「Samba逆引きリファレンス出版記念」

トラブルフリーのSamba設定教えます!!

日本Sambaユーザー会
2009/10/30
武田 保真

目次

- 講師紹介
- 壱: Samba導入前のポイント
- 弐: Samba運用前の設定のポイント
- TIPS
- Q&A

講師紹介：武田 保真

- 日本Sambaユーザー会/日本LDAPユーザー会所属
- オープンソース･ソリューション･テクノロジ株式会社
  - http://www.osstech.co.jp
  - 2001年頃より、Samba2.2日本語版の開発に携わる
  - 現在は業務でSambaの構築、サポート、修正などを行っている
- 著書
  - Samba逆引きリファレンス (秀和システム)
  - 徹底解説 Samba LDAPサーバー構築(技術評論社)
  - Linux RAID入門(技術評論社)
  - 逆引きUNIXコマンド(技術評論社)

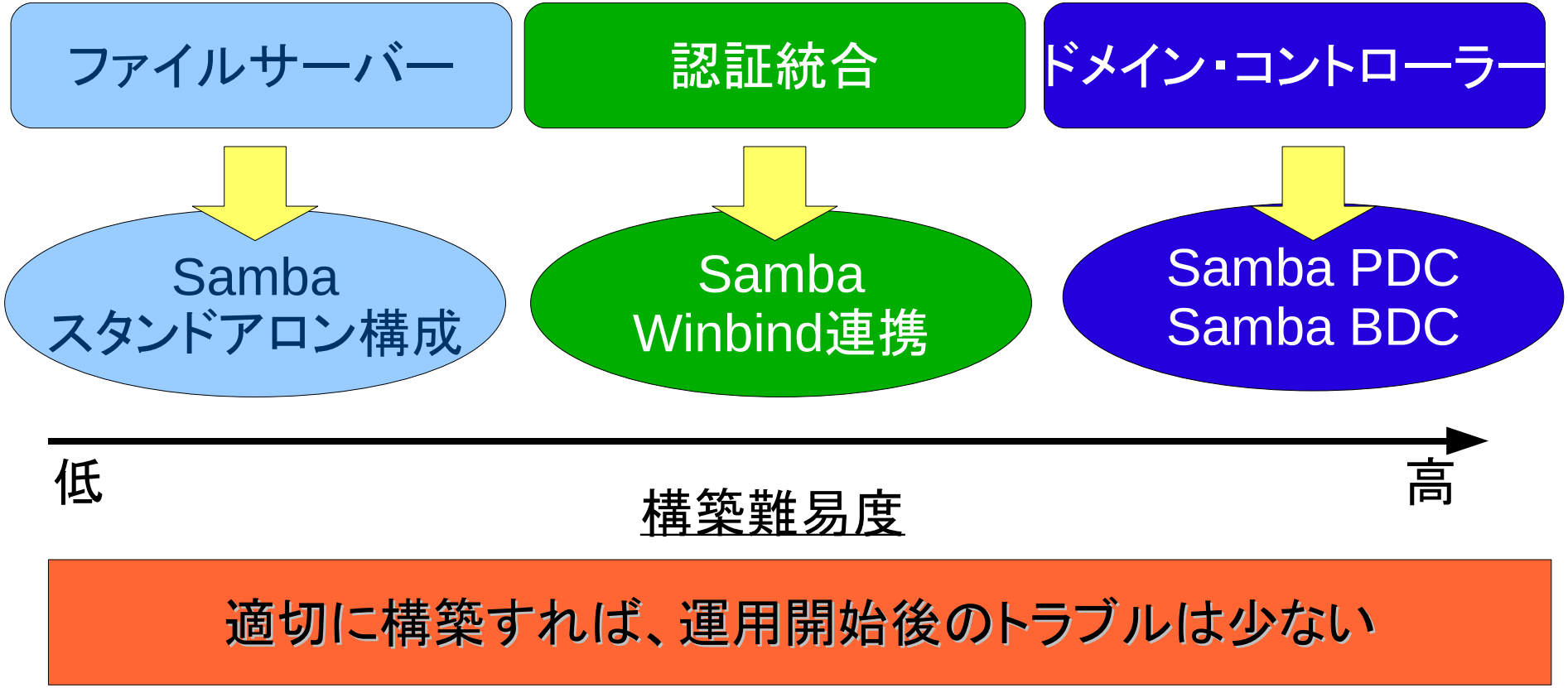
本セミナーの目的

- Sambaの設定ではまるポイントを知ってもらい、Sambaを活用してもらうための情報を提供します

壱: Samba導入前の検討ポイント

1. 構成の検討

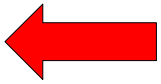
- 導入目的



2. ハードウェアの選択

- ハードウェア構成選択時の検討ポイント
  - 同時使用ユーザー数が増えると、必要なメモリが増える
    - deadtimeパラメーターでアイドルセッションは切断可能
    - Windowsクライアントはアクセスが発生すると自動で接続を回復
  - スタンドアロン構成
    - サーバー 1台 + ストレージ領域(内蔵HDD/外付けディスクなど)
  - Active Directoryメンバー構成(Winbind連携)
    - Active Directoryドメインコントローラーが複数台あれば冗長化可能
  - ドメイン・コントローラー構成
    - 最低でも PDC/BDCの2台構成、BDCは増やすことが可能
    - クラスタソフトと組み合わせて Active-Active構成の冗長化も可能

