

SSH 接続ソフト PuTTY 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 4 つに分かれます。

- ・コントロールパネルで鍵ペアを作る
- ・putty.exe と puttygen.exe のダウンロードする
- ・秘密鍵を PuTTY で利用できる形式にコンバートする
- ・PuTTY で SSH 鍵認証で SV-Basic の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。

The screenshot shows the SV-Basic Control Panel interface. The left sidebar contains navigation options: Home, Web, Mail, Smart Release, and SSH (highlighted with a red box). The main content area is titled 'SSH' and displays the following information:

- 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。
- Buttons: 鍵ペア作成 (highlighted with a red box), 公開鍵登録
- Toggle: 無効 OFF 有効 (with a dropdown menu set to 20)
- Fields: フィンガープリント, コメント

At the bottom, there is explanatory text: 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。

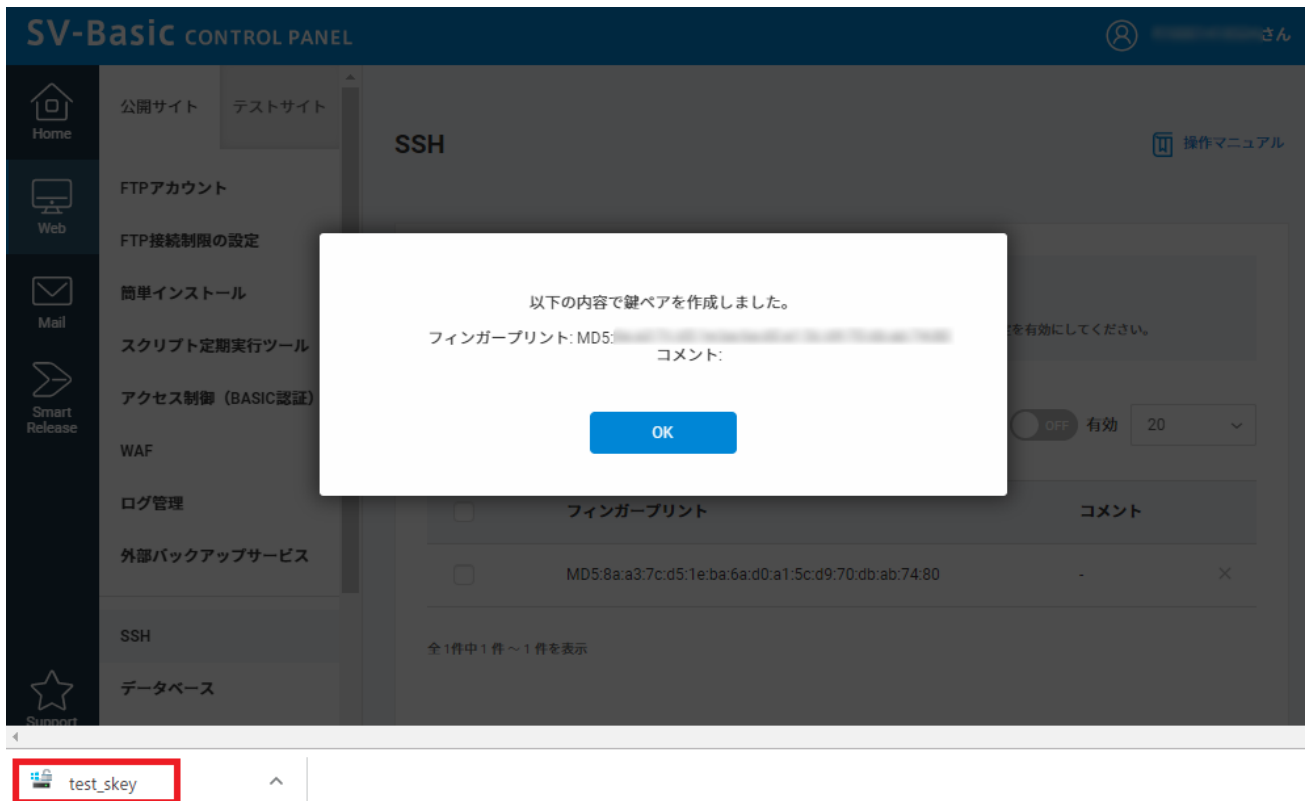
鍵ペアを作成します。

秘密鍵ファイル名を入力します。

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、パソコン本体に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

Home

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

putty.exe と puttygen.exe のダウンロードする

PuTTYDownloadPage(<http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html>)

