日本LDAPユーザ会 設立準備セミナー

ユーザ会の紹介とLDAP入門

設立発起人代表：小田切耕司

オープンソース・ソリューション・テクノロジ株式会社

【お問い合わせ先】

http://www.ldap-jp.org

講師著作紹介

- 2006年5月 技術評論社 LDAP Super Expert
  - 巻頭企画
  - [新規／移行]LDAPディレクトリサービス導入計画
  - http://www.gihyo.co.jp/magazines/ldap-se
- 技術評論社 Software Design 2006年7月号
  - ネットワーク運用／管理 五輪書（ごりんのしょ）
  - 「壱：地の巻」Sambaファイルサーバ
  - http://www.gihyo.co.jp/magazines/SD/contents/200607
- 2006年5月 翔泳社 開発の現場 vol.005
  - オープンソース案件指南帖
  - 総論編：オープンソースの基礎知識
  - http://www.shoeisha.com/mag/kaihatsu/
- 2006年5月 IDG月刊Windows Server World 2006年3月、4月号
  - 3月号：Shall we Samba?【お手軽導入編】
  - 4月号：Shall We Samba?【超本格運用編】
- 2005年10月 日経BP社 セキュアなSambaサーバの作り方
  - http://itpro.nikkeibp.co.jp/linux/extra/mook/mook12/index.shtml

Part 1.

日本LDAPユーザ会紹介

日本LDAPユーザ会とは？(1)

- 目的
  - LDAPに関する情報交換
    - 技術情報、イベント情報、人的交流
  - LDAPの普及促進
- 具体的な活動内容
  - Webによる情報発信
    - www.ldap-jp.org → www.ldap.jp へ移行予定
  - メーリングリストによる情報交換
  - 技術セミナー、OSCのようなイベントに参加
    - ついでに懇親会（人的交流もはかる）

日本LDAPユーザ会とは？(2)

- 発起人
  技術評論社LDAP Super Expertの著者やWebで著名な人
  - 小野寺 尚文
  - 樽石 将人(レッドハット株式会社)
  - 稲地 稔(NECソフトウェア北海道)
  - 中満 英生
  - 関口 薫
  - 太田 俊哉(日本電気株式会社)
  - 濱野 賢一朗(リナックスアカデミー)
  - 武田 保真(オープンソース・ソリューション・テクノロジ株式会社)
  - 佐藤 文優(オープンソース・ソリューション・テクノロジ株式会社)
  - 竹内 英雄(オープンソース・ソリューション・テクノロジ株式会社)

日本LDAPユーザ会とは？(3)

- 今後の予定
  - 正式発足は4／1
  - それまでに以下を準備
  - スタッフ募集
  - Webの整備（CMSの導入など）
  - 正式設立セミナーを4月にやりたい

セミナー会場探索中

Part 2.
LDAPユーザ会が必要な背景
（Sambaとの関連性）

現在のシステム認証基盤の問題点

- 個人情報保護法や内部統制など企業システムのセキュリティを見直したり、強化する動き
- セキュリティの基本はアクセス制御
  - 誰がどんなリソースをアクセスできるのか、定義し制御する。
- アクセス制御をちゃんとするにはユーザ認証が基本
- Windows Active Directoryを使って認証しているユーザは大変多いがユーザ数に比例してライセンス料が必要
- ユーザ認証の重要性は誰もが気付いているが、それを見直す際に他のLDAP製品を検討比較しようという意識はまだ低い
- 情報不足とエンジニア不足、コスト予測できないなど不安要素がいっぱい

システム認証基盤構築のメリット

- ユーザが利用している認証が必要なシステム例
  ほとんどのシステムはユーザ名とパスワードによる認証
  - メールサーバ
  - ファイルサーバ
  - Webサーバ
  - Web Proxy
  - FTPサーバ
  - SSH
  - TELNET
  - SCP
  - 業務システム
- これらのパスワードがすべて違うと不便！
  しかし、すべて同じで変更も1度ですべて同期して行われたらとっても便利！
- 認証基盤を統合すればそれが可能になる！

