OSSTech

Linux Professional Institute Japan LPI-JAPAN

LPICレベル3 Specialty
LPI 300 Mixed Environment Exam
技術解説セミナー
OpenLDAP / Samba編

オープンソース・ソリューション・テクノロジ株式会社
代表取締役 チーフアーキテクト 小田切耕司

お問い合わせ info@osstech.co.jp

Part 1.
LPIC 300出題範囲

300試験範囲：出題範囲詳細（Ver1.0）

- 主題390：OpenLDAP の設定
  - 390.1 OpenLDAPのレプリケーション
  - 390.2 ディレクトリの保護
  - 390.3 OpenLDAPサーバのパフォーマンスチューニング
- 主題391：OpenLDAPの認証バックエンドとしての利用
  - 391.1 PAMおよびNSSとLDAPの統合
  - 391.2 アクティブディレクトリおよびKerberosとLDAPの統合
- 主題392：Sambaの基礎
  - 392.1 Sambaの概念とアーキテクチャ
  - 392.2 Sambaを設定する
  - 392.3 Sambaの保守
  - 392.4 Sambaのトラブルシューティング
  - 392.5 国際化
- 主題393：Sambaの共有の設定
  - 393.1 ファイルサービス
  - 393.2 Linuxファイルシステムと共有/サービスのパーミッション
  - 393.3 プリントサービス
- 主題394：Sambaのユーザとグループの管理
  - 394.1 ユーザアカウントとグループアカウントの管理
  - 394.2 認証と許可およびWindbind
- 主題395：Sambaのドメイン統合
  - 395.1 SambaのPDCとBDC
  - 395.2 Samba4のAD互換ドメインコントローラ
  - 395.3 Sambaをドメインメンバーサーバとして設定する
- 主題396：Sambaのネームサービス
  - 396.1 NetBIOSとWINS
  - 396.2 アクティブディレクトリの名前解決
- 主題397：LinuxおよびWindowsクライアントの操作
  - 397.1 CIFS連携
  - 397.2 Windowsクライアントの操作

OSSTech

Linux Professional Institute Japan LPI-JAPAN

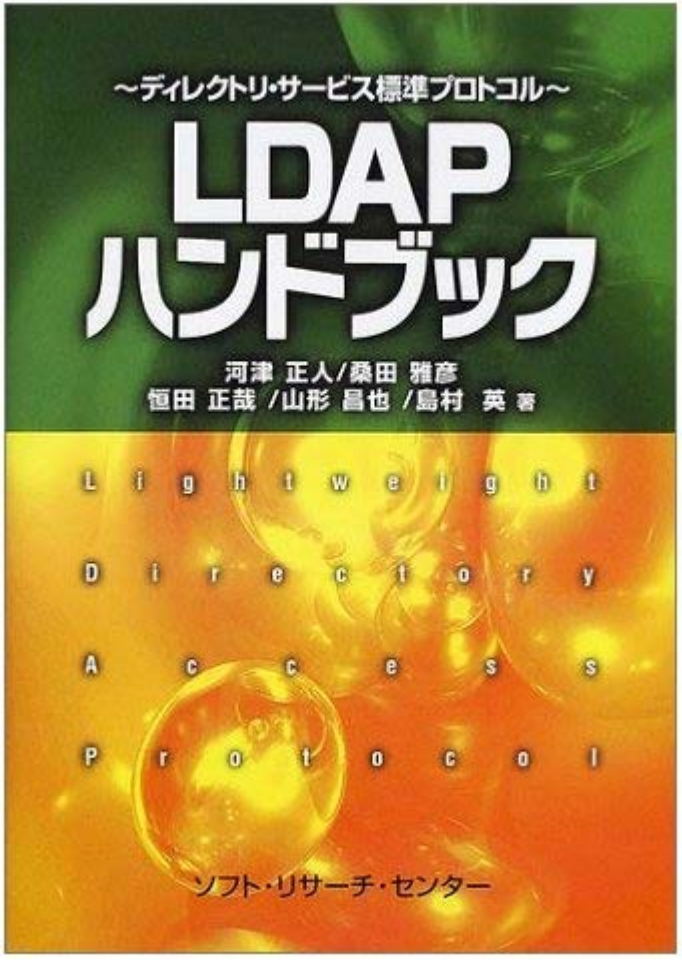
LDAP概念と設計入門

概念　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
  - Oracle Directory Server, Red Hat Directory Server, Novell eDirectoryなど
  - MS Active DirectoryもLDAP準拠（認証はKerberos）
- 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梱されるオープンソースのLDAP
  - Red Hat Directory Server
    - かつてのNetscape Directory ServerをOSSにしたもの（RHは有償、Fedoraは無償）
  - OpenDJ
    - ForgeRockが中心で開発されているJavaで書かれたLDAP

LDAP概念を勉強のための参考書

- LDAPハンドブック
  - ディレクトリ・サービス標準プロトコル
  - 出版社: ソフトリサーチセンター（2002/0
  - 発売日: 2002/03



LDAPとRDBMSの違い

- LDAPはネットワークプロトコル、SQLは言語

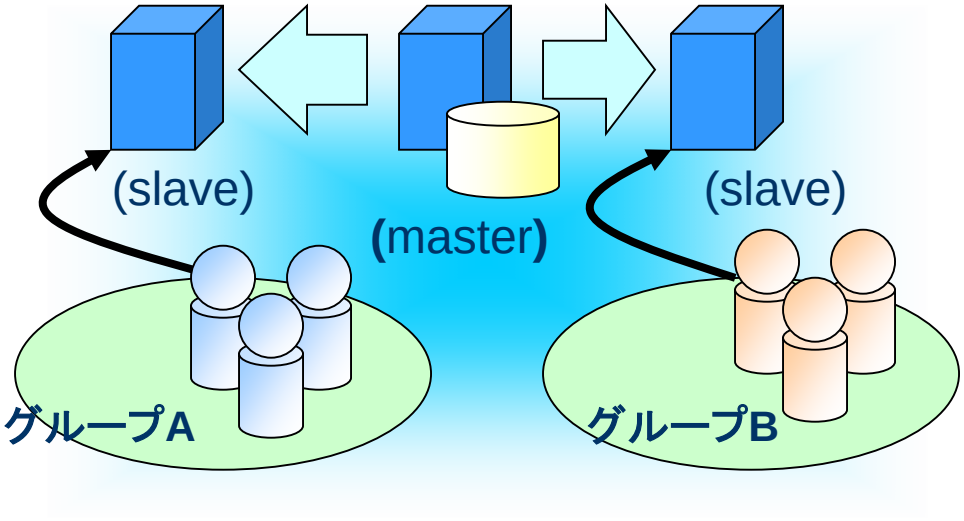
	LDAP	RDBMS
用途	検索性能重視、頻繁な更新には向かない	検索だけでなく頻繁な更新も重視
構造	木構造（行や列といった概念はない）	表構造（行や列が存在）
スキーマ	既存の登録済みスキーマ(ObjectClass)を利用するのが一般的	ユーザが業務に合わせて個別に設計し、利用する
更新	トランザクションの概念はない (トランザクション機能を持った製品もある) 大量更新には向かないので1時間に数件といった更新頻度のものに利用する	トランザクションの概念あり 1秒間に何十、何百もの更新に耐えられる設計となっている
分散	ツリーの枝単位で分散配置が可能	キーの範囲で分散配置が可能
操作	LDAP（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概念に関する勘違い

- RDBMSは永続的なユーザ情報を蓄えるために使う、LDAPは管理情報を集約するために使う
  （社員DBはRDMS、全社認証システムはLDAP）
- LDAPは検索重視となっているが、RDBより必ずしも早いわけではない
- LDAPはスケールアウト型負荷分散がやりやすいから
- 更新がすぐに反映されるとは限らない
  - ユーザ追加やパスワード変更がすぐにされないことがある（だからWindowsはパスワードをキャッシュする）
- マルチマスターの利用は要注意
  - トランザクションやロックの概念が弱い
  - uid,gidの自動割り振りをLDAPでやると危険

負荷分散方法1:レプリケーション

- 同じ内容のサーバを複数用意する
  - サーバを増やすだけでスケールアウトする
  - 負荷分散装置やldap.confで負荷を分散
  - 1つのサーバが持つデータ量は同じなので規模が大きくなると更新性能が低下
  - Syncreplではサブツリーだけを複製することも可能



OpenLDAPのレプリケーション

OSSTech

- マスター／スレーブ方式
  - マスターだけが更新でき、スレーブは参照のみ
    - スレーブを更新しようとするとupdaterefが返るのでクライアントの責任でマスターに接続して更新する
  - マスターからスレーブへ複製する方式には、replogとsyncreplの2種類ある。
    - replog はpush型（マスターからスレーブを更新）
    - syncrepl はpull型（スレーブからマスターを検索して自身を更新）
    - replogよりsyncreplの方がスケールアウトしやすい
- マルチマスター方式
  - お互いにsyncreplで複製しあうことで実現している
  - どちらも更新可能だが同時に2台を更新してはいけない
  - OpenLDAPではミラーモードと呼ぶ
  - 3台以上のマルチマスターも可能だが設計や品質に十分注意すること
- 上記どちらの方式でもLDAPの更新完了とレプリケーションの完了は非同期
  - 更新したデータがすぐに参照できる保証がない

