Samba 2.2系列から Samba 3.0系列への 移行のポイント

Sambaドメインのアップグレード！

日本Sambaユーザ会 / NTTデータ

たかはし もとのぶ (高橋基信)

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

本セッションのねらい

- Samba 2.2系列からSamba 3.0系列へのアップグレードのポイントを理解する
- いまさら何故Samba 2.2か？
  - 現状もSamba 2.2を使っているサイトは多いようである → いつかはアップグレードしないといけない
  - しかし、市場にはSamba 2.2系列の情報がほとんどなくなってきている
  - Sambaドメインのアップグレードについては、意外と情報がない

All Rights Reserved, Copyright TAKAHASHI Motonobu 2006

Samba 2.2からの移行

- パラメータに関しては、基本的に上位互換
  - 基本的なパラメータは変更なし→移行不要
    - SSL機能など実質的に使用されていない機能で廃止されたものもある
- 移行のポイント
  - １．国際化関連機能
    - 大幅に変更、ファイル名の移行要→要移行
  - ２．ドメイン機能サポート
    - 大幅に拡張、LDAPデータ形式の変更要→移行を要検討
  - ３．新機能、拡張された機能
    - 多くの機能拡充が行われている→任意に導入を検討

All Rights Reserved, Copyright TAKAHASHI Motonobu 2006

1. 国際化関連機能

- 日本語(国際化)の処理が大幅に変更
  - Samba 2.2系列までは、Samba内部に文字コード変換ロジックを同梱
  - Samba 3.0系列では、外部の`iconv()`関数を用いたロジックに全面変更
    →文字コード変換は`iconv()`関数次第
  - ネットワーク上の文字コードがMS-DOS互換(日本語環境ではシフトJIS)からUnicode(UCS-2)に変更
    - Samba内部の文字コードも変更
  - 関連するパラメータが全面的に変更

All Rights Reserved, Copyright TAKAHASHI Motonobu 2006

Samba 2.2までの日本語処理の実装

- Samba 2.2系列までは基本的に同一
  - 文字コード変換ロジックは、Samba内部で実装
  - 日本語処理に必要なパラメータ

```
[global]
  client code page = 932
  coding system    = SJIS/EUC/CAP/HEX/UTF8/UTF8-MACなど
```

  - Samba 日本語版では、「シフトJIS正規化」や機種依存文字対応などを行っている
  - ネットワーク上の文字コードはMS-DOS互換

All Rights Reserved, Copyright TAKAHASHI Motonobu 2006

Samba 3.0系列の日本語処理の実装

- Samba 2.2までとは大きく異なる
  - 文字コード変換ロジックは、**iconv()**に依存
    - ただし、**UCS-2**など一部は内部で実装
    - **iconv()**は標準的な文字コード変換関数
    - Samba独自に拡張することもできる(CP850など)
  - 日本語処理に必要なパラメータ

```
[global]
  dos charset      = CP932
  unix charset     = CP932/EUCJP-MSなど（デフォルトUTF-8)
```

  - ネットワーク上の文字コードはUnicode

All Rights Reserved, Copyright TAKAHASHI Motonobu 2006

日本語パラメータの比較

- Samba 3.0系列では外部の**iconv()**関数が必須（**GNU libiconv/glibc**のもの以外は動作未確認）

従来の **coding system**	Samba 3.0の **unix charset**	Samba 3.0での現状
SJIS	CP932	glibc-2.3.2以前/**GNU libivonv**については、パッチ適用が必要。glibc-2.3.3以降では対応
EUC(EUC3)	EUCJP-MS	同上
JIS	なし	実装上サポートできない
CAP	CP932 + vfs_cap	CP932に順ずる。CAP自体はVFSで対応
HEX	CP932 + vfs_hex	同上。HEX自体はVFSで対応（ミラクル・リナックス社提供）
UTF8	UTF-8	問題なし
UTF8-Mac	MACOSXFS	charset_maxosxfsモジュールにより対応

libiconv/glibcへのパッチ:

http://www2d.biglobe.ne.jp/~msyk/software/libiconv-patch.html

All Rights Reserved, Copyright TAKAHASHI Motonobu 2006

日本語対応パッチの適用状況

- 主要Linuxディストリビューションでは、対応済
  - 大半がglibc-2.3.3以降に移行、glibcにパッチを適用済 → 実質的に問題なし
- FreeBSDでは、Portsレベルで対応
  - WITH_EXTRA_PATCHESをYesにしてGNU libiconv (converter/libiconv)をコンパイル
- （汎用の）商用UNIX
  - 独自にGNU libiconvにパッチを適用してインストールする必要がある

