

ディレクトリプロトコルの拡張提案と

5 N-8

運用上の検討課題について

宮内直人、中川路哲男、勝山光太郎、水野忠則

三菱電機(株) 情報電子研究所

1. はじめに

OSI(Open Systems Interconnection)の普及、発展に伴い、各種の応用層プロトコルの標準化も順調に進み、各地で実装が試みられている。ISOやCCITTでは、OSIの応用層サービスの中にネットワーク管理サービスの一つとして、ディレクトリサービスを標準化している^[1]。ディレクトリは、1989年にIS(International Standard)化されたが、実際にディレクトリを構築し運用するためには、幾つかの問題が残っている。本報告では、ディレクトリシステムの構築、運用の際の問題点と解決方法を提案する。

2. ディレクトリの概要

ディレクトリは、ネットワークの構成要素の物理的な位置等の情報を管理するサービスであり、ディレクトリ情報の照会、変更、追加、削除の機能を提供する。

図1にディレクトリのモデルを示す。図1に示すように、ディレクトリは、次の3つの部分から構成される。

(1)DUA(Directory User Agent)

DUAは、ディレクトリ情報にアクセスする応用プロセスである。ユーザがディレクトリを利用するための窓口としての役割を果たす。

(2)DSA(Directory System Agent)

DSAは、ディレクトリサービスを提供する応用プロセスである。DUAから要求されたオペレーションを、DIBにアクセスすることによって処理する。

(3)DIB(Directory Information Base)

ディレクトリサービスを提供するために、必要な情報を持つ各エンティティのアドレス情報等を格納するデータベースである。

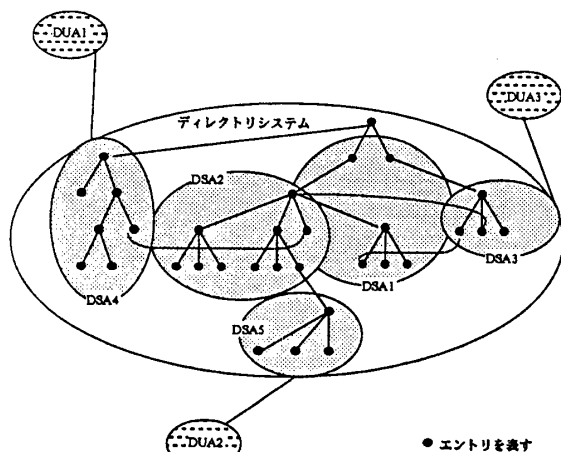


図1: ディレクトリシステムのモデル

ディレクトリの用意するオペレーションの種類は、基本的には次の11種類である。

アソシエーション関係

DirectoryBind, DirectoryUnbind

問合せ関係

Read, Compare, Abandon, List, Search

更新関係

AddEntry, RemoveEntry, ModifyEntry, ModifyRDN

これらのオペレーションに加えて、分散ディレクトリのオペレーションが11種類ある。

アソシエーション関係

DSABind, DSAUnbind

問合せ関係

chainedRead, chainedCompare, chainedAbandon, chainedList, chainedSearch

更新関係

chainedAddEntry, chainedRemoveEntry, chainedModifyEntry, chainedModifyRDN

3. ディレクトリの運用上の問題点と解決案

現在のISは、基本的な操作を行なう上では、ほとんど不足がない。しかし、実際にディレクトリを運用するためには、幾つかの問題点があると考えられる。ここでは、集中型と分散型に分けて、運用上の問題点について考察し、その解決案を示す。

3.1. 集中型・分散型に共通な問題

(1)アクセス制御の問題

現在のISは、認証方法として、簡易認証と強認証の2種類を規定しているが、一度認証をパスしてしまうと、読み出しも書き換えも可能になってしまう。また、特定のエントリに関する読みだし、書き換えなどにも配慮がない。アクセス制御に関しては、後述するように、ISの補遺として標準化作業が行なわれているが、作業が完了するまでの当面の対策として、次の方法が考えられる。

アクセス権を含んだ認証を行なう。すなわち、ユーザにパスワードを登録させる際に、エントリへのアクセス権も登録させる。DSAは、ユーザの名前によって、エントリへのアクセス権を判断することができる。しかし、この方法では、エントリが変更された時や追加された場合など、動的なアクセス権を用意することができない。

(2)検索する名前問題

現在のISでは、ユーザフレンドリな名前から、マシン依存の名前を検索、更新することはできるが、その逆をするためには、複数の操作が必要になる。

(3)更新系に関する一括操作の問題

現在のISでは、一回の更新系の操作で、一括削除、一括修正をすることができない。例えば、現在は leaf-entry のみに削除操作が決められているが、あるエントリの下すべてを削除したり、あるDSAの管理しているすべてのエントリを削除したいという要求が出てくると考えられる。

当面の対策としては、DUAを使うアプリケーションプログラムに一括更新の操作を吸収させる方法がある（DUAに対して、複数回の更新操作を行なう）。しかし、基本標準に、このような操作を認める操作を用意すべきかもしれない。

