LinuC レベル 2
技術解説無料セミナー
2022/09/23 開催

主題	2.07 ネットワーククライアントの管理

エスディーテック株式会社
デザインエンジニアリング本部
末永 貴一

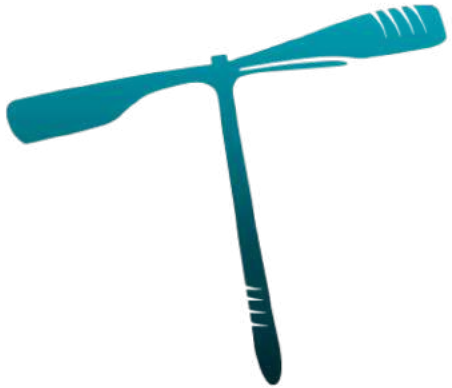
自己紹介

■自己紹介

エスディーテック株式会社 sdtech Sustainable Design & Technology

– デザインエンジニアリングでUI/UXソフトウェアの企画・開発・研究開発を行う企業

http://www.sdtech.co.jp



Linux関連文章の執筆

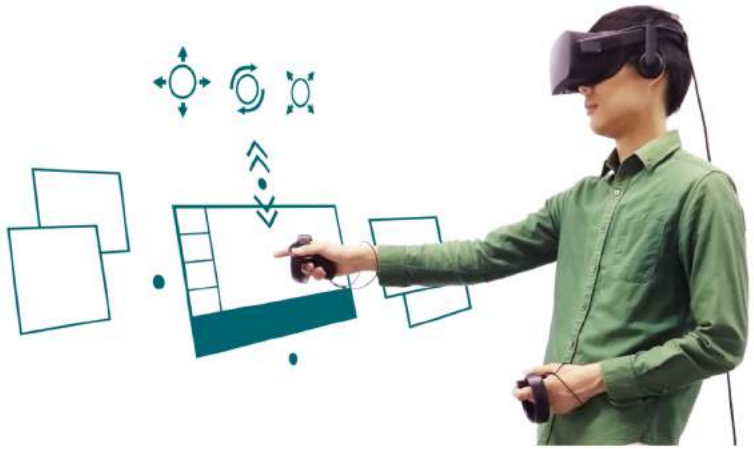
・@IT 「Linuxをいまから学ぶコツ教えます」
・@IT 「Linuxに触れよう」
・日経Linux「Xと次世代「Wayland」を知る」
・LPIC Level1,2 1回で合格必達テキスト+問題集

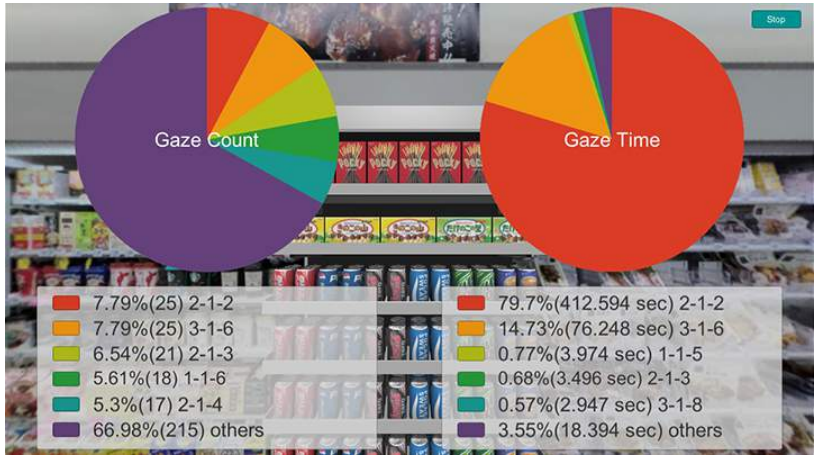
など

自己紹介

■TRITO VR

素早いトライ＆エラーを実現する
VRを活用した設計シミュレーター





LinuCレベル１／レベル２ Version10.0とは

■LinuCとは

クラウド時代の即戦力エンジニアであることを証明するLinux技術者認定

✓現場で「今」求められている新しい技術要素に対応

- オンプレミス／仮想化・コンテナを問わず様々な環境下でのサーバー構築
- 他社とのコラボレーションの前提となるオープンソースへの理解
- システムの多様化に対応できるアーキテクチャへの知見

