OSSを活用したシステム認証基盤構築のノウハウ

Samba/LDAPによるWindowsドメイン管理
権限の分離と委譲

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

OSSTech

Copyright © 2006 Open Source Solution Technology Corporation All Rights Reserved.

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
業務内容	ソフトウエアの企画、開発、販売およびメンテナンス ソフトウエアおよびシステムの導入に関するコンサルティング ソフトウエアに関する教育、研修、支援 ソフトウエア関連の出版業務 前各号に付帯関連する一切の業務
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	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

Copyright © 2006 Open Source Solution Technology Corporation All Rights Reserved.

講師の最近著作紹介

- **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 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
- 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

Copyright © 2006 Open Source Solution Technology Corporation All Rights Reserved.

セキュリティと認証

- 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OSSを使おうという意識はまだ低い

Copyright © 2006 Open Source Solution Technology Corporation All Rights Reserved.

皆さんの周りにある認証が必要なシステム

- 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！

Copyright © 2006 Open Source Solution Technology Corporation All Rights Reserved.

OSSを使った認証基盤の構築

- OSSだからこその親和性
  OSSのSambaとOpenLDAPを使ってUnix/ Linux/ Windows/ Mac Osの統合認証が可能になる。
- 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

Copyright © 2006 Open Source Solution Technology Corporation All Rights Reserved.

OSSを使った認証基盤構築への課題

- 既存のNTドメイン、ADドメインをどうするか？
  移行できるのか？
- 既存のWindowsドメインを統合できないか？
- NISやNIS+をLDAPへ移行できるのか？
- 信頼性はあるのか？
- スケーラビリティはどうやって確保するのか？
- OSSの認証基盤は誰がサポートしてくれるのか？

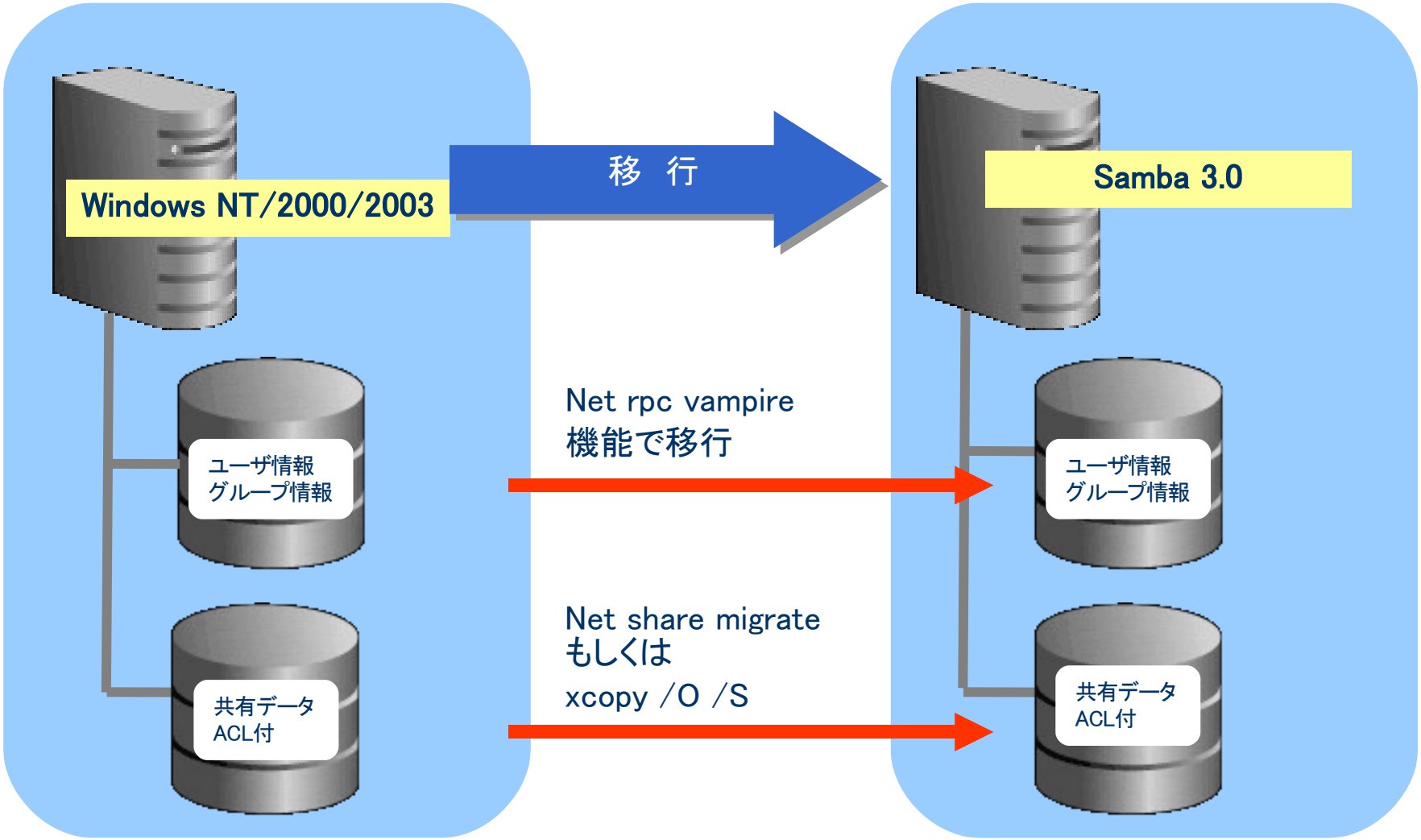
Copyright © 2006 Open Source Solution Technology Corporation All Rights Reserved.

SambaによるWindowsドメインの移行

- Samba 3.0から可能になったvampire(吸血鬼)機能やnet share migarete機能により、単一のWindowsドメインを移行するのは(Samba.2.2に比べれば)比較的簡単にできるようになりました。
- Windowsから自動移行可能なドメイン・リソース
  - ユーザ／グループ情報
  - 共有情報、共有設定
  - 共有データ
  - ACLも移行できるが完全互換でないため事前調査は重要
- Sambaを使うとWindowsだけでなく、Unix,Linux,業務アプリの認証統合が可能になる。

Copyright © 2006 Open Source Solution Technology Corporation All Rights Reserved.

