

OS混在環境における Windows、Unix、Linux認証統合 ノウハウ



OSSTech

2007/3/28
オープンソース・ソリューション・テクノロジー株式会社

代表取締役 小田切耕司

お問い合わせ info@osstech.co.jp

目次

- OSSTech社紹介
- 認証統合が必要な背景
- LDAPによる認証統合
- SambaとLDAPを使った分散管理
- Active Directoryを使った認証統合
- コンサルティング・サービスおよびサポート・サービス・メニュー

Part 1.

オープンソース・ソリューション・テクノロジー 会社紹介

会社概要

会社名	オープンソース・ソリューション・テクノロジー株式会社
英語表記	Open Source Solution Technology Corporation
社名略称	OSSTech(オー・エス・エス・テック)または OSSテクノロジー
業務内容	<ul style="list-style-type: none"> ・ソフトウェアの企画、開発、販売およびメンテナンス ・ソフトウェアおよびシステムの導入に関するコンサルティング ・ソフトウェアに関する教育、研修、支援
役員	代表取締役 小田切 耕司 技術取締役 武田 保真
オフィス	〒141-0031 東京都品川区西五反田2-6-3 東洋ビル Tel & FAX : 03-6670-5764
Webページ	http://www.osstech.co.jp/
設立	2006年9月
資本金	800万円
所属団体等	<ul style="list-style-type: none"> ・Linuxコンソーシアム理事 ・社団法人コンピュータソフトウェア協会(CSAJ) ・オープンソースソフトウェア協会
主要取引先 および パートナー様	<ul style="list-style-type: none"> ・デル株式会社 ・日本電信電話株式会社 ・日本電気株式会社 ・株式会社 大塚商会 ・キャノンマーケティングジャパン株式会社 ・富士通ネットワークソリューションズ株式会社 ・株式会社 日立情報システムズ ・株式会社 博報堂 ・大分シーイーシー株式会社 ・Data Foundation 株式会社 ・ミラクル・リナックス株式会社

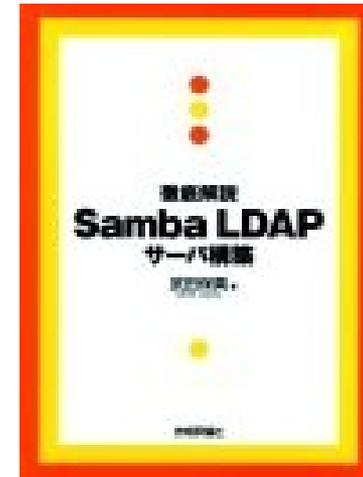
オープンソース・ソリューション・テクノロジー株式会社

- 昨年 9月に設立
- **OSに依存しないOSSのソリューションを中心に提供**
 - Linuxだけでなく、SolarisやFreeBSDも！
- **Samba、LDAPなどによる認証統合ソリューションを提供**
 - 製品パッケージ提供
 - 製品サポート提供
 - 技術コンサルティング提供

<http://www.osstech.co.jp>

社員による著作紹介

- ◆ **小田切**
- ◆ 技術評論社 Software Design 2006年7月号
 - 「巻:地の巻」Sambaファイルサーバ
- ◆ 翔泳社 開発の現場 vol.005
 - 総論編:オープンソースの基礎知識
- ◆ 技術評論社 LDAP Super Expert
 - [新規/移行]LDAPディレクトリサービス導入計画
- ◆ IDG月刊Windows Server World
 - 3月号:Shall we Samba?【お手軽導入編】
 - 4月号:Shall We Samba?【超本格運用編】
- ◆ 日経BP社 セキュアなSambaサーバの作り方
- ◆ **武田**
- ◆ 日経ITPro「Sambaウォッチ」
 - ◆ 2006年10月～現在連載中
- ◆ 「徹底解説 Samba LDAP サーバ構築 (技術評論社)」



Part 2.

認証統合が必要な背景



OSSTech

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！

Part 3.