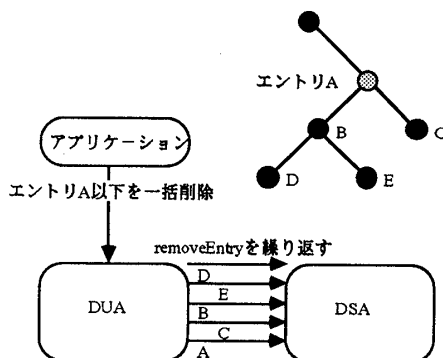


図2: エントリの一括削除の例

(4)操作する名前の問題

現在のISでは、操作を行なう対象となるエントリは、名前によって表されている。しかし、名前として使用すべき属性に関する定義がない（付録には、記述されているが、標準の一部になっていない）。例えば、組織単位クラスに属するエントリに対して操作を行なう時、組織単位クラスの組織単位名属性を指定して操作を行なうのが自然だと思うが、現在の標準では、組織単位クラスのその他の属性を指定しても構わないように見える。

運用する際には、運用前に、操作するエントリの名前の基準を決定し、その他の属性での操作を認めない、等の考慮が必要である。表1に、操作するエントリの名前の基準案を示す。

表1: 操作の際に指定するエントリ名の属性 (案)

対象クラス	操作の際指定する名前の属性
国	国名
組織	組織名
組織単位	組織単位名
地域	地域名
人	人名

なお、新たに登録するクラスについても、同様の基準が必要である。（ただし、DSA側では、基本的には、ISに書かれているすべての属性に関して、操作できなければならない）

また、異なるオブジェクトクラスに同一の属性値が含まれる場合（CommonName属性など）、どのクラスの名前なのか判定できないという問題もある。

3.2. 分散型に特有な問題

(1)更新操作のサポートに関わる問題

ディレクトリでは、理論的に1つのDIBを複数のDSAが管理している。エントリを更新（特に追加）する場合、どのDSAを操作対象とするか考慮すべきである。例えば、

AddEntryによって、エントリを加える場合、どのDSAにエントリを加えるかという問題がある。すべての追加エントリを、親エントリと同じDSAに加えるという方法もあるが、運用・管理の容易さを考慮すると、最良の方法ではない。

対策としては、エントリのクラスによってDSAを決める、等が考えられる。

(2)知識の問題

現在のISでは、各DSAが、お互いのエントリに関する情報の一部を知識として保持している。しかし、更新操作が行なわれる際に、知識を変更する手段を用意していない。この場合、知識と実際の情報に不整合が生じる。エントリに関する更新が行なわれた時に、更新情報をブロードキャストするような機構が必要かも知れない。

(3)コピーエントリの問題

現在のISでは、異なるDSAで、同一の情報（コピーエントリ）を持つことが認められているが、知識としてどのDSAの情報を持つか、あるいは更新を行なう際に、その他のコピーも更新されるかどうかは、インプリメントマターとなっている。これらのことを放置すると、運用・管理上混乱を生じる恐れがある。

対策としては、次のことが考えられる。

コピーエントリの所在（どのDSAが管理しているか）がわかっているならば、コピーとオリジナルの差は、ほとんど意味がない。従って、知識としては、オリジナル/コピーのどちらを保持してもよい。オリジナルかコピーのいずれかに更新操作が行なわれる時は、更新操作の結果を返す前に、認識しているすべてのコピー（あるいはオリジナル）に対して、同様の更新操作を発行して、結果を待つ。認識しているオリジナルとコピーから応答が到着した時点で、DUAに対して応答を返す。

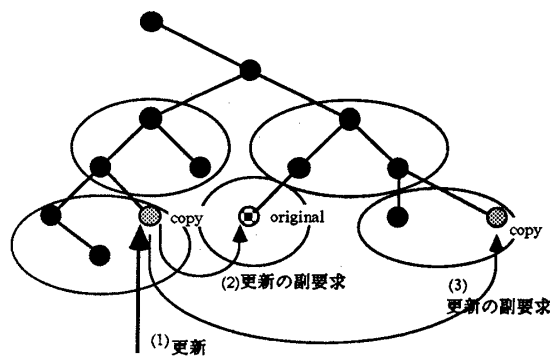


図3: コピーエントリの更新例

4. おわりに

ディレクトリの運用に関する問題点と、その解決方法の提案を行なった。

なお、ディレクトリの標準化作業は、大筋で終了しているが、細かな部分では、標準の補遺に関する作業が進行している。補遺に関する作業項目としては、複製情報の分散管理方法、アクセス制御、ディレクトリが保持する情報を更新する際の手順の規定、（現在の標準は、情報の一部を更新するにとどめている。）及びより短い、あるいはより多くのユーザフレンドリーな名前形式のサポートなどがあり、1992年の完成を目指して作業が行なわれている。

参考文献

- [1]ISO-9594 The Directory (1989).