

Samba の Windows ドメイン連携 のすべて

日本Sambaユーザ会

たかはしもとのぶ(高橋基信)

monyo@samba.gr.jp

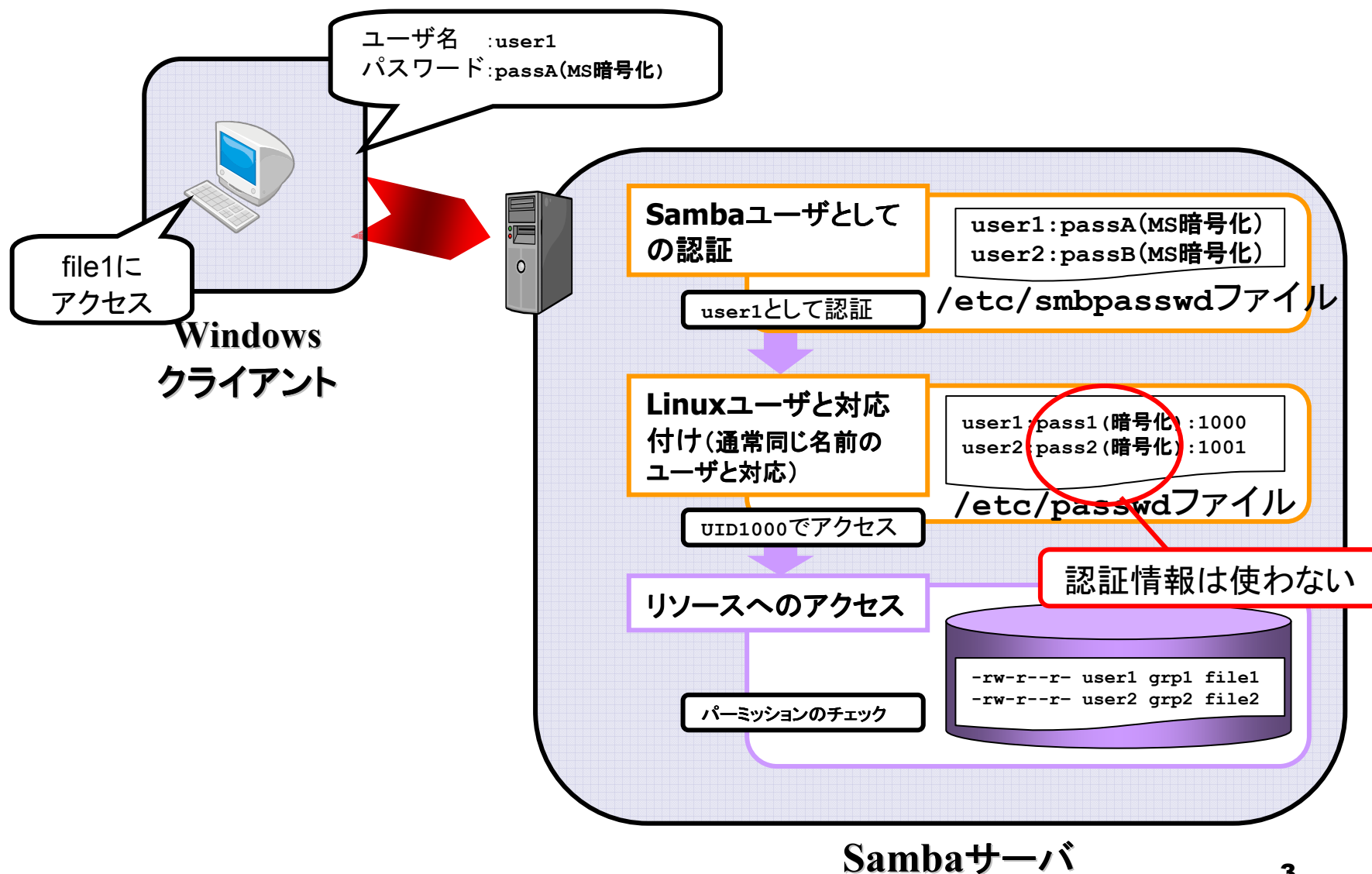
Windows ドメイン連携で実現できること

- 要は、Windowsドメインに「参加」できること
 - Sambaサーバ上のユーザ認証をWindowsドメインに委任できる
 - WindowsドメインのユーザやグループをSambaサーバ上で使える (Winbind機構)
 - Samba以外のプロダクトのログイン認証にも利用できる

