LinuC/LPIC レベル3 Specialty

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

LPI-JAPAN

© Open Source Solution Technology Corporation 2018 All Rights Reserved.

Part 1.

300試験 出題範囲

LPI-JAPAN

© Open Source Solution Technology Corporation 2018 All Rights Reserved.

300試験範囲：出題範囲詳細

- 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

LinuC

© Open Source Solution Technology Corporation 2018 All Rights Reserved.

LDAP概念と設計入門

LPI-JAPAN

© Open Source Solution Technology Corporation 2018 All Rights Reserved.

概念 LDAPとは?

- Lightweight Directory Access Protocol
  - 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)
  - 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・サービスをを軽量化した実装
  - X.500のDAP以外の機能は提供されない
- LDAPの用途
  - アカウント情報等の管理情報の集約 (ディレクトリ機能)
  - ユーザー認証、電話帳、リソース管理などに利用
- 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

© Open Source Solution Technology Corporation 2018 All Rights Reserved.

LDAPの関連RFC

- RFCにより標準化 → 多種多様な機器・ソフトでの対応
  - RFC2307（LDAP基本スキーマ）
  - RFC2696（ページリザルトオペレーション）
  - RFC2849（LDIFフォーマット）
  - RFC3062（パスワード拡張オペレーション）
  - RFC3673、3698（LDAP v3）
  - RFC4511（LDAPプロトコル）
  - RFC4512（LDAP DIT）
  - RFC4513（LDAP 認証）

LinuC

© Open Source Solution Technology Corporation 2018 All Rights Reserved.

LDAPの通信経路

通信プロトコル (URI Scheme)	接続ポート (TCP/UDP Port)
LDAP (非暗号化) LDAP StartTLS(暗号化通信)	389/TCP
LDAPS (暗号化通信)	636/TCP
CLDAP ＊ Active Directroryで一部利用	389/UDP
LDAPi	IPC（Inter-Process Communication :プロセス間通信）

LinuC

© Open Source Solution Technology Corporation 2018 All Rights Reserved.

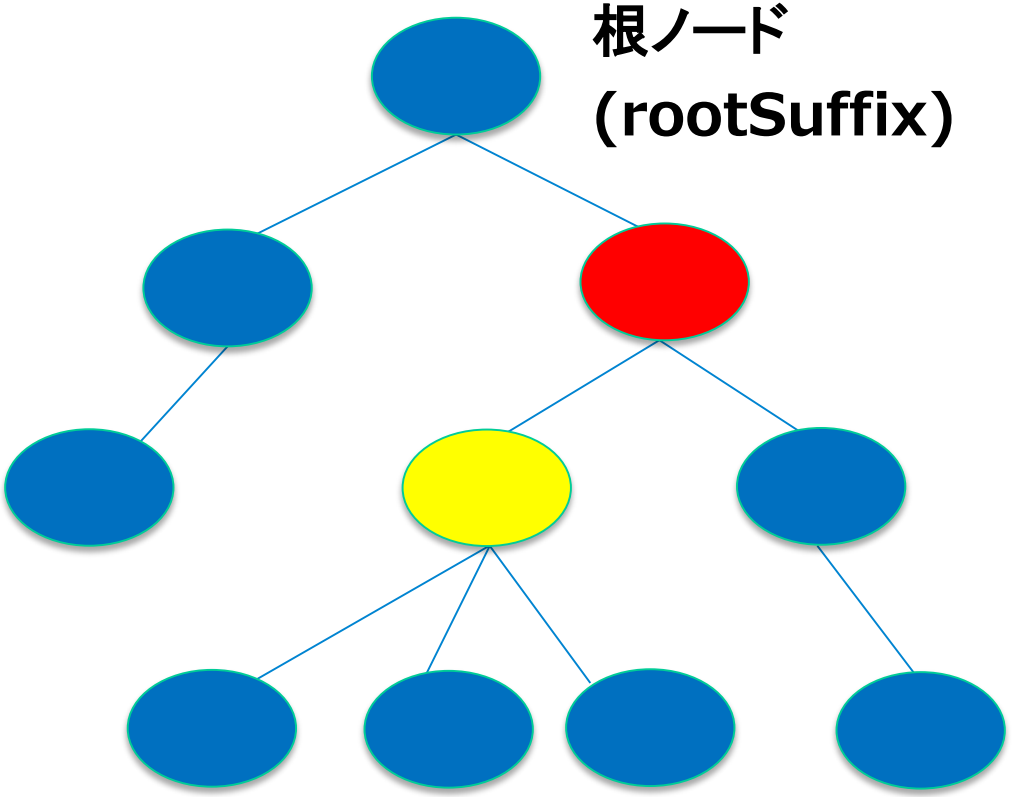
LDAPのデータ構造

LPI-JAPAN

© Open Source Solution Technology Corporation 2018 All Rights Reserved.

LDAPのデータ構造

- DIT (Directory Information Tree) によるツリー構造
  - ツリーの各ノードがLDAPのエントリー
  - 各ノードで完結した情報

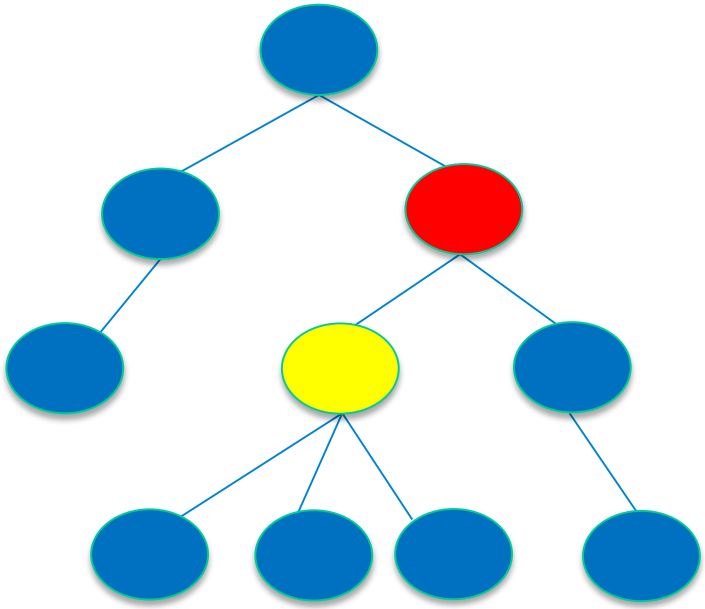


© Open Source Solution Technology Corporation 2018 All Rights Reserved.

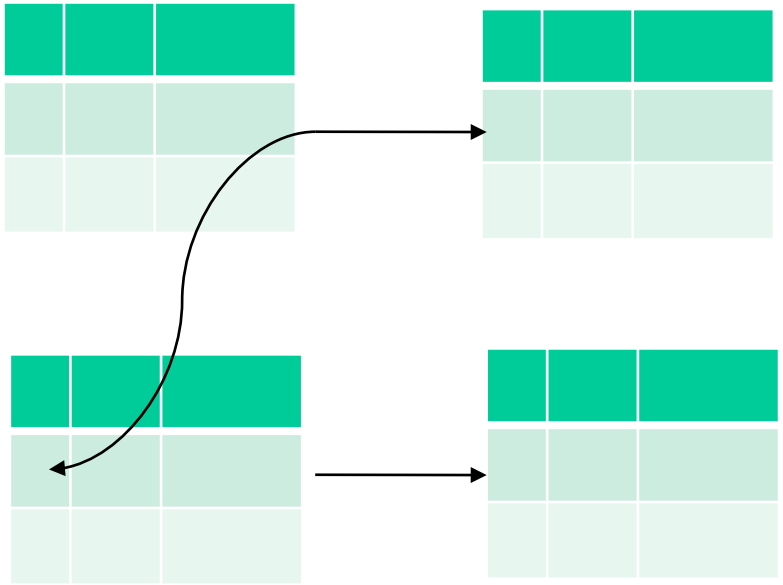
LDAP と RDBMS の違い

- LDAPはリレーションを持てない
- トランザクションなど厳密なデータ管理モデルではない
  - 認証と検索に特化したアーキテクチャ

LDAP



RDBMS



© Open Source Solution Technology Corporation 2018 All Rights Reserved.

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

© Open Source Solution Technology Corporation 2018 All Rights Reserved.

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

© Open Source Solution Technology Corporation 2018 All Rights Reserved.

LDAPのエントリー構造

LPI-JAPAN

© Open Source Solution Technology Corporation 2018 All Rights Reserved.

エントリー構造

- **LDAPスキーマで定義された値で構成**

エントリーの構成要素	内容
DN (Distinguished Name：識別子)	LDAPのDIT上の位置を表す エントリーの任意の属性を利用可能
オブジェクトクラス (objectClass)	エントリーの構成を決定する
属性 (attribute)	エントリーに保持する各種の値 objectClassの定義に従って任意の属性を保持可能 DNに利用した値は、必須
管理属性	LDAPシステムが管理用に自動的に付与

© Open Source Solution Technology Corporation 2018 All Rights Reserved.

エントリー構造例

dn : uid=yamada,ou=Users,dc=example,dc=com エントリのDN

objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson

← オブジェクトクラス

uid: yamada

DNに使っている属性

cn: 山田 太郎
sn: 山田
mail: yamada@example.com

← 属性

structuralObjectClass: inetOrgPerson
entryUUID: 6f640329-1508-4f98-9048-9d857...
creatorsName: cn=Manager,dc=example,dc=com
createTimestamp: 20150915210052Z
modifiersName: cn=Manager,dc=example,dc=com
modifyTimestamp: 20150915220352Z

← 管理属性

© Open Source Solution Technology Corporation 2018 All Rights Reserved.

LDAPのスキーマ設計

LPI-JAPAN

© Open Source Solution Technology Corporation 2018 All Rights Reserved.

スキーマ定義

- エントリーの構造を定義
  - 利用できる値の種類や、検索条件など
- 標準的なスキーマをあらかじめ用意
  - 足りなければ拡張スキーマとして定義
- OpenLDAPでは core.schemaはソースコードに組み込み
- 定義する値の種類

定義	内容
objectClass	属性の入れ物 1つ以上のAttributeTypeを持つ
AttributeType	各属性の定義

© Open Source Solution Technology Corporation 2018 All Rights Reserved.

オブジェクトクラス と 属性

- オブジェクトクラスに定義された属性をエントリに利用できる
- オブジェクトクラスにはMUST属性・MAY属性がある

dn : uid=yamada,ou=Users,dc=example,dc=com ← エントリのDN

objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
← オブジェクトクラス

uid: yamada
cn: 山田 太郎
sn: 山田
mail: yamada@example.com
← 属性

© Open Source Solution Technology Corporation 2018 All Rights Reserved.

属性の定義 (AttributeType)

- 属性を構成する要素
  - OID
  - NAME
  - DESC
  - SUP
  - 照合規則
  - SYNTAX
  - 単一値制限、長さ制限

© Open Source Solution Technology Corporation 2018 All Rights Reserved.

属性の基本要素(1)

定義	概要	備考
OID	属性の一意な値(重複禁止) IANAで定義	独自のOIDを定義する場合、IANAからOIDを取得
NAME	属性の名前	
DESC	属性の説明	

OIDの申請は以下のURLより

http://pen.iana.org/pen/PenApplication.page

© Open Source Solution Technology Corporation 2018 All Rights Reserved.