All Rights Reserved, Copyright TAKAHASHI Motonobu 2006

日本語ファイル名の移行

- 細かい実装の違いにより、**UTF-8**以外ではファイル名の移行が必要
  - SJIS → CP932のように同じ文字コード間の移行であっても、変換が必要な文字がある

Ⅰ Ⅱ Ⅲ Ⅳ Ⅴ Ⅵ Ⅶ Ⅷ Ⅸ Ⅹ №.℡㈱ の13文字

- 技術的な詳細は、以下を参照
  - **http://www.miraclelinux.com/technet/samba30/migration.html**
- 移行ツール　ー　**smbfnconv**コマンド

All Rights Reserved, Copyright TAKAHASHI Motonobu 2006

smbfnconvコマンド（1）

- ファイル名の移行を行うスクリプト
  - 各ファイルに対して、移行後のファイル名を持つハードリンクを作成する
  - 万一移行に失敗しても、元のファイルに被害が発生しないので、やり直しができる
- インストール
  - 日本Sambaユーザ会で配布されているアーカイブにミラクル・リナックス社のパッチを適用して使用する
    - `http://www.miraclelinux.com/technet/samba30/migration.html`

All Rights Reserved, Copyright TAKAHASHI Motonobu 2006

smbfnconvコマンド（2）

- smbfnconvコマンドの書式

```
$ smbfnconv -f <Samba 2.2系列文字コード> -t <Samba
3.0系列文字コード> -p <変換先ディレクトリ> <変換元ディレクトリ>
```

- 使用例（SJISからCP932への変換）

```
$ mv 共有ディレクトリ 共有ディレクトリ.old
$ mkdir 共有ディレクトリ
$ cd 共有ディレクトリ.old
$ smbfnconv -f sjis -t cp932 -p ../共有ディレクトリ .
```

All Rights Reserved, Copyright TAKAHASHI Motonobu 2006

2. ドメイン機能サポート

- Samba 2.2系列
  - 基本的な認証機能を提供
  - ユーザ単位の細かい設定変更ができない
- Samba 3.0系列
  - 通常必要な機能をほぼサポート
    - アカウントポリシー、ユーザー権利など
  - ただし、ユーザ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制限
    - アカウントポリシーはサポートできず、他Samba 2.2系列レベルのサポートとなる機能がある

All Rights Reserved, Copyright TAKAHASHI Motonobu 2006

Sambaドメインの機能比較

- ドメイン機能のサポート状況

斜体は要移行
★付きは、新機能）

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)
ユーザデータベース	◎（SAM）	○（大半の属性を格納）	△（一部の属性のみ格納）
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★	◎	◎	×

※ユーザ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

All Rights Reserved, Copyright TAKAHASHI Motonobu 2006

Sambaドメインの機能比較（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	◎	×（設定可能。動作せず）	×
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	◎	×（設定可能。動作未確認）	×

All Rights Reserved, Copyright TAKAHASHI Motonobu 2006

ユーザデータベース

- Samba 2.2系列までのユーザデータベース
  - **smbpasswd**ファイル
  - Samba 2.2ベースのLDAP（コンパイル時指定）
- Samba 3.0系列におけるユーザデータベース
  - **tdbsam**ファイル
  - Samba 3.0ベースのLDAP
  - Samba 2.2系列までのもの、その他（拡張可能）

  - 使用するユーザデータベースは設定で切り替え可

All Rights Reserved, Copyright TAKAHASHI Motonobu 2006

ユーザデータベース(2)

- ユーザデータベースとサポートレベル
  - Samba 3.0系列では、ユーザデータベースが拡張され、大半の情報がユーザ単位で設定可能
  - Samba 3.0系列のSamba 2.2系列互換のユーザデータベース(**smbpasswd**ファイルなど)では、ドメイン単位でしか設定できない
  - 例:ログオンスクリプトの場合
    - Samba 2.2系列/Samba 3.0系列の互換ユーザデータベース
      - **logon script**パラメータにより、ドメイン一律で設定
    - Samba 3.0系列の拡張ユーザデータベース(LDAP/など)
      - **pdbedit**コマンドにより、ユーザ個々に設定
        logon scriptパラメータはデフォルト値を設定するのみ

```
logon script = %U.bat
```

