株式会社ケイ・シー・シー

Linux Professional Institute Japan LPI-JAPAN

LPICレベル3　300技術解説無料セミナー

2014/3/21

株式会社ケイ・シー・シー
西日本センターユニット　ITラーニングセンター
村田　一雄

© LPI-Japan 2014. All rights reserved.

講師プロフィール

■会社概要

株式会社ケイ・シー・シー

http://www.kcc.co.jp/

■講師紹介

西日本センターユニット　ITラーニングセンター所属

Linuxをメインにネットワーク・セキュリティ・Java・LPIC資格取得講座など
様々な技術研修を担当

Linux Professional Institute

© LPI-Japan 2014. All rights reserved.

アウトライン

株式会社クイ・シー・シー

1. LPIC レベル3　試験概要
   - LPIC試験概要

2. 技術解説項目
   - 主題392　Sambaの基礎
   - 主題393　Sambaの共有の設定
   - 主題394　Sambaのユーザとグループの管理

Linux Professional Institute

© LPI-Japan 2014. All rights reserved.

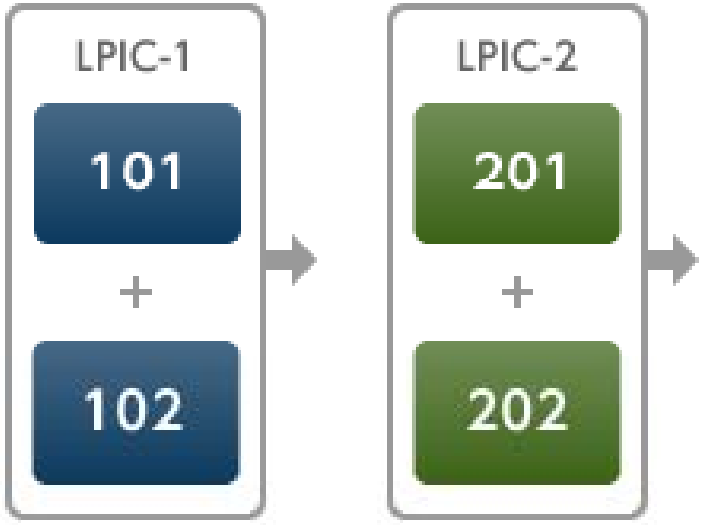
株式会社ケイ・シー・シー

LPICレベル3　試験概要

Linux Professional Institute

© LPI-Japan 2014. All rights reserved.

LPIC試験の構成



LPIC-3（下記の3試験のうちいずれかを選択）

- 300 LPIC-3 Mixed Environment
- 303 LPIC-3 Security
- 304 LPIC-3 Virtualization & High Availability
- 301 + 302 2014年3日31に配信終了予定

© LPI-Japan 2014. All rights reserved.

LPI 300 Mixed Environment Examの出題範囲

株式会社クイ・シー・シー

- 主題390: OpenLDAPの設定(8)
- 主題391: OpenLDAPの認証バックエンドとしての利用(4)
- 主題392: Sambaの基礎(11)
- 主題393: Sambaの共有の設定(9)
- 主題394: Sambaのユーザとグループの管理(9)
- 主題395: Sambaのドメイン統合(9)
- 主題396: Sambaのネームサービス(5)
- 主題397: LinuxおよびWindowsクライアントの操作(5)

© LPI-Japan 2014. All rights reserved.

LPICレベル3 300　技術解説

主題392　Sambaの基礎

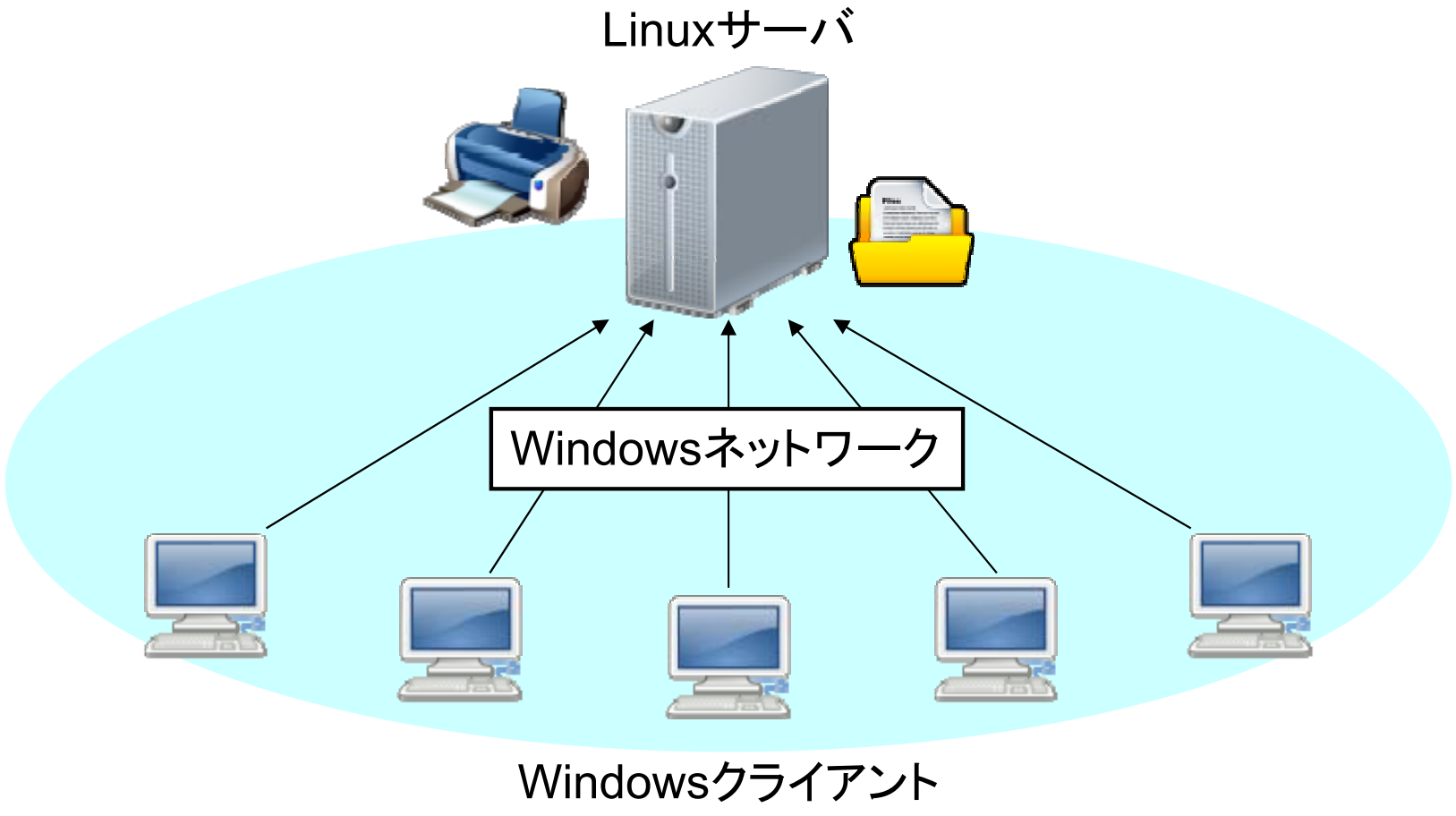
392.1	Sambaの概念とアーキテクチャ	重要度2
392.2	Sambaを設定する	重要度4