WindowsからSambaへの移行



Copyright © 2006 Open Source Solution Technology Corporation All Rights Reserved.

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

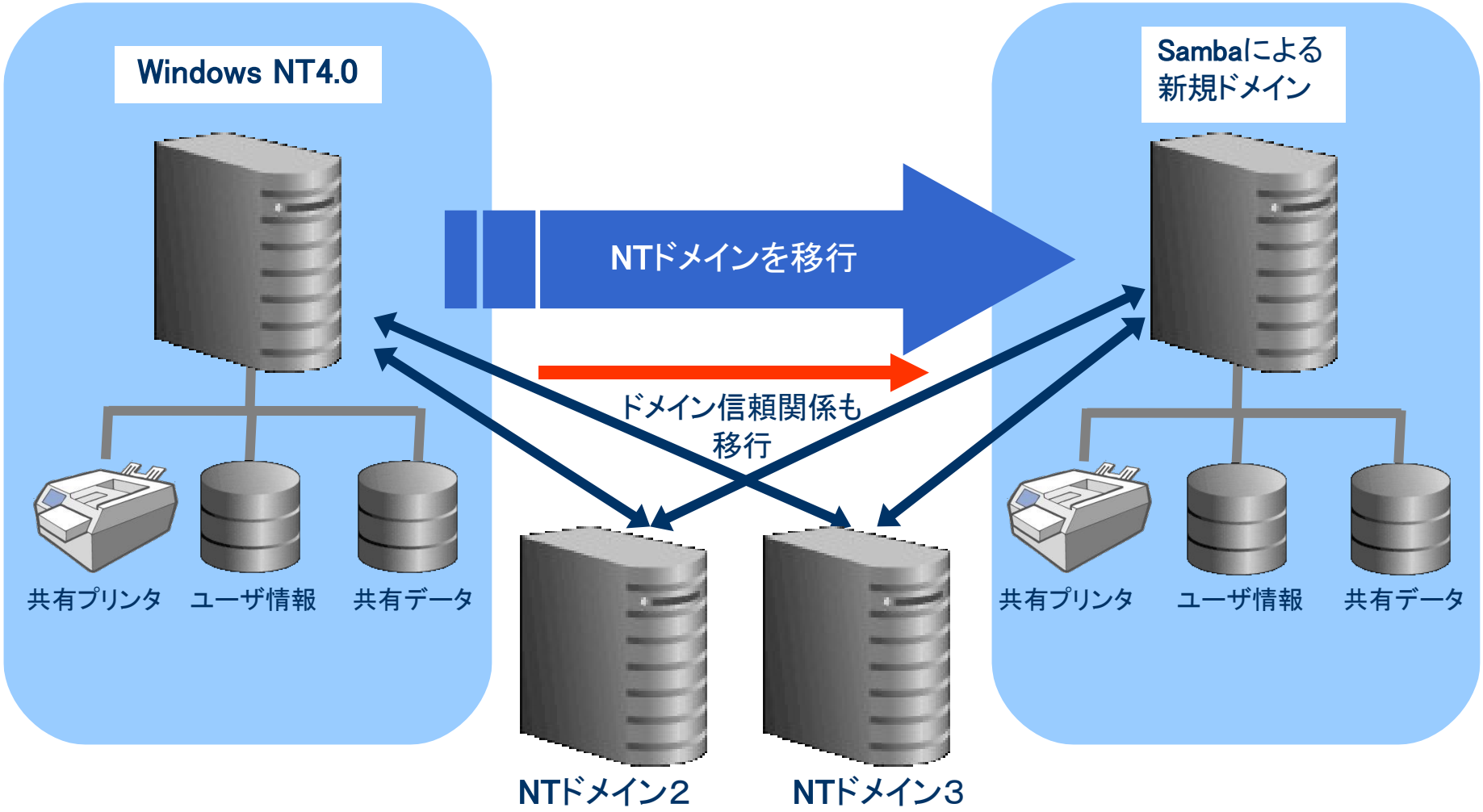
Copyright © 2006 Open Source Solution Technology Corporation All Rights Reserved.

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。

Copyright © 2006 Open Source Solution Technology Corporation All Rights Reserved.

vampireと手作業による移行



Copyright © 2006 Open Source Solution Technology Corporation All Rights Reserved.

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

Copyright © 2006 Open Source Solution Technology Corporation All Rights Reserved.

