Samba最新動向

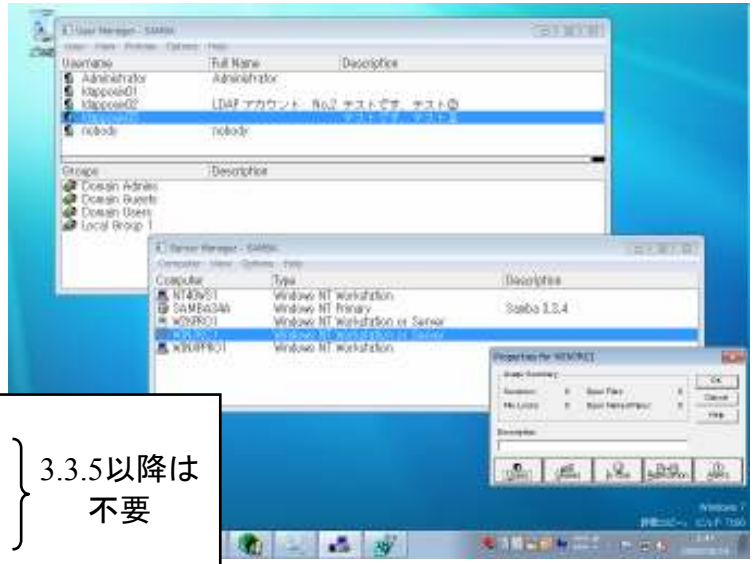
日本Sambaユーザ会

たかはし　もとのぶ（髙橋基信）

monyo@samba.gr.jp

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
- 懸案だった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



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

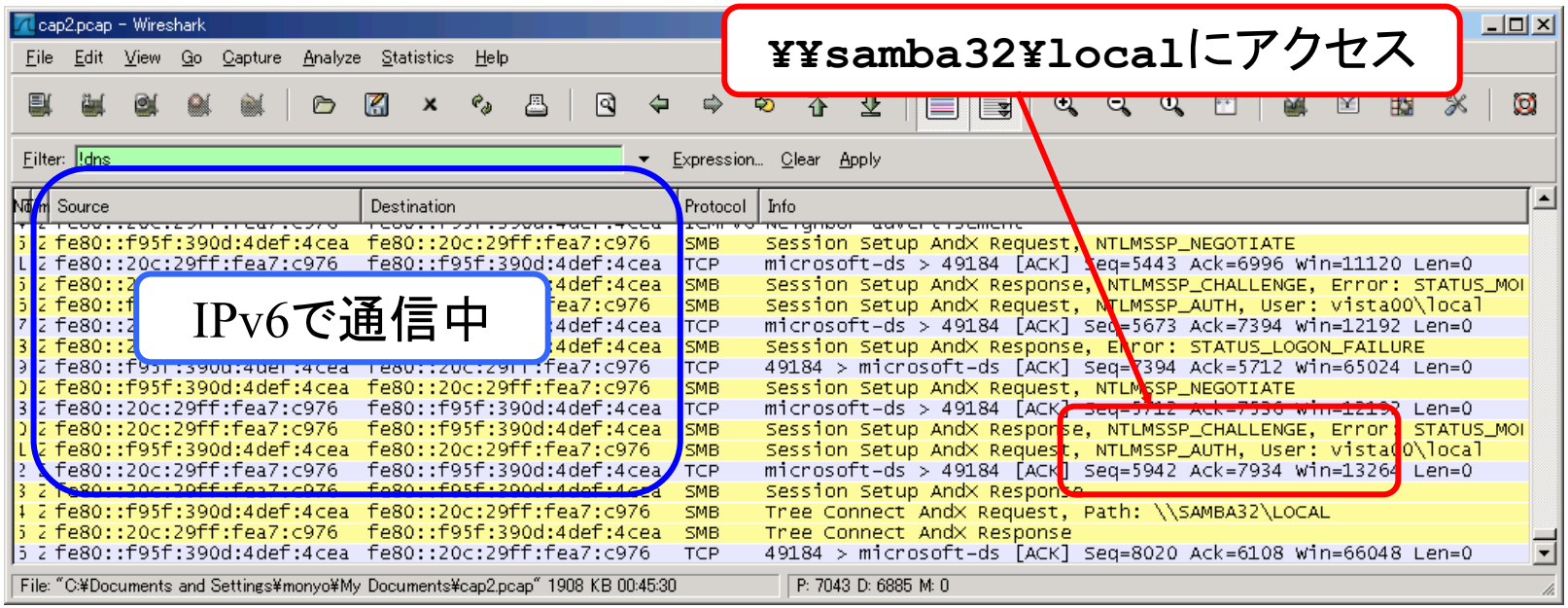
```
HKLM¥System¥CCS¥Services¥Netlogon¥Parameters
RequireStrongKey = 0
RequireSignOrSeal = 0

HKLM¥System¥CCS¥Services¥LanManWorkstation¥Parameters
DWORD(32bit)形式 DNSNameResolutionRequired = 0
DWORD(32bit)形式 DomainCompatibilityMode = 1
```

3.3.5以降は不要

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

IPv6対応　－　設定

- **OS**が対応していれば、自動的に有効
  - 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 3.2系列の新機能

- Active Directory関連の互換性強化
  - Windows Server 2008ドメインへの参加に対応
  - Windows Server 2008ドメインとの信頼関係確立に対応
  - Windows Server 2003のフォレスト間信頼に対応
  - Winbind機構がUPN名ログオンに対応
  - LDAP署名に対応
- セキュリティ強化
  - Secure by Default
  - CIFS独自のネットワーク暗号化に対応（Windowsは非対応）
- IPv6対応
  - Windows Vista/Server 2008からのIPv6アクセスに対応