LDAPを使った認証統合



OSSTech

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

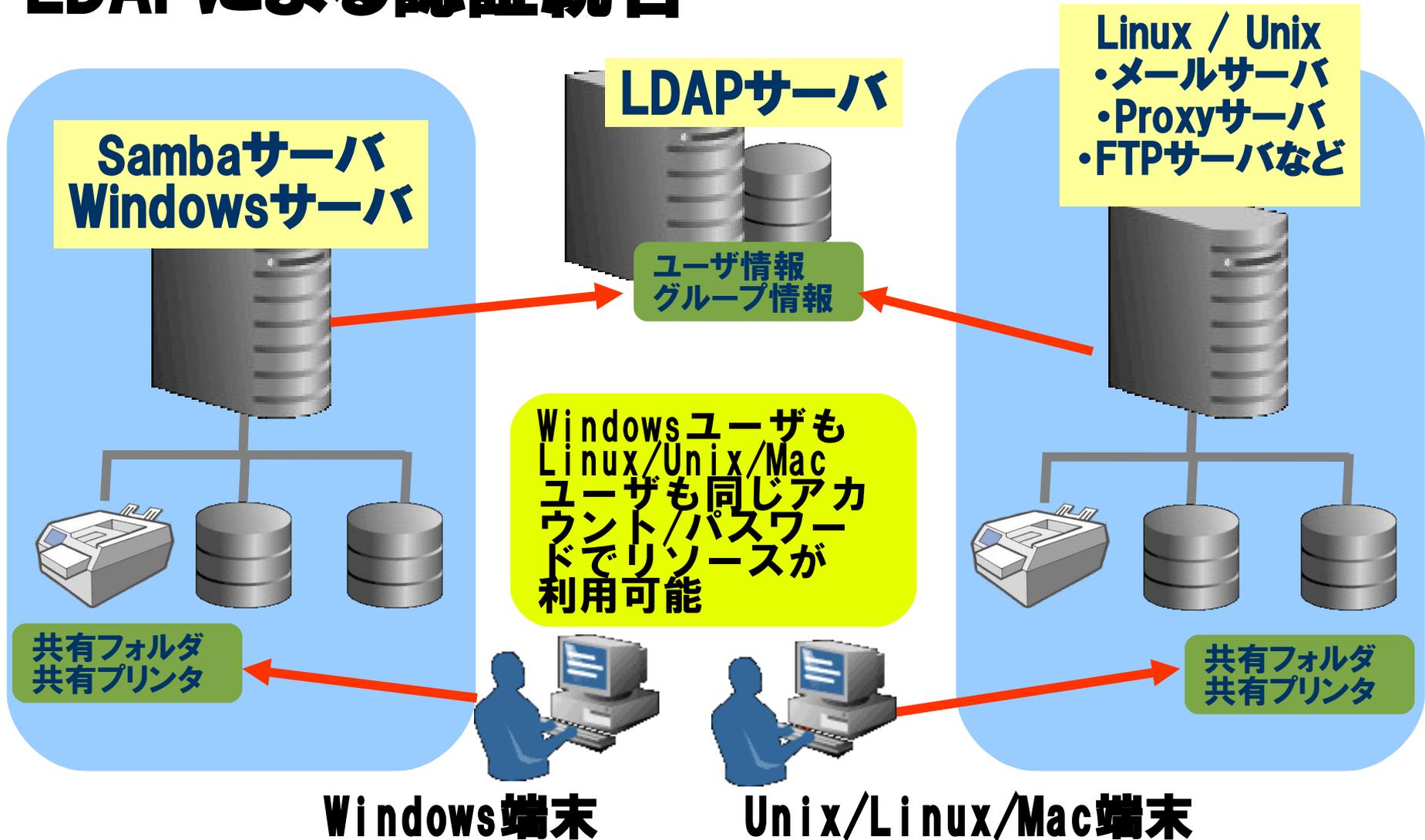
- **Active Directoryの代わりとしてのOSS認証基盤**
OSSのSambaとOpenLDAPを使い、既存のWindowsドメインを移行したり、Active Directoryの代わりにOSSシステム認証基盤を導入。
- **既存のNISやNIS+からLDAPへの移行**
OSSのSambaとOpenLDAPを使い、Windowsクライアントの認証だけでなく、Unix, Linux, Macの認証統合を行う。
- **Active DirectoryによるUnix, Linux, Macの認証統合**
OSSのSambaを使い、Unix, Linux, Macクライアントおよ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

最近で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

Linux / Unix
Samba 3.0
 ・ファイルサーバ
 ・メールサーバ
 ・Proxyサーバ
 ・FTPサーバなど

Windows 2000/2003
Active Directory

認証要求

ユーザ管理はすべてWindows上でを行いLinuxやUnixにユーザを作成する必要はない

共有フォルダ
共有プリンタ

共有フォルダ
共有プリンタ

ユーザ情報
グループ情報

Unix/Linux/Mac端末

Windows端末

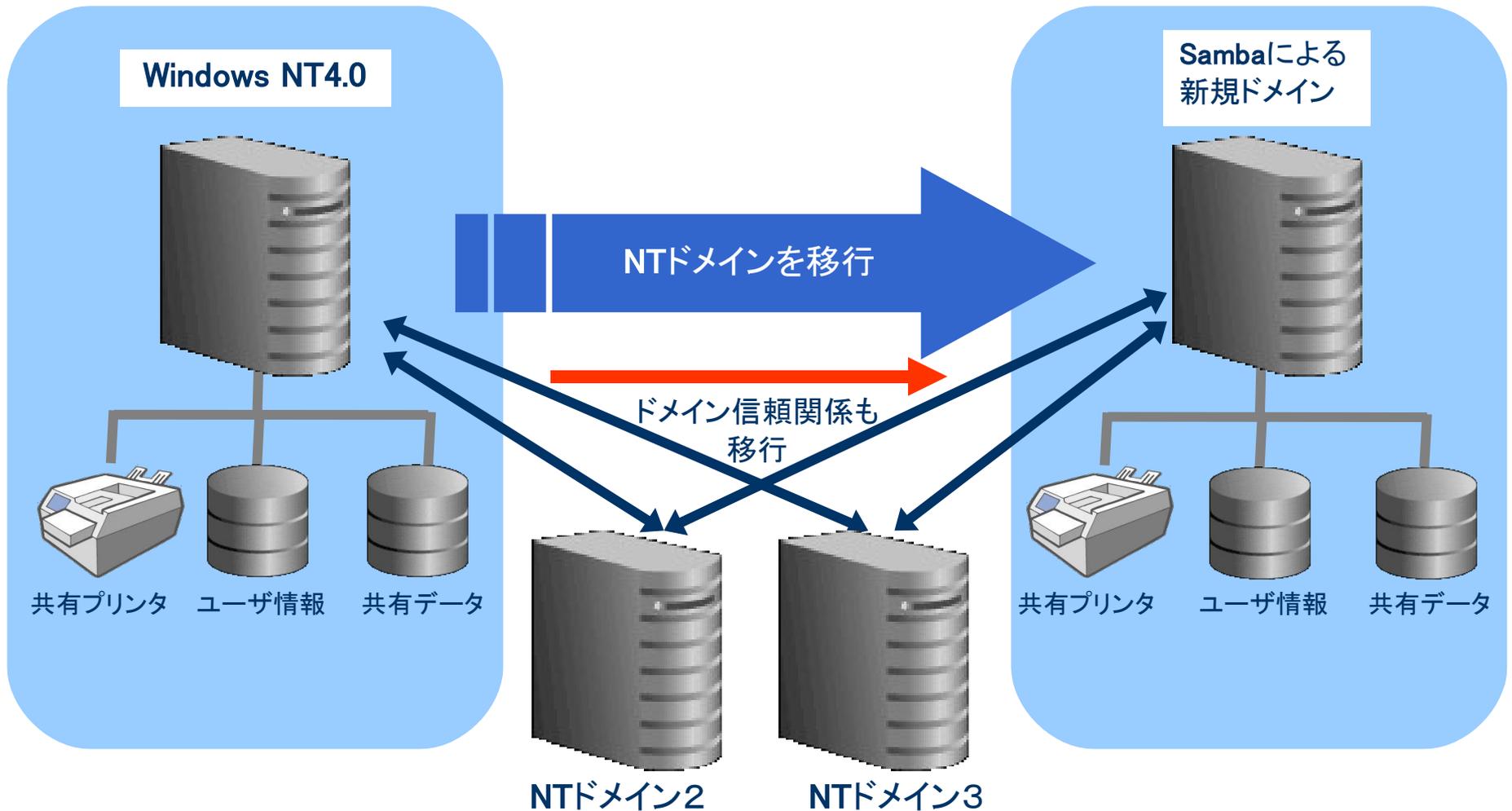
最近は複数システムの統合が増える

- 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
 - 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
-
- 複数ドメインを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