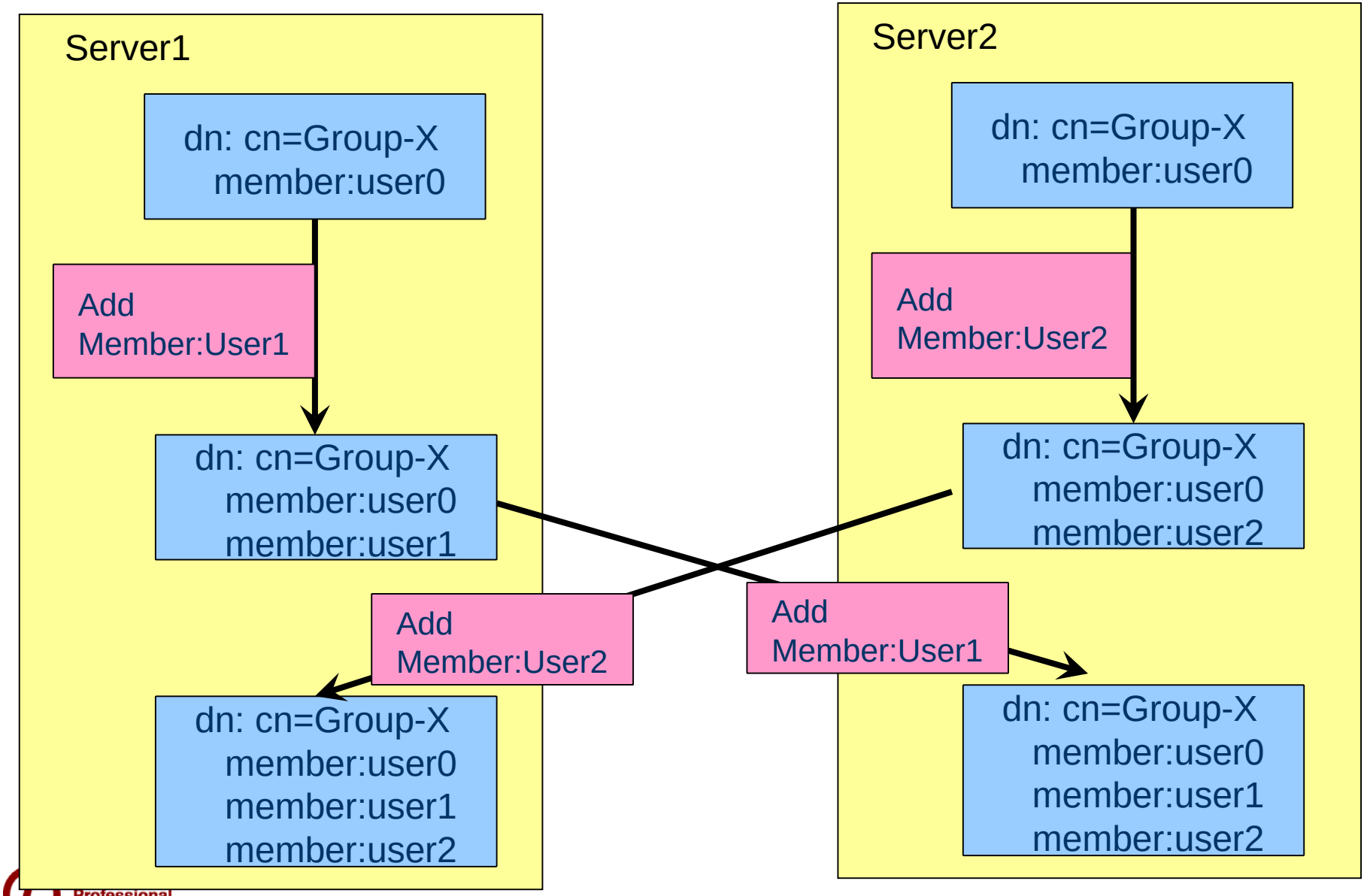
replog(slurpd)は古い方式のため非推奨(試験に出ない)

- replogは運用が大変
  - エラーリカバリは手操作
  - スレーブの追加時にマスターを止める必要あり
  - スレーブ故障後の修復でもマスターを止める必要あり
  - スレーブ台数が多いと性能劣化
- syncreplは運用が楽
  - エラーリカバリは自動
  - スレーブの追加時にマスターを止める必要なし
  - スレーブ故障後の修復でもマスターを止める必要なし
    データを空にして再起動すれば自動修復
  - syncreplはOpenLDAP 2.4以降が安全

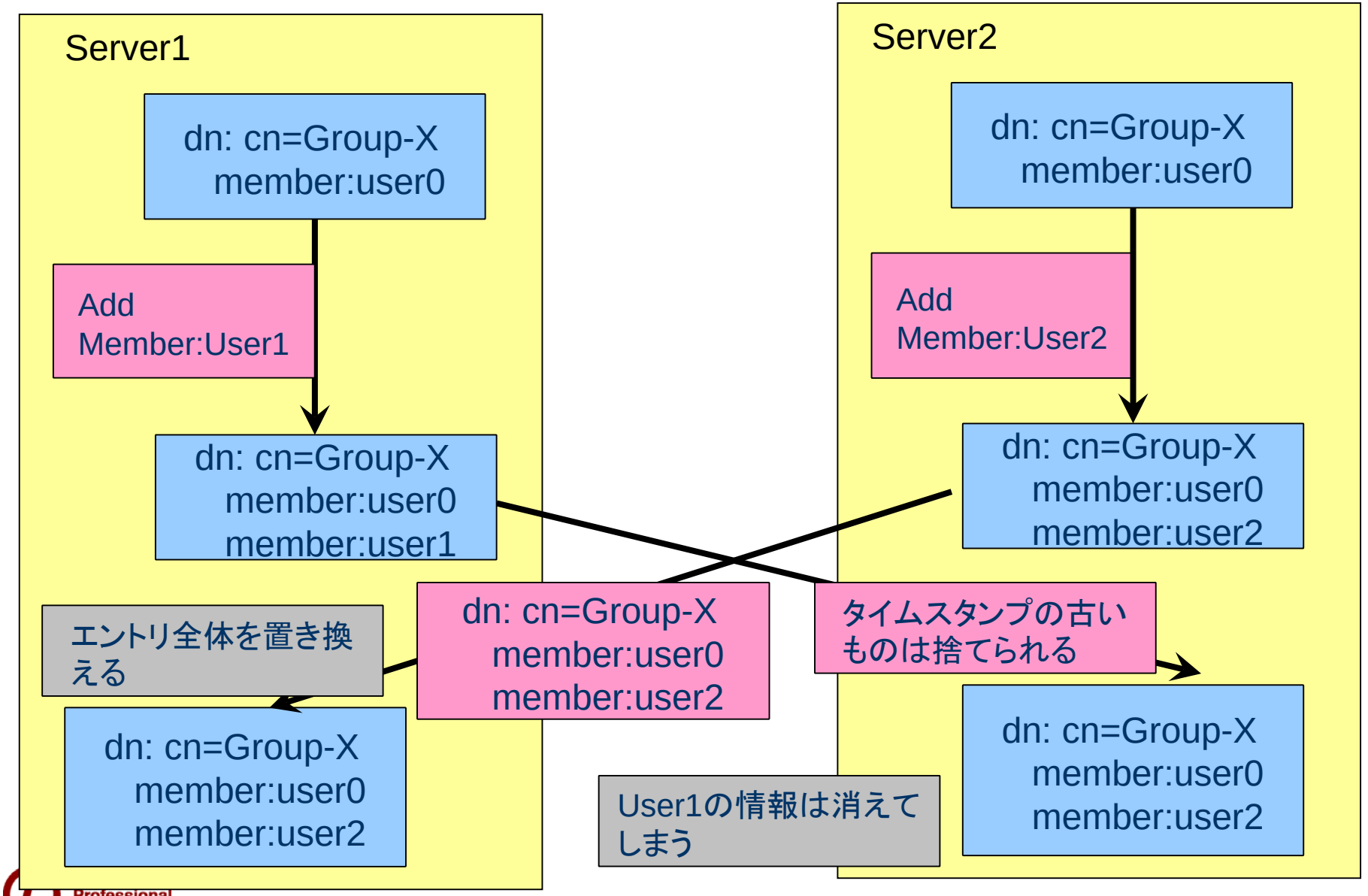
複数LDAPを同時更新してはいけない！

- OpenLDAP 2.4よりマルチマスター(ミラーモードに対応)
- マルチマスター構成は書き込み可能なLDAPサーバーを複数設置する機能
- 1台のLDAPサーバーが故障しても、ほかのサーバーに切り替えができればサービスに影響がない
- データの整合性はデータベースのようなロックする機能を使わずタイムスタンプを使って管理しているので、連続の書き込みが異なるLDAPサーバーに分散された場合は、データの不整合が発生する可能性がある。
- 基本的に書き込み操作を1台のLDAPに集中するデザインが必須である。
- 例えば、ユーザのuid,gid自動割り振りをLDAPのカウントを使ってやるのは危険である。

