OSC 2017 Tokyo

Sambaによる ファイルサーバ入門

日本Sambaユーザ会
太田 俊哉

http://wiki.samba.gr.jp

講師紹介

太田俊哉

- 日本Sambaユーザー会スタッフ（発起人）
- 本業は.....
  - オープンソースに関する仕事色々
  - 対外的な活動も(日本OSS推進フォーラムとか)

本日のお品書き

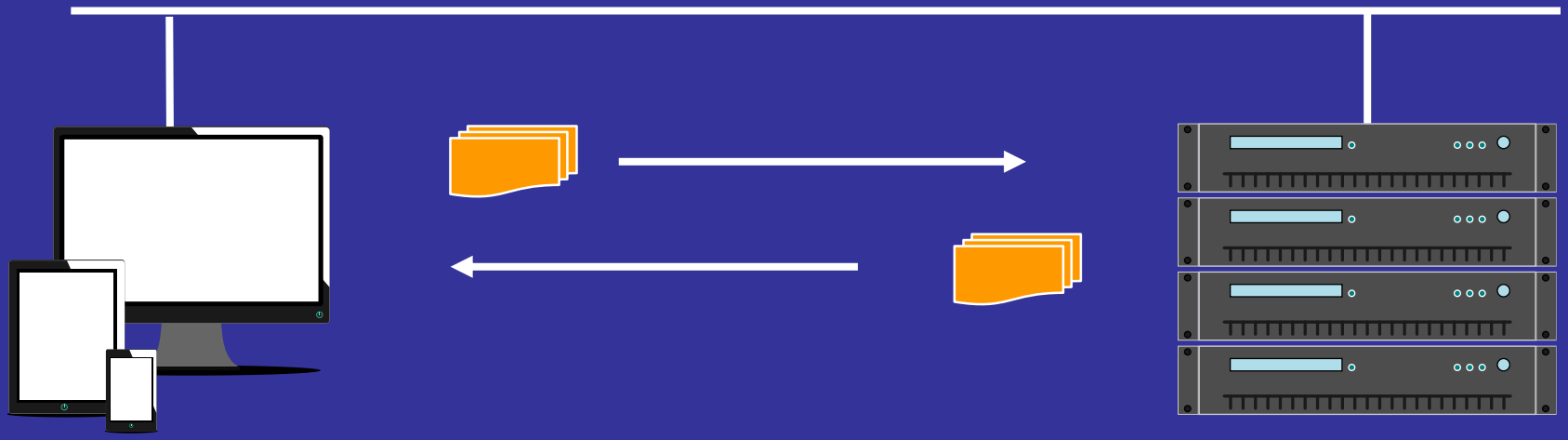
- ファイル共有とは
- Sambaとは
- Sambaのインストール
- Sambaの初期設定
- クライアントからのアクセス方法
- まとめ

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
- まとめ

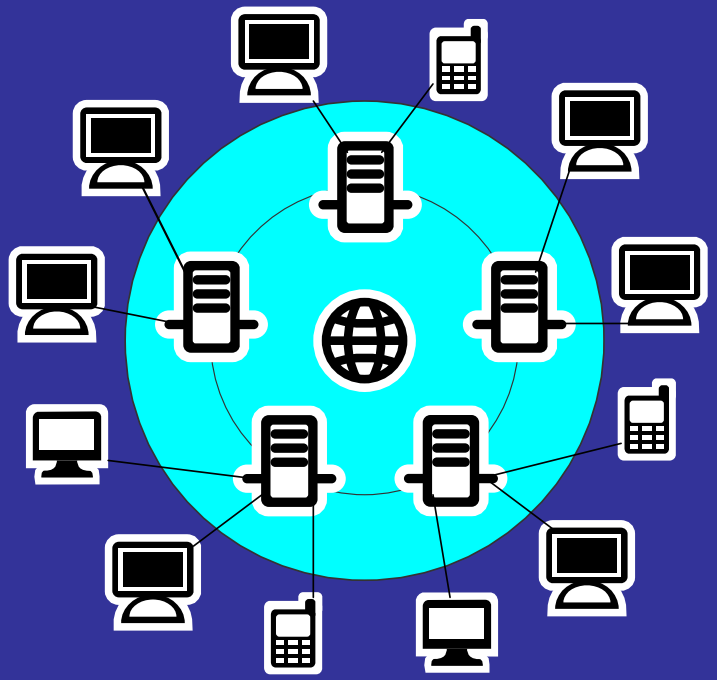
ファイル共有とは

- 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



ファイル共有のメリット

- 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出来る
- 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
  - トラフィック輻輳の回避

