

2009年2月18日(水) 13時30分～16時30分

LPICレベル3技術解説セミナー
「302 Mixed Environment Exam」
受験のための勉強法
Samba編

オープンソース・ソリューション・テクノロジー株式会社
代表取締役 チーフアーキテクト 小田切耕司



Linux
Professional
Institute

お問い合わせ info@osstech.co.jp



OSSTech

目次

1. 講師紹介、OSSTech社紹介
2. Samba機能と特徴
3. Windows移行 Q & A
4. Sambaのインストールと設定
5. Sambaサーバ運用と管理コマンド
6. やってはいけないSambaサーバ構築

講師紹介
オープンソース・ソリューション・テクノロジー
会社紹介



Linux
Professional
Institute



OSSTech

講師著作紹介

- ◆ @IT やってはいけないSambaサーバ構築:2008年版
- ◆ 日経コミュニケーション2007年11/15号から3回連載
Windows管理者に送るSamba活用の道しるべ
- ◆ 技術評論社 Software Design 2006年7月号
 - ネットワーク運用/管理 五輪書(ごりんのしょ)
 - 「壱:地の巻」Sambaファイルサーバ
 - <http://www.gihyo.co.jp/magazines/SD/contents/200607>
- ◆ 2006年5月 翔泳社 開発の現場 vol.005
 - オープンソース案件指南帖
 - 総論編:オープンソースの基礎知識
 - <http://www.shoeisha.com/mag/kaihatsu/>
- ◆ 2006年5月 技術評論社 LDAP Super Expert
 - 巻頭企画
 - [新規/移行]LDAPディレクトリサービス導入計画
 - <http://www.gihyo.co.jp/magazines/ldap-se>
- ◆ 2006年5月 IDG月刊Windows Server World 2006年3月、4月号
 - 3月号: Shall we Samba?【お手軽導入編】
 - 4月号: Shall We Samba?【超本格運用編】
- ◆ 2005年10月 日経BP社 セキュアなSambaサーバの作り方
 - <http://itpro.nikkeibp.co.jp/linux/extra/mook/mook12/index.shtml>



オープンソース・ソリューション・テクノロジー株式会社

- 2006年9月に設立
- **OSに依存しないOSSのソリューションを中心に提供**
 - Linuxだけでなく、SolarisやFreeBSDへも対応！
- **Samba、LDAPなどによる認証統合ソリューションを提供**
 - 製品パッケージ提供
 - 製品サポート提供
 - 技術コンサルティング提供

<http://www.osstech.co.jp>

会社概要

会社名	オープンソース・ソリューション・テクノロジー株式会社	所属 団体等	<ul style="list-style-type: none"> Linuxコンソーシアム 理事 LPI-Japanビジネス・パートナー
英語表記	Open Source Solution Technology Corporation		
社名略称	OSSTech(オーエスエステック)または OSSテクノロジー	主要 取引先 および パートナー 様	<ul style="list-style-type: none"> デル(株) (株)野村総合研究所 サン・マイクロシステムズ(株) キャノンITソリューションズ(株) (株)バッファロー (株)大塚商会 日本電信電話(株) 日本電気(株) 伊藤忠テクノソリューションズ(株) 新日鉄ソリューションズ(株) (株)日立システムアンドサービス ミラクル・リナックス株式会社
業務内容	<ul style="list-style-type: none"> ソフトウェアの企画、開発、販売およびサポート システムの導入に関するコンサルティング ソフトウェアに関する教育、研修、支援 		
役員	代表取締役 小田切 耕司 技術取締役 武田 保真		
オフィス	〒141-0022 東京都品川区東五反田1-10-7 アイオス五反田ビル Tel & FAX : 03-5422-9373		
Webページ	http://www.osstech.co.jp/		
設立	2006年9月		
資本金	1080万円		

「302 Mixed Environment Exam」: 出題範囲

- **主題 310: 概念、アーキテクチャおよび設計**
- **主題 311: Sambaのコンパイルとインストール**
- **主題 312: Sambaの設定と使用法**
- **主題 313: ユーザとグループの管理**
- **主題 314: CIFS、NetBIOS、およびActive Directoryとの連携**
- **主題 315: セキュリティとパフォーマンス**

Part 1.

Samba機能と特徴



**Linux
Professional
Institute**



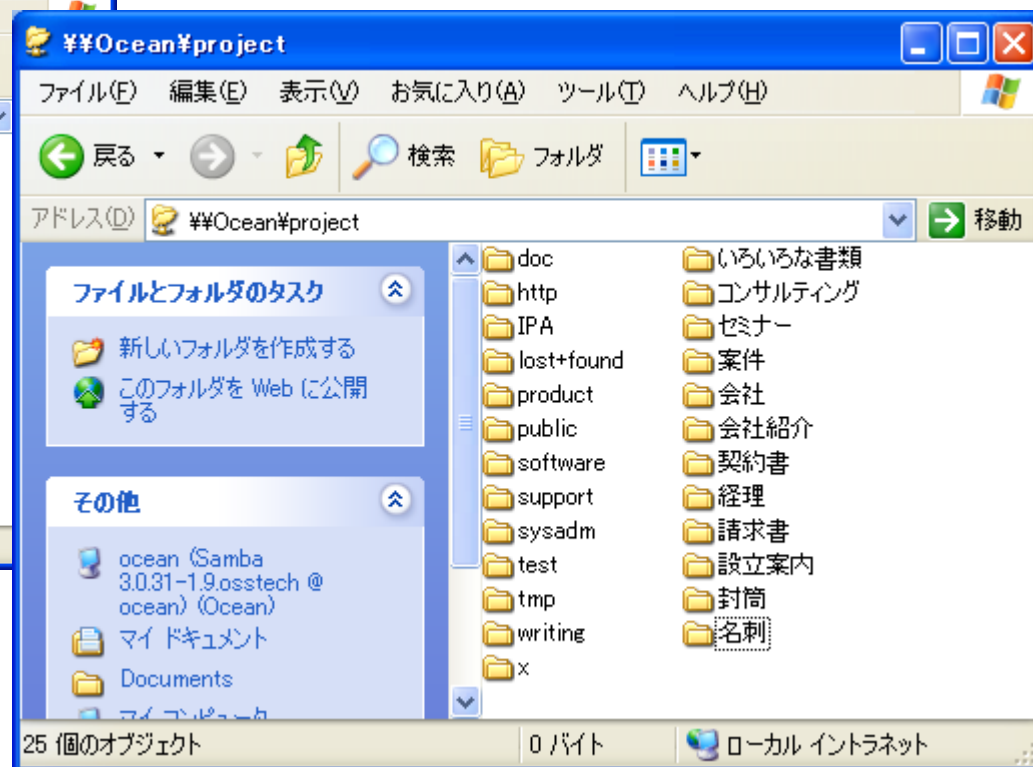
OSSTech

Samba (サンバ)とは

LINUXなどのUNIX系OS上で稼動する、Windowsのファイル、プリンタ共有機能を提供するオープンソースソフトウェア



Sambaサーバへアクセスした画面



ユーザーはWindowsで構築した
サーバーと見分けがつかない

WindowsファイルサーバをSambaで構築する理由

セキュリティ対策

Windowsに比べ、ウィルスなどの被害が圧倒的に少ない。

コスト削減

Windowsサーバでは、アクセスするユーザごとにCAL(Client Access License)が必要

サーバーの低価格化によりOSライセンスコストの割合が増加

高い信頼性

連続運転に強い

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

シェルのスクリプト化によって、運用の効率化が可能

修正モジュールの適用に、OSリブートの必要がない

Sambaの機能概要

ファイルサーバ機能

Samba3.0はWindowsと同等以上の機能をサポート

プリンタサーバ機能

クライアントPCにプリンタドライバを自動配布、PDFライター

Windows GUIによる管理機能

ユーザ管理、共有管理がWindowsの GUI画面で可能

ドメインコントローラ機能

NTドメインのドメインコントローラが備えるユーザ情報、システムポリシー、ログオンスクリプトなどを実装。

WINSサーバ機能

Windowsネットワークで使われる「コンピュータ名」をIPアドレスに変換

Windowsドメイン連携/Winbind機能

LinuxサーバをWindowsドメインに参加させることができる

Windowsドメイン内のユーザIDやグループIDをLinuxサーバ上で使用

1. Sambaのファイルサーバ機能

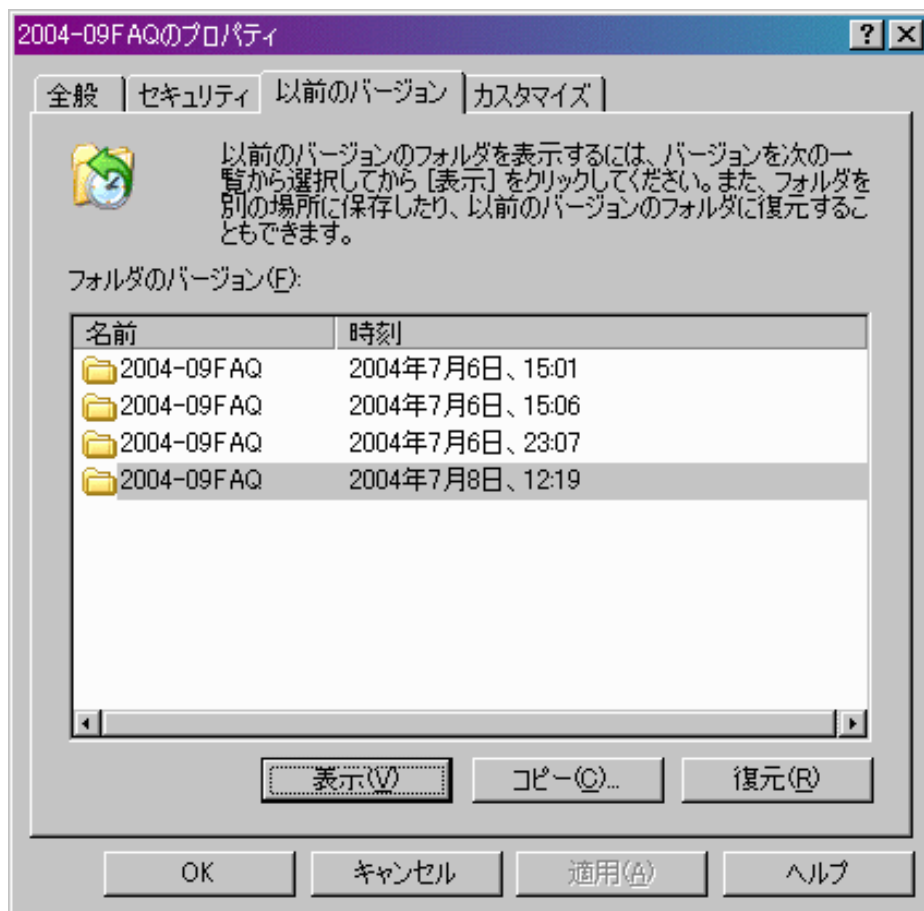
Samba3.0はWindowsと同等以上の機能をサポート

- ユーザ/グループによる容量制限(ディレクトリ単位にも対処可)
- 論理ボリューム・マネージャ
- 日本語ディレクトリ/ファイル名
- ゴミ箱機能:ユーザが誤って削除したファイルを復元 ★
- ユーザホーム機能:ユーザ名のついた専用の共有 ★
- 分散ファイルシステム(MS-DFS) /オフラインファイル機能
- ACL(アクセスコントロールリスト)による詳細なアクセス許可の設定
Windows NTFSと同様のアクセス制御が可能
- ホスト名によるアクセス制御 ★
- ボリューム・シャドー・コピー(スナップショット)機能 *次スライド参照