✓全面的に見直した「今」身につけておくべき技術範囲を網羅

今となっては使わない技術やコマンドの削除、アップデート、新領域の取り込み

✓Linuxの範疇だけにとどまらない領域までカバー

セキュリティや監視など、ITエンジニアであれば必須の領域もカバー

クラウドを活用できるITエンジニアに必須の技術がまとまっている

AWSなどのパブリッククラウドを活用するための技術

間が欠けている状態

オンプレミスのサーバーサイドLinux技術

【今まで／その他】

AWSなどのパブリッククラウドを活用するための技術

仮想マシン／コンテナ技術、クラウドセキュリティ、アーキテクチャ、ほか

オンプレミスのサーバーサイドLinux技術

LinuC Version10.0

今回のテーマ

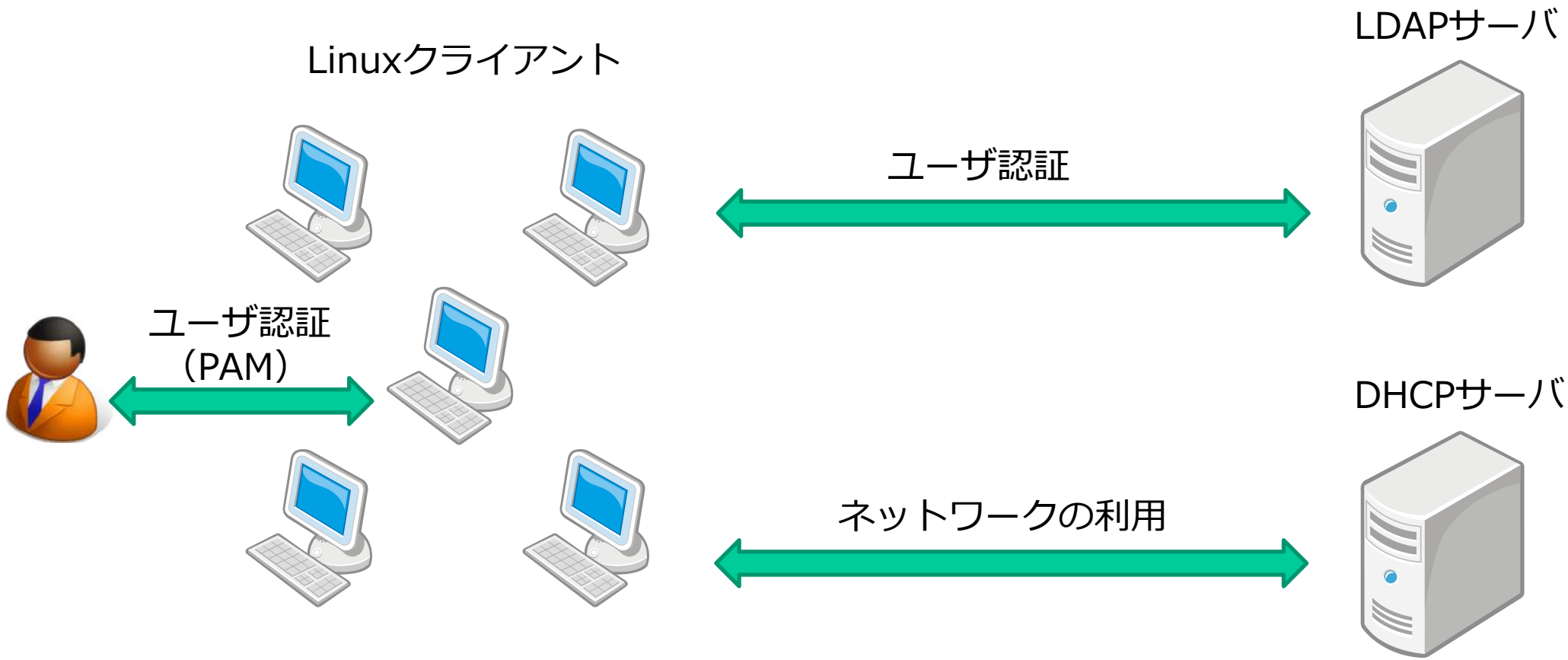
主題2.07：ネットワーククライアントの管理

- ✓ LinuxによるN/Wクライアント管理
- ✓ PAM
- ✓ LDAP
- ✓ DHCP

Linuxによるネットワーククライアント管理とは

■LinuxによるLAN内のクライアント管理

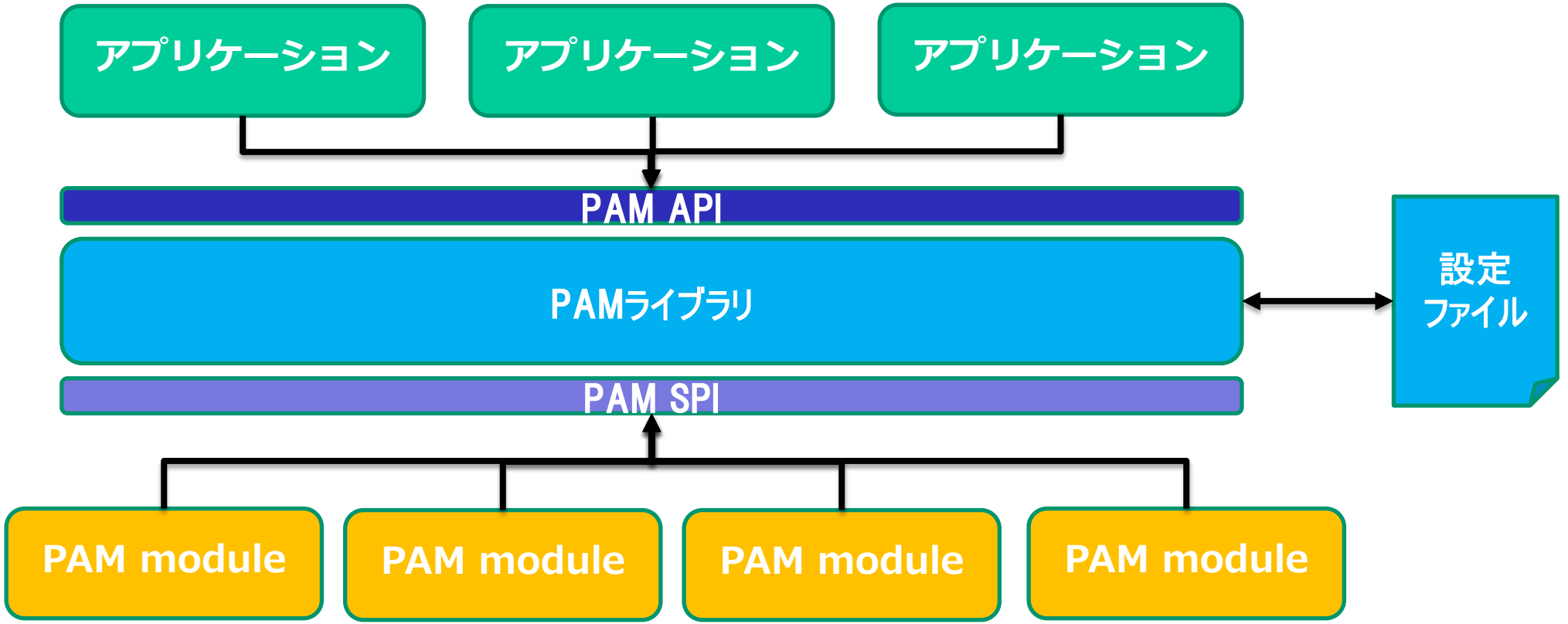
主題2.07におけるPAM、LDAP、DHCPの各テーマの関係性



