

Samba/LDAPによる 既存複数Windowsドメインの 統合とその方式比較



OSSTech

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 チーフアーキテクト
小田切耕司

odagiri@osstech.co.jp

Shall we Samba ? : <http://blog.odagiri.org/>

講師の著作紹介

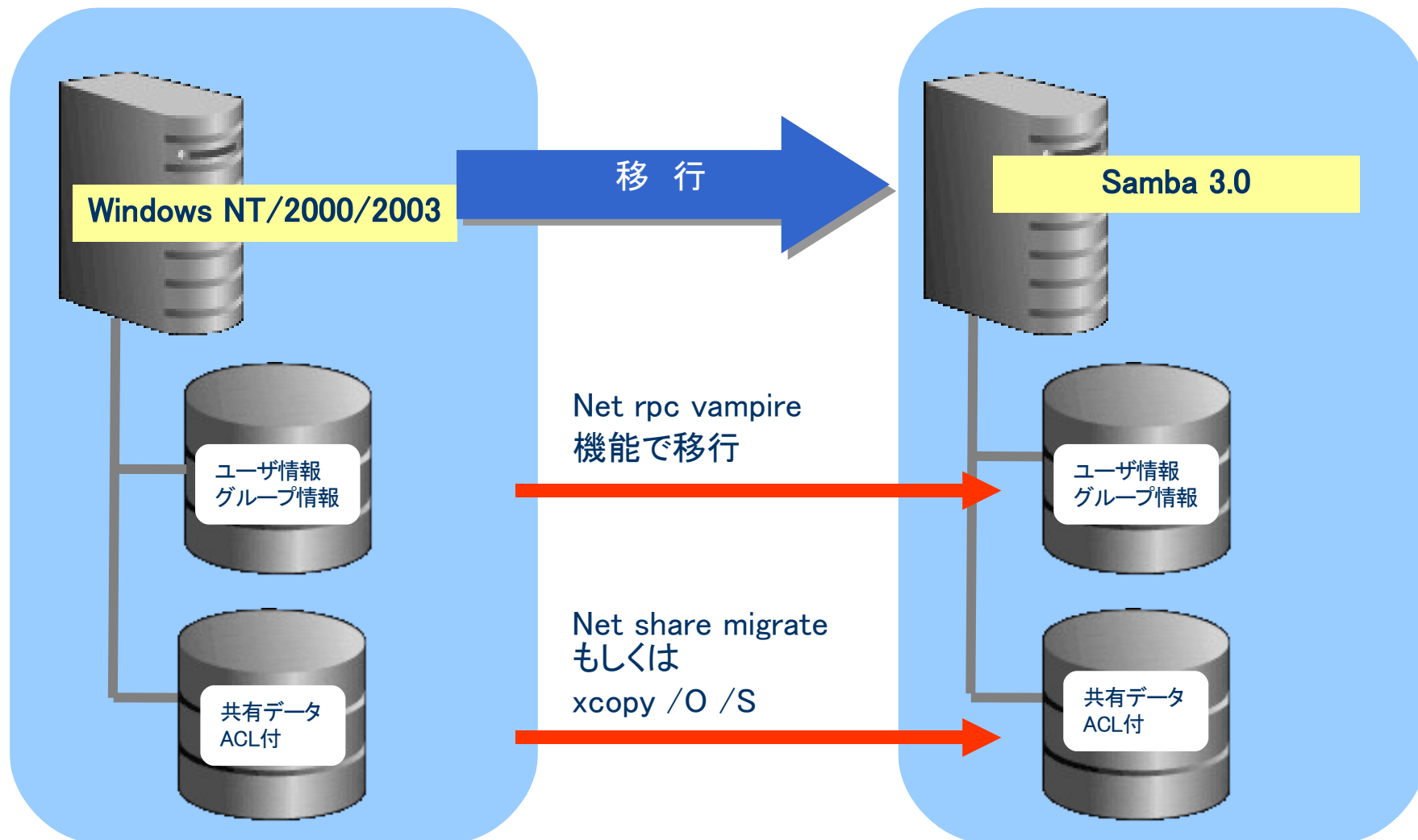
- ◆ **技術評論社 Software Design 2006年7月号**
 - ネットワーク運用／管理 五輪書(ごりんのしょ)
 - 「巻:地の巻」Sambaファイルサーバ
 - <http://www.gihyo.co.jp/magazines/SD/contents/200607>
- ◆ **2006年5月 翔泳社 開発の現場 vol.005**
 - オープンソース案件指南帖
 - 総論編:オープンソースの基礎知識
 - <http://www.shoeisha.com/mag/kaihatsu/>
- ◆ **2006年5月 技術評論社 LDAP Super Expert**
 - 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>



SambaによるWindowsドメインの移行

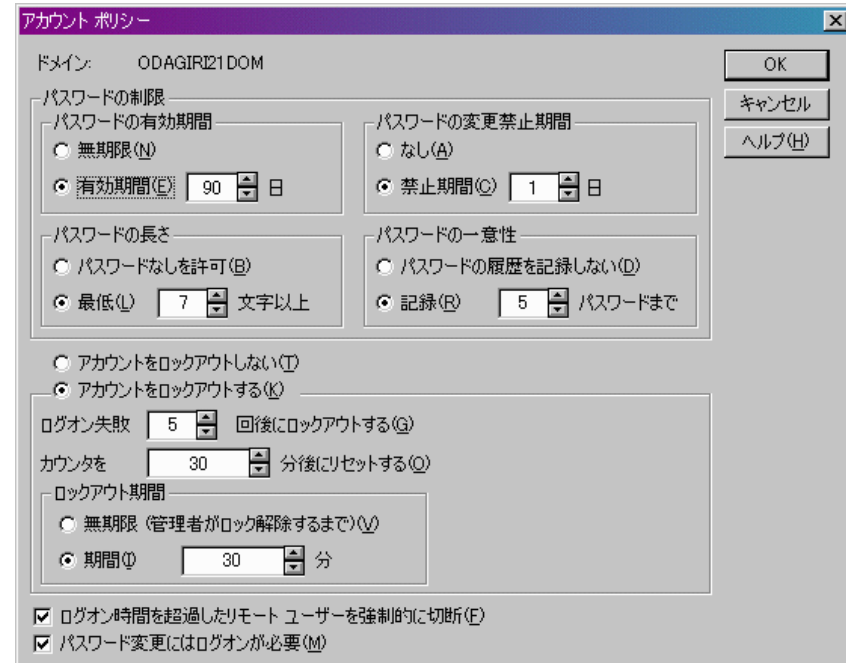
- Samba 3.0から可能になったvampire(吸血鬼)機能やnet share migarete機能により、単一のWindowsドメインを移行するのは(Samba.2.2に比べれば)比較的簡単にできるようになりました。
- Windowsから自動移行可能なドメイン・リソース
 - ユーザ／グループ情報
 - 共有情報、共有設定
 - 共有データ
 - ACLも移行できるが完全互換でないため事前調査は重要