商用LDAPの操作ログによるマルチマスターの動き

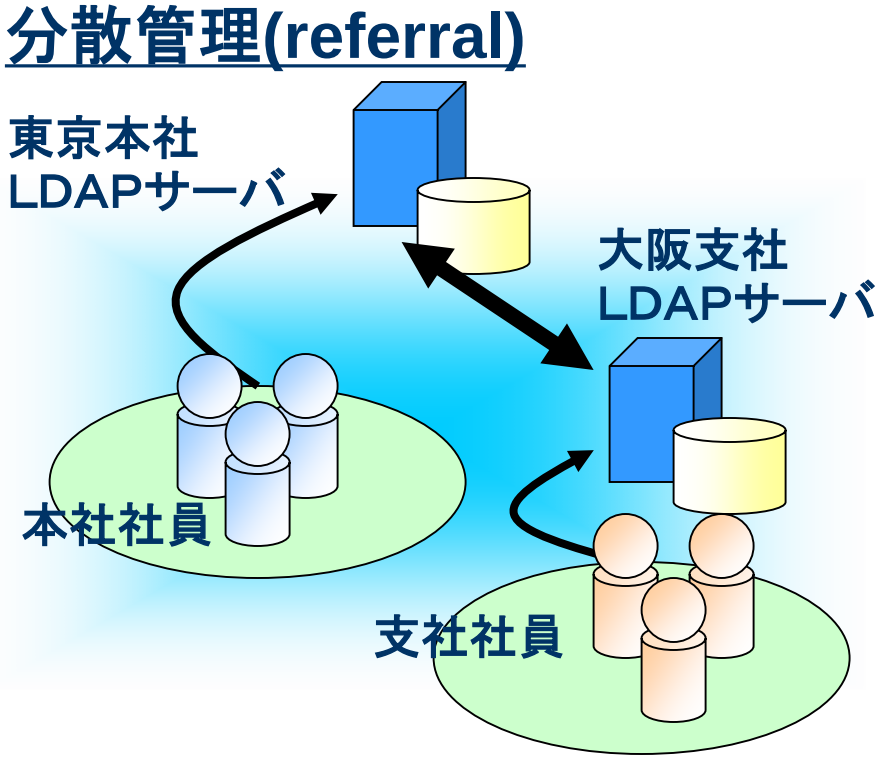


OpenLDAPのエントリ複製方式によるミラーモードの動き



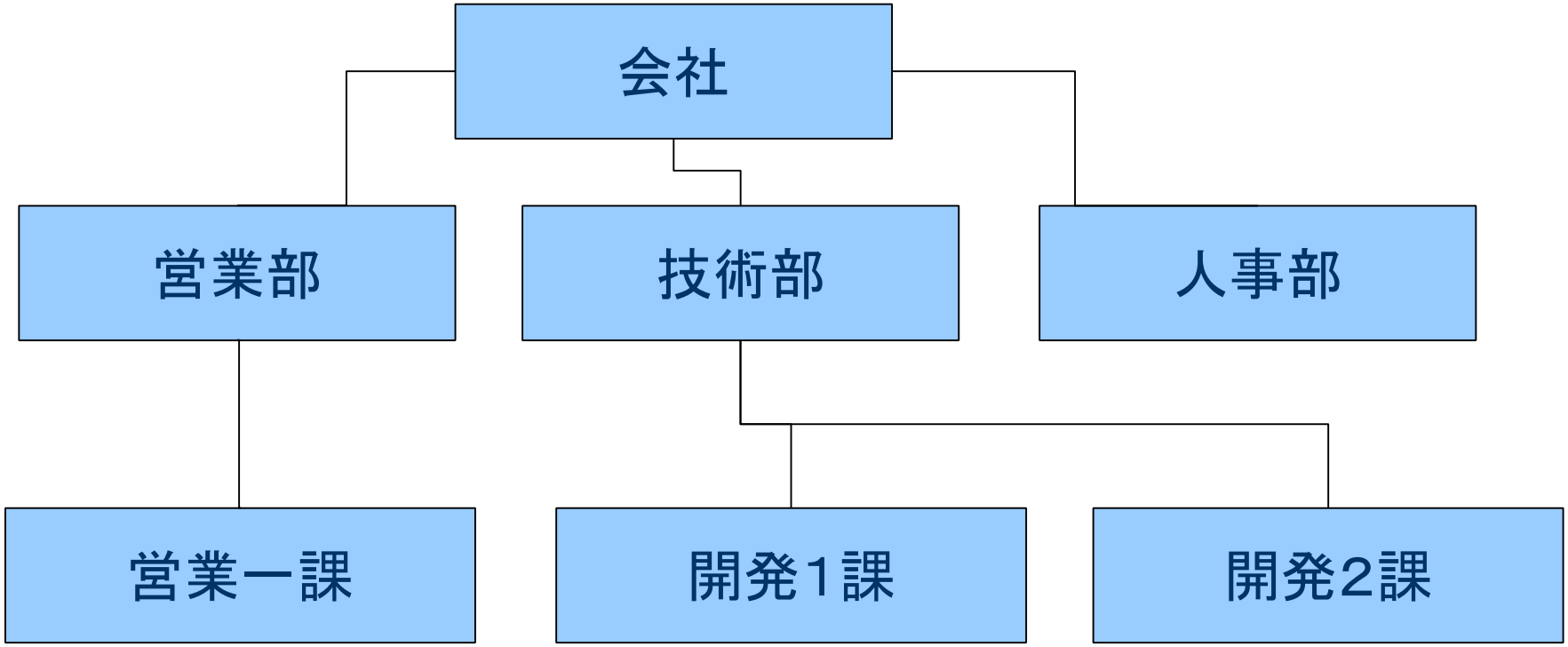
負荷分散方法2:リファラル

- サブツリー単位でサーバを分散する
  - ldap.confでbaseツリーを変える(負荷分散というよりも管理分散)
  - 1サーバがもつデータ量が減るので更新性能も上がる
  - referralが返ったら別なサーバを見に行くのはプログラム側の責任



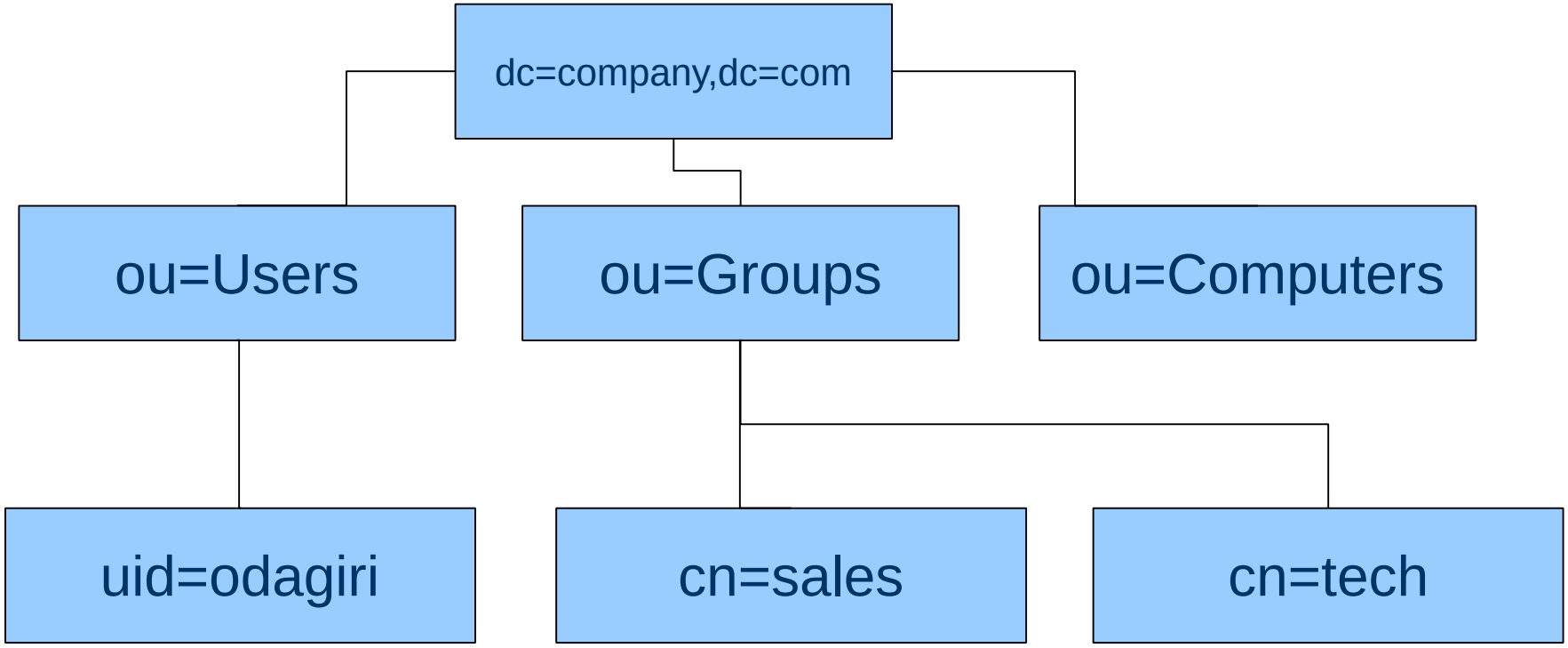
DIT (Directory information Tree) の概念

- 概念として組織構造をあげる書籍が多いが. . .