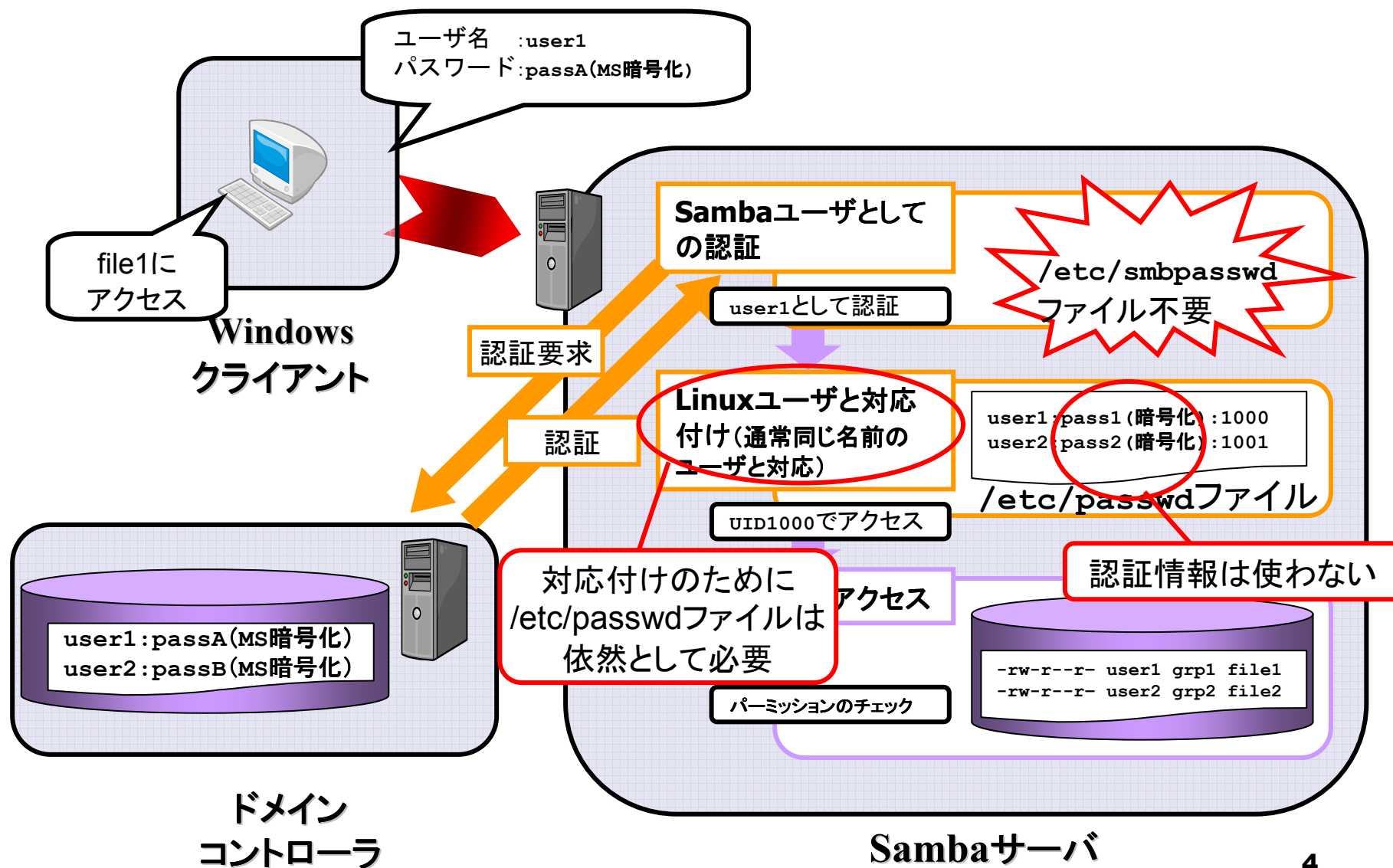
```
$ id 'W2K8AD1¥samba01' ← 指定したユーザのuidとgidを参照
uid=10001(W2K8AD1¥samba01) gid=10000(W2K8AD1¥domain users)
groups=10000(W2K8AD1¥domain users)
```

基本的には、これ以上でも以下でもありません

ユーザ認証をSambaサーバで実施



ユーザ認証をWindowsドメインで実施



Windowsドメインへの「参加」機能

- Windowsとほぼ同等の機能を実装
 - Kerberosを用いたADへの参加をサポート
(NTドメインに対する参加もサポート)
 - NetBIOS不要 & DNS必須、IPv6環境でもOK
 - 任意のOUにコンピュータアカウントを作成可能
 - DNSの動的更新もサポート
 - net ads dns registerコマンド
 - セキュリティ機能のサポート
 - セキュアチャネルの暗号化、LDAP署名
 - client schannel / client ldap sasl wrapping
 - コンピュータアカウントのパスワード変更間隔の制御
 - machine password timeout

Sambaの設定概要

■ securityパラメータを使う

□ security = domain

- Windows NTドメイン(古い！)に対する参加方法
- Sambaドメインに参加する場合以外は非推奨
- 必要な設定
 - NetBIOS名の名前解決(ドメイン名<1B>など)
 - smb.confの設定変更

□ security = ads

- Active Directoryドメインに対する参加方法
- 基本的にはこちらを使うこと
- SambaとWindowsサーバの組み合わせにより若干設定が異なる場合も

ADSの設定手順(1)

- security = adsで必要な設定
 - DNSサーバをADのDCに設定
 - 参加先ドメインのSRVレコードが解決できることを確認

```
$ host -t SRV _ldap._tcp.pdc._msdcs.w2k8ad1.local.
_ldap._tcp.pdc._msdcs.w2k8ad1.local SRV 0 100 389 w2k8srv1.w2k8ad1.local
```

- DCとの時刻同期(±5分以内)
 - ntpやnet time setコマンドを用いるのが一般的
- Sambaサーバの停止
- smb.confの設定変更
 - realm→ドメイン名のFQDNを
大文字で
 - workgroup→ドメイン名の
NetBIOS名
- /etc/krb5.confの設定変更(Kerberos認証)

```
[global]
workgroup = W2K8AD1
realm = W2K8AD1.LOCAL
security = ads
ldap ssl = no (Samba 3.3.0のみ)
```

.....

ADSの設定手順(2)

- security = adsで必要な設定(続)
 - /etc/krb5.confの設定変更(Kerberos認証)

```
[libdefaults]
    (default_realm = W2K8AD1.LOCAL)
.....
    (default_tkt_enctypes = RC4-HMAC DES-CBC-CRC DES-CBC-MD5)

[realms]
    W2K8AD1.LOCAL = {
        kdc = w2k8srv1.w2k8ad1.local
    }

[domain_realm]
    .w2k8ad1.local = W2K8AD1.LOCAL
    w2k8ad1.local = W2K8AD1.LOCAL
```

- カッコ内の設定は場合によって必要
- kdc行の指定はIPアドレスでも可

- Active Directoryドメインへの参加

```
# net ads join -U Administrator
Administrator's password: ←パスワードを入力
Using short domain name -- W2K8AD1
Joined 'SAMBA33A' to realm 'w2k8ad1.local'
No DNS domain configured for samba33a. Unable to perform DNS Update.
DNS update failed!
```

「No DNS domain.....」のエラーは
とりあえず無視してよい

ADSの設定手順: 注意点

□ ありがちなトラブル

■ 時刻が同期されていない → 時刻同期

```
[2010/01/13 11:29:06, 0] libsmb/cliconnect.c:cli_session_setup_spnego(859)
  Kinit failed: Clock skew too great
Failed to join domain: Time difference at domain controller
```

