旧: idp.properties ファイルの変更

idp.properties ファイルの変更

IdPのentityIDやScopeや証明書などのプロパティ値をidp.properties ファイルに設定します。
entityIDやScopeは、インストール時に入力した値で設定されているので、証明書を設定します。

参照先ディレクトリ（/opt/shibboleth-idp/credentials/）に、サーバ証明書(server.crt)と秘密鍵(server.key)をそれぞれのファイル名でコピーしてください。
また、Tomcatが"tomcat"ユーザで起動されるようになっている場合は、以下のように秘密鍵にアクセス権限をかけるとともに"tomcat"ユーザで参照できるように設定します。

```
chown root:tomcat /opt/shibboleth-idp/credentials/server.key
chmod 640 /opt/shibboleth-idp/credentials/server.key
```

⚠ ここで設定したパーミッションをShibboleth IdPアップデート時に変更されないよう注意が必要です。詳細は IdPv3アップデートに関する情報 をご参照ください。

/opt/shibboleth-idp/conf/idp.properties ファイルを以下のように編集してください。

```
idp.signing.key= %{idp.home}/credentials/server.key
idp.signing.cert= %{idp.home}/credentials/server.crt
idp.encryption.key= %{idp.home}/credentials/server.key
idp.encryption.cert= %{idp.home}/credentials/server.crt
```

idp.entityID.metadataFileを空にし、entityIDをURLとしてアクセスした際に/opt/shibboleth-idp/metadata/idp-metadata.xmlの内容が返される機能を無効化してください。当該ファイルはインストール時に自動生成されるもので、自己署名証明書が使われている等メタデータとして不正確なものです。

```
# Set the entityID of the IdP
idp.entityID = https://...(略)...

# Set the file path which backs the IdP's own metadata publishing endpoint at /shibboleth.
# Set to empty value to disable and return a 404.
idp.entityID.metadataFile=
↑先頭の「#」を削除してコメントを解除し、さらに値を空にしてください。

# Set the scope used in the attribute resolver for scoped attributes
```

詳細: Manage or Disable IdP Metadata Publishing Endpoint - Identity Provider 3 - Shibboleth Wiki