Samba3.0/LDAPによる ドメイン移行トラブル事例

オープンソース・ソリューション・テクノロジ株式会社
2006/10/19
技術部　コンサルタント　竹内　英雄

目次

- ユーザ、グループ、マシンアカウント情報の移行
  - NT、Active Direcotory(windows 2000,2003 server)からの移行
    - 既存ドメインのセキュリティ識別子(SID：Secutity Identifier)入手、設定
    - SambaをBDCとしてドメインへ参加
    - 既存ドメインの情報収集、確認
    - PDCから情報吸い上げ
    - 既存PDCを停止し、SambaをPDCへ昇格

ユーザ、グループ、マシンアカウント情報の移行(１)

- Windows2000、WindowsXPがドメインログオンしている NTドメインやActive Directory(以下AD)の情報 (ユーザ、グループ、マシンアカウント情報)を Samba3.0+OpenLDAPに移行してみよう。
  - AD
    - サーバ名:take-server.takeads2003.com ドメイン名 : takeads2003
  - NT
    - サーバ名:takeuchi-nt.takent.com ドメイン名 : takent
  - Samba
    - サーバ名:adtest.takeuads2003.com もしくは adtest.takent.com

既存ドメインのSID入手、設定(１)

- まず移行に必要なものを揃えていこう

SIDの入手には

rpcclient <ドメイン名> -U ユーザ名%パスワード -c 'lsaquery'
(Linuxにて実施)

getsid ￥￥サーバ名 ユーザ名 ￥￥サーバ名 ユーザ名
(Windowsにて実施)

既存ドメインのSID入手、設定（２）

- **表示結果**
  - rpcclientはSIDのみが表示
  - getsidは2ユーザ分のSIDが表示
    - ユーザのSID比較が目的の為
    - 相対識別子（RID：Relative Identifier)付き
- Windowsで使用するgetsidコマンドは Resource Kit Tools に収録

既存ドメインのSID入手、設定（３）

- 取得したSIDをSambaに設定

```
net setlocalsid S-1-5-21-xxxx-xxxx-xxxx
```

- 設定したSIDの確認

```
net getlocalsid
net getlocalsid ドメイン名
```

SambaをBDCとしてドメインへ参加(１)

BDCとしてドメインへ参加させるには

net rpc join -S <PDCのマシン名> -w <ドメイン名>-U ユーザ名%パスワード BDC
(Linuxにて実施)

SambaをBDCとしてドメインへ参加（２）

- net rpc jonの実行
  - コマンドラインに「Joined domain ドメイン名」表示
- 移行前はBDCとしてドメインに登録
  - net rpc joinによってPDCへ事前追加は必要なし
  - smb.confもBDC用としておく（抜粋）
    - domain master = no
    - os level = 64より低く（通常BDCは32）
    - wins server = PDCのIPアドレス
- Windows側で名前が追加されていることを確認

既存ドメインの情報収集、確認(１)