3. OSの選択

- 選択肢と注意点
  - Linux
    - ファイルシステムの制限値(Ext3)
      - 最大ファイルシステムサイズ 16TB、最大ファイルサイズ 2TB
  - Solaris10
    - ファイルシステムの制限値(ZFS)
      - 最大ファイルシステムサイズ 16エクサバイト、最大ファイルサイズ 16エクサバイト
      - Quota: Solaris10 U7(05/09)まではグループQuotaが利用できない
      - ACL: NFSv4互換ACL ... NTFS ACLとの親和性が高い
    - 所属グループ制限
      - 最大 32グループ  要注意
  - FreeBSD
    - すいません。使ったこと無いです。でもZFSと組み合わせるのは有りかも

4. Sambaのバージョンの選択

- Sambaのバージョンの選択基準は?
  - 一つ前のstableバージョンの最新がお勧め

Samba 3.4系	コードが頻繁に変更されるため、トラブルが多い
★ Samba 3.3系	3.4系のバグ修正がほぼ全てバックポートされる 最新の機能を利用可能
★ Samba 3.2系	大きなトラブルは残っていない 最新の機能への対応は別途バックポートが必要 Samba 3.3との機能的な違いはほとんど無い
Samba 3.0系	対応できない機能が増えてきた コードベースもかなり違うためバックポートは難しい

弐: Samba運用前の設定のポイント

ファイルサーバー構成

1. ファイルサーバー構成

- 全体設定

UTF-8-MAC対応のlibiconvが必要

unix charset	UTF-8を設定する。 Mac OS XからNFSを利用する場合 UTF-8-MAC
passdb backend	tdbsam/ldapsamを設定する。 パスワードポリシーが使えないのでsmbpasswdは使わない。
log level	通常運用時は 0 または 1。 3以上に設定すると、ログの書き出しによる性能劣化が顕著。
syslog	特別な要件が無い限り 0 を設定する。 syslogに追加で書き出す必要性は無い。

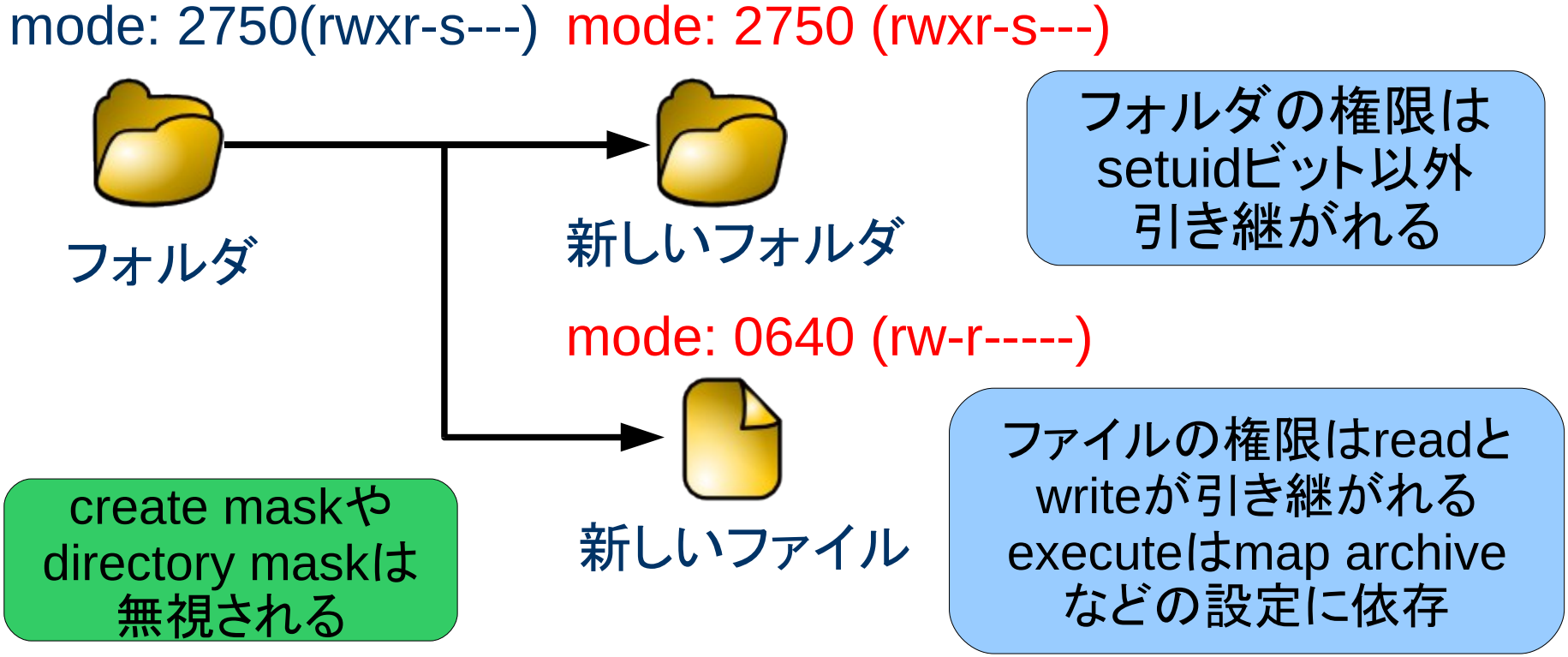
1-2. アクセス権の設定

- ファイルサーバー運用前のポイントはアクセス権の設定
  - グループ単位のアクセス権の管理が望ましい(運用が楽)
  - 共有フォルダの最上位に、デフォルトACLを設定して、下位フォルダは、ACLを引き継ぐ設定にする
  - 最上位のフォルダにはsetgidビットを設定しておく
- お勧め設定パラメーター

```
inherit permissions = yes
inherit acls = yes
store dos attributes = yes
dos filemode = yes
```

