Apache 2.0 Policy Agent

リファレンスマニュアル

オープンソース・ソリューション・テクノロジ(株)

作成日: 2013 年 1 月 11 日

更新日: 2012 年 2 月 15 日

リビジョン: 1.1

目次

1. はじめに

本ドキュメントは Apache 2.0 Policy Agent の利用マニュアルです。Apache 2.0 Policy Agent のインストール方法及び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パッケージインストール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。

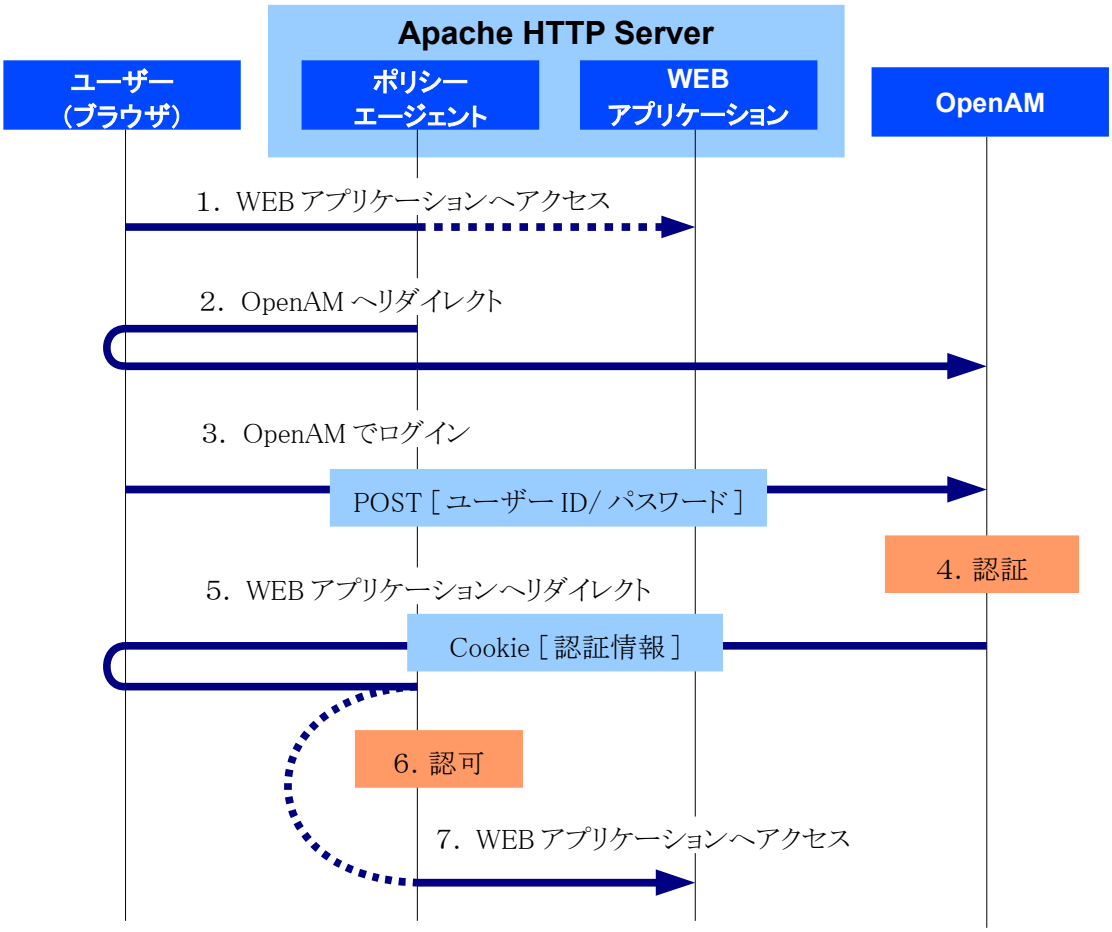
2. ポリシーエージェント概要

ポリシーエージェントは保護された WEB リソースへアクセスするユーザーのリクエストを止め、OpenAM による認証・認可が済むまでリソースへのアクセスを拒否します。

2.1 処理概要

「保護対象の WEB アプリケーション」-「ポリシーエージェント」-「OpenAM」によるシングルサインオンのフローを説明します。

なお、ここではポリシーエージェントが認可を行うものとします。また、ポリシーエージェントは WEB アプリケーションと同じサーバーにインストールされているものとします。



1. ユーザーは保護対象の WEB アプリケーションにアクセスします。
2. ポリシーエージェントは WEB アプリケーションへのアクセスを止め、OpenAM のセッション Cookie を利用して認証済みかどうかを判断します。認証済みでない場合は OpenAM へリダイレクトします
3. ユーザーは OpenAM でログインを行います。