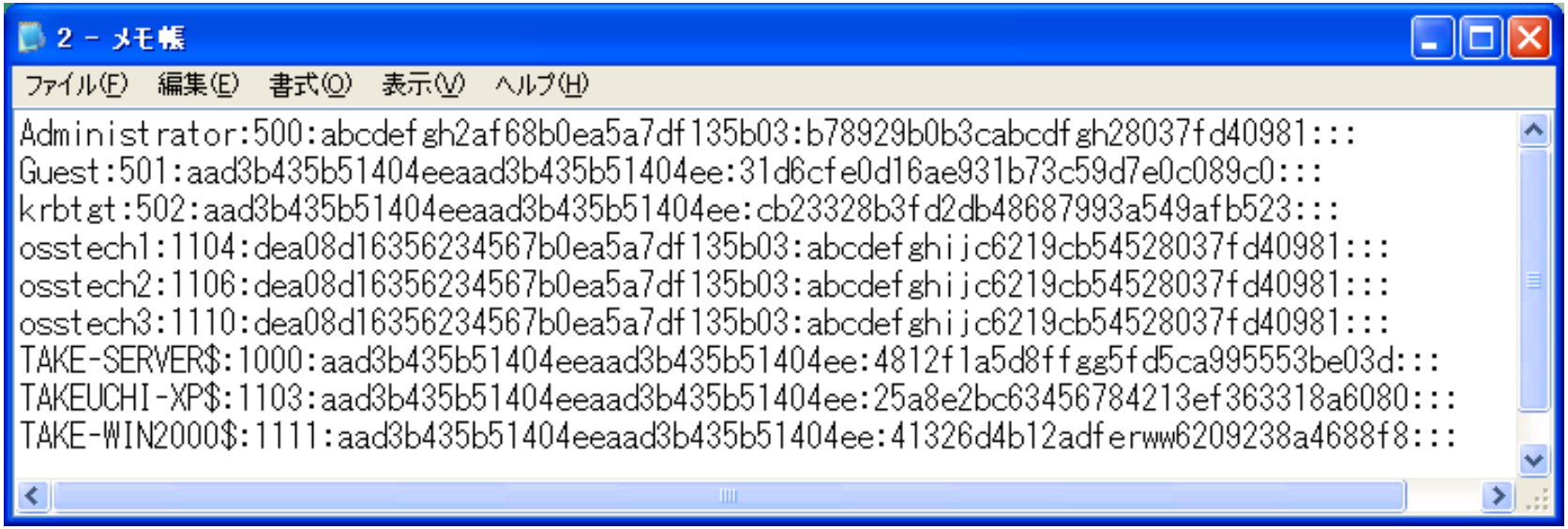
情報収集するには

ユーザ、マシンアカウント情報
PWDUMP2もしくはPWDUMP3の情報
(Windowsにて実施)

グループ情報
net group、net localgroup
(Windowsにて実施)

既存ドメインの情報収集、確認（２）

- pwdump2とpwdump3の違い
  - pwdump3はマシンアカウントのLANMANハッシュパスワードがない
    - 必要ない。pwdump2の結果は統一でsetされているだけ

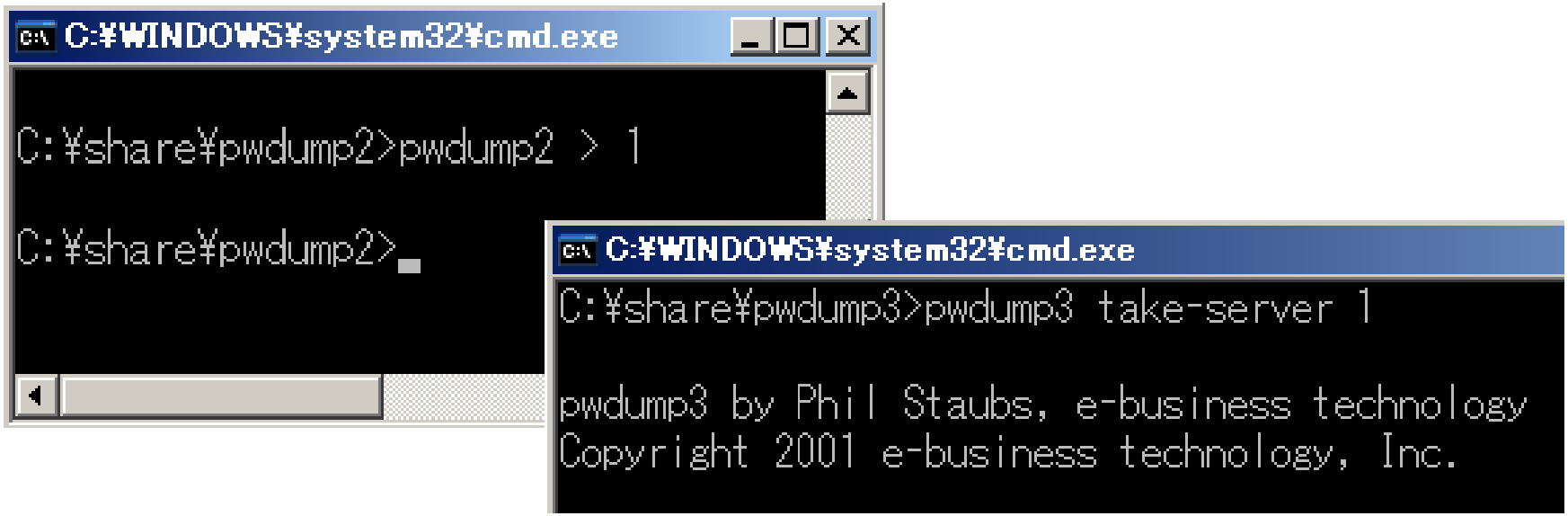


既存ドメインの情報収集、確認（３）

- pwdumpの結果
  - ハッシュされているとはいえ、パスワード情報そのもの
    - 流出すれば問題
  - 確認するうえでは必須なツール
- 取り扱いに注意すること
- 先ほどのパスワードは加工しています。

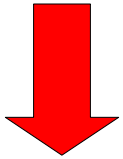
既存ドメインの情報収集、確認(３-１)

- pwdump2 (http://www.bindview.com/Services/razor/Utilities/Windows/pwdump2_readme.cfm)
- pwdump3 (http://packetstormsecurity.org/Crackers/NT/pwdump3.zip)



既存ドメインの情報収集、確認(４)