➤LVMの機能により、アクセス中のファイルのスナップショットを作成し、WindowsのShadowCopyクライアントから削除されたファイルを復活。
修正前のファイルの取り出しなどが可能

★:Windows2003で実装されていない機能

1-1. ボリューム・シャドー・コピー



「以前のバージョン」からファイル
を復元可能

2. プリンタサーバ機能

プリンタドライバ自動配布機能

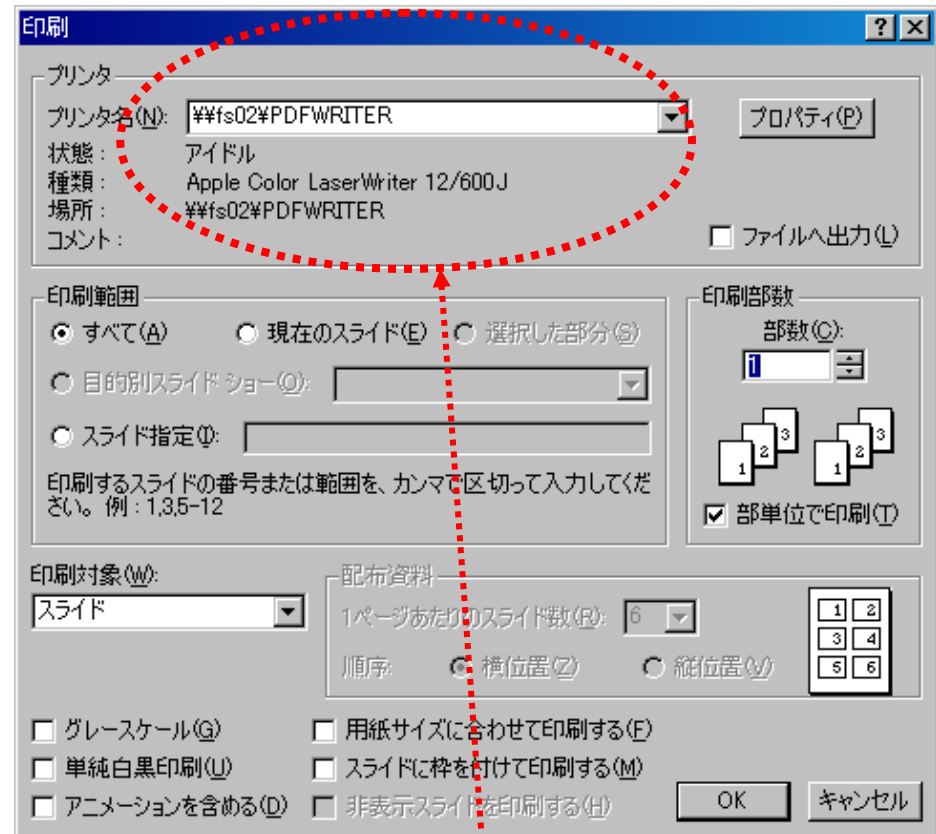
Windowsクライアント用のプリンタドライバをSamba側に予め配置しておき、自動的にダウンロード

PDFライター機能

Sambaが提供する共有プリンタに

印刷するとPDFが生成

GhostScriptのPS2PDFを使用しているため、ライセンス不要



PDFライターがプルダウンで選択できる

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 2000 / XP / Vista / 2003/ 2008に対応