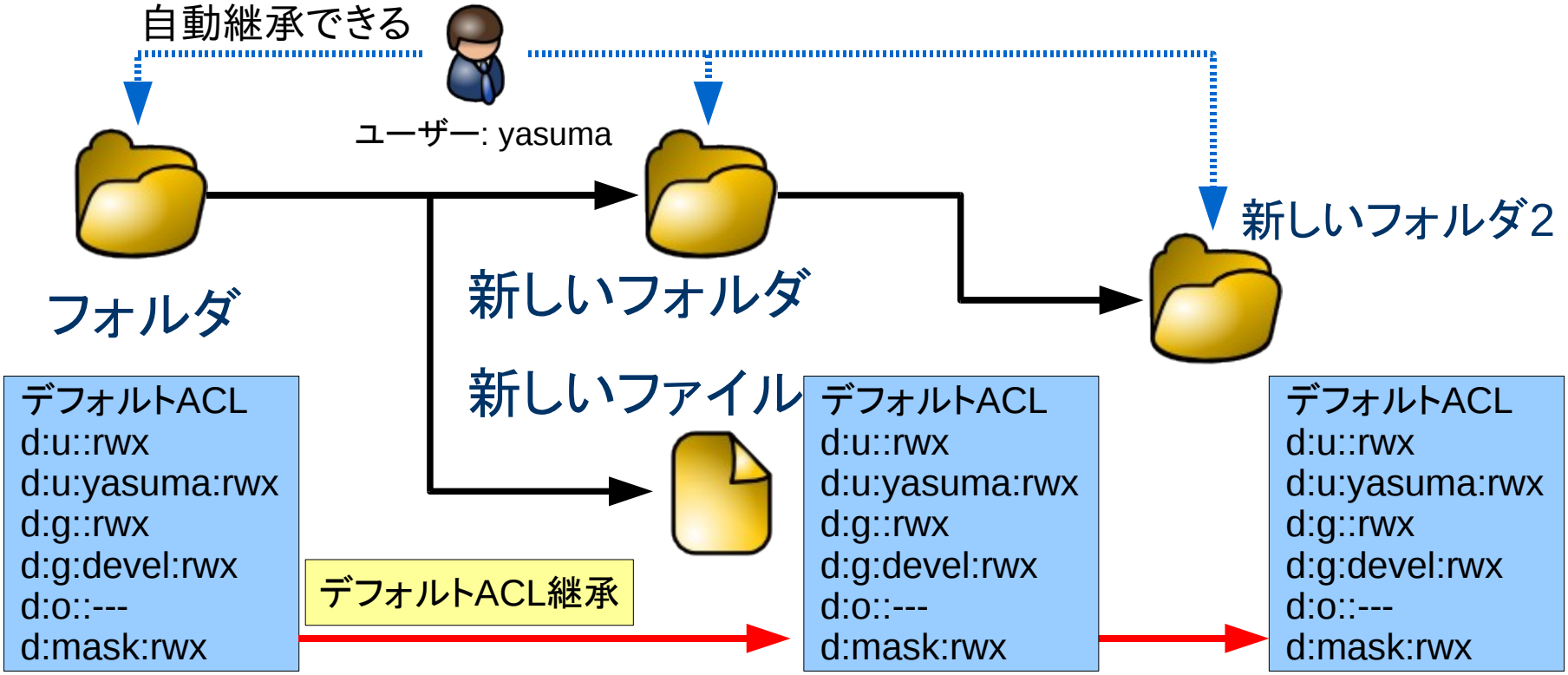
パラメーター詳細(inherit permissions)

- inherit permissions = yes (デフォルト値 no)
  - 新しくフォルダやファイルを作成するときに、上位のフォルダの権限を引き継ぐ
  - 所属グループ、Everyoneに対する読み込み、書き込み権の設定を自動で継承