- 名前(ユーザ、グループ、マシンアカウント)
  - 全角英数字、半角カナの名前を使用
  - （　括弧を使用しているグループ名



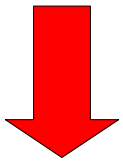
トラブル発生！！

移行時に必ず失敗する(処理は続く)
使用しない名前に変更しておく

上記は事例を元にしており、これ以外にも制約がある可能性

既存ドメインの情報収集、確認(５)

- ローカルグループ
- グループのネスト



トラブル発生！！

ローカルグループ名の移行は可能だがメンバーが移行されない
グローバルグループの使用へ変更しておく

現在のSambaではグループのネストが正常に動作しない

PDCから情報吸い上げ(１)

- 情報が揃い、不安材料を除いたら実際に移行開始

PDCより情報を吸い上げるには

net rpc vampire -S <PDCのマシン名> -U Administrator%パスワード
(Linuxにて実施)

PDCから情報吸い上げ（２）

- net rpc vampire
  - その名の通り、情報を吸い上げる
    - ユーザ名、パスワード、グローバルグループ、マシンアカウント、マシンアカウントパスワード等
- 表示されるメッセージに注意
  - 既に登録済みのアカウントへのメッセージ
  - sambaSamAccountの登録失敗
    - ユーザ登録が多い場合などまれに発生する
    - posixAccount情報は移行される
    - 発生したユーザはsambaへアクセスができない

PDCから情報吸い上げ（３）

- 必ずLDIF(LDAP Data Interchange Format)を確認
  - マシンアカウントのパスワードがpwdumpの結果と違う
    - ドメイン再参加か？
  - SambaSamAccount関係が移行されていない
    - パスワードは再設定か？

PWDUMP2もしくはPWDUMP3の情報を
使用する

PDCから情報吸い上げ（４）

- マシンアカウントのパスワードが違う場合
  - 下記のような記述をしたファイルを用意
    - パスワードの部分はpwdumpの結果より

```
dn: uid=TAKEUCHI-XP$,ou=Computers,dc=takeads2003,dc=com
sambaNTPassword: 25A8E2BC63456784213EF363318A6080
```

```
ldapmodify -x -W -D [bind DN] -f ファイル名
```

PDCから情報吸い上げ（５）

- SambaSamAccountの登録失敗
  - ユーザ登録が以下のように不足している場合

PDCから情報吸い上げ（６）

- SambaSamAccountの追加

```
smbldap-usermod -a osstech1
```

- ダミーパスワードの設定

```
smbldap-passwd osstech1
```

PDCから情報吸い上げ（７）

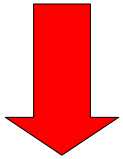
- pwdumpの結果使用
  - 下記のようなファイルを用意
    - パスワード、SIDの1104はpwdumpの結果より

```
dn: uid=osstech1,ou=Users,dc=takeads2003,dc=com
sambaSID: S-1-5-21-2423074760-413414226-2072458839-1104
sambaLMPassword: DEA08D16356234567B0EA5A7DF135B03
sambaNTPassword: ABCDEFGHIJC6219CB54528037FD40981
```

ldapmodify -x -W -D [bind DN] -f ファイル名

PDCから情報吸い上げ（８）

- SambaSamAccountの追加をした場合、
  必ずダミーパスワードの設定を忘れない



トラブル発生！！

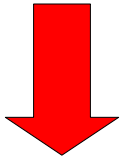
sambaPwdLastSet: 0の場合
ログインが拒否される

既存PDCを停止し、SambaをPDCへ昇格(１)

- 移行が終了したら、PDCを停止し、BDCをPDCへ昇格
  - smb.confもPDC用としておく
    - domain master = yes
    - os level = 64
    - wins support = yes
- sambaを再起動後、ドメインログオンを実施してみよう

既存PDCを停止し、SambaをPDCへ昇格(２)

- smb.confのnetbios nameを変更
- /etc/samba/secrets.tdbの削除

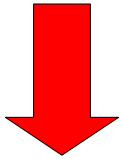


トラブル発生！！

必ずSIDをset し直す必要がある
/etc/samba/secrets.tdbにnetbios名と共にSID値がsetされている

既存PDCを停止し、SambaをPDCへ昇格（３）

- **再起動後もドメインログオンに問題なし**
  - NTドメインへドメインログオンしていたWindows2000、XP
  - ADへドメインログオンしていたWindows2000、XP



