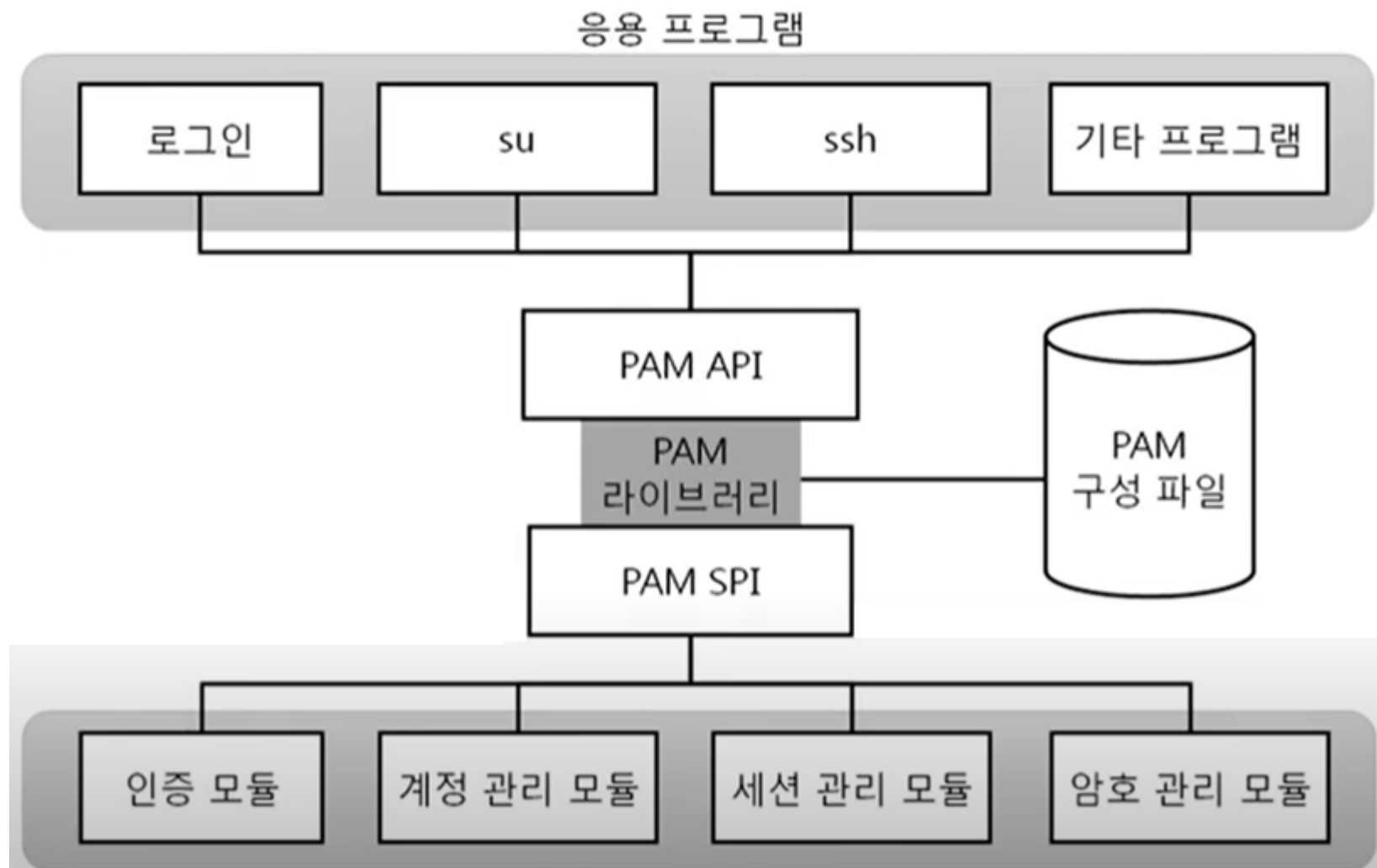


# PAM(Pluggable Authentication Module)

- 사용자를 인증하고 서비스에 대한 접근을 제어하는 모듈화된 방법
- 응용 프로그램들에게 사용자 인증 방법을 선택할 수 있는 공유 라이브러리의 묶음 제공
- PAM 목적은 소프트웨어 개발과 안전한 권한 부여 및 인증 체계를 분리하는 것
  - 특정 서비스에 대한 사용자(또는 그룹)들의 허가 목록 파일
  - 특정 서비스에 대한 사용자(또는 그룹)들의 거부 목록 파일
  - 사용자의 패스워드 길이 제한
  - 메모리 및 프로세스 제한 등



/etc/pam.d/remote

```
#auth required pam_securetty.so  
#password requisite pam_pwquality
```

/etc/pam.d/su

```
#auth required pam_securetty.so  
#password requisite pam_pwquality
```