© LPI-Japan 2014. All rights reserved.

Sambaの概要

Sambaとは

- UNIX系OSをWindowsネットワークに接続するための機能を実装したサーバソフトウェア
- 主にファイル共有機能、プリントサーバ機能、ドメイン管理機能を提供

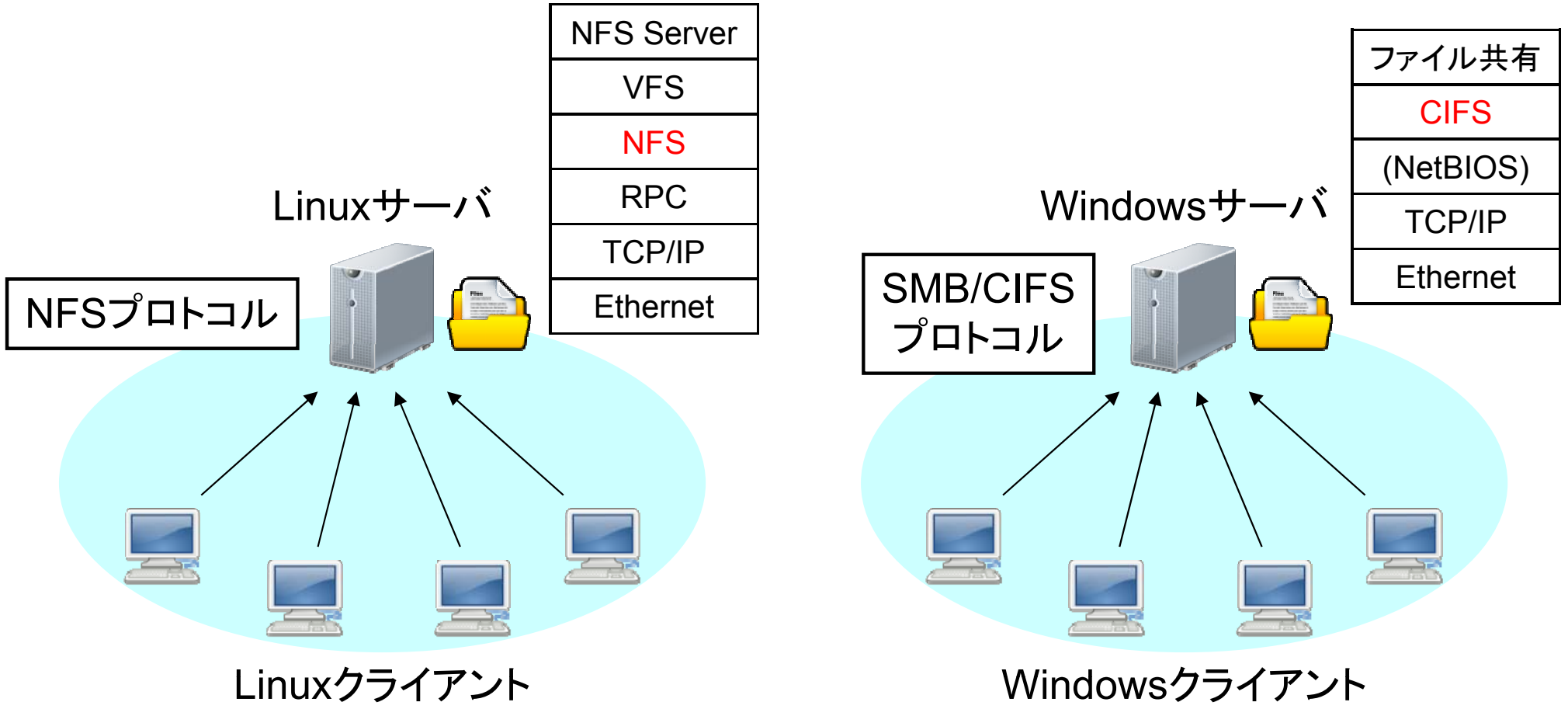


© LPI-Japan 2014. All rights reserved.

