# credentials/secrets.propertiesの生成

V3からV4にアップデートした場合、以下のようなwarningが記録されるようになりますが設定ファイルの構成の違いによるものですので無視して大丈夫です。

```
WARN [net.shibboleth.idp.installer.impl.CurrentInstallStateImpl:158] - Unable to find property resource '/opt/shibboleth-idp
/credentials/secrets.properties' (check idp.additionalProperties?)
```

V4以降ではパスワードやsaltの情報など機密性を要するもののためのファイルとして credentials/secrets.properties が使われるようになっております。
V3から引き続きアップデートされているかたでこの新書式への移行を希望される場合は以下の手順に従ってください。

### 新書式への移行手順：

1. まず以下のような内容で /opt/shibboleth-idp/credentials/secrets.properties を作成します。またjettyユーザーのみ読み込みできるように適切にパーミッションを設定します。

```
# vi /opt/shibboleth-idp/credentials/secrets.properties
下記の内容で作成
# chown root:jetty /opt/shibboleth-idp/credentials/secrets.properties
# chmod 640 /opt/shibboleth-idp/credentials/secrets.properties
```

**secrets.propertiesテンプレート**

```
# This is a reserved spot for most properties containing passwords or other secrets.
# Created by install at YYYY-MM-DDTtt:tt:tt.tttttttZ

# Access to internal AES encryption key
idp.sealer.storePassword =
idp.sealer.keyPassword =

# Default access to LDAP authn and attribute stores.
idp.authn.LDAP.bindDNCredential             =
idp.attribute.resolver.LDAP.bindDNCredential = %{idp.authn.LDAP.bindDNCredential:undefined}

# Salt used to generate persistent/pairwise IDs, must be kept secret
idp.persistentId.salt =
```

2. 再度 secrets.properties を開き、パスワードおよびsaltの値を埋めてください。それぞれ以下のファイルに記述があるはずです。
/opt/shibboleth-idp/conf/idp.properties:

**idp.properties**

```
（略）

# Settings for internal AES encryption key
#idp.sealer.storeType = JCEKS
#idp.sealer.updateInterval = PT15M
#idp.sealer.aliasBase = secret
idp.sealer.storeResource = %{idp.home}/credentials/sealer.jks
idp.sealer.versionResource = %{idp.home}/credentials/sealer.kver
idp.sealer.storePassword = cookiepass
idp.sealer.keyPassword = cookiepass

（略）
```

/opt/shibboleth-idp/conf/ldap.properties:

**ldap.properties**

```
（略）

# bind search configuration
# for AD: idp.authn.LDAP.bindDN=adminuser@domain.com
idp.authn.LDAP.bindDN                           = uid=myservice,ou=system
idp.authn.LDAP.bindDNCredential                 = myServicePassword


（略）
```

/opt/shibboleth-idp/conf/saml-nameid.properties:

**saml-nameid.properties**

```
（略）

# Do *NOT* share the salt with other people, it's like divulging your private key.
#idp.persistentId.algorithm = SHA
idp.persistentId.salt = changethistosomethingrandom
# BASE64 will match V2 values, we recommend BASE32 encoding for new installs.
idp.persistentId.encoding = BASE32

（略）
```

3. secrets.properties が完成しましたら、移行元ファイルの該当行は不要となりますので削除してください。

以上