

LinuC レベル1 Version10.0

技術解説無料セミナー

2020/11/07 開催

主題	1.08 システム管理
	1.10 セキュリティ
副題	1.08.1 アカウント管理
	1.10.1 セキュリティ管理業務の実施 (sudo)

本日の講師



株式会社エンライズコーポレーション (LPI-Japanアカデミック認定校)
橋本 明子

■所属

株式会社エンライズコーポレーション
人財育成部 マネージャ



#LinuC学習中

■経歴

講師派遣業務に従事
(Solaris、Linux、NW、Storage、プログラミング…etc)
→産業機器のプログラマーとして従事
→社内育成の責任者へ

■現在

社員の成長＝会社の成長を掲げ、社内の人財育成に注力
IT未経験者の入社後研修や社員研修の企画/実施/運営/管理
eラーニングサイト教材の監修 等





■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技術者認定資格

✓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

■Version10.0と従来の出題範囲の比較



#LinuC学習中

テーマ	Version 10.0	従来
LinuC-1	仮想技術 ・仮想マシン／コンテナの概念 ・クラウドセキュリティの基礎	← (Version10.0で新設)
	オープンソースの文化 ・オープンソースの定義や特徴 ・コミュニティやエコシステムへの貢献	← (Version10.0で新設)
	その他 → (Version10.0で削除)	アクセシビリティ、ディスククォータ、プリンタの管理、SQLデータ管理、他
LinuC-2	仮想化技術 ・仮想マシンの実行と管理(KVM) ・コンテナの仕組みとDockerの導入	← (Version10.0で新設)
	システムアーキテクチャ ・クラウドサービス上のシステム構成 ・高可用システム、スケーラビリティ、他	← (Version10.0で新設)
	その他 ・統合監視ツール(zabbix) ・自動化ツール(Ansible)	← (Version10.0で出題範囲に含む)
	その他 → (Version10.0で削除)	RAID、記憶装置へのアクセス方、FTPサーバーの保護、他

今回のテーマ

Linuxのアカウント管理に必要な知識を理解する

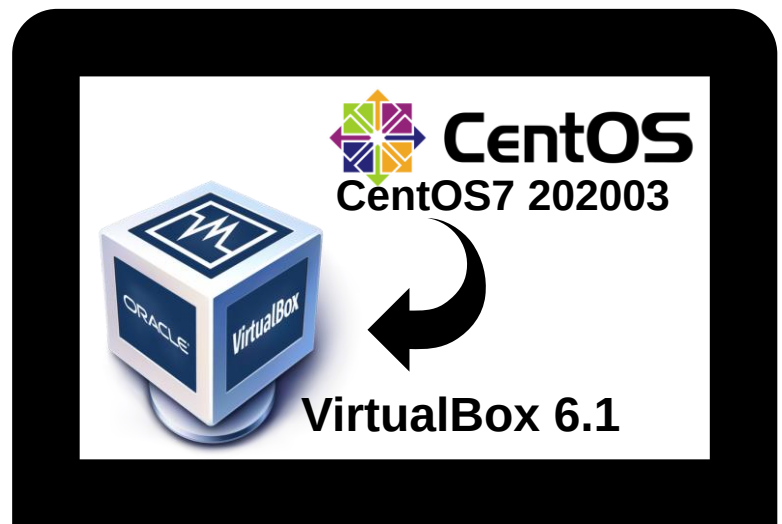
対象範囲

主題	1.08 システム管理
	1.10 セキュリティ
副題	1.08.1 アカウント管理
	1.10.1 セキュリティ管理業務の実施 (sudo)

■講師使用の実機環境



#LinuC学習中



Windows10 Pro

- Virtual Boxとは
ホストOS型の仮想化ソフトウェアの一つ。
ソフトウェアとしてPCを再現する技術。
Windows/Mac/Linux上でも動作。
ダウンロードは下記より。
<http://www.oracle.com/technetwork/server-storage/virtualbox/downloads/>
- CentOSとは
有名なRedhat系Linuxディストリビューションの一つ。
CentOS Projectが提供。
ダウンロードは下記より。
<https://www.centos.org/download/>