ドメイン統合の問題点

- 既存のNTドメインをAD(Active Directory)へ移行するのは容易ではない。
→再設計になるのでSambaに移行しても手間暇はあまりかわらない
- NTからADにするとCAL(クライアント・アクセス・ライセンス)を買い直さないといけないケースが発生する。
(違法コピーの発覚)
- SambaとOpenLDAPで認証統合、ドメイン統合をやりたいと思ってもどうやるか解らない。事例が少ない。

vampireと手作業による移行



Part 4.

SambaとLDAPを使った分散管理



OSSTech

Samba3.0のドメイン機能はNT4.0互換らしいが、Active Directoryのフォレストのような分散管理はできないか？

■ 管理の分散と権限委譲

- 一つのドメインの下に複数の部門が存在
- 部門にはそれぞれの管理者が存在し、自分の部門だけのユーザ、共有フォルダを管理したい
- 他部門のユーザや共有フォルダに関して設定変更できないようにしたい

SambaとLDAPを使ったドメイン統合方式

- 一つのベースサフィックスの下に複数のOU(組織単位)を持ったDITを作成。既存のNTドメインをひとつのOUに対応させる。Sambaドメインは単一にする
 - ADと一番近い形

LDAPのOUツリーを使うことで分散管理を実現

■ 統合認証と権限委譲

➤ 以下のような例をあげて実現できる機能を説明します

➤ 想定環境

☒ドメイン名: OSSTECH

☒部門: ドメインの下に以下の3つの部門が存在

– SALES: 営業部門

– MKTG: マーケティング部門

– TECH: 技術部門

☒管理者

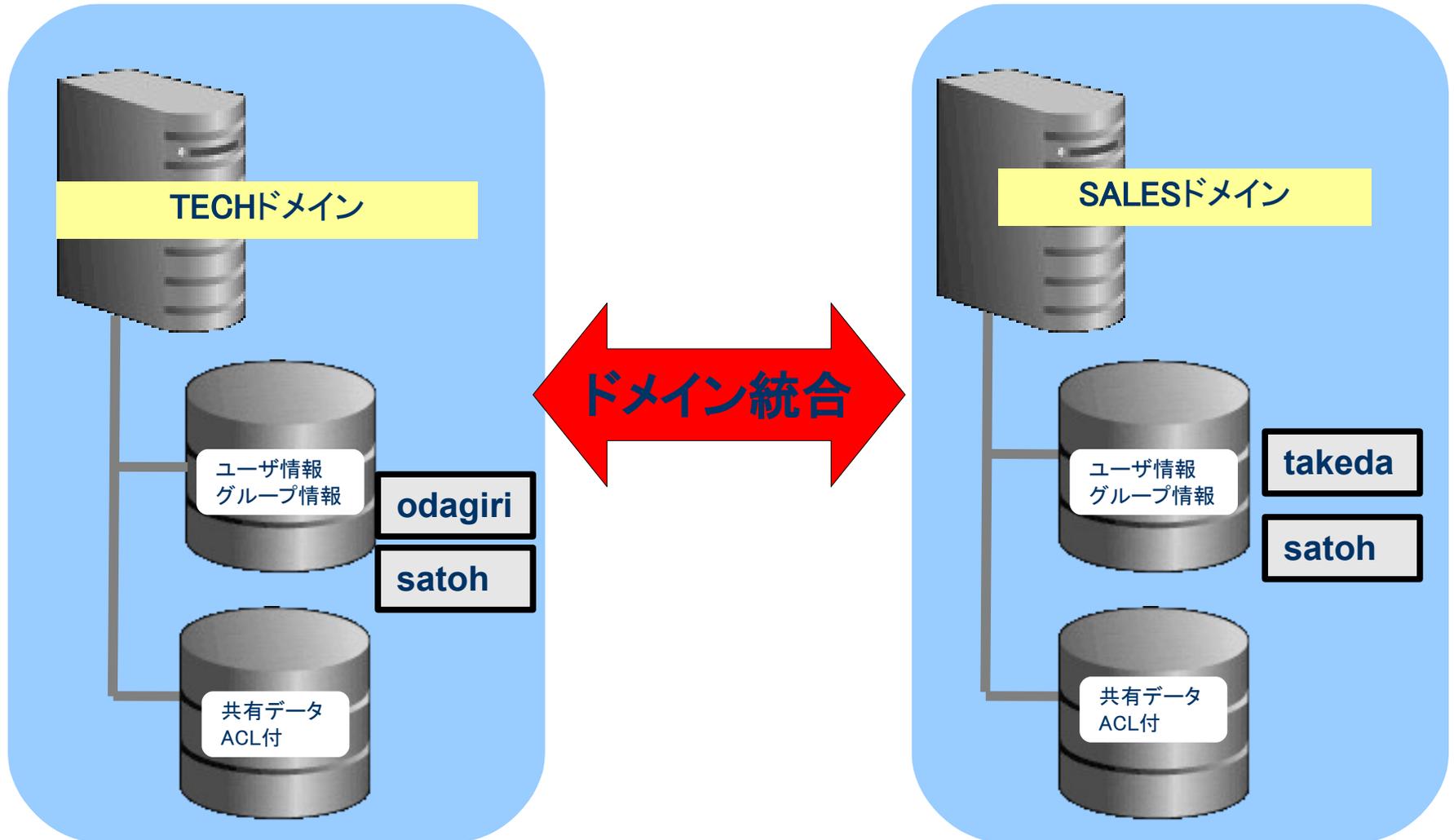
– ドメインの管理者: Administrator

– SALESの管理者: salesadmin

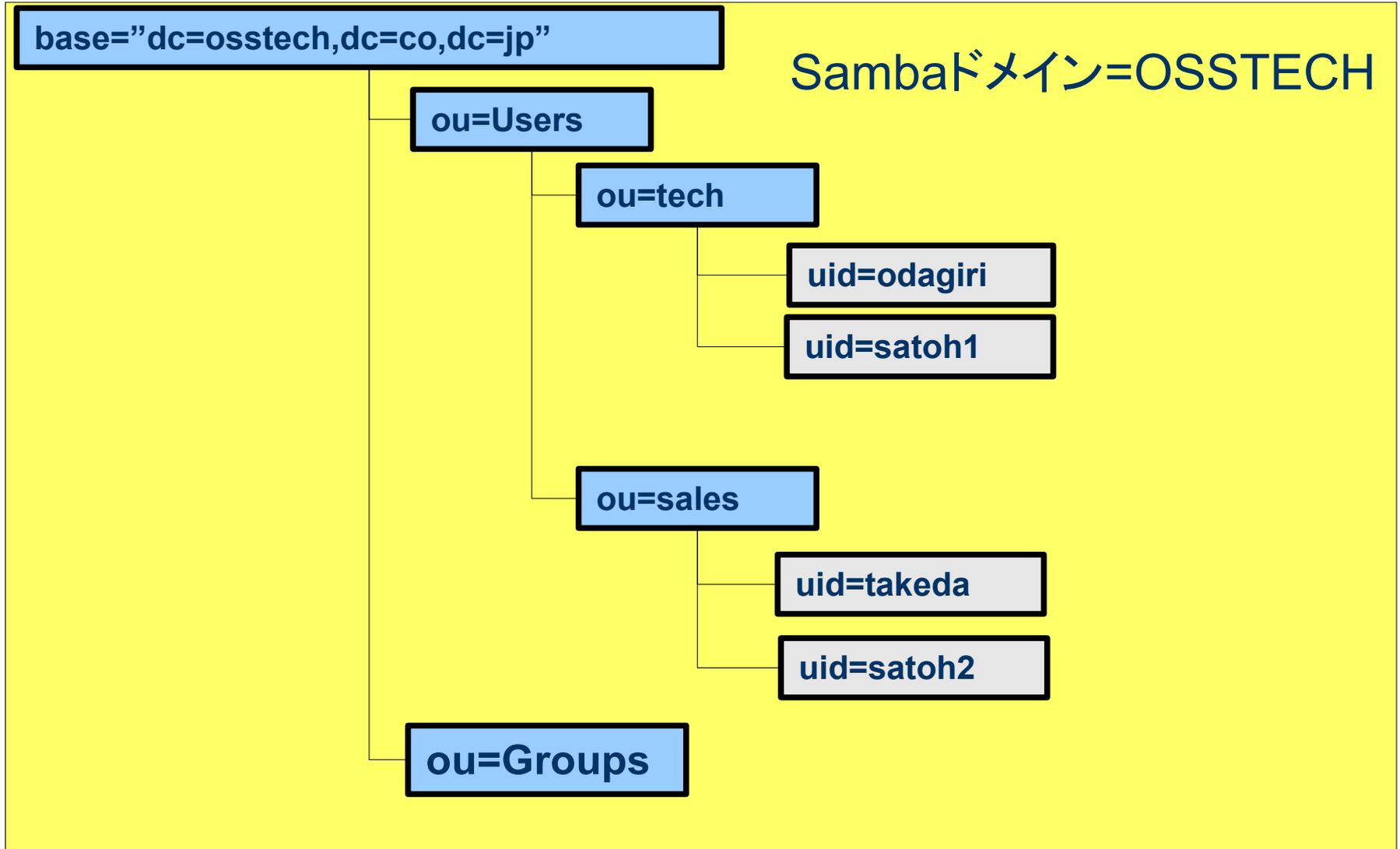
– MKTGの管理者: mktgsadmin