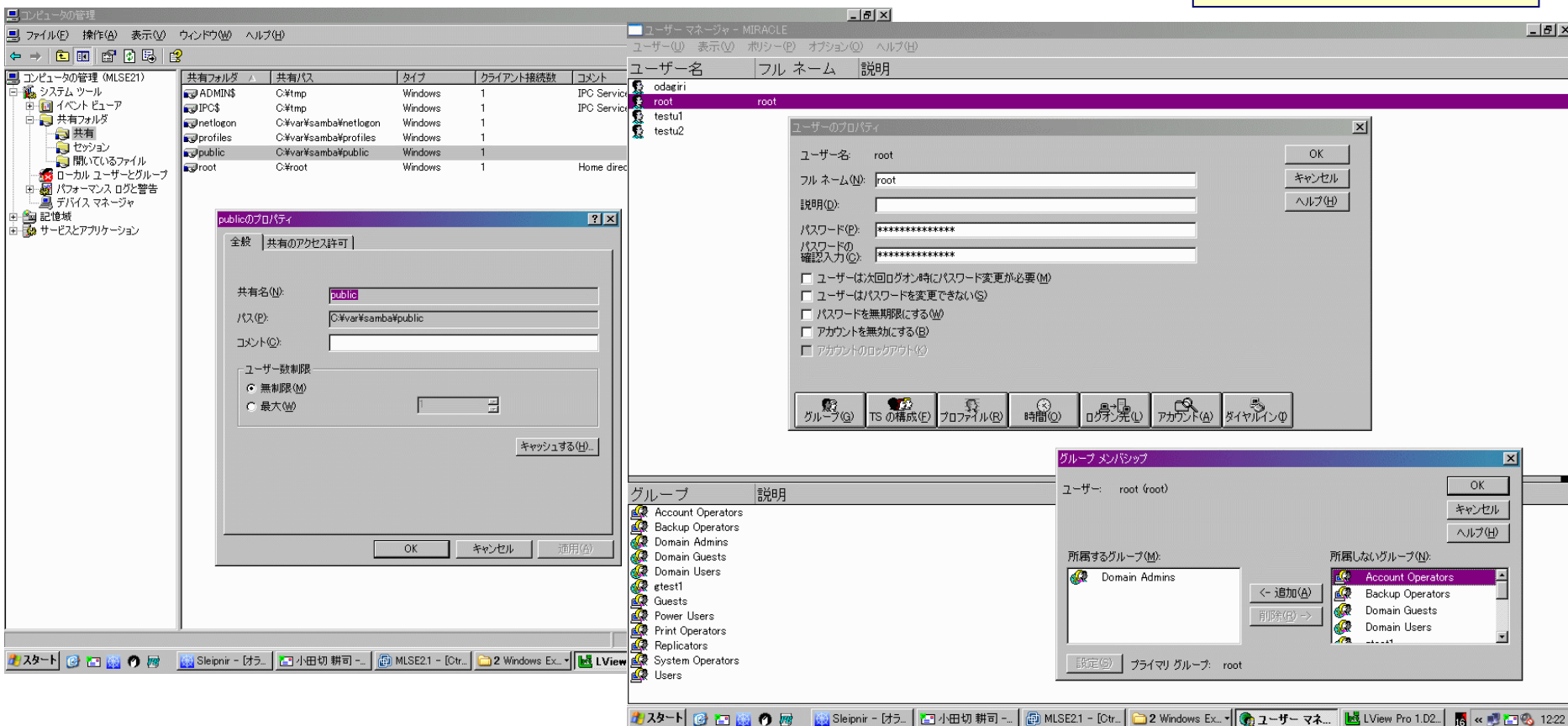


3. Windows GUIによるSamba管理画面

ユーザ管理、共有管理がWindows GUIで可能

共有管理機能

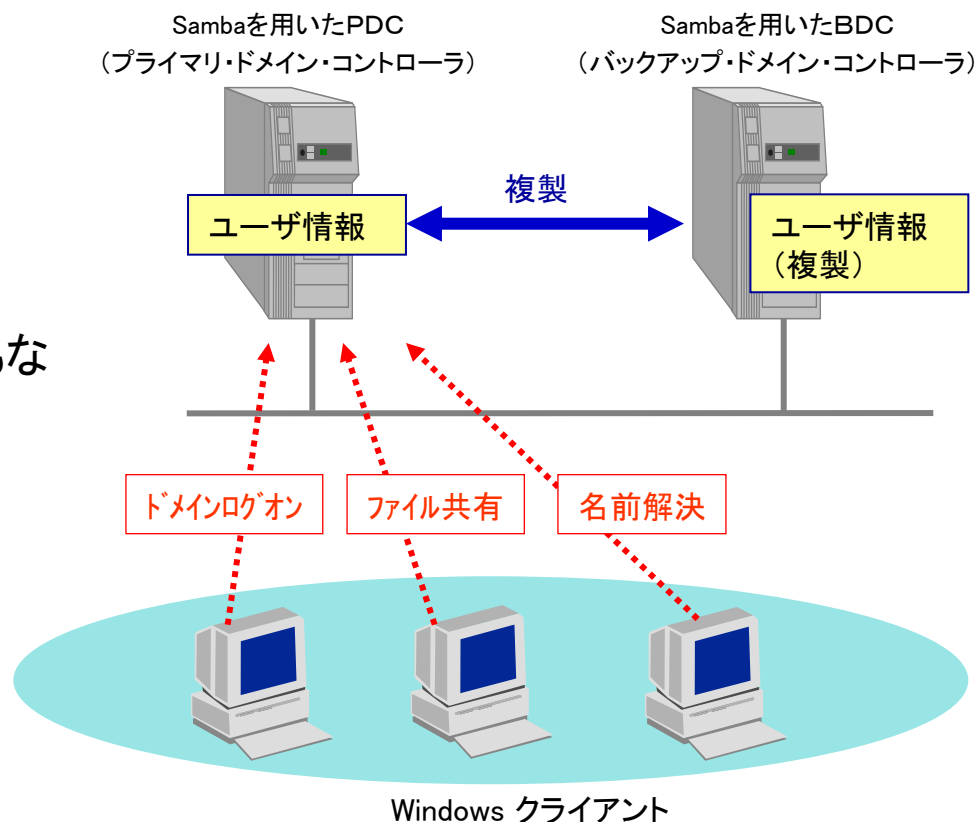
ユーザ管理機能



4. ドメイン・コントローラ機能とは？

ドメインコントローラ(DC)は、Windowsドメインを構築する際にユーザ情報などを管理するサーバのこと。

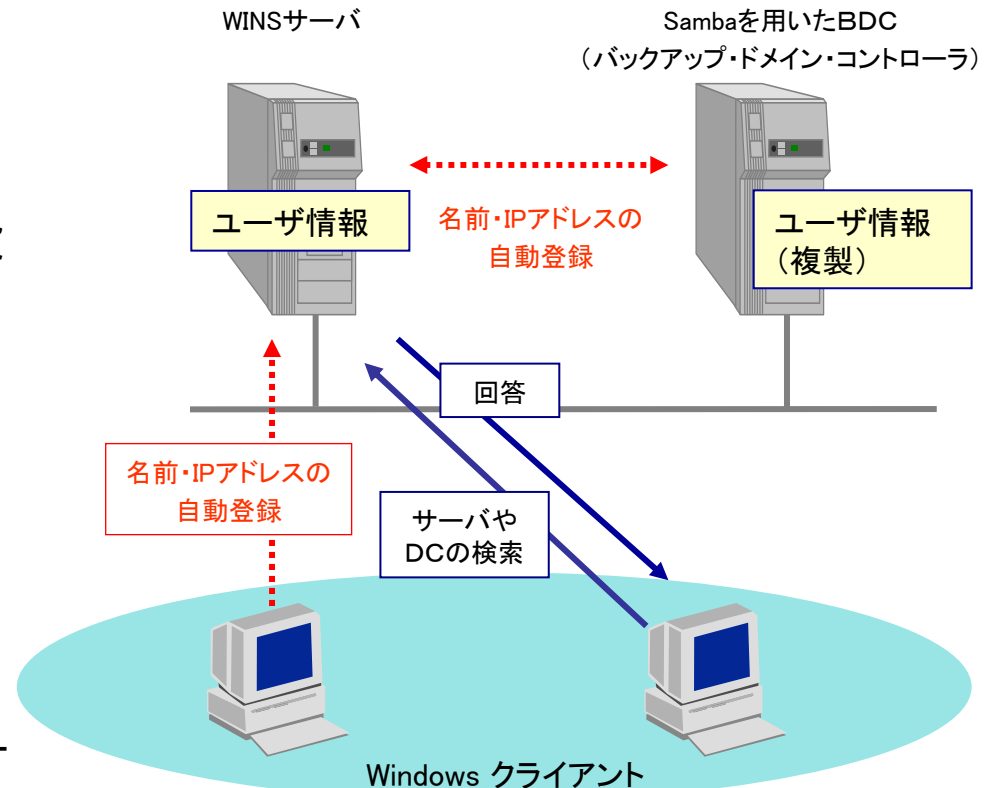
- PDC: ユーザ情報を格納・管理
- BDC: PDCで管理されているユーザ情報の複製を保持
※参照のみで、追加・変更は不可
- Sambaサーバは、PDCにもBDCにもなれるが、ユーザ情報複製には、ディレクトリ・サービスの「LDAP」が必要



5. WINSサーバ機能

Windowsネットワークで使われる「コンピュータ名」をIPアドレスに変換する機能

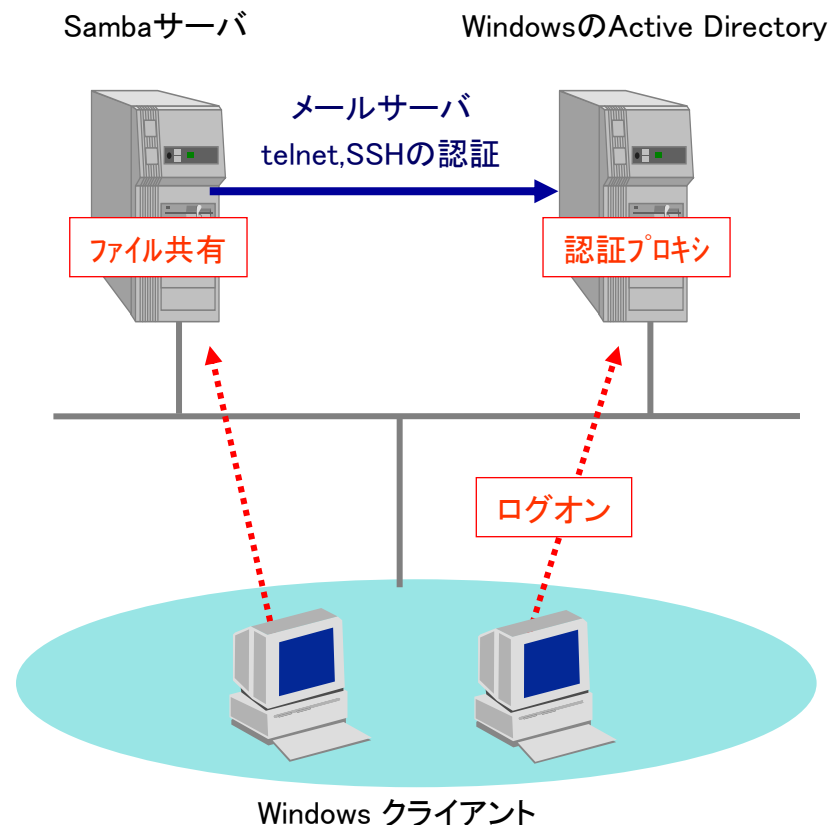
- Windowsのファイルサーバやドメインコントローラを探すためのネームサービス
- UNIXでいうDNSは管理者による手動設定だが、WINSはクライアント主導の自動設定で運用管理が楽である
- 複数ネットワークにまたがるWindowsドメインを構築するには必須のサーバ
- Samba標準ではWINSの複製機能を持っていない。OSSTechではアドオンモジュールで複製機能を提供している。



6. Winbind(認証プロキシ)機能とは？

Linux/UNIXのユーザ管理や認証をWindowsのディレクトリサービス「Active Directory」で統合管理する機能

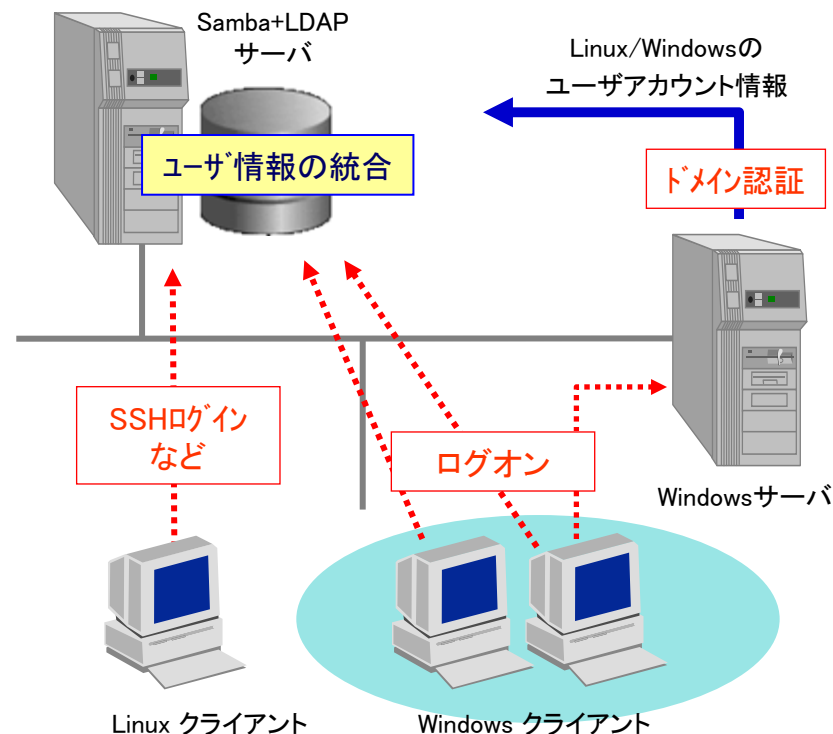
- Linux/UNIXの上でのアカウント管理をする必要がなくなる。
- Windowsのドメインコントローラにユーザやグループを追加すると、自動的にLinux/UNIXの上でも利用可能。
- ファイルサーバSambaのアクセスや認証だけでなく、POP, IMAP, TELNET, FTP, SSHなどNSS/PAMに対応したすべてのLinux/UNIX上のアプリケーションが利用できる。



7. LDAPサーバによる認証統合

LDAP (Lightweight Directory Access Protocol) は、ディレクトリにアクセスするためのプロトコルで、Sambaのドメイン構築やユーザ管理を安全に運用するために不可欠な機能

- ユーザ管理を LDAP サーバに集中し、Samba のドメイン管理機能と連携することで、Windows/Linux/UNIX のユーザ管理を統合できる。
- この機能を利用することで、Windows サーバで構築されているファイルサーバやドメインコントローラ機能を、Linux 上に構築された Sambaサーバへ移行することが可能。



