Begi:net

Linux Professional Institute Japan LPI-JAPAN

LPICレベル3技術解説無料セミナー
Samba+LDAPで ドメインコントローラーを 構築してみよう

主催：特定非営利活動法人エルピーアイジャパン

講師：宮原 徹（株式会社びぎねっと）

本日のアジェンダ

Begi.net

- Windowsドメインについて
  - PDCとBDC
  - Samba＋OpenLDAPとWindowsドメイン
- Sambaによるドメインコントローラーの構築
  - SambaとOpenLDAPを使ったPDCの構築
  - BDCの構築

Windowsドメインとは

Begi.net

- Windows Networkのユーザー情報をドメインコントローラーが一元管理する仕組み
  - ユーザー名とパスワード
  - その他ユーザー個別の設定
- 各クライアントにユーザー情報の登録不要
- ログオン認証はドメインコントローラーが行う
- ファイル共有に対するアクセスもドメインに登録された情報で管理される
  - ドメインコントローラーとファイルサーバが別々のマシンでも、情報はネットワーク経由でやり取りされる

PDCとBDC

Begi.net

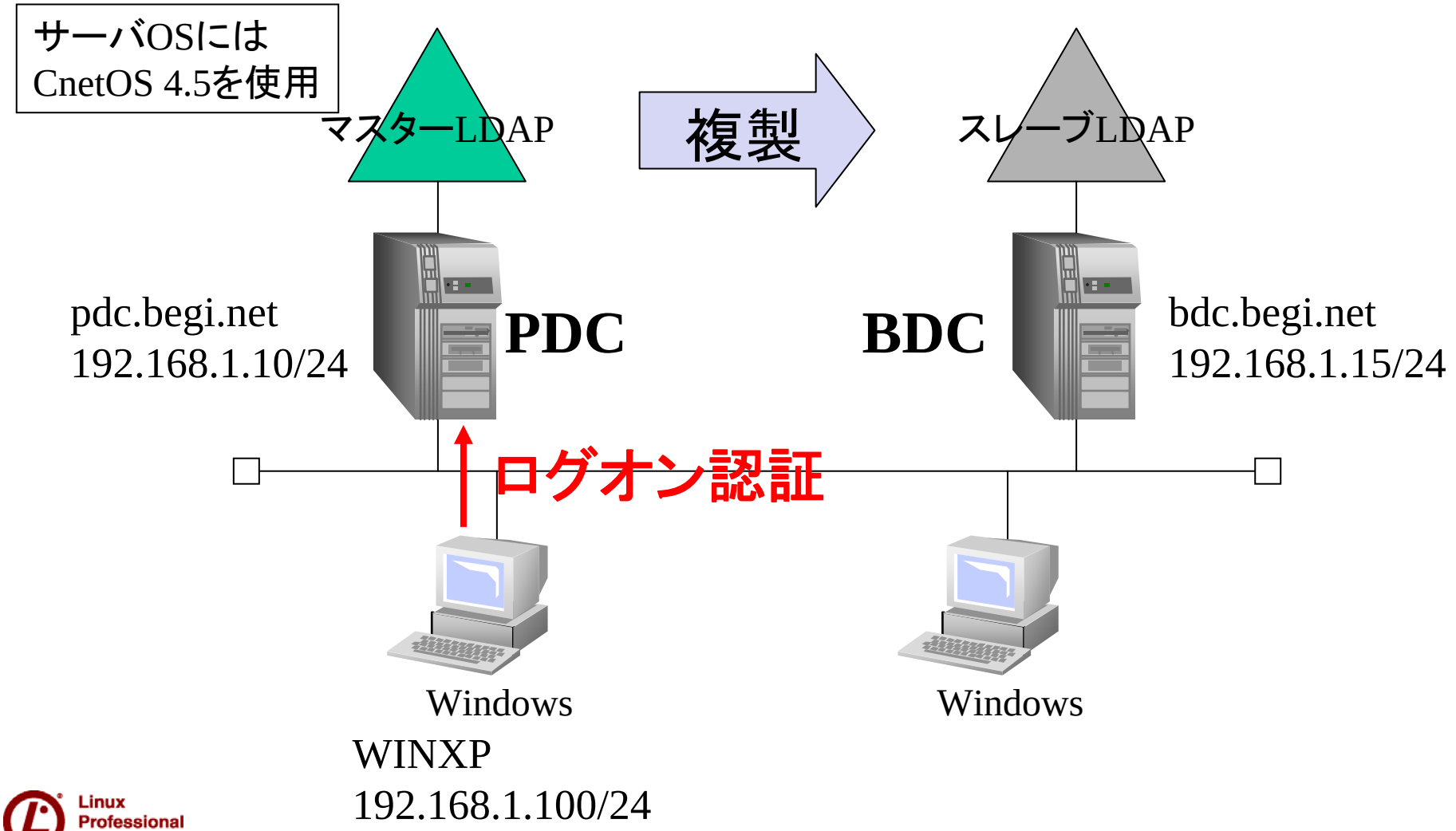
- PDC(Primary Domain Controller)
  - ドメインに登録されている情報のマスターを管理するドメインコントローラー
  - ユーザーのログオン認証を行う
  - 1つのドメインに1つ必要
- BDC(Backup Domain Controller)
  - PDCから情報を受け取り保持するドメインコントローラー
  - PDCに代わってログオン認証を行うこともある
    - 負荷が高い場合
    - PDCに障害が発生した場合
  - 1つのドメインに複数存在可能

SambaとOpenLDAP

Begi.net

- Samba単体では、単独のドメインコントローラー（PDCのみ）を実現可能
- ドメイン情報の複製が必要となるPDC・BDCの構成では、情報管理にOpenLDAPが必要
  - LDAPv3をサポートするLDAPサーバ
  - ユーザー名やグループ名、パスワード情報を管理
  - Sambaに対してドメインの情報を提供
  - LDAPサーバ間で情報の複製が可能

SambaとOpenLDAPによる構成



Sambaのインストール

Begi.net

RPMパッケージをインストールする

- samba-common　　:Sambaに共通のファイル
- samba　　:Sambaサーバ
- samba-client　　:Samba付属のクライアント
- samba-swat　　:Samba設定用SWAT

1.yumコマンドでインストール

- # yum install samba-common samba samba-client samba-swat

SWATの使用

Begi.net

- SWAT(Samba Web Admin Tool)を使用することで Webブラウザから Sambaの設定が行える

1. /etc/xinetd.d/swatを修正
   - disable = noに設定(# chkconfig swat onでも可)
   - only_from行をコメントアウト
2. xinetdを再起動
   - # service xinetd restart
3. WebブラウザでSWATに接続
   - http://*server_address*:901/
   - http://を省略しないこと
   - 管理者rootで認証し、詳細表示モードに変更
   - 文字コードの設定を行っておく(dos charset = CP932)

