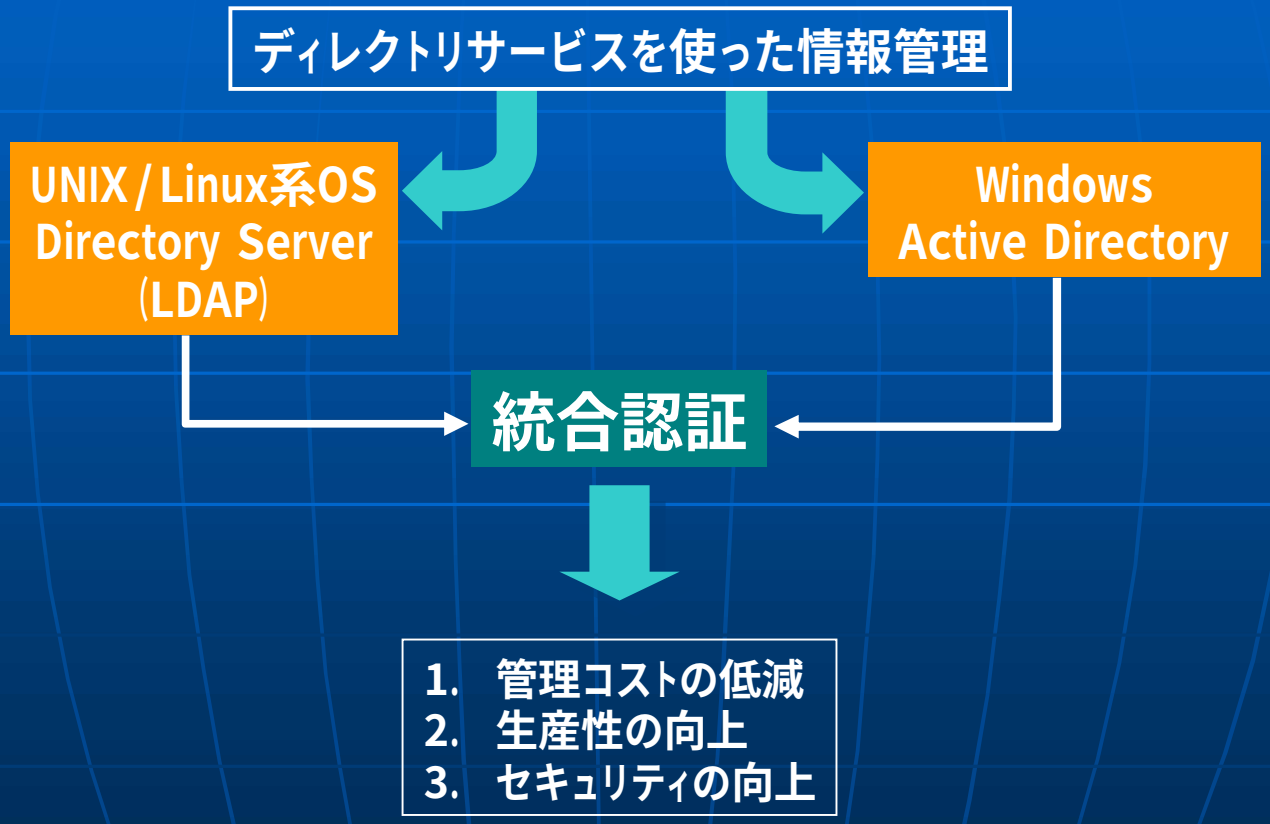
UNIX - Windows統合認証

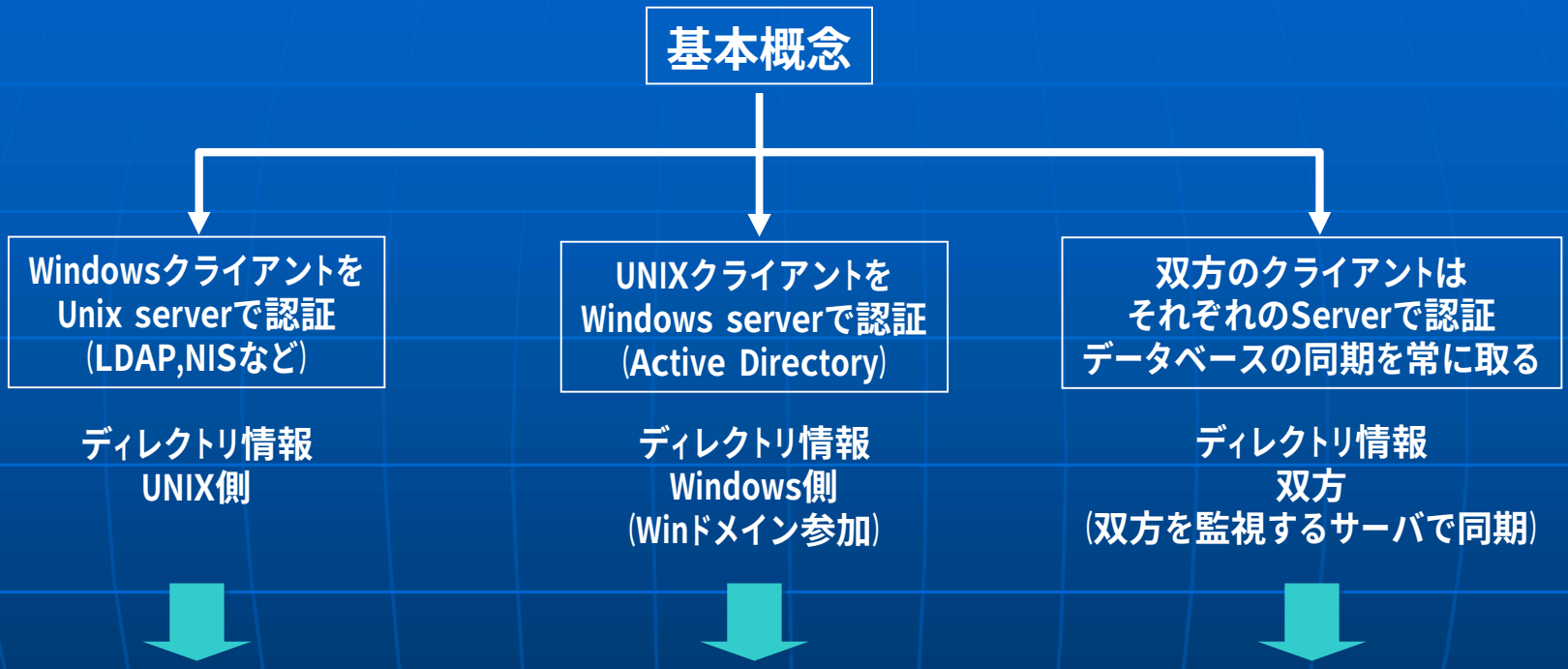
名古屋大学情報連携基盤センター
葛生和人

第3回東海地区CSI報告会
2006年12月15日 (金) 名古屋大学情報連携基盤センター

アカウント情報，個人情報の管理



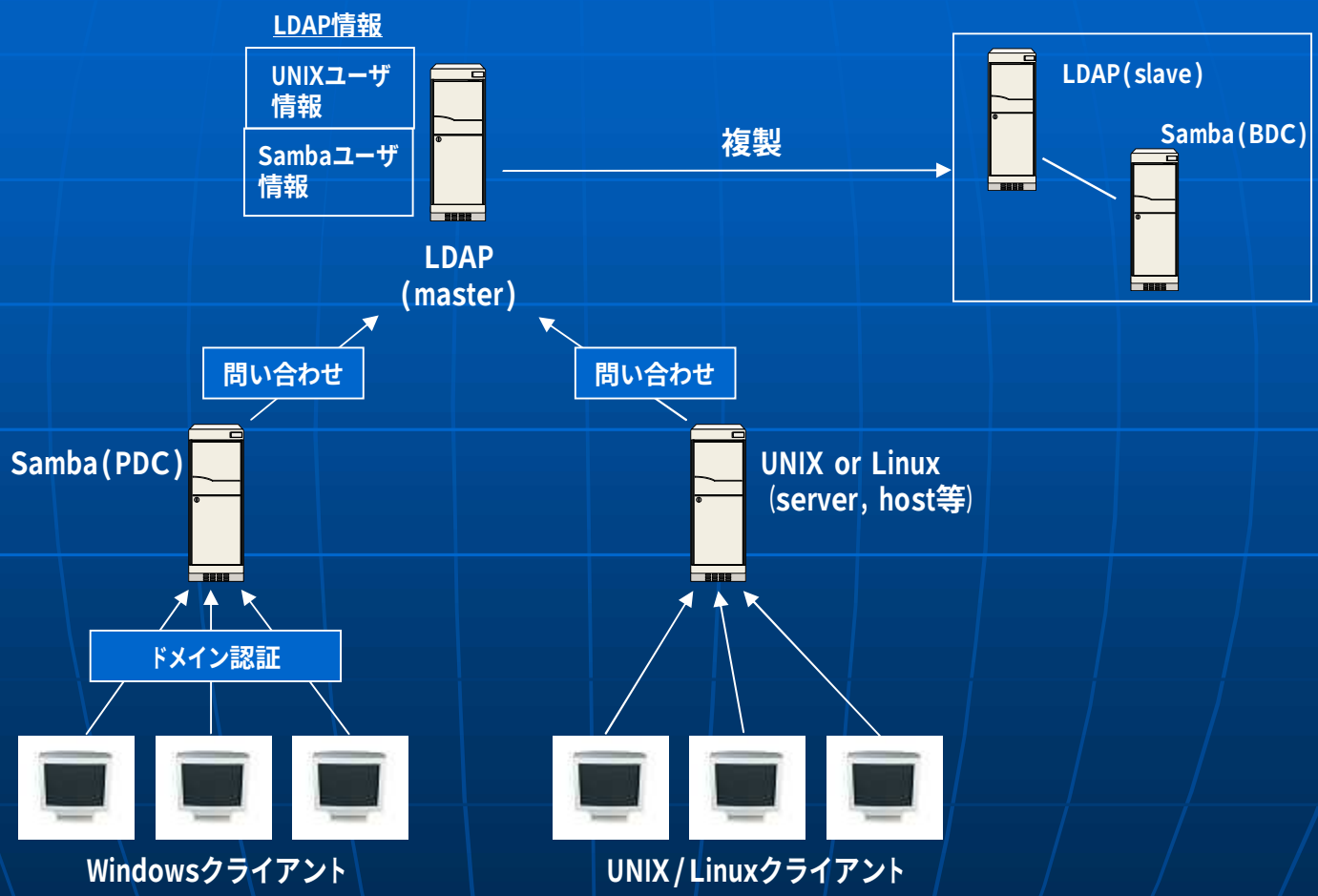
統合認証へのアプローチ



Samba - LDAP連携

WindowsクライアントをUnix Serverで認証

Samba - LDAP連携のためのシステム構成



Samba - LDAP連携

WindowsクライアントをUnix Serverで認証

Samba - LDAP連携のためのシステム構築

Sambaドメインの構築

PDCとしてSambaを起動：smb.conf（ドメイン設定）

↓

クライアントマシンアカウントの作成，登録

↓

Windowsクライアントのドメイン参加　- Windowsメニューより -