■ 自身のFQDNの名前解決失敗 → hostsなどで名前解決

```
Using short domain name -- W2K8AD1
Failed to set servicePrincipalNames. Please ensure that
the DNS domain of this server matches the AD domain,
Or rejoin with using Domain Admin credentials.
```

```
192.168.135.188 centos54.w2k8ad1.local centos54
```

■ Kerberos関連 → とりあえずdefault_tkt_enctypesを設定

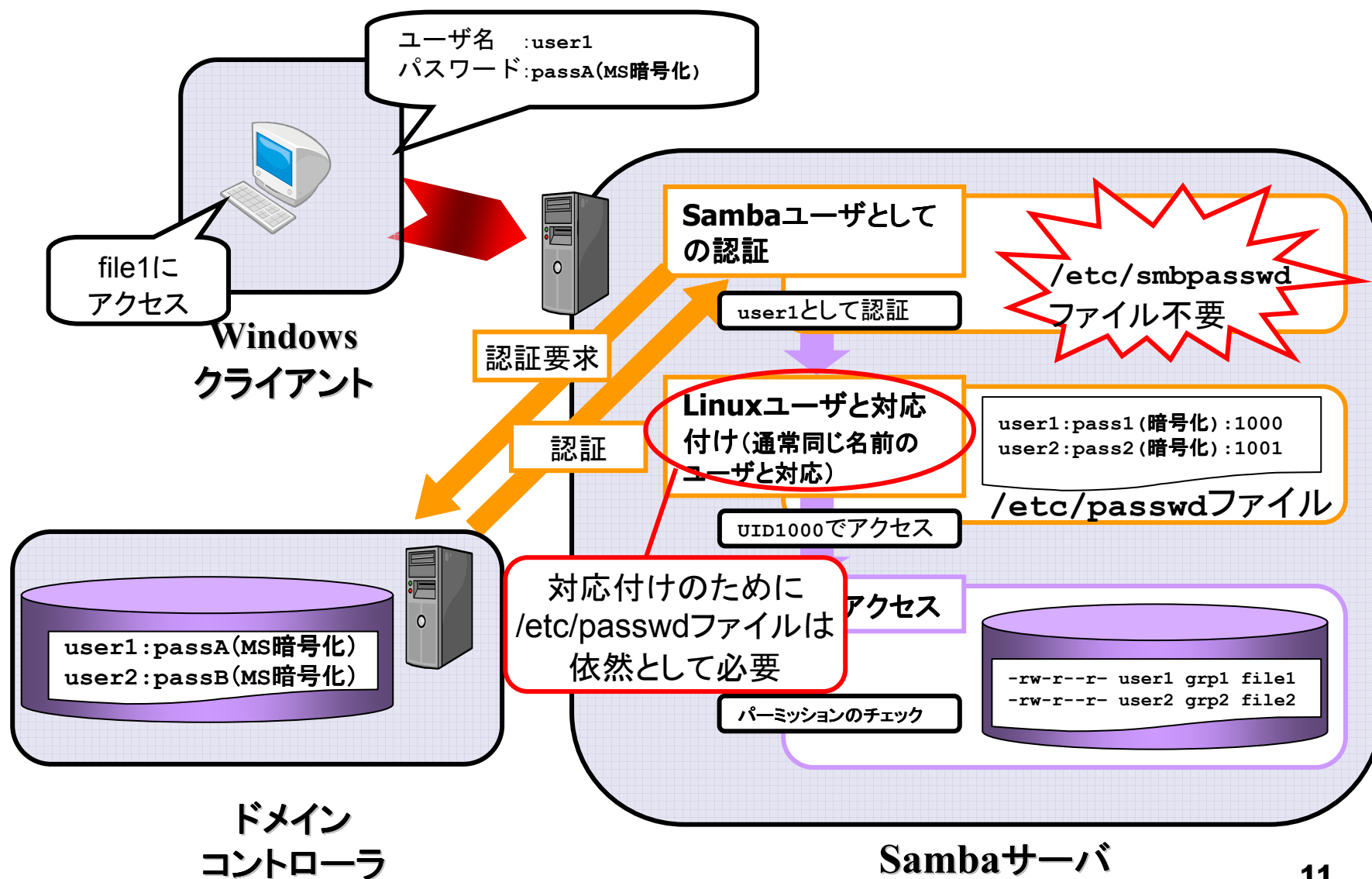
```
[2009/03/08 18:52:46, 0] libsmb/cliconnect.c:cli_session_setup_spnego(785)
  Kinit failed: Cannot resolve network address for KDC in requested realm
Failed to join domain!
```

```
[libdefaults]
  default_tkt_enctypes = RC4-HMAC DES-CBC-CRC DES-CBC-MD5
```