インストール時のパラメータ

ネットワークとホスト名 : Ehternet オン
ソフトウェアの選択 : GNOME Desktop

■コマンド書式



#LinuC学習中

プロンプト

Linuxがコマンドを受け付ける準備が整ったことを表す記号



コマンドライン

\$ コマンド名 [オプション] [引数] ←

↑
Linuxに出す指示
意味のある英単語や
省略形が多い

↑
コマンドの実行内容を
選択/調整するための文字列
-a、-i、-r など
ハイフンと英字の組み合わせが基本

↑
コマンド動作する対象
ファイル名が多い

[]…必要に応じてつける

←…エンターキーを押す

■アカウントとは

システム、アプリケーションを利用時に必要になる権利のこと。

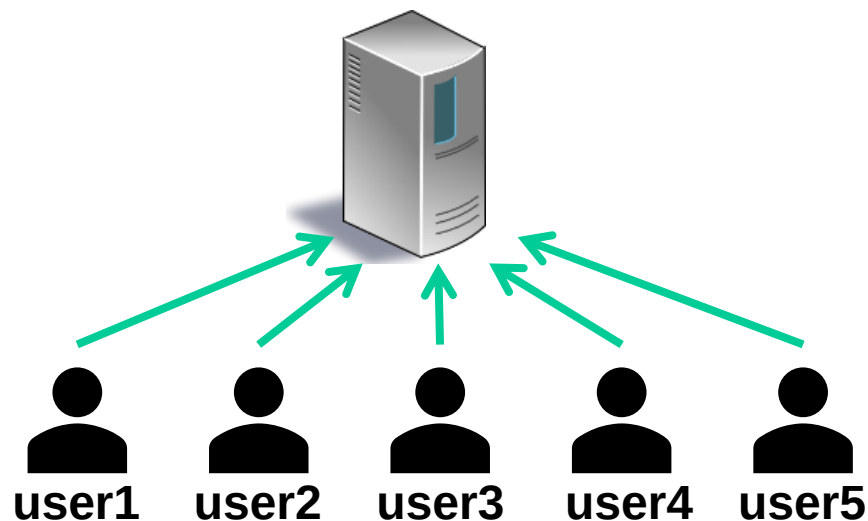


#LinuC学習中

Linuxシステムはマルチユーザー環境のため、システムや利用ユーザーを保護するためにユーザー名とパスワードの組み合わせが正しいユーザーのみログインが可能。

■マルチユーザー環境とは

複数のユーザーが同時にログインし、並列で処理が実行できる環境のこと。



■管理者ユーザー（スーパーユーザー）

「root」

Linux内のあらゆる権限を行使できる特別なユーザー。
インストール時に生成される。



#LinuC学習中

■一般ユーザー

「名称任意」

Linux内の閲覧権限を持ち、管理者ユーザーに決められた範囲で操作を行えるユーザー。
OSインストール時にやアプリケーションのインストール時に生成される場合が多いが、
管理者ユーザーがコマンドにより生成することも可能。

■Linuxのユーザー体系

Linuxのユーザーは必ず一つ以上のグループに所属する。



#LinuC学習中



プライマリグループ
ユーザーがメインで所属し、
ファイルなどを作成した際に
所有グループとなる。
1ユーザーに1つ。

サブグループ
1ユーザーで0個以上のサブ
グループに参加出来る。ア
クセス権の参照に使われる。

■ユーザーアカウント情報 /etc/passwd

※passwordではない

■グループアカウント情報 /etc/group

■パスワード情報 /etc/shadow



#LinuC学習中

ユーザーアカウント情報は/etc/passwdファイルに存在する。



#LinuxC学習中

enrise:x:1000:1000:enrise:/home/enrise:/bin/bash

①ユーザ名 ②パスワード ③UID ④GID ⑤コメント ⑥ホームディレクトリ ⑦ログインシェル

※④にはプライマリグループのGIDが表示される。

グループアカウント情報は/etc/groupファイルに存在する



#LinuxC学習中

enrise:x:1000:enrise

①グループ名 ②パスワード ③GID ④ユーザリスト

※④にはサブグループとして所属しているユーザが表示される。

/etc/passwdファイルや/etc/groupファイルの
パスワード欄は「x」となっており、
実際のパスワード情報は/etc/shadow (gshadow) ファイルに格納される。



#LinuC学習中

enrise:\$6\$BLdL4jAH\$VURek9UcSaCR4tbqcDm1fe7jDe
zw9F9xaF3io7Ib6JKGUY69OVaRcvr2.44WfpVCenTSBr
TIwgJwsEoCtePU.1:16898:3:90:10:7:17166:

