Samba 3.2 による
Windows ドメインコントローラー/ファイルサーバー
管理者ガイド

作成日: 2008 年 12 月 18 日

更新日: 2009 年 4 月 16 日

リビジョン: 1.2

目次

目次

1. 序章

1.1 本書の目的

本書は Samba を利用して各種 UNIX OS を Windows ドメインコントローラおよびファイルサーバーと利用するための運用ガイドです。

1.2 対象システム

本書が対象とするシステム構成は以下の通りです。

- UNIX OS
  - Sun Solaris 10 (Update 3 以降を推奨)
  - Red Hat Enterprise Linux 4 (Update 5 以降を推奨),
  - Red Hat Enterprise Linux 5 (Update 1 以降を推奨)
  - CentOS 4 (Update 5 以降を推奨)
  - CentOS 5 (Update 1 以降を推奨)
- Windows ドメイン/ファイルサーバーソフトウェア
  - Samba 3.2.6 以降
- ディレクトリサーバーソフトウェア
  - OpenLDAP 2.2.13 以降 (2.3 以降を推奨)
- LDAP ユーザー/グループアカウント管理ツール
  - smbldap-tools 0.9.5 以降
- Windows クライアント
  - Microsoft Windows Vista Business/Enterprise/Ultimate
  - Microsoft Windows XP Professional (サービスパック 2 以降を推奨)
  - Microsoft Windows 2000 Professional (サービスパック 4 以降を推奨)

  ※Microsoft 社によるサポート期間内のバージョンあるいはサービスパックのみ
- 前提条件
  - 各システムの環境構築は完了していること。本書では構築手順に関しては触れておりません。
  - Samba をドメインコントローラとして稼動させること。スタンドアロンサーバーあるいは

ドメインメンバーサーバーは対象外です。

- ユーザーとグループのアカウント情報をすべてディレクトリサーバー（LDAP）で管理すること。
- UNIX 上のファイルシステムが ACL（Access Control List）をサポートし、有効化されていること。

2. ユーザーとグループアカウントの管理

ドメインのユーザーアカウントとグループアカウントの管理手順について解説します。

2.1 ユーザーとグループの仕様

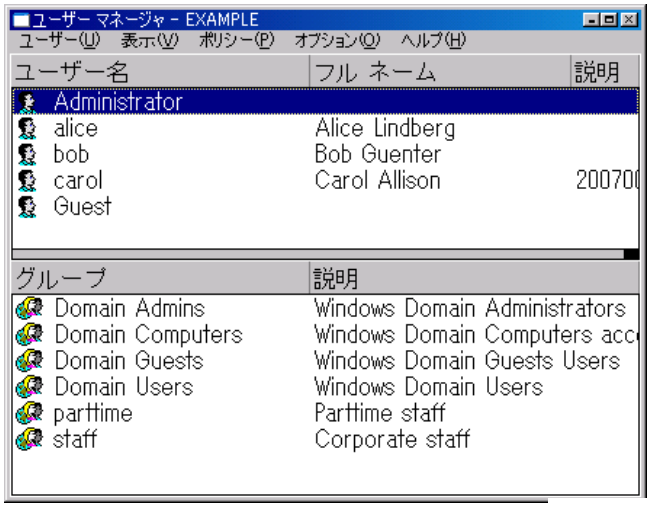
- ユーザー名とグループ名に次のような制限があります。
- 英数字（a～z、A～Z、0～9）、ハイフン「-」、アンダースコア「_」、ピリオド「.」だけを含めることができます。
- 日本語（全角文字、半角カナ）や記号類（\ / { } [ ] ( ) < > + * = : ; , ! ? | @ # $ % & ~ ^ ‘ ’ ”）を含めることはできません。（例外として、コンピュータアカウントには名前の最後に「$」が自動的に付加されます）
- 最大で 20 文字まで指定できます。コマンドラインから 20 文字を超える名前のユーザーあるいはグループを作成することができますが、ドメインユーザーマネージャで管理できなくなります。
- 大文字と小文字は区別されません。例えば、「alice」と「ALICE」は同一と見なされます。
- 同一の名前を持つユーザーとグループを作成することが可能ですが、Windows クライアントはそのような形態を考慮して設計されていません。例えばユーザー「foo」が存在する場合、グループ「foo」を登録するようなことは避けてください。

Samba の仕様により、グループに次のような制限があります。

- グローバルグループのメンバーにグローバルグループを含めることはできません。
- ローカルグループのメンバーにグローバルグループを含めることができますが、Windows と同一の機能が提供できないことがあります。

2.2 ドメインユーザーマネージャのインストール

Windows のドメインユーザーマネージャを利用して GUI でユーザーとグループアカウントを管理することができます。ドメインの Administrator ユーザーなど、ユーザーとグループの管理権限が必要で



す。

ドメインユーザーマネージャのアイコン

2.2.1 ドメインユーザーマネージャによる管理の制限

動作環境に次のような制限があります。

- Windows Vista では動作しません。Windows 2000 または XP でのみ動作します。

Samba の仕様により、ドメインユーザーマネージャの利用に以下のような制限があります。

- ユーザー名とグループ名の変更はできません。
- ローカルアカウント（ローカルユーザー、ローカルグループ）の管理はできません。
- 「ユーザーはパスワードを変更できない」オプションの有効化はできません。
- 「TS の設定」、「ダイヤルイン」の設定は利用できません。

2.2.2 ドメインユーザーマネージャの入手

ユーザーマネージャ（USRMGR.EXE）は以下のいずれかから入手することができます。

- Windows NT Server 4.0 のインストール CD-ROM
  - CD-ROM 内の \clients\srvtools 以下
- Windows NT Server Tools for Windows NT Workstation 4.0
  （マイクロソフト サポート情報 JP173673）
  - http://support.microsoft.com/kb/173673/
    英語版ドメインユーザーマネージャとヘルプファイル（日本語の表示・編集も可能）
- Windows 2000 Service Pack 4 ネットワーク インストール
  - http://www.microsoft.com/japan/technet/downloads/win2k.mspx
    日本語版ドメインユーザーマネージャ（ヘルプファイルは含まれていない）

    ダウンロードした w2ksp4_ja.exe を -x オプションを付けて実行して SP4 の内容を展開し、展開先\i386\usrmgr.ex_ ファイルを expand コマンドで展開する

ドメインユーザーマネージャを Windows クライアントの適当な場所にインストール（コピー）します。

2.2.3 ドメインユーザーマネージャの起動

ドメインユーザーマネージャを利用するには、ドメインのユーザーとグループの管理権限を持つユーザー（ドメインの Administrator など）でプライマリドメインコントローラ（PDC）に接続する必要

があります。

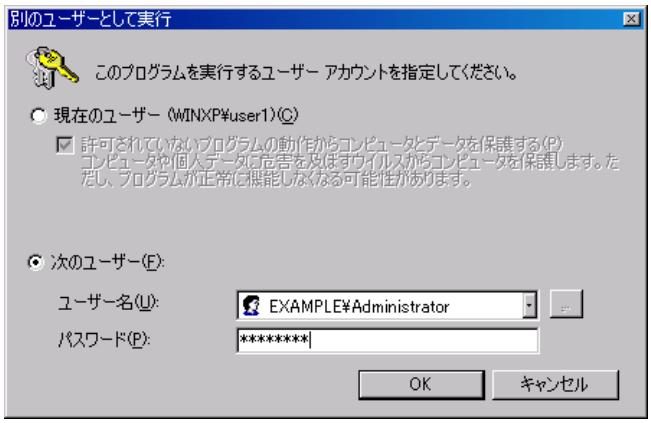
ドメインユーザーマネージャの起動: ドメインログオンを利用している場合

1. Windows のログオン画面で操作対象のドメインを選択し、選択したドメインの任意のユーザー名とパスワードを入力してドメインログオンします。
2. ドメインユーザーマネージャを起動します。
   - 管理権限を持つユーザー（Administrator など）でドメインログオンした場合:

     ドメインユーザーマネージャのアイコンをダブルクリックして起動します。
   - 管理権限を持たないユーザーでドメインログオンした場合:

     ① ドメインユーザーマネージャのアイコンをマウス右ボタンでクリックしてメニューを開き、[別のユーザーとして実行(A)...] をクリックします。[別のユーザーとして実行] ダイアログが開きます。

     ② [別のユーザーとして実行] ダイアログで、[次のユーザー(F)] をクリックし、[ユーザー名(U)] と [パスワード(P)] に管理権限を持つドメインユーザー（「*ドメイン名**ユーザー名*」という形式）とパスワードを入力して [OK] ボタンをクリックします。

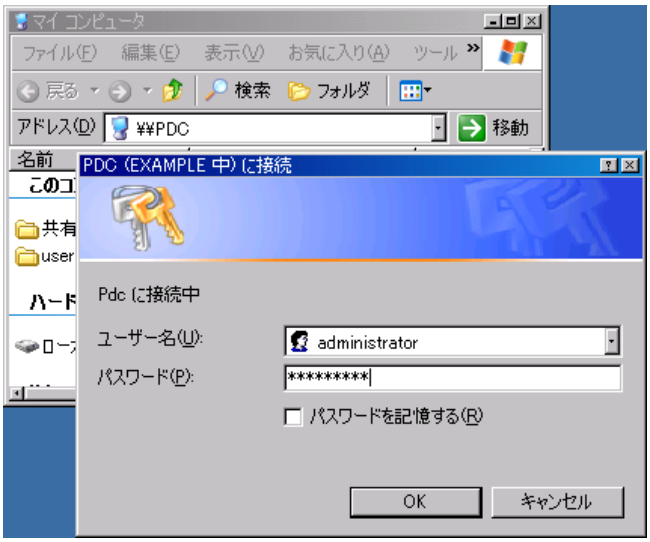


ドメインユーザーマネージャの起動: ドメインログオンを利用しない場合

1. Windows のログオン画面で任意のローカルユーザーでローカルログオンします。※
2. 操作対象のドメインのプライマリドメインコントローラに接続します。
   - エクスプローラの場合:

     ① アドレスバーに「*PDC のサーバー名*」と入力し Enter キーを押します。

     ② [*PDC のサーバー名*（*ドメイン名* 中）に接続] ダイアログが開くので、[ユーザー名(U)] と [パスワード(P)] に管理権限を持つドメインのユーザー名とパスワードを入力して [OK] ボタンをクリックします。

