

Sambaによる ファイルサーバ入門

日本Sambaユーザ会

太田 俊哉



講師紹介と資料の取扱いについて

太田俊哉

- 日本Sambaユーザー会スタッフ（発起人）
- 本業は.....

資料の取扱いについて

- CC BY-SA 4.0です

本日のお品書き

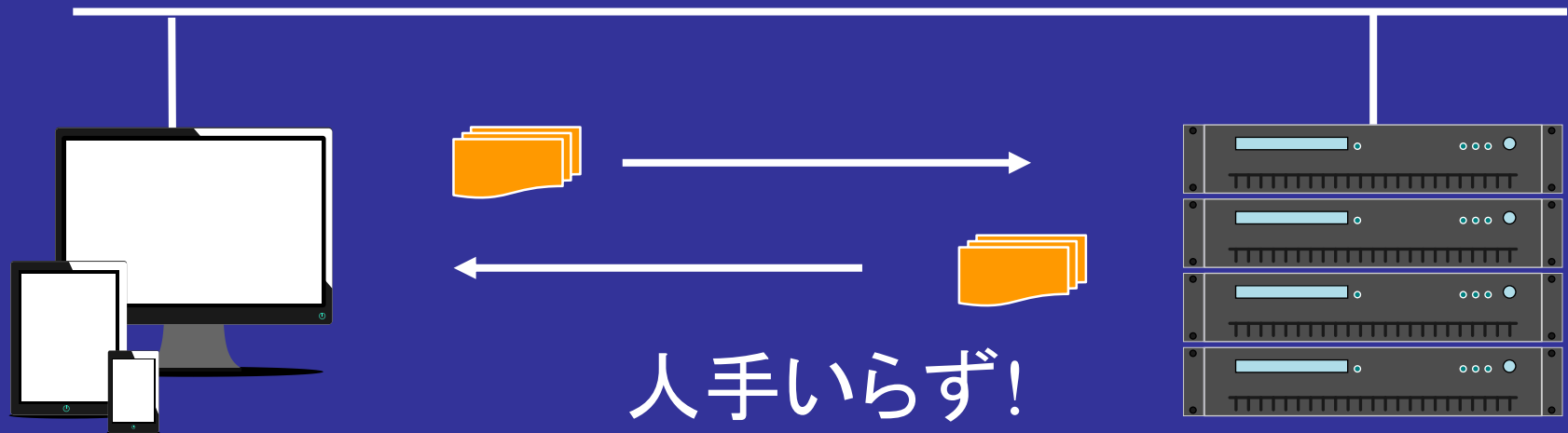
- ファイル共有とは
- Sambaとは
- Sambaのインストール
- Sambaの初期設定
- クライアントからのアクセス方法
- ドメインにメンバサーバとして参加する
- まとめ

ファイル共有とは

- ファイル共有とは
- Sambaとは
- Sambaのインストール
- Sambaの初期設定
- クライアントからのアクセス方法
- ドメインにメンバサーバとして参加する
- まとめ

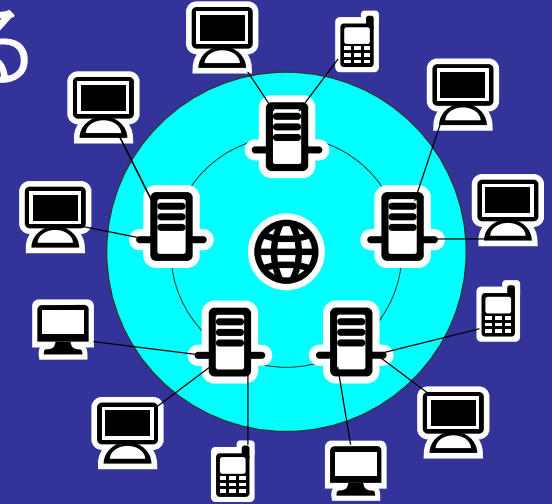
ファイル共有とは

- ローカルネットワークやインターネット上で、あるコンピュータ内のファイルに、他コンピュータからのアクセスをさせる仕組み



ファイル共有のメリット

- 複数の人が同じファイルを使える
 - 組織をまたがった利用も可能
 - デバイスをまたがった利用も可能
- 1箇所にファイルがあるので管理が楽
 - バックアップ等を集中して処理できる
- メールで送信しなくてもすむ
 - 送信の手間が省ける
 - メールボックスパンクの回避



LAN用とインターネット用

- 大きく分けて、LAN用とインターネット用がある
- LAN用(今回の説明はこちら)
 - 組織内部で使うことを前提としているもの
Windowsでのファイル共有など
- インターネット用
 - いわゆるネットワークストレージ
どこでもインターネットに繋がっていれば使える

ファイル共有のしくみ

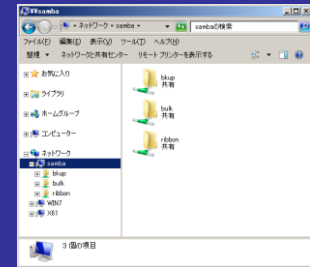
- あらかじめ決められた手順で、互いにアクセス
→ファイル共有のためのプロトコル

- ローカルなネットワーク

- NFS, **SMB(Samba)**, Apple Filing Protocol(AFP)など

- インターネット上

- Dropbox, Google Drive, OneDrive など



Sambaとは

- ファイル共有とは
- **Sambaとは**
- Sambaのインストール
- Sambaの初期設定
- クライアントからのアクセス方法
- ドメインにメンバサーバとして参加する
- まとめ

