Samba + OpenLDAPによるWindows ドメインコントローラの構築
～もうWindowsドメインサーバはいらない？！～

ミラクル・リナックス株式会社
日本Sambaユーザ会 副代表幹事
小田切 耕司
odagiri@miraclelinux.com

目次

- 講師紹介
- なぜSambaを使うのか？
- Samba 2.2新機能
- Winbind/LDAPSAM機能
- LDAPSAMによるPDC構築
- 既存環境をLDAP環境へ移行
- WinNT/2000サーバからの移行
- Samba応用機能およびMIRACLE LINUXのSamba拡張機能紹介

講師紹介

- 1997年「UNIX-Windowsネットワーキング」(テクノプレス)
  日本初のSamba本！
- 1998年「SAMBA/NFSによるUNIX-Windowsネットワーキング」(テクノプレス)
  売れて増刷！
- 1999年3月 LinuxWorld Conference Japan'99
  『Samba : LinuxとWindowsの共存環境構築 』
- 1999年11月日本Sambaユーザ会設立　代表幹事
- 2000年　日経Linux10月号～6回連載
  「企業/学校におけるSambaサーバー構築/運用テクニック」
- 2001年1月
  三菱電機からミラクル・リナックス株式会社へ転職
- 2001年　日経Linux 6月号～6回連載
  「実践Sambaサーバー構築/運用テクニック」
- 2002年　日経Linux 3月号～6回連載
  「Samba 2.2によるサーバー構築運用テクニック」
- 2002年3月 日本Webminユーザーズグループ設立 副代表幹事
- 2002年10月 日経11月号
  「複数サーバのユーザ管理をLDAPで統合しよう」

Part 1. Samba概要

Sambaとは何か？

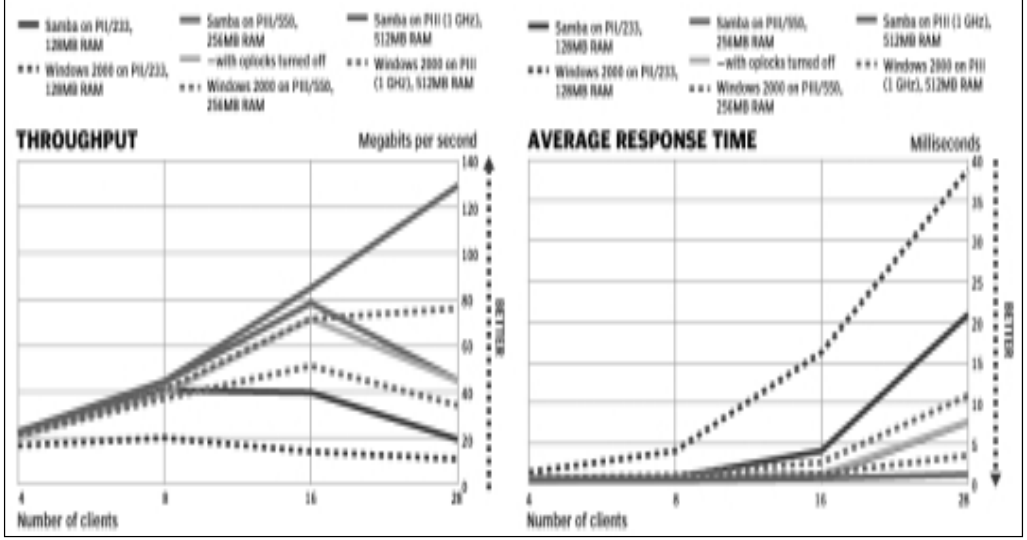
- Samba(「サンバ」と呼称します)は、Linux および UNIXマシンを Windows NT/2000互換のファイルサーバ/プリント・サーバにするオープン・ソース・ソフトウェアです。GPL (GNU General Public License) の元、自由に利用することができます。
- Windowsﾄﾞﾒｲﾝｺﾝﾄﾛｰﾗ機能をはじめとするさまざまな管理機能も搭載
- Windows NT/2000 Serverを置き換えることを可能にします。

なぜWindowsﾌｧｲﾙｻｰﾊﾞをLinuxで構築するの？

- **圧倒的に安い導入コスト**
  - Win2000ｻｰﾊﾞではCAL(ｸﾗｲｱﾝﾄｱｸｾｽﾗｲｾﾝｽ)が必要
  - ｺｽﾄ比較例）
    １０台のファイルサーバを１０００人で使用する場合、Windows 2000サーバの価格を１３万円、１ユーザのクライアントアクセスライセンスを５３００円とすると導入にはサーバライセンス費用だけで**６６０万円**かかることになりますが、MIRACLE LINUXでは**６０万円、１／１０のｺｽﾄ**で導入できます。
- **高い性能**
  - 必要なH/Wﾘｿｰｽ がWin2000より少なく、ｽﾙｰﾌﾟｯﾄも高い
- **高い信頼性**
  - 連続運転に強い（ﾒﾓﾘ･ﾘｰｸがない）
  - オープンソースなので障害調査しやすく、修正も可能
- **運用のしやすさ**
  - UNIXのｼｪﾙｺﾏﾝﾄﾞを活用して運用を効率化可能
    ｻｰﾊﾞ台数が増えるほど効果的
  - 修正モジュール適用にOSのﾘﾌﾞｰﾄが必要ない
    - OSｲﾝｽﾄｰﾙも２０分ほどで完了

Windows 2000よりLinux+Sambaは高性能

- http://www.pcmag.com/article/0,2997,s%253D1474%2526a%253D16554,00.asp



１万登録ユーザ、3000同時接続を検証

- MIRACLE LINUX Standard Edition V2.1 の性能検証をOSDL（オープン・ソース・デベロップメント・ラボ）と共同で行い、Linux ファイルサーバとして1万ユーザを登録し、3千の同時ユーザ接続が可能であることを実証しました。
- これにより、MIRACLE LINUX 上で Windows ネットワーク用の大規模な Linux ファイルサーバ構築が実現可能なことが実証されたことになります。
- プレスリリース(2002年10月8日)
  http://www.miraclelinux.com/pressroom/details/2002100801.html
- Linux Conference 2002の発表資料
  http://www.miraclelinux.com/technet/lc2002_samba/