属性の基本要素(2)

定義	概要	備考
照合規則 ・EQUALITY(一致) ・ORDERING(順序) ・SUBSTR(部分一致)	属性の検索方法	照合規則が適切に定義されていない場合、属性を検索できない
文法 (SYNTAX)	数値・文字種など、属性に含める値の制約	文法に定義されていない文字・形式は保存できない
単一値制限 (SINGLE-VALUE)	1エントリに同一属性は1つのみに制限する場合に利用	
管理属性 (NO-USER-MODIFICATION)	ユーザーによる更新不可	通常は利用しない

http://www.openldap.org/doc/admin24/schema.html

© Open Source Solution Technology Corporation 2018 All Rights Reserved.

照合規則：EQUALITY

名前	説明
caseIgnoreMatch	英大小文字区別なし･スペース無視
caseExactMatch	英大小文字区別あり･スペース無視
caseIgnoreIA5Match	ASCII文字列･英大小文字区別なし･スペース無視
caseExactIA5Match	ASCII文字列･英大小文字区別あり･スペース無視
numericStringMatch	数値文字列
distinguishedNameMatch	DN形式

他

© Open Source Solution Technology Corporation 2018 All Rights Reserved.

照合規則：ORDERING / SUBSTR

ORDERING

名前	説明
caseIgnoreOrderingMatch	英大小文字区別なし･スペース無視
caseExactOrderingMatch	英大小文字区別あり･スペース無視
numericStrringOrderingMat	数値文字列

SUBSTR

名前	説明
caseIgnoreSubstringsMatch	英大小文字区別なし･スペース無視
caseExactSubstringsMatch	英大小文字区別あり･スペース無視
numericStrringSubstringsM	数値文字列

© Open Source Solution Technology Corporation 2018 All Rights Reserved.

OID	説明
1.3.6.1.4.1.1466.115.121.1.7	TRUE / FALSE
1.3.6.1.4.1.1466.115.121.1.12	DN形式
1.3.6.1.4.1.1466.115.121.1.15	UTF-8文字列
1.3.6.1.4.1.1466.115.121.1.26	ASCII文字列
1.3.6.1.4.1.1466.115.121.1.27	整数値
1.3.6.1.4.1.1466.115.121.1.36	数値文字列

他

© Open Source Solution Technology Corporation 2018 All Rights Reserved.

属性定義例

■「description」の定義

attributetype (2.5.4.13	OIDの定義
NAME 'description'	オブジェクト名
DESC 'RFC2256: descriptive information'	説明
EQUALITY caseIgnoreMatch	照合規則(一致)
SUBSTR caseIgnoreSubStringsMatch	照合規則(部分一致)
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 {1024}	文法

© Open Source Solution Technology Corporation 2018 All Rights Reserved.

オブジェクトクラスの定義 (objectClass)

- objectClassを構成する要素
  - OID
  - NAME
  - DESC
  - SUP
  - 型
  - MUST属性
  - MAY属性

© Open Source Solution Technology Corporation 2018 All Rights Reserved.

オブジェクトクラスの基本要素(1)

定義	概要	備考
OID	属性の一意な値(重複禁止) IANAで定義	独自のOIDを定義する場合、 IANAからOIDを取得
NAME	属性の名前	
DESC	属性の説明	
SUP	継承する上位の属性	定義済みのobjectClassを利用 (特に指定ない場合top)

OIDの申請は以下のURLより

http://pen.iana.org/pen/PenApplication.page

© Open Source Solution Technology Corporation 2018 All Rights Reserved.

オブジェクトクラスの基本要素(2)

定義	概要	備考
型：Abstruct (抽象型)	任意に作成可能 topを既定(SUP)に持つ	
型：Structural (構造型)	Abstruct型のobjectClassを継承 エントリーに1つ定義必須	
型: Auxiliary (補助型)	任意の数を設定可能 補助型のみで構成不可	
MUST属性	エントリーに必ず保持すべき属性	
MAY属性	エントリーが保持可能な属性	

オブジェクトクラスのMUSTにもMAYにも指定されていない属性は保持できない

© Open Source Solution Technology Corporation 2018 All Rights Reserved.

オブジェクトクラス定義例

■「inetOrgPerson」の定義

objectclass (2.16.840.1.113730.3.2.2	OIDの定義
NAME 'inetOrgPerson'	オブジェクト名
DESC 'RFC2798: Internet Organizational Person'	説明
SUP organizationalPerson	継承元クラス
STRUCTURAL	型
MAY (audio $ businessCategory $ carlicense $ departmentNumber $ displayName $	属性名

inetOrgPerson には MUST属性は指定されていないが、継承元のorganizationalPersonで指定されているため、「cn」と「sn」が必須

© Open Source Solution Technology Corporation 2018 All Rights Reserved.

LDIF形式

© Open Source Solution Technology Corporation 2018 All Rights Reserved.

LDIFとは

- LDIF (LDAP Data Interchange Format)
  - RFC2849 で定義
  - LDAPのデータをテキスト形式で表現
  - UTF-8文字列、バイナリ値はBASE64エンコーディング
  - 標準形式と更新形式の表現方法
  - 各エントリは空行1行で区切る
  - LDIFを用いて、LDAPの操作、バックアップなどが可能

© Open Source Solution Technology Corporation 2018 All Rights Reserved.

標準形式

```
dn: uid=yamada,ou=Users,dc=example,dc=com
 objectClass: inetOrgPerson
 uid: yamada
 cn: 山田 太郎
 sn: 山田
 userPassword::
e1NTSEF9IUUrUnBvalZDa2lEbDcwZmtHQmxwa3FieEhlSTFWcUs4K1Rsc...

dn: uid=tanaka,ou=Users,dc=example,dc=co
 objectClass: ......
```

LinuC

© Open Source Solution Technology Corporation 2018 All Rights Reserved.

LDIF：更新形式(概要)

項目	キーワード	説明
changeType	add	エントリ追加
	modify	エントリ変更
	delete	エントリ削除
	modrdn	エントリ移動
modify時の操作種別	add	属性追加
	replace	属性置換
	delete	属性削除

- 1エントリ中の複数の属性を操作する場合、「-」のみの行で区切る

© Open Source Solution Technology Corporation 2018 All Rights Reserved.

LDIFによるエントリ修正

```
dn: uid=yamada,ou=Users,dc=example,dc=com
changetype: modify
add: mail
mail: taro@example.com
-
replace: description
description: 学生
-
delete: gecos
```


© Open Source Solution Technology Corporation 2018 All Rights Reserved.

LDAPの操作

LPI-JAPAN

© Open Source Solution Technology Corporation 2018 All Rights Reserved.

LDAPの操作種別

- 参照系
  - エントリ検索
  - エントリ比較
- 更新系
  - エントリ追加
  - エントリ更新
  - エントリ削除
  - エントリ移動

© Open Source Solution Technology Corporation 2018 All Rights Reserved.

LDAPのコマンド

コマンド名	用途
ldapsearch	LDAPのエントリー、属性などを条件に従って検索し表示する
ldapcompare	指定したDNが、指定した属性の値を保持しているか比較する
ldapadd	LDAPのエントリを新規追加する
ldapmodify	LDAPの既存エントリの内容を更新する
ldapdelete	LDAPの既存エントリを削除する
ldapmodrdn	LDAPの既存エントリのDN(ツリーの場所)を変更する
ldappasswd	LDAPの既存エントリのユーザーのパスワードを変更する
ldapurl	LDAP検索のURL表現を表示する

© Open Source Solution Technology Corporation 2018 All Rights Reserved.

OpenLDAPの標準オプション

オプション	意味
-x	シンプル認証方式で認証する (通常必要)
-D <接続DN>	LDAPに接続する際のユーザーのDNを指定
-W	-Dオプションで指定したユーザーのパスワードを入力する
-h	接続先ホスト名
-H ldap://host	接続先 LDAP URL名 (ldaps://も指定可能)
-b <baseDN>	LDAPツリーの操作対象のベースDN
-f <filename>	LDIFファイル名
<filter>	検索時の検索フィルタ
<attrs>	検索結果に含める属性

© Open Source Solution Technology Corporation 2018 All Rights Reserved.

LDAPコマンドの利用例

■LDAP検索

```
$ ldapsearch -x -W -D “cn=admin,dc=example,dc=com” -H
ldaps://ldap01 -b dc=example,dc=com '(uid=yamada)' uid mail

dn: uid=yamada,ou=Users,dc=example,dc=com
uid: yamada
mail: yamada@example.com
```

■LDAPエントリ追加

```
$ ldapadd -x -W -D  “cn=admin,dc=example,dc=com” -f
testuser01.ldif
```


© Open Source Solution Technology Corporation 2018 All Rights Reserved.

LDAPフィルタ

検索条件		指定例
一致	=	'(uid=yamada)'
部分一致	=xx*	'(uid=ta*)'
順序比較	>=,<=	'(uidNumber>=2000)'
存在	=*	'(objectClass=*)'

論理記号		指定例
AND	&	'(&(gidNumber=2000)(mail=*example.com))'
OR	|	'(|(gidNumber=1000)(gidNumber=3000))'
NOT	!	'(!(gidNumber=2000))'

LinuC

© Open Source Solution Technology Corporation 2018 All Rights Reserved.

OpenLDAPコマンド TIPS

- LDIF表示 桁折り返し禁止

```
$ ldapsearch -x -D “cn=admin,dc=example,dc=com” -LLL -o ldif-nowrap
```

- システム属性表示

```
$ ldapsearch -x -D “cn=admin,dc=exampe,dc=com” '(uid=yamada)' +
```

