

VA Linux Business Forum 2003

2003/06/20(金)

次世代Samba 3.0の 最新動向と諸問題



たかはし もとのぶ (高橋基信)

日本Sambaユーザ会 幹事

monyos@samba.gr.jp

<http://www.samba.gr.jp/>

講師紹介 – たかはしものぶ

- 日本Sambaユーザ会幹事
 - Sambaドキュメントの翻訳
 - Samba日本語版の作成(Samba 2.0系列)
- 各所にて講演や雑誌の執筆をおこなう
 - Software Design, UNIX USER 各誌他
- Microsoft 技術者としても活動
 - 日経各誌で記事執筆、講演など
 - アンドキュメンテッドMicrosoftネットワーク執筆
- <http://www.monyo.com/>

セミナーの概要

- Samba 概要
- Samba の入手とインストール
- Samba 3.0 の機能強化点
 - 国際化処理の変更
 - VFS機能
 - BDC機能
 - グローバルグループ機能
 - 認証機能の拡張
 - Active Directory参加機能
 - WINS機能の強化
 - セキュリティ機能の向上(NTLMv2、SMB署名)
 - SWAT国際化機能
 - リモート管理機能の強化
 - 管理コマンドの強化

Samba概要 – Sambaとは

- **Windows NT 互換のサーバ**機能を提供
 - ファイル、印刷サーバをはじめ、各種の機能を提供
 - 各種UNIX互換OS(**Linux**, FreeBSD等)上で動作
- **オープンソース**(GPL準拠)
 - 誰でもソースの解析や、改良が可能
 - 無償で入手が可能
- **実績**がある
 - 企業内導入も多数
 - 各種Linuxに標準添付。その他HPやSGIでも正式サポート

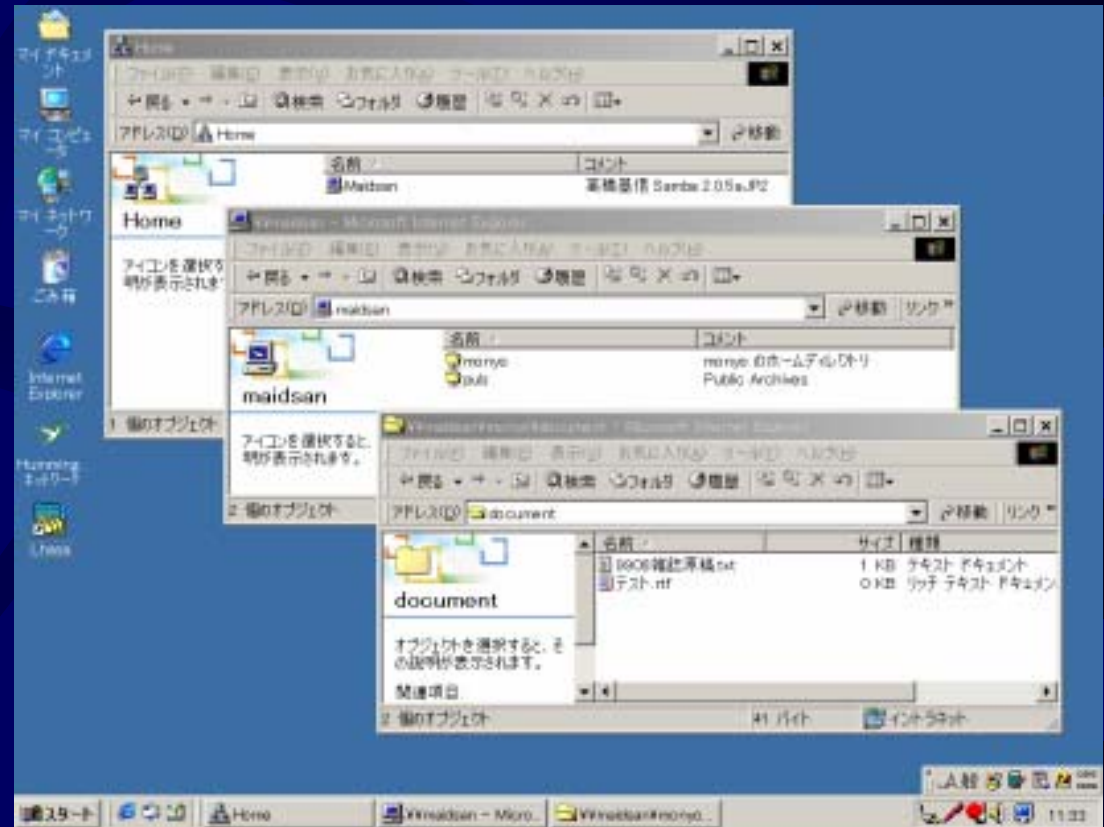
Microsoft, WindowsはMicrosoft Corporationの米国およびその他の国における商標または登録商標です。
その他の製品および会社名は、各社の登録商標又は商標です。

Samba概要 – Samba紹介

- ファイル・プリンタサーバ機能の実行

Windows のサ
ーバと全く同じ

クライアントの
設定変更不要



Samba概要 – Sambaの主要機能(1)

- ファイル・印刷サーバ
 - 日本語ファイル名(Samba日本語版で完全サポート)
 - ACL(ただしOSがサポートしている場合)
 - NT互換のドライバ自動ダウンロード機能
 - Windows GUIからの共有管理
 - DFS機能 / VFS機能
 - UNIXとWindowsのファイルシステムの差分吸収
 - UNIX側のアクセス権のマッピング
 - 作成日付の対応、その他細かい機能差の吸収