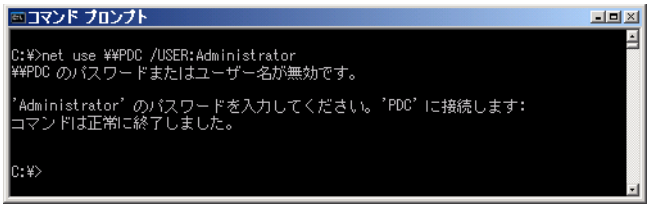


- コマンドプロンプトの場合:

  ① net use コマンドを PDC のサーバー名と管理権限を持つドメインユーザーを指定して実行します:

  net use *PDC のサーバー名* /USER:*ユーザー名*

  ② パスワードを求められるので、指定したユーザーのパスワードを入力します。



3. ドメインユーザーマネージャを起動します。

※ドメインユーザーと同名のローカルユーザーとパスワードでローカルログオンすると、ドメインコントローラに接続した際に自動的に同名のドメインユーザーとして認証・認可されます。そのドメインユーザーに管理権限がない場合、ユーザーとグループを管理することはできません。

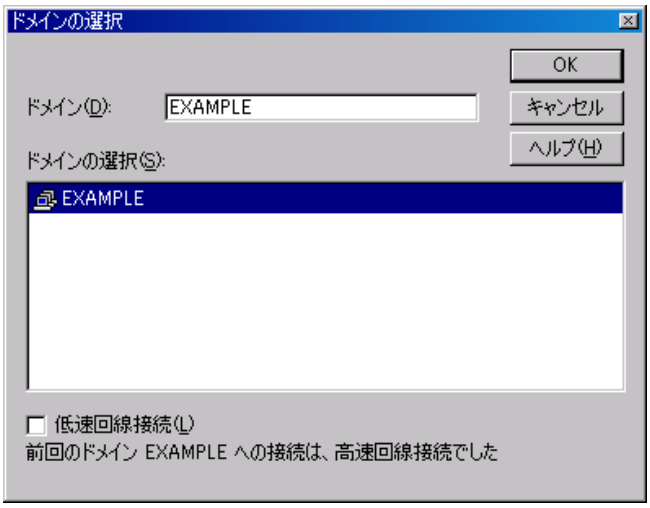
ドメインの選択

ドメインユーザーマネージャを起動したあとに、管理するドメインを選択する必要があります。

1. 最新の日本語版ドメインユーザーマネージャの場合、ドメインユーザーマネージャを起動すると、最初に次のようなダイアログを表示します。[はい(Y)] ボタンをクリックして、次に進みます。

古い日本語版ドメインユーザーマネージャや英語版ドメインユーザーマネージャの場合はローカルアカウントの管理画面になるので、[ユーザー(U)] メニューから [ドメインの選択(S)...] を実行します。

2. [ドメインの選択] ダイアログが表示されるので、管理したいドメインを選択して [OK] ボタンを押します。



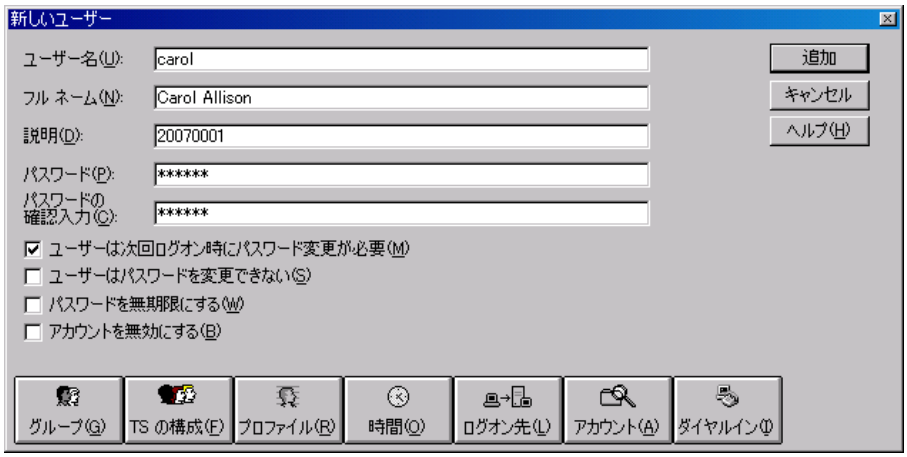
3. 選択したドメインの管理画面が表示されます。

2.3 ドメインユーザーマネージャによるユーザーアカウントの管理

2.3.1 ユーザーの作成

1. ドメインユーザーマネージャの [ユーザー(U)] メニューから [新しいユーザー(U)] を実行します。

2. [新しいユーザー] ダイアログに必要な属性を入力あるいは選択し、[追加] ボタンを押すと、ユーザーが作成されます。



3. 複数のユーザーを作成する場合は、続けて［新しいユーザー］ダイアログで操作します。

4. ユーザーの作成が完了したら、［キャンセル］ボタンを押して［新しいユーザー］ダイアログを閉じます。

5. ドメインユーザーマネージャのユーザー名一覧に作成したユーザーが表示されていない場合は、F5 キーを押すか［表示(V)］メニューから［最新の情報に更新(R)］を実行してください。

2.3.2 ユーザーの変更（パスワードの変更）

1. ドメインユーザーマネージャのユーザー名一覧からユーザー名をダブルクリックするか、ユーザー名を選択して Enter キーもしくは［ユーザー(U)］メニューから［プロパティ(P)］を実行します。

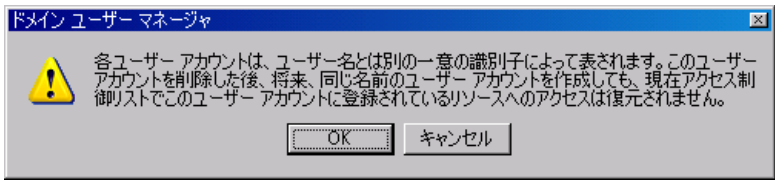
2. ［ユーザーのプロパティ］ダイアログで適宜属性やパスワードを変更し、［OK］ボタンを押すと、ユーザー情報が変更されます。

3. ドメインユーザーマネージャのユーザー名一覧に変更したユーザーが反映されていない場合は、F5 キーを押すか［表示(V)］メニューから［最新の情報に更新(R)］を実行してください。

2.3.3 ユーザーの削除

1. ドメインユーザーマネージャのユーザー名一覧からユーザー名を選択して Delete キーもしくは［ユーザー(U)］メニューから［削除(D)］を実行します。

2. ユーザー名と識別子（SID）の関係に関する警告と削除の確認ダイアログが表示されるので、内容を確認の上［OK］ボタンを押します。



3. 最後の確認ダイアログが表示されるので、［はい(Y)］ボタンを押すとユーザーが削除されます。

4. ドメインユーザーマネージャのユーザー名一覧に削除したユーザーが表示されている場合は、F5 キーを押すか［表示(V)］メニューから［最新の情報に更新(R)］を実行してください。

2.4 ドメインユーザーマネージャによるグループアカウントの管理

2.4.1 グループの作成

1. ドメインユーザーマネージャの［ユーザー(U)］メニューから［新しいグローバル グループ(G)］を実行します。

2. ［新しいグローバル グループ］ダイアログに必要な属性を入力あるいは選択し、［OK］ボタンを押すと、グループが作成されます。

3. ドメインユーザーマネージャのグループ名一覧に作成したグループが表示されていない場合は、F5 キーを押すか［表示(V)］メニューから［最新の情報に更新(R)］を実行してください。

2.4.2 グループの変更

1. ドメインユーザーマネージャのグループ名一覧からグループ名をダブルクリックするか、グループ名を選択して Enter キーもしくは［ユーザー(U)］メニューから［プロパティ(P)］を実行します。

2. ［グローバル グループのプロパティ］ダイアログで必要な属性を変更し、［OK］ボタンを押すと、グループ情報が変更されます。

3. ドメインユーザーマネージャのグループ名一覧に変更したグループが反映されていない場合は、F5 キーを押すか［表示(V)］メニューから［最新の情報に更新(R)］を実行してください。

2.4.3 グループの削除

1. ドメインユーザーマネージャのグループ名一覧からグループ名を選択して Delete キーもしくは［ユーザー(U)］メニューから［削除(D)］を実行します。

2. グループ名と識別子（SID）の関係に関する警告と削除の確認ダイアログが表示されるので、内容を確認の上［OK］ボタンを押します。

3. 最後の確認ダイアログが表示されるので、［はい(Y)］ボタンを押すとグループが削除されます。※

4. ドメインユーザーマネージャのグループ名一覧に削除したグループが表示されている場合は、F5 キーを押すか［表示(V)］メニューから［最新の情報に更新(R)］を実行してください。

※ユーザーのプライマリグループとなっているグループは削除できません。削除しようとすると、アクセスは拒否されます。該当するユーザーのプライマリグループを変更するか、ユーザーを削除する

必要があります。

2.5 コマンドラインによるユーザーアカウントの管理

Samba 付属のコマンドと Samba + LDAP 環境用の管理ツール smbldap-tools を利用することで、UNIX ホストにログインし、コマンドラインでユーザーアカウントを管理することができます。表示以外の操作には root ユーザー権限が必要です。各コマンドの構文については「6.1 smbldap-tools コマンドの構文」を参照のこと。

UNIX 標準のユーザーアカウント管理コマンド useradd, usermod, userdel, passwd, chsh コマンドなどは利用できません。

2.5.1 ユーザーの表示（smbldap-usershow）

smbldap-usershow コマンドでユーザーアカウントの情報を表示することができます。

以下にユーザーアカウント alice の情報を表示する例を示します。

```
# /opt/osstech/sbin/smbldap-usershow alice
dn: uid=alice,ou=Users,dc=example,dc=jp
objectClass: top,person,organizationalPerson,inetOrgPerson,posixAccount,shadowAccount,sambaSamAccount
cn: alice
sn: alice
givenName: alice
uid: alice
uidNumber: 1010
gidNumber: 513
homeDirectory: /home/alice
loginShell: /bin/bash
gecos: User
sambaSID: S-1-5-21-4294967295-4294967295-4294967295-3020
displayName: User
sambaPwdCanChange: 1179213822
sambaPwdMustChange: 2147483647
sambaLMPassword: C187B8085FE1D9DFAAD3B435B51404EE ※
sambaNTPassword: A9F0DD57E1EDAB5BB55A9AC0A99C15EC ※
sambaPasswordHistory: 0000000000000000000000000000000000000000000000000000000000000000
sambaPwdLastSet: 1179213822
sambaAcctFlags: [U          ]
userPassword: {SMD5}0Y+k4a3EwoOG2O+WIDK6CyC/8IE= ※
sambaLogonScript: logon.bat
sambaHomeDrive: H:
```