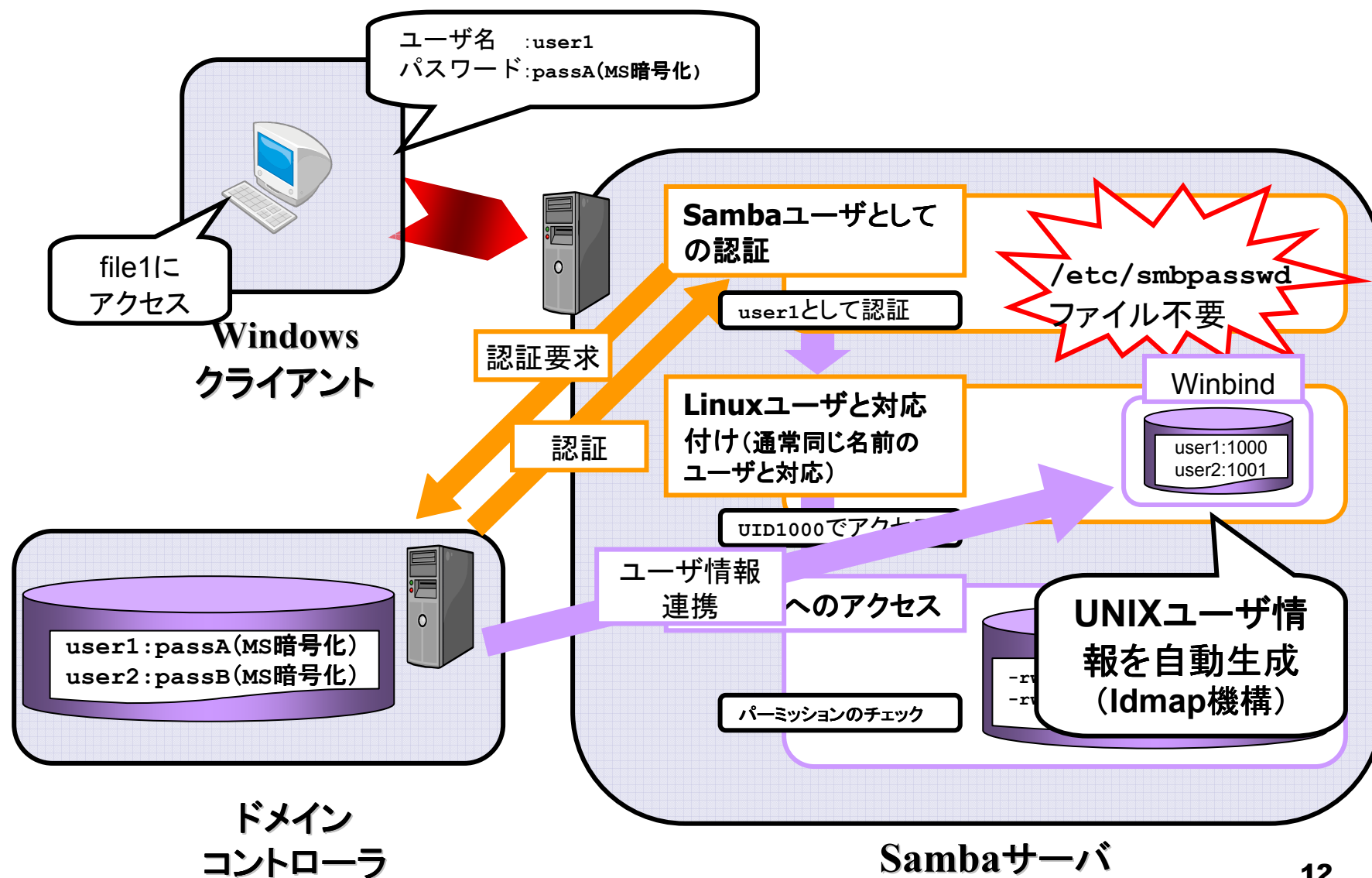
Winbind機構

- ユーザ認証だけでなく、ユーザやグループの情報もWindowsドメインから取得する機能
 - ユーザ認証を委任してもユーザ情報はSambaサーバで独自に持たないといけないのは不便
- 設定
 - smb.conf
 - NSSの設定
 - /etc/nsswitch.confファイルの修正
 - nss_winbindモジュールのインストール
 - PAMの設定 (Samba以外の認証も行う場合)
 - pam_winbindモジュールのインストール

Winbind機構なし(Windowsドメインで認証)



Winbind機構あり



自動生成されるユーザ、グループ名の設定

■ UNIX流儀に近い名前に変更できる

```
$ getent passwd 'W2K8AD1¥samba01'
W2K8AD1¥samba01:*:10001:10000::/home/W2K8AD1/samba01:/bin/false
```

□ デフォルトは「*Domain Name¥Username*」

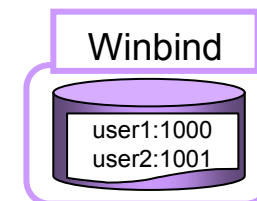
■ 「¥」が入るので、扱いが若干面倒

□ カスタマイズ例

■ *Domain Name_Username* ← 「¥」を「_」に変更

■ *domain_name¥username* ← すべて小文字 & 空白を「_」に変更

■ *Username* ← ユーザ名のみに変更



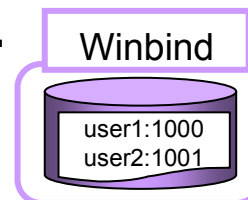
UNIXユーザ情
報を自動生成
(Idmap機構)

グループ名もこのカスタマイズの影響を受ける

自動生成されるユーザ情報の設定

■ ホームディレクトリ, シェルもカスタマイズ可

```
$ getent passwd 'W2K8AD1¥samba01'
W2K8AD1¥samba01:*:10001:10000:::/home/W2K8AD1/samba01:/bin/false
```



- デフォルトは「/home/DomainName/Username」
「/bin/false」

UNIXユーザ情報
を自動生成
(Idmap機構)

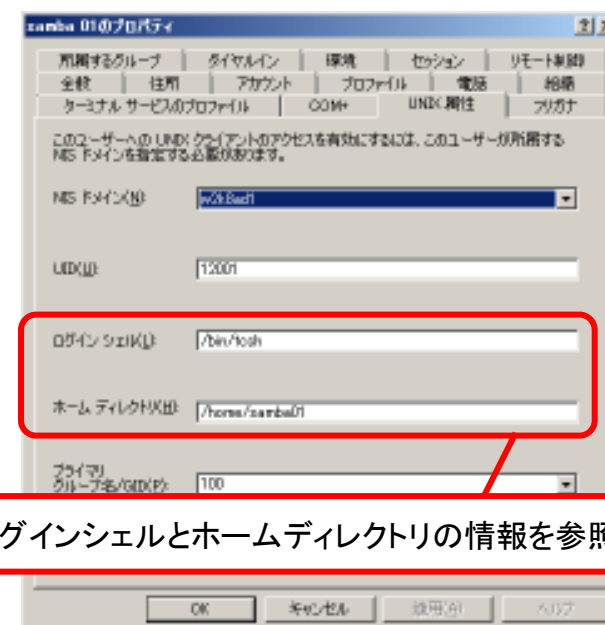
□ 変更の方式

■ 全ユーザー一律で変更

- template shell / template homedir
パラメータを使用

■ ユーザごとに変更

- Active DirectoryのUNIX属性にある
ログインシェル、ホームディレクトリ
値を参照させる



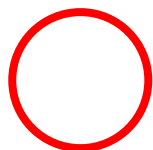
ユーザ、グループ名指定方法の注意

■ smb.confでの設定方法

□「*DOMAIN¥User*」形式で指定すること



```
[share]
valid users = +"Domain Users" +monyo
```



```
[share]
valid users = +"W2K8AD1¥Domain Users" +W2K8AD1¥monyo
```