①ユーザ名 ②暗号化されたパスワード ③パスワードに関する情報

■ユーザー情報の確認①

\$ id [ユーザー名] ↵

※ユーザー名省略時は「操作中のユーザー」

■ユーザー情報の確認②

\$ getent データベース [キー] ↵



#LinuC学習中

■ユーザーの切り替え

\$ su - [ユーザー名] ↵

※ユーザー名省略時は「root」ユーザーに切り替える

※一般ユーザーから別ユーザーに切り替えるときは別ユーザーのパスワードが必須



#LinuC学習中

■元のユーザーに戻る

\$ exit ↵

■管理者権限コマンドの実行

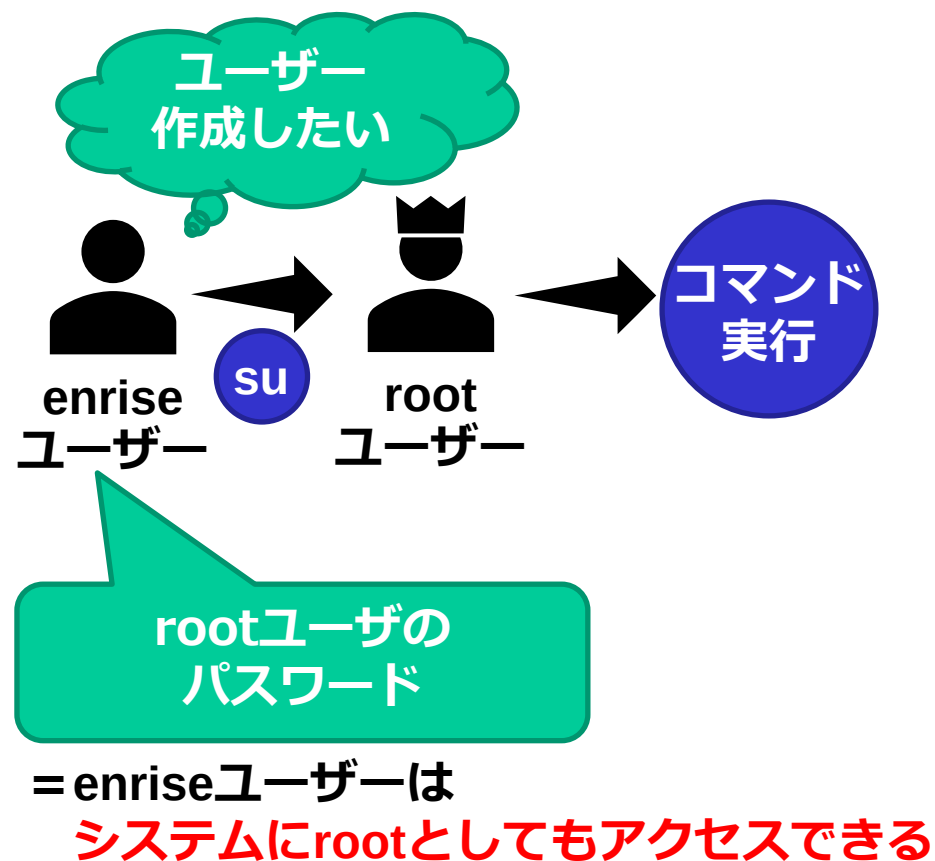
\$ sudo 管理コマンド ↵

※/etc/sudoersファイルに記載が必要

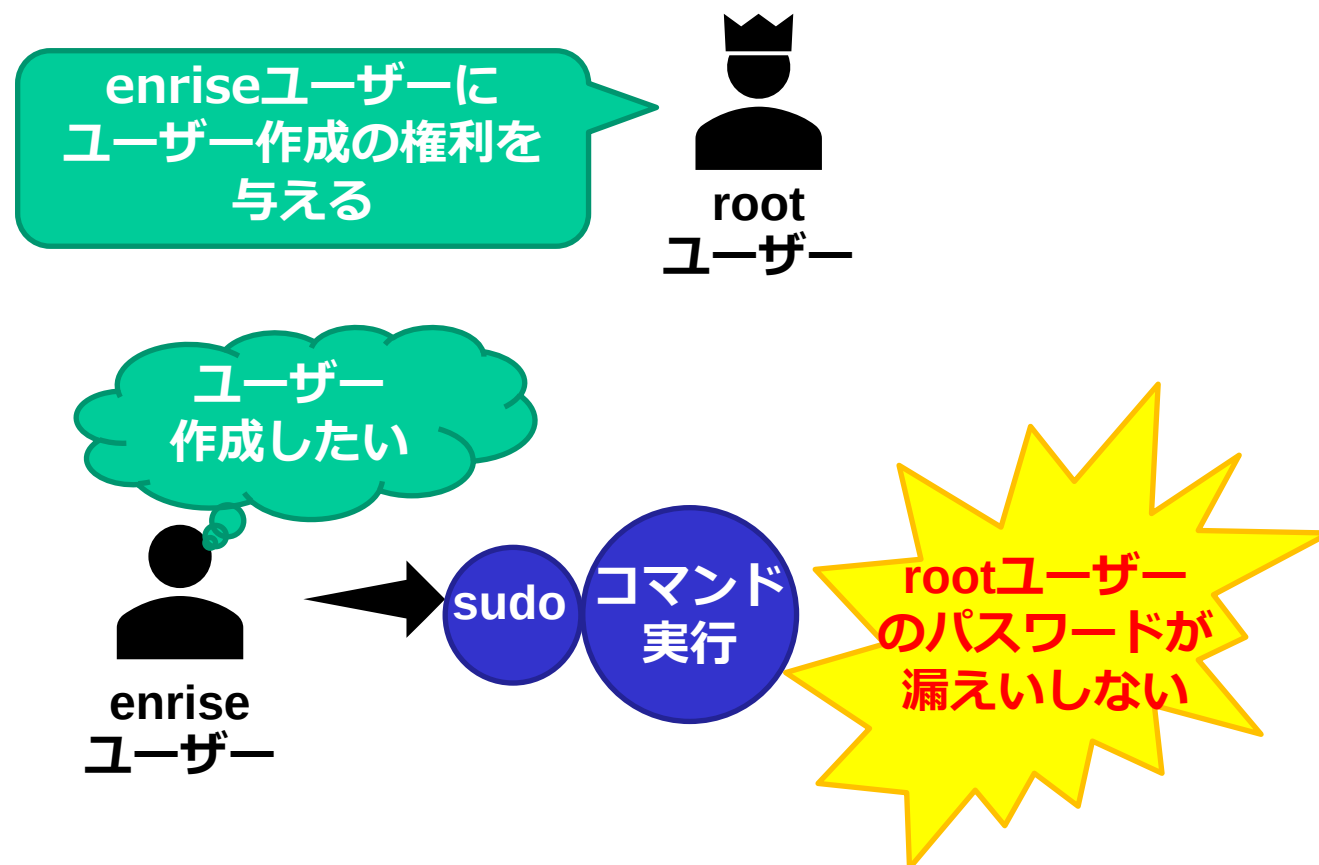


#LinuC学習中

■suコマンド



■sudoコマンド



■ **/etc/sudoers** ファイル

sudo コマンドで管理コマンドを実行する許可を与えるファイル。
編集は「**visudo**」コマンドから行う。



#LinuC 学習中

【/etc/sudoers ファイルの書式】

ユーザ名 ホスト名=(実行ユーザ名) [NOPASSWD:] コマンド

【設定例】

```
# visudo
(略)
```

```
#enrise ユーザに useradd コマンドを使用させるときの設定
enrise ALL=(ALL) /sbin/useradd
```

■ユーザーの作成

【useraddコマンドの書式】



#LinuC学習中

```
# useradd [オプション] ユーザー名↵
```

コマンド実行例	意味
# useradd testuser↵	testuserユーザーをデフォルト値で作成
# useradd -u 1111 testuser↵	testuserユーザーの UID を1111で作成
# useradd -g users testuser↵	testuserユーザーの プライマリグループ をusersで作成
# useradd -G testusers testuser↵	testuserユーザーの サブグループ をtestusersで作成
# useradd -c TestUser testuser↵	testuserユーザーの コメント をTestUserで作成
# useradd -d /home/DIR testuser↵	testuserユーザーの ホームディレクトリ を/home/DIRで作成 ※/etc/login.defsで「CREATE_HOME no」の場合、 -m オプションが必要
# useradd -s /bin/tcsh testuser↵	testuserユーザーの ログインシェル を/bin/tcshで作成

※オプションは一度に複数指定可能

■useraddコマンドのオプションとファイルの関係



#LinuC学習中

/etc/passwdファイル

```
enrise:x:1000:1000:enrise:/home/enrise:/bin/bash
```

-u
-g
-c
-d
-s

/etc/groupファイル

```
enrise:x:1000:enrise
```

-G

<例題挑戦>

主題1.08 システム管理

1.08.1 アカウント管理 (<https://linuc.org/study/samples/1142/>)

