OpenAM 14 認証 POST プロセスクラス リファレンスマニュアル

OSSTech **株式会社**

更新日 2022 年 7 月 14 日
リビジョン 1.2

目次

1 はじめに

1.1 本書の目的

本ドキュメントは OpenAM 14 の認証 POST プロセスクラスの利用マニュアルです。 認証 POST プロセスクラスの設定方法について記載しております。

RPM パッケージのインストール方法については別紙の OpenAM 代理認証オプション (mod_authproxy) 管理者ガイドを参照してください。本ドキュメントに関する記載内容について疑問点等がある場合には、弊社サポート窓口までお問い合わせください。

2 認証 POST プロセスクラス概要

認証 POST プロセスクラスを用いることで、認証プロセスの最後に独自の処理追加することができます。弊社で提供する各認証 POST プロセスクラスの概要について説明します。

2.1 AuthProxyPAP

OpenAM に導入することで、 OpenAM ログイン時にユーザーが入力した「ユーザー名」と「パスワード」、 BASIC 認証用に「Authorization ヘッダーの値」を生成し、セッションプロパティに保持します。 LDAP に暗号化された状態で保存されたパスワードを復号しセッションプロパティに保持することもできます。

保持したセッションプロパティは、 OpenAM Agent 経由で mod_authproxy が取得し、代理認証を行う際に使用されます。

設定方法ついては別紙の 「OpenAM 代理認証オプション (mod_authproxy) 管理者ガイド」や 「LDAP の代理認証用パスワードの暗号化格納ガイド」を参照してください。

2.2 SetCookiePAP

OpenAM に導入することで、ユーザーの OpenAM へのログイン時とログアウト時に任意の Cookie をブラウザにセットすることができます。

2.3 SetLoginDatePAP

OpenAM に導入することで、ユーザーが OpenAM にログインした時刻をユーザーエントリの LDAP 属性にセットし、セッションプロパティに保持することができます。セッションプロパティに保持したログイン時刻は OpenAM Agent 経由で保護されたアプリケーションに 渡したり、 SAML のアサーションに含めることができます。

2.4 SetSessionIDPAP

OpenAM に導入することで、ユーザーが OpenAM にログインした際のセッション ID をセッションプロパティに保持することができます。 保持したセッション ID は OpenAM Agent 経由で保護されたアプリケーションに渡したり、 SAML のアサーションに 含めることができます。

2.5 SetSessionPropertyPAP

OpenAM に導入することで、LDAP 属性を加工してセッションプロパティに保存することができます。「LDAP の属性 + “固定の文字列”」や「LDAP 属性の SHA-1 ハッシュ値」といった加工が可能です。本機能は osstech-openam-14-postauthplugin-1.2-2 以降で利用可能です。

3 認証 POST プロセスクラスの設定

3.1 AuthProxyPAP の導入

AuthProxyPAP の導入方法ついては別紙の「OpenAM 代理認証オプション (mod_authproxy) 管理者ガイド」や「LDAP の代理認証用パスワードの暗号化格納ガイド」を参照してください。

3.2 SetCookiePAP の導入

本節では、SetCookiePAP の設定方法について説明します。

3.2.1 SetCookiePAP の読み込み

OpenAM に SetCookiePAP を読み込む設定を行います。作業は OpenAM 管理コンソールにより行います。

1. OpenAM に管理者 (amAdmin) でログインします。
2. OpenAM 管理コンソールで認証 POST プロセスクラスを設定する画面を表示します。
   - 「レルム」 → 「最上位のレルム (またはサブレルム)」→ 「認証」 →「設定」 → 「ポスト認証プロセス」
3. 認証ポストプロセスクラスの設定に “jp.co.osstech.oam.authentication.pap.SetCookiePAP” を登録します。
4. 画面右上の「保存」をクリックします。

