5.2 パスワードの管理

5.2.1 パスワードの期限設定

シャドウパスワードを使用してアカウントの管理を行っている場合、パスワードエージング機能（パスワードの期限設定）が使用できます。

パスワードエージング機能は、ユーザーに対して定期的にパスワード変更を強制することができるため、セキュリティの向上を図ることができます。

■ パスワード期限の確認

パスワードの期限確認は、chage コマンドの「-l」オプションを用います。

```
# chage -l mickey
Last password change                                    : Nov 12, 2012
Password expires                                        : never
Password inactive                                       : never
Account expires                                         : never
Minimum number of days between password change          : 0
Maximum number of days between password change          : 99999
Number of days of warning before password expires       : 7
```

Last password change	パスワードの最終更新日を表します。
Password expires	パスワードの有効期限日を表します。 「Last password change」と「Maximum number ...」から自動的に算出されます。
Password inactive	パスワードの有効期限に依存するアカウント期限日を表します。 「Last password change」、「Maximum number ...」、「inactive」から自動的に算出されます。
Account expires	パスワードの変更とは無関係な、アカウントの期限日を表します。 無期限にする場合は 1969-12-31 を設定します。
Minimum number of days between password change	パスワード変更後、再度のパスワード変更を禁止する期間です。 期限を指定しない場合、 0 を設定します。
Maximum number of days between password change	パスワードの有効期限です。 パスワード変更後にこの期間を過ぎた場合、ログイン時にパスワード変更を強制します。パスワード期限を無効にする場合、99999 を設定します。
Number of days of warning before password expires	パスワードの期限切れの何日前から警告するか設定します。 警告期間に入ると、ログイン時に警告が表示されます。

■ パスワード期限の設定

chage コマンドの引数にユーザー名のみを指定した場合は、対話的にユーザーのパスワード期限を変更することができます。変更点のみを入力します。

```
# chage  mickey
Changing the aging information for mickey
Enter the new value, or press ENTER for the default

    Minimum Password Age [0]: ↵
    Maximum Password Age [99999]: 90
    Last Password Change (YYYY-MM-DD) [2012-09-01]: ↵
    Password Expiration Warning [7]: 14
    Password Inactive [-1]: ↵
    Account Expiration Date (YYYY-MM-DD) [1969-12-31]: ↵
#
```

また、オプションを指定することにより、非対話で設定することができます。

```
# chage  -M  90  -W  14  mickey
# chage  -l  mickey
Last password change                                    : Sep 01, 2012
Password expires                                        : Nov 30, 2012
Password inactive                                       : never
Account expires                                                 : never
Minimum number of days between password change          : 0
Maximum number of days between password change          : 90
Number of days of warning before password expires       : 14
```

書式

```
chage [-m 最小]  [-M 最大]  [-W 警告]  [-I 無効]
      [-d 最近の変更]  [-E アカウント期限切れ]  ユーザー名
```

- 初回のログイン時にパスワード変更を強制したい場合には、パスワード変更日付に 0 を指定します。

```
 # chage  -d  0  mickey
```

- パスワードの有効期限は、最短でも 30 日は設定します。

パスワード有効期限が切れた場合は、ログイン時にパスワードの変更が強制されます。

```
login: mickey
Password: 現在のパスワード
You are required to change your password immediately (password aged)
Changing password for mickey
(current) UNIX password: 現在のパスワード
New UNIX password: 新しいパスワード
Retype new UNIX password: 新しいパスワード
$
```

■ パスワード期限のデフォルト値

ユーザー登録時にパスワード期限やアカウント期限を明示しない場合にはデフォルト値が使用されます。デフォルト値は以下のファイルに記述されています。

- /etc/default/useradd
- /etc/login.defs

/etc/default/useradd

```
# useradd defaults file
GROUP=100
HOME=/home
INACTIVE=-1 ←―― パスワード無効日数
EXPIRE= ←―― アカウントの期限
SHELL=/bin/bash
SKEL=/etc/skel
```

/etc/login.defs

```
      :
PASS_MAX_DAYS   99999 ←―― パスワードの有効期限
PASS_MIN_DAYS   0 ←―― パスワードの最小日数
PASS_MIN_LEN    5
PASS_WARN_AGE   7 ←―― パスワード期限切れ警告開始日数
      :
```