ファイル共有機能　2/2

■UNIX系OS・Windowsでのファイル共有

- UNIX系OSでは、NFS（Network File System）プロトコルを使用
- Windowsでは、SMB/CIFSプロトコルを使用

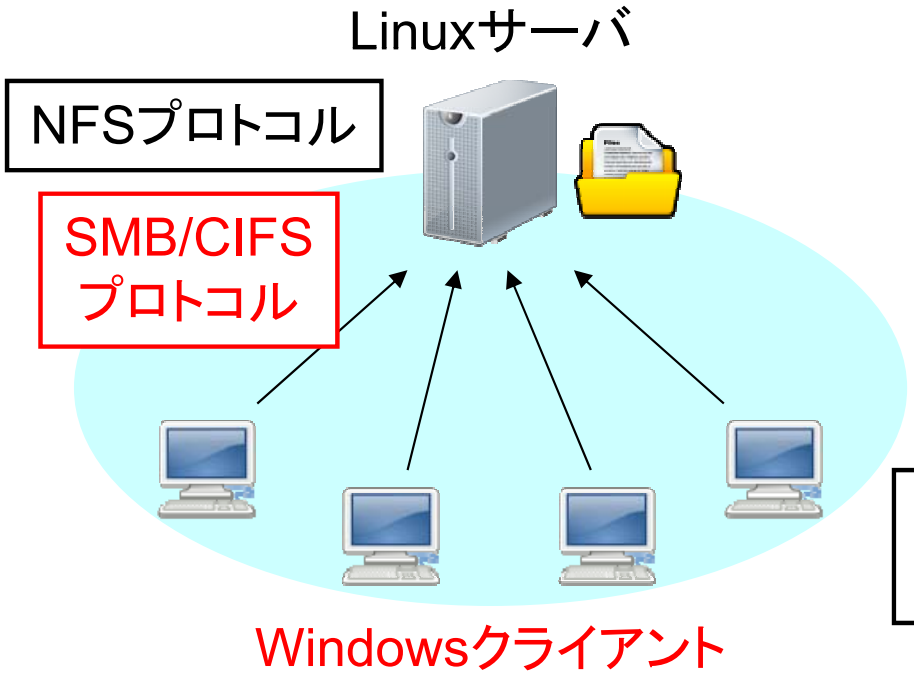


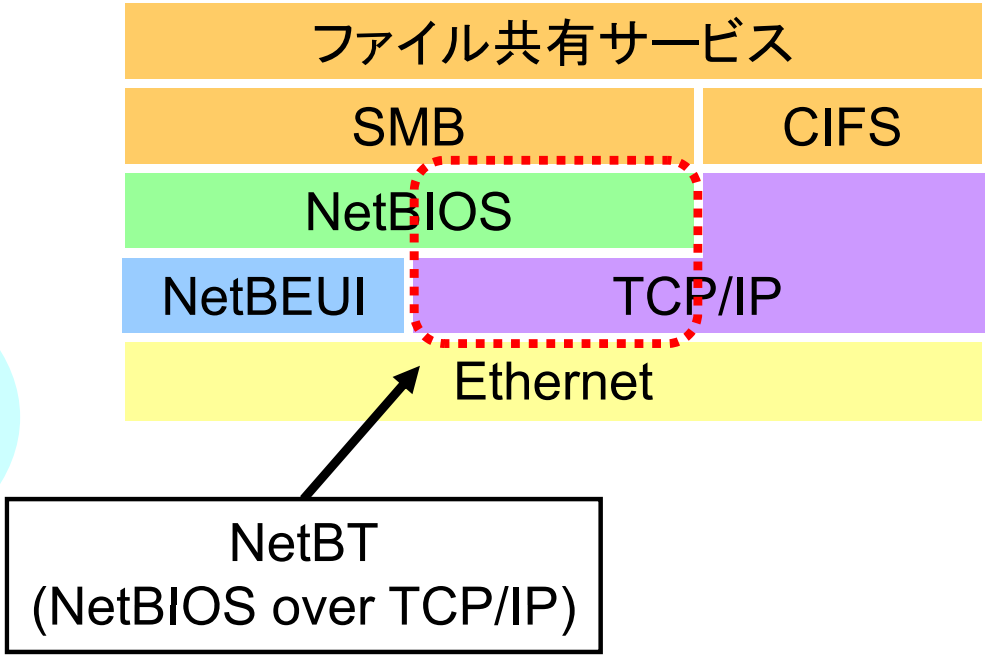
© LPI-Japan 2014. All rights reserved.

ファイル共有機能　2/2

■Sambaのファイル共有機能

- SambaにSMB/CIFSプロトコルを実装することで、Windowsネットワーク上でのファイル共有を実現





© LPI-Japan 2014. All rights reserved.

SMB/CIFSプロトコル概要

SMB（Server Message Block）

- Windowsでネットワーク上のファイル共有・プリンタ共有を実現するプロトコル
- Microsoft社が独自開発
- 下位レイヤにNetBIOSインターフェイスを利用

CIFS（Common Internet File System）

- SMBプロトコルを拡張し、Windows以外のOSやアプリケーションでも利用できるように仕様を公開したプロトコル
- 下位レイヤにTCP/IPプロトコルを利用
  - NetBIOSインターフェイスは使用しない（445/tcpポートを使用）

© LPI-Japan 2014. All rights reserved.

NetBIOS・NetBEUI概要

NetBIOS

- コンピュータがネットワークを利用するために呼び出すアプリケーション インターフェイス（API）
- 通信相手の指定にはNetBIOS名（後述）を使用する （※TCP/IPではIPアドレスで通信相手を指定）