All Rights Reserved, Copyright TAKAHASHI Motonobu 2006

ユーザデータベースの移行（1）

- 変更しない場合
  - ユーザデータベース自体は移行不要
  - Samba 3.0系列でSamba 2.2ベースのLDAPを用いる場合の注意点
    - **configure** 時に **--with-ldapsam** オプションの指定を行う
    - Samba 2.2ベースのスキーマファイルをインストールする
- LDAPデータベース以外の移行
  - **pdbedit** コマンドを使用する

```
# pdbedit -i smbpasswd:/etc/smbpasswd ¥
        -e tdbsam:/etc/samba/passdb.tdb
```

All Rights Reserved, Copyright TAKAHASHI Motonobu 2006

ユーザデータベースの移行(2)

- LDAPデータベースの移行
  - **convertSambaAccount** コマンドを使用する
    - examples/LDAP以下に存在する移行スクリプト
    - Samba 2.2系列ドメインの認証データを格納したLDIFファイルをSamba 3.0系列の形式に変換する
  - 移行手順
    - Samba 2.2ドメインのデータをLDIF形式にエクスポート

```
# ldapsearch -x -W -D “cn=Manager,dc=samba,dc=local" –LLL ¥
   > samba22.ldif
```

All Rights Reserved, Copyright TAKAHASHI Motonobu 2006

ユーザデータベースの移行(3)

- 移行手順(続)
  - Samba 2.2ドメインのSIDを取得

```
# rpcclient <Samba 2.2ドメインのPDC> -U Administrator%パスワード ¥
  -c 'lsaquery'
```

  - convertSambaAccountによるLDIFファイルの形式変換

```
# convertSambaAccount --sid=<Samba 2.2ドメインのSID> ¥
  --input=samba22.ldif --output=samba30.ldif ¥
  --changetype=add
```

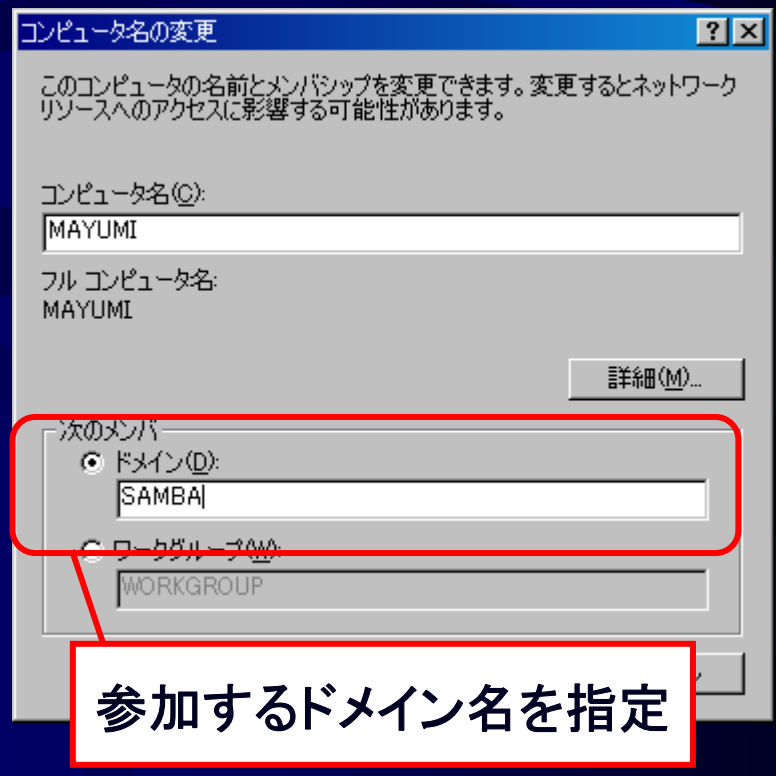
  - LDIFファイルのインポート

```
# ldapsearch -x -W -D “cn=Manager,dc=samba,dc=local" –LLL ¥
   > samba22.ldif
```

All Rights Reserved, Copyright TAKAHASHI Motonobu 2006

マシンのドメイン参加機能、その移行

- 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
- Samba 3.0系列での変更
  - コンピュータアカウントの自動作成は **`add machine script`**パラメータに移行
  - ユーザー権利により、**root**以外のユーザによる参加作業が可能



All Rights Reserved, Copyright TAKAHASHI Motonobu 2006

グローバルグループ機能

- Samba 2.2系列のグローバルグループ機能
  - 特定のグローバルグループのみをサポート
    - **`domain admin group`** (Domain Admins グループ)
    - **`domain guest group`** (Domain Guests グループ)
- Samba 3.0 系列のグローバルグループ機能
  - 任意のグローバルグループをサポート可能
    - **`net groupmap`** コマンドによる対応付けが必要に

