OpenAM 14 コマンドライン 利用手順書

OSSTech **株式会社**

更新日 2023 年 5 月 8 日
リビジョン 1.6

目次

1 要旨

本文書は OpenAM に付属するコマンドラインツールの利用手順書です。以下のコマンドの利用方法について説明します。

ssoconfigurator	OpenAM の初期設定を行うコマンドラインツールです。
ssoadm	OpenAM の設定情報の変更や取得を行うコマンドラインツールです。

2 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。

OpenAM 1 号機	`openam01.example.co.jp`
OpenAM 2 号機	`openam02.example.co.jp`
ロードバランサー	`sso.example.co.jp`

2.2 OpenAM 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`
ログなどのディレクトリ	`/opt/osstech/var/lib/tomcat/data/openam/openam`
OpenAM 1 号機の URL	http://openam01.example.co.jp:8080/openam/
OpenAM 2 号機の URL	http://openam02.example.co.jp:8080/openam/
ロードバランサーの URL	https://sso.example.co.jp/openam/

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/openam` [*1]

[*1] インストールガイドの war 名の変更に従った設定であればコンテキストディレクトリは変わりません。

項目	値
設定情報ディレクトリ	`/opt/osstech/var/lib/tomcat/data/example`
ログなどのディレクトリ	`/opt/osstech/var/lib/tomcat/data/example/example`
OpenAM 1 号機の URL	http://openam01.example.co.jp:8080/example/
OpenAM 2 号機の URL	http://openam02.example.co.jp:8080/example/
ロードバランサーの URL	https://sso.example.co.jp/example/

本文書では、OpenAM コンテキスト名を{OPENAM_CONTEXT_NAME}と表記します。

3 ssoadm コマンド利用のための設定

本章では ssoadm コマンドを利用するための事前設定について説明します。設定作業はすべての OpenAM サーバーに対して行います。

3.1 パスワードファイルの準備

ssoadm コマンドを実行する際には、OpenAM 管理者アカウントのパスワードを記述したファイルを用意しておく必要があります。以下の内容を実行してファイルを作成します。ファイルの所有者とパーミッションにご注意ください。

```
# (umask 0077 && touch password.txt)
# chown root:root password.txt
# chmod 400 password.txt
# vim password.txt
パスワードを記述して保存
（パーミッションはファイルの所有者のみ読み込み可能とする必要があります）
```

パスワードファイルは ssoadm コマンド実行時に必要であり、作業が終了したら削除してください。

3.2 サイト構成の定義を追加

OpenAM でサイト構成を設定している場合、ssoadm コマンドに定義の追加が必要です。サイト構成を設定していない場合は本手順は不要です。

1. /opt/osstech/bin/ssoadm をエディタで開きます。内容はシェルスクリプトです。事前にバックアップを取得しておいてください。
2. 以下の★行の定義を追加します。変更したら保存します。

```
$JAVA_HOME/bin/java -Xms256m -Xmx512m -cp "$CLASSPATH" \
    $DEBUG \
    -D"sun.net.client.defaultConnectTimeout=3000" \
    -D"openam.naming.sitemonitor.disabled=true" \
    -D"com.iplanet.am.serverMode=false" \
    -D"com.sun.identity.sm.notification.enabled=false" \
    -D"bootstrap.dir=/opt/osstech/var/lib/tomcat/data/openam" \
    -D"com.iplanet.services.debug.directory=/opt/osstech/share/openam14/
       ssoAdminTools/debug" \
```

```
    -D"com.iplanet.services.debug.level=message" \
    -D"com.sun.identity.log.dir=/opt/osstech/share/openam14/ssoAdminTools/log" \
    -D"definitionFiles=com.sun.identity.cli.AccessManager,
       com.sun.identity.federation.cli.FederationManager" \
    -D"commandName=ssoadm" \
    -D"amconfig=AMConfig" \
    -D"java.version.current=java.vm.version" \
    -D"java.version.expected=1.4+" \
    -D"am.version.current=com.iplanet.am.version" \
    -D"am.version.expected=14.x.x" \
    -D"com.iplanet.am.sdk.package=com.iplanet.am.sdk.remote" \
    -D"com.sun.identity.idm.remote.notification.enabled=false" \
    -Djava.security.egd=file:/dev/urandom \
★   -D"com.iplanet.am.naming.map.site.to.server=[サイトの URL]=[サーバーの URL]" \
    $JAVA_OPTS \
```

