5S－02

メタディレクトリシステムにおける同期アーキテクチャの開発

志賀賢太†，川上順彦†，平島陽子†，菊地聡†，由井仁‡
†(株)日立製作所 システム開発研究所
‡(株)日立製作所 ソフトウェア事業部

1. はじめに

昨今，LDAP (Lightweight Directory Access Protocol)[1][2]が，ディレクトリアクセスプロトコルのインターネット標準として定着し，高信頼化技術[3]などの研究開発も行われている．

一方，企業情報システムにおける TCO (Total Cost of Ownership)削減を目的とし，従来，個別に運用管理されていた各種アプリケーション(以下，AP と記す)の資源情報を，ディレクトリサービスを用いて一元管理するメタディレクトリシステムが注目されている．

そこで筆者らは，LDAP を用いたメタディレクトリシステムである JP1/User Administration (以下，JP1/UA と記す)を開発した．JP1/UA は，AP のユーザアカウントの追加・削除，及び AP に依存しない共通情報(ex.電話番号，パスワード)の変更を一元化するため，メタディレクトリに対する更新を AP へ自動反映するディレクトリ同期機能を備える．

本稿では，JP1/UA の拡張性・汎用性に富むディレクトリ同期アーキテクチャ，及び組織階層情報の管理を一元化するスキーマ変換について述べる．

2. メタディレクトリのスキーマ

JP1/UA におけるメタディレクトリのデータ構造(スキーマ)の特長を図 1に示す．

(1) AP 資源情報格納方式

一般的なディレクトリ情報(ex.メールアドレス)と，AP 資源情報を異なるエントリに格納し，さらに同一資源を表すエントリを同種リンクにより関連付ける方式を採用(一般情報，及び AP 資源情報を格納するエントリを，各々共通エントリ，固有エントリと呼ぶ)．本方式の場合，共通エントリに複数の固有エントリを関連付けることが可能なため，同一 AP に複数アカウントを持つユーザの登録等，様々なニーズに対応可．

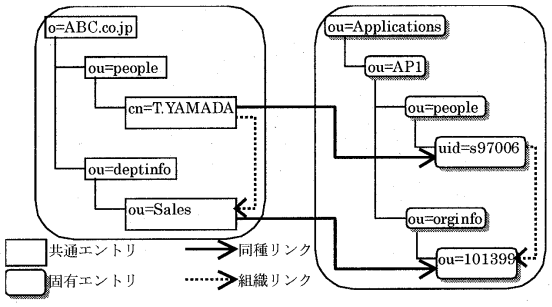

図 1 メタディレクトリのスキーマの特長

(2) エントリ配置方式

従来，組織階層に従ってツリー状に配置していたエントリを種別毎に並列配置し，さらにユーザと所属組織，及び組織と上位組織を組織リンクにより関連付ける方式を採用．本方式の場合，エントリの識別名である DN (Distinguished Name)が組織階層の変更に関わらず一定であるため，従来はユーザ情報の移動(削除・追加)が必要であった人事異動に，組織リンクの変更のみで対応可．

3. 開発目標

多種多様な AP 資源情報を一元管理するには，固有エントリの更新を AP へ反映すると共に，共通，及び固有エントリに格納される共通情報を単一操作で更新可能にするディレクトリ同期機能が必要となる．本機能の開発目標は以下の通りである．

(1) 新規導入される AP に迅速に対応可能なように，高い拡張性・汎用性を確保する．

(2) 共通情報である組織階層情報は，従来，複数 AP にて重複管理されており，組織改正や人事

Development of Synchronization Architecture on Meta-Directory System
Kenta Shiga†, Norihiko Kawakami†, Youko Hirashima†, Satoshi Kikuchi†, Hitoshi Yui‡
†Systems Development Laboratory,Hitachi,Ltd.
‡Software Division,Hitachi,Ltd.

