

PuTTY 0.75で導入された新しい鍵形式(PPK バージョン 3)に関するエラー

はじめに

PuTTY 0.75 ではデフォルトの秘密鍵フォーマットが新しくなっていますが(PPK バージョン 3)、PuTTY 0.74 以前のバージョンでこれを読み込むことができません。PuTTY 本体については鍵を作ったバージョンと同じバージョンのものを用いていれば問題になりませんが、WinSCP のように内部的に PuTTY を使っている場合はそのバージョンが問題になります。

- WinSCP はバージョン 5.19 で PPK バージョン 3 に対応しました。それ以前のバージョンをご利用の場合は 5.19 以降にアップデートするか、以下の手順で PPK バージョン 2 をご利用ください。
- (2022/1/5) FileZilla は 3.54.1 では未対応でしたが、3.57.0 では対応できているようです。

他のソフトでも 'Unable to load key file "new.ppk" (PuTTY key format too new)' のようなエラーメッセージが表示された場合はほぼ間違いなくこの鍵形式の問題だと思われます。

対応方法

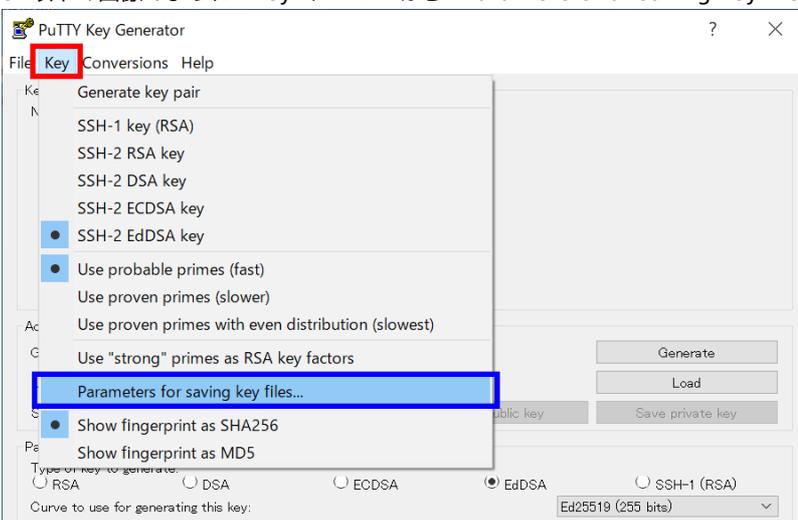
以下の対応が可能です。しばらく待たば FileZilla 等のソフトについても順次対応されると期待されますので、状況によってはそれも一つの選択肢となります。

- PuTTY (PuTTYgen) 0.74 以前を使って鍵を作る
- PuTTY (PuTTYgen) 0.75 以降で鍵を作る際に PPK version 2 を指定する

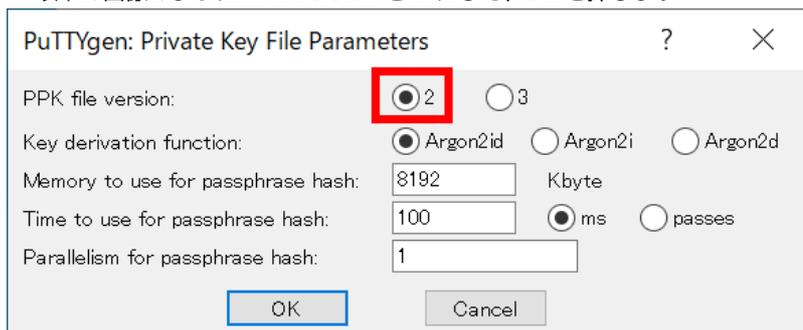
0.74 以前のバージョンで作った鍵については問題無く利用できます。0.75 以降で古い形式の鍵が必要な場合は以下の手順に従ってください。

PuTTYgen 0.75 以降で PPK バージョン 2 を利用する方法

1. PuTTYgen のウィンドウを開きます
- 2a. (既存の鍵の形式を変更する場合は "Load" ボタンを使うなどして鍵ファイルを読み込みます)
- 2b. (鍵を新規作成する場合は形式を指定の上 Generate ボタンをクリックして生成します(クリック後マウスを動かしてください)。上部に表示されている OpenSSH 形式の公開鍵についてもメモ帳に貼り付けるなどして保存してください。)
3. 以下の画像のように "Key" メニューから "Parameters for saving key files..." を選びます。



4. 以下の画像のように PPK version を 2 にして、OK を押します



5. PuTTYgen のメインウィンドウで "Save private key" より鍵を保存します。(秘密鍵の形式変更では OpenSSH 形式の公開鍵は変わりません。)

鍵の生成、読み込み前に PPK バージョンの切り替えを行っても問題ありません。

参考

- <https://www.chiark.greenend.org.uk/~sgtatham/putty/wishlist/ppk3.html> (英語)