LDAP入門 & 活用事例紹介

日本LDAPユーザ会

オープンソース・ソリューション・テクノロジ株式会社
http://www.osstech.co.jp/

技術取締役 武田 保真

2007年7月20日

講師紹介(TAKEDA Yasuma)

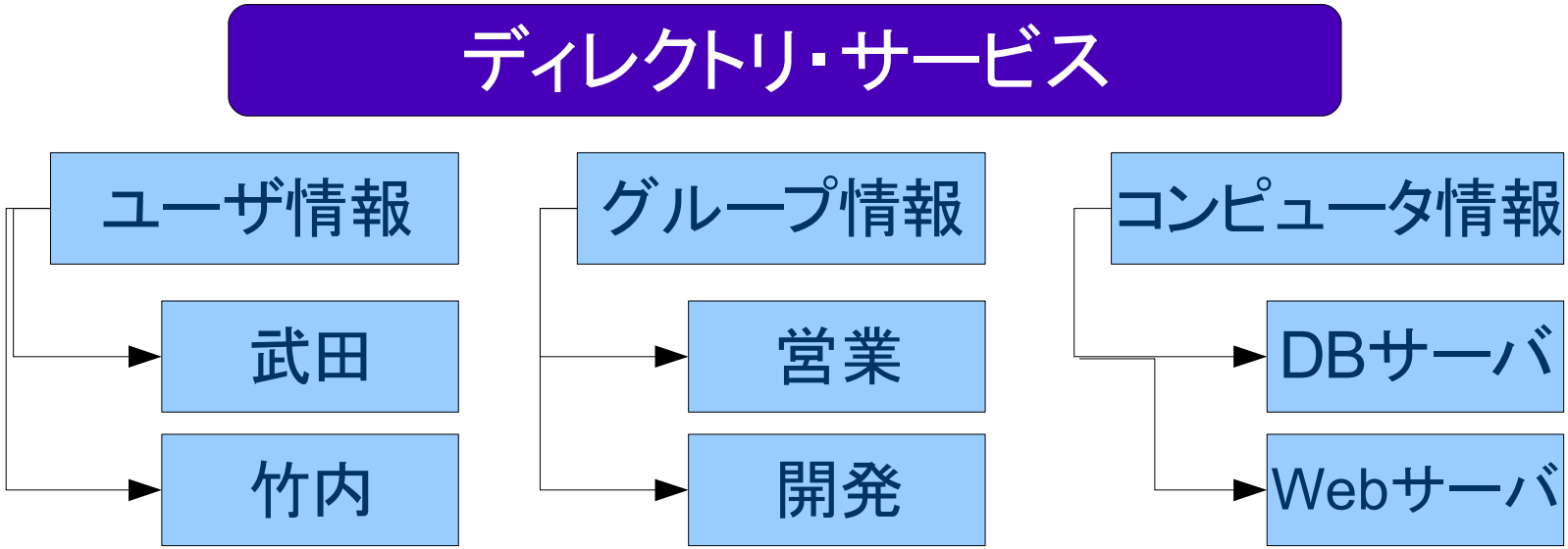
- 昨年 9月に オープンソース・ソリューション・テクノロジ(株)設立
  - Samba、LDAPを中心にOSSのソリューション提供
- 著書
  - 「徹底解説 Samba LDAPサーバ構築」 技術評論社
  - 「Linux RAID入門」 技術評論社
- 日経ITpro連載 Sambaウォッチ
  http://itpro.nikkeibp.co.jp/article/COLUMN/20070202/260584/

Part1

ディレクトリ・サービスとLDAP

ディレクトリ・サービスとは? 「Wikipediaより」

- ネットワーク上のユーザ情報、グループ情報、コンピュータ情報、アプリケーション、各種設定情報などを、記憶し、検索しやすいようにまとめたもの
- 情報の管理は、集中管理に限らず、分散環境での情報管理も可能