5.2.2 アカウントのロック

一時的にユーザーのログインを禁止したり、各種サービスの提供を中止したりする場合には、アカウントをロックします。アカウントのロックは passwd コマンド、もしくは usermod コマンドを使用します。

passwd コマンドの例

```
# grep  mickey  /etc/shadow
mickey:$1$chKlWlkR$N4YZFadQETS71Jvc0vzn//:13123:0:99999:7::
# passwd  -l  mickey          ← アカウントのロック
Locking password for user mickey.
passwd: Success
# grep  mickey  /etc/shadow   ← 暗号化文字列の先頭に「!!」が付加される
mickey:!!$1$chKlWlkR$N4YZFadQETS71Jvc0vzn//:13123:0:99999:7:::
# passwd  -u  mickey          ← アカウントのロック解除
Unlocking password for user mickey.
passwd: Success.
# grep  user1  /etc/shadow    ← 暗号化文字列の先頭の「!!」が削除される
mickey:$1$chKlWlkR$N4YZFadQETS71Jvc0vzn//:13123:0:99999:7:::
```

usermod コマンドの例

```
# usermod  -L  mickey
# grep  mickey  /etc/shadow   ← 暗号化文字列の先頭に「!」が付加される
mickey:!$1$chKlWlkR$N4YZFadQETS71Jvc0vzn//:13123:0:99999:7:::
# usermod  -U  mickey
# grep  mickey  /etc/shadow
mickey:$1$chKlWlkR$N4YZFadQETS71Jvc0vzn//:13123:0:99999:7:::
```

passwd コマンドと usermod コマンドによるアカウントロックの方法には若干の違いがあるため、ロックを行ったコマンドで解除する必要があります。

また、アカウントロックは/etc/shadow 内のパスワードフィールドの暗号化文字列を操作するため、独自に認証機能を持つ（システムアカウントのパスワードを使わない）アプリケーションでは利用できません。

5.2.3 パスワード強化設定

パスワードは文字数を多く様々な種類の文字を組み合わせることによって、他人に推測されにくくすることができます。passwd コマンドを用いてパスワードを変更する際に、以下の設定を行うことにより単純なパスワードの設定を拒否することができます。

■ cracklib ・ pam_cracklib

cracklib は、単純なパスワードや辞書に登録されているパスワードを検査するライブラリです。一般的なディストリビューションでは、passwd コマンドが用いる PAM モジュール[23]に pam_cracklib モジュールを設定することにより、passwd コマンド実行時に cracklib を使用することができます。pam_cracklib モジュールの設定を変更することにより、パスワード文字列に含まれる小文字、大文字、数字、その他の文字数を制限することができます。

■ /etc/pam.d/system-auth

pam_cracklib モジュールの設定は、/etc/pam.d/system-auth ファイルに記述します。

/etc/pam.d/system-auth

```
#%PAM-1.0
auth        required      pam_env.so
auth        sufficient    pam_fprintd.so
auth        sufficient    pam_unix.so nullok try_first_pass
auth        requisite     pam_succeed_if.so uid >= 500 quiet
auth        required      pam_deny.so
account     required      pam_unix.so
account     sufficient    pam_localuser.so
account     sufficient    pam_succeed_if.so uid < 500 quiet
account     required      pam_permit.so
password    requisite     pam_cracklib.so try_first_pass retry=3 type=
password    sufficient    pam_unix.so sha512 shadow nullok try_first_pass use_au
thtok
password    required      pam_deny.so
session     optional      pam_keyinit.so revoke
session     required      pam_limits.so
session     [success=1 default=ignore] pam_succeed_if.so service in crond quiet
use_uid
session     required      pam_unix.so
```

[23] PAM（Pluggable Authentication Modules）とは、login や su などのユーザー認証を必要とするアプリケーションが利用する、共通の認証の仕組みです。認証部分がモジュールとして提供されるため、各アプリケーションは使用するモジュールを選択することにより認証方法を選択することができます。

pam_cracklib モジュールでは、一般ユーザーが自分のパスワードを passwd コマンドで変更する際に、文字の種類ごとにパスワードに設定する文字数を制限することができます。