Sambaの機能

- Windows NT/2000互換のファイルサーバ
  - ファイル共有、プリンタ共有
  - DFS（分散ファイルシステム）機能（ルートにもメンバにもなれる）
- Windows NT/2000互換のクライアント管理機能
  - ドメインコントローラ（ドメイン・ログオンが可能）
  - ユーザアカウントの統合管理（PDCだけでユーザ管理可能）
  - WINSサーバ機能（Windowsマシンの名前解決）
  - マスタブラウザ機能（ネットワークコンピューター覧の提供）
  - プリンタドライバ自動配布機能（簡単プリンタ設定）
  - 移動プロファイル（複数ユーザ/マシンでの共有利用）
  - ユーザポリシーの配布（利用者の操作制限）
  - ユーザホーム機能（ユーザ専用共有）
  - QUOTA:容量制限機能（ユーザ、グループ毎の使用量制限）

Samba 2.2の新機能

- ドメイン・メンバ機能→**Winbind機能**
  - Windowsサーバに登録されたユーザ情報をLinuxで利用可能になった。
- ドメイン・コントローラ機能→**LDAPSAM機能**
  - LDAPSAM機能によりユーザ情報をすべてLDAPのみで統一管理でき、BDCも設置可能になった。
- MS-DFS機能
- プリンタドライバ配布機能

複数サーバの管理機能の充実

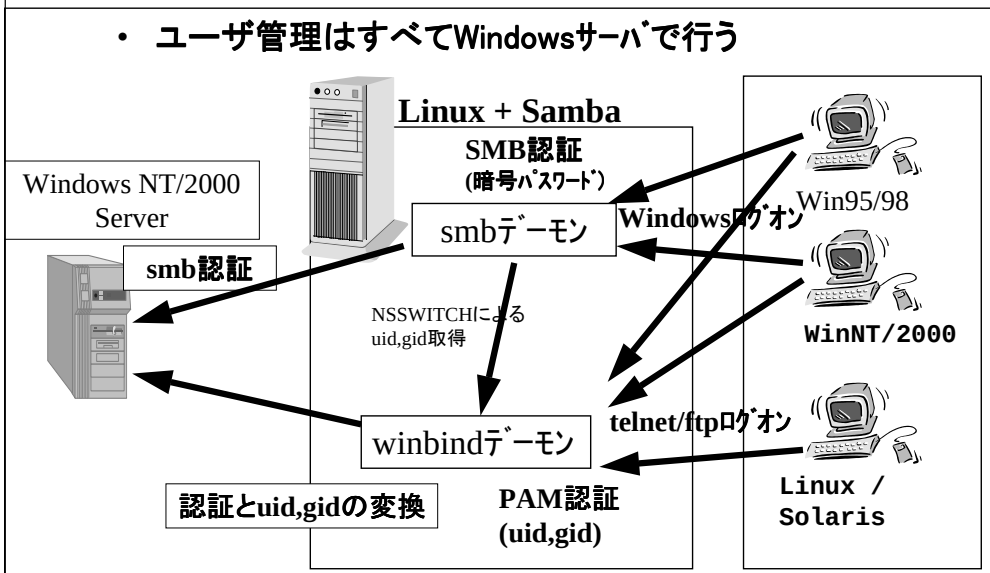
Samba Winbind機能

- **Windows NT/2000**サーバが**PDC**としてドメインが構成されている場合にのみ採用可能。
- **Windows 2000**サーバの**Active Directory**を使用すればユーザ管理ドメインをツリー構造にでき、ある程度の大規模ユーザシステムを構築できる。
- **Samba**サーバが複数台になってもユーザ管理は１台の**Windows**の**PDC**で操作すれば良い。

ユーザ管理を既存の
WindowsNT/2000サーバに統合

Winbindによるユーザ管理機能

- **ユーザ管理はすべてWindowsサーバで行う**



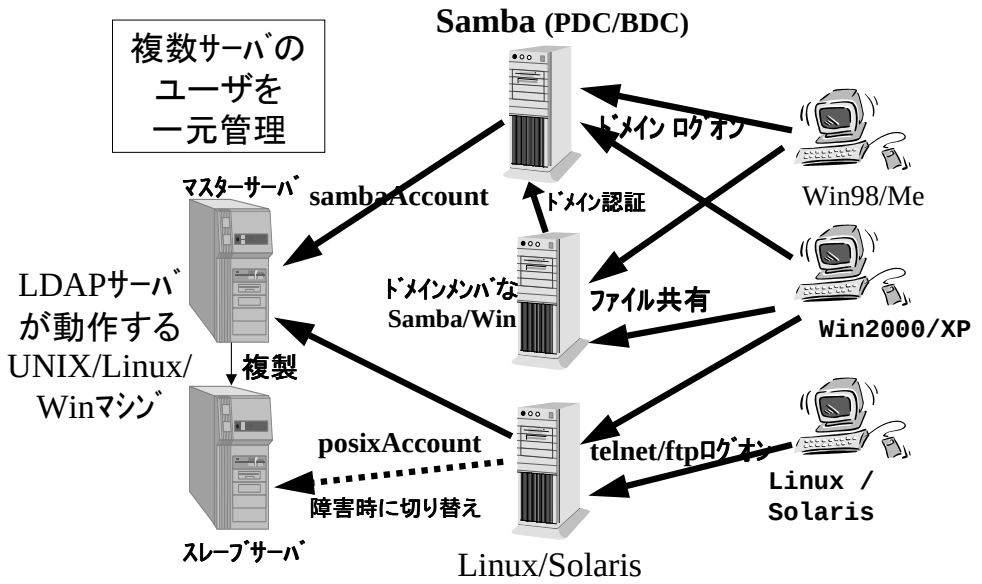
Samba LDAPSAM機能

- ユーザ情報を**LDAP**サーバで管理
- **Samba**サーバを**PDC/BDC**としてドメイン構成可能
  - **Windows**ドメインのユーザも**LDAP**サーバで管理可能に
- ユーザ管理ドメインをツリー構造にでき、大規模ユーザシステムを構築できる。
- 専用のｵﾌﾟｼｮﾝ**(--with-ldapsam)**でｺﾝﾊﾟｲﾙする必要がある。**MIRACLE LINUX**よりパッケージ提供。

ユーザ管理をLDAPに統合

Samba LDAP機能

- **Windows**ﾄﾞﾒｲﾝ認証やUNIXの認証がすべてLDAPで統合可能になる



Part 2.

