秘密鍵に含まれている公開鍵の確認手順について

OpenSSLを用いてPEM形式(テキストファイル）の秘密鍵に含まれている公開鍵を確認する手順について解説します。

①OpenSSLで以下のコマンドを入力します。

openssl rsa -pubout < 秘密鍵ファイル名

例）秘密鍵ファイル「server.key」の公開鍵を確認する場合
openssl rsa -pubout < server.key

②秘密鍵ファイルの作成時に入力したパスフレーズを入力します。

※設定されている場合のみ

③以下のような公開鍵の文字列が表示されます。

＜公開鍵サンプル＞

```
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAtCIwXZGEPhPCafsG15cW
lf2nDhO+FxPIf4kuRjmgVKmgiUgKODThgg8JCdYVm7ZverLjUHLFnj2ZXHcJ2Csv
zw2Gy6IF3Wg+tEWNi6YzgaUboja5RsAwUzKVzK/K3AoL/ypTqan388VMn0vN28xX
Ndl4sfVudZS9MGHa1goYcwogVy+WNHYZASRJKIMSZJYkLknsajUBk99GvfOVkvTq
R6AOGQOHUos6GNOlfoDtgfa6DLsMFIDCS1fIR4eu5kOBZcZdeOgN1fbpB6mD43Oa
xmFVRosEwILww68B/riCeViKfOP1vQyjJHHdUH88VMunLnJN6LAdajQ3Km4uwgVw
owIDAQAB
-----END PUBLIC KEY-----
```

④公開鍵比較ツールで比較対象のCSRや証明書ファイルの結果を表示し、の文字列と一致しているか比較します。

＜公開鍵比較サンプル＞

秘密鍵とサーバ証明書の公開鍵が不一致の場合、サーバ証明書をインストールできません。
ほかに公開鍵の一致する秘密鍵やサーバ証明書がないか、お確かめください。

万が一、公開鍵の一致する組み合わせがない場合、秘密鍵とCSRを再作成のうえ、サーバ証明書ご申請が必要となります。（同じ公開鍵の秘密鍵は作成できません。）