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



DFSツリー: ¥¥WORLD¥¥MANAGER¥¥JINJI

実サーバ: ¥¥JINJI¥¥JINJI



DFSツリー: ¥¥WORLD¥¥MANAGER¥¥SALES

実サーバ: ¥¥SALES¥¥SALES



DFSツリー: ¥¥WORLD¥¥PLAN

実サーバ: ¥¥PLAN¥¥PLAN

8. Sambaのセキュリティ機能

ACL機能

Windowsと同等の共有やフォルダに対するアクセス制御

監査機能

誰がどのファイルにアクセスしたかログに保存

課金機能

誰がどの位サーバを利用していたか課金情報を保存

リアルタイムウィルスチェック機能

F-SecureやSophosアンチウィルス製品と連携

Hide UnReadable機能

参照権のないファイルを表示させない

Hide UnWritable機能

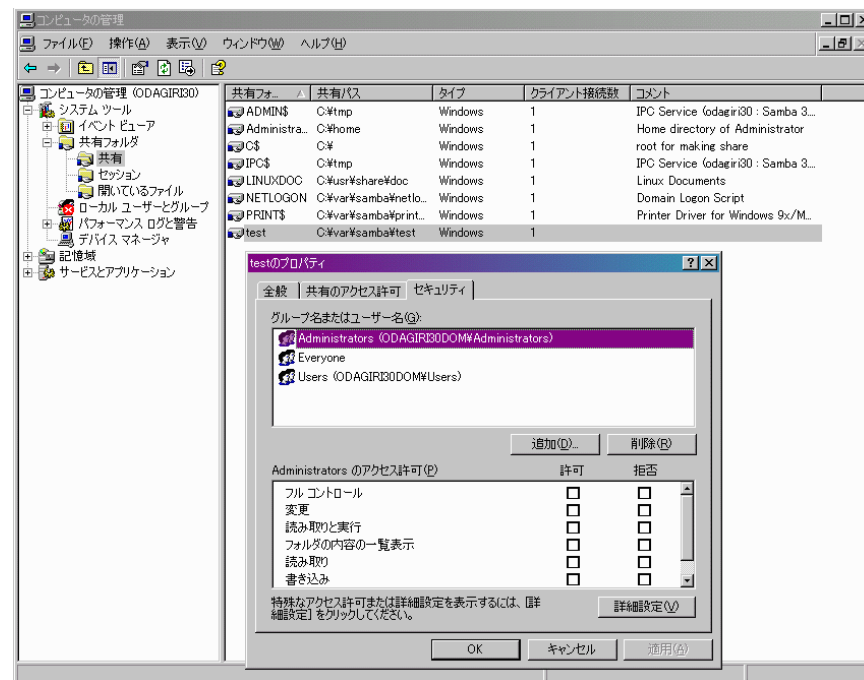
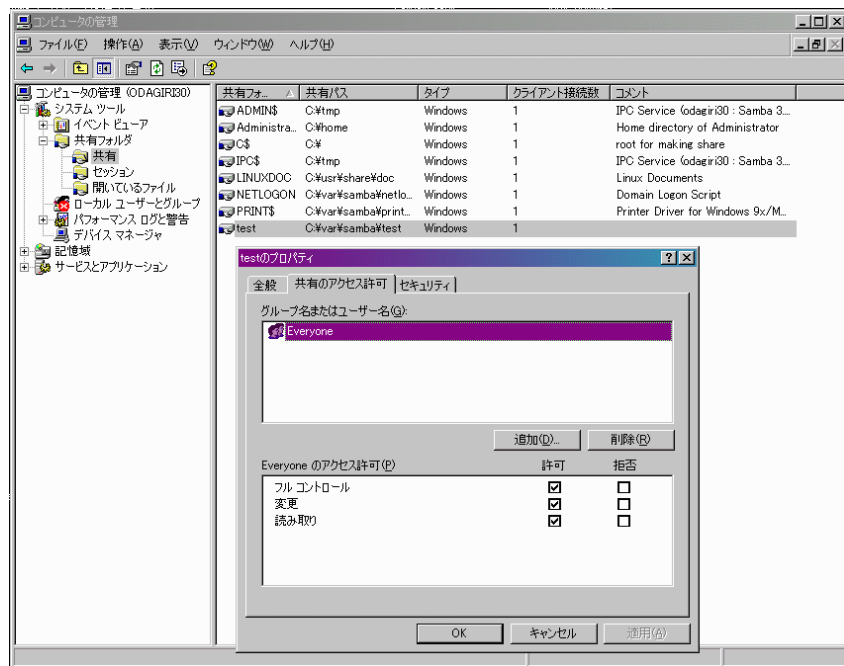
更新権のないファイルを表示させない

Hide Files機能

任意のファイルを表示させない

8. Sambaのセキュリティ機能: ACL機能

Windowsと同等の共有やフォルダに対するアクセス制御



8. Sambaのセキュリティ機能：監査機能

誰がどのファイルにアクセスしたかログに保存

共有単位で監査情報を出すか、出さないか設定

ログはすべてシスログに保存

UNIXのsyslogdに送信することも可能

出力例

```
Feb 24 17:26:30 dhcp-0144
smbd_abs_audit[1402]: open /usr/share/public/
新規テキスト ドキュメント.txt (fd 26)
[odagiri@10.1.0.115] for writing

Feb 24 17:26:40 dhcp-0144
smbd_abs_audit[1402]: close
/usr/share/public/新規テキスト ドキュメント.txt (fd
26) [odagiri@10.1.0.115]
```

8. Sambaのセキュリティ機能:課金機能

誰がどの位サーバを利用していたか課金情報を保存

(情報漏洩事故が起きたときに)ある時間に利用していたユーザを特定可能(utmp,wtmp機能、wコマンド、acコマンド)

出力例

odagiri	smb/2	10.1.0.152	Sat Oct 1 04:39 - 04:54	(00:15)
yasuma	smb/18	10.1.1.34	Sat Oct 1 17:01 - 17:40	(00:38)

Oct 31	total	368.67		
	odagiri		48.00	
	yasuma		24.00	
Nov 1	total	408.19		
	odagiri		1095.32	
	tonoki		1095.32	
Today	total	9310.18		

8. Sambaのセキュリティ機能： リアルタイムウィルスチェック機能

F-SecureやSophosアンチウィルス製品と連携

ファイルを共有にコピーした時点でリアルタイムにウィルスチェック
対応S/W

Clamd

Icap

Mks32

Sophos

Fprotd

Kavp

Oav

TrendMicro

8. Sambaのセキュリティ機能

Hide UnReadable機能

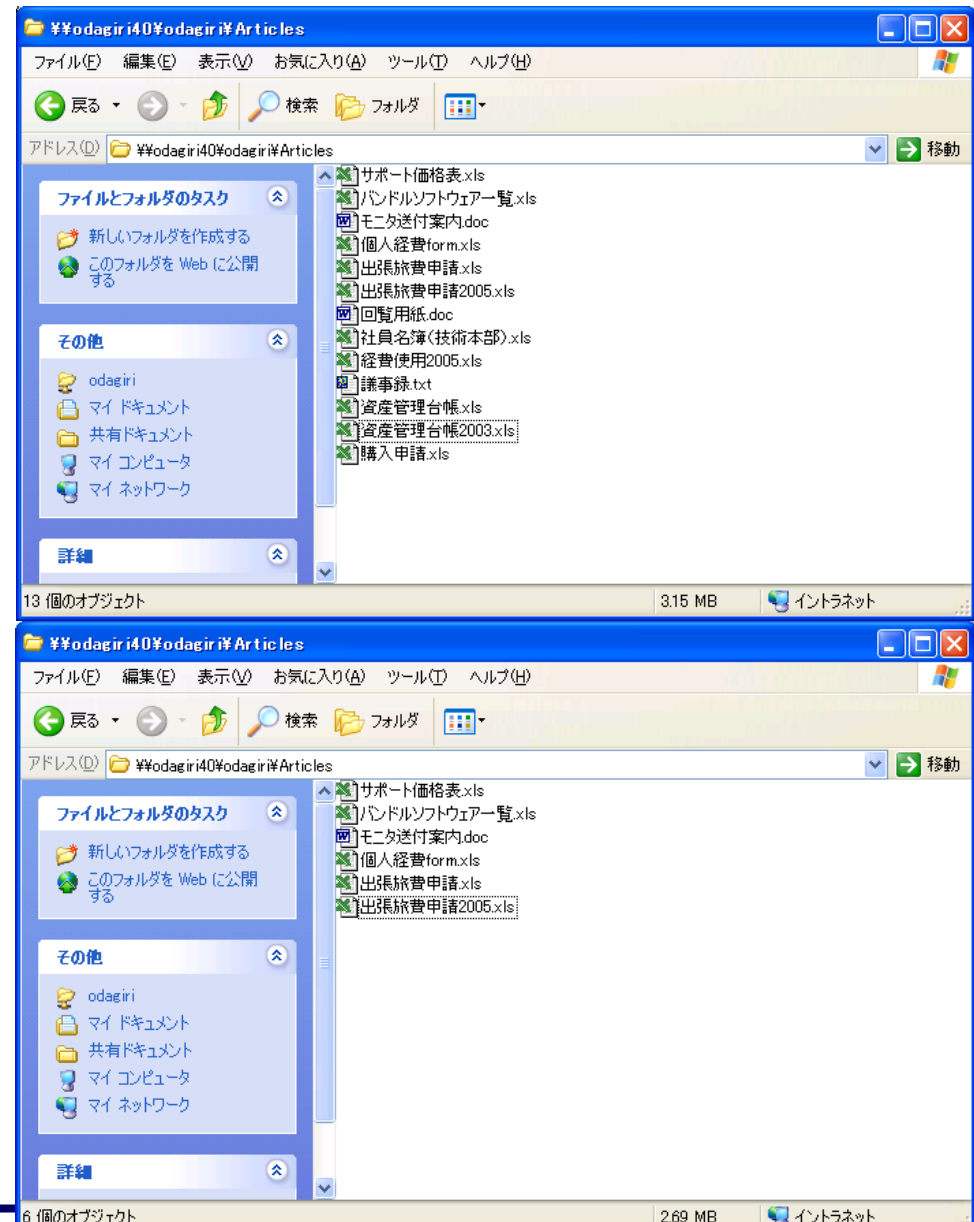
参照権のないファイルを表示させない

Hide UnWritable機能

更新権のないファイルを表示させない

Hide Files機能

任意のファイルを表示させない



Part 2.

Windows移行 Q & A



**Linux
Professional
Institute**



OSSTech

Windowsドメイン移行に関するQ&A

Q. SambaでWindowsNTドメインを移行できますか？

A. はい、できます。

- SambaにはWindowsのドメインコントローラになる機能があり、PDC(プライマリドメインコントローラ)にもBDC(バックアップドメインコントローラ)にもなれます。
- さらにSamba 3.0にはnet vampireコマンドがあり、WindowsNTドメインに登録された
- ユーザ情報、グループ情報、マシンアカウントを移行させることができます。

Q. 現在WindowsマシンをDNSサーバ、WINS (Windowsインターネットネームサービス)サーバ、DHCPサーバとして利用しています。これをSambaに移行することはできますか？

A. はい、できます。

SambaはWINSサーバになることができ、Linux OSが標準搭載している製品コンポーネントでDNSサーバ、DHCPサーバを構築することができます。

Windowsドメイン移行に関するQ&A

Q. SambaでWindows ADドメインを移行できますか？

A. できる場合とできない場合があります。

- Active Directoryが混在モード(2000のデフォルト)の場合、Sambaのnet vampireコマンドで移行できる(できないこともある)
- ldapsearchやnet userコマンドでユーザ情報、グループ情報を取り出し、これを加工することで移行することもできる。この場合、パスワードはPWDUMPツールを使うとNTハッシュ形式で取り出せる。(これはLDAPのuserPasswordにあたるsshaやmd5ではないので要注意)
- 上記の2方式のどちらかを使えばユーザ情報／グループ情報／マシンアカウントが移行できますが、クライアントマシンのドメイン再参加が必要
- グループポリシーは移行できないため、ADの完全置き換えはできません。
- Samba4からAD互換となり、完全移行ができる(予定)