LDAPを使った認証基盤構築メリット

- 標準プロトコルLDAPだからこその親和性
  OSSのSambaとOpenLDAPを使うとUnix/ Linux/ Windows/ Mac Osの統合認証が可能になる。
- OSSを使うとクライアントに比例するCAL（クライアントアクセスライセンス）を不要にすることで、コストを大幅に削減することができる。
- 導入コストだけでなく、運用コストの削減
  ユーザ管理の一元化と分散管理
- 内部統制とセキュリティの強化

LDAPを活用したシステム認証基盤構築例

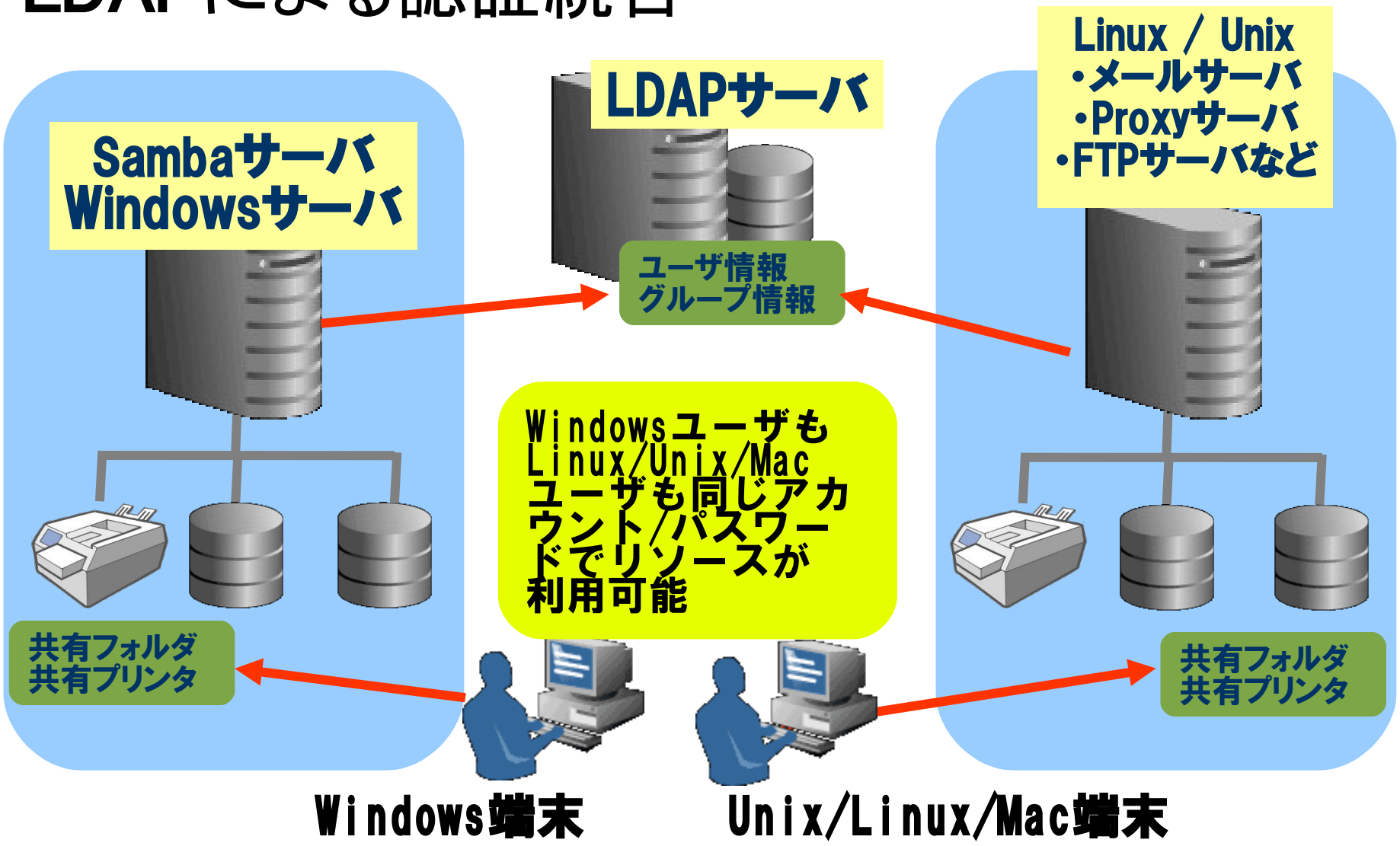
- Active Directoryの代わりとしてのOSS認証基盤
  OSSのSambaとOpenLDAPを使い、既存のWindowsドメインを移行したり、Active Directoryの代わりにOSSシステム認証基盤を導入。
- 既存のNISやNIS+からLDAPへの移行
  OSSのSambaとOpenLDAPを使い、Windowsクライアントの認証だけでなく、Unix,Linux,Macの認証統合を行う。
- Active DirectoryによるUnix,Linux,Macの認証統合
  OSSのSambaを使い、Unix,Linux,Macクライアントおよびサービス（メール、Web、FTPなど）の認証をWindows Active Directoryを使って行う。