Sambaとは

- Windowsサーバ互換のファイル・プリンタ共有と、Active DirectoryのDCを実現するソフトウェア
 - Unix系OS(*BSD/Linux等)、MacOS Xなどで動作
 - Windows Server 2008+ α の機能を実装
- 広く利用されている
 - 企業内での利用(CAL不要なことがメリットの1つ)
 - アプライアンス製品でも利用(NASなど)

Sambaのメリット

- Windows系OSとUnix*系OSを使う場合は便利
 - sftpのように、専用ツールでアップロード/ダウンロードしなくても、単にファイルのドラッグアンドドロップでファイルのコピーや移動ができる。
- AD連携すると、ユーザやグループの一元管理もできる。
 - 設定は少々面倒だが、組織全体で管理ができるメリットがある。

Sambaのインストール

- ファイル共有とは
- Sambaとは
- **Sambaのインストール**
- Sambaの初期設定
- クライアントからのアクセス方法
- ドメインにメンバサーバとして参加する
- まとめ

Sambaのインストール

- インストール時にメニューで選択するだけ(CentOS7)



ベース環境

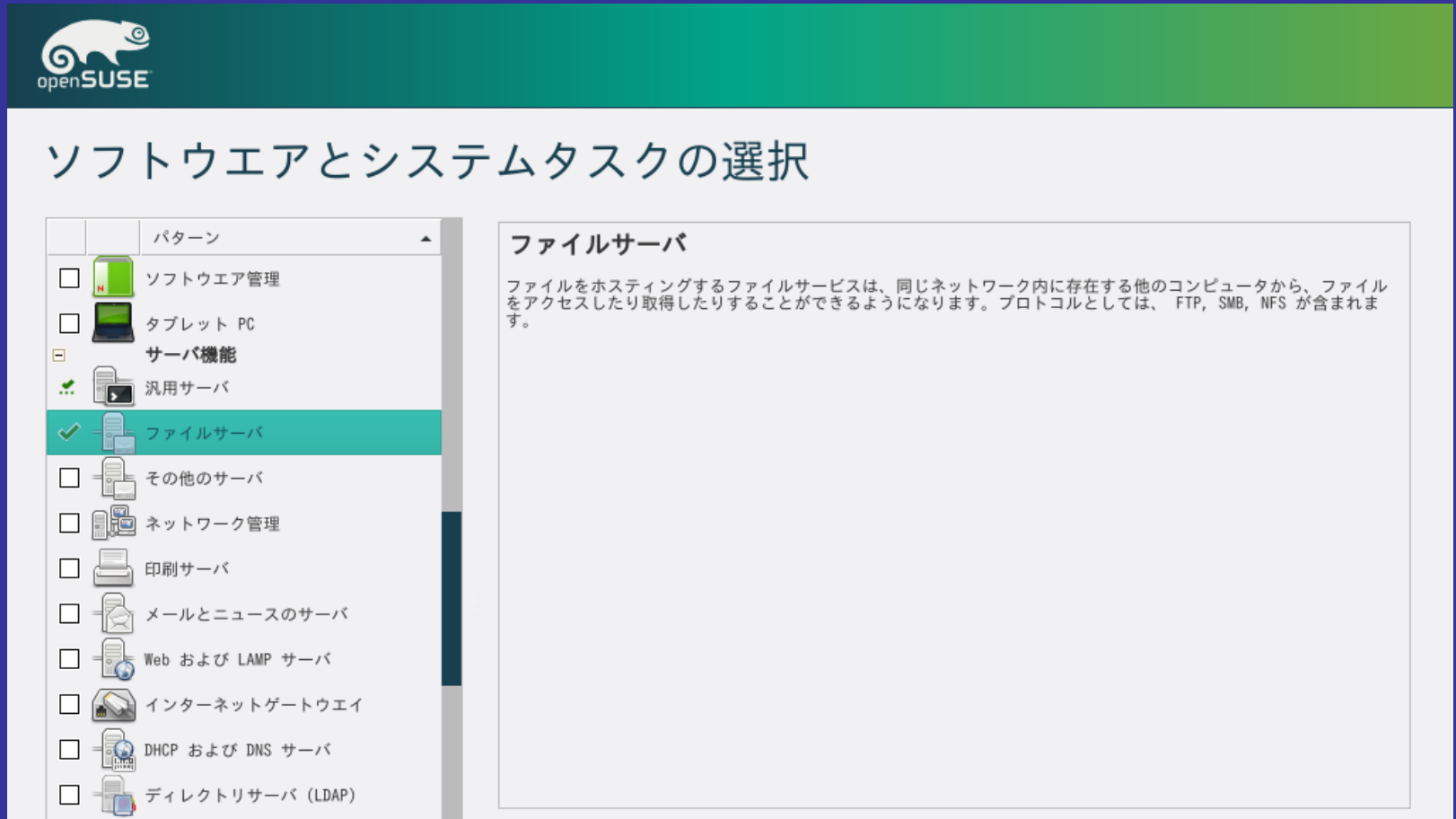
- 最小限のインストール
基本的な機能です。
- Compute Node
計算と処理を行うためのインストールです。
- インフラストラクチャサーバー
ネットワークインフラストラクチャのサービスを動作させるサーバーです。
- ファイルとプリントサーバー
企業向けのファイル、プリントおよびストレージサーバーです。
- ベーシック Web サーバー
静的および動的なインターネットコンテンツの配信を行うサーバーです。
- 仮想化ホスト
最小の仮想化ホストです。
- サーバー (GUI 使用)
GUI を使用してネットワークインフラストラクチャのサービスを動作させるサーバーです。
- GNOME Desktop
GNOME は非常に直観的でユーザーフレンドリーなデスクトップ環境になります。
- KDE Plasma Workspaces
KDE Plasma Workspaces は高度な設定が可能なグラフィカルユーザーインターフェイスであり、パネルやデスクトップ、システムアイコン、デスクトップウィジェットなど数多くのパワフルな KDE アプリケーションを搭載しています。
- 開発およびクリエイティブワークステーション
ソフトウェア、ハードウェア、グラフィックまたはコンテンツ開発向けのワークステーションです。