- 「サイトの URL」はサイト構成の定義を行った URL で通常は LB 経由の URL です。本書では以下となります。
  - https://sso.example.co.jp/{OPENAM_CONTEXT_NAME}
- 「サーバーの URL」は自身を示す URL であり OpenAM サーバーのホスト名です。本書では以下となります。
  - http://openam01.example.co.jp:8080/{OPENAM_CONTEXT_NAME}
  - http://openam02.example.co.jp:8080/{OPENAM_CONTEXT_NAME}

例として本書の OpenAM 構成の 1 号機でコンテキスト名を openam とすると、設定する内容は以下のとおりです。

```
    -D"com.iplanet.am.naming.map.site.to.server=https://sso.example.co.jp/openam=
http://openam01.example.co.jp:8080/openam" \
```

3.3 サービス (認証連鎖名) の指定

ssoadm コマンドの一部のサブコマンドを利用する場合、最上位のレルムの「モジュールベースの認証」を有効にしておくか ssoadm コマンドで amAdmin の認証を行うサービス (認証連鎖名) の指定が必要です。ここではサービス (認証連鎖名) の指定の手順を示します。

1. /opt/osstech/bin/ssoadm をエディタで開きます。内容はシェルスクリプトです。事前にバックアップを取得しておいてください。
2. 以下の★行の定義を追加します。変更したら保存します。

以下の★の 2 行の定義を追加します。

```
    -D"com.iplanet.am.sdk.package=com.iplanet.am.sdk.remote" \
    -D"com.sun.identity.idm.remote.notification.enabled=false" \
    -Djava.security.egd=file:/dev/urandom \
    -D"com.iplanet.am.naming.map.site.to.server=https://sso.example.co.jp/openam=
http://openam01.example.co.jp:8080/openam" \
★   -D"org.forgerock.openam.ssoadm.auth.indexType=service" \
★   -D"org.forgerock.openam.ssoadm.auth.indexName=ldapService" \
    $JAVA_OPTS \
```

以下に、「モジュールベースの認証」が有効でなければ実行できないサブコマンドを列挙します。

- **add-svc-attrs**
- **set-svc-attrs**

3.4 設定情報ディレクトリの確認

ssoadm コマンドでは OpenAM の設定情報ディレクトリが指定されています。OpenAM のコンテキスト名をデフォルトの openam から変更している場合など、設定情報ディレクトリをデフォルト値から変えている場合 ssoadm コマンドの定義の変更が必要です。設定情報ディレクトリをデフォルトから変更していない場合は本手順は不要です。

1. /opt/osstech/bin/ssoadm をエディタで開きます。内容はシェルスクリプトです。事前にバックアップを取得しておいてください。
2. 以下の★行 (2 箇所) の設定情報ディレクトリを変更します。変更したら保存します。

```
CLASSPATH="/opt/osstech/var/lib/tomcat/data/openam" ★
…
$JAVA_HOME/bin/java -Xms256m -Xmx512m -cp "$CLASSPATH" \
    $DEBUG \
    -D"sun.net.client.defaultConnectTimeout=3000" \
    -D"openam.naming.sitemonitor.disabled=true" \
    -D"com.iplanet.am.serverMode=false" \
    -D"com.sun.identity.sm.notification.enabled=false" \
    -D"bootstrap.dir=/opt/osstech/var/lib/tomcat/data/openam" \ ★
```

/opt/osstech/var/lib/tomcat/data/openam を使用環境のディレクトリに変更してく

ください。

3.5 動作確認

ssoadm コマンドの実行例です。

```
# /opt/osstech/bin/ssoadm list-servers -u amadmin -f パスワードファイル

http://openam01.example.co.jp:8080/{OPENAM_CONTEXT_NAME}
http://openam01.example.co.jp:8080/{OPENAM_CONTEXT_NAME}
```