NetBEUI（NetBIOS Extended User Interface）

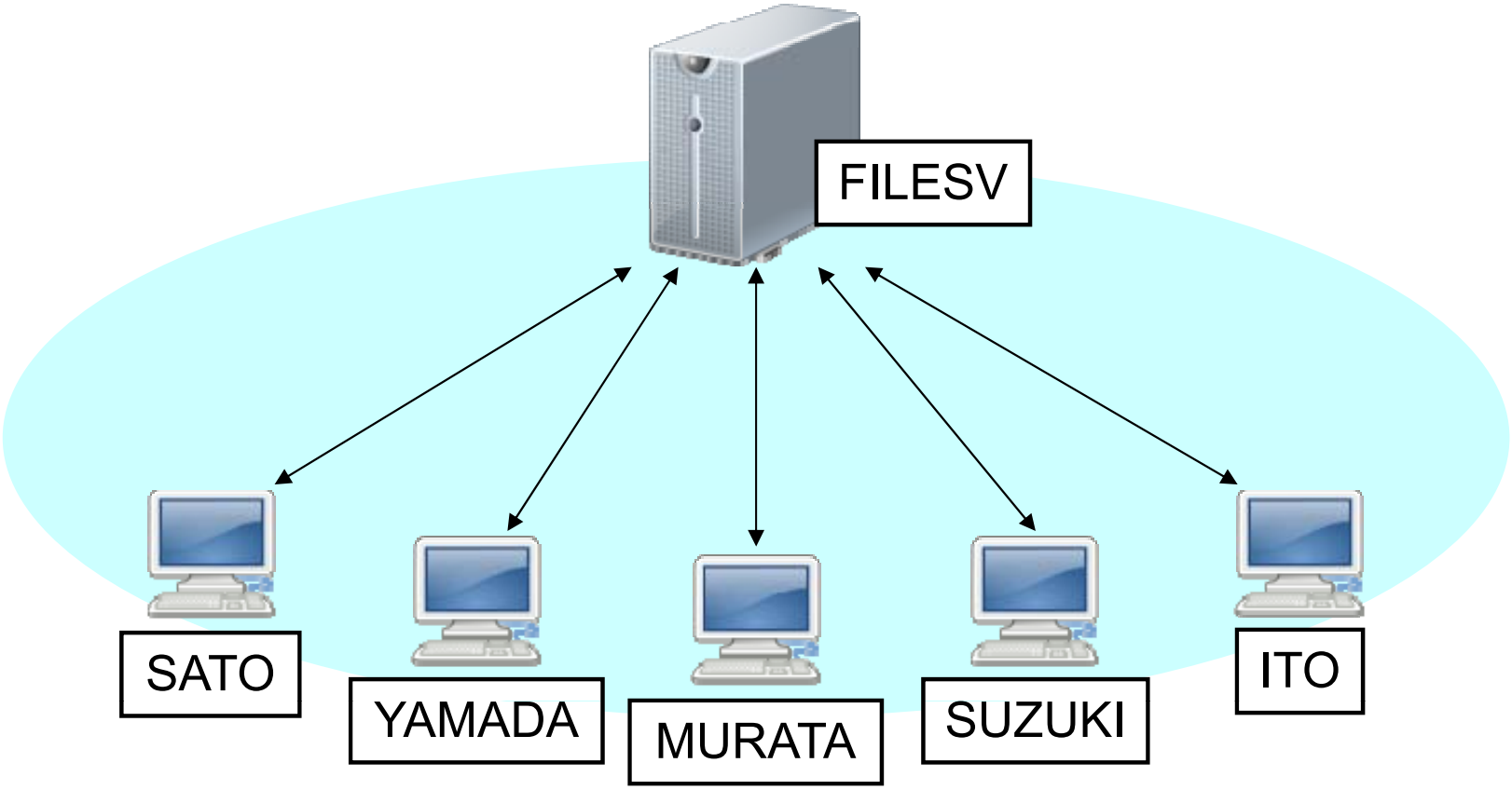
- IBMのLAN Managerで採用された、NetBIOSを拡張したプロトコル
- ルータを越えない範囲でノード間通信が可能（単一ネットワーク内で利用）

© LPI-Japan 2014. All rights reserved.

NetBIOS名

NetBIOS名とは

- ネットワークに接続したコンピュータや各種ネットワークサービス（ファイル共有など）を識別するためにつけられる最大16バイトの文字列
- 単一のネットワークに接続されているノードは個々にユニークな名前を持っている

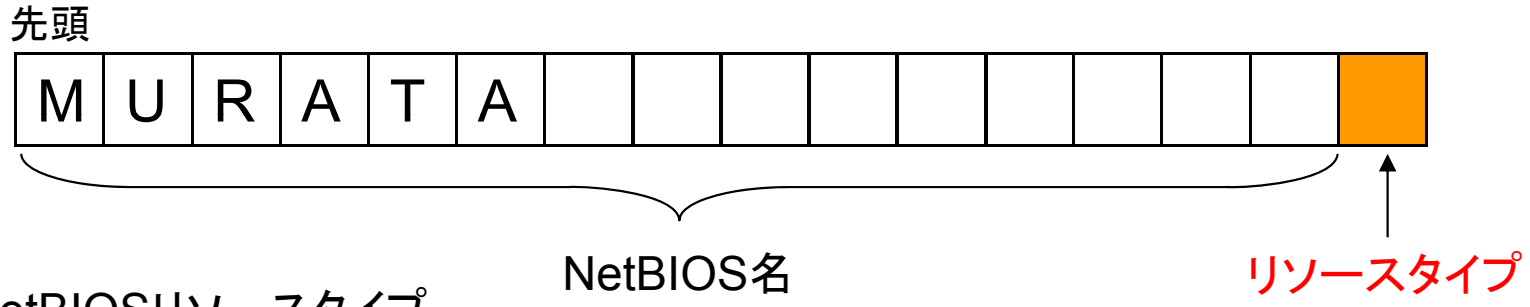


© LPI-Japan 2014. All rights reserved.

NetBIOS名の仕組み

NetBIOSリソースタイプ（サフィックス・ノードタイプ）

- コンピュータやネットワークサービスの種類を表す値
- NetBIOS名の16バイト目（最後の1バイト）を使用
  - コンピュータに任意でつけられるNetBIOS名は最大15バイト分となる



主なNetBIOSリソースタイプ

名前	リソースタイプ	役割
コンピュータ名	00	ワークステーションサービス（クライアント）
コンピュータ名	03	メッセンジャーサービス
コンピュータ名	20	ファイル・サーバサービス
ドメイン名	1B	ドメインマスタブラウザ
ドメイン名	1C	ドメインコントローラ
ドメイン名	1D	マスターブラウザ

© LPI-Japan 2014. All rights reserved.

NBTでの名前解決

■NetBIOS名とIPアドレスの解決
- ブロードキャストによる名前解決
- WINSサーバによる名前解決
- ローカルファイル（lmhostsファイル）による名前解決

■（参考）Windowsクライアントのノードタイプ
- Bノード　　ブロードキャストのみで名前解決
- Pノード　　WINSサーバへの問い合わせのみで名前解決
- Mノード　　ブロードキャスト　→　（失敗時）WINSサーバ
- Hノード　　WINSサーバ　→　（失敗時）ブロードキャスト

© LPI-Japan 2014. All rights reserved.