Samba概要 – Sambaの主要機能(2)

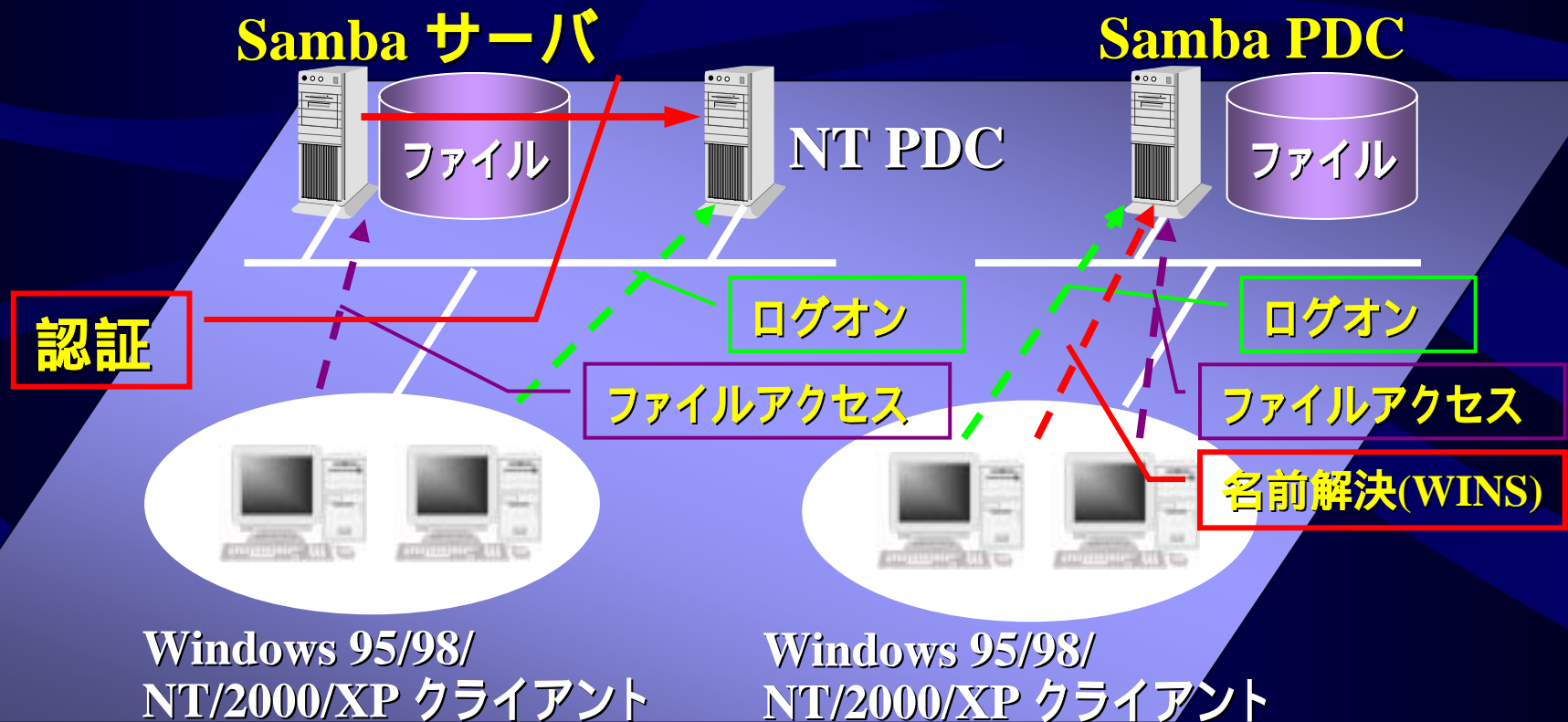
- ドメインコントローラ・認証
 - PDC機能
 - ログオンスクリプト、システムポリシー
 - LDAPによる認証の統合
- メンバサーバ機能
 - NTドメインのアカウントを自動作成
 - Winbind機能
 - NTドメインのアカウント情報を利用
 - Samba以外に対しても、PAM経由で認証情報提供

Samba概要 – Sambaの主要機能(3)

- ブラウジング機能
 - マスタブラウザとして機能
 - ドメインマスタブラウザとして機能
- WINS機能
 - WINSサーバ、クライアント
 - WINS登録を契機にしたDNSへの自動登録
- セキュリティ機能
 - ホスト・IPアドレスベースのアクセス制御
 - 暗号化パスワード

Samba概要 – Samba紹介

• Samba のあるネットワーク



Sambaの現状

- Samba 2.2シリーズ
 - 2001年4月リリース (Samba 2.2.0)
 - 最新版は Samba 2.2.8a (2003/04/07)
- Samba 3.0シリーズ
 - 最新版は Samba 3.0.0beta1 (2003/06/07)
 - 今年中にはリリースされる感触
 - そろそろ情報収集が必要か

