属性証明書を利用するアクセス制御

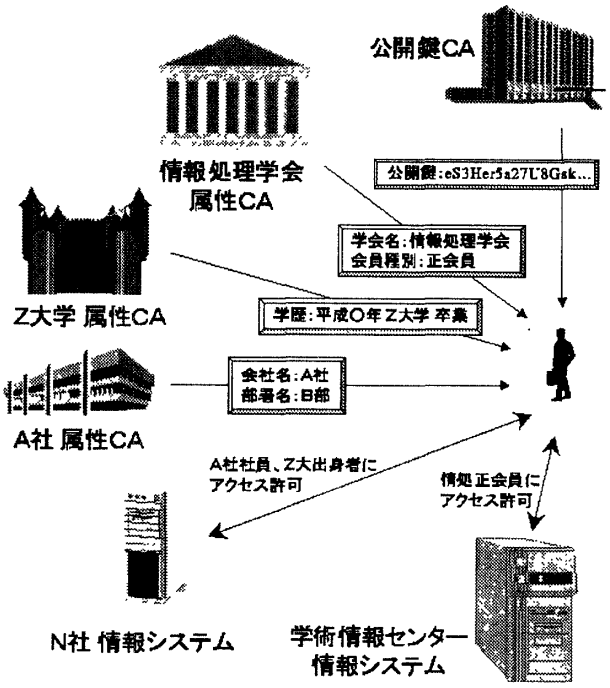
4H－11

山岡 誉侍　　宮内 宏
NEC　C＆Cメディア研究所

1　はじめに

重要な情報を守るために有効な方法として、アクセス制御技術がある。しかし、オペレーティングシステム（OS）内やイントラネット内などの環境における既存のアクセス制御の方法は、ユーザ情報を情報システム内に蓄えることを前提にしている。インタネットが普及し、情報システムに対して不特定多数の利用者が見込まれる現在においては、このアクセス制御の方法では対応できないサービスが増えることが予想できる。

本稿では、属性証明書を利用したアクセス制御を提案する。この方法は、ユーザ情報を分散管理することにより、不特定多数のユーザに対してのアクセス規則の設定を可能にする。



2　基本概念

まず、本稿の提案の基本概念を述べておく。

情報システムにとって不特定多数のユーザを対象にアクセス制御を行うためには、ユーザを何らかの情報によってグループ化できればよい。そこでアクセス規則をユーザの“属性”により設定する方法を用いる。

属性の利用にあたっては、未知のユーザの属性情報が正しいかどうか確認できなければならない。そこで、ユーザの属性情報を保証する機関“属性CA”と、それが発行する証明書“属性証明書”を用いる。

さらに情報システムでは、アクセス許可を行うためにはユーザが本人かどうかを確認するユーザ認証を行う必要がある。そこで本稿では、認証のために公開鍵証明書を使用する。

Access Control with Attribute Certificates
Kouji Yamaoka, Hiroshi Miyauchi
C&C Media Research Laboratories, NEC Corporation

3　アクセス規則の属性による設定

本稿では、ユーザの一部の情報を与える、あるいは、ユーザの特性を記述するデータを、“属性”と定義する。属性は、情報の項目の“属性型”と、その実現値の“属性値”から構成される。属性型としては、会社名、部署名、学歴、免許、などが考えられる。

既存のアクセス制御の方法では、何らかの基準でユーザをグループ化することでアクセス規則を単純にしている。ユーザが個別に登録されていない不特定多数が利用するような情報システムにおいても、アクセス規則を属性（あるいは、属性の論理式、演算式、条件式）により設定し、ユーザの側で属性を提示することで、さらに柔軟な制御が可能になる。

4　属性CAによるユーザ管理の分散

ユーザの属性情報の保証のために、信頼できる第三者機関“属性CA(Certification Authority)”のデジ

タル署名が付加した“属性証明書”を用いる。属性証明書により、ユーザは属性情報の正当性を主張でき、情報システムは属性情報の確認ができる。

ユーザには多種多様の属性情報が考えられるため、1つの属性CAでユーザの全ての属性を証明するような形態は現実的ではない。各属性の保証は、適切な属性CAにより行われるべきである。極端な場合は、1つの属性に対して1つの属性CAが対応するというようなことも考えられる。適切な属性CAによる分散管理は、各属性CAの負担が軽くなるという利点もある。

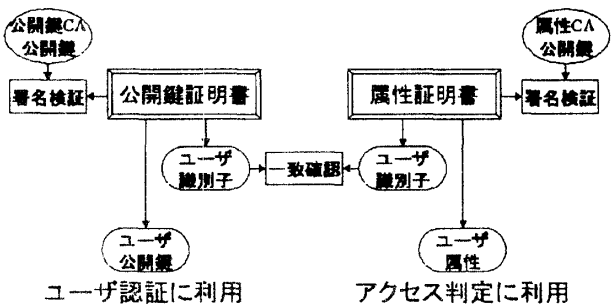
当然、情報システムを利用する際には、属性証明書は当人以外には使用できないような仕組みが必要になる。

5 属性証明書の利用方法

属性証明書が提示したユーザのものであることを確認するための1つの方法として、公開鍵証明書を使用する方法がある。この方法は、秘密鍵の所持によりユーザは正当性を主張し、公開鍵により確認する、非対称暗号系の認証方法に基づいている。

公開鍵証明書にはユーザを示す識別情報が含まれていて、この識別子がある範囲内で一意であるとする。また、ユーザの属性証明書にも同じ識別子を含めるようにする。

この条件のもとでは、公開鍵証明書によりユーザ認証は行える。識別子の一致により、属性証明書が提示した認証ユーザの属性を表示していることがわかる。また、属性証明書の属性CAの署名の検証で証明書の正当性がわかる。以上の手続きにより、ユーザの属性が確認できる。



よって、ユーザは公開鍵CA、属性CAより証明書の発行を受け、また、情報システムは公開鍵CA、属性CAの公開鍵の入手により、情報システム内でのアクセス判定が可能になる。

6 サービスへの適用例

例えば、情報処理学会が正会員に対してそれを証明する属性証明書を発行すれば、学術情報センターでは個別の利用申請の必要なしに情報検索サービスを提供することが出来る。

本稿の提案を採用することにより、多種多様のサービス形態が可能になると考えられる。

7 おわりに

本稿では、不特定多数のユーザが利用する情報システムにおいても適応できる、属性証明書を利用したアクセス制御について述べた。

この方法には、

- ユーザ情報を蓄えておく必要がないため、情報システムでのユーザ管理が簡易
- ユーザの属性を用いるので、アクセス規則の設定が単純
- 管理を分散しているため、各属性CAのユーザ管理の負担が軽い

などの利点がある。

この方法は高度なセキュリティを保っており、インタネットの普及により、組織や団体などによる機密度の異なる情報発信が一般的になる際には、重要な役割を演じるものと考えられる。

参考文献

[1] D.E.R. デニング 著、上園忠広 他訳
暗号とデータセキュリティ
培風館、1988

[2] 宮崎博、鮫島吉喜
ユーザ属性情報にもとづいたアクセス制御方式
情報処理学会 第52回全国大会、4-349、1996