- LDAP パスワードポリシーエラー確認

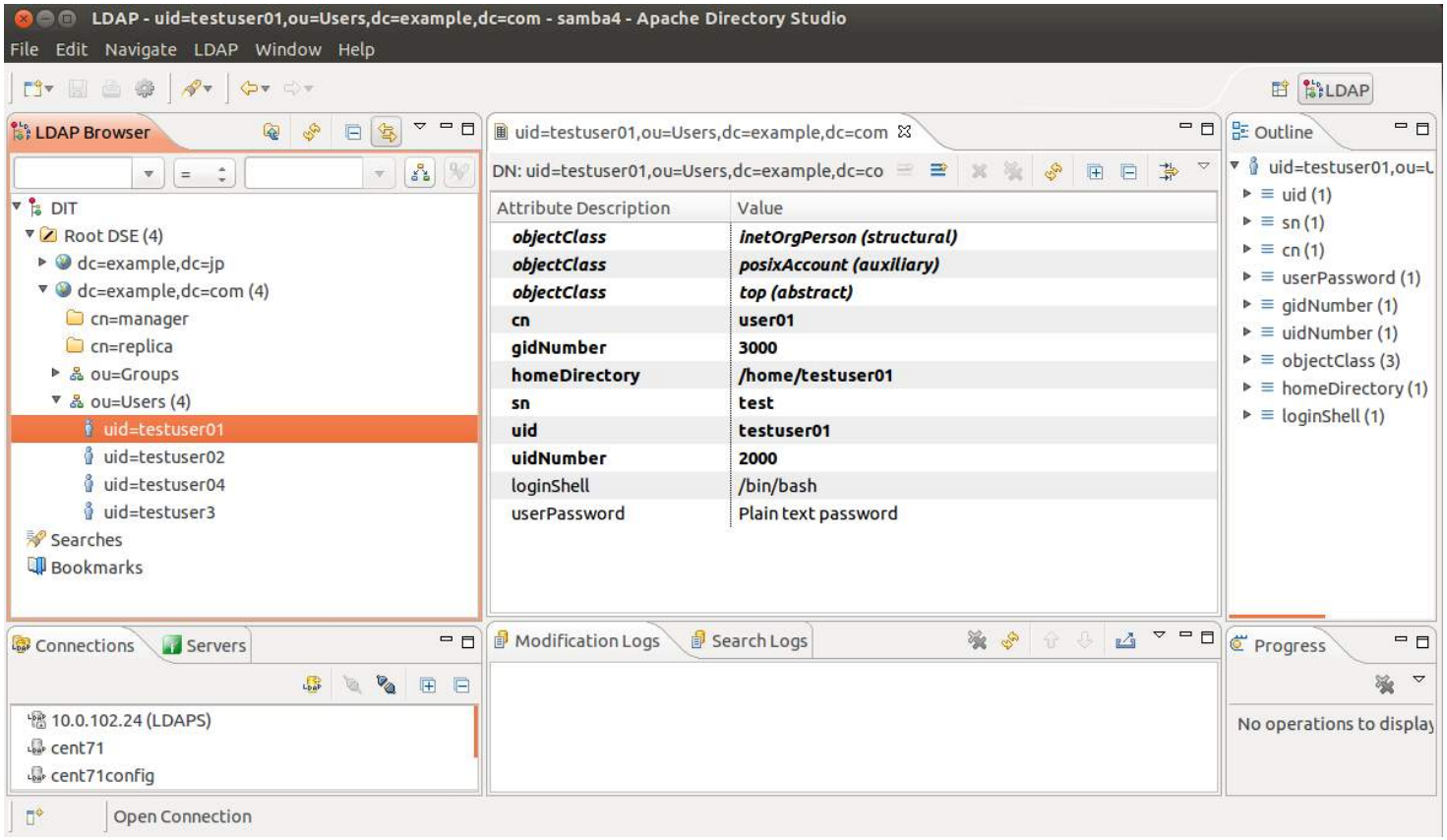
```
$ ldapsearch -x -D “uid=yamada,ou=Users,dc=example,dc=com” -W -e policy
```

LinuC

© Open Source Solution Technology Corporation 2018 All Rights Reserved.

LDAP GUI操作ツール

- Apache Directory Studio
  - https://directory.apache.org/studio/



© Open Source Solution Technology Corporation 2018 All Rights Reserved.

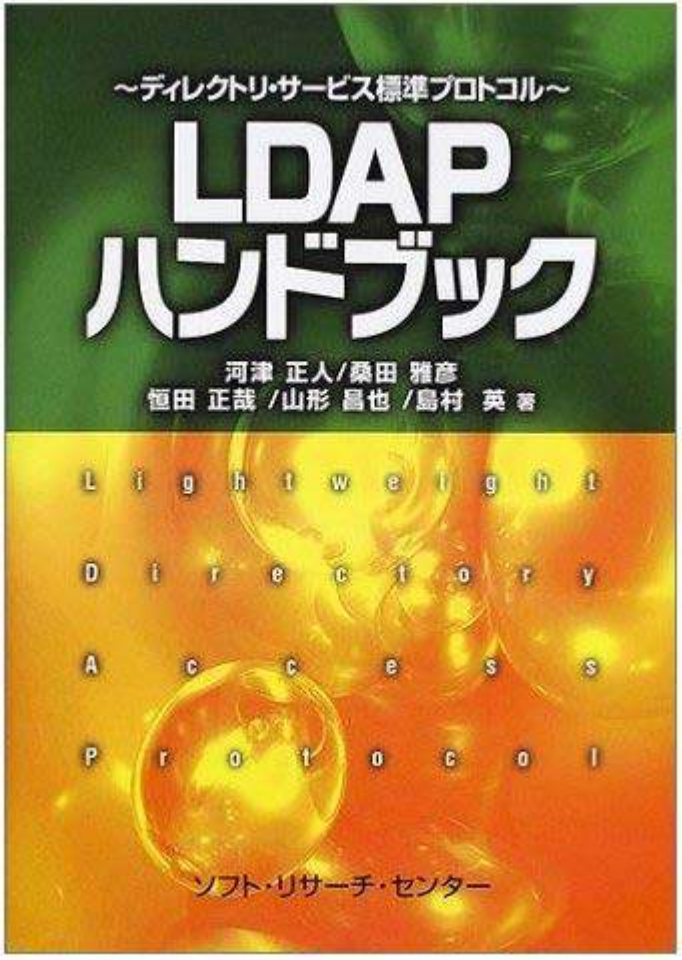
OpenLDAPの管理コマンド

コマンド名	用途
slapadd	LDIFからエントリをデータベースに直接投入する
slapcat	データベースから直接エントリをLDIF形式で出力する
slapindex	インデックス情報を再更新する
slappasswd	平文パスワードをハッシュ化パスワード文字列に変換する
slapacl	ACLの評価結果を表示する
slaptest	設定ファイルの構文チェックを実施する

© Open Source Solution Technology Corporation 2018 All Rights Reserved.

LDAP概念を勉強のための参考書

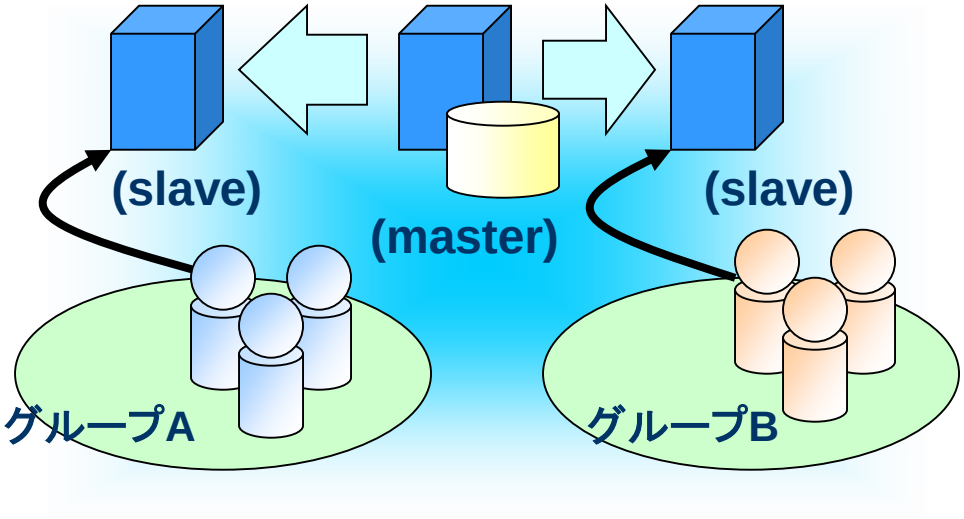
- LDAPハンドブック
  - ディレクトリ・サービス標準プロトコル
  - 出版社: ソフトリサーチセンター（2002/0
  - 発売日：2002/03



© Open Source Solution Technology Corporation 2018 All Rights Reserved.

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



© Open Source Solution Technology Corporation 2018 All Rights Reserved.

OpenLDAPのレプリケーション

- 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

© Open Source Solution Technology Corporation 2018 All Rights Reserved.

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

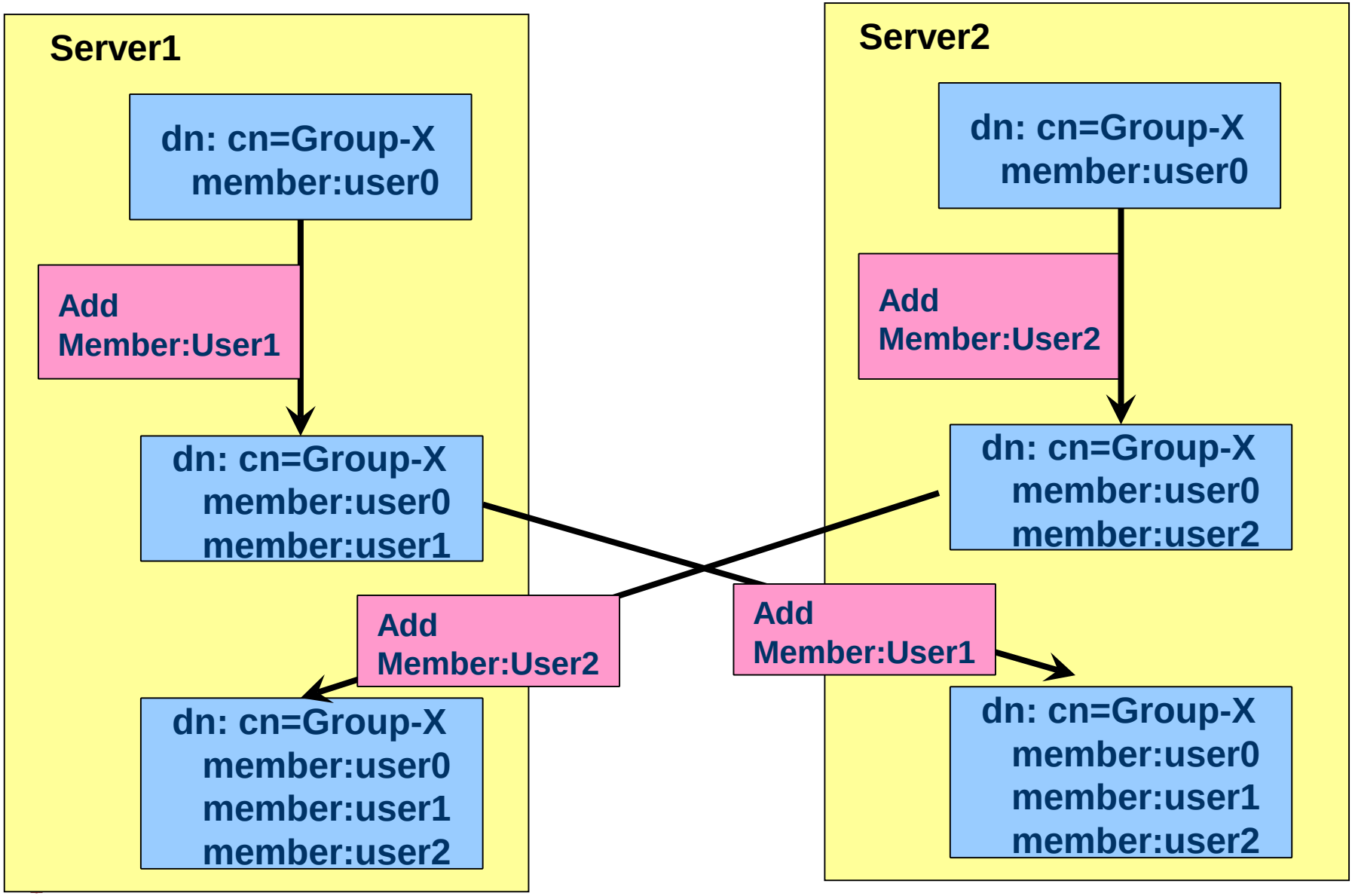
© Open Source Solution Technology Corporation 2018 All Rights Reserved.