4. OpenAM は POST されたユーザー ID とパスワードで認証を行います。

5. 認証が終了したら、OpenAM はセッション Cookie を付加して WEB アプリケーションへリダイレクトします。ポリシーエージェントはリダイレクトされた WEB アプリケーションへのアクセスを再度止めて、OpenAM のセッション Cookie から認証済みかどうかを判断します。

6. ポリシーエージェントは WEB アプリケーションへのアクセスを許可します。

7. ユーザーは WEB アプリケーションへアクセスします。

2.2 認証・認可

ポリシーエージェントは OpenAM と連携して認証と認可を行います。認証と認可の違いは以下の通りです。

- 認証 ― ユーザーが本人であることを確認する
- 認可 ― 認証されたユーザーが適切なリソースのみにアクセスするように権限を制御する

2.2.1 認証

ポリシーエージェントはユーザーが認証されていない場合に OpenAM にリダイレクトして認証を促します。

ただし、例外として認証を必要としない URL を OpenAM で設定することができます。設定方法は『3.3 適用されない URL の設定』を参照してください。

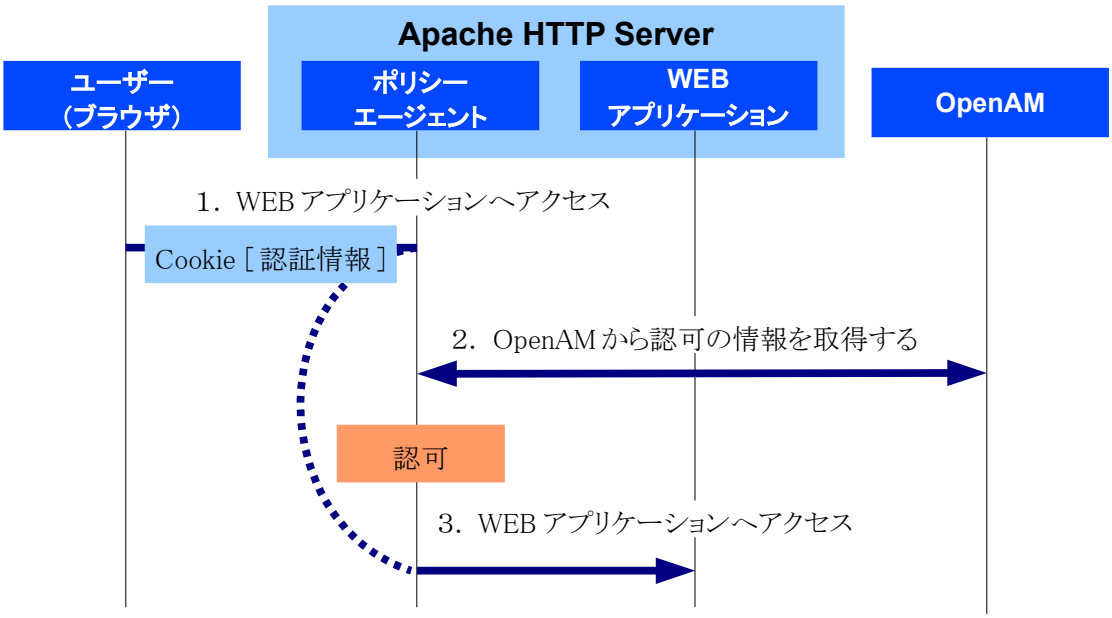
2.2.2 認可

認可は以下の2つの方法があります。

- OpenAM で設定するポリシーによりポリシーエージェントが認可を行う方法
- ポリシーエージェントから Cookie やヘッダーで渡されるユーザーの属性を利用して保護対象の WEB アプリケーション自身が判定する方法