以上で完了です。

3.2.2 SetCookiePAP のプロパティファイルの設定

SetCookiePAP のプロパティファイルを設定します。 war 名が openam の場合、プロパティファイルの配置場所は下記の通りです。

```
/opt/osstech/share/tomcat7/webapps/openam/WEB-INF/classes/SetCookiePAP.properties
```

プロパティファイルで設定する項目は下記の通りです。

項目名	初期値	説明
login.CookieXX ※ XX には任意の数値を入れます。	なし	ユーザーが OpenAM にログイン成功時、 OpenAM から応答される Set-Cookie ヘッダーに追加したい値を設定します。デフォルトでは、Set-Cookie には何も追加されません。 設定例: login.Cookie01=amcookie01=""; Domain=.example.co.jp; Expires=Thu, 01-Jan-1970 00:00:10 GMT; Path=/

項目名	初期値	説明
logout.CookieXX ※ XX には任意の数値を入れます。	なし	ユーザーが OpenAM からログアウト時、 OpenAM から応答される Set-Cookie ヘッダーに追加したい値を設定します。デフォルトでは、 Set-Cookie には何も追加されません。 設定例: logout.Cookie01=amcookie01=""; Domain=.example.co.jp; Expires=Thu, 01-Jan-1970 00:00:10 GMT; Path=/

設定が完了したら Tomcat の再起動を行い、設定内容を反映させます。

3.3 SetLoginDatePAP の導入

本節では、SetLoginDatePAP の設定方法について説明します。

3.3.1 SetLoginDatePAP の読み込み

OpenAM に SetLoginDatePAP を読み込む設定を行います。作業は OpenAM 管理コンソールにより行います。

1. OpenAM に管理者 (amAdmin) でログインします。
2. OpenAM 管理コンソールで認証 POST プロセスクラスを設定する画面を表示します。
   - 「レルム」 → 「最上位のレルム (またはサブレルム)」→ 「認証」 →「設定」 → 「ポスト認証プロセス」
3. 認証ポストプロセスクラスの設定に “jp.co.osstech.oam.authentication.pap.SetLoginDatePAP” を登録します。
4. 画面右上の「保存」をクリックします。

以上で完了です。

3.3.2 SetLoginDatePAP のプロパティファイルの設定

SetLoginDatePAP のプロパティファイルを設定します。 war 名が openam の場合、プロパティファイルの配置場所は下記の通りです。

```
/opt/osstech/share/tomcat7/webapps/openam/WEB-INF/classes/SetLoginDatePAP.properties
```

プロパティファイルで設定する項目は下記の通りです。

項目名	初期値	説明
logindate.attribute.name	なし	ユーザーが OpenAM にログイン成功時、 OpenAM がログイン時刻をセットする LDAP 属性名を設定します。 デフォルトでは、ログイン時刻は LDAP 属性にセットされません。時刻は UNIX time としてセットされます。ログイン時刻、前回ログイン時刻をセッションにセットするにはこの値の設定が必要です。 本設定に設定する属性名は「レルム」 →「最上位のレルム (またはサブレルム)」→ 「データストア」の “ユーザー属性” にも設定しておく必要があります。 設定例: logindate.attribute.name=title
current.session.name	なし	ユーザーが OpenAM にログイン成功時、 ログイン時刻を OpenAM がセットするセッションプロパティ名を設定します。 デフォルトでは、ログイン時刻はセッションにセットされません。logindate.attribute.name の値があり、この値の設定がない場合、ログイン時刻は CurrentLoginDate としてセットされます。 設定例: current.session.name=CurrentSessionTime
old.session.name	なし	ユーザーが OpenAM にログイン成功時、そのユーザーが前回にログインした時刻を OpenAM がセットするセッションプロパティ名を設定します。 デフォルトでは、前回ログイン時刻はセッションにセットされません。logindate.attribute.name の値の設定があり、この値の設定がない場合、前回ログイン時刻は OldLoginDate としてセットされます。 設定例: old.session.name=OldSessionTime