にアクセスし、

PuTTY: putty.exe

PuTTYgen: puttygen.exe をダウンロードしてください。



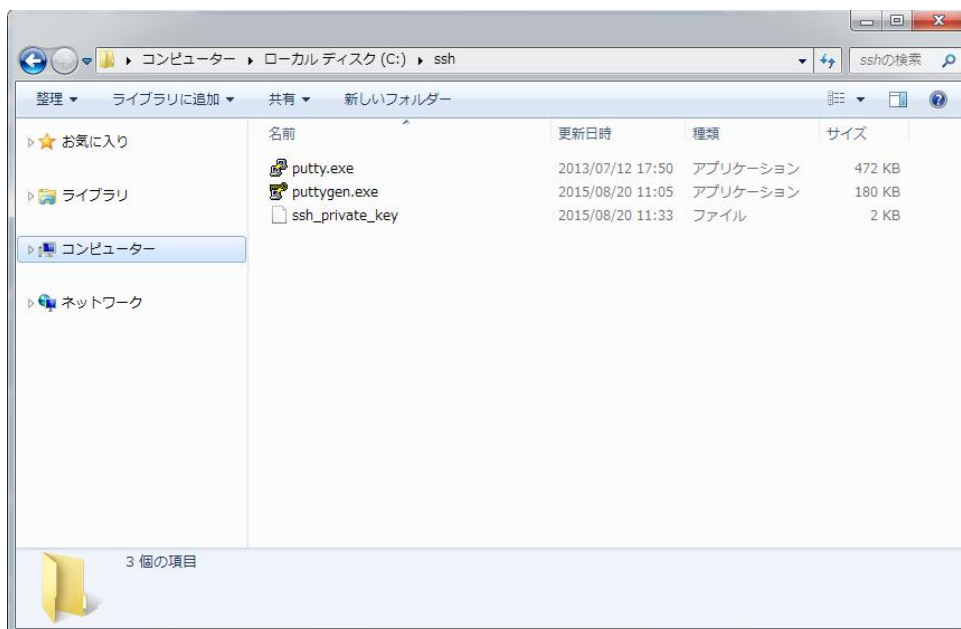
The screenshot shows the PuTTY Download Page with a list of binaries. The following table summarizes the content of the 'Binaries' section:

Binary Name	File Name	Download Method	Signature	Signature
PuTTY	putty.exe	(or by FTP)	(RSA sig)	(DSA sig)
PuTTYtel	puttytel.exe	(or by FTP)	(RSA sig)	(DSA sig)
PSCP	pscp.exe	(or by FTP)	(RSA sig)	(DSA sig)
PSFTP	psftp.exe	(or by FTP)	(RSA sig)	(DSA sig)
Plink	plink.exe	(or by FTP)	(RSA sig)	(DSA sig)
Pagant	pagant.exe	(or by FTP)	(RSA sig)	(DSA sig)
PuTTYgen	puttygen.exe	(or by FTP)	(RSA sig)	(DSA sig)

Additional information from the screenshot:

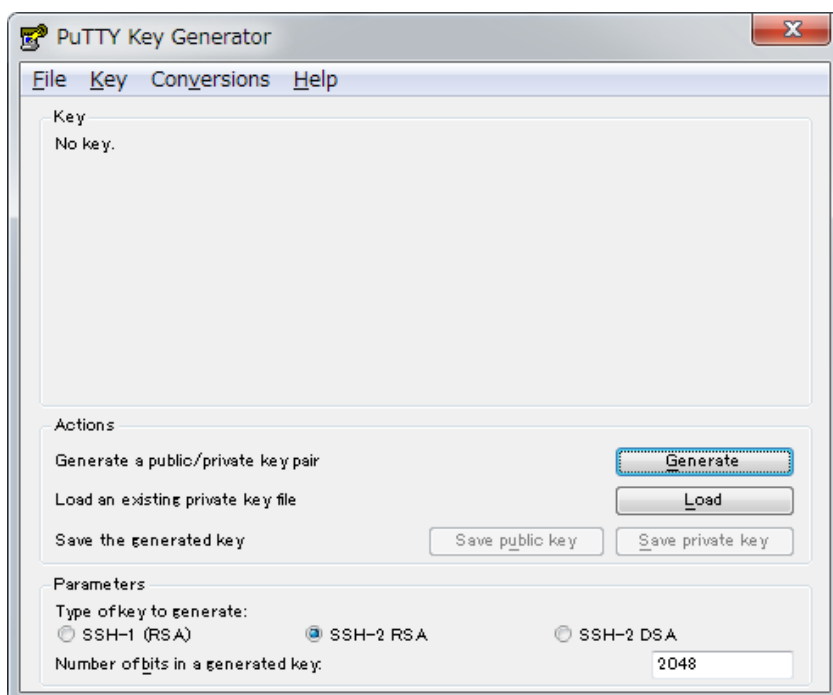
- LEGAL WARNING:** Use of PuTTY, PSCP, PSFTP and Plink is illegal in countries where encryption is outlawed. I believe it is legal to use PuTTY, PSCP, PSFTP and Plink in England and Wales and in many other countries, but I am not a lawyer and so if in doubt you should seek legal advice before downloading it. You may find [this site](#) useful (it's a survey of cryptography laws in many countries) but I can't vouch for its correctness.
- Use of the Telnet-only binary (PuTTYtel)** is unrestricted by any cryptography laws.
- There are cryptographic signatures available for all the files we offer below. We also supply cryptographically signed lists of checksums. To download our public keys and find out more about our signature policy, visit the [keys page](#). If you need a Windows program to compute MD5 checksums, you could try the one at [this site](#). (This MD5 program is also cryptographically signed by its author.)
- Binaries**
 - The latest release version (beta 0.65)**
 - This will generally be a version I think is reasonably likely to work well. If you have a problem with the release version, it might be worth trying out the latest development snapshot (below) to see if I've already fixed the bug before reporting it to me.
 - For Windows on Intel x86**
- A ZIP file containing all the binaries (except PuTTYtel), and also the help files**
- Zip file: [putty.zip](#) (or by FTP) (RSA sig) (DSA sig)
- A Windows installer for everything except PuTTYtel**
- Installer: [putty-0.65-installer.exe](#) (or by FTP) (RSA sig) (DSA sig)
- Checksums for all the above files**
- MD5: [md5sums](#) (or by FTP) (RSA sig) (DSA sig)
- SHA-1: [sha1sums](#) (or by FTP) (RSA sig) (DSA sig)
- SHA-256: [sha256sums](#) (or by FTP) (RSA sig) (DSA sig)

