

1

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。

- ・ putty.exe と puttygen.exe のダウンロードする
- ・ puttygen.exe で鍵ペアを生成する。
- ・ 公開鍵を CHM-2Z のサーバーへ登録する
- ・ putty.exe で SSH 鍵認証で CHM-2Z のサーバーへ接続する

## 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 represents the content of the 'Binaries' section:

Binary Name	File Name	Download Method	RSA sig	DSA sig
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 includes:

- 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 065)**  
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-GSI-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)











3

### 公開鍵を CHM-□ のサーバーへ登録する

コピーした公開鍵の文字列を、CHM-□ のウェブコントロールパネルの SSH の「公開鍵登録」に貼り付け、「登録する」ボタンをクリックすると公開鍵が登録されます。

※秘密鍵の情報は登録しないでください。

※公開鍵の情報は 1 行のテキスト文字列情報として貼り付けてください。改行はしないでください。

利用開始する

**公開鍵一覧**

公開鍵が登録されていません。SSH のご利用には、鍵ペアをご用意ください。

**鍵ペア作成**

SSH-2 RSA 形式の鍵ペアを作成します。

秘密鍵ファイル名[必須]	<input type="text"/>
パスフレーズ	<input type="text"/>
コメント	<input type="text"/>

作成する

**公開鍵登録**

登録可能な鍵の種類は SSH-2 RSA (鍵の bit 数が 2048 bit 以上) および ECDSA です。

登録する

**お客様のご利用状況**  
※2018/01/25 01:00現在の情報です。

---

**■ 契約情報**

プラン名    Managed Plan CHMZ1  
 サーバ名    |                          
 IPアドレス    |                        

[▶ お問い合わせ](#)

---

**■ ディスク使用状況**

<span style="color: red;">■</span>	ウェブ	: 0.10MB
■	メール	: 2.06MB
■	データベース	: 0.00MB

[▶ ディスク使用量について](#)

◀ BACK

▲ TOP

Copyright 2009 KDDI Web Communications Inc. All Rights Reserved.