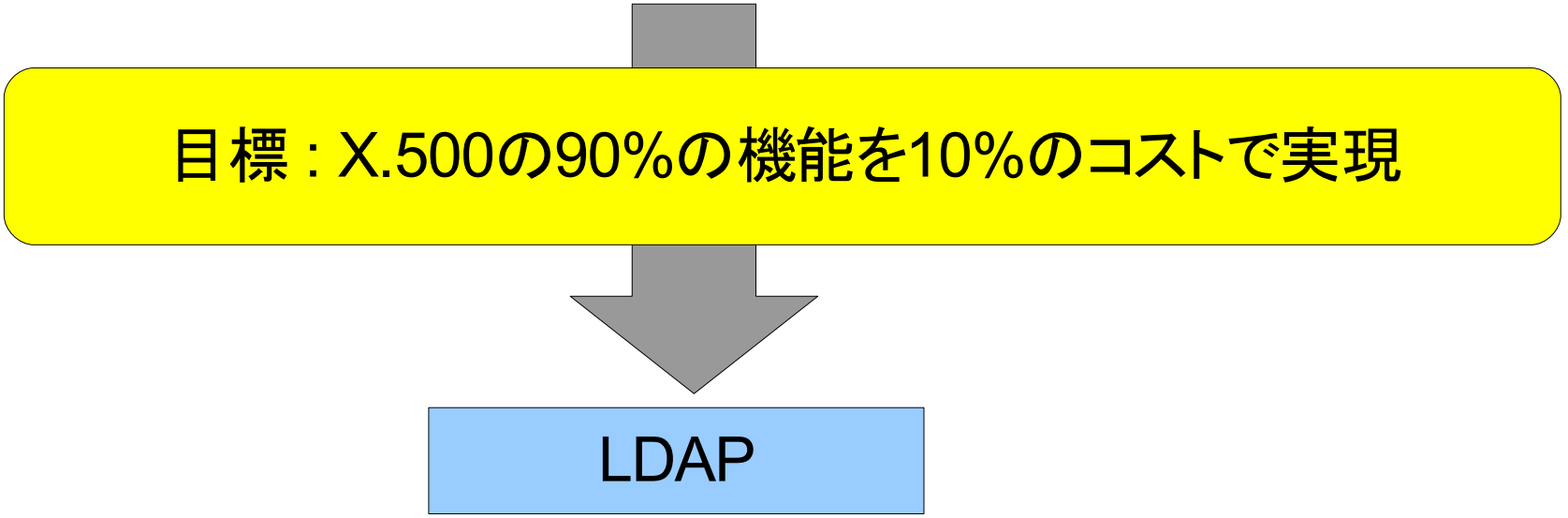


様々なディレクトリ・サービス

- ディレクトリ・サービスにアクセスするためのプロトコルを「DAP(Directory Access Protocol)」と呼ぶ
- LDAP以外のディレクトリ・サービスの例
  - NIS、NIS+、DNSなど
- ディレクトリ・サービスを提供する1990年代の商用アプリケーション
  - Novell Netware
  - Lotus Notes
  - MS Exchange
- これらのプロトコルは独自プロトコルで実装

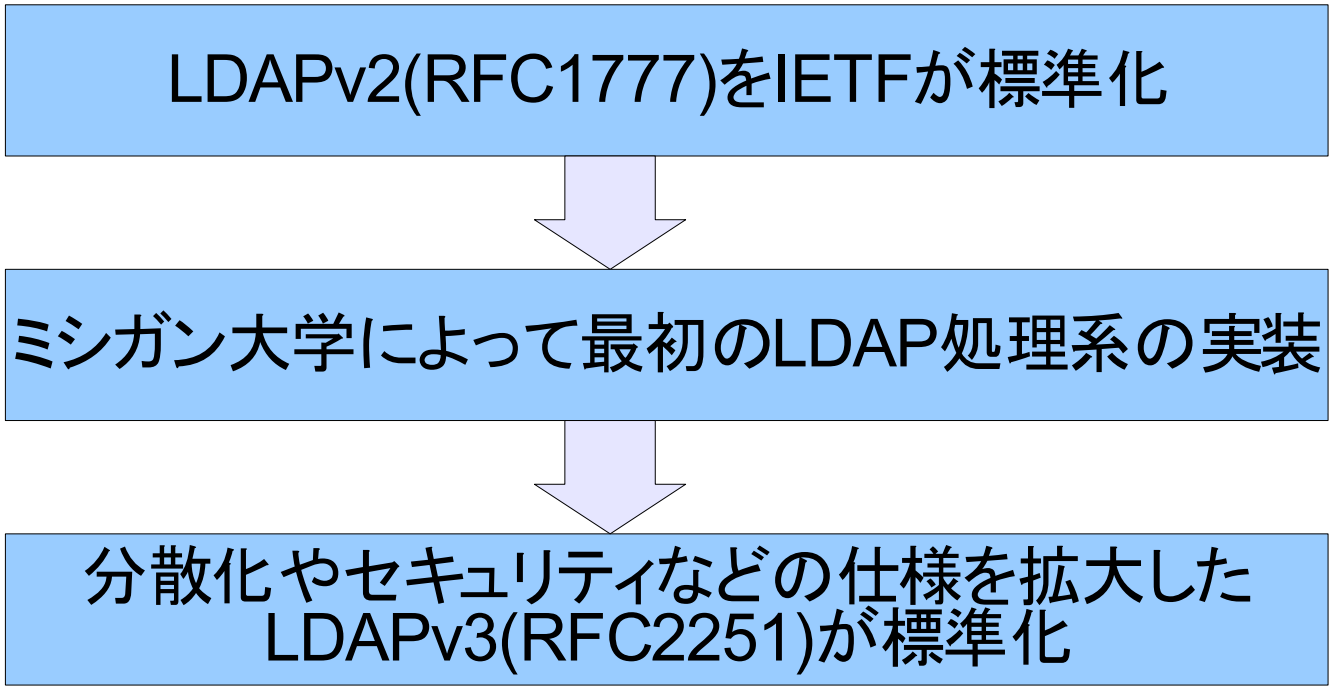
LDAPとは?

