

# Samba最新動向

日本Sambaユーザ会

たかはし もとのぶ(高橋基信)

[monyo@samba.gr.jp](mailto:monyo@samba.gr.jp)

# Samba 3系列の開発状況

- Samba4開発の遅延にともない、Samba4で導入予定だった機能（Active Directory (AD) のドメインコントローラ (DC) 以外）を順次実装
  - 主要な機能はほぼ実装済
  - 内部実装の改善以外は、Windowsの機能強化への追従が主
    - 目に見える機能強化はほとんどないのが現状
    - 今後もSamba 3系列の大幅な機能強化は考えにくい
  - 最新Samba 3.6.0は08/09にリリース
    - Samba 3.7.0はなさそう
      - 「リリースする事態にならないことを願いたい」とのこと

# Samba 3.6.0 (2011/08/09リリース)

## ■ 特徴

### □ SMB2 (Vista以降で採用) が正式サポート

- SMB2により、遅延の大きいNWでパフォーマンス向上  
⇒SMB2を導入したい場合は、考慮すべきリリース

### □ Idmap機構の改良

- alloc/バックエンド機構の隠蔽化 (より直感的な設定に)
    - Idmap関連の文法も変更あり
  - 新Idmap/バックエンドautoridのリリース
    - Samba側でのバックアップ不要というridの長所がなくなるため、使用を推奨しない。ridを適切に構成することを推奨
- ⇒複数ドメイン環境以外では、ほぼ影響なし

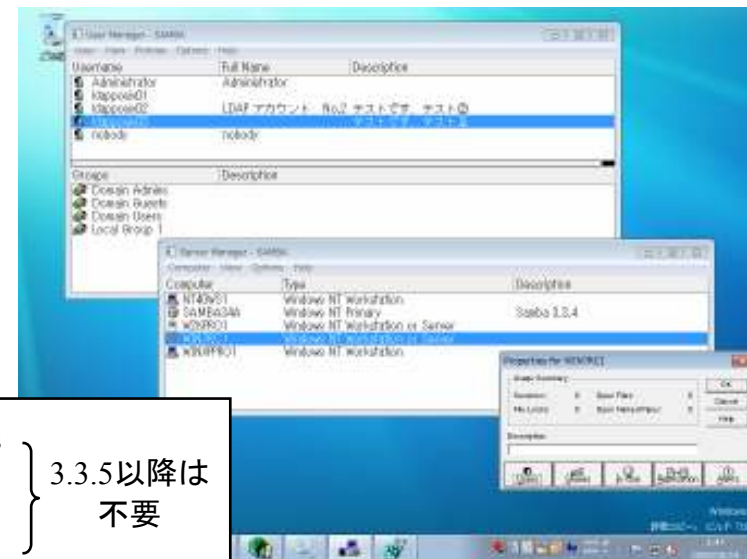
リリースノート翻訳: <http://cgi.samba.gr.jp/mailman/archives/samba-jp/2011-August/002791.html>

## 参考: Windows 7 (Windows Server 2008 R2) 対応

- ファイルサーバとしての使用は、問題なし
- Sambaドメインへのログオンも実現

□ Samba 3.2.12/3.3.2以降

- Windows 7マシンの  
レジストリ変更が必要



```
HKLM\Software\Classes\Netlogon\Parameters
RequireStrongKey = 0
RequireSignOrSeal = 0
} 3.3.5以降は不要

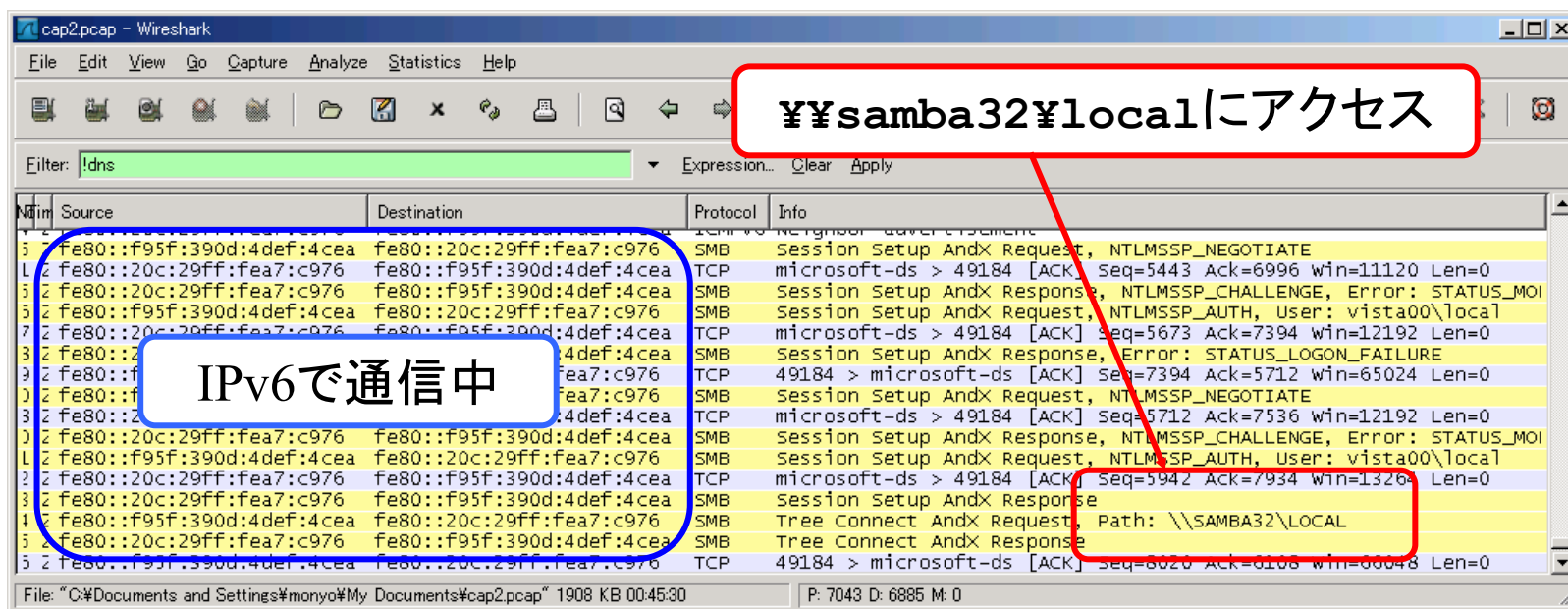
HKLM\Software\Classes\LanManWorkstation\Parameters
DWORD (32bit) 形式 DNSNameResolutionRequired = 0
DWORD (32bit) 形式 DomainCompatibilityMode = 1
```