最近は認証基盤システムの新規構築、再構築、統合が増えています。

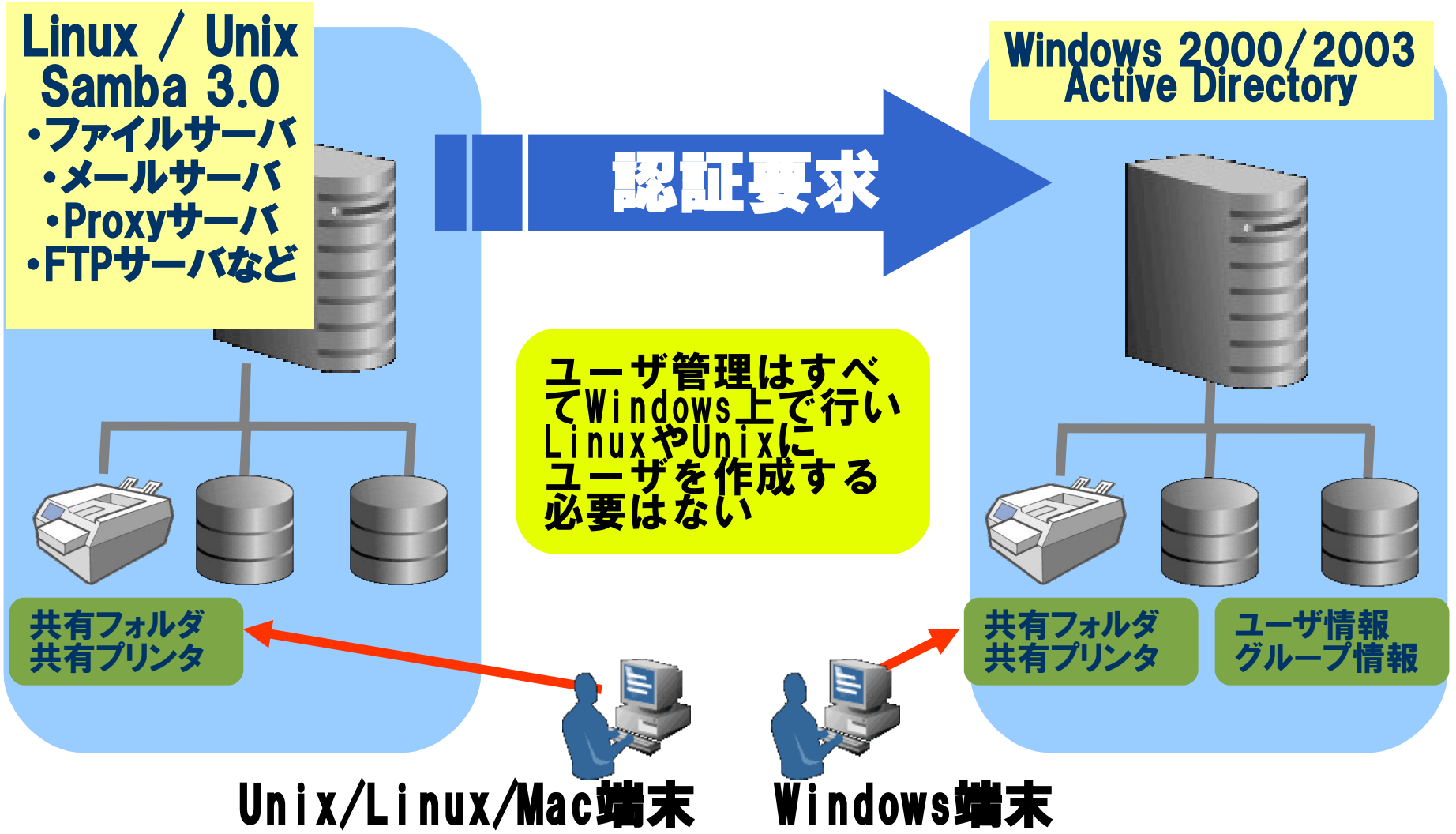
- 内部統制の強化や個人情報漏洩問題からセキュリティを強化する方向
- 情報システム部が知らないWindowsドメインの乱立
- 古いUnix NISドメインの再構築
- 使われていないユーザアカウントの放置
- 安易なパスワード、長期間変更されないパスワード

