SSH接続マニュアル

1 公開サイトへの SSH 接続と、テストサイトへの SSH 接続を切り替える方法について

1 つの秘密鍵、公開鍵で SSH 接続する際にポート番号を切り替えるだけで、公開サイトとテストサイトへ の接続を切り替えることが出来ます。SSH のユーザー名と接続先のサーバー名は変更せず、ポート番号のみ変更してください。

公開サイトへの SSH 接続と、テストサイトへの SSH 接続を切り替える方法
・公開サイトへ接続する場合のコマンド
$ ssh -p 公開サイトの SSH ポート番号 -l ad999xxxxx ad999.secure.ne.jp
・テストサイトへ接続する場合のコマンド
$ ssh -p テストサイトの SSH ポート番号 -l ad999xxxxx ad999.secure.ne.jp

2 複数のサーバーへ SSH 接続する場合

お客さまがご利用されるお手元の PC 内に ACE01 のコントロールパネルで生成した秘密鍵を複数保管する場合、秘密鍵の名称や保管ディレクトリを変更する必要がございます。
ここでは、Mac OS X を例にして、1 台の PC にて複数の秘密鍵を利用する方法を説明します。

手順 1　秘密鍵を作成する	
【サーバーA】	【サーバーB】
サーバーA のウェブコントロールパネルにて、鍵ペアを作成する。秘密鍵ファイル名 server-a。パスフレーズを設定するかは任意です。	サーバーB のウェブコントロールパネルにて、鍵ペアを作成する。秘密鍵ファイル名 server-b。パスフレーズを設定するかは任意です。
ローカル PC に ~/.ssh/server-a というディレクトリを作成する。	ローカル PC に ~/.ssh/server-b というディレクトリを作成する。
作成した秘密鍵ファイル(server-a)を、~/.ssh/server-a のディレクトリ内に移動する。	作成した秘密鍵ファイル(server-b)を、~/.ssh/server-b のディレクトリ内に移動する。
~/.ssh/server-a/server-a のパーミッションを 600 にする。	~/.ssh/server-a/server-b のパーミッションを 600 にする。

手順 2　config ファイルを作成する

~/.ssh/ ディレクトリに config という名称のファイルを作成します。

~/.ssh/config ファイルを開いて以下のように記述します。

（ファイルの記述例）

```
Host server-a
 User ad999XXXXX
 Port ポート番号　　←公開サイト、またはテストサイトの SSH ポート番号を指定してください。
 HostName ad999.secure.ne.jp
 TCPKeepAlive yes
 identitiesonly yes
 identityfile ~/.ssh/server-a/server-a

Host server-b
 User ae999XXXXX
 Port ポート番号　　←公開サイト、またはテストサイトの SSH ポート番号を指定してください。
 HostName ae999.secure.ne.jp
 TCPKeepAlive yes
 identitiesonly yes
 identityfile ~/.ssh/server-b/server-b
```

~/.ssh/config ファイルを保存して、パーミッションを 600 にする。

手順 3　Mac OS X のターミナルを使って SSH 接続を開始する

【サーバーA】に SSH 接続するためのコマンド	【サーバーB】に SSH 接続するためのコマンド
$ ssh server-a この後、秘密鍵にパスフレーズを設定していた場合は、入力ダイアログが表示されるので パスフレーズを入力すると、~/.ssh/config ファイルに記述した server-a のサーバーに SSH 接続されます。	$ ssh server-b この後、秘密鍵にパスフレーズを設定していた場合は、入力ダイアログが表示されるので パスフレーズを入力すると、~/.ssh/config ファイルに記述した server-b のサーバーに SSH 接続されます。