選択した環境のアドオン

- バックアップクライアント
バックアップサーバーに接続しバックアップを実行するためのクライアントツール
- バックアップサーバー
インフラストラクチャのバックアップを集中化するソフトウェアです。
- デバッグツール
正しく動作しないアプリケーションをデバッグし、パフォーマンスの問題を分析するツールです。
- ディレクトリ接続クライアント
ディレクトリサービスによって管理されるネットワークに統合するための接続クライアント
- ゲストエージェント
ハイパーバイザー配下で稼働する場合に使用するエージェントです。
- ハードウェアモニタリングユーティリティ
サーバーハードウェアの監視用ツールセットです。
- High Availability
High Availability サービスや共有ストレージのインフラストラクチャ
- Java プラットフォーム
CentOS Linux Server Platform と Desktop Platform の Java サポート
- 大規模システムのパフォーマンス
大規模システム向けのパフォーマンスサポートツールです。
- ネットワークファイルシステムクライアント
システムがネットワークストレージに接続できるようにします。
- パフォーマンスツール
システムおよびアプリケーションレベルのパフォーマンス問題を分析するツールです。
- Linux 向けリモート管理
OpenLMI and SNMP など、CentOS Linux 向けのリモート管理インターフェースです。
- Resilient Storage
GFS2 ファイルシステムなど、クラスタ化したストレージです。

Sambaのインストール

- インストール時にメニューで選択するだけ(openSUSE)



The screenshot shows the openSUSE logo at the top left. Below it is the title "ソフトウェアとシステムタスクの選択". On the left is a list of software patterns with checkboxes. The "ファイルサーバ" (File Server) option is checked and highlighted in green. On the right is a text box titled "ファイルサーバ" with a description in Japanese.

openSUSE

ソフトウェアとシステムタスクの選択

パターン
<input type="checkbox"/> ソフトウェア管理
<input type="checkbox"/> タブレット PC
<input checked="" type="checkbox"/> サーバ機能
<input checked="" type="checkbox"/> 汎用サーバ
<input checked="" type="checkbox"/> ファイルサーバ
<input type="checkbox"/> その他のサーバ
<input type="checkbox"/> ネットワーク管理
<input type="checkbox"/> 印刷サーバ
<input type="checkbox"/> メールとニュースのサーバ
<input type="checkbox"/> Web および LAMP サーバ
<input type="checkbox"/> インターネットゲートウェイ
<input type="checkbox"/> DHCP および DNS サーバ
<input type="checkbox"/> ディレクトリサーバ (LDAP)

ファイルサーバ

ファイルをホスティングするファイルサービスは、同じネットワーク内に存在する他のコンピュータから、ファイルをアクセスしたり取得したりすることができるようになります。プロトコルとしては、FTP, SMB, NFS が含まれます。

1111

Sambaのインストール

- 個別にインストールする場合
 - あとから追加する場合など
 - ◆ パッケージの利用が簡単(rpm,deb,pkg(FreeBSD)など)
 - ソースからコンパイルするのはやや難しい
 - ◆ コンパイルする場合には、コンパイル環境の準備や configureオプションに注意が必要
- Samba/パッケージ例 (RHEL/CentOS/Fedora等)
 - samba-common 基本ファイルなど
 - samba サーバ機能
 - samba-client クライアントコマンドなど

Sambaの初期設定

- ファイル共有とは
- Sambaとは
- Sambaのインストール
- **Sambaの初期設定**
- クライアントからのアクセス方法
- ドメインにメンバサーバとして参加する
- まとめ

Sambaの初期設定でやること

- スタンドアロンかAD連携するか、ADのDCになるかを決める
- その後、おおよそ以下の流れで設定する
 - smb.confの設定
 - 共有の設定
 - ユーザ・パスワードの設定
 - SELinuxの設定(CentOS7等)
- GUIで設定できるOS/ディストリビューションもある(openSUSEとか)

Sambaの初期設定(smb.conf)

- 設定ファイルはsmb.conf

- Linuxで、パッケージを利用している場合は、
/etc/samba 以下にある

- ディストリビューションでひな形を用意している

- セクション

- [homes] ユーザのホームディレクトリの共有設定

- [printers] サーバに接続されたプリンタの設定

- [共有名] 個別の共有設定

```
[セクション名]  
  パラメータ名=パラメータ値 [パラメータ値....]  
:  
[セクション名]  
:
```

するしないの設定は、
yes/no で行う

smb.confの設定(基本)

● workgroup

- ワークグループ名/ドメイン名を設定
- 既存ネットワーク接続時は同じものを設定
- 既定値は WORKGROUP

● security

- セキュリティモード(認証方法)を設定
- auto/user/domain/ads から選択
- 通常では指定しない(autoが既定値)かuser を指定
(Sambaが管理する認証情報でユーザ単位に認証)

smb.confの設定([global])

- passdb backend

- Samba用パスワード保存ファイル
- 通常は既定値のまま(tdbsum)

- printing

- 印刷システムの指定
- 既定値はOS依存
- Linuxではcupsになっていることが多い
- 印刷しないのであれば気にしなくて良い

smb.confの設定[(global)]