※ root で実行すると、上記例のようにパスワード情報 sambaLMPassword, sambaNTPassword, userPassword も含めて表示されます。sambaLMPassword と sambaNTPassword はパスワード相当の情報になるため、取り扱いにご注意ください。

LDAP に登録されているすべてのユーザーを表示させる場合は、ユーザー名に「*」を指定します。

```
# /opt/osstech/sbin/smbldap-usershow '*'
```

上記の場合、詳細な情報も一緒に表示されるので、エントリのみを調べたい場合は以下のように grep コマンド と組み合わせてください。

```
# /opt/osstech/sbin/smbldap-usershow '*' | grep ^dn:
```

2.5.2 ユーザーの作成（smbldap-useradd）

smbldap-useradd コマンドでユーザーアカウントを作成することができます。

以下にユーザーアカウント bob を作成する例を示します。この例では、-a オプションは Windows アカウント情報の付加（デフォルトは UNIX アカウント情報のみ）、-m オプションはホームディレクトリの作成、-P オプションはユーザーの作成後にパスワードの入力を求めることを意味します。

```
# /opt/osstech/sbin/smbldap-useradd -a -m -P bob
Changing UNIX and samba passwords for bob
New password: パスワード
Retype new password: パスワード(確認)
```

2.5.3 ユーザーの変更（smbldap-usermod）

smbldap-usermod コマンドでユーザーアカウントを変更することができます。

以下にユーザーアカウント carol を変更する例を示します。この例では、-s オプションで UNIX ログインシェルを /bin/sh に、-g オプションでプライマリグループを staff に変更することを意味します。

```
# /opt/osstech/sbin/smbldap-usermod -s /bin/sh -g staff carol
```

以下にユーザー david を無効にする例を示します。

```
# /opt/osstech/sbin/smbldap-usermod -I david
```

以下にユーザー david を有効にする例を示します。

```
# /opt/osstech/sbin/smbldap-usermod -J david
```

2.5.4 ユーザーの削除（smbldap-userdel）

smbldap-userdel コマンドでユーザーカウントを削除することができます。

以下にユーザーアカウント carol を削除する例を示します。この例では、-r オプションで同時にホームディレクトリを削除することを意味します。

```
# /opt/osstech/sbin/smbldap-userdel -r carol
```

※削除前の確認は行なわれないので、実行する前に確認するようご注意ください。

2.5.5 ユーザーのパスワード変更（smbldap-passwd）

smbldap-passwd コマンドでユーザーのパスワードを変更することができます。

以下にユーザーアカウント carol のパスワードを変更する例を示します。

```
# /opt/osstech/sbin/smbldap-passwd carol
Changing UNIX and samba passwords for carol
New password: 新しいパスワード
Retype new password: 新しいパスワード(確認)
```

2.6 コマンドラインによるグループアカウントの管理

Samba 付属のコマンドと Samba + LDAP 環境用の管理ツール smbldap-tools を利用することで、UNIX ホストにログインし、コマンドラインでグループアカウントを管理することができます。表示以外の操作には root ユーザー権限が必要です。各コマンドの構文については「6.1 smbldap-tools コマンドの構文」を参照のこと。

UNIX 標準のグループアカウント管理コマンド groupadd, groupmod, groupdel, gpasswd コマンドなどは利用できません。

2.6.1 グループの表示（smbldap-groupshow）

smbldap-groupshow コマンドで既存グループアカウントの情報を表示することができます。

以下にグループアカウント staff の情報を表示する例を示します。

```
# /opt/osstech/sbin/smbldap-groupshow staff
dn: cn=staff,ou=Groups,dc=example,dc=jp
objectClass: top,posixGroup,sambaGroupMapping
cn: staff
gidNumber: 1006
sambaSID: S-1-5-21-4294967295-4294967295-4294967295-3013
sambaGroupType: 2
displayName: staff
memberUid: bob,alice
```

LDAP に登録されているすべてのグループを表示するには、グループ名に「*」を指定します。

```
# /opt/osstech/sbin/smbldap-groupshow '*'
```

上記の場合、詳細な情報も一緒に表示されるので、エントリのみを調べたい場合は以下のように grep コマンド と組み合わせてください。

```
# /opt/osstech/sbin/smbldap-groupshow '*' | grep ^dn:
```

2.6.2 グループの作成（smbldap-groupadd）

smbldap-groupadd コマンドでグループアカウントを作成することができます。

以下にグループアカウント parttime を作成する例を示します。この例では、-a オプションは Windows アカウント情報を付加（デフォルトは UNIX アカウント情報のみ）することを意味します。

```
# /opt/osstech/sbin/smbldap-groupadd -a parttime
```

2.6.3 グループの変更（smbldap-groupmod）

smbldap-groupmod コマンドでグループアカウントを変更することができます。

以下にグループアカウント parttime を変更する例を示します。この例では、-m オプションでユーザー alice と bob をメンバーに追加、-x オプションでユーザー carol をメンバーから削除することを意味します。

```
# /opt/osstech/sbin/smbldap-groupmod -m alice,bob -x carol parttime
adding user alice to group parttime
```

```
adding user bob to group parttime
deleting user carol from group parttime
```

2.6.4 グループの削除（smbldap-groupdel）

smbldap-groupdel コマンドでグループアカウントを削除することができます。

以下にグループアカウント parttime を削除する例を示します。

```
# /opt/osstech/sbin/smbldap-groupdel parttime
```

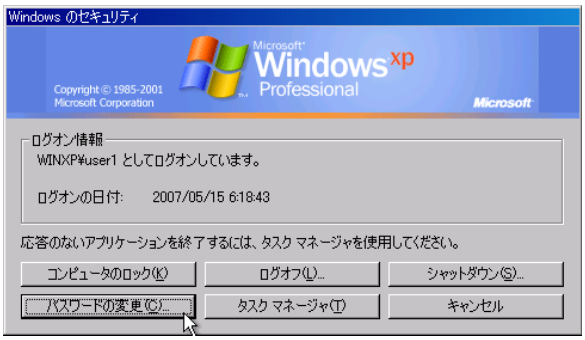
※削除前の確認は行なわれないので、実行する前に確認するようご注意ください。また、Windows ドメインユーザーマネージャの場合と異なり、ユーザーのプライマリグループとなっているグループも削除できます。プライマリグループを削除すると誤動作の原因となりますのでご注意ください。

2.7 一般ユーザーによるパスワードの変更

一般ユーザーは、自身のパスワードを変更することができます。

2.7.1 Windows クライアントからのパスワード変更

1. Windows クライアントに任意のユーザーでログオンします。ローカルログオンでもドメインログオンでも構いません。
2. Ctrl キー、Alt キー、Delete キーを同時に押し、[Windows セキュリティ] ダイアログを開きます。



3. [パスワードの変更(C)...] ボタンを押し、[パスワードの変更] ダイアログを開きます。

4. [ユーザー名(U)] にパスワードを変更したいドメインのユーザー名、[ログオン先(L)] にドメ

イン名、各パスワード入力欄に新旧パスワードを入力し、[OK] ボタンを押します。パスワードが変更されます。

2.7.2 Windows 簡易ログオンの無効化（Windows XP 以降）

Windows ドメインログオンを利用しておらず、かつ簡易ログオン画面（いわゆる「ようこそ画面」）を利用している場合、Windows クライアントからドメインのパスワードを変更することはできません。以下に簡易ログオンを無効化する手順を示します。（Windows XP の場合）

1. Windows クライアントにローカルコンピュータの管理権限を持つユーザー（Administrator など）でローカルログオンします。

2. [スタート] メニューなどからコントロールパネルを開き、[ユーザー アカウント] を開きます。

3. [ユーザーのログオンやログオフの方法を変更する] を開きます。

   オフラインファイルが有効になっている場合、オフラインファイルの設定を変更するかどうかを尋ねるダイアログが表示されるため、[キャンセル] ボタンを押します。

4. [ようこそ画面を使用する(W)] チェックボックスのチェックを外し、[オプションの適用] ボタンを押します。

2.7.3 コマンドラインによるパスワードの変更

UNIX ホストにログインできる一般ユーザーは、Samba 付属の smbpasswd コマンドで自身のパスワードを変更することができます。

```
$ /opt/osstech/bin/smbpasswd
Old SMB password: 現在のパスワード
New SMB password: 新しいパスワード
Retype new SMB password: 新しいパスワード(確認)
Password changed for user carol
```

3. ファイル共有の管理

3.1 ファイル共有の仕様

共有名には次のような制限があります。

- 以下の文字を含めることはできません。手順によってはそれらを含めた共有を作成することができますが、クライアントからアクセスできないなど、予測不可能な障害が発生します。

  %<>*?|/\+=;:",[]

- ダラーマーク「$」を共有名の最後に含めると隠し共有となり、共有名の一覧に表示されなくなります。

- 「global」、「homes」、「printers」という名前は予約されているため、利用できません。

- 最大で 80 文字まで指定できます。

ドメインログオンを利用していない場合、次のような制限があります。

- ドメインログオンでなくローカルログオンしたユーザーで共有にアクセスした場合、アクセス権を編集する際、ドメインのユーザーとグループをアクセス権に追加することはできません。ローカルユーザーには、ドメインユーザーとグループの一覧を取得する権限が与えられていません。

3.2 Windows のコンピュータの管理ツールによるファイル共有の管理

Windows の管理ツールのひとつ「コンピュータの管理」を利用して、ファイルサーバー上のファイル共有を管理することができます。ドメインの Administrator ユーザーなど、ファイル共有の管理権限が必要です。

3.2.1 コンピュータの管理ツールによる管理の制限

Samba の仕様により、コンピュータの管理ツールの利用に以下のような制限があります。

- [システムツール] - [共有フォルダ] 以下の [共有] だけを管理することができます。それ以外の管理には対応していません。

- コンピュータの管理ツールで設定・変更した共有のアクセス権は、Samba の設定ファイル smb.conf ではなく、共有の付加情報を保持するためのデータベースファイル share_info.tdb に保存されます。share_info.tdb はバイナリ形式であるため、直接編集することはできません。