- LDAP(エルダップ:Lightweight Directory Access Protocol)
  - ディレクトリ・サービスに接続するためのプロトコル(DAP)の1つ
- ITU勧告 X.500モデルをサポートするディレクトリ・サービスにアクセスするためのプロトコルとして設計
- X.500モデルの実装は非常に困難だったため普及せず



LDAPの標準化

- コンピュータ・ネットワークの拡大に伴い、各種情報の統合管理の必要性が増加



商用LDAP製品

- Sun Java System Directory Server(サン・マイクロシステムズ)
- Active Directory(マイクロソフト)
- Tivoli Directory Server(IBM)
- Enterprise Directory Server(NEC)
- Oracle Internet Directory(オラクル)
- Info Directory(富士通)
- Novell eDirectory(Novell)
- RedHat Directory Server(レッドハット)

オープンソースのディレクトリサーバ

- OpenLDAP
  - ほとんどのOSで利用可能なLDAPスイート
    - RedHat, Debian, FreeBSD, Solaris、Windowsなど
  - http://www.openldap.org
- Fedora Directory Server
  - かつてのNetscape Directory Serverをレッドハットがオープンソース化
  - http://directory.fedoraproject.org
- OpenDS
  - サンが開発中のJavaベースのディレクトリ・サーバー
  - http://opends.dev.java.net

Part2

LDAPの基本概念

LDAPの基本アクセス

- アクセスの種類
  - エントリの追加　: ldapadd
  - エントリの削除　: ldapdelete
  - エントリの変更　: ldapmodify
  - エントリの検索　: ldapsearch
- LDIF(LDAP Data Interchange Format)形式
  - データ交換の基本フォーマット
  - テキストデータ : UTF-8
  - バイナリデータ : base64エンコーディング
  - 「属性 : データ」で1行

LDIFの例

- 1エントリの最初は、「dn : 識別名(Distinguished Name)
- 空白行でエントリの区切り

```
dn: dc=osstech,dc=co,dc=jp
objectClass: dcObject,organization
o: osstech
dc: osstech

dn: ou=Users,dc=osstech,dc=co,dc=jp
objectClass: top,organizationalUnit
ou: Users

dn: uid=Administrator,ou=Users,dc=osstech,dc=co,dc=jp
cn: Administrator
sn: Administrator
objectClass: top,person,organizationalPerson
objectClass: inetOrgPerson,posixAccount,shadowAccount
gidNumber: 0
uid: Administrator
uidNumber: 0
userPassword:: e1NTSEF9YTlCdFpmYVVVeTVLWUtSaWFWaFo=
homeDirectory: /home
```

LDAPとRDBMSの違い

- LDAP(プロトコル)とSQL(言語)
- ディレクトリサービスにはACID特性が無い
  - 書き込んだデータがすぐ読めるという保証は無い

	LDAP	RDBMS
用途	検索性能重視、更新には不向き	検索だけでなく更新も重視
構造	木構造	表構造(行と列)
スキーマ	登録済み既存スキーマを利用	データに合わせて設計
更新	トランザクションの概念無し	トランザクションの概念あり
分散	ツリーの枝単位で分散配置可能	キーの範囲で分散配置可能
操作	LDAPで操作、操作は単純	SQLで操作、複雑な操作も可能
検索	木の枝葉をたどる感じ	表の行を操作する感じ

LDAPで何が可能か?