複数サーバのユーザ管理を LDAPで統合しよう

複数サーバのユーザ管理問題点

- Linux/UNIX マシンを使用するにはユーザー登録が必要であり，一つひとつのマシンにそれぞれユーザー登録していくのは面倒
- Linux/UNIX の場合，NFS やファイル・コピーの関係で同じユーザーのuid , gid はすべてのマシン間で同一にしなければならないのだが，統合管理が容易ではない
- Windows NT/2000/XP マシンにも同様にユーザー登録，パスワード設定が必要。特にサーバーや共有マシンがあるとLinux/UNIX のようにコマンドで一括登録するのが容易でなく面倒

管理コストの増大

従来の方式と問題点

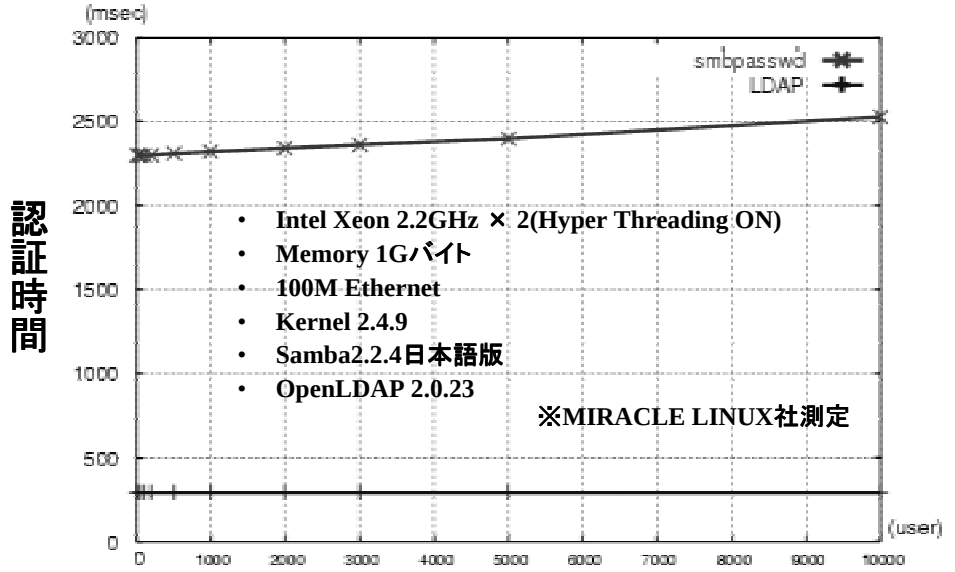
- NIS（Network Information System ）とは
  - 米Sun Microsystems 社が開発、/etc/passwd , group , hosts ファイルをネットワーク上で集中管理する仕組み
- NIS やNIS+が最近使われない理由
  - アクセス制御機能が乏しいため，セキュリティの面で問題がある
  - 拡張性や性能に問題があり，大規模システムでの使用に適さない
  - 運用や設定が難しい
  - Windows やSamba との連携が容易でない
  - SUN Solaris では今後NIS/NIS+はサポートを縮小する予定。LDAP に移行するように推奨している

現在のサーバ管理には機能不足

LDAPを使うことの利点

- 機能拡張性が高い
  ユーザー管理だけでなく，組織情報の管理，コンピュータの管理，アプリケーションの管理，メール・アドレス帳，電話帳などいろいろな用途で自由に拡張して使用できる
- UNIX/Linux だけでなくSamba やWindows でも利用できる
- 性能に関しても拡張性が高い
  商用のLDAP 製品は数十億のデータ・エントリでも実運用に耐える処理性能を備えている。
  Linux ディストリビューションに添付されるオープンソースのOpenLDAP も数千～数万エントリでの実績が多数ある
- 細かなアクセス制御機能を有しており，SSL などでの暗号化も可能でセキュリティが強固である
- ディレクトリを木構造で管理でき，サーバーの分散管理が可能である
- 複製機能を備えており，障害にも対応できる

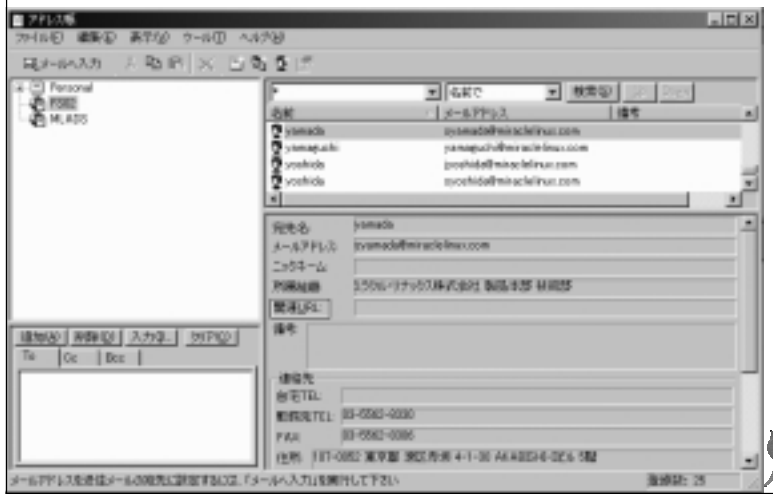
LDAP認証はsmbpasswd認証よりも8倍高速！



LDAP (Lightweight Directory Access Protocol)概要

- LDAP はディレクトリ・サービスの一つ
- 高機能だが運用負荷や開発コストが高かったITU- T 勧告のX.500 ディレクトリ・サービスを「90 %の機能を10 %のコストで実現する」ために設計
- LDAP をサポートした商用製品
  - Windows2000 Active Directry
    http://www.microsoft.com/japan/windows2000/techinfo/howitworks/default.asp#section2
  - Novell eDirectry
    http://www.novell.co.jp/products/nds/productinfo.html
  - iPlanet Directory Server（現在まだLinux では動作しない）
    http://ja.iplanet.com/products/ids5_0/index.html
  - IBM SecureWay Directory
    http://www-6.ibm.com/jp/software/ec/ecprod/be/moreinfo.html
  - Oracle9i ApplicationServer :Internet Directory
    http://www.oracle.co.jp/9i/9ias/func.html
  - ロータスドミノディレクトリ
    http://www.lotus.co.jp/home.nsf/Content/DP2_Notes_Domino_R50_outline
- OpenLDAP（http://www.openldap.org/）
  - Linux ディストリビューションに同こんされるオープンソースのLDAP