- max log size

- Sambaが出すログファイルの最大サイズ(Kb)
- このサイズを超えるとログファイルが切り替わる

- log level

- 何も指定しないと 0 で、起動終了メッセージ程度が記録される
- デバッグ時には状況に応じて数字を大きくする(が、そうするとログファイルにどんどん記録される)

smb.confの設定[(globalの設定例)]

- 次のような設定を記述する
 - ワークグループ名はKIKAKU
 - 認証情報はSamba が管理する
 - ログファイルをちょっと多めにする

```
[global]
  workgroup = KIKAKU
  security = user
  max log size = 100
  passwd backend = tdbsam
  :
```

共有の設定(1)

- path

- 共有の対象ディレクトリ(=ファイルを置く場所)

- read only

- 更新がある共有ではNo と設定する
- ただし、ファイルシステムレベルの書き込みできる権限が必要
- シノニム (writeableなど)もあるので注意

- browseable

- yes とすることで、共有の一覧に表示されるようになる

共有の設定(2)

● 簡単な設定例

- 共有名は「pubdata」とする
- 書き込みが出来るようにする
- aclが使えるようにする
 - ◆ ファイルシステムで対応していることが必要

```
[pubdata]
```

```
comment = public data
```

```
path = /var/samba/pubdata
```

```
read only = No
```

```
inherit acls = yes
```


ユーザとグループ

- Unix系OSでの利用者管理
≠Windows系での利用者管理
 - パスワード管理方法の差異
 - 文字コード
- user,group,other (パーミッション)とACLの差異
- 入門レベルでは、英数字のみのユーザ名で

重要

ユーザー・パスワードの設定

- あらかじめUnix*側でユーザが作成されている必要がある(useradd コマンドなどで)
- pdbedit コマンドでユーザを作成する
 - 作成時にパスワードも同時に指定する
 - Windowsログオン時のパスワードと同じにすると管理が楽
- 複数のユーザをどうまとめるかを考えておく
 - グループの概念
 - アクセス制御

pdbeditの実行例

```
[root@cent7 samba]# pdbedit -a azureuser
new password:
retype new password:
Unix username:      azureuser
NT username:
Account Flags:      [U          ]
User SID:           S-1-5-21-1249057497-2155902979-2420647544-1001
Primary Group SID: S-1-5-21-1249057497-2155902979-2420647544-513
Full Name:
Home Directory:    ¥¥cent7¥azureuser
HomeDir Drive:
Logon Script:
Profile Path:      ¥¥cent7¥azureuser¥profile
Domain:            CENT7
Account desc:
Workstations:
Munged dial:
Logon time:        0
Logoff time:       Thu, 07 Feb 2036 00:06:39 JST
Kickoff time:     Thu, 07 Feb 2036 00:06:39 JST
Password last set: Tue, 28 Feb 2017 23:13:38 JST
Password can change: Tue, 28 Feb 2017 23:13:38 JST
Password must change: never
Last bad password  : 0
Bad password count : 0
Logon hours        : FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
```

Sambaの起動・停止

- パッケージを用いている場合は、起動スクリプトを用いるのが便利
 - 古いCentOS/RHEL/Fedora/openSUSEだと、
`/etc/init.d/samba`
 - 新しいCentOS/RHEL/Fedora/openSUSEだと、
`systemctl`
 - FreeBSD だと `/usr/local/etc/rc.d/samba.sh`
 - 基本的には、プロセス `smbd` と `nmbd` を起動する
 - ◆ `samba daemon` はAD管理用
 - ◆ `winbindd daemon` はAD連携用

SELinuxの設定(1)

- CentOS6/7などではselinuxの機能が既定値でONになっている
- そのままだと書き込みが出来ない
- とりあえずOFFにする

```
# setenforce permissive
```

としてはいけません!

SELinuxの設定(2)

- SELinuxとSambaを共存させるためには
 - booleanパラメータの設定
 - ◆ あらかじめSELinux内に含まれている条件付きポリシー `samba_enable_home_dirs` をOnにする。既定値ではOff。
- 共有用ディレクトリへのタイプ付与
 - あらかじめSamba用のパターンは「`samba_share_t`」として用意されている。設定には `chcon` を使う。
- これでSE Linuxを有効してSambaが使える。
 - OSC 2018Tokyo/Fallの資料も参照のこと

SELinuxで脆弱性を緩和

● CVE-2017-7494

- リモートから任意のコードを実行可能な脆弱性
- メンテ終了のSamba 3.5系列にも影響あり
- しかし、SELinuxを有効にしていれば、外部ディレクトリから実行可能なモジュールのロードを**ブロック!**
→SELinuxを使う意義がある

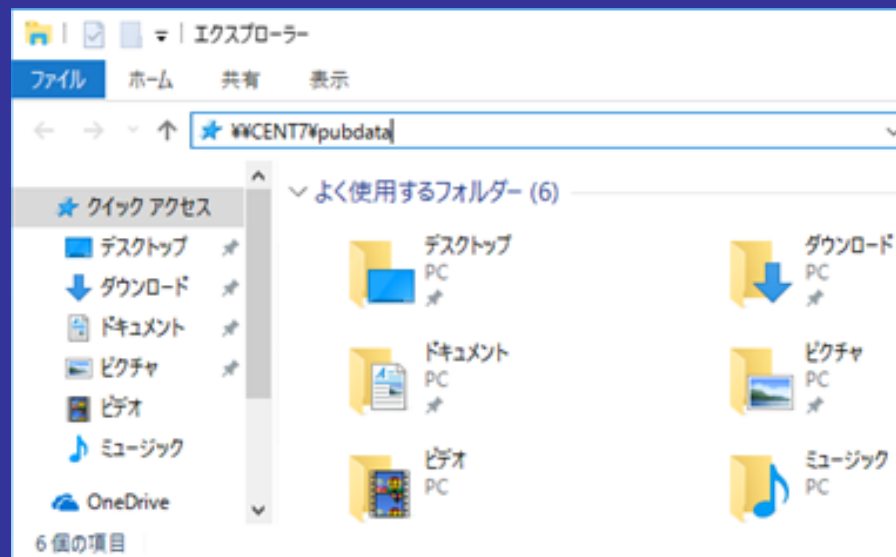
<https://access.redhat.com/security/cve/CVE-2017-7494>