- ユーザ情報の統合管理
  - Mailアドレス
  - パスワードの一元管理(FTP, SSH, Proxyなど)
- UnixとWindowsの認証統合(Samba + LDAP)
- Webサーバのアクセス制御
- 電話帳、メールアドレス帳(メールソフトなどから利用)
- PKI(公開キー)の保管

OpenLDAP標準スキーマ

- スキーマの定義を見ることで、どのような情報を格納可能か判別することができる
- core.schema
  - OpenLDAPのベースとなるスキーマ
    - RFC 2252/RFC 2256 (LDAPv3)
    - RFC 1274 (uid/dc)
    - RFC 2079 (URI)
    - RFC 2247 (dc/dcObject)
    - RFC 2587 (PKI)
    - RFC 2589 (Dynamic Directory Services
    - RFC 2377 (uidObject)
  - これらだけでは何もできないが、他のスキーマの基礎となる

各種スキーマ(1)

- cosine.schema
  - X.500やX.400で規定された各種アトリビュートの定義
    - RFC1274 : host, manager, DocumentIdentifier
    - DNSレコードを表すAレコード、MXレコード、NXレコード、SOAレコード、CNAMEレコードなど
      - これらを利用することでDNS情報の格納が可能]
- inetorgperson.schema
  - インターネット、特にメールアドレス帳に使われる属性の定義
    - メールアドレス、社員番号、オフィス、自宅住所、会社の電話番号、自宅の電話番号、写真など

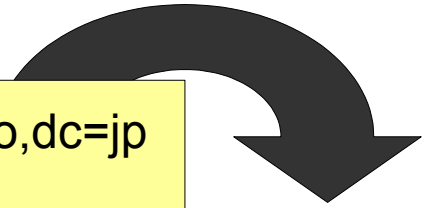
各種スキーマ(2)

- misc.schema
  - mailLocalAddressやnisMailAliasなどメールサーバ用の属性定義
- nis.schema
  - posixAccountやposixGroupなど、UNIXのユーザ認証統合に利用される情報の定義
  - NISをLDAPに置き換えるためのスキーマも含む
- samba.schema
  - Sambaによって提供されるスキーマ。Windows/Unixの認証統合に利用。

各種スキーマ(3)

- java.schema
  - javaClassName, javaCodeBaseなどJava Object (RFC 2713)を扱うためのスキーマ
- corba.schema
  - corbalor, corbaRepositoryIdなどCorba Object(RFC 2714)を扱うためのスキーマ

アドレス帳の構築例



dn: uid=ユーザ名, ou=Users, dc=ドメイン名,dc=co,dc=jp
objectClass: posixAccount
objectClass: inetOrgPerson
cn: ユーザ名
sn: 名字
givenname: 名前
mail: メールアドレス
o: 会社名
ou: 所属
title: 役職
employeeNumber: 社員番号
telephoneNumber: 電話番号
mobile: 携帯電話
st: 都道府県
l: 市区
street: 番地

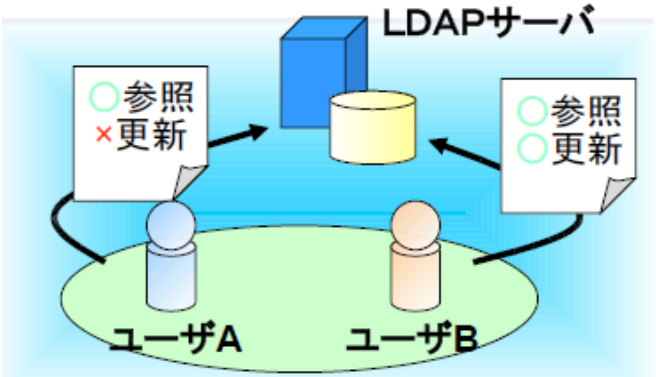
dn: uid=yasuma, ou=Users,dc=osstech,dc=co,dc=jp
objectClass: posixAccount
objectClass: inetOrgPerson
cn: yasuma
sn: 武田
givenname: 保真
mail: yasuma@osstech.co.jp
o: オープンソース・ソリューション・テクノロジ株式会社
ou: 技術部
title: 技術取締役
employeeNmber: 2
telephoneNumber: 03-xxxx-xxxx
mobile: 090-xxxx-xxxx
st: 東京都
l: 品川区西五反田
stree: 2-6-3