Samba - LDAP連携設定

OS - LDAP連携設定（nss,pam）　authconfig

↓

Samba用ldap設定：slapd.conf
samba schema追加
LDAPアクセス制限追加

↓

LDAP管理者pwのSambaへの登録

Samba - LDAP連携

Windowsクライアント をUnix Serverで認証

Samba - LDAP連携のためのシステム構築（続き）

Samba - LDAP連携支援ツールの設定
（smbldap - tools）

smbldap_conf.pm 設定

SID, suffix, usersou, computersou, groupsou, ...

```
#   net getlocalsid
SID for domain SAMBA30 is : S-1-5-21-1894714753-225945833-1167789036
```

Samba用LDAPサーバ初期情報の登録

WidowsでWell knownとして扱われているユーザ＆グループ情報を投入
（新規エントリの追加）

```
#   /usr/local/sbin/smbldap-populate.pl
Using builtin directory structure
adding new entry : dc=domain,dc=com
adding new entry : ou=People,dc=domain,dc=com
.....
```

初期登録されたAdministratorにPWを設定

```
#   smbldap-passwd.pl Administrator
Changing password for Administrator
.....
```

Samba - LDAP連携

Windowsクライアント をUnix Serverで認証

Acrive Directory情報のNTドメインからの移行

Samba 3.0に含まれる　net vampire 機能を利用 (一括移行)

移行可	ユーザ情報 グループ情報 マシンアカウント情報
移行不可	グループポリシー ケルベロス認証

Samba - LDAP連携

Windowsクライアント をUnix Serverで認証

Acrive Directory情報のNTドメインからの移行 (続き)

