

Mac OS のターミナルを利用した、SSH 鍵認証での接続手順について説明します。手順は以下の 3 つに分かれます。

- ・コントロールパネルで鍵ペアを作る
- ・Mac OS に秘密鍵を設置する
- ・Mac OS のターミナルを利用して SSH 鍵認証で SV-Basic サーバーへ接続する

1

コントロールパネルで鍵ペアを作る

コントロールパネルにログインして【 Web 】 > 【 公開サイト 】または【 テストサイト 】 > 【 SSH 】 > 【 鍵ペア作成 】を選択します。

SV-Basic CONTROL PANEL

Home 公開サイト テストサイト

Web FTPアカウント FTP接続制限の設定 簡単インストール スクリプト定期実行ツール アクセス制御 (BASIC認証) WAF ログ管理 外部バックアップサービス SSH データベース iQube+

SSH 操作マニュアル

SSHアカウント：未設定

SSHアカウントはまだ設定されていません。鍵ペアを生成するか、公開鍵をご登録のうえ、設定を有効にしてください。

鍵ペア作成 公開鍵登録 無効 OFF 有効 20

フィンガープリント コメント

SSH(Secure Shell)は、サーバーに対して遠隔から接続するための仕組みで、サーバー内のファイル操作などを行うことができます。SSHクライアントソフトに、登録したSSHアカウントを設定し利用します。