SWAT 文字コード設定

Windowsドメインの設定手順

Begi.net

- Samba+OpenLDAPによるPDCの構築
  1. OpenLDAPのインストール
  2. Sambaの設定
  3. smbldap-toolsのインストール
  4. ユーザーの登録とWindowsログオン
- BDCの構築
  1. OpenLDAPによる情報複製の設定
  2. Sambaの設定

OpenLDAPの設定手順

Begi.net

- ドメイン情報を格納するためのLDAPサーバを設定する

1. LDAPパッケージのインストール
2. LDAP認証の設定と確認
3. LDAPサーバの設定
4. LDAPサーバの起動

LDAP用語の基礎知識

Begi.net

- DN:Distinguished Name 識別名
  - ディレクトリ内でオブジェクトを一意に識別できる名前
- DC:Domain Component
  - ドメインを表すために使用
- OU:Organizational Unit 組織単位
  - ドメイン内部を組織単位に分割するために使用
  - ユーザーやグループなどのオブジェクトをまとめるためにも使用
- CN:Common Name 共通名
- クラス（objectClass）
  - データのテンプレート
  - オブジェクトの属性を定義
  - ユーザ、グループなどLDAPで管理するデータの種類によって用意されている

LDAPパッケージのインストール

Begi.net

- 必要なパッケージ
  - openldap-servers
  - openldap-clients

1. yumでインストール
   - # yum install openldap-servers openldap-clients

- 同様に「アプリケーションの追加/削除」からインストールも可能
  - 「ネットワークサーバ」→「openldap-servers」
  - 「システムツール」 → 「openldap-clients」

LDAP認証の設定

Begi.net

1. authconfigコマンドを実行
2. 認証の設定
   - ユーザー情報：「LDAPを使用」にチェック
   - 認証：「LDAP認証を使用」にチェック
   - LDAP設定
     - サーバ：127.0.0.1 ←自分自身のIPアドレスを指定
     - ベースDN：dc=begi,dc=net

- X Windowの「システム設定」ー「認証」でも同様に設定可能

LDAP認証設定の確認

Begi.net

- ユーザー情報：/etc/nsswitch.conf
  - passwd: files ldap
  - shadow: files ldap
  - group: files ldap
- 認証：/etc/pam.d/system-auth
  - auth sufficient pam_ldap.so use_first_pass
  - account [default=bad success=ok user_unknown=ignore] pam_ldap.so
  - password sufficient pam_ldap.so use_authtok
  - session optional pam_ldap.so
- LDAP設定：/etc/ldap.conf
  - host 127.0.0.1
  - base dc=begi,dc=net

LDAPの設定

Begi.net

1. スキーマ設定ファイルのコピー
   - スキーマ設定は/etc/openldap/schemaに入れる
   - # cp /usr/share/doc/samba-*x.y.z*/LDAP/samba.schema /etc/openldap/schema/
     - *x.y.z*はインストールしたバージョンにより異なる
2. LDAP管理者パスワードの生成
   - パスワードをMD5を使ってダイジェスト化
   - # slappasswd -h {MD5} -s ldapadmin
     - “ldapadmin”がパスワード(シークレット)

/etc/openldap/slapd.confの設定

Begi.net

■/etc/openldap/slapd.confに以下の追加と修正

1.追加

- include /etc/openldap/schema/samba.schema

2.修正

- suffix "dc=begi,dc=net"
- rootdn "cn=Manager,dc=begi,dc=net"
- rootpw {MD5}TmZgZ01/Z0/29bOPByMr4A==
  - slappasswdの結果をコピー＆ペースト

Linux Professional Institute

LDAPサーバの起動

Begi.net

1. OpenLDAPサーバの起動
   - # service ldap start
2. LDAPポートの確認
   - # netstat -tl
3. システム起動時に自動起動するように設定
   - # chkconfig ldap on

Sambaの設定手順

Begi.net

- SambaをLDAPサーバと連携したPDCとして設定

1. Sambaの設定
2. 管理者パスワードの設定
3. smbldap-toolsのインストールと設定
   - Perlのモジュールをインストール

/etc/samba/smb.confの設定(1)

Begi.net

- 基本オプション
  - workgroup = BEGINET
- セキュリティオプション
  - passdb backend = ldapsam:ldap://localhost
  - admin users = Administrator
- ログオンオプション
  - domain logons = yes
- ブラウジングオプション
  - domain master = yes

Linux Professional Institute

※SWATで設定する場合、「詳細表示」(Advanced)で行う

/etc/samba/smb.confの設定(2)

Begi.net

LDAPオプション

- ldap admin dn = cn=Manager,dc=begi,dc=net
- ldap group suffix = ou=Groups
- ldap machine suffix = ou=Computers
- ldap passwd sync = yes
- ldap suffix = dc=begi,dc=net
- ldap user suffix = ou=Users

Winbindオプション

- winbind nested groups = no

Linux Professional Institute

※SWATで設定する場合、「詳細表示」(Advanced)で行う

設定項目について(1)

