ＬＤＡＰディレクトリを活用した業務運用管理システムの開発

1Ｐ－4

原田 道明*　小林 康祐**　三宅 純一**　坪井 克弘***

*三菱電機(株) 情報技術総合研究所　**三菱電機(株) 電力情報システム技術センター
***中部電力(株) 情報システム部

1. 序

企業等の業務運用において、システム構築基盤の異種性・分散化に伴う管理情報の分断化と管理の複雑化が問題となっている。LDAP[1]プロトコルの出現を契機に普及の進むディレクトリ技術は管理情報の統合に有効だが、OS・WWW・電子メール等に応用先が限定されていて業務運用管理に十分な管理情報を持たないのが現状である。

筆者らは職制情報や業務システムの展開配置等、企業等の業務システム運用に向けて詳細化された管理情報スキーマと、認証／アクセス制御・業務起動制御機能のプロトタイプ開発を行った。人事異動・組織改正や指名業務・代行業務を考慮して流動的な業務環境に対応できる柔軟性、業務サーバ等の配置構成に対する位置透過性が特徴である。

2. システム構成

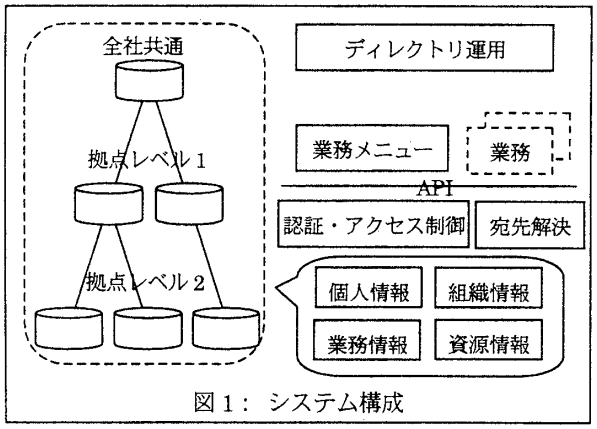

図１：システム構成

(1) ディレクトリ

既存の LDAP 対応ディレクトリ製品を活用し、スキーマを拡張して下記の情報を格納した。

- 組織情報

  組織階層に沿った DIT(Directory Information Tree)に組織単位・職位の構成情報を格納する。

- 個人情報

  個人の認証情報・資格・勤務形態等の属性や、所属先との関連付けを格納する。

- 業務情報

  業務アプリケーションのアクセス権情報、配置情報、起動条件等の属性を格納する。

- 資源情報

  DNS 階層に沿った DIT にサーバ・プリンタ・端末等の構成情報を格納する。また、拠点・フロアへの配置情報も格納する。

(2) 業務メニューGUI

エンドユーザが使用する GUI。個人の職務権限に応じた業務の表示・起動を行う。

- ログイン機能

  個人認証と、アクセス制御に用いる個人属性・端末属性の取得を行う。

- 業務メニュー表示機能

  個人・端末属性に応じて許可される業務の一覧をメニュー表示する。

- 業務起動制御機能

  メニュー上で選択した業務の適切なサーバ、起動パラメータを決定して起動する。

(3) 業務アプリケーション向け API

管理機能の組込み容易性や機能拡張に対する保守性を考慮し、認証・アクセス制御処理、および宛先解決処理に対する API を提供する。

(4) ディレクトリ運用機能

データ運用に必要な機能を提供する。

- データエントリ
- 汎用計算機からの人事情報の取込み支援
- 端末系 OS とのアカウント情報の同期

Development of Business System Management Facility with LDAP Directory by HARADA Michiaki*, KOBAYASHI Yasumasa**, MIYAKE Junichi** & TSUBOI Katsuhiro***
*Information Technology R&D Center, Mitsubishi Electric Corp.
**Information Systems Engineering Center, Power & Industrial Systems Group, Mitsubishi Electric Corp.
***Information Systems Dept., Chubu Electric Power Co., Inc.

