Samba3.0/4.0ロードマップ
と
Windows Vistaの対応状況

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
技術取締役　武田　保真

Samba3.0系の過去と未来

- 2003年9月25日 samba-3.0.0リリース
- 2004年8月19日 samba-3.0.6リリース
  - LDAP schema拡張による非互換発生。
- 2005年4月14日 samba-3.0.14aリリース
- 2005年8月19日 samba-3.0.20リリース
  - 3.0.14aからコードの大幅な変更を含んだため、途中のバージョンを抜かして、3.0.20としてリリース。
- 2006年9月1日 samba-3.0.23cリリース
  - 現在の最新版

最近のSambaの修正

- 2006年3月30日 samba-3.0.22
  - [セキュリティ] CAN-2006-1059
  - ログレベル5以上で、マシンアカウントのパスワードがwinbinddのログに含まれる脆弱性を修正(脆弱性の影響範囲: samba-3.0.21～3.0.21c)
- 2006年7月10日 samba-3.0.23
  - Windows Server 2003 R2でサポートされたRFC2307のスキーマオブジェクトの対応
  - winbinddにofflineモードを追加
  - root権限を必要としない共有管理ツールの追加
  - 対応づけのできないユーザ、グループへの対処の追加
- 2006年7月21日 samba-3.0.23a
  - "winbind use default domain = yes"の時のドメイン名の処理の不具合修正
  - pam_winbindモジュールの引数処理の修正
  - winbinddを利用していないメンバーサーバ上でのローカルユーザ作成時の不具合修正
  - ACLにユーザがグループを追加する際の不具合修正
  - "kernel oplocks = yes"の時の不具合修正

最近のSambaの修正(2)

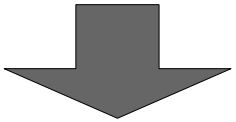
- 2006年8月8日 samba-3.0.23b
  - メンバーサーバにおけるsmb.confへのドメインアカウント名を利用する場合の制約の変更
  - ドメインコントローラに不正なIPアドレスが含まれている場合に、net ads joinコマンドが失敗する不具合の修正
  - SMB署名の不具合の修正
  - smbpasswdバックエンドでSambaをドメイン運用したときに、ドメインに参加できない不具合の修正
- 2006年9月1日 samba-3.0.23c
  - Active Directoryのドメインポリシーでパスワードを無期限に設定した場合の不具合の修正
  - 「valid users」パラメータなどを利用する際の不具合の修正

Samba3.0.24のTodoと今後

- MS-RPCの処理を、Samba4のライブラリ部分から移植
- winbinddのofflineモードの修正
- winbinddにActive Directoryのサイト機能追加
- ドメイン参加時にDDNSとの連携

参照: http://wiki.samba.org/index.php/TODOs_for_3.0.24

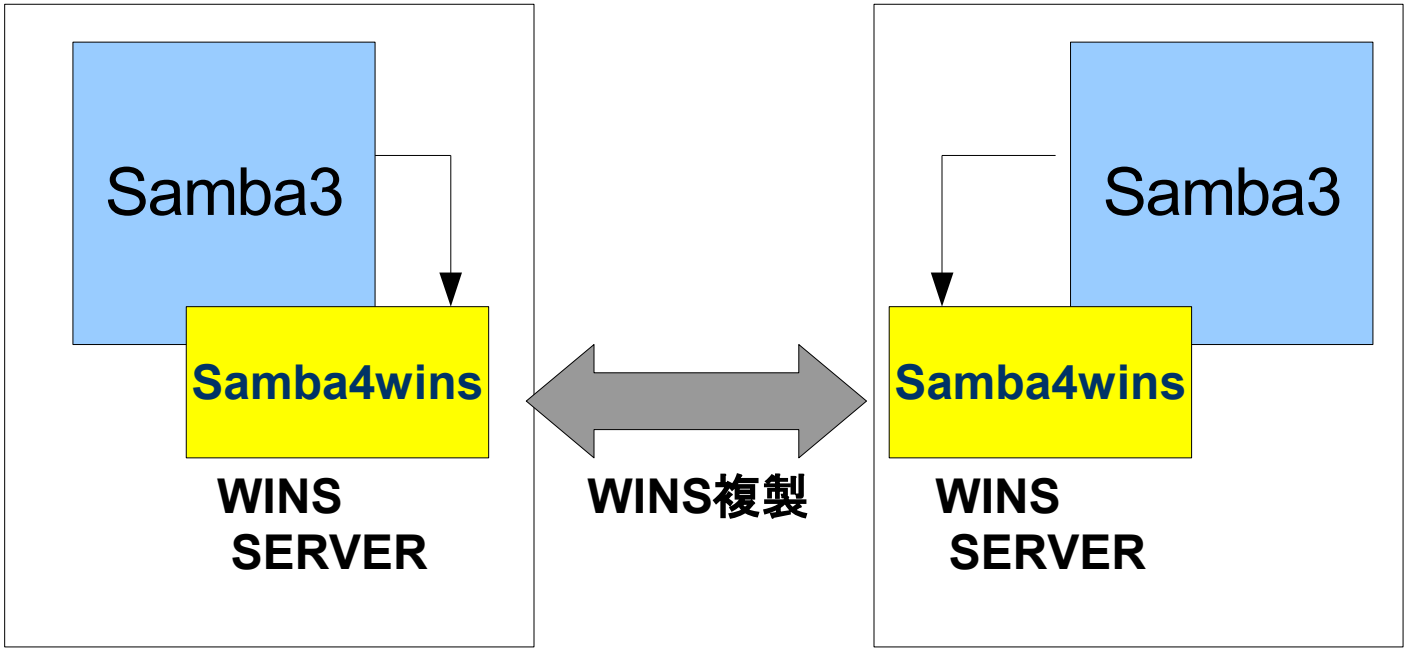
開発・修正対象のほとんどがwinbind関連機能(AD連携)



Samba3.0で提供のNTドメイン互換機能はほぼ完成形

Samba4winsの紹介

- Samba4のコードを利用したSamba3用のWINS複製サーバ機能
- Samba 3.0.20以降で利用可能



Samba4

- Samba4**の開発目標**
- Samba4**のロードマップ**
- Samba4**の構成**
- **体験**!! Samba4 (Technology Preview)