- Samba の設定ファイル smb.conf で定義した共有のアクセス権は、コンピュータの管理ツールから参照・変更することはできません。

3.2.2 コンピュータの管理ツールの起動

コンピュータの管理ツールでファイルサーバーの共有を管理するには、共有の管理権限を持つユーザー（ドメインの Administrator など）でファイルサーバーに接続する必要があります。

コンピュータの管理ツールの起動：ドメインログオンを利用している場合

1. Windows のログオン画面で操作対象のファイルサーバーが属するドメインを選択し、選択したドメインの任意のユーザーでドメインログオンします。

2. コンピュータの管理ツールを起動します。

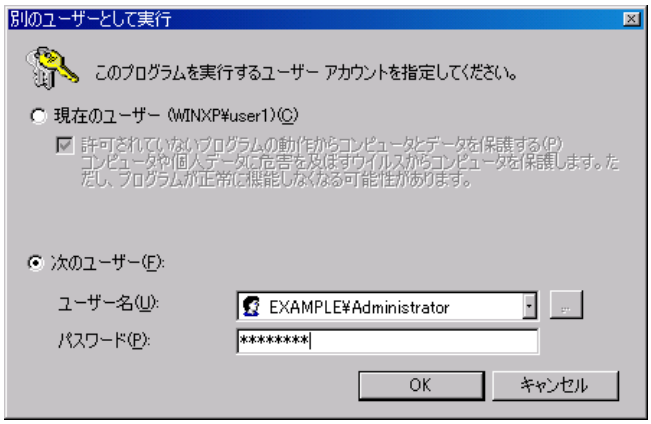
   - 共有の管理権限を持つユーザー（Administrator など）でドメインログオンした場合:

     [スタート] メニュー - [すべてのプログラム(P)] - [管理ツール] フォルダの [コンピュータの管理] アイコンをクリックして起動します。

   - 共有の管理権限を持たないユーザーでドメインログオンした場合:

     ① [スタート] メニュー - [すべてのプログラム(P)] - [管理ツール] フォルダの [コンピュータの管理] アイコンをマウス右ボタンでクリックしてメニューを開き、[別のユーザーとして実行(U)...] をクリックします。

     ② [別のユーザーとして実行] ダイアログが開くので、[次のユーザー(F)] をクリックし、[ユーザー名(U)] と [パスワード(P)] に管理権限を持つドメインユーザー（「*ドメイン名**ユーザー名*」という形式）とパスワードを入力して [OK] ボタンをクリックします。



コンピュータの管理ツールの起動：ドメインログオンを利用しない場合

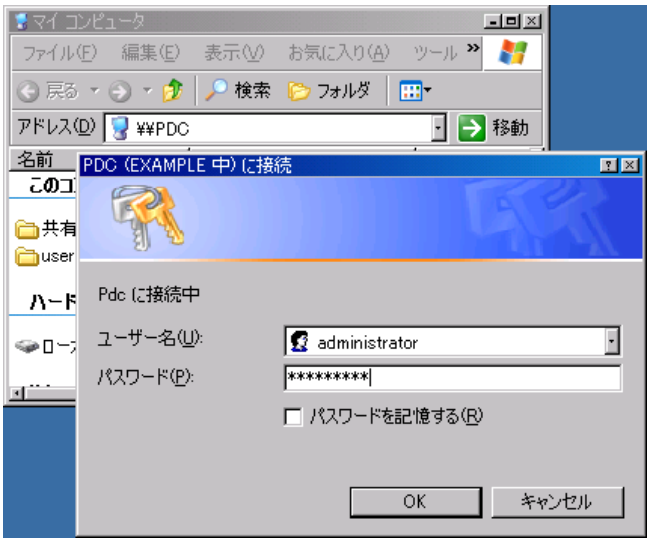
1. Windows のログオン画面で任意のローカルユーザーでローカルログオンします。※

2. 操作対象のファイルサーバーに接続します。

   - エクスプローラの場合:

     ① アドレスバーに「*ファイルサーバー名*」と入力し Enter キーを押します。

     ② [*ファイルサーバー名*（*ドメイン名* 中）に接続] ダイアログが開くので、[ユーザー名(U)]と [パスワード(P)] に管理権限を持つドメインのユーザー名とパスワードを入力して [OK] ボタンをクリックします。

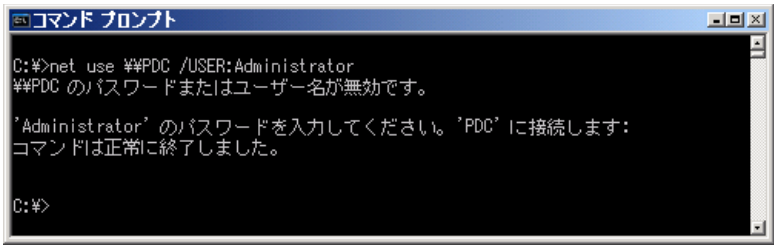


- コマンドプロンプトの場合:

  ① net use コマンドをファイルサーバー名と管理権限を持つドメインユーザーを指定して実行します:

  net use *ファイルサーバー名* /USER:*ユーザー名*

  ② パスワードを求められるので、指定したユーザーのパスワードを入力します。



3. [スタート] メニュー - [すべてのプログラム(P)] - [管理ツール] フォルダの [コンピュータの管理] アイコンをクリックして起動します。

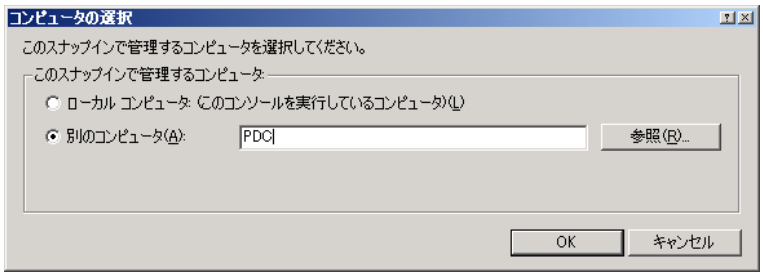
※ドメインユーザーと同名のローカルユーザーとパスワードでローカルログオンすると、ファイルサーバーに接続した際に自動的に同名のドメインユーザーとして認証・認可されます。そのドメインユーザーに管理権限がない場合、ユーザーとグループを管理することはできません。

ファイルサーバーの選択

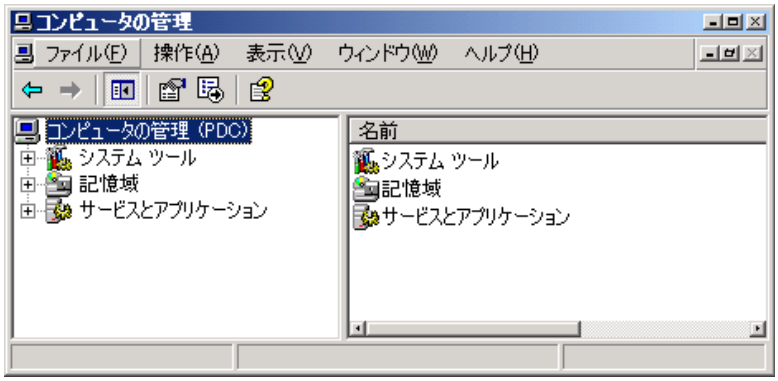
コンピュータの管理ツールを起動したあとに、管理するファイルサーバーを選択する必要があります。

1. コンピュータの管理ツールを起動すると、最初はローカルコンピュータの管理画面が表示されます。[操作(A)] メニューの [別のコンピュータへ接続(C)...] を実行し、[コンピュータの選択] ダイアログを開きます。

2. [別のコンピュータ(A)] にファイルサーバー名を入力し、[OK] ボタンを押します。

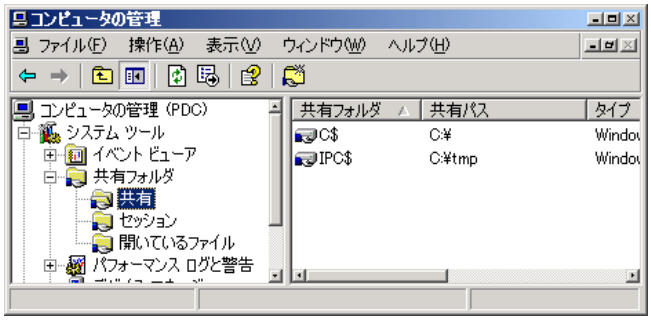


3. ファイルサーバーの管理画面が表示されます。



3.2.3 ファイル共有の一覧表示

コンピュータの管理ツール画面の左側のペイン内から［システム ツール］-［共有フォルダ］以下の［共有］を開くと、右側のペインに共有の一覧が表示されます。



標準で以下の共有が定義されています。

- C$（D$, E$ ... も同様）

  デフォルト共有。ファイル共有に利用できるファイルサーバー上のディレクトリを指しており、共有を作成する際はこの中から共有したいディレクトリを選択します。

  この共有は削除（停止）しないようにご注意ください。

- IPC$

  リモート IPC 共有。サーバーをリモート管理するための IPC（Inter-Process

Communication, プロセス間通信）機能を提供する特殊な共有です。操作することはできません。

共有一覧の各項目の意味は以下の通りです。

- 共有フォルダ

  クライアントからアクセスする際に利用される共有の名前です。

- 共有パス

  共有しているサーバー上のディレクトリ（フォルダ）です。

  すべて「C:\～」と表示されますが、UNIX にはドライブの概念はなく、実際には「C:\」がファイルサーバー上のルートディレクトリ（/）を示します。同様に、例えば「C:\share\project」のように表示されている場合は、ファイルサーバー上の /share/project ディレクトリを共有していることを意味します。