WindowsからSambaへの移行



自動では難しいが手動で移行できるもの

- システムポリシー
 - デスクトップやメニューなどに関するセキュリティポリシーを設定
- アカウントポリシー
 - パスワード履歴や有効期限
- ユーザマネージャ(vampire では移行可能)
 - ログオンできる時間帯やワークステーションを制限



アカウント ポリシー

ドメイン: ODAGIRI21.DOM

パスワードの制限

パスワードの有効期間

無期限(N)

有効期間(E) 90 日

パスワードの変更禁止期間

なし(A)

禁止期間(C) 1 日

パスワードの長さ

パスワードなしを許可(B)

最低(L) 7 文字以上

パスワードの一意性

パスワードの履歴を記録しない(D)

記録(R) 5 パスワードまで

アカウントをロックアウトしない(T)

アカウントをロックアウトする(K)

ログオン失敗 5 回後にロックアウトする(Q)

カウンタを 30 分後にリセットする(Q)

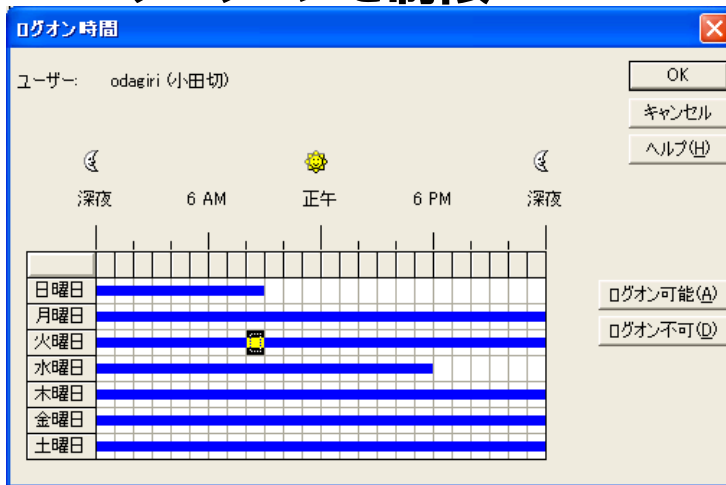
ロックアウト期間

無期限(管理者がロック解除するまで)(V)

期間(W) 30 分

ログオン時間を超過したリモート ユーザーを強制的に切断(E)

パスワード変更にはログオンが必要(M)



ログオン時間

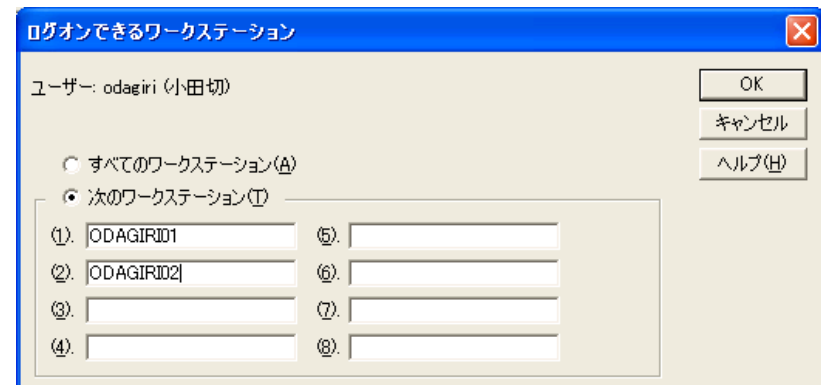
ユーザー: odagiri (小田切)

深夜 6 AM 正午 6 PM 深夜

| | | |
|-----|-----------|-----------|
| 日曜日 | 深夜 - 6 AM | ログオン可能(A) |
| 月曜日 | 深夜 - 6 PM | ログオン可能(A) |
| 火曜日 | 深夜 - 6 PM | ログオン可能(A) |
| 水曜日 | 深夜 - 6 PM | ログオン可能(A) |
| 木曜日 | 深夜 - 6 PM | ログオン可能(A) |
| 金曜日 | 深夜 - 6 PM | ログオン可能(A) |
| 土曜日 | 深夜 - 6 PM | ログオン可能(A) |

ログオン可能(A)

ログオン不可(Q)



ログオンできるワークステーション

ユーザー: odagiri (小田切)

すべてのワークステーション(A)

次のワークステーション(T)

(1) ODAGIRI01 (5) []

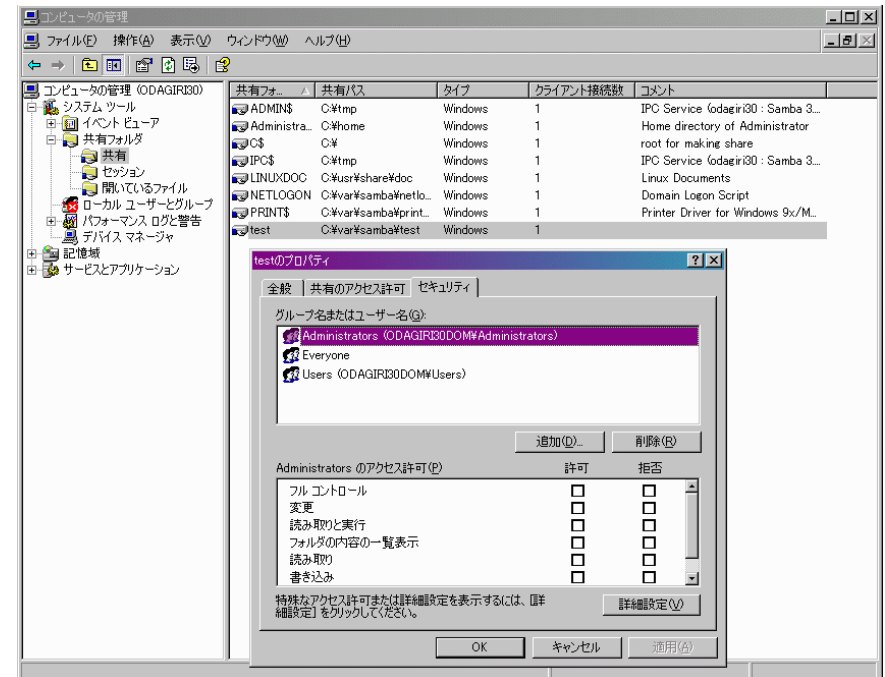
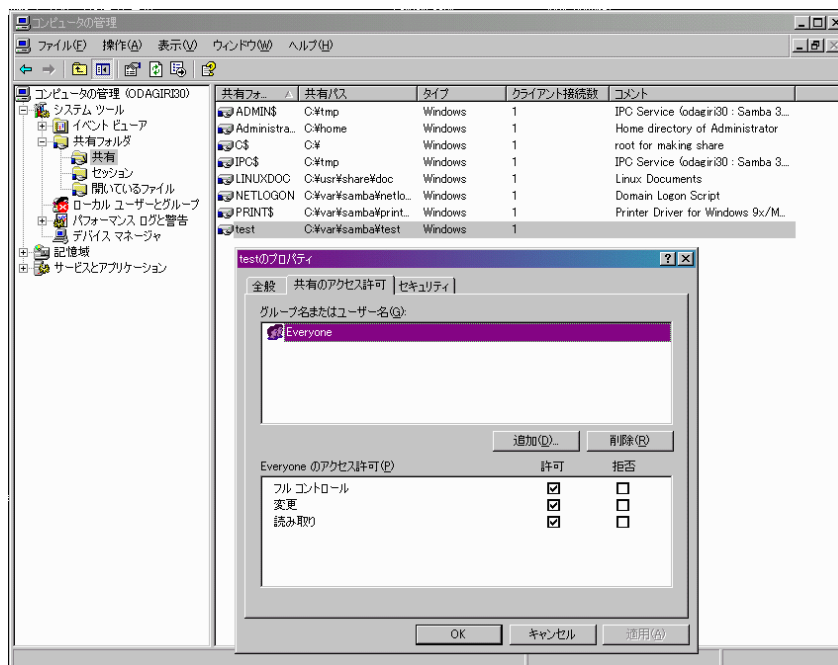
(2) ODAGIRI02 (6) []