鍵ペアを作成します

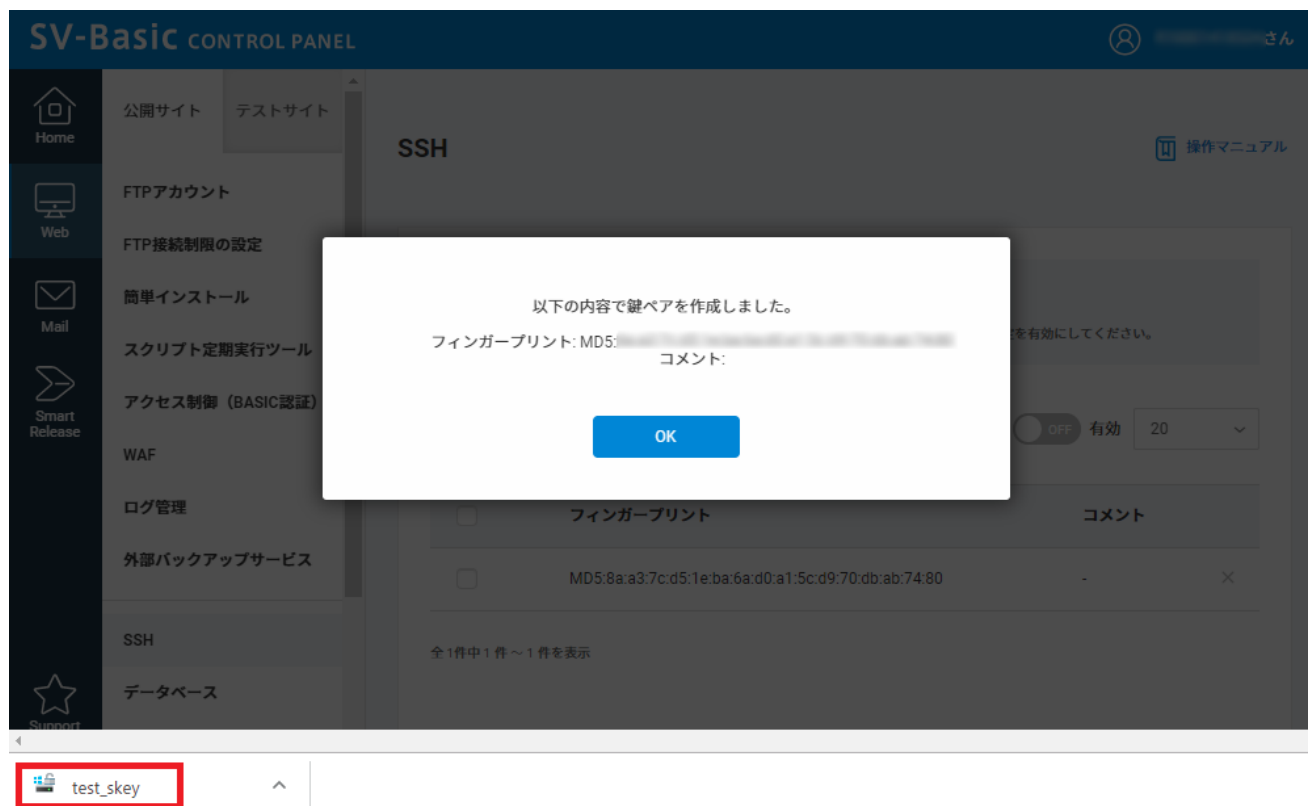
秘密鍵ファイル名を入力します。

Mac の OSX のターミナルで SSH 接続される場合は、秘密鍵のファイル名は「id_rsa」をご利用ください。

パスフレーズ、コメントを設定します。

※秘密鍵ファイル名の入力は必須項目ですが、パスフレーズとコメントは未入力でも鍵を作成できます。

鍵ペアの作成が完了しますと、Mac OS に秘密鍵のファイルがダウンロードされます



鍵ペアの作成が完了しますと、パソコン本体にファイルがダウンロードされます。この時点で、公開鍵はSV-Basicのサーバー上に設定されます。秘密鍵はPCにダウンロードされ、SV-Basicのサーバー上からは削除されます。秘密鍵の取り扱いには十分ご注意ください。

【ON/OFF】 ボタンをクリックして有効化します。

SV-Basic CONTROL PANEL

公開サイト テストサイト

SSH

SSHを有効にしました。
SSHは一つのアカウントでテストサイト、公開サイトへ接続できます。ポート番号を分けて接続してください。

SSHアカウント：設定済み

公開サイトポート番号：10399
テストサイトポート番号：10398

鍵ペア作成 公開鍵登録 無効 ON 有効 20

フィンガープリント コメント

MD5: [REDACTED]