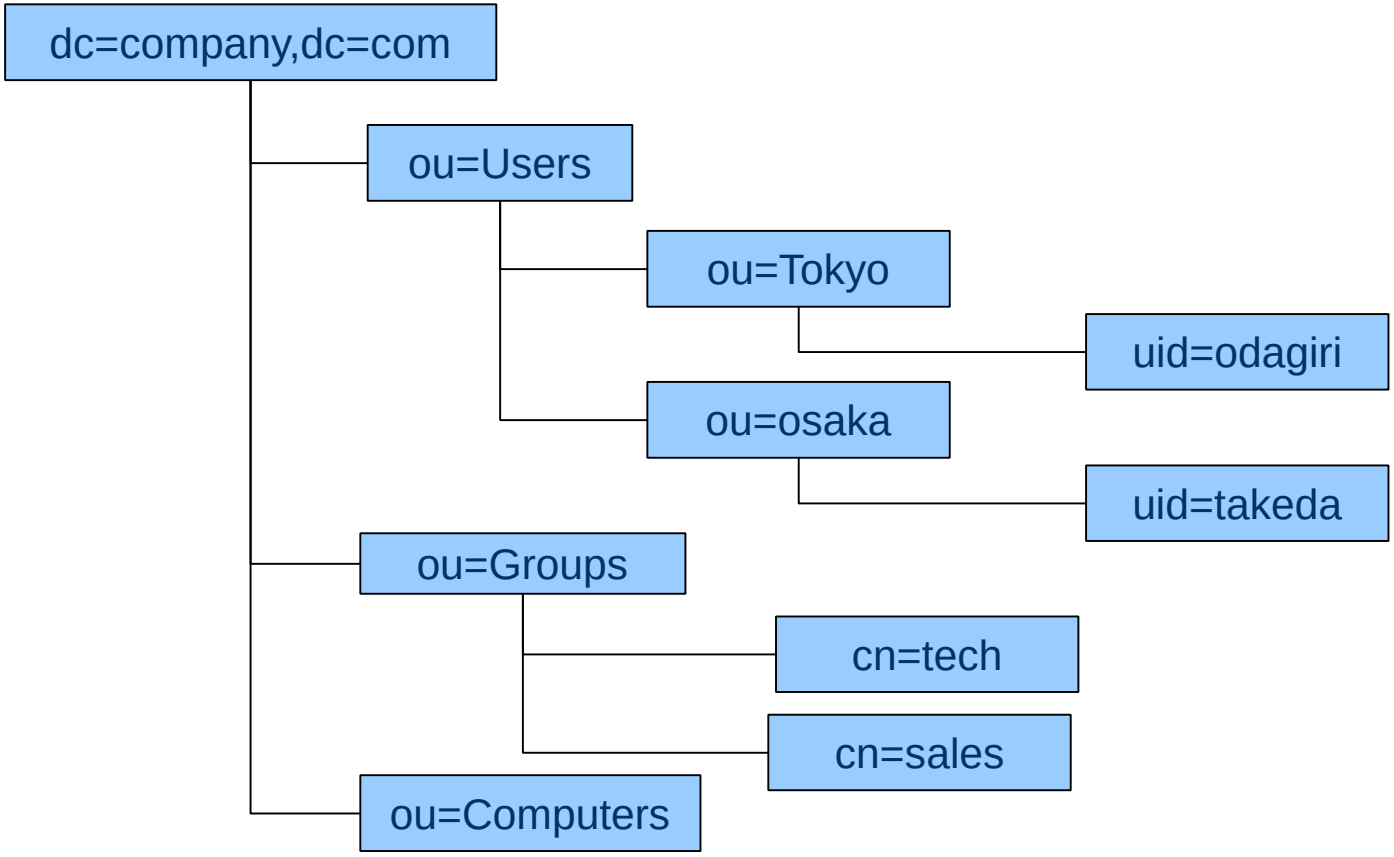
DIT (Directory information Tree) の概念

- 実構造としては管理単位で分ける



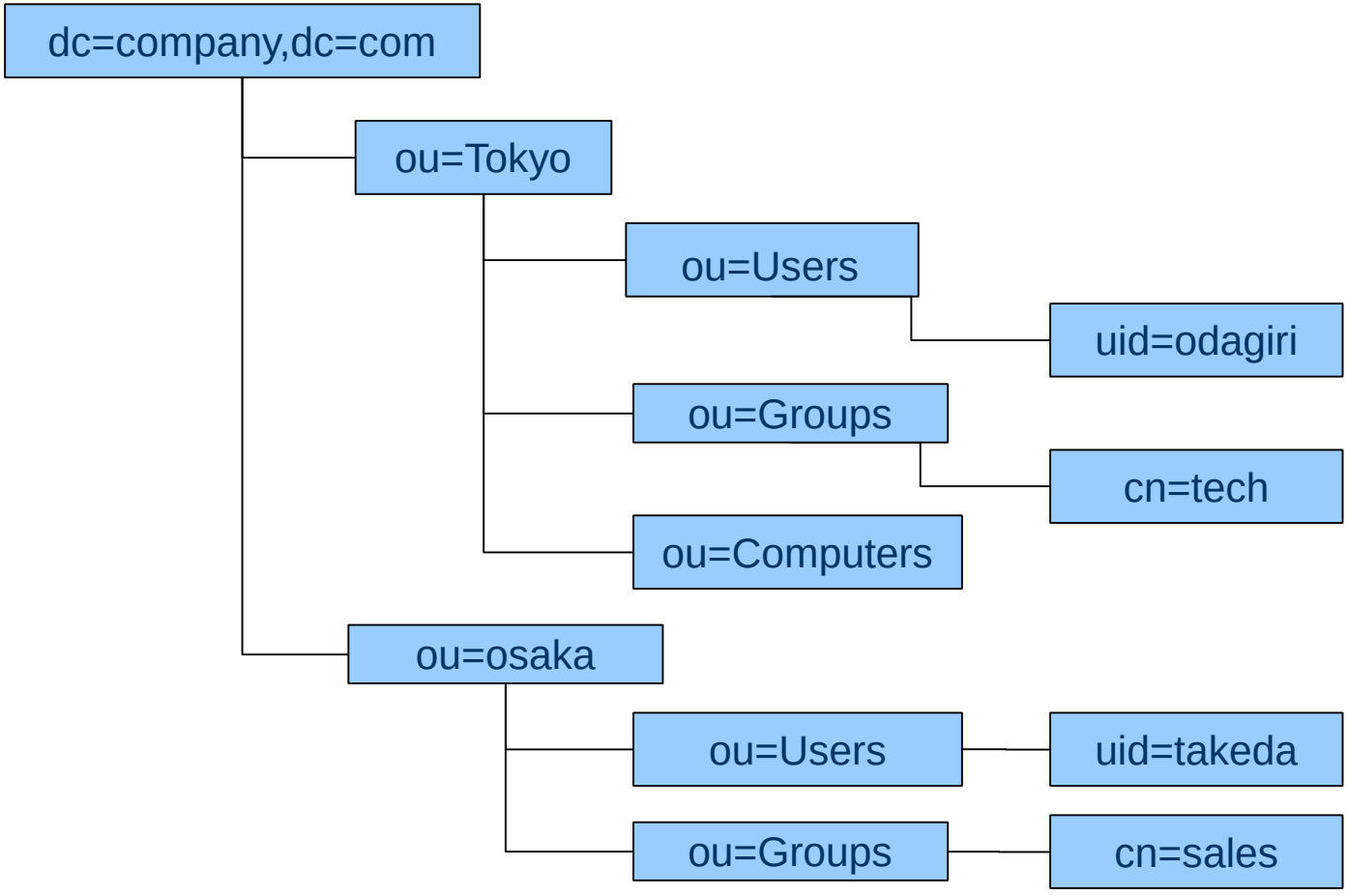
DIT (Directory information Tree) の設計

- 組織構造にマッピングしないこと、管理対象で分ける



DIT (Directory information Tree) の設計

- 組織構造にマッピングしないこと、管理対象で分ける



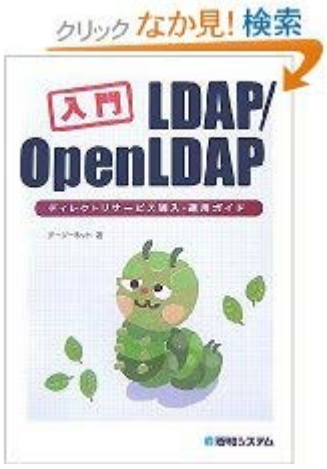
OpenLDAP レプリケーション設定

OpenLDAPサーバーのレプリケーション設定

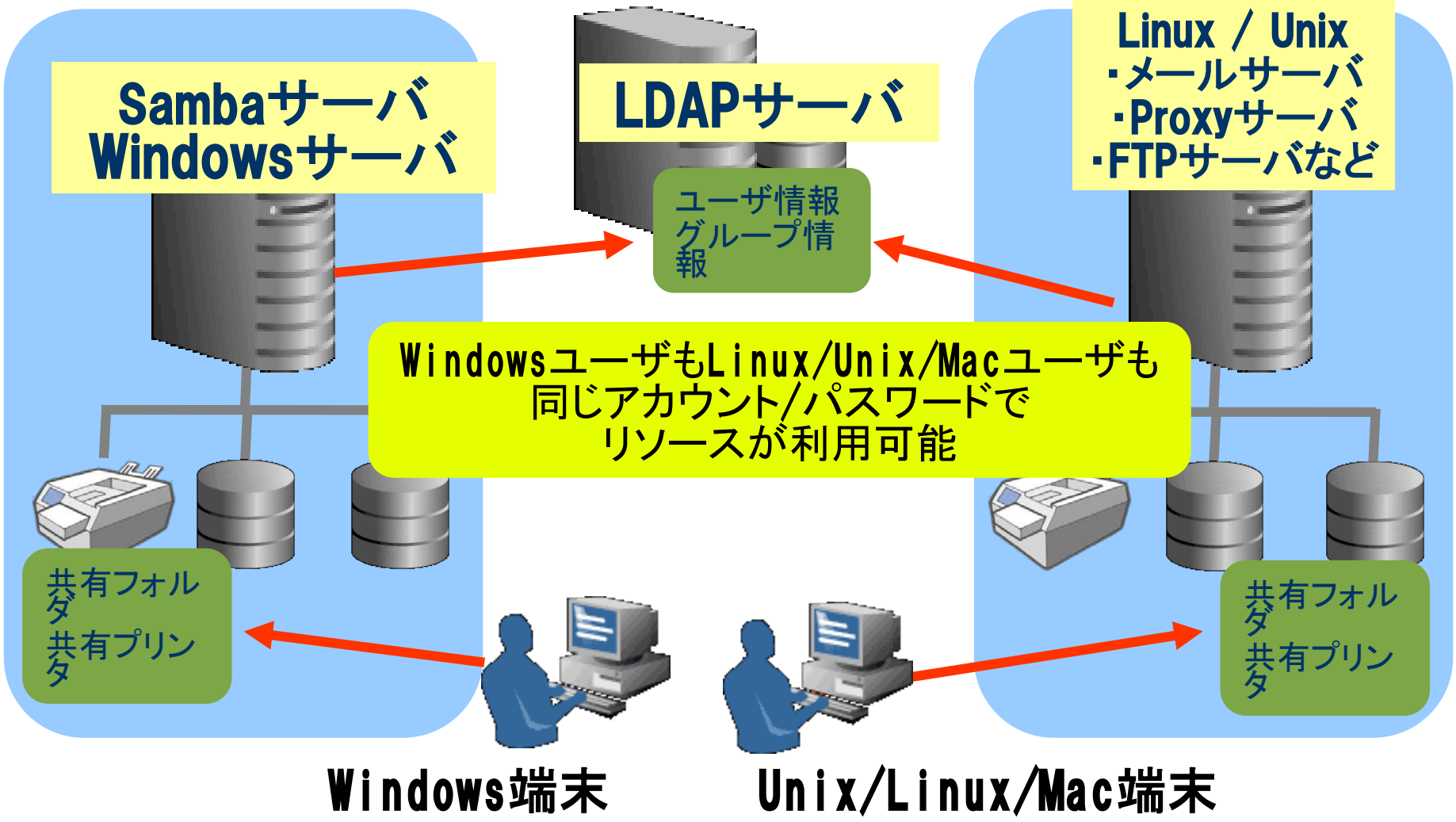
- シングル構成の設定はレベル2の試験範囲
- レベル3では冗長化構成(レプリケーション)が試験範囲
- コンパイルは試験範囲外なので、CentOSなどの標準のOpenLDAPを使ってインストールや設定の勉強をする
- OpenLDAPはどんどん新しくなるので、書籍の情報では古いことがある。
  - www.openldap.org のドキュメントを読むしかない
- コンパイルするのに必要なライブラリは、OS標準のものを使うのが一般的だがBDBだけはOpenLDAP専用のものを使う
  - RedHatのRPMではBDBはOS標準と違う専用のものを使うようにビルドされている。
    - ✓ 上記理由からRed HatではOpenLDAPのBDBリカバリにdb_recover は使わない ！ slapd_db_recover を使う

OpenLDAP勉強のための参考書

- OpenLDAP入門
  - オープンソースではじめるディレクトリサービス
  - 出版社: 技術評論社
  - 発売日: 2003/07
- 入門LDAP/OpenLDAP
  - ディレクトリサービス導入・運用ガイド
  - 出版社: 秀和システム
  - 発売日: 2007/10