- タイプ

  共有の種類（プロトコル種別）です。

- クライアント接続数

  共有に接続しているクライアントの数です。

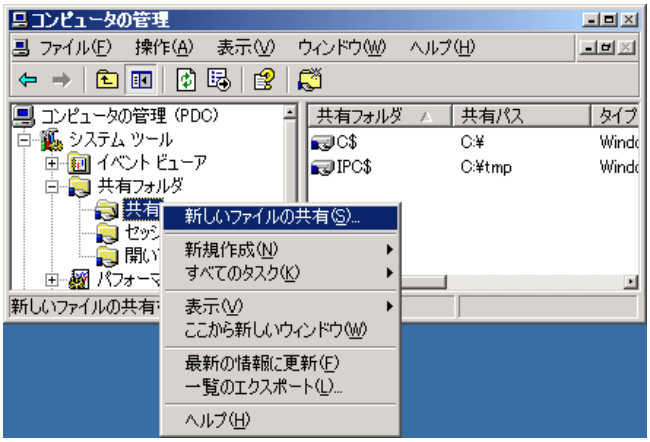
- コメント

  共有のコメントです。任意の文字列を設定することができます。

3.2.4 ファイル共有の作成

1. コンピュータの管理ツール画面の左側のペイン内から［システム ツール］-［共有フォルダ］以下の［共有］を開きます。

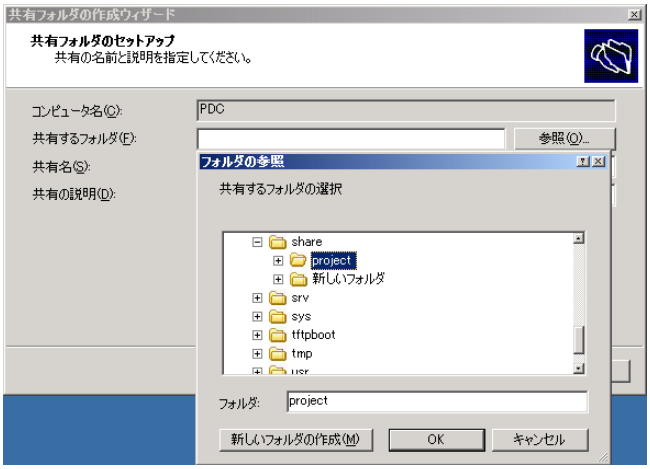
2. ［操作(A)］メニューから［新しいファイルの共有(S)...］を実行するか、左側ペインの［共有］をマウス右ボタンでクリックし、メニューから［新しいファイルの共有(S)...］を実行し、［共有フォルダの作成ウィザード］を開きます。



3. ［次へ(N) >］ボタンを押し、［共有フォルダのセットアップ］画面に移動します。

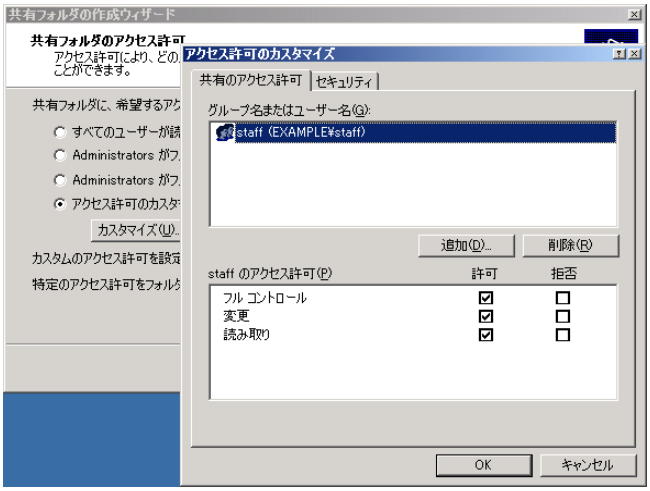
4. [参照(O)...] ボタンを押し、[フォルダの参照] ダイアログを開きます。

5. [フォルダの参照] ダイアログ内のファイルサーバーのディレクトリ一覧から共有するディレクトリを選択し、[OK] ボタンを押します。この画面内でディレクトリを作成・変更・削除することもできます。



6. [共有名(S)] と [共有の説明(D)] (コメント) の欄に入力し、[次へ(N) >] ボタンを押します。

7. [共有フォルダのアクセス許可] 画面で適宜アクセス権を設定し、[次へ(N) >] ボタンを押します。この時点で共有が作成されます。



8. 最後の画面で [完了] ボタンを押し、ウィザードを終了します。

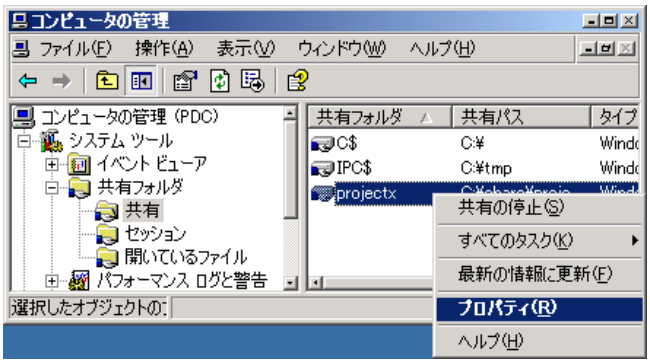
3.2.5 ファイル共有の変更

1. コンピュータの管理ツール画面の左側のペイン内から [システム ツール] - [共有フォルダ] 以下の [共有] を開きます。

2. 右側ペインの共有一覧から共有を選択し、[操作(A)] メニューから [プロパティ(R)] を実行

するか、共有名をマウス右ボタンでクリックしてメニューから［プロパティ(R)］を実行し、［*共有名* プロパティ］ダイアログを開きます。

3. 適宜変更を加えたら［OK］ボタンを押し、ダイアログを閉じます。

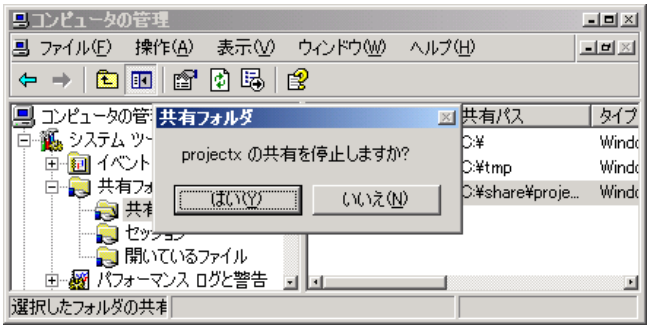


3.2.6 ファイル共有の削除（停止）

1. コンピュータの管理ツール画面の左側のペイン内から［システム ツール］-［共有フォルダ］以下の［共有］を開きます。

2. 右側ペインの共有一覧から共有を選択し、[操作(A)］メニューから［共有の停止(S)］を実行するか、共有名をマウス右ボタンでクリックしてメニューから［共有の停止(S)］を実行します。

3. 確認のダイアログが表示されるので、[はい(Y)］ボタンを押します。



3.3 アクセス制御

アクセス制御には共有フォルダ全体のアクセス制御と、共有フォルダ内のフォルダ/ファイルごとのアクセス制御の２種類が存在します。

3.3.1 共有フォルダのアクセス制御

共有フォルダのアクセス制御に利用できるパラメータを以下に示します。

```
[共有名]
valid users = アクセスを許可するユーザー/グループ
invalid users = アクセスを禁止するユーザー/グループ
```

```
write list = ファイル・フォルダの更新を許可するユーザー/グループ
read list = ファイル・フォルダの読み取りのみ許可するユーザー/グループ
hosts allow = アクセスを許可するクライアントのホスト名、IP アドレス、ネットワークアドレス
hosts deny = アクセスを禁止するクライアントのホスト名、IP アドレス、ネットワークアドレス
```

ユーザーを指定する場合は、ユーザー名を空白やカンマで区切って羅列します。

```
valid users = takeuchi, takeda
```

グループを指定する場合は、グループ名の先頭にアットマーク「@」を指定します。

```
valid users = @manager
invalid users = @sales, guest
```

ネットワークアドレスでアクセス制御をする場合は、ネットワークアドレスとネットマスク長を指定します。

```
hosts allow = 192.168.0.0/16
```

3.3.2 共有内のフォルダ/ファイルのアクセス制御

共有内にあるフォルダやファイルのアクセス制御は ACL の利用の有無で管理方法が異なります。

ACL を使用しない場合

- アクセス権表示　　：ls -l コマンド
- アクセス権変更：　chmod コマンド
- 所有者の変更：　　chown コマンド
- グループの変更：　chgrp コマンド

ACL を使用している場合

- アクセス権表示：　getfacl コマンド

  （ls -l の結果と一致しないことがあります。getfacl の表示を優先してください）
- アクセス権変更：　setfacl コマンド
- 所有者の変更：　　chown コマンド
- グループの変更：　chgrp コマンド

3.3.3 Samba で ACL を使うときの注意事項

Linux や UNIX で ACL(Access Control List)に対応したファイルシステムを利用することで、Samba のファイルサーバー機能で ACL を利用することができます。しかしながら Linux/UNIX が提供する ACL 機能は POSIX(UNIX 標準)に準拠しており、Windows の ACL 機能とは一部機能や動作が異なります。

このためシンプルな使い方では問題になりませんが、Windows で複雑な ACL を指定していたものを Samba に移行すると問題が発生することがあります。

ここではその違いと問題点について解説します。

Windows ACL と Samba ACL の違い

- POSIX ACL では UNIX の u(ser),g(roup),o(ther)に対して、r(参照), w(更新), x(実行)を付与していく形で設定しますが、この 3つ(ugo)の設定は必須になります。g のみを設定したり、g と o の 2つのみ設定するということはできません。
- Windows の場合、ACL の属性として Samba よりも細かく権限を設定できます。

    1. フォルダのスキャン/ファイルの実行
    2. フォルダの一覧/データの読み取り
    3. 属性の読み取り
    4. 拡張属性の読み取り
    5. ファイルの作成/データの書き込み
    6. ファイルの作成/データの追加
    7. 属性の書き込み
    8. 拡張属性の書き込み
    9. 削除
    10. アクセス許可の読み取り
    11. アクセス許可の変更
    12. 所有権の取得

- これらの権限は Samba の ACL で以下のように対応しています。

    1,2,3,4,10　　→ r(参照)

    5,6,9　　→ w(更新)

    7,8,11,12 は所有者および管理者（uid=0 のユーザー）のみ可能で Samba ACL に対応するものはありません。

- POSIX ACL の x (実行)は Windows のフォルダのスキャン、一覧に対応し、ファイルの実行には対応しません。
- そのため Samba では所有者の x(実行)を DOS のアーカイブ属性にグループの x(実行)を DOS のシステム属性に Other の x(実行)を DOS の隠しファイル属性にマッピングしています。
- Windows では Everyone フルコントロールがデフォルトですが、これは UNIX の user::rwx,group::rwx,other::rwx に相当します。