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

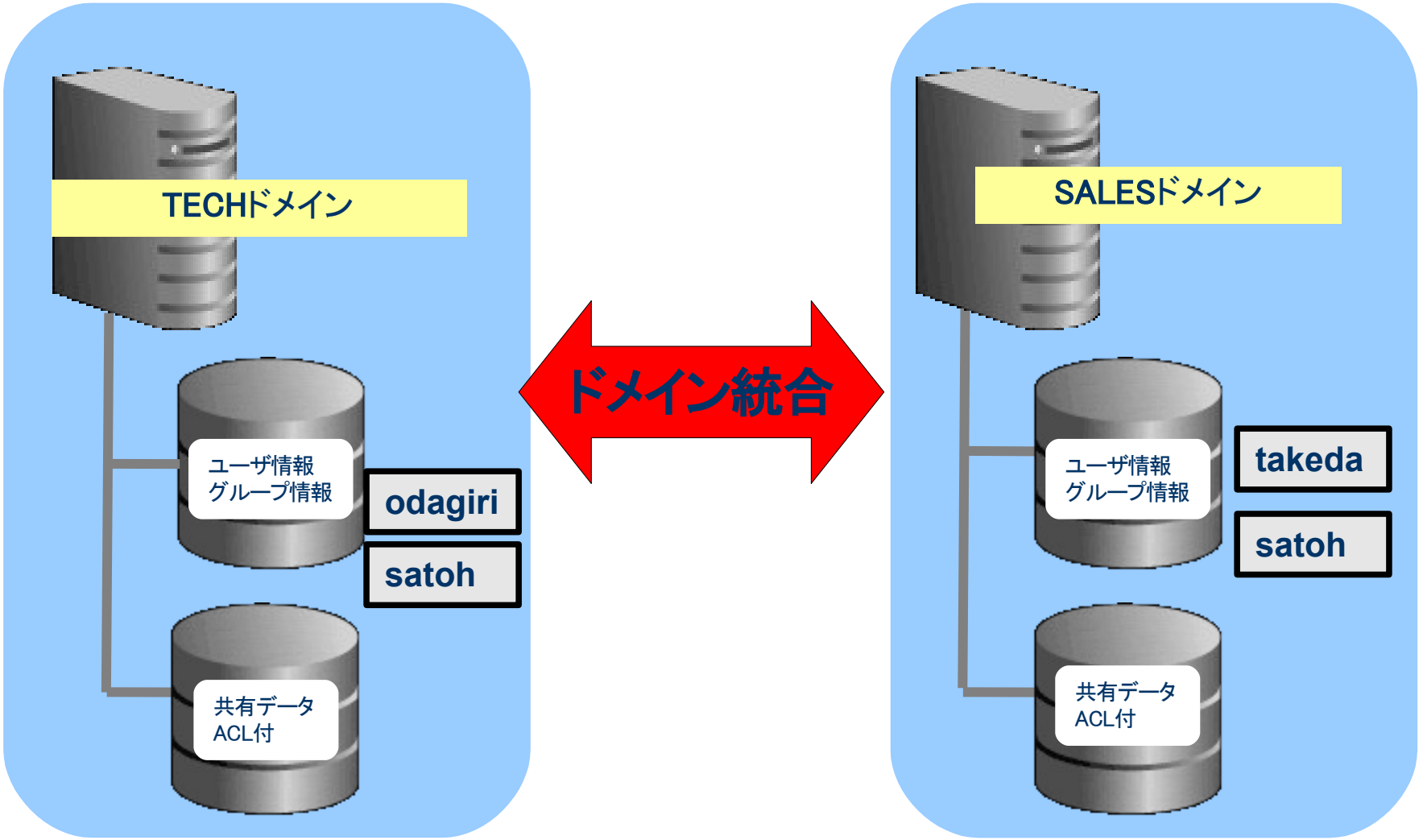
Copyright © 2006 Open Source Solution Technology Corporation All Rights Reserved.

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

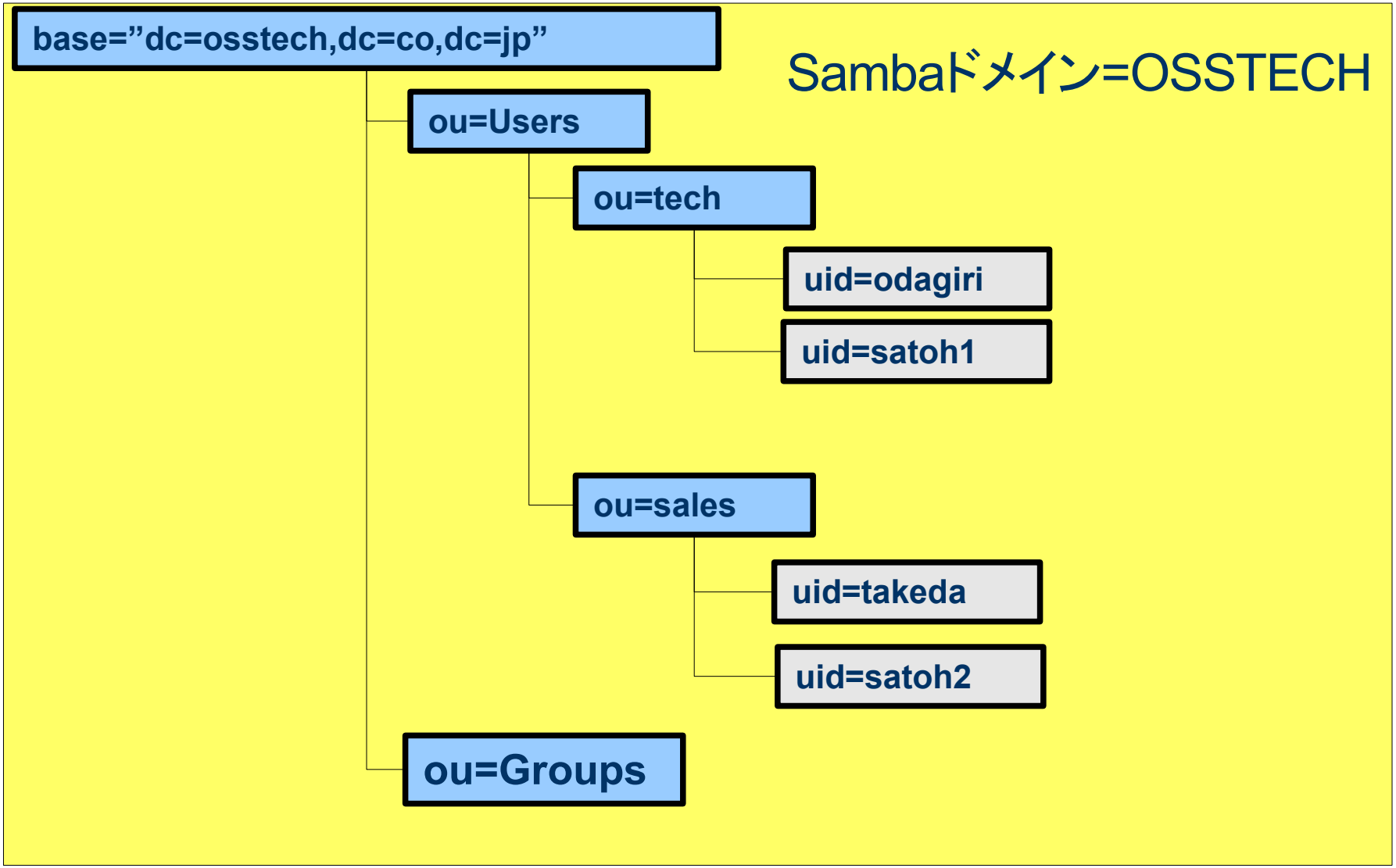
Copyright © 2006 Open Source Solution Technology Corporation All Rights Reserved.

統合前のWindowsドメイン イメージ



Copyright © 2006 Open Source Solution Technology Corporation All Rights Reserved.

