Samba でここまでできる!
ー Windowsドメインからの移行ポイント ー

Sambaで構築するドメインの機能を一挙紹介！

日本Sambaユーザ会

たかはし もとのぶ (高橋基信)

おおた としや(太田俊哉)

http://www.samba.gr.jp/

本セッションのねらい

- Sambaでドメインを構築するビジネス的な意義を理解する
  - なぜ今Sambaなのか
- Samba 3.0系列で構築する、Windowsドメインの**機能**について理解する
  - 従来、**設定方法**についての解説は多かったが、各種機能の使用方法や、細かい制限事項の解説が少なかった
    → 移行にあたって、どういったポイントがあり、Sambaでなにができてなにができないかを理解する

概要

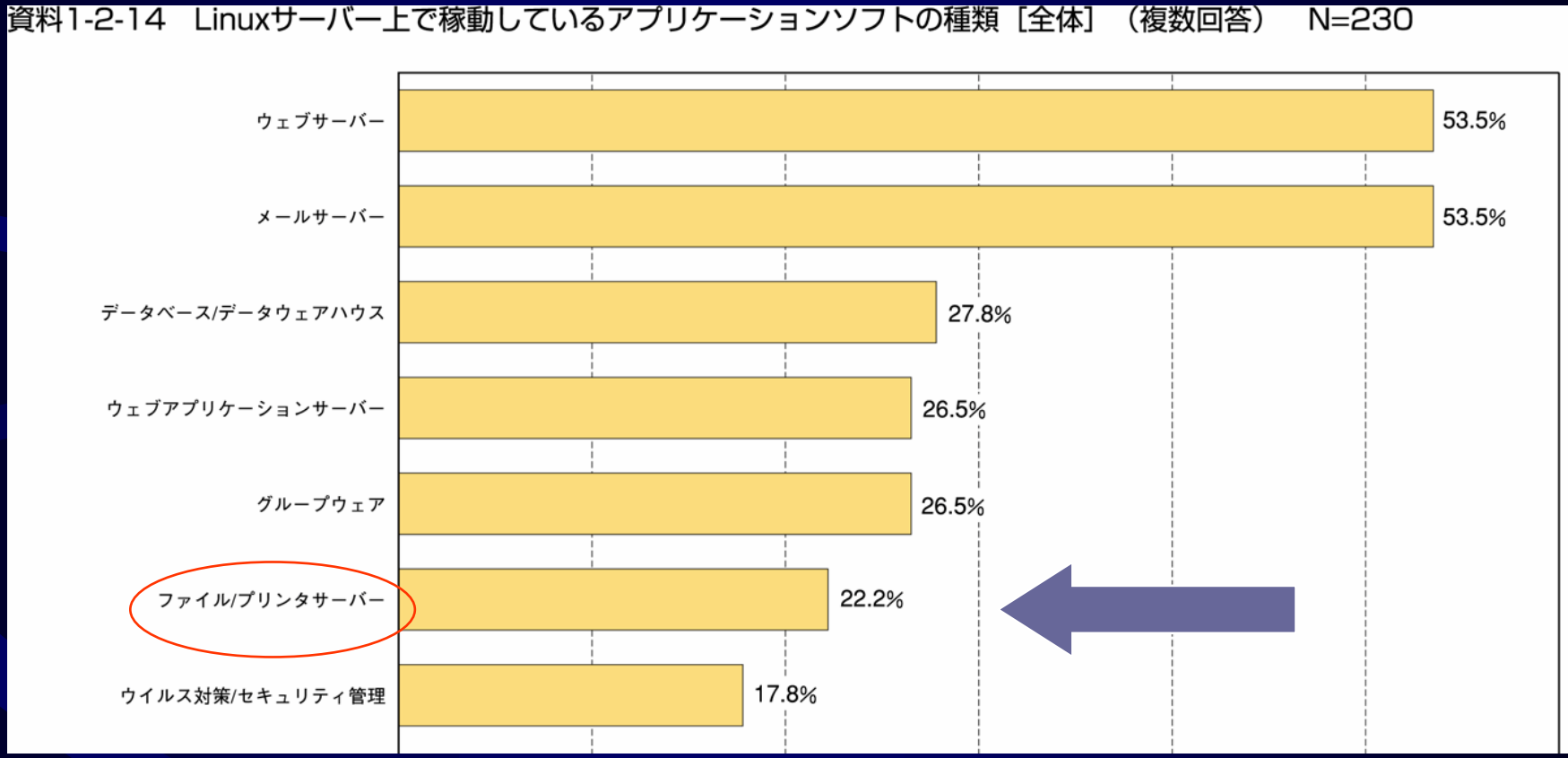
- 本セッションのねらい
- なぜ、いまSambaか?
- Sambaドメイン
  - 各種機能について
    概要 / 詳細 / 制限 / 設定…
- ドメイン移行

Samba利用のキーワード

- セキュリティ
  - **Windows**ターゲットのウィルスには感染しない
  - サーバ上のデータは守りたい
- コスト
  - **CAL**はほとんどの利用場面で必要になった
- 安定性
  - **Linux**自身の安定性、メンテナンスの容易さ
- オプション機能
  - ゴミ箱機能、ユーザホーム機能などなど