Begi.net

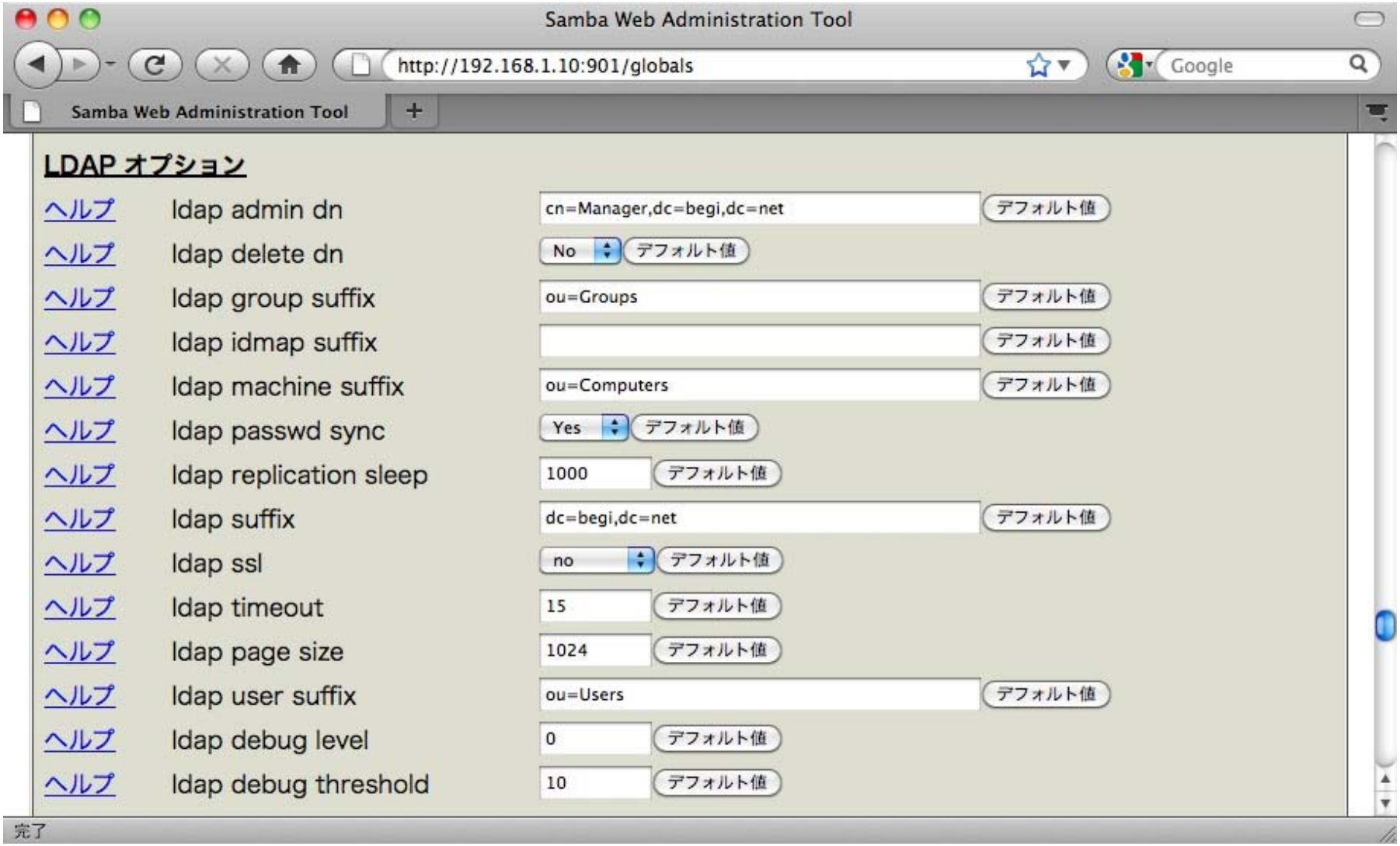
- workgroup
  - ドメイン名を指定
- passdb backend
  - Sambaのユーザー情報の格納先を指定
  - smbpasswd tdbsam ldapsamの3種類から選択可能
- admin users
  - Samba管理者のユーザー名を指定
  - コンピュータがドメインに参加する際に必要
- domain logons
  - ドメインログオンをサポートするドメインコントローラになる
- domain master
  - ドメインマスタブラウザになる

設定項目について(2)

Begi.net

- ldap admin dn
  - LDAPサーバの管理者ユーザーをDNで指定する
- ldap suffix
  - LDAPの検索ベースを指定する
- ldap machine suffix/ldap user suffix/ldap group suffix
  - ドメイン情報の各格納先(OU)を指定する
- ldap passwd sync
  - SambaとUNIXのパスワード情報を同期させる
- winbind nested groups
  - デフォルトがyesなので正常動作のためにnoに設定
  - 設定しないとsmbプロセスが落ちる

SWAT LDAP設定


Samba Web Administration Tool
http://192.168.1.10:901/globals
Google
Samba Web Administration Tool
LDAP オプション
ヘルプ ldap admin dn cn=Manager,dc=begi,dc=net デフォルト値
ヘルプ ldap delete dn No デフォルト値
ヘルプ ldap group suffix ou=Groups デフォルト値
ヘルプ ldap idmap suffix デフォルト値
ヘルプ ldap machine suffix ou=Computers デフォルト値
ヘルプ ldap passwd sync Yes デフォルト値
ヘルプ ldap replication sleep 1000 デフォルト値
ヘルプ ldap suffix dc=begi,dc=net デフォルト値
ヘルプ ldap ssl no デフォルト値
ヘルプ ldap timeout 15 デフォルト値
ヘルプ ldap page size 1024 デフォルト値
ヘルプ ldap user suffix ou=Users デフォルト値
ヘルプ ldap debug level 0 デフォルト値
ヘルプ ldap debug threshold 10 デフォルト値
完了

LDAP管理者パスワードの設定

Begi.net

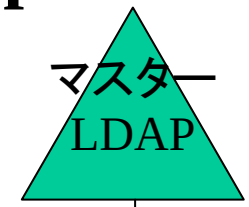
- SambaがOpenLDAPに接続する際に使用するパスワード
  - 設定値は/etc/samba/secrets.tdbに保存される
- slapd.confでのrootpwの設定値と対応させる
  - rootpw　:ldapadmin ←実際にはハッシュ値
- ユーザー名はsmb.confに設定したldap admin dnの値が使用される
  - ldap admin dn　:cn=Manager,dc=begi,dc=net

1. smbpasswdコマンドに-wオプションで実行
   - # smbpasswd -w ldapadmin ←パスワードを指定

管理者パスワードの関係

Begi.net

OpenLDAP



slapd.conf

ユーザー名：rootdn "cn=Manager,dc=begi,dc=net"

パスワード：rootpw {MD5}TmZgZ01/Z0/29bOPByMr4A==

slappasswd -h {MD5} -s ldapadminの結果を記述

それぞれのユーザー名／パスワードを一致させること

smb.conf

ユーザー名：ldap admin dn = cn=Manager,dc=begi,dc=net

パスワード：smbpasswd -w ldapadmin

/etc/samba/secrets.tdbに格納される

Samba

smbldap-toolsパッケージのインストール

Begi.net

1. RPMforgeを有効にする
   - http://rpmrepo.org/RPMforge/Using から使用しているディストリビューションに合わせたRPMパッケージをダウンロードしてインストール
2. smbldap-toolsパッケージをインストール
   - # yum install smbldap-tools
3. Sambaを起動しておく
   - # service smb start
4. 初期化を行う
   - # cd /usr/share/doc/smbldap-tools-x.y.z
   - # ./configure.pl
     - LDAPへの接続パスワードを聞かれるのでldapadminを入力

SIDについて

Begi.net

- SID(Security Identifier・セキュリティ識別子)
- Windows内部のオブジェクトを識別するための一意の値
  - 「S-?-?-?」といった形式になっている
  - ドメイン毎に異なるSID値を持っている
- /etc/samba/secrets.tdbに保管されている
- ローカルドメインのSID値の確認
  - # net getlocalsid
- ローカルドメインのSID値の設定
  - # net setlocalsid SID
- その他のドメインのSID値の確認
  - # net rpc getsid [domain]