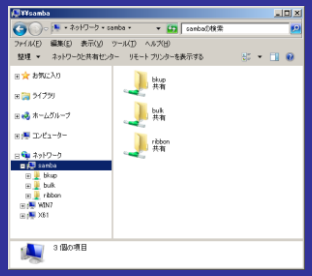
LAN用とインターネット用

- 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

ファイル共有に使われるプロトコル

- NFS
  - Unix系OS同士でファイル共有をする
  - Windowsからでも使えた(一部のみ)
- SMB
  - Microsoftが実装したファイル共有の仕組み
  - Windows以前から存在
  - Windows-Unix*のファイル共有としても使える
    - →Sambaが機能を提供
- そのほかにもいくつかあります

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
- まとめ

Sambaとは

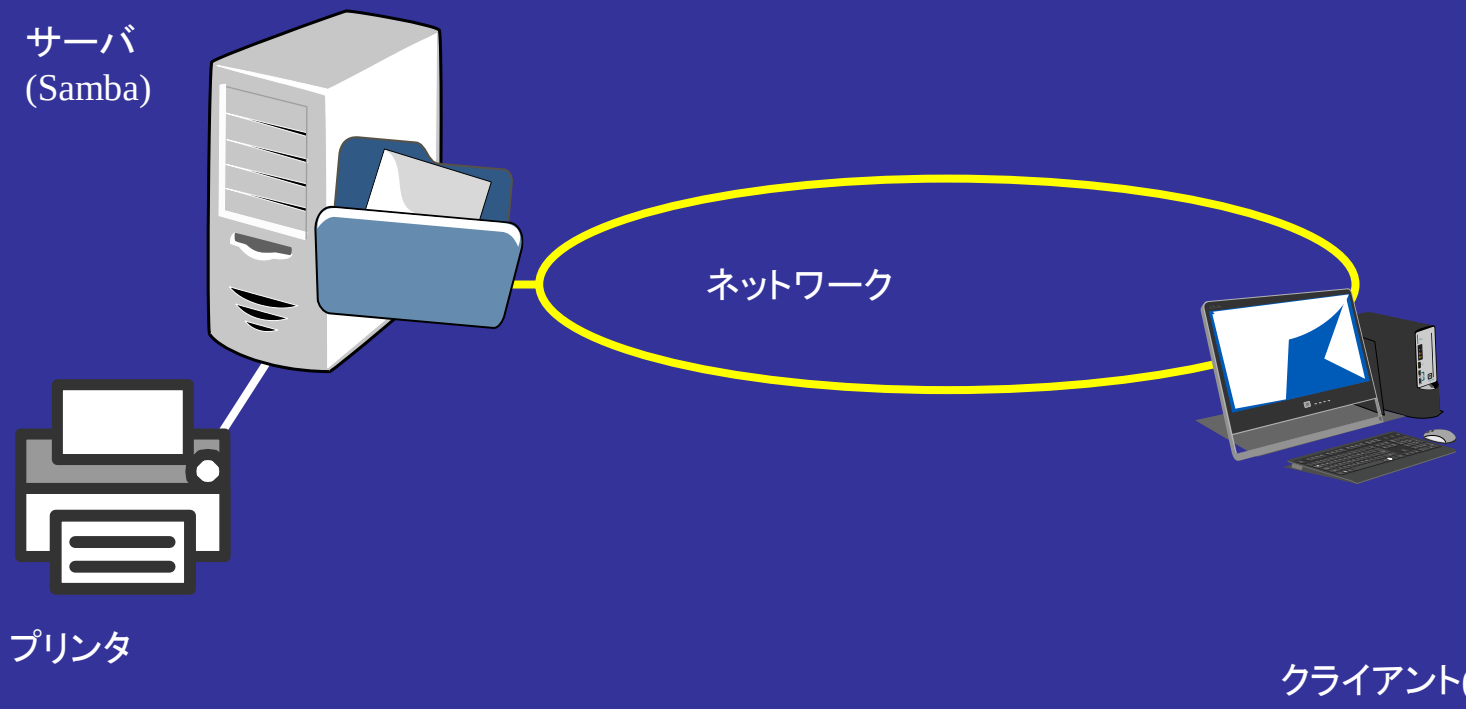
- Windowsサーバ互換のファイル・プリンタ共有と、Active DirectoryのDCを実現するソフトウェア
  - Unix系OS(*BSD/Linux等)、MacOS X などで動作
  - Windows Server 2008+αの機能を実装
  - プロトコルとしてはSMBを使う
- 広く利用されている
  - 企業内での利用(CAL不要なことがメリットの1つ)
  - アプライアンス製品でも利用(NASなど)