アーカイブの入手

- 基本的にソースアーカイブを入手
 - ベータ版アーカイブを取得
 - `ftp://ftp.samba.gr.jp/pub/samba/beta/`
 - 現在の最新版は `samba-3.0.0beta1.tar.{gz,bz2}`
- 日本Sambaユーザ会提供のCVSスナップショット
 - `ftp://ftp.samba.gr.jp/pub/samba-jp/cvs/snapshot/`
 - `samba-head.snapshot-YYYYMMDD.tar.{gz,bz2}`
- CVSリポジトリから直接取得
 - `http://www.samba.org/samba/cvs.html`

コンパイルとインストール

- 基本的には通常のフリーソフトウェアと同じ

```
$ gzip -dc samba-3.0.0beta1.tar.gz | tar xf -
$ cd samba-3.0.0beta1/source
$ ./configure --with-libiconv=(libiconvインストールパス) ¥
  (任意のオプション)
$ make
$ su
# make install
```

- 実用上パッチを適用したGNU libiconvがインストールされていることが必須
- Samba 3.0の新機能サポートに configure オプションは不要
- PAM対応のOS(殆どのLinux、Solaris等)では、configure 時に--with-pamを指定すること

コンパイルとインストール

• Sambaが依存しているプロダクトなど

– iconv()関数(GNU libiconv)

- 日本語利用 (UTF-8以外)のためにはlibiconv-1.8に含まれるiconv()に以下のパッチを適用することが必須

<http://www2d.biglobe.ne.jp/~msyk/software/libiconv-patch.html>

- 日本語の文字コード変換ロジックについては、iconv()の実装によって微妙に異なる。現時点では、GNU libiconv-1.8以外は未検証

– MIT Kerberos5

- Active Directoryと連携する場合は必須

– その他

- OpenLDAP / OpenSSL など。必要に応じて

configureオプション

- 目立った追加はない
 - 極力デフォルトの機能として取り込んでいく方針

<code>--with-smbwrapper</code>	No	smbmountに代わるsmbsh機能を有効にする
<code>--with-smbmount</code>	No	Linuxカーネルのsmbfsをサポートするコマンドを作成する
<code>--with-pam</code>	No	PAM認証機構をサポートする
<code>--with-pam_smbpass</code>	No	他のプログラムが利用可能なPAMモジュールを構築する
<code>--with-syslog</code>	No	syslogへの出力機能をサポートする
<code>--with-quotas</code>	No	QUOTA機能をサポートする
<code>--with-utmp</code>	自動	utmpによるユーザのアクセス記録の収集をサポートする
<code>--with-manpages-langs</code>	<u>en</u>	<u>インストールするマニュアルページを選択する</u>
<code>--with-acl-support</code>	No	ACL機能をサポートする
<code>--enable-cups</code>	<u>自動</u>	<u>新しい印刷機能であるCUPSのサポートを有効にする</u>
<code>--with-winbind</code>	自動	Winbindを構築する
<code>--with-ads</code>	<u>Yes</u>	<u>Active Directoryサポート</u>
<code>--with-shared-modules</code>	<u>なし</u>	<u>拡張モジュールをコンパイルする</u>

Samba 3.0の機能強化点(1)

- 全般
 - 国際化処理の変更(文字コード)
- ファイル・プリンタサーバ
 - VFS機能の改良
- ドメインコントローラ・認証
 - BDC機能
 - 信頼関係
 - 任意のグローバルグループ
 - 利用可能な認証方式の拡張

Samba 3.0の機能強化点(2)

- メンバサーバ機能
 - Active Directoryクライアント機能
- WINS機能
 - WINS複製機能
 - 静的マッピング機能
- セキュリティ機能
 - NTLMv2対応、セキュアチャネルの署名対応
- 管理性の向上
 - SWATの国際化
 - Windows GUIからの管理可能な項目の増加

国際化処理の変更

- 日本語(国際化)の処理が大幅に変更
 - Samba 2.2系列までは、Samba内部に文字コード変換ロジックを同梱
 - Samba 3.0では、外部の`iconv()`関数を用いたロジックに全面変更
 - ネットワーク上の文字コードがMS-DOS互換(シフトJIS)からUnicode(UCS-2)に変更
 - Samba内部の文字コードも変更
 - 関連するパラメータが全面的に変更

従来Sambaの日本語処理の実装

- Samba 2.2系列までは基本的に同一
 - 文字コード変換ロジックは、Samba内部で実装
 - 日本語処理に必要なパラメータ

```
[global]
  client code page = 932
  coding system    = SJIS/EUC/CAP/HEX/UTF8/UTF8-MACなど
```