Windowsドメイン移行に関するQ&A : サーバ管理

Q. 現在BDC(バックアップドメインコントローラ)として利用しているWindowsマシンをPDCをSambaに移行後もそのままBDCとして利用できますか？

A. いいえ、できません。

SambaをPDCとした時はBDCもSambaマシンでなくてはなりません。これはSambaがSAM(ユーザ管理情報)の複製をサポートしていないためです。

Q. WindowsマシンがPDCとなっているWindowsドメインにSambaをBDCとして設置できますか？

A. いいえ、できません。

WindowsをPDCとした時はBDCもWindowsマシンでなくてはなりません。これはSambaがSAM(ユーザ管理情報)の複製をサポートしていないためです。

Windowsドメイン移行に関するQ&A

Q. 現在のWindowsドメインは別なNT4ドメインと信頼関係を結んでいます。これも移行することはできますか？

A. はい、できます。

Samba 3.0はドメインの信頼関係をサポートしています。ただし、信頼関係は移行ツール(vampireコマンド)で移行後に手動で行うことを推奨します。

Q. 現在のWindowsドメインは別なADドメインと信頼関係を結んでいます。これも移行することはできますか？

A. はい、できます。

Samba 3.0はドメインの信頼関係をサポートしています。但し、明示的な片方向の信頼関係はサポートしていますが、ADの推移的な双方向の信頼関係はサポートしていないので、移行ツール(vampireコマンド)で移行後に信頼関係を手動で設定することを推奨します。

Windowsドメイン移行に関するQ&A

Q. 現在のWindowsドメインは別なNT3.51ドメインと信頼関係を結んでいます。これも移行することはできますか？

A. いいえ、できません。

NT3.51ドメインと信頼関係は現在正しく動作していません。

Q. WindowsマシンをセカンダリのWINSサーバとして利用しています。SambaマシンをプライマリのWINSサーバとした場合、このままWindowsマシンをWINSサーバとして利用できますか？

A. 利用は推奨しません。

WINSサーバを期待通りの動作で運用させるにはプライマリとセカンダリの間で定期的にPUSHまたはPULLの同期作業が必要ですが、SambaのWINSサーバはPUSHまたはPULLの同期を現在まだサポートしていません。そのためSambaマシンをプライマリのWINSサーバにした場合は、セカンダリのWINSサーバは静的マッピングによる手動メンテナンスを行って運用する必要があります。このような運用方法は推奨しません。

Windowsドメイン移行に関するQ&A

Q. NTドメイン移行後、Samba PDCマシンを旧NT PDCと同じマシン名、同じIPアドレスで運用しようと思いますが、大丈夫ですか？

A. はい、問題ありません。

但し、UNIX系OSでも使えるコンピュータ名に限られます。

Q. SambaでWindowsNTドメインを移行した時、ユーザのパスワードも移行できますか？

NTドメインの時のパスワードがそのまま使えますか？

A. はい、そのまま使えます。

Q. SambaでWindowsNTドメインを移行した時、システムポリシーは移行できますか？

A. はい、できます。

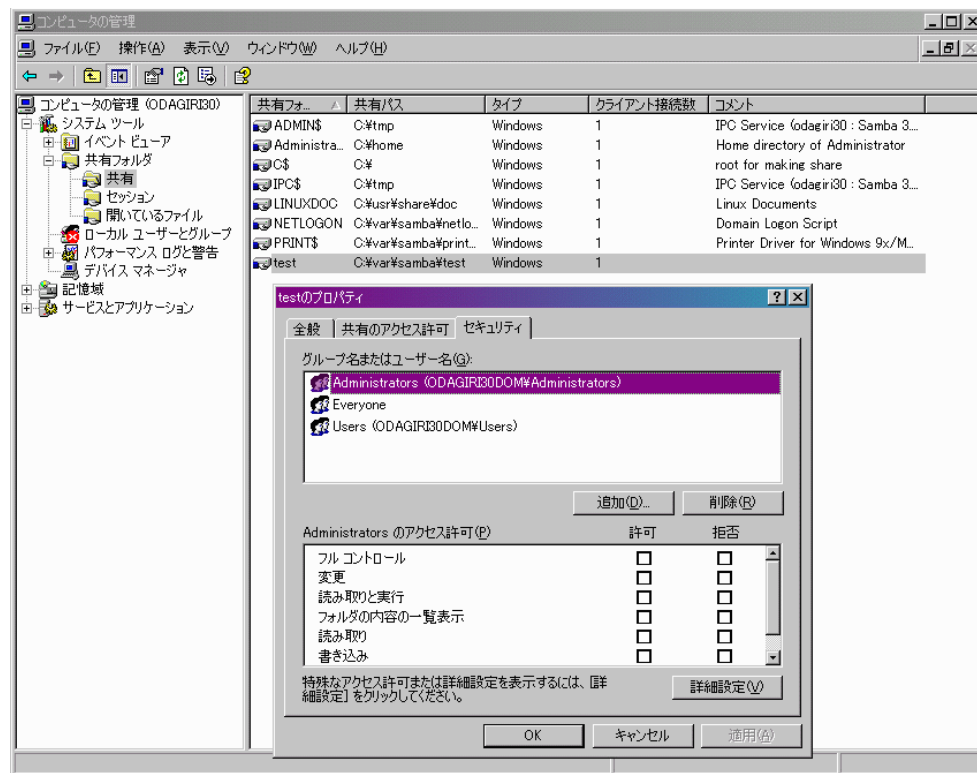
NTのNETLOGONディレクトリにあるNTCONFIG.POLファイルをコピーするだけでそのまま使えます。

Windowsドメイン移行に関するQ&A

**Q. Sambaでの共有管理は
難しいですか？**

A. GUIで管理できます。

Samba 3.0ではWindowsからGUIで共有の管理ができるようになって
います。
最新のLinuxではACLが利用できるので
アクセス制御もGUIで簡単にできます。



ACL設定画面

Windowsドメイン移行に関するQ&A

Q. SambaでWindowsNTドメインを移行した時、アカウントポリシーは移行できますか？

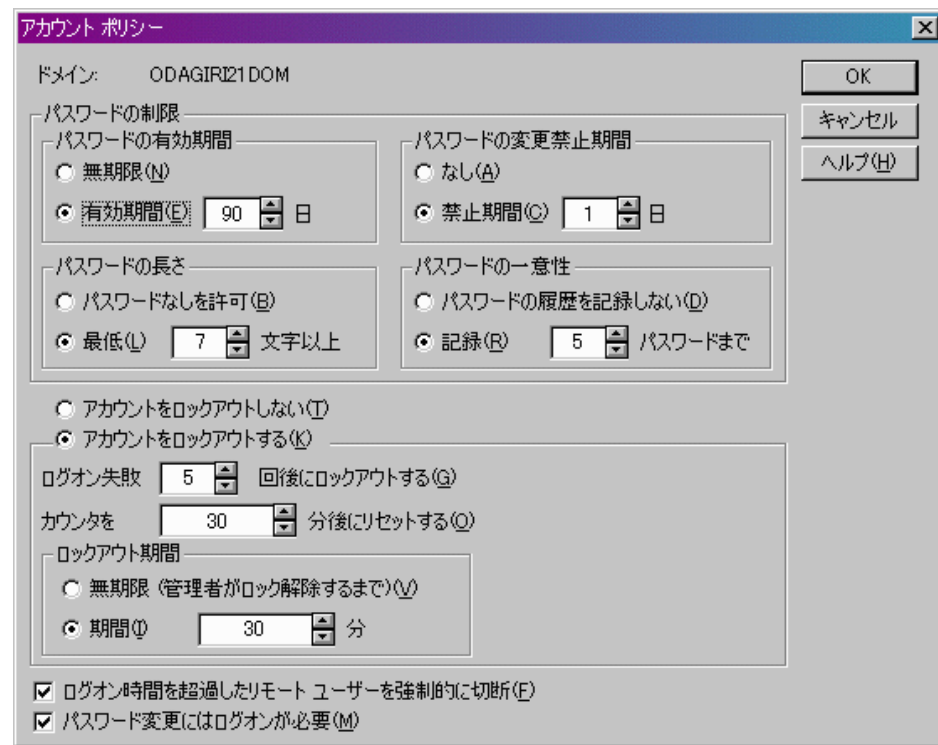
A. いいえ、できません。

Samba3.0でアカウントポリシーは利用できませんが、vampireコマンドで移行はできません。ユーザマネージャを使って手動で設定ください。

Q. Sambaのアカウントポリシーの設定で「パスワード履歴」の機能は使えますか？

A. はい、使えます。

Samba 3.0.7以降で利用できるようになっています。



ユーザマネージャ設定画面

Windowsドメイン移行に関するQ&A

Q. 移動プロファイルは移行できますか？

A. はい、移行できます。

NTの移動プロファイルをSambaのプロファイル共有にコピーすることで移行できます。
この時、Sambaの設定ファイル(smb.conf)のプロファイル共有のセクションに
profile acls = yesと指定しておいてください。

Q. ローカルプロファイルは継続して利用できますか？

A. はい、利用できます。

Sambaに移行した場合もユーザSIDはSamba PDCに引き継がれますので、
スタートメニューやデスクトップもそのまま継続利用できます。

Q. 移行作業中に既存ドメインは利用できますか？

A. いいえ、利用できません。

ユーザがパスワード変更などをすると完全な移行がうまくいきません。
また、ユーザがパスワード変更しなくて、マシンパスワードはユーザの気がつかない
ところで更新されるため、移行作業はネットワークから切り離して行うことが推奨され
ます。

Windowsドメイン移行に関するQ&A

Q. ADのグループポリシーは移行できますか？

A. いいえ、できません。

現在のSamba3はADと非互換のためグループポリシーは移行できません。
(利用もできません)