putty.exe、puttygen.exe と、SV-Basic のコントロールパネルで生成した秘密鍵(ファイル名 : ssh_private_key)を Windows の C:¥ssh のフォルダ内に保存した状態として説明します。

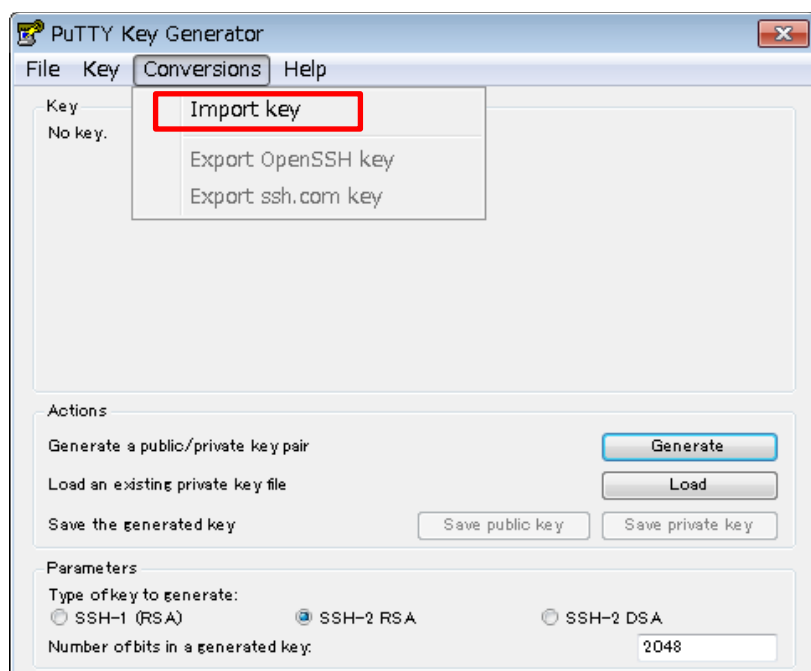


3 秘密鍵を PuTTY で利用できる形式にコンバートする

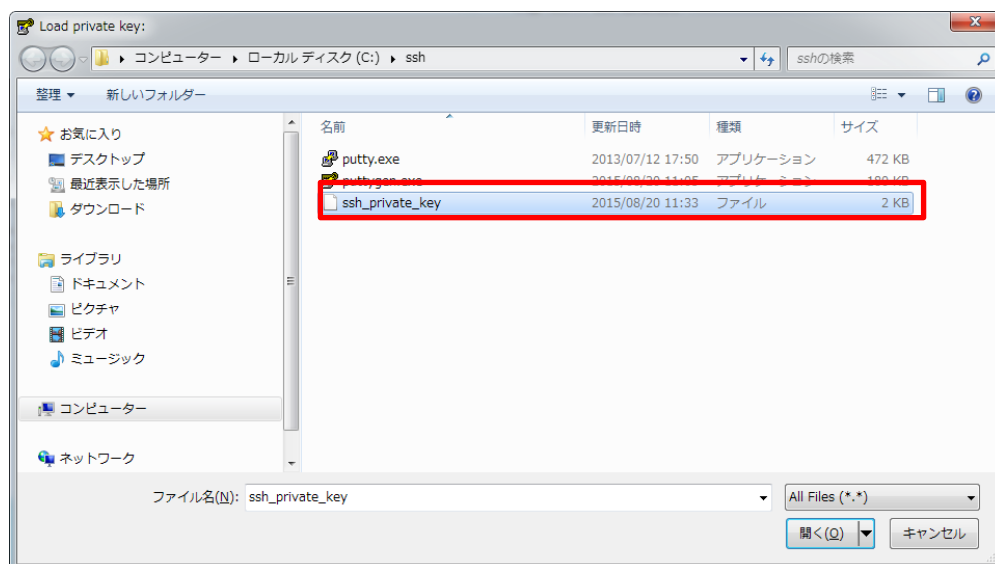
puttygen.exe を起動してください。