LDAPを利用する利点

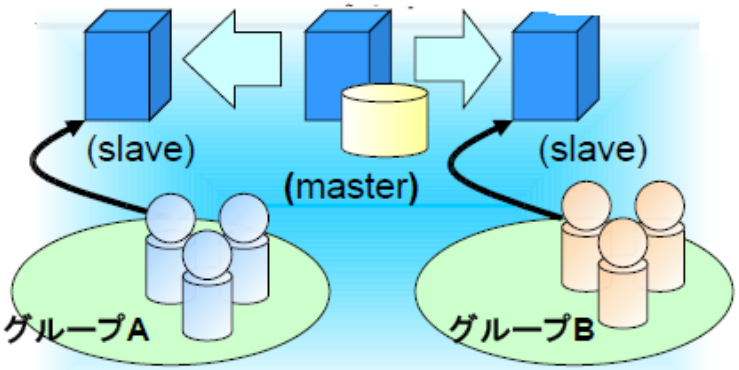
- 機能拡張性が高い
  - ユーザ情報の管理だけでなく、組織情報、コンピュータ、アプリケーションの管理、あるいはメール・アドレス帳、電話帳など様々な用途に拡張して利用可能
- 標準化による相互接続性の高さ
  - Unix、Linux、Windowsとプラットフォームを選ばない
- 性能に関しても拡張性が高い
  - 商用LDAP製品は数十億のデータ・エントリでも実運用に使える処理性能。オープンソース製品でも数千、数万エントリの実績多数
- アクセス制御によるセキュリティ確保
  - 通信の暗号化、ACIによるアクセス権の設定可能
- ディレクトリは木構造で、分散管理が可能
- 複製機能による可用性の確保

LDAP各機能の概念図

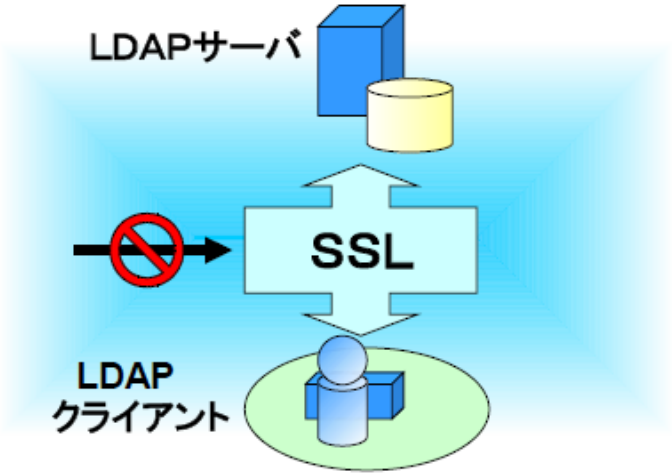
アクセス制御



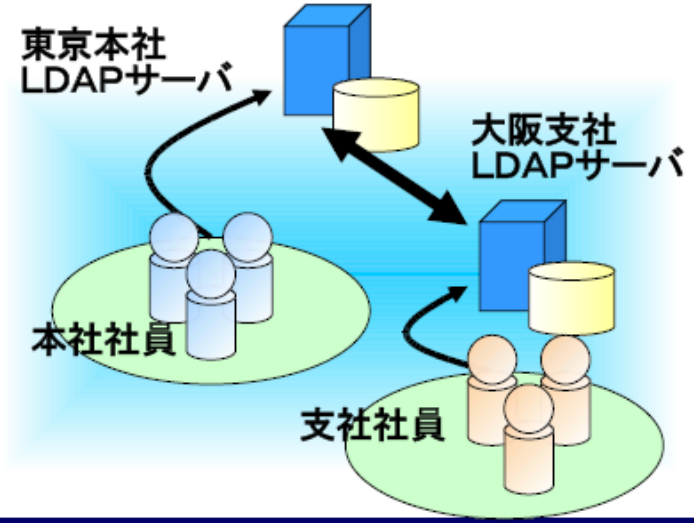
レプリケーション



通信経路暗号化



分散管理(referral)