上記のように、OpenAM サーバーの一覧が取得できれば正常に動作しています。正常な結果が得られない場合は「トラブルシューティング」を参照して問題を解決してください。

4 ssoadm コマンドの基本仕様

本章では ssoadm コマンドの基本的な仕様について説明します。

4.1 基本書式

ssoadm コマンド[*2]は OpenAM の各設定をサブコマンド、サービス名、属性値を指定して設定します。

```
# ssoadm サブコマンド -u amadmin -f パスワードファイル -e usr -s サービス名 -a 属性値
```

4.2 オプション

オプションはすべてのサブコマンドで指定可能なグローバルオプションと、特定のサブコマンドのみで指定可能なオプションに分類されます。

以降の章で各サブコマンドについて詳細に解説しますが、オプションの説明についてはサブコマンドに特有のオプションのみを解説します。グローバルオプションや、複数のサブコマンドで共通するオプションに関する説明は本節をご参照ください。

4.2.1 グローバルオプション

グローバルオプションについて説明します。

- -d, --debug
  - デバッグモードで動作します。ssoadm のログに記録される内容を標準出力や標準エラー出力にも出力します。
- -?, --help
  - コマンドの利用方法を表示します。
- -l, --locale
  - コマンドの実行結果メッセージのロケール ([ja_JP.UTF-8]、「C」など) を指定します。
- -v, --verbose
  - 詳細メッセージを表示します。
- -V, --version
  - ssoadm コマンドのバージョンを表示します。

[*2] コマンドの絶対パスは/opt/osstech/bin/ssoadm です。

4.2.2 サブコマンド用オプション

サブコマンドで指定可能なオプションのうち、多くのサブコマンドで指定可能な共通のオプションについて説明します。

- -u, --adminid OpenAM 管理ユーザ名
  - OpenAM の管理ユーザ名を指定します。管理者ユーザーはデフォルトは amadmin です。
- -f, --password-file OpenAM 管理者パスワード記述ファイル
  - OpenAM 管理者のパスワードを記述したファイルを指定します。パスワード記述ファイルはファイルの所有者のみが読み込み可能となるようなパーミッションを設定する必要があります。
- -e, --realm レルム名
  - 設定変更対象のレルムを指定します。
- -s, --servicename サービス名
  - サービス名を指定します。各設定項目はいくつかのサービス (設定単位のまとまり) に分類されており、ssoadm コマンドから設定を変更する場合は、該当の設定項目が含まれるサービスを指定する必要があります。
- -a, --attributevalues 設定属性値
  - 設定する属性値を指定します。「属性名=属性値」の形式で指定します。例を以下に示します。
    - `sun-idrepo-ldapv3-config-ldap-server=ldap.example.co.jp:389`
  - -a オプションを指定可能なコマンドでは、多くの場合 -D オプションも利用可能です。ただし、同時に指定することはできません。-a オプションや -D オプションが指定可能なコマンドでは、必ずどちらかのオプションを指定する必要があります。
- -p, --append
  - 複数の設定値を持つ属性において、新たに属性値を追加する場合に指定します。このオプションを指定しない場合、すでに設定されている値は削除され、新しく指定した値のみが保存されます。
  - このオプションは -a(--attributevalues) オプションを利用する場合のみ指定します。 -D オプション利用時には、このオプションは指定しません。
- -D,--datafile ファイル名
  - 設定属性値が記載されたファイル名を指定します。
  - ファイルの例を以下に示します。ユーザデータストア設定の例です。

```
sun-idrepo-ldapv3-config-ldap-server=ldap.example.co.jp:389
sun-idrepo-ldapv3-config-authid=cn=admin,dc=example,dc=jp
sun-idrepo-ldapv3-config-authpw=admin
sun-idrepo-ldapv3-config-organization_name=dc=example,dc=jp
sun-idrepo-ldapv3-config-ssl-enabled=true
sun-idrepo-ldapv3-config-referrals=false
sun-idrepo-ldapv3-config-people-container-name=ou
sun-idrepo-ldapv3-config-people-container-value=Users
sun-idrepo-ldapv3-config-group-container-name=ou
sun-idrepo-ldapv3-config-group-container-value=groups
```