公開鍵の登録が完了すると、公開鍵一覧で確認することができます。

【利用開始する】ボタンをクリックします。

ホーム > 制作ツール > SSH利用開始・利用停止

## SSH利用開始・利用停止

このページのヘルプ

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、  
ご利用を開始してください。

利用開始する

公開鍵一覧			
1	フィンガー プリント		削除
	コメント		

公開鍵一括削除

### 鍵ペア作成

SSH-2 RSA 形式の鍵ペアを作成します。

秘密鍵ファイル名[必須]	<input type="text"/>
パスフレーズ	<input type="text"/>

ご意見    ログアウト

ショートカットメニュー

【ホーム】

お客様のご利用状況  
※2018/01/25 01:00現在の情報です。

■契約情報

プラン名    Managed Plan CHMZ1  
サーバ名      
IPアドレス   

お問い合わせ

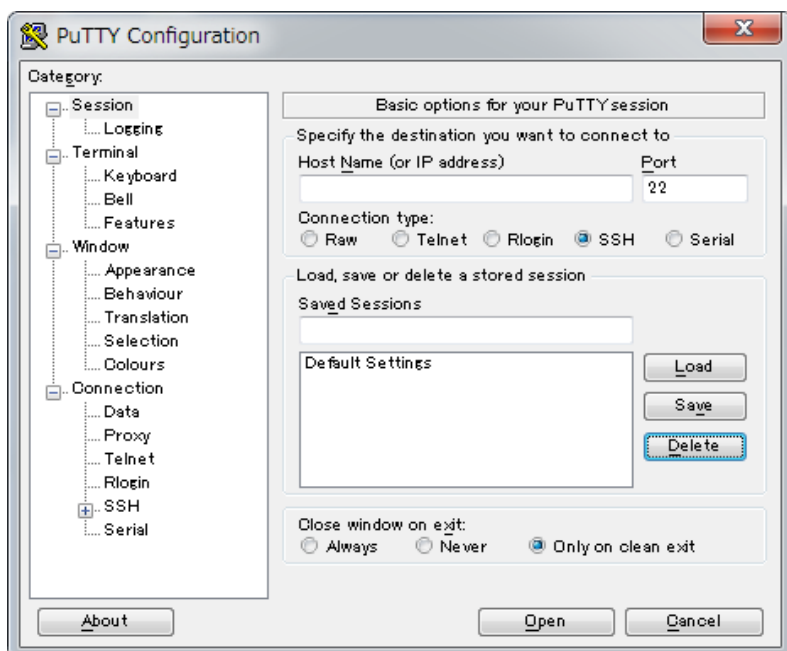
■ディスク使用状況



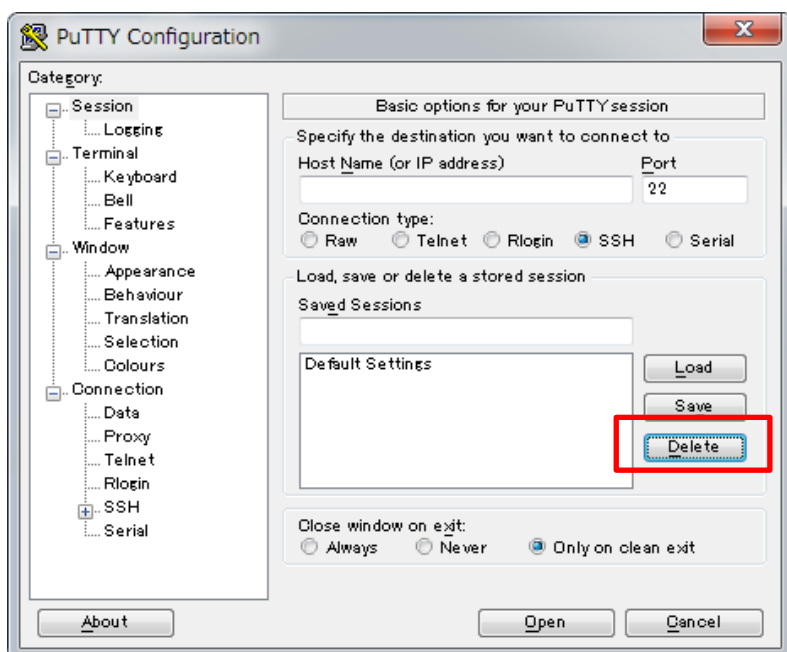


4

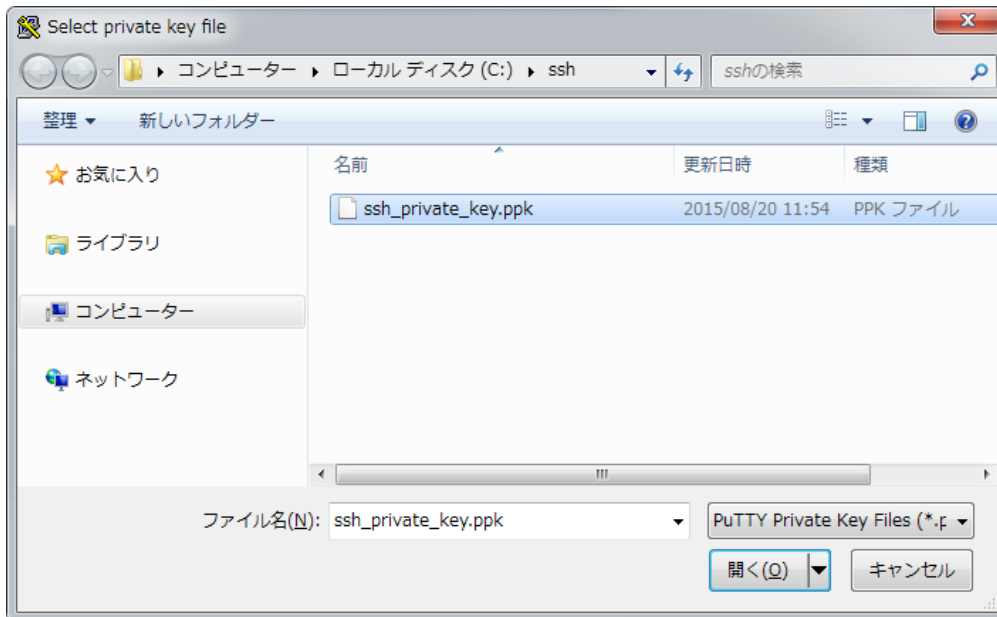
putty.exe で SSH 鍵認証で CHM-2Z のサーバーへ接続する  
putty.exe を起動します。