Windows 7 からSamba 3.5.4 サーバで構築したSambaドメインにアクセス

[http://wiki.samba.gr.jp/mediawiki/index.php?title=Windows\\_7からSambaドメインにログオンできない](http://wiki.samba.gr.jp/mediawiki/index.php?title=Windows_7からSambaドメインにログオンできない)

# 参考: IPv6対応

- Samba 3.2以降では、プラットフォームが対応していれば、自動的に対応
  - IPv6環境でのADドメイン参加も確認



Windows Vistaからの通信例  
¥¥samba32¥¥local に接続したところ

# Samba 4系列の開発状況

- ADのDCを目玉機能として2003年に開発着手
- 2005年から開発版バイナリの提供を開始
  - 長期にわたり停滞 ⇒ 2007年12月にマイクロソフト社から公式にプロトコル情報の開示を受け、ようやく開発が加速
  - 最新版は2011/06/24リリースのalpha16
  - ここまでDC機能に特化して開発
- 2010/12/23リリースのalpha14では、実運用が開始されていることがアピールされる

Although still in development, samba4 is already used in a couple of production sites ... (alpha14リリースノートより)

## 参考 : Samba 4系列の開発の軌跡(2008年迄)

- samba-4.0.0TP1～TP5
  - Active Directoryログオンのサポートと改善
- 2007/09/06 samba-4.0.0alpha1
  - グループポリシーのサポート
  - ADUC (Active Directory ユーザーとコンピュータ) による管理のサポート
  - Winbind機構のサポート
- 2007/12/17 samba-4.0.0alpha2
- 2008/04/15 samba-4.0.0alpha3
  - SWATサポートが停止(開発者不足ほか)
- 2008/06/05 samba-4.0.0alpha4
  - Pythonサポートが必須に(Pythonがないとインストールできません)
  - SMB2サポートの開始
  - ユーザ情報のWinbind機構への格納開始
- 2008/06/30 samba-4.0.0alpha5
  - SMB2署名のサポート開始

## 参考 : Samba 4系列の開発の軌跡(2009年)

- 2009/01/21 samba-4.0.0alpha6
  - JavaScriptサポートの停止(Pythonで代替)
  - 様々な内部コンポーネントが大きく改善
- 2009/02/26 samba-4.0.0alpha7
  - Windows 7サポートの開始
- 2009/06/19 samba-4.0.0alpha8
  - Windows Server 2008互換のスキーマを実装
- 2009/11/30 samba-4.0.0alpha9
  - ユーザのプロパティを完全サポート
  - AD上のアクセス許可がWindows Server 2008互換に
  - WindowsとのDRS(ディレクトリ複製サービス)のサポート開始
- 2009/12/08 samba-4.0.0alpha10
  - alpha9の致命的なバグ(DRS関連)修正

## 参考 : Samba 4系列の開発の軌跡(2010年)

- 2010/01/10 samba-4.0.0alpha11
  - RID割り当て機構の改善により重複の可能性が排除
- 2010/09/20 samba-4.0.0alpha13(alpha12は正式リリースされず)
  - ビルドシステムがWAFへ変更
  - Winbind機構が大幅に改善
  - DRS関連の大幅な改善
  - 動的DNSのサポート開始(ただしWindowsのDCとの相互運用性なし)
- 2010/12/23 samba-4.0.0alpha14(コードネーム:randomdata)
  - DRS関連の大幅な改善
  - バックアップ用のスクリプトが添付
  - netコマンドがsamba-toolコマンドに名称変更
  - Sambaの実運用が始まっていることがアピール

## 参考 : Samba 4系列の開発の軌跡(2011年～)

- 2011/04/23 samba-4.0.0alpha15
- 2011/06/24 samba-4.0.0alpha16
  - smbd/nmbd/winbinddバイナリの提供開始(デュアルバイナリ化)

# Samba 4系列の今後

- 今年中にリリースされる可能性が高い
  - 最近の議論を見ている限り、Samba 3.6.0リリース後は、Samba 4.0リリースに注力すること
  - ADのDCとしての機能は、完成に近づいている
    - 実運用している箇所もある(とアピールできるレベル)
    - 主な残課題
      - DRS(ディレクトリ複製サービス)の完成度アップ
      - アップグレード、移行のサポート強化
  - デュアルバイナリ化(わたしの造語ですが...)
    - DC機能以外のファイルサーバ機能などは、従来のSamba3系列の延長としてサポート

# デュアルバイナリ化

## ■ alpha16から、事実上Samba4にSamba3が同梱

### □ 従来のSamba 4⇒sambaプロセス

- ADのDCに特化 — 以降は、この「samba」を説明

### □ Samba 3互換⇒smbd/nmbd/winbinddプロセス

- ファイルサーバ機能など従来からの機能を提供

- Samba 3系列の延長線上にある

### □ sambaをDCとして用い、ファイルサーバとしてはsmbd/nmbd/winbinddを用いる形態が想定

- 同一IPでの共存は不可。同一サーバ上の異なるIPで動作させることは可能

Samba 4とは.....

ADのDCに特化したサーバに従来のSambaを同梱したもの 12

# sambaプロセスとは

## ■ ADのDCに特化

- nmbd、smbd、winbinddを包含した単一プロセス

## ■ DCとして必要なサービスの大半を単独で実装

- 外部ライブラリへの依存性を極力排除

- Kerberos (Heimdal Kerberosをソースに取り込み)

- LDAP (独自実装)

- OpenLDAPの使用は考慮されていない (alpha15以降)

- 別プロダクトと連携する機能

- DNS (BIND)、NTP (ntpd)

- スクリプティング (Python) ← Pythonがないとビルド不可

## 参考：別プロダクトとの連携

### ■ BINDとの連携

- BIND 9.7.2rc1以降で、Kerberosを用いたAD独自の「セキュリティで保護された動的更新」をサポート
  - 簡単な設定方法がSamba4-HOWTOに記載されている
  - BIND以外のDNSサーバはサポートの予定なし