ドメインの初期化とユーザー登録

Begi.net

- SambaがPDCとして動作するために必要な初期情報をLDAPサーバに登録

1. ユーザーおよびクライアントコンピュータを登録
2. 初期ドメインデータの作成
3. ユーザーの登録
4. コンピュータの登録
5. ドメイン参加とWindowsドメインログオン

初期ドメインデータの作成

Begi.net

1. 初期ドメインデータの作成
   - ドメインの動作に必要な初期データを作成する
   - # smbldap-populate -a Administrator -b guest
   - -aオプションで指定するユーザー名はsmb.confで admin usersに設定したユーザーを指定する
   - /var/lib/ldap/にファイルが作成される
2. ドメイン管理者のパスワード設定
   - パスワード：domainadmin
   - -aオプションのユーザー名とパスワードはWindows コンピュータをドメインに参加させる時に必要

ドメインユーザー設定

Begi.net

- ユーザー登録
  - # smbldap-useradd -a -m *username*
  - -mオプションでホームディレクトリも同時に作成
- ユーザーパスワード設定
  - # smbldap-passwd *username*
- コンピュータ登録
  - # smbldap-usreadd -w *computer_name*
- ユーザー情報修正
  - # smbldap-usermod *options username*
- ユーザー削除
  - # smbldap-userdel *username*

ユーザーとコンピュータの登録

Begi.net

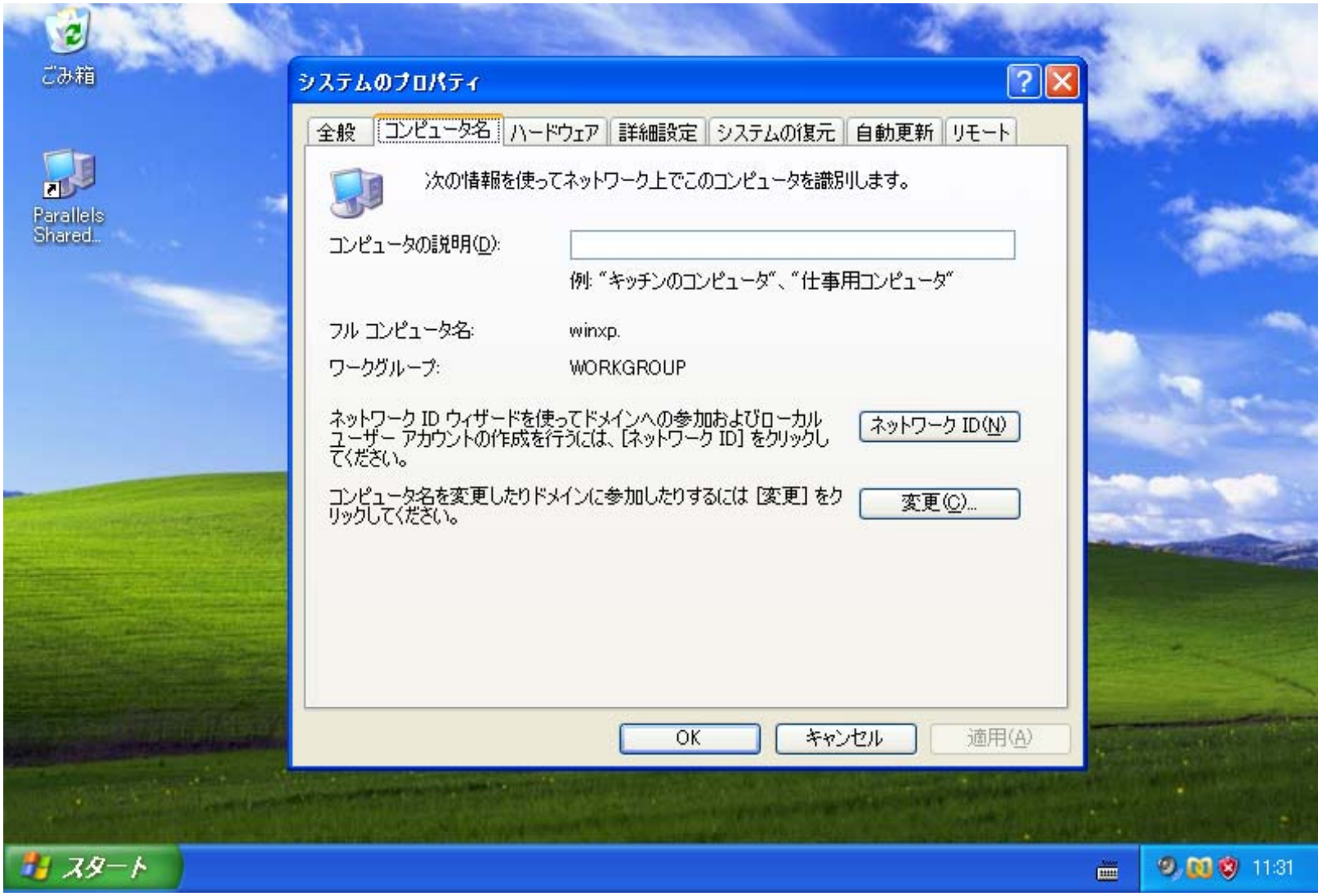
1. ユーザーbeginetを登録
   - # smbldap-useradd -a -m beginet
   - # smbldap-passwd beginet
     - パスワード：beginet
2. クライアントコンピュータwinxpを登録
   - # smbldap-useradd -w winxp
3. 確認
   - # getent passwd
   - # smbldap-usershow beginet
   - # smbldap-usershow winxp$ ←末尾に$が付く