Sambaの利用状況(1)

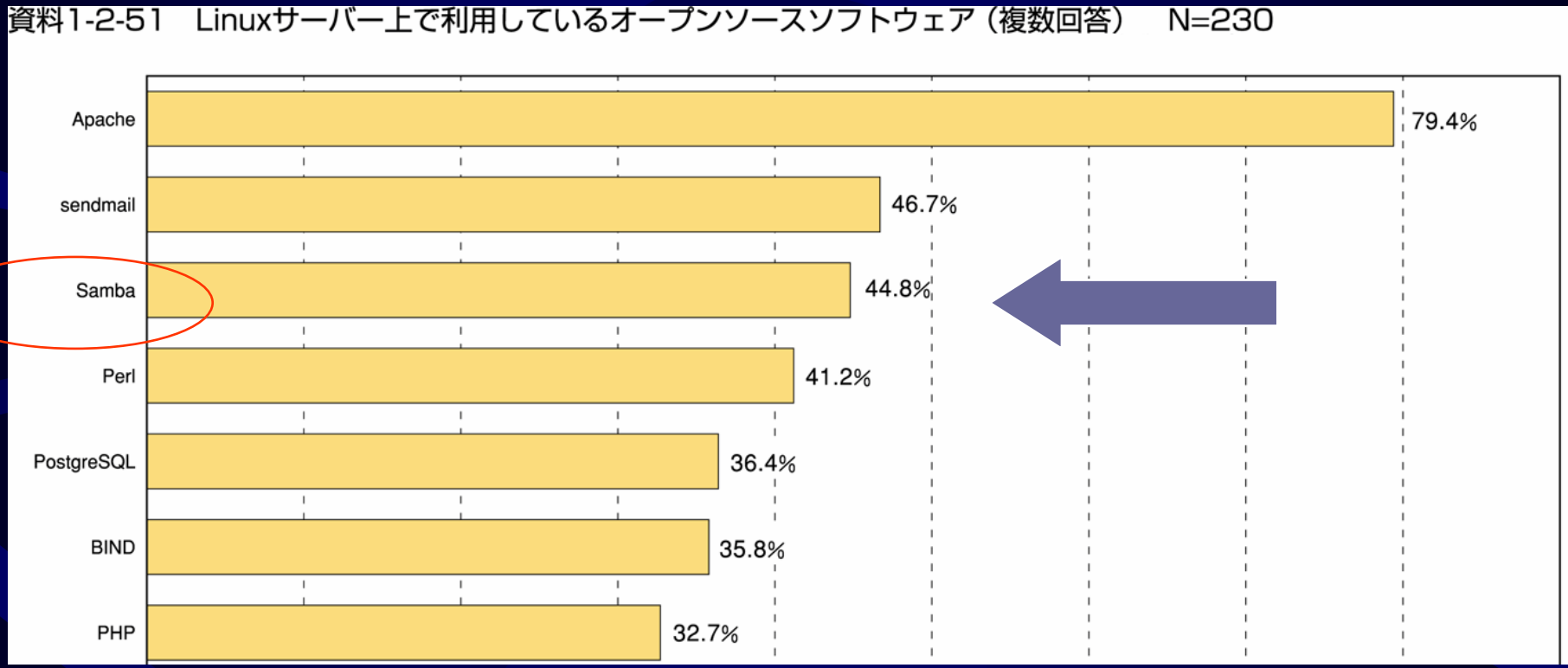
- ファイルサーバとしての利用は20%以上



出典:オープンソース白書 （c）インプレス/矢野経済研究所 2005-2006

Sambaの利用状況(2)

- Sambaの利用率は50%弱



出典:オープンソース白書 （c）インプレス/矢野経済研究所 2005-2006

最近のSambaの利用動向

- 単純ファイルサーバからドメイン機能を利用する方向へ
  - **Samba開発元もその方向で強化をはかっている**
  - 個人的な利用からグループ、組織、全社への利用へ
  - **Windows NTからの移行案件**
  - プリントサーバとしての利用は少ない
- **NASの中身にも**
  - 玄い箱とか白い箱とか(低価格NAS)
  - 大きなものでも使われています(**Ex: NECのNV7000**)

ドメインサーバとしてのSamba

- Samba自身のドメインサーバ機能が向上
- Windowsドメインからの移行機能も向上
  (vampire機能、migrate機能など)
- Windows NTのサポート切れ
  →CAL買い直しは高く付く
  →Sambaってどうよ?

Sambaとサポート

- 業務に使う場合にはサポートが欲しい
- OSSだから自己責任...は企業には通用しない
- サポートは有償...定着してきた
- 各社、OSSへのサポートも開始
  - 大手ベンダーもSambaサポート
    - (日経コンピュータ 2005/08/08)

期は熟した!