Samba4からAD互換となります。

表 1. SambaとWindows Server 2003との比較

機能	Samba 2.2	Samba 3.0	Windows Server 2003
リソース管理			
ユーザー情報の格納場所	LDAP、簡易DB、テキスト、NISなどが利用可能	LDAP、簡易DB、テキスト、NIS、MySQLなどが利用可能	Active Directory または内部の簡易DB
ユーザー情報の複製機能	△LDAPの複製機能を利用	△LDAPの複製機能を利用	○
日本語ユーザー名	△username map機能を使えば可能	△username map機能を使えば可能	○
日本語グループ名	×	△groupmap機能を使えば可能	○
グローバルユーザー/ローカルユーザー	×	○	
グローバルグループ/ローカルグループ	×	○	○
ネストグループ (ローカルグループの中にグローバルグループを入れ子にするような階層化)	×	○	○
日本語コンピュータ名	△username map機能を使えば可能	△username map機能を使えば可能	○
通信プロトコル			
LANMAN認証	○	○	○
NTLM認証	○	○	○
NTLMv2認証	×	○	○
Kerberos5認証	×	△メンバサーバの時のみ可能	○
セキュアチャネル	×	○	○
SMB署名	×	○	○
SPNEGO (RFC2478で規定されたSimple and Protected NEGociation)	×	○	○
ドメイン管理			
ドメインログオン	○	○	○
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)	○	○	○
ログオンスクリプト	◎ログオンスクリプトの動的生成/変更可能	◎ログオンスクリプトの動的生成/変更可能	○固定スクリプトを実行可能
移動プロファイル	○	◎読み込み専用プロファイルもサポート	○
NT 4.0相当のユーザーポリシー (NT 4.0/2000/XP)	○	○	×
Windows 98相当のグループポリシー (95/98/Me)	○	○	×
Windows 2000/2003相当のグループポリシー	×	×Samba4で対応予定	○
複雑なパスワードの強制	×	○外部モジュールを使って可能	○
パスワード履歴	×	○	○
明示的な片方向の信頼関係	×	○	○
推移的な双方向の信頼関係	×	×Samba4で対応予定	○
ファイル/プリントサーバ機能			
ユーザー/グループによる容量制限	◎ディレクトリ単位にも対処可能	◎ディレクトリ単位にも対処可能	○
論理ボリュームマネージャ	○Linux OSに依存	○Linux OSに依存	○
ボリュームシャドーコピー (スナップショット) 機能	×	○ただし、Linux側でXFSもしくはLVM2を搭載している必要あり	○NTFS必須
ゴミ箱機能	○	○	×
マッキントッシュ連携	○Netatalkをインストールすることで可能	○Netatalkをインストールすることで可能	○マッキントッシュサービスをインストールすることで可能
UNIX NFS連携	○カーネルレベルによるOPLOCK連携可能	○カーネルレベルによるOPLOCK連携可能	○Service for UNIXをインストールすることで可能
ユーザーホーム機能	○	○	×
MS-DFS (ルートおよびサブディレクトリ)	○	○	○
MS-DFS Proxy	×	○	○
ACL機能 (ユーザー/グループによるアクセス制御)	○Linux OSに依存	○Linux OSに依存 NTFS互換はSamba3.2とNFSv4 ACLの組み合わせで利用可能	○NTFS必須
ホスト名によるアクセス制御	○	○	×
日本語ディレクトリ/ファイル名	○	○	○
READ権のないファイルを見えなくする	○	○	×
WRITE権のないファイルを見えなくする	×	○	×
ユーザーモジュールによる共有機能の拡張・カスタマイズ	○標準で監査機能、ウイルスチェックなどを搭載。1つの共有に1つのモジュールだけ	○標準で監査機能、ウイルスチェックなどを搭載。1つの共有に複数のモジュールをロード可能	○WINAPIでユーザーが作成可能
同一サーバに複数のNetBIOS名を付ける	○smb.confで容易に指定可能	○smb.confで容易に指定可能	△レジストリ変更が必要でサポート対象外
スプールしながらの印刷	×	×	○
PDFライター機能	○GhostScriptとの連携	○GhostScriptとの連携	×
プリンタドライバ配布機能	○	○	○
WINS機能			
WINSサーバ	○	○	○
WINSクライアント	○	○	○
WINS複製	×	△外部スクリプトによりPushは可能	○
WINS静的マッピング	○ wins.datの直接編集	○ wins.datの直接編集	○
WINSとDNSとの連携	○ wins hook機能	○ wins hook機能	×
ブラウジング			
ドメインマスタブラウザ	◎ワークグループ構成でも可能	◎ワークグループ構成でも可能	○
リモートアナウンス	◎任意のワークグループ、ドメインにも可	◎任意のワークグループ、ドメインにも可	○信頼するドメインのみ
ポテンシャルブラウザ	○	○	○

Part 3.

Sambaのインストールと設定



**Linux
Professional
Institute**



OSSTech

Sambaのインストール

- **LPIC試験勉強のためにはconfigure ; make installでのインストールを必ずやっておくこと。**
- **実運用システムではmake installはやらないこと！**
- Linuxディストリビューションに依存したコマンドでインストールするのが一般的なやり方
 - RedHat系
 - yum install samba*
 - rpm -i samba*.rpm
 - Debian系
 - apt-get install samba
 - dpkg -i samba*.deb

RHEL5/Fedora10でのSamba configureオプション

```
./configure --prefix=/usr --exec-prefix=/usr --bindir=/usr/bin
--sbindir=/usr/sbin --sysconfdir=/etc --datadir=/usr/share
--includedir=/usr/include --libdir=/usr/lib --libexecdir=/usr/libexec
--localstatedir=/var --sharedstatedir=/usr/com
--mandir=/usr/share/man --infodir=/usr/share/info
--with-acl-support --with-ads --with-automount --with-dnsupdate
--with-libsmbclient --with-mmap --with-pam --with-pam_smbpass
--with-quotas --with-sendfile-support --with-syslog --with-utmp
--with-vfs --with-winbind --without-smbwrapper --with-lockdir=/var/cache/samba
--with-piddir=/var/run --with-mandir=/usr/share/man --with-privatedir=/etc/samba
--with-logfilebase=/var/log/samba --with-libdir=/usr/lib/samba
--with-configdir=/etc/samba --with-pammodulesdir=lib/security
--with-swatdir=/usr/share/swat --with-shared-modules=idmap_ad,idmap_rid

--with-cifsupcall

# --with-cluster-support ¥
# --with-aio-support ¥
```

configureオプション

<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>	No	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>--with-cups</code>	自動	<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-ads</code>	自動	<u>Active Directoryクライアント機能のサポートを有効にします</u>
<code>--with-libsmbclient</code>	Yes	クライアントライブラリである、libsmbclientを有効にします
<code>--with-winbind</code>	自動	Winbindを構築する

Sambaの設定

- 設定ファイル
 - (/etc/samba/)smb.conf
- Sambaとしては上記だけだが利用する機能によっていろいろなファイルを設定する必要がある。
 - LDAPと連携する場合
 - LDAPやnss,pamの設定
 - smbldap.confなど(smbldap-tools関係)
 - ADと連携する場合
 - DNS, NTP, KRB5の設定、
 - nssやpamの設定

smb.conf の設定

- [global]セクションと[共有]セクション
 - [global]セクションにはSamba全体の設定を指定
マニュアルに(G)と書いてあるパラメータが指定可能
 - [共有]セクションには共有の設定を指定
マニュアルに(S)と書いてあるパラメータ
 - マニュアルに(S)と書いてあるパラメータを[global]セクションに指定するとすべての共有セクションに指定したことになる。(G)となっているものを共有セクションには記述できない
- 特殊な予約済み共有
 - [homes] セクション
ユーザホーム共有。共有名が自動的にユーザ名に変換される。
 - [printers]セクション
プリンタスプールのための設定。プリンタ名に変換される。
 - [NETLOGON]セクション
ログオンスクリプトのための共有
 - [PRINT\$]セクション
プリンタードライバーを自動ダウンロードさせるための共有
 - [IPC\$]セクション
認証や管理のための共有

smb.conf 内で利用できる置換変数(マクロ)

- %U: セッションのユーザ名 (クライアントが接続時に 送信したものであるが、実際に接続したユーザ名と同じであるとは 限らない)。
- %G: %U のプライマリグループ。
- %h: Samba が動作しているマシンの インターネットホスト名。
- %m: クライアントマシンの NetBIOS 名 (ポート139が必要、445のみでは利用不可)
- %L: サーバの NetBIOS 名。
- %M: クライアントマシンのインターネットホスト(DNS)名。
- %R: プロトコルのネゴシエーションを経て選択された プロトコルレベル。これは CORE、COREPLUS、LANMAN1、LANMAN2、NT1 のいずれかの値をとる。
- %d: サーバプロセスのプロセス ID。
- %a: リモートマシンのアーキテクチャ。現在認識できるのは Samba (Samba)、Linux の CIFS ファイルシステム (CIFSFS)、OS/2 (OS2)、Windows for Workgroups (WfWg)、Windows 9x/Me (Win95)、Windows NT (WinNT)、Windows 2000 (Win2K)、Windows XP (WinXP)、Windows XP 64-bit(WinXP64)、2003R2 (Win2K3)を含むWindows Server 2003 (Win2K3)と、Windows Vista (Vista) である。それ以外のものは“UNKNOWN”となる。
- %I: クライアントマシンの IP アドレス。
- %i: クライアントが接続してきたサーバの IP アドレス。
- %T: 現在の日付と時間。
- %D: 現ユーザが所属するドメインかワークグループ名。
- %w: Winbind のセパレータ
- %\$(envvar): 環境変数envvarの値。
- %S: 現在のサービス名 (存在する場合)。
- %P: 現在のサービスのトップディレクトリ (存在する場合)。
- %u: 現在のサービスのユーザ名 (存在する場合)。
- %g: %u のプライマリグループ。
- %H: %u で指定されたユーザのホームディレクトリ。
- %N: NIS のホームディレクトリサーバの名前。これは NIS の auto.map エントリから取得される。Samba が --with-automount オプションをつけて コンパイルされていない場合、このオプションは %L と同じになる。
- %p: NIS auto.map エントリから取得された サーバの ホームディレクトリのパス。NIS auto.map エントリは %N:%p のように分割されている。

[global]セクションのパラメータ:security

- **security = user (ユーザ認証モード)**
 - 共有(ファイル/プリンタ)を個別のユーザを使ってアクセスする。
 - Linuxアカウントが必要なので、新規ユーザのためには新しくアカウントを作成する必要がある。
 - SambaだけでWindowsドメインやWindowsワークグループを作成する場合に適しているが、パスワードはLinux用とは別にSamba専用のものを別に管理する必要がある。これがデフォルトの値である。
 - Windowsユーザの認証はSambaによってNTLM/NTLMv2認証となる。
- **security = ads (ADドメイン認証モード)**
 - ユーザ管理/認証はWindows ADドメインにしてもらうため、Sambaでユーザ管理やパスワード管理は不要である。
 - すでに、Windows ADドメインが構築されていて、そこにSambaマシンを追加する場合に適している。
 - winbindデーモンを起動し、NSS,PAMにwinbindを使用すること。
 - Windowsユーザの認証はADによってKerberos認証となる。

