1T－4

X.500ディレクトリを用いた電子認証システムの実装

岸本　康成　空　一弘　窪田　光裕
ＮＴＴ情報通信研究所

1. はじめに

ネットワークにおけるセキュリティの必要性から，公開鍵を用いた暗号化・認証の技術が不可欠となりつつある。公開鍵方式を利用するには通信相手の公開鍵を公開鍵証明書の形で取得する必要がある。公開鍵証明書の取得を容易にするには，公開鍵証明書を一括管理できるシステムが不可欠である。現在，公開鍵証明書を管理できるシステムの1つとして，分散管理機能を持つX.500ディレクトリ[1),2)]がある。

今回，我々はインターネット上に電子認証システムを構築し，公開鍵証明書の管理にX.500ディレクトリを用いたので報告する。本稿では，まずX.500ディレクトリによる公開鍵証明書管理の概要について述べた後，3章で実際に試作したシステムの説明を行う。

2. X.500ディレクトリによる公開鍵証明書管理

X.500ディレクトリでは情報をツリー構造で格納している（図1）。このツリーをDIT(Directory Information Tree)と呼ぶ.ツリー上の各ノードは実世界のオブジェクトに対応しており，エントリと呼ばれる。エントリは通信に関するさまざまな情報を属性として持つ。セキュリティ関連の属性を持つオブジェクトクラスとして厳密認証利用者、証明機関の２種類がある。厳密認証利用者は実世界では一般の公開鍵ユーザに該当し，属性として，利用者証明書を持つ。一方，証明機関は公開鍵証明書に署名し信用を与える非常に社会的に信頼された企業・団体に対応するものであり，属性として，証明機関証明書，失効証明書リスト（無効となった利用者証明書の一覧），失効証明機関リスト（無効となった証明機関証明書の一覧）を持つ。

X.500ディレクトリへのアクセスはDUA(Directory User Agent)からDAP(Directory Access Protocol)により行われる。特にインターネットからX.500ディレクトリへアクセスする場合は，LDAP[3)]（Lightweight Directory Accsess Protocol）をLDAP/DAP Gatewayを用いてDAPに変換してアクセスするのが一般的である。

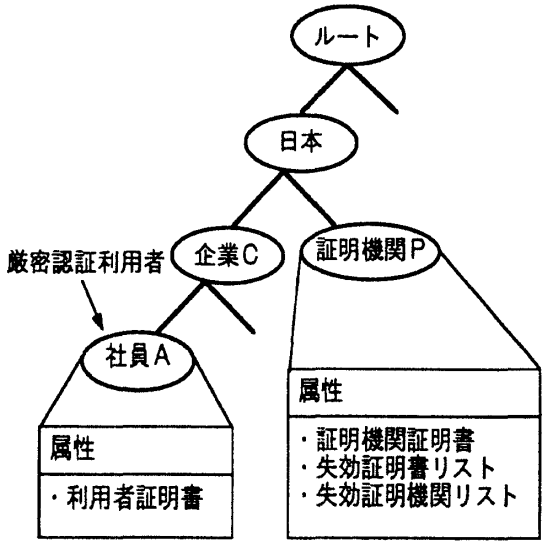

図1　X.500ディレクトリの情報格納構造

3. 電子認証システムへの適用

ディジタル署名を用いた認証では，認証相手の公開鍵証明書が必要である。ディレクトリで公開鍵証明書管理を一元的に行うことにより、公開鍵証明書の取得は容易になる。そこで今回，認証時に必要となる公開鍵証明書をディレクトリから取得するインターネット上の電子認証システムを構築した（図2）。本認証システムはインターネット上の買い物客が電子商店のホームページの認証を行うものである。買い物客はホームページから署名ファイルをダウンロードし，署名ファイルに格納された電子商店のURLに対する署名を電子商店の公開鍵証明書により署名検証することにより、電子商店の認証を行う。本システムを実現するには，以下に示す２つの機能が必要である。

①ディレクトリへの公開鍵証明書登録等の処理を行う公開鍵管理機能

②買い物客が電子商店からダウンロードした署名の検証機能

以下に各機能の実現方法について述べる。

Implementation of Electronic Authentication System Using X.500 Directory

Yasunari Kishimoto,Kazuhiro Sora,Teruhiro Kubota
NTT Information and Communication Systems Laboratories