Sambaドメイン ― 概要

- **Sambaドメイン**とは
  - **Samba**でドメインコントローラを構築したドメインのことを便宜上「**Samba**ドメイン」と呼称
- 基本的には**Windows NT Server 4.0**以前で構築したドメイン（便宜上**NT**ドメインと呼称）と同等
  - 設定、運用を行ううえでは**NT**ドメインの運用知識が不可欠
    →**NT**ドメインの各種技術情報を適宜参照のこと

Sambaドメイン ー 管理

- 大半はNTドメインの管理ツールで管理可能
  - NTドメインでの運用ノウハウを流用可能
  - ADSIなどによるスクリプト管理も可能
  - 一部機能については、Sambaサーバ上でのコマンドによる管理が必要

ドメイン ユーザー マネージャ

サーバマネージャ

Sambaドメイン ー 管理(続)

- NTドメインの管理ツール
  - 「ドメイン ユーザー マネージャ(`usrmgr.exe`)」
  - 「サーバー マネージャ(`srvmgr.exe`)」
  - 入手方法
    - Windows NT Server /Windows 2000 Serverに同梱
      - Windows 2000 Serverではメニューに登録されていない
    - Windows NT Server 4.0のCD-ROM(1枚目)
      - `Clients¥Srvtools¥Winnt`フォルダ以下
    - 「173673: [NT]NT Workstation 4.0 用の Windows NT サーバツール」
      - 英語版のツールが入手可能(日本語の使用は可能)

Sambaドメイン ― 機能

- 通常必要な機能はほぼサポート
  - **Windows NT**のドメインコントローラとの混在ができない点は注意 → **SAM**の複製ができない
  - 認証データベースとして**LDAP**や**TDB**を用いていない場合は、サポートできる機能が大幅に制限
  - **Samba**のバージョンアップに伴い、細かい機能のサポートが向上
    - できるだけ新しいバージョンの**Samba**を用いた方がよい
    - **Windows**マシンの更新プログラムに**Samba**が対応する間、一部機能に問題が発生することがある

Sambaドメイン ー 機能（続）

- ドメイン機能のサポート状況

種類 / 機能	NTドメイン	Sambaドメイン（3.0系列）	Sambaドメイン(2.2系列)
BDC（SAMの同期）	◎	△	×→△Samba 2.2.3
マシンのドメイン参加	◎	◎	○→◎
グローバルグループ	◎	◎	△
システムポリシー	◎	◎（※）	◎
移動プロファイル	◎	◎（※）	△
アカウントポリシー	◎	○→◎Samba 3.0.3/3.0.6	×
ユーザー権利	◎	△→○Samba 3.0.11/3.0.20	×
信頼関係	◎	◎	×

※認証データベースとして**LDAP**や**TDB**を利用していない場合、Samba 2.2系列と同等のサポート

◎フルサポート / ○ほぼサポート（通常の使用では問題なし） / △部分的にサポート（通常の使用でもかなり制限がある） / ×サポートなし

Sambaドメイン ー 機能（続）

- ユーザ属性のサポート状況

種類 / 機能	NTドメイン	Sambaドメイン（3.0系列)	Sambaドメイン(2.2系列)
フルネーム	◎	◎（※）	△
説明	◎	◎（※）	△
アカウントフラグ	◎	○一部未実装	○一部未実装
プロファイルパス	◎	◎（※）	△
ログオンスクリプト	◎	◎（※）	△
ホームディレクトリ	◎	◎（※）	△
ログオン可能時間	◎	◎	×
ログオン先	◎	◎	×
アカウントの期限	◎	◎	×
ローカルアカウント	◎	×	×
ダイヤルイン情報	◎	×実装中	×

ポイント ー 認証データベース（1）

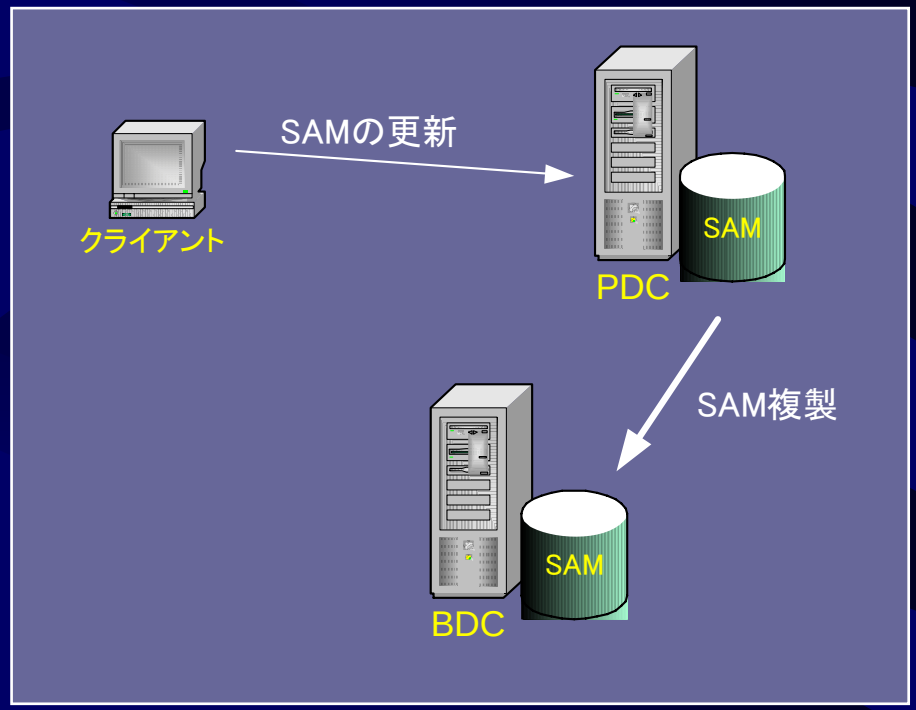
- 認証データベースとは
  - ドメインの認証情報の格納先
  - **NT**ドメインでは、認証情報を**SAM**に格納（管理者が意識する必要なし）
  - **Samba**ドメインでは、認証情報の格納先を選択できる（管理者が意識して設定する必要あり）