SambaをBDCとしてWindowsドメインに参加させる

BDC用にsmb.conf設定 (ドメイン設定)

↓

BDCとしてSambaを起動 しNTドメインに参加させる.

```
#   net rpc join -S TESTSV
Joined domain NTDOM
```

↓

ドメインコントローラの情報 (ユーザアカウント, グループアカウント, マシンアカウントなど) をSambaサーバに複製

```
#   net rpc vampire -S TESTSV -U administrator%password
```

SambaをPDCとしてLDAPと連携

Windows側サーバの停止

↓

PDC用にsmb.conf設定 (ドメイン設定)

↓

PDCとしてSambaを再起動

GINA - LDAP連携

Windowsクライアントを Unix Serverで認証

GINA（Graphical Identification aNd Authentification）

- WINLOGON.exeが持つログオン管理機能を拡張
- Windows起動時にユーザIDとパスワードを得て認証

GINA実行シーケンス

Windows起動時よりシャットダウンまで

WlxNegotiate ・・・GINA.dllの開始
↓
WlxInitialize
↓
WlxDisplaySASNotice ・・・[Ctl]+[Alt]+[Del]を待つダイアログボックス
↓
WlxLoggedOutSAS・・・ログオン情報ダイアログボックス → LDAPへの問い合わせ
⋮
WlxLogoff
↓
WlxShutdown

