けた場合でも他者のACIAへの影響は最小限にすることは可能である。

11. おわりに

我々は福岡オンライン認証実験プロジェクトの一環として、3権威分立モデルに基づいたデジタル認証システムを提案し、実証実験を行っている。

本稿では、この認証基盤の中核になる証明書リポジトリのディレクトリーサービスに対するプライバシー保護の方法について提案を行った。

本稿で提案したプライバシー保護のモデルは、従来のディレクトリーシステムのアクセス制御の上位レイヤとしてプライバシ管理のレイヤを設けるものである。このプライバシ管理レイヤは、ディレクトリーサービスのプロキシーとして実現する。

プライバシー管理レイヤでのアクセス管理は、アクセス管理エージェントと呼ぶ自律的なプロセスの監視によって実現する。

アクセス管理エージェントによるアクセス権の割立ては、情報要求者に定義されている信用情報と、エージェントの所有者が、信用情報と対にして定義するロールによって決定される。この判断には直観主義的型理論を利用する。

レイヤの分離によって、既存のシステムとの連続性を持ちつつ、プライバシー管理の手段を定義することができた。

今後実際のアプリケーションに対して本モデルを適用し運用実験の評価を行う予定である。

参考文献

[1] 山崎重一郎他:福岡オンライン認証実験WG :http://www.k-isit.or.jp/dccf/,1997

[2] ITU Rec. X.509 (1993) | ISO/IEC 9594-8: including Draft Amendment 1: Certificate Extensions (Version 3 certificate).1993

[3] ITU Rec. X.500 (1993) | ISO/IEC 9594-1: The Directory: Overview of Concepts, Models, and Services, 1993

[4] 大山実、他: X500ディレクトリ入門,東京電気大学出版局,1997.

[5] Deborah Russell,G.T.Gangemi Sr.,(山口英監訳): Computer Security Basics,アスキー出版局,1994.

[6] Michael Burrows,Martin Abadi, Roger Needham.:Proc.Royal Soociety,Serieas A. Vol.426,No.1871,pp233-271,1989.

[7] 山崎重一郎,須賀祐治,荒木啓二郎: モバイルエージェントによる電子発注と電子決済の統合モデルの提案,情報処理学会DPS研究会,97-DPS-85-22, 1997.

[8] 山崎重一郎,須賀祐治,村上美幸,荒木啓二郎: 認証, 証明書発行, 利用ポリシー適用の"3権威分立モデル"に基づくデジタル認証システムについて, 情報処理学会DPS研究会,98-DPS-86-8, 1998.

[9] Ravi S.Sandhu: Lattice-Based Access Control Models,IEEE Computer Vol.26, No. 11,pp9-19,1993.

[10] Ravi S.Sandhu, Edward J. Coyne: Role-Based Access Control Models,IEEE Computer Vol.29, No. 2,pp38-47,1996.

[11] Takayuki Tachikawa, Hiroaki Higaki,Makoto Takizawa: Purpose-Oriented Access Control Model iin Object-Based Systems,Proceedings of ICOIN-11 Vol.2,pp8B-1.1-8B-1.7,1997.

[12] 双紙正和,加藤丈治,前川守: 分散環境における、プロクシを利用した柔軟なセキュリティ制御,情報処理学会論文誌,Vol.39 No.3,pp810-817,1998.

[13] B. Kaliski: RFC1424 IETF Privacy Enhancement for Internet Electronic Mail: Part IV: Key Certification and Related Services: 1993

[14] VISA Card, Master Card: SET Secure Electronic Transaction Specification ,1997

[15] 榎原猛編: プライバシー権の総合的研究,法律文化社 1991.

[16] Jed Rubenfeld, (後藤光男、森下史郎、北原仁訳): The right of privacy, 敬文堂, 1997.

[17] Per Martin-Lof:Intuitionistic Type Theory, Notes by Giovanni Sambin of a series of lecturees give in Padua, BIBLIOPOLIS, 1980.