ポイント ― 認証データベース(2)

- 注意点
  - **Samba 3.0系列で拡張されたユーザ情報を格納できる認証データベースを用いる**
    →TDBファイルやSamba 3.0系列のLDAPなど
    - **smbpasswdファイルやSamba 2.2系列互換のLDAPスキーマでは、拡張されたユーザ情報を格納できない**
  - **`passdb backend`パラメータの設定が必要**
    - デフォルト設定は**smbpasswd**ファイルなので注意
  - 必要な場合、認証データベースを移行する
    - **`pdbedit -i-e`コマンド**

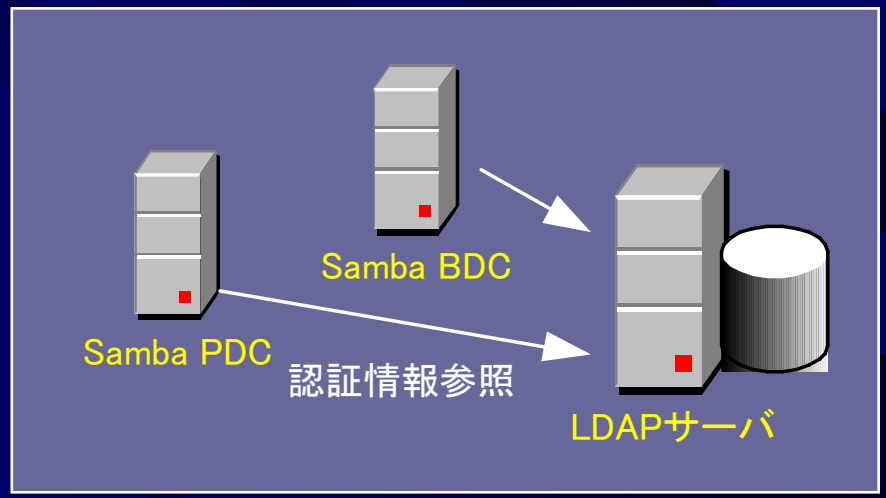
ポイント － BDC（1）

- **BDC（バックアップドメインコントローラ）とは**
  - **PDC（プライマリドメインコントローラ）からドメインの認証情報などを格納したSAMの複製を受けて機能するドメインコントローラ**
  - **SAMの更新ができない他は、基本的にPDCと同じ**



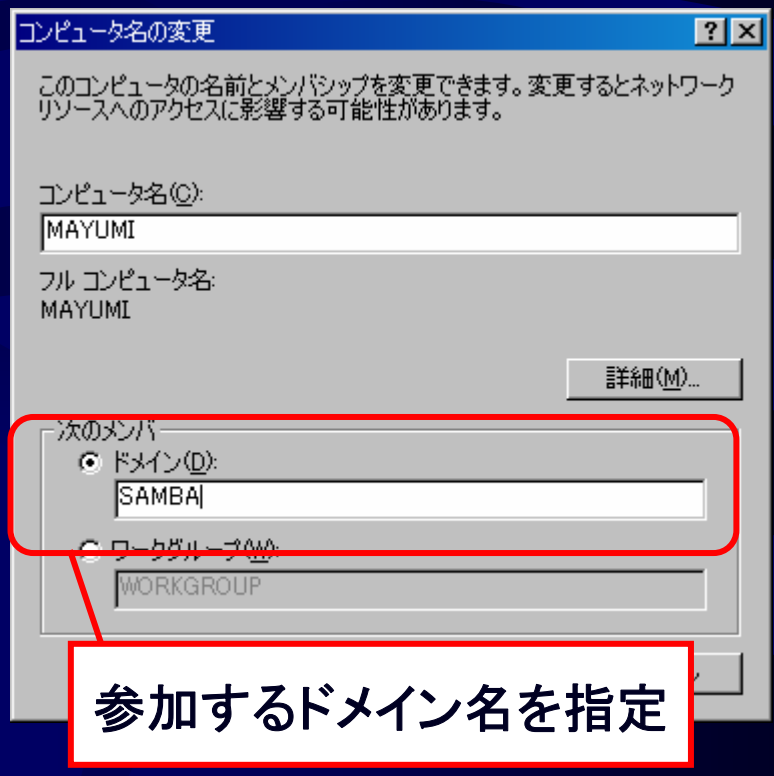
ポイント － BDC（2）

- 制限事項
  - PDC⇔BDC間のSAM同期プロトコルが未サポート
    - Windows NT ServerのPDCとSambaのBDC、その逆といったドメインコントローラの混在構成は不可
    - BDCを構築する場合は、PDC、BDCともSambaで構成した上で、LDAP認証データベースを用いて認証情報の一元管理を行うのが一般的



