

# TortoiseGit による SSH 通信用秘密鍵・公開鍵生成手順

2013/6/20

## ■ 秘密鍵と公開鍵について

秘密鍵と公開鍵は、通信データを暗号化・複合化する際に、一対で扱われるものである。

以下の特徴がある。

- ・秘密鍵と公開鍵とは、何桁かの数字の集まりであり、通常テキストファイルの形式で保存される。
- ・秘密鍵と公開鍵は、ユーザー自身が作成する。
- ・秘密鍵はそのままユーザーが自分の PC に保持する。(秘密鍵がそれを作成した PC の外に出る事は基本的にない)
- ・秘密鍵は、「パスフレーズ」と呼ばれる一種のパスワードで保護されている為、万が一秘密鍵が漏洩しても、パスフレーズを知らなければ扱う事ができない。
- ・秘密鍵と公開鍵は一緒に作成され、公開鍵は通信先のサーバーに保存する。
- ・公開鍵の受け渡し方法はサーバーによりさまざま。
- ・秘密鍵、公開鍵共に幾つかの規格がある為、サーバーに合わせた規格を使用する。

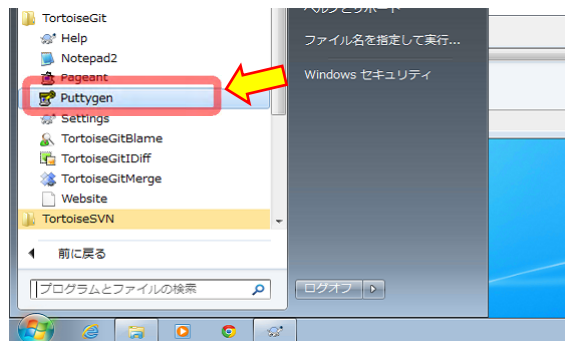
## ■ 秘密鍵と公開鍵の生成方法①：puttygen を使用する方法

前提①：Windows 上で鍵を生成する。

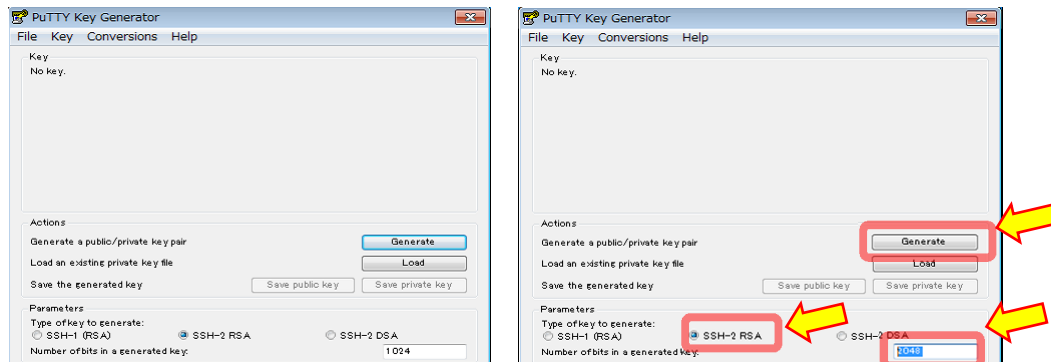
前提②：TortoiseGit をインストールしている。

前提③：サーバー側で SSH-2 という方式の通信サービスが稼働している。(RSA 認証方式が使用可能) ※SSH 通信に対応したサーバーなら、大抵がこの状態と思ってよい。

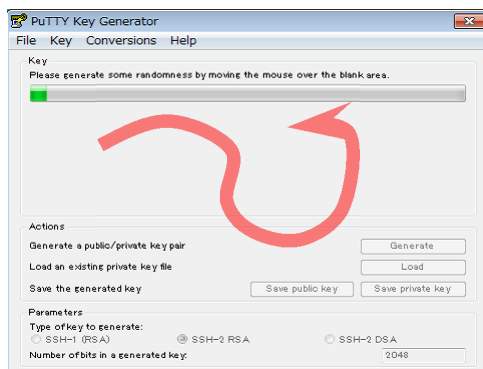
手順①： スタートメニューから「TortoiseGit」→「Puttygen」を実行。