3. 分散データ配置

1～2万端末の大規模組織への適用を想定し、管理効率・性能を考慮して以下のデータ配置とした。

- 個人情報・組織情報・業務情報

全社共通ＤＢをマスタとして一元管理する。負荷対策のため各拠点に複製を配する。

- 資源情報

資源構成を即時反映するため、各拠点をマスタとして全拠点で単一のDITを構成する。

4. 認証／アクセス制御

(1) アクセス制御方式

- 制御手順

ユーザ認証時に個人・端末の属性情報を含むログイン文脈情報を生成し、業務情報のACL (アクセス制御リスト)と照合する。ACLは (個人の職位レベル>= 部長)といった属性照合式による許可／拒否対象者の指定の並びで与えられる。

- アクセス制御属性の拡張

ディレクトリの組織情報・資源情報を用いて得られる派生属性（個人の担当職位や所属先組織単位の属性、端末の所属ドメイン・フロア等の属性）の検索処理を追加することで、アクセス制御に用いる属性を容易に追加できる。

(2) アクセス制御のための組織情報モデル

個人情報・組織情報の概要を図2に示す。

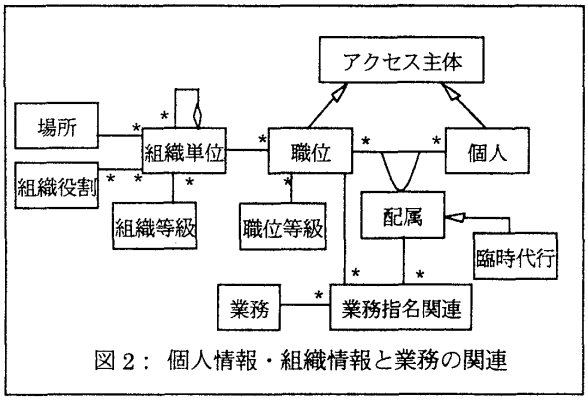

図2： 個人情報・組織情報と業務の関連

- 人事異動・組織改正の考慮

職位や職位等級（部長・課長等）・組織単位・役割（人事部門・技術部門等）を用いて記述したACLは人事異動に際して修正不要である。さらに、個人エントリはDIT上で組織単位の配下に配置せずフラットに配置し、配属を用いて組織単位と関連付けることで、人事異動・組織改正に対して個人エントリの識別名を修正不要とした。

- 指名代行業務等への対応

実業務では上長が一定の担当者に特定の業務を委任する場合がしばしばある。図中の業務指名関連クラスは業務・委任元職位・委任先個人を関連付けて上記の関係を表現する。また、上長不在時の臨時代行の権限は、配属クラスに「臨時代行」というサブクラスを持たせて表現する。

5. 業務起動制御

業務情報・資源情報は印刷・業務サーバの宛先決定、S/W配布等に活用できる。今回は業務起動時のサーバ宛先・起動パラメータ決定を実装した。

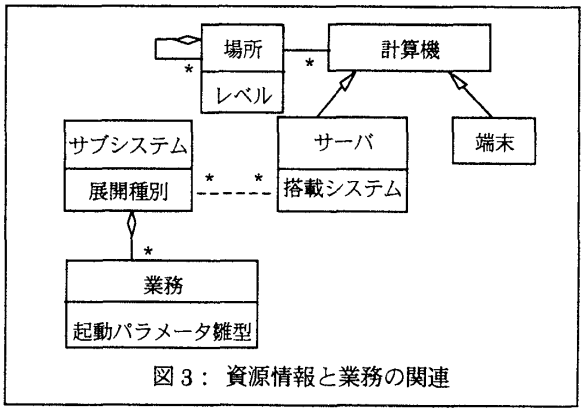

図3： 資源情報と業務の関連

業務のサーバへの展開は全社に1台・拠点毎・フロア毎・部署毎に1台、といった少数のパターンに帰着される。端末の所在・個人の配属先、起動対象業務の展開種別を照合してサーバを決定し位置透過性を実現する。業務の起動パラメータは端末・ユーザ属性を埋め込んだパラメータ雛型を用いて決定する。社員番号・端末ＩＤ等・所属等の情報を動的に起動パラメータに反映する。

6. まとめ

LDAPディレクトリを用いた業務システム管理向けの認証・アクセス制御・業務起動制御方法の実現例を示した。今後、実システム適用を通じて性能・信頼性・運用効率の評価・改善を行う。

参考文献

[1] RFC2251, Lightweight Directory Access Protocol (v3)