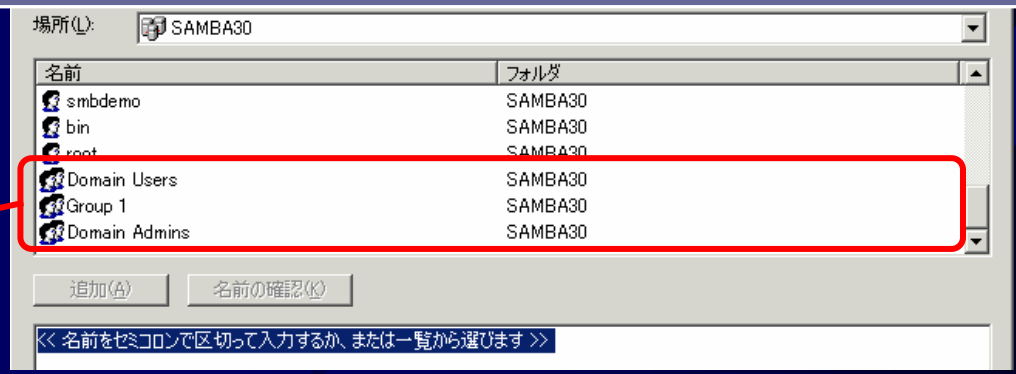
All Rights Reserved, Copyright TAKAHASHI Motonobu 2006

グローバルグループ機能の移行

- Samba 3.0 の機能を用いて再設定
  - **net groupmap** コマンドでグループを対応付け
    - 一般のグローバルグループと同様に設定していく

```
#net groupmap modify NTgroup='Domain Admins' UNIXgroup=domadm
    ←UNIX側domadmグループを既存のDomain Adminsグローバルグループとして公開
#net groupmap add rid=1000 NTgroup='Group 1' UNIXgroup=group1
    ←UNIX側group1グループに対し、Group 1グローバルグループを作成の上公開
#net groupmap list | grep "Group 1"
                          ←Group 1グローバルグループのSIDを確認
Group 1 (S-1-5-21-1108995562-3116817432-1375597819-1000) -> group1
```

クライアント側からは
グローバルグループ
として認識される



All Rights Reserved, Copyright TAKAHASHI Motonobu 2006

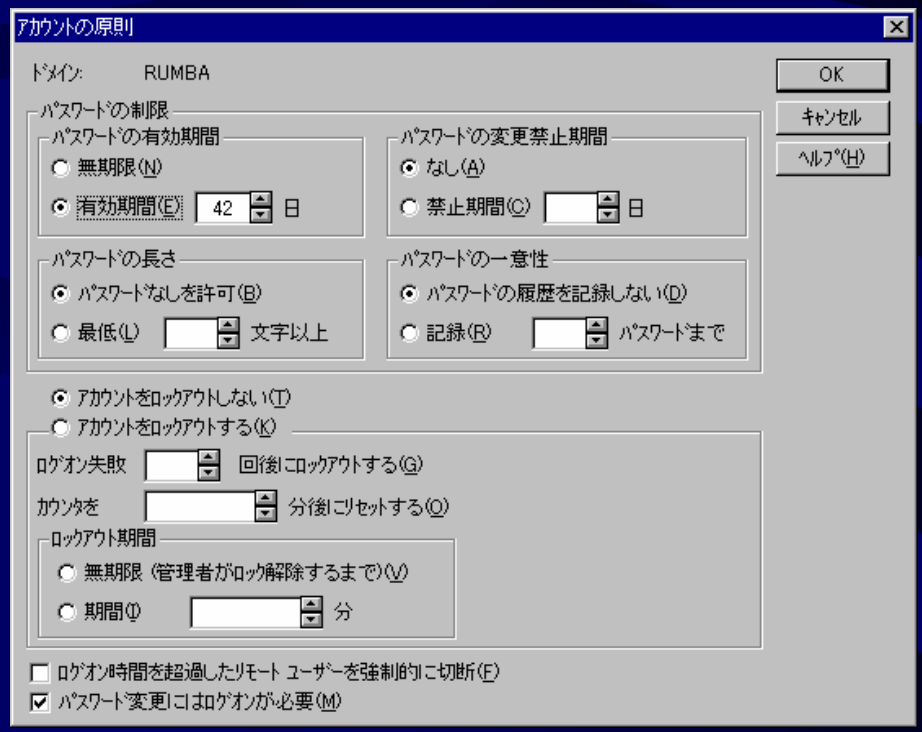
ドメインの新機能、拡張機能

- 以下の機能が追加、拡張
  - アカウントポリシー（新規）
  - ユーザー権利（新規）
  - ユーザー属性(拡張）
  - 信頼関係(新規）
  - ドメインのリモート管理機能（新規）
- 基本的には Samba 2.2系列でサポートされていないため、移行不要
  - Samba 3.0系列のドメインで新規に設定すればよい