➔Windows,Unix,Linux認証統合要求
➔複数WindowsドメインとUnix NISドメインをLDAPを使った単一ドメインへ統合
➔ユーザアカウントの厳密な管理
➔システムポリシーの強化

LDAPによる認証統合



Active DirectoryによるUnix,Linux,Macの認証統合



Part 3.

LDAP入門

LDAPとは?

- ディレクトリサービスを利用するための規約の1つ(RFCで定義)
  - ディレクトリサービスとは、キーを基に関連情報を取り出す仕組み
  - ユーザ管理、電話帳、リソース管理などに利用
  - **高機能だが運用負荷や開発コストが高かったITU- T 勧告のX.500 ディレクトリ・サービスを「90 %の機能を10 %のコストで実現する」ために設計**
- 商用LDAP製品も多数存在
  - SUN DS,IBM SecureWay,Novell eDirectory,Oracle Internet Directoryなど
  - MS Active DirectoryもLDAP準拠
    - でもUnixでADをLDAPとして使うのは大変(Sambaを使うと良い)
- オープンソースソフト
  - OpenLDAP
    - **Linux ディストリビューションに同こんされるオープンソースのLDAP**
    - Red Hat、SuSE、Debianなどに採用済み
  - Fedora Directory Server
    - かつてのNetscape Directory ServerをOSSにしたもの

LDAPとRDBMSの違い

- LDAP(ネットワークプロトコル)とSQL(言語)
- ディレクトリサービスにはACID特性がないことに注意！
  - 今書いたデータが今すぐ読めるとは限らない！

	LDAP	RDBMS
用途	検索性能重視、頻繁な更新には向かない	検索だけでなく頻繁な更新も重視
構造	木構造(行や列といった概念はない)	表構造(行や列が存在)
スキーマ	既存の登録済みスキーマ(ObjectClass)を利用するのが一般的	ユーザが業務に合わせて個別に設計し、利用する
更新	トランザクションの概念はない (トランザクション機能を持った製品もある) 大量更新には向かないので1時間に数件といった更新頻度のものに利用する	トランザクションの概念あり 1秒間に何十、何百もの更新に耐えられる設計となっている
分散	ツリーの枝単位で分散配置が可能	キーの範囲で分散配置が可能
操作	LDAP(ネットワークプロトコル)で操作 プロトコルは単純	SQL(プログラム言語)で操作 複雑な操作が可能
検索手法	木の枝葉をたどるイメージ	表の行を走査するイメージ

LDAPで何ができるか？

- Linuxユーザの統合管理
  (Mail,FTP,Telnet,Proxy,sshなど)
- Samba/Windowsユーザの統合管理
- Webサーバ(Apache)のアクセス制御
- 電話帳、メールアドレス帳
- PKI(公開キー)の保管場所として

OpenLDAPが標準で提供するスキーマ(1)