Samba4の開発目標

- Sambaによる Active Directory サーバの実現
- 従来のSambaの実装の大幅な書き直し

Samba4で実現されている、実現予定の機能など

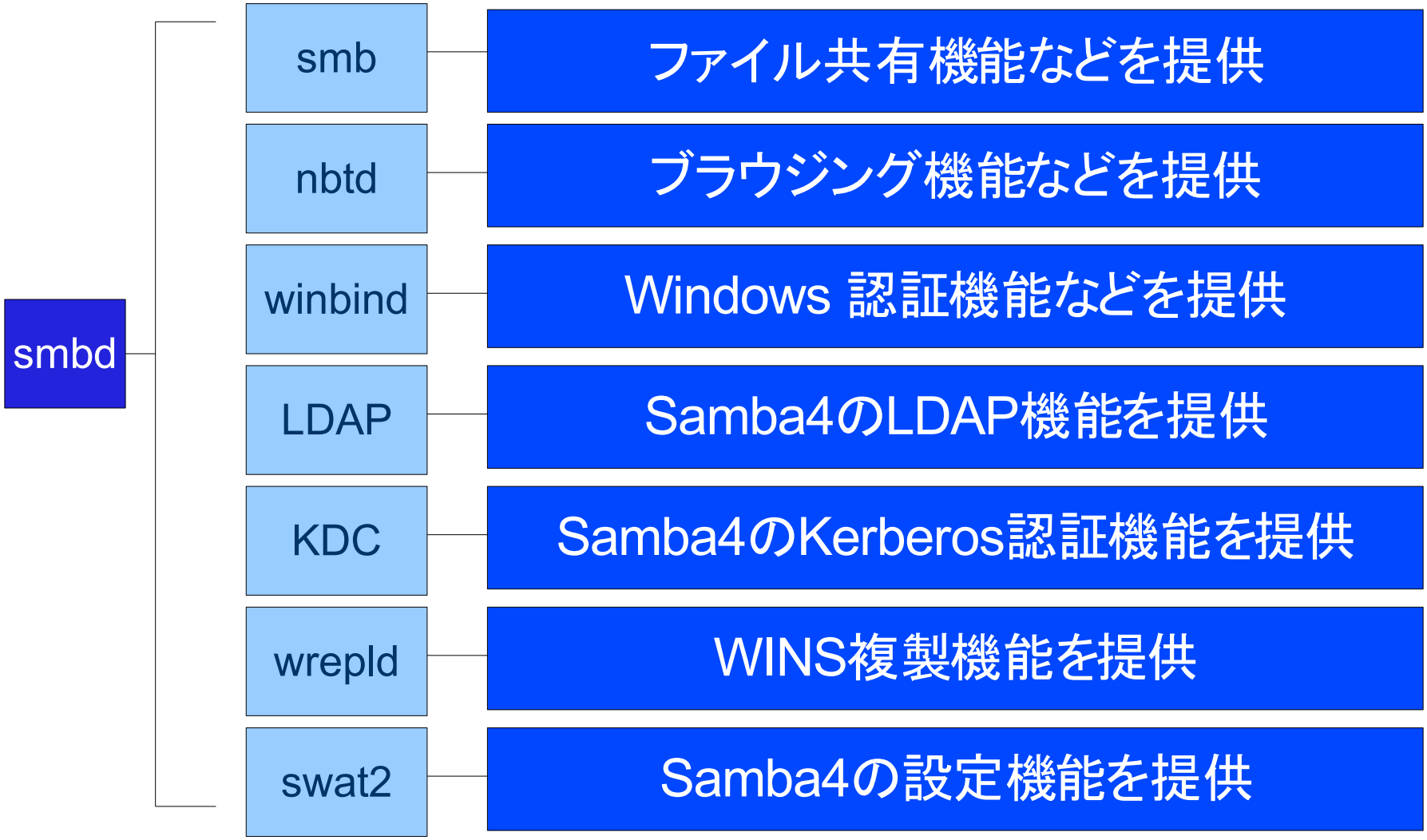
- Active Directoryのドメインコントローラ機能
- NTFSと同等のファイル共有機能
- Active Directoryと同等のLDAPサーバ機能
- Kerberosサーバ機能の組み込み
- 柔軟なプロセスモデル
- SWAT2

Samba4のロードマップ

- 2006年 1月 24日
  - samba-4.0.0tp1 (Technology Preview1)リリース
- 2006年 3月 22日
  - samba-4.0.0tp2 (Technology Preview2)リリース
- 2006年 10月10日現在
  - samba-4.0.0tp3-xxxx SVN上で開発中
- リリースまでに
  - alpha版、beta版、RC版とリリースされるのが一般的

となると.... 早くても来年後半のリリースか?

Samba4の構成



Samba4の構成(2)

- Samba4では、組み込まれたLDAP機能を利用し、ユーザ情報などは全てLDAPデータとして格納される
- NTVFSと呼ばれるレイヤを実装し、論理的にNTFSと同等の操作を実現。ただし、実際にUNIX - Windows間においてACLなどの整合性を一致させるためには、たとえばLinux kernel 2.6で利用可能なXATTR属性を利用する必要がある。
- Windows Vistaで導入されるSMB 2.0(通称 SMB2)対応コードが実装済み

Samba4のビルド

- パッケージは無いのでSubversionから最新ソースを取得し、コンパイルするのが最善の方法

```
$ svn co svn://svnanon.samba.org/samba/branches/SAMBA_4_0 samba4

$ cd samba4/source
$ ./autogen.sh
$ ./configure
$ make proto all
$ su
# make install
```

Samba4の初期設定

- 初期設定スクリプトを利用
  - スクリプトでADドメインコントローラの初期設定が可能

初期化スクリプトの実行

```
# PATH=/usr/local/samba/bin:$PATH
# cd source
# ./setup/provision --realm=OSSTECH.CO.JP --domain=OSSTECH –adminpass=secret
.... 初期化処理 ...

Setting up DNS zone: osstech.co.jp
Please install the zone located in /usr/local/samba/private/osstech.co.jp.zone into your DNS server
```

Samba4のBIND設定

- Active DirectoryはLDAP、Kerberos、DNSなどの連携により実現。LinuxではBINDの設定が必要
- Provisioningにより作成されたzoneファイルを/var/namedにコピー
- /etc/named.confにAD用のzone設定を追加

```
...
zone “osstech.co.jp” {
        type master;
        file “osstech.co.jp.zone”
};
...
```