(3) [] (7) []

(4) [] (8) []

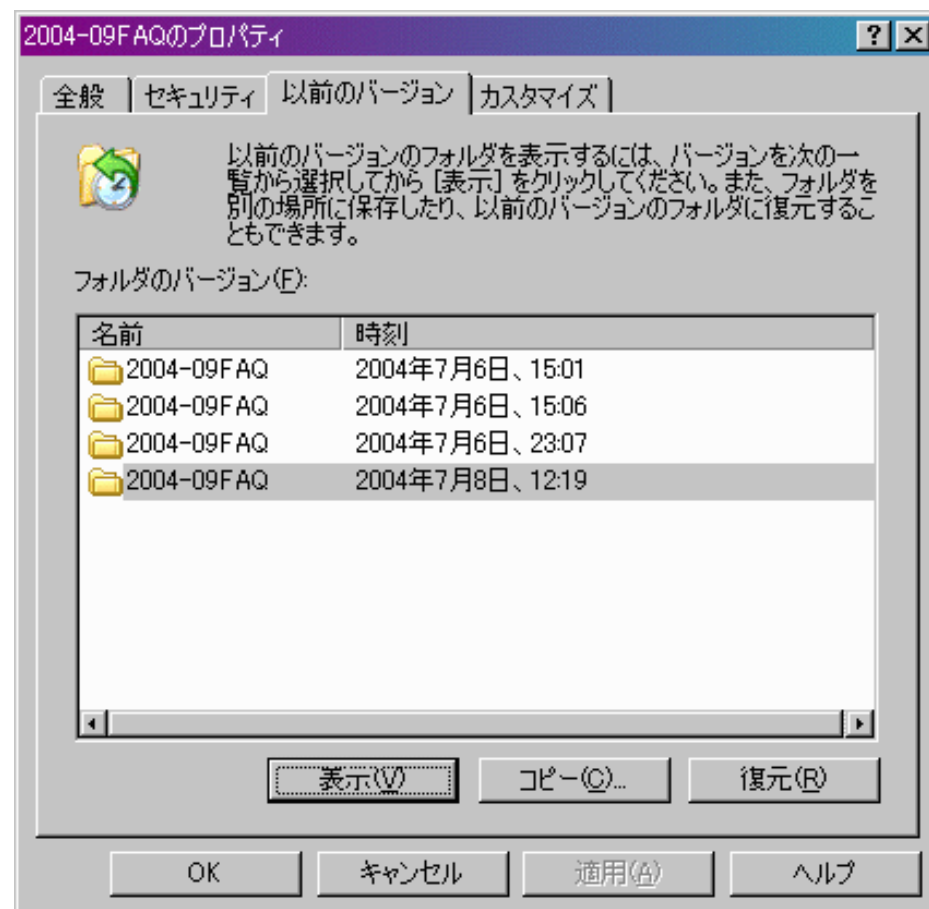
ファイル／フォルダのアクセス権の移行

- ACLは完全に移行できないケースがあるので、事前調査が重要



VSS(ボリューム・シャドウ・コピー・サービス)

- 「以前のバージョン」からファイルを復元可能 (→右図)
- Kernel 2.4まではLVM+XFSが必要
- Kernel 2.6からはLVM2のみで構築可能。ext3でも利用可能。



