OpenAM 14 OpenLDAP 認証モジュール
利用手順書

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

本文書は、OSSTech 版 OpenAM 14 に含まれる OpenLDAP 認証モジュールの利用手順書です。

OpenLDAP 認証モジュールを利用することで、OpenLDAP のパスワードポリシー (slapo-ppolicy) に対応した認証を行うことが可能となります。OpenLDAP のパスワードポリシーについては、OpenLDAP のドキュメントをご参照ください

なお、本文書では、OpenLDAP パスワードポリシーのうち、主に認証時に利用するポリシーについて解説します。OpenLDAP にはパスワード変更時に利用可能なポリシー (パスワードの複雑性の設定など) もありますが、OpenAM からユーザーのパスワード変更を行う機会は少ないため、パスワード変更時のポリシーについては割愛します。

2 想定システム構成

本文書で想定するシステム構成です。

2.1 ホスト名

本文書では、ホスト名を以下のように仮定しています。

【機器】	【ホスト名】
OpenAM 1 号機	oam1.sso.example.co.jp
OpenAM 2 号機	oam2.sso.example.co.jp
ロードバランサー	lb.sso.example.co.jp

2.2 OpenAM のコンテキスト名と設定情報ディレクトリ

OpenAM は、初期設定時に、コンテキスト名を基にして設定情報を保存するためのディレクトリを作成します。ディレクトリのパスは任意に指定可能です。OSSTech 版 OpenAM のデフォルト値は以下のようになります。

【項目】	【値】
コンテキスト名	openam
コンテキストディレクトリ	/opt/osstech/share/tomcat/webapps/openam
設定情報ディレクトリ	/opt/osstech/var/lib/tomcat/data/openam
設定情報ディレクトリ (OpenAM のログなど)	/opt/osstech/var/lib/tomcat/data/openam/openam
OpenAM の URL	http://lb.sso.example.co.jp/openam/

本文書では、OpenAM のコンテキスト名、インストールディレクトリ (コンテキストディレクトリ)、設定情報ディレクトリを以下のように表記します。

【項目】	【表記】
コンテキスト名	{OPENAM_CONTEXT_NAME}
コンテキストディレクトリ	{OPENAM_CONTEXT_DIR} (/opt/osstech/share/tomcat/webapps /{OPENAM_CONTEXT_NAME} となります)
設定情報ディレクトリ	{OPENAM_CONF_DIR} (/opt/osstech/var/lib/tomcat/data /{OPENAM_CONTEXT_NAME} となります)
設定情報ディレクトリ (OpenAM のログなど)	{OPENAM_CONF_DIR}/{OPENAM_CONTEXT_NAME} (/opt/osstech/var/lib/tomcat/data /{OPENAM_CONTEXT_NAME} /{OPENAM_CONTEXT_NAME} となります)
OpenAM の URL	http://lb.sso.example.co.jp /{OPENAM_CONTEXT_NAME}/

例として、コンテキスト名を「example」とした場合は以下のようになります。

【項目】	【値】
コンテキスト名	example
コンテキストディレクトリ	/opt/osstech/share/tomcat/webapps/example
設定情報ディレクトリ	/opt/osstech/var/lib/tomcat/data/example
設定情報ディレクトリ (OpenAM のログなど)	/opt/osstech/var/lib/tomcat/data/example/example
OpenAM の URL	http://lb.sso.example.co.jp/example/

3 OpenLDAP 認証モジュール設定

本章では、OpenLDAP 認証モジュールの設定方法について説明します。

OpenAM において、OpenLDAP のパスワードポリシーに対応した認証を行うためには、ユーザーデータストア標準の認証モジュールではなく、OpenLDAP 認証モジュールを利用する必要があります。

ここでは、あるレルムの認証方式として、OpenLDAP 認証モジュールを利用するための設定方法を説明します。OpenAM が複数台構成の場合、設定作業は 1 号機のみに対して行います。

1. OpenAM に管理者ユーザーでログインします。
2. 対象レルム →「認証」→「モジュール」を開きます。
3.「モジュールの追加」ボタンをクリックします。
4.「名前」に任意のモジュール名を入力し、「タイプ」は「OpenLDAP」を選択して、「作成」ボタンをクリックします。
5. 各パラメーターを入力し、「変更の保存」をクリックします。以下はパラメータの例です。