### ■ ntpdとの連携

- ntpd 4.2.6以降で--enable-ntp-signdを有効にしてconfigureすることでSamba 4互換NTPをサポート

### ■ Python

- Sambaの各種コマンドがPythonで書かれるように

# 参考 : sambaプロセスの使用ポート

## ■ WindowsのDCと同一

| ポート  | プロトコル   | 用途                                     |
|------|---------|----------------------------------------|
| 42   | tcp     | WINS複製                                 |
| 88   | tcp/udp | Kerberos                               |
| 135  | tcp     | MS-RPC                                 |
| 137  | udp     | NetBIOSネームサービス                         |
| 138  | udp     | NetBIOSデータグラム                          |
| 139  | tcp     | ファイルサービス                               |
| 389  | tcp/udp | LDAP                                   |
| 445  | tcp     | Direct Hosting of SMB                  |
| 464  | tcp/udp | kpasswd                                |
| 646  | tcp/udp | LDAPS                                  |
| 3268 | tcp     | グローバルカタログ (3269 LDAPSによるグローバルカタログも実装中) |

参考 : <http://support.microsoft.com/kb/179442/ja>

# Samba 4のDC機能(1)

## ■ Windows Server 2008とほぼ互換

□ ADUC (Active Directoryユーザーとコンピュータ) からWindowsサーバと同様に管理可能

□ よくも悪くもWindowsそのものとしての管理が可能

■ Windows Server 2008と同等のスキーマをサポート

■ グループポリシー

□ グループポリシーのアクセス許可、継承のブロック、複数箇所へのGPOのリンクなど、細かい機能もサポート

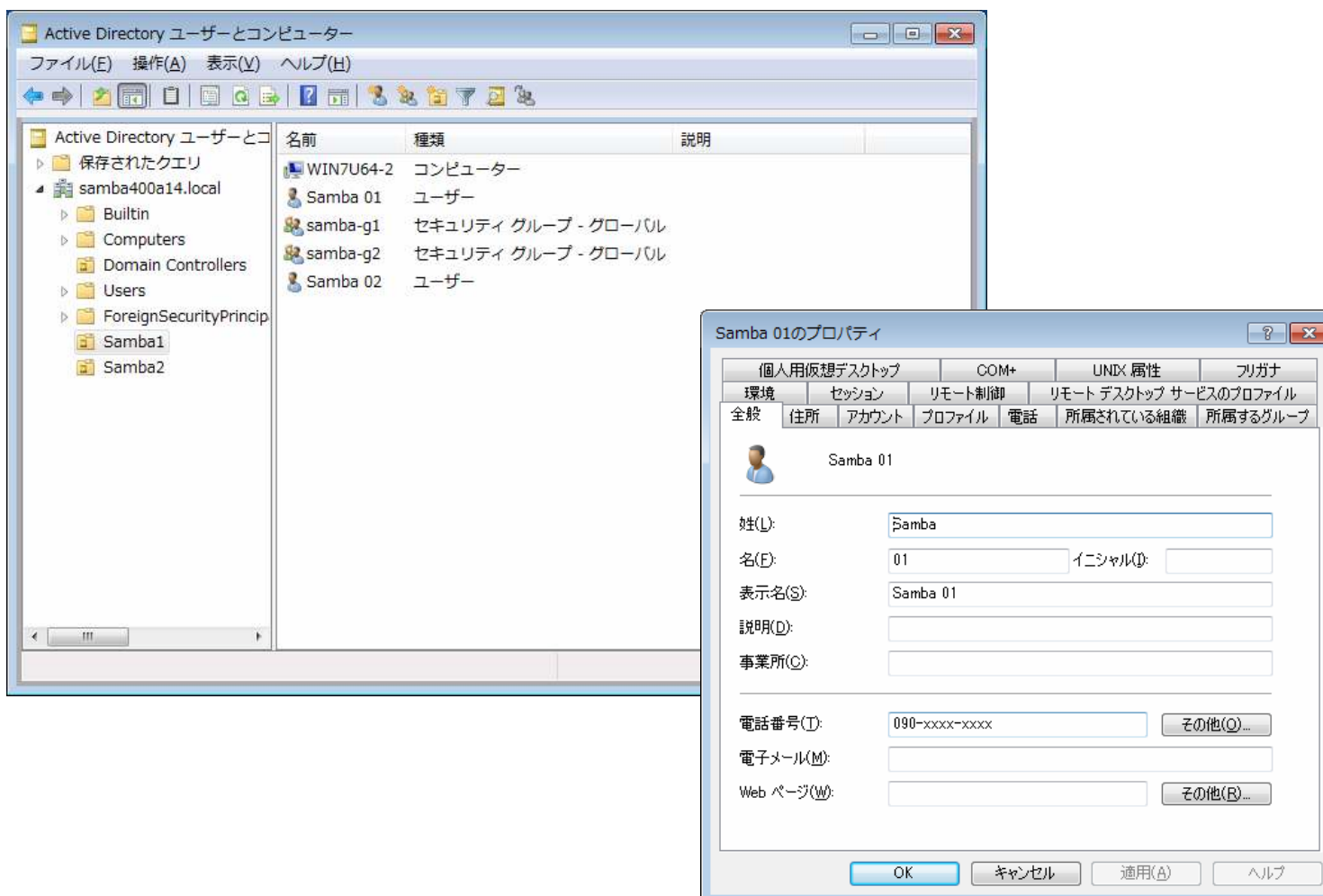
■ ユーザー属性の設定、編集

■ サイト、FRS

□ 設定は可能。動作は未検証

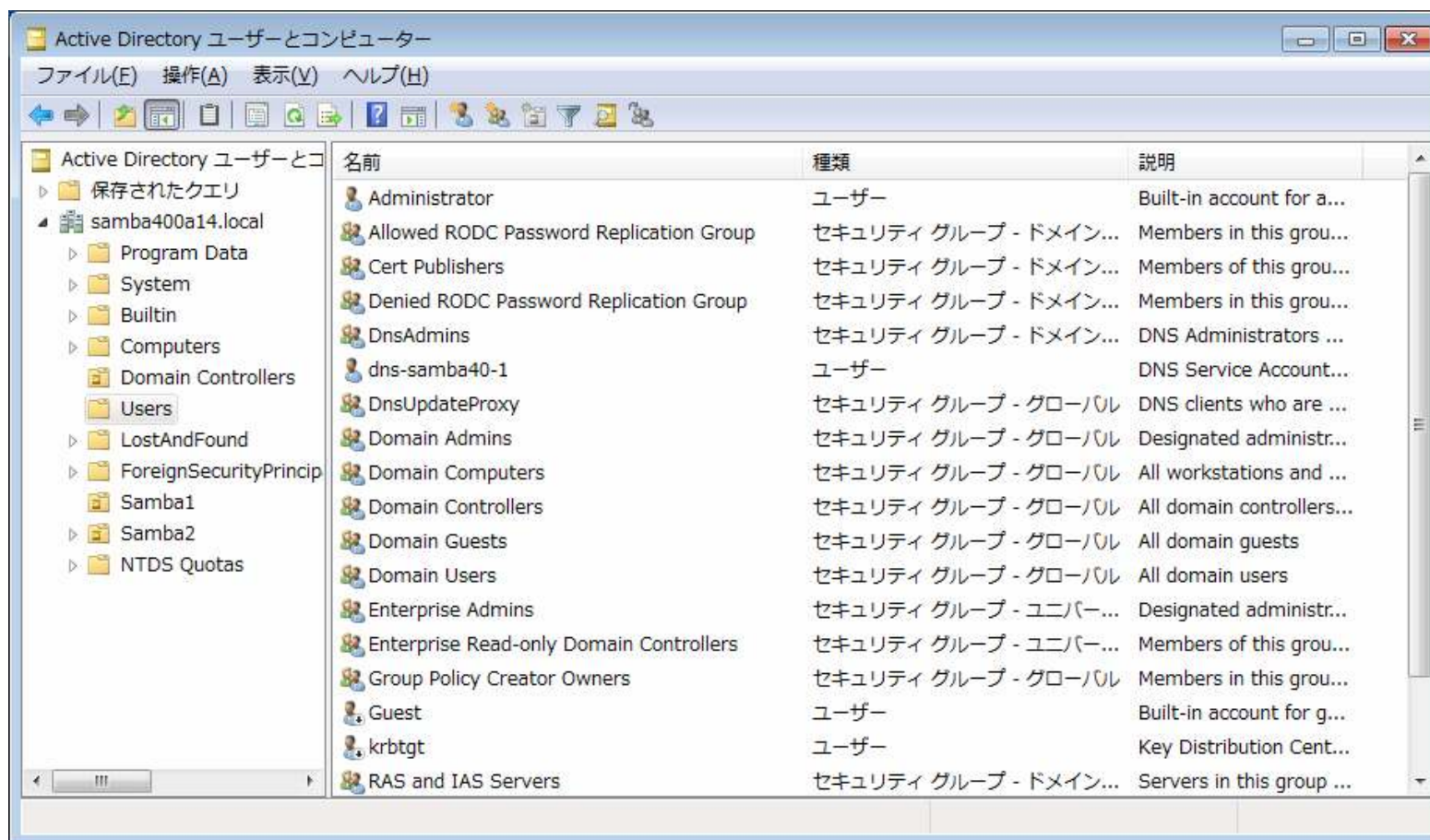
# 参考: Samba 4のDC機能

## ■ ADUCによる管理



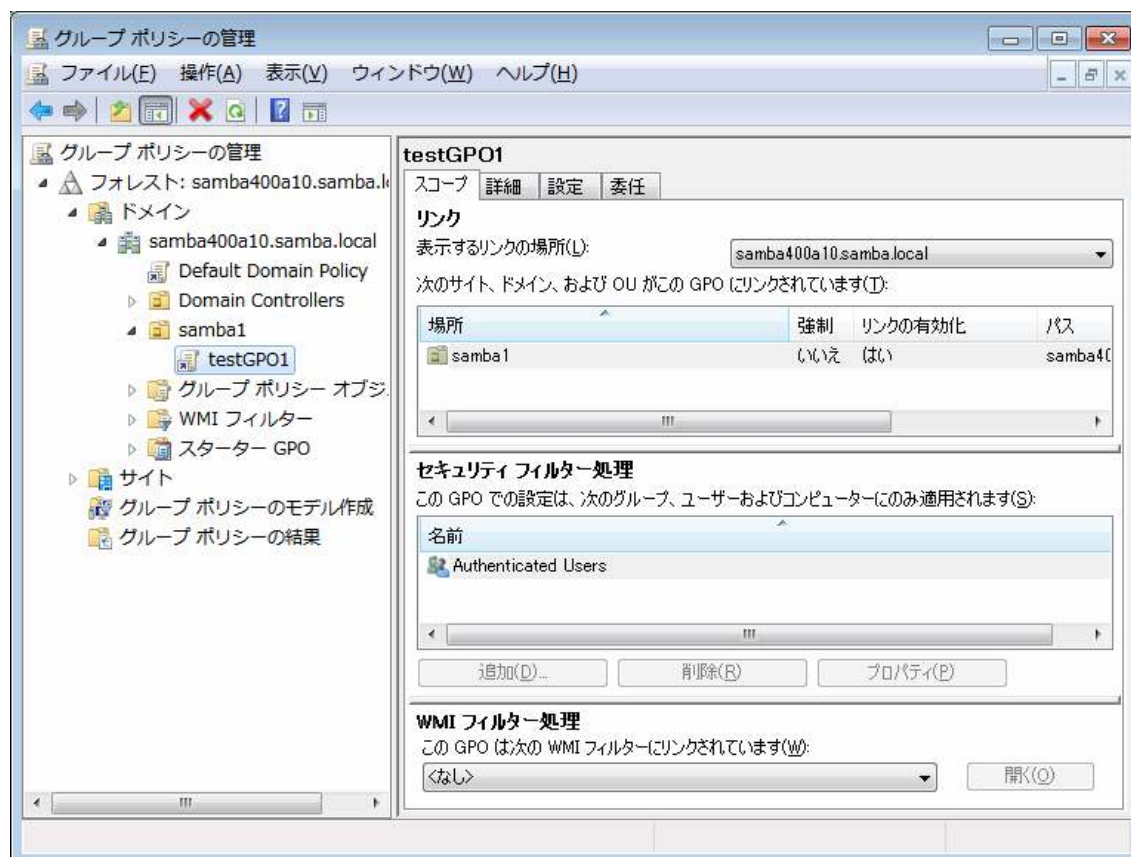
# 参考: Samba 4のDC機能

## ■ ADUCによる管理



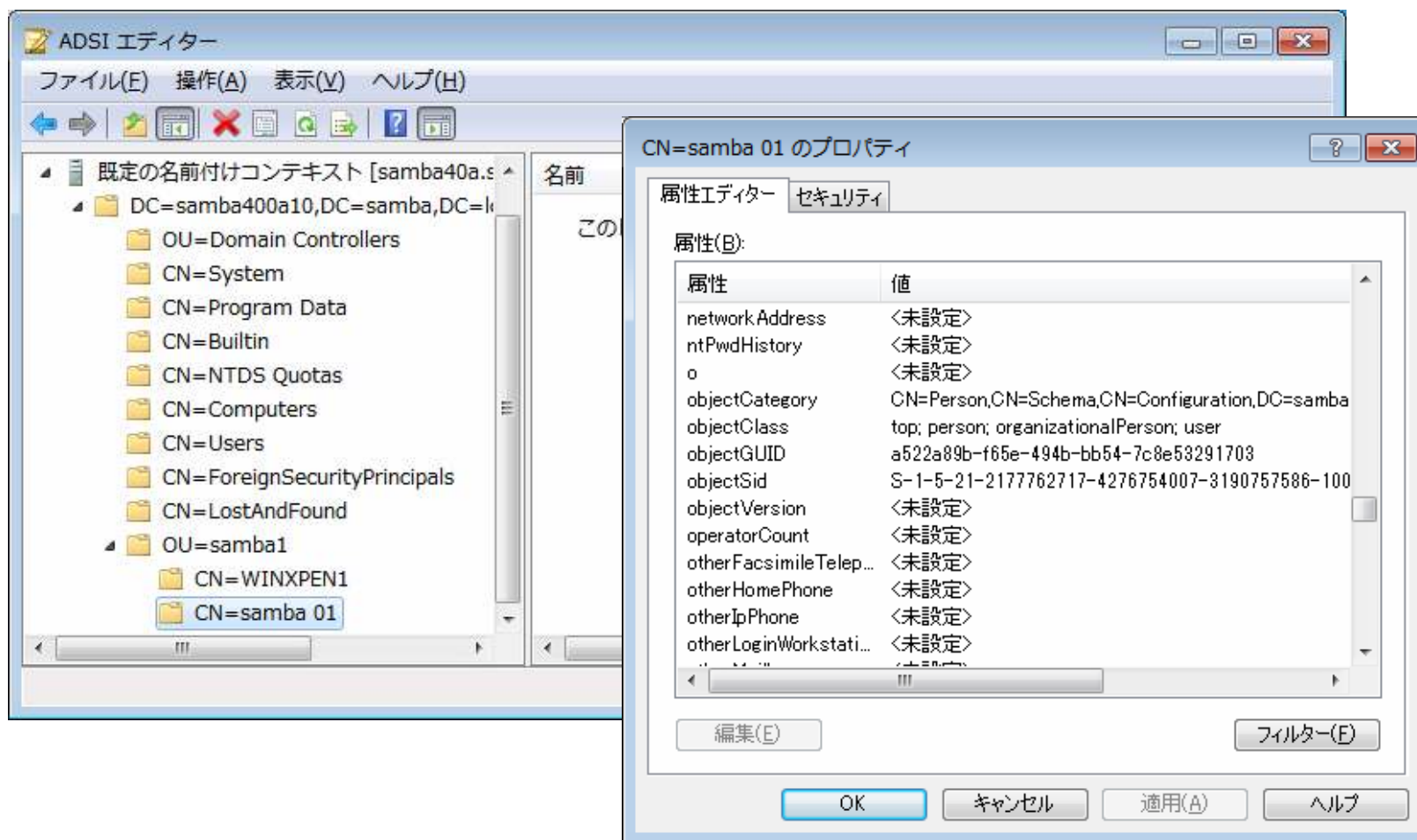