ドメイン参加とドメイン認証

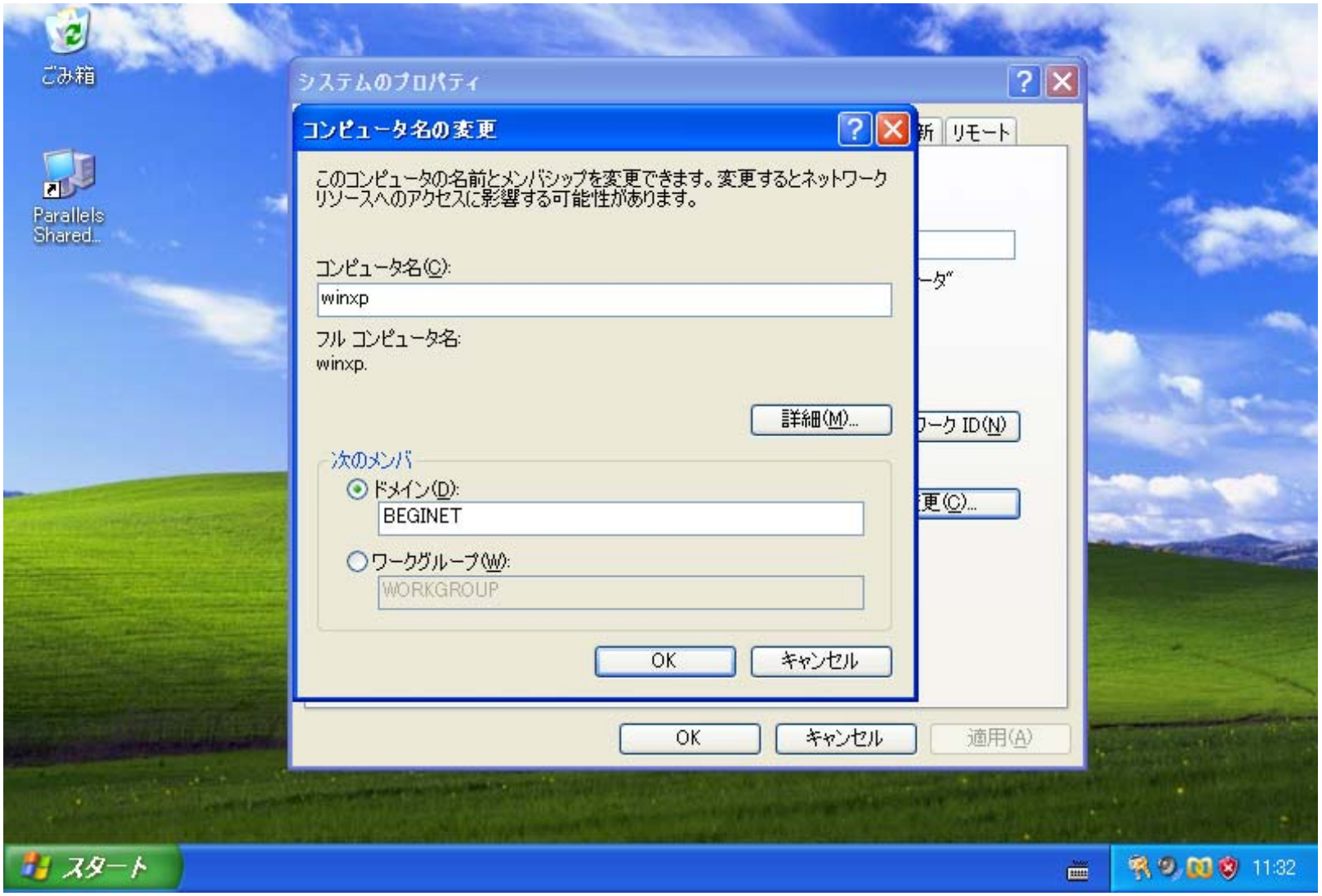
Begi.net

1. Windowsクライアントのドメイン参加設定
   1. ローカル管理者権限でログオン
   2. 「システムのプロパティ」→「コンピュータ名」→「変更」ボタンをクリック
   3. コンピュータ名をドメインに登録したコンピュータ名に設定（ここではwinxp）
   4. ドメイン名：beginet
   5. 管理者ユーザー名／パスワードが必要
   6. 「Administrator/domainadmin」を入力
   7. ドメイン参加後、Windowsクライアントを再起動
2. ドメイン認証
   - ログオンダイアログでログオン先をドメインに変更
   - 移動プロファイルの問題が発生（後述）

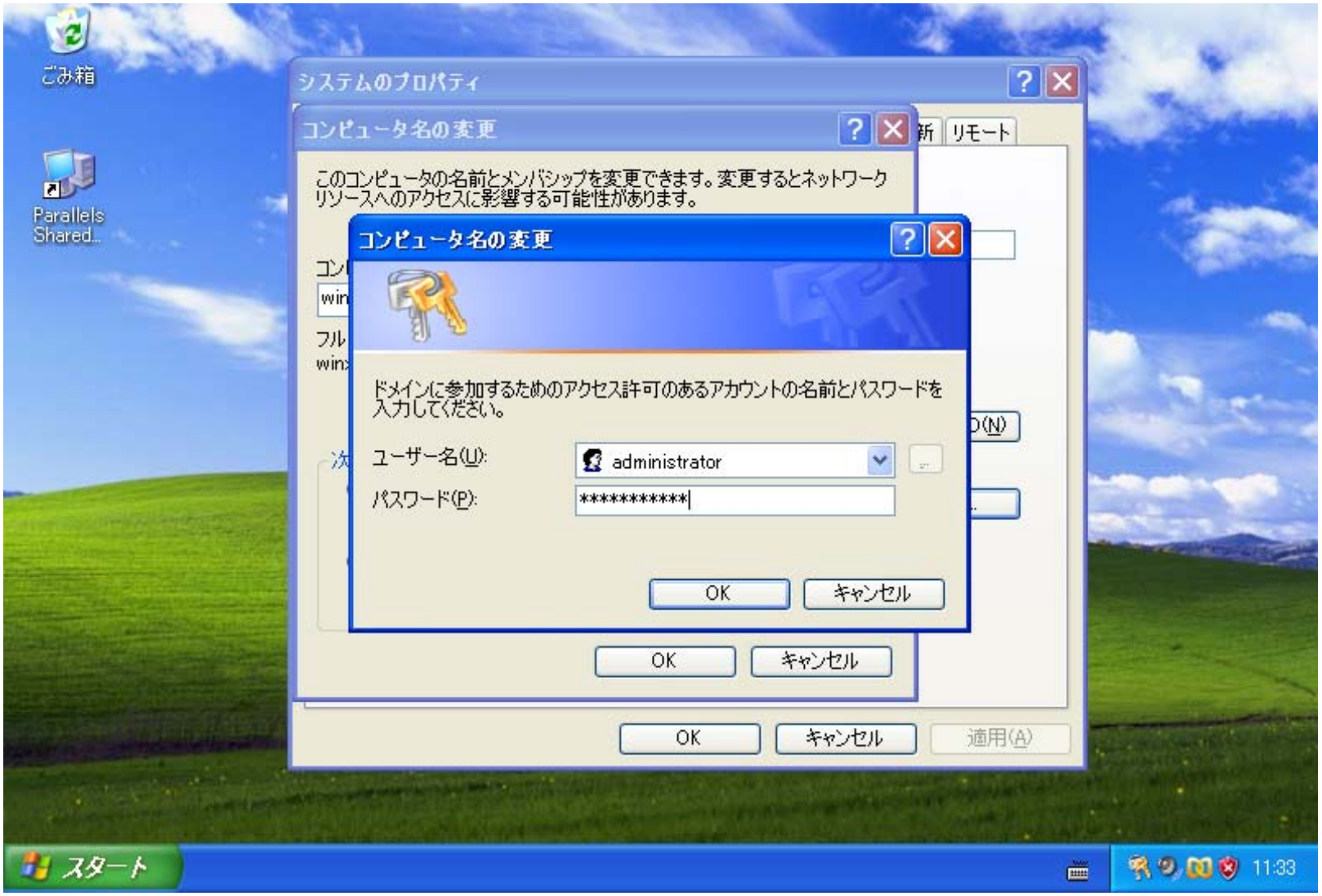
ドメイン参加(1)