LDAPで何ができるか？

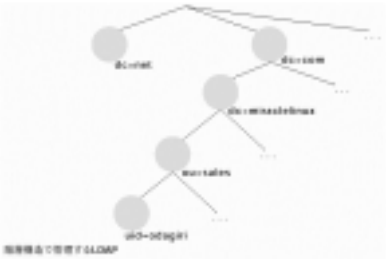


- Linuxユーザの統合管理
- Sambaユーザの統合管理
- Webサーバ（Apache）のアクセス制御
- 電話帳、メールアドレス帳

LDAPとRDBMSの違い

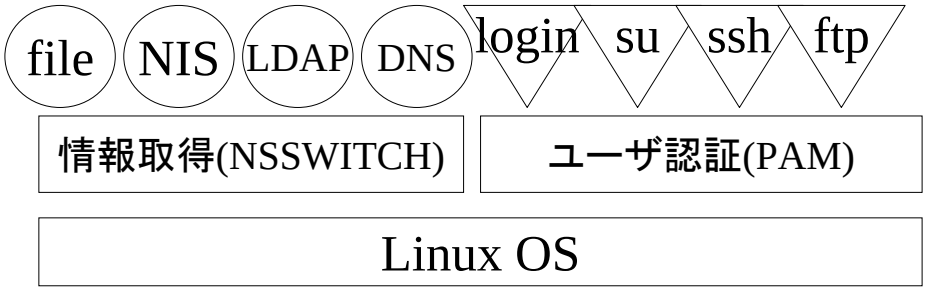
- LDAP(ネットワークプロトコル）とSQL（言語）

	LDAP	RDBMS
用途	検索性能重視、頻繁な更新には向かない	検索だけでなく頻繁な更新も重視
構造	木構造（行や列といった概念はない）	表構造（行や列が存在）
更新	トランザクションの概念はない	トランザクションの概念あり
分散	ツリーの枝単位で分散配置が可能	キーの範囲で分散配置が可能
操作	LDAP（ネットワークプロトコル）で操作 プロトコルは単純	SQL（プログラム言語）で操作 複雑な操作が可能
検索手法	木の枝葉をたどるイメージ	表の行を走査するイメージ



Linux/UNIXのユーザ管理機構

- NSSWITCH機能
  - /etc/nsswitch.confで、各種情報の取得先を指定可能
- PAM認証機構
  - /etc/pam.d/の中でアプリケーションごとの認証ルールを指定可能
- LDAP認証を使うには、NSS,PAMのサポートが必須
  - NSS,PAMに対応しないSUN4,HP-UX10に対しては、NIS-LDAPゲートウェイ(ypldapd: http://www.padl.com/)で対応可能



ネームサービススイッチ機能

- LDAPを認証で使用するには/etc/nsswitch.confを以下のように変更

```
passwd:   files   ldap
group:    files   ldap
shadow:   files   ldap
hosts:    files   dns   wins
```

- /lib/libnss_ldap.so.2が呼ばれる。
- /lib/libnss_wins.so.2 を使うとWINS(Windows Internet Name Service)を使って名前解決可能

プラグマブル認証機能

- /etc/pam.d/system-authに以下を設定

```
[root@ts02 /etc]# cat /etc/pam.d/system-auth
#%PAM-1.0
# This file is auto-generated.
# User changes will be destroyed the next time authconfig is run.
auth        required      /lib/security/pam_env.so
auth        sufficient    /lib/security/pam_unix.so likeauth nullok
auth        sufficient    /lib/security/pam_ldap.so use_first_pass
auth        required      /lib/security/pam_deny.so

account     required      /lib/security/pam_unix.so
account     [default=ok user_unknown=ignore service_err=ignore system_err=ignore] /lib/security/pam_ldap.so

password    required      /lib/security/pam_cracklib.so retry=3
password    sufficient    /lib/security/pam_unix.so nullok use_authtok md5 shadow
password    sufficient    /lib/security/pam_ldap.so use_authtok
password    required      /lib/security/pam_deny.so

session     required      /lib/security/pam_limits.so
session     required      /lib/security/pam_unix.so
session     optional      /lib/security/pam_ldap.so
session     required      /lib/security/pam_mkhomedir.so skel=/etc/skel umask=0022
```

- /etc/pam.d/sshdなどに以下を設定

```
#%PAM-1.0
auth        required    /lib/security/pam_stack.so    service=system-auth
account     required    /lib/security/pam_stack.so    service=system-auth
password    required    /lib/security/pam_stack.so    service=system-auth
session     required    /lib/security/pam_stack.so    service=system-auth
```


Part 3：実践編

- Linux,Samba,Windowsユーザすべてを OpenLDAPで管理する
  - ① パッケージインストール
  - ② LDAPサーバの設定
  - ③ LDAPクライアントの設定
  - ④ Sambaの設定
  - ⑤ Windowsクライアントの設定

OpenLDAP導入と設定

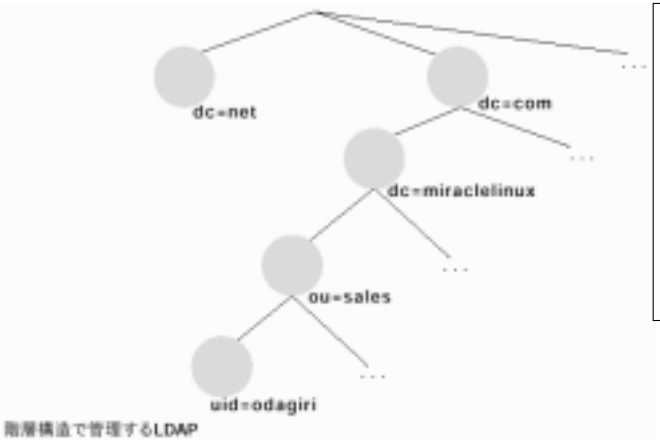
- インストールCDのRPM
  - nss_ldap
  - nscd
  - openldap
  - openldap-client
  - openldap-servers（サーバマシンのみ）
- http://www.miraclelinux.com/technet/openldap/
  - smbldap-tools
  - samba-2.2.4.ja-ldap(通常のﾊﾟｯｹｰｼﾞは不可)
- 「rpm –Uvh パッケージ名」で導入

OpenLDAPサーバの設定

- 設定ファイル
  サーバ：/etc/openldap/slapd.conf
  クライアント：
  NSS,PAM用：/etc/ldap.conf
  Ldapaddなどの管理コマンド用:/etc/openldap/ldap.conf
- OpenLDAP 管理者ガイド
  http://www.interq.or.jp/earth/inachi/openldap/admin/index-ja.html
- Red Hat Linux 7.2 リファレンスガイド
  http://www.jp.redhat.com/manual/Doc72/RH-DOCS/rhl-rg-ja-7.2/ch-ldap.html

/etc/slapd.confﾊﾟﾗﾒｰﾀ(1)