- Samba 日本語版では、「シフトJIS正規化」や機種依存文字対応などを行っている
- ネットワーク上の文字コードはMS-DOS互換

Samba 3.0の日本語処理の実装

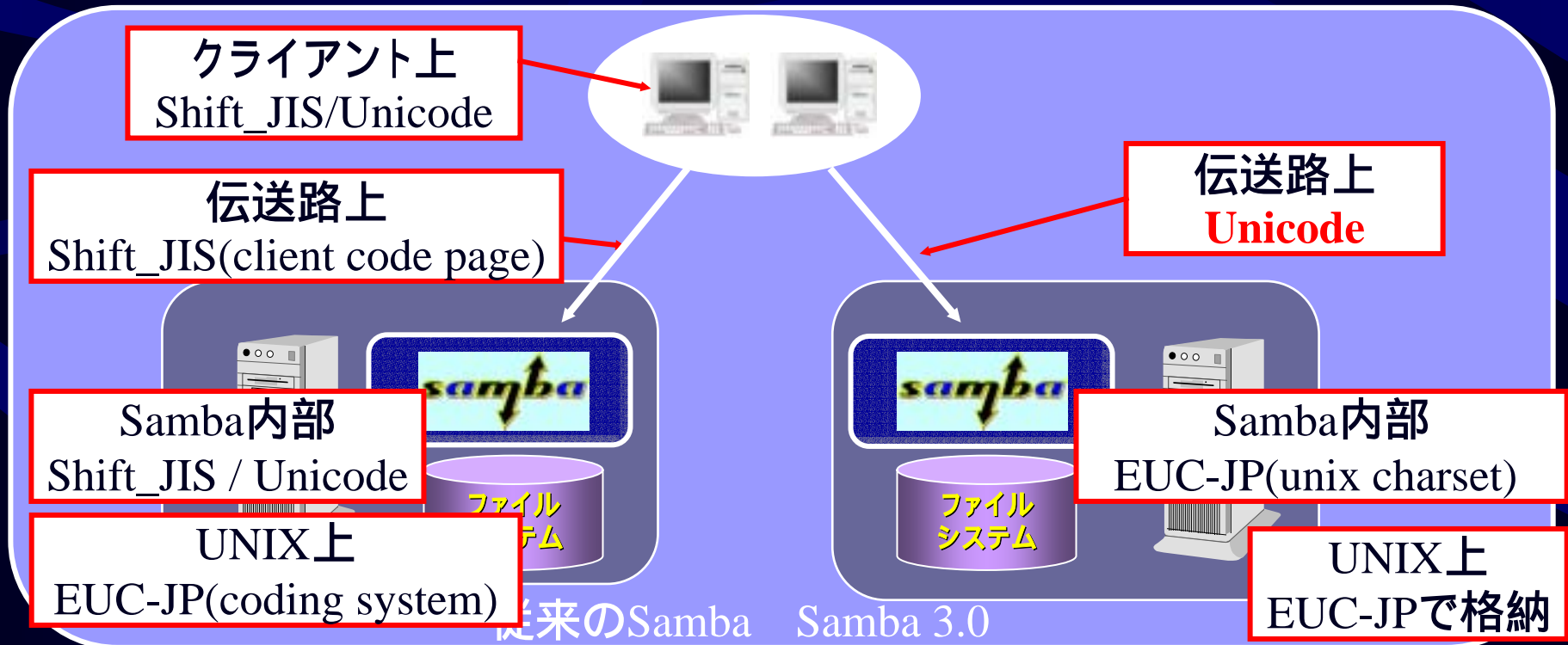
- Samba 2.2までとは大きく異なる
 - 文字コード変換ロジックは、`iconv()`に依存
 - ただし、ucs-2など一部は内部で実装
 - `iconv()`は標準的な文字コード変換関数
 - 独自に拡張することもできる
 - 日本語処理に必要なパラメータ

```
[global]
  dos charset      = CP932(ただし必須ではない)
  unix charset     = CP932/EUC-JPなど(デフォルトUTF-8)
  display charset  = CP932など
```

- ネットワーク上の文字コードはUnicode

文字コードの変更

- ネットワーク上の文字コードはUnicodeに
 - シフトJIS正規化問題が自然解消
 - Samba内部は、unix charset で指定した文字コード



日本語処理に必要なパラメータ

- Samba 2.2系列とはパラメータが異なる

パラメータ	説明
<code>unix charset</code>	UNIX上のファイルシステムで用いられている文字コード(符号化形式)をあらわします。デフォルトUTF-8
<code>dos charset</code>	Windows側でUnicodeを使用しない場合に使用する文字コードを指定します。 日本語を利用する場合は、CP932 に設定します。
<code>display charset</code>	SWATの画面に表示される文字コードを指定します。

- 各パラメータの値には、`iconv()`関数がサポートする各種形式を指定
 - 現時点でCAPやHEXはサポートされていない
 - JIS系列はSambaの実装上正常動作しない

日本語処理に必要なパラメータ(2)

• Samba 2.2系列との比較

従来の coding system	Samba 3.0の unix charset	Samba 3.0での現状
SJIS	CP932	現状ではiconv()側の実装の問題のため、一部問題が発生。パッチ適用により解決
EUC	EUC-JP (EUCJP-MS)	現状ではiconv()側の実装の問題のため、利用できない。 EUCJP-MSパッチ適用により、ほぼ解決
JIS		実装上サポートできない
CAP/HEX	現時点ではなし	VFSでの実装を検討中。 <u>HEXについては現在確認中</u>
UTF8	UTF-8	問題なし
UTF8-Mac	現時点ではなし	モジュールでおそらく実装可能

libiconv-1.8へのパッチ:

<http://www2d.biglobe.ne.jp/~msyk/software/libiconv-patch.html>

日本語関連パラメータの問題点

- `iconv()`化に伴い、多数の問題が発生
 - CAPやHEXがサポートされていない
 - VFSで対応したい。簡単に確認した限り動作しそう
 - `unix charset=EUC-JP`がうまく動作しない
 - `libiconv`の作者にWindowsとの互換性を重視したEUC-JPロケールの実装を行ってくれるよう連絡
 - 当面はパッチで対応
 - UTF8-Macの扱い
 - モジュールで実現か?
 - 各所における実装のデグレード対処
 - 地道な検証と regression test が必要