※ドメイン名を指定しない場合は、UNIX上のグループ名を指定したとみなされる

自動生成されるグループのメンバ情報

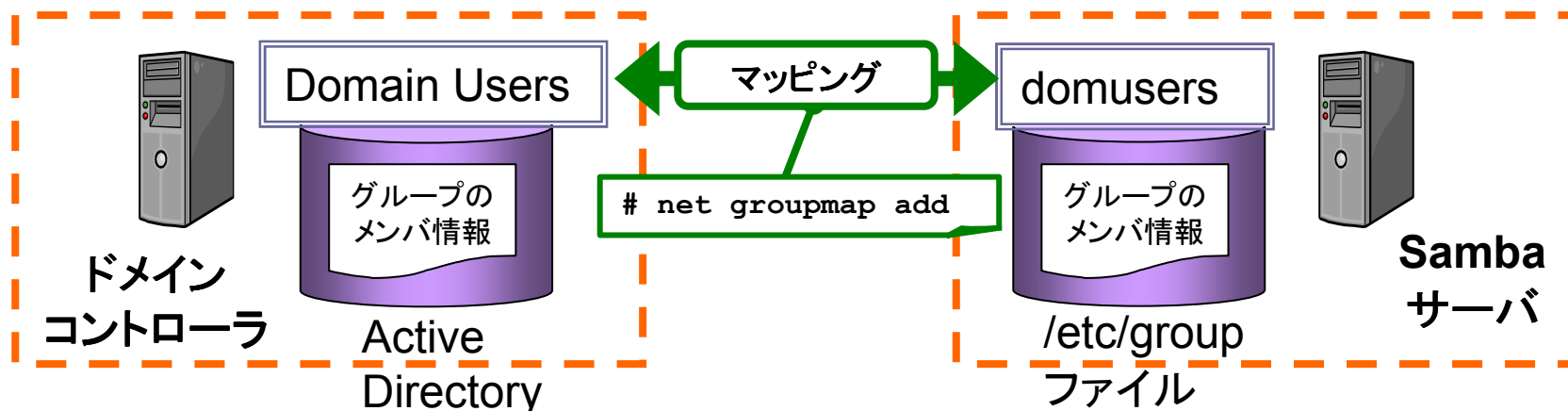
■ Winbind環境では/etc/groupを参照しない

```
$ getent group 'W2K8AD1¥Domain Users'
W2K8AD1¥Domain Users:x:10017: W2K8AD1¥ldap01,W2K8AD1¥ldap02, ...
```