■作成されるユーザーのデフォルト値

useraddのデフォルト値は**-D**オプションで確認

※/etc/default/useraddファイルでも確認可能

```
# useradd -D
GROUP=100      ← GIDの指定 ※1
HOME=/home     ← ホームディレクトリは/home以下にユーザー名で設定
INACTIVE=-1    ← パスワード無効後、ユーザーアカウントが停止する期間
EXPIRE=        ← ユーザーアカウントの有効期間
SHELL=/bin/bash ← デフォルトのログインシェル名
SKEL=/etc/skel  ← ホームディレクトリのテンプレートディレクトリ
CREATE_MAIL_SPOOL=yes ← メールの受信フォルダの作成有無
```

※1 /etc/login.defsファイルで「USERGROUPS_ENAB yes」の場合、
ユーザー名と同じ名前グループを作成し、プライマリグループとする。

■/etc/login.defsファイル

作成されるユーザーの設定値に影響を与えるファイル



#LinuC学習中

■作成されるユーザーのホームディレクトリ

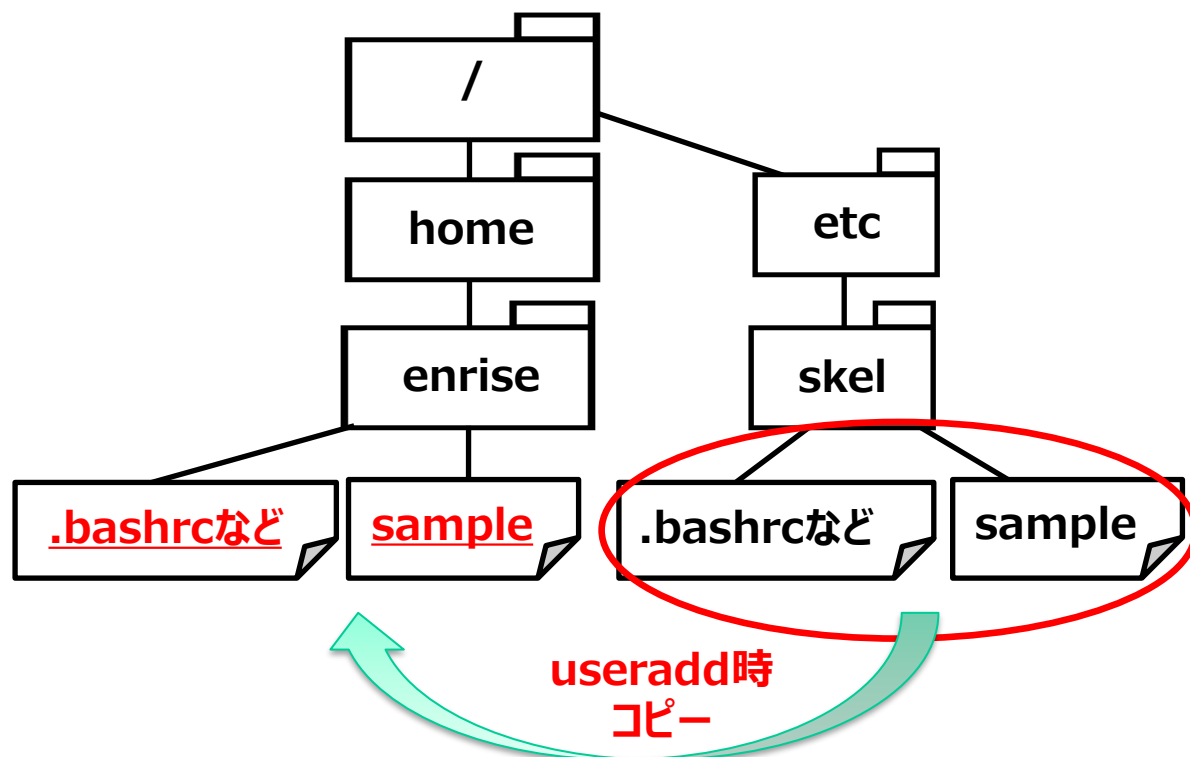
ユーザー作成と同時に作成されるホームディレクトリは、初めからいくつかの隠しファイルが含まれているが、