    (Samba では other::rwx を Everyone フルコントロールにマッピングしていますが、これは正確ではありません)

- Samba ACL ではファイルの所有者はユーザーのみでグループとすることができません。その代わりファイルにはグループ属性が存在します。

- Windows ではファイルの所有者をユーザーにもグループにもすることができますが、グループ属性に対応するものがありません。

- Windows ではファイルのアクセス権をフルコントロールにすればファイル所有者以外でもアクセス権や ACL を変更することが可能ですが、Linux/UNIX 上では所有者以外アクセス権や ACL を変更することができません。(弊社提供の Samba ではこちらの問題を修正してあります。)

MS-Office 製品の問題

Word や Excel などの MS-Office 製品はファイルを編集し、上書き保存する場合(ノートパッドなどのテキストエディタとは異なり)正確な意味での上書きを行いません。そのため既存のアクセス権設定が変わってしまうことがあります。(アクセス権や ACL が変更されてしまうことがある)

例えば、Word は「文書.doc」を上書き保存する時、以下のシーケンスで行います。

1. 更新後のファイルを「文書Ａ.doc」で新規作成
2. 更新前のファイルを「文書.doc」→「文書Ｂ.doc」に RENMAE
3. 「文書Ａ.doc」→「文書.doc」に RENMAE
4. 「文書Ｂ.doc」のアクセス権を「文書.doc」に設定
5. 「文書Ｂ.doc」を削除

問題は１と５の時点で発生します。まず１の時点では所有者とグループ属性が変わってしまいます。Windows でも所有者は変わるのですが、グループ属性が存在しません。

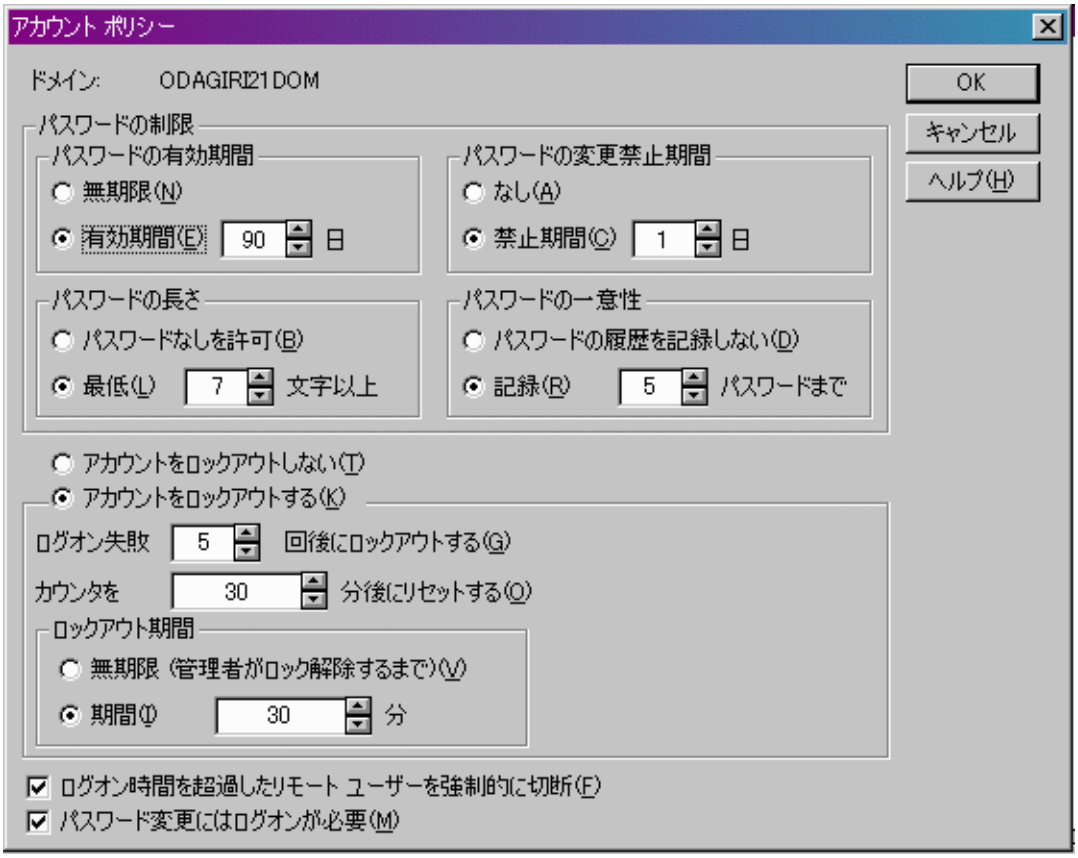
また、５の時点で Office 2000 は「文書.doc」と「文書Ｂ.doc」のアクセス権と許可属性を比較し、ある条件を満たすと「文書.doc」の ACL が既存と異なってしまうことがあります。

※ Samba 3.0.14a 以降かつ Office 2002 以降では正しく ACL が設定されるようになっていますが、Office 2000 では問題が発生することがあります。

4. ドメインポリシーの管理

4.1 アカウントポリシーの管理

2.2章で紹介したドメインユーザーマネージャの「ポリシー」メニュー「アカウント」からアカウントポリシーを起動し、ドメイン全体のアカウントポリシーを設定できます。



上記ダイアログ ボックスでは、すべてのユーザーアカウントがパスワードをどのように使わなければならないか、および不正なログオンが連続して行われた後にユーザーアカウントが自動的にロックアウトされるようにするかどうかを制御します。

- [パスワードの有効期間]
- [パスワードの変更禁止期間]
- [パスワードの長さ]
- [パスワードの一意性]
- [アカウントをロックアウトしない]
- [アカウントをロックアウトする]

- ［ログオン時間を超過したリモート ユーザーを強制的に切断］
- ［パスワード変更にはログオンが必要］

上記のアカウントの原則を管理するには以下の手順で行います。

1. ［原則］メニューの［アカウント］をクリックします。
2. 必要に応じて、［パスワードの有効期間］、［パスワードの変更禁止期間］、［パスワードの長さ］、および［パスワードの一意性］の各グループで値を入力します。

   または、［無期限］、［なし］、［パスワードなしを許可］、［パスワードの履歴を記録しない］をクリックします。
3. ［アカウントをロックアウトする］をクリックし、次に［ログオン失敗ー回後にロックアウトする］ボックスと［カウンタをー分後にリセットする］ボックスに値を入力します。また、［ロックアウト期間］で値を設定します。

   または、［アカウントをロックアウトしない］をクリックします。
4. 必要に応じて、［ログオン時間を超過したリモート ユーザーを強制的に切断］チェック ボックスをオンまたはオフにします。
5. 必要に応じて、［パスワード変更にはログオンが必要］チェック ボックスをオンまたはオフにします。

［OK］をクリックする前に、次のガイドラインに沿った設定が行われているかどうかを確認してください。

- ［パスワードの変更禁止期間］の［なし］を選択した場合は、［パスワードの一意性］の［パスワードの履歴を記録しない］もクリックしてください。
- ［パスワードの一意性］で値を入力した場合は、［パスワードの変更禁止期間］の［禁止期間ー日］にも値を入力してください。

※上記はマイクロソフト社のアカウントポリシーのヘルプに記載されている事項なので守ることを推奨します。マイクロソフト社のドキュメントでは、［パスワードの一意性］を設定し、［パスワードの変更禁止期間］を設定しないと［パスワードの一意性］が有効にならない、とありますが、実際には機能します。

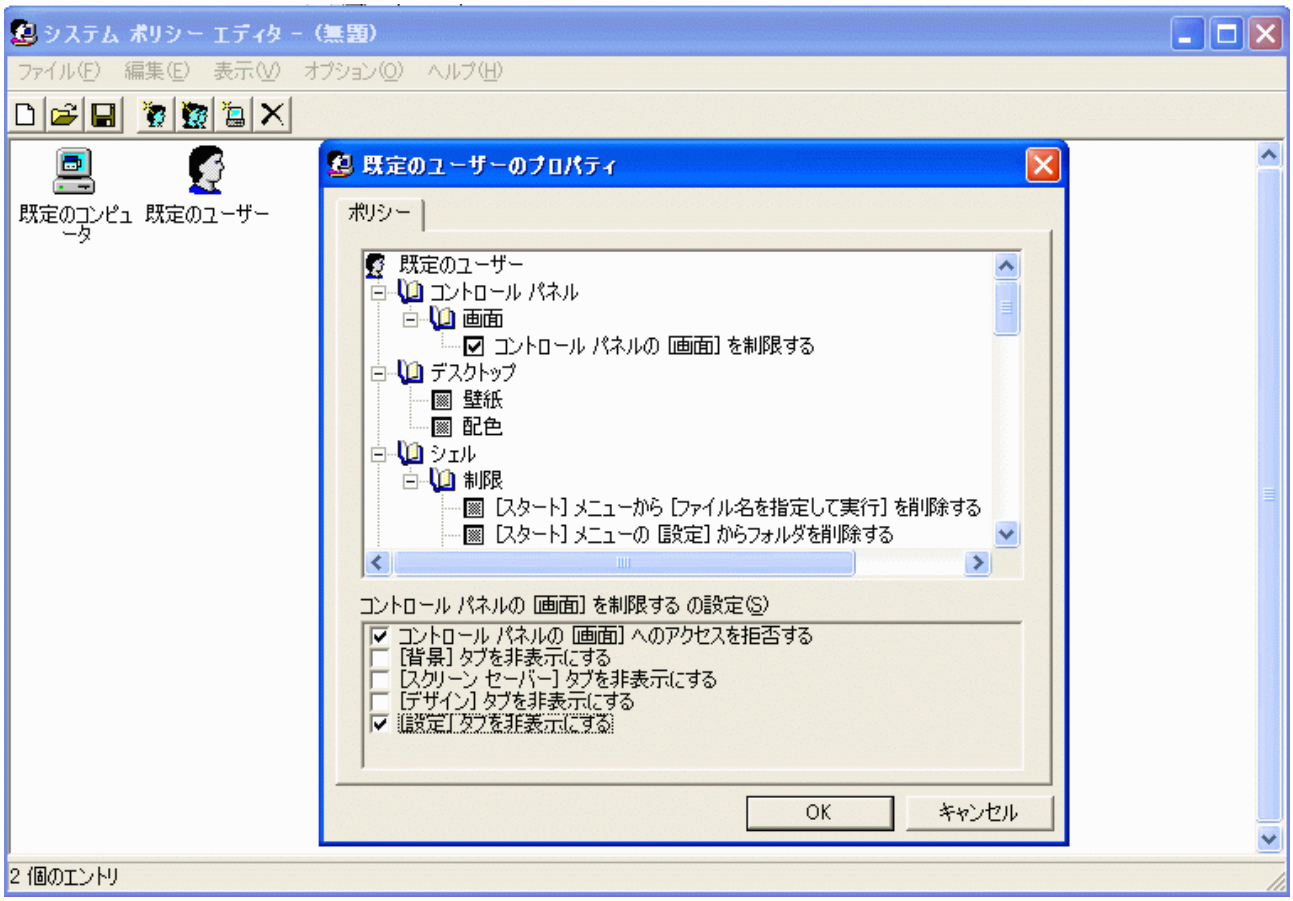
各オプションで設定できる値は、次のとおりです。

- ［パスワードの有効期間］および［パスワードの変更禁止期間］で指定できる日数は、1 から 999 までです。
- ［パスワードの長さ］で指定できる文字数は、1 から 14 までです。
- ［パスワードの一意性］の［記録ーパスワードまで］に指定できるパスワード数は、1 から 24 までです。