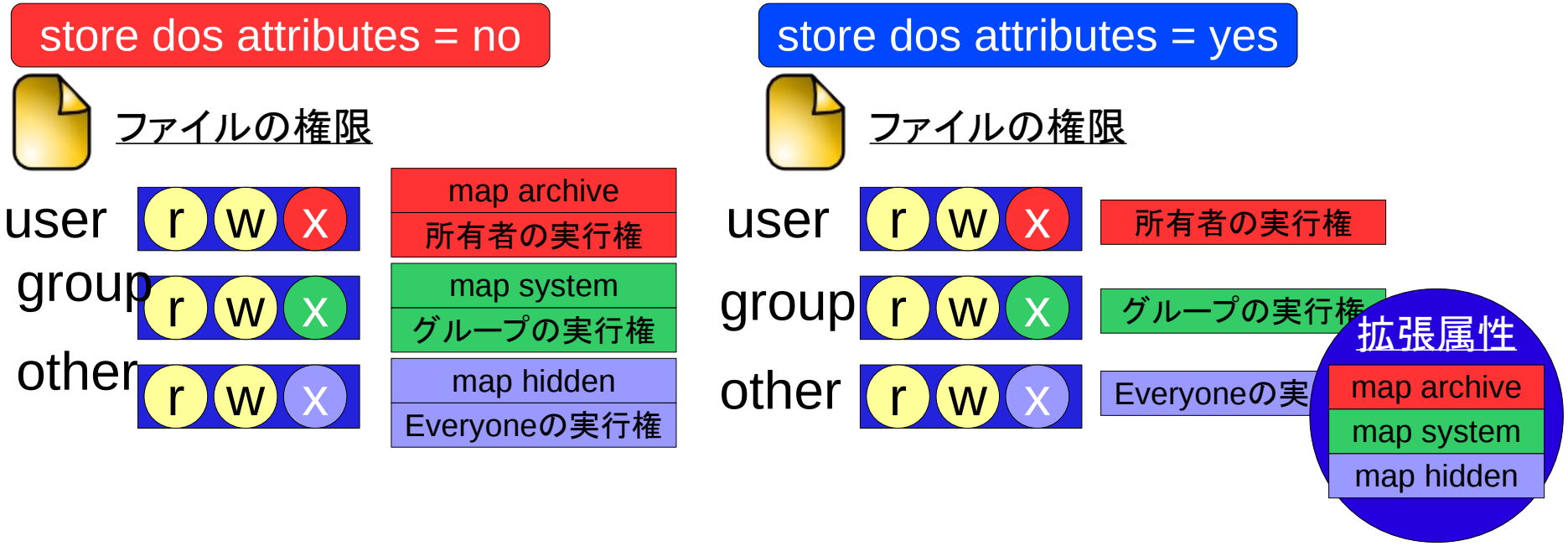
パラメーター詳細(inherit acls)

- inherit acls = yes (デフォルト値: no)
  - 新しくフォルダやファイルを作成するときに、上位フォルダに設定されたデフォルトACLを引き継ぐ
  - セカンダリグループや個々のユーザーのアクセス権を付与するときに、アクセス権を自動継承できる



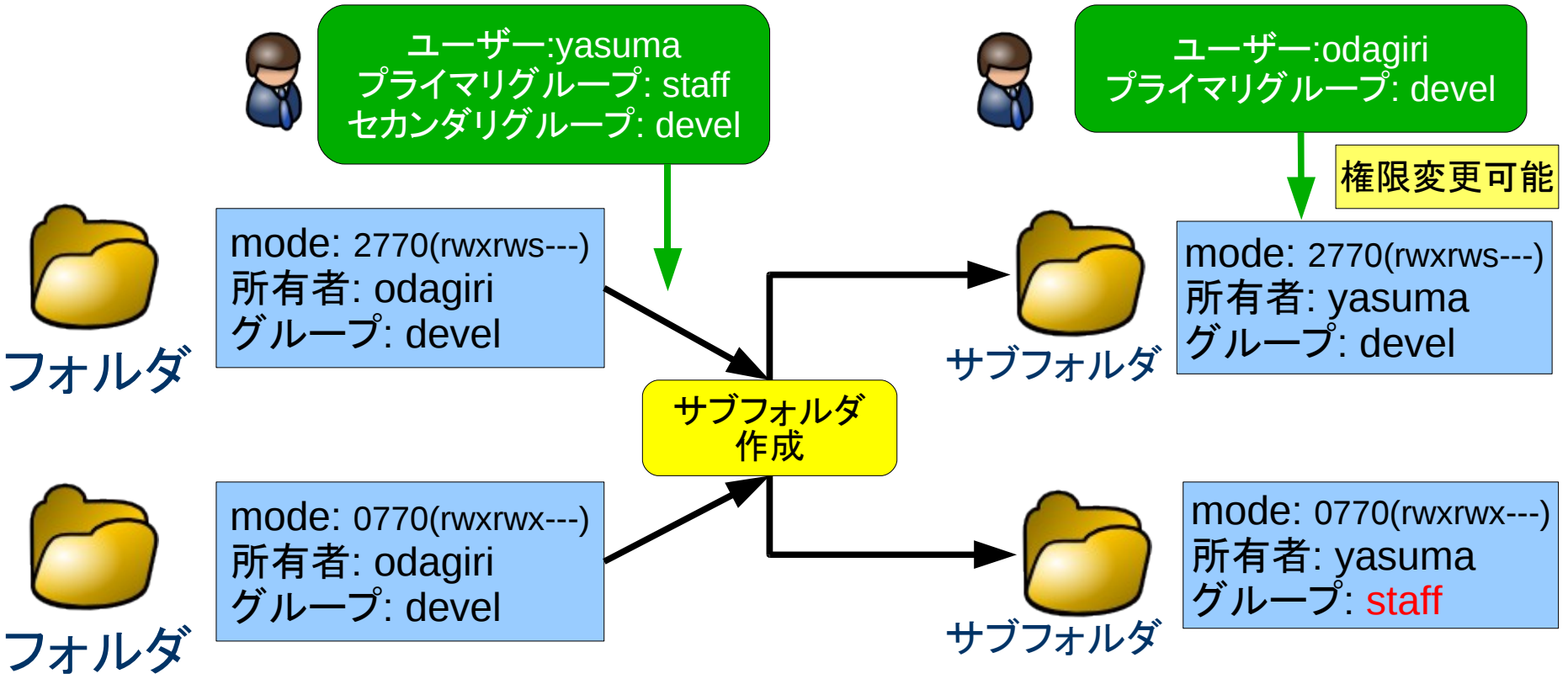
パラメーター詳細(store dos attributes)