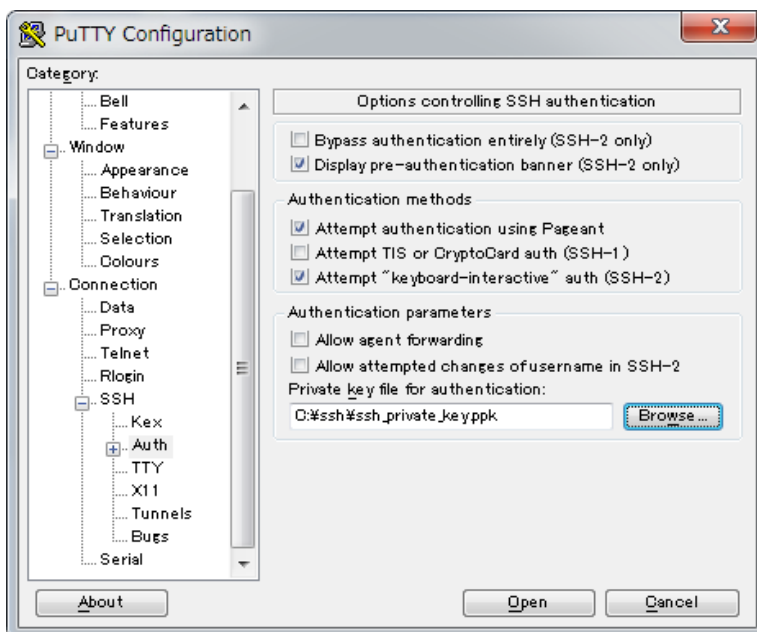
PuTTY Configuration のウィンドウの左側メニューの「Connection」 - 「SSH」 - 「Auth」 を選択し、  
ウィンドウ右側の「Browse」 ボタンをクリックしてください。



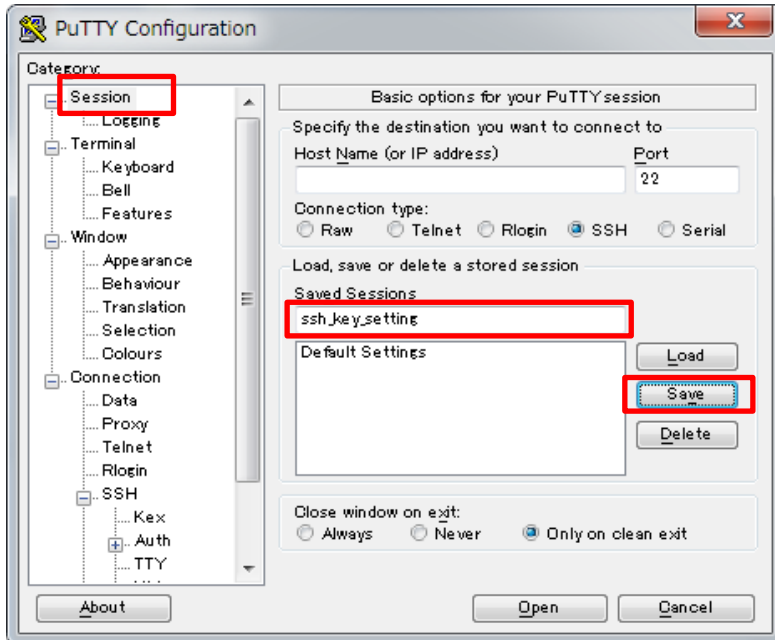
C:\\$ssh¥ssh\_private\_key.ppk を選択して「開く」をクリックしてください。