- 標準提供のスキーマを見ればLDAP何ができるかわかる
- core.schema
  - OpenLDAPの核となるスキーマで以下のRFCで定義されたスキーマが定義されている。
    - ・RFC 2252/2256 (LDAPv3)
    - ・RFC 1274 (uid/dc)
    - ・RFC 2079 (URI)
    - ・RFC 2247 (dc/dcObject)
    - ・RFC 2587 (PKI)
    - ・RFC 2589 (Dynamic Directory Services)
    - ・RFC 2377 (uidObject)
  - これだけでは何もできないが、CNやOUなど他のスキーマを使うための基本部分が定義されている。
- cosine.schema
  - X.500やX.400で規定されたアトリビュートなど以下のようなものが定義されている。
    - ・RFC1274で定義されるhost,manager, documentIdentifierなど
    - ・DNSレコードである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
  - これらからDNSレコードの格納先としてLDAPサービスが利用できることがわかる。

OpenLDAPが標準で提供するスキーマ(2)

- inetorgperson.schema
  - インターネット特にメールアドレス帳のためのスキーマで以下のようなものが定義される。
    - メールアドレス、社員番号、オフィスと自宅住所、会社と自宅の電話番号、写真、
- misc.schema
  - mailLocalAddressやnisMailAliasなどメールサーバが使うスキーマが定義される。
- nis.schema
  - posixAccountやposixGroupなどLinux/UNIXのユーザ認証統合に必須なスキーマが定義される。
  - NISをLDAPに置き換えるのに必要なスキーマも定義されている。
- samba.schema
  - このスキーマはOpenLDAPではなく、Sambaパッケージによって提供されるが、Sambaを使ってWindows/Linux/UNIXのユーザ認証統合に必須なスキーマが定義される。
  - WindowsドメインをSambaに置き換えるのに必要なスキーマも定義されている。
- java.schema
  - javaClassName, javaCodebaseなどJava Object（RFC 2713)を扱うためのスキーマが定義される。
- corba.schema
  - corbaIor、corbaRepositoryIdなどCorba Object（RFC 2714）を扱うためのスキーマが定義される。

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
facsimileTelephoneNumber: FAX番号
mobile: 携帯電話
st: 都道府県
l: 市区
street: 番地
postalAddress: 番地
postOfficeBox: ビル名
postalCode: 郵便番号
homePostalAddress: 自宅住所
homePhone: 自宅電話

dn: uid=odagiri, ou=Users, dc=osstech,dc=co,dc=jp
objectClass: posixAccount
objectClass: inetOrgPerson
cn: odagiri
sn: 小田切
givenname: 耕司
mail: odagiri ＠ 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: チーフアーキテクト
employeeNumber: 1
telephoneNumber: 03-1234-5678
facsimileTelephoneNumber: 03-8765-4321
mobile: 090-5432-1234
st: 東京都
l: 品川区西五反田
street: 2-6-3
postalAddress: 2-6-3
postOfficeBox: 東洋ビル
postalCode: 107-0052
homePostalAddress: 神奈川県藤沢市藤沢123-45
homePhone: 0466-23-4567

LDAPへのデータ投入

実行例）Windows上でuser-sjis.txtを作成し、Linux上に転送した場合

```
# iconv -f SJIS -t UTF8 user-sjis.txt -o user-utf8.ldif
```

- -f SJISは入力ファイルがSJISで記述されていることを示す。
- -t UTF8は出力ファイルをUTF-8に変換することを意味する。
- user-sjis.txtは入力ファイル名、-o　user-utf8.ldifは出力ファイル名を意味する。

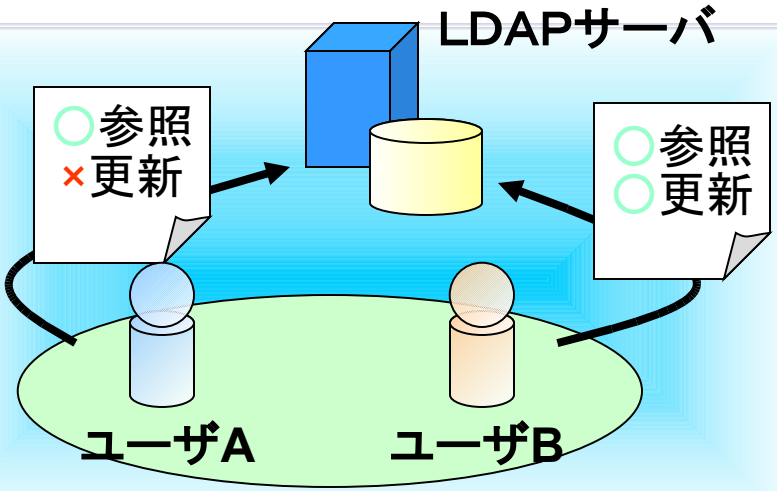
```
# ldapmodify -x -w secret -D cn=Manager,dc=osstech,dc=co,dc=com -f user-
    utf8.ldif
```