# 参考: Samba 4のDC機能

## ■ グループポリシーの管理によるGPO管理



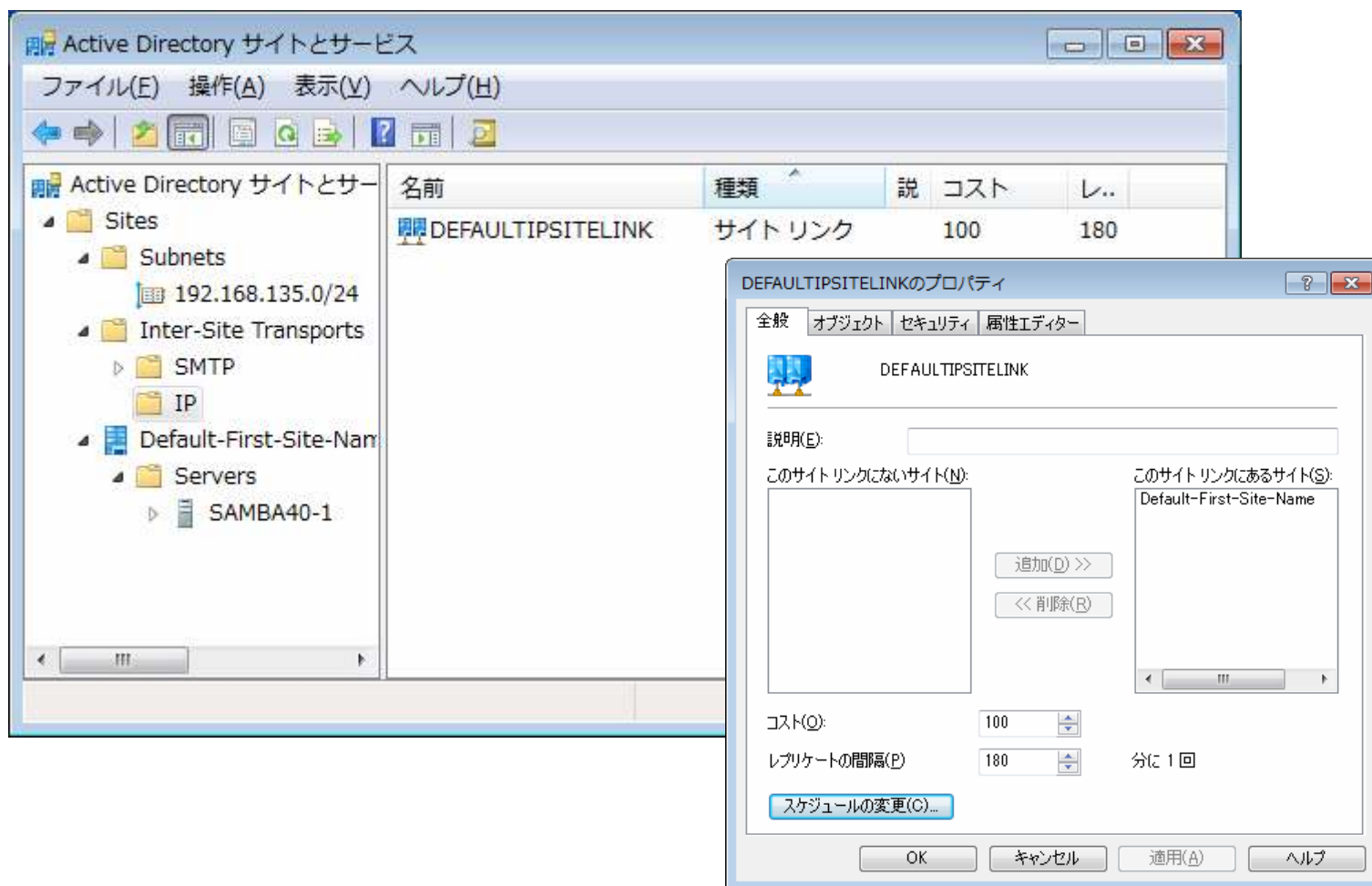
# 参考: Samba 4のDC機能

## ■ ADSIエディタによる編集にも対応



# 参考: Samba 4のDC機能

## ■ Active Directoryサイトとサービスによる管理



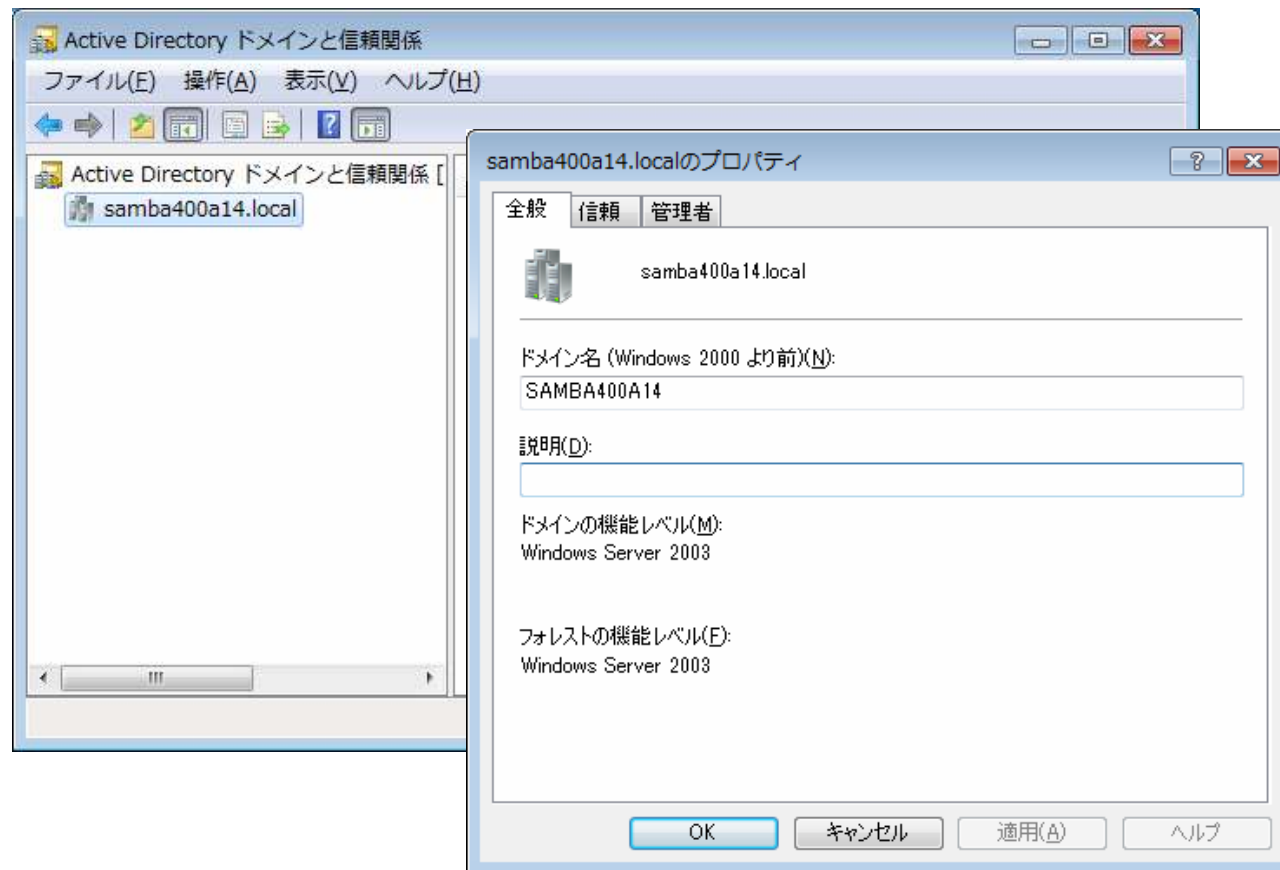
# Samba 4のDC機能(2)

## ■ Windows Server 2008とほぼ互換

- 信頼関係、ドメインの機能レベルもサポート
  - 機能レベル自体は、現在Windows Server 2003
  - RODCサポート
  - Windows 7も当然サポート
- WindowsのDCとSambaのDCの混在も可能
  - ディレクトリ複製プロトコル(DRS)をサポート
- Exchange Serverもサポート
- 既存のADからの移行もサポート予定