4.3 ログ

4.3.1 出力先

ssoadm コマンドのログは以下のディレクトリに出力されます。

- 一般ログ
  - /opt/osstech/share/openam14/ssoAdminTools/log
- デバッグログ
  - /opt/osstech/share/openam14/ssoAdminTools/debug

4.3.2 デバッグログのログレベルの変更

デバッグログのログレベルの変更方法を記載します。 ssoadm コマンドのログレベルは OpenAM の設定と連動しています。 OpenAM のログレベルを変更することで ssoadm コマンドのログレベルを変更することが出来ます。

- 「デプロイメント」-「サーバー」-「(サーバー名)」-「一般」-「デバッグ」-「デバッグレベル」

もしくは、ssoadm ファイルに定義を追加することで、OpenAM のログレベルを変更せずに ssoadm コマンドのログレベルを設定することも可能です。

1. /opt/osstech/bin/ssoadm をエディタで開きます。内容はシェルスクリプトです。事前にバックアップを取得しておいてください。
2. 以下の部分を追加・変更します。変更したら保存します。

```
$JAVA_HOME/bin/java -Xms256m -Xmx512m -cp "$CLASSPATH" \
    $DEBUG \
    -D"sun.net.client.defaultConnectTimeout=3000" \
    -D"openam.naming.sitemonitor.disabled=true" \
    -D"com.iplanet.am.serverMode=false" \
    -D"com.sun.identity.sm.notification.enabled=false" \
    -D"bootstrap.dir=/opt/osstech/var/lib/tomcat/data/openam" \
    -D"com.iplanet.services.debug.directory=/opt/osstech/share/openam14/
       ssoAdminTools/debug" \
    -D"com.sun.identity.log.dir=/opt/osstech/share/openam14/ssoAdminTools/log" \
    -D"definitionFiles=com.sun.identity.cli.AccessManager,
       com.sun.identity.federation.cli.FederationManager" \
    -D"commandName=ssoadm" \
    -D"amconfig=AMConfig" \
    -D"java.version.current=java.vm.version" \
    -D"java.version.expected=1.4+" \
    -D"am.version.current=com.iplanet.am.version" \
    -D"am.version.expected=14.x.x" \
    -D"com.iplanet.am.sdk.package=com.iplanet.am.sdk.remote" \
    -D"com.sun.identity.idm.remote.notification.enabled=false" \
    -Djava.security.egd=file:/dev/urandom \
    -D"com.iplanet.services.debug.level=message" \  # 追加・変更
    com.sun.identity.cli.CommandManager "$@"
```

「com.iplanet.services.debug.level」パラメータに指定できるのは以下の通りです。

ログレベル	出力内容
error	エラーメッセージだけがログに書き込まれます。
warning	エラーメッセージ、警告メッセージがログに書き込まれます。
message	エラーメッセージ、警告メッセージ、および情報メッセージがログに書き込まれます。 最も情報量の多いログとなります。

4.4 戻り値

ssoadm コマンドは以下の値を返します。

値	説明
0	正常終了
0 以外	異常終了

4.5 サービス名と属性名について

OpenAM の各種設定値は、OpenAM 内蔵の LDAP サーバーである OpenDJ にて管理されています。 ssoadm コマンドで指定するサービス名や属性は、OpenDJ のエントリ名、属性名、属性値に対応しています。

ssoadm コマンドで指定可能なサービス名や属性名は膨大な数になりますが、OpenAM の公式ドキュメントではそれらの情報がまとめられていません。

本文書では、指定する頻度が高いサービス名や属性名について本文内で解説しています。本文書で解説していない設定属性値については、OpenAM 管理コンソールの設定値と OpenDJ に保存されている情報を見比べて、設定対象のサービス名や属性名を確認する必要があります。