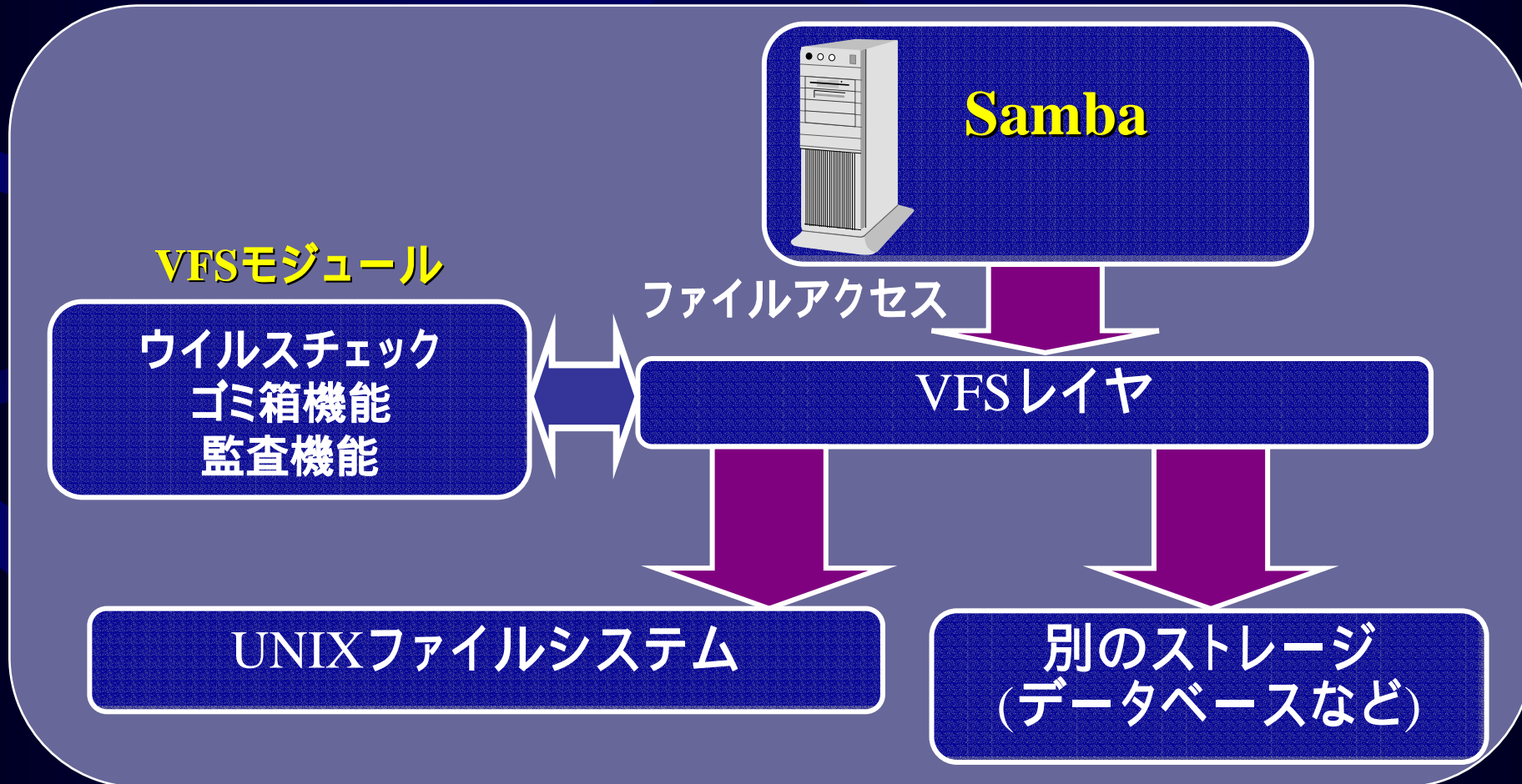
Samba 2.2までの日本語機能の設定

• 各文字コード設定の特徴

coding system	特徴
euc (EUC方式)	UNIX上で日本語のファイル名を表示できる 一部のSJIS 固有の文字は使えない(EUC3で対応)
sjis (シフトJIS方式)	Windowsとのファイル名の互換性が最大になる <u>SJIS非対応のUNIXでは問題が発生することがある</u>
cap (CAPと互換性のある方式)	MacintoshファイルサーバのCAPと互換性がある ファイル名がASCII文字で表現されるので判読困難
hex (独自のエンコード方式)	<u>ファイル名がASCII文字だけの為、UNIXとの互換性が最大になる</u> ファイル名がASCII文字だけで表現されるので判読困難

VFS機能

- ファイルシステムのレイヤを仮想化



VFS機能

• VFS機能の設定例

```
[share]
  vfs object = audit.so
  vfs options =
  vfs path = /usr/local/samba/lib
```

• 現在存在するVFSモジュール

- audit / extd_audit (監査機能)
- recycle (ゴミ箱機能)
- netatalk (NetAtalk用の特殊フォルダを不可視に)
- fake_perms (パーミッションを読み取り専用にみせる)

BDC機能のサポート

- NTドメインのBDCとして機能

```
[global]
domain logons = yes
domain master = no      PDCの場合はyesにする
```