Samba 3.2系列の新機能(2)

- クラスタ対応（実験的）
  - CTDBと連携したフェイルオーバークラスタ機能を実装
- NTFS対応の強化
  - 代替データストリームに対応
  - 長いファイルパス(内部的に1024バイト超）対応
    - Windowsの仕様上はパス名制限なし、ファイル名は最大255「文字」
- レジストリへの設定情報格納
  - ファイル編集ではなく、net conf コマンド、Windowsのレジストリツール（現在未対応）での設定変更が可能に
- 各種認証データベースの直接編集機能が追加
  - 新規に追加された`net sam`コマンドにより実現

Samba 3.3/3.4系列の新機能

- NTFS互換のACLサポート（3.3.0）
  - `vfs_acl_xttr/vfs_acl_tdb`モジュールによる。表示のみサポート
- IdMap機構のポリシー変更(3.3.0)
  - Samba 3.0.25以降の複雑な設定方法以外に、簡単な設定方法もサポート
- Winbind機構によるホームディレクトリ自動作成サポート(3.3.0)
- Windows 7ドメイン参加対応（3.2.12/3.3.2）
- デフォルトのpassdbバックエンドが`tdbsam`に変更(3.4.0)

Samba 3.5/3.6系列の新機能

- SMB2の実験的サポート(3.5.0)
  - `max protocol = smb2`
- Windows完全互換の時刻精度のサポート（3.5.0）
  SMB2の実用レベルのサポート（3.6.0）
- セキュリティ強化
  - デフォルトではNTLMv2のみ有効
- ldmap機構の改定（Allocバックエンドの廃止）

→ 機能的にはSamba 3.2系列の延長線上にある機能改修版

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

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

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
- 2011/04/23 samba-4.0.0alpha15

Samba 4系列の現状（1）

- DCとしては、完成に近づいている
  - DRSの完成度が一定レベルになればリリースか
  - 実運用している箇所もある（とアピールできるレベル）
    - Samba 4.0.0alphaをDCとして、ファイルサーバとしてはSamba 3系列を使用する形態

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

- ファイルサーバとしてはこれから
  - ブラウジング、印刷ほか、あまりケアされていない
    - ただし、Samba 3のコードを流用して一気に進むかも

Samba 4系列の現状(2)

- Samba 3.6の次にリリース？
  - 今年中にリリースか
    - 現在の最新バージョンはSamba 3.5.8
    - Samba 3.6はそろそろリリースされる予定
    - Samba 3.7系列がリリースされるかどうかは微妙
      - 「リリースする事態にならないことを願いたい」とのこと
    - 現在、9ヶ月ごとにバージョンアップするポリシー
  - 最近の議論を見ている限り、Samba 3.6リリース後は、Samba 4.0リリースに注力するとのこと
    - AD対応など、Samba 3系列ではそろそろ限界

Samba 4概要（1）

- プロセス名は「samba」
  - 従来のnmbd、smbd、winbinddすべてを統合
- Windowsサーバとして必要なサービスの大半を実装
  - 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の使用も考慮されているが、優先度は低い
  - 実装されていないサービス
    - DNS（BIND用の定義ファイルあり）、NTP

Samba 4概要(2)

- BINDとの連携
  - BIND 9.7.2rc1以降でKerberosを用いたAD互換のセキュアな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 9.8 と連携して、セキュリティで保護された動的更新を実現できるように動いている
- NTP
  - ntpd 4.2.6以降で--enable-ntp-signdオプションをつけてconfigureすることでSamba 4互換のNTPをサポート

Samba 4概要（3）

- 参考：Sambaがオープンしているポート
  - 従来のnmbd、smbd、winbinddすべてを統合

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のDCとSambaのDCの混在も可能
    - スキーマ
      - Windows Server 2008と同等のスキーマをサポート
    - 信頼関係、ドメインの機能レベル
    - サイト、FRS
      - 設定は可能。動作は未検証
  - Windows 7を完全サポート

Samba 4のDC機能(2)

- 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
    - 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、複数個所への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
  - Exchange Serverもサポート