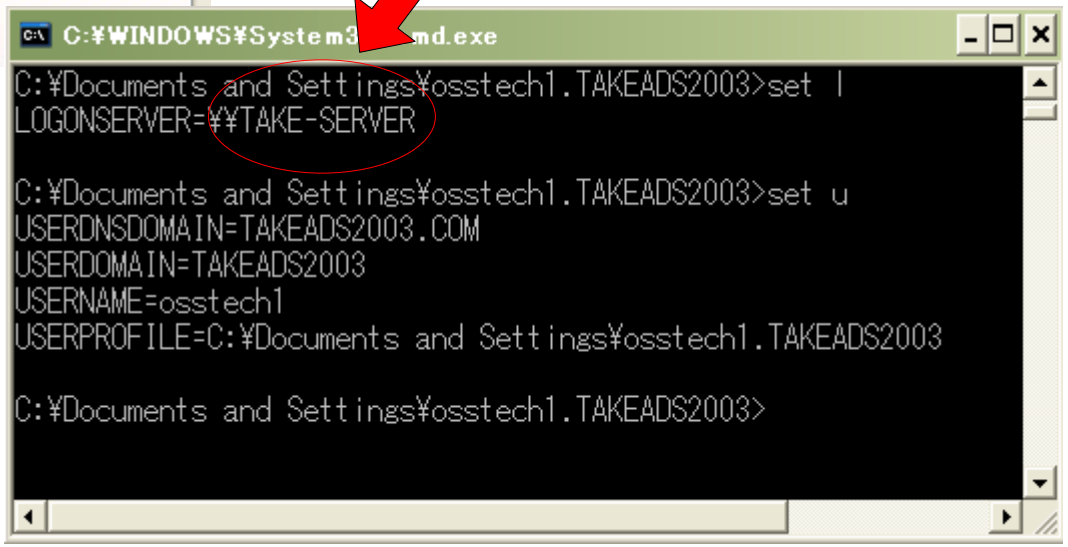
トラブル発生！！

何回か実行するとADへドメインログオンしていた
Windows XPがログインできない

既存PDCを停止し、SambaをPDCへ昇格(４)

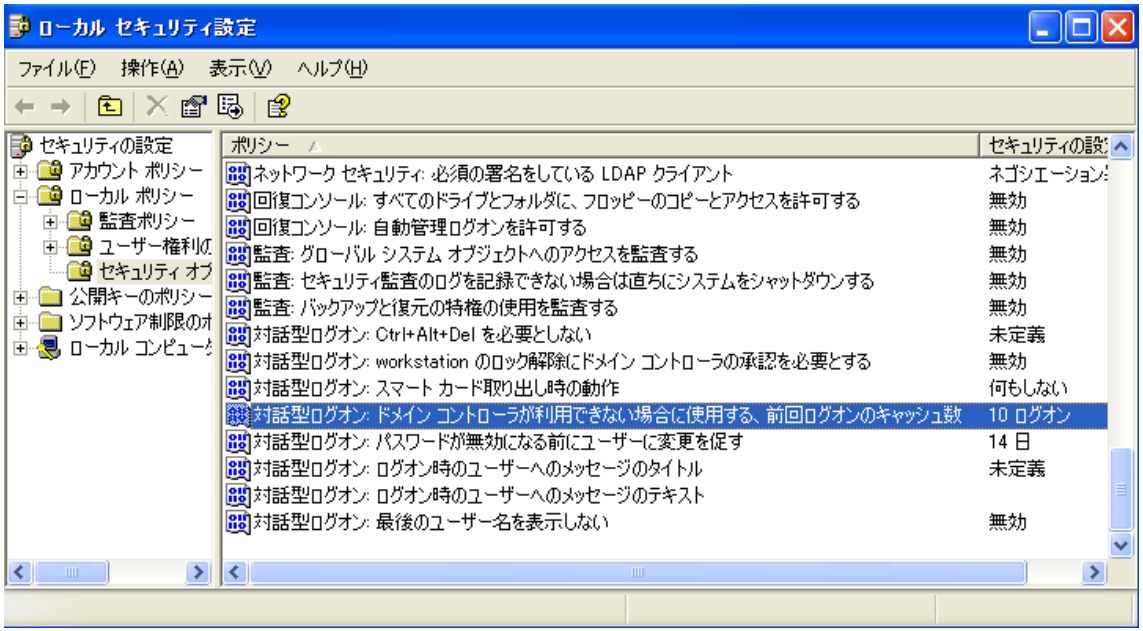
- Windowsにて確認

注目



既存PDCを停止し、SambaをPDCへ昇格(５)

- setコマンドのLOGONSERVERがADのサーバ名のままに
  - 以下のキャッシュの設定が有効に
  - ADは停止していてもLOGONSERVERとして残る