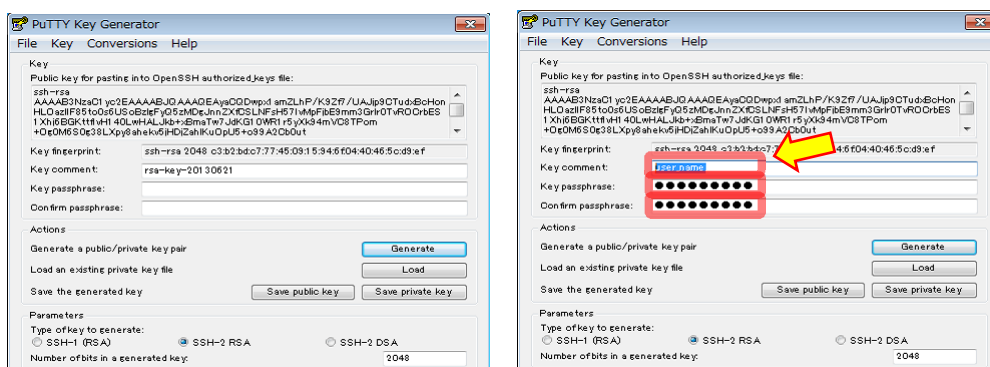
手順②： PuTTY Key Generator が起動したら、まず、「Parameters」にて、「SSH-2 RSA」を選択し、「Number of bits in a generated key」に「2048」を入力し、「Generate」ボタンを押す。



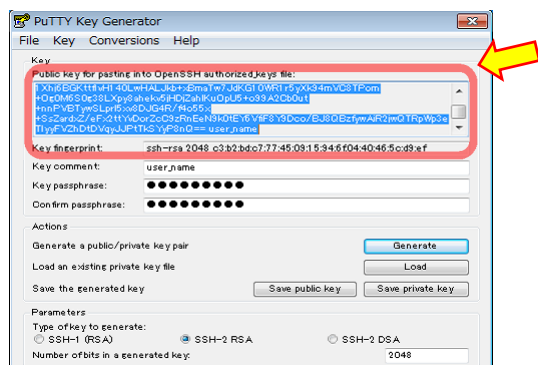
手順③： ウィンドウの上でマウスカursorをぐるぐる動かすとプログレスバーが進むので、完了するまで動かし続ける。（これによって不規則な鍵を生成する）



手順④： 鍵の生成が完了したら、「key-comment」欄にユーザーIDを入力し、「Key passphrase」欄と「Confirm passphrase」欄に同じパスワードを入力する。



手順⑤：「Public key for pasting into OpenSSH authorized\_keys file」欄の文字列が、サーバー上に配置する公開鍵。これを全文選択してメモ帳などにコピーし、「(ユーザーID) .pub」といったファイル名で保存する。

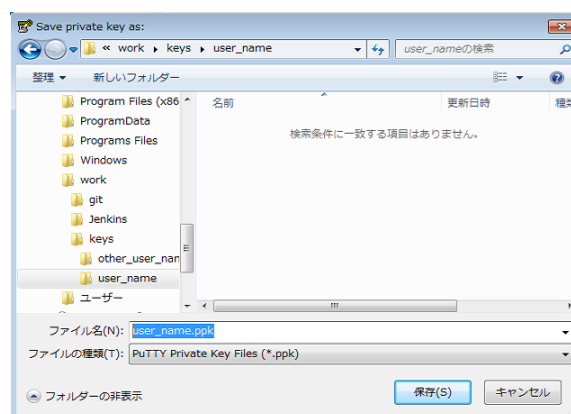
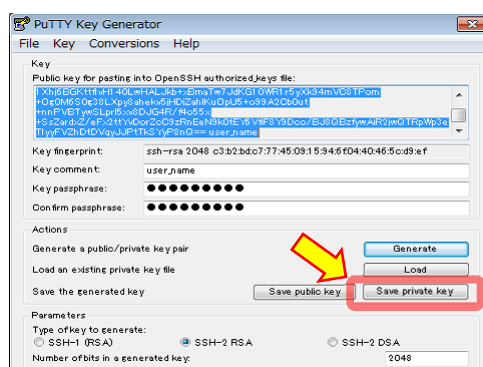