LDAPによる認証統合

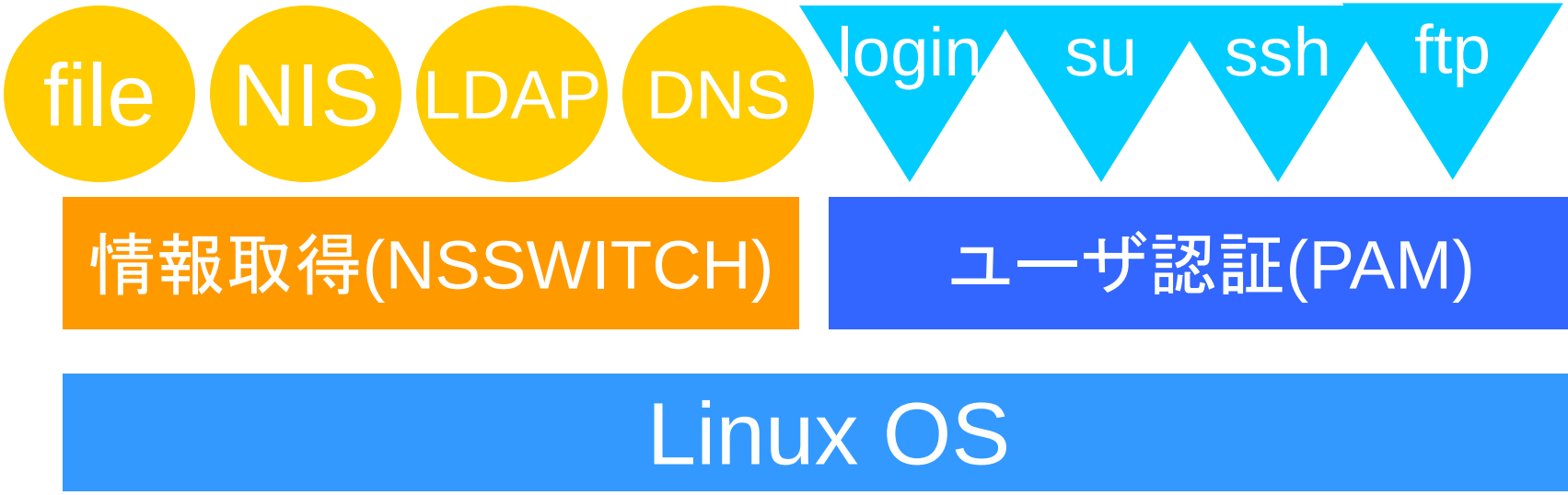


LDAPの設定

- LDAPサーバとしての設定
  - slapd.confの設定
- LDAPクライアントとしての設定
  - NSS設定
  - PAM設定
  - ldap.conf設定

LDAPクライアントとしての設定

- NSS(ネーム・サービス・スイッチ)機能
  - システムのユーザ名、グループ名、ホスト名の解決方法を設定
  - /etc/nsswitch.confで、各種情報の取得先を指定可能
- PAM認証機構
  - アプリケーション毎の認証方法を設定
  - /etc/pam.d/の中でアプリケーションごとの認証ルールを指定可能



NSS：ネームサービススイッチ機能

- LDAPを認証で使用するには/etc/nsswitch.confを以下のように変更

```
passwd:   files   ldap
group:    files   ldap
shadow:   files   ldap
hosts:    files   dns   wins
```

- /lib/libnss_ldap.so.2が呼ばれる。
- /lib/libnss_wins.so.2 を使うとWINS (Windows Internet Name Service) を使って名前解決可能
- RHEL6からはSSSD(System Security Services Daemon)が利用されるので、ldapの代わりにsssと記述される。

PAM：プラグマブル認証機能

- /etc/pam.d/system-authに以下を設定

```
[root@fs02 /etc]# cat /etc/pam.d/system-auth
#%PAM-1.0
# This file is auto-generated.
# User changes will be destroyed the next time authconfig is run.
auth        required      /lib/security/pam_env.so
auth        sufficient    /lib/security/pam_unix.so likeauth nullok
auth        sufficient    /lib/security/pam_ldap.so use_first_pass
auth        required      /lib/security/pam_deny.so

account     required      /lib/security/pam_unix.so
account     [default=ok user_unknown=ignore service_err=ignore system_err=ignore] /lib/security/pam_ldap.so

password    required      /lib/security/pam_cracklib.so retry=3
password    sufficient    /lib/security/pam_unix.so nullok use_authtok md5 shadow
password    sufficient    /lib/security/pam_ldap.so use_authtok
password    required      /lib/security/pam_deny.so

session     required      /lib/security/pam_limits.so
session     required      /lib/security/pam_unix.so
session     optional      /lib/security/pam_ldap.so
session     required      /lib/security/pam_mkhomedir.so skel=/etc/skel umask=0022
```

- RHEL6からはSSSD(System Security Services Daemon)が利用されるので、pam_ldapの代わりにpam_sssと記述される。

OpenLDAPサーバの設定

設定ファイル

- サーバ：/etc/openldap/slapd.conf または /etc/openldap/slapd.d
- クライアント：
  - NSS,PAM用：/etc/ldap.conf
  - □ ldapaddなどの管理コマンド用:/etc/openldap/ldap.conf

OpenLDAP 管理者ガイド

http://www.ldap.jp/doc

Red Hat Enterprise Linux 6マニュアル

https://access.redhat.com/site/documentation/ja-JP/Red_Hat_Enterprise_Linux/6/html/Deployment_Guide/SSSD-Introduction.html

https://access.redhat.com/site/documentation/ja-JP/Red_Hat_Enterprise_Linux/6/html/Deployment_Guide/ch-Directory_Servers.html#s1-OpenLDAP

OpenLDAPサーバーの設定ファイル

- OpenLDAP 2.4から設定は
  - /etc/openldap/slapd.conf ファイルから
  - /etc/openldap/slapd.d/ ディレクトリに存在する設定データベースを使用
- しかし、/etc/openldap/slapd.d/ ディレクトリ内を直接編集するのは推奨されていない
- あらかじめ slapd.conf ファイルで設定し、動作確認してから /etc/openldap/slapd.d/ ディレクトリを作成するのが良い。
- 以下のコマンドを実行することで新しい形式に変換可能

```
slaptest -f /etc/openldap/slapd.conf -F /etc/openldap/slapd.d/
```

- 以降の解説では、slapd.conf ファイルで設定することを前提

レプリケーションのための設定

- マスター／スレーブ方式
  - マスター設定
    overlay syncprov
  - スレーブ設定
    updateref “ldap://ldapマスター/“
    syncrepl rid=1　provider=”ldap://マスター”
- マルチマスター(ミラーモード)
  overlay syncprov
  serverID 1 or 2(サーバー毎に変えるかDNS名を追記)
  syncrepl rid=1 provider=“ldap://相手のLDAPサーバー“
  mirrormode on

マスター／スレーブ設定例

- マスター（ldap1）

```
overlay syncprov
```

- スレーブ

```
syncrepl rid=1
  provider="ldap://ldap1"
  type=refreshAndPersist
  retry="5 10 30 +"
  searchbase="dc=example,dc=jp"
  scope=sub
  schemachecking=off
  binddn="cn=slave,dc=example,dc=jp"
  bindmethod=simple
  credentials="xxxxxxxxx"
updateref "ldap://ldap1"
```

type=refreshAndPersistを付けると
マスター／スレーブ間のセッションが繋がったままになる

ミラーモード設定例

- マスター1 (ldap1)

```
overlay syncprov
serverID 1
syncrepl rid=2
  provider="ldap://ldap2"
  type=refreshAndPersist
  retry="5 10 30 +"
  searchbase="dc=example,dc=jp"
  scope=sub
  schemachecking=off
  binddn="cn=slave,dc=example,dc=jp"
  bindmethod=simple
  credentials="xxxxxxxxx"
mirrormode on
```

- マスター2 (ldap2)

```
overlay syncprov
serverID 2
syncrepl rid=1
  provider="ldap://ldap1"
  type=refreshAndPersist
  retry="5 10 30 +"
  searchbase="dc=example,dc=jp"
  scope=sub
  schemachecking=off
  binddn="cn=slave,dc=example,dc=jp"
  bindmethod=simple
  credentials="xxxxxxxxx"
mirrormode on
```

serverIDにDNS名を付けることで複数台とも同じ設定することも可能
syncreplも複数記述

BDBコマンドとパラメータ

- 現在OpenLDAPの推奨バックエンドはBDBなので、BDBのチューニングやコマンドを知ることも重要
- slapd.conf
  - checkpoint 〈更新量〉〈間隔〉
  - cache size 〈エントリ数〉
- DB_CONFIG
  - cachesize
  - DB_LOG_AUTOREMOVE
  - lg_max
- db_recover (slapd_db_recover)コマンド
  予期しないアプリケーション、データベース、またはシステムの障害が発生した後、データベースを整合性のある状態に復元します。
- db_verify (slapd_db_verify)コマンド
  ファイルおよびファイル内に含まれるデータベースの構造を検証します。
- db_archive(slapd_db_archive)
  不要になったログファイルを表示したり、削除する

Samba機能と特徴

Sambaとは？

OSSTech

機　能	Samba 3	Samba 4
ファイルサーバ機能	Samba3.6からSMB2対応	SMB2,SMB3(Windows8)対応
	NASとして使うには現時点ではSamba4より安定	サーバーサイドコピーなどに対応
		CTDBによるクラスター機能対応
ドメインコントローラ機能	NTドメイン互換	Active Directory(Win2008R2)互換
	NTLMv2認証	Kerberos認証（Kerberosサーバー内蔵）
	システムポリシー	グループポリシー
	冗長化には外部のLDAPが必要	LDAPを内蔵しているためSambaのみで冗長化が可能
Windows GUIによる管理機能	Windows2000のUSRMGR Windows 7,8で動作しない	RSAT対応 Windows 7,8で動作可能
名前解決機能	NTドメイン互換なのでWINSサーバーが必要	ADドメイン互換なのでDNSによる名前解決が必要
	SambaがWINSサーバー機能を持つ	WINSサーバーは不要 SambaがDNSサーバー機能を内蔵
	DNSでSamba3 DCを見つけることはできない	DNSがないとSamba4 DCを見つけられない

WindowsサーバーをSambaで構築するメリット

- **コスト削減**
  - Windowsサーバでは、アクセスするユーザごとにCAL (Client Access License) が必要
  - サーバーの低価格化によりOSライセンスコストの割合が増加
- **セキュリティ対策**
  - Windowsに比べ、ウィルスなどの被害が圧倒的に少ない。
- **高機能**
  - 設定ファイルにスクリプトを定義するだけで機能拡張が可能
    ユーザ管理、共有管理機能、ユーザホーム自動作成、パスワードチェック
  - VFSモジュールを開発することで機能拡張が可能
    クラスタ機能、監査機能、ACL制御、容量制限、ウィルスチェック
- **高い信頼性**
  - 連続運転に強い
  - オープンソースなので障害調査でき、不具合修正も可能
- **運用のしやすさ**
  - シェルスクリプトによる運用の効率化が可能
  - 修正モジュールの適用に、OSリブートの必要がない