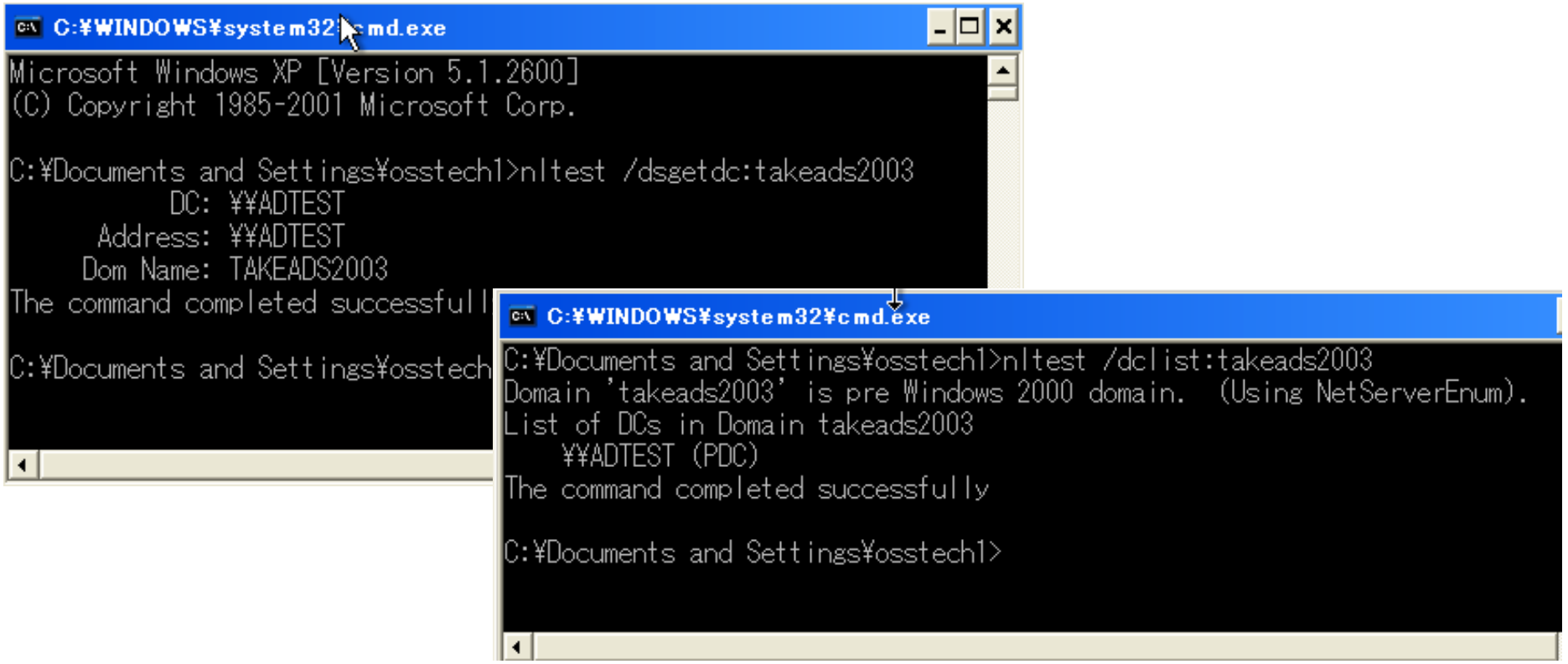


既存PDCを停止し、SambaをPDCへ昇格(６)