※ [Save public key] ボタンで保存されるファイルとは形式が違うので注意。  
多くの SSH サーバー (Git でよく使用されるサーバー) は、上記の形式 (OpenSSH 形式) で扱われる。途中改行を一切含まない、長い 1 行の文字列である点に注意。

公開鍵 (OpenSSH 形式) の内容例：

```
ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAQEAwPkbM7r13MftK9Lb+hHDP4qLslSxkXV6tbK+dY2tF
9tDihq2jqzw9zWic8L5vOztL7bfaNobfOwTa8mWtPgN6b58kEZAAtWJ4JH5XIB/USP6k7x01YX
mDABsnDRm7RwfXfv8BM9/d9lJPXv6bGKxux4BmRZOn+IW8HSBoATBAj2fPykFewTAQh9d0
Ncmu5O0bttbiVkYL3vaRTj6ofSrYXFvGrdmK+UvUsoWun4DG7Z4LF43hBvUWPJ+K97fa6CnI
+Rr1P40DiAfiiP+QtMdzcMkcj/LenouPMMKZsM/0yMhoZxxnJ6lwgXbZ51R2yxLJGAE00CVjY
PvZCL1DOhw== user_name
```

手順⑥：[Save private key] ボタンを押し、秘密鍵をローカル PC 上に保存し、以後ファイルをむやみに他者やサーバーにコピーしたり紛失したりしないように各自名を付ける。