Sambaとは

- 最新バージョンは4.6系
  - 3.6系以前と4.0系で大きく機能が異なる
  - 3世代のみサポート(4.3以前はサポート終了)
    - リリース間隔はほぼ半年
    - ベンダサポートはもっと古い物までやっている
- シンプルなファイル共有の実現には十分な機能が揃っている
  - 単なるファイルサービスを行うサーバとして簡単に使える
  - ADのDCになったりAD連携することも可能

Sambaの利用イメージ

- サーバ（Unix系OS）にSambaをインストール
- クライアント（Windows）の設定はほとんど不要

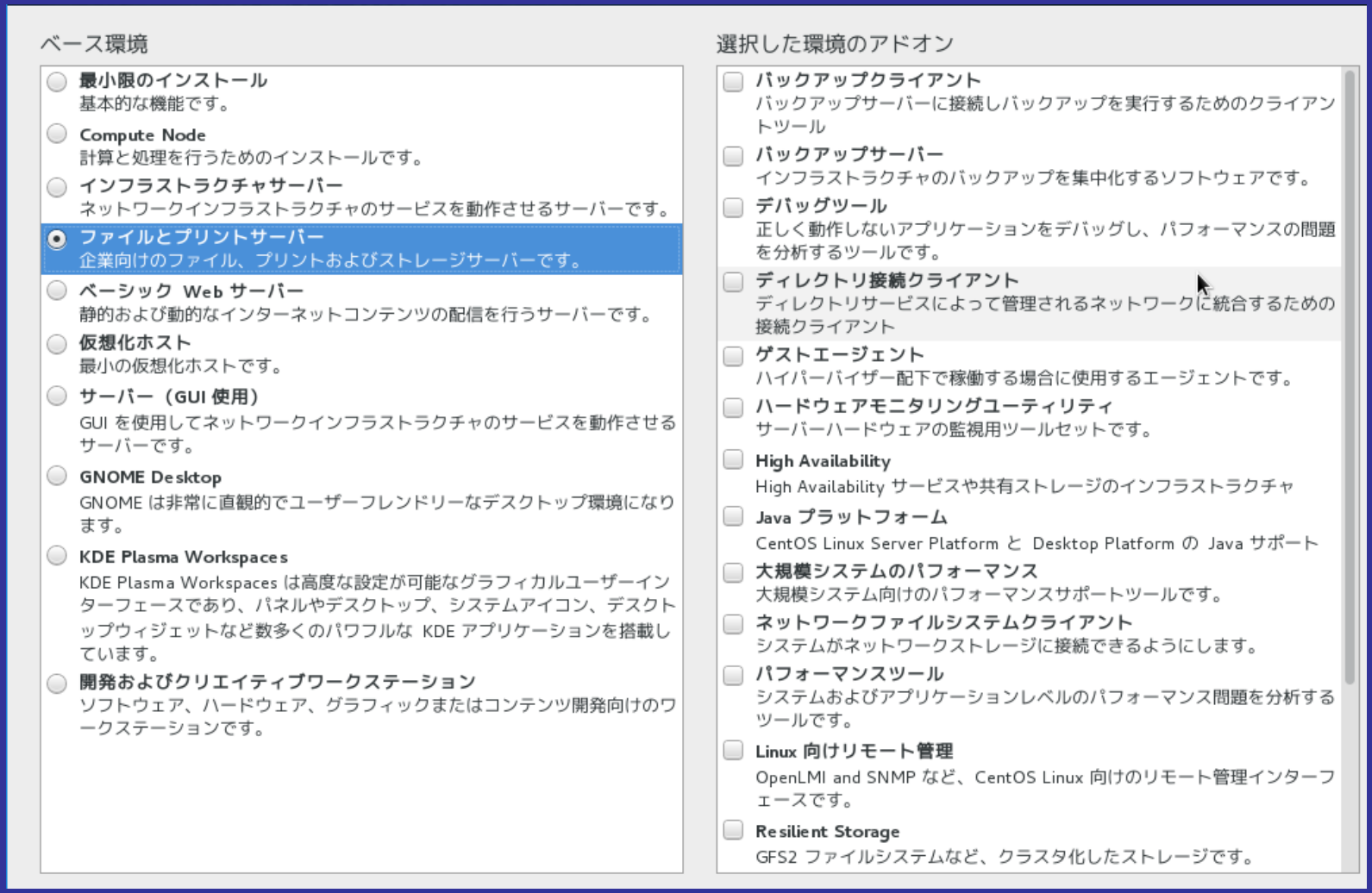


Sambaのインストール

- 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
- まとめ

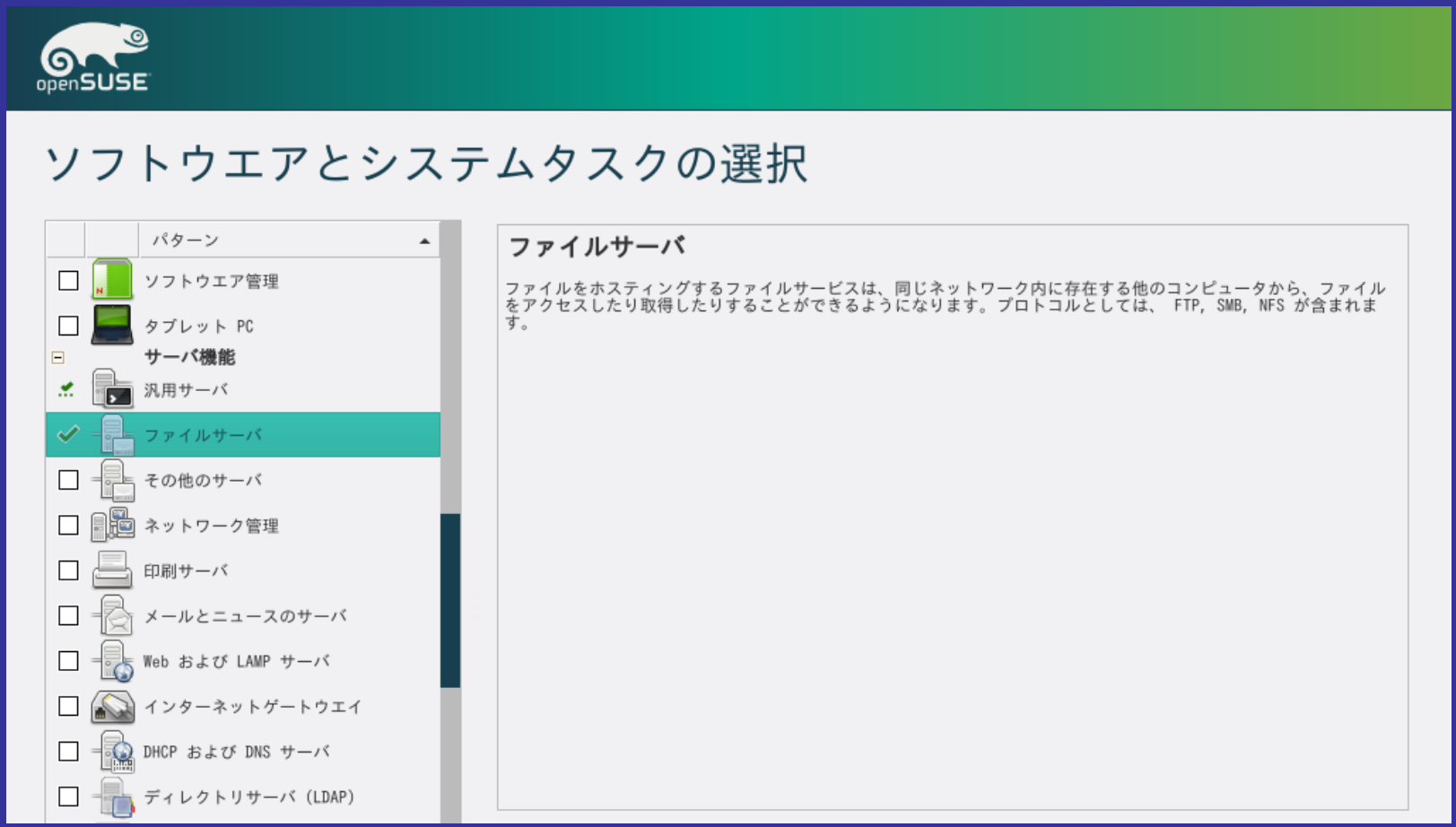
Sambaのインストール

- インストール時にメニューで選択するだけ(CentOS7)



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)



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

インストールするバージョン

- 複数のバージョンがパッケージとして用意されている場合がある
  - たとえばFreeBSD
  - 基本的には最新版を推奨、ただし