- suffix ベース・サフィックスを指定する
  通常はﾄﾞﾒｲﾝ名をﾍﾞｰｽに指定
  例）suffix dc=miraclelinux,dc=com
  suffix "ou=sales,ou=yokohama,o=miraclelinux,c=jp"



CN=commonName
L=localityName
ST=stateOrProvinceName
O=organizationName
OU=organizationalUnitName
C=countryName
STREET=streetAddress
DC=domainComponent
UID=userid

/etc/slapd.confﾊﾟﾗﾒｰﾀ(2)

- rootdn
  LDAPサーバの管理者のDN(Distinguished Name：識別名)を指定する。
  なお管理者DNを含むユーザDNには、英大文字、英子文字の区別はない。
  管理者DNの例）
  - rootdn "cn=Manager,dc=miraclelinux,dc=com"
- rootpw
  LDAPサーバの管理者パスワードを設定する。
  - そのままのパスワードを指定するか暗号化したものを設定する
  - 例）miracleというパスワードをMD5ハッシュする
    # slappasswd -s miracle -h {MD5}
  - rootdnをLDAPに登録されているユーザを指定し、LDAPの中にパスワードが格納されていれば、rootpwを指定する必要はない。

/etc/slapd.confﾊﾟﾗﾒｰﾀ(3)

- include
  - 与えたファイルから追加の設定情報を読み込む。
  - 通常はスキーマ定義ファイルを読み込むために使用する
    例) include /etc/openldap/schema/samba.schema
- database
  - LDAPのデータを格納するのに使用するバックエンド・データベースを指定。現在ldbm, shell, passwd のいずれかを指定できる。
    通常ldbmを使用
- directory
  - LDBMファイルを格納するディレクトリを指定
  - 例）directory /var/lib/ldap
- index
  - 作成する索引の属性とタイプを指定する。
    - 例1) uid,gidに関してequal（等値）検索用の索引を作成
      index uidNumber,gidNumber eq
    - 例2) mail（メールアドレス）、surname（名字）に関して、equal検索用とsubinitial（前方一致）の索引を作成
      index mail,surname eq,subinitial

/etc/slapd.confﾊﾟﾗﾒｰﾀ(4)

- Slapd.confの例：サフィックスを"dc=miraclelinux,dc=com"、管理者DNを"cn=Manager,dc=miraclelinux,dc=com"、管理者パスワードをmiracle

```
include /etc/openldap/schema/core.schema
include /etc/openldap/schema/cosine.schema
include /etc/openldap/schema/inetorgperson.schema
include /etc/openldap/schema/nis.schema
include /etc/openldap/schema/redhat/rfc822-MailMember.schema
include /etc/openldap/schema/redhat/autofs.schema
include /etc/openldap/schema/redhat/kerberosobject.schema
include /etc/openldap/schema/samba.schema
database  ldbm
directory /var/lib/ldap
suffix "dc=miraclelinux,dc=com“
rootdn "cn=Manager,dc=miraclelinux,dc=com“
rootpw miracle
index  objectClass,uidNumber,gidNumber,memberUid  eq
index  cn,mail,surname,givenname              eq,subinitial
index  uid                                    pres,eq
index  rid                                    eq
```

- 設定が終了したら、OpenLDAPデーモンを起動させる。
  # service ldap restart
- システム起動時に自動的に動くように以下を設定
  # chkconfig ldap on

LDAPクライアントをauthconfigで設定

- authconigにより/etc/nsswitc.confと/etc/openldap/ldap.conf、/etc/pam.d/system-authが変更される。
- authconfig実行例（ユーザ情報の設定）
  NSSWITCHの設定が行われる。

- authconfig実行例（認証の設定）
  PAMの設定が行われる。

LDAPによるLinuxユーザの統合管理

- **smbldap-toolsによる管理**
  - **smbldap_conf.pm**
    LDAPサーバやSambaのデフォルト設定を記述するファイル
  - **smbldap-populate.pl**
    LDAPサーバの初期化を行う（rootツリーとデフォルトユーザの登録）
  - **smbldap-useradd.pl**
    UNIX/Linux およびSamba/Windowsユーザ アカウントを追加する
  - **smbldap-userdel.pl**
    UNIX/Linux およびSamba/Windowsユーザ アカウントを削除する
  - **smbldap-usermod.pl**
    UNIX/Linux およびSamba/Windowsユーザ アカウントを変更する
  - **smbldap-usershow.pl**
    UNIX/Linux およびSamba/Windowsユーザ アカウント情報を表示する
  - **smbldap-passwd.pl**
    UNIX/Linux およびSamba/Windowsユーザのパスワードを設定／変更する
  - **smbldap-groupadd.pl**
    UNIX/Linux およびSamba/Windowsのグループを追加する
  - **smbldap-groupdel.pl**
    UNIX/Linux およびSamba/Windowsのグループを削除する
  - **smbldap-groupmod.pl**
    UNIX/Linux およびSamba/Windowsのグループを変更する
  - **smbldap-groupshow.pl**
    UNIX/Linux およびSamba/Windowsのグループを表示する

LDAPによるSambaユーザの統合管理

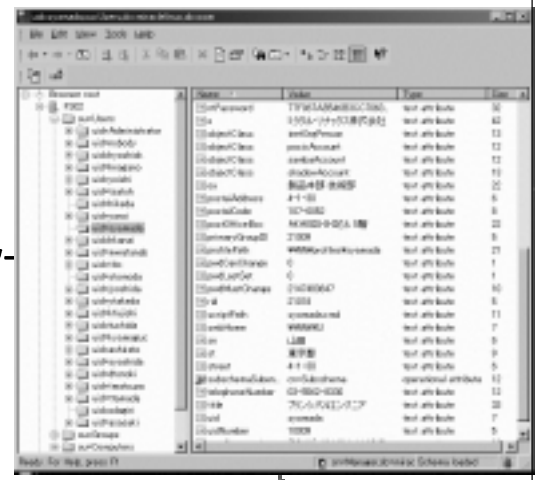
- **ユーザの登録**
  - **ユーザ・アカウントは英大文字は使用せず、英子文字、数字のみで15バイト以下。日本語も使用不可**
  - **例）yamadaというユーザを登録し、パスワードを設定**

```
# smbldap-useradd.pl -a -m yamada

# smbldap-passwd.pl yamada
```