- 非Winbind環境では/etc/groupファイルを参照
- Winbind環境

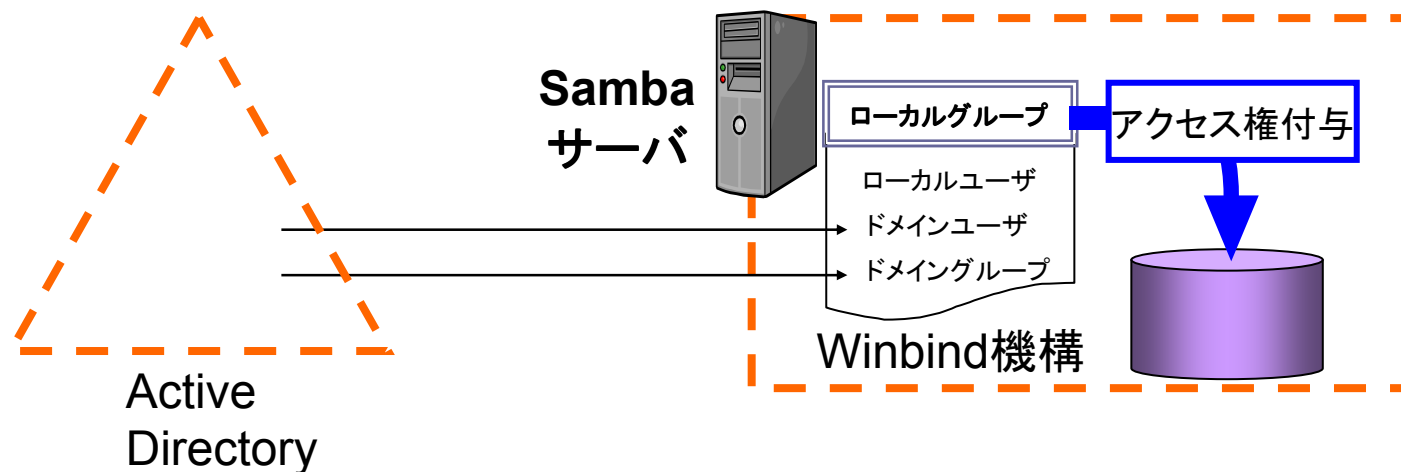
■ Windows上のマッピング元グループの設定

- UNIX側のグループ情報はGID以外使われない
- グローバルグループのネスティングにも対応



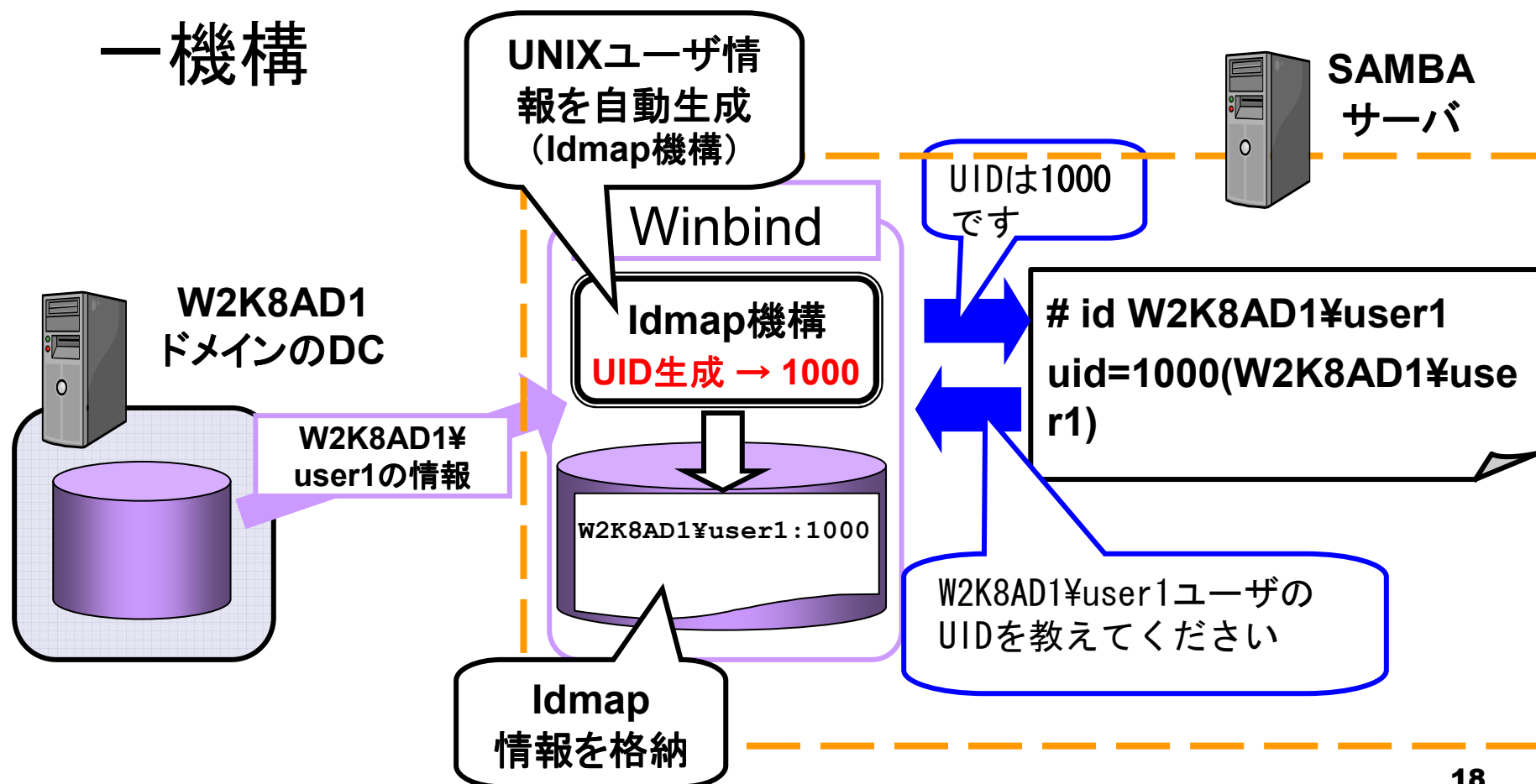
ローカルグループのサポート

- Winbind環境では、Windowsと同様のローカルグループもサポートされる
 - Sambaサーバ上のユーザに加え、ドメインのグローバルグループやユーザもメンバに追加できる
 - こちらも/etc/groupの情報は参照されない
 - メンバの追加、削除はWindowsから行うか、専用のコマンド(net sam / net groupmap)経由