    - ディストリビューションでは古いバージョンをメンテナンスしている場合もある(バックポート)
    - ディストリビューション以外から最新版を持ってくる手もある (open build serice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
- まとめ

Sambaの初期設定でやること

- 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)

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
  - 既存のネットワークに接続する場合は同じものを設定
  - 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([grobal])

- 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になっている場合が多い
  - 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
    passdb 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)
- Windows 上ではどうしているか?
  (グループ、ACL)

- 入門レベルでは、英数字のみのユーザ名で

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         : FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
```

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

CentOS7などの場合

- systemdを使う場合
  設定はすべて systemctl コマンドで
- サービスの有効化
  #systemctl enable smb.service
  #systemctl enable nmb.service
- サービスの個別起動
  # systemctl [start|stop|restart] smb.service
  # systemctl [start|stop|restart] nmb.service

CentOS6などの場合

- 自動起動設定は chkconfig
  # chkconfig smb on
- サービスの個別起動は service コマンド
  # service smb [start|stop|restart]
- smbcontrol コマンドもあります
  設定ファイルを再認識させる場合など

SELinuxの設定(1)

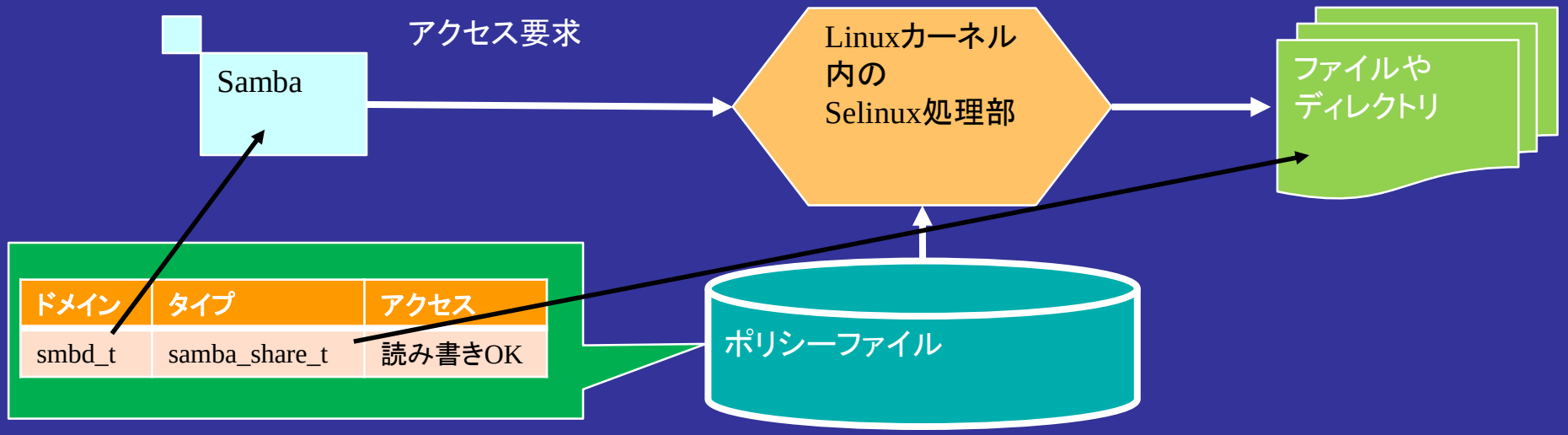
- CentOS6/7などではselinuxの機能が既定値でONになっている
- そのままだと書き込みが出来ない
- とりあえずOFFにする