異動時の更新作業が膨大であった．そこで，組織階層情報の一元管理を実現する．

4. ディレクトリ同期アーキテクチャ

ディレクトリ同期機能のアーキテクチャを図 2に示す．3章(1)の目標を達成するため，本機能を，AP 非依存の処理を行う共通同期処理部とスキーマ変換部，各 AP 固有の処理を行う固有同期処理部に分割した．以下，各モジュールの動作を説明する．

(1) 共通同期処理部

固有エントリ更新時は，その更新を対応する固有同期処理部へディスパッチする．一方，共通エントリ更新時は，その更新を固有エントリの更新へスキーマ変換した上でディスパッチする．

(2) スキーマ変換部

前述のスキーマ変換処理を実行する．筆者らは，単純な文字列操作(コピー，結合，分割等)の組合わせで，多種多様なスキーマ変換に対応可能なことに着目し，文字列操作の実行モジュールを部品化し部品の組合わせをスキーマ変換規則にて定義可能とすることで，スキーマ変換部を汎用化した．

(3) 固有同期処理部

固有エントリの更新内容の文法チェック，及び更新内容に基づいたAPのDB更新処理を実行する．管理対象AP毎にプラグイン可能である．

上記のアーキテクチャにより，APの新規導入に固有同期処理部の開発のみで対応可能となり，高い拡張性・汎用性を確保した．

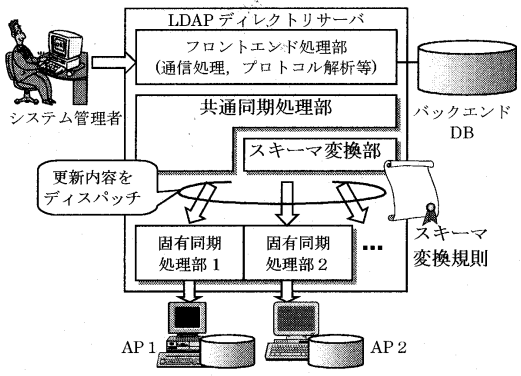

図 2 ディレクトリ同期アーキテクチャ

5. 組織階層情報の一元管理

3章(2)の目標の達成には，組織リンクに関するスキーマ変換が必要である．ここで，組織リンクは組織エントリのDNをユーザエントリ等に格納することで表すため，上記スキーマ変換には，同一組織を表す共通ー固有エントリ間のDN変換が必要である．しかし，両エントリのDNの命名規則が異なるため，コピー等の文字列操作ではDN変換に対応できない．

そこで，同一組織を表す共通エントリと固有エントリが同種リンクにより関連付けられることに着目したDN変換方式を開発した．

本方式の処理概要を図 3に示す．本方式では，LDAPの検索機能を使用し，組織を表す共通エントリ，及びそれと同種リンクにより関連付けられている固有エントリを探索する事でDN変換を実現した．

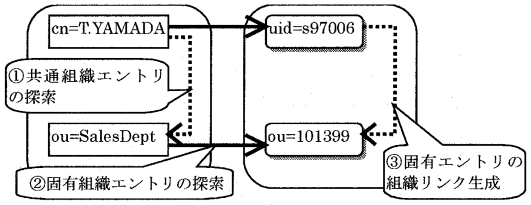

図 3 DN 変換方式の処理概要

6. おわりに

本稿では，メタディレクトリシステムJP1/UAにおける拡張性・汎用性に富む同期アーキテクチャ，及び組織階層情報を一元管理可能なスキーマ変換機能について述べた．今後，ディレクトリ同期処理の並列化による性能向上などを行う予定である．

参考文献

[1] Wahl,M.他 : Lightweight Directory Access Protocol (v3), RFC2251 (1997)

[2] Howes,T. 他 : A Scalable, Deployable, Directory Service Framework for the Internet : INET'95 (1995)

[3] 菊地他 : 基幹システムにおける高信頼ディレクトリ・サーバ，情報処理学会研究報告分散システム運用技術，97-DSM-7 (1997)