※ファイルの拡張子は「.ppk」。秘密鍵にも幾つかの形式があるが、TortoiseGit では、この .ppk の形式 (PuTTY 形式) が使用される。

秘密鍵 (PuTTY 形式) の内容例：

```
PuTTY-User-Key-File-2: ssh-rsa
Encryption: aes256-cbc
Comment: user_name
Public-Lines: 6
```

```

AAAAB3NzaC1yc2EAAAABJQAAAQEAYaCQDwpx1amZLhP/K9Zf7/UAJp9CTudxBcH
onHL0azIIF85to0s6USoBzlgFyQ5zMDgJnnZXfCSLNFsH571vMpFjbE9mm3GrLr0
TvROCRbES1Xhj6BGKttfVH140LwHALJkb+xBmaTw7JdKG10WR1r5yXk94mVC8TP
om+Og0M6S0g38LXpy8ahekv5jHDjZahIKuOpU5+o99A2Cb0ut+nnPVBtywSLprl5
xv8DJG4R/f4o55x+SsZardxZ/eFx2ttYvDorZcC9zRnEeN9k0tEY6VfiF8Y9Dco/
BJ8QBzfywAiR2jwQTRpWp3eTIyyFVZhDtDVqyJJPtTkSYyP8nQ==
Private-Lines: 14
ct6DvZmJ/JPd90suwAoI2VKZA8a1eKYRyt0Nv/9tvdGyRDPp9n+aUj+Yt/i6aZal
fuSMjik0WMvrDHW1KN1N46esti+EDLCUsLDpyl4XtrUC//sdZ2ZMj+8jV109fDwy
WhUB2aPa66RTIS0D/qO1Eo8MKCx/EHH8uvVUEshnVu5VeBThbe5D3TwjWWS6hmCs
QIIRyR+m+HKP0MqDfgMJ+bLjhn4Y4lpmBFqit2P0vF5ZS/Mq8laVQ/5MhXfEUC
Dvff9ZZ69p2l/sJbuJbG+EYACfPMJJZO4220QG3X0019SQgWuZf5x27+hy5tKos
e06TNMYZoji1hif66p8WBj1WMh4RjQFXwUX0+nsjlZJ0Uw9zhrqws458Zluq5pKM
3SQtyA1EgMM+jK3gEKvJqnic6zz3pWkBTdvORX34IIOxj2s/al6kgwVChA7H+akq
QPPenoD10kuwlyPlvHybH9T7uYqSlx9rGbTe23hxmqaAhpCV0v2Bc5MVAD8JLUtZk
wQLTs24T+gr3nAwCdrXG9D58Fx1t1UQDvaLh8CDyXGhlmy0iue7nsiZl30TSV7XC
Yy14CeXIDWPt6mR0fI0rRD2g5A8+5Pu3bFuCACIAJjUYF8xMnm2Ob76zul4wF+4W
V2ZpyFg8oda/HPvCZ7WApIFez/IWT9oRPQvozZcGRH+yiA4Ox5KD+oJkkLUn2Fmy
UxpAaB/9AyLuKh8rFGRJpkpdlC+41QfbKTBRZR7Tsr1wfAM1JHk6X8dP+v/nr
NZCr+ut8Y0gTX7nPFw8ifOEM6LtkQGVmla3yKxOz+/EMt8gvYlAmo+uq0Tvv1a65
zztcS2zW2Cp7oBLUojYd0IVDKxQtZ/ZNOwoaB7uznsH+xzX5TUa7lID5dKr42zGK
Private-MAC: 0e39ab3db21a808adc8be806fa44bfcdb7db97d9

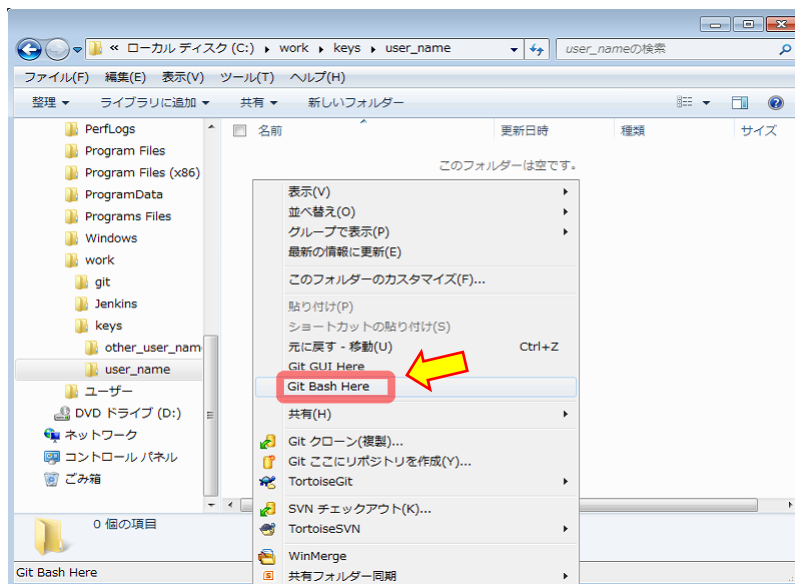
```

## ■ 秘密鍵と公開鍵の生成方法②：ssh-keygen コマンドを使用する

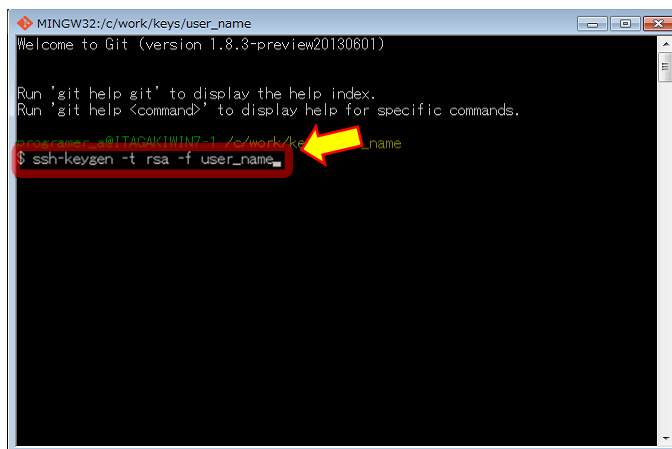
### 方法

前提：msysGit がインストールされている。(Linux 上で鍵を生成する場合の手順もほぼ同様)