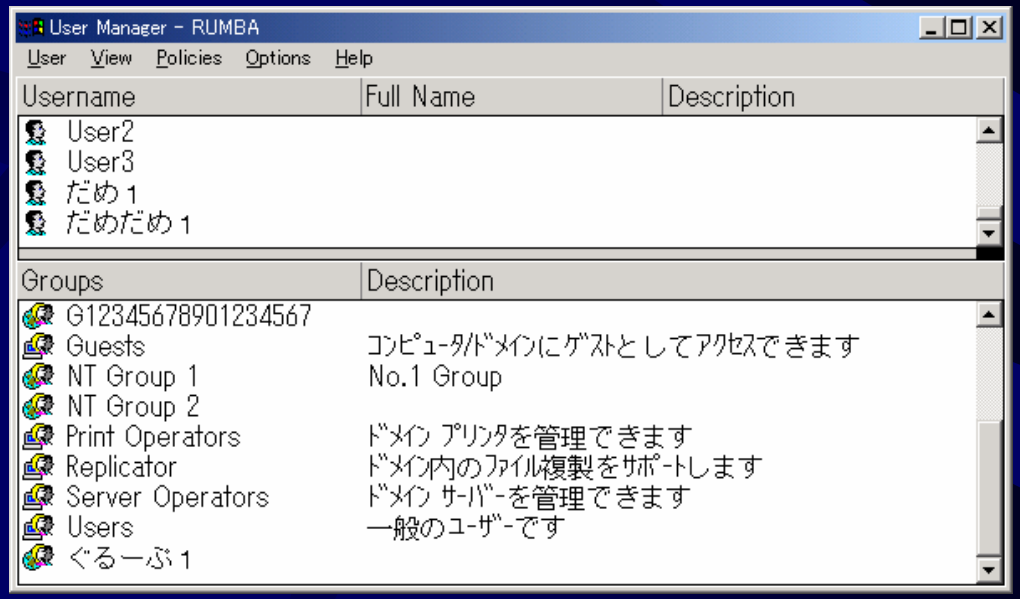
ポイント ー マシンのドメイン参加

- マシンのドメイン参加とは
  - **Windows NT/2000/XP**などのマシンをドメインに参加させるために必要な操作
- 制限事項
  - 原則として**root**ユーザでの作業が必要
    - ユーザー権利（Samba 3.0.11以降）を用いることで、**root**以外のユーザによるドメインの参加作業が可能
      →NTドメインと同等に



ポイント － 日本語のユーザ名など

- ユーザー名、グローバルグループ名への日本語の使用
  - NTドメインでは問題なく可能
  - Sambaドメインでも一応可能
    - 確認した限り動作
- 注意点
  - 一般的にUNIXマシンでは非サポート
    - 使用を避けるのが無難



ポイント ー システムポリシー（1）

- システムポリシーとは
  - ドメイン内のユーザ、グループ、マシン単位で、一括して各種設定を行うNTドメインの機能
  - システムポリシーエディタで作成したポリシーファイルをNETLOGON共有に配置することで有効になる
    - ファイル名は
      NTconfig.pol
      Config.pol