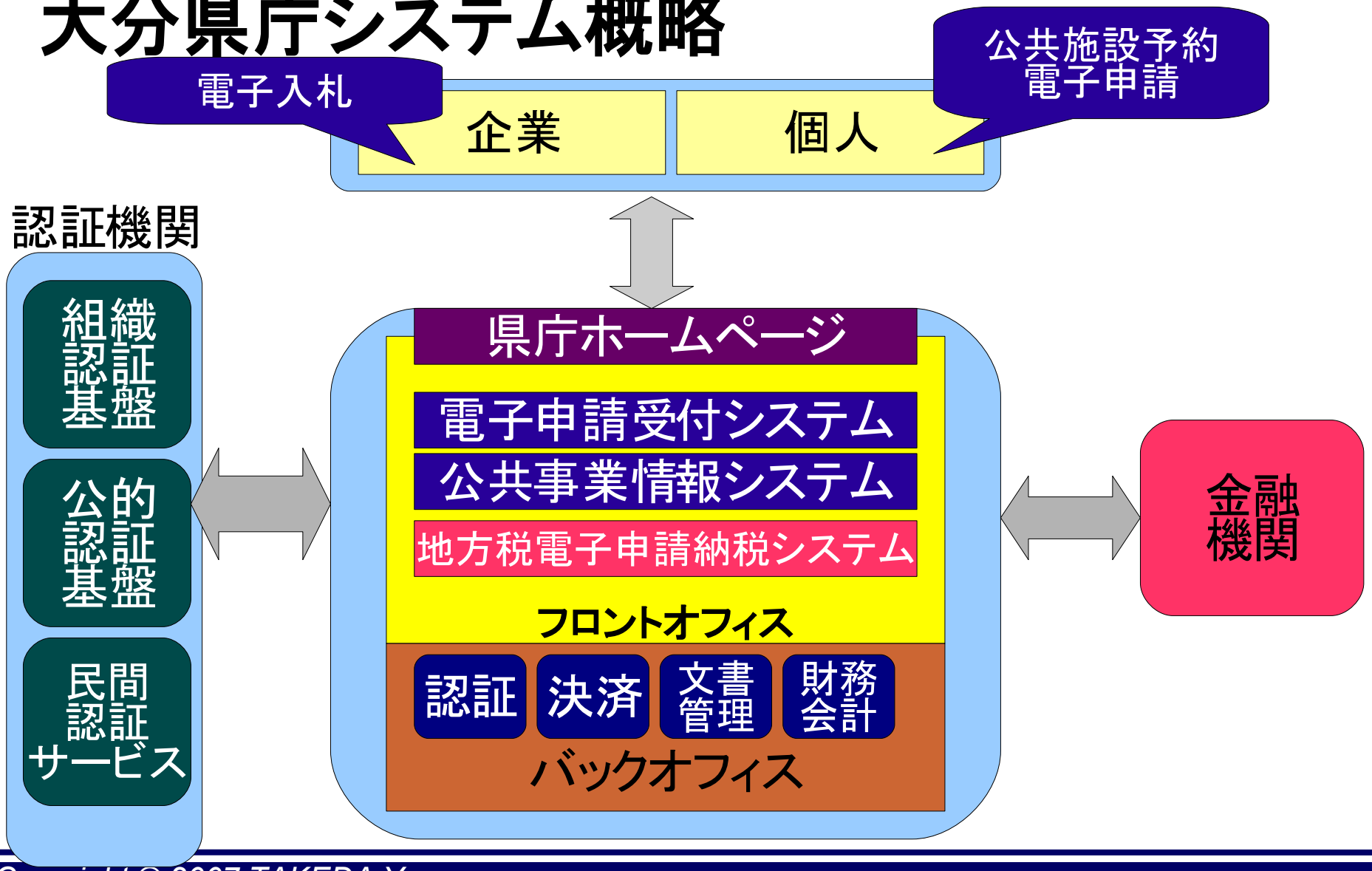
Part3

LDAP活用事例紹介

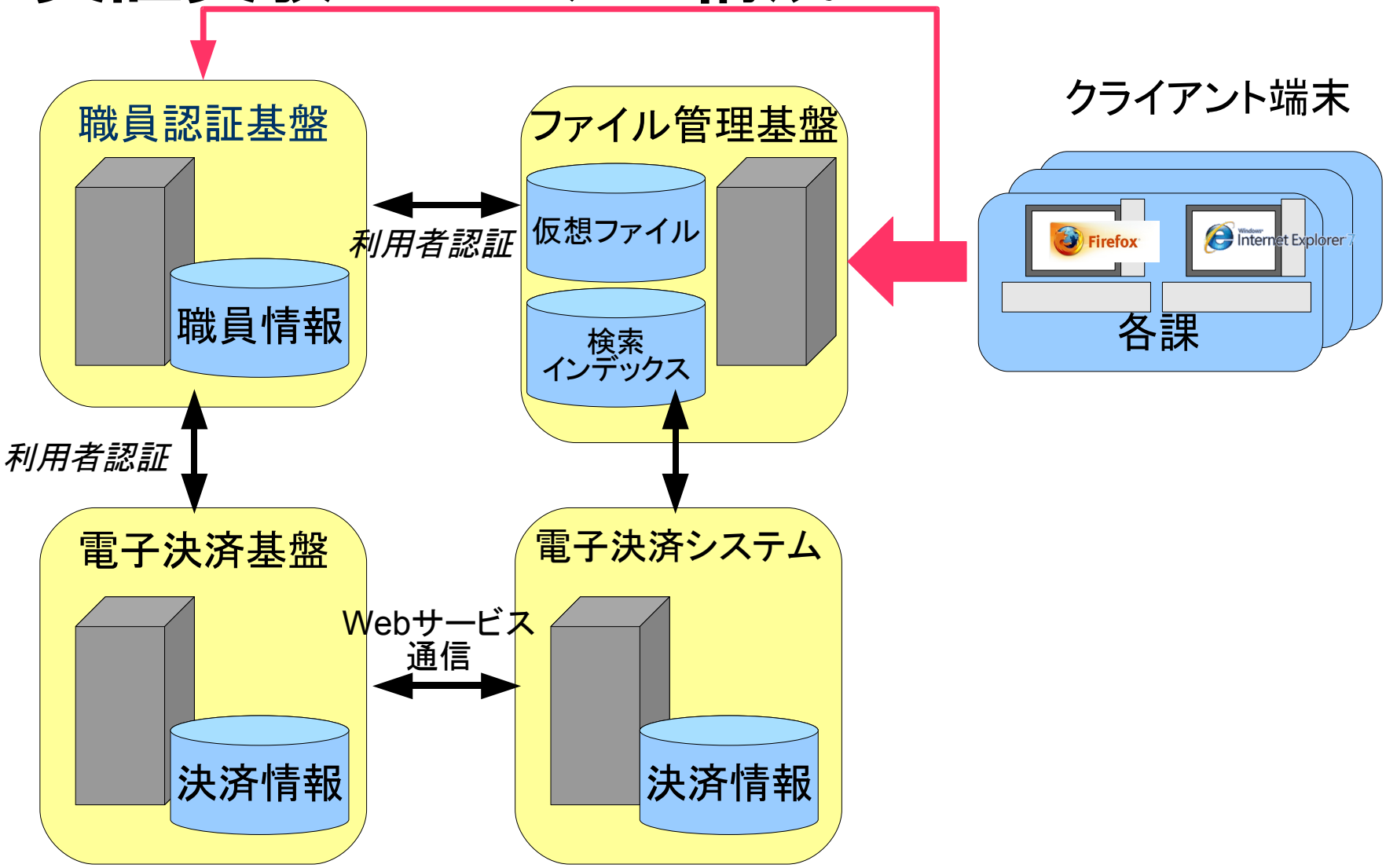
認証基盤構築事例

- IPA(独立行政法人 情報処理推進機構)の公募事業
  - 「自治体基盤システムでのOSS活用に向けての導入実証実験」
  - http://www.ipa.go.jp/software/open/ossc/2006/stc/jichitai2006.html
  - http://www.ipa.go.jp/software/open/ossc/2006/stc/report/oita.html
- 大分県庁の実証実験システム
  - システムの構築をOSSで推進できるか調査
  - 実証実験の対象
    - 職員認証基盤
    - 電子決済基盤
    - ファイル管理基盤