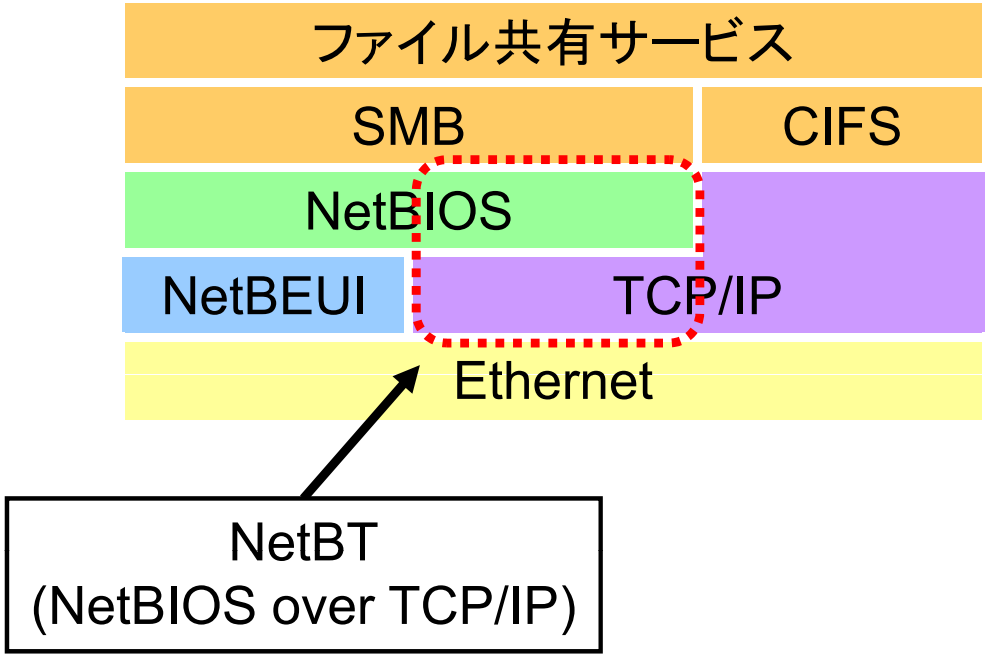
NBT（NetBIOS over TCP/IP）

■NetBEUIのデメリット

- ルータを越えたセグメントへの通信ができない（単一セグメントでの通信）
- ネットワークに負荷がかかる（ブロードキャストを多用）

■NetBIOS over TCP/IP

- NetBIOSをTCP/IPネットワークで利用できるよう開発されたプロトコル
- TCP/IPの機能を使いながら、従来のWindowsサービスを利用可能
- 企業ネットワークとの統合も可能



Linux Professional Institute
© LPI-Japan 2014. All rights reserved.

Sambaデーモンプロセス

smbd

- Sambaの中心的なデーモン
- ファイル共有機能を提供
- クライアントからの接続を監視し、接続要求ごとにsmbdの子プロセスを生成

nmbd

- NBTのネームサーバリクエストを認識し、応答
- WINSサーバ機能、WINS proxy機能の提供
- ブラウジング機能の提供

winbindd

- ネームサービススイッチ機能を提供
- Windowsサーバのユーザ情報やグループ情報などのシステム情報の取得と名前解決を行い、UNIXユーザの情報を自動作成してマッピングする

© LPI-Japan 2014. All rights reserved.

Sambaのデーモンプロセス

Sambaデーモンが使用するポート番号

Sambaデーモン	サーバ側 ポート番号	目的
nmbd	137/udp	ネームサービス（名前解決・ブラウジング）
nmbd	138/udp	データグラムサービス（名前解決・ドメインログイン）
smbd	139/tcp	セッションサービス（ファイル共有）
smbd	445/tcp	Direct Hosting of SMB（Windows2000以降）
winbindd	（なし）	
swat	901/tcp	SWAT（Webブラウザ上でのSamba管理）

© LPI-Japan 2014. All rights reserved.

株式会社クイ・シー・シー

LPICレベル3 300　技術解説

主題393　Sambaの共有の設定

393.1 ファイルサービス　重要度4
393.2 Linuxファイルシステムと共有/サービスのパーミッション　重要度3

Linux Professional Institute

© LPI-Japan 2014. All rights reserved.

Sambaの設定ファイル

smb.confの構成

- [*セクション名*]から次のセクションが始まるまでをセクションといい、セクションごとに設定を記述する
- セクション名は基本的に共有名に対応
  - global, homes, printersは利用不可
- [*セクション名*$]と記述すると隠し共有となり、ブラウジング一覧に表示されなくなる
- boolean型の値をとる場合は以下で指定
  - yes / no
  - true / false
  - 0 / 1
- コメントの記述
  - シャープ記号(#)
  - セミコロン(;)

```
[global]                          ┐
   パラメータ名 = 値               │
   ;パラメータ名 = 値              ├ セクション
   #コメント                      │
   ...                            ┘

[homes]
   パラメータ名 = 値
   ...

[printers]
   パラメータ名 = 値
   ...

[セクション名1]
   パラメータ名 = 値
   ...

[セクション名2]
   パラメータ名 = 値
   ...
```


© LPI-Japan 2014. All rights reserved.

smb.confの特殊なセクション

- [global]セクション
  - Samba全体の設定を記述するセクション
  - 他セクションで必要な値が定義されていない場合のデフォルトの設定を記述

- [homes]セクション
  - ユーザのホームディレクトリを共有するための設定を記述するセクション
  - 基本的にはpathパラメータを利用して共有ディレクトリを指定
  - pathパラメータの指定がない場合、ユーザのホームディレクトリを共有ディレクトリに指定

- [printers]セクション
  - /etc/printcapで定義されたプリンタが一括して共有

© LPI-Japan 2014. All rights reserved.

smb.confで利用できる変数と設定確認

Samba変数

%L	サーバのNetBIOS名（Sambaを445/tcpで稼動させる場合には利用不能）
%U	セッションのユーザ名
%G	%Uのプライマリグループ名
%S	現在のサービス名
%u	現在のサービスのユーザ名
%g	%uのプライマリグループ
%H	%uのホームディレクトリ
%m	クライアントマシンのNetBIOS名
%M	クライアントマシンのホスト名

smb.confの設定確認

- testparmコマンド
  - 構文の誤りをチェックするが、Sambaの実際の機能をチェックするものではない

© LPI-Japan 2014. All rights reserved.