LDAPのGUIクライアントの紹介

- Linuxでのみ使用可能なツール
  - GQ（日本語利用不可）：
    http://biot.com/gq/
- Windowsでのみ使用可能なツール
  - Softerra LDAP Browser（無償、図は実行例）、LDAP Administrator（有償）：
    http://www.ldapadministrator.com/
- LinuxでもWindowsでも使用できるツール
  - LDAP Browser/Editor（JDK 1.2.2移行が必要）
    http://www.iit.edu/~gawojar/ldap/



WindowsドメインをLDAP+Sambaで構築

- SambaでWindowsドメインを構築し、Windowsマシンをドメインメンバにすることで、Windows 9x / NT / 2000 / XP マシンもLDAPで管理することが可能になる
- SambaのPDCで可能なこと
  - ドメインログオン（シングルサインオン)
  - NTLM認証（チャレンジ＆レスポンス方式）
  - ログオンスクリプト
  - 移動プロファイル
  - NT4相当のユーザポリシー(NT4/2000/XP)
  - Win98相当のグループポリシー(95/98/Me)
- SambaのPDCでまだできないこと
  - Win2000相当のグループポリシー
  - Kerberos認証（チケット方式）
  - 他ドメインと信頼関係を結ぶ
  - ワークステーションのログオン可能時間を制限する。
- Samba 2.2.4でBDCになることは出来るがSAMの複製ができない。LDAPの複製機能を使用することでSambaをPDC,BDCにできる
- smbldap-toolsを使って管理することでLinuxパスワード(MD5)、Windowsパスワード(LANMAN)の違いを意識することなくユーザを管理可能
- Windowsクライアントからのパスワード変更も可能

/etc/samba/smb.confの設定(1)

- ldap server
  - LDAPサーバが稼働しているホスト名を指定する。
  - デフォルトはlocalhost（同一マシン）である。
  - 例）ldap server = ldap1.miraclelinux.com
- ldap suffix
  - アカウント検索のためのDN(Distinguished Name)を指定する。
  - 例）ldap suffix="dc=miraclelinux,dc=com"
- ldap admin dn
  - LDAP管理者のDNを指定する。これは/etc/openldap/slapd.confに指定したものと同一とする。また、この管理者のパスワードは以下のsmbpasswdコマンドで設定する。
    - smbpasswd -w パスワード
  - 例）ldap admin dn = "cn=Manager,ou=people,dc=miraclelinux,dc=com"

/etc/samba/smb.confの設定(2)

- ldap filter
  - sambaAccountオブジェクトクラスからログイン名、uidを検索するためにフィルタを指定する。これはデフォルトのままで使用する。
  - ldap filter = "(&(uid=%u)(objectclass=sambaAccount))"
- ldap port
  - LDAPサーバにアクセスするときのポート番号を指定する。
  - SSLで暗号化する場合は636を使用し、暗号化しない場合は389を使用する。
- ldap ssl
  - LDAPとの通信をSSLで暗号化する場合はon、しない場合はoffとする。LDAPv3 StartTLS 拡張を使用する場合はstart_tls を使用する。

/etc/samba/smb.confの設定(3)

- PDC,BDC,ドメインメンバの設定

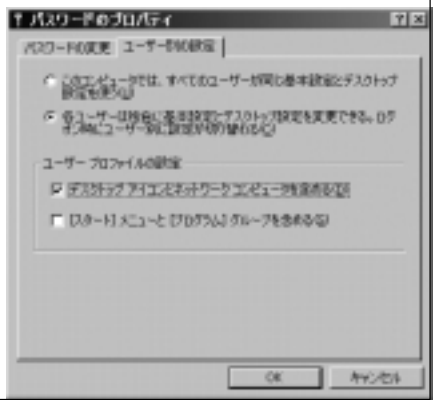
	PDC	BDC	ﾄﾞﾒｲﾝ ﾒﾝﾊﾞ
domain logon	yes	yes	no
domain master	yes	no	no
os level	64	32	20
preferred master	yes	yes	no
local master	yes	yes	yes
security	user	user	user

smb.conf設定例

```
[global]
      coding system = euc
      client code page = 932
      workgroup = MIRACLELINUX
      encrypt passwords = Yes
      passwd program = /usr/local/sbin/smbldap-passwd.pl -o %u
      passwd chat = *New*password* %n¥n *Retype*new*password* %n¥n *passwd:*all*authentication*tokens*updated*successfully*
      unix password sync = Yes
      deadtime = 15
      read size = 65536
      socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192
      lm announce = False
      dns proxy = No
      ldap server = ldap1
      ldap port = 389
      ldap suffix = "dc=miraclelinux,dc=com"
      ldap admin dn = "cn=Manager,dc=miraclelinux,dc=com"
      ldap ssl = no
      printer admin = Administrator
      printing = lprng
      dos filetimes = Yes
      dos filetime resolution = Yes
      domain logons = Yes
      os level = 64
      preferred master = yes
      domain master = yes
      local master = yes
      wins support = yes
      domain admin group = " @"Domain Admins" "
[homes]
      comment = %S's Home Directories
      read only = No
      browseable = No
[NETLOGON]
      comment = Script for Domain Logon
      path = /var/samba/netlogon
      admin users = Administrator
      write list = Administrator
[profiles]
      path = /var/samba/profiles
      writeable = yes
      browseable = no
      create mode = 0600
      directory mode = 0700
```


Windows 95/98/Meのドメイン参加

- Windows 95/98/Meクライアントからドメインログオンするには，[コントロールパネル] - [ネットワーク]- [Microsoft ネットワーククライアント] のプロパティを以下のように設定する。
- Windowsドメインでの設定と同様に、[コントロールパネル] -[パスワード] の"ユーザ別の設定" タブで，以下のように，ユーザ別の設定" をチェックしておくことで、ユーザプロファイルの利用も可能になる。



Windows NT/2000/XPのドメイン参加

- Windows 95/98/Meはドメイン・ログオンするのにに Samba PDC上で何も設定が必要ないが、SambaとWindows NT/2000/XPをドメイン・メンバに加える場合は、PDCマシンの上でドメイン・メンバ・マシンのマシンアカウントを作成する必要がある。
- PDCマシン上でrootになり、以下を実行する必要がある。

```
# smbldap-useradd.pl -a -d /dev/null
  -s /bin/false domainadd –g Administrators
# smbldap-usermod.pl -u 0 domainadd
# smbldap-passwd.pl domanadd
```