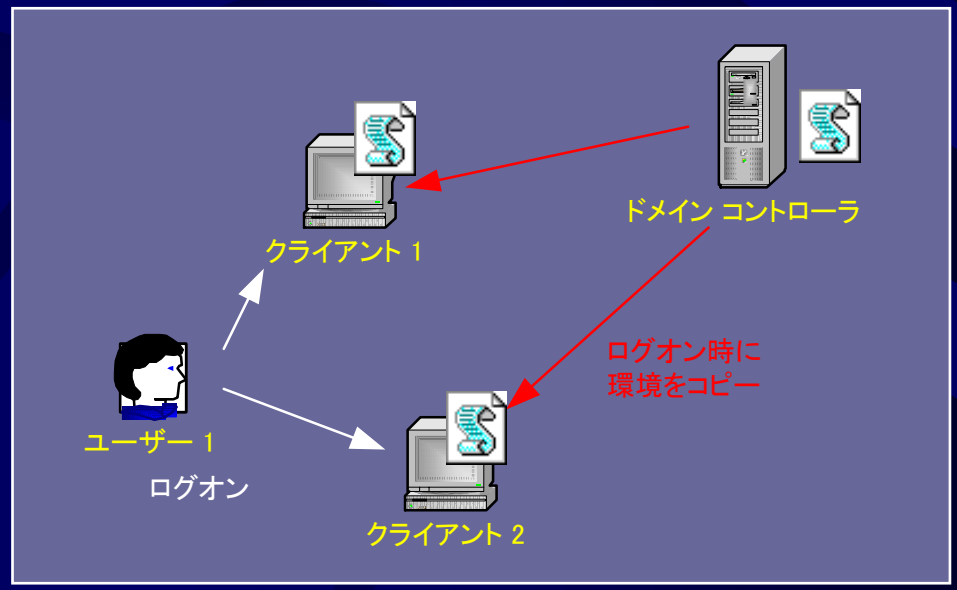
システムポリシーエディタ

ポイント ー システムポリシー（2）

- 注意点
  - ポリシーファイル（NTConfig.polなど)はそのまま移行可能
    - Sambaドメインの全ドメインコントローラのNETLOGON共有にコピーすればよい
  - すべてのドメインコントローラ上にNETLOGON共有を明示的に用意しておくこと
    - 一般ユーザからは読み取り専用にしておくこと

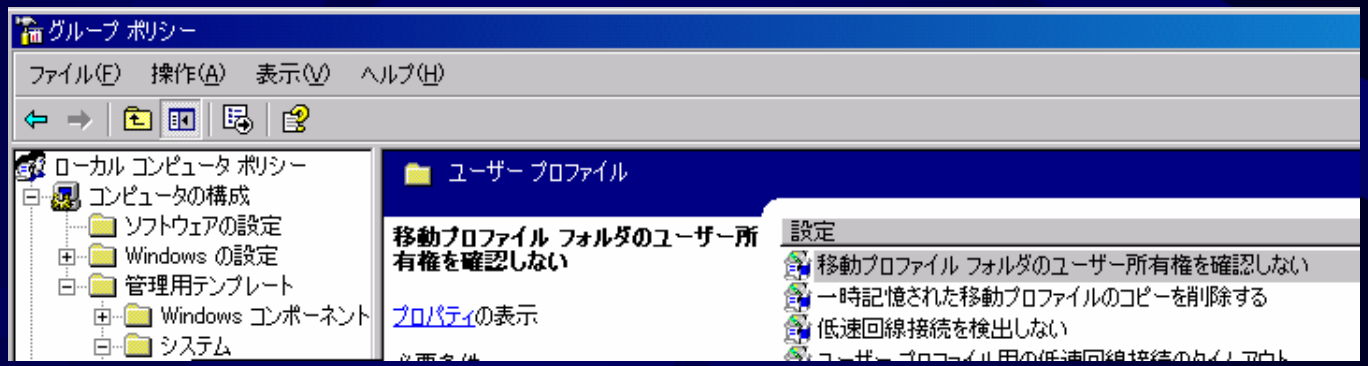
ポイント ー 移動プロファイル（1）

- 移動プロファイルとは
  - 各ユーザのデスクトップ設定をネットワーク上の共有に保存し、ドメイン内のどのマシンでログオンしても同じデスクトップ環境を実現する機能