手順①：エクスプローラーにて、鍵を生成したいフォルダ上で右クリックし、コンテキストメニューから「Git Bash Here」を実行する。



手順②： シェル（コマンドプロンプト）が起動したら、`ssh-keygen -t rsa -f`（ユーザーID） というコマンドを実行する。

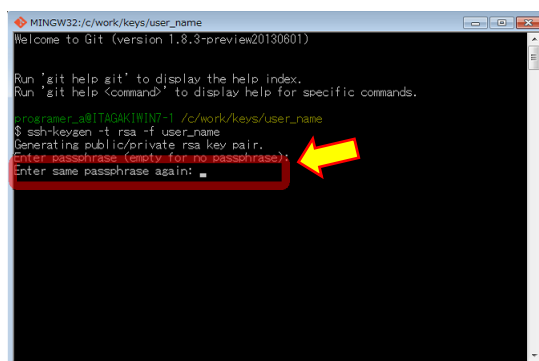


```
MINGW32:/c/work/keys/user_name
Welcome to Git (version 1.8.3-preview20130601)

Run 'git help git' to display the help index.
Run 'git help <command>' to display help for specific commands.

programer_a@ITAGAKIWIN7-1 /c/work/keys/user_name
$ ssh-keygen -t rsa -f user_name
```

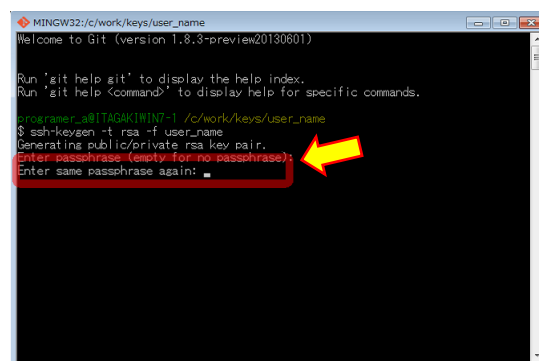
手順③： 続いてパスフレーズを 2 回入力すると、同フォルダにユーザーID をファイル名とした公開鍵ファイルと秘密鍵ファイルが生成される。（公開鍵ファイルは拡張子が `.pub` で、秘密鍵ファイルは拡張子なし）



```
MINGW32:/c/work/keys/user_name
Welcome to Git (version 1.8.3-preview20130601)

Run 'git help git' to display the help index.
Run 'git help <command>' to display help for specific commands.

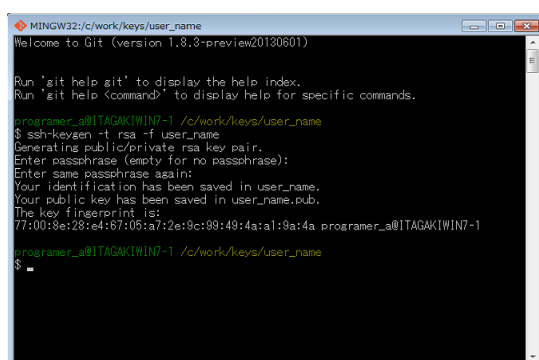
programer_a@ITAGAKIWIN7-1 /c/work/keys/user_name
$ ssh-keygen -t rsa -f user_name
Generating public/private rsa key pair.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
```



```
MINGW32:/c/work/keys/user_name
Welcome to Git (version 1.8.3-preview20130601)

Run 'git help git' to display the help index.
Run 'git help <command>' to display help for specific commands.

programer_a@ITAGAKIWIN7-1 /c/work/keys/user_name
$ ssh-keygen -t rsa -f user_name
Generating public/private rsa key pair.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
```

