

PAM

(Pluggable Authentication Modules)

2012/9/9

1

ユーザ認証 (ローカル)

- /etc/passwd
 - 暗号化されたパスワードが誰にでも見えてしまう
- /etc/shadow
 - 暗号化されたパスワードはrootのみが見れる
- DES
 - 4qA47fywT8smU (実質11文字)
- MD5
 - \$1\$zMIIZ8NDSctENoJ7KxWgzflvrsIj931 (実質22文字)

2012/9/9

2

ユーザ認証 (リモート)

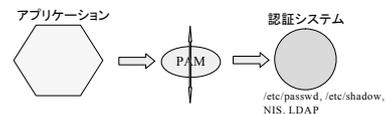
- NIS, NIS+
 - NISサーバとパスワードファイル(他のファイルも)を共有可能
 - ネットワーク上で暗号化されたパスワードを盗聴可
- LDAP
 - ディレクトリサービス(簡易データベース)
 - Transport Layer Security (TLS) をサポート
 - slapasswd
 - Simple Authentication and Security Layer (SASL)
- その他 smbpasswd, htpasswd

2012/9/9

3

PAM

- ユーザ認証と許可をアプリケーションから分離する
 - 認証: Authentication
 - その人が誰であるかを確認する
 - 許可: Authorization
 - その人に何を許可するか決める(サービスを割り当てる)



2012/9/9

4

PAMの設定

- /etc/pam.d
 - サービス名のついたファイル
 - login poweroff qpopper sshd wdm xscreensaver chsh
 - other ppp reboot su xdm ftp passwd samba system-auth
 - system-auth: 各設定ファイルから参照されるデフォルト設定
 - login: loginコマンド使用時設定
 - other: 該当するサービスファイルが無い場合の設定(通常全て禁止)

2012/9/9

5

login

auth	required	/lib/security/pam_securetty.so
auth	required	/lib/security/pam_stack.so service=system-auth
auth	required	/lib/security/pam_nologin.so
account	required	/lib/security/pam_stack.so service=system-auth
account	required	/lib/security/pam_stack.so service=system-auth
password	required	/lib/security/pam_stack.so service=system-auth
session	required	/lib/security/pam_stack.so service=system-auth
session	optional	/lib/security/pam_console.so

タイプ

- auth: 認証時に使用されるモジュール(プログラム)
- account: 許可の確認に使用されるモジュール
- passwd: passwordの変更で使用されるモジュール
- session: ユーザの認証前または認証後に使用したいモジュール

機能

- required: 認証に失敗した場合、認証を拒否
- sufficient: 認証が成功し、かつその前の required 型で認証に成功した場合に認証を与える
- optional: これ以外の全てで失敗した場合、このモジュールがタイプの認証を与える

2012/9/9

6

system-auth

```
auth      required  /lib/security/pam_env.so
auth      sufficient /lib/security/pam_unix.so likeauth nullok
auth      required  /lib/security/pam_deny.so
account   required  /lib/security/pam_unix.so
password  required  /lib/security/pam_cracklib.so retry=3 type=
password  sufficient /lib/security/pam_unix.so nullok use_authtok md5 shado
password  required  /lib/security/pam_deny.so
session   required  /lib/security/pam_limits.so
session   required  /lib/security/pam_unix.so
```

2012/9/9

7

PAMの利用

- SambaとLinuxのパスワードの統合
- PAMモジュールの作成(独自認証)
- その他……………

2012/9/9

8