Sambaのサービス起動

- namedを起動

```
# /sbin/service named start
```

- smbdを起動
  - デバッグ、開発用の1プロセスモードの起動

```
# /usr/local/samba/sbin/smbd -M single
```

- 運用の場合
  - サービスごとにsmbdプロセスが起動

```
# /usr/local/samba/sbin/smbd
```

Samba4のADドメインにWindows参加

- administrator、初期化時のパスワードでADドメインに参加可能
- Kerberos認証のために、マシンの時刻合わせが重要。
  - マシンの時刻がずれている場合、「Administrator」のユーザ、パスワードが間違っているというエラーとなるため、原因が分かりにくい
- Samba3で必要だったマシンアカウント作成の作業は不要

Samba4のユーザ作成とパスワード設定

- ユーザ作成
  - あらかじめUNIXユーザアカウントが必要

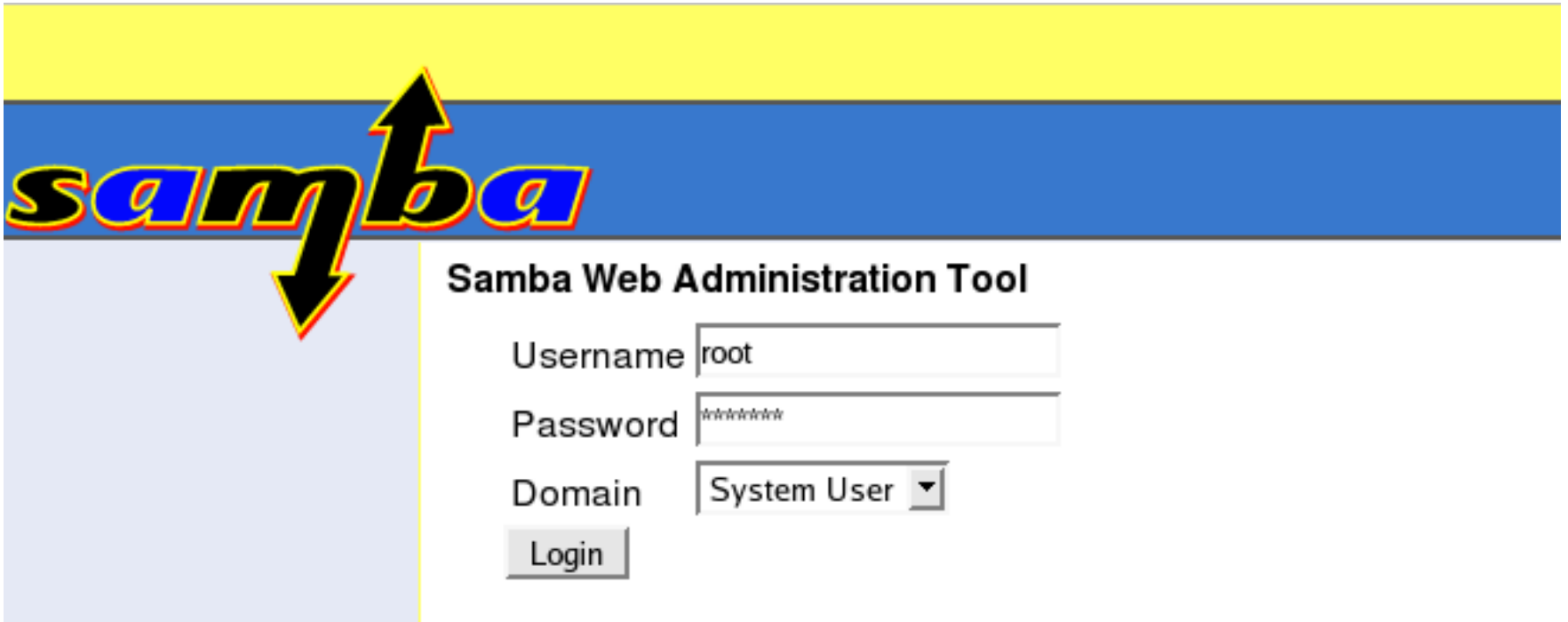
```
# /usr/bin/useradd yasuma

# PATH=/usr/local/samba/bin:$PATH
# cd source/setup
# ./newuser –adduser yasuma –password secret
```

- パスワード設定・変更

```
# PATH=/usr/local/samba/bin:$PATH
# cd source/setup
# sh setpassword –username yasuma –newpassword password2
```

