# OSIディレクトリの高度化

1F－1

空　一弘　　窪田光裕　　田中博巳
NTT情報通信研究所

## 1. はじめに

近年のインターネットの著しい発展に伴い，全世界に分散配置された様々な情報にアクセスすることが可能となった．この代表的な情報提供サービスとしてはWWW (World Wide Web) がある．WWWは手軽な情報発信を行う分野には適するが，体系的な情報をきめ細かくアクセス制御して管理すべき分野には適さない．

これに対してISO/ITU-Tでは，OSIの応用層のサービスの一つとして，通信に関する情報に関する分散データベースであるX.500ディレクトリを規格化している[1]．OSIディレクトリサービスはWWWの欠点を補う性格を持つもので，インターネット上でもWWWと共存して利用されている．

我々は，これまでにインターネット上で動作するOSIディレクトリシステムを構築し[2]，社内ネットワークにて運用開始している．今回，分散処理機能，公開鍵証明書管理機能，GUI保守機能を新たに実現したので報告する．

## 2. 分散処理機能

### (1) 分散処理の実現形態

WWWでは，利用者が複数の情報サーバを直接意識しながら渡り歩く形態で分散処理を実現する．

一方OSIディレクトリでは，情報サーバとなるDSA (Directory System Agent) 間で協調動作を行う形態で分散処理を実現する．これにより，分散管理された情報の所在を意識せずに仮想的に単一の情報サーバと見做して利用できる (図1)．

### (2) アクセス制御機能の実現

ITU-T勧告X.501では，実世界の人間や機器等のオブジェクトを表すエントリや，オブジェクトの各種特徴を表す属性と呼ばれる情報単位毎に，アクセス者やアクセス種別に応じたアクセス制御を行う枠組みが規定されている．分散ディレクトリにおいてこれを実現するには，複数のDSA間でアクセス者に関する情報を正確に共有する必要がある．

我々のシステムは，パスワードで相互認証されたDSA間では転送される要求や結果が信頼できるという前提で実現した．この時，エンドユーザの識別名は最初に要求を受けたDSAで認証されているので，要求の転送先のDSAでもこれをアクセス者名として信頼して使用することができ，複数のDSA間でも正しくアクセス制御を行うことが可能となった．

### (3) 高速な条件検索

OSIディレクトリでは，基本的な情報単位であるエントリをツリー構造に配置して情報管理する．この中の部分ツリーに対する条件検索はOSIディレクトリへの一般的アクセス形態の一つであり，その性能向上は主要な課題の一つである．

従来の我々のシステムでは，市販のRDBMS (Relational Database Management System) を使用してデータ管理しているが，テーブル構成の工夫により高速な条件検索を実現している．今回，従来方式を副作用がないように拡張し，検索対象の部分ツリーが複数のDSAに分散した場合でも単一のDSAに存在する場合と同等の性能を達成した．

## 3. 公開鍵証明書管理機能

### (1) 公開鍵証明書の必要性

近年，通信のセキュリティの確保が注目されているが，その主要な技術として，暗号化による情報の隠蔽と，署名による情報の正当性証明がある．

これらの処理には公開鍵と秘密鍵を対で使用する公開鍵方式が一般的に利用されている．この公開鍵

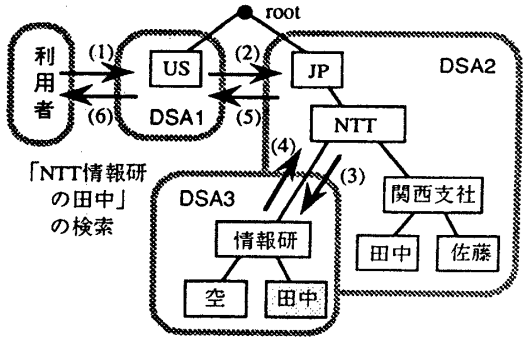


図1　分散ディレクトリ処理

---

Enhancements for OSI Directory System
Kazuhiro Sora, Teruhiro Kubota and Hiromi Tanaka
NTT Information and Communication Systems Laboratories
1-2356 Take, Yokosuka, Kanagawa 238-03, Japan

方式を用いて暗号化や署名付与を行う場合，証明機関の署名が付与された公開鍵である証明書を，広く一般に配布するサービスが不可欠となる．

(2) OSIディレクトリを用いた証明書管理

ITU-T勧告X.509では，OSIディレクトリを用いた公開鍵証明書の管理・配送機能を規定している．この機能を備えたシステムを構築することにより，インターネットでの安全・確実な通信が実現できる．