- ただし、Windows NTのPDCとのSAMの同期は未サポート(実装中)
- Samba同士のSAMの同期は可能
 - LDAP(またはNIS+)などのディレクトリサービス
 - smbpasswdファイルなどを直接複製 (rsyncなど)

信頼関係のサポート

- 別ドメインと信頼関係を構築可能
 - smbpasswd -i コマンドで信頼関係用アカウントを作成する

```
root# smbpasswd -a -i rumba   ドメイン名(ここではrumba)を入力
New SMB password:           信頼関係用のパスワード
Retype SMB password:        再度入力
Added user rumba$
```

- Windows 側からは通常の信頼関係構築と同様に操作する

グローバルグループ機能

- 従来のグローバルグループ機能
 - Samba 2.2系列では、特定のグローバルグループのみをサポート
 - `domain admin group` (Domain Admins グループ)
 - `domain guest group` (Domain Guests グループ)
 - Samba 3.0 では、任意のグローバルグループをサポート可能に
 - <http://www.samba.org/ftp/unpacked/samba/docs/htmldocs/groupmapping.html>

グローバルグループ機能(2)

- Samba 3.0 のグローバルグループ機能
 - 任意のグローバルグループをサポート可能
 - smbgroupedit コマンドでグループを対応付ける

```
#smbgroupedit -a group1 -n "Group 1" -td
    UNIX側group1グループをGroup 1グローバルグループとして公開
#smbgroupedit -vs | grep "Group 1"
    Group 1グローバルグループのSIDを確認
Group 1 (S-1-5-21-1108995562-3116817432-1375597819-3449) -> group1
```

- クライアント側からは
通常のグローバル
グループとして表示さ
れる



認証機能の拡張

- 任意の認証機構を任意の順番で適用可能
 - `passwd backend`パラメータ
 - 複数の認証方式を任意の順番に組み合わせて使うことが可能に
 - 250ユーザまでは`tdbsam`、それ以上はLDAPが推奨
 - 独自の認証機能を拡張可能
 - 従来は、コンパイル時に指定
 - しかも、LDAPやNIS+を有効にすると`smbpasswd`ファイルによる認証は無効になってしまう

認証機構の拡張(2)

- **passdb backendパラメータ**
 - 複数の認証方式を任意の順番に組み合わせて指定

```
[global]
    passdb backend = ldapsam:ldap://ldap.home.monyo.com ¥
    smbpasswd guest
(デフォルトは passdb backend = smbpasswd guest)
```

キーワード	認証方式
smbpasswd	デフォルト、従来からの方式(ファイルのパス名を指定)
tdbsam	TDB形式のデータベース(ファイルのパス名を指定)
ldapsam	LDAPサーバ(LDAPサーバのURLを指定)
nisplussam	NIS+サーバ(NIS+ドメイン名を指定)
mysql	mysqlのデータベース
guest	ゲスト認証

Active Directory参加機能

- Windows 2000と同じKerberos認証をサポート
 - MIT Kerberos 5が必要
 - NetBIOSが無効な環境でもADドメイン参加が可能
 - Samba 2.2までと同じ方法でも参加自体は可能
 - ただし、NTと同様のNetBIOSを利用した方式となる
 - 「security = ADS」が追加

```
[global]
realm = <ADのドメイン名(大文字)>
ads server = DC名
security = ADS
encrypt passwords = yes
```

Active Directory参加(1)

- Samba 3.0コンパイル、インストール
 - source/config.hが以下のようにになっていることを確認

```
#define HAVE_KRB5 1
#define HAVE_LDAP 1
```

- /etc/krb5.conf を修正

```
[realms]
  W2K.HOME.MONYO.COM = {      Active Directoryのドメイン名
                              (Kerberos Realm名)必ず大文字で記述すること
  kdc = miyu.w2k.home.monyo.com:88      DCのFQDN名
}
```

- smb.conf修正

Active Directory参加(2)

• kinitコマンド実行

```
[root@maple]# kinit administrator
Password for administrator@W2K.HOME.MONYO.COM:
Administrator のパスワード
```

- このコマンドを実行する前に、Administratorのパスワードを一度は変更しておく必要がある

• net ads joinコマンド実行

```
[root@maple]# ./net ads join
Joined 'MAPLE' to realm 'W2K.HOME.MONYO.COM'
```

• Sambaの起動

WINS機能の強化

- 別WINSサーバとの複製をサポート
 - 専用のデーモン `wrep1d` により実現
 - 複製先は `smb.conf` ファイルで指定する
 - 現段階では検証レベルで不安定

```
[global]
wins partners = 192.168.1.10
```

- WINS静的エントリ機能(実装予定)
 - `winsedit` コマンドにより編集機能を実装予定
 - WINSデータベースのTDB化も合わせて実装予定

セキュリティ機能の向上

- Windows と同レベルのSMBセキュリティを実装

機能	Windows NT/2000/XP	Samba 2.2	Samba 3.0
LMレスポンス抑止	可能 LMCompatibilityLevel	可能 lanman auth	可能 lanman auth
NTLMレスポンス抑止	可能 LMCompatibilityLevel	不可能	可能 ntlm auth
NTLMv2対応	可能(NT 4.0 SP4以降) LMCompatibilityLevel	不可能	可能
SMB署名	可能(NT 4.0 SP3以降)	不可能	不可能?
セキュアチャネル 署名・暗号化	署名、暗号化可能 (NT 4.0 SP4以降)	不可能	署名可能 server schannel