文字数や種類の制限には、以下のオプションを pam_cracklib モジュールの設定に追加します。

オプション名	効果	デフォルト値
dcredit	パスワードに含むべき数字の数を負数で指定	1
ucredit	パスワードに含むべきアルファベットの大文字の数を負数で指定	1
lcredit	パスワードに含むべきアルファベットの小文字の数を負数で指定	1
ocredit	パスワードに含むべき数字、アルファベット以外の文字数を負数で指定	1
minlen	パスワードの最小文字数	9

例) 数字、大文字、その他の文字を最低 1 文字含む 8 文字以上のパスワードを要求する場合

```
    :
account   required    pam_permit.so

password  requisite   pam_cracklib.so try_first_pass retry=3 type= ¥
                      dcredit=-1  ucredit=-1  lcredit=0 ocredit=-1   minlen=8
password    sufficient    pam_unix.so sha512 shadow nullok try_first_pass use_au
thtok
    :
```

※ 参考　minlen と dcredit、ucredit、lcredit、ocredit の関係

dcredit などに 0 以上の値を設定した場合は、文字種ごとの文字数を制限する代わりに、minlen で設定するパスワードの最小文字数から dcredit などの文字数が引かれた値を最小文字数として設定するはたらきを持ちます。

パスワードに含まれる字種によらずパスワードの最小文字数を 10 に設定する

```
      dcredit=0 ucredit=0 lcredit=0 ocredit=0 minlen=10
```

パスワードに数字を含む場合には、1 文字分に限り、パスワードの最小文字数を短く設定することを許可する

(数字を含むパスワードであればパスワードの最小文字数は 9 文字、数字を含まない場合には 10 文字)

```
      dcredit=1  ucredit=0 lcredit=0 ocredit=0 minlen=10
```

【実習】 パスワードの管理

1. atom ユーザーにパスワード期限を 90 日に設定し、パスワードの最近の変更の日付を 0 に設定します。これにより、atom ユーザーは次回ログイン時にパスワードの変更を強制されます。

```
# chage  -M  90  -d  0  atom
# chage  -l  atom
```

2. Ctrl + Alt + F2 によりコンソールに切り替えて、atom ユーザーでログインします。このとき、パスワードの変更が強制されます。

```
stationX login:  atom
Password:  system5
(current) UNIX password:  system5
New UNIX password:  qwer12#$
Retype new UNIX password:  qwer12#$
```

3. Alt + F1 または、Alt + F7 で X の画面に戻ります。

4. パスワードの設定を強化するため、pam_cracklib モジュールに設定を追加します。/etc/pam.d/system-auth を以下の通り編集し、数字、アルファベットの大文字、記号を含む 8 文字以上のパスワードを要求するように設定します。

```
# vi  /etc/pam.d/system-auth
```

/etc/pam.d/system-auth

```
    :
password  requisite pam_cracklib.so try_first_pass retry=3 type=  ¥
                    dcredit=-1  ucredit=-1  lcredit=0 ocredit=-1   minlen=8
password  sufficient  /lib/security/$ISA/pam_unix.so nullok use_authtok md5
shadow
password  required   /lib/security/$ISA/pam_deny.so
    :
```

5. Ctrl + Alt + F2 によりコンソールに切り替えて、atom ユーザーのパスワードを変更します。

ログインしていない場合はログインを行う

```
stationX login: atom
Password:  qwer12#$
```

```
$ passwd
Changing password for user atom.
Changing password for atom
(current) UNIX password:  qwer12#$
New UNIX password:  atom1234
BAD PASSWORD: is too simple
New UNIX password:  5678ATOM!/
Retype new UNIX password:  5678ATOM!/
passwd: all authentication tokens updated successfully.
$ exit
```

cracklib の制限をクリアしていないパスワード

6. Alt + F1 または、Alt + F7 で X の画面に戻り、root ユーザーで atom ユーザーのパスワードを戻しておきます。

```
# passwd  atom
Changing password for user atom.
New UNIX password:  sys1234
Retype new UNIX password:  sys1234
passwd: all authentication tokens updated successfully.
#
```

※ root ユーザーは pam_cracklib モジュールの制限を受けません。