Samba 4のDC機能（3）

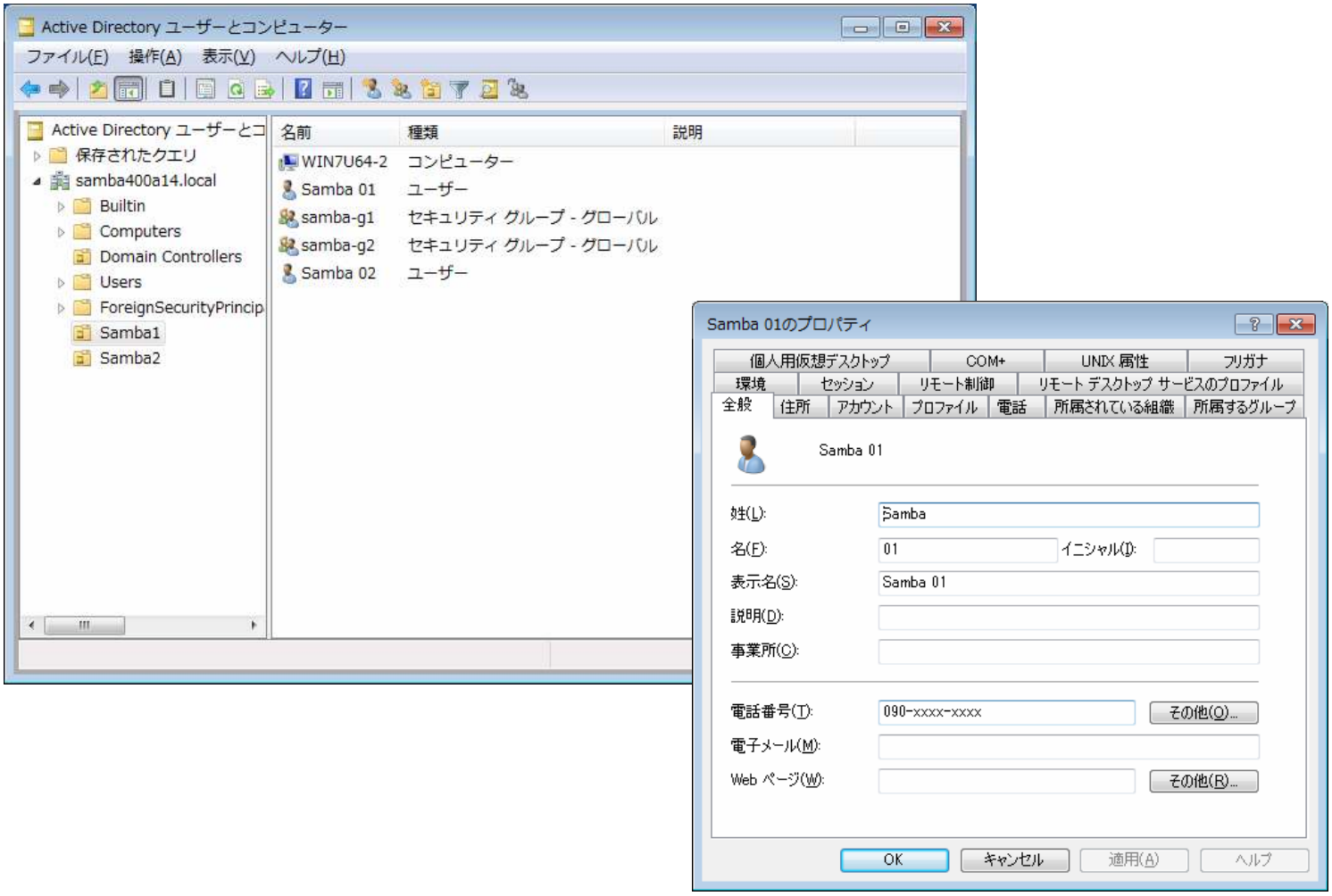
- Windows Server 2008とほぼ互換
  - UNIX上からの管理
    - samba-toolにより、ある程度の管理が可能
      - ただし、ADの管理自体は基本的にはGUIからの操作をお奨め

```
# 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 targer 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
```