```
# setenforce permissive
```

としてはいけません!

SELinuxの設定(2)

- SELinuxでは、プロセス(=Samba)からのアクセスをシステムが強制的に制御。あらかじめSambaが使う範囲を許可しておかないと、書き込みが出来ない。



SELinuxの設定(3)

- ファイルやディレクトリには、アクセス制御のためのタイプが設定される

```
# ls -l
total 0
drwxrwxrwx. 2 root root 44 Mar  1 10:59 pubdata
# ls -Zl
total 0
drwxrwxrwx. 2 unconfined_u:object_r:var_t:s0   root root 44 Mar  1 10:59 pubdata
                                              ここ
# cd pubdata
# ls -lZ
-rw-rw-r--. azureuser azureuser unconfined_u:object_r:var_t:s0   aaa.txt
-rwxr--r--. azureuser azureuser system_u:object_r:var_t:s0       hello-world.txt
```

- アクセスできるようにするためには、Sambaが使うディレクトリに、Sambaからのアクセスを可能にするように設定を行う。

SELinuxの設定(4)

- boolian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を使う。
  - Sambaの場合は、samba_enable_home_dirs がある。これをOnにする。既定値ではOff。

```
#  getsebool samba_enable_home_dirs
samba_enable_home_dirs --> off
```

Onにする。

```
# setsebool -P samba_enable_home_dirs 1
```

SELinuxの設定(5)

- 共有用ディレクトリへのタイプ付与
  - あらかじめSamba用のパターンは用意されている。「samba_share_t」。
  - 設定には chcon を使う。