大分県庁システム概略



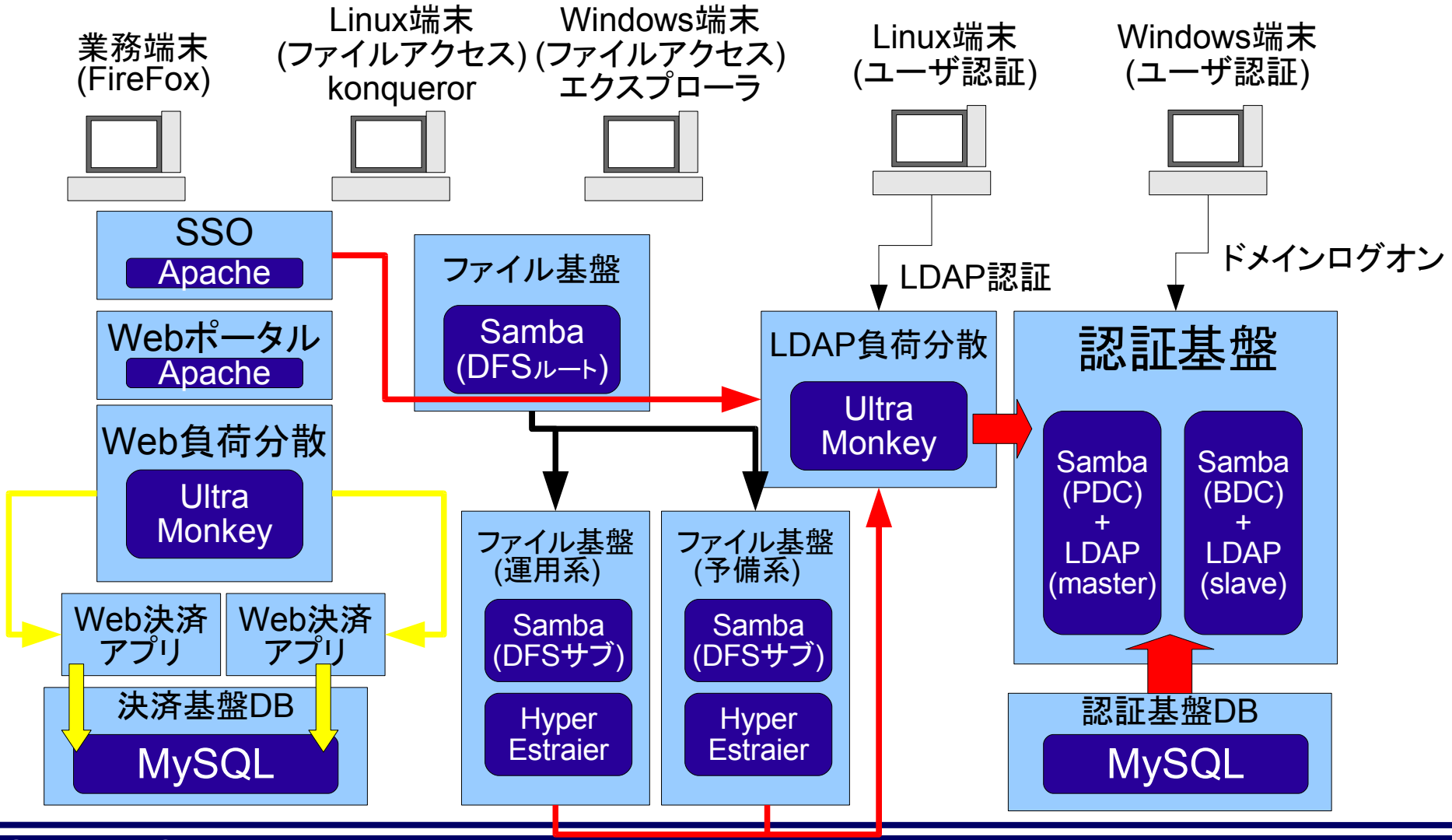
実証実験のシステム構成



システム詳細

	必要機能	実装方法
職員認証基盤	•Linuxによるディスクレス・シンクライアント •OSSのWebブラウザで業務の実現 •OA業務はOpenOfficeを利用	•KnoppixベースのCDブートLinuxの利用
	•上記 Linuxクライアントの認証基盤統合	•OpenLDAPによるLDAPでの認証統合 •KnoppixのLDAP認証対応
	•既存Windowsクライアントの利用も可能	•Samba LDAPによるWindowsドメイン構築 •Windowsクライアントはドメイン参加
	•Webベースの業務では、一度認証したら再度認証は不要(Single Sign On)	•認証基盤はOpenLDAPと連携 •SSOはApacheのmod_sso改造版で実現
	•県庁職員 5000人に対応のパフォーマンス •今後のスケールアウトに対応した拡張性	•Ultra Monkeyによる負荷分散クラスタ構築 •OpenLDAP/Samba/Apacheをクラスタ構造
電子決済基盤	•Webブラウザにより複数システムから共通の決済基盤を利用可能	•決済基盤APIをWebサービスで公開し、相互利用
	•決済文書としてファイル交換を可能	•Webサービスでファイル送受信可能に実装

最終構成(概略図)



大規模システム構成時の注意点

- ソフトウェアのチューニング
  - OpenLDAPのバックエンドデーターベース(Berkley DB)のバージョン、バグ修正
  - カーネルパラメータの修正
    - システムで同時オープン可能な最大ファイル数の拡大(filemax)
  - 同時接続数の拡大
    - ldapユーザの接続数の制限値の拡大(ulimit)

付録

- 大分県庁実証実験システム詳細記事
  - ThinkIT : http://www.thinkit.co.jp/free/article/0706/15/3/
- RHEL4/RHEL5 OpenLDAP性能比較データ
  - 日経Systems 8月号(7/26発売) 記事掲載予定

日本LDAPユーザ会紹介

- http://ldap.jp
  - 各種セミナー資料
    - LDAPユーザ会設立記念セミナー
    - OSC2007 Hokkaido LDAPセミナー
  - 技術情報
    - OpenLDAP manデータ日本語化
    - LDAPベンチマークツール slamdの利用方法
  - メーリングリスト [ldap-users]
- スタッフ募集中
  - staff@ldap.jp