PAM認証

■PAM認証とは

Linuxのシステムアプリケーションに対して認証、セキュリテイサービスを提供するフレームワーク



PAMサービスモジュール

PAM認証

■設定

・設定ファイルと設定フォーマット

設定ファイルは/etc/pam.d以下

・ファイルの基本フォーマット

<type> <control> <module-path> <module-arguments>

・設定項目

type：**auth**、**account**、**session**

control：**requisite**、**required**、**sufficient**、**optional**

auth ：　　認証方法の設定、認証の許可

account：　期限や有効性の確認

password：パスワード変更など

session：　ログインからログアウトまでの挙動

requisite：認証などに失敗したら以降の処理を行わずに失敗。

required：認証などに失敗しても、以降の処理を続行。

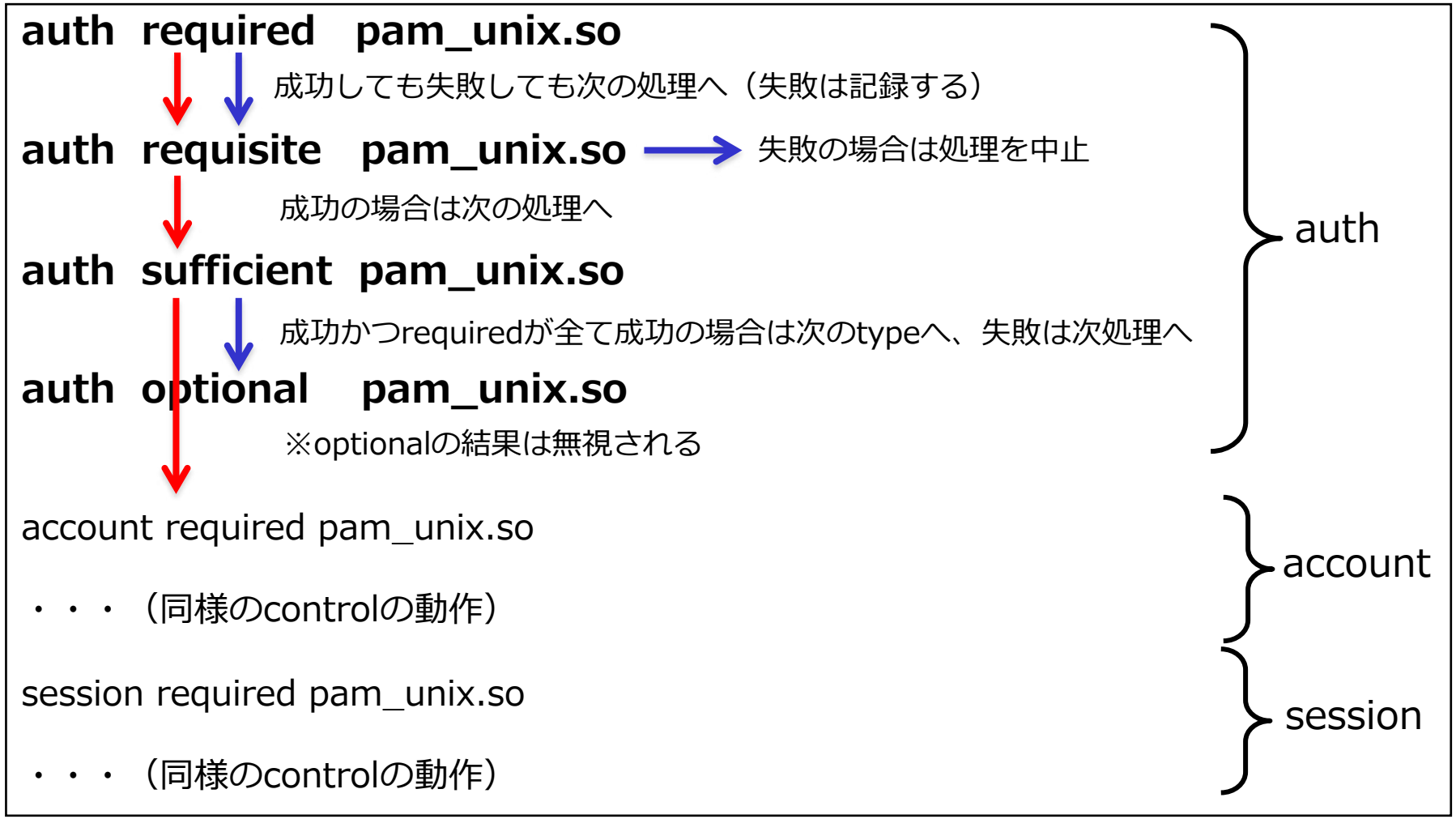
sufficient：認証などに成功したら、以降の処理を行わず成功と判断。

optional：成否に関係なく処理を行う