- store dos attributes = yes (デフォルト値: no)
  - システム属性や隠しファイル属性をファイルシステムの拡張属性に記録
  - map hidden/map system/map archiveの代わりとなるので、ファイル・フォルダの実行ビットを共用しなくてよい
  - ファイルシステムが拡張属性に対応している必要あり



パラメーター詳細(dos filemode)

- dos filemode = yes (デフォルト値: no)
  - ファイル・フォルダの権限の変更を、ファイルの所有者だけでなく、グループの更新権を持つユーザーにも許可
  - フォルダのsetgidビットと組み合わせてフォルダの更新権をグループ単位で制御



Active Directory
メンバーサーバー構成

2. Active Directoryメンバー構成(winbind)

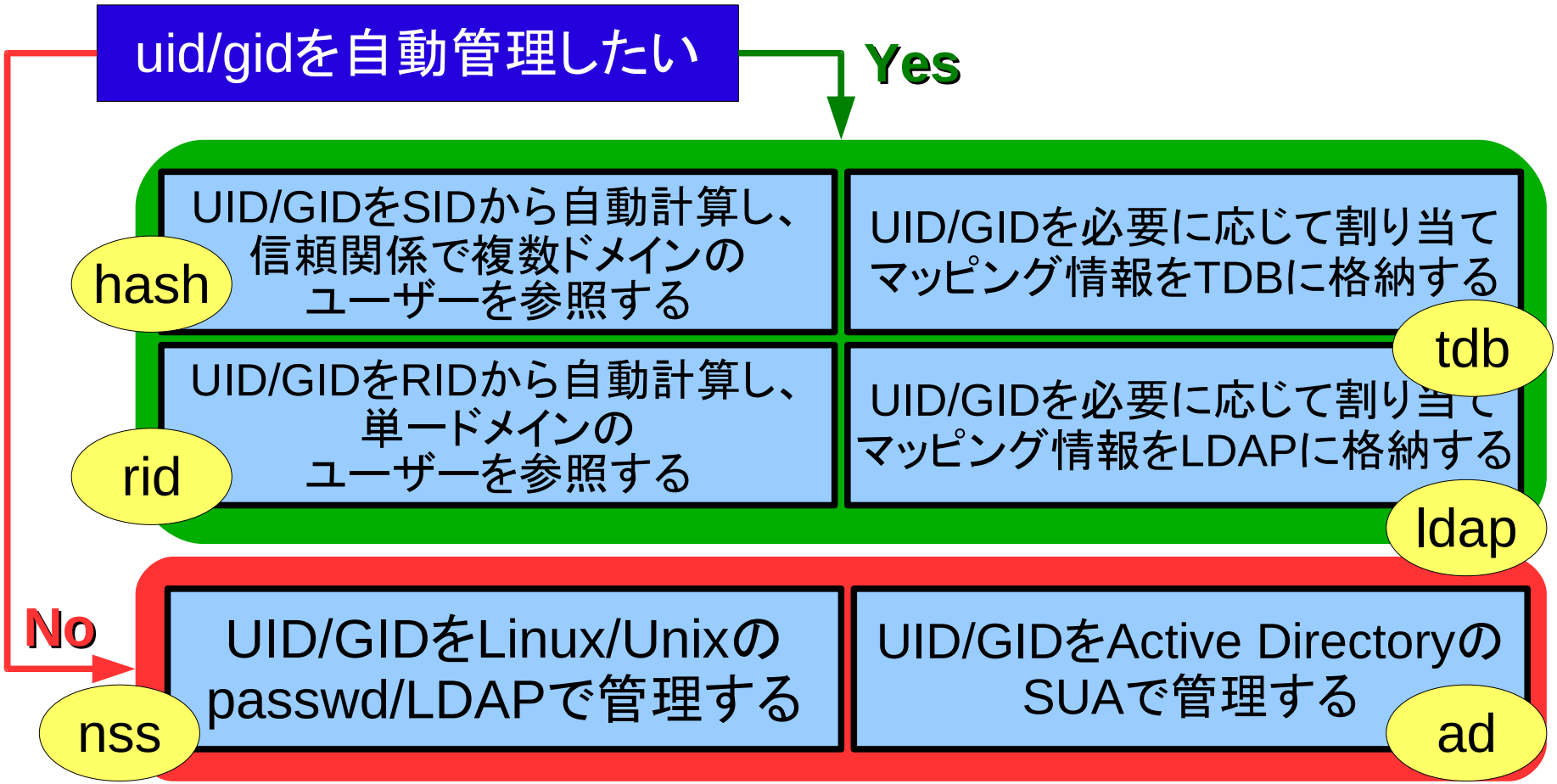
- Active Directoryのユーザー情報をLinux/Unixで参照
- 複数台のドメインコントローラーに対して冗長設定可能

基本設定

workgroup	Active Directoryの短いドメイン名
realm	Active Directoryのフルドメイン名(大文字)
password server	ドメインコントローラーのIPアドレス 複数台ある場合は、複数記載
security	「ads」を記載