「**/etc/skel**」がひな形のディレクトリとなっているためである。

あらかじめユーザーのホームディレクトリに配布しておきたいファイルがあればスケルトンディレクトリに配置をしておくとい。



#LinuC学習中



■ユーザーのパスワード設定

【passwdコマンドの書式】

```
$ passwd [オプション] [ユーザー名]↵
```

※オプションなしでパスワード変更
※ユーザー名省略時は現在のユーザー

オプション	意味
-l	指定アカウントをロック (lock)
-u	指定アカウントをアンロック (unlock)



#LinuC学習中

■ユーザーの情報変更

【usermodコマンドの書式】



#LinuC学習中

usermod [オプション] ユーザー名↵

コマンド実行例	意味
# usermod -l user testuser↵	testuserユーザーの 名前 をuserに変更
# usermod -u 2222 testuser↵	testuserユーザーのUIDを2222に変更
# usermod -g users testuser↵	testuserユーザーのプライマリグループをusersに変更
# usermod -G testusers testuser↵	testuserユーザーのサブグループをtestusersに変更
# usermod -c TU testuser↵	testuserユーザーのコメントをTUに変更
# usermod -d /home/DIR testuser↵	testuserユーザーのホームディレクトリを/home/DIRに変更
# usermod -s /bin/tcsh testuser↵	testuserユーザーのログインシェルを/bin/tcshに変更
# usermod -L testuser↵	testuserユーザーのアカウントを ロック
# usermod -U testuser↵	testuserユーザーのアカウントを アンロック

■ユーザーの削除

【userdelコマンドの書式】



#LinuxC学習中

```
# userdel [オプション] ユーザー名↵
```

コマンド実行例	意味
# userdel testuser↵	testuserユーザーを削除
# userdel -f testuser↵	testuserユーザーが ログイン中でも 削除
# userdel -r testuser↵	testuserユーザーの ホームディレクトリ、メールディレクトリも合わせて 削除



■グループの作成

【groupaddコマンドの書式】

```
# groupadd [オプション] ユーザー名↵
```

コマンド実行例	意味
# groupadd testgroup↵	testgroupグループをデフォルト値で作成
# groupadd -g 1111 testgroup↵	testgroupグループの GID を1111で作成

■グループの情報変更

【groupmodコマンドの書式】

```
# groupmod [オプション] ユーザー名↵
```

コマンド実行例	意味
# groupmod -g 2222 testgroup↵	testgroupグループの GID を2222へ変更
# groupmod -n group testgroup↵	testgroupグループの 名前 をgroupへ変更

■グループの削除

【groupdelコマンドの書式】



#LinuC学習中

groupdel [オプション] ユーザー名↵

コマンド実行例	意味
# groupdel testgroup↵	testgroupグループを削除 ※プライマリグループになっているグループは削除不可
# groupdel -f testgroup↵	testgroupグループがプライマリグループでも強制的に削除

<例題挑戦>

主題1.08 システム管理

1.08.1 アカウント管理 (<https://linuc.org/study/samples/1285/>)

■chsh - シェルの変更

`usermod -s シェル ユーザー名` と同等。



#LinuC学習中

■vipw - ユーザー情報の変更

`/etc/passwd`ファイルの直接編集。`usermod`でできることと同等。

`-s`でshadowファイル、`-g`でgroupファイルの編集も可能。

■gpasswd - グループパスワード設定やユーザーの所属グループ変更



分類	ファイル	説明
ユーザー	<code>/etc/passwd</code>	ユーザー情報
	<code>/etc/shadow</code>	ユーザーのパスワード情報
	<code>/etc/default/useradd</code>	ユーザー作成時のデフォルト情報
グループ	<code>/etc/group</code>	グループ情報
ユーザー &グループ	<code>/etc/login.defs</code>	ユーザー作成時のユーザーやグループ、 パスワード設定時のルール



分類	コマンド	説明
ユーザー	# useradd [オプション] ユーザー名↵	ユーザーの作成
	# passwd [オプション] [ユーザー名]↵	ユーザーのパスワード設定
	# usermod [オプション] ユーザー名↵	ユーザー情報の変更
	# userdel [-r] ユーザー名↵	ユーザーの削除
グループ	# groupadd [オプション] グループ名↵	グループの作成
	# gpasswd [オプション] グループ名↵	グループのパスワード設定 ユーザーの所属グループの調整
	# groupmod [オプション] グループ名↵	ユーザー情報の変更
	# groupdel グループ名↵	ユーザーの削除