これで、SSH 接続するときを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。



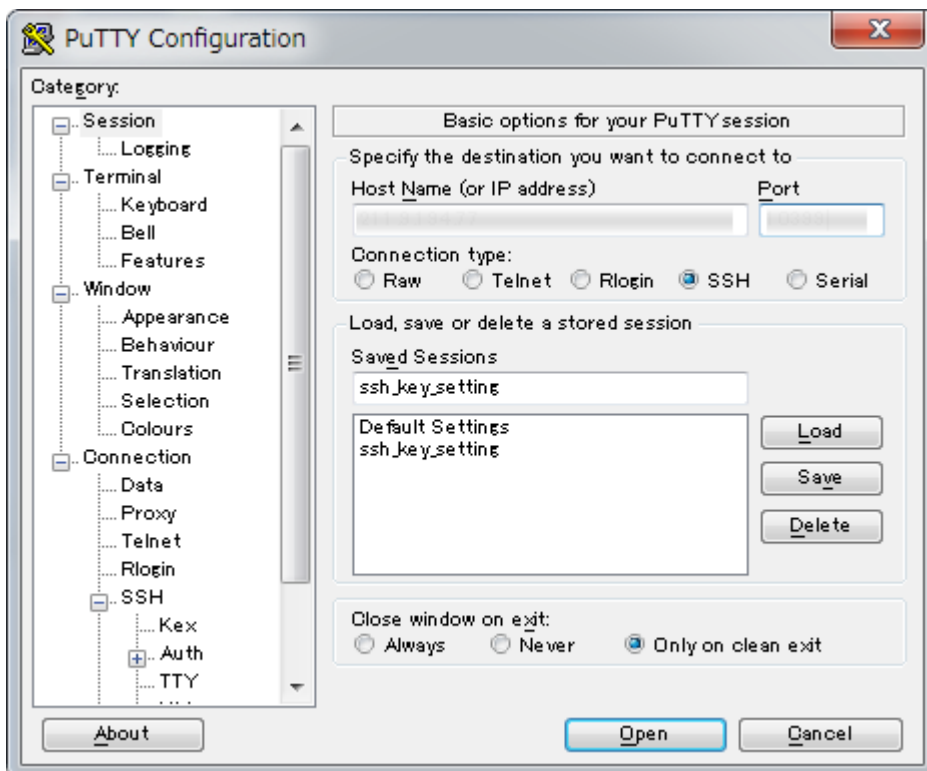
ここから、PuTTY で SSH の接続を開始します。

「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 CHM-2Z 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、ウェブコントロールパネルの【お客様情報】>【プログラムのパスとサーバの情報】の「SSH ポート番号」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。