項目名	初期値	説明
logindate.format	なし	OpenAM がセッション値としてセットするログイン時刻のフォーマットを指定します。 フォーマットは SimpleDateFormat クラスで用意されているパターンに従います。この値の指定がない場合、「EEE MMM dd HH:mm:ss zzz yyyy」を指定した場合と同様です。 設定例: logindate.format=yyyyMMddHHmmss

設定が完了したら Tomcat の再起動を行い、設定内容を反映させます。

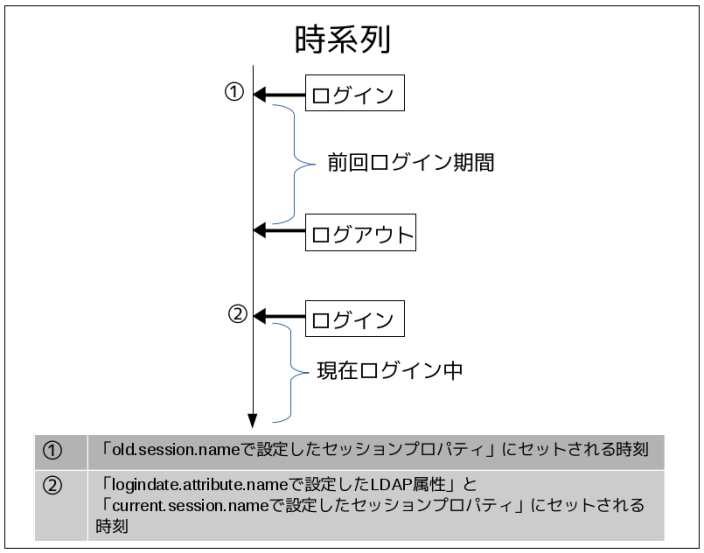

図 1　セットされるログイン時刻と時系列

3.4 SetSessionIDPAP の導入

本節では、SetSessionIDPAP の設定方法について説明します。

3.4.1 SetSessionIDPAP の読み込み

OpenAM に SetSessionIDPAP を読み込む設定を行います。作業は OpenAM 管理コンソールにより行います。

1. OpenAM に管理者 (amAdmin) でログインします。
2. OpenAM 管理コンソールで認証 POST プロセスクラスを設定する画面を表示します。
   - 「レルム」 → 「最上位のレルム (またはサブレルム)」→ 「認証」 →「設定」 → 「ポスト認証プロセス」
3. 認証ポストプロセスクラスの設定に “jp.co.osstech.oam.authentication.pap.SetSessionIDPAP” を登録します。
4. 画面右上の「保存」をクリックします。

以上で完了です。

3.4.2 SetSessionIDPAP のプロパティファイルの設定

SetSessionIDPAP はプロパティファイルを使用しません。セッション ID は PAP-SET-iPlanetDirectoryPro というセッションプロパティ名としてセットされます。

3.5 SetSessionPropertyPAP 導入

本節では、 SetSessionPropertyPAP の設定方法について説明します。

3.5.1 SetSessionPropertyPAP の読み込み

OpenAM に SetSessionPropertyPAP を読み込む設定を行います。作業は OpenAM 管理コンソールにより行います。

1. OpenAM に管理者 (amAdmin) でログインします。
2. OpenAM 管理コンソールで認証 POST プロセスクラスを設定する画面を表示します。
   - 「レルム」 → 「最上位のレルム (またはサブレルム)」→ 「認証」 →「設定」 → 「ポスト認証プロセス」
3. 認証ポストプロセスクラスの設定に “jp.co.osstech.oam.authentication.pap.SetSessionPropertyPAP” を登録します。
4. 画面右上の「保存」をクリックします。