PAM認証

■PAM認証の動作例

例えば・・・



PAM認証

PAM認証の動作

PAMの挙動は目に見えないが、pam_echo.so等のモジュールを使ってデバッグ的に出力をする等して動作確認もできる。（ミスがあるとログインできなくなる等の問題が発生するため注意）

pam_echo.soの使い方

```
auth required pam_echo.so 出力したい文字列
```

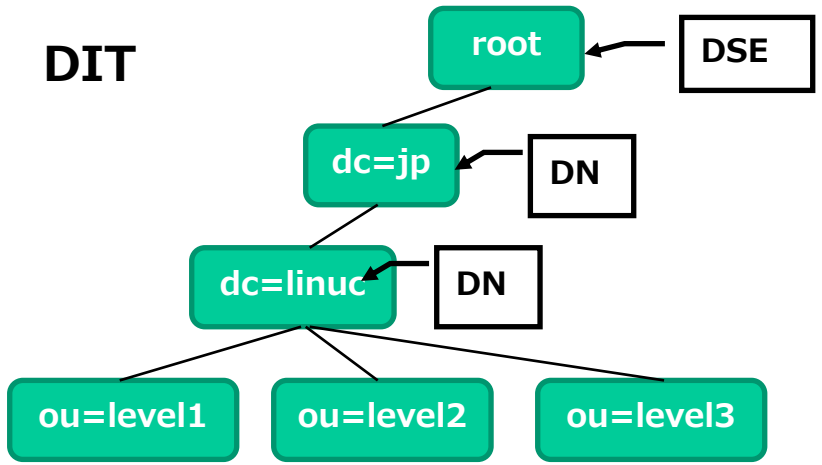
LDAP

■LDAPとは

ディレクトリサービスとは、分散したネットワーク上の各種リソース（ユーザ、サーバ、アプリケーション、プリンタなど）を論理的な名前で管理しやすく系統立ててエンドユーザや管理者に提供する、情報データベースシステム。
→ LDAPはディレクトリサービスのプロトコル。

・LDAPの用語

エントリ：データオブジェクト
DIT(Directory Information Tree)：エントリを階層管理するための管理構造
DSE(Directory Service Entry)：ルートのエントリ
DN(Distinguished Name)：エントリの識別子
RDN(Relative Distinguished Name)：相対識別子