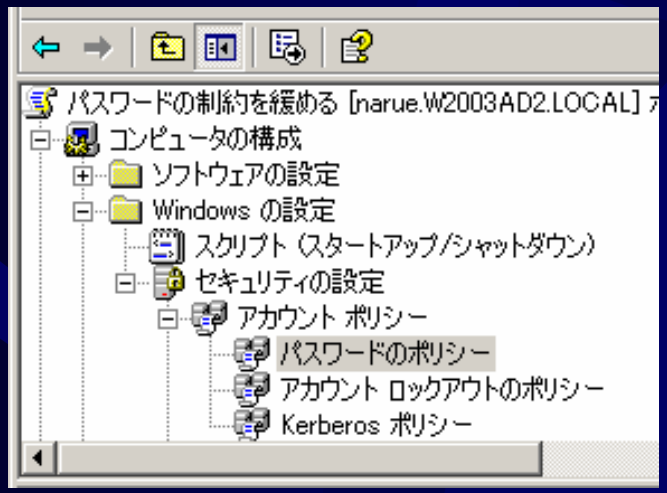
ポイント ー 移動プロファイル（2）

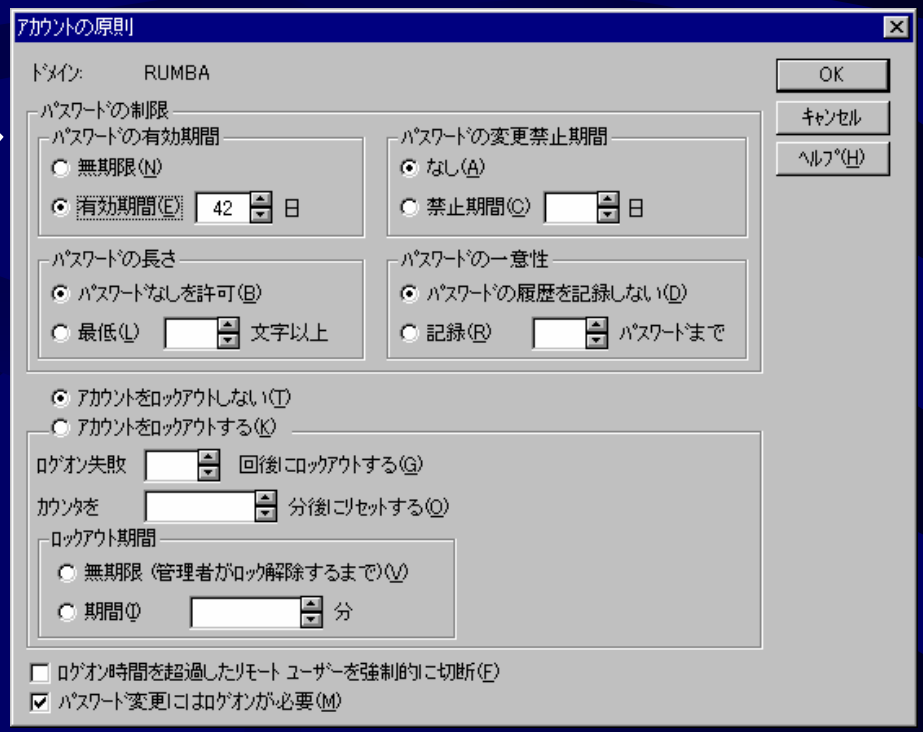
- 注意点
  - 移動プロファイルの設定をユーザ毎に保存したい場合は、認証データベースにLDAPやTDBを用いる
  - 移動プロファイルをSambaサーバに保存する場合
    - 「`profile acls = yes`」の設定を行う、もしくは
    - GPOの「移動プロファイル フォルダのユーザー所有権を確認しない」を有効にする



ポイント　－　アカウントポリシー（1）

- アカウントポリシーとは
  - ドメイン内のユーザのパスワードに関する各種セキュリティ機能
  - **Active Directory** では、**GPO**における以下の各設定に相当





アカウントポリシーの設定画面
（ドメイン ユーザー マネージャ）

ポイント　ー　アカウントポリシー（2）

- 注意点
  - Samba 3.0.0では、未サポートの属性あり
    - パスワードの履歴（Samba 3.0.6以降）
    - ロックアウト(Samba 3.0.3以降)
  - 現在のSamba 3.0系列では、完全サポート

ポイント － ユーザ属性（1）

- ユーザー属性とは
  - 「ドメイン ユーザー マネージャ」から設定可能なユーザーのさまざまな属性

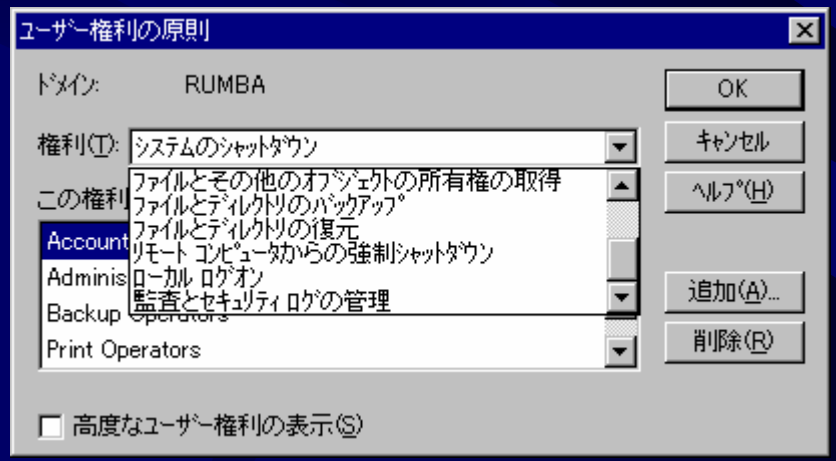
ポイント ー ユーザ属性（2）

- 注意点
  - 認証データベースにsmbpasswdファイルなどを用いている場合は、Samba 2.2系列レベルのサポートとなるので注意
    - Samba 2.2レベルのサポートの場合、大半の属性は、設定できないか、パラメータにより、ドメイン単位での一括指定しかできない
- 制限事項
  - 以下の属性はサポートされていない
    →ただし通常の運用では問題なし

属性	説明
ローカルアカウント	ネットワークログオンのみ可能なアカウント
ダイヤルイン情報	RAS接続の可否などの設定

ポイント　－　ユーザー権利（1）

- ユーザー権利とは
  - 特定のユーザーに特殊な権利を付与する機能
    - 一部の管理作業を一般ユーザーに委任することが可能
- Samba 3.0.11以降でサポート開始
  - ただし、現時点でサポートされているユーザ権利は一部