【項目名】	【設定値】
プライマリ LDAP サーバー	localhost:389 (デフォルトで入力されている値は削除します)
ユーザー検索の開始 DN	ou=Users,dc=osstech,dc=co,dc=jp (デフォルトで入力されている値は削除します)
バインドユーザー DN	cn=oam,dc=osstech,dc=co,dc=jp
バインドユーザーパスワード	「バインドユーザー DN」のパスワードを入力
ユーザープロファイルの取得に使用する属性	uid
認証するユーザーの検索に使用する属性	uid
ユーザー検索フィルタ	(objectclass=inetorgperson)

【項目名】	【設定値】
検索範囲	サブツリー
LDAP Connection Mode	LDAP (セキュアなプロトコルを使用する場合は、 LDAPS または StartTLS を選択する。)
ユーザー DN をデータストアに返す	無効 (有効のチェックをはずす) ※認証用の LDAP とユーザーデーターストアの LDAP が同じ OpenLDAP であれば有効にします。
LDAP Behera パスワードポリシーサポート	有効

6. 左側のメニューより、「認証」→「認証連鎖」→「認証連鎖の追加」をクリックします。
7. 「認証連鎖名」に任意の名前を入力し、「作成」をクリックします。
8. 認証連鎖の設定画面が表示されますので、「モジュールの追加」をクリックします。
9. 「モジュールの選択」のプルダウンから先程作成した認証モジュールの名前を選択し、「基準の選択」は「Required」を選択します。
10. 「OK」をクリックし、認証連鎖の設定画面に戻ったら、「変更の保存」をクリックします。
11. 左側のメニューより、「認証」→「設定」→「Core」をクリックします。
12. 「Core」の「組織認証設定」で、先程作成した認証連鎖の名前を選択し、「変更の保存」をクリックします。

以上で完了です。

4 OpenAM 画面解説

本章では、OpenLDAP のパスワードポリシーに抵触した際に表示される OpenAM の画面などについて説明します。

4.1 OpenAM 画面一覧

OpenAM へログインする際に OpenLDAP のパスワードポリシーに抵触した場合に表示される画面のメッセージについて説明します。

同じポリシーに抵触した場合でも、以下のような条件により、表示される画面が異なることがあります。

- 認証の際に入力したパスワードが正しいパスワードの場合と、不正なパスワードの場合
- 一つのポリシーに抵触している場合と、同時に複数のポリシーに抵触している場合

以下、各条件時の表示画面について、表で示します。

単一のポリシーに抵触している場合

【ポリシー (関連する OpenLDAP の設定ディレクティブ)】	【正しいパスワード入力時に表示される画面】	【不正なパスワード入力時に表示される画面】
アカウントロックアウト (pwdLockout)	「4.2 アカウントロックアウト画面」を参照	「4.2 アカウントロックアウト画面」を参照
パスワード有効期限前の警告 (pwdExpireWarning)	「4.4 パスワード有効期限切れ前の警告画面」を参照	通常の認証失敗画面
パスワード有効期限切れ (pwdMaxAge)	「4.3 パスワード有効期限切れ画面」を参照	通常の認証失敗画面
パスワード期限切れ後の認証猶予回数が有効な期間 (pwdGraceAuthnLimit)	「4.5 パスワード期限切れ後の認証猶予回数が有効な期間に表示される画面」を参照	通常の認証失敗画面

【ポリシー (関連する OpenLDAP の設定ディレクティブ)】	【正しいパスワード入力時に表示される画面】	【不正なパスワード入力時に表示される画面】
次回ログイン時にパスワード変更必須 (pwdMustChange)	「4.6 次回ログイン時にパスワード変更が必須の場合の画面」を参照	通常の認証失敗画面