– TECHの管理者: techadmin

統合前のWindowsドメイン イメージ

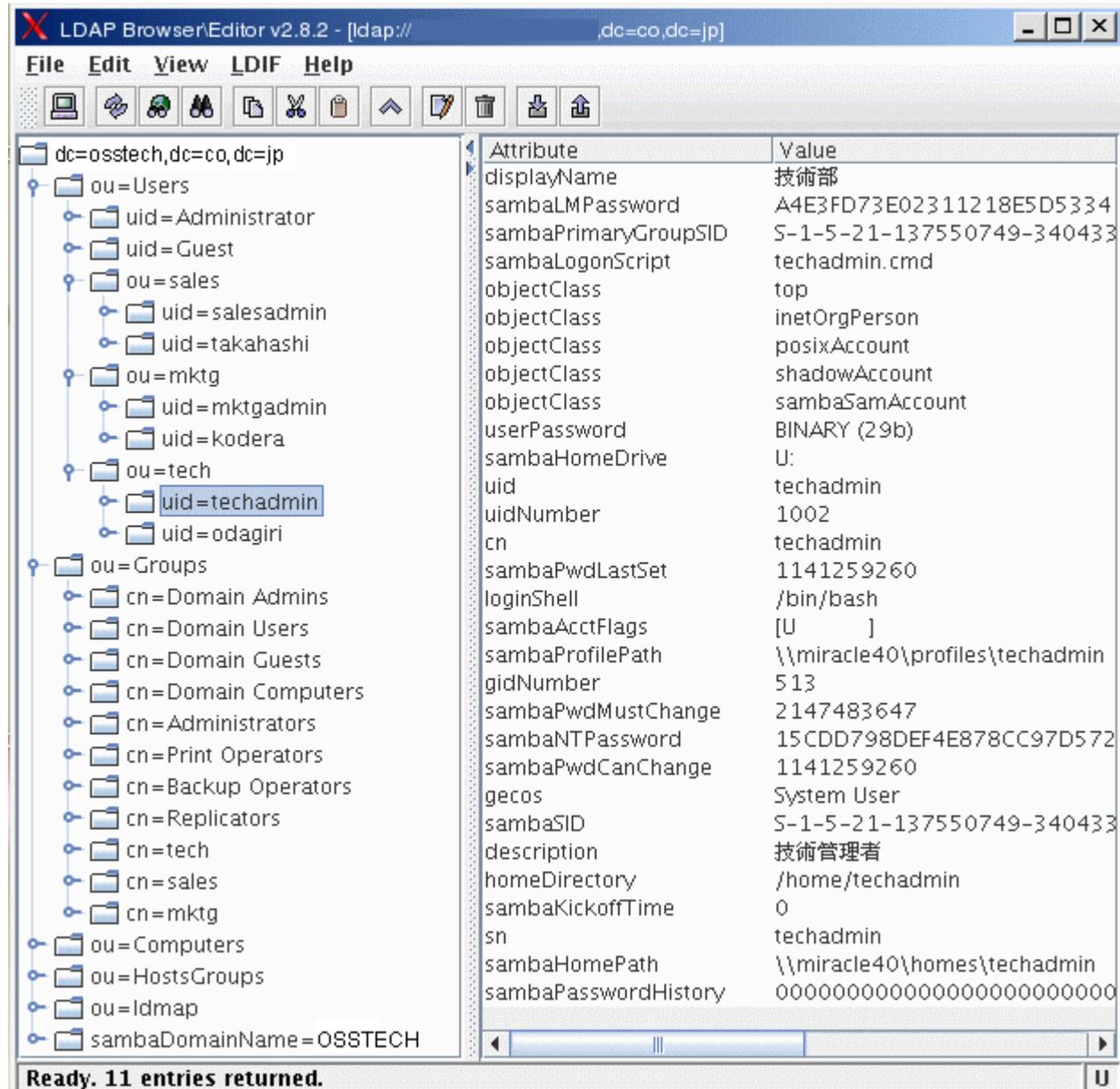


単一ベースサフィックス、単一ドメイン方式



ディレクトリ構造

- ディレクトリサービスLDAPの中に構築されるディレクトリ構造は図のように階層構造になります



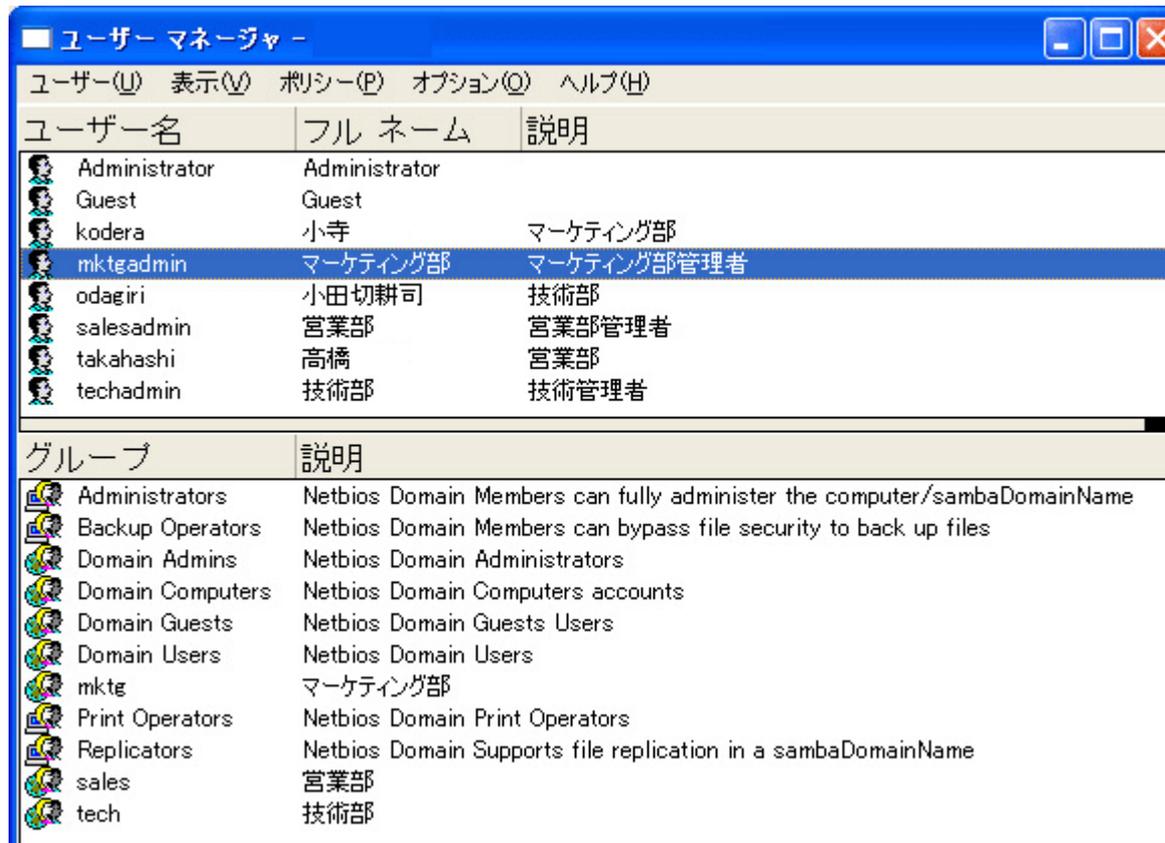
The screenshot shows the LDAP Browser/Editor interface. The left pane displays a hierarchical directory tree for the domain 'dc=osstech,dc=co,dc=jp'. The right pane shows the details for the selected entry 'uid=techadmin'.