```
# chcon -t samba_share_t /var/samba/pubdata -R

# ls -lZ
drwxrwxrwx. root root unconfined_u:object_r:samba_share_t:s0 pubdata

# ls -lZ
-rw-rw-r--. azureuser azureuser unconfined_u:object_r:samba_share_t:s0 aaa.txt
-rwxr--r--. azureuser azureuser system_u:object_r:samba_share_t:s0 hello-world.txt
```

これでSE Linuxを有効にしながらSambaが使える。

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

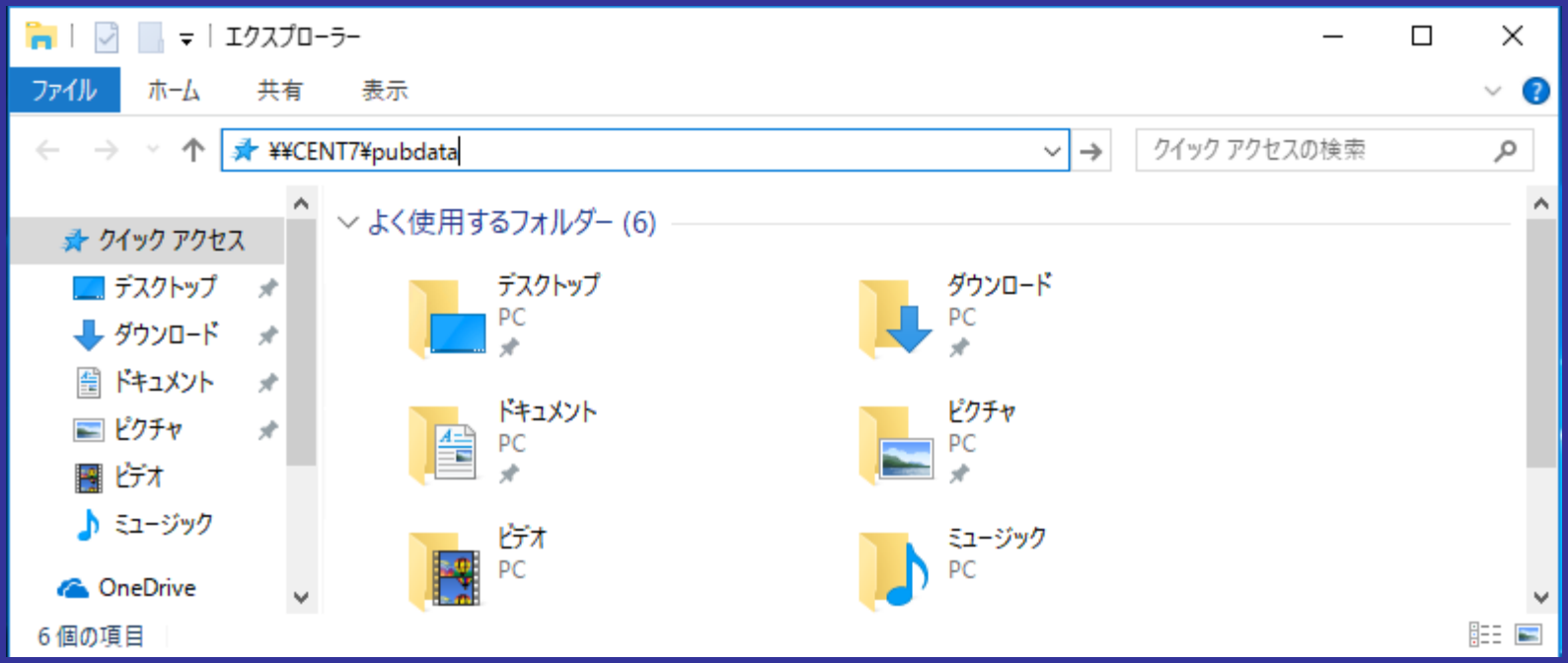
https://access.redhat.com/security/cve/CVE-2017-7494

クライアントからのアクセス方法

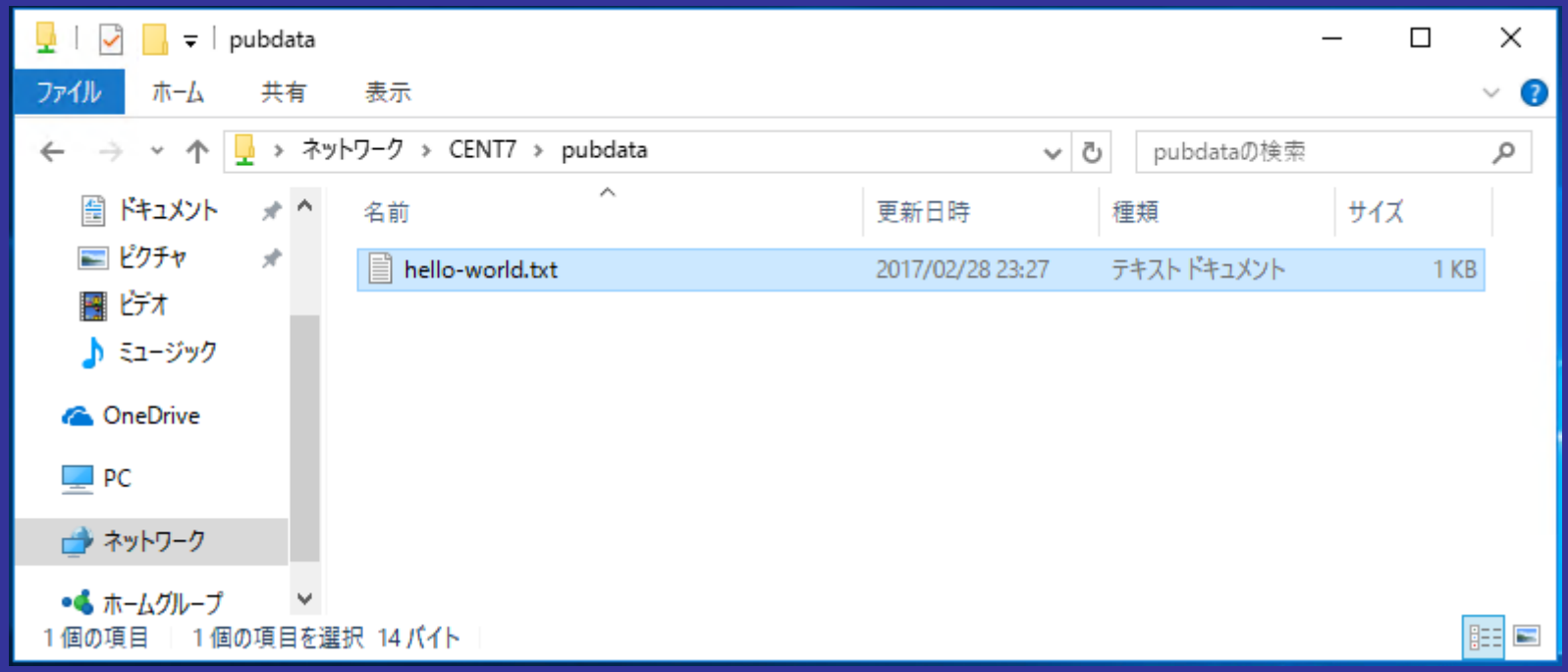
- ファイル共有とは
- Sambaとは
- Sambaのインストール
- Sambaの初期設定
- **クライアントからのアクセス方法**
- まとめ

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