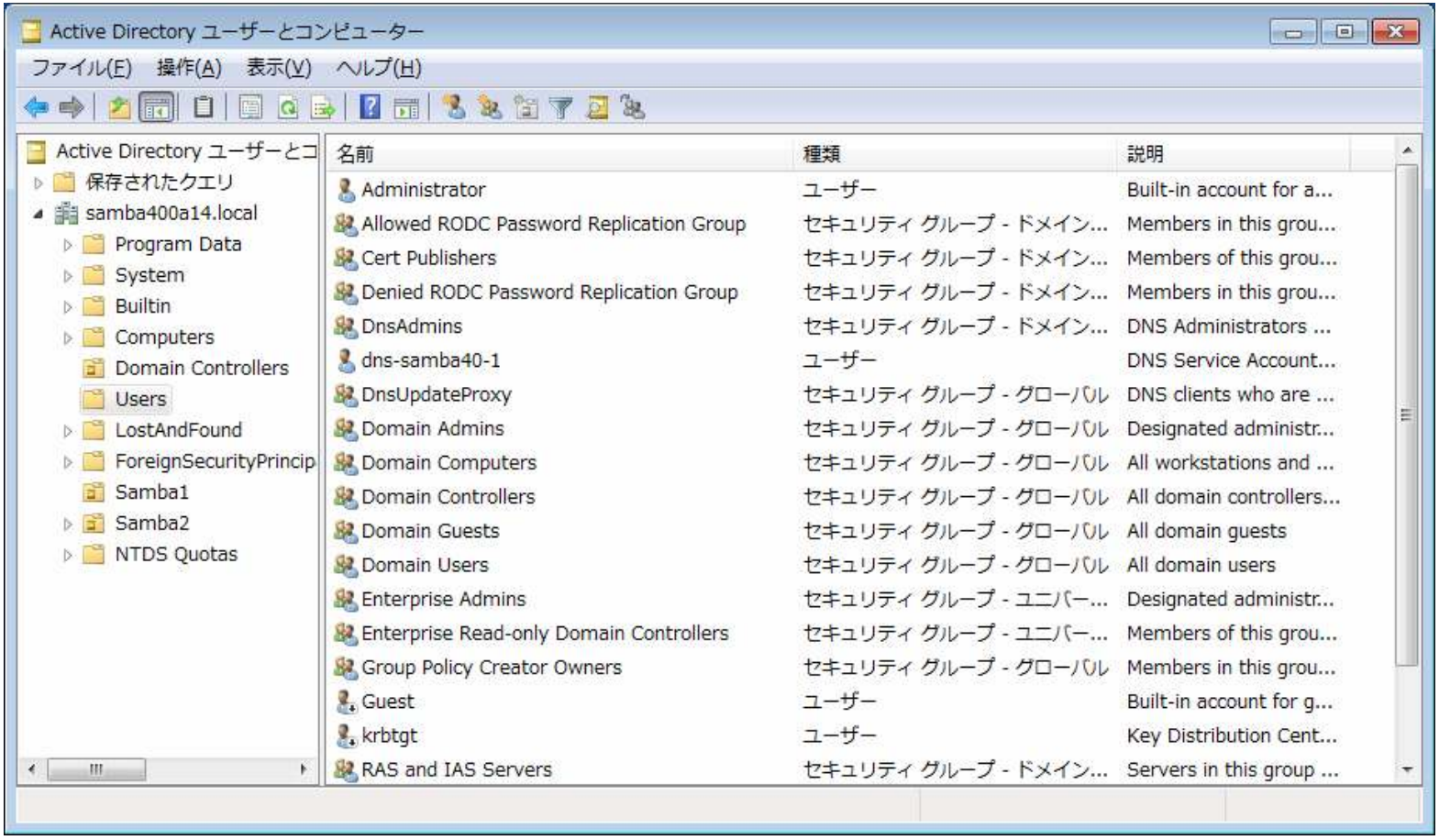
Samba 4のDC機能

- ADUCによる管理



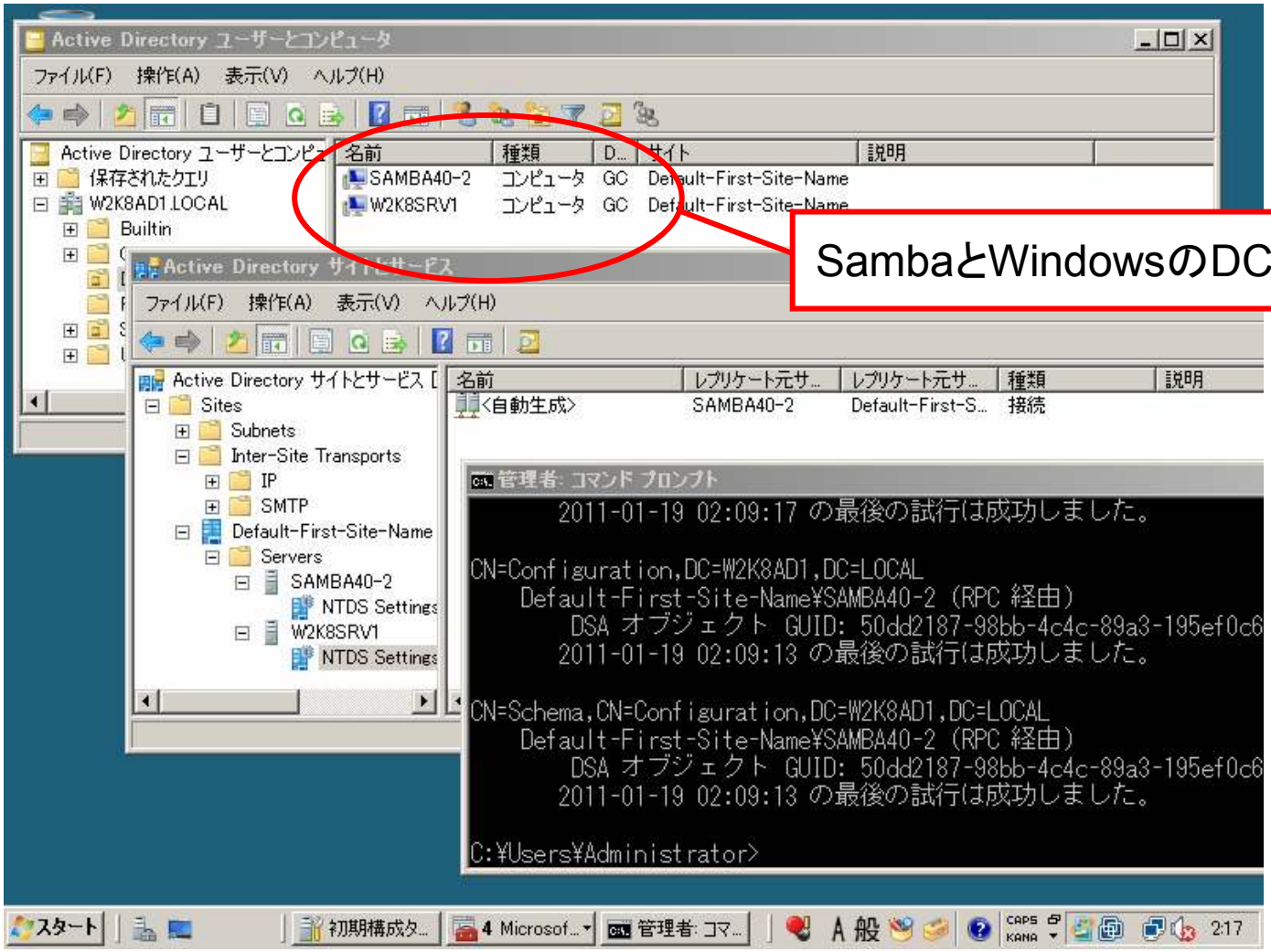
Samba 4のDC機能

- ADUCによる管理



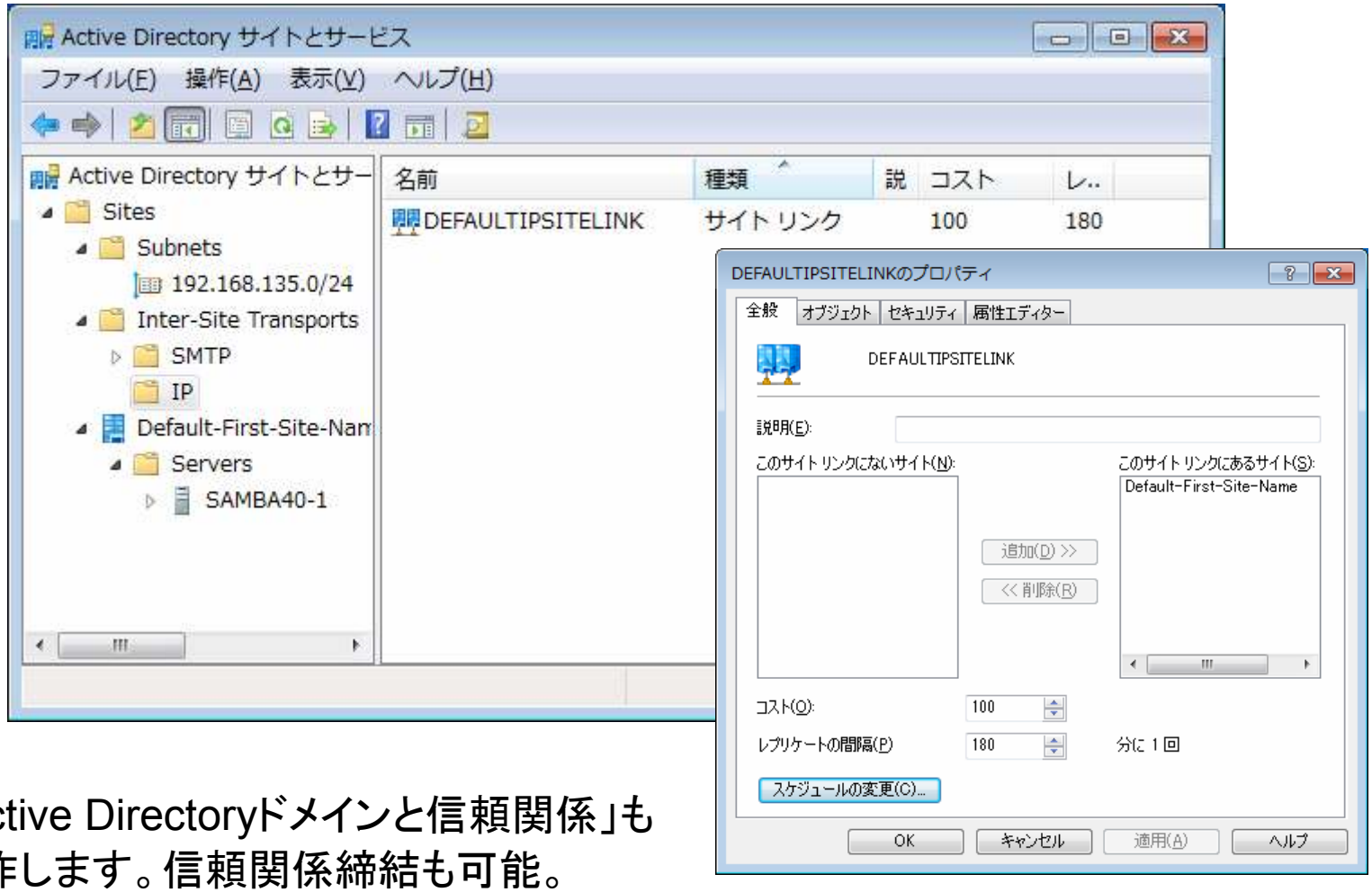
Samba 4のDC機能

- SambaのDCとWindowsのDCの混在



Samba 4のDC機能