OSSTech

Linux Professional Institute Japan LPI-JAPAN

Windows移行 Q & A

Windowsドメイン移行に関するQ&A

- **Q. SambaでWindows ADドメインを移行できますか？**
- **A. はい、できます。**
  - Samba4を既存のWindows ADドメインに参加させ、「FSMO:Flexible Single Master Operation」(操作マスター)をSamba4へ転送することで移行可能です。
  - FSMO転送後は既存のWindows ADのDCは撤去可能です。
  - Samba4はGC(Global Catalog)を持つことも可能です。
- **Q. 現在WindowsマシンをDNSサーバー、Kerberosサーバー、DHCPサーバー、Radiusサーバーとして利用しています。これをSambaに移行することはできますか？**
- **A. はい、できます。**
  - Samba4はDNSサーバーとKerberosサーバーになることができ、Linux OSが標準搭載している製品コンポーネントでDHCPサーバーやRadiusサーバーを構築することができます。

- **Q. 現在DC(ドメインコントローラ)として利用している Windowsマシンを、SambaのDC移行後もそのままDCとして利用できますか？**
- **A.　はい、可能です。**
  - SambaとWindowsのDCの混在利用が可能です。
  - FSMOはSambaとWindowsのどちらのDCでも構いません。

- **Q. Samba4をDCとなっているADドメインに Windowsサーバーを DCとして設置できますか？**
- **A. はい、可能です。**
  - Samba4で新規構築したADドメインにWindowsサーバーをDCとして参加させることが可能です。

Windowsドメイン移行に関するQ&A

- Q. ADドメイン移行後、Samba4マシンを旧Windows DCと同じマシン名、同じIPアドレスで運用しようと思いますが、大丈夫ですか？
- A. はい、可能です。しかし、そのためにはSamba4をDCに追加後、既存ADのDCを撤去後に同じホスト名、IPアドレスでSamba4を構築します。SIDは引き継がれるのでアクセス権やプロファイルもそのまま使えます。

- Q. SambaでWindows ADドメインを移行した時、ユーザのパスワードも移行できますか？ADドメインの時のパスワードがそのまま使えますか？
- A. はい、そのまま使えます。

- Q. ADのグループポリシーは移行できますか？
- A. はい、移行可能です。
  - Samba4をDCとして参加させて、SYSVOL共有を複製することでグループポリシーがSamba4へ移されます。（rsyncなどの複製サービスは別途必要）

Windowsドメイン移行に関するQ&A

- **Q. 移動プロファイルは移行できますか？**
- **A. はい、移行できます。**
  - 移動プロファイルをSambaのプロファイル共有にコピーすることで移行できます。

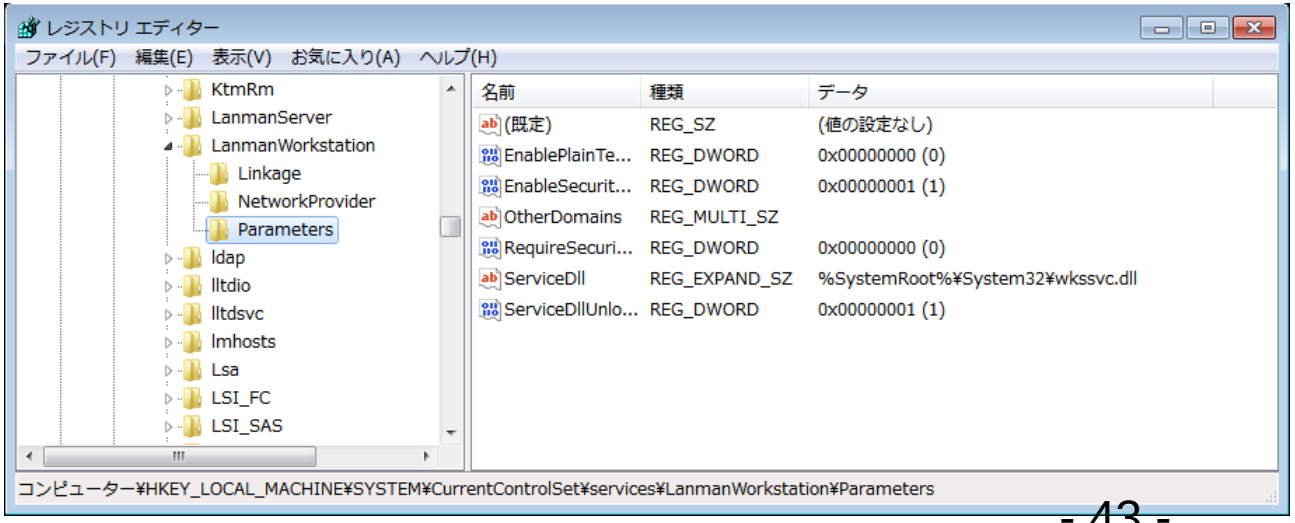
- **Q.ローカルプロファイルは継続して利用できますか？**
- **A.はい、利用できます。**
  - Sambaに移行した場合もユーザSIDはSamba DCに引き継がれますので、スタートメニューやデスクトップもそのまま継続利用できます。

- **Q. 移行作業中に既存ドメインは利用できますか？**
- **A. はい、利用できます。**
  - SambaをDCに追加する作業などで既存のADドメインを止める必要はありません。
  - しかし、FSMOを転送するときはユーザー追加などはできる限りしないようにしましょう。

Samba 4による Active Directory構築

- 最新のWindows 8も含め、Windows Serverと同等のドメイン認証機能を利用可能

- Samba 3 で必要であったレジストリ変更操作は不要
  - HKLM¥SYSTEM¥CurrentControlSet¥Services¥Lanman¥Workstation¥Parameters¥DNSNameResolutionRequired = 0
  - HKLM¥SYSTEM¥CurrentControlSet¥Services¥Lanman¥Workstation¥Parameters¥DomainCompatibilityMode = 1



- Linux上は samba-toolコマンド
  - ドメイン管理系操作をサポート
    - ドメイン管理系
      - domain、drs、fsmo、gpo、sites
    - ユーザー・グループ管理系
      - user、group
    - DNS管理
      - dns
    - ouの追加については未サポート
- Windows端末からはMicrosoft標準ツール(RSAT)
  - Windows Vista、7、8用それぞれ提供

- DCとクライアント間の時刻は同期させる
  - クライアントをDCの時刻に合わせる

- Samba4
  - # service ntpd start
  - # chkconfig ntpd on
    - ntpの設定については今回は省略
- Windowsクライアント（Windows7）
  - ドメインに参加するとDCと自動的に時刻同期を行う
    - HKLM¥SYSTEM¥CurrentControlSet¥Services¥W32Time¥Parameters¥Type = NT5DS（ドメイン参加前はNTP）

    http://support.microsoft.com/kb/223184/ja

Samba 4 AD DC 設定情報

項目	設定内容
サーバー名	cent65k1
DNS名	samba4dom.com
NT ドメイン名	SAMBA4DOM
DNS フォワード先	192.168.2.2
サーバーの役割	DC
Administratorのパスワード	P@ssw0rd

- Administratorユーザーのパスワードは複雑性を満たす必要あり
  - 英大文字/英小文字/数字/記号のうち、3種類以上を含む
  - 文字列長は7文字以上

- 対話形式でドメイン設定
  - samba-tool コマンドでドメイン設定する際、「--interactive」を利用
    - 利用しない場合、オプションで個々に指定

```
# /opt/osstech/bin/samba-tool domain provision --interactive --use-rfc2307
```

- Realm [SAMBA4DOM.COM]:
- Domain [SAMBA4DOM]:
- Server Role (dc, member, standalone) [dc]:
- DNS backend (SAMBA_INTERNAL, BIND9_FLATFILE, BIND9_DLZ, NONE) [SAMBA_INTERNAL]:
- DNS forwarder IP address (write 'none' to disable forwarding) [XX.XX.XX.XX]:
- Administrator password:
- Retype password:

Samba 4 AD DC起動/確認1

OSSTech

- /etc/krb5.confと/etc/resolv.conf を修正
- Samba4プロセス起動

```
# service osstech-samba start
```

- smbclientによるアクセス確認

```
# /opt/osstech/bin/smbclient //localhost/netlogon -U
    Administrator
Enter Administrator's password:
Domain=[SAMBA4DOM] OS=[Unix] Server=[Samba 4.1.0-59.el6]
smb: ¥>
```

Samba 4.1 より、smbclientに「-m SMB2/SMB3」を指定することで SMB2/SMB3プロトコルでの通信も可能。

- Kerberos 確認
  - チケット発行
  - # kinit administrator@SAMBA4DOM.COM
  - Password for administrator@SAMBA4DOM.COM:
  - Warning: Your password will expire in 41 days on Wed Dec 11 01:28:00 2013
  - チケット確認
  - # klist
  - Ticket cache: FILE:/tmp/krb5cc_0
  - Default principal: administrator@SAMBA4DOM.COM
  - Valid starting Expires Service principal
  - 10/30/13 02:32:16 10/30/13 12:32:16 krbtgt/SAMBA4DOM.COM@SAMBA4DOM.COM
  - renew until 11/06/13 02:32:13

Samba 4 AD DC起動/確認3

OSSTech

- SRV、Aレコード確認
  - # host -t SRV _ldap._tcp.samba4dom.com.
  - _ldap._tcp.samba4dom.com has SRV record 0 100 389 takeuchi104.samba4dom.com.
  - # host -t SRV _kerberos._udp.samba4dom.com.
  - _kerberos._udp.samba4dom.com has SRV record 0 100 88 takeuchi104.samba4dom.com.
  - # host -t A takeuchi104.samba4dom.com.
  - takeuchi104.samba4dom.com has address 10.0.104.104

- ユーザーの登録状況を確認
  - # /opt/osstech/bin/samba-tool user list
  - Administrator
  - krbtgt
  - Guest

- ユーザー登録
  - ユーザー名:cui-user1
  - パスワード:Secret123$
  - # /opt/osstech/bin/samba-tool user add cui-user1
  - New Password:
  - Retype Password:
  - User 'cui-user1' created successfully

- オプションを指定して登録
  - ユーザー名:cui-user2
  - パスワード:Secret123$
  - 姓:テスト
  - 名:ユーザー
  - # /opt/osstech/bin/samba-tool user add cui-user2 Secret123$ ￥ --surname=テスト -given-name=ユーザー

    User 'cui-user2' created successfully

他にもオプションは存在するが、ADで登録する時の項目すべてを設定できるわけではない

- root権限によるパスワード強制変更
  - ユーザー名:cui-user1
  - 新パスワード:P@ssw0rd
  - # /opt/osstech/bin/samba-tool user setpassword ¥ --newpassword=P@ssw0rd cui-user1

    Changed password OK

- ユーザー自身によるパスワード変更
  - 該当ユーザーの認証やポリシー制限あり
    - ユーザー名:cui-user2
    - 元パスワード:Secret123$
    - 新パスワード:P@ssw0rd

```
$ /opt/osstech/bin/samba-tool user password ¥  --
  newpassword=P@ssword --password=Secret123$
Changed password OK
```