SWAT国際化機能の同梱

• Samba日本語版の成果が同梱

- デフォルトで機能が有効になっている
- SWATからの文字コード関連パラメータの変更は、現状問題がある



SWAT国際化機能の同梱(2)

- インストールおよび使用の注意点
 - SWATから文字コード関連パラメータを変更できない
 - 変更してもよいが、日本語などは文字化けしてしまう
 - `make install`ではメッセージカタログのファイルがインストールされない
 - Sambaのアーカイブの`source/po`ディレクトリにある`msg`という拡張子のファイルを、手作業で`smb.conf`と同じディレクトリにコピーする
 - メッセージカタログがソースと同期されていない
 - `make update-po`に相当するメッセージカタログのテンプレートファイルの更新コマンドが存在しない

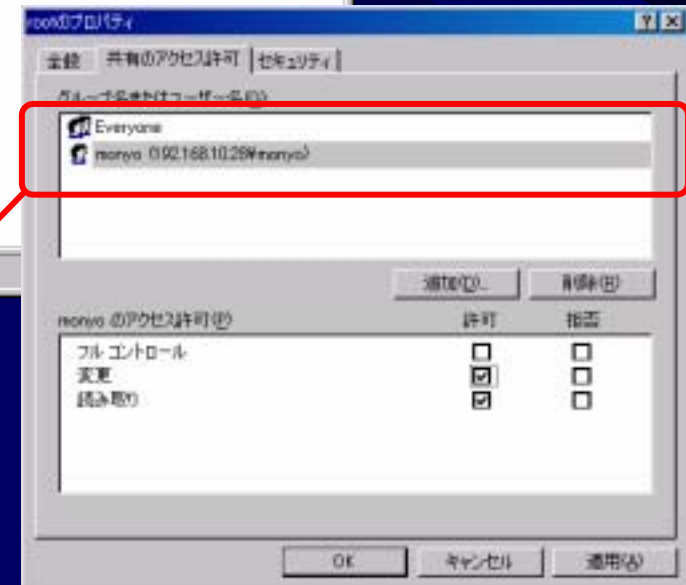
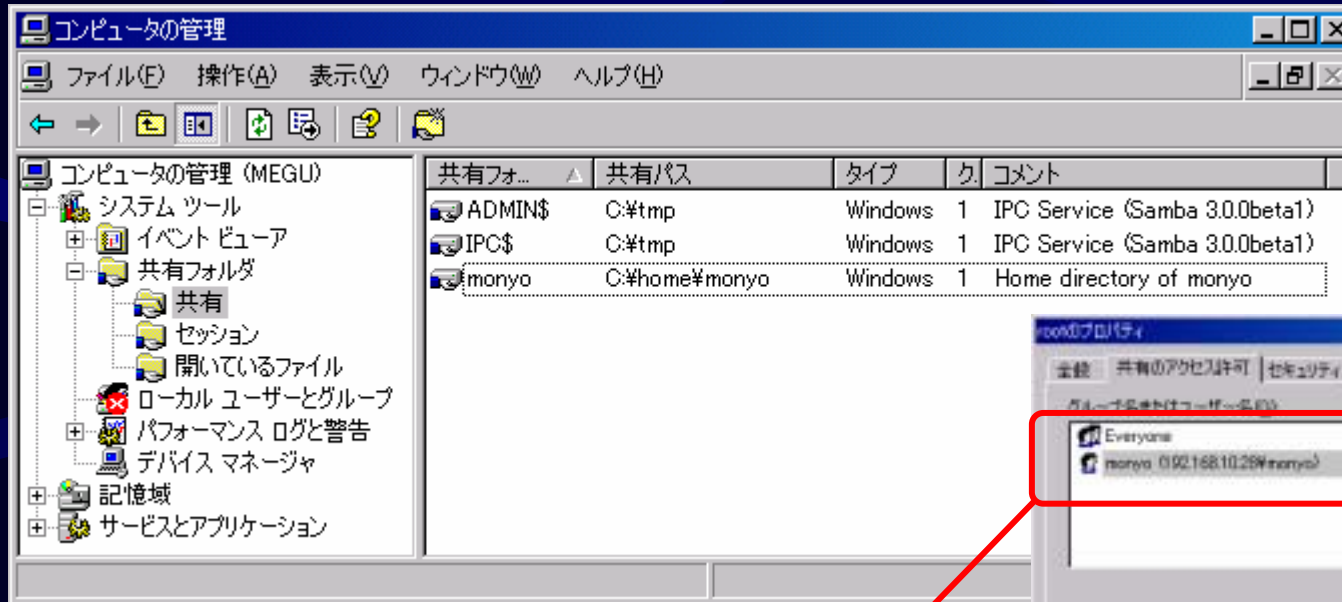
リモート管理機能の強化

- Windows のGUIからSambaの管理が可能に

対象	操作	パラメータ名
共有	作成 削除 修正	add share command delete share command change share command
プリンタ	作成 削除	add printer command delete printer command
グループ	作成 メンバ追加 削除 メンバ削除	add group script add user to group script delete group script delete user from group script
共有アクセス権	(操作)	(アクセス権はtdbに格納)
シャットダウン	実行 中断	shutdown command abort shutdown command

リモート管理機能の強化

- サーバマネージャや、コンピュータの管理を使用



共有へのACLを設定可能
(ACL機能の有無に関わらず)