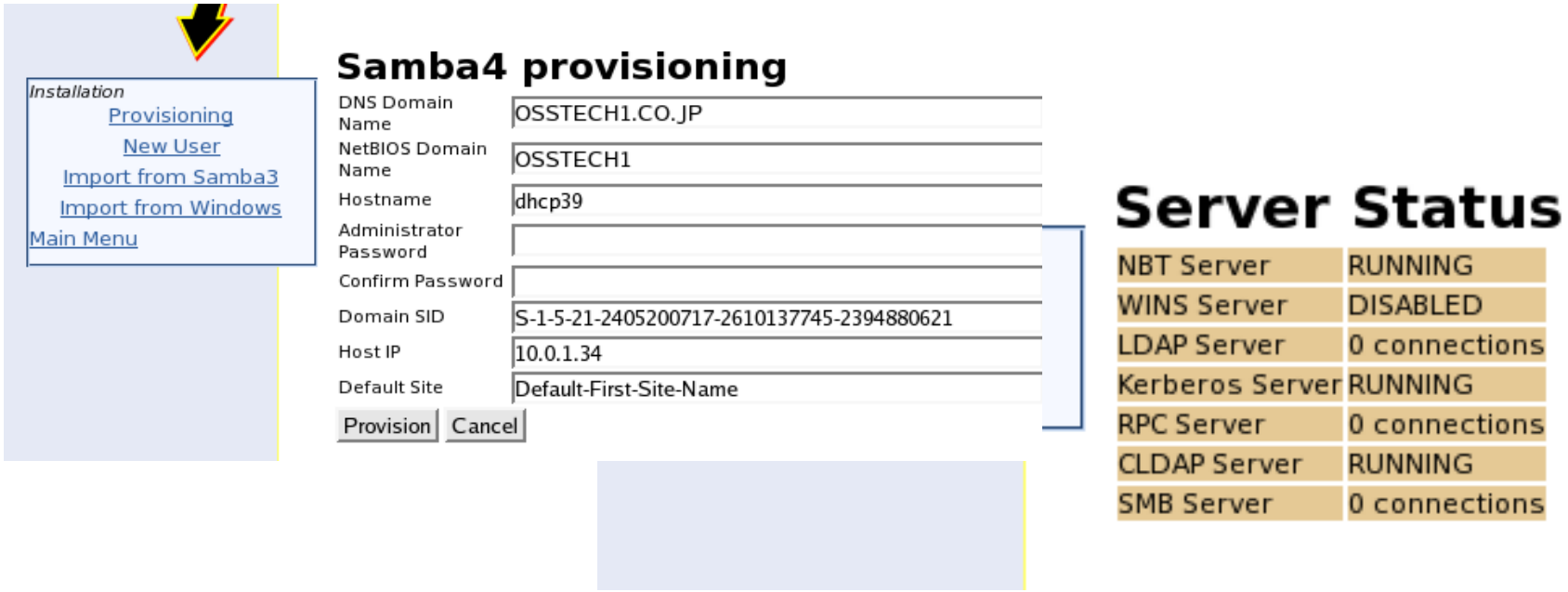
Samba4のSWAT

- smbd起動後にhttp://localhost:901にアクセス
- ユーザ名: root、rootのパスワードで認証可能



Samba4のSWAT(2)

- qooxdoo(クックスドゥ)によるGUIインターフェース改善
- 現在はサーバステータスの表示、Samba4の初期化(provisioning)、ユーザ追加機能などのみ実装

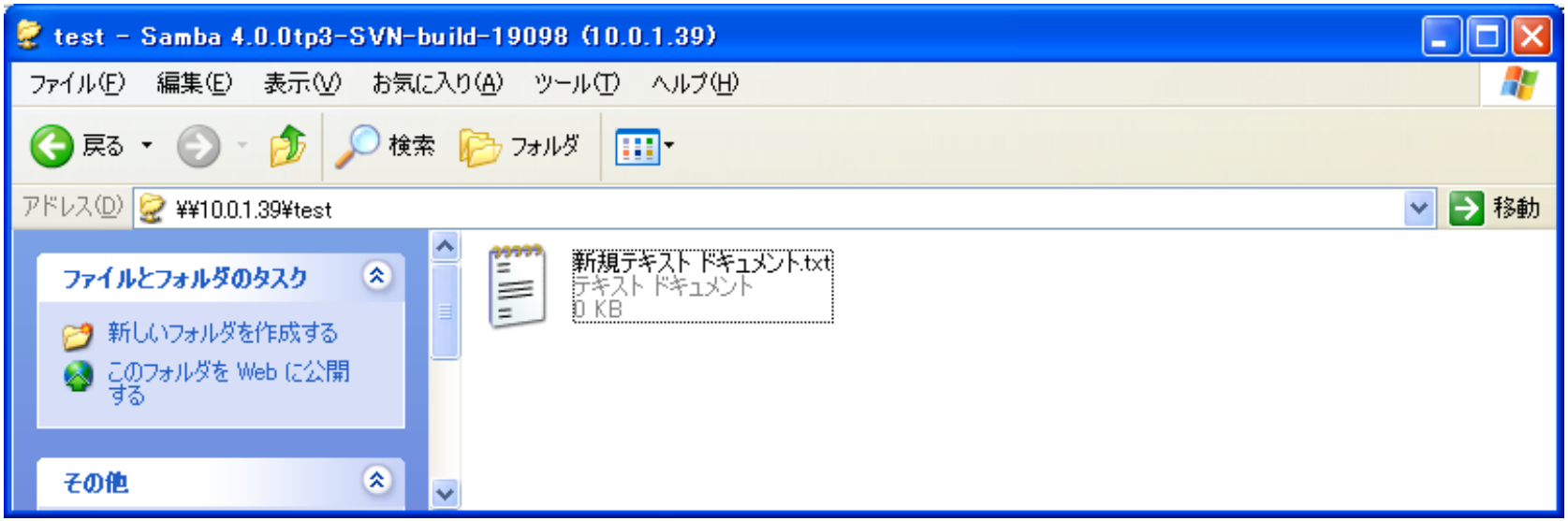


Samba4のパラメータ

- **サーバの役割の指定**(server role)
  - standalone ... **ファイルサーバ**
  - member server ... **メンバーサーバ**
  - pdc ... **プライマリ・ドメイン・コントローラ**
  - bdc ... **バックアップ・ドメイン・コントローラ**
- **Samba4の国際化関係パラメータ**
  - **Samba3のiconvの実装概念を引き継ぎ、以下の3つのパラメータによる設定が有効**
    - unix charset
    - dos charset
    - display charset

Samba4のファイルサーバ機能

- ユーザ認証は正常に行われる
- ファイルの作成、削除なども可能



Samba4のまとめ

Samba4のコアとなるコンポーネントの完成度は高まっている

Active Directory実現に必要なコンポーネントをほとんど
Samba4に取り込んであるため、Samba3よりも設定が簡単

ユーザ管理など、運用に必要なツールがほとんど
出来上がっていないため、実際に利用するのはまだ難しい

Windows Vistaについて

- Windows Vistaのおさらい
- Samba3.0のファイル共有機能
- Samba3.0にドメインログオン
- Windows VistaからSambaのパスワード変更
- Windows VistaでUSRMGR.EXE