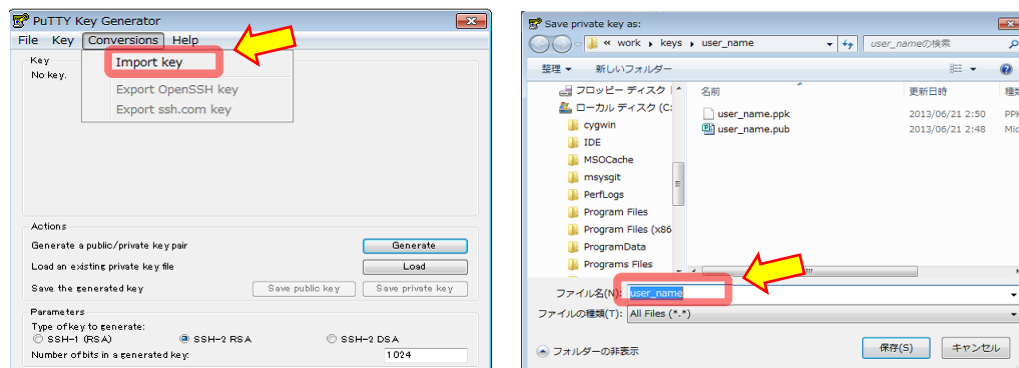


```
MINGW32:/c/work/keys/user_name
Welcome to Git (version 1.8.3-preview20130601)

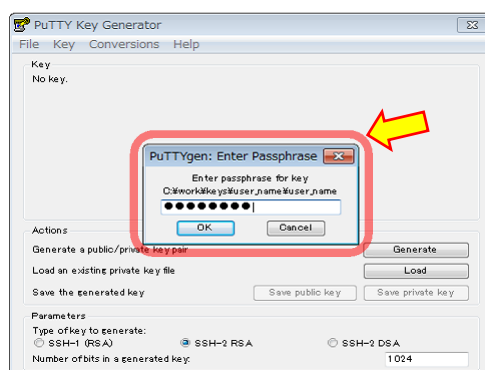
Run 'git help git' to display the help index.
Run 'git help <command>' to display help for specific commands.

programer_a@ITAGAKIWIN7-1 /c/work/keys/user_name
$ ssh-keygen -t rsa -f user_name
Generating public/private rsa key pair.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in user_name.
Your public key has been saved in user_name.pub.
The key fingerprint is:
77:00:8e:28:e4:67:05:a7:2e:9c:99:49:4a:a1:9a:4a programer_a@ITAGAKIWIN7-1
programer_a@ITAGAKIWIN7-1 /c/work/keys/user_name
$
```

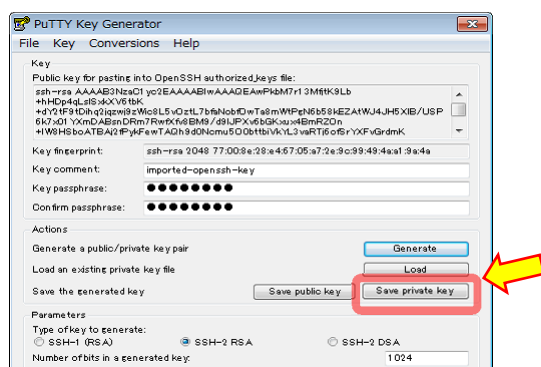
手順④：ここで生成された秘密鍵は OpenSSH 形式の秘密鍵である為、TortoiseGit で使えるように、PuTTY 形式のファイル（.ppk ファイル）に変換する必要がある。その為に、まず、pputtygen を起動し、作成した秘密鍵を[Conversions]→[Import Key] メニューを実行してインポートする。