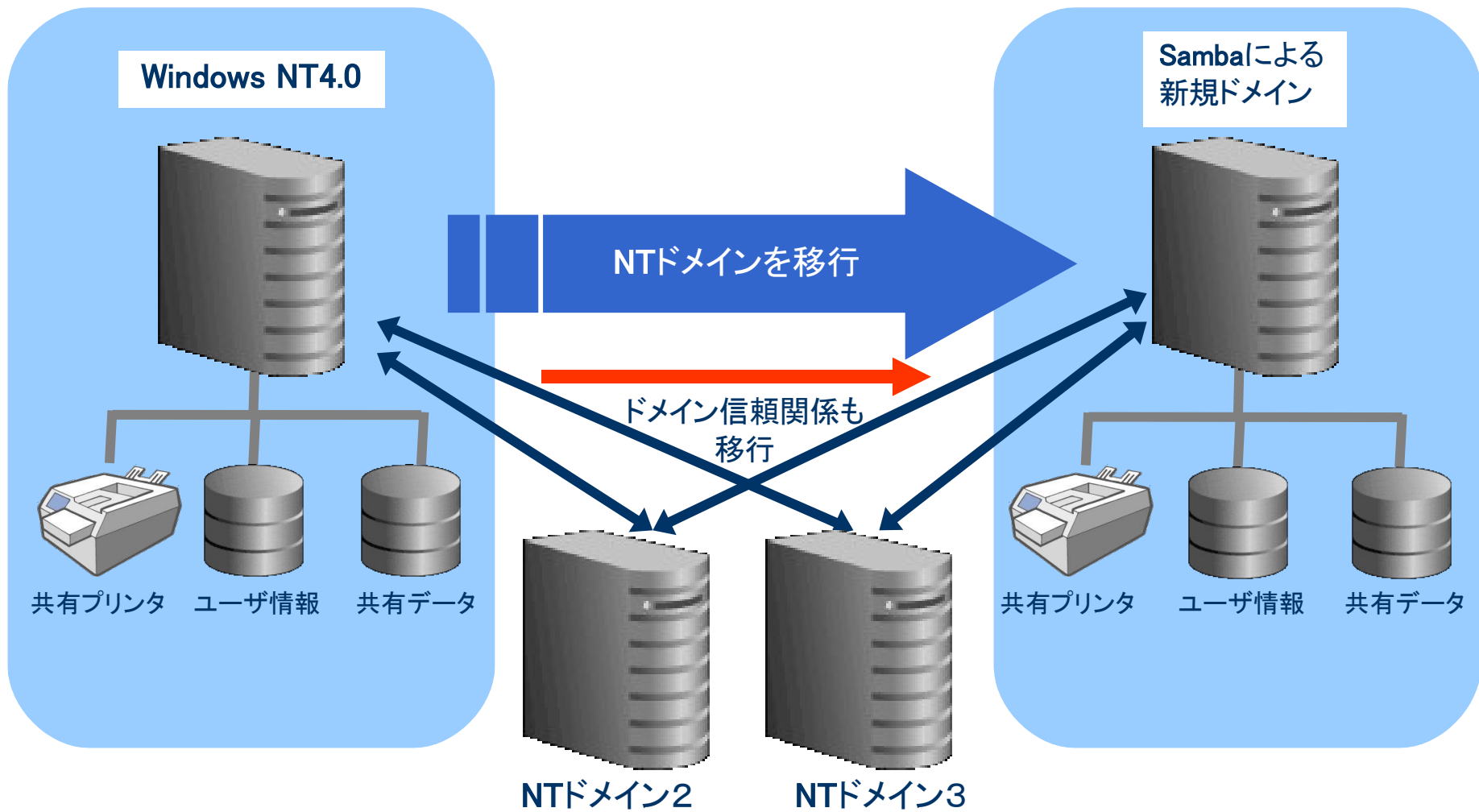
最近は複数システムの統合が増える

- 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。**

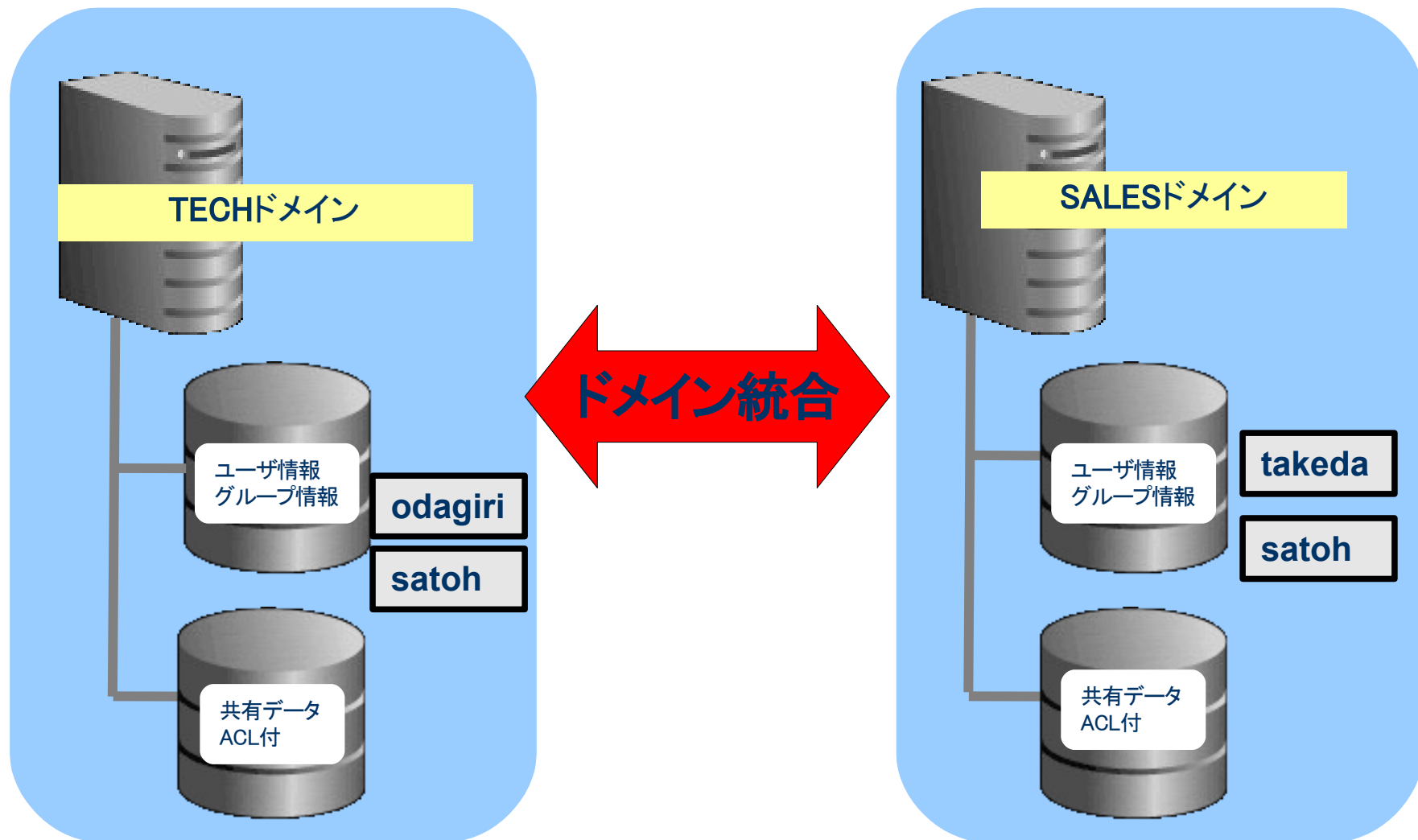
vampireと手作業による移行



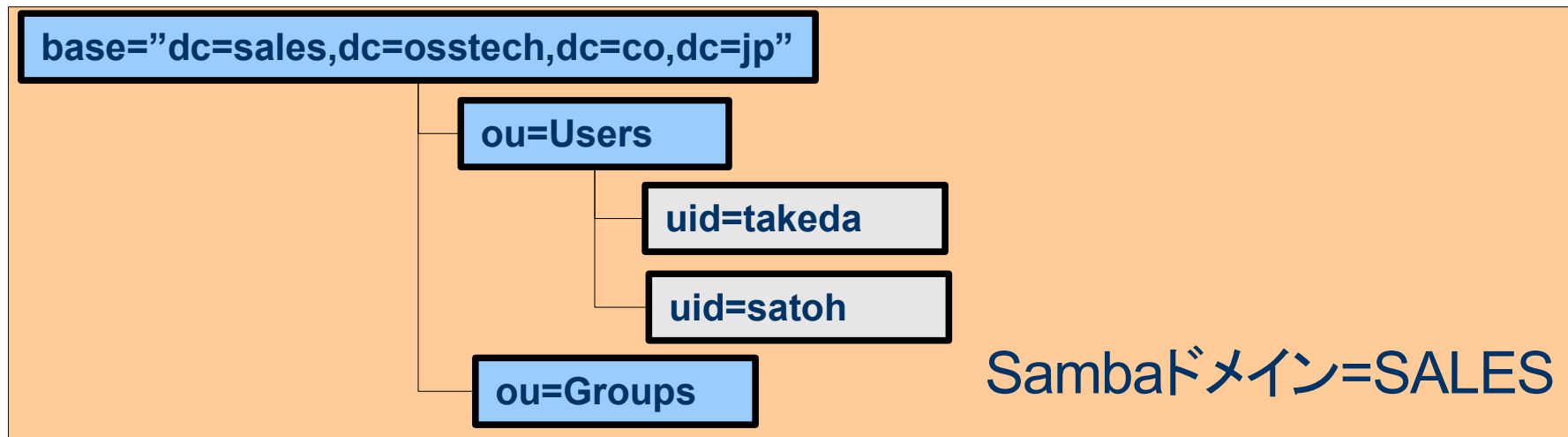
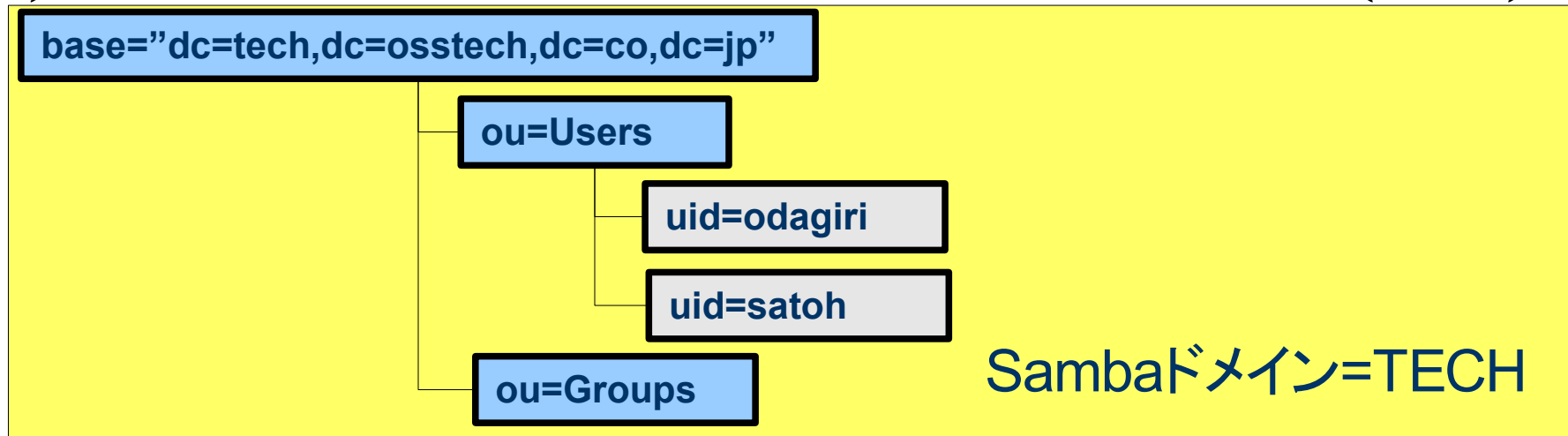
SambaとLDAPを使ったドメイン統合方式

- A) 一つのLDAPに複数のベースサフィックスを持ったDITを作成。既存のNTドメインをひとつのベースサフィックスに対応させる。Sambaドメインは複数になるので信頼関係を結ぶ。→あまり綺麗ではないが簡単な方法
- B) 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ドメインは複数にし、信頼関係を結ぶ。→業務アプリやメールサーバとの連携が可能
- C) 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