パラメータの種類

■グローバルパラメータ

- globalセクションでのみ利用できるパラメータ
- 「パラメータ名（G)」と記述　　ex.）map to guest(G)

■ローカルパラメータ

- 各セクションで設定するパラメータ
- 「パラメータ名（L)」と記述　　ex.）browseable(L)

© LPI-Japan 2014. All rights reserved.

smb.confの主なパラメータ

パラメータ名	機能・役割
browseable	共有の表示を設定
hosts allow	指定したホストだけ共有へのアクセスを許可（他はすべて拒否）
valid users	指定したユーザ・グループ（@, +で指定）だけ共有へのアクセスを許可
read only	共有に対する読み取りを設定
writeable	共有に対する書き込みを設定
write list	書き込みを許可するユーザリストを設定
read list	読み取りを許可するユーザリストを設定
admin users	共有内でのアクセスユーザをrootに指定
force user	共有内でのアクセスユーザを強制的に指定
force group	共有内でのアクセスグループを強制的に指定
map to guest	ゲスト認証要求時の動作を設定
guest ok	ゲスト認証でのアクセスを設定

© LPI-Japan 2014. All rights reserved.

ファイル共有の作成

作成方法

- smb.confに[*共有名*]でセクションを作成し、設定を記述
- [homes]セクションには、ユーザのホームディレクトリを共有するための設定を記述

```
[global]
   ...

[homes]
   comment = %U's Home
   browseable = no
   writeable = yes
   valid user = %S
   ...

[share]
   commemt = Share
   path = /mnt/share
   browseable = yes
   writeable = yes
   ...
```

ユーザのホームディレクトリ設定

ファイル共有の設定を記述

© LPI-Japan 2014. All rights reserved.

[homes]セクションの二重表示

株式会社クイ・シー・シー

■ホームディレクトリの表示

- [homes]セクションでは、ユーザのホームディレクトリが自動的に共有ディレクトリとして設定される
  - 「murata」ユーザの場合、「/home/murata」が共有ディレクトリとなるため、pathパラメータの記述は不要
- [homes]セクション内で「browseable = yes」と設定すると、「マイネットワーク」では、「homes」という共有とユーザのホームディレクトリが両方表示される

■ホームディレクトリを二重表示されないようにする方法

- [global]セクションで「browseable = no」と設定し、表示させたい共有セクションで「browseable = yes」と設定する
  - 「browseable = yes」と設定した共有のみ表示される
- [homes]セクションを有効にし、「valid users = %S」と設定し、他のユーザがアクセスできないよう制限する

© LPI-Japan 2014. All rights reserved.

[IPC$]セクション

IPC（Inter-Process Communication）とは

- Windowsネットワークにおいて、マシンの公開リソースの一覧取得やリソースの利用準備を行う際に利用される共有
- Sambaを起動すると自動的に[IPC$]という隠し共有が作成される
- セキュリティ上「IPC$」共有にアクセスさせたくない場合は、「hosts allow」パラメータおよび「hosts deny」パラメータで設定する

IPC$へのアクセス制限例

```
[IPC$]
   hosts allow = 192.168.1.
```


© LPI-Japan 2014. All rights reserved.

ユーザ単位のアクセス制限

- 共有へのアクセスをユーザ単位で設定
  - 「valid users」パラメータで設定

murataユーザだけ共有へのアクセスを許可

```
valid users = murata
```

trainerグループだけ共有へのアクセスを許可

```
valid users = @trainer
```

educグループ(Linuxマシンのグループ)だけ共有へのアクセスを許可

```
valid users = +educ
```


© LPI-Japan 2014. All rights reserved.

共有に対する読み書き単位のアクセス制限

■ユーザ単位で共有内のファイルへの読み書きを制御

- 「read only = yes」あるいは「writeable = no」
  - 共有に対して読み取りは可能だが、書き込みは不可
- 「read only = no」あるいは「writeable = yes」
  - 共有に対して書き込みを許可

■特定のユーザにのみ読み書きを制御

- 「write list(L)」あるいは「read list(L)」で指定

rootユーザとstaffグループにのみ書き込みを許可

```
read only = yes
write list = root @staff
```


© LPI-Japan 2014. All rights reserved.

共有へアクセスするユーザの制御

共有内でrootとする設定

- 「admin users = [*ユーザ名*]」と設定すると、指定されたユーザは、設定された共有内でrootとしてアクセス許可される

share共有内でmurataユーザをrootとしてアクセス

```
[share]
   admin users = murata
   ...
```

共有内で強制的にアクセスユーザを指定

- 「force user = [*ユーザ名*]」と設定すると、指定された共有内では強制的に設定されたユーザの権限でアクセス許可される
- 「force group = [*グループ名*]」と設定すると、指定された共有内では強制的に設定されたグループの権限でアクセス許可される

share2共有内でmurataユーザとしてアクセス

```
[share2]
   force users = murata
   ...
```


© LPI-Japan 2014. All rights reserved.

ゲスト共有

ゲスト認証

- Sambaサーバにアカウントを持たないユーザがアクセスした場合に、特定のアカウントにマッピング
- 「map to guest」パラメータの指定によりゲスト認証時の動作を設定できる

map to guestパラメータの値

パラメータ名	機能・役割
Never	ゲスト認証を許可しない（デフォルト）
Bad User	「guest ok = yes」（ゲスト認証が許可）の場合、Sambaサーバにアカウントが存在しないユーザをゲストユーザとみなす
Bad Password	「guest ok = yes」（ゲスト認証が許可）の場合、Sambaサーバにアカウントが存在しないユーザや、パスワードが一致しなかったユーザを、ゲスト認証とみなす

© LPI-Japan 2014. All rights reserved.

SWATによるSambaの管理

SWAT（Samba Web Administration Tool）

- Webブラウザ上でのSamba管理ツール
- 901/tcpポートを使用
- デフォルトではスーパーサーバ経由（xinetdデーモン）で起動
- アクセス時はWebブラウザで以下のURLを入力
  http://<*Sambaサーバ*の*IPアドレス*> **:901**

SWAT使用上の留意事項

- smb.conf編集時、SWATが設定内容を再生成
  - コメント行、デフォルト設定が削除される
  - パラメータの並び順も変更される
- パスワードが暗号化されずに送信
  - 編集にはSambaのrootユーザパスワードが必要

© LPI-Japan 2014. All rights reserved.