ツールバーの「Conversions」 - 「Import key」をクリックしてください。



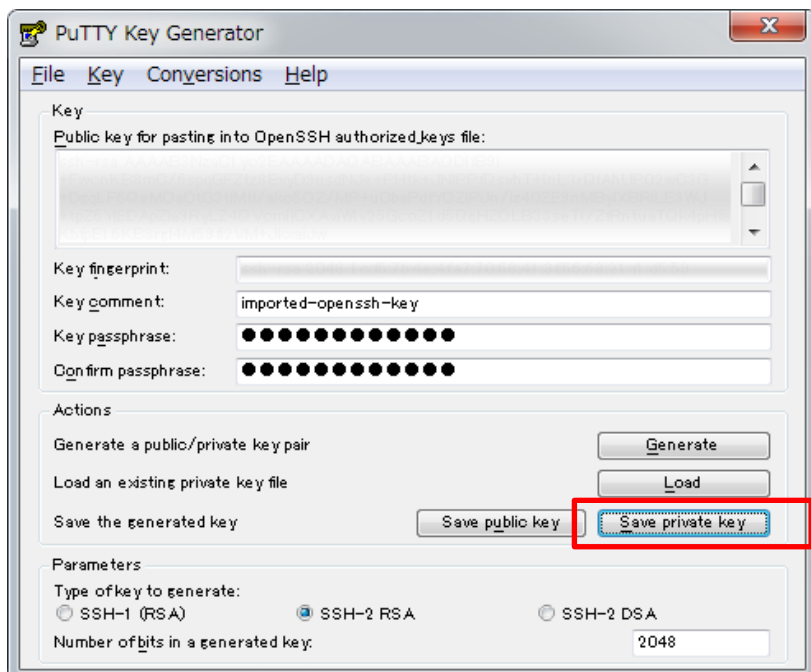
C:¥ssh¥ssh_private_key を選択してください。



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」をクリックしてください。



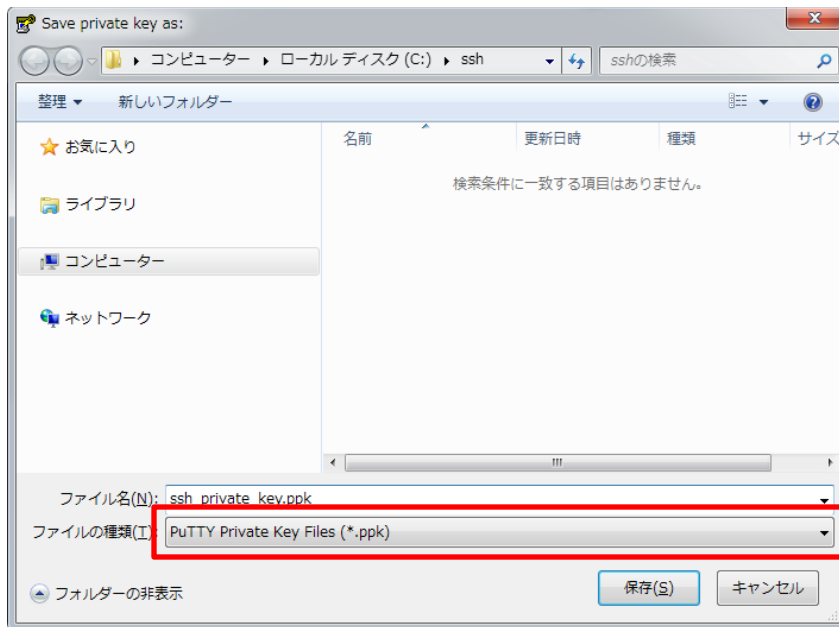
秘密鍵を読み込んだ状態で、「Save private key」をクリックしてください。