ごみ箱
Parallels Shared...
システムのプロパティ
全般
コンピュータ名
ハードウェア
詳細設定
システムの復元
自動更新
リモート
次の情報を使ってネットワーク上でこのコンピュータを識別します。
コンピュータの説明(D):
例: "キッチンのコンピュータ"、"仕事用コンピュータ"
フル コンピュータ名:
winxp.
ワークグループ:
WORKGROUP
ネットワーク ID ウィザードを使ってドメインへの参加およびローカル ユーザー アカウントの作成を行うには、[ネットワーク ID] をクリックしてください。
ネットワーク ID(N)
コンピュータ名を変更したりドメインに参加したりするには [変更] をクリックしてください。
変更(C)...
OK
キャンセル
適用(A)
スタート
11:31

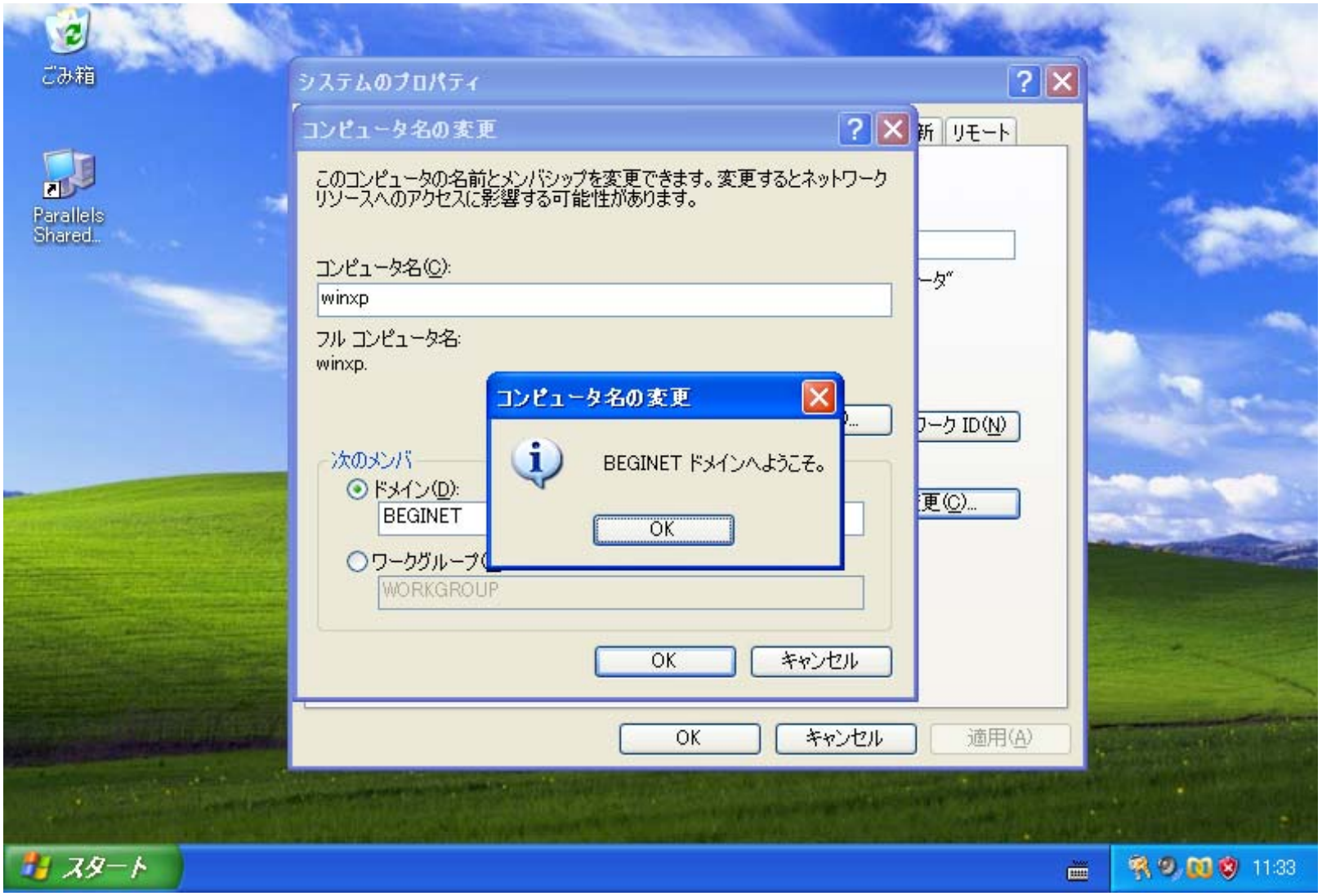
ドメイン参加(2)


ごみ箱
Parallels Shared...
システムのプロパティ
コンピュータ名の変更
このコンピュータの名前とメンバシップを変更できます。変更するとネットワーク リソースへのアクセスに影響する可能性があります。
コンピュータ名(C):
winxp
フル コンピュータ名:
winxp.
詳細(M)...
次のメンバ
ドメイン(D):
BEGINET
ワークグループ(W):
WORKGROUP
OK
キャンセル
リモート
OK
キャンセル
適用(A)
スタート
11:32

ドメイン参加(3)


ごみ箱
Parallels Shared...
システムのプロパティ
コンピュータ名の変更
このコンピュータの名前とメンバシップを変更できます。変更するとネットワーク リソースへのアクセスに影響する可能性があります。
リモート
コンピュータ名の変更
ドメインに参加するためのアクセス許可のあるアカウントの名前とパスワードを入力してください。
ユーザー名(U):
administrator
パスワード(P):
****
OK
キャンセル
OK
キャンセル
OK
キャンセル
適用(A)
スタート
11:33

ドメイン参加(4)


ごみ箱
Parallels Shared...
システムのプロパティ
コンピュータ名の変更
このコンピュータの名前とメンバシップを変更できます。変更するとネットワーク リソースへのアクセスに影響する可能性があります。
コンピュータ名(C):
winxp
フル コンピュータ名:
winxp.
次のメンバ
ドメイン(D):
BEGINET
ワークグループ(
WORKGROUP
OK
キャンセル
リモート
適用(A)
コンピュータ名の変更
BEGINET ドメインへようこそ。
OK
スタート
11:33