なお、ここではユーザーは既に OpenAM での認証を終えているものとし、認証のフローは省略します。

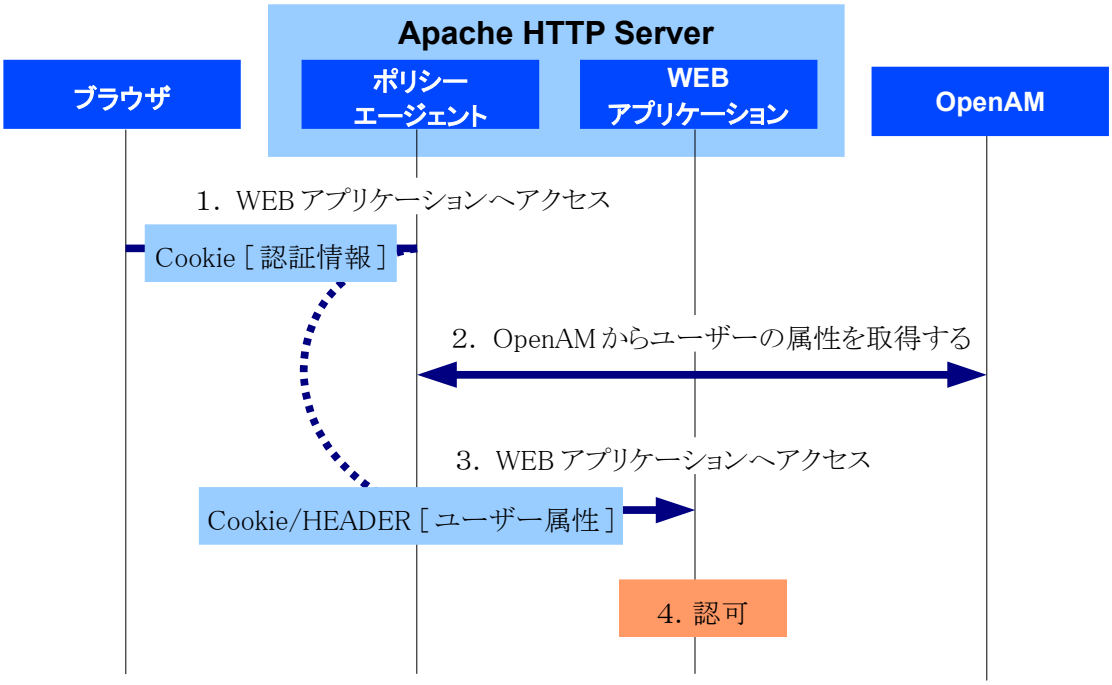
ポリシーエージェントが認可を行う



1. ユーザーは保護対象の WEB アプリケーションへアクセスします。
2. ポリシーエージェントは WEB アプリケーションへアクセスを止め、OpenAM のセッション Cookie から認証済みかどうかを判断します。認証済みの場合は OpenAM と通信して認可を行い、WEB アプリケーションへのアクセスを許可します。
3. ユーザーは WEB アプリケーションへアクセスします。

なお、ポリシーエージェントで認可を行う場合は OpenAM でポリシーを設定する必要があります。設定方法は『5 ポリシーの設定』を参照してください。

保護対象の WEB アプリケーションが認可を行う



1. ユーザーは保護対象の WEB アプリケーションへアクセスします。
2. ポリシーエージェントは WEB アプリケーションへアクセスを止め、OpenAM のセッション Cookie から認証済みかどうかを判断します。認証済みの場合は OpenAM と通信してユーザー情報を取得します。
3. ポリシーエージェントは WEB アプリケーションへのリクエストに Cookie または HEADER を利用してユーザー情報を付加します。ユーザー属性は OpenAM のデータストア(LDAP など)から取得したものです。
4. WEB アプリケーションはリクエストに付加されたユーザー情報を利用してアクセス許可・拒否を判断します。

なお、WEB アプリケーションが認可を行う場合はポリシーエージェントで認可を行わない設定が必要です。その設定方法は『3.4 認証のみ有効(SSO のみモード)』を参照してください。またリクエストに付加するユーザー属性の設定方法は『3.5 ユーザー属性の取得の設定』を参照してください。

3. ポリシーエージェントの設定

この章では OpenAM でポリシーエージェントの設定を行う方法を説明します。

3.1 エージェントプロファイルの作成

OpenAM 側でポリシーエージェント設定(エージェントプロファイル)を作成します。

1. OpenAM に管理者ユーザーでログインします。
2. 「アクセス制御」→「レルム名」→「エージェント」→「Web」を選択します。
3. 「エージェント」の「新規」をクリックします。
4. 各項目を入力します。
   a) 「名前」: エージェントプロファイルの名前を入力します(例として、“apache20”と入力したものとします)。
   b) 「パスワード」: エージェントの認証を行なうためのパスワードを入力します。ここで入力したパスワードは、エージェントをインストールする際に入力する必要があります。
   c) 「設定」:「集中」を選択します。
   d) 「サーバー URL」: OpenAM の URL を入力します。ポート番号も指定してください。
   e) 「エージェント URL」: エージェントの URL を入力します。ポート番号も指定してください。
5. 「作成」をクリックします。

3.2 初期設定

ポリシーエージェントの基本設定について説明します。

1. OpenAM 管理コンソールの「アクセス制御」 → 「レルム名」 → 「エージェント」 → 「Web」 → 対象のエージェントを開きます。
2. 「グローバル」タブの以下のオプションを変更します。これらのオプションは Apache Policy Agent では対応していないため無効にします。
   - 「プロファイル」 → 「通知を有効」: 無効 (有効のチェックをはずす)
   - 「一般」 → 「エージェントのデバッグファイルローテーション」: 無効 (有効のチェックをはずす)
   - 「監査」 → 「ローカル監査ログのローテーション」: 無効 (有効のチェックをはずす)
3. 画面右上の「保存」をクリックして設定を保存します。