All Rights Reserved, Copyright TAKAHASHI Motonobu 2006

アカウントポリシー

- 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
- Samba 3.0系列で新規にサポート
  - Samba 3.0.6以降で、完全サポート
  - Windows側のツールから設定可能

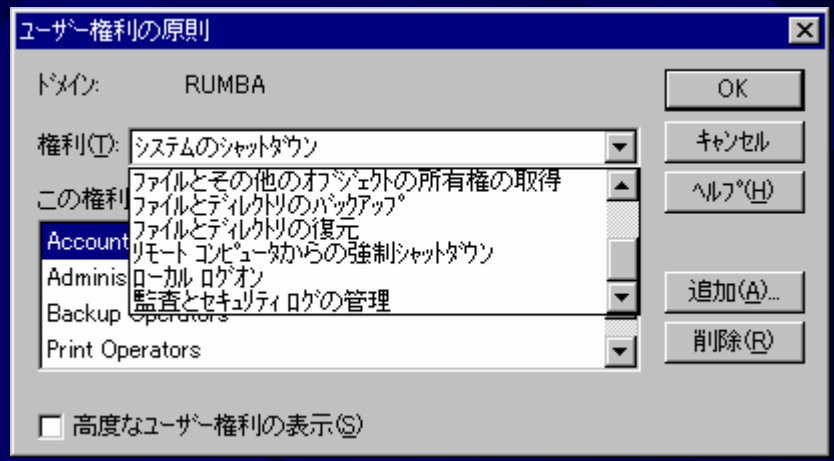


アカウントポリシーの設定画面
(ドメイン ユーザー マネージャ)

All Rights Reserved, Copyright TAKAHASHI Motonobu 2006

ユーザー権利

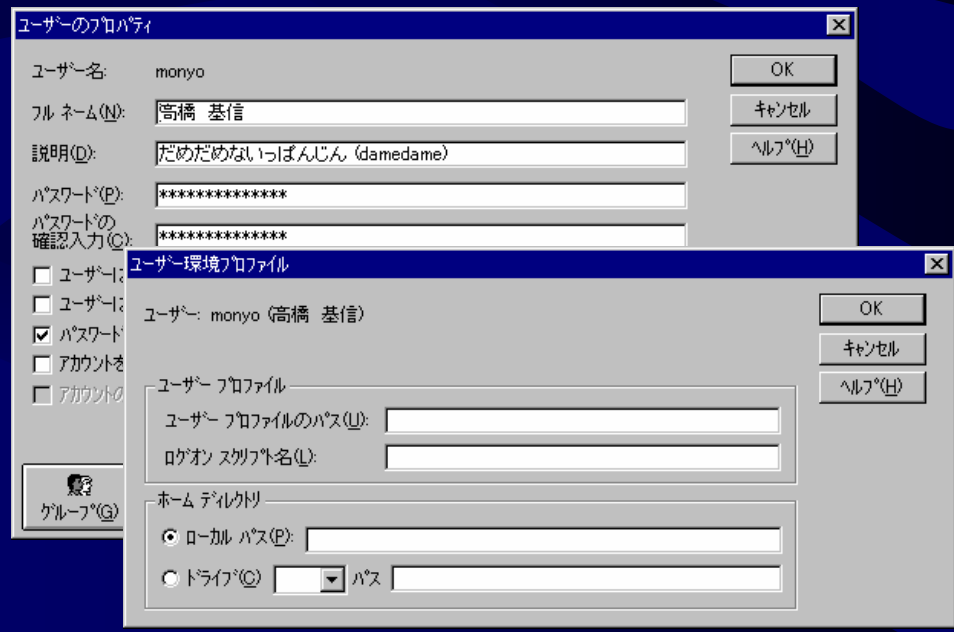
- ユーザー権利とは
  - 特定のユーザに特殊な権利を付与する機能
    - 一部の管理作業を一般ユーザに委任することが可能
- Samba 3.0.11以降でサポート開始
  - **enable privileges** パラメータ
  - 現時点でサポートされているユーザ権利は一部
    - ユーザの管理
    - ディスクの管理
    - プリンタの管理
    - etc…