[global]セクションのパラメータ:security

- security = domain (NTドメイン認証モード)
 - ユーザ管理／認証は既存のSamba/WindowsNTドメインにしてもらうため、該当Sambaでユーザ管理やパスワード管理は不要である。
 - すでに、Samba/NTドメインが構築されていて、そこにSambaマシンを追加する場合に適している。
 - winbindデーモンを起動し、NSS,PAMにwinbindを使用すること。
 - Windowsユーザの認証はSamba/NTによってNTLM/NTLMv2認証となる。
- security = share (共有認証モード)
 - 共有(ファイル／プリンタ)を決まった固定ユーザを使ってアクセスする。(認証ユーザを共有する)
 - パスワードだけで、アクセス制御できるため、新規ユーザのために新しくアカウントを作成する必要がない。
 - 小規模な部門サーバやSOHO用に適しているが、不特定多数が使用する(個別にアカウントが作成できない)場合にも対応できる。
- security = server (サーバ認証モード)
 - 共有(ファイル／プリンタ)を個別のユーザを使ってアクセスする。
 - 必ずUNIXアカウントが必要なので、新規ユーザのためには新しくアカウントを作成する必要がある。
 - しかし、ユーザ認証は他のWindowsサーバやSambaサーバにしてもらうため、Samba専用のパスワード管理は不要である。
 - すでに、SambaやWindowsによるWindowsワークグループが構築されていて、そこにSambaマシンを追加する場合に適している。
 - Windowsユーザの認証はSamba/NTによってNTLM/NTLMv2認証となる。

[global]セクションのパラメータ:charset

- 文字コードの設定
 - **unix charsetが重要**
 - サーバ側に格納するときの文字コードを決める
 - UTF-8 , EUCJP-MS , CP932 , UTF-8-Macなど
 - Vista/2008/MacOSでJIS X 0213(JIS 2004)を使うにはUTF-8必須
 - OSでサポートされていない文字コードは利用しない方が良い
 - dos charsetはcp932固定
 - NT系2000以降はUNICODEなので必須ではない
 - display charsetはSWATの画面に表示される文字コードを指定
 - unix charsetと同じで良い (localeに合わせるのがデフォルト)

```
[global]
unix charset      = UTF-8
display charset  = UTF-8
dos charset       = CP932
```

[global]セクションのパラメータ:passwd backend

- 「security=user」(デフォルト)の場合にユーザ／パスワード情報の格納先を指定
- ドメインコントローラ(PDC,BDC)や大規模の場合は、LDAPSAMを使用
- ワークグループ／小規模の時のみTDBSAMを利用
(security=adsの時もTDBSAMが良い)
- smbpasswdは移行時のみ

```
[global]
passwd backend = ldapsam:ldap://ldp1.osstech.co.jp
```

Active Directoryのメンバ参加機能

- Windows 2000/2003/2008と同じKerberos認証をサポート
 - クライアント機能のみ。DCになれる訳ではない
 - ADのDCはDNSで検索する(SRVレコード必須)ので resolv.confの設定を忘れずに
 - password server の指定は必須ではない
 - NTPやkrb5の設定も必要

```
[global]
security = ADS
realm = <ADのドメイン名(大文字)>
```

[global]セクションのパラメータ:その他

- workgroup
 - Sambaの所属する(あるいはクライアントへ応答する)Windowsワークグループ名/Windowsドメイン名を指定する。
- server string
 - 「ネットワークコンピューター一覧」で詳細表示した時、「サーバの説明」と「プリンタの説明」に表示する文字列を指定する。
文字列の中の%v は Samba バージョン番号と置換され、%h は ホスト名に置換される。
 - 既定値: server string = Samba %v
例: server string = Samba %v on %h Linux
- map to guest
 - UNIXにユーザアカウントがない場合、guest接続を許すかどうか指定する。設定は下記の3種類がある。
 - Never
guest接続を許さない。既定値。
 - Bad User
ユーザ名が無かった場合、ゲストログインとして扱い、"guest account" で接続する。
 - Bad Password
不正なパスワードの場合、ゲストログインとして扱い、“guest account” で接続する。
これは、任意のユーザがパスワードをタイプミスしたり、暗号化パスワードを設定し忘れていても、なにも言われずに "guest" としてログインしてしまうことに注意。
- socket options
TCPネットワークに詳しくない方は設定しないこと

共有セクション用のパラメータだが[global]セクションに設定すると良いパラメータ

- **store dos attributes = yes**
 - DOSの隠し属性やシステム属性を保持する
 - map hidden, map system, map archive をyesにする代わりにこれをyesにする。
 - ドメインログオンするとメモ帳が起動してしまう、というようなトラブルを防止する
- ea support = yes
 - 上記の**store dos attributes = yes** とするための設定
- dos filetime resolution = yes
 - ファイルのタイムスタンプの解像度をDOSと同じ2秒単位に合わせる
- dos filemode = yes
 - ファイルの更新権があればACLを変更できるようにする。

共有セクション用パラメータ

- **writable / read only**
 - 共有を更新可能とする不可とするか
 - 「*writable = yes*」と「*read only = no*」は同じ意味
- path
 - 共有のサーバ上のパス
- create mask
- directory mask
- force create mode
- force directory mode
 - create mask とforce create mode はファイルのアクセス権を制御
 - directory mask とforce directory mode はディレクトリのアクセス権を制御
 - create mask とdirectory mask はファイル／ディレクトリへのアクセス権を制限(禁止)する時に利用する。(chmod ug-rwなどと同等)
 - force create modeとforce directory modeはファイル／ディレクトリへのアクセス権を許可する時に利用する。(chmod ug+rwなどと同等)
- guest only
 - guest ok = yes の時、全てのファイル操作は guest によって実行されたことになる。
- guest ok
 - 接続するときにパスワードが不要になり、guestでアクセス可能となる。

例1) 誰でもアクセス可能な共有の設定

- Linuxにアカウントがあっても、なくても誰でもアクセス(更新・参照)できる。
- /home/kikaku の属性を 777(rwxrwxrwx)とする。(chmod 777 /home/kikaku)
- ファイルの所有者はGuest(Nobody)となる
- **Samba動作確認用のもっとも簡易な設定**

```
[global]
    unix charset      = UTF-8
    map to guest      = bad user

[PUBLIC]
    path = /home/kikaku
    read only = No
    guest only = Yes
    guest ok = Ye
```

例2) UNIXにアカウントを持つユーザは誰でもアクセス可能な共有の設定

- /home/kikaku の属性を 755(rwxr-xr-x)とし、ディレクトリの所有者をkikakuというLinuxユーザとする。Linuxにアカウントとパスワードの設定のあるものは、この共有に誰でもアクセス(更新・参照)できる。しかし、Linuxにアカウントのないものはアクセスできない。

```
[global]
    unix charset      = UTF-8

[企画]
comment = 企画の共有フォルダ
path = /home/kikaku
read only = No
force user = kikaku      # 全員が、kikakuというUNIXユーザでアクセス
```

例3) 決まったユーザ(グループ)だけが、アクセス可能な共有の設定

- /home/kikaku の属性を 775(rwxrwxr-x)とし、同一のUNIXグループだけが更新でき、他のUNIXグループは参照が可能な共有を作成する。(valid usersとinvalid usersで、更にグループ内のユーザを制限可能)
UNIXにアカウントとパスワードの設定のないものはアクセスできない。

```
[global]
  unix charset = UTF-8
  workgroup = OSSTECH
  passdb backend = tdbsam
  store dos attributes = yes
  ea support = yes
  dos filetime resolution = yes
  dos filemode = yes
[企画]
  comment = 企画の共有フォルダ
  path = /home/kikaku
  read only = No
  valid users = @kikaku
  create mask = 0664
  directory mask = 0775
  force create mode = 0664
  force directory mode = 0775
```

Part 4.

Sambaサーバ運用と管理コマンド



**Linux
Professional
Institute**



OSSTech

Sambaの運用コマンド

- `pdbedit`コマンド
 - ユーザ／パスワード情報の管理
 - LDAP, TDB, `smbpasswd`ファイルなどを透過的に編集、表示
- `net`コマンド
 - ユーザとグループの管理
 - `smb.conf`に *add user script* などの設定が必要
 - ドメインのSID管理
 - Windows AD/NTドメインへの参加
 - リモートからWindowsドメインも管理可能
- `smbpasswd`コマンド
 - かつてはユーザ管理コマンドだったが、今は一般ユーザが自分のパスワードを変更するために利用
 - リモートのWindowsパスワードの変更も可能
 - 例外) `smbpasswd -w <LDAPの管理者パスワード>`

Sambaの運用コマンド

- **smbstatus**コマンド
 - Sambaに接続しているユーザ表示
 - ユーザがオープンしているファイルを表示
- **smbclient**コマンド
 - LinuxからSambaやWindows共有へアクセスするコマンド
- **testparm**コマンド
 - smb.confのチェックコマンド
 - スペルミスなどや設定ミスを見つけるために利用
- **nmblookup**コマンド
 - NBT(NetBIOS over TCP/IP)を使ったNetBIOS名の表示／検索
 - Windowsのnbtstat 相当
- **mount.cifs**コマンド
 - Samba/Windows共有をLinuxのファイルシステムとしてmountする
 - 従来のmount.smbfsはサポートされなくなっていく
 - mount.smbfs と違いDFSリンクをたどれる

ユーザーの管理

- `pdbedit`コマンドを使ったユーザー追加
 - `useradd odagiri`
 - `pdbedit -a odagiri`
- `net user`コマンドを使ったユーザー追加
 - `net rpc user add odagiri`
 - 予め`smb.conf`に
add user script = /usr/sbin/useradd %u
と設定しておく

グループの管理

- net groupmapコマンドを使ったグループ追加
 - groupadd sales
 - net groupmap add unixgroup=sales ¥
type=domain ntgroup=sales
- net userコマンドを使ったユーザー追加
 - net rpc group add sales
 - 予めsmb.confに
add group script = /usr/sbin/groupadd %g
と設定しておく

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	to list domains
		file	to list open files on a server
		group	to list user groups
		groupmember	to list users in a group
		password	to change the password of a user
		printq	to list the print queues on a server
		server	to list servers in a domain
		session	to list clients with open sessions to a server
		share	to list shares exported by a server
		user	to list users
		validate	to check whether a user and the corresponding password are valid

netコマンド(2)

	コマンド	サブコマンド	説明
net	rpc	join	to join a domain
		user	to add, delete and list users
		changetrustpw	to change the trust account password
		abortshutdown	to abort the shutdown of a remote server
		shutdown	to shutdown a remote server
	ads	join <org_unit>	joins the local machine to a ADS realm
		leave	removes the local machine from a ADS realm
		testjoin	tests that an exiting join is OK
		user	list, add, or delete users in the realm
		group	list, add, or delete groups in the realm
		info	shows some info on the server
		status	dump the machine account details to stdout
		password ...	change a user's password using an admin account(note: use realm in UPPERCASE)
		chostpass	change the trust account password of this machine in the AD tree
		printer [info publish remove] ...	lookup, add, or remove directory entry for a printer
search	perform a raw LDAP search and dump the results		

