

2.3.8もしくはそれ以前のIdPで認証前にログにエラー

```
1:19:57.770 - ERROR [org.opensaml.xml.security.SigningUtil:250] - Error during signature verification java.security.  
SignatureException: Signature length not correct: got 256 but was expecting 128
```

ブラウザには以下のエラーが表示されます。

```
Error Message: Message did not meet security requirements
```

以下の条件を全て満たす場合、認証要求(AuthnRequest)の署名検証時に確率的に問題が発生することが確認されています。IdPのバグで、2.4.0で修正されました。SPメタデータに記載されている不要な証明書を削除することにより回避可能です。

詳細: <https://issues.shibboleth.net/jira/browse/JXT-99>

1. IdPがJava 7を使用している。
2. 接続しようとしているSPのメタデータに1024bitの証明書と2048bitの証明書が混在している。
3. SPが認証要求(AuthnRequest)に署名している。