Attribute	Value
displayName	技術部
sambaLMPassword	A4E3FD73E02311218E5D5334
sambaPrimaryGroupSID	S-1-5-21-137550749-340433
sambaLogonScript	techadmin.cmd
objectClass	top
objectClass	inetOrgPerson
objectClass	posixAccount
objectClass	shadowAccount
objectClass	sambaSamAccount
userPassword	BINARY (29b)
sambaHomeDrive	U:
uid	techadmin
uidNumber	1002
cn	techadmin
sambaPwdLastSet	1141259260
loginShell	/bin/bash
sambaAcctFlags	[U]
sambaProfilePath	\\miracle40\profiles\techadmin
gidNumber	513
sambaPwdMustChange	2147483647
sambaNTPassword	15CDD798DEF4E878CC97D572
sambaPwdCanChange	1141259260
gecos	System User
sambaSID	S-1-5-21-137550749-340433
description	技術管理者
homeDirectory	/home/techadmin
sambaKickoffTime	0
sn	techadmin
sambaHomePath	\\miracle40\homes\techadmin
sambaPasswordHistory	000000000000000000000000

Ready. 11 entries returned.

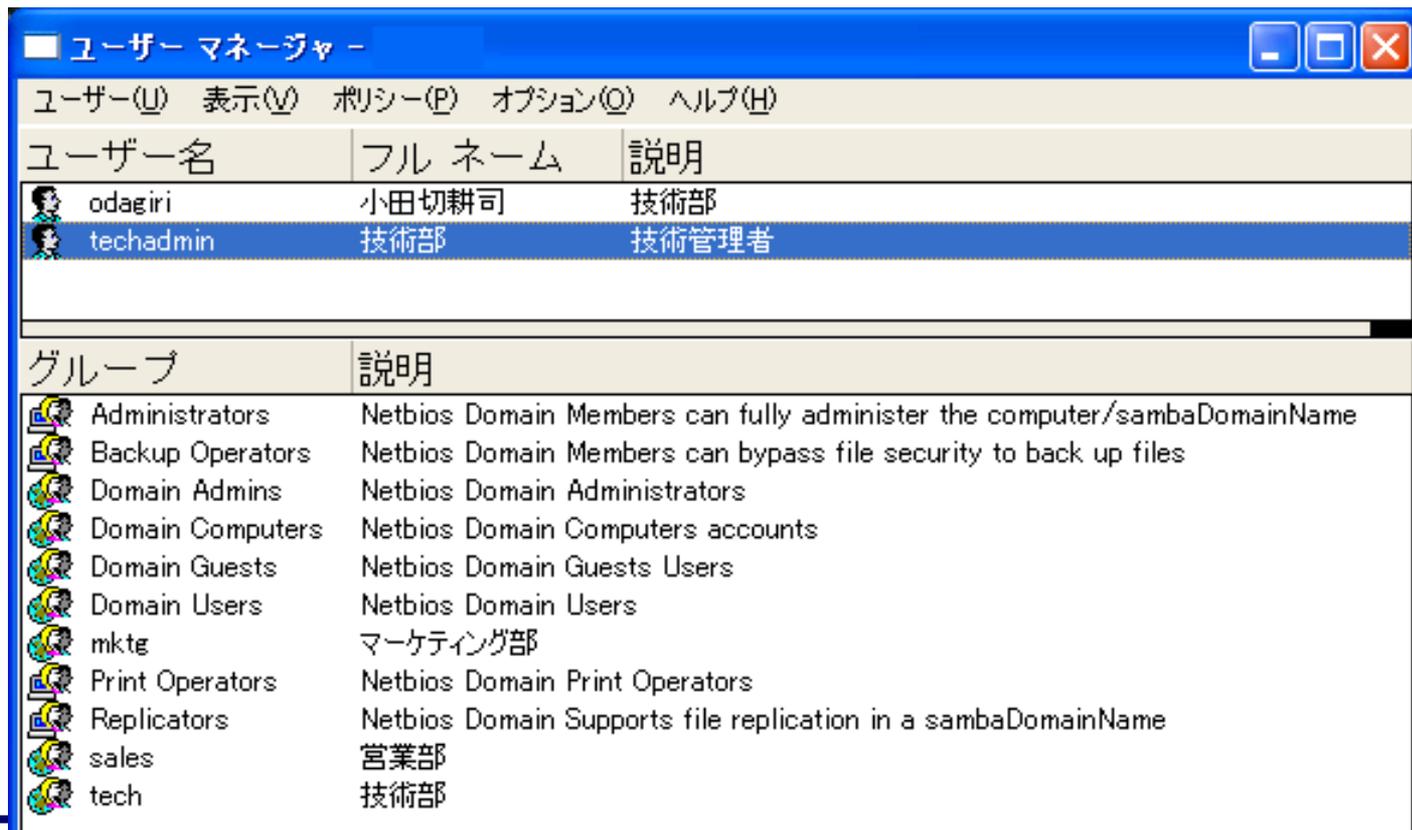
ドメイン管理者によるユーザマネージャ画面

- ドメインの管理者Administratorはドメイン全体の管理ができます
- ドメインに存在する全ユーザ／グループが参照できます
- 設定変更およびグループ追加は可能ですが、部門へのユーザ追加はできません