実用上考慮すべきポイント

Begi.net

移動プロファイルの利用

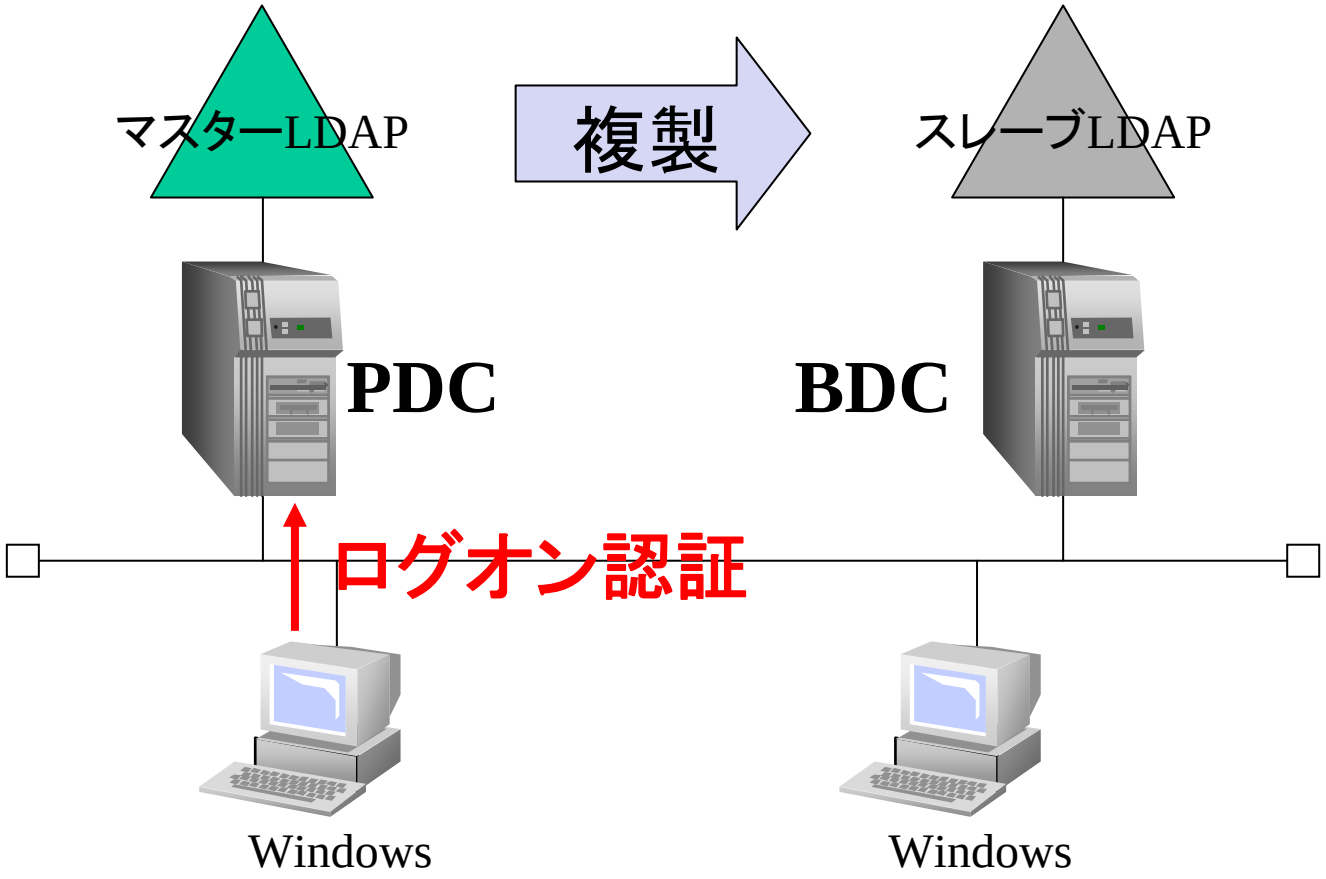
- smbldap-useradd.plの設定ではユーザー名が入る
- ¥¥*NETBIOS NAME*¥profiles¥usernameと設定される
- profilesというファイル共有を作っておく必要がある
  1. # mkdir /home/profiles
  2. # chmod 777 /home/profiles
  3. SWAT等で/home/profilesをprofiles共有として設定
     - 読み書き可能(read only = no)に設定すること
     - ゲストアクセス可能(guest ok = yes)に設定すること

Begi:net

Linux Professional Institute Japan LPI-JAPAN

SambaによるPDC－BDCの構築

SambaとOpenLDAPによる構成



BDCの構築手順

Begi.net

■PDCと同様の作業

1. SambaとOpenLDAPとをインストール
2. 認証にLDAP使用を設定（authconfig）
   - BDCでもlocalhostのLDAPを参照するように設定すること
3. スキーマ設定ファイルsamba.schemaのコピー

■BDC独自の作業

1. OpenLDAPの複製を設定
   - PDCからLDAPの情報ファイルをBDCにコピー
   - マスター／スレーブ間で複製を設定
2. SambaをBDCとして設定
   - ドメインマスターにならないサーバとして設定
   - ユーザー情報はOpenLDAPサーバから取得

BDCへのLDAP情報のコピー

Begi.net

1. PDCのSambaとOpenLDAPサーバを停止する
   - PDC # servive smb stop
   - PDC # service ldap stop
2. PDCのLDAP情報をアーカイブ
   - PDC # cd /var/lib
   - PDC # tar cvf /root/ldap_data.tar ldap
3. ldap_data.tarをPDCからBDCへコピー
   - BDC # scp root@192.168.1.10:/root/ldap_data.tar /root
4. LDAP情報をコピー
   - BDC # tar xvf ldap_data.tar
   - BDC # rm -rf /var/lib/ldap/*
   - BDC # cp -p /root/ldap/* /var/lib/ldap/

LDAP情報複製の設定(PDC側)

Begi.net

- /etc/openldap/slapd.confに以下の設定を追加
  - replogfile /var/lib/ldap/openldap-master-replog
  - replica host=192.168.1.15
    binddn="cn=Manager,dc=begi,dc=net"
    bindmethod=simple credentials=ldapadmin

- hostには更新情報を伝播させたいスレーブのIPアドレス(ここでは192.168.1.15)を指定
- マスターに対する変更は差分ログとして記録される
- スレーブに対してbinddnで接続認証する
  - スレーブに管理者ユーザーのDNが存在しなくてはいけない
  - 簡易認証・パスワードはldapadminで接続

LDAP情報複製の設定(BDC側)

Begi.net

- /etc/openldap/slapd.confを以下のように設定
  - include /etc/openldap/schema/samba.schema
  - suffix "dc=begi,dc=net"
  - rootdn "cn=Manager,dc=begi,dc=net"
  - rootpw {MD5}TmZgZ01/Z0/29bOPByMr4A==
  - updatedn "cn=Manager,dc=begi,dc=net"
  - updateref ldap://192.168.1.10