4.2 システムポリシーの管理

システムポリシーを使うと Windows クライアントを含めてさらにセキュリティを強化できます。ただし、この機能は Windows NT 4.0 互換の機能なため、Windows NT 4.0 もしくは Windows 2000 サーバーのポリシーエディタが必要になります。

ポリシーエディタ(POLEDIT.EXE)を使ってポリシーファイル（ファイル名はNTCONFIG.POL）を作成し、Sambaの NETLOGON 共有にコピーするだけで利用できます。



5. ドメインの管理

Windows クライアントのドメインへの参加手順とコンピュータアカウント（マシンアカウントとも呼ばれる）の管理手順について解説します。Windows クライアントをドメインに参加させると、ドメインにクライアントマシンごとのコンピュータアカウントが作成されます。

Windows クライアントをドメインに参加させるには、参加させる Windows クライアントの管理権限（ローカルユーザー Administrator など）と、ドメインのコンピュータアカウントの管理権限（ドメインユーザー Administrator など）または UNIX の管理権限（root など）が必要です。

5.1 ドメインメンバーとコンピュータアカウントの管理

ドメインに参加できるのは特定のエディションの Windows に限られます。

- ドメインメンバー機能を持つ Windows:
  - Windows Server シリーズ（2003, 2000）
  - Windows Vista Business/Enterprise/Ultimate シリーズ
  - Windows XP Professional
  - Windows 2000 Professional
- ドメインメンバー機能を持たない Windows:
  - Windows Vista Home シリーズ
  - Windows XP Home

ドメインに参加させる Windows クライアントのコンピュータ名に次のような制限があります(DNS のドメインサフィックス部分は除く)。

- 英数字（a～z、A～Z、0～9)、ハイフン「-」だけを含めることができます。
- 数字だけが含まれる名前を指定することはできません。
- 日本語（いわゆる全角文字）や記号類などを含めることはできません。
- 最大で 15 文字まで指定できます。15 文字を超える名前のコンピュータ名を設定することもできますが、ドメインメンバーにすることができなくなります。
- 大文字と小文字は区別されません。例えば、「alice-pc」と「ALICE-PC」は同一と見なされます。

5.2 Windows クライアントのドメインへの参加

1. Windows クライアントにローカルコンピュータの管理権限を持つユーザー（Administrator など）でローカルログオンします。
2. [スタート] メニューなどからコントロールパネルを開き、[システム] を開きます。

3. [コンピュータ名の変更] ダイアログを開きます。

   Windows Vista の場合:

   [コンピュータ名、ドメイン、ワークグループの設定] の [設定と変更] ボタンを押します。

   Windows XP の場合:

   [システムのプロパティ] ダイアログの [コンピュータ名] タブを開き、[変更(C)...] ボタンを押します。

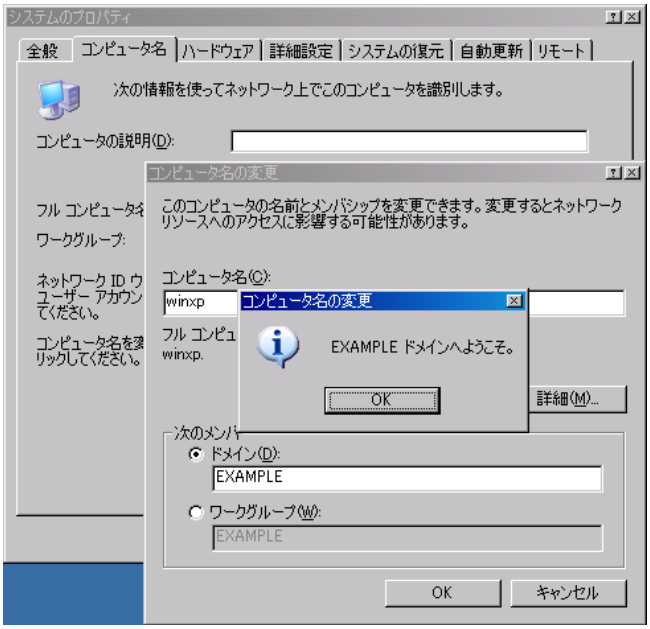
   Windows 2000 の場合:

   [システムのプロパティ] ダイアログの [ネットワーク ID] タブを開き、[プロパティ(R)] ボタンを押します。

4. [コンピュータ名の変更] ダイアログの [次のメンバ] で [ドメイン(D)] を選択し、入力欄に参加先のドメイン名を入力して [OK] ボタンを押します。

5. コンピュータアカウントの管理権限を持つユーザー（ドメインの Administrator など）のユーザー名とパスワードの入力を求められるので、適宜入力し、[OK] ボタンを押します。これにより、自動的にコンピュータアカウントが作成されます。

6. [*ドメイン名* へようこそ。] という表示のダイアログが表示されるので、[OK] ボタンを押します。



7. コンピュータの再起動が必要である旨を示すダイアログが表示されるので、[OK] ボタンを押します。

8. [システムのプロパティ] ダイアログの [OK] ボタンを押します。

9. 再起動するかどうかを問うダイアログが表示されるので、[はい(Y)] ボタンを押して再起動します。

5.3 コマンドラインによるコンピュータアカウントの管理

Samba 付属のコマンドと Samba + LDAP 環境用の管理ツール smbldap-tools を利用することで、UNIX ホストにログインし、コマンドラインでコンピュータアカウントを管理することができます。実行には root ユーザー権限が必要です。各コマンドの構文については「6.1 smbldap-tools コマンドの構文」を参照のこと。

5.3.1 コンピュータアカウントの作成（smbldap-useradd）

smbldap-useradd コマンドでコンピュータアカウントを作成することができます。コンピュータアカウントは、Windows クライアント上でのドメイン参加手順の過程で自動的に作成されるため、通常は手動による作成は不要です。

以下にコンピュータアカウント alice-pc を作成する例を示します。この例では、-w オプションは Windows コンピュータアカウント情報の付加（デフォルトは UNIX アカウント情報のみ）を意味します。-w オプションはコンピュータアカウントを作成する場合は必須です。コンピュータアカウントにホームディレクトリやシェルなどは不要です。

```
# /opt/osstech/sbin/smbldap-useradd -w alice-pc
```

コンピュータアカウントは、コンピュータ名にダラーマーク「$」を付加した名前で登録されます。上記実行例の場合、「alice-pc$」という名前のアカウントになります。

5.3.2 コンピュータアカウントの削除（smbldap-userdel）

smbldap-userdel コマンドでコンピュータアカウントを作成することができます。コンピュータアカウントが削除された Windows クライアントからはドメインログオンができなくなります。

以下にコンピュータアカウント alice-pc を削除する例を示します。コンピュータアカウントはコンピュータ名にダラーマーク「$」を付加した名前で登録されるため、引数には「alice-pc$」を指定する必要があります。

```
# /opt/osstech/sbin/smbldap-userdel alice-pc$
```

5.4 管理者パスワードの変更

5.4.1 LDAP(cn=Manager ユーザー)

このユーザーの変更箇所は多数あるので、必ず忘れずに全てのパスワードを変更するようにしてください。（例として新規のパスワードを secret とします。）

/etc/smbldap-tools/smbldap_bind.conf

```
slavePw="secret"
masterPw="secret"
```

上記両方とも変更してください。

/etc/samba/secrets.tdb

このファイルは手動ではなく、以下のコマンドによって変更可能となります。

```
# smbpasswd -w secret
```

LDAP 内の設定

LDAP に登録されているユーザーのパスワードを変更します。一般ユーザーとは違い、こちらは smbldap-tools では変更できませんので注意してください。

```
# ldappasswd -x -D cn=Manager,dc=example,dc=co,dc=jp -W cn=Manager,dc=example,dc=co,dc=jp -S
```

まず、cn=Manager ユーザーの新しいパスワードを入力します。

```
New password: パスワード
Re-enter new password: パスワード
```

次に今まで使用していた cn=Manager のパスワードを入力します。

```
# ldappasswd -x -D cn=Manager,dc=example,dc=co,dc=jp -W -S cn=Manager,dc=example,dc=co,dc=jp
Enter LDAP Password: パスワード
```

成功すると、以下のようなメッセージが表示されます。

```
Result: Success (0)
```

同様に複製者のパスワード変更は以下のように実施します。

```
# ldappasswd -x -D cn=Manager,dc=example,dc=co,dc=jp -W -S cn=replica,dc=example,dc=co,dc=jp
```

注意点として、Samba が使用するパスワードは上記のコマンドでは変更されません。よって LDAP 管理者のパスワード変更時のみの利用としてください。

パスワードが変更されているか確認するには以下の方法を実施します。

```
# ldapsearch -x -W -D cn=manager,dc=example,dc=co,dc=jp
```

ここで新規に設定したパスワードで情報が取得できればパスワードの設定は成功していますが、間違っている場合には以下のエラーが表示されます。

```
ldap_bind: Invalid credentials (49)
```

5.4.2 Samba(Administrator ユーザー)

Administrator ユーザーのパスワード変更方法は一般ユーザーと同様です。

```
# /opt/osstech/sbin/smbldap-passwd Administrator secret
```