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 -Lv
username:          odagiri
user ID/Group:    1008/1008
user RID/GRID:    3416/3417
Full Name:        ODAGIRI Koji
Home Directory:   ¥¥FS01¥odagiri
HomeDir Drive:
Logon Script:
Profile Path:     ¥¥FS01¥profiles¥odagiri
```

ヘルプ画面

ユーザ情報の詳細表示

Part 5.

やっではいけないSambaサーバ構築



**Linux
Professional
Institute**



OSSTech

Webの情報を鵜呑みにしないこと！

- ブログに星の数ほどの設定記録があるが、玉石混合
- まともな内容は実はほとんどない
- 特に掲示板ベースのQ&Aは間違いだらけ
- 1年以上前の情報は役に立たない
- Samba2.x系の情報はSamba3系に当てはまらないことが多い。Samba 3系も互換性の問題あり
- 心配ならSamba-JPメーリングリストに聞きましょう

やってはいけないSambaサーバ構築

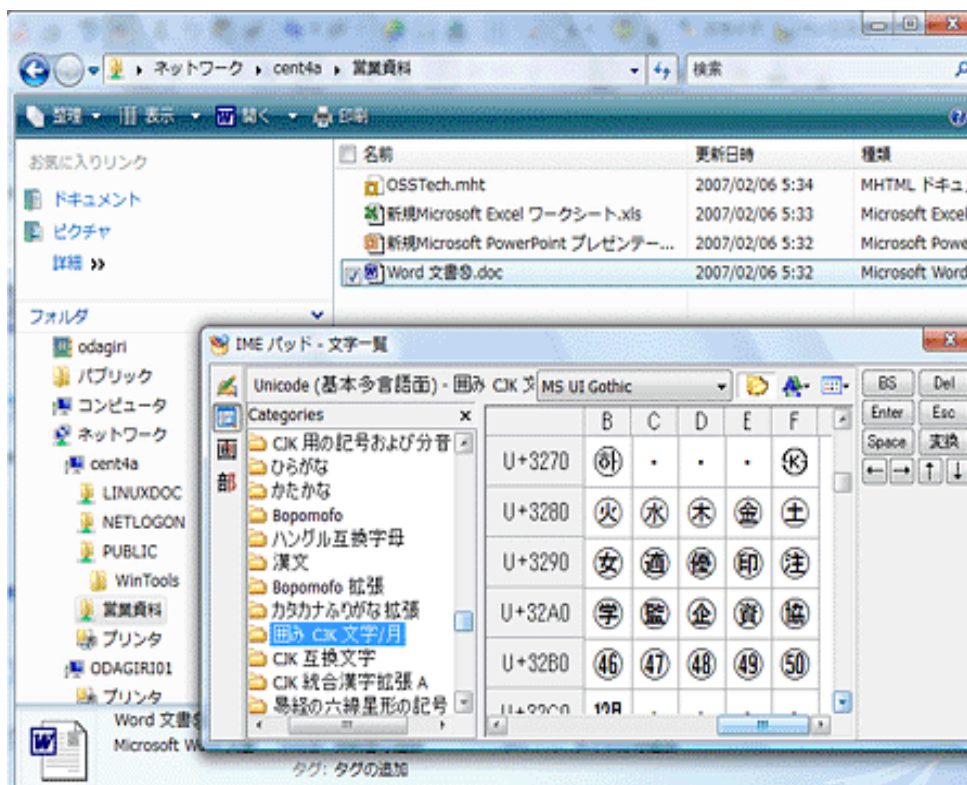
- バージョンの古いSambaは使うな！
- EUC/SJIS/CAP/HEXは使うな！
- Security=share/server/domainは使うな！
- smbpasswdファイルは使うな！
- smbpasswdコマンドでユーザ登録するな！
- smb.confを修正しなくても共有は使える！
- winbind separatorを使うな！
- idmap backend=ridを使いましょう！

バージョンの古いSambaは使うな！

- Samba3.0系は互換性の問題で実はいくつか分類がある
 - 3.0.0～3.0.14
バグが多く絶対使ってはいけないバージョン
 - 3.0.14a～3.0.20b
ドメインサーバ構築はまずまず
Active Directoryのドメインメンバは避けた方が良い
 - 3.0.21～3.0.24
ドメインサーバ構築実績多い
Active Directoryのドメインメンバもまずまず
 - 3.0.25～3.0.28
品質劣化が激しい。なるべく使わない方が良い。
 - 3.0.28a～3.0.34
VistaやWindows2008連携を使うなら最新3.0.34を推奨

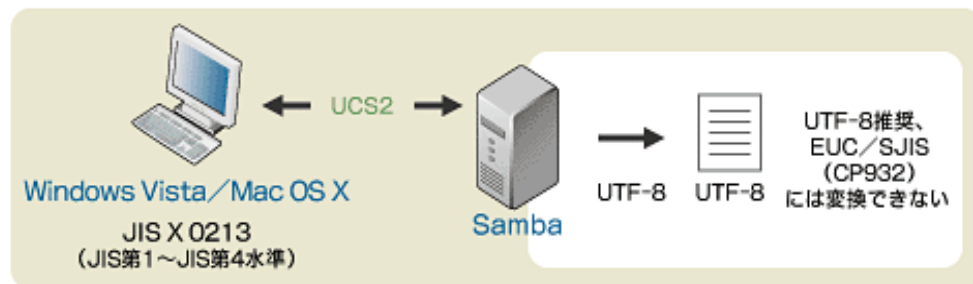
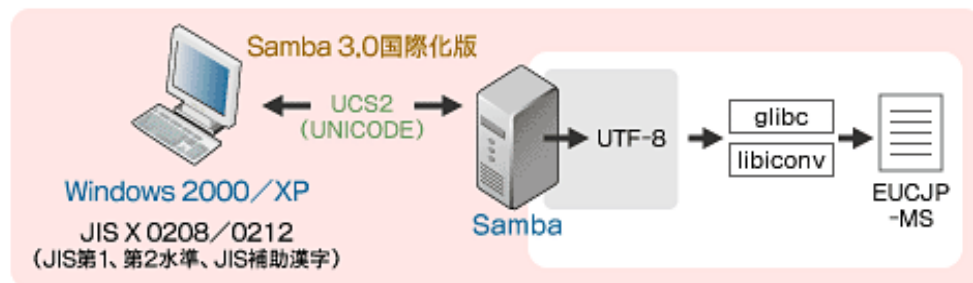
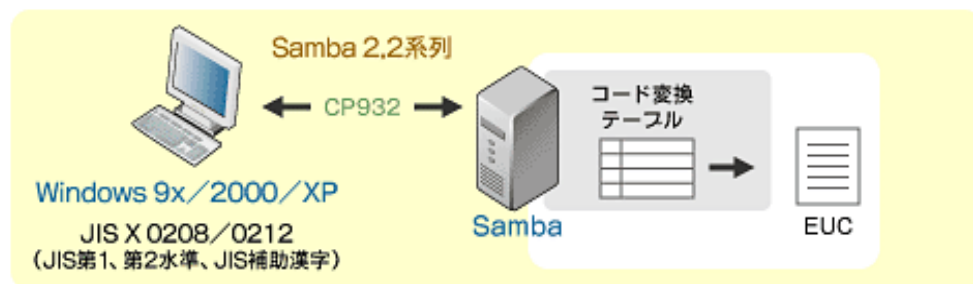
EUC/SJIS/CAP/HEXは使わない！

- Windows Vista/2008からJIS X 0213(JIS2004)がサポート
 - EUC/SJIS/CAP/HEXでは利用できない文字



EUC/SJIS/CAP/HEXは使うな！

- Unix charset = utf-8もしくははutf-8-macが推奨
 - dos charsetはどうでもいいがCP932をとりあえず指定
(Mac OS Xでは指定不可)



Security=share/server/domainは使いな！

- VistaやWindows 2008 Serverでセキュリティ強化
 - Security=share/server/domainでは動かないケースが発生
 - Samba 3.0.29でsecurity=domainの動作確認（3.0.28a以前では利用できない）
- Active Directoryのメンバにするときは security=adsを使う

smbpasswdファイルは使うな！

- smbpasswdファイルは古い形式
- スタンドアロン構成ではtdbsamを使う
- ドメイン構成や大規模(300ユーザ以上)ではLDAPを使うこと

smbpasswdコマンドでユーザ登録するな！

- smbpasswdはユーザが自分のパスワードを変更するコマンドであってユーザ登録をするコマンドではない
- ユーザ登録はpdbeditコマンドで行う
 - tdbsam/ldapsam/smbpasswdを使ってもpdbedit
 - あらかじめOSのユーザ登録をしておく
 - useradd user1
 - pdbedit -a user1
 - smbldap-toolsを使うとOSのユーザ登録とpdbeditコマンド相当を一度にやってくれる
 - smnldap-useradd -a user1
- 今後はnetコマンドが標準になる可能性あり

smb.confを修正しなくても共有は使える！

- 最新のSambaにはUsershare機能があり、smb.confを修正しなくても共有追加する機能が備わった
 - Mac OS Xでのsmb共有作成はUsershare機能で実現
- smb.confへの事前設定
 - usershare allow guests = Yes
 - usershare max shares = 100
 - usershare owner only = No
 - usershare path = /etc/samba/usershares
- 共有設定を置くディレクトリは1775で作成
 - stickyビットが必要
 - グループに更新権を与えれば複数ユーザで共有作成

winbind separatorを使うな！

- security=adsを使ってActive Directoryのドメインメンバにする時の注意事項
- 時刻をADのDCにあわせる (ntpdの設定)
- DNSサーバーはADのDCを指す
- krb.confでもケロベロスサーバとしてADのDCを指す
- winbind separatorはデフォルトが良い
 - +や@、: 記号は使わない
 - どうしても¥がいやな場合は、__かーを使う

idmap backend = ridを使おう

- Active Directoryのドメインメンバにする時や他のドメインと信頼関係を結ぶ時の注意事項
- Windows SID(RID)とuid,gidのマッピングにtdbやLDAPを使っていると、DBが壊れた時に情報が失われる。
- 計算式で一意に決まるRID方式が推奨
- Samba 3.0.24以前と3.0.25以降で互換性がない

```
[global]
```

```
idmap domains = MAIN TRUSTED1
```

```
idmap config MAIN:backend = rid
```

```
idmap config MAIN:base_rid = 1000
```

```
idmap config MAIN:range = 10000 - 49999
```

```
idmap config TRUSTED1:backend = rid
```

```
idmap config TRUSTED1:base_rid = 1000
```

```
idmap config TRUSTED1:range = 50000 - 99999
```