全1件中1件～1件を表示

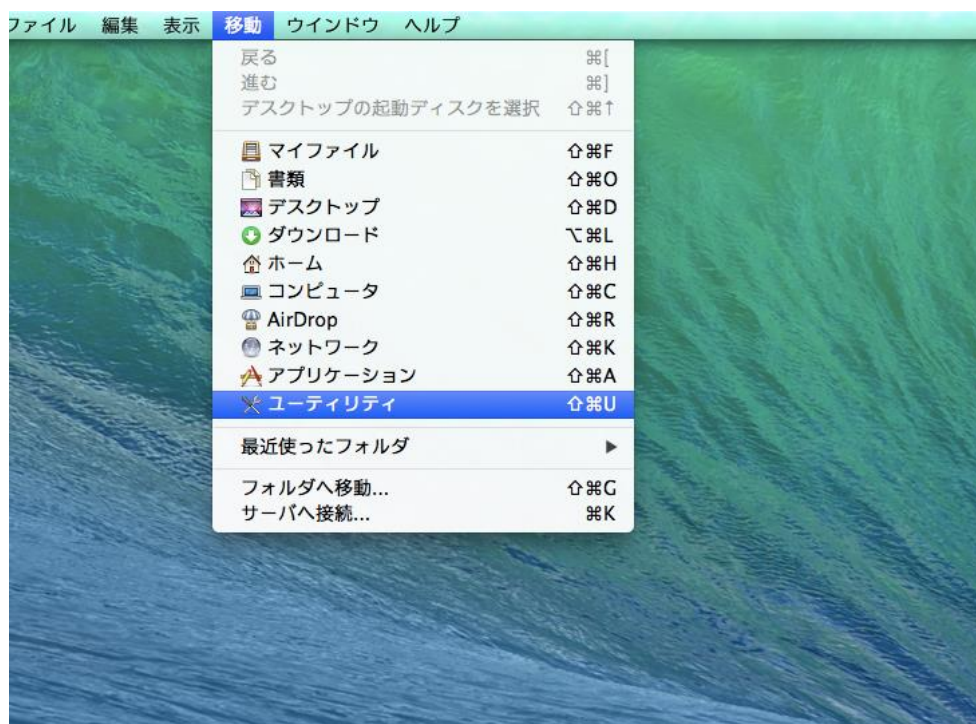
2

Mac OS に秘密鍵を設置する

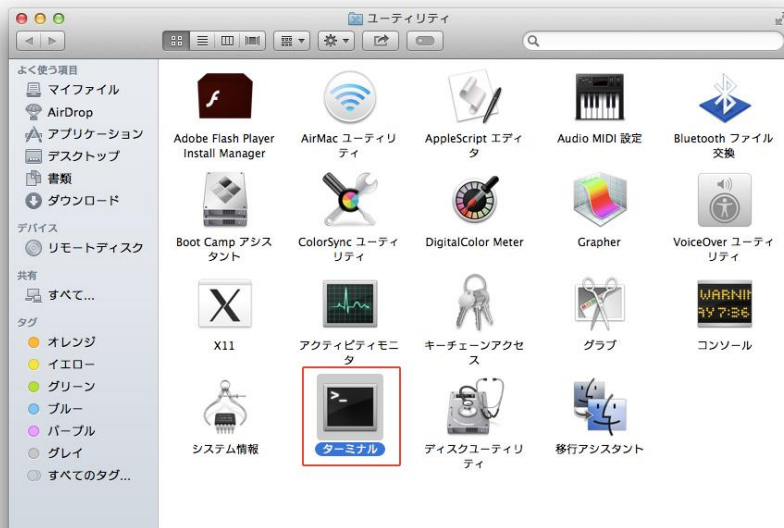
ここでは、コントロールパネルで作成した秘密鍵のファイル名を id_rsa、秘密鍵を Mac OS のデスクトップ上に保存した状態の想定で説明をします。