手順⑤：インポート時にパスフレーズの確認が求められるので、パスフレーズを入力する。



手順⑥：インポートが完了したら、[Save private key] ボタンを押し、PuTTY 形式の秘密鍵ファイルを保存する。

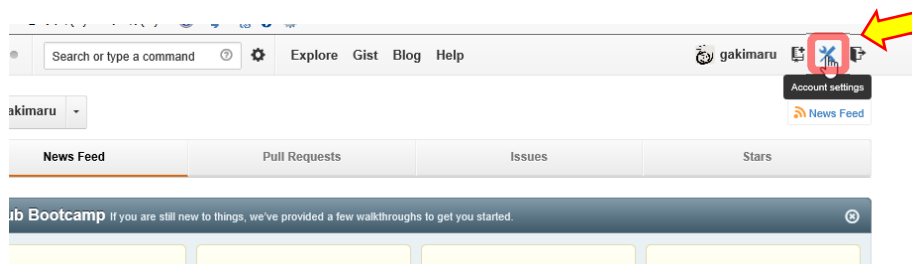


## ■ 公開鍵をサーバーに送る方法（GitHub の例）

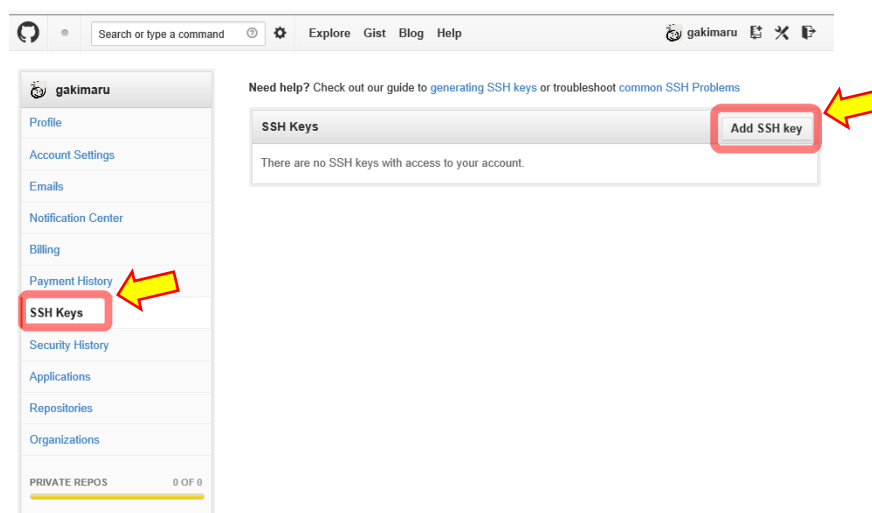
前提①：既に GitHub のアカウントを持っている。

前提②：事前に GitHub 上でリポジトリを作成している。

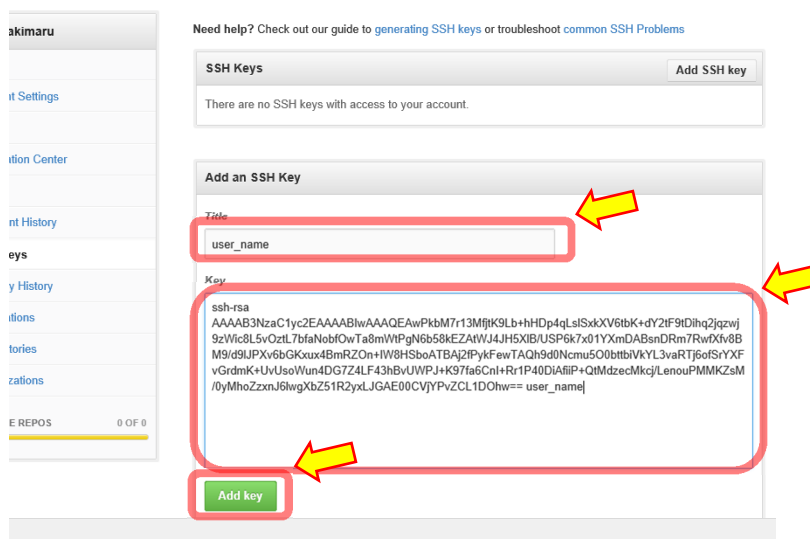
手順①： GitHub の Web サイト <https://github.com/> にアクセスし、サインインしたら、「Account Settings」を実行する。



手順②： アカウント設定画面を開いたら、左側のメニューから「SSH Keys」を選択し、右側の「SSH Keys」欄右上の「Add SSH Key」ボタンを押す。