- -DはLDAP管理者のDN、-Wは管理者パワード

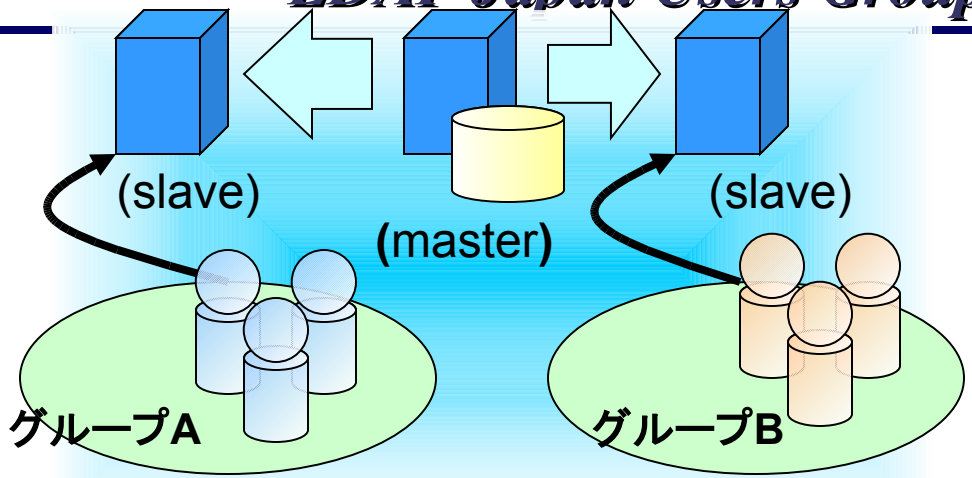
LDAPを使うことの利点

- 機能拡張性が高い
  ユーザー管理だけでなく，組織情報の管理，コンピュータの管理，アプリケーションの管理，メール・アドレス帳，電話帳などいろいろな用途で自由に拡張して使用できる
- UNIX/Linux だけでなくSamba やWindows でも利用できる
- 性能に関しても拡張性が高い
  商用のLDAP 製品は数十億のデータ・エントリでも実運用に耐える処理性能を備えている。
  Linux ディストリビューションに添付されるオープンソースの OpenLDAP も数千～数万エントリでの実績が多数ある
- 細かなアクセス制御機能を有しており，SSL などでの暗号化も可能でセキュリティが強固である
- ディレクトリを木構造で管理でき，サーバーの分散管理が可能である
- 複製機能を備えており，障害にも対応できる

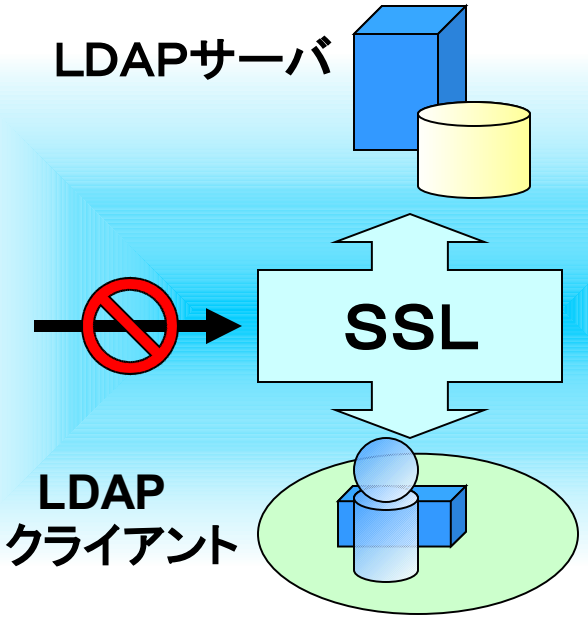
アクセス制御



レプリケーション



通信経路暗号化



分散管理(referral)