以上で完了です。

3.5.2 SetSessionPropertyPAP のプロパティファイルの設定

SetSessionPropertyPAP のプロパティファイルを設定します。 war 名が openam の場合、プロパティファイルの配置場所は下記の通りです。

```
/opt/osstech/share/tomcat/webapps/openam/WEB-INF/classes/SetSessionPropertyPAP.properties
```

項目名	初期値	説明
session.propertyXX.name ※ XX には任意の数値を入れます。	なし	セットするセッションプロパティ名を設定します。
session.propertyXX.template ※ XX には任意の数値を入れます。	なし	セットするセッションプロパティ値の生成方法を定義します。固定値や LDAP の属性値など組み合わせを指定します。

3.5.2.1 template の設定で記載可能なシンタックス

session.propertyXX.template で指定可能なシンタックスを説明します。

シンタックス	説明
${attribute(“[属性名]”)}	データストアの属性値がセットされます。属性が存在しない場合は空文字となります。 マルチバリューの場合は一つの値のみ取り出されます。(取り出される値は制御出来ません)
${sha1(“ハッシュ化したい値”)}	引数で指定した値の SHA-1 ハッシュ値がセットされます。

3.5.2.2 template のサンプル

session.propertyXX.template で指定した設定値によりセットされる値の例を示します。

データストアの属性が以下の通りとします。

```
sn: YAMADA
givenName: TARO
```

SetSessionPropertyPAP.properties を以下のように設定した場合

```
session.property01.name=fullName
session.property01.template=${attribute("sn")} ${attribute("givenName")}

session.property02.name=helloUser
session.property02.template=Hello ${attribute("sn")} ${attribute("givenName")}.

session.property03.name=hash
session.property03.template=${sha1("stringToBeConvertedIntoHashValue")}

session.property04.name=hashedLDAP
session.property04.template=${sha1(attribute("sn"))}

session.property05.name=hashedHelloUser
session.property05.template=${sha1("Hello "+attribute("sn")+" "
 + attribute("givenName")+".")}
```

セッションプロパティは下記表のとおりセットされます。

名前	値
fullName	YAMADA TARO
helloUser	Hello YAMADA TARO
hash	eUs7mzx467aImuPXqjV/skVUXhQ=
hashedLDAP	e8hHSmHHzSPMpfPm8bxNBUjga5s=
hashedHelloUser	pSQZ1DrHo3jikajKhVx1jFJzhUQ=

4 [参考] Policy Agent のセッション設定

認証 POST プロセスクラスでセットした OpenAM のセッションプロパティを OpenAM Agent 経由で保護されたアプリケーションに渡すには、以下の設定を行います。 作業は OpenAM 管理コンソールより行います。

1. OpenAM に管理者 (amAdmin) でログインします。
2. OpenAM 管理コンソールで Agent の「セッション属性処理」を設定する画面を出します。
   - 「レルム」 → 「最上位のレルム (またはサブレルム)」 → 「エージェント」→ 「web」 → 対象のエージェントを選択 → 「アプリケーション」
3. 「セッション属性処理」の「セッション属性フェッチモード」で HTTP_HEADER にチェックを入れます。
4. 「セッション属性マップ」でマップキーにセッションプロパティ名、対応するマップ値には保護しているアプリケーションにセッション値を渡す際の HTTP ヘッダー名を設定します。以下に設定例を示します。

マップキー	対応するマップ値
CurrentLoginDate	Session-CurrentLoginDate
OldLoginDate	Session-OldLoginDate
PAP-SET-iPlanetDirectoryPro	Session-PAP-SET-iPlanetDirectoryPro

5. 画面右上の「保存」をクリックします。

以上で完了です。

5 改版履歴

- 2019 年 12 月 24 日 リビジョン 1.0
  - 初版作成
- 2021 年 03 月 01 日 リビジョン 1.1
  - SetSessionPropertyPAP を新規追加
- 2022 年 07 月 14 日 リビジョン 1.2
  - 表紙の社名を OSSTech 株式会社に変更