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。

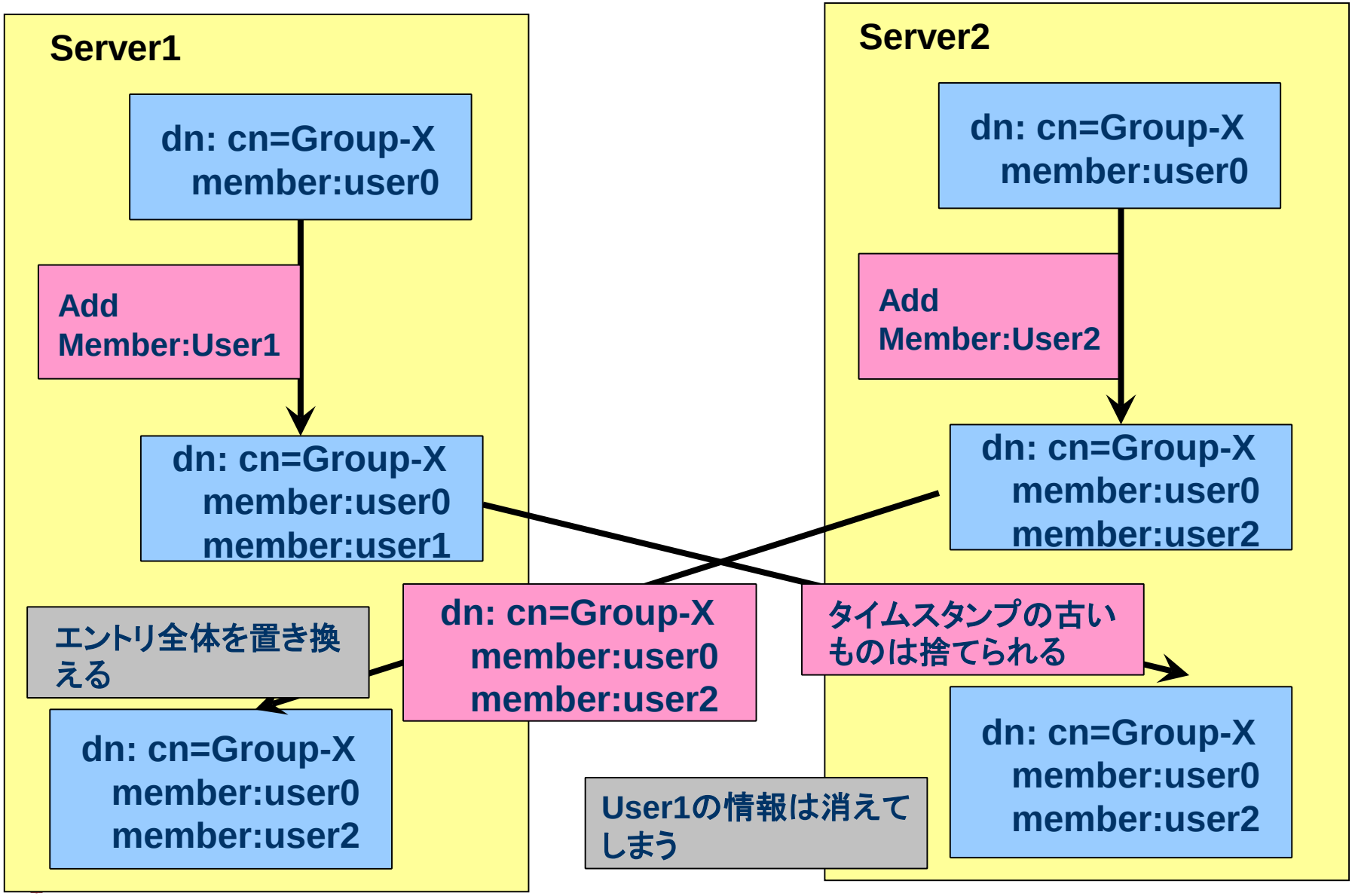
© Open Source Solution Technology Corporation 2018 All Rights Reserved.

商用LDAPの操作ログによるマルチマスターの動き



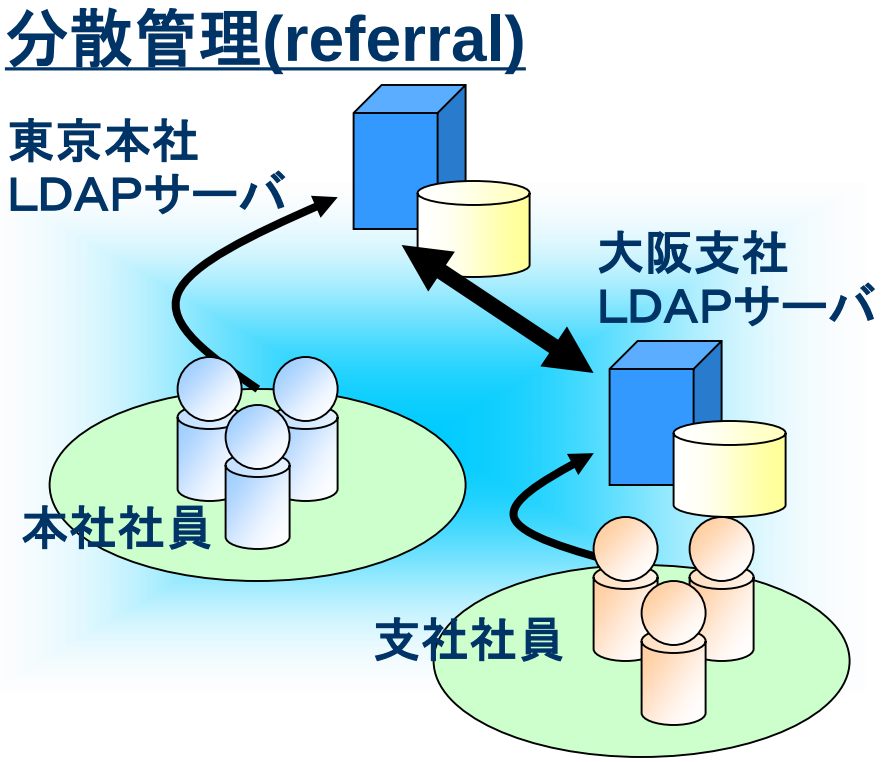
© Open Source Solution Technology Corporation 2018 All Rights Reserved.

OpenLDAPのエントリ複製方式によるミラーモードの動き



© Open Source Solution Technology Corporation 2018 All Rights Reserved.

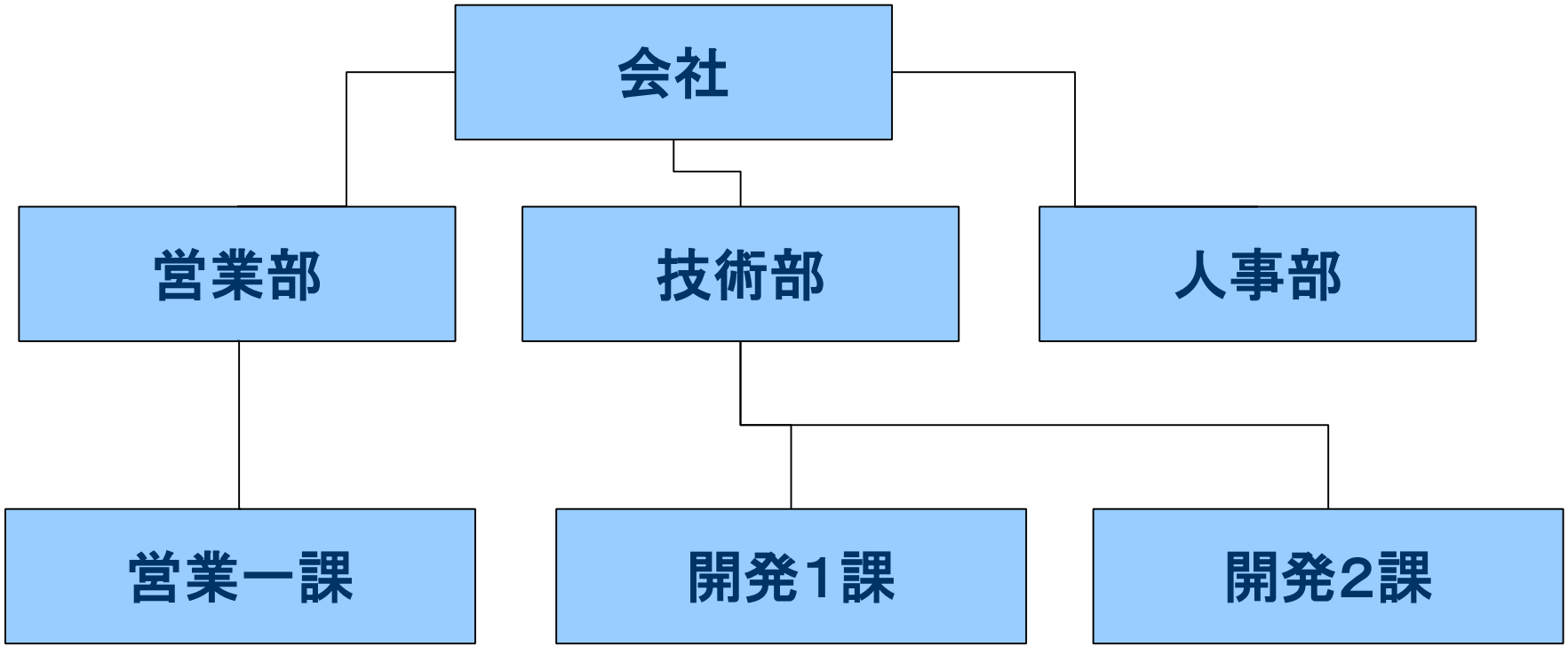
- サブツリー単位でサーバを分散する
  - ldap.confでbaseツリーを変える(負荷分散というよりも管理分散)
  - 1サーバがもつデータ量が減るので更新性能も上がる
  - referralが返ったら別なサーバを見に行くのはプログラム側の責任



© Open Source Solution Technology Corporation 2018 All Rights Reserved.