**/lib/security**

pam\_securetty.so

pam\_nologin.so

pam\_wheel.so

pam\_pwquality.so

/etc/securetty

/etc/nologin

/etc/group

/etc/security/pwquality.conf

## ◆ PAM의 구성

- 라이브러리
  - /lib64/security(또는 /lib/security)
- PAM을 이용하는 서비스 디렉터리
  - /etc/pam.d
  - /etc/pam.d/other

# PAM 지원 모듈 목록

```
[root@localhost security]# pwd
/lib64/security
[root@localhost security]# ls
pam_access.so      pam_exec.so        pam_issue.so       pam_loginuid.so
pam_cap.so         pam_faildelay.so   pam_keyinit.so     pam_mail.so
pam_chroot.so      pam_faillock.so    pam_krb5            pam_mkhome.so
pam_console.so     pam_filter          pam_krb5.so         pam_motd.so
pam_cracklib.so    pam_filter.so      pam_krb5afs.so      pam_namespace.so
pam_debug.so       pam_fprintd.so     pam_lastlog.so      pam_nologin.so
pam_deny.so        pam_ftp.so         pam_limits.so       pam_oddjob_mkhome.so
pam_echo.so        pam_gnome_keyring.so pam_listfile.so     pam_permit.so
pam_env.so         pam_group.so       pam_localuser.so    pam_postgres.so
[root@localhost security]#
```

# PAM 설정 파일

```
[root@localhost pam.d] # pwd
/etc/pam.d
[root@localhost pam.d] # ls
atd                  gdm-password~    postlogin          su
chfn                 gdm-pin          postlogin-ac       su-l
chsh                 gdm-smartcard    ppp                sudo
config-util         ksu              remote             sudo-i
crond                liveinst         runuser            system-auth
cups                 login            runuser-l          system-auth-ac
fingerprint-auth    other            setup              systemd-user
fingerprint-auth-ac password          smartcard-auth     vlock
gdm-autologin        password-auth    smartcard-auth-ac  vmtoolsd
gdm-fingerprint      password-auth-ac smtp                xserver
gdm-launch-environment pluto
gdm-password         polkit-1
[root@localhost pam.d] #
```

# PAM 설정 파일 구성

```
[root@localhost pam.d] # pwd
/etc/pam.d
[root@localhost pam.d] # ls -l login
-rw-r--r--. 1 root root 796 6월 18 2014 login
[root@localhost pam.d] # cat login
#%PAM-1.0
auth [user_unknown=ignore success=ok ignore=ignore default=bad] pam_securetty.so
auth      substack      system-auth
auth      include       postlogin
account   required      pam_nologin.so
account   include       system-auth
password  include       system-auth
# pam_selinux.so close should be the first session rule
session   required      pam_selinux.so close
session   required      pam_loginuid.so
session   optional      pam_console.so
# pam_selinux.so open should only be followed by sessions to be executed in the us
er context
session   required      pam_selinux.so open
session   required      pam_namespace.so
session   optional      pam_keyinit.so force revoke
session   include       system-auth
session   include       postlogin
-session  optional      pam_ck_connector.so
[root@localhost pam.d] #
```

# PAM 설정 파일 구성

<u>type</u>	<u>control</u>	<u>module_name</u>	<u>module-arguments</u>
①	②	③	④

auth	include	postlogin
account	required	pam_nologin.so
session	include	system-auth
session	required	pam_namespace.so
password	include	system-auth

/etc/pam.d/login



## ① Type

auth	include	postlogin
account	required	pam_nologin.so
session	include	system-auth
session	required	pam_namespace.so
password	include	system-auth

- 어떤 타입의 인증이 사용될 것인지를 알려주는 항목

type	설명
account	<p>사용자 계정을 확인하는 절차 제공</p> <ul style="list-style-type: none"> <li>- 사용자가 해당 서비스에 접근이 허용되는지 여부</li> <li>- 계정 활성화/비활성화 여부 확인</li> <li>- 패스워드 기간 만료 여부를 검사</li> <li>- 특정 시간대에 접속 시도 가능여부 확인</li> </ul>
auth	<p>사용자 패스워드 유효성 검사와 같은 서비스 인증 절차에 사용</p> <ul style="list-style-type: none"> <li>- 다중 모듈(Kerberos Ticket과 같은 연동도 가능)</li> </ul> <p>사용자를 인증하고 자격증명 절차 제공</p> <ul style="list-style-type: none"> <li>- 패스워드를 통해 인증</li> </ul>
password	<p>사용자가 패스워드 등의 인증 방법을 변경하도록 할 때 제공하는 방법</p> <p>패스워드 변경 시 최소길이/복잡도 설정 등과 관련</p>
session	<p>사용자가 인증 받기 전/후에 해야 할 것을 지정</p> <p>홈 디렉터리 마운트/언마운트, 로그인/로그아웃 서비스 제한 등 포함</p>

auth	include	postlogin
account	required	pam_nologin.so
session	include	system-auth
session	required	pam_namespace.so
password	include	system-auth

