ディレクトリベース認証システム

4L－04

三菱電機株式会社 情報通信システム開発センター
石井 洋，五月女 健治，大沼 聡久，三浦 健次郎，小宮 崇，森本 和成
代表 hishii@icc.melco.co.jp

1．はじめに

今日、インターネット上の大手検索サイトや大手プロバイダサイトなどはインターネット上に散らばる膨大な情報の玄関的な役割を果たし、『ポータル』と呼ばれている。

近年、企業でも企業内に散在するイントラネット/エクストラネットシステム、レガシーシステムなどの入口として『企業ポータル』が構築されるようになってきた。

当社では、ディレクトリDBを用いた企業ポータルシステムをいくつか構築してきた経験を生かし、Web 業務に特化した横展開が可能な標準システムを構築した。

本稿では、この標準システムの機能・特徴について報告する。

2．機能

当社で手がけた企業ポータルに対する客先要件を下記にあげる。

①認証
ID/PASSWORD あるいは認証書による認証を行う

②シングルサインオン
ポータルで1度認証した後は、業務アプリケーション利用時には認証情報の入力を行わない

③アクセス制御
利用者の権限を判定して、アプリケーションの使用を制限する

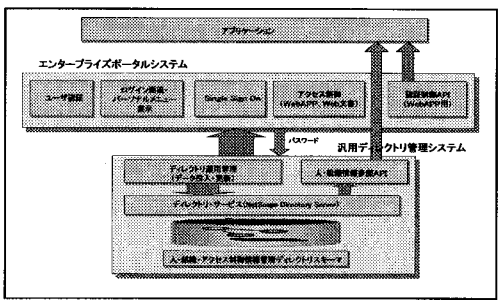

図1 機能構成

④パーソナルメニュー表示
利用者の使用できる業務メニュー情報だけを表示する

⑤共通情報の一元化
利用者情報、組織情報などの共通情報を企業ポータルで一元的に管理を行い、業務アプリケーションは必要に応じて情報を取得する

これらの客先要件をもとに必要機能の選定を行い、標準システムの構築を行った。

3．システム実現方式

図2に標準システム構成を示す。今回の開発部分は網掛けの部分である。

標準システムはイントラでの利用だけではなく、社外からのアクセスも想定し、その通信は

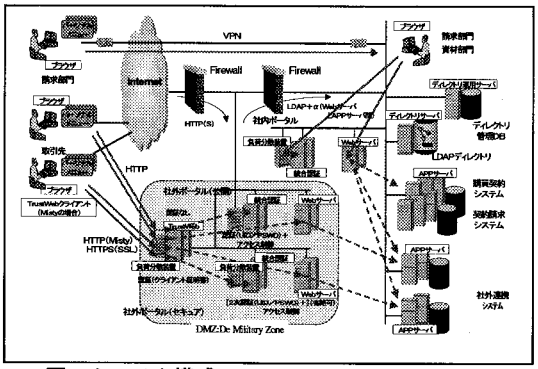

図2 システム構成

MISTY による暗号化通信（既存パッケージ：「TrustWeb」を使用）を行う。

認証は、利用者が入力したID/PASSWORDをディレクトリに問合せることで行う。

シングルサインオンは、ポータルから業務アプリケーション起動時に共通鍵によるワンタイムチケットが発行され、業務アプリケーションはこのチケットによって利用者が認証済みかどうかを判定する。同時に利用者情報を取得する時にもチケットを使用する。

The Standard Enterprise Portal And Authentication System Using The Directory Database
Hiroshi ISHII, Kenji SAOTOME, Akihisa OONUMA,Takashi KOMIYA,Kazunari MORIMOTO
Information & Communication Systems Development Center, MITSUBISHI ELECTRIC CORPORATION

アクセス制御は、ディレクトリに格納された業務アプリケーションACL情報から実行権限を判断し、権限を持たないアプリケーションは起動できない。ACLには、利用者ID・利用者役職・利用者社員区分・所属組織・定義グループを組合せた条件を設定することが可能である。

パーソナルメニューは、利用者が利用可能なメニューのみを表示する。

共有情報の一元化は、業務システムで各々抱えていた利用者や組織情報をポータルで一元管理することにより運用負荷を軽減する。

4．本標準システムの特徴

本標準システムの最大の特徴は、下記にあげる2点である。

①独自設計のディレクトリスキーマ構造

②ディレクトリ情報取得ＡＰＩ

図3に組織・利用者情報のスキーマ概略構造図を示す。

組織クラスは実際の企業内の組織階層をそのままの形で格納している。(他のパッケージ製品は横並びに格納している。) また、利用者クラスは横並びに格納されている。

組織クラスには役職クラスが、利用者クラスには配属クラスが複数ぶら下がり、それぞれのオブジェクトが相互にリンクされている。

このような構造をとることにより、下記のメリットがある。

①組織から利用者が、利用者から組織が相互にたどれる。

②配属/役職クラスを持たせることで、本務/兼務/代理などの配属状態に対応可能。加えて、配属先での利用者の役職を表現することが可能。

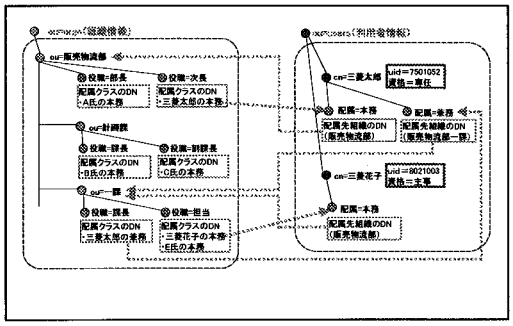

図3 組織情報と利用者情報

③配属/役職クラスを増やしたことによる（人事異動時などの）運用負荷はほとんど変わらない。

次に、表1にディレクトリ情報取得ＡＰＩの概要機能を示す。

表1 情報取得ＡＰＩの機能

No	機能名	説明
1	認証情報取得	認証の確認
2	個人情報取得	利用者に関する情報 名前,資格,Email等
3	配属情報取得	組織が持つすべての属性情報
4	組織情報取得	組織が持つすべての属性情報
5	組織単位情報取得	組織が持つすべての属性情報
6	役職情報取得	組織がもつすべての役職の情報
7	上位組織情報取得	基準組織の上組織
8	下位組織情報取得	基準組織の上組織

API を用意することにより下記のメリットがある。

①業務アプリケーションの開発者ははデータベースの種類や内部構造(スキーマやオブジェクトクラス)を意識することなくアプリケーションの開発が可能

②ディレクトリデータベースに API のスペック以上の検索オペレーションが発生しない。（例えば全情報検索など大負荷の操作が発生しない）

5．まとめ

現在、ある客先に本標準システムを適用し、システムを構築中である。システム適用により、個々の業務アプリケーションで認証機能と利用者情報管理機能を作成する必要が無くなり、全体の開発量は大幅に縮小される。

これと平行して本標準システムにワークフロー対応の機能拡張を行っている最中である。

また、今後はセキュアモバイル、バイオメトリックス認証、ドメインなどＷｅｂ業務以外をスコープに含めたシングルサインオンの拡大などを行い、機能を使い勝手を向上していく計画である。