All Rights Reserved, Copyright TAKAHASHI Motonobu 2006

ユーザー属性

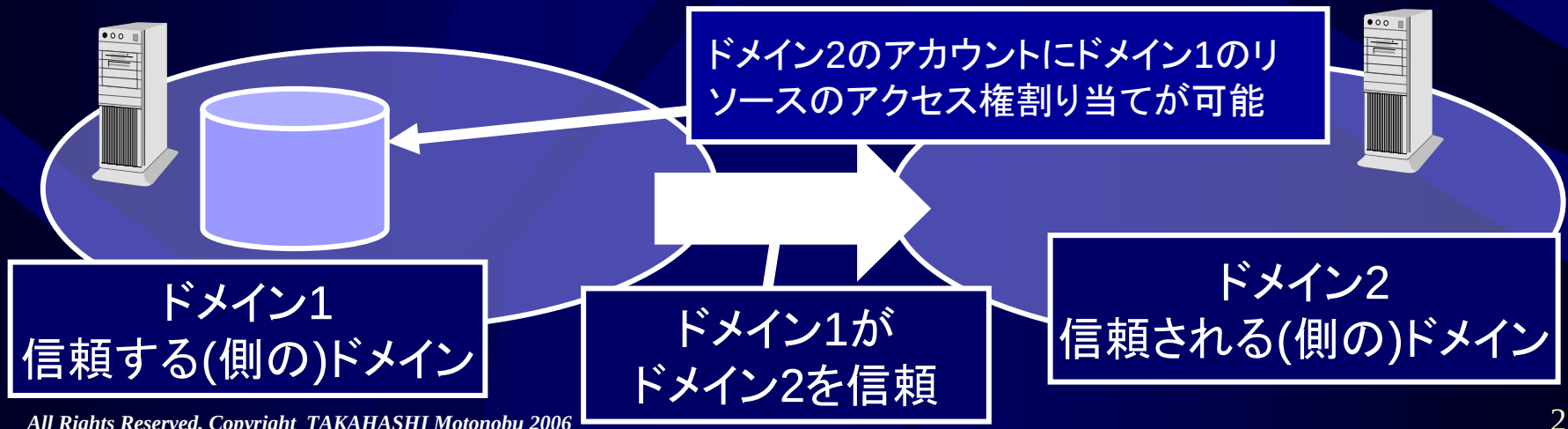
- ユーザー属性とは
  - 「ドメイン ユーザー マネージャ」から設定可能なユーザーのさまざまな属性
  - Samba 2.2系列では、大半が未サポート **or** ドメインで一括設定
  - Samba 3.0系列では、ほぼすべてサポート **and** ユーザごとに設定可能に



All Rights Reserved, Copyright TAKAHASHI Motonobu 2006

信頼関係

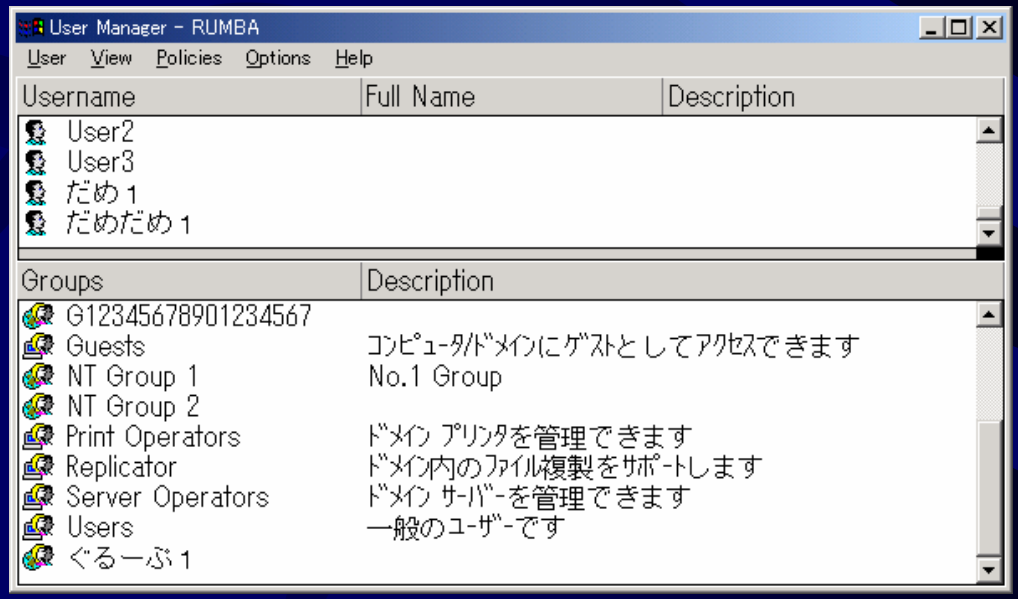
- 信頼関係とは
  - 別ドメインのユーザ、グループに対してリソースへのアクセス許可を割り当てる機能
- Samba 3.0系列で新規サポート
  - ただし、明示的な一方向の信頼関係のみサポート（NTドメインと同等）