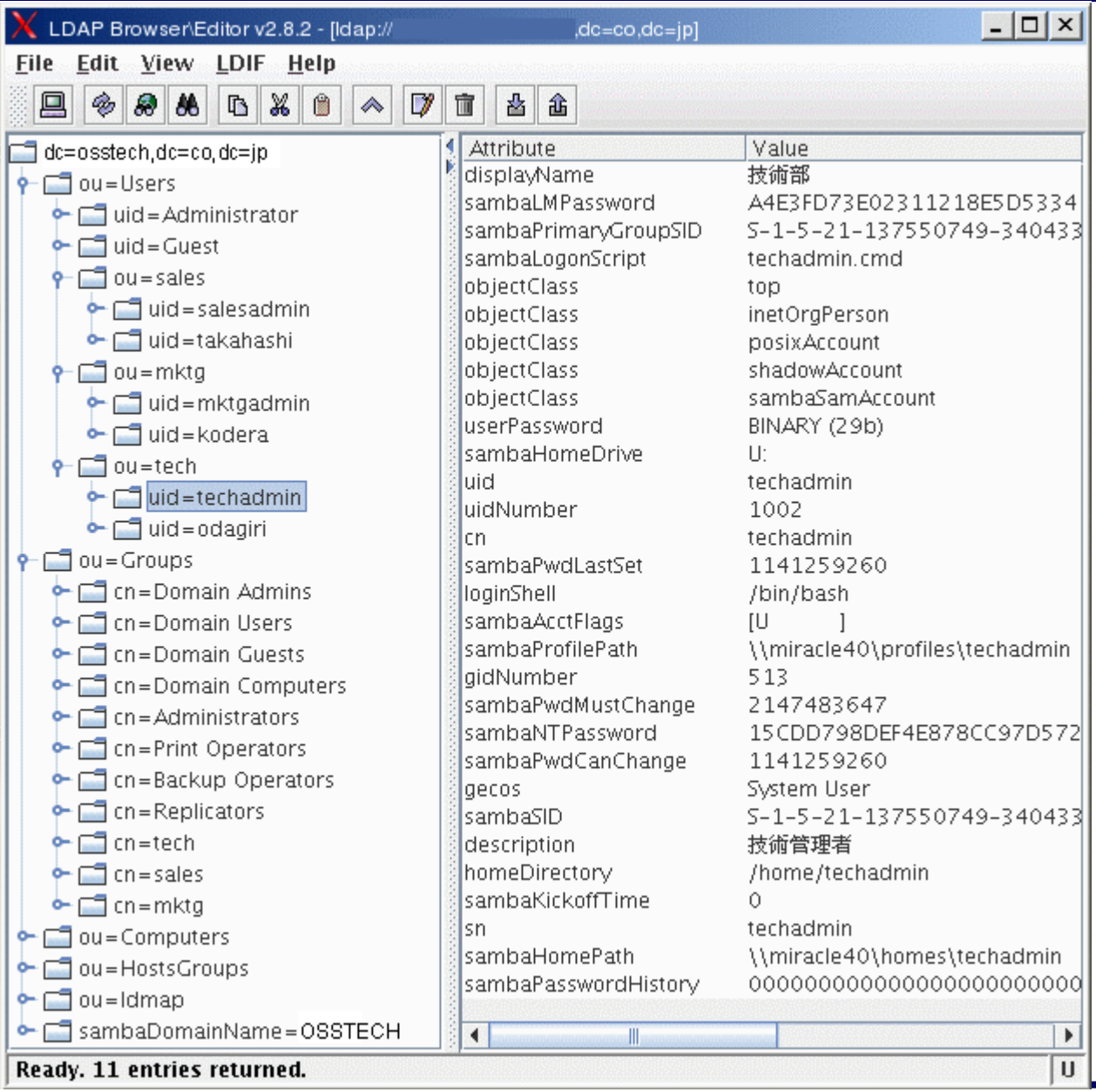
単一ベースサフィックス、単一ドメイン方式



Copyright © 2006 Open Source Solution Technology Corporation All Rights Reserved.

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



Copyright © 2006 Open Source Solution Technology Corporation All Rights Reserved.