そこで今回，我々のDSAにこの証明書管理機能を追加した．ここでは，X.509で規定されているRSA暗号アルゴリズムやRSA署名アルゴリズムの他に，NTTで開発した楕円DH暗号アルゴリズムやESIGN署名アルゴリズムの公開鍵証明書も扱えるよう情報形式を拡張した．

また，OSIディレクトリの利用者インタフェースであるDUA (Directory User Agent) において，ESIGNアルゴリズムを用いて公開鍵に署名を行い証明書を作成する証明機関向け機能や，OSIディレクトリから検索した証明書の署名を検証する一般利用者向け機能を実現した (図2)．

## 4. GUI保守端末

(1) 格納情報の保守機能の必要性

OSIディレクトリのような情報提供サービスを行う場合，格納された情報を適宜更新し最新の情報を維持していくことは不可欠である．

そこで，今回，情報保守者向けの端末機能を追加した．本機能は，Xウインドウ上にGUIとして実現したため，情報の保守作業を簡単な操作で行える．

(2) 社員録管理に有効な機能の実現

OSIディレクトリを用いて社員録を管理する場合，一般に組織階層に従ってディレクトリのツリーを構築する．この時，組織整備や人事異動に伴い，特定の部署や個人の情報を別の部署に移動させるケースが頻発する．

ところが，ITU-T勧告X.511 (1988年版) では，個人を表すエントリや，部署を表す部分ツリーを一括移動させるサービスが規定されていない．そこで，今回作成した保守端末ではエントリや部分ツリーの一括複写や一括削除を行うマクロ機能を用意した．本機能により，1回の操作で情報を移動できるようになった．

また，古い情報からの検索を可能とするため，古いエントリは完全に削除せずに新しいエントリへのリンクを残しておくことが望ましい．そこで，一括複写マクロ機能の延長として，このリンク情報を格納した属性や，複写を行った日時を格納した属性を自動的に更新する機能も実現した (図3)．

## 5. 終わりに

構築したOSIディレクトリシステムに対して，分散処理機能，鍵管理・配送機能，GUI保守機能を追加し，実運用に必要な機能を整備した．

今後の課題として，分散ディレクトリの各DSAにおける処理時間とDSA間の通信時間を考慮した性能分析や，証明書管理機能の電子取引システム等への適用があげられる．

## 参考文献

[1] ITU-T Recommendations X.500-X.521 (1988)

[2] 空他：RDBMSによるOSIディレクトリの実現，情報処理学会 第95回DBS研究会，p.p.85-94 (1993)

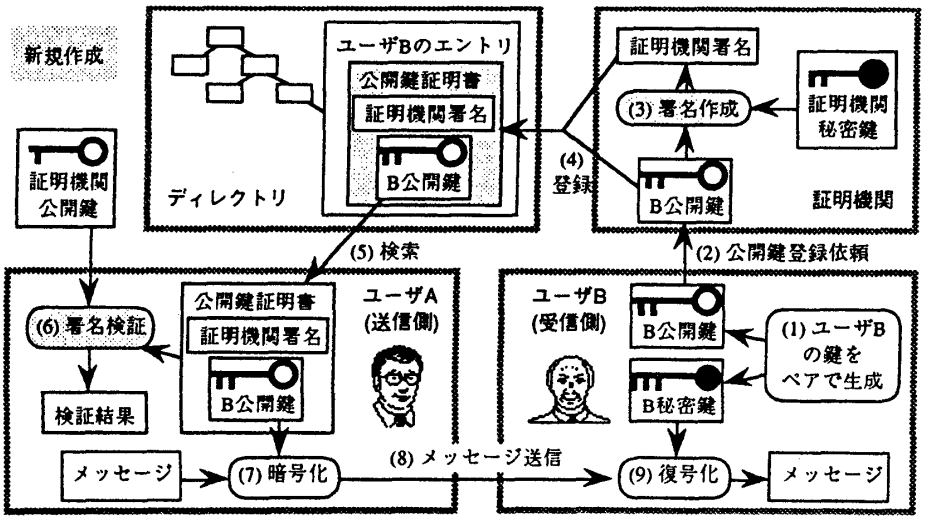


図2 OSIディレクトリを用いた証明書管理

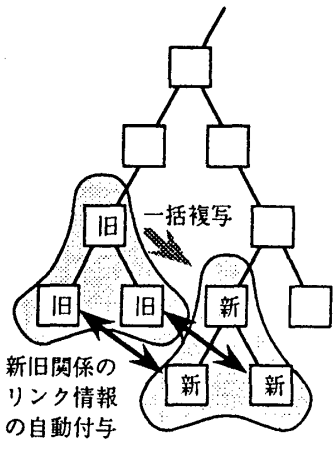


図3 一括複写マクロ機能