SambaのWindows Vista対応状況

- **検証環境**

Windows Vista
RC1

CentOS 4.4
samba 3.0.10-1.4E

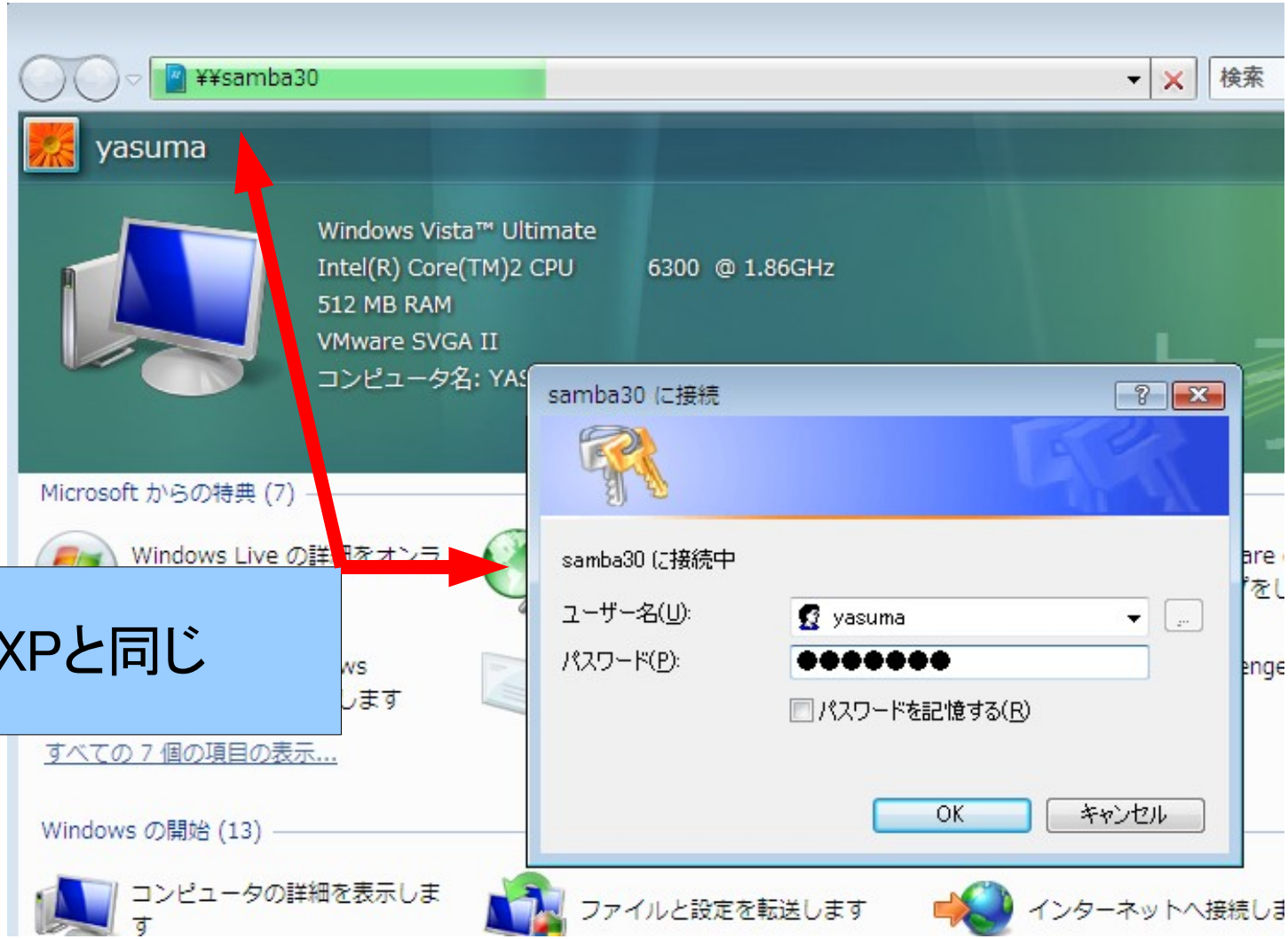
Windows Vistaのおさらい

- Windows Vistaの各Editionと機能差分
  - Home Edition
  - Home Premium Edition
  - Business Edition
  - Enterprise Edition
  - Ultimate Edition → RC1で提供中

[注意]
Windows XPと同様にHome系Editionはドメイン参加不可能

http://itpro.nikkeibp.co.jp/article/COLUMN/20060606/240133/

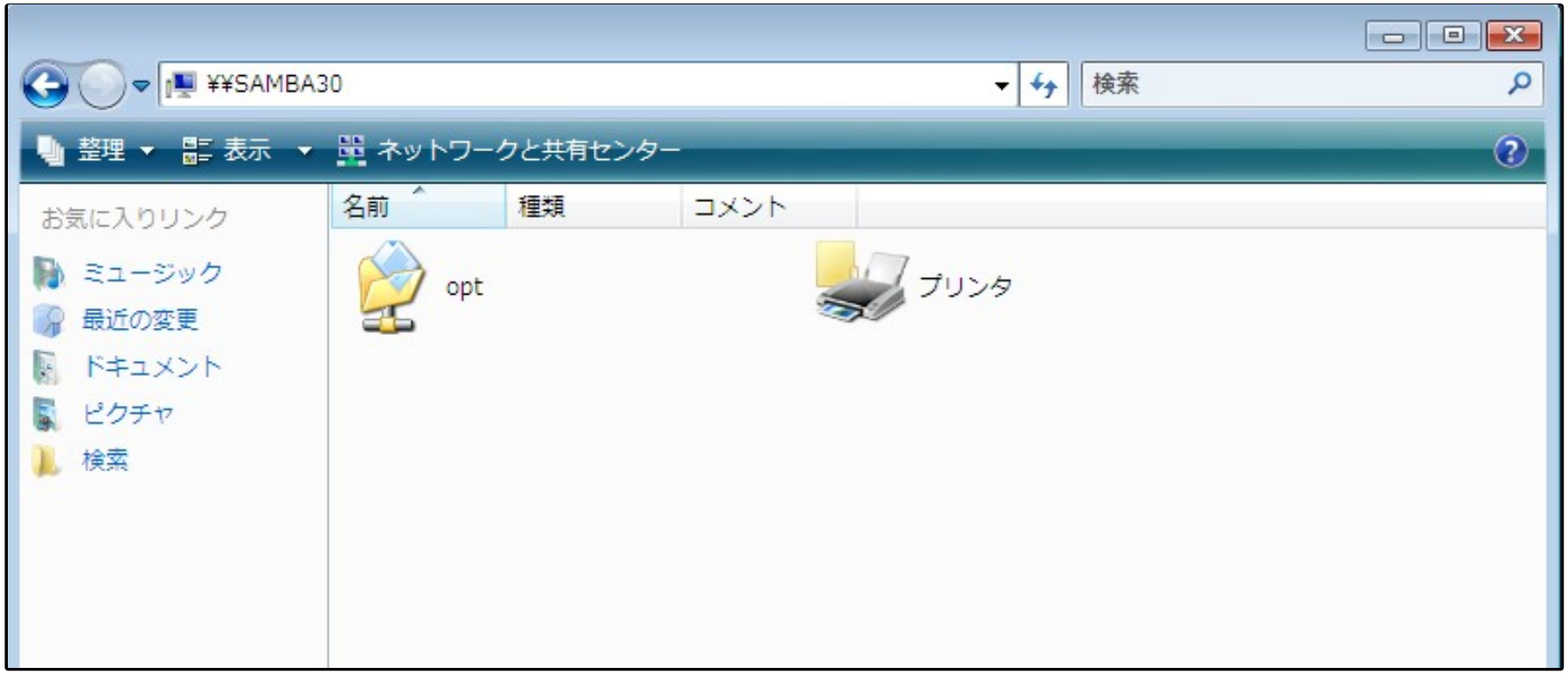
Windows VistaでSamba3.0ファイル共有にアクセス



Windows XPと同じ

Windows VistaでSamba3.0ファイル共有にアクセス(2)

