http://home.opaopa.org/solaris9/ssh.html
https://qiita.com/tsuyoshi_cho/items/b28e5529636f06e84b5e

鍵の形式

PEM 形式より、OpenSSH 形式の方が新しい。PEM 形式の秘密鍵はヘッダの下に暗号化についての情報が記載されている。

拡張子	形式	ヘッダ (か先頭行) の書式
拡張子なし	OpenSSH private key(PEM 形式)	-----BEGIN RSA PRIVATE KEY-----
拡張子なし	OpenSSH private key(OpenSSH 形式)	-----BEGIN OPENSSH PRIVATE KEY-----
.pub	OpenSSH public key (authorized_keys に直接追加できる)	(1 行で書かれる) 種別 公開鍵 コメント
.ppk	PuTTY private(and public) key	PuTTY-User-Key-File-2: ...
.ppk.pub	PuTTY public key (RFC 4716)	---- BEGIN SSH2 PUBLIC KEY ----
.bin	ssh.com(SECSH) private key	---- BEGIN SSH2 ENCRYPTED PRIVATE KEY ----

鍵の作成

OpenSSH の鍵作成

■ PEM 形式

```
ssh-keygen
ssh-keygen -f hoge -t rsa
ssh-keygen -f hoge -m PEM
```

など。 -f はファイル指定。 -t は 暗号の種類。

■ OpenSSH 形式

-o オプションを使う

```
ssh-keygen -o
```

鍵形式の変換

変換元形式	変換先形式	変換方法	備考
OpenSSH 形式	PEM 形式	ssh-keygen -p -f 変換元 -m pem	本来はパスフレーズの変更コマンドだが、形式変換が可能

PEM 形式	OpenSSH 形式	ssh-keygen -p -f 変換元 -o	本来はパスフレーズの変更コマンドだが、形式変換が可能

鍵の設置場所

--	公開鍵（サーバー）	秘密鍵（クライアント）
OpenSSH1	~/.ssh/authorized_keys	~/.ssh/identity
OpenSSH2	~/.ssh/authorized_keys	~/.ssh/id_dsa OR ~/.ssh/id_rsa

公開鍵、秘密鍵のパーミッションは自分だけが参照できる状態にする。
他人が見れる状態になっていると鍵が無効になることがある。