LPICレベル3 300　技術解説

主題394　Sambaのユーザとグループの管理

394.1 ユーザアカウントとグループアカウントの管理　　重要度4
394.2 認証と許可およびWinbind　　重要度5

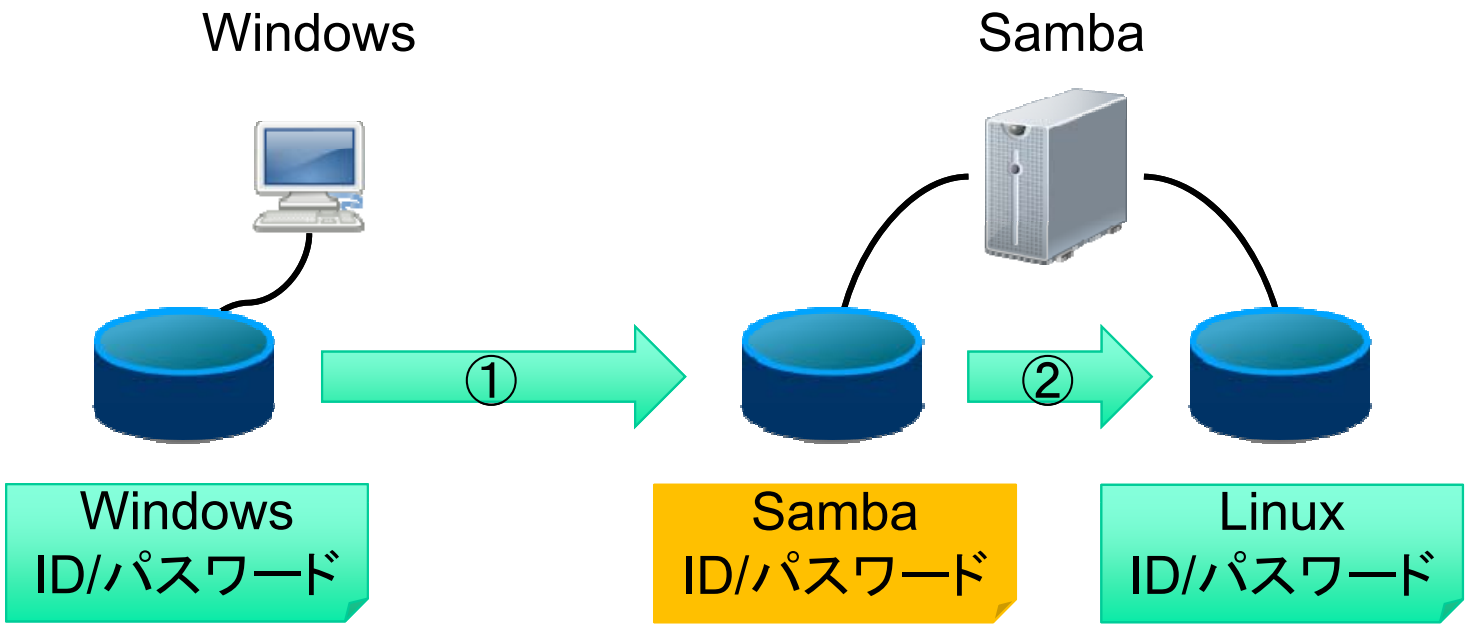
© LPI-Japan 2014. All rights reserved.

パスワード認証の流れ

■パスワード認証の手順

① Sambaユーザの認証

② SambaユーザをLinux UIDにマッピング



© LPI-Japan 2014. All rights reserved.

Samba認証データベースの種類

- smbpasswdファイル（ローカルファイル）
  - Samba2.2まで利用されたテキストベースのファイル
  - Winbind機能の使用不可
- TDB（Trivial Database）
  - Samba3.0でサポートされたバイナリ形式の簡易データベース
  - 拡張子「.tdb」がつけられる
- LDAP
  - ディレクトリサービスによる認証情報の一元管理
  - OpenLDAPサーバの構築が必要

© LPI-Japan 2014. All rights reserved.

認証データベース・ユーザ認証方式の指定

認証データベースの指定

- passdb backend (G)パラメータを使用

パラメータ値	認証データベース	設定例
smbpasswd	smbpasswdファイル	smbpasswd:/etc/samba/smbpasswd
tdbsam	TDB形式データベース	tdbsam:/etc/samba/smbpasswd.tdb
ldapsam	LDAPディレクトリ	ldapsam:ldap://192.168.1.100:389

ユーザ認証方式の指定

- security (G)パラメータを使用

パラメータ値	説明
share	パスワードのみで認証（共有単位での認証）
user	ユーザ名とパスワードのみで認証（デフォルト）
server	他のSambaサーバで認証
domain	ドメインコントローラによる認証
ads	Active Directoryのドメインコントローラによる認証

© LPI-Japan 2014. All rights reserved.

Sambaユーザの管理

pdbeditコマンド

- ユーザアカウントの追加・削除・変更・一覧表示・取り込みに対応
  （パスワードの変更にはsmbpasswdコマンドを使用）
- すべての認証データベースに対応

オプション	説明
-L	Sambaユーザの表示
-a	Sambaユーザの追加
-x	Sambaユーザの削除
-i	Sambaユーザ情報のインポート
-e	Sambaユーザ情報のエクスポート

認証データベースの移行

- smbpasswd形式からtdbsam形式、ldapsam形式への移行で利用

```
pdbedit –i smbpasswd:/etc/samba/smbpasswd –e  tdbsam:/usr/local/samba/private/passwd.tdb
```


© LPI-Japan 2014. All rights reserved.

smbpasswdコマンド

- Sambaユーザのパスワード設定・変更を行う
- 認証データベースにsmbpasswdを利用する場合、ユーザの作成・削除が可能

オプション	説明
-a *Sambaユーザ名*	Sambaユーザの追加 アカウントが存在する場合は無視され、通常のパスワード変更コマンドとして動作する
-x *Sambaユーザ名*	Sambaユーザの削除
-d *Sambaユーザ名*	Sambaユーザを無効にする
-e *Sambaユーザ名*	Sambaユーザを有効にする

© LPI-Japan 2014. All rights reserved.

パスワード・ユーザ名のマッピング

SambaパスワードとLinuxアカウントパスワードの同期

- smbpasswdコマンドでパスワードが変更されたタイミングで同期

```
unix password sync = yes
passwd program = /usr/bin/passwd %u
```

WindowsユーザとSambaユーザのマッピング

- 基本的にはWindowsユーザと同名のSambaユーザの認証情報を利用
- Windowsとは異なるSambaユーザとマッピングするには、username map パラメータを使用する

username mapパラメータの設定

```
username map = /etc/samba/smbusers
```

/etc/samba/smbusersファイルの内容
（左にSambaユーザ、右にWindowsユーザを記述）

```
smbuser1 = murata
smbuser2 = fukuda
guest = *
```


© LPI-Japan 2014. All rights reserved.