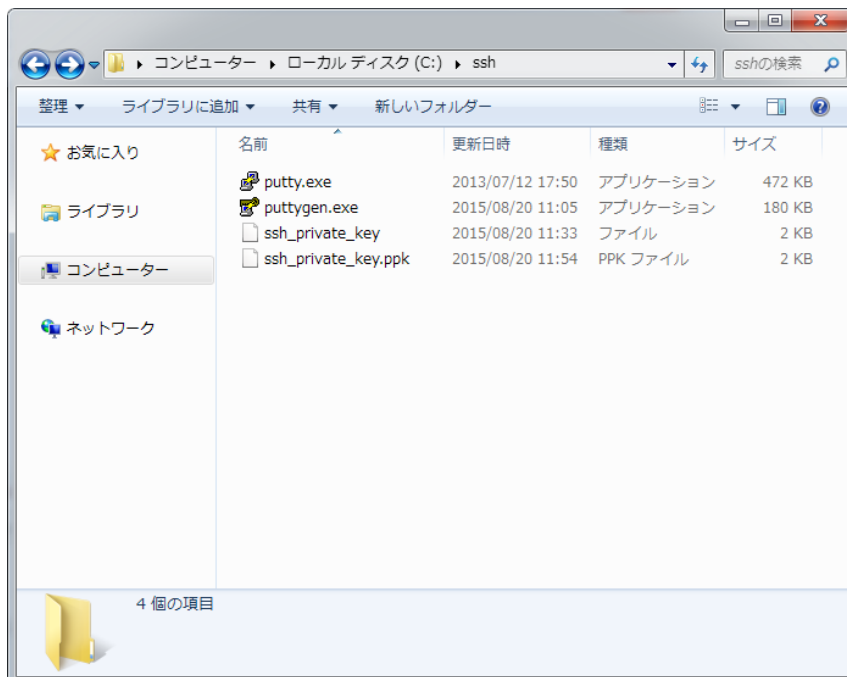
コンバート後の秘密鍵のファイル名を指定してください。

ここでは必ずファイル名のあとに拡張子「.ppk」を付けてファイルを保存してください。

例では ssh_private_key.ppk というファイル名にしています。



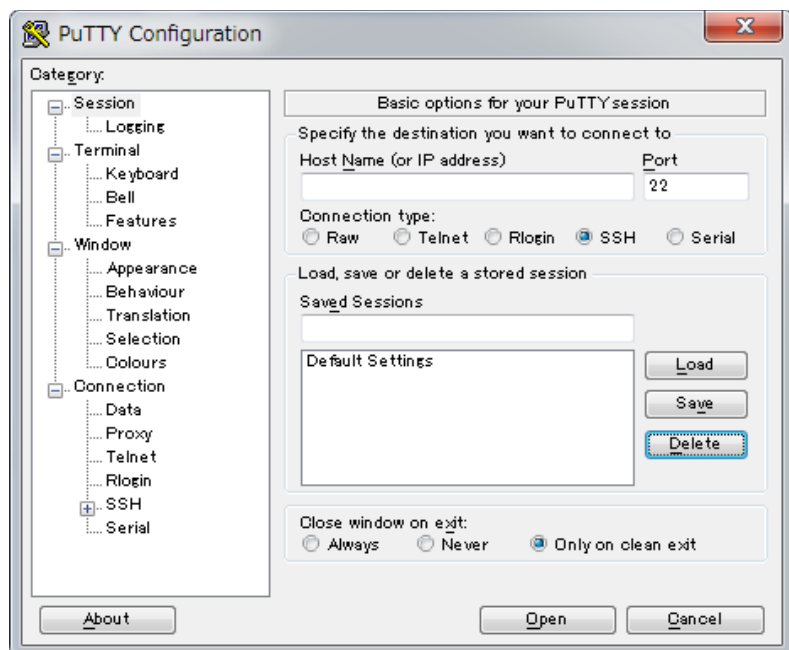
以上で秘密鍵のコンバートは終了です。



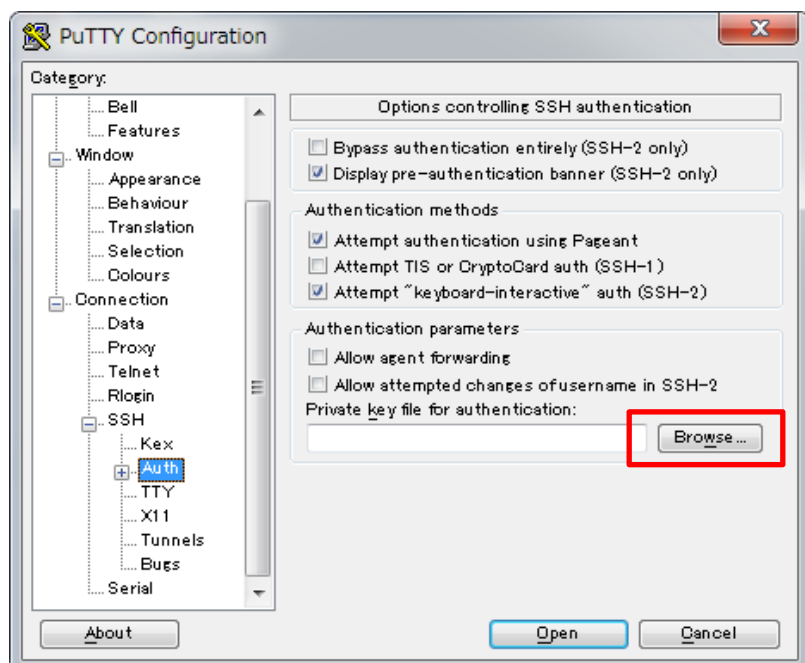