以上で完了です。

3.3 適用されない URL の設定

認証を必要としない URL を設定する方法を説明します。

1. OpenAM 管理コンソールの「アクセス制御」→「レルム」の対象レルム →「エージェント」→「Web」→対象のエージェントを開きます。
2. 「アプリケーション」タブの「適用されない URL」にエージェントで保護しない URL を設定します。
3. 画面右上の「保存」をクリックして設定を保存します。

以上で完了です。

もし、保護する URL が限られている場合は、2の「適用されない URL」に保護する ULR を設定し、「適用されない URL の反転」にチェックを入れて保存します。

3.4 認証のみ有効（SSO のみモード）

エージェント上でポリシーによる認可を行わず、認証が完了したユーザーであれば全てのリソースにアクセス可能（認証のみ）とする設定です。設定手順は以下のようになります。

1. OpenAM 管理コンソールの「アクセス制御」→「レルム」の対象レルム→「エージェント」→「Web」を開きます。
2. 「エージェント」の一覧から、対象のエージェントをクリックします。
3. 「グローバル」タブの「一般」セクションの「SSO のみモード」をチェックし、有効にします。
4. 画面右上の「設定」をクリックし設定を保存します。

この設定を有効にした場合、ポリシーの設定をしていてもそれらは全て無視され、認証されたユーザーは全てのリソースにアクセス可能となります。

3.5 ユーザー属性の取得の設定

HTTP ヘッダーにユーザーデータストア（LDAP など）のユーザー属性を格納し、Agent やリバースプロキシの保護下にあるアプリケーションにユーザー情報を渡して認可に利用するための設定方法について説明します。

1. OpenAM 管理コンソールの「アクセス制御」→「レルム」の対象レルム→「エージェント」→「Web」を開きます。
2. 「エージェント」の一覧から、対象のエージェントをクリックし、「アプリケーション」タブを開きます。
3. 「プロファイル属性処理」の「プロファイル属性フェッチモード」から「HTTP_HEADER」を選択します。
4. 「プロファイル属性マップ」に以下の要領でマッピングを追加します。

- 「マップキー」：ユーザーデーターストアの属性名(例：uid)
- 「対応するマップ値」：ヘッダー名(例：UID)

5. 画面右上の「保存」をクリックし設定を保存します。

以上で完了です。

なお、情報を Cookie に格納する場合は、3の「プロファイル属性フェッチモード」に「HTTP_COOKIE」を指定します。

4. ポリシーエージェントのインストール

この章ではポリシーエージェントをインストールする方法を説明します。

4.1 エージェントのインストール

Apache Policy Agent のインストール手順を説明します。

1. 事前にインストールに必要な情報を収集しておきます。

   『3.1 エージェントプロファイルの作成』の手順で設定された OpenAM 側の情報を確認してください。

   - エージェントプロファイルの名前(例:“apache20”)
   - パスワード(例:“password”)
   - サーバー URL(例:“http://sso.example.co.jp:8080/openam”)
   - エージェント URL(例:“http://agent.example.co.jp:80”)

2. Apache HTTP Server (httpd)を停止します。

```
# /sbin/service httpd stop
```

3. パスワードファイルを作成します。

   エージェントが OpenAM と通信する際に使用するパスワードをファイルに記述します。パスワードファイルはエージェントインストール時にのみ必要であり、インストール後は削除してもかまいません。パスワードファイルにはパスワードを平文で記述します。パスワードファイルは一行で記述し、改行コードを含まないものである必要があります。echo コマンドの”-n”オプションや tr コマンドを使用してパスワードファイルを生成します。

```
# echo -n  “password”  > passwd
```

   もしくは

```
# vim passwd
(パスワードを記述して保存)
# tr -d '¥n' < passwd
```

   以下のようなファイルとなります(末尾に改行コードを含みません)。

```
password
```

   以上でパスワードファイルの作成は完了です。記述したパスワードはエージェントインストール時に暗号化されてエージェントの設定ファイルに保存されます。

4. エージェントのインストーラーを実行します。

```
# cd /opt/osstech/share/openam-agent-apache20/bin
```

```
# ./agentadmin --install
Please read the following License Agreement carefully:

[Press <Enter> to continue...] or [Enter n To Finish]
n      #「n」を入力

Do you completely agree with all the terms and conditions of this License
Agreement (yes/no): [no]: yes    #「yes」と入力
```

Apache HTTP Server の設定ファイルが存在するディレクトリのパスを入力します。

```
Enter the complete path to the directory which is used by Apache Server to
store its configuration Files. This directory uniquely identifies the
Apache Server instance that is secured by this Agent.
[ ? : Help, ! : Exit ]
Enter the Apache Server Config Directory Path [/opt/apache/conf]: /etc/httpd/conf
```

OpenAM の URL を入力します。

```
Enter the URL where the OpenSSO server is running. Please include the
deployment URI also as shown below:
(http://opensso.sample.com:58080/opensso)
[ ? : Help, < : Back, ! : Exit ]
OpenSSO server URL: http://sso.example.co.jp:8080/openam
```

