

PGP鍵のインポート



本ページの記述は古いものです。現在は [貴学にてSPをインストールする場合の構築手順](#) にフィンガープリントの確認方法およびインポート方法が含まれております。

PGP鍵のインポート (★)

素の状態ではyumコマンドにてインストールを実行すると、

```
Importing GPG key 0x7D0A1B3D "security:shibboleth OBS Project <security:shibboleth@build.opensuse.org>" from http://download.opensuse.org/repositories/security:/shibboleth/CentOS_5/repodata/repomd.xml.key
Is this ok [y/N]:
```

と聞かれますが、PGP鍵を確認せずにインストールすることは大変危険です。
このPGP鍵を確認するためにあらかじめ以下の手順を実行してください。

Shibboleth関連のPGP鍵は以下のURLにあります。

https://shibboleth.net/downloads/PGP_KEYS

リンク先のテキストには

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
(中略)
-----END PGP PUBLIC KEY BLOCK-----
```

となっているところがいくつかありますが、そのうち"OBS security:shibboleth RPM repository key"の文字列のすぐ下にあるもの（2020年3月時点で11カ所中最後から3番目）を（-----から始まる行も含めて）コピーして、以下のコマンド等で新たに作成したKEYSというファイルにペーストしてください。
※vi以外のテキストエディタを使う場合、最終行に改行が入らないエディタがありrpmコマンドで失敗する場合がありますので、念のため最終行に改行を入れてください。

```
vi KEYS
```

次に以下のコマンドを実行し、

```
gpg --with-fingerprint KEYS
```



お使いのGPGのバージョンが2.1.14もしくはそれ以降の場合は以下を実行してください。

```
gpg -n --import --import-options import-show KEYS
```

以下のフィンガープリント（指紋）と一致することを確認してください。

```
pub 1024D/7D0A1B3D 2008-06-30 security:shibboleth OBS Project <security:shibboleth@build.opensuse.org>
フィンガー・プリント = 6519 B5DB 7C1C 8340 A954 ED00 73C9 3745 7D0A 1B3D
```

※この鍵IDおよびフィンガープリントの値は今後変更になる可能性があります。値が異なっている場合は事務局までご連絡いただければ幸いです。

下記コマンドで、このPGP鍵をインポートすれば完了です。

```
# rpm --import KEYS
```

このとき

```
エラー: KEYS: インポート読み込みに失敗しました(0)。
```

とエラーが出る場合は改行コードの問題が考えられます（WindowsでKEYSを作成した場合など）。その場合は以下のコマンドでエラーが解消されるか確認してください。

```
# tr -d ¥¥r < KEYS > KEYS.lf ; rpm --import KEYS.lf
```

エラー: KEYS: key 1 import failed.

とエラーが出る場合はすでにPGP鍵がインポートされている可能性があります。以下のコマンドで

```
# rpm -qa gpg-pubkey
```

次の出力が含まれる場合はすでにPGP鍵がインポートされていますので次に進んでください。

```
gpg-pubkey-7d0a1b3d-53ea2ad3 （最後のハイフン以降は異なっても問題ありません）
```

念の為下記コマンドでこのPGP鍵を用いて署名検証が行われることをチェックしてください。

```
# grep gpgcheck /etc/yum.repos.d/shibboleth.repo  
gpgcheck=1 ← =1であれば署名検証が行われる
```

ここまで終了したら、[元に戻って「yum install shibboleth」の所](#)から続きを行ってください。