4

putty.exe で SSH 鍵認証で SV-Basic のサーバーへ接続する

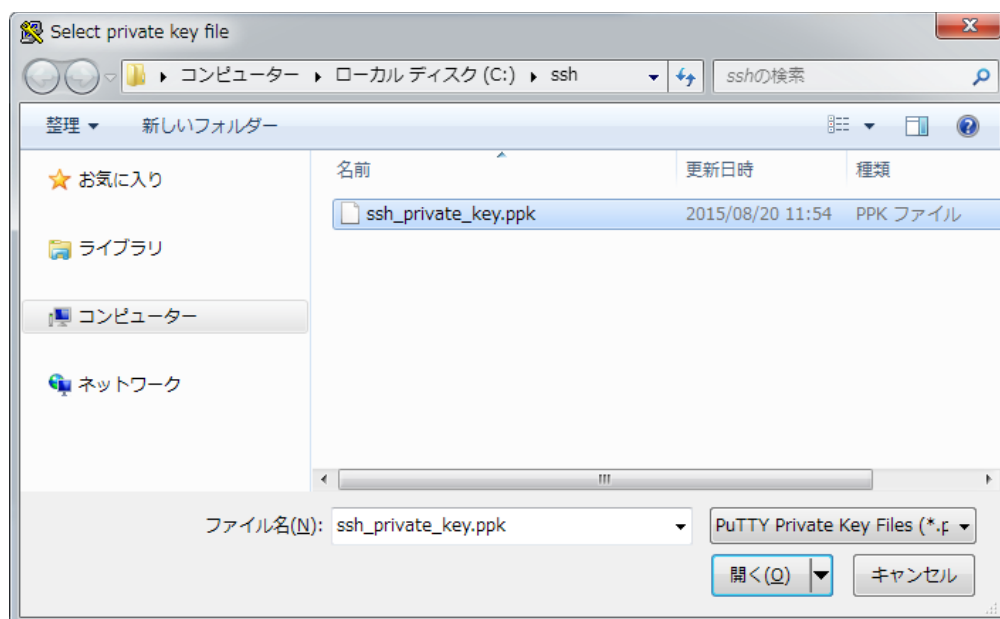
putty.exe を起動します。



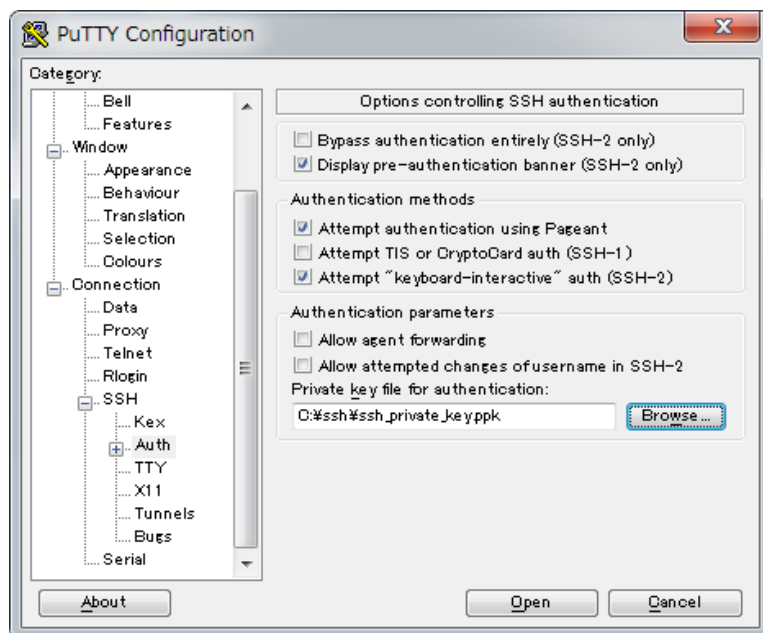
PuTTY Configuration のウィンドウの左側メニューの「Connection」 - 「SSH」 - 「Auth」を選択し、ウィンドウ右側の「Browse」ボタンをクリックしてください。