エージェントが稼働する Apache HTTP Server の URL を入力します。必ず、ポート番号(「:80」の部分)も指定してください。

```
Enter the Agent URL as shown below: (http://agent1.sample.com:1234)
[ ? : Help, < : Back, ! : Exit ]
Agent URL: http://agent.example.co.jp:80
```

事前に OpenAM 側で作成しておいた、エージェントプロファイルのプロファイル名を入力します。

```
Enter the Agent profile name
[ ? : Help, < : Back, ! : Exit ]
Enter the Agent Profile name: apache20
```

エージェントのパスワードファイルを指定します。

```
Enter the path to a file that contains the password to be used for identifying
the Agent.
[ ? : Help, < : Back, ! : Exit ]
Enter the path to the password file: /opt/osstech/etc/openam-agent-apache20/passwd
```

これまで入力したパラメーターの確認メッセージが表示されます。問題がない場合は「1」を選択し Enter を入力します。

```
---------------------------------------------
SUMMARY OF YOUR RESPONSES
---------------------------------------------
```

```
Apache Server Config Directory : /etc/httpd/conf
OpenAM server URL : http://sso.example.co.jp:8080/openam
Agent URL : http://agent.example.co.jp:80
Agent Profile name : apache20
Agent Profile Password file name : /opt/osstech/etc/openam-agent-apache20/passwd

Verify your settings above and decide from the choices below.
1. Continue with Installation
2. Back to the last interaction
3. Start Over
4. Exit
Please make your selection [1]:
```

インストールログが表示されます。

```
Creating directory layout and configuring Agent file for Agent_001 instance ...DONE.

Reading data from file /opt/osstech/etc/openam-agent-apache20/passwd and encrypting it ...DONE.

Generating audit log file name ...DONE.

Creating tag swapped OpenSSOAgentBootstrap.properties file for instance Agent_001 ...DONE.

Creating a backup for file /etc/httpd/conf/httpd.conf ...DONE.

Adding Agent parameters to
/opt/osstech/etc/openam-agent-apache20/Agent_001/config/dsame.conf file ...DONE.

Adding Agent parameters to /etc/httpd/conf/httpd.conf file ...DONE.


SUMMARY OF AGENT INSTALLATION
---------------------------
Agent instance name: Agent_001
Agent Bootstrap file location:
/opt/osstech/etc/openam-agent-apache20/Agent_001/config/OpenAMAgentBootstrap.properties
Agent Configuration Tag file location
/opt/osstech/etc/openam-agent-apache20/Agent_001/config/OpenAMAgentConfiguration.properties
Agent Audit directory location:
/opt/osstech/etc/openam-agent-apache20/Agent_001/logs/audit
Agent Debug directory location:
/opt/osstech/etc/openam-agent-apache20/Agent_001/logs/debug


Install log file location:
/opt/osstech/etc/openam-agent-apache20/installer-logs/audit/install.log
```

```
Thank you for using OpenSSO Policy Agent
```

5. 設定ファイルを編集してデバッグログのローテーションを無効にします。

   OpenSSOAgentBootstrap.properties に下記の行を追加します。

```
com.sun.identity.agents.config.debug.file.rotate = false
```

   OpenSSOAgentBootstrap.properties は下記のディレクトリに配置されています。(「XXX」はインストール毎に割り当てられる連番です。)

   /opt/osstech/etc/openam-agent-apache20/Agent_XXX/config

6. Apache HTTP Server (httpd)を起動します。

   Apache HTTP Server を起動するには、OpenAM で『3.1 エージェントプロファイルの作成』の操作が完了している必要があります。

```
# /sbin/service httpd start
```

7. 必要に応じてパスワードファイルを削除します。

```
# rm /opt/osstech/etc/openam-agent-apache20/passwd
```

Apache HTTP Server は既にエージェントにより保護されているため、この状態(何もポリシーを設定していない状態)でアクセスすると、「403 Forbidden」となるはずです。

5. ポリシーの設定

この章では、OpenAM エージェントのポリシー設定について説明します。

5.1 参照ポリシーの作成

※この操作はサブレルムを利用して構築した場合のみ必要です

サブレルムでポリシーを作成する場合は、事前に「/ (最上位のレルム)」で参照ポリシーを作成しておく必要があります。ここでは、参照ポリシーを新規作成する手順を説明します。