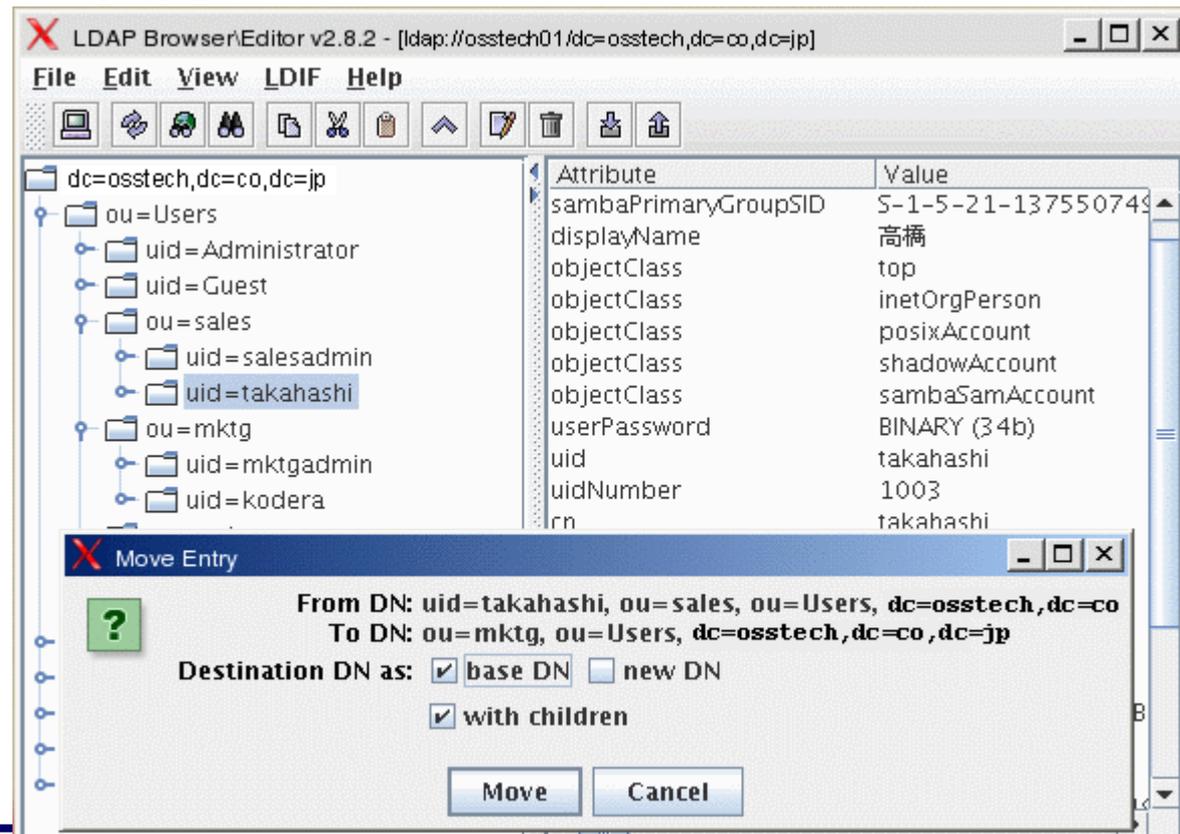
部門管理者によるユーザマネージャ画面

- 部門の管理者は自部門のユーザ管理、共有管理ができます
- グループ追加および自部門へユーザ登録、設定変更が可能です
- 他部門のユーザは見ることはできません
- グループに関して、ドメインに存在する全グループが参照できますが、グループに所属する他部門のユーザは見ることはできません



部門間でのユーザ移動

- ドメイン管理者Administratorが部門間のユーザ移動が可能です
- 操作はWindowsのユーザマネージャではなく、LDAP Editorを使って行います (LDAP Editorはフリーのプログラムです。<http://www-unix.mcs.anl.gov/~gawor/ldap/>)
- ユーザをクリックして、別部門のOUにドラッグします
- 所属するグループは変更されないので、ユーザマネージャで所属グループは変更ください



Part 5.

Active Directoryによる認証統合



OSSTech

Active Directoryによる認証統合

- Windows Active DirectoryもLDAPとしてアクセス可能
- SFU(Service for Unix)やAD4Unix(Active Directory for Unix)をWindowsサーバにインストールすることでUnixやLinuxからADユーザでログインできる。
- Mac OS Xも標準でAD認証に対応

ADによるUnix認証統合の問題点

- Windowsサーバにアドオンソフトをインストールする必要あり
- Windowsサーバ側でUnixユーザ(uid,gid)を意識した管理が必要で負荷が増大
- Solaris10のLDAPクライアントとADは相性が悪く、設定はできるが、運用するとトラブルが多い

SambaのWinbind機能を使った ADによるUnix認証統合

- Windowsサーバにアドオンソフトをインストールする必要なし
- Windowsサーバ側でUnixユーザ(uid,gid)を意識した管理が不要(ridをuid,gidに自動変換)
- Solaris10でも安定した運用が可能
- ※Solaris10標準付属のSambaはWinbindの機能を持っていない
- ※多くのLinuxディストリビューションに同梱されているSamba 3.0.23以下のバージョンはWinbindに関する不具合が多いので実用に耐えない

Part 6.

コンサルティング・サービス サポート・サービス メニュー

FreeOSに関するサポートとコンサルティング

- 弊社が検証したDELL PowerEdgeへのFreeOS導入サービス
- 上記OSへのさまざまなOSSの導入および設定
- 御客様が導入したFreeOSやOSSに関する問い合わせや障害調査
- 導入設定は20万円～
- 問い合わせ／障害解析は5万円～

問い合わせ (1インシデント5時間以内)			ダンプ解析／ソースコード解析 (1インシデント40時間以内)		
インシデント数	価格	有効期限	インシデント数	価格	有効期限
1	5万円	3ヶ月	1	50万円	3ヶ月
5	21万円	1年	5	210万円	1年
10	36万円	1年	10	360万円	1年