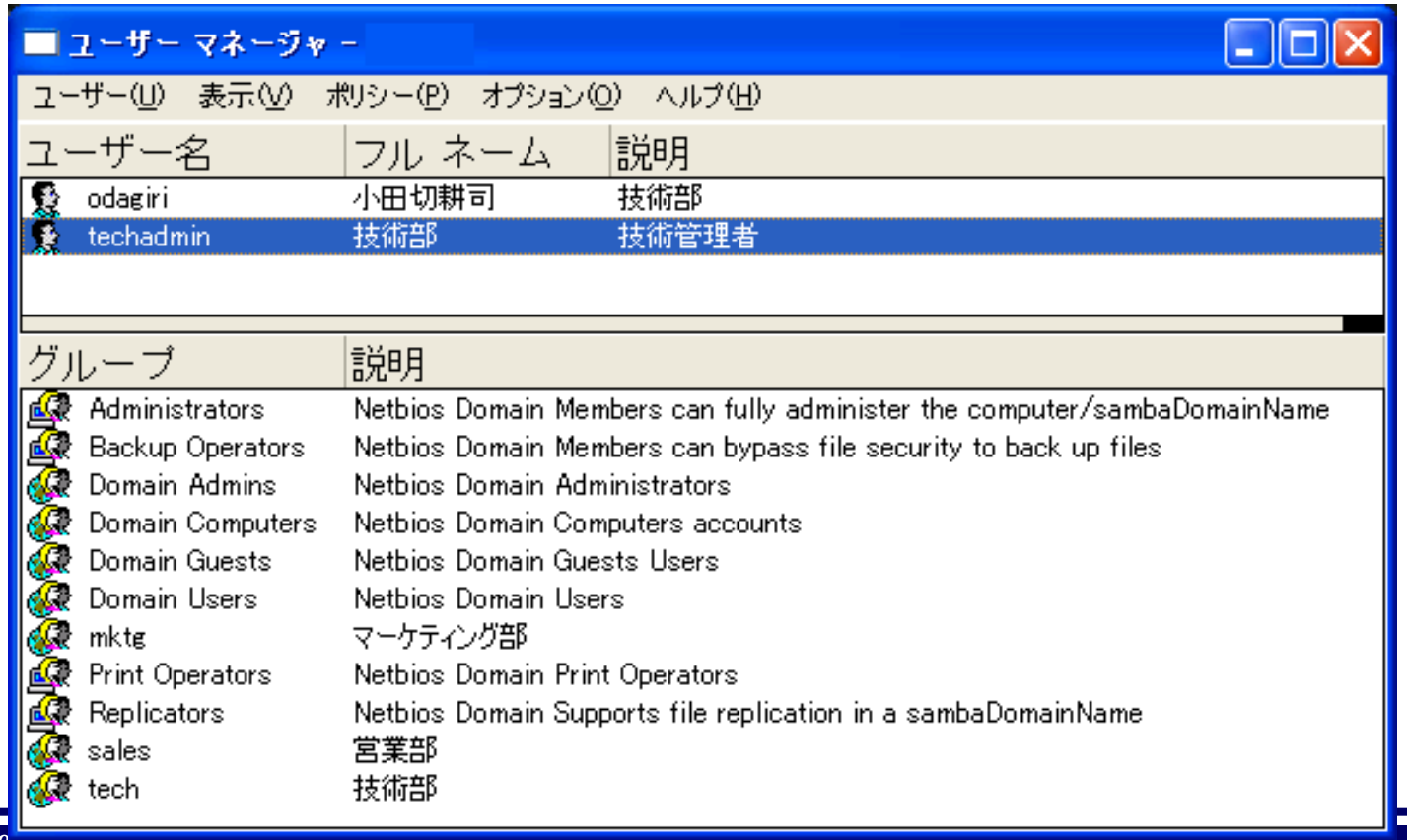
ドメイン管理者によるユーザマネージャ画面

- 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

Copyright © 2006 Open Source Solution Technology Corporation All Rights Reserved.

部門管理者によるユーザマネージャ画面

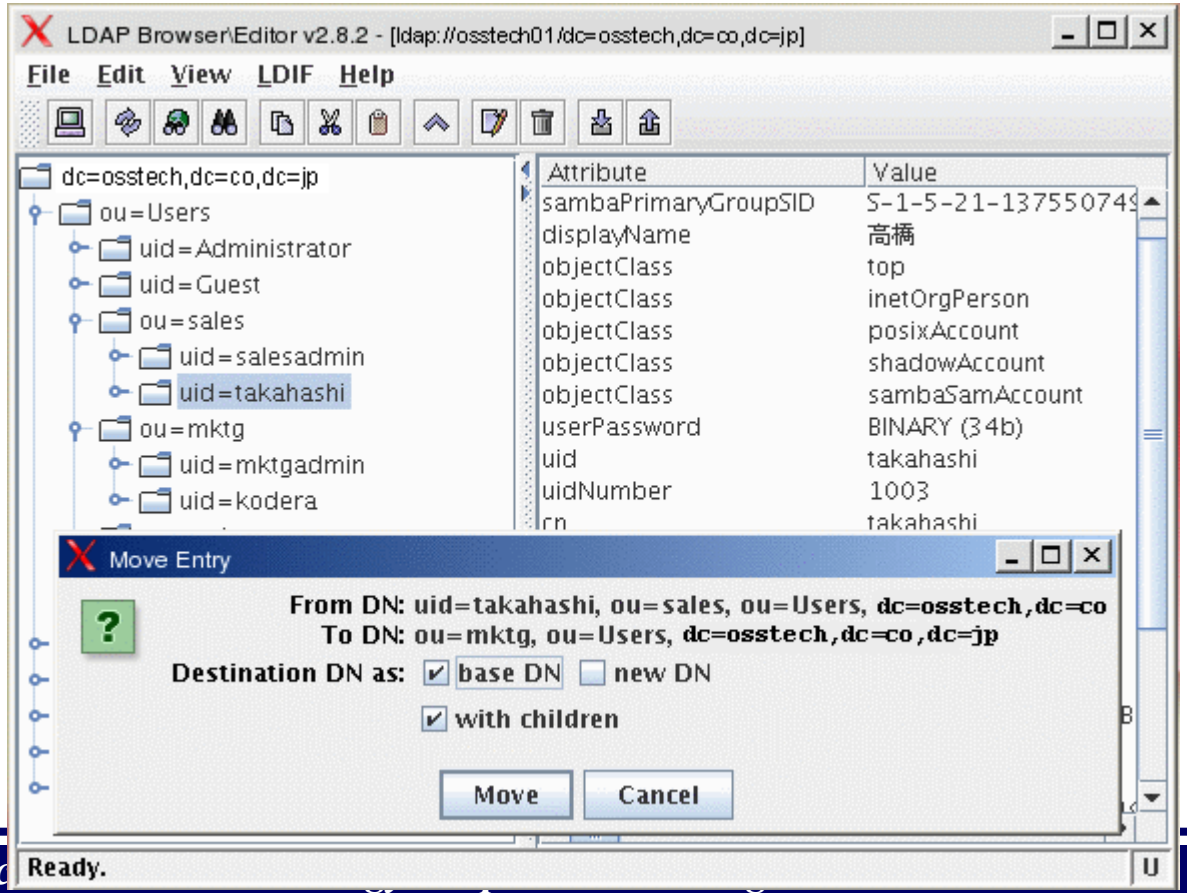
- 部門の管理者は自部門のユーザ管理、共有管理ができます
- グループ追加および自部門へユーザ登録、設定変更が可能です
- 他部門のユーザは見ることができません
- グループに関して、ドメインに存在する全グループが参照できますが、グループに所属する他部門のユーザは見ることができません



Copyright © 2006 Open Source Solution Technology Corporation All Rights Reserved.