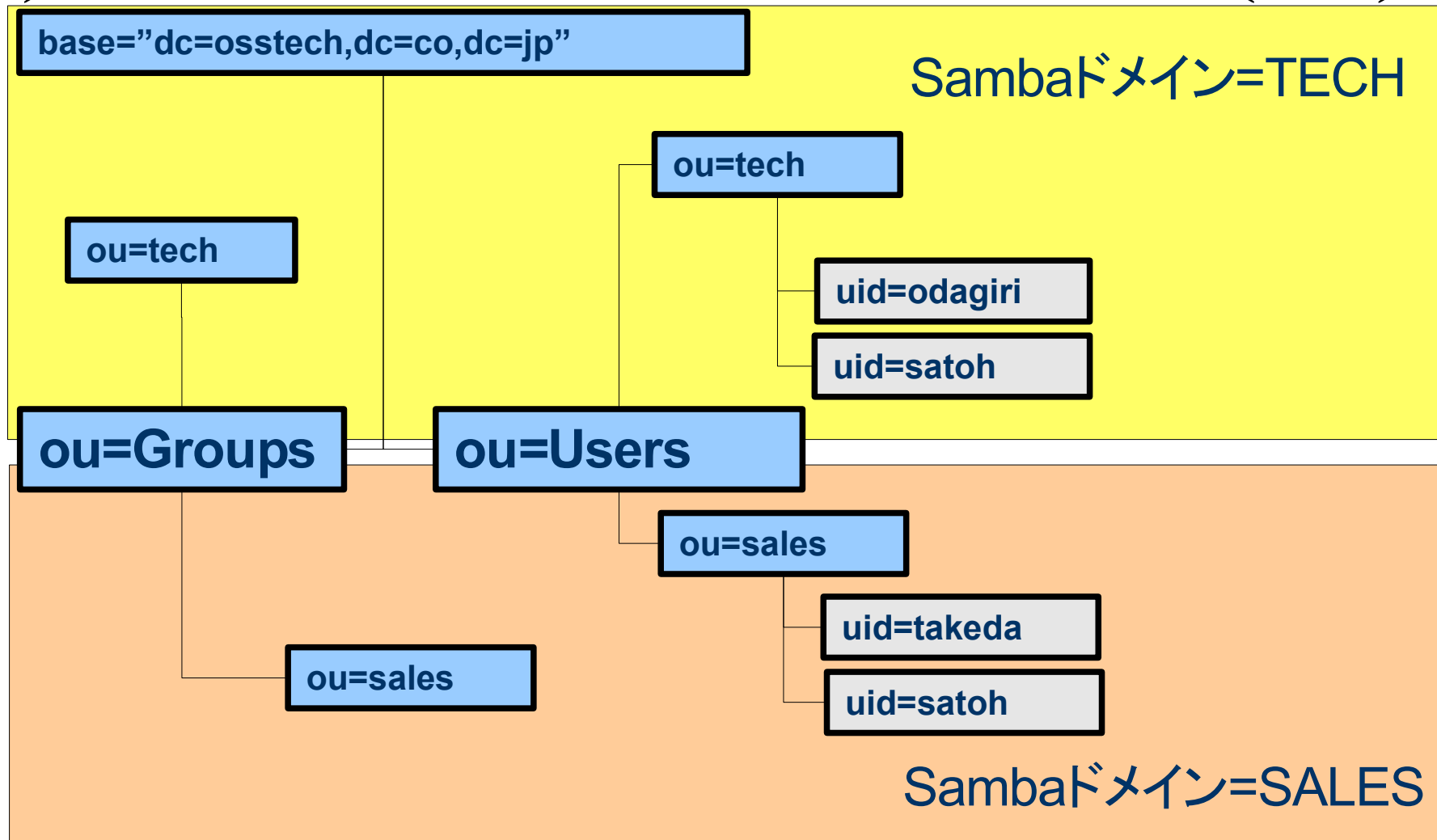
統合前のWindowsドメイン イメージ



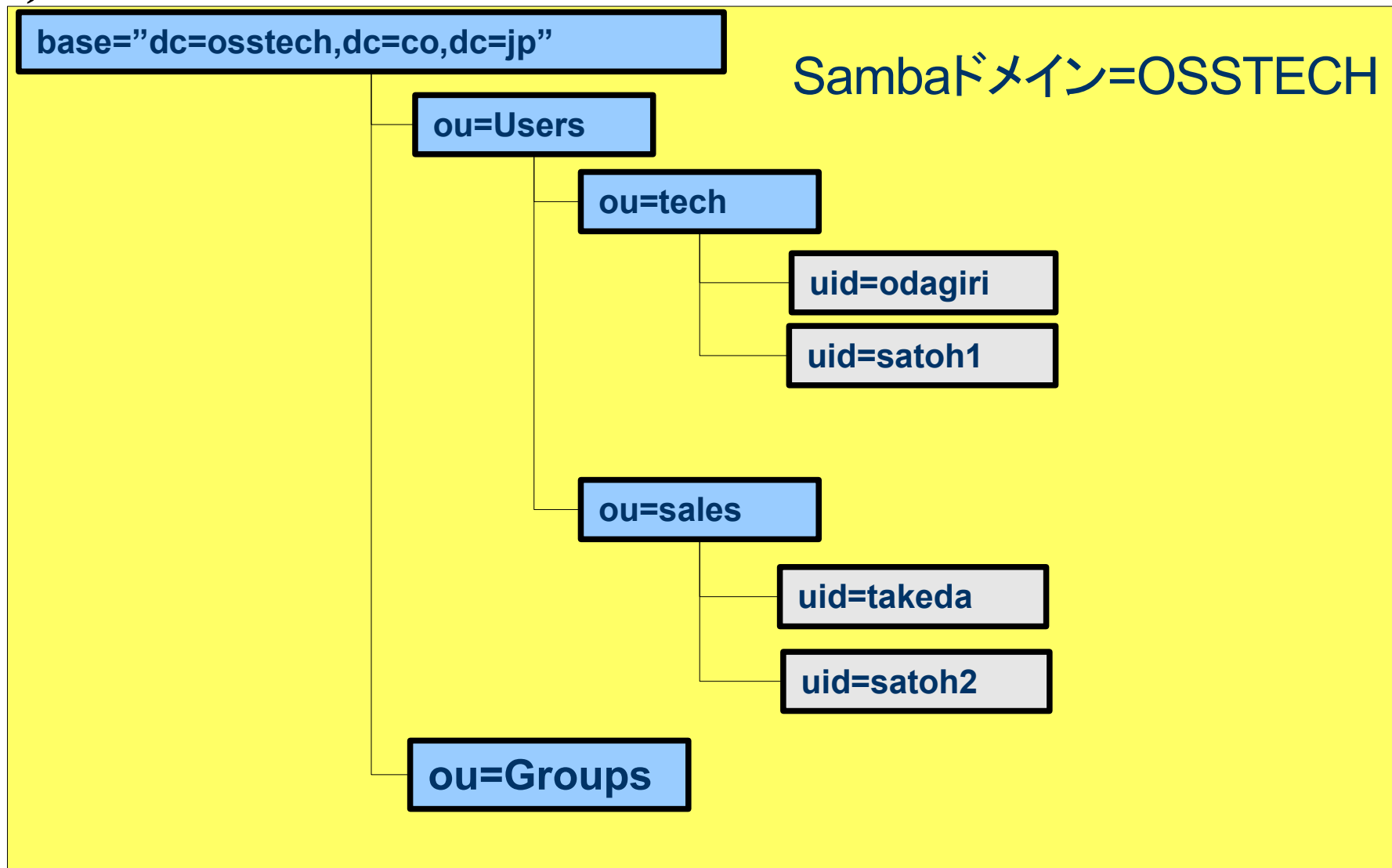
A) 複数ベースサフィックス、複数ドメイン方式(DIT)



B) 単一ベースサフィックス、複数ドメイン方式(DIT)