クライアントからのアクセス方法

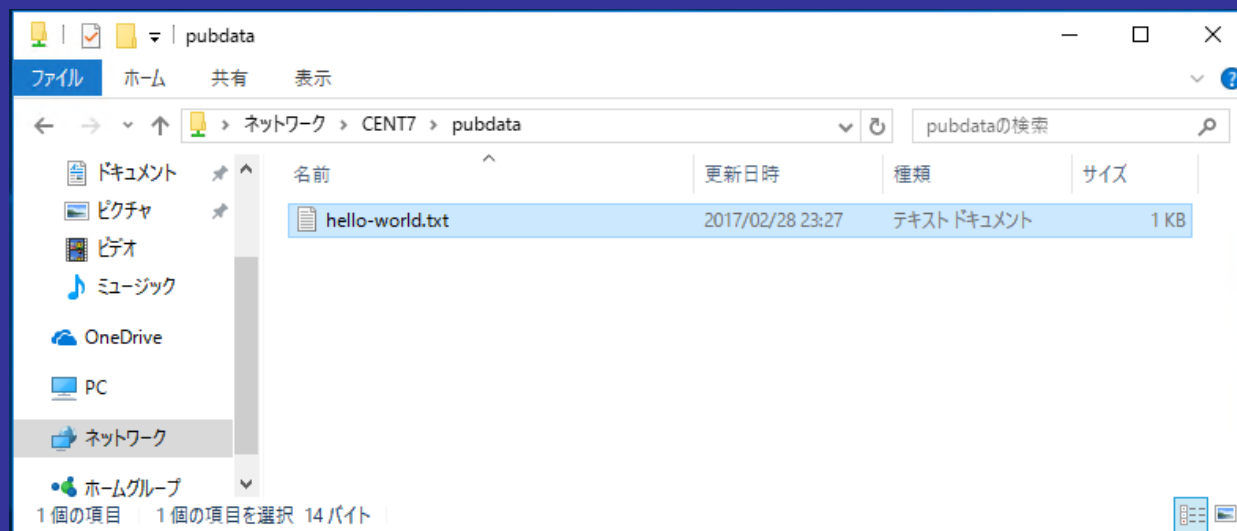
- ファイル共有とは
- Sambaとは
- Sambaのインストール
- Sambaの初期設定
- クライアントからのアクセス方法
- ドメインにメンバサーバとして参加する
- まとめ

Windows 10から繋いでみる

- エクスプローラを開き、接続先のUNCを入力

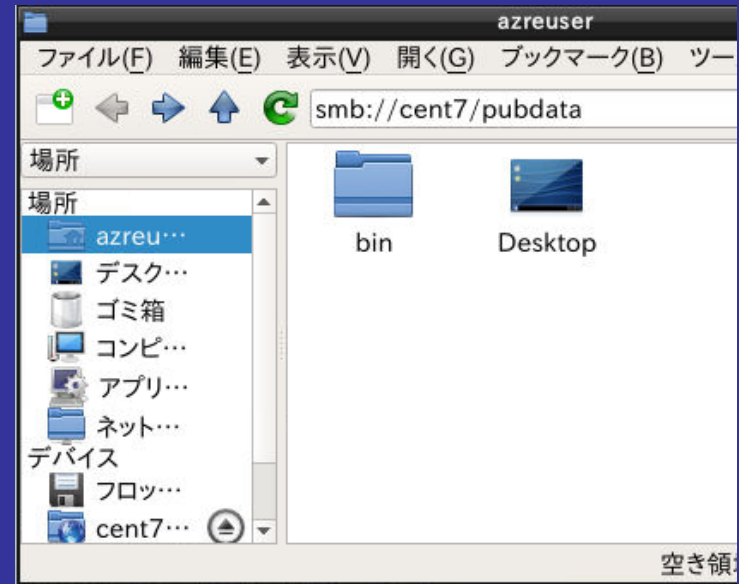


- 繋がった

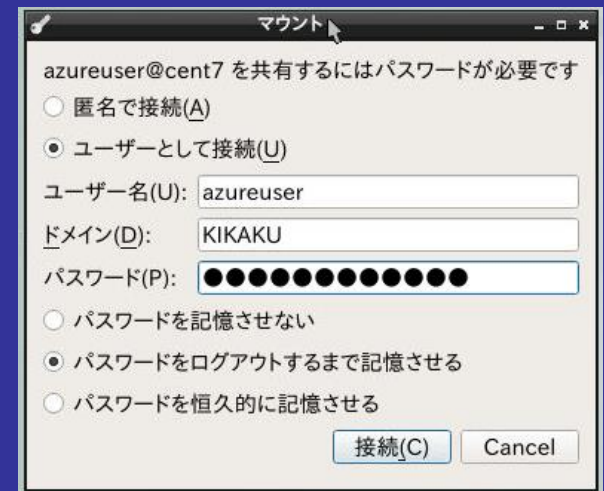


Linuxから繋いでみる(1)