- ファイル共有へのアクセスは問題無し



Windows VistaをSamba3.0ドメインに参加(1)

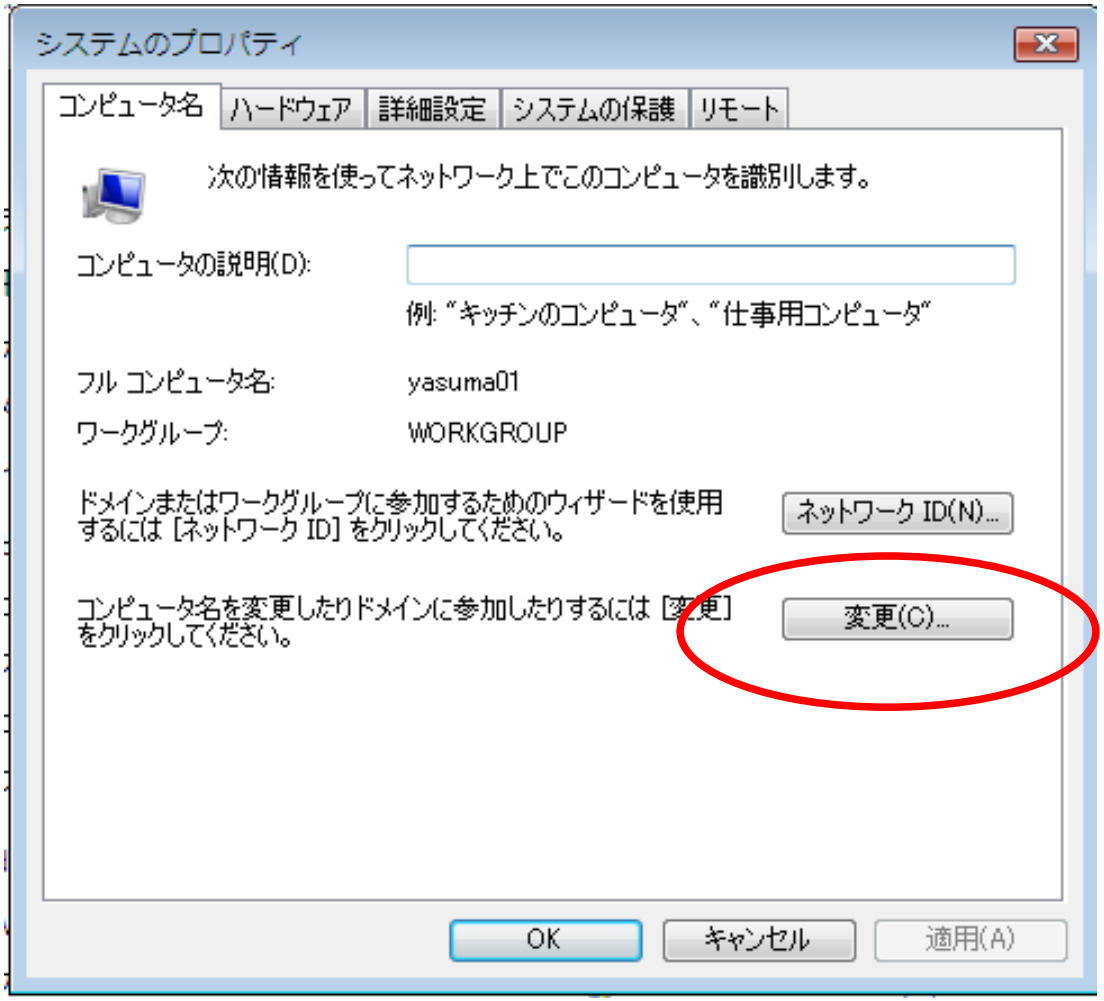
コントロールパネル

↓

システムとメンテナンス

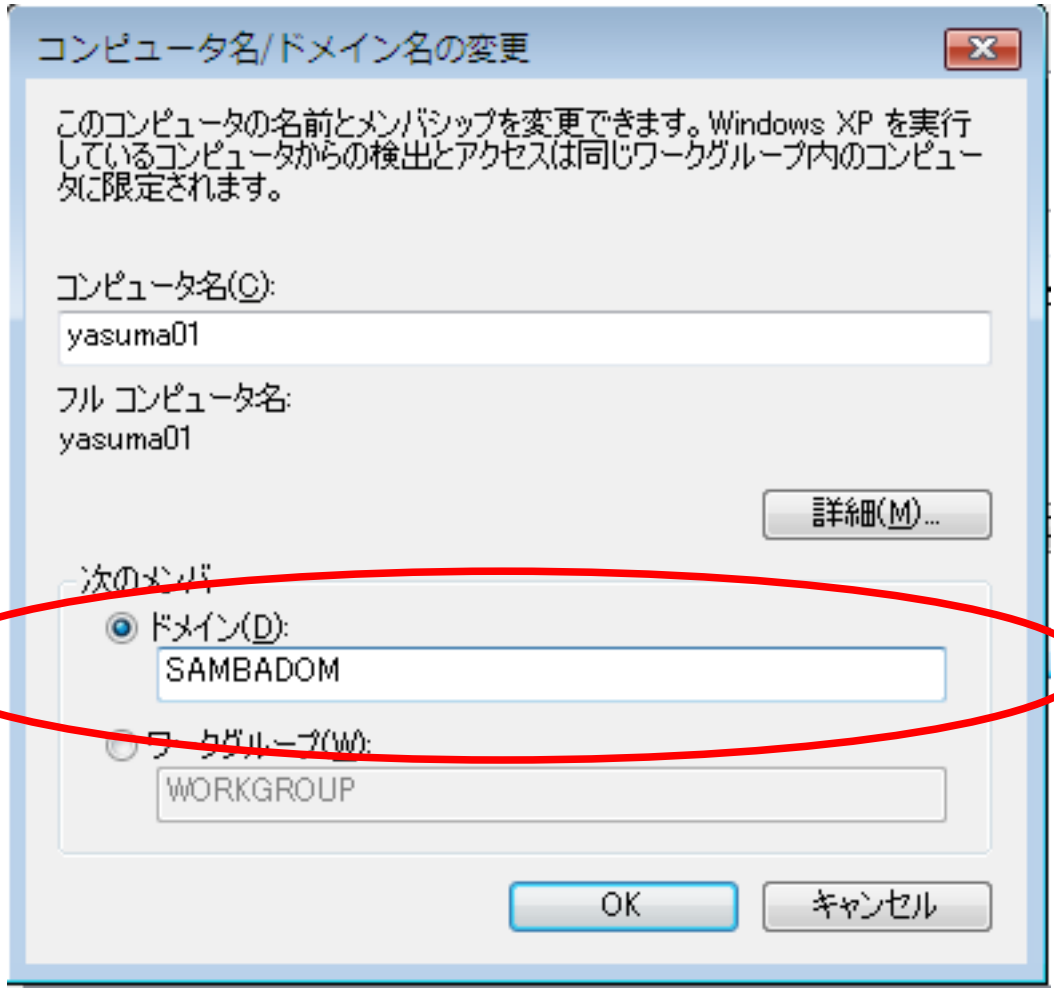