C:\ssh ¥ ssh_private_key.ppk を選択して「開く」をクリックしてください。



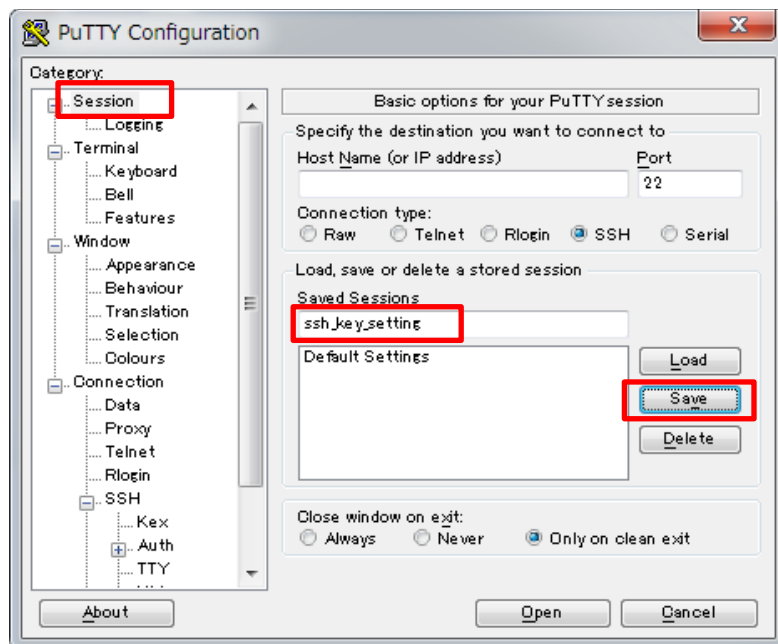
これで、SSH 接続するとき利用する秘密鍵の指定が完了です。



PuTTY Configuration のウィンドウの左側メニューの「Session」を選択してください。

必要に応じて、PuTTY の設定を保存してください。「Saved Sessions」の欄に設定名を入力して

「Save」ボタンをクリックすると設定を保存することができます。



ここから、PuTTY で SSH の接続を開始します。

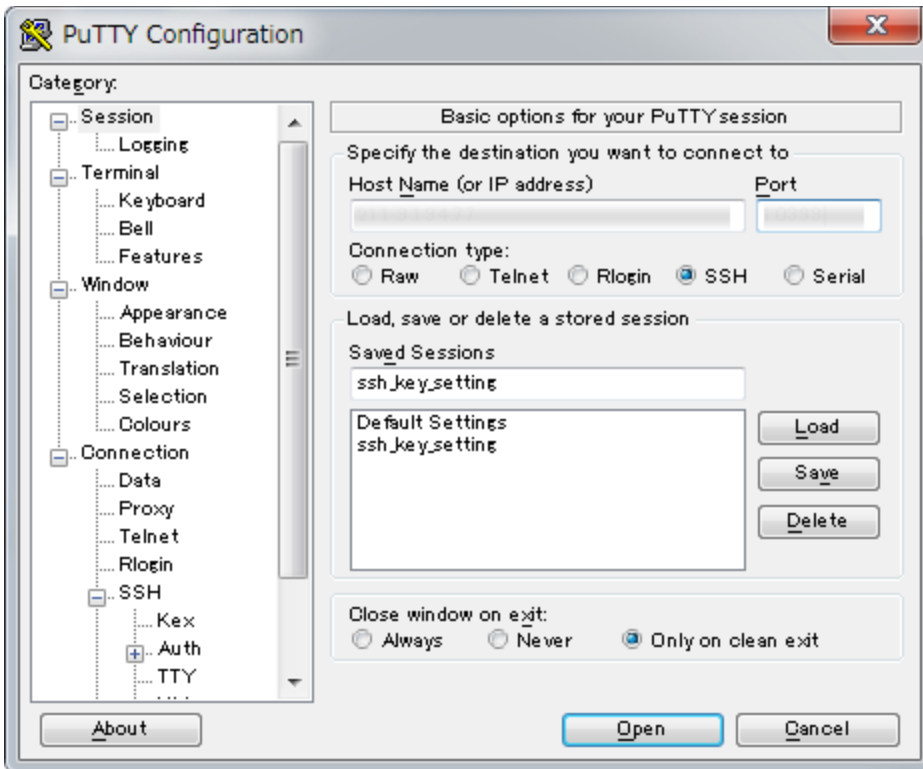
「Host Name(or IP address)」に、接続先となるサーバーの IP アドレスを入力してください。

IP アドレスは SV-Basic のサーバーのウェブサーバーの IP アドレスを入力してください。

「Port」に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。

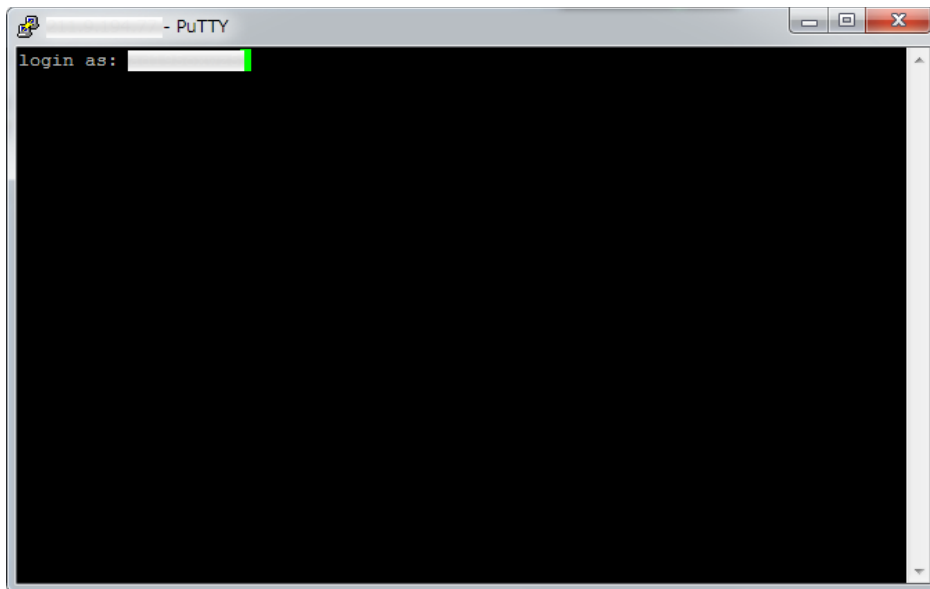
各設定値を入力後、Window 右下の「Open」ボタンをクリックしてください。