- 試しにXPで一度もログインしていないユーザでログイン

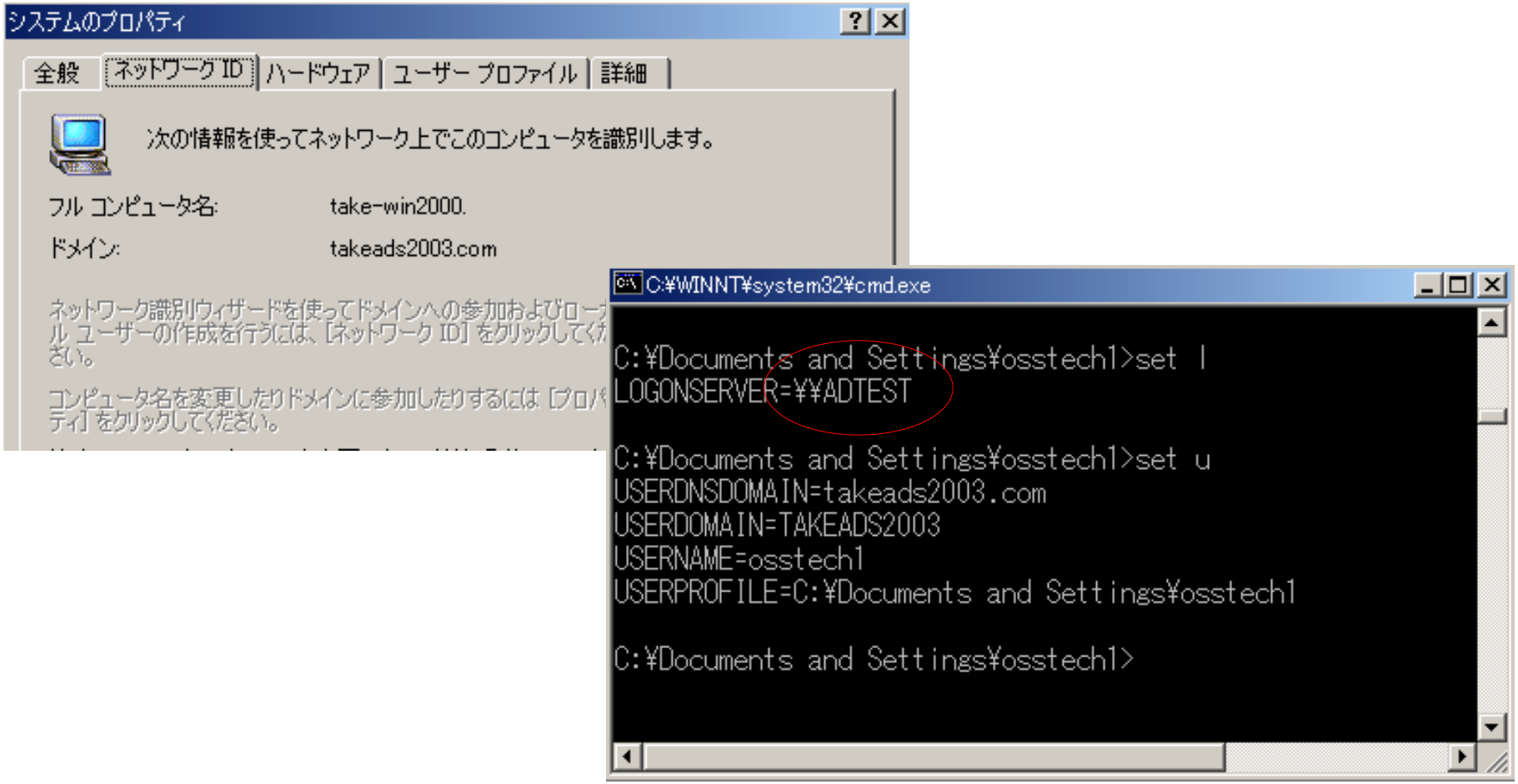
既存PDCを停止し、SambaをPDCへ昇格(７)

- 以下のコマンドを実行
  - ドメインとしては特に問題なし
    （しかし依然 LOGONSERVERの値は変わらず）



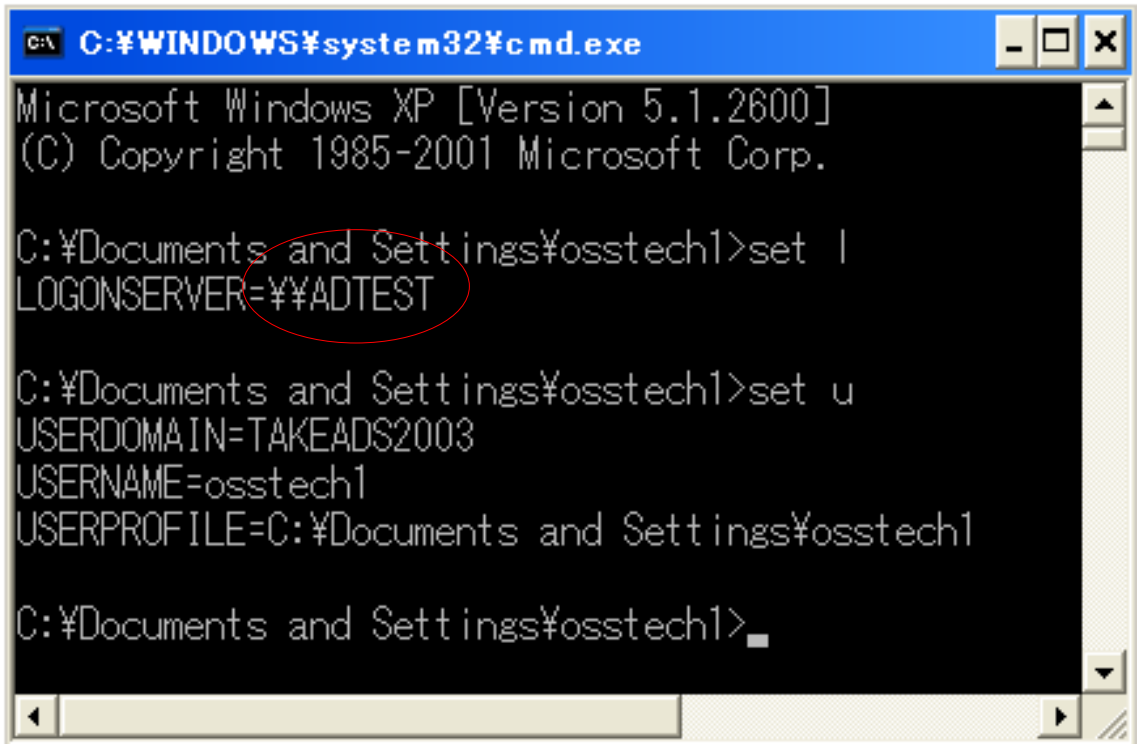
既存PDCを停止し、SambaをPDCへ昇格(８)