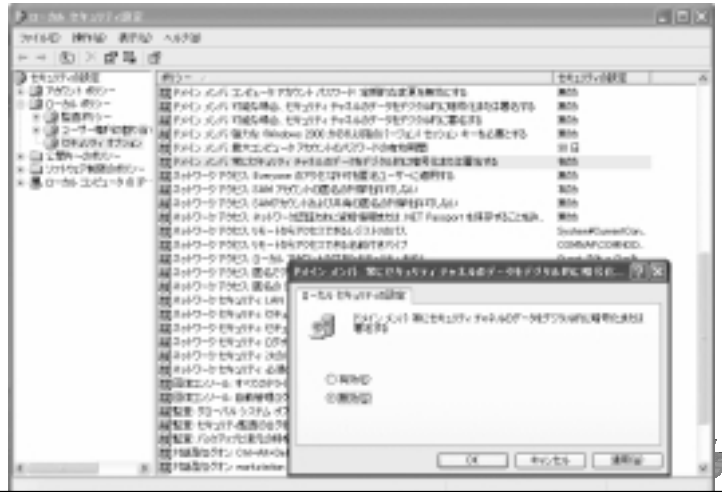
- 上記は、1度だけ実行する。
- 以下はドメイン・メンバのマシン分実行する。
- `# smbldap-useradd.pl -w Windowsマシン名`
- （マシン名は英大文字は使用せず、英子文字、数字のみで15バイト以下とすること。日本語も使用不可）

Windows NT/2000/XP上での作業

① Administratorとしてログオンする。
② コントロールパネルの「システム」のプロパティを起動し、「ネットワークID」タブの「ネットワークID」のボタンを押す。
③ 「ユーザアカウントとドメイン情報」の入力で、Samba PDCで設定したAdministratorユーザとパスワード、ドメイン名を入力する。
④ 「ドメインへようこそ」というダイアログが表示されることを確認する。

Windows XPをSambaﾄﾞﾒｲﾝに参加させる時の注意事項

- Windows XPはWindows2000よりセキュリティが強化されているため、「コントロールパネル」の「管理ツール」から「ローカル セキュリティ ポリシー」を起動し、「ローカル ポリシー」の「セキュリティ」オプションにおいて、「ドメイン メンバ：常にセキュリティ チャネルのデータをデジタル的に暗号化または署名する」を「無効」にする。
- これでWindows 2000と同等のレベルになり、問題なくSambaドメインログインできる。



SambaのWindowsドメインへログオンしよう！

- 設定を行なったら、Windows クライアントをリブートし、設定したWindowsドメインにログオンする。
- ログオンスクリプトが動作すれば、設定は正しく動いている。

WindowsからのSambaパスワード変更

- Windowsマシンを利用する一般ユーザからは、
  - unix password sync
  - passwd program
  - passwd chat

  を設定してあれば以下の方法で行える。(Linuxのパスワードも同時に変更)
- SWATからのパスワード変更
- Windows 95/98/Meのコントロールパネルでのパスワード変更（ただし、SambaをPDCにし、ドメインログオンしている場合だけ）
- Windows NT/2000/XPにおいてCtrl+Alt+Deleteを押してでたパスワード変更メニューで変更

Part 4：移行編

- 既存環境からSambaによるドメイン環境への移行

既存Samba環境からLDAP環境への移行

- 移行のためのツール
  - /usr/share/openldap/migration/migrate_all_online.sh などを使用して、/etc/passwd,groupをLDAPへ移行
  - Sambaのソースコードファイルexamples/LDAPの中にある import_smbpasswd.pl を使用して/etc/samba/smbpasswd を LDAPへ移行

    # cat /etc/samba/smbpasswd | import_smbpasswd.pl

Windows NT/2000サーバからの移行

- 移行のためのツール
  - PWDUMP2
    WinNT/2000のユーザ名とパスワード、マシンアカウントを抽出できる
    http://razor.bindview.com/tools/desc/pwdump2_readme.html
  - net group ｺﾏﾝﾄﾞ
    Windowsｻｰﾊﾞの標準ｺﾏﾝﾄﾞ
    ｸﾞﾙｰﾌﾟ情報が抽出できる
  - smbldap-tools
    - smbldap-migrate-accounts.pl
      PWDUMPを使ってWindows NT/2000 マシンのユーザ アカウント情報を移行するツール
    - smbldap-migrate-groups.pl
      Windows NT/2000 マシンのグループ情報を移行するツール

Windows NT/2000 DCからの移行手順（Samba 2.2の場合）

① WindowsドメインにSambaを追加して、SIDをコピーする
 # smbpasswd -S <ドメイン名> -r <PDC名>
② WinNT/2000ｻｰﾊﾞ上でAdministrator権限でPWDUMP2を実行し、ユーザ名とパスワード、マシンアカウントを抽出
③ WinNT/2000ｻｰﾊﾞ上でAdministrator権限でnet groupｺﾏﾝﾄﾞを実行し、グループ情報を抽出
④ 日本語ﾕｰｻﾞ名、ﾏｼﾝ名、ｸﾞﾙｰﾌﾟ名の変更またはﾏｯﾋﾟﾝｸﾞﾌｧｲﾙの作成
⑤ Linux上にpwdumpﾌｧｲﾙとｸﾞﾙｰﾌﾟDUMPﾌｧｲﾙを転送
⑥ smbldap-migrate-accounts.plでユーザ アカウント情報を移行
⑦ smbldap-migrate-groups.pl でグループ情報を移行
⑧ Windowsサーバを停止し、SambaをPDCとして設定

Windows NTサーバからの移行手順（Samba 3.0の場合）

① WinNTｻｰﾊﾞのBDCとしてSambaを設定
② ユーザ情報とパスワード、マシンアカウントを複製
③ WinNTｻｰﾊﾞを切り離し、SambaをPDCに昇格

Part 5：応用編

- Sambaの便利な機能
- MIRACLE LINUXが提供するSamba拡張機能

MS-DFS機能

DFSルート
¥¥WORLD¥MANAGER

複数台のSambaサーバを１台の仮想ファイル・サーバに見せる

Windowsプリンタドライバ自動配布機能

◆Windowsのプリンタドライバをクライアントに配布し、自動設定する機能

◆Windows 95 / 98 / Me / NT / 2000 / XPに対応

MIRACLE LINUXの特長(1)

- MIRACLE LINUX Standard Edition V2.1およびRed Hat Linux Advanced Server 2.1 powered by MIRACLEにてSamba 2.2.4日本語版を提供
- MIRACLE LINUX独自の機能をSambaにアドオンして提供
- バックアップや運用管理に汎用的な製品が利用できる（商用製品はオプション）
  - Red Hat 7.1対応の汎用製品が利用可能
  - バックアップ：Bakbone社Netvault
  - ウィルス防止：Trendmicro社ServerProtect for Linux
  - SNMP：「Net-DMS for MIRACLE LINUX」 http://www.nuritelecom.co.jp/