2-1. winbindの設定

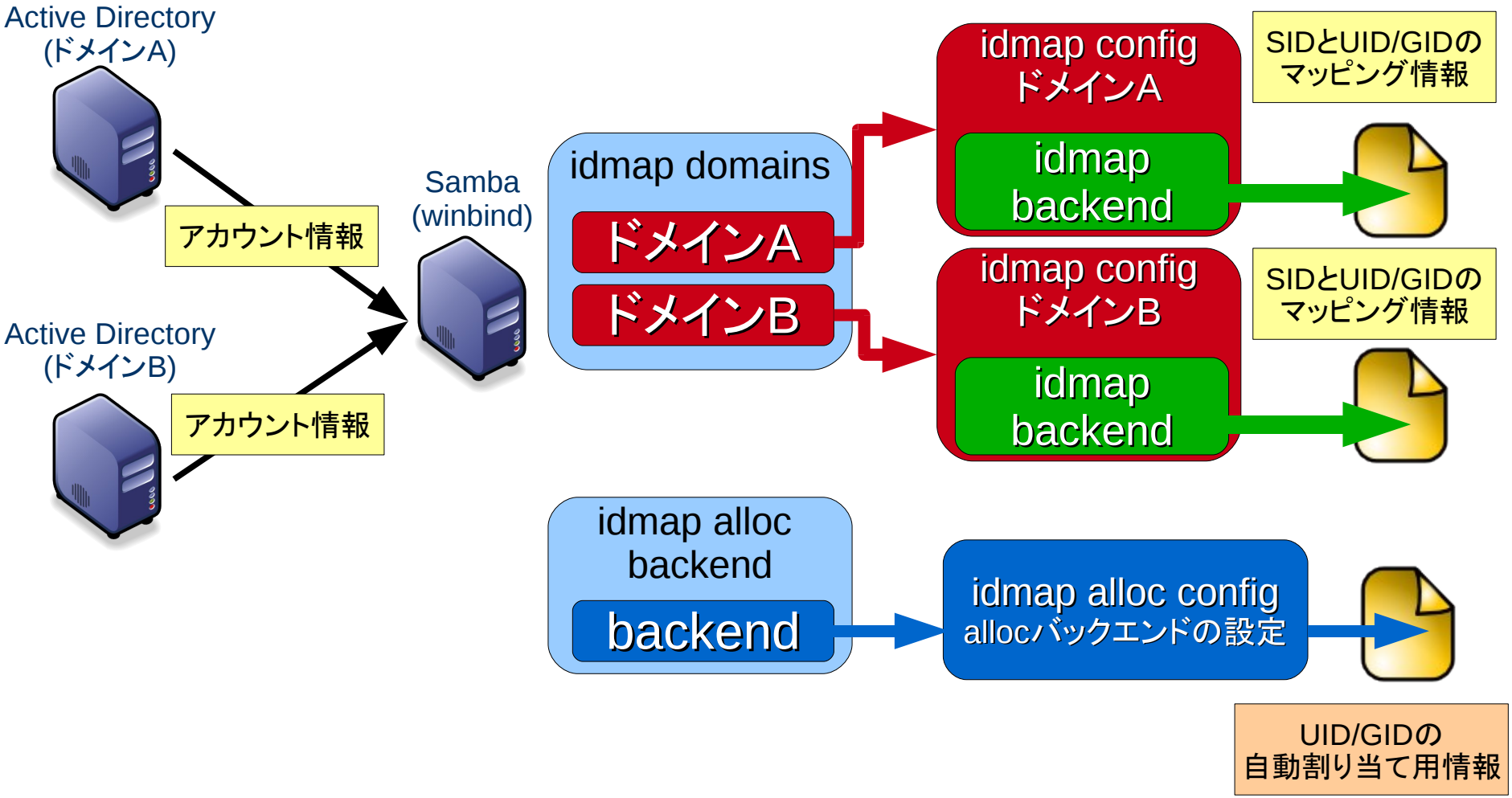
- idmapバックエンドの選択



idmapバックエンドの設定概念(3.0.25～3.2)

idmap domains	winbindで参照するドメインのリスト
idmap config	ドメインごとのUID/GIDの割り当て方法の設定
idmap alloc backend	UID/GIDの自動割り当てに利用する情報の格納方法 * idmap_ad、idmap_nss、idmap_hash、idmap_ridには不要
idmap alloc config (オプション)	UID/GIDの自動割り当てに関する全体設定 * idmap alloc backendと関連

idmapバックエンドの概念図



idmapバックエンドの設定概念(3.3～3.4)

idmap backend	winbindでデフォルトで使用するbackend
idmap uid	winbindで自動で割り当てるUIDの範囲
idmap gid	winbindで自動で割り当てるGIDの範囲
idmap config (オプション)	ドメインごとのUID/GIDの割り当て方法の設定
idmap alloc backend (オプション)	UID/GIDの自動割り当てに利用する情報の格納方法
idmap alloc config (オプション)	UID/GIDの自動割り当てに関する全体設定

IDMAPバックエンド: idmap_tdb

- デフォルトのバックエンド
- ADのSIDとUID/GIDのマッピングをTDBファイルに保存
  - TDBファイルが失われるとマッピング情報が不明になる
  - 複数のSambaサーバー間でマッピングを共有できない

[設定例(Samba 3.3以降)]
idmap backend = tdb (省略可能)
idmap uid = 10000 - 200000
idmap gid = 10000 - 200000

IDMAPバックエンド: idmap_ldap

- ADのSIDとUID/GIDのマッピングをLDAPに保存
  - 複数のSambaサーバー間でマッピングを共有可能
- LDAPへ適切に格納するための指定が複雑

[設定例(Samba 3.3以降)]
ldap suffix = dc=example,dc=com
ldap idmap suffix = ou=Idmap
ldap ssl = no
ldap admin dn = cn=Manager,dc=example,dc=com
idmap backend = ldap:ldap://localhost/
idmap uid = 10000 - 200000
idmap gid = 10000 - 200000
idmap alloc backend = ldap
idmap alloc config: ldap_url = ldap://localhost
idmap alloc config: ldap_base_dn = ou=Idmap,dc=example,dc=com