DIT (Directory information Tree) の概念

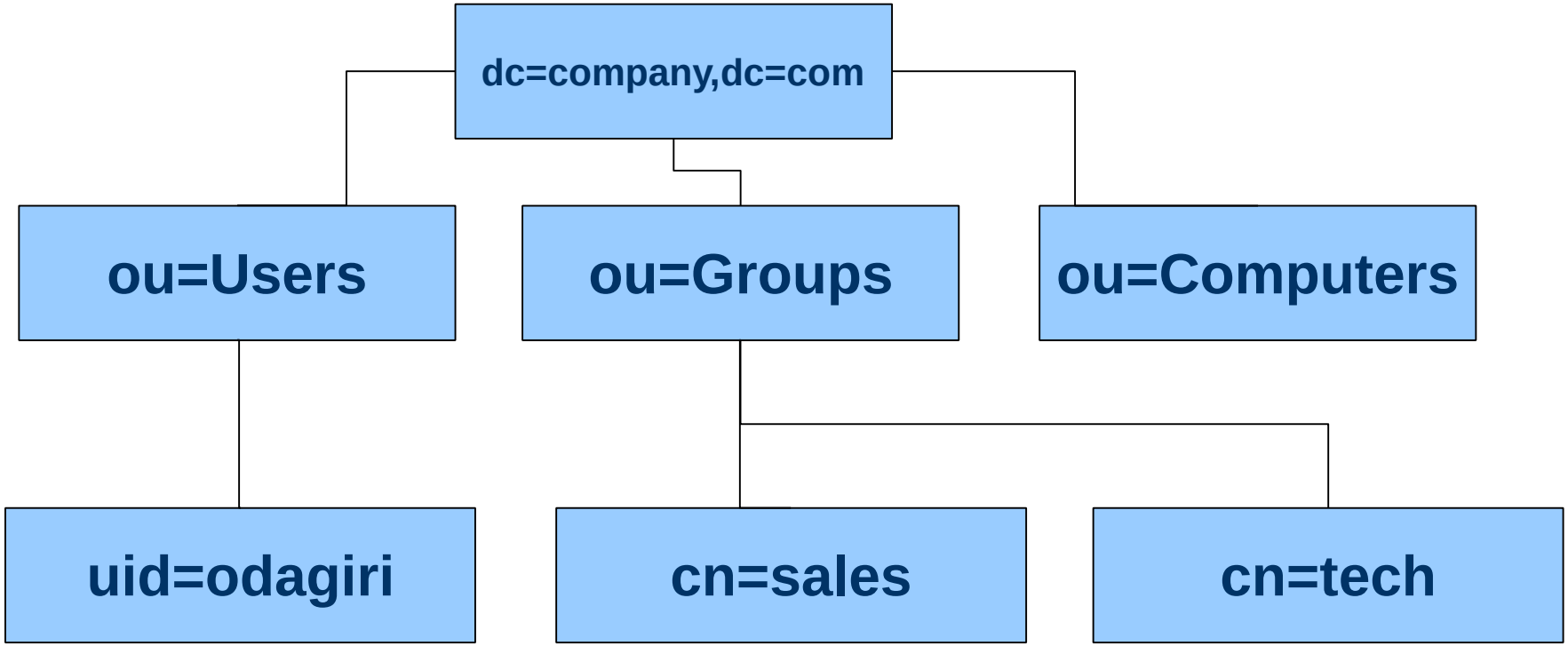
- 概念として組織構造をあげる書籍が多いが. . .



© Open Source Solution Technology Corporation 2018 All Rights Reserved.

DIT (Directory information Tree) の概念

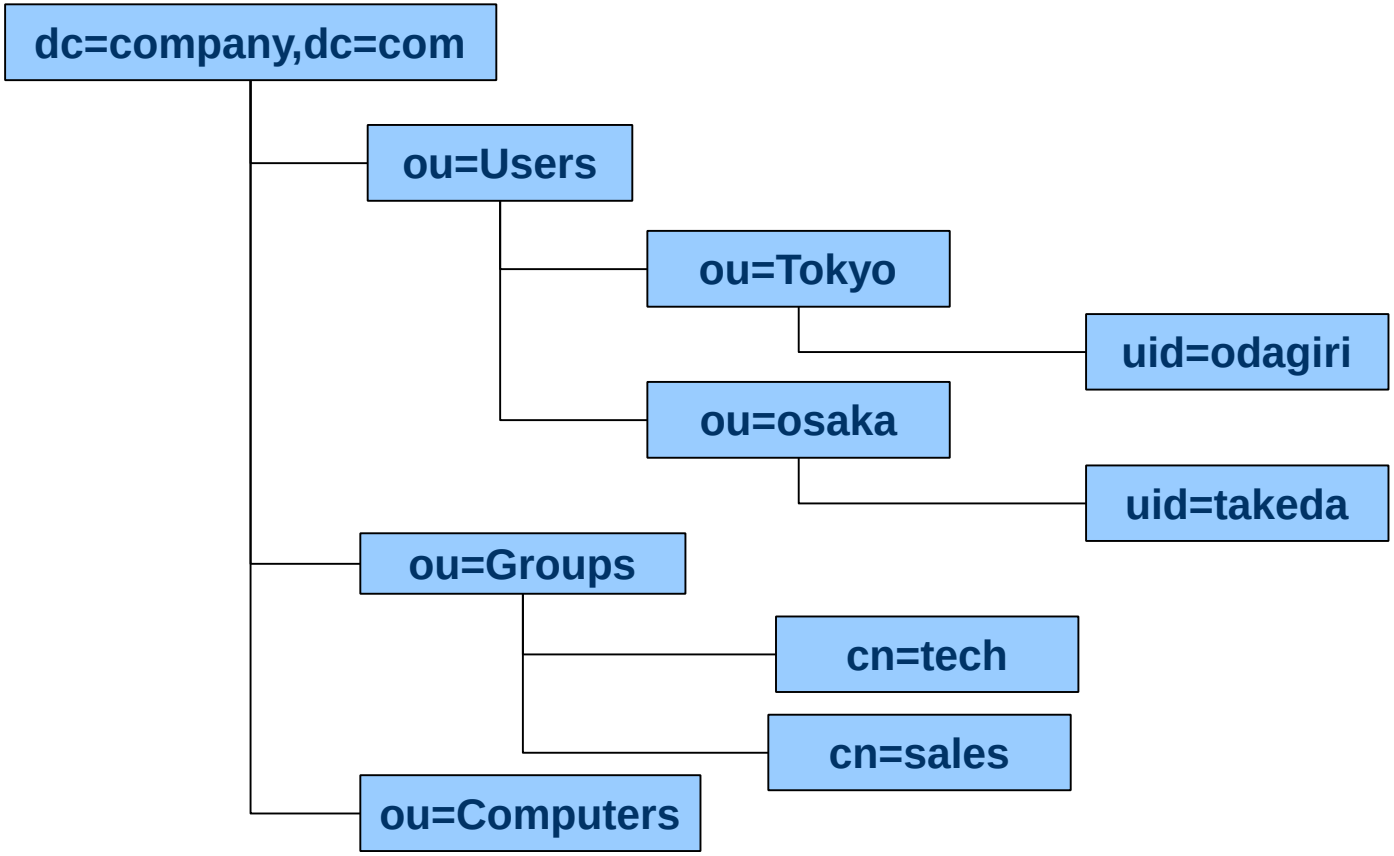
- **実構造としては管理単位で分ける**



© Open Source Solution Technology Corporation 2018 All Rights Reserved.

DIT (Directory information Tree) の設計

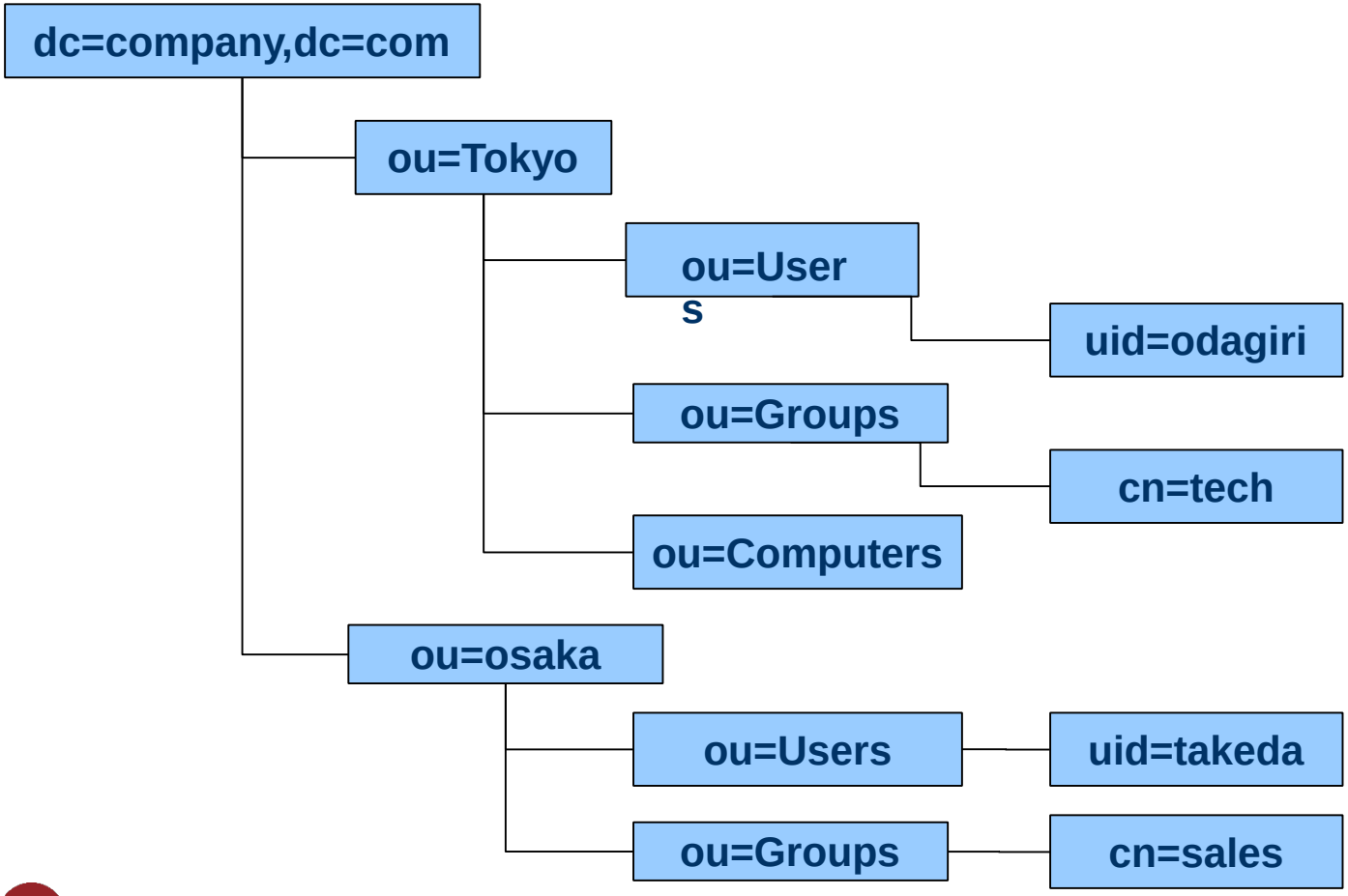
- **組織構造にマッピングしないこと、管理対象で分ける**



© Open Source Solution Technology Corporation 2018 All Rights Reserved.

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**



© Open Source Solution Technology Corporation 2018 All Rights Reserved.

OpenLDAP
レプリケーション設定

LPI-JAPAN

© Open Source Solution Technology Corporation 2018 All Rights Reserved.