部門間でのユーザ移動

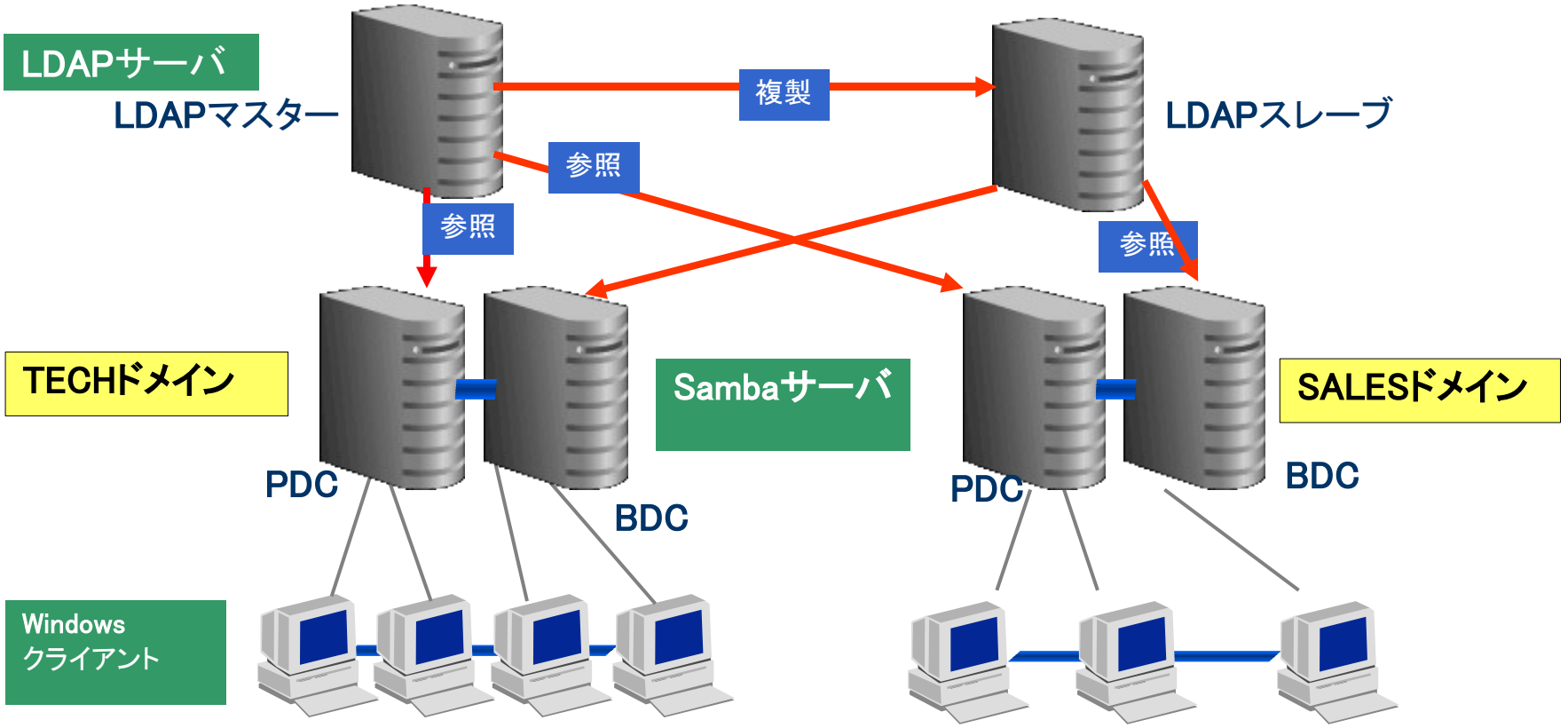
- ドメイン管理者Administratorが部門間のユーザ移動が可能です
- 操作はWindowsのユーザマネージャではなく、LDAP Editorを使って行います
  （LDAP Editorはフリーのプログラムです。http://www-unix.mcs.anl.gov/~gawor/ldap/ ）
- ユーザをクリックして、別部門のOUにドラッグします
- 所属するグループは変更されないので、ユーザマネージャで所属グループは変更ください



Copyright © 2006 Open Sourc

システム構成図(1)

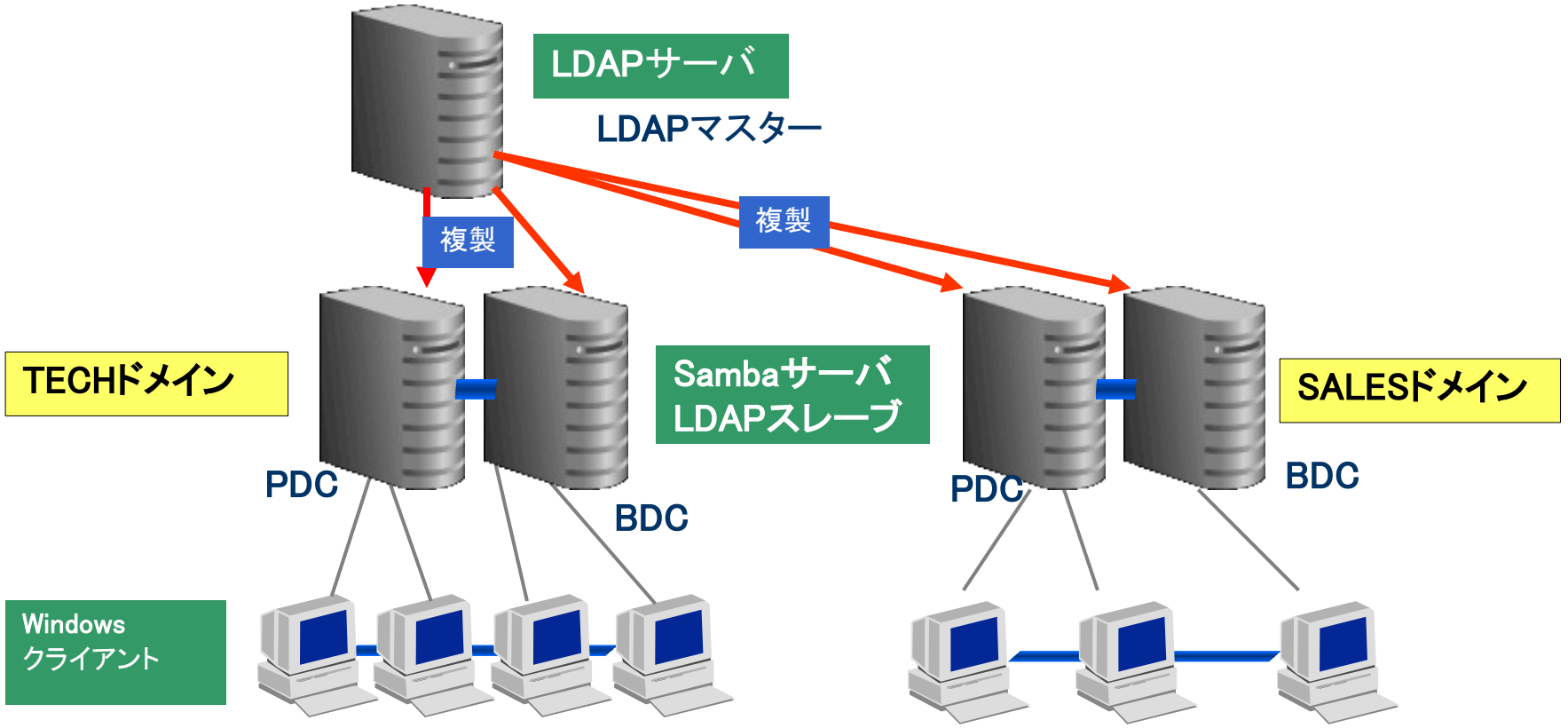
A),B),C)どのケースでもLDAPサーバは1台でも良い。(スレーブサーバは必要)
A),B)のケースでSambaサーバは、ドメインの数だけあれば良いが1台でも構わない。
(規模が大きい場合や信頼性が必要な場合はBDCも用意する)