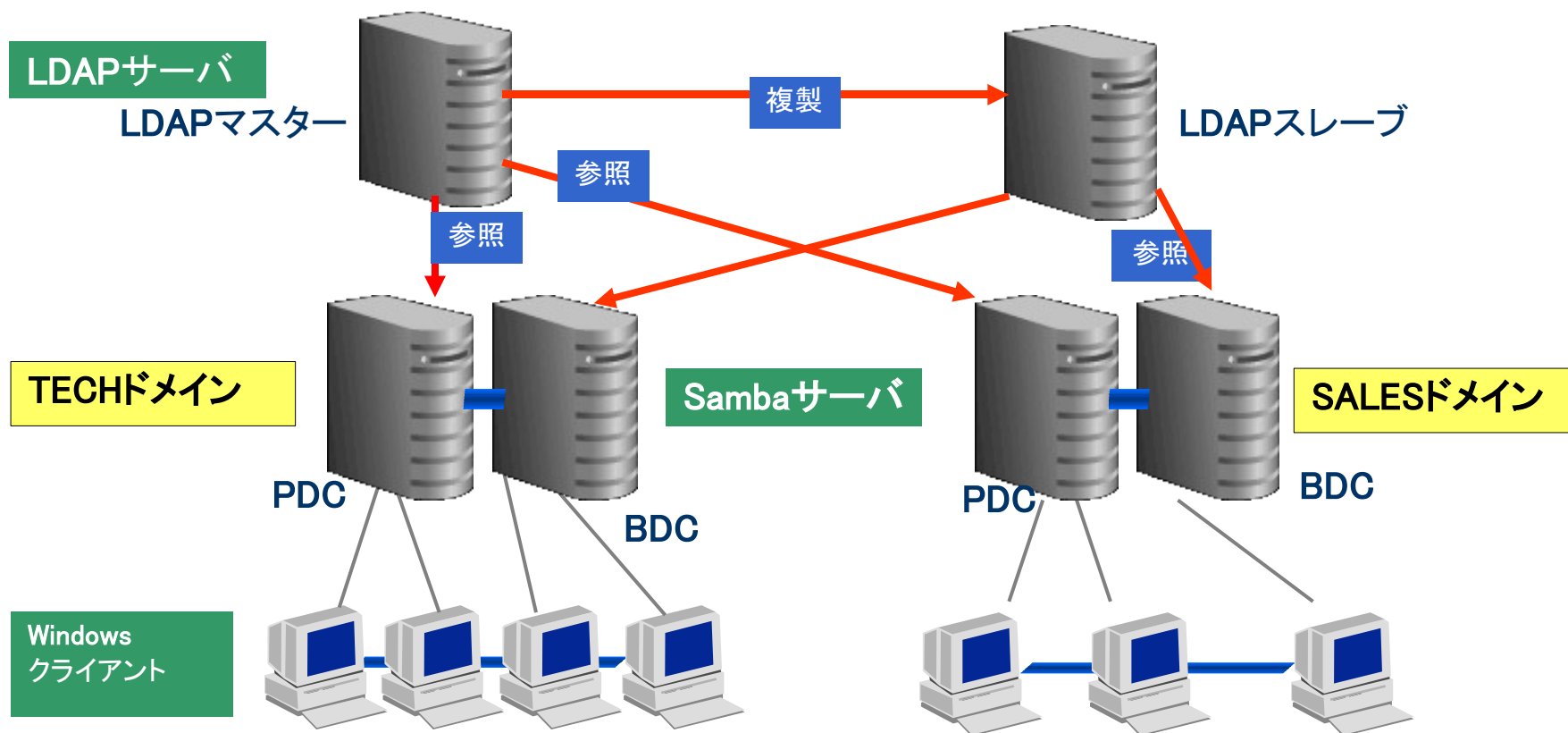


C) 単一ベースサフィックス、単一ドメイン方式



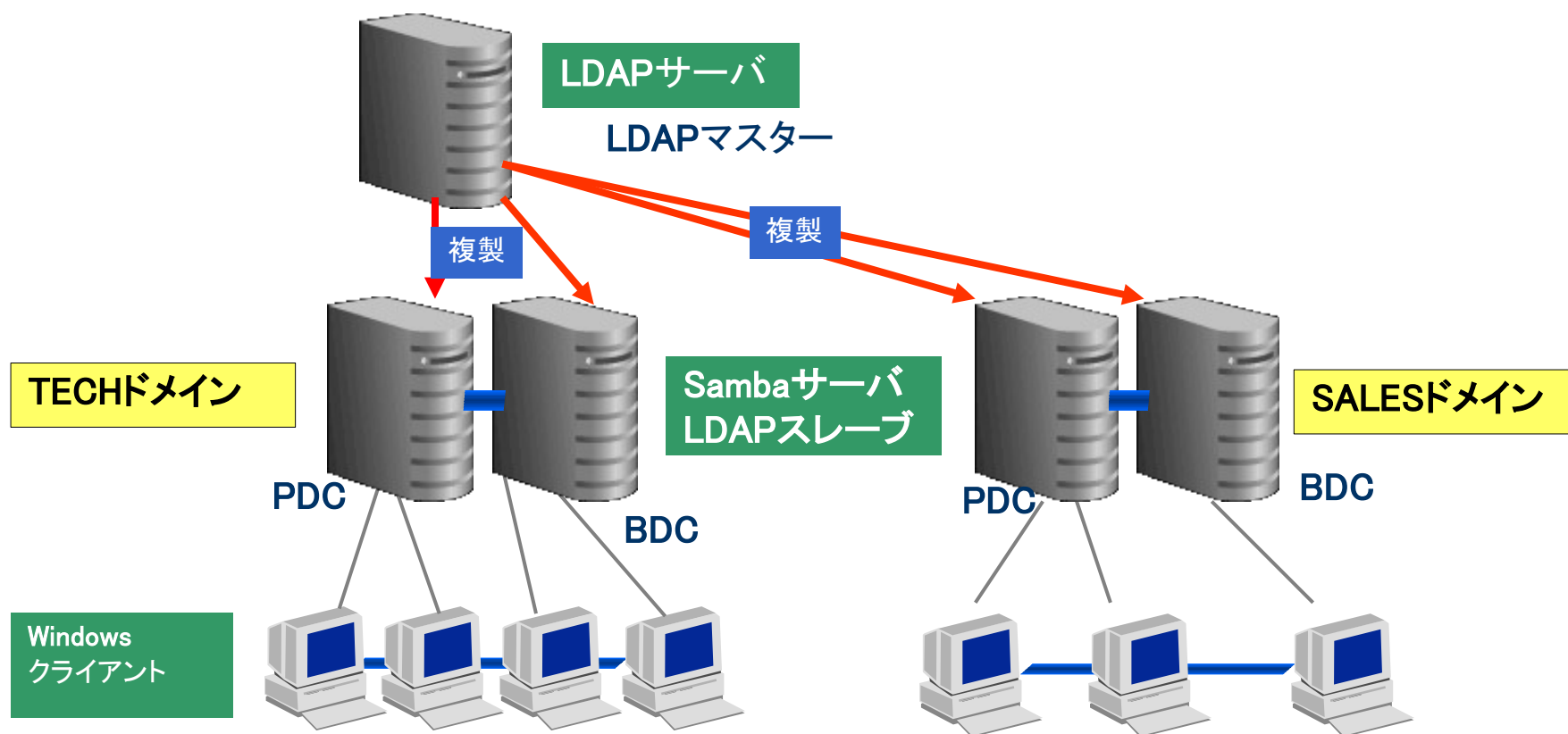
システム構成図(1)

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)



システム構成図(2)