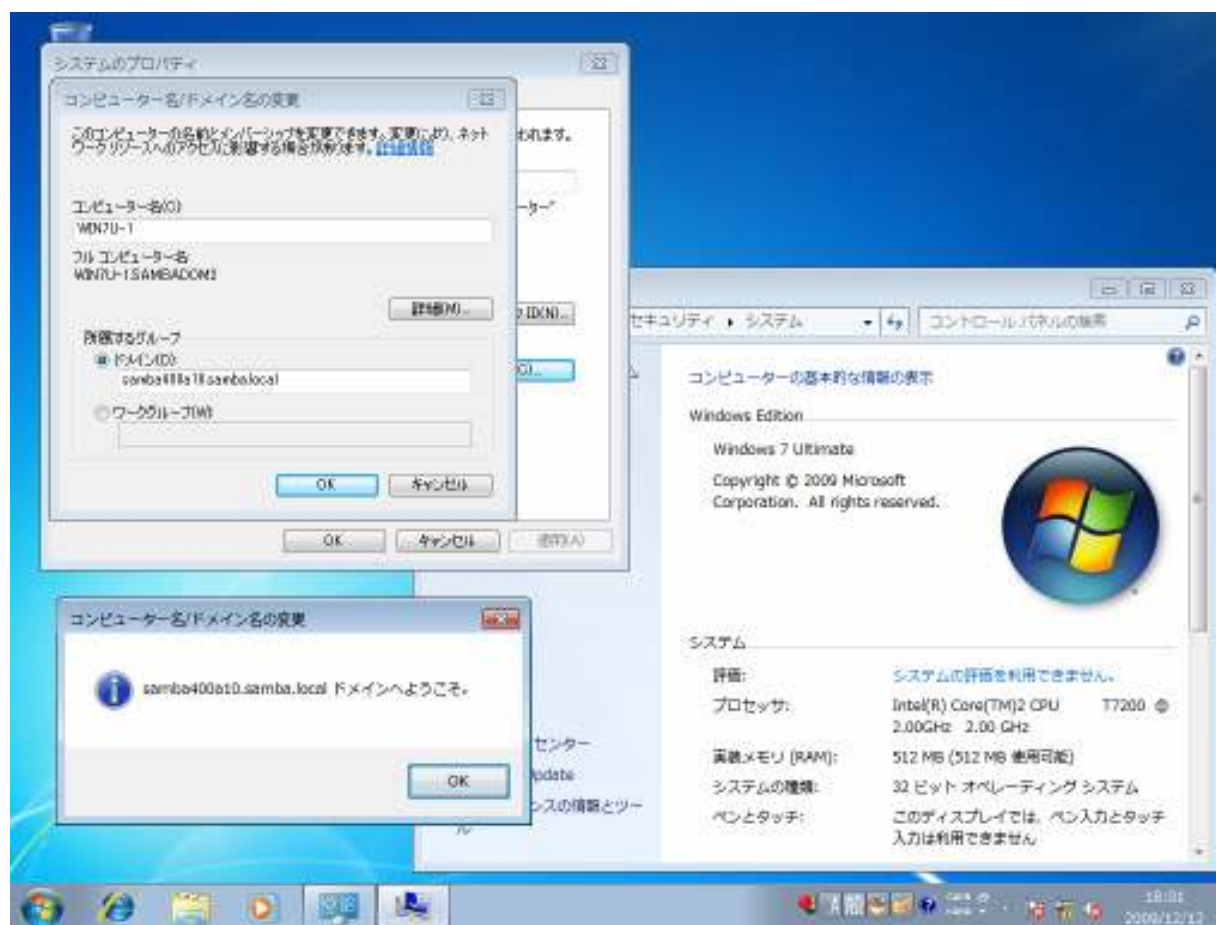
# 参考: Samba 4のDC機能

## ■ Active Directoryドメインと信頼関係による管理



# 参考: Samba 4のDC機能

## ■ Windows 7も完全サポート



# 参考: Samba 4のDC機能

## ■ SambaのDCとWindowsのDCの混在

The screenshot shows the Active Directory console with two windows open. The top window, 'Active Directory ユーザーとコンピュータ', displays a table of domain controllers. The bottom window, 'Active Directory サイトとサービス', shows the replication topology. A red circle highlights the two DCs in the top window, and a red box with text points to them.

| 名前        | 種類     | D... | サイト                     | 説明 |
|-----------|--------|------|-------------------------|----|
| SAMBA40-2 | コンピュータ | GC   | Default-First-Site-Name |    |
| W2K8SRV1  | コンピュータ | GC   | Default-First-Site-Name |    |

SambaとWindowsのDCが共存

```

C:\>管理者: コマンド プロンプト

2011-01-19 02:09:17 の最後の試行は成功しました。

CN=Configuration,DC=W2K8AD1,DC=LOCAL
Default-First-Site-Name¥SAMBA40-2 (RPC 経由)
DSA オブジェクト GUID: 50dd2187-98bb-4c4c-89a3-195ef0c6
2011-01-19 02:09:13 の最後の試行は成功しました。

CN=Schema,CN=Configuration,DC=W2K8AD1,DC=LOCAL
Default-First-Site-Name¥SAMBA40-2 (RPC 経由)
DSA オブジェクト GUID: 50dd2187-98bb-4c4c-89a3-195ef0c6
2011-01-19 02:09:13 の最後の試行は成功しました。

C:\Users\Administrator>
  
```

# Samba 4のDC機能(3)

## ■ UNIXからのSambaサーバ管理機能も実装

□ samba-toolにより、ある程度は実現

■ 基本的にはWindowsからの管理が前提

```
# samba-tool
Usage:
samba-tool <command> [options]
Available commands:
    password    Changes/Sets the password on a user account
                [server connection needed]
    samdump     dump the sam of a domain
    samsync     synchronise into the local ldb the sam of an NT4
                domain
    gpo         Administer group policies
    setexpiry   Sets the expiration of a user account
    fsmo        Makes the target DC transfer or seize a fsmo role
                [server connection needed]
    pwsettings  Sets password settings
    group       Group management
    gpo2        GPO commands
    machinepw   Gets a machine password out of our SAM
```

```
rodc          RODC commands
domainlevel   Raises domain and forest function levels
acl           NT ACLs manipulation
vampire       Join and synchronise a remote AD domain to the
                local server [server connection needed]
enableaccount Enables a user
export        Dumps the sam of the domain we are joined to
                [server connection needed]
user          User management [server connection needed]
spn           SPN management [server connection needed]
time          Retrieve the time on a remote server [server
                connection needed]
setpassword   (Re)sets the password on a user account
join          Joins domain as either member or backup domain
                controller [server connection needed]
newuser       Creates a new user
drs           DRS commands
ldapcmp       compare two ldap databases
```

# sambaプロセスの機能まとめ

- sambaプロセスはADのDCに特化
  - ファイルサーバなどは、従来のsmbdを使う
- 一度sambaプロセスを起動したら、後はWindowsの管理ツールから管理する形態
  - よくも悪くもWindowsサーバと一緒に(^\_^;;
  - ADの機能や管理ツールの操作方法、ファイアウォールの設定などについては、当然ですがM\$のドキュメントを参照するのが早いですActive Directory知らない扱えません