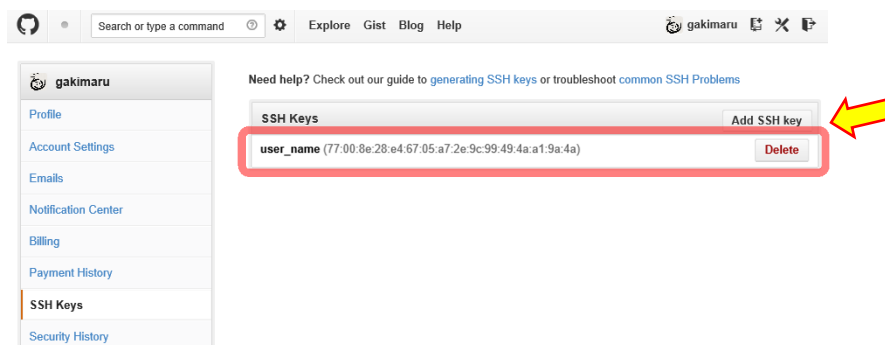


手順③： 「Title」欄に鍵の見出しを入力し、「Key」欄に公開鍵（.pub ファイル）の内容をコピー（この公開鍵の形式は、先述の、途中に一切の改行がない一行のテキストで表される形式）、入力完了したら、画面下側の「Add key」ボタンを押す。



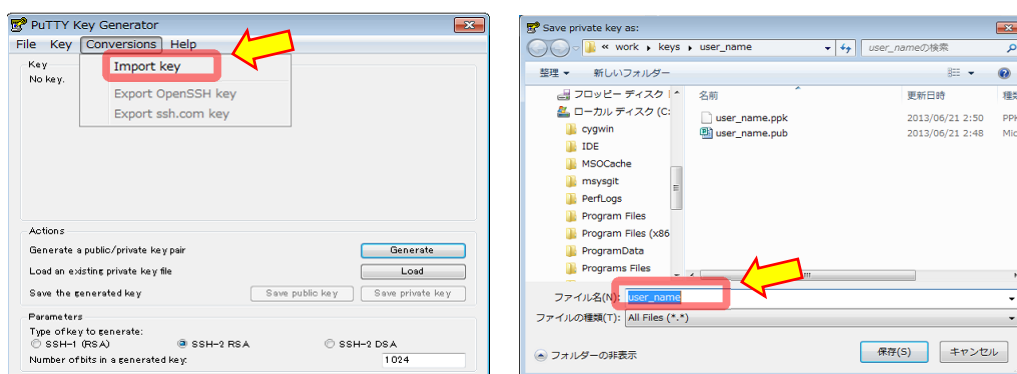


手順④： 完了すると、追加された鍵の情報がリストに表示されるようになる。

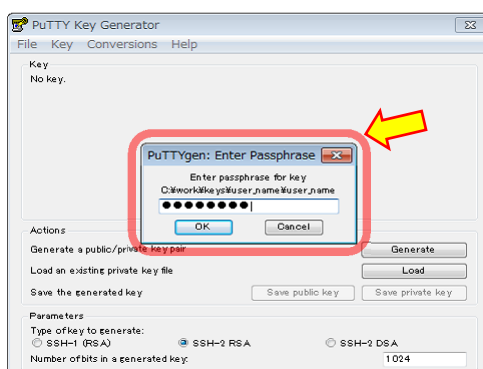


## ■ 秘密鍵のパスフレーズを変更する方法：puttygen を使用する方法

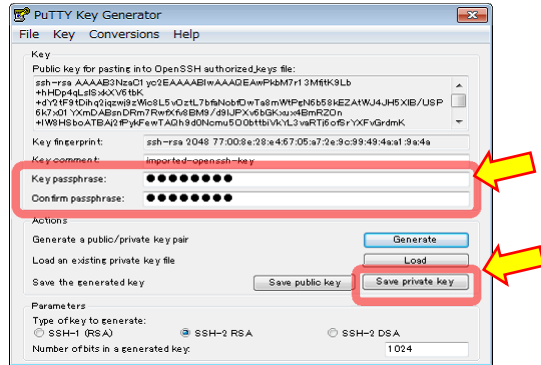
手順①： まず、pputtygen を起動し、既存の秘密鍵を [Conversions] → [Import Key] メニューを実行してインポートする。(PuTTY 形式でも OpenSSH 形式でも良い。)



手順②： インポート時にパスフレーズの確認が求められるので、パスフレーズを入力する。



手順③： インポートが完了したら、改めてパスフレーズを入力し直した上で、[Save private key] ボタンを押し、PuTTY 形式の秘密鍵ファイルを保存する。（公開鍵は変わっていないので、保存し直す必要はない。）



以上