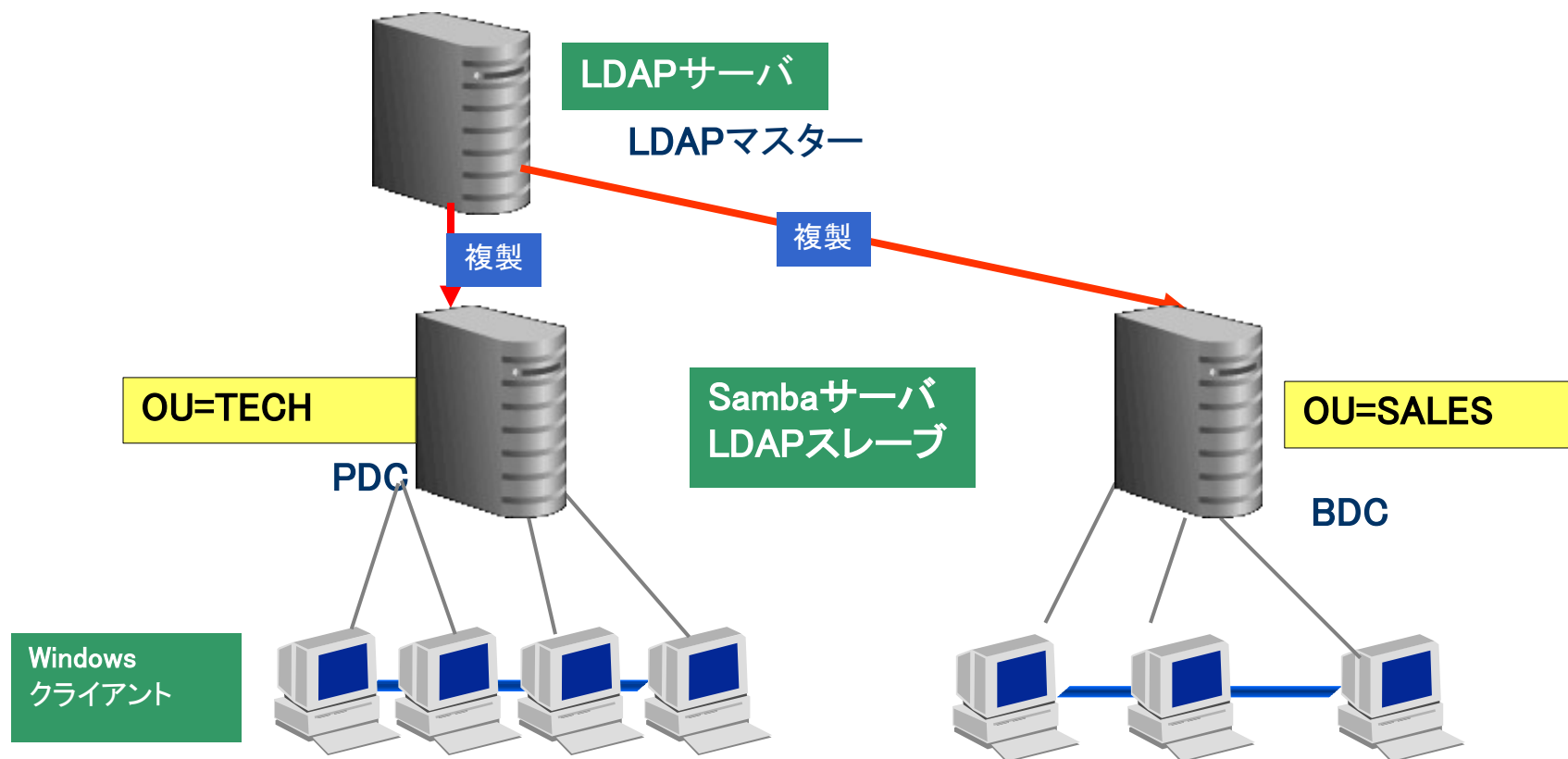
マスターLDAPサーバを1台だけにし、Sambaサーバの上でLDAPスレーブを動かす構成
Sambaサーバは、ドメインの数だけあれば良いが1台でも構わない。
(規模が大きい場合や信頼性が必要な場合はBDCも用意する)



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

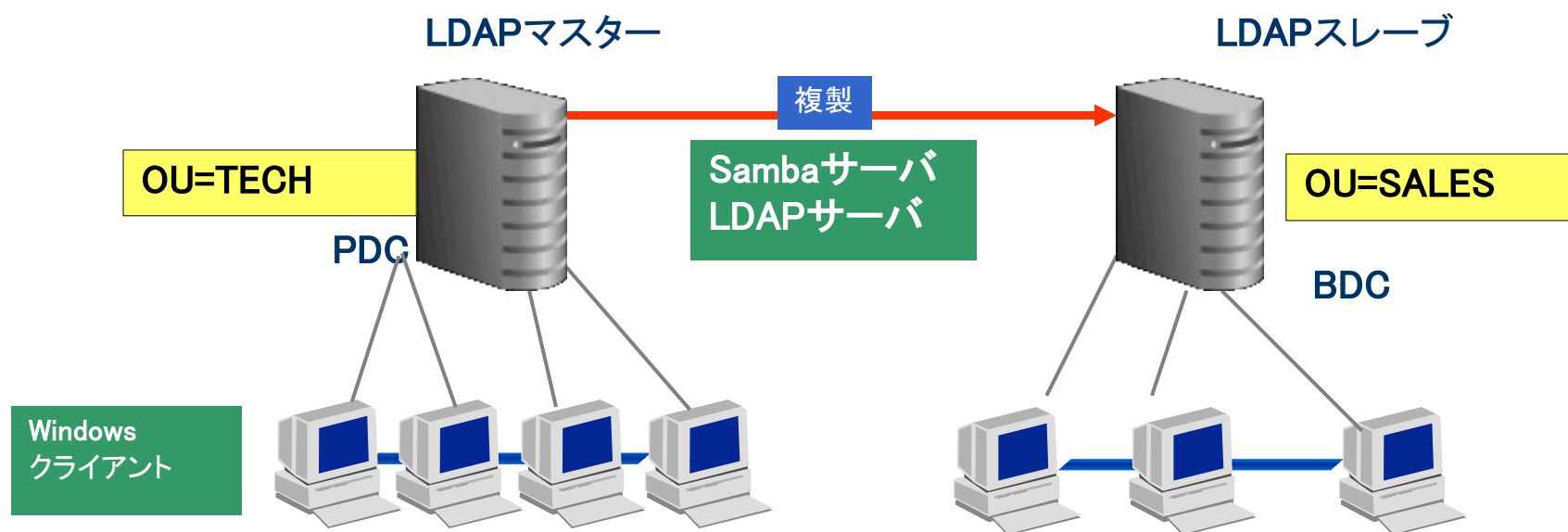
Sambaサーバは、OUの数だけあれば良いが1台でも構わない。

(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)



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)



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。



OSSTech

【お問い合わせ先】

オープンソース・ソリューション・テクノロジー株式会社

info@osstech.co.jp

http://www.osstech.co.jp