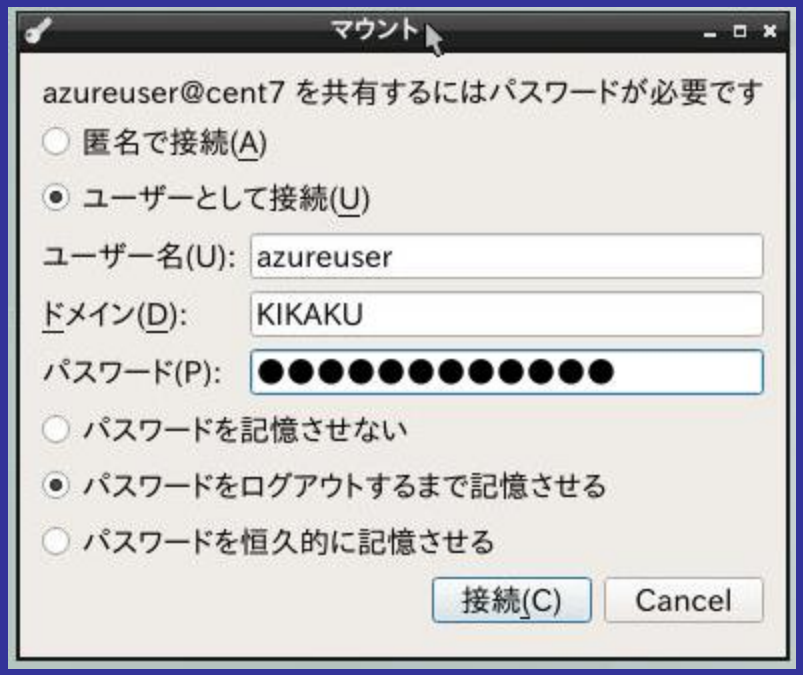
繋がった


pubdata
ファイル
ホーム
共有
表示
ネットワーク › CENT7 › pubdata
pubdataの検索
ドキュメント
ピクチャ
ビデオ
ミュージック
OneDrive
PC
ネットワーク
ホームグループ
名前
更新日時
種類
サイズ
hello-world.txt
2017/02/28 23:27
テキスト ドキュメント
1 KB
1 個の項目
1 個の項目を選択 14 バイト

Linuxから繋いでみる

- lxqt上でのPCManFM
  アドレスバーに入力

ユーザ名やパスワードを入力



繋がった


/
ファイル(F) 編集(E) 表示(V) 開く(G) ブックマーク(B) ツール(T) ヘルプ(H)
smb://cent7/pubdata
場所
場所
azreu…
デスク…
ゴミ箱
コンピ…
アプリ…
ネット…
デバイス
フロッ…
cent7…
txt
aaa.txt
txt
hello-world.txt
2 個のアイテム

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

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）
- 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

日本 samba ユーザ会

http://wiki.samba.gr.jp