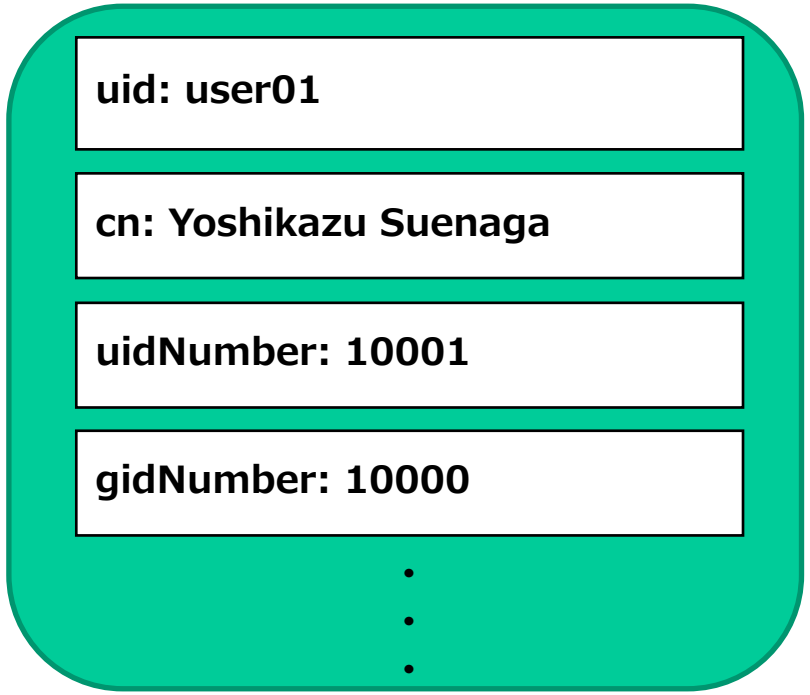
LDAP

■LDAPのデータモデル

・LDAPの用語

オブジェクトクラス：格納データの型
スキーマ：オブジェクトクラスの定義
属性：データの格納対象（dc,o,ou,uid等）
LDIF(LDAP Data Interchange Format)：LDAPに入力するデータのフォーマット