## ② control

- PAM이 무엇을 해야 할 지를 알려줌

control	설명
required	지정된 모듈을 통한 인증이 실패하면 인증 거부 - 인증이 거부되기 전에 해당 서버에 등록된 다른 모듈들을 호출 한 후 거부 - 다른 인증들이 성공하더라도 해당 인증이 실행할 경우 인증 거부
requisite	이 모듈의 인증이 실패할 경우에 즉시 거부
sufficient	이전에 요청되었던 모듈이 실패하더라도 이 모듈에 의해서 인증이 성공할 경우 인증 승인한다.
optional	서비스에 대한 응용프로그램의 성공/실패가 중요하지 않다는 것을 의미 - 성공/실패 판단 시에는 무시, 모듈에 대한 성공/실패가 없다면 이 모듈이 응용프로그램에게 주는 결과로 결정
include	이 항목 다음에는 모듈명 대신에 <b>PAM 관련 서비스</b> 가 옴 해당 서비스 인증을 통과해야 가능하도록 설정할 때 사용

### ③ module\_name

- 사용하는 모듈명을 명기하는 부분
- 절대경로를 입력하거나 /lib/security에 있는 모듈명 기입

### ④ module-arguments

- 지정한 모듈이 사용하는 인수를 기입
- 여러 인수를 사용하는 경우에는 공백으로 구분
- 인수에 공백을 포함시키려면 대괄호([])를 사용해서 묶음

```
[root@localhost pam.d]# head -4 remote
#%PAM-1.0
auth      required      pam_securetty.so
auth      required      pam_faillock.so deny=3 unlock time=60
auth      substack      password-auth
```

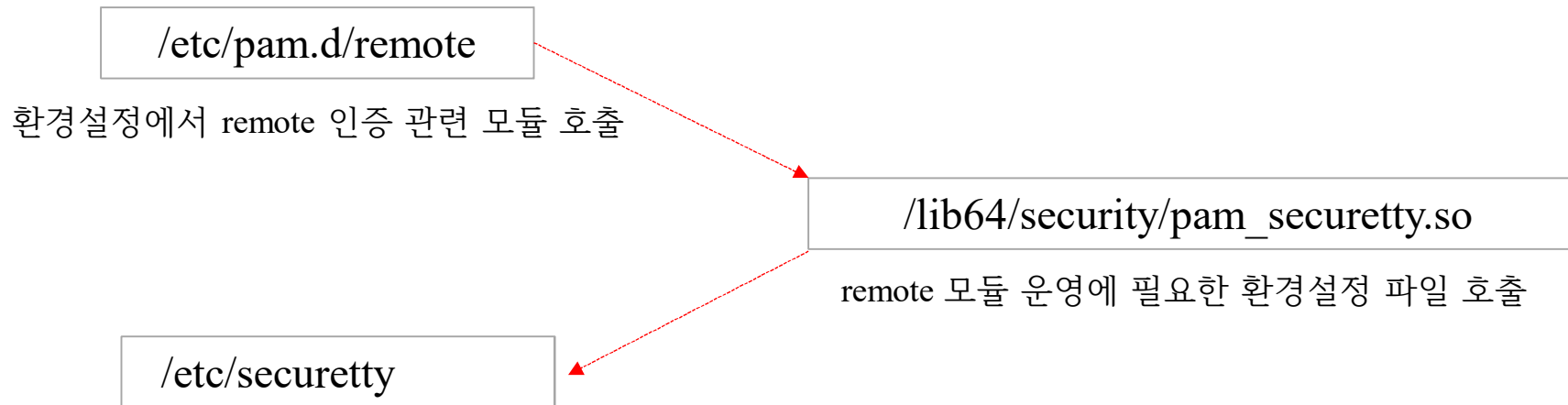
auth required pam\_faillock.so deny=3 unlock\_time=60

- 인증을 처리하는데 pam\_faillock.so 모듈 사용
- 실패 3회(deny=3)이면 30초동안 계정 잠금(unlock)


# PAM 주요 모듈

## pam\_securetty.so


- 접속하는 계정이 root인 경우 /etc/securetty 파일에 기록된 터미널을 통하는 경우에만 허가하도록 하고, 그 외 사용자는 항상 인증에 성공한 것으로 처리
- /etc/pam.d/login와 /etc/pam.d/remote 설정



```
[root@localhost pam.d]# cat remote
#%PAM- 1.0
auth        required    pam_securetty.so
auth        substack     password-auth
```



```
[root@localhost security]# ls *securetty*
pam_securetty.so
[root@localhost security]#
```



```
[root@localhost security]# cat /etc/securetty
console
tty1
tty2
tty3
tty4
tty5
```