All Rights Reserved, Copyright TAKAHASHI Motonobu 2006

ドメインのリモート管理

- Windows のツールからSambaドメインの管理が可能となる機能が追加
  - ユーザ管理(ドメイン ユーザー マネージャなど)
  - コンピュータ管理(サーバー マネージャなど)
  - 共有管理(同上)
- この機能をサポートする各種パラメータが新規追加



All Rights Reserved, Copyright TAKAHASHI Motonobu 2006

3. 新機能、拡張された機能

- 以下の項目ごとに簡単に記載
  - ファイル、プリンタサーバ機能
  - ドメイン機能（省略）
  - ユーザデータベース機能（省略）
  - メンバサーバ機能
  - セキュリティ機能
  - SWAT国際化機能
  - リモート管理機能

All Rights Reserved, Copyright TAKAHASHI Motonobu 2006

ファイル、プリンタサーバ機能

- ファイルサーバ機能
  - ACL対応機能の向上
    - POSIX ACLを実装したプラットフォームでは、NTFSと同程度の細かいアクセス許可を設定可能
      →ただし、完全互換ではない
  - ボリュームシャドウコピー機能
  - ゴミ箱機能、監査機能、その他
- プリンタサーバ機能
  - NT互換の印刷機構実装
    - プリンタサーバをGUIから制御可能

All Rights Reserved, Copyright TAKAHASHI Motonobu 2006

メンバサーバ機能(1)

- Windows 2000と同じKerberos認証をサポート
  - MIT Kerberos 5が必要
  - NetBIOSが無効な環境でもADドメイン参加が可能
  - Samba 2.2までと同じ方法でも参加自体は可能
    - ただし、NTと同様のNetBIOSを利用した方式となる
  - 「**security = ADS**」が追加

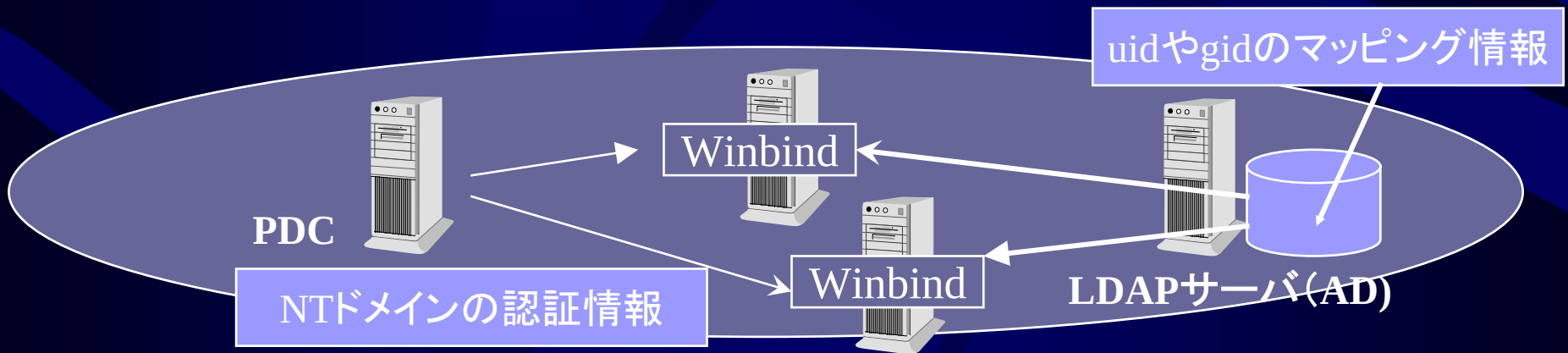
```
[global]
  realm = <ADのドメイン名(大文字)>
  ads server = DC名
  security = ADS
  encrypt passwords = yes
```

All Rights Reserved, Copyright TAKAHASHI Motonobu 2006

メンバサーバ機能(2)

- **Winbindの機能向上**
  - **uidやgidをマシン間で統一**
    - 情報は、LDAPやActive Directory（AD)に格納する

```
[global]
  idmap backend = ldap://ldap.home.monyo.com
```