ここでは secret が新規パスワードとなります。

6. コマンドの使用方法

6.1 smbldap-tools コマンドの構文

smbldap-tools は、UNIX と Windows（Samba）のユーザーアカウントやグループアカウントの情報を LDAP サーバーで維持・管理するためのツール群です。

6.1.1 smbldap-passwd

ユーザーのパスワードを変更するコマンドです。管理権限を持つユーザーは任意のユーザーのパスワードを旧パスワードの入力なしに変更することができます。

構文

`smbldap-passwd` *[オプション] [ユーザー名]*

オプション

- `-s`
  ユーザーの Windows パスワードのみを変更する。
- `-u`
  ユーザーの UNIX パスワードのみを変更する。

6.1.2 smbldap-usershow

ユーザーの情報を表示するコマンドです。管理権限を持つユーザー（root など）で実行すると、パスワード情報も表示することができます。パスワード情報はハッシュ化されていますが、平文のパスワードに相当する情報であるため、取り扱いにはご注意ください。

構文

`smbldap-usershow` *ユーザー名*

オプション

オプションはない。

6.1.3 smbldap-useradd

ユーザーを新規作成するコマンドです。実行には管理権限が必要です。

構文

`smbldap-useradd` *[オプション] ユーザー名*

オプション

- -a
  ユーザーを Windows ユーザーアカウントとして作成する。このオプションを省略すると UNIX ユーザーアカウント情報のみ作成され、Windows（Samba）サービスは利用できない。

- -w
  ユーザーを Windows コンピュータアカウントとして作成する。

- -i
  ユーザーを Windows ドメイン間信頼アカウントとして作成する。

- -u *UID*
  ユーザーに割り当てる UID（UNIX ユーザー ID）値を指定する。

- -g *グループ名*
  ユーザーのプライマリグループを指定する。

- -G *グループ名[,グループ名...]*
  ユーザーに割り当てるサブグループを指定する。複数割り当てる場合はカンマ「,」で区切って列挙する。

- -d *ディレクトリ*
  ユーザーの UNIX ホームディレクトリの場所を指定する。

- -m
  ホームディレクトリを作成し、ホームディレクトリのテンプレート /etc/skel 以下をコピーする。

- -k *ディレクトリ*
  ホームディレクトリの作成に利用するテンプレートディレクトリを指定する。（-m オプションと同時に利用）

- -s *シェル*
  ユーザーの UNIX ログインシェルを指定する。

- -c *コメント*
  ユーザーの付加情報（コメント）を指定する。

- -p *パスワード*

  引数に指定されたパスワードを指定する。（この機能は弊社独自の機能）

- -A *フラグ値*
  一般ユーザーの自身のパスワード変更の可否を指定する(フラグ値は 0 が不許可、1 が許可)。デフォルトは 1（許可）。

- -B *フラグ値*
  次回のログオン時にパスワードの変更を要求するかどうかを指定する(フラグ値は 0 が要求しない、1 が要求する)。Windows ドメインログオンする場合のみ有効となる。デフォルトは 0（要求しない）。

- -P
  ユーザーを作成後、パスワードの入力を求める。

- -C *\\サーバー名\共有名*
  Windows ドメインログオン時のユーザーのホームフォルダとするファイル共有のネットワークパス名（UNC）を指定する。smb.conf ファイルの logon home パラメータに該当し、smb.conf の指定より優先される。

- -D *ドライブ名*
  Windows ドメインログオン時のホームフォルダに割り当てるドライブ名を指定する。smb.conf ファイルの logon drive パラメータに該当し、smb.conf の指定より優先される。

- -E *スクリプト名*
  Windows ドメインログオン時に実行するスクリプトを指定する。スクリプトファイルはドメインコントローラの NETLOGON 共有内に置き、このオプションには NETLOGON 共有からの相対パス形式で指定する必要がある。smb.conf ファイルの logon script パラメータに該当し、smb.conf の指定より優先される。

- -F *\\サーバー名\共有名\フォルダ名*
  Windows ドメインログオン時のユーザーの移動プロファイルの保存先とするファイル共有のネットワークパス名（UNC）を指定する。smb.conf ファイルの logon path パラメータに該当し、smb.conf の指定より優先される。

- -H [*アカウントフラグ*]
  ユーザーのアカウント制御フラグをスクウェアブラケット「[」、「]」で括って指定する。指定できるフラグと意味は以下の通り：

  - U　ユーザーアカウント（W, S, I フラグと排他）
  - W　コンピュータアカウント(ワークステーション)（U, S, I フラグと排他）
  - S　コンピュータアカウント(サーバー)（U, W, I フラグと排他）
  - I　ドメイン間信頼アカウント（U, W, S フラグと排他）
  - X　パスワードが無期限
  - N　パスワードなし
  - D　無効なアカウント
  - L　自動的にロックされたアカウント
  - M　MNS ログオンアカウント
  - T　一時重複アカウント

6.1.4 smbldap-usermod

ユーザーの情報を変更するコマンドです。実行には管理権限が必要です。

構文

smbldap-usermod *[オプション] ユーザー名*

オプション

- -a
  ユーザーに Windows ユーザーアカウント情報を追加する。
- -u *UID*
  ユーザーの UID（UNIX ユーザー ID）値を指定する。
- -g *グループ名*
  ユーザーのプライマリグループを指定する。
- -G *グループ名[,グループ名...]*
  ユーザーに割り当てるサブグループを指定する。複数割り当てる場合はカンマ「,」で区切って列挙する。
- -d *ディレクトリ*
  ユーザーの UNIX ホームディレクトリの場所を指定する。
- -s *シェル*
  ユーザーの UNIX ログインシェルを指定する。
- -c *コメント*
  ユーザーの付加情報（コメント）を指定する。
- -A *フラグ値*
  一般ユーザーのによる自身のパスワード変更の可否を指定する(フラグ値は 0 が不許可、1 が許可)。デフォルトは 1（許可）。
- -B *フラグ値*
  次回のログオン時にパスワードの変更を要求するかどうかを指定する(フラグ値は 0 が要求しない、1 が要求する)。Windows ドメインログオンする場合のみ有効となる。デフォルトは 0（要求しない）。
- -C *\\サーバー名\共有名*
  Windows ドメインログオン時のユーザーのホームフォルダとするファイル共有のネットワークパス名（UNC）を指定する。smb.conf ファイルの `logon home` パラメータに該当し、smb.conf の指定より優先される。
- -D *ドライブ名*
  Windows ドメインログオン時のホームフォルダに割り当てるドライブ名を指定する。smb.conf ファイルの `logon drive` パラメータに該当し、smb.conf の指定より優先される。
- -E *スクリプト名*
  Windows ドメインログオン時に実行するスクリプトを指定する。スクリプトファイルはドメインコントローラの NETLOGON 共有内に置き、このオプションには NETLOGON 共有からの相対パス形式で指定する必要がある。smb.conf ファイルの `logon script` パラメータに該当し、smb.conf の指定より優先される。
- -F *\\サーバー名\共有名\フォルダ名*
  Windows ドメインログオン時のユーザーの移動プロファイルの保存先とするファイル共有のネットワークパス名（UNC）を指定する。smb.conf ファイルの `logon path` パラメータに該当し、smb.conf の指定より優先される。
- -H [*アカウント制御フラグ*]

ユーザーのアカウント制御フラグをスクウェアブラケット「[」、「]」で括って指定する。指定できるフラグと意味は以下の通り:

- U　ユーザーアカウント（W, S, I フラグと排他）
- W　コンピュータアカウント(ワークステーション)（U, S, I フラグと排他）
- S　コンピュータアカウント(サーバー)（U, W, I フラグと排他）
- I　ドメイン間信頼アカウント（U, W, S フラグと排他）
- X　パスワードが無期限
- N　パスワードなし
- D　無効なアカウント
- L　自動的にロックされたアカウント
- M　MNS ログオンアカウント
- T　一時重複アカウント

- -I
  ユーザーを無効にする。-H, -J オプションと同時に指定することはできない。
- -J
  ユーザーを有効にする。-H, -I オプションと同時に指定することはできない。

6.1.5 smbldap-userdel

ユーザーを削除するコマンドです。実行には管理権限が必要です。

構文

smbldap-userdel *[オプション] ユーザー名*

オプション

- -r
  ユーザーのホームディレクトリを削除する。

6.1.6 smbldap-groupshow

グループの情報を表示するコマンドです。

構文

smbldap-groupshow *グループ名*

オプション

オプションはない。

6.1.7 smbldap-groupadd

グループを作成するコマンドです。実行には管理権限が必要です。

構文

`smbldap-groupadd` *[オプション] グループ名*

オプション

- `-a`
  グループを Windows グループアカウントとして作成する。このオプションを省略すると UNIX グループアカウント情報のみ作成され、Windows（Samba）サービスは利用できない。
- `-g` ***GID***
  グループの GID（UNIX グループ ID）値を指定する。

6.1.8 smbldap-groupmod

グループの情報を変更するコマンドです。実行には管理権限が必要です。

構文

`smbldap-groupmod` *[オプション] グループ名*

オプション

- `-a`
  グループに Windows グループアカウント情報を追加する。
- `-g` ***GID***
  グループの GID（UNIX グループ ID）値を指定する。
- `-m` *ユーザー名[,ユーザー名...]*
  グループのメンバーに追加するユーザーを指定する。複数のユーザーを追加する場合はカンマ「,」で区切って列挙する。
- `-x` *ユーザー名[,ユーザー名...]*
  グループのメンバーから削除するユーザーを指定する。複数のユーザーを削除する場合はカンマ「,」で区切って列挙する。

6.1.9 smbldap-groupdel

グループを削除するコマンドです。実行には管理権限が必要です。

構文

`smbldap-groupdel` *グループ名*

オプション

オプションはない。

7. 改版履歴

- 2009-04-16　リビジョン 1.2
  - Windows 2000 Service Pack 4 の入手先を変更、USRMGR.exe 展開手順を追加
- 2009-03-04　リビジョン 1.1
  - スタイルと書式設定を更新。
  - PDF 版で目次から各章へのリンクが機能しない問題を修正。
  - 画面スナップショット（イメージ） 枠の［アンカー］を［段落へ］にすると、前後の段落の増減によりイメージが不意に移動してしまうことがあるため、［アンカー］を［文字として］に変更。
- 2008-12-18　リビジョン 1.0
  - 初版