IDMAPバックエンド: idmap_rid

- ADのユーザー・グループのRIDから、UID/GIDを計算
  - UID/GID = RID - BASE_RID + (rangeの最小値)
- idmap alloc backend不要
  - IDは全て計算で算出されるので、IDのマッピングは不変
- 複数ドメイン利用時は、UID/GIDが重ならないようにrangeを分ける必要あり

```
[設定例(Samba 3.3以降)]
idmap backend = rid
idmap uid = 10000 - 20000
idmap gid = 10000 - 20000
```

IDMAPバックエンド: idmap_hash

- ADのユーザー・グループのSIDから、UID/GIDをハッシュで計算
  - 32bitの数値のUIDに変換されるので、数値で扱うのは大変
- idmap alloc backend不要
  - IDは全て計算で算出されるので、IDのマッピングは不変
- 複数ドメイン利用時もIDが重ならない

```
[設定例(Samba 3.3以降)]
idmap backend = hash
idmap uid = 10000 - 4000000000
idmap gid = 10000 - 4000000000
```

IDMAPバックエンド：idmap_ad

- Active DirectoryのSUA機能を利用している環境用
  - ADのユーザーのuidNumber、gidNumberを参照
  - ユーザーの所属するプライマリグループにgidNumberが設定されていないと、そのユーザーの利用不可

[設定例(Samba 3.3以降)]
idmap backend = tdb (省略可能)
idmap uid = 10000 - 200000
idmap gid = 10000 - 200000
idmap config WIN2008: backend = ad
idmap config WIN2008: range = 10000- 99999
idmap config WIN2008: schema_mode = rfc2307

IDMAPバックエンド: idmap_nss

- UID/GIDはOSに登録済みの情報を利用する環境用
  - /etc/passwdや、LDAP認証などで、ADとLinux/Unixの双方のOSに同じユーザー情報がある場合
  - winbindはADのSIDとUID/GIDをユーザー名でマッピング

[設定例(Samba 3.3以降)]
idmap backend = tdb (省略可能)
idmap uid = 10000 - 200000
idmap gid = 10000 - 200000
idmap config WIN2008: backend = nss
idmap config WIN2008: range = 10000- 99999

Kerberosの設定(krb5.conf)

- 基本設定項目

default_realm	Active Directoryのドメイン名を「大文字」で設定
kdc	Kerberos認証に利用するためのドメイン・コントローラーを設定 複数のドメイン・コントローラーを利用可能な場合は複数設定
domain_realms	DNSとレルム名のマッピングを指定 左辺がDNS名、右辺がレルム名(大文字)

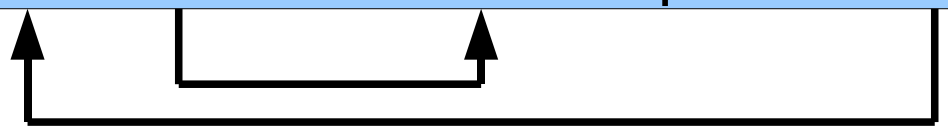
- 設定時の注意
  - 信頼関係を結んでいるADドメインがある場合は、信頼関係先のドメインに関するレルムも設定

DNS/ホスト名の設定

- Active DirectoryのDNSを参照するための/etc/resolv.conf設定
  - ADのDNSに登録されている各種SRVレコードが動作に必要
- net ads join時に次の名前解決処理ができる必要あり
  - ホスト名 → IPアドレスの変換
  - IPアドレス→ FQDNの変換

/etc/hostsの設定例(Sambaサーバー : fs1)

192.168.0.10　fs1.example.com fs1



時刻合わせ

- Kerberos認証は時刻合わせが大事
  - ドメインコントローラーと、Sambaサーバー間の時刻がずれるとドメイン参加に失敗したり、認証に失敗したりする
- net ads infoコマンドで時刻差を確認
- ntpなどで時刻合わせを実施
  - net time setでドメインコントローラーの時刻をSambaサーバーに設定可能

```
# net ads info
... 省略 ...
KDC Server: 192.168.10.1
Server time offset: 13
```

```
# net time set
2009年 10月 23日 金曜日 18:15:32 JST
```