- lxqt上でのPCManFMアドレスバーに入力

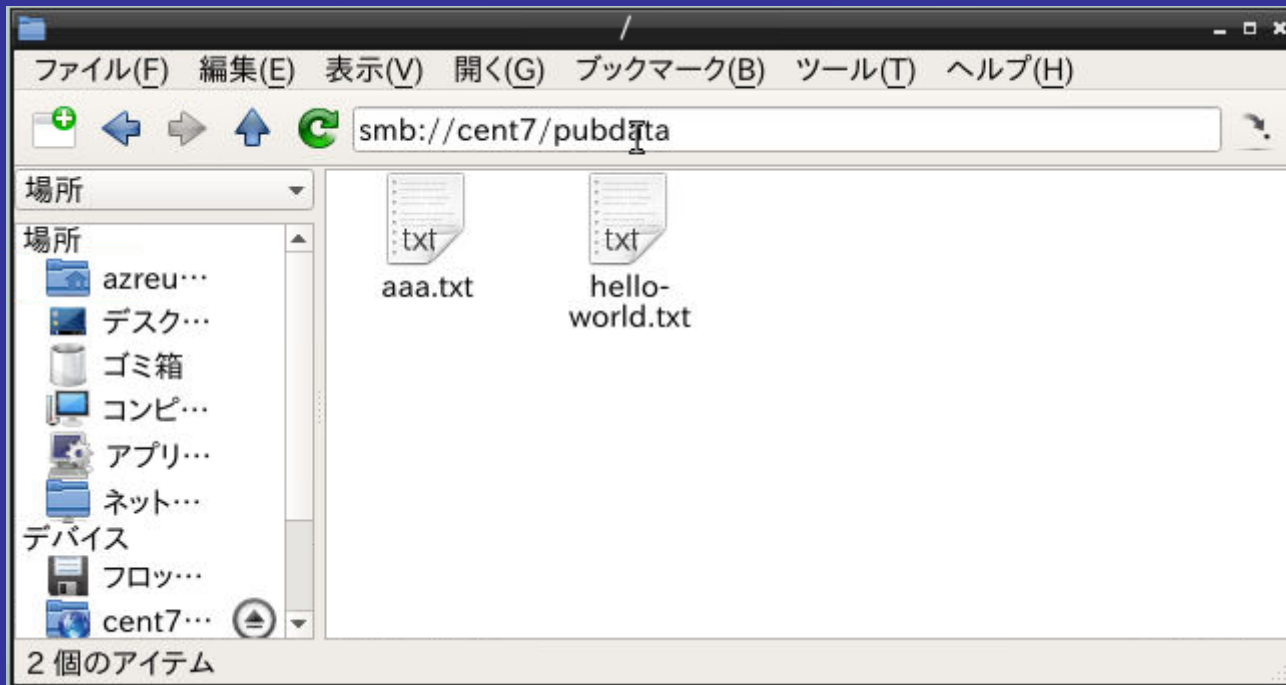


- ユーザ名、パスワードを入力



Linuxから繋いでみる(2)

● つながった



ドメインにメンバサーバとして参加する

- ファイル共有とは
- Sambaとは
- Sambaのインストール
- Sambaの初期設定
- クライアントからのアクセス方法
- ドメインにメンバサーバとして参加する
- まとめ