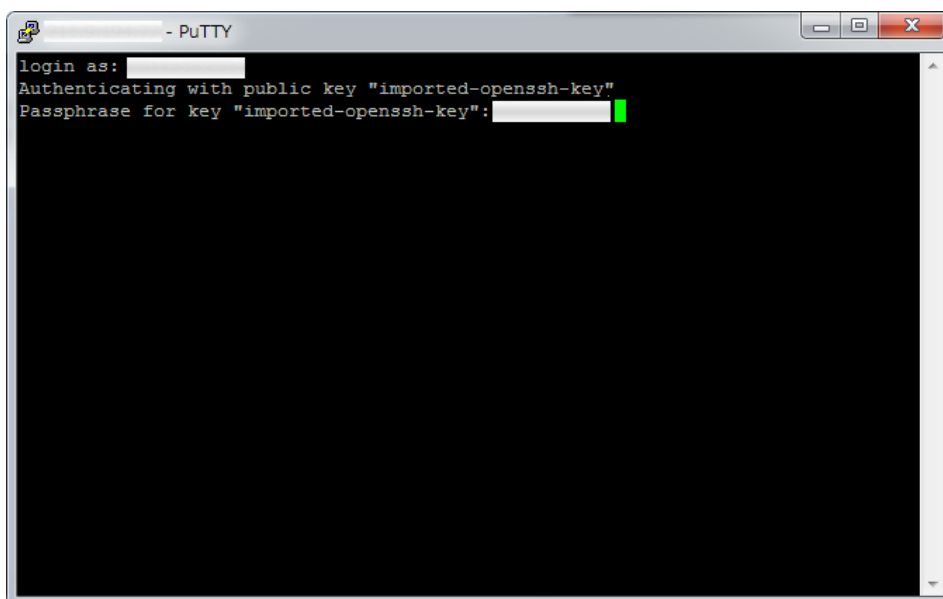
PuTTY でサーバーへ接続がされました。

login as:ウェブコントロールパネルID

を入力して Enter キーを押してください、

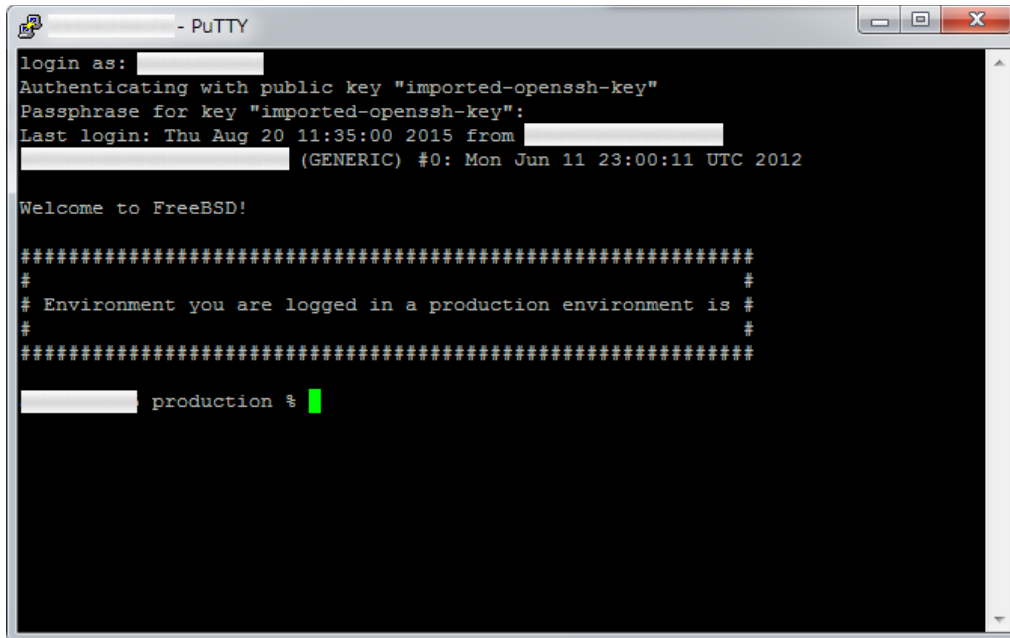


鍵ペアを生成するときにパスフレーズを設定した場合は、パスフレーズを入力し Enter キーを押してください、



正常に SSH 鍵認証が行われ、SSH 接続がされると以下ようになります。

(公開サイトに接続された例です)



```
login as: [redacted]
Authenticating with public key "imported-openssh-key"
Passphrase for key "imported-openssh-key":
Last login: Thu Aug 20 11:35:00 2015 from [redacted]
[redacted] (GENERIC) #0: Mon Jun 11 23:00:11 UTC 2012

Welcome to FreeBSD!

#####
#
# Environment you are logged in a production environment is #
#
#####

[redacted] production % █
```