- 一緒に移行されたWindows2000は平気か？？



既存PDCを停止し、SambaをPDCへ昇格(９)

- Sambaサーバ側のマシンアカウントはそのまま
  - ドメインの再参加を実施
    - パスワードやパスワードの期限が変更される程度で特に変わったエントリが追加されるわけでもない



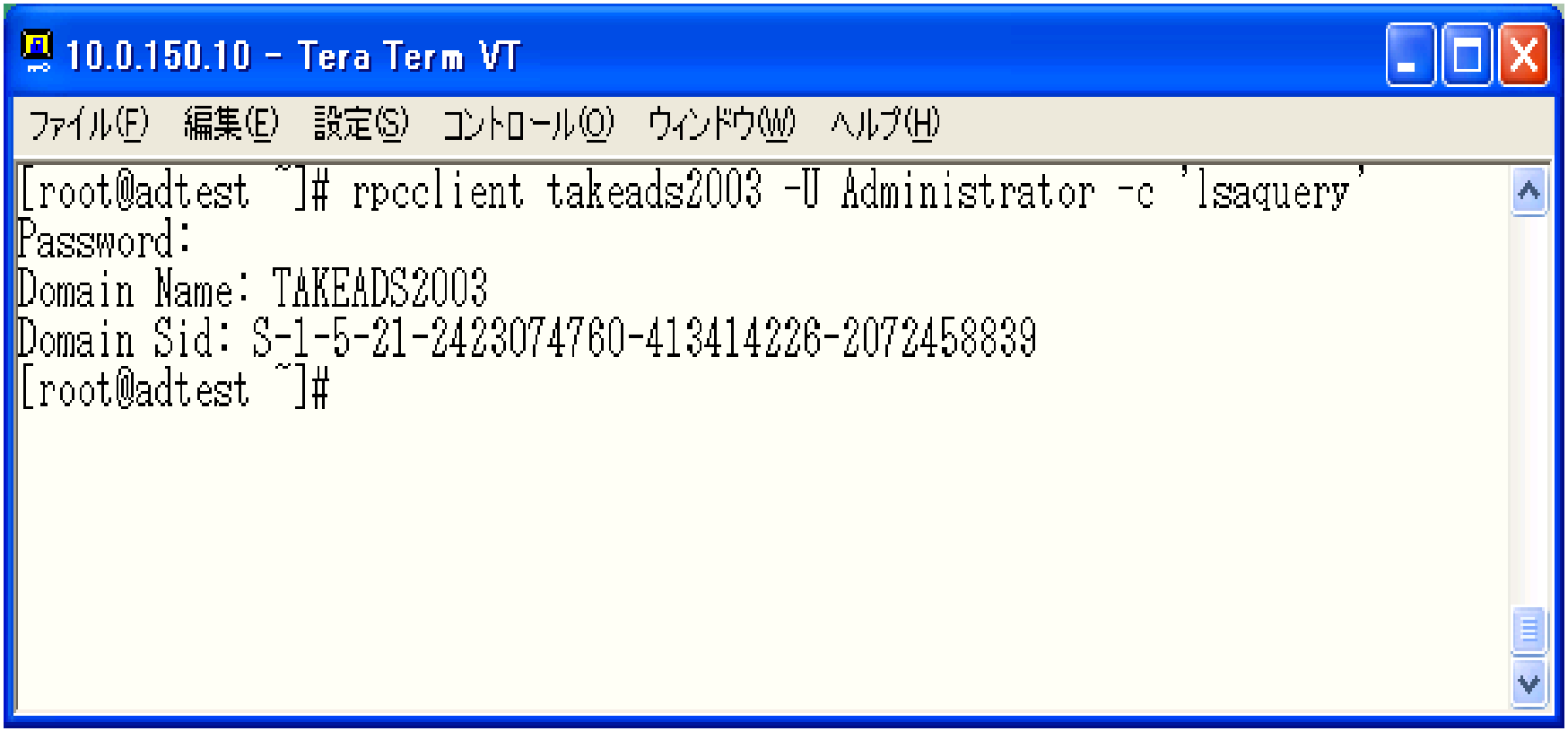
既存PDCを停止し、SambaをPDCへ昇格(１０)