- ただし、ユーザー作成直後は、デフォルトのパスワードポリシーによりエラーとなる。
- ERROR: Failed to change password : samr_ChangePasswordUser3 for ¥ 'SAMBA4DOM¥cui-user2' failed: NT_STATUS_PASSWORD_RESTRICTION

samba-toolコマンドによるグループ管理 1

- グループの登録状況を確認
  - # /opt/osstech/bin/samba-tool group list
  - Domain Computers
  - Domain Admins
  - Domain Users

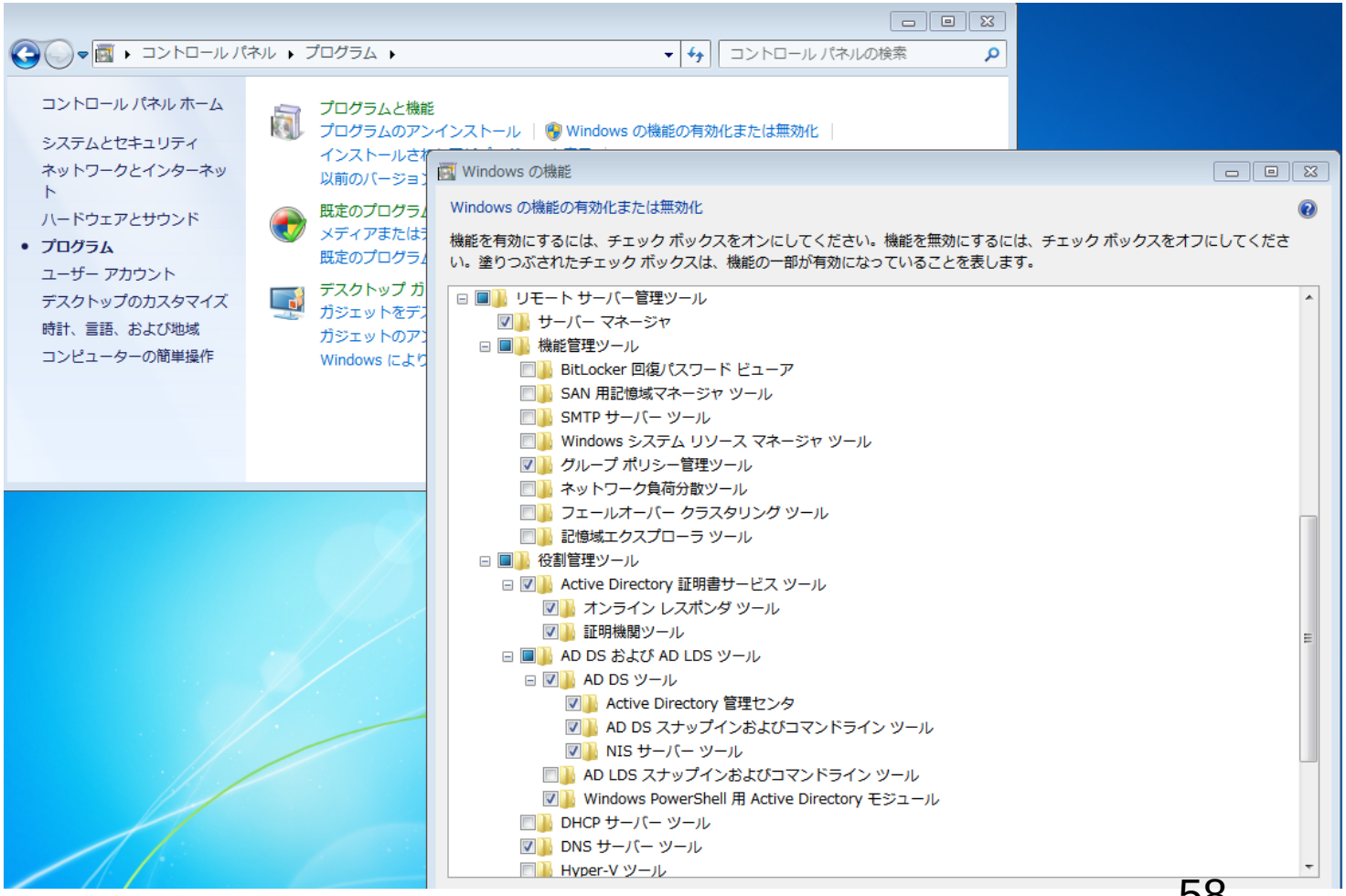
- グループ登録
  - グループ名:cui-group1
  - # /opt/osstech/bin/samba-tool group add cui-group1
  - Added group cui-group1

- グループにメンバーを所属
  - # /opt/osstech/bin/samba-tool group addmembers cui-group1 ￥ cui-user1,cui-user2
  - Added members to group cui-group1
- グループのメンバーを確認
  - # /opt/osstech/bin/samba-tool group listmembers cui-group1
  - cui-user1
  - cui-user2

Windows7をドメイン参加させ、ADを管理

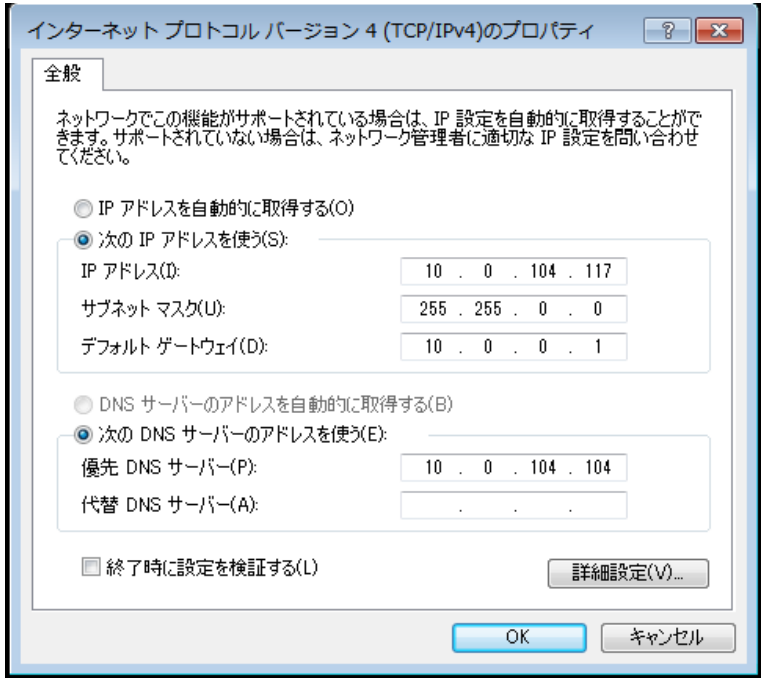
RSATを利用するための準備

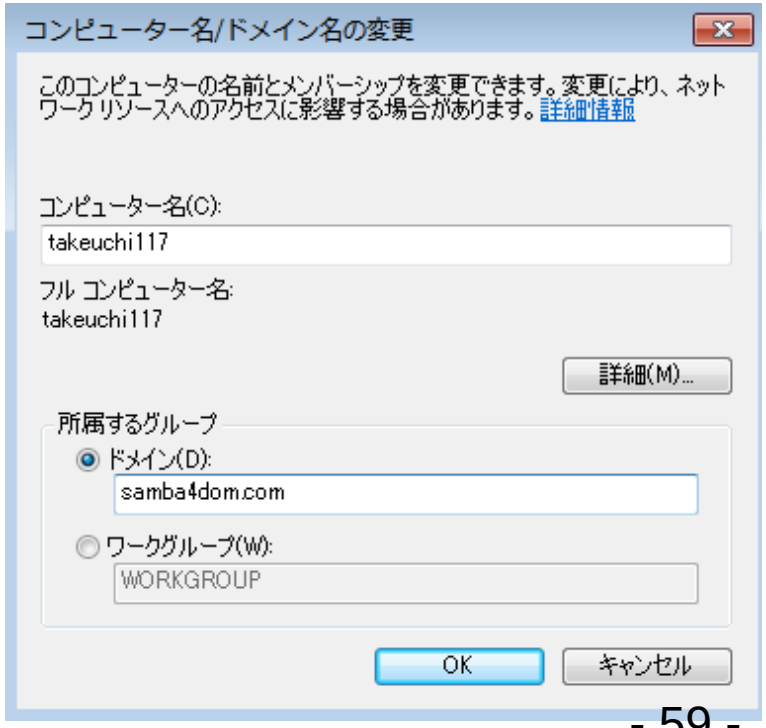
- RSATはインストールしただけでは利用不可
  - [コントロールパネル]-[プログラム]-[Windowsの機能の有効化または無効化]で[リモートサーバー管理ツール]を有効に



Windows7をドメイン参加

- Windows7をSamba4での AD DCにドメイン参加
  - DNSサーバーをSamba4サーバーに変更
  - ドメインをsamba4dom.comに変更





RSATによる情報確認

- RSATの起動は[コントロールパネル]-[システムとセキュリティ]-[管理ツール]
  - samba-toolコマンドで登録した情報の確認
  - Computersの確認
  - DNSマネージャー

RSATによる管理

- 組織単位(ou)の新規追加
- ユーザー登録
- グループ登録
  - グループにメンバー追加
- GPOを設定
  - Default Domain Policy を利用

- GPOに設定項目が存在するが利用不可
- samba-toolコマンドで設定する必要がある
  - 現状のポリシー確認
    - # /opt/osstech/bin/samba-tool domain passwordsettings show

項目	ポリシー内容	設定内容
Password complexity	パスワードの複雑性	on
Store plaintext passwords	暗号化を元に戻せる状態で パスワードを保存	off
Password history length	パスワードの履歴保持	24
Minimum password length	パスワードの長さ	7
Minimum password age (days)	パスワードの変更禁止期間（日）	1
Maximum password age (days)	パスワードの有効期間（日）	42

パスワードポリシー 2

```
# /opt/osstech/bin/samba-tool domain passwordsettings set ¥
 --complexity=on/off
--store-plaintext=on/off
--history-length=回数
--min-pwd-length=長さ
--min-pwd-age=日数
--max-pwd-age=日数
```

Windows AD DCからSamba4 AD DCに切替

Windows AD DC 設定情報

項目	設定内容
サーバー名	takeuchi28
DNS名	testdom.com
NT ドメイン名	TESTDOM
realm	testdom.com
サーバーの役割	DC
Administratorのパスワード	P@ssw0rd