ドメインにメンバサーバとして参加する

● 複数台サーバがある場合のユーザ(ID)管理

- 各サーバごとに個別に登録
→ 台数が多くなると管理が大変。uid/gidが異なると、覚えたり管理するのが大変。



- 管理サーバに登録
→ 管理サーバ作成等の手間はかかるが、あとの管理が楽。どのサーバへも、同じユーザ、パスワードでアクセスできる。



IDを共通化するしくみ

- NIS

古い。ほぼ使われていない。

- LDAP

よく使われている。大規模向け。LDAPの仕組みはちょっと難しい。

- Active Directory

Windowsの世界での標準。Sambaを使う事で利用可能。

- Sambaを使う場合、ADがあるならそこに参加するのが楽

SambaサーバをADに参加

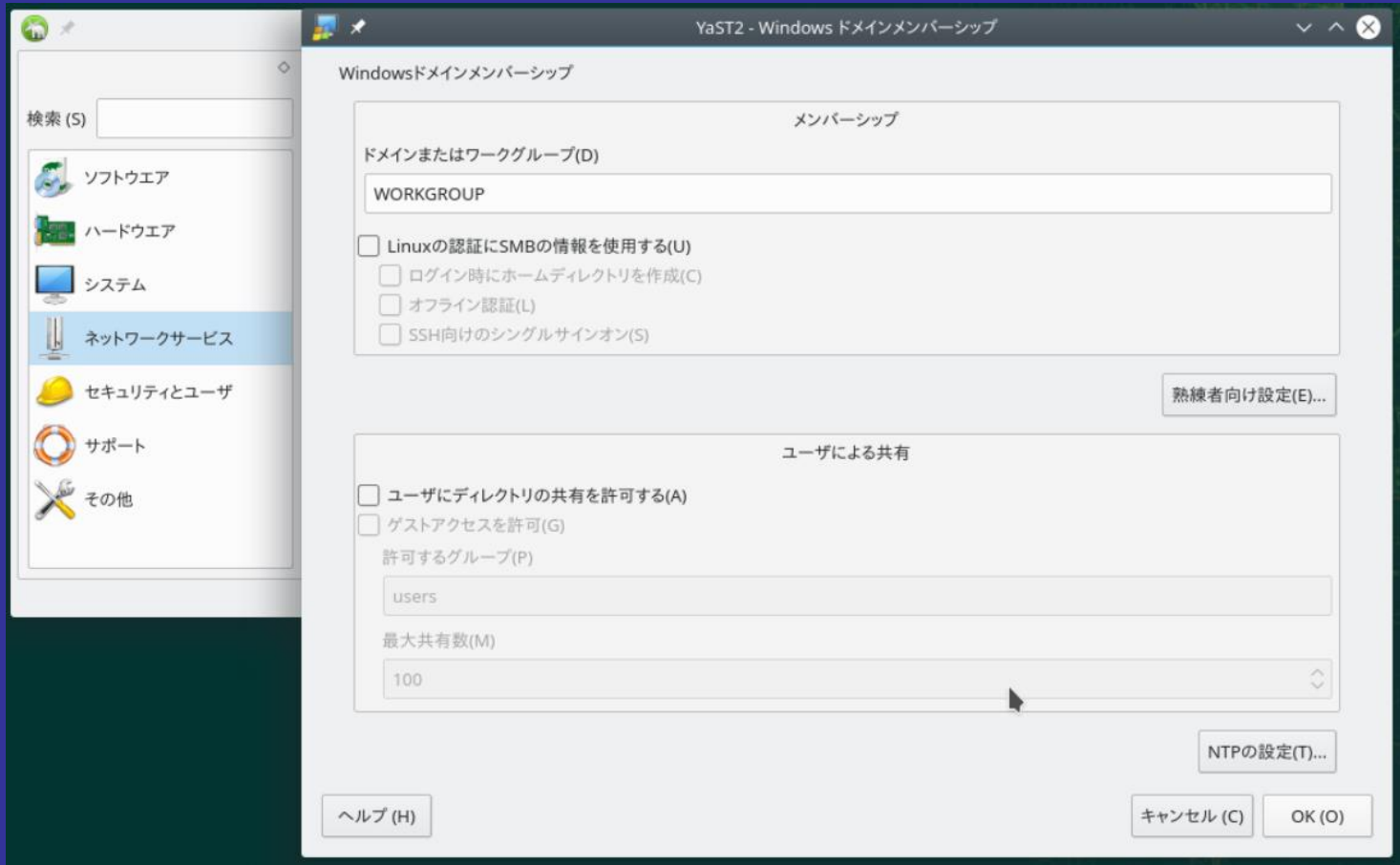
- やることは、WindowsマシンをADに参加させることと同じ。
 - Sambaはサーバなので、WindowsサーバをADに参加させることと同じ。
 - ADのドメインを指定し、ADの管理者でJoin操作を行う。

AD参加の例(1)

- openSUSEの場合、GUI画面でJoinが可能
- AD参加の例
 - Windows Serverは2012R2
 - openSUSE 15.0でKDE環境
 - ドメインは example.jp

AD参加の例(2)

- YastでWindowsドメインメンバーシップを起動



AD参加の例(3)

- ドメイン名を入力し、必要な箇所にチェック

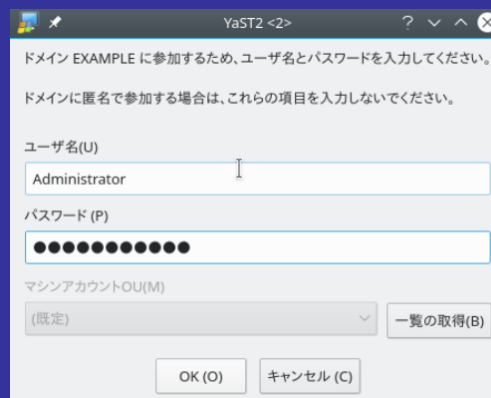
The screenshot shows the YaST2 configuration window for Windows Domain Membership. The window title is "YaST2" and the main title is "Windowsドメインメンバーシップ". The "メンバーシップ" section contains a text field for the domain name, which is "EXAMPLE.JP". Below this, there are four checked options: "Linuxの認証にSMBの情報を使用する(U)", "ログイン時にホームディレクトリを作成(C)", "オフライン認証(L)", and "SSH向けのシングルサインオン(S)". A button labeled "熟練者向け設定(E)..." is located to the right of these options. The "ユーザによる共有" section contains three unchecked options: "ユーザにディレクトリの共有を許可する(A)", "ゲストアクセスを許可(G)", and "許可するグループ(P)". The "許可するグループ(P)" text field contains the value "users". Below this, the "最大共有数(M)" text field contains the value "100". A button labeled "NTPの設定(T)..." is located to the right of these options. At the bottom of the window, there are three buttons: "ヘルプ(H)", "キャンセル(C)", and "OK(O)".

AD参加の例(4)