ログオン機能拡張を利用してLDAPへのバインド，問い合わせ処理を追加

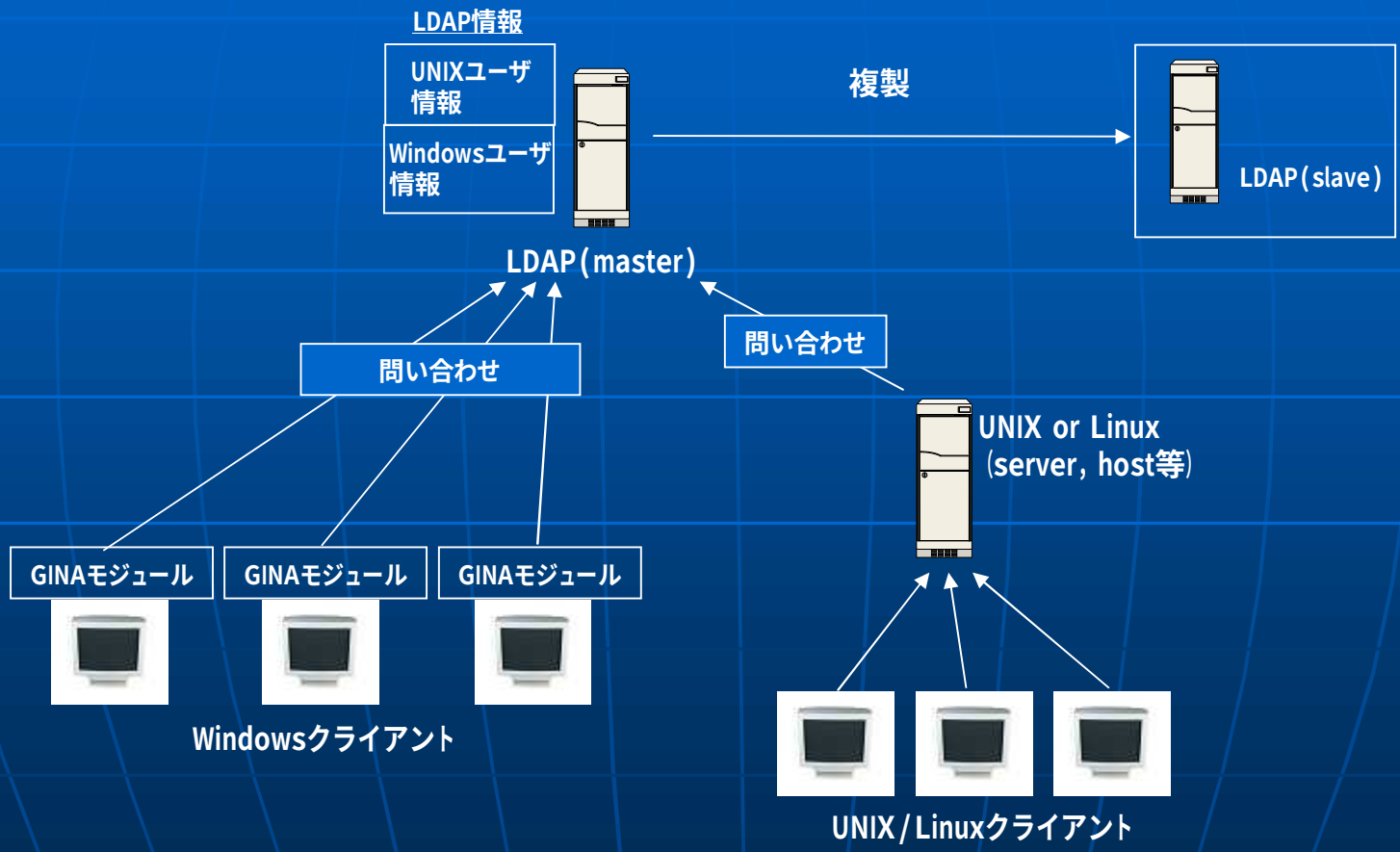
⇩

フリーウェア，サードベンダ製モジュール（pGINA,coGINA）

GINA - LDAP連携

WindowsクライアントをUnix Serverで認証

GINA - LDAP連携のためのシステム構成



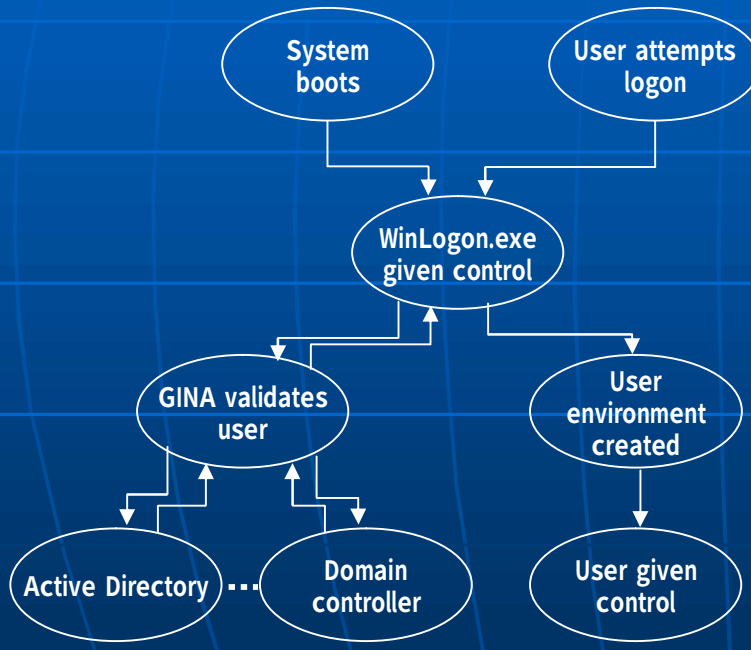
GINA - LDAP連携

WindowsクライアントをUnix Serverで認証

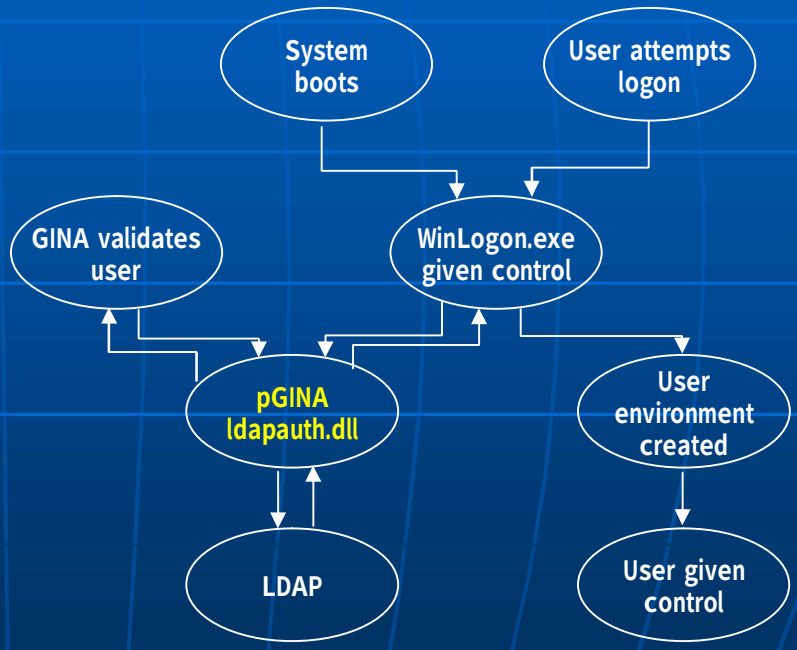
GINAを利用したLDAP連携ーサードベンダ製モジュール（1）ー

pGINA : Pluggable Graphical Identification aNd Authentification

→ Microsoft GINAに対するadd - on DLL



msGINA - AD連携による認証（従来）



pGINA - LDAP連携による認証

GINA - LDAP連携
Windowsクライアントを Unix Serverで認証

GINAを利用したLDAP連携ーサードベンダ製モジュール（2）ー

CO - GINA：製品名シー・オー・ギナ（Version2.3以降）

→ コンセプトはpGINAと同じ

LDAPへバインドするためのモジュール部分（サンプル）

```
・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・
LDAP* pldap = ldap_init(szHost, LDAP_PORT);
if(!pldap)
{
		return LdapGetLastError();
}