ドメイン・コントローラー構成

OpenLDAPサーバー構築時の注意

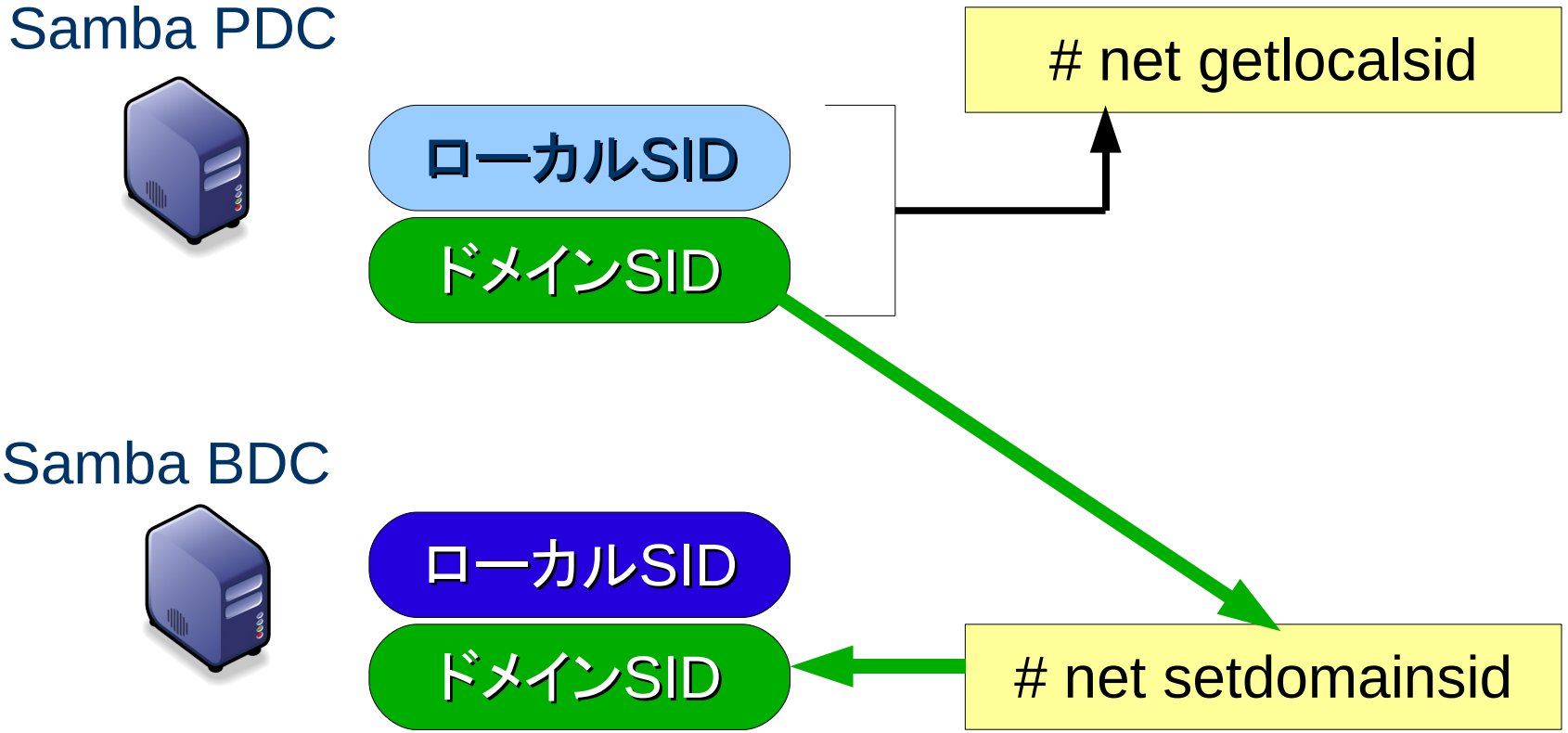
- loglevelの設定に注意
  - OpenLDAPのログは、デバッグ用途に実装されているため、非常に負荷が高い
  - 環境によっては、Sambaからの検索処理が一定時間内に得られないことがある
    - smb.confのldap timeoutで、タイムアウト時間を伸ばすことが可能
- アクセス権の設定
  - 一般ユーザー権限には次の属性の読み取りを禁止
    - userPassword、sambaLMPassword、sambaNTPassword、sambaPasswordHistory
- スレーブサーバーの設定
  - updaterefの設定を忘れない

smb.confの設定時の注意

- LDAPサーバーを冗長化している場合、次の設定も冗長化しておく
  - smb.confのpassdb backend
  - /etc/ldap.confのhost(もしくはuri)
- LDAPサーバーとのSSL接続設定
  - Samba 3.3からldap sslのデフォルト値が「start tls」に変更

ローカルSIDとドメインSID

- Sambaのドメインコントローラーでの SID
  - ドメインSIDは共通、ローカルSIDは異なる



smbldap-tools設定の注意

- Samba 3.0.25以降のパスワードポリシーに一部対応していない
  - -Bオプションの「次回ログオン時のパスワード変更」が設定できない
- smbldap-passwdコマンドで設定したパスワードの有効期限は45日
  - defaultMaxPasswordAgeの設定を削除
- デフォルトで移動プロファイルが有効
  - sambaProfilePathの設定が不要なら、smbldap.confからuserProfileをコメントアウト

Windows 7/2008R2のドメイン参加

- Samba 3.2.12/Samba 3.3.5以降必須
  - ドメイン参加時に「DNSのプライマリサフィックスが見つかりません」エラーが表示される、が無視して良い...多分
  - Samba 3.0.36以降で、一応ドメイン参加は可能(注)
- レジストリに以下の値を追加
  - HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManWorkstation\Parameters
    - DWORD(32bit)形式 DNSNameResolutionRequired = 0
    - DWORD(32bit)形式 DomainCompatibilityMode = 1
- Samba 3.0.36の場合、以下の変更も必要
  - HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters
    - RequireSignOrSeal = 0
    - RequireStrongKey = 0

TIPS

- 特定のクライアントのログだけ取得
  - include文を活用

/etc/samba/smb.confファイル

```
[global]
... 省略 ...
include = /etc/samba/%m.conf
```

include文を
入れる場所に注意

/etc/samba/[コンピューター名].confファイル

```
log level = 5
max log size = 10000
```

コンピューター名は
小文字

最近のトラブル

- Guestアカウントを削除 → smbdが起動不可
  - guest accountパラメーターに指定したUNIXアカウントは必須
- NetAppがSamba 3.2ドメインコントローラーにドメイン参加不可
  - Samba 3.2のバグ。Samba 3.2.9以降で修正済み

Q & A