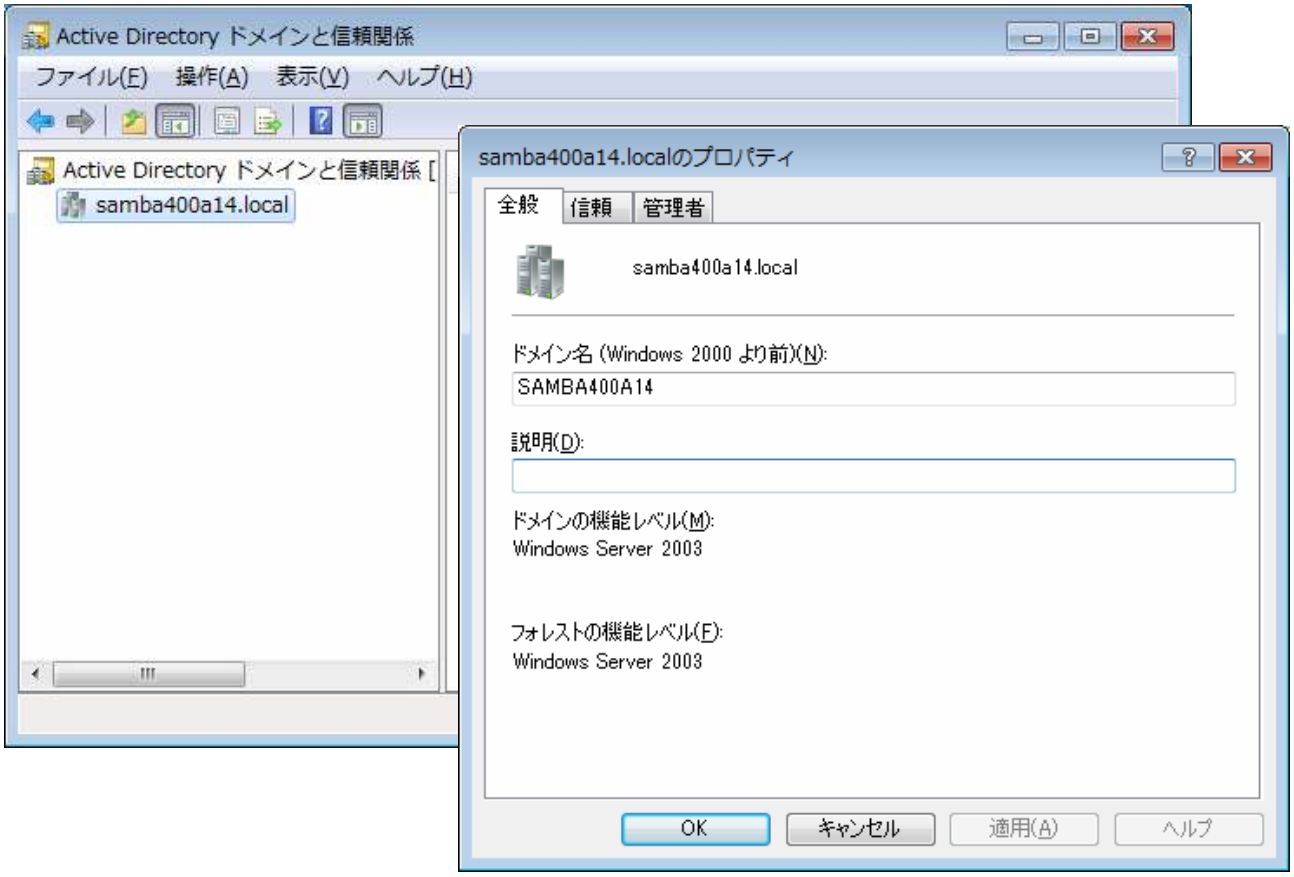
- Active Directoryサイトとサービスによる管理



「Active Directoryドメインと信頼関係」も動作します。信頼関係締結も可能。

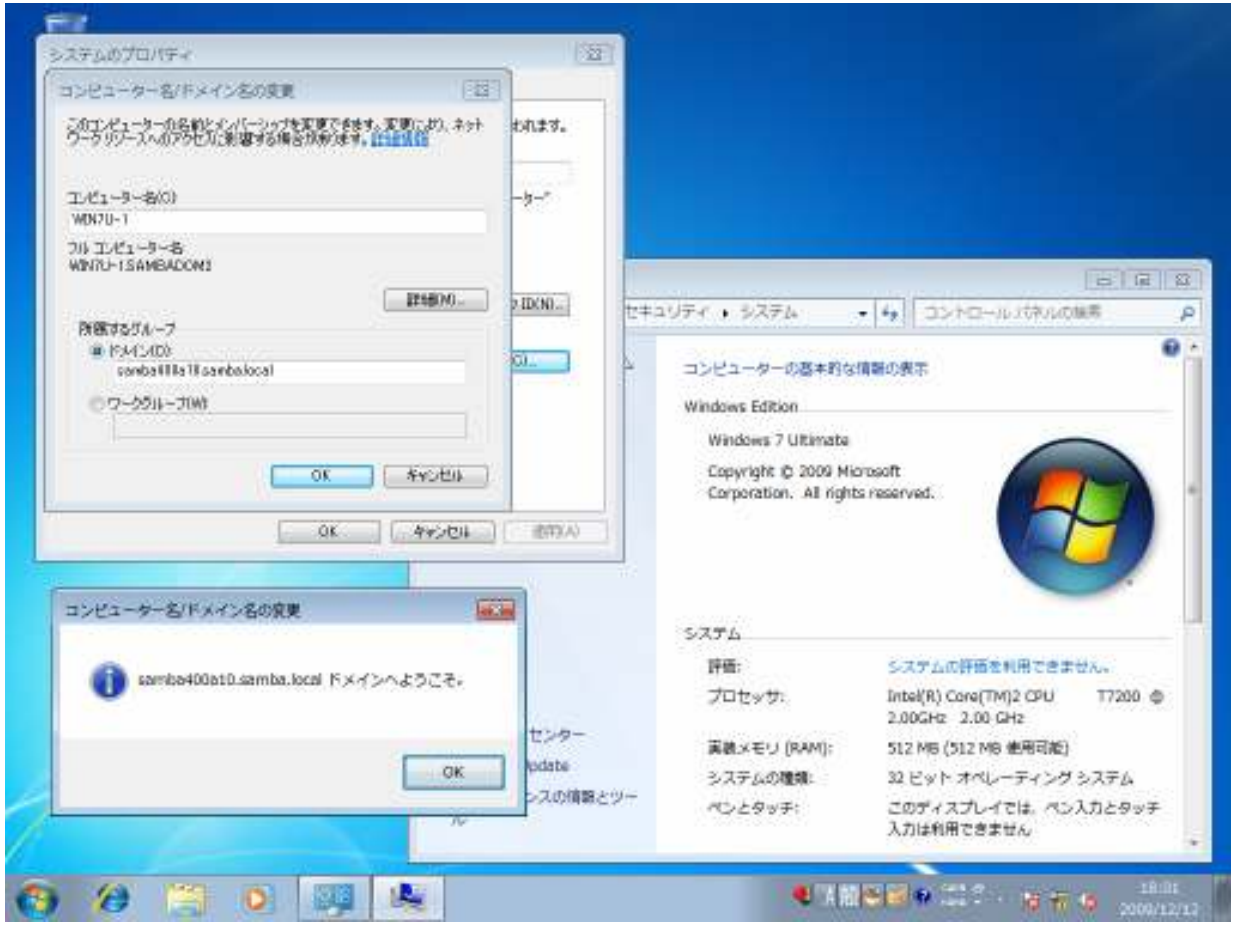
Samba 4のDC機能

- Active Directoryドメインと信頼関係による管理



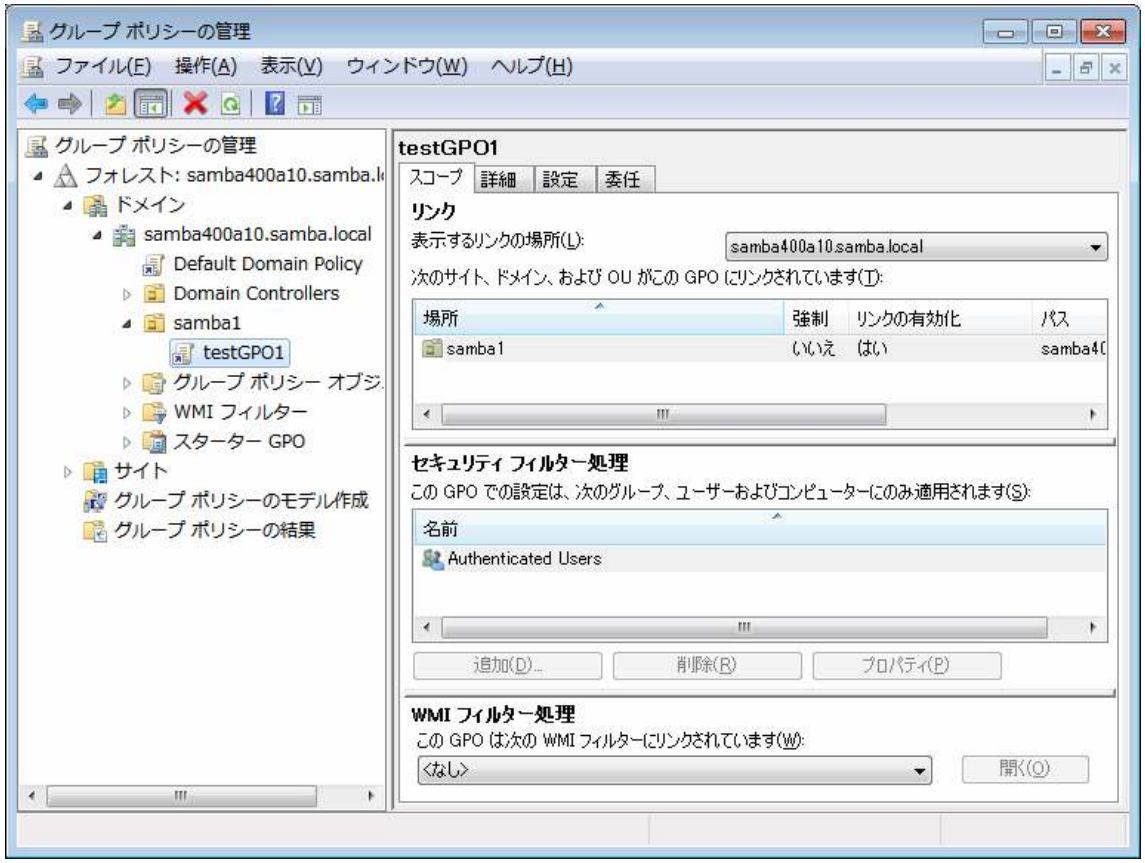
Samba 4のDC機能