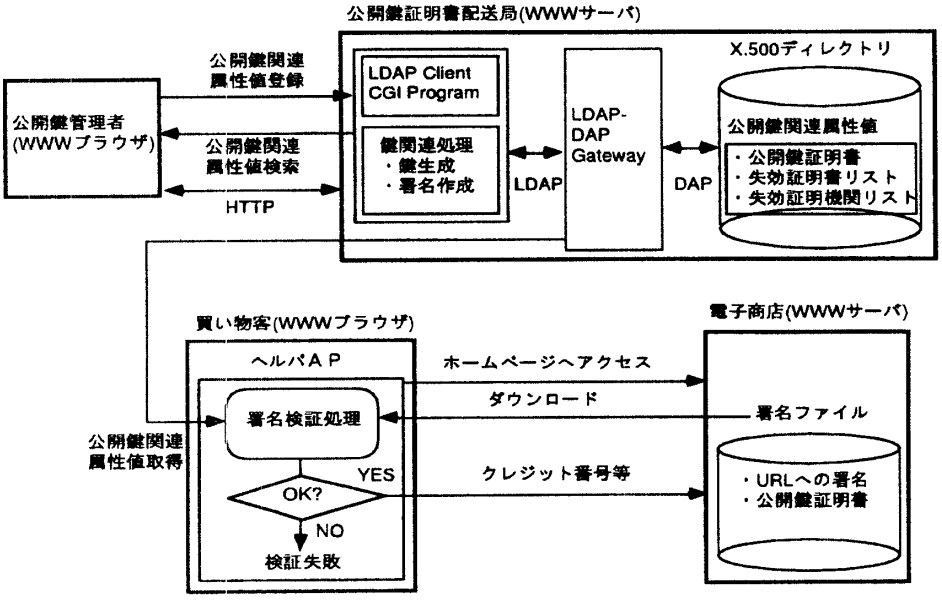

図2　電子認証システムの概略図

3.1　公開鍵管理機能

ディレクトリで公開鍵証明書を管理する場合,ディレクトリに対して公開鍵証明書の登録・削除・検索等の処理を行う機能が必要である。本システムでは,この機能をWWWブラウザ上のインタフェースとして実現した。ディレクトリでは公開鍵証明書以外に,さまざまな情報が管理されるので,インタフェースは公開鍵証明書管理に特化した形ではなく,汎用的なディレクトリインタフェースとした。インタフェースの実現はブラウザで入力したディレクトリ操作内容を公開鍵証明書配送局のCGIプログラムでLDAPに変換することにより行う。

一方,新規に公開鍵証明書を登録する場合は公開鍵証明書の作成が必要となる。本システムでは公開鍵証明書配送局に鍵生成・署名生成機能を持たせることによって,汎用的なディレクトリインタフェースの中に公開鍵証明書の作成の機能を組み込んだ。

3.2　署名検証機能

署名検証処理はダウンロードされた署名を電子商店の公開鍵により検証する処理と電子商店の公開鍵証明書検証処理の２つの処理からなる。これらの処理を実現するには,買い物客の端末側で以下の２つの処理を実装する必要がある。

①公開鍵による署名検証処理

②X.500ディレクトリから公開鍵関連属性値（公開鍵証明書，失効証明書リスト，失効証明機関リスト）を読み出す処理

本システムではWWWブラウザ上のヘルパAPにこれらの処理を組み込むことにより,署名検証機能を実現した。

さらに性能上の観点から,公開鍵証明書検証処理におけるX.500ディレクトリへのアクセス回数を減らすため，ヘルパAPに公開鍵関連属性値のキャッシュを行う機能を追加した。この機能は過去にX.500ディレクトリから取得した公開鍵証明書，失効証明書リスト,失効証明機関リストを検証済か否かで分類した形で一定の利用期限を設けて再利用するものであり，X.500ディレクトリへの負荷の削減，公開鍵証明書検証処理時間の短縮の効果が期待できる。

4．おわりに

本稿では，X.500ディレクトリによる公開鍵証明書管理の適用例として,インターネット上の電子認証システムの実装方法について示した。本システムに限らず，X.500ディレクトリは公開鍵によるセキュリティ技術を利用したさまざまなシステムに利用できる。

今後は，X.500ディレクトリによる公開証明書鍵管理の運用面・性能面からみた評価を行う予定である。

参考文献

1)The Directory:Overview of Concepts,Models and Services. ITU-T X.500, 1993.

2)The Directory:Authentication Framework. ITU-T X.509, 1993.

3)W.Yeong,T.Howes,S.Kille,Lightweight Directory Access Protocol. Request For Comments(RFC)1777,March,1995.