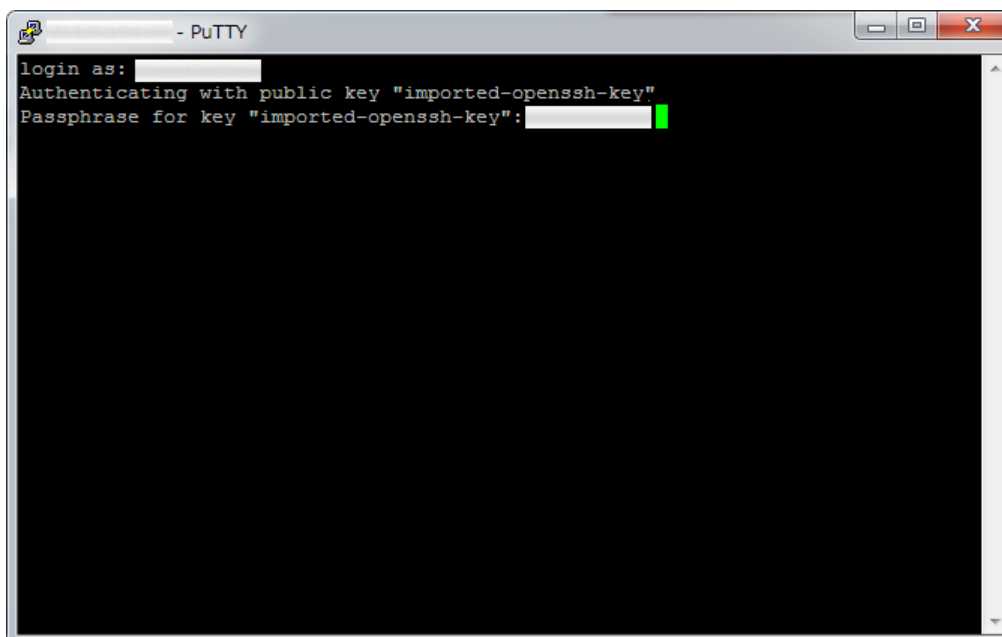


PuTTY でサーバーへ接続がされました。

login as: ウェブコントロールパネルのユーザー  
ID を入力して Enter キーを押してください。

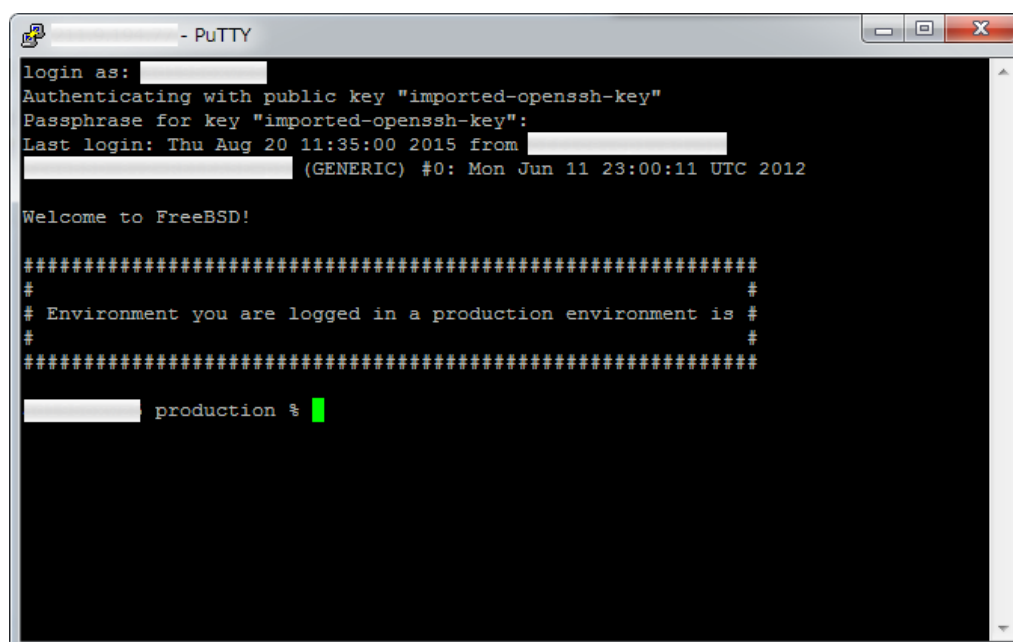


鍵ペアを生成するときにパスフレーズを設定した場合は、パスフレーズを入力し Enter キーを押してください。



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 % █
```