管理コマンドの強化

- netコマンド
 - リモートからWindows NT系マシンやSambaの管理、構成を実現
 - コマンドラインベースなのでバッチ処理可能
- pdbeditコマンド
 - パスワード情報の表示、編集
 - LDAP、smbpasswdファイルなどを透過的に編集、表示
- smbtreeコマンド
 - ブラウズリスト、共有一覧の表示

netコマンド(1)

• netコマンド

- 多数のオプションをサポート
 - net <コマンド> <サブコマンド> <オプション>
- RAP = Remote Administration Protocol

	コマンド	サブコマンド	説明
net	rap	domain	ドメインの一覧を表示
		file	サーバ上でオープンされているファイルを表示
		group	ユーザグループを表示
		groupmember	グループ中のメンバを表示
		password	ユーザのパスワードを変更
		printq	サーバ上の印刷キューを表示
		server	ドメインに所属するサーバを表示
		session	サーバに対してセッションを張っているクライアントを表示
		share	サーバが公開している共有を表示
		user	ユーザの一覧を表示
		validate	ユーザおよび設定されているパスワードが適切かどうかを確認

netコマンド(2)

	コマンド	サブコマンド	説明
net	rpc	join	ドメインに参加
		user	ユーザの一覧表示および追加、削除
		changepw	信頼関係アカウントのパスワードの変更
		abortshutdown	リモートマシンのシャットダウン中断
		shutdown	リモートマシンのシャットダウン
	ads	join <org_unit>	ローカルマシンをActive Directoryドメインのレルムに参加
		leave	ローカルマシンをActive Directoryドメインのレルムから削除
		testjoin	現在の参加状態をテスト
		user	レルム中のユーザの一覧および追加、削除
		group	レルム中のグループの一覧および追加、削除
		info	サーバの情報を表示
		status	マシンアカウントの詳細を標準出力に出力
		password ...	管理者によりユーザのアカウントを変更(注意: レルム名は大文字で指定)
		chostpass	このマシンのActive Directoryにおける信頼関係パスワードの変更
		printer [info publish remove] ...	プリンタのディレクトリエントリの表示および追加、削除
		search	低レベルのLDAP検索の実施および結果の出力

pdbeditコマンド

- 認証データベース中の情報の表示、編集、追加
 - プロファイル情報(ホームディレクトリなど)を個別に設定可能

```
options:
  -l                list usernames
  -v                verbose output
  -w                smbpasswd file style
  -u username       print user's info
  -f fullname       set Full Name
  -h homedir        set home directory
  -d drive          set home dir drive
  -s script         set logon script
  -p profile        set profile path
  -a               create new account
  -m               it is a machine trust
  -x               delete this user
  -i file           import account from file (smbpasswd style)
  -D debuglevel     set DEBUGLEVEL (default = 1)
```

```
[root@mana head]# pdbedit -u monyo -v
username:          monyo
user ID/Group:     1008/1008
user RID/GRID:     3416/3417
Full Name:         TAKAHASHI Motonobu
Home Directory:    ¥¥mana¥monyo
HomeDir Drive:
Logon Script:
Profile Path:      ¥¥mana¥monyo¥profile
```

ヘルプ画面

ユーザ情報の詳細表示

smbtreeコマンド

- ブラウズリストを表示
 - 日本語には対応していない
 - マスタブラウザに対する問い合わせ、ブロードキャストによる問い合わせの双方に対応

```

mony@mana:/home/mony/Work/Samba/head - mayu VT
File Edit Setup Control Window Help
[mana:/home/mony/Work/Samba/head]
[mana:/home/mony/Work/Samba/head]/usr/local/samba-head.20020227/bin/smbtree -b
Password:
V2K
SMB
NT40002
  VVHANA
    VVHANA\mony
    VVHANA\ADMIN$
    VVHANA\IPC$
    VVHANA\group1
    VVHANA\private
    VVHANA\public
  HOME
    VVMEGUMI
  客M Windows XP Professional
    VVMEGUMI\WC$
    VVMEGUMI\serverroot$
  VFN: 18C
    めANZ(英語)
    VVMEGUMI\ADMIN$
    VVMEGUMI\TEMP
    VVMEGUMI\SharedDocs
    VVMEGUMI\IPC$
    VVMEGUMI\dos_exlanen
  VVMAYU
    VVMAYU\mony
    VVMAYU\ip
    VVMAYU\ADMIN$
  for Debian))
    VVMAYU\IPC$
  for Debian))
    VVMAYU\lmp
    VVMAYU\cdrom
    VVMAYU\club
    VVMAYU\netlason
  VVMARI
  客M Windows 98
[mana:/home/mony/Work/Samba/head]

```

Samba 2.2からの移行

- パラメータに関しては、基本的にはそのまま
 - ただし、国際化関連については大幅な変更
 - Windows 9x互換の印刷機能のサポートが廃止
- LDAPサポート
 - Samba 2.2の機構をそのまま利用したい場合は、
configure時に`--with-ldapsam`を追加
- 認証データベースの記述方法が変更
 - 詳細は`passwd backend`パラメータを参照

日本Sambaユーザ会

- Sambaに関する技術情報の収集、公開や普及活動を実施しております
 - 日本Sambaユーザ会の各種活動
 - ドキュメント作成
 - Webサイト運営
- などへのご協力をお願いいたします