ULONG version = LDAP_VERSION3;
ldap_set_option(pldap, LDAP_OPT_VERSION, &version);
l_timeval timeout = {5, 0};
if(ldap_connect(pldap, &timeout) != LDAP_SUCCESS)
{
		return LdapGetLastError();
}

ULONG ulID = ldap_bind_s(pldap, szUsername, szPassword, LDAP_AUTH_SIMPLE);
if(ulID != LDAP_SUCCESS)
{
		return ulID;
}
ldap_unbind(pldap);
・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・
```

GINA - LDAP連携

WindowsクライアントをUnix Serverで認証

GINAを利用した認証における留意点

以下のような場合を含め，予期せぬ状況への対応，処理操作を
予め設定しておく必要あり．
（既成のモジュールを利用する場合を含む）

1. サーバー接続が停止したとき，認証プロセスが停止したとき
2. 認証に失敗したとき
3. 認証後にログオンするためのWindowsアカウント
4. 認証成功後にWindows側にアカウントが無い場合
5. パスワード変更手順
6. Windows側のアカウントのパスワードが異なる場合
7. Windows側のアカウントがロックされた場合
8. Windows側のパスワード変更が禁止された場合
9. ・・・・・・・

SFU - Windows Services for UNIX -

UNIXクライアントをActive Directoryで認証

SFU(Windows Services for UNIX)