Idmap機構

- 自動生成されるユーザにマップされるUIDやGIDを生成し、その情報を保持するWinbindの一機構



Idmap/バックエンド

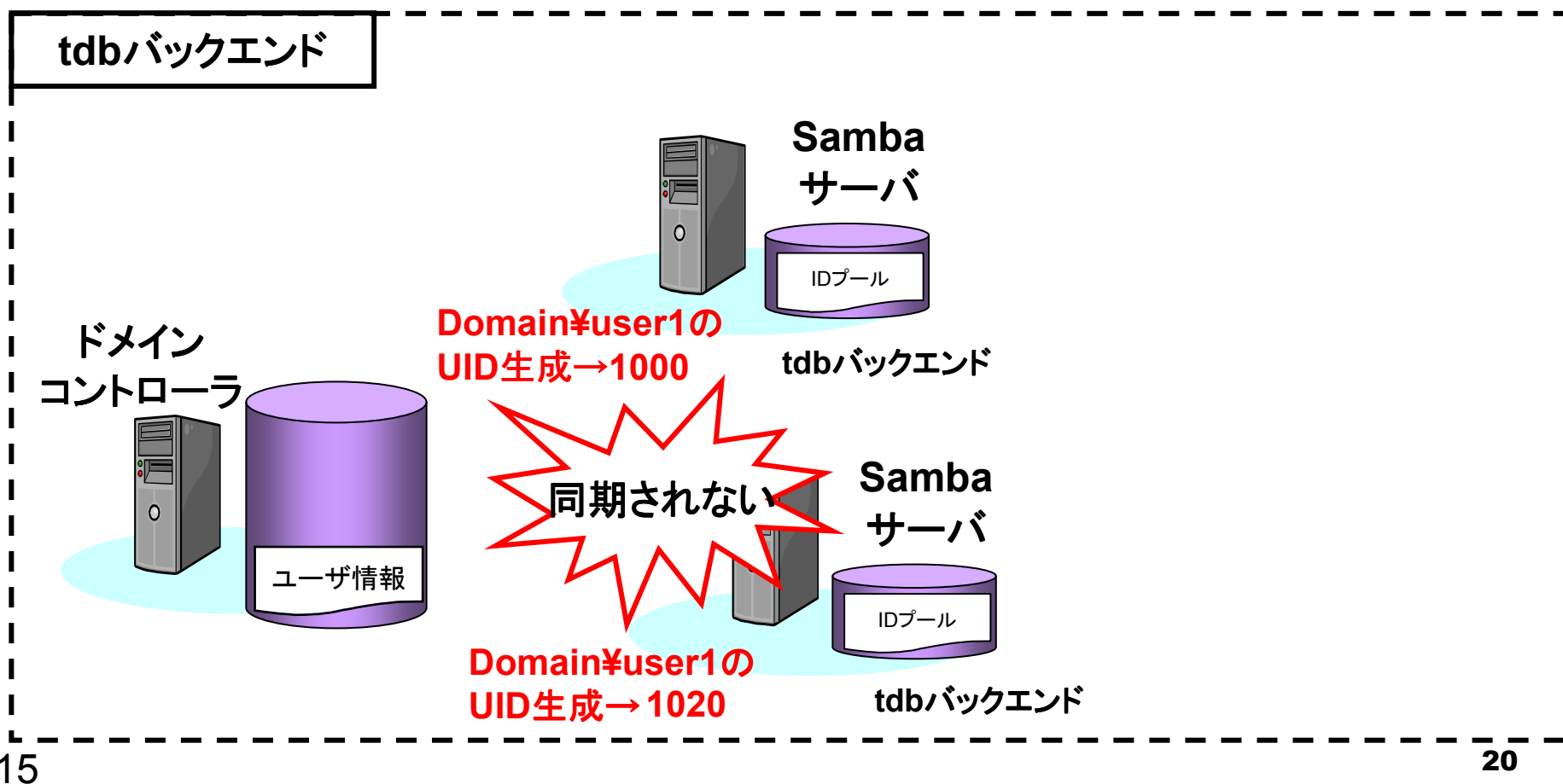
■ Idmap情報の生成、保持の方法は選択可能

□ tdbもしくはridがお勧め

名称	ID生成	格納場所	一元管理	概要
tdb	プールから 払い出し	TDB ファイル	各サーバごと	もっとも古い機構で、IDは未使用ID領域から順に生成される
ldap	プールから 払い出し	LDAP ディレクトリ	可能	TDBと同時期から存在する。ID格納場所をLDAPにすることで、複数サーバ間で生成したIDの一元管理可能な点が特徴
ad / (adex)	UNIX属性	AD	可能	Active DirectoryのUNIX属性に設定されたUID情報を用いる。LDAPサーバを立てることなく、IDの一元管理が可能
rid / autorid	計算式	(なし)	可能	Active Directoryの各ユーザ、グループに付与されているRID値から自動生成された値を用いる。IDの管理自体が不要
nss	/etc/passwdファイル		各サーバごと	/etc/passwdのUID情報をそのまま用いる。LDAPで認証統一している場合などに便利

Idmapバックエンド

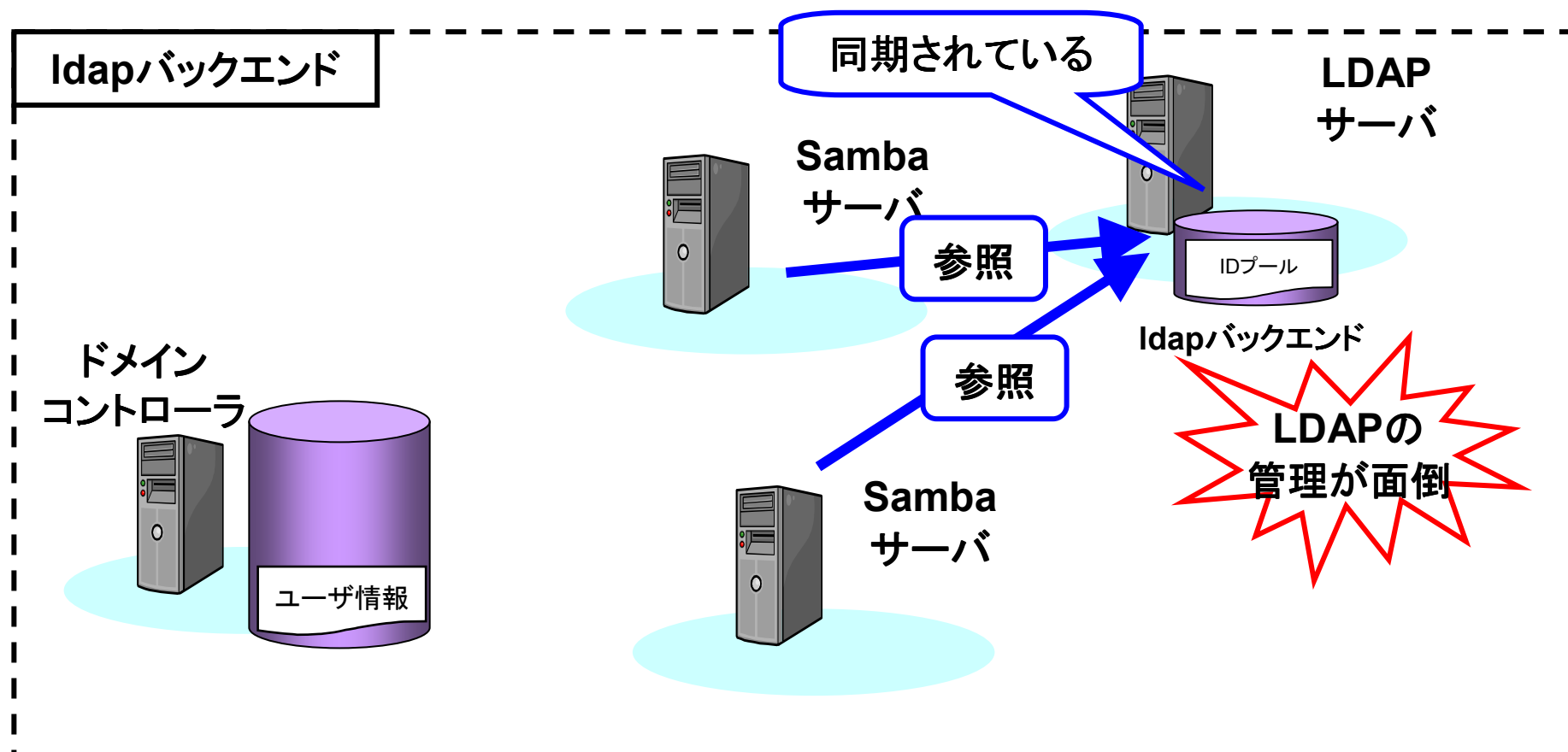
- Idmap情報の生成、保持の方法は選択可能
 - tdbもしくはridがお勧め



