IdPで認証時のエラーにより再ログインが要求される (Exception unwrapping data: Tag mismatch!)

IdPでログイン済みなのにSSOせず、下記のエラーが idp-process.log に出力されて、再度ログイン画面が表示されます。

```
2020-11-27 13:12:52,167 - xxx.xxx.xxx.xxx - ERROR [net.shibboleth.utilities.java.support.security.DataSealer:252] - Exception
unwrapping data: Tag mismatch!
2020-11-27 13:12:52,178 - xxx.xxx.xxx.xxx - ERROR [org.opensaml.storage.impl.client.ClientStorageService:453] - StorageService
shibboleth.ClientSessionStorageService: Exception unwrapping secured data
net.shibboleth.utilities.java.support.security.DataSealerException: Exception unwrapping data
        at net.shibboleth.utilities.java.support.security.DataSealer.unwrap(DataSealer.java:253)
Caused by: javax.crypto.AEADBadTagException: Tag mismatch!
        at java.base/com.sun.crypto.provider.GaloisCounterMode.decryptFinal(GaloisCounterMode.java:623)
```

IdPは、コンポーネントDataSealerにてAES秘密鍵を使ってcookie等を暗号化しています。詳細は SecretKeyManagement を参照してください。

上記エラーは、バージョンアップ等によりIdPに切り替えた際、または複数のIdPによるIdPクラスタリング環境において、コンポーネントDataSealerのAES秘密鍵が異なるため暗号化されたcookie等が復号できなかったことを示すエラーメッセージです。

復号できなかったことにより、IdPは認証済みの情報が取得できず再度ログイン画面を表示して再認証を要求します。

IdPを切り替えた場合は、利用者が新IdPで再認証することで順次新しい秘密鍵で暗号化したcookie等に置き換わりますので、無視しても大丈夫です。無視できない場合は旧IdPからコンポーネントDataSealerのAES秘密鍵をコピーしてください。

IdPクラスタリング環境では、基本的に共通のAES秘密鍵を使う必要があります。1台目のコンポーネントDataSealerのAES秘密鍵をその他のIdPにコピーしてください。

コピーするファイルは下記になります。

- /opt/shibboleth-idp/credentials/sealer.*