Winbind

Sambaユーザの作成手順

① Linuxユーザを作成（useraddコマンド、passwdコマンド）
② Sambaユーザを作成（pdbeditコマンド、smbpasswdコマンド）
③ （必要に応じて）ユーザ名・パスワードのマッピング（前頁参照）

Winbindとは

- Windowsドメインのアカウント情報からLinuxユーザの情報を自動的に生成するしくみ
- Winbindを利用するとSambaサーバでユーザを作成する際に、対応するLinuxユーザを個別に作成する必要がなくなる
- Winbind機能はwinbinddデーモンが提供
- winbinddはNSS経由でWindowsドメインのアカウント情報（SID）の取得と名前解決を行い、対応するLinuxユーザのUID/GIDを動的に割り当て、Samba認証データベースに保存する
- PAMに対応しており、Samba以外のアクセス認証にも対応

© LPI-Japan 2014. All rights reserved.

Winbindのインストール・設定　1/2

■パッケージのインストール

- winbindあるいはsamba-winbindパッケージをインストール

■NSS・PAM関連モジュール

- モジュールファイルを適切なディレクトリにコピーして配置

サービス名	モジュール
NSS	/lib/libnss_winbind.so
PAM	/lib/security/pam_winbind.so

■Winbindの設定

- /etc/nsswitch.confにwinbindを追加

```
passwd: files winbind
group: files winbind
```

- /etc/pam.d/system-authに以下の設定を追加

```
auth      sufficient    pam_winbind.so
account   sufficient    pam_winbind.so
```


© LPI-Japan 2014. All rights reserved.

Winbindのインストール・設定　2/2

smb.confの設定

- Winbindを利用する場合、Windowsドメインあるいは Active Directoryドメインに参加する必要がある

パラメータ名	説明
idmap uid	winbinddが動的に割り当てるUIDの範囲を指定
idmap gid	winbinddが動的に割り当てるGIDの範囲を指定

Winbind設定例

```
[global]
security = domain もしくは ads
...
idmap uid = 10000-11000
idmap gid = 10000-11000
...
```


© LPI-Japan 2014. All rights reserved.

idmap機能

Winbindにおける問題点（Samba2.2系）

- 複数のSambaサーバ運用時に自動生成されたユーザのUID/GIDが不一致となる
  - 同一のWindowsドメインのアカウントに対しても、アクセスするSambaサーバによって異なるUIDがマッピングされてしまう
- NFSなどUIDでユーザをマッピングするサービスでは致命的

idmap機能とは

- 複数のSambaサーバが個々に管理している認証データベースをLDAPサーバで一元化し、同じUIDがマッピングされるようにするしくみ

© LPI-Japan 2014. All rights reserved.

idmap機能の設定

LDAPサーバでの設定

- マッピング情報を格納するオブジェクトをあらかじめ作成しておく

Sambaサーバでの設定

パラメータ名	説明
idmap backend	LDAPサーバのアドレスを指定
idmap admin dn	LDAPサーバから情報を取得するための識別名（DN）を指定
ldap suffix	LDAPのベースサフィックスを指定
ldap idmap suffix	idmapマッピング情報のために使用するサフィックスを指定

idmap設定例

```
idmap uid = 10000-11000
idmap gid = 10000-11000
idmap backend = ldapsam:ldap://ldap.example.com
idmap admin dn = “cn=Manager, dc=example, dc=com
ldap suffix = dc=example, dc=com
ldap idmap suffix = ou=Idmap
```


© LPI-Japan 2014. All rights reserved.

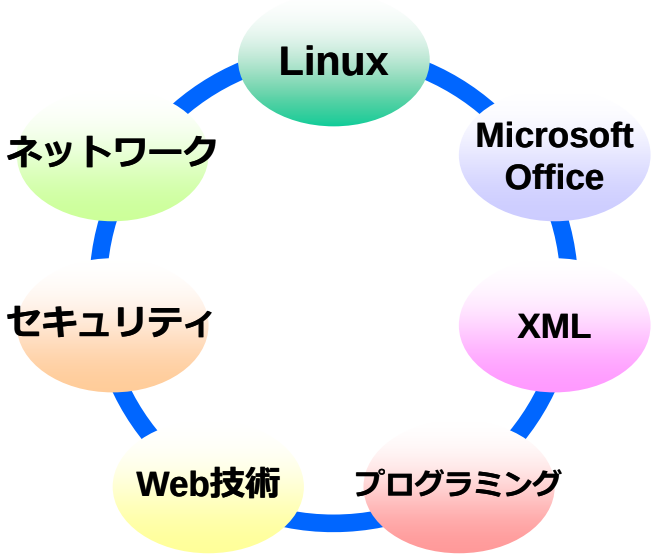
ご参考

■カスタマイズ研修のご案内

- LPIC試験対策研修
- Linux基礎、Linuxサーバ構築
- その他、ネットワーク・セキュリティ・Web技術など、
  各種IT研修をカスタマイズして提供

弊社研修サービスホームページ

http://www.kcc.co.jp/lpic/



IT技術研修

- ●Linux（基礎・システム管理・サーバ構築）
- ●ネットワーク（TCP/IP・LAN/WAN・無線技術）
- ●セキュリティ（技術解説・セキュリティマネジメント）
- ●XML（XML/DTD・XSLT・XML Schema）
- ●Web技術（HTML4/5・CSS・JavaScript・jQuery・Ajax）
- ●プログラミング（C・Java・Android・PHP・Objective-C）
- ●Microsoft Office（基礎/応用・VBA　※2007/2010対応）

資格試験対策

- ◆LPICレベル1～3
- ◆XMLマスター・ベーシック
- ◆CompTIA A+・Network+・Security+
- ◆Ruby技術者認定試験 Silver
- ◆情報処理技術者試験

© LPI-Japan 2014. All rights reserved.

ご清聴ありがとうございました

© LPI-Japan 2014. All rights reserved.