Idmapバックエンド

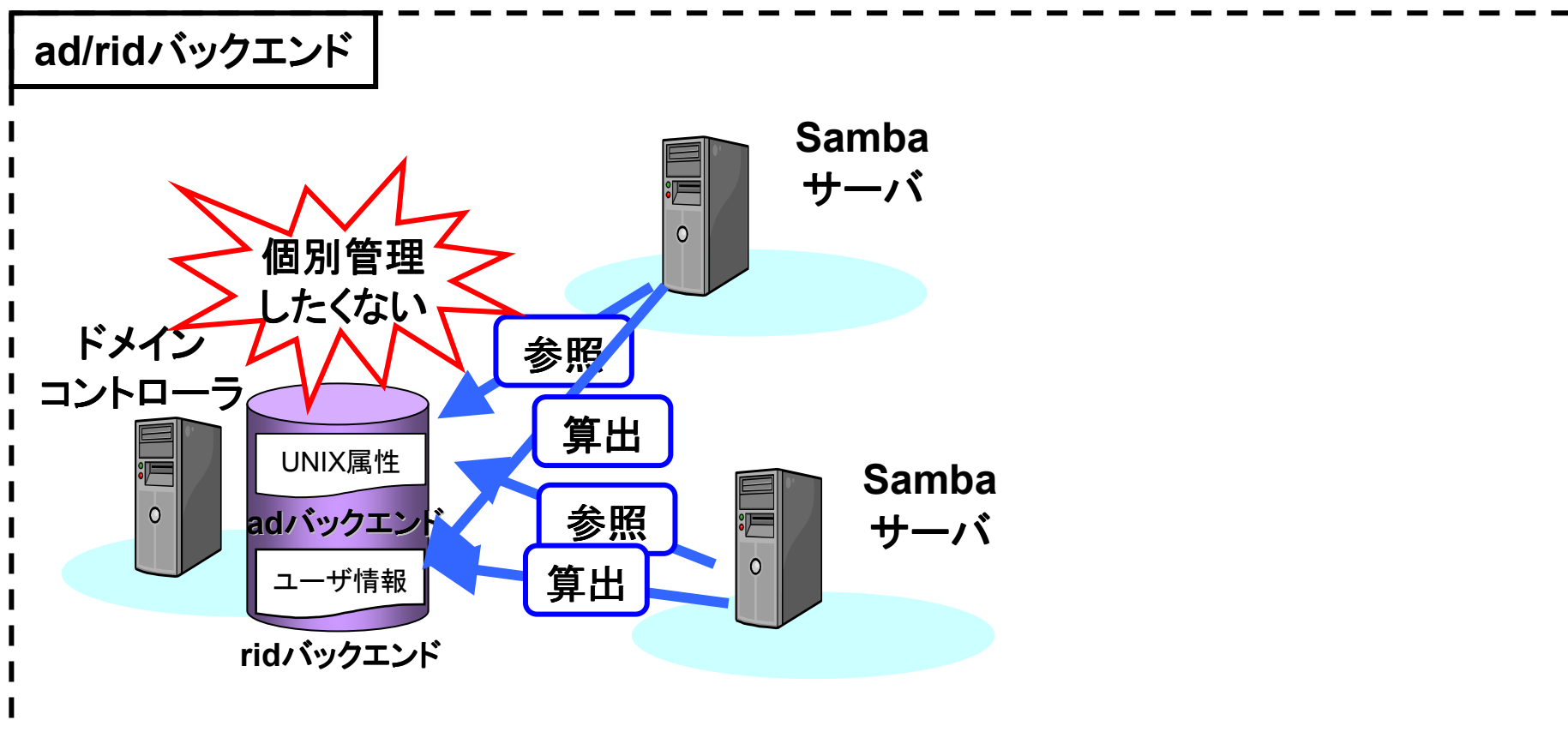
■ Idmap情報の生成、保持の方法は選択可能

□ tdbもしくはridがお勧め



Idmapバックエンド

- Idmap情報の生成、保持の方法は選択可能
 - tdbもしくはridがお勧め



Idmap機構の設定

■ バージョンによって設定方法が異なる

- Samba 3.0.24以前
 - 全ドメイン一律設定、比較的簡単
- Samba 3.0.25～3.2.X
 - ドメインごとにIdmap機構を設定可能、複雑
 - 複数Idmap機構間で払い出すIDの重複を防ぐ機構 (alloc backend機構) が導入、かなり複雑
- Samba 3.3.0～3.5.X
 - 3.0.24以前、以降両者の長所を組み合わせ。3.0.24以前の方法はデフォルト値として再定義。3.0.25以降の方法でドメインごとにも設定可能
- Samba 3.6.0以降
 - alloc backend機構が隠蔽 (Samba内部で暗黙的に機能する形に)
 - 3.0.24以前の設定方法は混乱を避けるため非推奨に。別途デフォルト値を設定する構文が追加

PAMによる認証のサポート

- pam_winbindにより各プロダクトを認証
 - SSHでのログイン時の認証をADのパスワードで行うなど
 - nss_winbind (Sambaの動作にも必要)と組み合わせて用いる