↓

システム



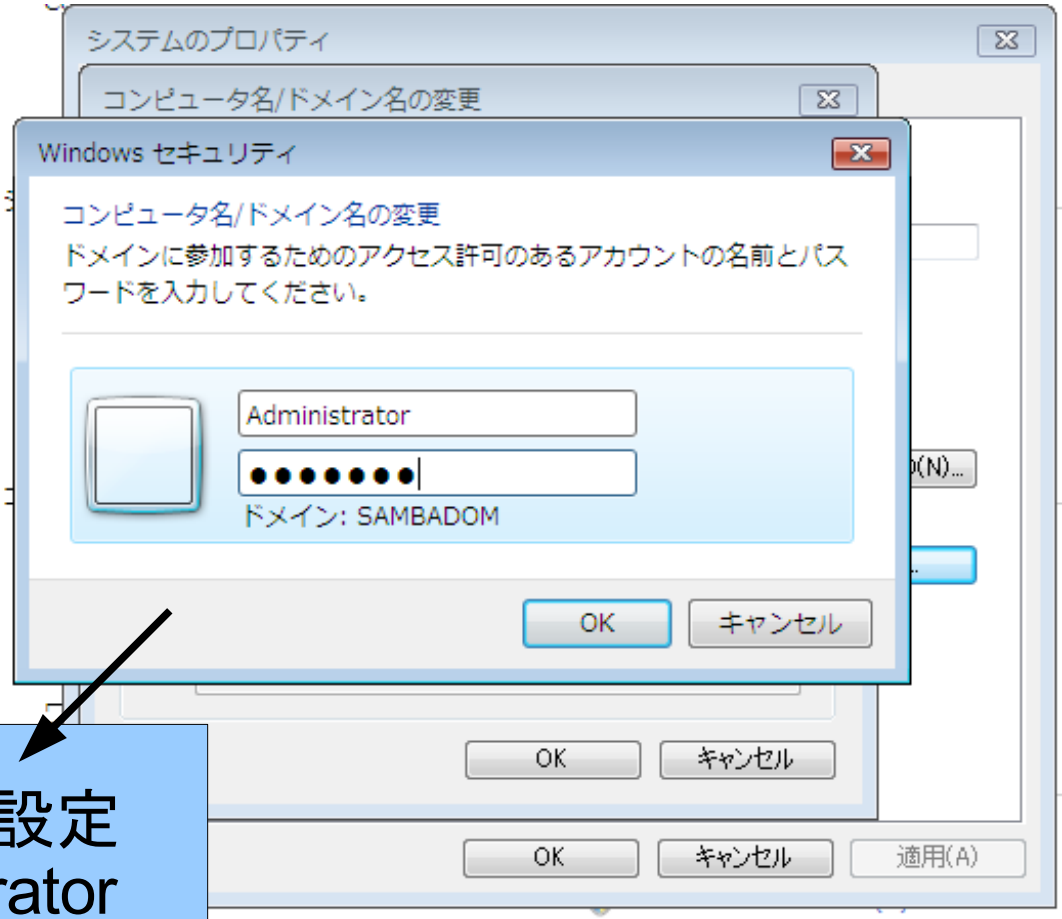
Windows VistaをSamba3.0ドメインに参加(2)

ドメイン名の入力



Windows VistaをSamba3.0ドメインに参加(3)