Copyright © 2006 Open Source Solution Technology Corporation All Rights Reserved.

システム構成図(2)

マスターLDAPサーバを1台だけにし、Sambaサーバの上でLDAPスレーブを動かす構成
Sambaサーバは、ドメインの数だけあれば良いが1台でも構わない。
（規模が大きい場合や信頼性が必要な場合はBDCも用意する）



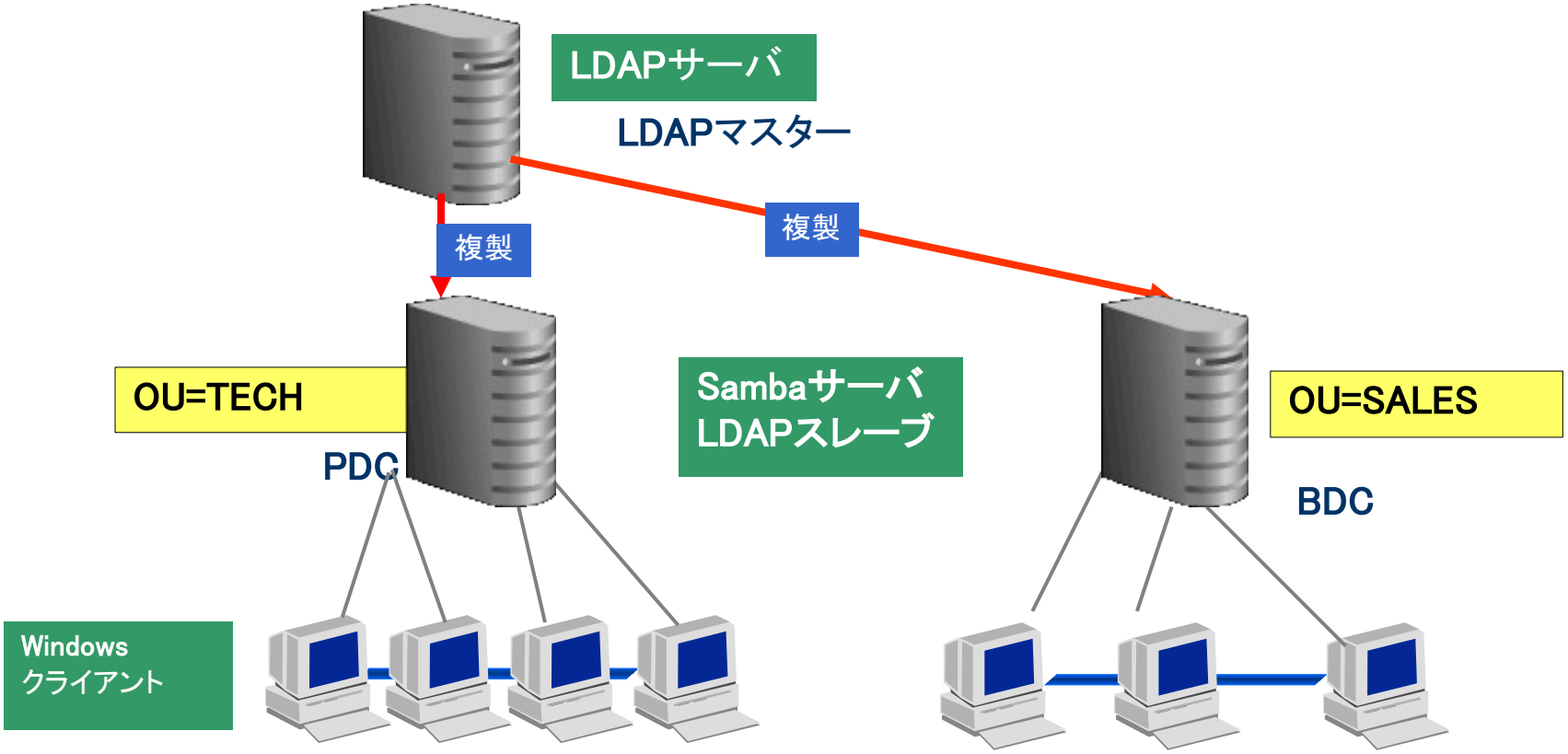
Copyright © 2006 Open Source Solution Technology Corporation All Rights Reserved.