1. OpenAM 管理コンソールの「アクセス制御」→「/ (最上位のレルム)」→「ポリシー」を開きます。
2. 「新規参照」をクリックします。
3. 「一般」の「名前」を入力します。
4. 「ルール」の「新規」をクリックします。
5. 「サービスタイプ」は「URL ポリシーエージェント (リソース名あり)」を選択し、「次へ」をクリックします。
6. 「名前」にアクセス制御対象のリソースを表す名前を入力します。
7. 「リソース名」にアクセス制御対象のリソースのルートパスの URL を入力します。
8. 画面右上の「終了」をクリックします。
9. 「新規参照」画面に戻るため、「参照」の「新規」をクリックします。
10. 「値」から、このポリシーの参照を許可するレルムを選択します。「名前」に適当な名前を入力し、画面右上の「終了」をクリックします。
11. 「新規参照」画面に戻るため、画面右上の「了解」をクリックします。
12. 「ポリシーの編集」画面に戻るため、画面右上の「保存」をクリックし設定を保存します。ここで「保存」をクリックすることでポリシーが保存されます。

5.2 ポリシーの作成

ポリシーには主にルール・対象・条件の3つの要素があります。

ポリシーの作成手順としては、まずポリシー名を決定し、そのあとにルール・対象・条件を追加していきます。

ポリシー		
├	ルール	アクセス制御対象 URL に対する許可・拒否の設定
├	対象	アクセスを許可・拒否するユーザーの設定

└ 条件	アクセスを許可・拒否する条件の設定

5.2.1 ポリシー

まずはポリシー名を設定します。

1. OpenAM 管理コンソールの「アクセス制御」→「レルム」の対象レルム→「ポリシー」を開きます。
2. 「新規ポリシー」をクリックします。
3. 「一般」の「名前」を入力します。
4. 画面右上の「了解」をクリックし設定を保存します。

ひきつづき、ルール・対象・条件を設定します。

5.2.2 ルール

アクセス制御対象の URL に対するアクセスの許可/拒否を設定します。

1. OpenAM 管理コンソールの「アクセス制御」→「レルム」の対象レルム→「ポリシー」を開きます。
2. 編集するポリシーをクリックします。
3. 「ルール」の新規をクリックします。
4. 「サービスタイプ」は「URL ポリシーエージェント (リソース名あり)」を選択し、「次へ」をクリックします。
5. 「名前」にアクセス制御対象のリソースを表す名前を入力します。
6. 「リソース名」にアクセス制御対象のリソースの URL を入力します。この URL は「親リソース名」の配下に属するリソースを表す URL しか入力できません。
7. 「アクション」でアクセス制御のルールを選択します。
8. 画面右上の「終了」をクリックします。**この状態では、ポリシーはまだ OpenAM に保存されていないため、ご注意ください。**
9. 「ポリシーの編集」画面に戻るため、画面右上の「保存」をクリックし設定を保存します。

ここで、「サービス iPlanetAMWebAgentService のリソース http://www.example.co.jp/ は現在の組織では管理できません。」いうエラーメッセージが表示された場合は、このポリシー設定の参照元である参照ポリシーで親リソースが定義されていません。「5.1 参照ポリシーの作成」の手順で参照ポリシーを定義してください。

注意点

OpenAM のポリシーでは、ユーザー(ブラウザ)から送出された HTTP リクエストのリソースパスとポリシーで定義されているリソースパスを厳格に比較します。たとえば、”http://www.example.co.jp/”などの URL にアクセスした場合に”http://www.example.co.jp/index.html”のコンテンツがユーザー(ブラウザ)に応答されることがありますが、ポリシーのルールで”http://www.example.co.jp/”へのアクセスを許可しているだけでは、「403 Forbidden」エ

ラーとなります。”http://www.example.co.jp/index.htm”というリソースへの明確なアクセス許可がルールに定義されていないためです。このため、アクセスを許可する場合は、そのリソースのパス(ファイルシステムのパスと一致)を正確にルールで定義してください。

ワイルドカードについて

「リソース名」にはワイルドカードを利用することができます。”http://www.example.co.jp/sampleapp/” の配下のすべてのコンテンツを許可する場合、”http://www.example.co.jp/sampleapp/*” と入力します。

ただし、”http://www.example.co.jp/sampleapp/content.jsp?param1=1”のようにURLにクエリストリングが付加されている場合は”http://www.example.co.jp/sampleapp/*?*”のように”?”をはさみ”*”を2回入力する必要があります。

5.2.3 対象

アクセスを許可する対象ユーザーを設定します。ここでは「OpenAM アイデンティティー対象」を対象として設定し、このレルムで管理されているユーザーにポリシーを適用する方法を説明します。