MIRACLE LINUXの特長(2)

- サーバ管理はWebminでWebブラウザから簡単GUI
  - 豊富なWebminコンポーネント
    - APC社のUPS管理
    - Mylex RAID DAC960設定
    - S/W RAID、LVM設定
- ドキュメント検索エンジン
  - Word,PDF,HTML,TXTファイルを自動検索
  - オプションで「デ変研」のDocCat、画像Catに対応
- PDFライター

Samba 2.2.4日本語版を採用

- **Windows 95 / 98 / Me / NT / 2000 / XP に対応**
  - **クライアント ライセンスは一切不要**
- **Windowsﾄﾞﾒｲﾝ･ｺﾝﾄﾛｰﾗになれる**
  - ドメインログオンや移動プロファイルのサポート
- **日本語対応**
  - 機種依存文字対応や日本語ドキュメント同梱
  - 日本語対応はミラクル・リナックス社がコミュニティに貢献
- **ゴミ箱機能**
  - 誤って削除してしまったファイルを復活
  - Windowsの場合、Undelete 2.0 for Windows NT/2000 (¥48,000)などの別途購入必要
    http://www.sohei.co.jp/ss/page_u.html
- **分散ファイルシステム（MS-DFS）をサポート**
  - 複数のファイルサーバを1台の仮想サーバに見せる
- **ユーザ毎／グループ毎の使用量制限**
  - 特定ユーザが資源を浪費することを防止
- **ユーザホーム機能**
  - 各ユーザ専用共有を提供

ﾄﾞｷｭﾒﾝﾄ検索機能(MIRACLE LINUX拡張）

- WindowsﾄﾞｷｭﾒﾝﾄをWebから簡単検索
- インデックスは定期的にバックエンドで自動実行
- 標準でTxt,html,doc,pdfに対応
- デ変研のDocCatを製品購入するとXLS,PPT、一太郎、花子にも対応
- デ変研の画像Cat を製品購入すると画像内の文字検索も可能、スキャナーサーバとの組み合わせも可

PDFライター (MIRACLE LINUX拡張）

- Sambaが提供する共有プリンタに印刷するとPDFが生成される
- GhostScriptのPS2PDFを使用しているので、ライセンス不要

Webmin:ｻｰﾊﾞ管理機能(MIRACLE LINUX拡張)

- Samba
- BIND
- FTPd
- DHCPd

Webmin:Samba設定機能

- 共有の作成
- ﾌﾟﾘﾝﾀ定義
- ｱｶｳﾝﾄ作成
- ﾊﾟｽﾜｰﾄﾞ変更
- SWAT 呼 び 出し

Webmin:SWAT(Samba Web管理ﾂｰﾙ)

- Webminにより暗号化
- Samba 2.2.4日本語版
- 日本語ﾄﾞｷｭﾒﾝﾄ

Webmin:ﾌｧｲﾙ･ﾏﾈｰｼﾞｬ

- ﾃﾞｨﾚｸﾄﾘの作成
- 属性変更(chmod)
- 所有者変更 (chown,chgrp)
- Samba共有を簡単に直接作成

MIRACLE LINUX 強力な新製品群紹介
～確かなエンタープライズ領域へ～

The Enterprise

- **Red Hat Linux Advanced Server powered by MIRACLE**

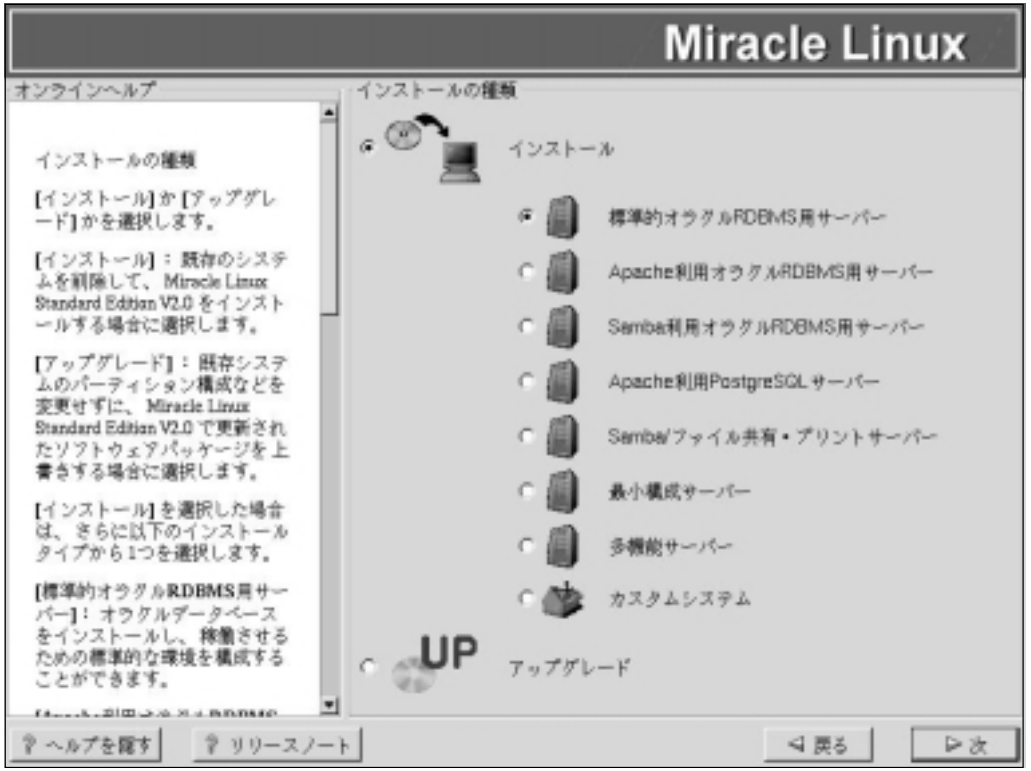
エンタープライズサーバOS、OraNAVI などのOracle特化の付加価値Oracle9i R1、R2対応予定 、Oracle9i Real Application Clusters対応Samba、PHP、PostgreSQL日本語対応

The Standard

- **MIRACLE LINUX Standard Edition**

業務システム向けサーバOS、小規模なファイル共有から大規模なクラスタ構成システムまで対応する拡張性、業務システムでの利用を前提とした高信頼性・高品質。

MIRACLE



MIRACLE

MIRACLE