システム構成図(3)

C)の場合、マスターLDAPサーバを1台だけにし、Sambaサーバの上でLDAPスレーブを動かす構成が可能

Sambaサーバは、OUの数だけあれば良いが1台でも構わない。

（規模が大きい場合や信頼性が必要な場合はBDCも用意する）



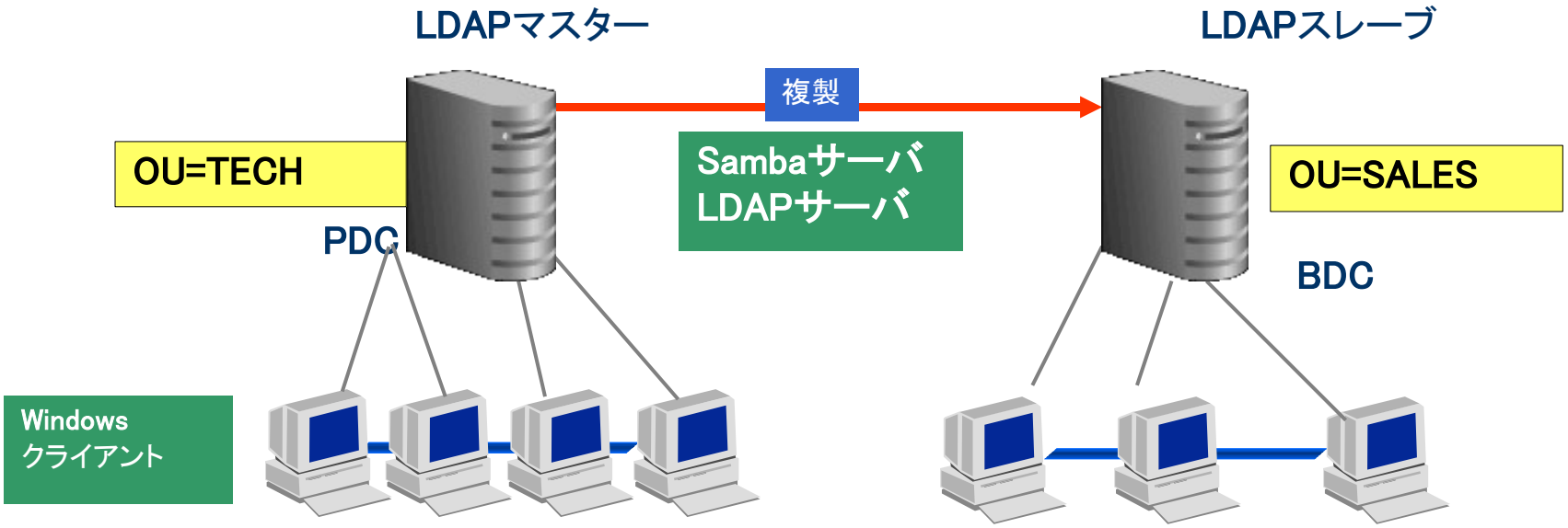
Copyright © 2006 Open Source Solution Technology Corporation All Rights Reserved.

システム構成図(4)

C)の場合、マスターLDAPサーバとPDCを1台用意し、もう一台のSambaサーバの上で
LDAPスレーブとBDCを動かす構成が可能

Sambaサーバは、OUの数だけあれば良いが1台でも構わない。

（規模が大きい場合や信頼性が必要な場合はBDCも用意する）



Copyright © 2006 Open Source Solution Technology Corporation All Rights Reserved.

実際の移行作業

- Vampireだけでは複数ドメイン統合は難しい。
- Pwdumpを使ってWindowsドメイン情報を取り出してスクリプトを使ってLDAPに投入するのが現実的

ドメイン統合は弊社へご相談ください。

Copyright © 2006 Open Source Solution Technology Corporation All Rights Reserved.

オンサイトWindows移行Samba/LDAP導入サービス

オンサイト・サービス：標準価格160万円(税込み168万円)

- 弊社エンジニアがお客様のところに出向きWindowsをLinuxへ移行します。
  - 2台のマシンにLinux,Samba,LDAPサーバを導入します。
  - LinuxはRed Hat, CentOS, MIRACLE LINUX, Debian が標準となります。
    - LINUX以外の場合はご相談ください
  - 1台をWindowsプライマリドメインコントローラ、LDAPマスタサーバとして設定し、もう一台をWindowsバックアップドメインコントローラ、LDAPスレーブサーバとして設定します。
  - 既存のWindowsドメイン環境からパスワードを含むユーザ情報やグループ情報をそのままLinuxのファイルサーバへ移行できます。
  - 既存の共有フォルダや共有プリンタを移行します。
  - お客様の要望により、既存のWindowsドメインとの信頼関係も設定します。
  - お客様からのコンサルティング申込後、設定パラメータをメールでヒアリングします。環境パラメータが決定したら現地での作業は1～2日で完了します。
  - 関東圏（東京、神奈川、埼玉、千葉）以外の場合、交通費・宿泊費を頂く場合があります。
  - 台数が2台以外の場合や条件が異なる場合はご相談ください。

Copyright © 2006 Open Source Solution Technology Corporation All Rights Reserved.

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。

Copyright © 2006 Open Source Solution Technology Corporation All Rights Reserved.

製品パッケージの提供サービス

- Red Hat , Fedora Coreを初めとするLinuxディストリビューションには最初からSambaやOpenLDAPが同梱されていますが、日本語対応パッチや国際化対応パッチ、日本語ドキュメントが不足している場合があります。
- UNIX/Linuxの上でSambaとLDAPでドメインコントローラを構築するためのツールSmbldap-toolsやLAM(LDAP Account Manager), Webmin,Usermin などのOSSパッケージが足りないこともあります。（特に商用UNIX系）
- これらをすべて製品パッケージとして提供します。
- 対応OSは商用Linuxだけでなく、SolarisやDebian, CentOS,FreeBSD,Windowsなどにも提供します。

Copyright © 2006 Open Source Solution Technology Corporation All Rights Reserved.

提供予定教育コンテンツ一覧

- Samba+LDAPによるWindowsファイルサーバおよびドメインコントローラの構築
  - Linuxによる Windowsファイルサーバの構築方法
  - Linuxによる Windowsドメインの構築方法
  - LDAPによる Linux/Unix/Windows/Mac認証統合
- ディレクトリサービス(LDAP)の導入と運用
  - LDAP概論、DITの概要と設計
  - スキーマの利用方法と設計
  - LDAPの導入とDITの構築
  - データ投入とデータの管理／操作
  - LDAP運用管理

Copyright © 2006 Open Source Solution Technology Corporation All Rights Reserved.

紹介した弊社のサービスは直接お客様に弊社から提供させて頂くことも可能ですし、システムインテグレータの方々を通して提供することも可能です。

OSSTech

【お問い合わせ先】

オープンソース・ソリューション・テクノロジ株式会社

http://www.osstech.co.jp

Copyright © 2006 Open Source Solution Technology Corporation All Rights Reserved.