1. OpenAM 管理コンソールの「アクセス制御」→「レルム」の対象レルム→「ポリシー」を開きます。
2. 編集するポリシーをクリックします。
3. 「対象」の新規をクリックします。
4. 「タイプ」で「OpenAM アイデンティティー対象」を選択します。
5. 「新規対象 – OpenAM アイデンティティー対象」画面で、以下の内容を入力します。
   a) 名前:この対象を識別する任意の名前です。
   b) 排他的:選択されていない場合はc)で設定するアイデンティティーに適用されます。選択されている場合は設定されていないアイデンティティーに適用されます。
   c) フィルタ:対象を検索するためのフィルタです。アイデンティティータイプから「ユーザー」もしくは「グループ」を選択し、「検索」をクリックすると検索結果が表示されます。検索結果からアクセス制御対象のユーザー/グループを選択し、「追加」/「すべてを追加」で「選択」エリアに追加します。
6. 画面右上の「終了」をクリックします。**この状態では、ポリシーはまだ OpenAM に保存されていないため、ご注意ください。**
7. 「ポリシーの編集」画面に戻るため、画面右上の「保存」をクリックし設定を保存します。

5.2.4 条件

アクセスを許可する条件を設定します。ここでは「LDAP フィルタ条件」を条件として設定し、LDAP フィルタで対象のユーザーエントリが見つかった場合にアクセスを許可する設定を説明します。

1. OpenAM 管理コンソールの「アクセス制御」→「レルム」の対象レルム→「ポリシー」を開きます。

2. 編集するポリシーをクリックします。

3. 「条件」の新規をクリックします。

4. 「タイプ」で「LDAP フィルタ条件」を選択します。

5. 「新規条件- LDAP フィルタ条件」画面で、以下の内容を入力します。

   a) 名前:この条件を識別する任意の名前です。

   b) ldapFilter:LDAP で対象を検索するためのフィルタです。

6. 画面右上の「終了」をクリックします。**この状態では、ポリシーはまだ OpenAM に保存されていないため、ご注意ください。**

7. 「ポリシーの編集」画面に戻るため、画面右上の「保存」をクリックし設定を保存します。

5.3 ポリシーの削除

ポリシーを削除する手順は以下のようになります。

1. OpenAM 管理コンソールの「アクセス制御」→「レルム」の対象レルム→「ポリシー」を開きます。

2. 削除するポリシーを選択します。

3. 「削除」をクリックします。

6. 冗長構成

ポリシーエージェントがロードバランサー背後にある場合の注意事項や設定方法を説明します。

6.1 ポリシーエージェント側

ポリシーエージェント自体はロードバランサーを考慮する必要はありません。保護対象の WEB アプリケーションの仕様に従って対応してください。

6.2 OpenAM 側

OpenAM にはポリシーエージェントでロードバランサーに対応するための設定があります。

1. OpenAM 管理コンソールの「アクセス制御」→「レルム」の対象レルム→「エージェント」→「Web」を開きます。
2. 「エージェント」の一覧から、対象のエージェントをクリックし、「高度」タブを開きます。
3. 「ロードバランサ」の以下のオプションにチェックします。
    - 「要求 URL プロトコルの上書き」
    - 「要求 URL ホストの上書き」
    - 「要求 URL ポートの上書き」
    - 「通知 URL の上書き」
4. 画面右上の「保存」をクリックし設定を保存します。

7. ログ

エージェントのログには以下の 2 種類のログがあります。それぞれのログについて、出力方法を説明します。

1. デバッグログ
2. 監査ログ

7.1 デバッグログ

7.1.1 デバッグログの出力先

デバッグログはエージェントが稼働するサーバーの以下のディレクトリに出力されます。

- /opt/osstech/share/openam-agent-apache20/Agent_XXX/logs/debug

7.1.2 ログレベルの変更

デバッグログには以下のログレベルがあります。

- すべて
- エラー
- メッセージ
- 情報
- 警告

デバッグログの出力設定は、管理コンソール(OpenAM 側)から行います。

1. OpenAM 管理コンソールの「アクセス制御」→「レルム名」→「エージェント」→「Web」→「エージェント」の対象エージェントを開きます。
2. 「一般」の「エージェントデバッグレベル」からデバッグレベルを選択します。
3. 画面右上の「保存」をクリックし設定を保存します。

設定後は Apache HTTP Server (httpd)を再起動してください。

7.2 監査ログ

7.2.1 監査ログの出力設定

監査ログを出力するための設定手順は以下のようになります。

1. OpenAM 管理コンソールの「アクセス制御」→「レルム」の対象レルム→「エージェント」→「Web」を開きます。
2. 「エージェント」の一覧から、対象のエージェントをクリックします。
3. 「監査」の「監査アクセスタイプ」から監査ログの出力方式を選択します。
   a) 「LOG_ALLOW」：アクセスが許可された場合にログ出力します。
   b) 「LOG_DENY」：アクセスが拒否された場合にログ出力します。
   c) 「LOG_BOTH」：アクセスが許可された場合と拒否された場合にログ出力します。
   d) 「LOG_NONE」：ログを出力しません。
4. 「監査ログ位置」からログの出力先を選択します。
   a) 「すべて」：OpenAM サーバーとエージェントが稼働するサーバー両方にログが出力されます。
   b) 「リモート」：OpenAM サーバーにログが出力されます。