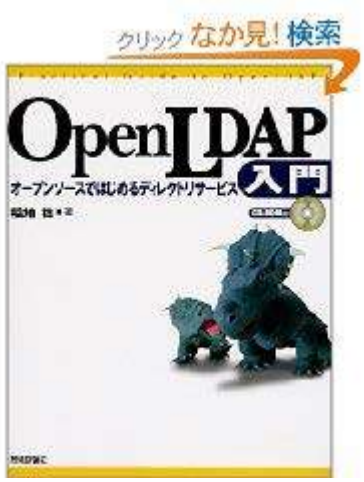
OpenLDAPサーバーのレプリケーション設定

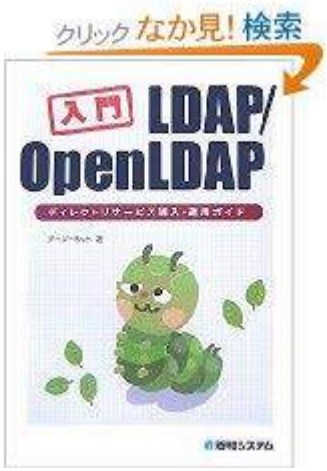
- シングル構成の設定はレベル2の試験範囲
- レベル3では冗長化構成(レプリケーション)が試験範囲
- コンパイルは試験範囲外なので、CentOSなどの標準のOpenLDAPを使ってインストールや設定の勉強をする
- OpenLDAPはどんどん新しくなるので、書籍の情報では古いことがある。
  - www.openldap.org のドキュメントを読むしかない
- コンパイルするのに必要なライブラリは、OS標準のものを使うのが一般的だがBDBだけはOpenLDAP専用のものを使う
  - RedHatのRPMではBDBはOS標準と違う専用のものを使うようにビルドされている。
    - ✓ 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

© Open Source Solution Technology Corporation 2018 All Rights Reserved.

OpenLDAP勉強のための参考書

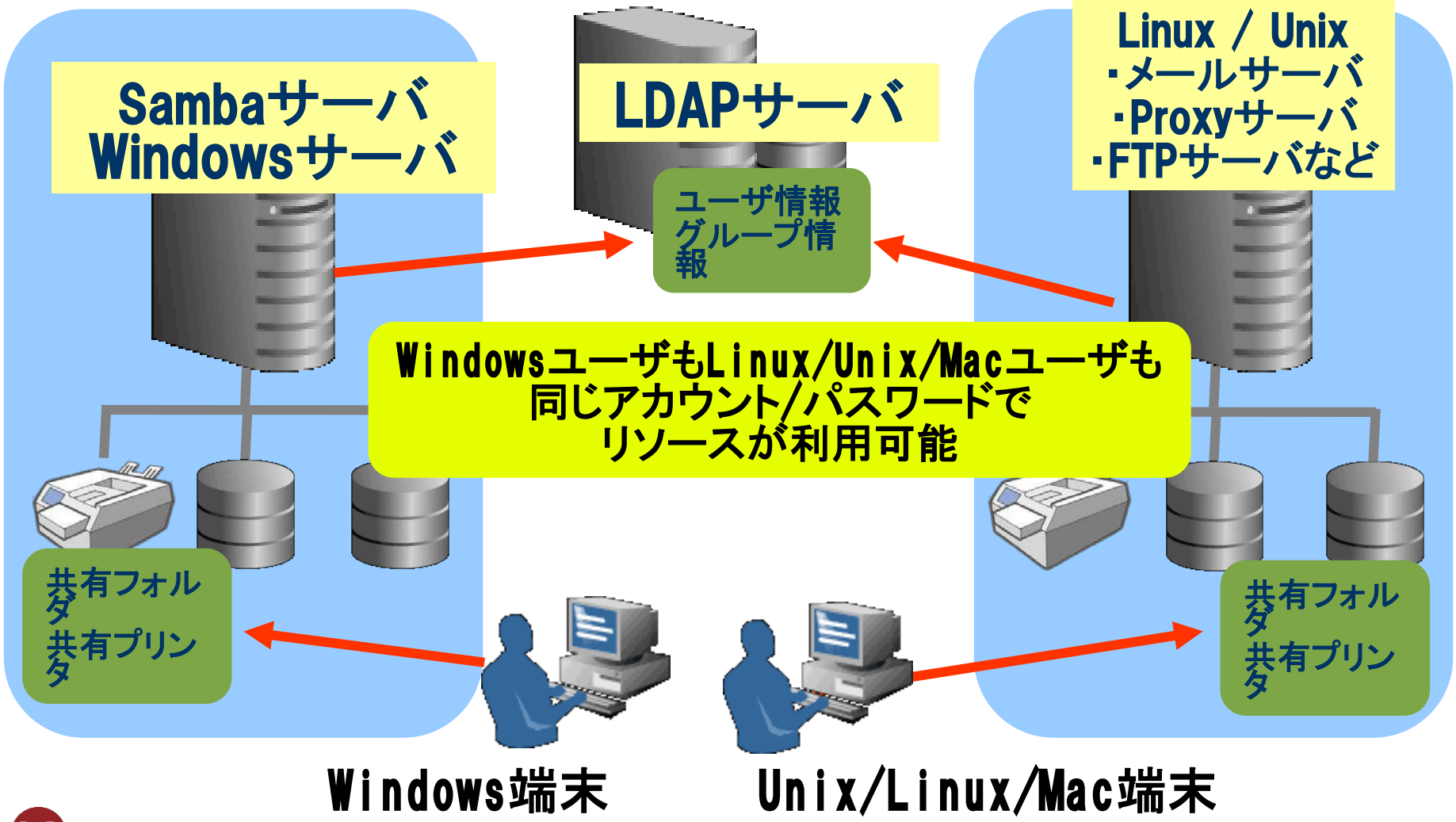
- OpenLDAP入門
  - オープンソースではじめるディレクトリサービス
  - 出版社: 技術評論社
  - 発売日: 2003/07
- 入門LDAP/OpenLDAP
  - ディレクトリサービス導入・運用ガイド
  - 出版社: 秀和システム
  - 発売日: 2007/10





© Open Source Solution Technology Corporation 2018 All Rights Reserved.

LDAPによる認証統合



© Open Source Solution Technology Corporation 2018 All Rights Reserved.

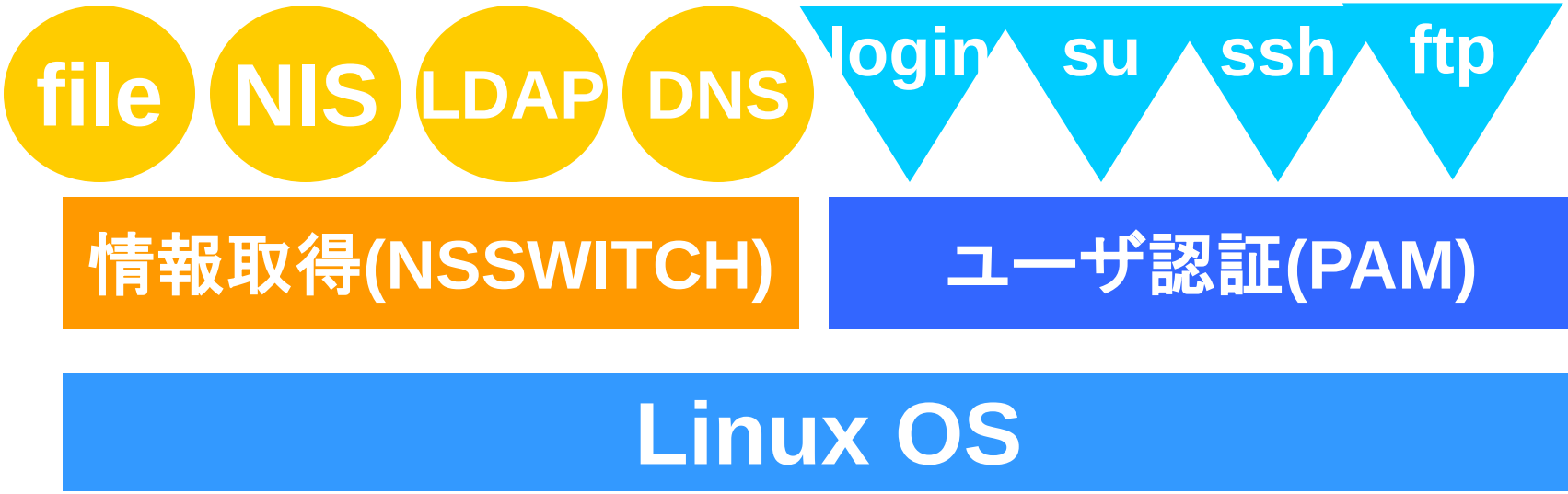
LDAPの設定

- 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

© Open Source Solution Technology Corporation 2018 All Rights Reserved.

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



© Open Source Solution Technology Corporation 2018 All Rights Reserved.

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。

© Open Source Solution Technology Corporation 2018 All Rights Reserved.

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。

© Open Source Solution Technology Corporation 2018 All Rights Reserved.

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

© Open Source Solution Technology Corporation 2018 All Rights Reserved.

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

© Open Source Solution Technology Corporation 2018 All Rights Reserved.

/etc/openldap/slapd.confﾊﾟﾗﾒｰﾀ(1)

- suffix ベース・サフィックスを指定する
  通常はﾄﾞﾒｲﾝ名をﾍﾞｰｽに指定
  例）suffix　dc=osstech,dc=co,dc=jp
  suffix "ou=sales,ou=yokohama,o=company,c=jp"

CN=commonName
L=localityName
ST=stateOrProvinceName
O=organizationName
OU=organizationalUnitName
C=countryName
STREET=streetAddress
DC=domainComponent
UID=userid

© Open Source Solution Technology Corporation 2018 All Rights Reserved.

/etc/openldap/slapd.confパラメータ(2)

- rootdn
  LDAPサーバの管理者のDN(Distinguished Name:識別名)を指定する。
  なお管理者DNを含むユーザDNには、英大文字、英子文字の区別はない。
  管理者DNの例)
  - rootdn "cn=Manager,dc=osstech,dc=co,dc=jp"
- rootpw
  LDAPサーバの管理者パスワードを設定する。
  - そのままのパスワードを指定するか暗号化したものを設定する
  - 例)secret1234というパスワードをSSHAハッシュする
    # slappasswd -s secret1234 -h {SSHA}
  - rootdnをLDAPに登録されているユーザを指定し、LDAPの中にパスワードが格納されていれば、rootpwを指定する必要はない。

LinuC

© Open Source Solution Technology Corporation 2018 All Rights Reserved.

/etc/openldap/slapd.confパラメータ(3)

- include
  - 与えたファイルから追加の設定情報を読み込む。
  - 通常はスキーマ定義ファイルを読み込むために使用する
    例) include /etc/openldap/schema/samba.schema
- database
  - LDAPのデータを格納するのに使用するバックエンド・データベースを指定。
- directory
  - databaseファイルを格納するディレクトリを指定
  - 例)directory /var/lib/ldap
- index
  - 作成する索引の属性とタイプを指定する。
    - 例1) uid,gidに関してequal(等値)検索用の索引を作成
      index uidNumber,gidNumber eq
    - 例2) mail(メールアドレス)、surname(名字)に関して、equal検索用とsubinitial(前方一致)の索引を作成
      index mail,surname eq,subinitial

© Open Source Solution Technology Corporation 2018 All Rights Reserved.

/etc/openldap/slapd.confパラメータ(4)

- Slapd.confの例：サフィックスを"dc=osstech,dc=co,dc=jp"、管理者DNを"cn=Manager,dc=osstech,dc=co,dc=jp"、管理者パスワードをsecret1234

```
include /etc/openldap/schema/core.schema
include /etc/openldap/schema/cosine.schema
include /etc/openldap/schema/inetorgperson.schema
include /etc/openldap/schema/nis.schema

database  bdb
directory /var/lib/ldap
suffix "dc=osstech,dc=co,dc=jp“
rootdn "cn=Manager,dc=osstech,dc=co,dc=jp“
rootpw secret1234
index  objectClass,uidNumber,gidNumber,memberUid  eq
index  cn,mail,surname,givenname                  eq,subinitial
index  uid                                        pres,eq
index  rid                                        eq
```

- 設定が終了したら、OpenLDAPデーモンを起動させる。
  # service ldap restart　※Red Hat系
- システム起動時に自動的に動くように以下を設定
  # chkconfig ldap on　※Red Hat系

© Open Source Solution Technology Corporation 2018 All Rights Reserved.

