# 分散システムにおけるディレクトリサービスのセキュリティへの適用

3D－2

辻　宏郷，中川路哲男，勝山光太郎

三菱電機(株)　情報システム研究所

## 1　はじめに

分散システムにおいて、ディレクトリサービスは資源の位置透過性を実現する上で不可欠な要素となっている。一方、オープン化された分散システムにおいて、通信に関わる虚偽の否定を防止するために、中立なエンティティを用いた否認不可機能が必要となる。我々は、ディレクトリサービスを拡張することによって、分散システムにおける否認不可サービスを実現することを検討した。本稿では、これらの検討結果について報告する。

## 2　分散システムとディレクトリサービス

ディレクトリサービスは、分散システムにおける様々な資源の情報を管理するサービスである。各々の資源に対して、一意に定まる名前と様々な属性情報を格納しており、これらの情報を登録・削除・検索する機能を提供する。図1は、ディレクトリサービスを用いてサーバの位置透過性を実現した例である。サーバは、自身の情報をディレクトリサービスに登録する。クライアントは、ディレクトリサービスを用いて処理可能なサーバを検索し、そこで得られたアドレス情報をもとにサービス要求を発行する。

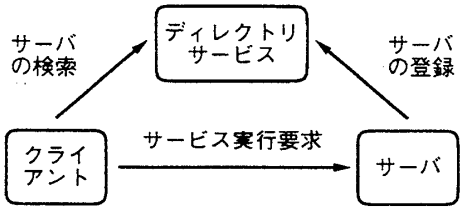


図1　ディレクトリを用いたサーバ位置透過性の実現

一方、分散システムのオープン化・広域化に伴い、端末や通信路の安全性を保証することが困難となっている。この様なシステムでは、セキュリティサービスを用いて、認証やアクセス制御を行う必要がある。ディレクトリサービスは、管理している情報に対する不正な利用を防止するために、この様なセキュリティ対策が考慮されている。例えば、OSIディレクトリ[2]は、利用者や他のディレクトリサーバに対する認証機能や、データのアクセス制御機能を持っている。従って、ディレクトリサービスに必要な情報を登録することによって、セキュリティ用データベースとして使用することは有効であると考えられる。

## 3　否認不可サービスのモデル

### 3.1　否認不可

否認不可（Non-repudiation）は、ある通信に関連するエンティティの一つが、その通信へ関与していることを虚偽に否定することを防止することである。文献[1]では、否認不可を下記の二種類の形式に分類している。

- **Non-repudiation with proof of origin**
  データの発信を発信者が虚偽に否定することの防止
- **Non-repudiation with proof of delivery**
  データの受信を受信者が虚偽に否定することの防止

例えば、分散システムにおいてオンラインショッピングを行う場合、顧客・販売会社間の意見の食い違いによるトラブルを避けるために、この様な機構が必要となる。

### 3.2　TTP

Trusted Third Party（TTP：信頼できる第三者）は、否認不可に関わる全てのエンティティから信頼された中立エンティティであり、否認不可を実現する上で不可欠な要素である。TTPは、データやその発信者・受信者の識別子をもとに、完全性（改変されていないこと）を保証する証拠（evidence）を生成する。さらに、その証拠を記録したり、確認するための機能を提供する。

---

**Application of Directory Service to Non-repudiation in Distributed Systems**
Hirosato TSUJI, Tetsuo NAKAKAWAJI, Kotaro KATSUYAMA
Computer & Information Systems Laboratory, Mitsubishi Electric Corporation.

### 3.3 否認不可のダイアグラム例

クライアントからサーバに対するサービス要求において、データ（サービス要求）に関する Non-repudiation with proof of origin を実現するダイアグラムの例を、下記に示す。

- クライアントは、TTP に証拠の生成を要求する。
- TTP は、生成した証拠を記録する。
- クライアントは、証拠と共にサービス要求をサーバに送る。
- サーバは、TTP に受信した証拠の確認を要求する。
- クライアント・サーバ間で論争が生じた場合は、調停者に証拠を送って判定を依頼する。必要な場合は、TTP に記録された証拠を利用する。

## 4 ディレクトリを用いた否認不可の実現

### 4.1 TTP としてのディレクトリ

本章では、ディレクトリサービスが認証・アクセス制御機能を備えていることに着目し、TTP に必要な拡張を行うことによって、否認不可サービスを実現することを提案する。まず、中立機関によって運用されるディレクトリ（マスターディレクトリ）を設置する。機密性を要求される暗号かぎや TTP が記録すべき証拠は、全てマスターディレクトリに記録する。発信者や受信者に関する情報は、通常ローカルなディレクトリに記録されているが、これらの情報については、マスターディレクトリに記録されなければならないこととする（図2）。

### 4.2 証拠の生成・記録・確認

マスターディレクトリは、TTP として証拠の生成・記録・確認機能を提供する。このため、証拠の生成に必要な情報と証拠を、ディレクトリサービスが格納するデータ（オブジェクト・属性）として定義する。また、必要ならば、データ構造中に暗号化方式を指定する属性を加えておく。証拠の生成を要求する発信者（あるいは受信者）は、生成に必要な情報をマスターディレクトリに登録する。マスターディレクトリは、これらの情報が登録された場合、証拠を生成して自動的にデータ登録できる様に拡張する。この時、証拠の生成はマスターディレクトリ自身が行うか、あるいは、同一ノード上の TTP プロセスが生成してディレクトリに登録する。証拠生成の要求者は、このデータを読み出すことで生成された証拠を受領し、同時に証拠はマスターディレクトリ上に記録される。さらに、データ値の照合規則を利用者が定義できることを利用し、証拠の確認に必要な照合規則を定義する。従って、属性の比較命令をマスターディレクトリに要求することで、証拠の確認を行うことができる。

### 4.3 管理用情報の記録

否認不可を実現する上で、かぎ等の管理情報に関する登録・変更・削除・一覧機能が必要となる。これらは、マスターディレクトリ上のデータとして記録することで、容易に管理することができる。

## 5 おわりに

本稿では、ディレクトリサービスのセキュリティ機能に着目し、分散システムにおける否認不可サービスの実現への適用可能性を検討した。実世界における運用で使用するためには、マスターディレクトリを運営する第三者機関の設立や、訴訟問題に発展した場合の法律の制定などが必要となる。今後は、具体的な実現メカニズムやディレクトリスキーマについて検討する予定である。

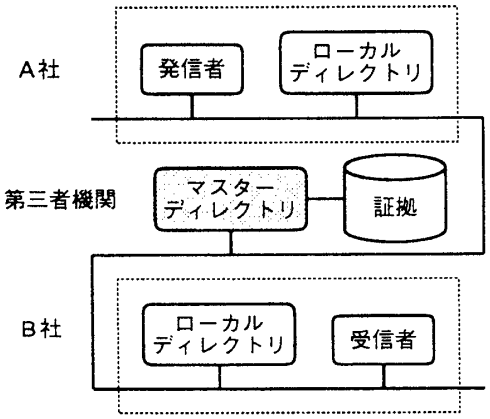


図2 マスターディレクトリ = TTP

## 参考文献

[1] ISO/IEC DIS 10181-4 : Security Framework in Open Systems - Part 4: Non-Repudiation, (1994).

[2] ISO/IEC 9594-1~9 : The Directory, (1993).

[3] OSF : Introduction to OSF $^{TM}$ DCE, (1992).