      OpenAM サーバーの監査ログの出力先は下記のディレクトリです。

      - /opt/osstech/share/tomcat6/openam/openam/log

   c) 「ローカル」：エージェントが稼働するサーバーにログが出力されます。

      エージェントが稼働するサーバーの監査ログの出力先は下記のディレクトリです。

      - /opt/osstech/share/openam-agent-apache20/Agent_XXX/logs/audit
5. 画面右上の「保存」をクリックし設定を保存します。

以上で完了です。

8. トラブルシューティング

ポリシーエージェントでエラーが発生した場合、デバッグログを確認してください。デバッグログの出力先については『7.1.1 デバッグログの出力先』を参照してください。

有効なログが出力されていない場合はログレベルの見直しが必要です。『7.1.2 ログレベルの変更』を参照してログレベルを変更し、エラーを再現してください。

また、OpenAM のポリシーにより WEB アプリケーションへのアクセスが拒否されている場合は監査ログも確認してください。監査ログの出力先については『7.2.1 監査ログの出力設定』を参照してください。

8.1 デバッグログ

8.1.1 ログフォーマット

デバッグログのサンプルを以下に示します。

```
2012-07-26 10:59:19.569    Error 11007:7f441704b2d0 AuthService: AuthService::processLoginStatus()
Exception message=[invalid password] errorCode='103' templateName=login_failed_template.jsp.
2012-07-26 11:02:47.983    Error 11009:7f441704b2d0 AuthService: AuthService::processLoginStatus()
Exception message=[Login Failed User not Active|user_inactive.jsp] errorCode='104'
templateName=user_inactive.jsp.
```

8.1.2 エラーケース

エラーケース、原因、対策の例を以下に示します。

- Invalid password

原因例	ポリシーエージェント設定でパスワードに誤りがある
対策例	ポリシーエージェントの再インストール

- Login Failed User not Active

原因例	ポリシーエージェントが有効ではない
対策例	OpenAM の管理コンソールでポリシーエージェントを有効にする

- An error occured while doing naming request. not found

原因例	ポリシーエージェントの設定でサーバー URL(OpenAM の URL)に誤りがある
対策例	ポリシーエージェントの再インストール

- Application user ID is not valid.

原因例	ポリシーエージェントの設定でエージェントプロファイルの名前に誤りがある
対策例	ポリシーエージェントの再インストール

8.2 監査ログ

8.2.1 ログフォーマット

監査ログのサンプルを以下に示します。

OpenAM サーバーにログを出力する場合

1行目はログの項目を示しています。最初のログがアクセスが許可されたケース、次のログがアクセスが拒否されたケースです。

```
#Fields: time Data LoginID ContextID IPAddr LogLevel Domain LoggedBy MessageID ModuleName NameID
HostName
"2012-07-20 12:30:46" "User demo was allowed access to http://agent.example.co.jp:80/app/index.html."
id=demo,ou=user,dc=opensso,dc=java,dc=net "Not Available" "Not Available" INFO
dc=opensso,dc=java,dc=net id=apache20,ou=agent,dc=opensso,dc=java,dc=net "Not Available"
amAgent_agent_example_co_jp_80.log "Not Available" 172.16.43.1
"2012-07-20 12:38:46" "User demo was denied access to http://agent.example.co.jp:80/app/index.html."
id=demo,ou=user,dc=opensso,dc=java,dc=net "Not Available" "Not Available" INFO
dc=opensso,dc=java,dc=net id=apache20,ou=agent,dc=opensso,dc=java,dc=net "Not Available"
amAgent_agent_example_co_jp_80.log "Not Available" 172.16.43.1
```

OpenAM のログの項目は以下の通りです。

項目	内容
time	時間
Data	ログの概要
LoginID	ログインユーザーの ID
ContextID	セッションに関連付けられた ID
IPAddr	IP アドレス
LogLevel	ログレベル
Domain	ドメイン
LoggedBy	ログを出力したユーザーの ID
MessageID	メッセージに関連付けられた ID
ModuleName	モジュール名
NameID	NameID
HostName	ホスト名

エージェントが稼動するサーバーにログを出力する場合

最初のログがアクセスが許可されたケース、次のログがアクセスが拒否されたケースです。

```
2012-07-26 15:53:41.678    Info 12607:7f4785d752d0 LocalAuditLog: User demo was allowed access to
http://agent.example.co.jp:80/app/index.html.
2012-07-26 16:04:51.641    Info 12612:7f4785d752d0 LocalAuditLog: User demo was denied access to
http://agent.example.co.jp:80/app/index.html.
```

9. 改版履歴

- 2013 年 1 月 11 日　　リビジョン 1.0
  - 初版作成
- 2013 年 2 月 15 日　　リビジョン 1.1

  RPM パッケージのインストール方法をパッケージインストールガイドに移行