Mac OS のターミナルを起動します。

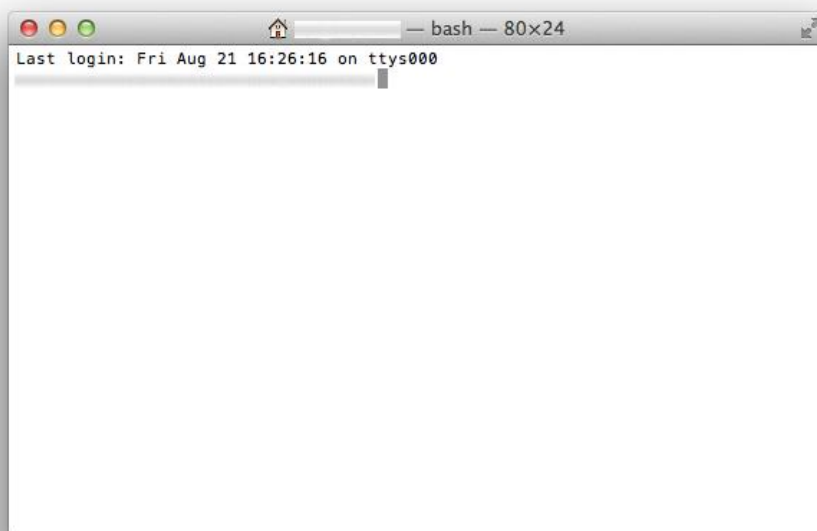
画面上部の「移動」メニュー-「ユーティリティ」をクリックしてください。



ユーティリティの中の、ターミナルを起動してください。



ターミナルの起動画面です。

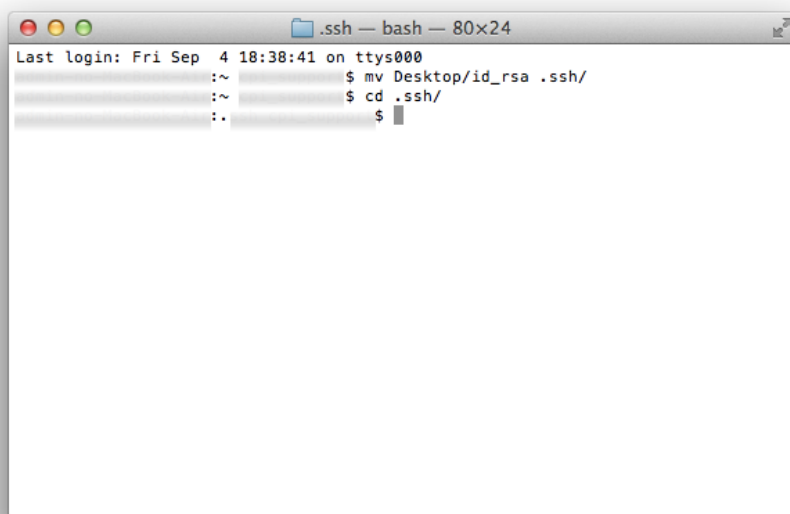


デスクトップ上の秘密鍵(id_rsa)を.sshディレクトリに移動します。以下のコマンドを入力してReturnキーを押してください。

```
mv Desktop/id_rsa .ssh/
```

./sshのディレクトリに移動します。以下のコマンドを入力してReturnキーを押してください。

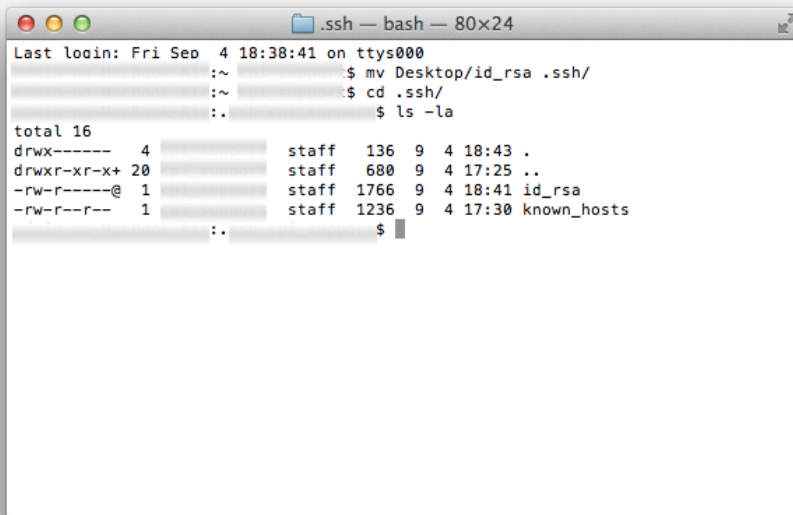
```
cd .ssh/
```



```
.ssh — bash — 80x24
Last login: Fri Sep  4 18:38:41 on ttys000
:~      $ mv Desktop/id_rsa .ssh/
:~      $ cd .ssh/
:~      $
```