- updatednはローカルのrootdn、マスター側のbinddnと同じ設定にする
- updaterefは更新要求を受けた時にマスターの所在を知らせる

LDAP情報複製の確認

Begi.net

1. PDC・BDCでOpenLDAPを起動
   - PDC # service ldap start
   - BDC # service ldap start
2. PDCでユーザーを追加
   - PDC # smbldap-useradd -a -m reptest
   - PDC # smbldap-passwd reptest
   - PDC # id reptest
3. BDCでユーザーを確認
   - BDC # id reptest

/etc/samba/smb.confの設定(1)

Begi.net

- 基本オプション
  - workgroup = BEGINET
- セキュリティオプション
  - passdb backend = ldapsam:ldap://localhost
  - admin users = Administrator
- ログオンオプション
  - domain logons = yes
- ブラウジングオプション
  - domain master = no ←ドメインマスターにはならない

※SWATで設定する場合、「詳細表示」(Advanced)で行う

/etc/samba/smb.confの設定(2)

Begi.net

LDAPオプション

- ldap admin dn = cn=Manager,dc=begi,dc=net
- ldap group suffix = ou=Groups
- ldap machine suffix = ou=Computers
- ldap passwd sync = yes
- ldap suffix = dc=begi,dc=net
- ldap user suffix = ou=Users

Winbindオプション

- winbind nested groups = no

Linux Professional Institute

※SWATで設定する場合、「詳細表示」(Advanced)で行う

SIDの設定

Begi.net

- BDCにはPDCと同じSIDを設定する必要がある

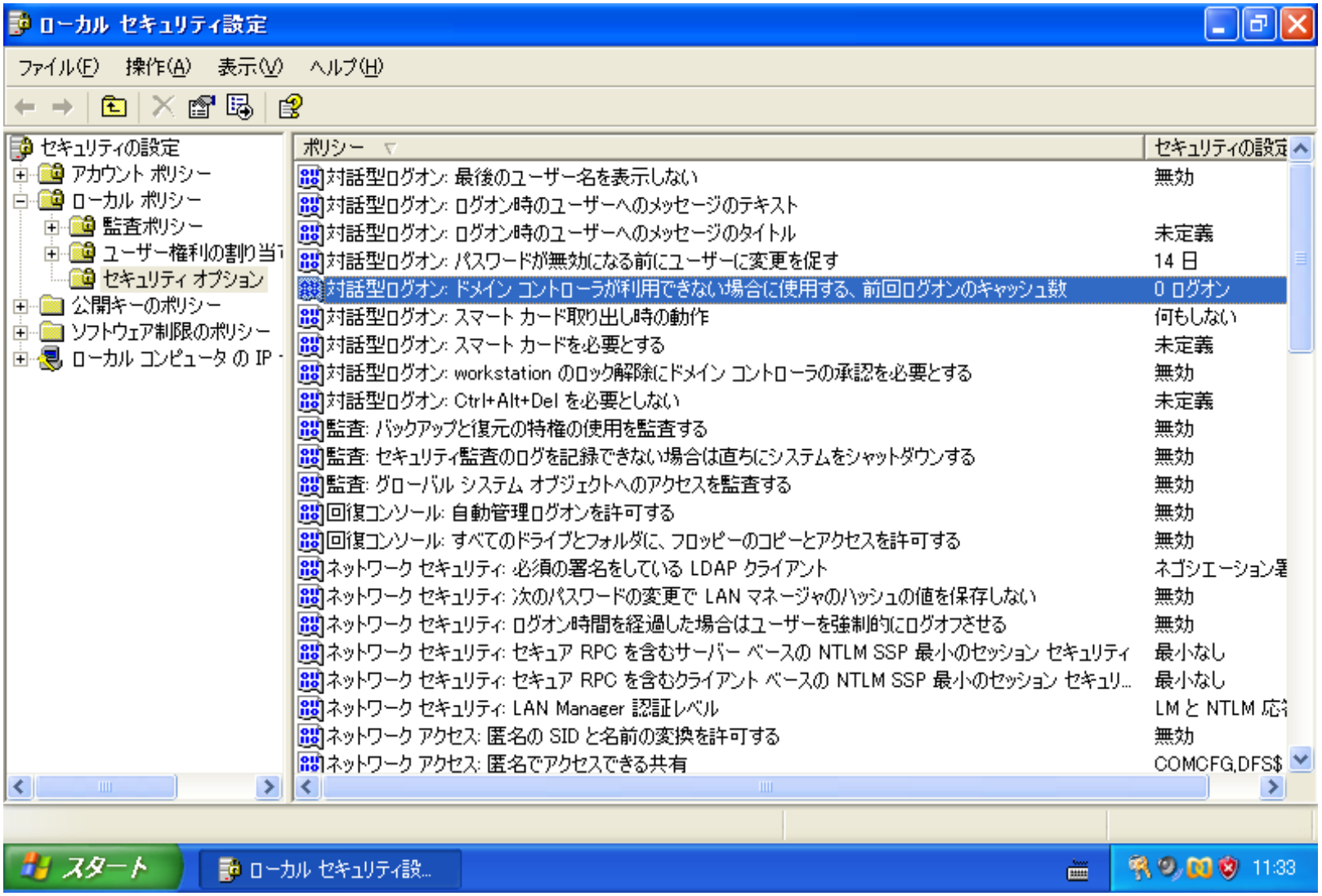
1. PDCのSambaは動作させておく
   - PDC # service smb start
2. BDCの/etc/samba/secrets.tdbを削除
   - BDC # rm /etc/samba/secrets.tdb
3. BDCのローカルSIDを設定
   - BDC # net rpc getsid -S PDC -U Administrator%domainadmin
4. BDCのSambaがスレーブLDAPサーバに接続する際のパスワードを設定
   - BDC # smbpasswd -w ldapadmin

BDCの動作の確認

Begi.net

1. あらかじめWindowsコンピュータのドメイン認証キャッシュに関する設定を変更しておく
   - 「コントロールパネル」→「管理ツール」→「ローカルセキュリティポリシー」→「ローカルポリシー」→「セキュリティオプション」→「対話型ログオン：ドメイン コントローラが利用できない場合に使用する、前回ログオンのキャッシュ数」を0に設定
   - 設定後、Windowsを再起動
2. PDC・BDC両方を動作させる
   - PDCで認証され、ログオンできる
3. PDC、BDC両方を停止する
   - ログオンできなくなる
4. BDCだけ動作させる
   - BDCで認証され、ログオンできる
   - PDC停止中のため、移動プロファイルが更新できないエラーが発生

ログオンキャッシュを無効にする(1)



ログオンキャッシュを無効にする(2)