# Samba 4のファイルサーバ機能

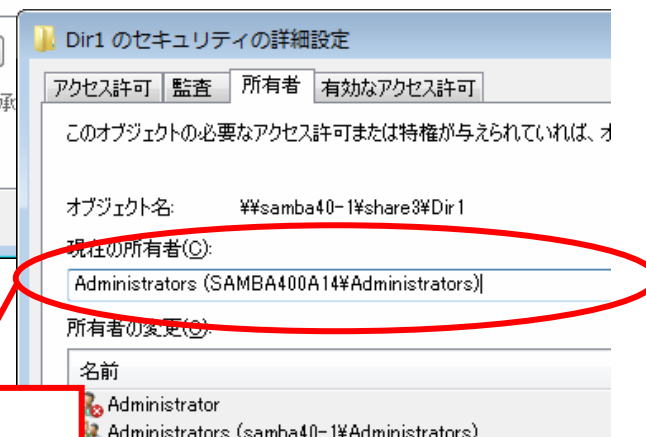
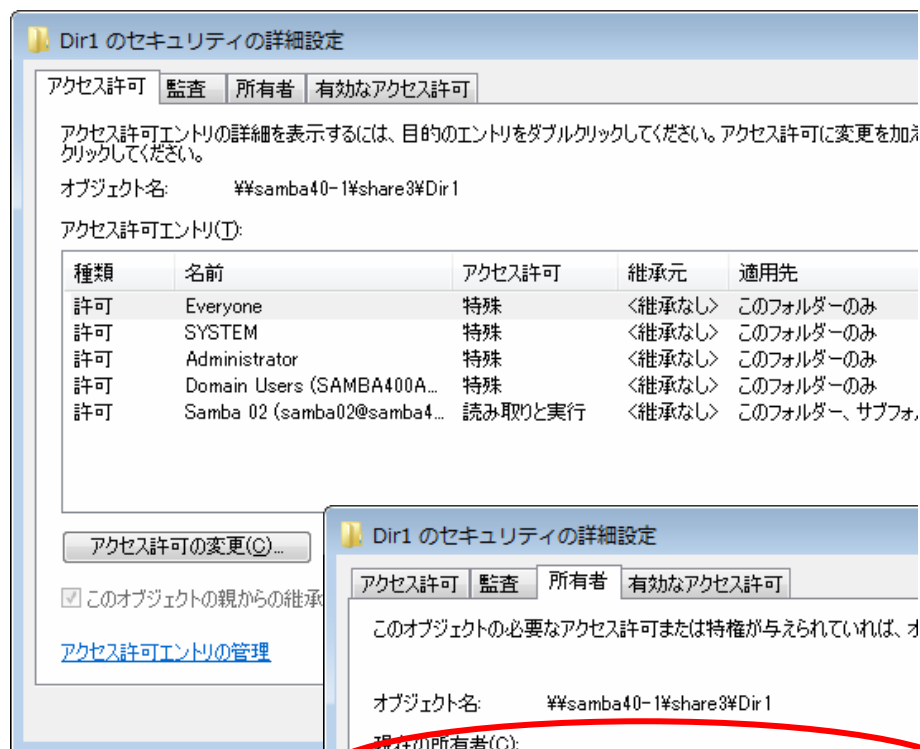
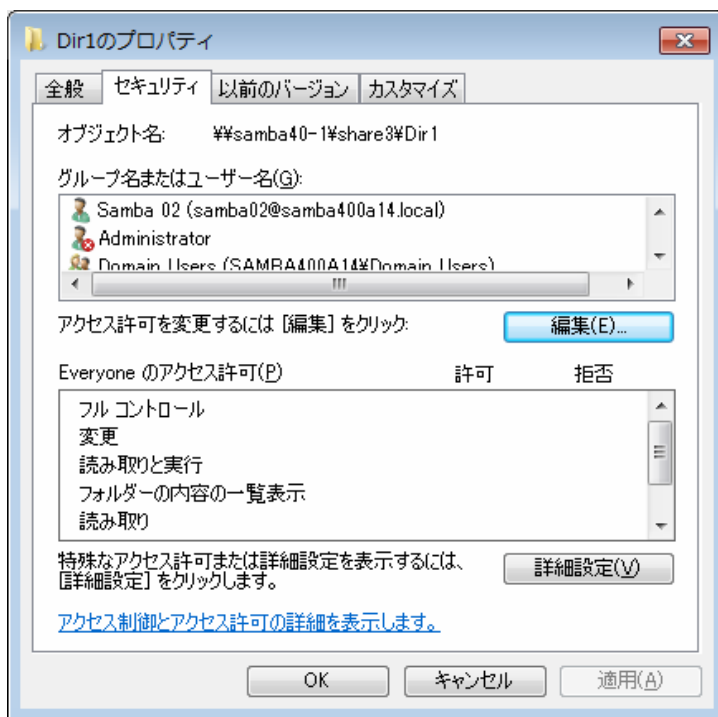
- デュアルバイナリ化により、最終的な落としどころは不透明に
  - 基本的にファイルサーバとしてはsmbdを使って欲しいというのが現状のメッセージ
  - sambaプロセスのファイルサーバ機能は、DC機能をサポートするために最低限必要な機能以外はサポートされない可能性も
    - nmbdのブラウジングや印刷機能もサポートされない模様

## Samba 4のファイルサーバ機能(2)

- UNIX環境との相互運用性より、Windowsからアクセスした際の互換性向上を優先
  - ACL、ファイル属性などは、すべて拡張属性に格納
    - POSIX ACLへのマッピングは(少なくともデフォルトでは)考慮されていない
      - UNIXファイルシステム上のパーミッション情報などは使用されていない様子
    - グループのファイル所有者や、継承機能などNTFS特有の機能も実現
    - 日本語関連はSamba 3と同様の設定
  - Winbind機能がデフォルトで有効
    - ただし既存のUNIXユーザとのマッピングはできない模様

# 参考: Samba 4のファイルサーバ機能

## ■ アクセス許可関連は、ADと高い互換性



グループが所有者

# 参考: Samba 4のファイルサーバ機能

## ■ Winbind機構がデフォルトで有効

□ Sambaで構築したADドメインのユーザは、原則すべてWinbind機構に格納される

■ /etc/passwdファイルには現れない

```
$ getent passwd
.....
bind:x:103:104::/var/cache/bind:/bin/false
ntp:x:104:105::/home/ntp:/bin/false
Administrator*:0:100::/home/%U:/bin/bash
Guest*:3000012:3000013::/home/%U:/bin/bash
krbtgt*:3000014:100::/home/%U:/bin/bash
dns-samba40-1*:3000015:100::/home/%U:/bin/bash
samba02*:3000021:100:Samba 02:/home/%U:/bin/bash
Samba01*:3000022:100:Samba 01:/home/%U:/bin/bash
```