- ADにWindows Xpをドメインログオンさせている
  - ドメインへの再参加が必須
    - SID(RIDを含む)さえ同じにしておけば環境は変わらない
    - Windows2000では平気の為、XP内の情報をクリアできれば解決か
      - あくまで憶測です、まだクリアできる方法は発見できていません
- NT場合はWindows2000、XPどちらでも問題なし
- 移行時にはlogonスクリプトを動作させておくと良い
  - ユーザが使用するlogonスクリプト名はLDAPへ移行される
  - ファイルはsambaのNETLOGON共有へ手動で保存

```
net use x: \\サーバ名\共有名
pause
```

既存ドメインのSID入手、設定(参考資料１)

- Linuxからの実行結果

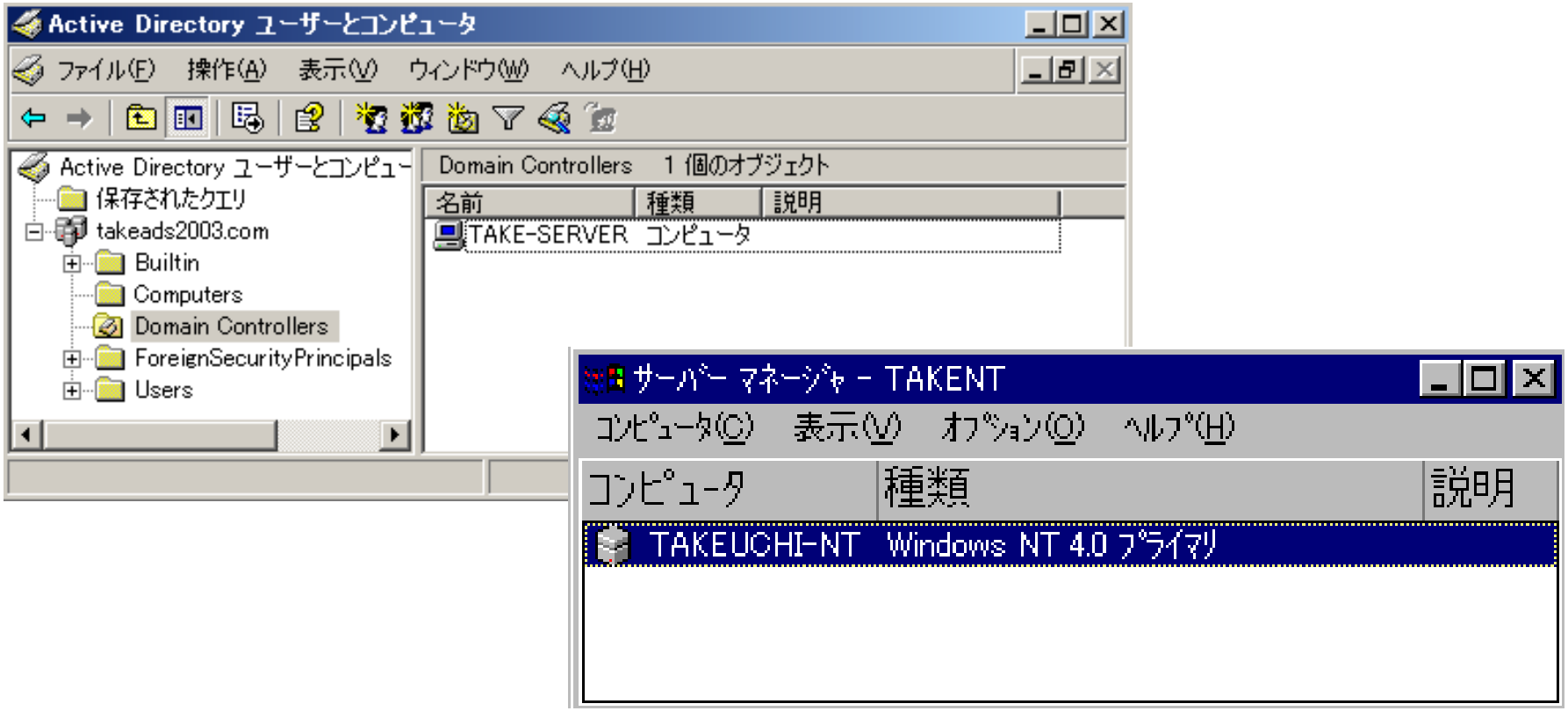


既存ドメインのSID入手、設定(参考資料2)

- Windowsからの実行結果

SambaをBDCとしてドメインへ参加(参考資料1)

- 参加前の状態



SambaをBDCとしてドメインへ参加(参考資料2)

- **参加後の状態:**(net rpc join**実行後**)