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

© Open Source Solution Technology Corporation 2018 All Rights Reserved.

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

© Open Source Solution Technology Corporation 2018 All Rights Reserved.

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

© Open Source Solution Technology Corporation 2018 All Rights Reserved.

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

© Open Source Solution Technology Corporation 2018 All Rights Reserved.

Samba機能と特徴

LPI-JAPAN

© Open Source Solution Technology Corporation 2018 All Rights Reserved.

Sambaとは？

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
	サポート終了 Windows 10から接続できない	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 8,10で動作しない	RSAT対応 Windows 8,10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

© Open Source Solution Technology Corporation 2018 All Rights Reserved.

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

LinuC

© Open Source Solution Technology Corporation 2018 All Rights Reserved.

Windows移行 Q & A

LPI-JAPAN

© Open Source Solution Technology Corporation 2018 All Rights Reserved.

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。

© Open Source Solution Technology Corporation 2018 All Rights Reserved.

Windowsドメイン移行に関するQ&A

- Q. Samba 4でSamba 3と同じNTドメインを構築できますか？
- A. はい、できます。
  - Samba4をWindows ADドメインモードで構築することもNTドメインモードで構築することもできます。
  - CentOS 7/RHEL 7のSamba 4は、NTドメインモードの構築はできますが、ADドメインモードで構築することは出来ません、Ubuntu 18.04は可能です。
- Q. Samba 3でNTドメインモードで構築したドメインサーバーをADモードのドメインコントローラーへバージョンアップ可能ですか？
- A. はい、できます。
  - Samba 3 から4のADドメインモードへパスワードやマシンアカウントを含め、バージョンアップ(移行)が可能です。
  - NTドメインモードからADドメインモードに変わってもクライアントマシンのドメイン再参加やパスワード再設定は必要ありません。

© Open Source Solution Technology Corporation 2018 All Rights Reserved.

- 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。

© Open Source Solution Technology Corporation 2018 All Rights Reserved.

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）

LinuC

© Open Source Solution Technology Corporation 2018 All Rights Reserved.

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。

© Open Source Solution Technology Corporation 2018 All Rights Reserved.

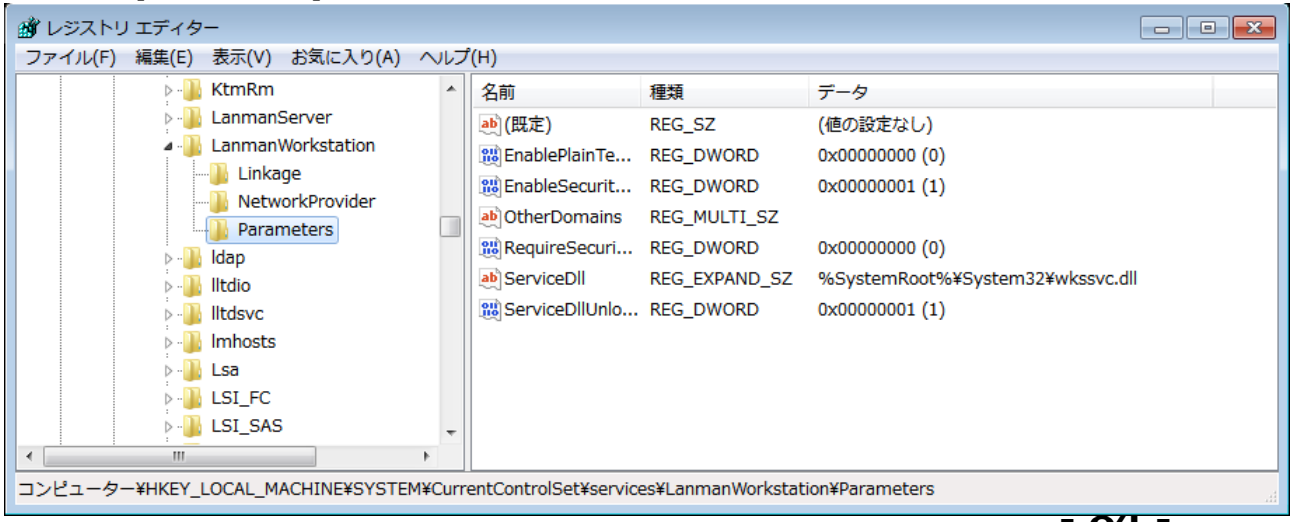
Samba 4による Active Directory構築

© Open Source Solution Technology Corporation 2018 All Rights Reserved.

Samba 4 と ドメインログオン

- 最新のWindows 10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



© Open Source Solution Technology Corporation 2018 All Rights Reserved.

UbuntuによるSamba 4 AD構築(1)

- **CentOS 7/RHEL 7のSamba 4はAD機能が無効化されている**
  Samba 4の勉強には不向き
- **Ubuntu 18.04 LTSを利用する**
  LTS(Long Time Support)で長期間利用可能
- **Server版を利用すること**
  Desktop版はDNSポートが捕まれているので設定が面倒
  (Ubuntu 18.04ではsystemd-resolvedがDNSポートをつかんでいる)
- **Samba 4は、DNS,Keroberos,LDAPのサーバーとして**
  動くのでDHCPとせずに固定IPとすること

© Open Source Solution Technology Corporation 2018 All Rights Reserved.

■ **固定IPとする設定**

```
# vi /etc/netplan/50-cloud-init.yaml

network:
   ethernets:
       ens33:
           addresses:
           - 192.168.1.180/24
           dhcp4: false
           gateway4: 192.168.1.2
           nameservers:
               addresses:
               - 192.168.1.2
               search:
               - osstech.co.jp
   version: 2


# netplan apply        設定変更の適用
# ip addr              設定確認
```


© Open Source Solution Technology Corporation 2018 All Rights Reserved.

UbuntuによるSamba 4 AD構築(3)

Sambaのインストール

```
# apt-get install samba winbind smbclient libnss-winbind
```

Windbindがないと Internal Errorが発生、 libnss-winbindはsmbstatusなどでユーザー名を表示するのに必要
smbclientは必須ではないが、動作確認にあったほうが良い

```
# systemctl stop smbd
# systemctl mask smbd
# systemctl stop nmbd
# systemctl mask nmbd
# systemctl stop winbind
# systemctl mask winbind
# systemctl stop systemd-resolved
# systemctl mask systemd-resolved
```

標準で動くデーモンはすべて止めて無効化する

testparmでエラーが出る場合

```
# vi /etc/security/limits.conf

#<domain>      <type> <item>         <value>
*                soft nofile         16384 ← 追記

# vi /etc/nsswitch.conf
passwd:         compat systemd winbind
group:          compat systemd winbind
```


© Open Source Solution Technology Corporation 2018 All Rights Reserved.

■ **Samba ADの構築**

```
# cd /etc/samba
# mv smb.conf smb.conf.org
# samba-tool domain provision --interactive --use-rfc2307
Realm: KOJI1804DOM.OSSTECH.CO.JP
 Domain [KOJI1804DOM]:
 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) [127.0.0.53]: 192.168.2.2
Administrator password:英大文字小文字数字記号が入った複雑なパスワード
Retype password:

# vi smb.conf



# systemctl unmask samba-ad-dc
# systemctl start samba-ad-dc
# systemctl enable samba-ad-dc
```


© Open Source Solution Technology Corporation 2018 All Rights Reserved.

Samba 4 と管理ツール

- 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 8、10用それぞれ提供

© Open Source Solution Technology Corporation 2018 All Rights Reserved.

- 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
  - ntpの設定については今回は省略
- Windowsクライアント（Windows 10）
  - 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

© Open Source Solution Technology Corporation 2018 All Rights Reserved.

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**

© Open Source Solution Technology Corporation 2018 All Rights Reserved.

- 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

```
# 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:

© Open Source Solution Technology Corporation 2018 All Rights Reserved.

Samba 4 AD DC起動/確認 1

- Samba4プロセス起動

- /etc/resolv.conf を修正
  DNSをサーバーをSamba自身 127.0.0.1 に設定

- smbclientによるアクセス確認

```
# 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。

© Open Source Solution Technology Corporation 2018 All Rights Reserved.

- ユーザーの登録状況を確認
  - # 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$
  - # samba-tool user add cui-user1
  - New Password:
  - Retype Password:
  - User 'cui-user1' created successfully

© Open Source Solution Technology Corporation 2018 All Rights Reserved.

samba-toolコマンドによるユーザー管理 2

- 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
  - # 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

© Open Source Solution Technology Corporation 2018 All Rights Reserved.

- 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
  - # samba-tool user setpassword ¥
    --newpassword=P@ssw0rd cui-user1

    Changed password OK

© Open Source Solution Technology Corporation 2018 All Rights Reserved.