Samba4をWindows AD DCに参加

OSSTech

```
# /opt/osstech/bin/samba-tool domain join testdom.com DC ¥  --
    realm=testdom.com -U testdom¥¥Administrator
Finding a writeable DC for domain 'testdom.com'
Found DC takeuchi28.testdom.com
Password for [TESTDOM¥Administrator]:

workgroup is TESTDOM
realm is testdom.com
....
Joined domain TESTDOM (SID S-1-5-21-325366957-3734438017-426939442) as a DC
```

- 起動
  - # service osstech-samba start
- SRV、Aレコード確認
  - # host -t SRV _ldap._tcp.testdom.com.
  - _ldap._tcp.testdom.com has SRV record 0 100 389 takeuchi28.testdom.com.
  - _ldap._tcp.testdom.com has SRV record 0 100 389 takeuchi114.testdom.com.
  - # host -t SRV _kerberos._udp.testdom.com.
  - _kerberos._udp.testdom.com has SRV record 0 100 88 takeuchi28.testdom.com.
  - _kerberos._udp.testdom.com has SRV record 0 100 88 takeuchi114.testdom.com.
  - # host -t A takeuchi114.testdom.com.
  - takeuchi114.testdom.com has address 10.0.104.114

操作マスターをSamba4に移動 1

OSSTech

- 現状の操作マスターの確認

```
# /opt/osstech/bin/samba-tool fsmo show
InfrastructureMasterRole owner: CN=NTDS  Settings, ¥ CN=TAKEUCHI28,CN=Servers,CN=Default-
    First-Site-Name,CN=Sites, ¥ CN=Configuration,DC=testdom,DC=com
RidAllocationMasterRole owner: CN=NTDS Settings, ¥ CN=TAKEUCHI28,CN=Servers,CN=Default-
    First-Site-Name,CN=Sites, ¥ CN=Configuration,DC=testdom,DC=com
PdcEmulationMasterRole owner: CN=NTDS Settings, ¥ CN=TAKEUCHI28,CN=Servers,CN=Default-
    First-Site-Name,CN=Sites, ¥ CN=Configuration,DC=testdom,DC=com
DomainNamingMasterRole owner: CN=NTDS Settings, ¥ CN=TAKEUCHI28,CN=Servers,CN=Default-
    First-Site-Name,CN=Sites, ¥ CN=Configuration,DC=testdom,DC=com
SchemaMasterRole owner: CN=NTDS Settings, ¥ CN=TAKEUCHI28,CN=Servers,CN=Default-First-
    Site-Name,CN=Sites,¥ CN=Configuration,DC=testdom,DC=com
```

操作マスターをSamba4に移動 2

OSSTech

- 操作マスターの移動

```
# /opt/osstech/bin/samba-tool fsmo transfer -role=all
```

- 移動後の操作マスターの確認

```
# /opt/osstech/bin/samba-tool fsmo show
InfrastructureMasterRole owner: CN=NTDS Settings, ¥ CN=TAKEUCHI114,CN=Servers,CN=Default-
    First-Site-Name,CN=Sites, ¥ CN=Configuration,DC=testdom,DC=com
RidAllocationMasterRole owner: CN=NTDS Settings, ¥ CN=TAKEUCHI114,CN=Servers,CN=Default-
    First-Site-Name,CN=Sites, ¥ CN=Configuration,DC=testdom,DC=com
PdcEmulationMasterRole owner: CN=NTDS Settings, ¥ CN=TAKEUCHI114,CN=Servers,CN=Default-
    First-Site-Name,CN=Sites, ¥ CN=Configuration,DC=testdom,DC=com
DomainNamingMasterRole owner: CN=NTDS Settings, ¥
    CN=TAKEUCHI114,CN=Servers,CN=Default-First-Site-Name,CN=Sites, ¥
    CN=Configuration,DC=testdom,DC=com
SchemaMasterRole owner: CN=NTDS Settings, ¥ CN=TAKEUCHI114,CN=Servers,CN=Default-First-
    Site-Name,CN=Sites, ¥ CN=Configuration,DC=testdom,DC=com
```

ユーザー登録/確認

- samba-toolコマンドでユーザー登録
  - ユーザー名:samba-add
  - パスワード:P@ssw0rd
  - # /opt/osstech/bin/samba-tool user add samba-add P@ssw0rd
- RSAT(Windows Server 2008 R2上)よりユーザー登録
  - ユーザー名:windows-add
  - パスワード:P@ssord
- Windows7 でドメインログオン
  - windows-add、samba-add両ユーザーでログオン

Windows AD DCをシャットダウン後

- samba-toolコマンドでユーザー登録
  - ユーザー名:samba-add1
  - パスワード:P@ssw0rd
    - # /opt/osstech/bin/samba-tool user add samba-add1 P@ssw0rd

- Windows7 でドメインログオン
  - samba-add1ユーザーでログオン

Windows AD DCにてdcpromoより本来、[Active Directoryドメインサービス]のアンインストールが可能だが、現状 DC=ForestZones の転送で失敗する為、今回はシャットダウンすることとする

付録.

Samba vs Windows比較表

参考資料：日経BP

Samba 4によるWindowsネットワーク構築

http://itpro.nikkeibp.co.jp/article/COLUMN/20131018/511929/

表１．SambaとWindowsサーバーとの比較

機能	Samba 3.6	Samba 4.1	Windows Server 2008/2012
リソース管理			
ユーザー情報の格納場所	LDAP、簡易DB、テキストなどが利用可能	内蔵LDAP 外部のLDAPも利用できるが制限有り	Active Diorectory または 内部の独自DB
ユーザー情報の複製機能	△LDAPの複製機能を利用 Windows互換の複製機能は持たない	○ Windows ADとも複製可能	○
日本語ユーザー名	△利用は推奨しないが username map機能を使えば可能	○	○
日本語グループ名	△利用は推奨しないが username map機能を使えば可能	○	○
グローバルユーザー／ローカルユーザー	○	○	○
グローバルグループ／ローカルグループ	○	○	○
ネステッドグループ（グループの中にグループを入れ子にするような階層化）	△AD互換のグループの入れ子はできない、一部NT互換のネステッドグループ（ローカルグループの中にグローバルグループを入れ子にするような階層化）は可能だが互換性も低く、GUIで管理するのは難しい	○	○
日本語コンピュータ名	△利用は推奨しないが username map機能を使えば可能	○	○
通信プロトコル／認証方式			
LANMAN認証	○	○	○
NTLM認証	○	○	○
NTLMv2認証	○	○	○
Kerberos5認証	△メンバサーバの時のみ可能	○	○
SMB2	○	○ サーバーサイドコピー対応	○
SMB3	×	○	○
セキュアチャネル	○	○	○
SMB署名	○	○	○
SPNEGO（RFC2478で規定されたSimple and Protected NEGOciation）	○	○	○
ドメイン管理			
ドメインレベル	NTドメイン	Windows 2008 ADドメイン互換	Windows 2008/2012 ADドメイン
ドメインログオン	○	○	○
PDC（プライマリドメインコントローラ）	○	○FSMO	○FSMO
BDC（バックアップドメインコントローラ）	○	○GC	○GC
ログオンスクリプト	◎ログオンスクリプトの動的生成／変更可能	◎ログオンスクリプトの動的生成／変更可能	○固定スクリプトを実行可能
移動プロファイル	◎読み込み専用プロファイルもサポート	○	○
NT 4.0相当のユーザーポリシー（NT 4.0／2000／XP）	○	×	×
Windows 98相当のグループポリシー（95／98／Me）	○	×	×
Windows 2008相当のグループポリシー	×	○	○
複雑なパスワードの強制	◎外部スクリプトを使って カスタマイズ可能	○	○
パスワード履歴	○	○	○
明示的な片方向の信頼関係	○	△開発中	○
推移的な双方向の信頼関係	×	△開発中	○
ファイル／プリントサーバ機能			
ユーザー／グループによる容量制限	◎ディレクトリ単位にも対処可能	◎ディレクトリ単位にも対処可能	○
論理ボリュームマネージャ	○Sambaが動作するOSに依存	○Sambaが動作するOSに依存	○
ボリュームシャドーコピー（スナップショット）機能	○Sambaが動作するOSに依存	○Sambaが動作するOSに依存	○NTFS必須
ゴミ箱機能	○	○	×
マッキントッシュ連携	○Netatalkをインストールすることで可能	○Netatalkをインストールすることで可能	○マッキントッシュサービスをインストールすることで可能
UNIX NFS連携	○カーネルレベルによる OPLOCK連携可能	○カーネルレベルによる OPLOCK連携可能	○Service for UNIX(SFU,SUA)をインストールすることで可能
ユーザーホーム機能	○	○	○
MS-DFS（ルートおよびサブディレクトリ）	○	○	○
MS-DFS Proxy	○	○	○
ACL機能 （ユーザー／グループによるアクセス制御）	○Sambaが動作するOSに依存 またはVFSモジュールでSamba上でのNTFS互換ACLサポート	○Sambaが動作するOSに依存 またはVFSモジュールでSamba上での NTFS互換ACLサポート	○NTFS必須
ホスト名によるアクセス制御	○	○	×
日本語ディレクトリ／ファイル名	○	○	○
READ権のないファイルを見えなくする	○	○	○
WRITE権のないファイルを見えなくする	○	○	×
ユーザーモジュールによる共有機能の拡張・カスタマイズ	○標準で監査機能、ウィルスチェックなどを搭載。1つの共有に複数のモジュールをロード可能	○標準で監査機能、ウィルスチェックなどを搭載。1つの共有に複数のモジュールをロード可能	○WINAPIでユーザーが作成可能
同一サーバーに複数のNetBIOS名を付ける	○smb.confで容易に指定可能	○smb.confで容易に指定可能	△レジストリ変更が必要でサポート対象外
スプールしながらの印刷	×	×	○
PDFライター機能	○GhostScriptとの連携	○GhostScriptとの連携	×
プリンタドライバ配布機能	○	○	○
名前解決機能			
DNSサーバー	×	○内蔵と外部の両方が利用可能	○
WINSサーバー	○	○	○
WINSクライアント	○	○	○
WINS複製	△外部スクリプトによりPushは可能	○	○
WINS静的マッピング	○ wins.datの直接編集	○	○
WINSとDDNSとの連携	○ wins hook機能	○	×
ブラウジング			
ドメインマスタブラウザ	◎ワークグループ構成でも可能	◎ワークグループ構成でも可能	○
リモートアナウンス	◎任意のワークグループ、ドメインにも可	◎任意のワークグループ、ドメインにも可	○信頼するドメインのみ
ポテンシャルブラウザ	○	○	○