エントリの中身

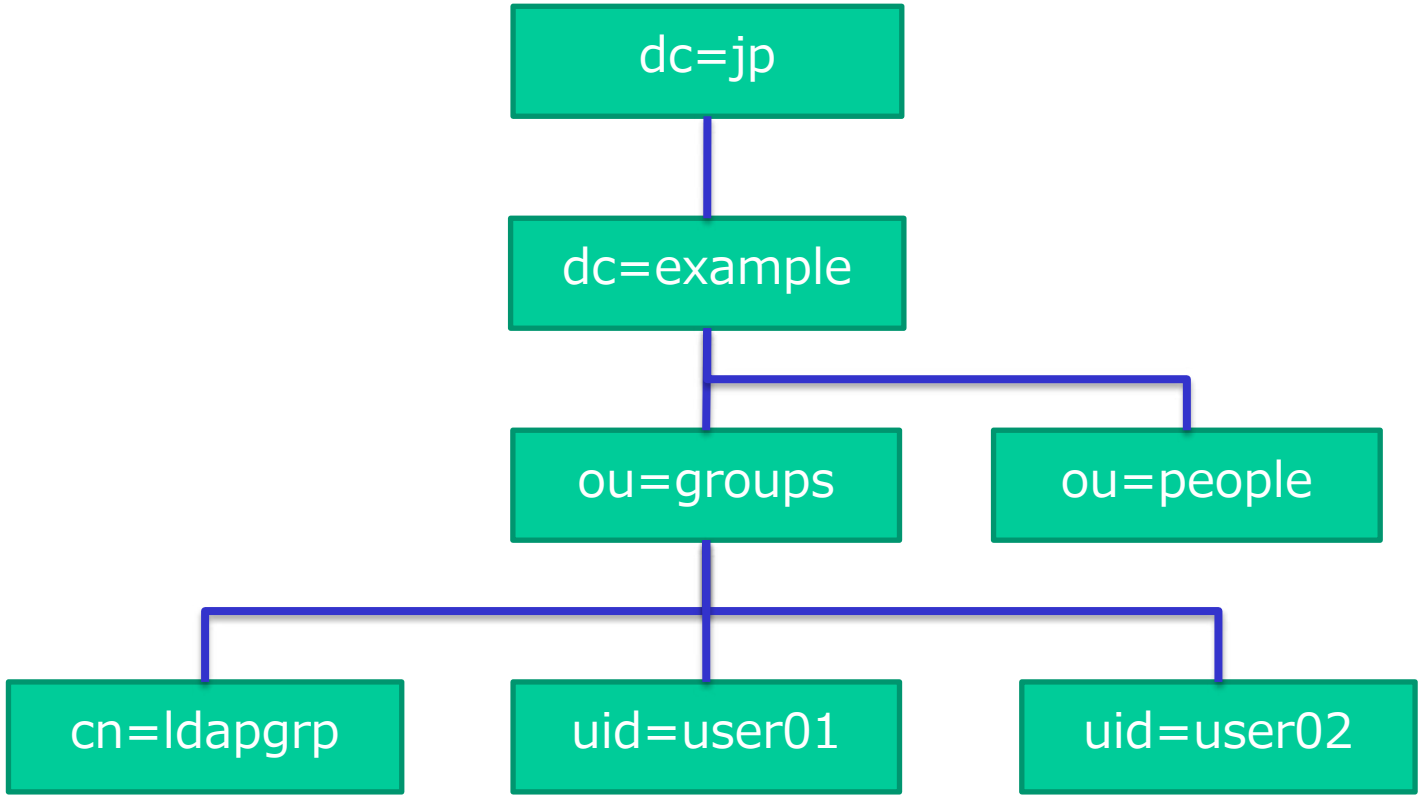


LDIFの例

```
dn: uid=user01,ou=groups,dc=example,dc=jp
uid: user01
cn: Yoshikazu Suenaga
sn: user01
objectClass: posixAccount
objectClass: inetOrgPerson
objectClass: shadowAccount
userPassword: e01ENX1UVDBjVmRiRXFvRCtvU1hGTUttbE9RPT0=
loginShell: /bin/bash
uidNumber: 10001
gidNumber: 10000
homeDirectory: /home/user01
```

■作成したDIT

phpLDAPadmin等を使えばグラフィカルにDITを表示することも可能。



phpLDAPadminの表示

SSSD

SSSD(System Security Services Daemon)とは

リモートディレクトリと認証システムにアクセスするためのシステムサービス。
SSSDクライアントであるローカルシステムをLDAP等の外部のバックエンドシステムに接続できるサービス。

sssdパッケージのインストール

```
# apt install sssd libpam-sss libnss-sss sssd-tools
```

設定は/etc/sssd/sssd.confで行う。sssd.confはインストールされないため手動で作成する。

SSSD

■sssctlコマンド

SSSDの動作確認を行うツール

1.sssd.confのチェック

```
# sssctl config-check
```

2.問い合わせ先ドメインのリスト

```
# sssctl domain-list
```

3.問い合わせ先ドメインの状態

```
# sssctl domain-status ドメイン名
```

4.ユーザーのキャッシュ情報表示

```
# sssctl user-show ユーザー名
```

SSSD

■SSSDとPAM

SSSDのインストール後にPAMにSSSDの認証フローが追加される。

/etc/pam.d/common-auth　（Ubuntu）

```
# here are the per-package modules (the "Primary" block)
auth    [success=3 default=ignore]      pam_unix.so nullok