同時に複数のポリシーに抵触している場合

【ポリシー (関連する OpenLDAP の設定ディレクティブ)】	【正しいパスワード入力時に表示される画面】	【不正なパスワード入力時に表示される画面】
アカウントロックアウト かつ パスワード有効期限切れ	「4.2 アカウントロックアウト画面」を参照	「4.2 アカウントロックアウト画面」を参照
アカウントロックアウト かつ 次回ログイン時のパスワード変更必要	「4.2 アカウントロックアウト画面」を参照	「4.2 アカウントロックアウト画面」を参照
アカウントロックアウト かつ パスワード有効期限切れ かつ パスワード期限切れ後の認証猶予回数が有効な期間	「4.2 アカウントロックアウト画面」を参照	「4.2 アカウントロックアウト画面」を参照
パスワード有効期限切れ かつ 次回ログイン時のパスワード変更必要	「4.6 次回ログイン時にパスワード変更が必須の場合の画面」を参照	通常の認証失敗画面

【ポリシー (関連する OpenLDAP の設定ディレクティブ)】	【正しいパスワード 入力時に表示される画面】	【不正なパスワード 入力時に表示される画面】
パスワード有効期限切れ かつ アカウントロックアウト かつ 次回ログイン時のパスワード変更必要	「4.2 アカウントロックアウト画面」を参照	「4.2 アカウントロックアウト画面」を参照

4.2 アカウントロックアウト画面

図 1　アカウントロックアウト画面

4.3 パスワード有効期限切れ画面

図 2　パスワード有効期限切れ画面

4.4 パスワード有効期限切れ前の警告画面

図 3　パスワード有効期限切れ前の警告画面

4.5 パスワード期限切れ後の認証猶予回数が有効な期間に表示される画面

図 4　パスワード期限切れ後の認証猶予回数が有効な期間に表示される画面

4.6 次回ログイン時にパスワード変更が必須の場合の画面

図 5　次回ログイン時にパスワード変更が必須の場合の画面

5 表示されるエラーメッセージの変更

本章では、パスワードポリシーに抵触した場合に表示される画面のエラーメッセージを変更する方法について説明します。

XML ファイルの変更をシステムに反映するためには、OpenAM の再起動を行ってください。

5.1 アカウントロックアウト画面

元の画面は「4.2 アカウントロックアウト画面」をご参照ください。

【項目】	【内容】
メッセージ	アカウントがロックされています。ロックを解除したい場合は、サービスデスクへお問い合わせください。
メッセージ定義ファイル	{OPENAM_CONTEXT_DIR}/config/auth/default_ja /OpenLDAP.xml
ファイル内の該当部分	header=" アカウントがロックされています。ロックを解除したい場合は、サービスデスクへお問い合わせください。"
メッセージ変更方法	メッセージを直接記述します。リンクも表示可能です (HTML タグはエスケープする必要があります。「5.3 認証モジュール設定ファイルへの HTML タグの記述」をご参照ください)。

5.2 パスワード有効期限切れ画面

元の画面は「4.3 パスワード有効期限切れ画面」をご参照ください。

【項目】	【内容】
メッセージ	パスワードが期限切れになりました。パスワードをリセットするには、サービスデスクにお問い合わせください。
メッセージ定義ファイル	{OPENAM_CONTEXT_DIR}/config/auth/default_ja /OpenLDAP.xml

【項目】	【内容】
ファイル内の該当部分	header=“パスワードが期限切れになりました。パスワードをリセットするには、サービスデスクにお問い合わせください。”
メッセージ変更方法	メッセージを直接記述します。リンクも表示可能です (HTML タグはエスケープする必要があります。「5.3 認証モジュール設定ファイルへの HTML タグの記述」をご参照ください)。

5.3 認証モジュール設定ファイルへの HTML タグの記述

認証モジュール設定ファイル[*1]の画面表示メッセージ記述部分には、HTML のリンクを挿入することも可能です。ただし、タグなどの HTML 特殊文字はエスケープする必要があります。

以下に、画面に表示されるメッセージにリンクを追加する例を示します。

```
header=" アカウントがロックされています。&lt;a href=&quot;http://www.example.co.jp
&quot;&gt; こちら&lt;/a&gt; からロック解除の手続きを行なってください。"
```

[*1] {OPENAM_CONTEXT_DIR}/config/auth/default_ja/OpenLDAP.xml

6 改版履歴

- 2019 年 12 月 9 日 リビジョン 1.0
  - 初版作成
- 2021 年 4 月 28 日 リビジョン 1.1
  - 設定情報ディレクトリのパスを修正
- 2022 年 7 月 14 日 リビジョン 1.2
  - 表紙の社名を OSSTech 株式会社に変更