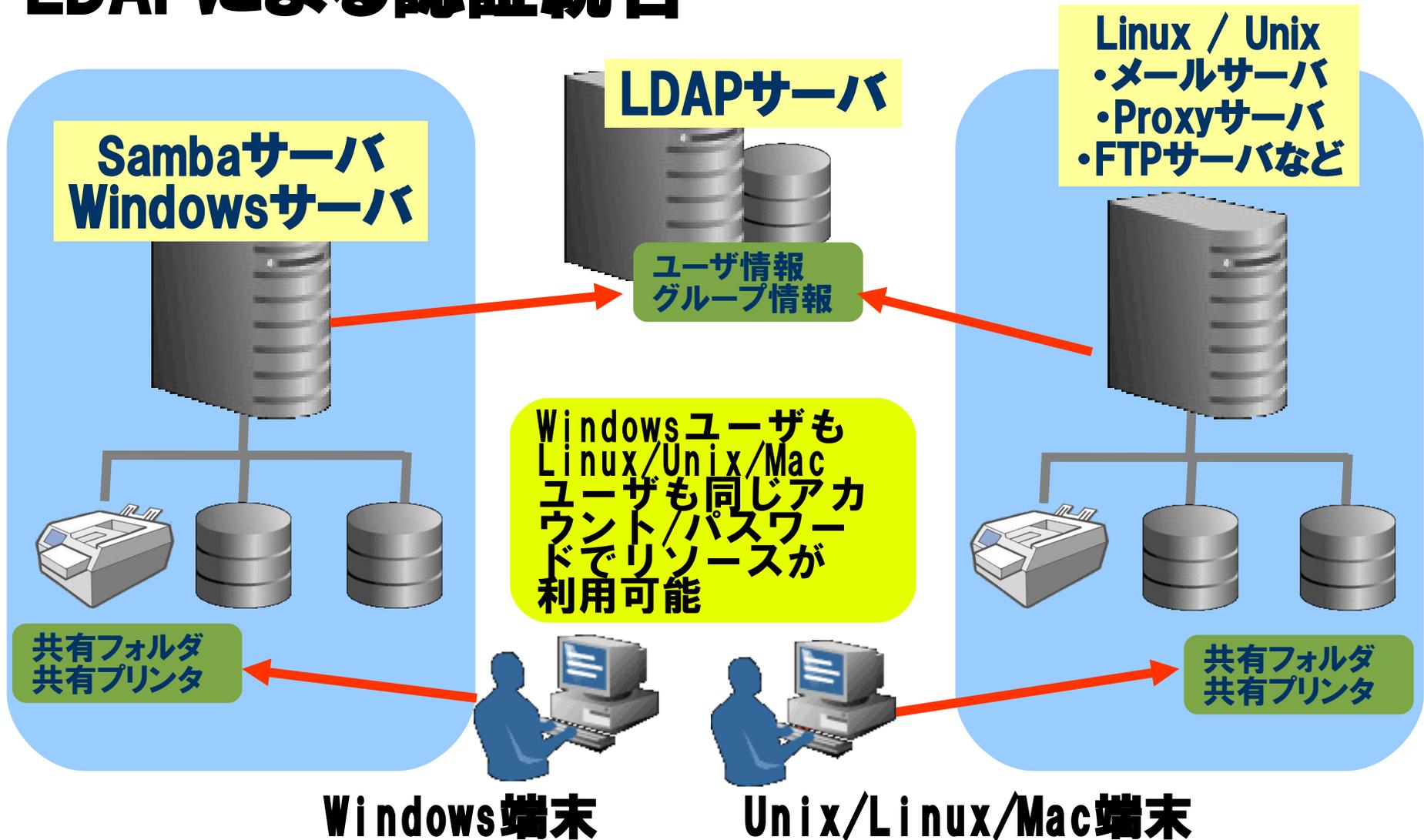
- お見積もり

お問い合わせ info@osstech.co.jp

コンサルティングサービスメニュー

- **OSS(オープンソース・ソフトウェア)を活用したシステム認証基盤構築サービスのご提案**
- **OSSや商用LDAP製品を使ったOSS認証基盤構築サービス**
OSSのSambaとOpenLDAP(もしくは商用LDAP製品)を使い、Windows, Unix, Linux, Macの認証統合を行う。
OSプラットフォームとしてLinuxだけでなく、Solarisなどの商用UNIXにも対応する。Active Directoryのような分散管理や権限委譲機能も提供。
- **既存のNISやNIS+からLDAPへの移行サービス**
古い商用UNIX認証環境をOSSのSambaとOpenLDAP(もしくは商用LDAP製品)を使い移行する。Windowsクライアントの認証にも対応可能。
- **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。
- **上記ソリューションのための製品、サポート、コンサルティングを提供**

LDAPによる認証統合



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

Linux / Unix
Samba 3.0
 ・ファイルサーバ
 ・メールサーバ
 ・Proxyサーバ
 ・FTPサーバなど

Windows 2000/2003
Active Directory

認証要求

ユーザ管理はすべてWindows上でを行い
 LinuxやUnixにユーザを作成する必要はない

共有フォルダ
 共有プリンタ

共有フォルダ
 共有プリンタ

ユーザ情報
 グループ情報

Unix/Linux/Mac端末

Windows端末

Samba/OpenLDAP保守サービス内容

サービスの種類		拡張サービス	サービスの内容
価格		Sambaのみ24万円/サイト・年 LDAPのみ 24万円/サイト・年 Samba+LDAP 36万円/サイト・年	Sambaサーバ運用に関する問い合わせ対応。 対応時間帯: 営業日の9時~17時
問い合わせ対応		○	Sambaサーバ運用に関する問い合わせ対応。 対応時間帯: 営業日の9時~17時
パッチの問い合わせ		○	コミュニティやディストリビュータから提供されている既存パッチに関する問い合わせ対応。
障害調査	発生現象の確認・調査	○	発生現象の確認と、過去に発生した障害の調査。
	メッセージの調査	○	Sambaサーバが出力する各種ログの調査。
	coreダンプの調査	○	Sambaが出力したcoreファイルの調査。
	再現環境の構築・評価	○	再現環境構築、評価。
	コミュニティへのフィードバック	○	新規障害判明時、コミュニティに対する障害報告と対応の働きかけを行う。 ただし、本サービスは障害解決を保証するものではない。
データの保障・復旧		コンサルティング・サービスで対応	ユーザデータの保障・復旧作業。
パフォーマンス分析・チューニング		コンサルティング・サービスで対応	Sambaサーバの性能情報収集、分析、チューニング作業。
パッチ作成		○	パッチ作成・適用。
Windowsドメインからの移行		コンサルティング・サービスで対応	既存のWindowsNTドメイン環境をクライアント側設定変更なし(ユーザやマシンの再登録なしで)にSamba環境へ移行します。
運用フェーズ前のサポート		コンサルティング・サービスで対応	システム設計、構築、性能チューニング、評価フェーズのサポート。