All Rights Reserved, Copyright TAKAHASHI Motonobu 2006

セキュリティ機能

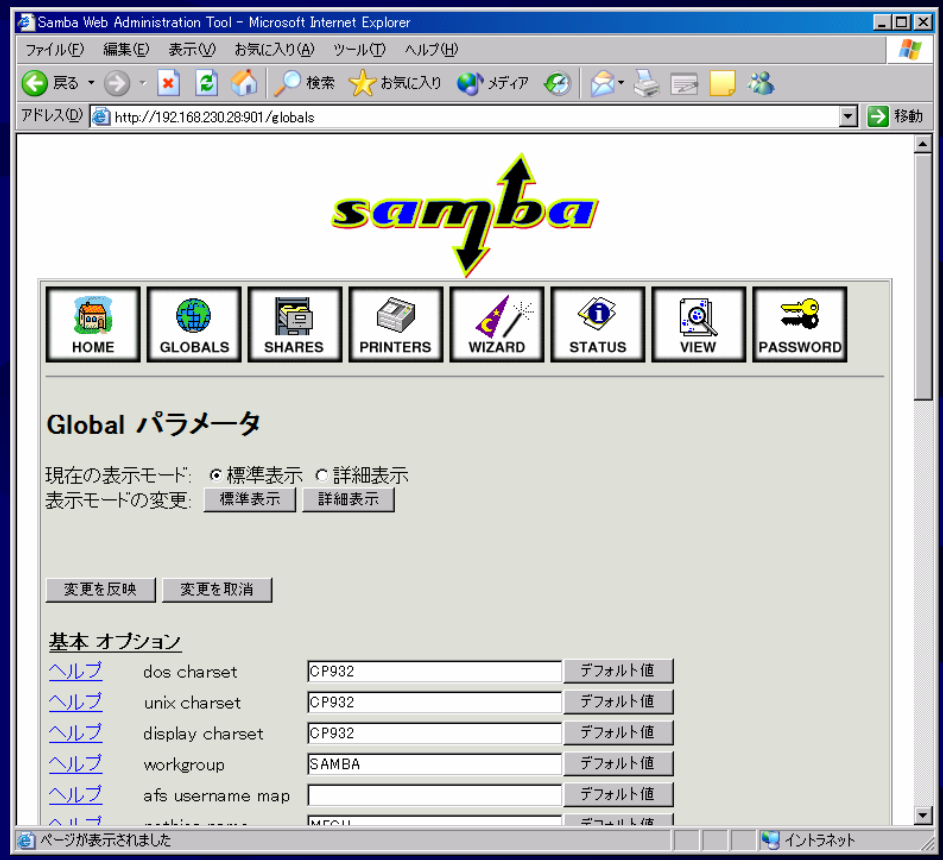
- Windows と同レベルのSMBセキュリティを実装

機能	Windows NT/2000/XP	Samba 2.2	Samba 3.0
LMレスポンス抑止	可能 `LMCompatibilityLevel`	可能 `lanman auth`	可能 `lanman auth`
NTLMレスポンス抑止	可能 `LMCompatibilityLevel`	不可能	可能 `ntlm auth`
NTLMv2対応	可能(NT 4.0 SP4以降) `LMCompatibilityLevel`	不可能	可能
SMB署名	可能(NT 4.0 SP3以降)	不可能	不可能?
セキュアチャネル署名･暗号化	署名、暗号化可能 (NT 4.0 SP4以降)	不可能	署名可能 `server schannel`

All Rights Reserved, Copyright TAKAHASHI Motonobu 2006

SWAT国際化機能

- Samba日本語版の成果が同梱
  - デフォルトで機能が有効になっている
  - 無効にすることも可能



All Rights Reserved, Copyright TAKAHASHI Motonobu 2006

リモート管理機能

- Windows からSambaサーバの管理が可能に
- netコマンドの新設
  - リモートからWindows NT系OSのマシンやSambaの管理、構成を実現
    - コマンドラインベースなのでバッチ処理可能

All Rights Reserved, Copyright TAKAHASHI Motonobu 2006

まとめ

- Samba 3.0系列への移行のポイント
  - １．国際化関連機能
    - パラメータ変更
    - ファイル名の移行
  - ２．ドメイン機能サポート
    - 認証データベース（特にLDAP）の移行
    - グローバルグループ
  - ３．新機能、拡張された機能
    - Windowsサーバとの互換性向上を目指すか？

All Rights Reserved, Copyright TAKAHASHI Motonobu 2006