- Windows 7も完全サポート



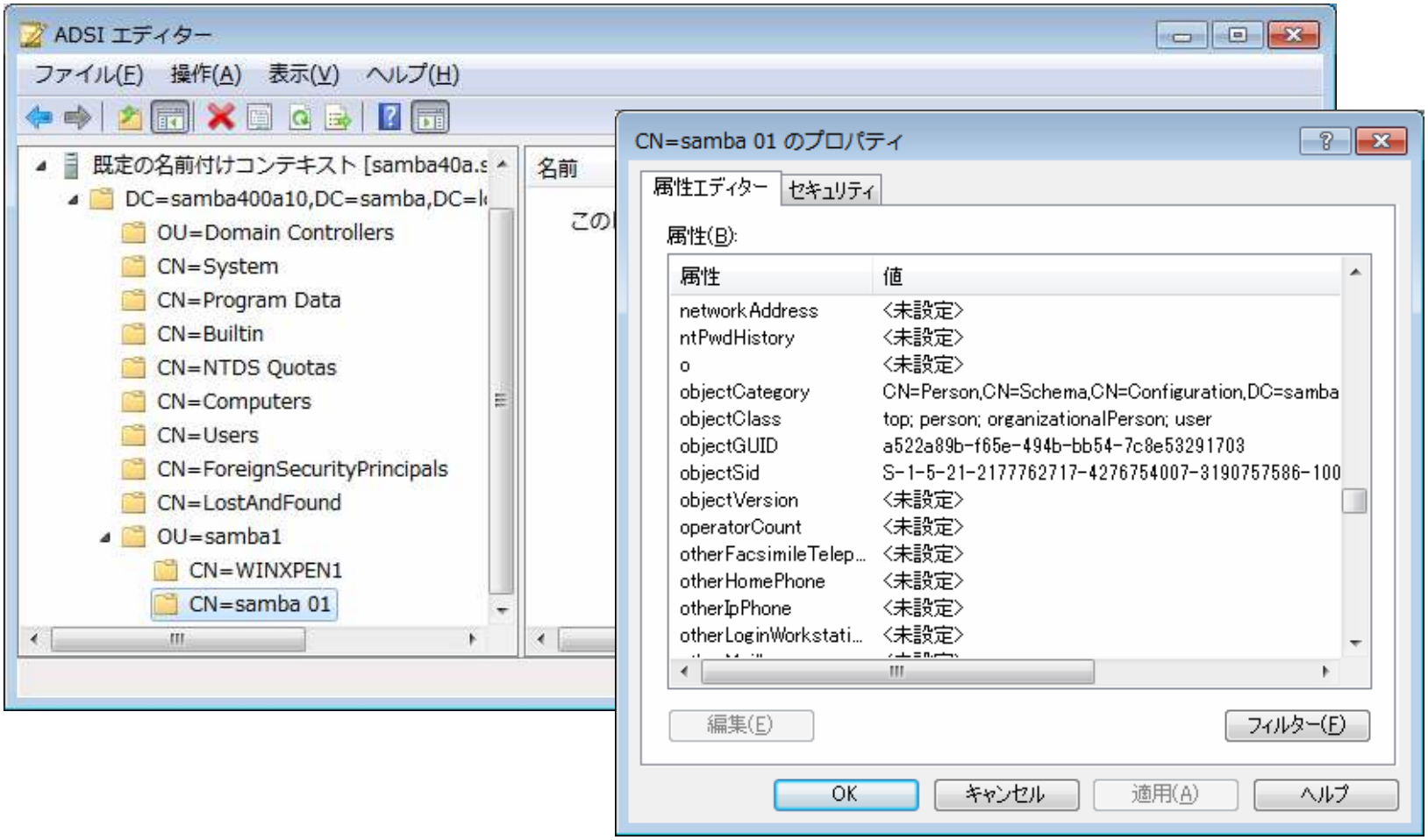
Samba 4のDC機能

- グループポリシーの管理によるGPO管理



Samba 4のDC機能

- ADSIエディタによる編集にも対応

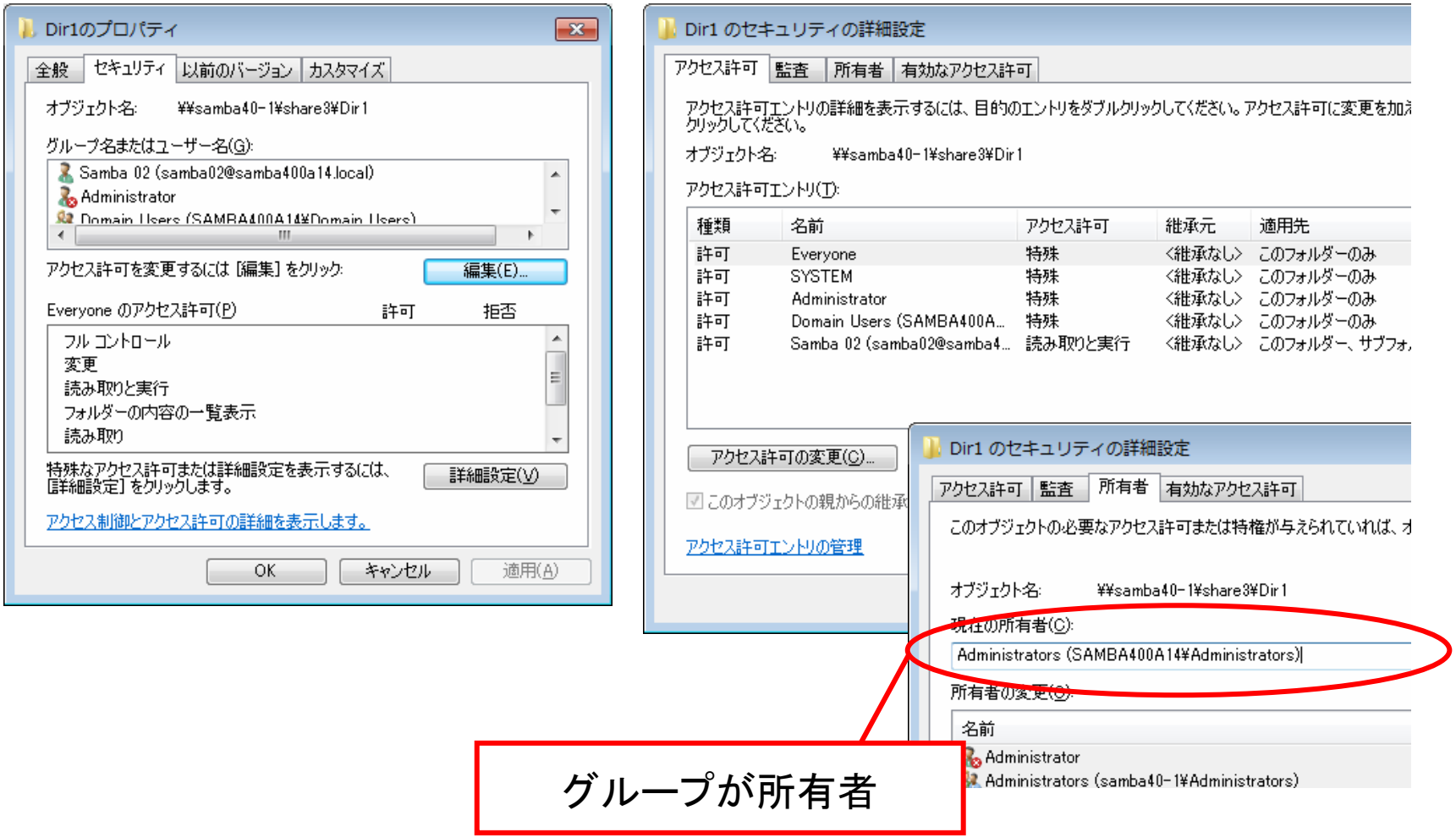


Samba 4のファイルサーバ機能

- 基本機能のWindows互換性はほぼ完全か
  - ACL、ファイル属性などは、すべて拡張属性に格納
    - グループのファイル所有者も実現
    - 日本語関連はSamba 3と同様の設定
  - 現状問題と思われる機能
    - 短いファイル名生成のロジックはSamba 3と同様（の問題点がある）
    - 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させている

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



Samba 4のファイルサーバ機能(2)

- 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
```

Samba 4のファイルサーバ機能(3)

- 高度な機能はこれから実装か
  - ホストベースDFS、ボリュームシャドウコピー、…
    - ドメインベースDFSがサポートされるかは微妙
- Samba 3を統合する形になるとのこと
  - 具体的にどうなるかは不明
- 現在サポートされていない機能
  - ファイルサーバ
    - まったく動作しないわけではないですが…
  - 印刷
  - ブラウジングなど