UNIXやLinuxのシステム環境との統合を目的としてWindowsシステムに
UNIX互換性を持たせるためのソフトウェア

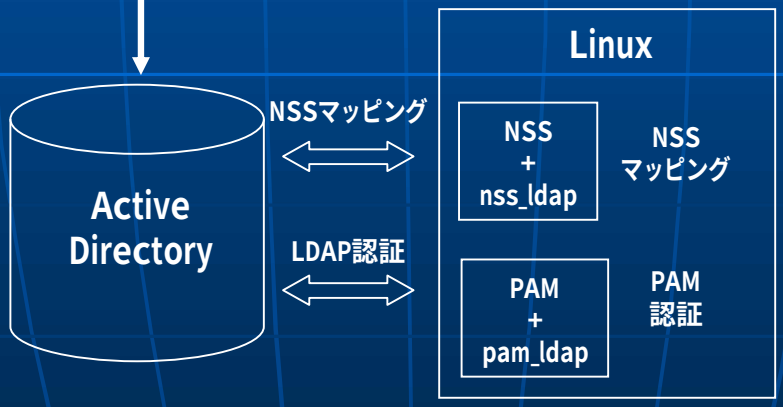
SFU付属のActive Directory用のNISサーバを利用

→ Linuxユーザ･グループ情報を一元的に管理

⇩

Active DirectoryスキーマをNISベースで拡張

↓

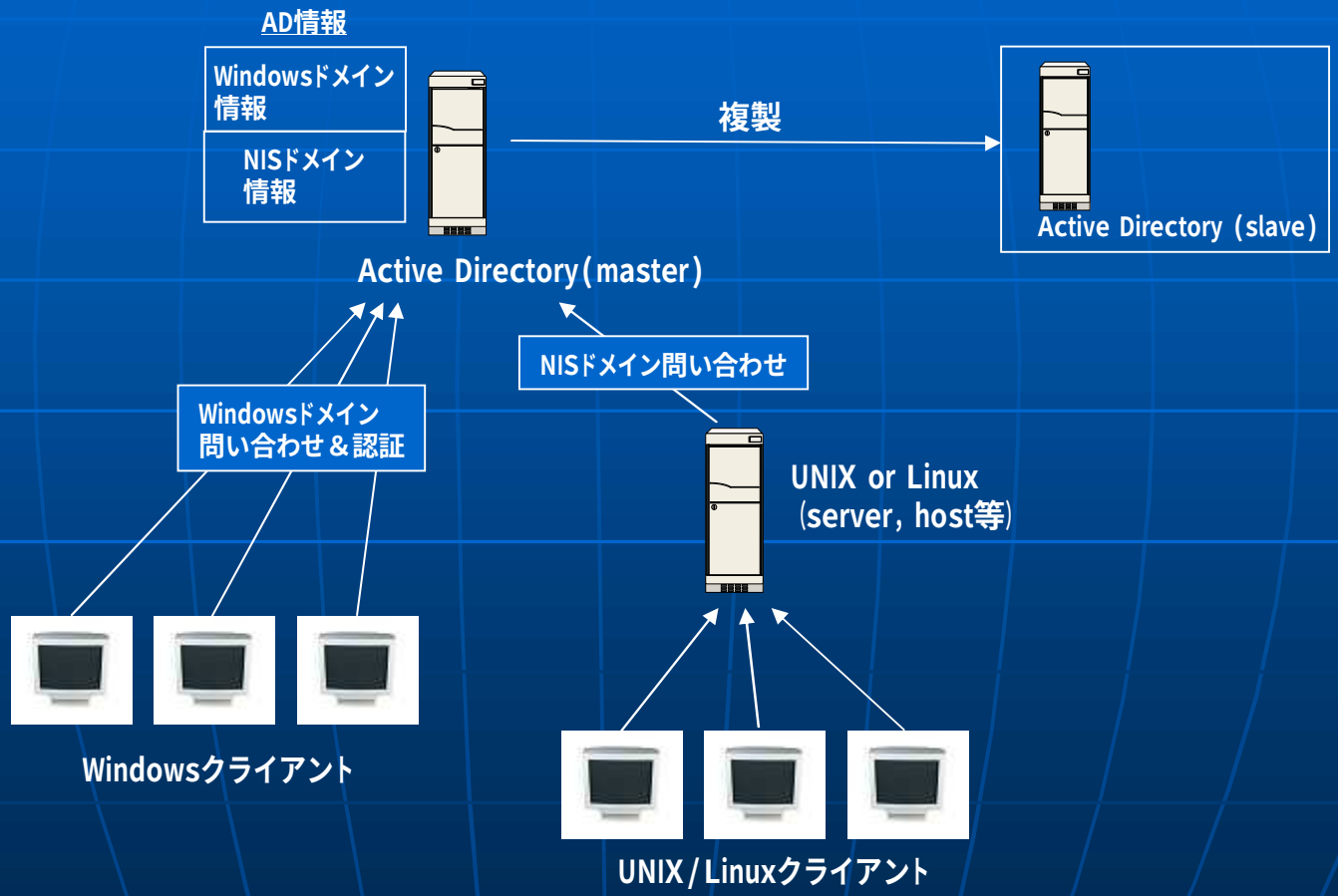


UNIX - Windows統合認証

SFU - Windows Services for UNIX -

UNIXクライアントをActive Directoryで認証

SFUを利用した統合認証システム構成



SFU - Windows Services for UNIX -

UNIXクライアントをActive Directoryで認証

SFUを利用した統合認証システムの構築

Windows Serverの設定

SFU (NISサーバコンポーネント付) のインストール

↓

ユーザアカウント, グループの設定 (UNIX属性設定)

↓

プロキシアカウントの設定

LDAPクライアントの設定

authconfigからActive Directoryを指定 (nss,pamの設定)