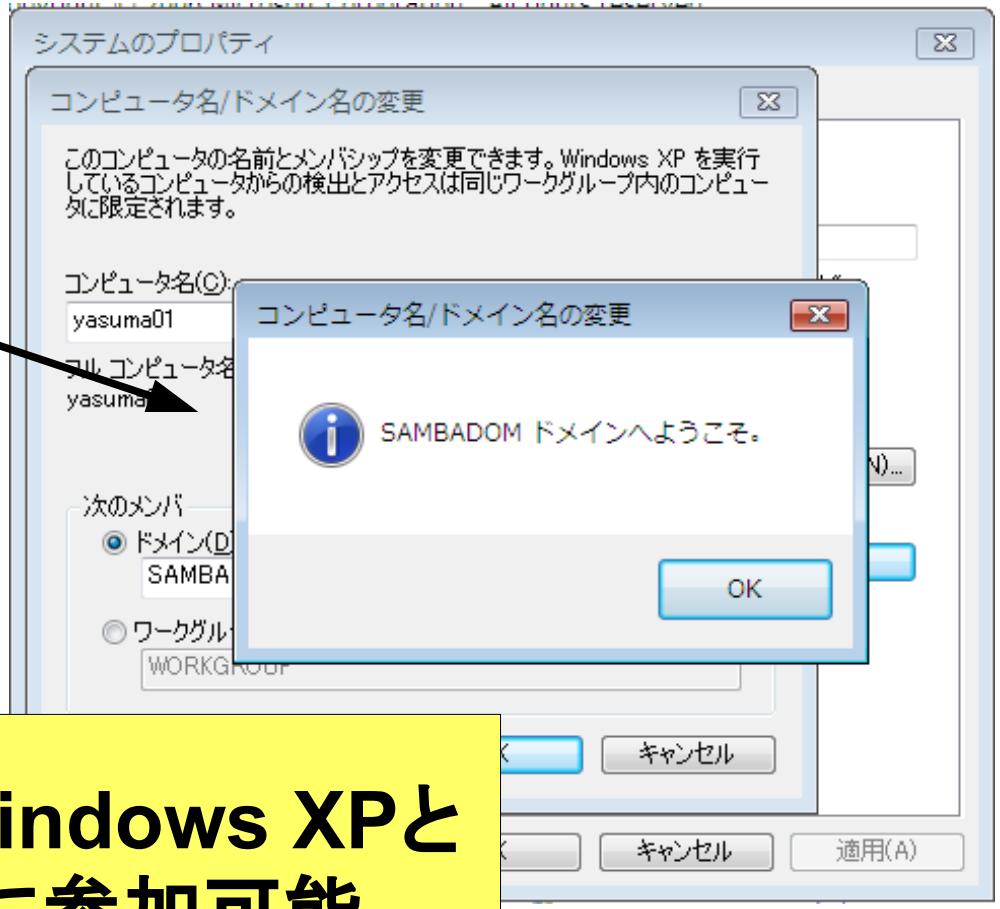
ドメイン管理者の
パスワード入力



画面 - smb.confに下記設定
admin users=Administrator

Windows VistaをSamba3.0ドメインに参加(4)

ドメイン参加成功!!



Windows VistaでもWindows XPと同様にSambaドメインに参加可能

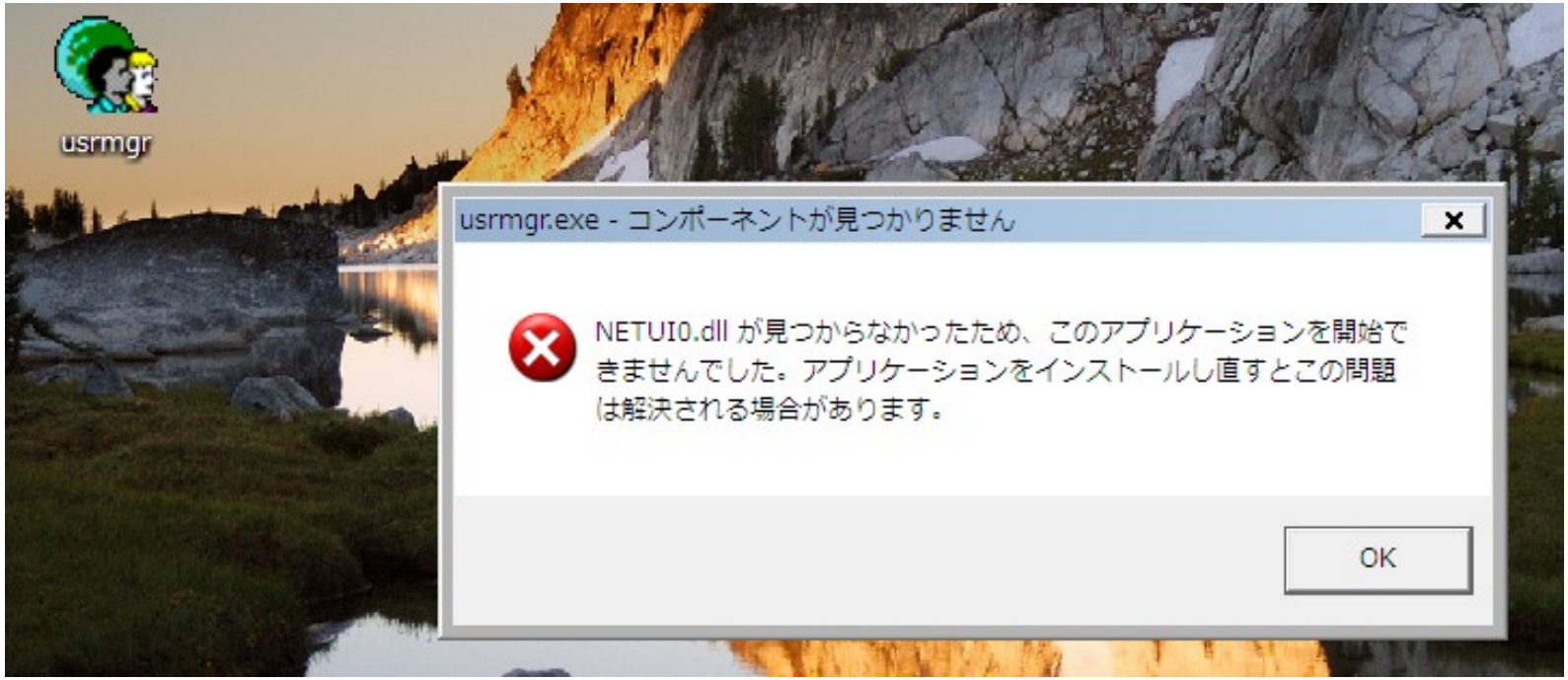
Sambaドメインへのログオン画面

Windows Vistaからのパスワード変更

- samba 3.0.23cでは問題無し
- CentOS 4のsamba 3.0.10ではパスワード変更不可能。Sambaのバージョンアップが必要

Windows Vista上でUSRMGR.EXE

- Samba**サーバのユーザ管理に**USRMGR(**ユーザマネージャ)を利用。**
- Windows Vista**上ではエラー発生**!!



Windows Vista上でUSRMGR.EXE

- USRMGR.EXEは以下の3つのDLLが必要

netui0.dll	netui1.dll	netui2.dll

- Windows XPやWindows 2000の「C:\WINDOWS\system32」フォルダに格納されている。

これらの3つのDLLをWindows Vistaの「C:\WINDOWS\system32」フォルダにコピーすると...

USRMGR.EXEも動作可能