- 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

```
$ 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

© Open Source Solution Technology Corporation 2018 All Rights Reserved.

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

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

© Open Source Solution Technology Corporation 2018 All Rights Reserved.

- グループにメンバーを所属
  - # 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
  - # samba-tool group listmembers cui-group1
  - cui-user1
  - cui-user2

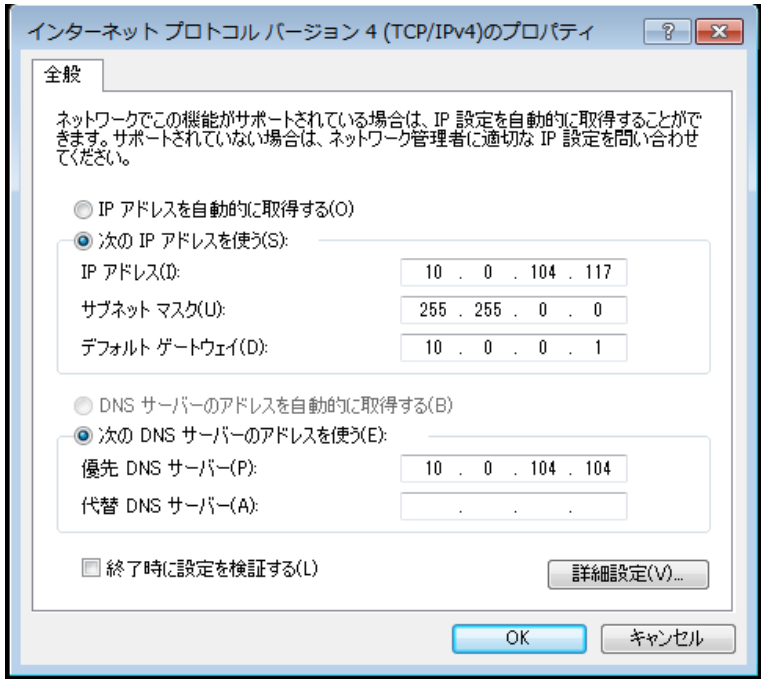
© Open Source Solution Technology Corporation 2018 All Rights Reserved.

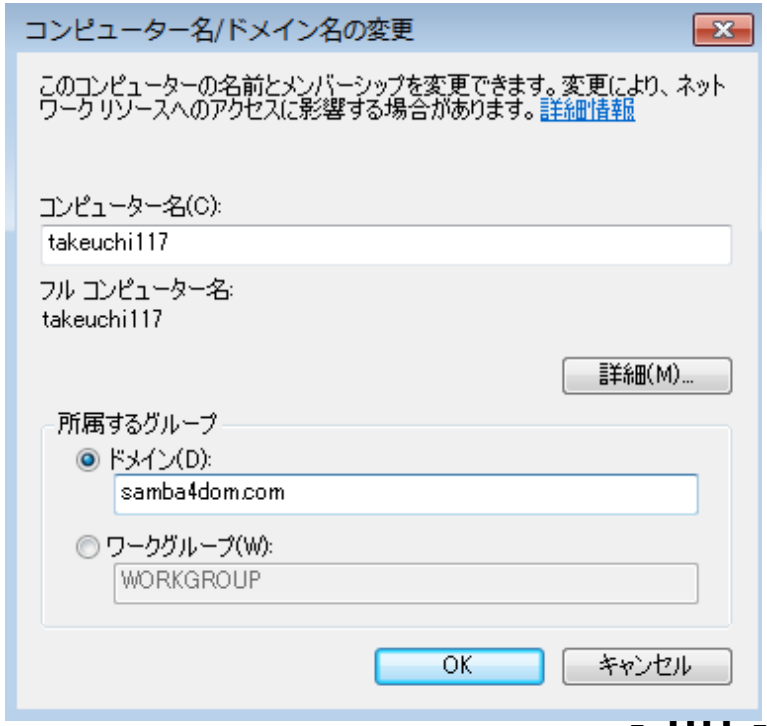
Windows10をドメイン参加させ、ADを管理

© Open Source Solution Technology Corporation 2018 All Rights Reserved.

Windows7をドメイン参加

- Windows 10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

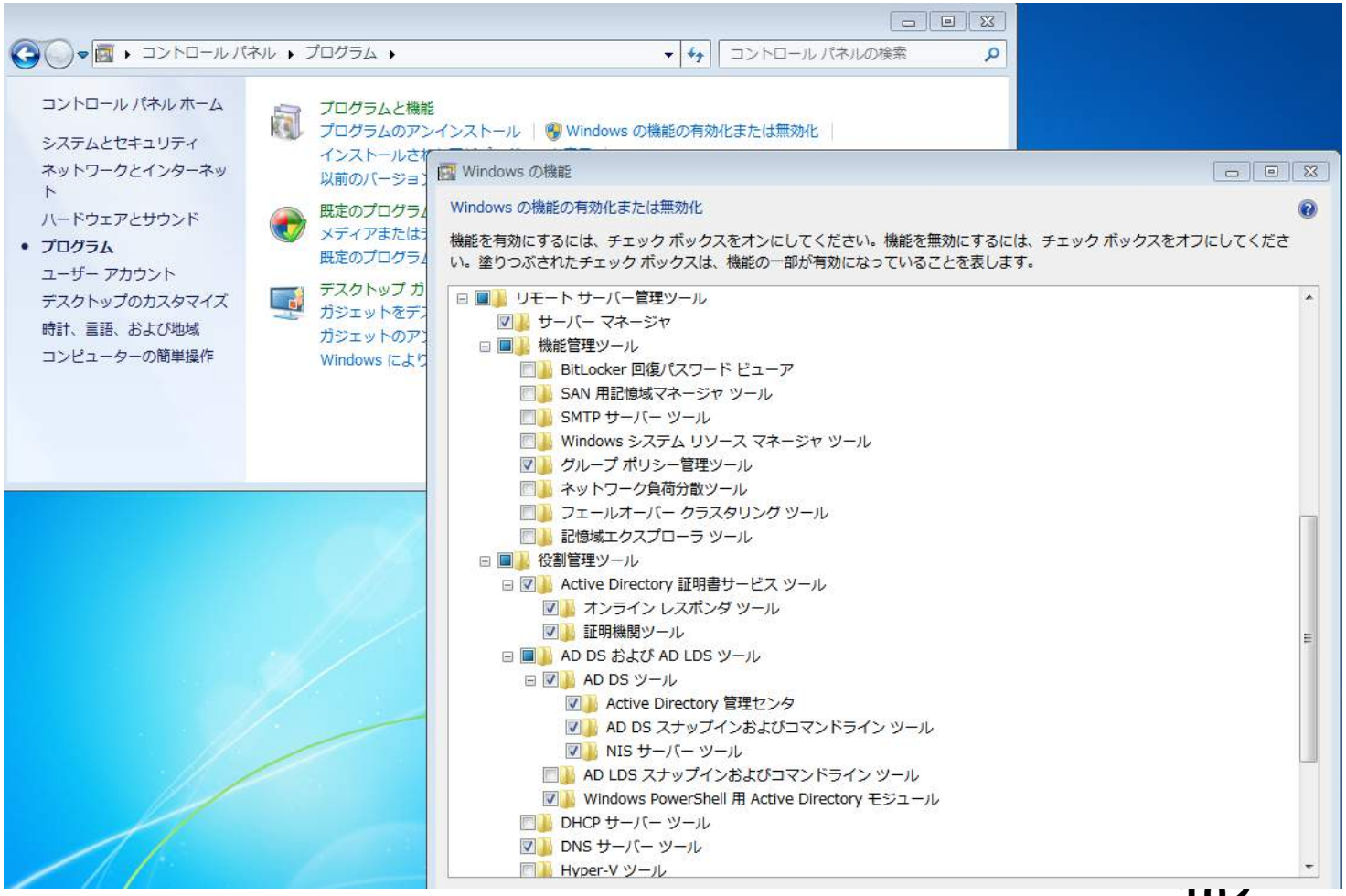




© Open Source Solution Technology Corporation 2018 All Rights Reserved.

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



© Open Source Solution Technology Corporation 2018 All Rights Reserved.

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

© Open Source Solution Technology Corporation 2018 All Rights Reserved.

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

© Open Source Solution Technology Corporation 2018 All Rights Reserved.

パスワードポリシー 1

- 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
    - # 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

© Open Source Solution Technology Corporation 2018 All Rights Reserved.

パスワードポリシー 2

```
# 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
```


© Open Source Solution Technology Corporation 2018 All Rights Reserved.

Windows AD DCから Samba4 AD DCに切替

© Open Source Solution Technology Corporation 2018 All Rights Reserved.

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

© Open Source Solution Technology Corporation 2018 All Rights Reserved.

２台目のSamba AD DCを構築するときも以下のコマンドを利用する
（/etc/resolv.confを１台目のAD DCへ向けること）

```
# 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
```


© Open Source Solution Technology Corporation 2018 All Rights Reserved.

- 起動
  - # systemctl start samba-ad-dc 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

© Open Source Solution Technology Corporation 2018 All Rights Reserved.

操作マスターをSamba4に移動 1

- 現状の操作マスターの確認

```
# 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
```


© Open Source Solution Technology Corporation 2018 All Rights Reserved.

操作マスターをSamba4に移動 2

- 操作マスターの移動

```
# samba-tool fsmo transfer –role=all
```

- 移動後の操作マスターの確認

```
# 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
```


© Open Source Solution Technology Corporation 2018 All Rights Reserved.
112

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
    - # 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
- Windows 10 でドメインログオン
  - windows-add、samba-add両ユーザーでログオン

© Open Source Solution Technology Corporation 2018 All Rights Reserved.

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
    - # samba-tool user add samba-add1 P@ssw0rd
- Windows 10 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

© Open Source Solution Technology Corporation 2018 All Rights Reserved.

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/

LPI-JAPAN

© Open Source Solution Technology Corporation 2018 All Rights Reserved.

表１．SambaとWindowsサーバーとの比較

機能	Samba 3.6	Samba 4.8	Windows Server 2008～2016
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利用は現状できない	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 Windows Server 2008R2互換	○
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 2008R2 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	△LLTDに未対応	○
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	△LLTDに未対応	○信頼するドメインのみ
ポテンシャルブラウザ	○	△LLTDに未対応	○

付録.

300例題

Samba 4 編

LPI-JAPAN

© Open Source Solution Technology Corporation 2018 All Rights Reserved.

392.1 例題1）

- Samba 4の機能でないものをすべて選びなさい。
  1. Windows NT互換のドメインコントローラーになれる
  2. マイクロソフトOfiiceなどのWindowsアプリケーションをLinux上で動作させることができる
  3. Windows Acrive Directory互換のドメインコントローラーになれる
  4. Windows 8.1のファイルサーバーになれる
  5. アップルMac OS Xのファイルサーバーになれる
  6. DNSサーバーになれる
  7. DHCPサーバーになれる
  8. Kerberosサーバーになれる
  9. LDAPサーバーになれる
  10. Radiusサーバーになれる

© Open Source Solution Technology Corporation 2018 All Rights Reserved.

392.1 例題2）

- Samba 4がWindows 8とファイル共有で使う標準のTCPポートは以下のどれですか？
  1. 135
  2. 137
  3. 138
  4. 139
  5. 445
  6. 464

© Open Source Solution Technology Corporation 2018 All Rights Reserved.

392.1 例題3）

- Samba 4 ADドメインモードにWindows 8でドメインログオンする時に使われる認証方式は以下のどれですか？

1. LANMAN認証
2. NTLM認証
3. NTLMv2認証
4. LDAP認証
5. Kerberos認証
6. Radius認証

© Open Source Solution Technology Corporation 2018 All Rights Reserved.

392.5 例題）

■Sambaファイルサーバーに関して、以下の文章で正しいものを全てあげなさい。

1. Windows Vista以降でサポートされたJIS2004（JIS X 0213）をファイル名に使うには、smb.confでunix charset=utf-8 とすれば良い
2. Windows Vista以降でサポートされたJIS2004（JIS X 0213）をファイル名に使うには、smb.confでunix charset=CP932とすれば良い
3. Windows Vista以降でサポートされたJIS2004（JIS X 0213）をファイル名に使うには、smb.confでunix charset=EUCJP-MS とすれば良い
4. smb.confでunix charset=utf-8 とした場合、ファイル名の長さは英数字使用の場合は１文字１バイト、漢字使用の場合は1文字２バイト使用される。
5. smb.confでunix charset=utf-16 とした場合、ファイル名の長さは英数字使用の場合も漢字使用の場合も1文字で２バイト使用される。

© Open Source Solution Technology Corporation 2018 All Rights Reserved.

396 例題)

■以下の内、誤っている文章を全てあげよ。

1. Samba 4（ADドメインモード）ではドメインコントローラーの検索はDNSまたはWINSによって行われる
2. Samba 4 （ADドメインモード）ではドメインコントローラーの検索はDNSのみによって行われる
3. Samba 3ではドメインコントローラーの検索はDNSまたはWINSによって行われる
4. Samba 4ではファイルサーバーの検索はDNSまたはWINSによって行われる
5. Samba 4でファイルサーバーに別名を付ける場合、smb.confのnetbios aliasesを使う。
6. Samba 4 （ADドメインモード）のドメインログイン環境ではWINSは不要である。
7. Samba 3のドメインログイン環境ではWINSは不要である。

© Open Source Solution Technology Corporation 2018 All Rights Reserved.