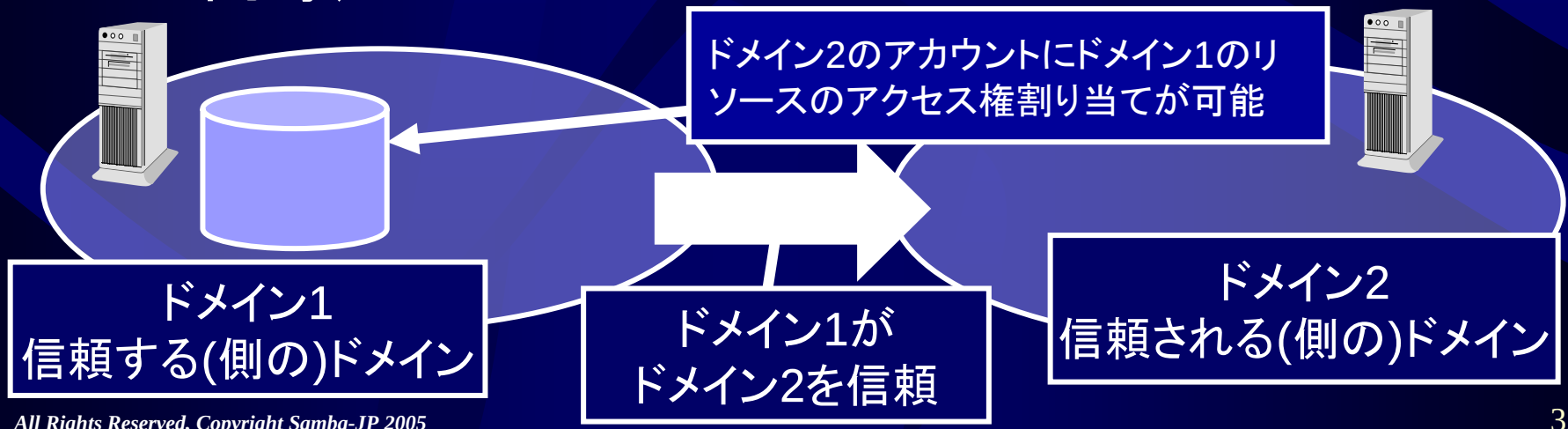
ポイント － ユーザー権利（2）

- 制限事項
  - 「ドメイン ユーザー マネージャ」からは設定不可
    - 設定の参照は可能
    - 設定はnet rpc rightsコマンドで行う必要がある
  - 利用可能なユーザ権利は一部のみ

```
# net rpc rights list -U root
Password:
     SeMachineAccountPrivilege  Add machines to domain
      SeTakeOwnershipPrivilege  Take ownership of files or other objects
             SeBackupPrivilege  Back up files and directories
            SeRestorePrivilege  Restore files and directories
     SeRemoteShutdownPrivilege  Force shutdown from a remote system
      SePrintOperatorPrivilege  Manage printers
           SeAddUsersPrivilege  Add users and groups to the domain
       SeDiskOperatorPrivilege  Manage disk shares
```

ポイント ー 信頼関係

- 信頼関係とは
  - 別ドメインのユーザ、グループに対してリソースへのアクセス許可を割り当てる機能
- 制限事項
  - 明示的な一方向の信頼関係のみサポート（NTドメインと同等）



ポイント　－　ドメイン移行（1）

- ドメイン移行とは
  - 既存のNTドメインの各種設定をSambaドメインに引きつぐ作業
  - Samba 3.0では、既存のNTドメインからの移行機能が充実
    - `net rpc vampire`コマンド
  - Samba 2.2系列からの移行もサポート
    - `pdbedit`コマンドによる認証データベース移行

ポイント － ドメイン移行（2）

- 制限事項
  - 一部移行できない設定がある

機能	Sambaドメイン（3.0系列）	移行方法
ユーザ（含コンピュータアカウント）	◎	net rpc vampire
グローバルグループ	◎	net rpc vampire
システムポリシー	◎	net rpc vampire＋ファイルコピー
移動プロファイル	◎	net rpc vampire＋ファイルコピー
アカウントポリシー	○→◎	net rpc vampire
ユーザー権利	△→○Samba 3.0.11以降	再設定（移行できない権利あり）
信頼関係	◎	net rpc vampire
ユーザー属性すべて		net rpc vampire＋ファイルコピー

ポイント　－　ドメイン移行（3）

- 日本語のユーザ名、グループ名、コンピュータ名
  - 少なくともLDAP環境では移行できない
    →LDAP側の仕様制限
    - TDBファイルの場合確認した限りでは動作するが、推奨できない

- 注意点
  - ファイルコピーが必要な機能がある
    - 設定自体は`net rpc vampire`コマンドで移行されるが、実ファイルは別途コピーする必要がある
      - システムポリシーのポリシーファイル
      - 移動プロファイルを構成する各ファイル
      - ログオンスクリプトのファイル

ポイント ーファイル共有移行(1)

- ファイル共有の移行
  - 基本的にはWindows側のファイルコピーで移行可能
  - Sambaの`net share migrate`コマンドで移行することも可能

機能	移行方法
ファイル共有のアクセス許可	移行できず
ファイル	ファイルコピー / net share migrate
ファイルのACL	ファイルコピー / net share migrate
ファイルのファイル属性	ファイルコピー / net share migrate

ポイント ーファイル共有移行(2)

- 制限事項
  - ACLの非互換性
    - WindowsのACLとUNIXのACLでは実装が異なるため、全く同じ設定はできない
      →NTFSで細かいACL設定を行っている場合は、移行前に確認が必須
  - ファイル属性の非互換性
    - Sambaではファイル属性の情報を格納するために、実行ビットを利用する
      → 実行ビットをUNIX側で使う場合、ファイル属性の保持ができない