ダウンロードしたファイルが真正なものであることの確認方法（一般化）

執筆中。以下はメモ書きです。

SP構築のほうにも同等の手順があります。（）

※ この方法はIdPのパッケージファイル自体の検証にも使えます。ダウンロードしたファイルが
　万一悪意により改竄されたものであった場合はシステムに重大な問題を抱えることになります
　ので、ご確認ください。
http://shibboleth.internet2.edu/downloads/maven2/edu/internet2/middleware/shibboleth-jce/1.1.0/
を見ていただくと、shibboleth-jce-1.1.0.jar.ascという署名ファイルがあります。
これを使って署名を検証する（ファイルが真正なものであることを確認する）方法を以下に示します。
1. (初回のみ)Shibboleth開発者のPGP鍵の設定
1.1 検証のためのPGP鍵は以下のURLにあります。
http://shibboleth.internet2.edu/downloads/KEYS
このKEYSは古いもので最新のものはSPの構築ガイドにある通りです。最新のものには
古い鍵が含まれないため古いバイナリの検証にはこれを使います。
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4カ所ありますが、そのうちの2番目の部分（直前に"Chad La Joie"
の文字列がある所です）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 KEYS
1.2 $ gpg --quiet --import KEYS ; gpg --fingerprint 0x146B2514
を実行し、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。
フィンガープリント:
pub   1024D/146B2514 2008-03-20
      Key fingerprint = BEAE 84EE 28F3 2507 02B1 6F07 23DE A65A 146B 2514
uid   Chad La Joie <xxxxxxxxxxx@xxxxxxxxx>

2. shibboleth-jce-1.1.0.jar.ascを同じディレクトリにダウンロードします。
$ wget http://shibboleth.internet2.edu/downloads/maven2/edu/internet2/middleware/shibboleth-jce/1.1.0/shibboleth-jce-1.1.0.jar.asc

3. $ gpg shibboleth-jce-1.1.0.jar.asc
を実行します。最初の2行が
gpg: Signature made Fri 21 Aug 2009 04:47:36 PM JST using RSA key ID A1EAE3E8
gpg: Good signature from "Chad La Joie <xxxxxxxxxxx@xxxxxxxxx>"
のように表示されれば成功です。