↓

ldap.confをSFUスキーマとのマッピングのため書き換え

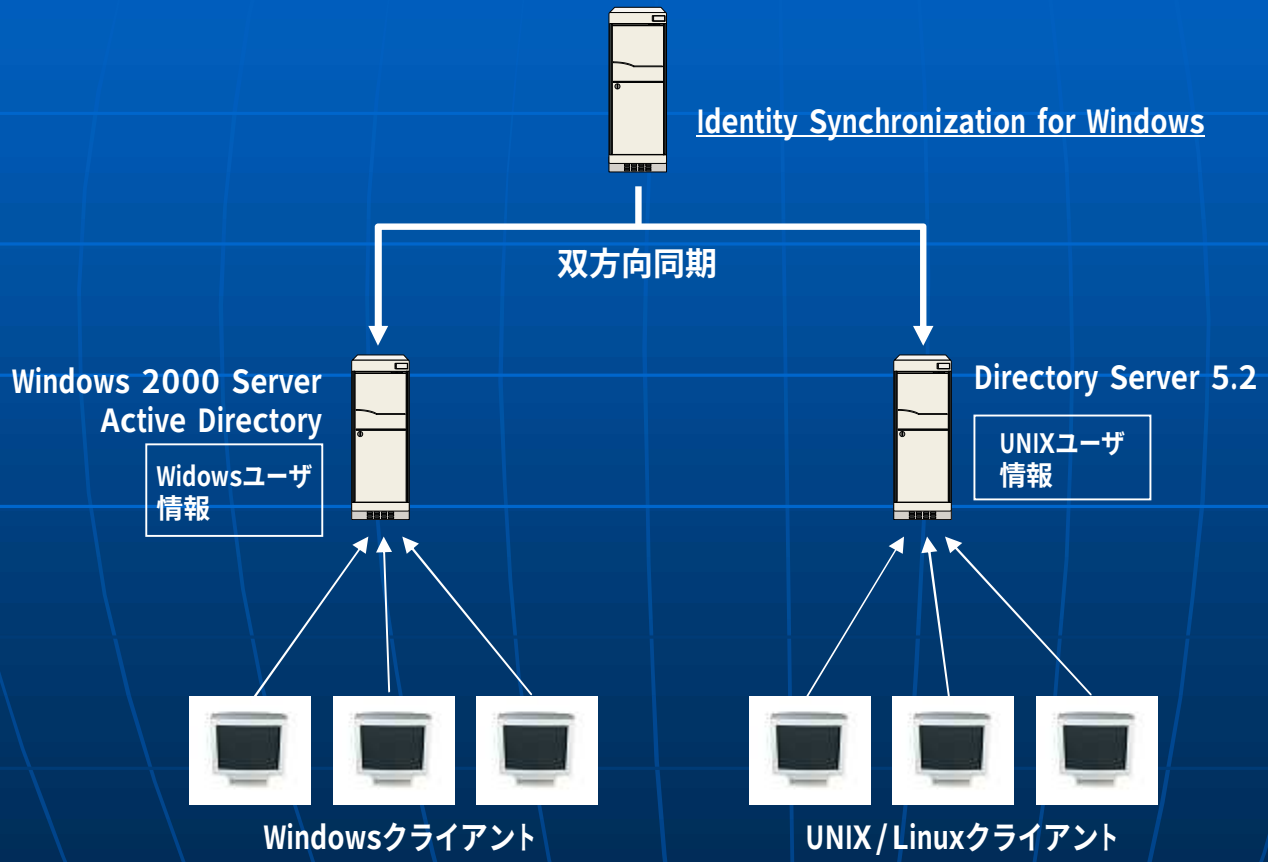
RFC 2307	Services for UNIX
posixAccount	User
shadowAccount	User
uid	sAMAccountName
uidNumber	msSFU30UidNumber
gidNumber	msSFU30GidNumber
・・・・・・・・・	・・・・・・・・・

Sun Java™ System Identity Synchronization for Windows

UNIX,Windows各クライアントをそれぞれのサーバで認証

System Identity Synchronization for Windowsを利用したシステム構成

Identity Synchronization for Windowsのサーバを追加してディレクトリサーバ間の双方向同期を常に取る.



まとめ

1. UNIX - Windows統合認証のためのソリューションに関して
   技術的な可能性，問題点など調査した．

2. 実装に関してはSamba - LDAP連携，SFUを確認，GINAに
   ついてもLDAPエントリ検索部分の基本的な動差状況を確認した．

3. Windows serverとしての機能は完全には継承できないなどの問題は
   残されているが，LDAPでの情報管理がすでに行われている環境では
   Samba - LDAP連携による統合管理が現状では有利である．

今後

クライアント数増加に伴う稼動上の問題点，機能的な問題点や不足点の
洗い出しなどの調査を引き続き行う必要がある．