- 参加確認



- AD管理者による承認

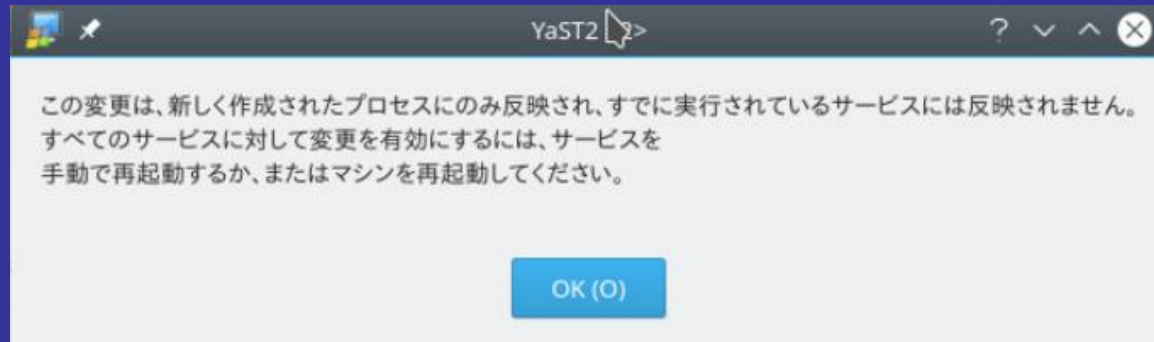


- 参加できた

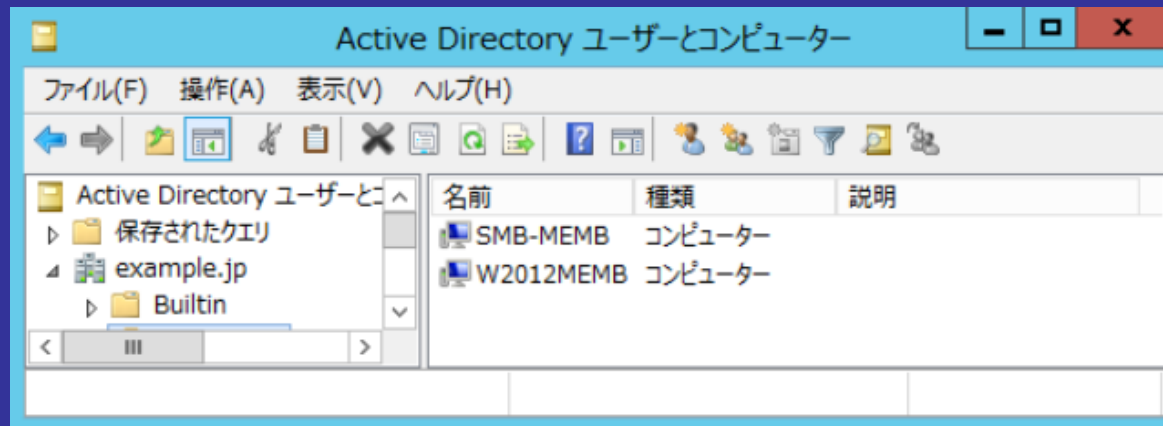


AD参加の例(5)

- ただしサービスの再起動は必要

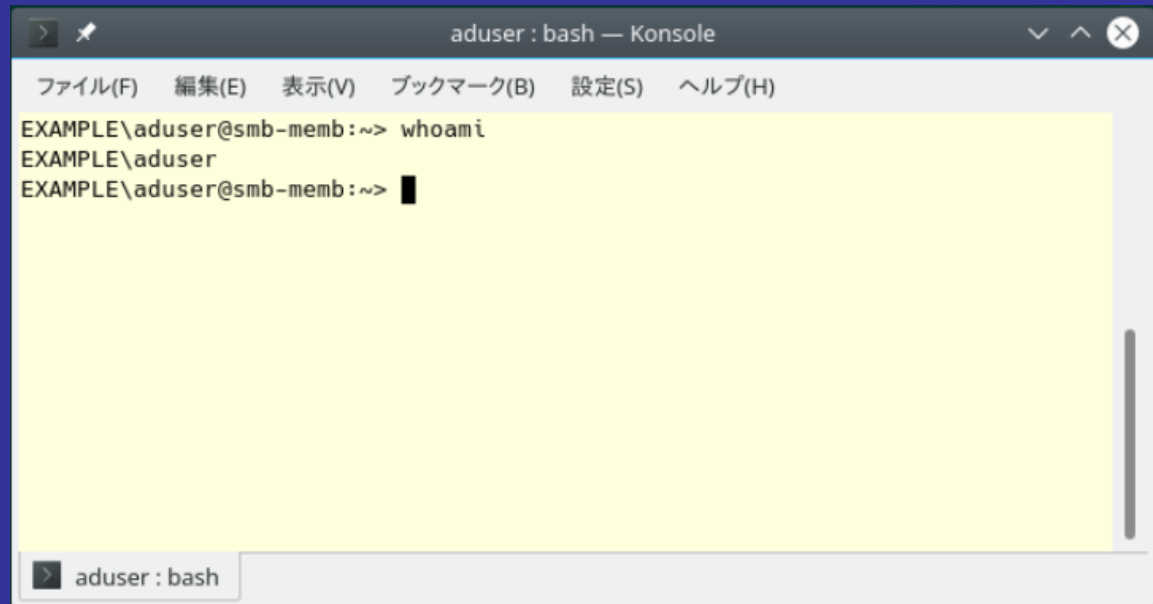


- AD上で見ても参加できている



AD参加の例(6)

- ドメインユーザでログインしてみる
- AD上のユーザでログインできた

A screenshot of a terminal window titled 'aduser : bash — Konsole'. The terminal shows the following commands and output:

```
EXAMPLE¥aduser@smb-memb:~> whoami
EXAMPLE¥aduser
EXAMPLE¥aduser@smb-memb:~> █
```

The terminal window has a menu bar with options: ファイル(F), 編集(E), 表示(V), ブックマーク(B), 設定(S), ヘルプ(H). The status bar at the bottom shows 'aduser : bash'.

AD参加時の注意

- CALは必要

- WindowsサーバをADのDCとして使うため、CALは必要。

- ユーザ管理はWindows側で

- Sambaサーバ上のみのユーザは、管理用のユーザにとどめておく。

まとめ

- 簡単な使い方ならば、インストールして多少の設定をすればすぐに使える
- OS/ディストリビューションごとに起動方法などは多少違うが、基本は同じ
- 多少、Unix*系の操作になれておく必要はある
- SELinuxとも共存できる
- Windows ADに参加することもできる

参考情報

- Sambaの本家サイト
 - <http://www.samba.org/>
- 日本Sambaユーザー会
 - <http://wiki.samba.gr.jp/>
 - 日本語による技術情報(マニュアル和訳あり)
- その他
 - openclipart <https://openclipart.org/>
- メーリングリストも用意しています

ご静聴ありがとうございました