.ssh ディレクトリ内のファイルリストを確認します。以下のコマンドを入力して Return キーを押してください。

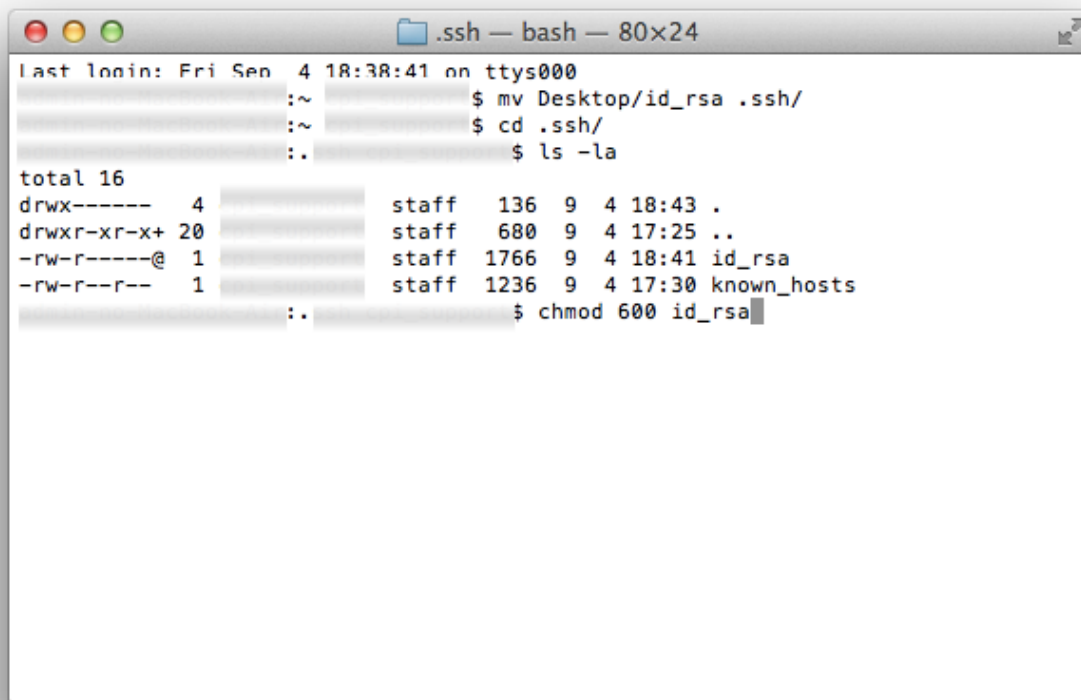
ls -la



```
.ssh -- bash -- 80x24
Last login: Fri Sep  4 18:38:41 on ttys000
:~ $ mv Desktop/id_rsa .ssh/
:~ $ cd .ssh/
:~ $ ls -la
total 16
drwx-----  4  staff  136  9  4 18:43 .
drwxr-xr-x+ 20  staff  680  9  4 17:25 ..
-rw-r-----@ 1  staff  1766  9  4 18:41 id_rsa
-rw-r--r--   1  staff  1236  9  4 17:30 known_hosts
:~ $
```


id_rsaファイルのパーミッションを600に変更します。以下のコマンドを入力してReturnキーを押してください。

```
chmod 600 id_rsa
```



```
.ssh — bash — 80x24
Last login: Fri Sep  4 18:38:41 on ttys000
:~ $ mv Desktop/id_rsa .ssh/
:~ $ cd .ssh/
:~ $ ls -la
total 16
drwx-----  4  staff  136  9  4 18:43 .
drwxr-xr-x+ 20  staff  680  9  4 17:25 ..
-rw-r-----@ 1  staff 1766  9  4 18:41 id_rsa
-rw-r--r--   1  staff 1236  9  4 17:30 known_hosts
:~ $ chmod 600 id_rsa
```

以上で Mac OS での秘密鍵の準備が完了です。

3 MacOS のターミナルを利用して SSH 鍵認証にて SSH 接続をする

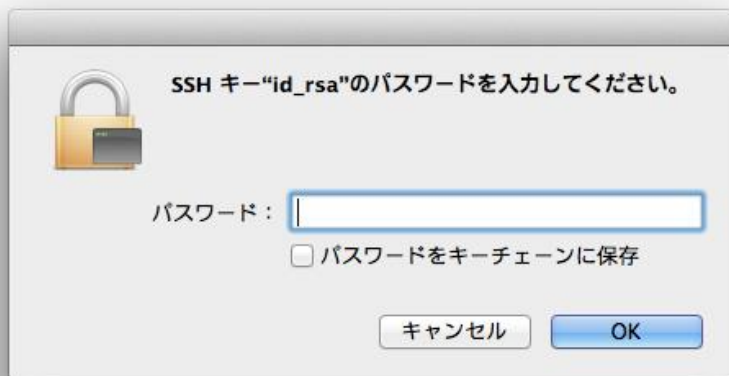
MacOS のターミナルを起動し、以下のようにコマンドを入力し return キーを押してください。

```
ssh -p (ポート番号) (WebコントロールパネルID)@(WebサーバーのIPアドレス)
```

「ポート番号」は公開サイト用のポート番号、またはテストサイト用のポート番号を入力してください、ポート番号は、コントロールパネルの【Home】>【バージョン・ポート番号】>【ポート番号】の「SSH (公開サイト/テストサイト)」に記載しています。



鍵ペアを生成するときにパスフレーズを設定した場合は、パスフレーズを入力し「OK」ボタンをクリックしてください、



鍵ペアを生成するときにパスフレーズを設定した場合は、パスフレーズを入力し「OK」ボタンをクリックしてください、