auth    [success=2 default=ignore]      pam_sss.so use_first_pass
auth    [success=1 default=ignore]      pam_ldap.so use_first_pass

# here's the fallback if no module succeeds
auth    requisite                       pam_deny.so

 .
 .
 .
 .
```

DHCP

■DHCPサーバ（静的割り当て設定）

DHCPサーバとは動的にクライアントに対してネットワーク設定（IP）を割り当てをする。
単に割り当てるだけではなく、ある特定の範囲でクライアントの制限を行うことが可能。

```
subnet 192.168.0.0 netmask 255.255.255.0 {
        option routers                  192.168.0.1;
        option subnet-mask              255.255.255.0;
        ・・・（省略）
        range 192.168.0.10 192.168.0.100;

        host linuc1 {
                hardware ethernet 00:90:96:0f:dc:3a;
                fixed-address 192.168.0.3;
        }
}
```

静的割り当て設定

登録されたMACアドレスのみ割り当てを行うようにすれば、管理外のPCのネットワーク接続を制限することも可能。

まとめ

■まとめ

- ✓ PAM
  - Linuxのシステム認証を制御するフレームワーク
  - Login、SSH等のシステム認証はPAMを使って認証される
- ✓ LDPA
  - ユーザ等のリソースを管理するためのディレクトリサービス
  - LinuxユーザをLDAPサーバ上で一元管理することができる
- ✓ SSSD
  - リモートディレクトリにアクセスするためのシステムサービス
- ✓ DHCP
  - 自動でIPアドレス等のネットワークを使用するための設定をクライアントに付与する
  - MACアドレスで設定するクライアントを限定することも可能（静的割り当て設定）

Q & A

ありがとうございました

https://www.sdtech.co.jp