ここでは、OpenDJ の構成について概要を説明します。ssoadm コマンドで指定するサービス名や属性を調査する際の参考としてください。

4.5.1 OpenDJ の DIT 構成

OpenDJ の DIT は以下のような構成となっています。

```
dc=openam,dc=osstech,dc=co,dc=jp
    |
    └──── ou=services
            ├──── 各種サービスの設定
            ├──── レルム設定エントリ（レルム 1）
            └──── レルム設定エントリ（レルム 2）
```

各エントリについて説明します。

- dc=openam,dc=osstech,dc=co,dc=jp
  - ルートエントリです。
- ou=services,dc=openam,dc=osstech,dc=co,dc=jp
  - 各種サービスの設定が、このエントリ以下の階層に保存されています。
    - 例:

ou=iPlanetAMAuthService,ou=services,o=usr,ou=services,dc=openam,
dc=osstech,dc=co,dc=jp

- ou=レルム名,ou=services,dc=openam,dc=osstech,dc=co,dc=jp
  - レルムの設定が保存されています。
  - 「ou=servies,ou=レルム名,ou=services,dc=openam,dc=osstech,dc=co,dc=jp」以下に各種サービスの設定が保存されています。

以下のいくつかのエントリの例を示します。

- ou=iPlanetAMAuthService,ou=services,o=レルム名,ou=services,dc=openam,
  dc=osstech,dc=co,dc=jp
  - 「7.3 「認証」タブ画面の設定」で指定する属性が保存されています。
- ou=データストア名,ou=default,ou=OrganizationConfig,ou=1.0,
  ou=sunIdentityRepositoryService,ou=services,o=レルム名,ou=services,
  dc=openam,dc=osstech,dc=co,dc=jp
  - ユーザーデータストア設定が保存されています。
- ou=エンティティー ID,ou=default,ou=OrganizationConfig,ou=1.0,
  ou=sunFMSAML2MetadataService,ou=services,o=レルム名,ou=services,
  dc=openam,dc=osstech,dc=co,dc=jp
  - エンティティー (SAMLIdP、SAML SP など) の設定が保存されています。

ほとんどの設定値は各エントリの「sunKeyValue」という属性に保存されています。sunKeyValue には 2 通りの形式で設定値が保存されます。

1. 「設定属性値=属性値」という形式
   - 例えば、sunKeyValue 属性値に「sun-idrepo-ldapv3-config-ldapserver=localhost:389」のような形式で保存されます。
2. XML 形式
   - sunKeyValue 属性値に XML 形式の値が保存されます。
   - 「メタデータサンプル」で解説する SAML エンティティーのメタデーターなどがこの形式に該当します。

一部の属性は「sunKeyValue」以外の属性にも保存されます。

4.5.2 OpenDJ への LDAP 接続方法

OpenDJ に LDAP 接続する方法について説明します。接続情報は以下の通りです。

項目	説明
ホスト	OpenAM サーバー稼働ホストのホスト名/IP アドレス
ポート	50389 (50389 はデフォルトのポート番号です。OpenDJ のポート番号を変更している場合はそのポート番号を指定してください)
接続に利用する DN	cn=Directory Manager
パスワード	OpenAM 管理者 (amadmin) のパスワード

ldapsearch コマンドを利用して LDAP 検索操作を実行する例を示します。

```
$ ldapsearch -x -W -D "cn=Directory Manager" -H "ldap://localhost:50389" -LLL \
-b dc=openam,dc=osstech,dc=co,dc=jp
```

5 OpenAM の初期設定

本章では、 ssoconfigurator コマンドを利用して OpenAM の初期設定を行う方法を説明します。ssoconfigurator コマンドを利用するには osstech-openam14-configtools-14.x.x-xx.el7.noarch.rpm をインストールする必要があります。インストールしていない場合には、以下のコマンドでインストールしてください。

```
# rpm -ivh {OPENAM_RPMS}/x86_64/\
osstech-openam14-configtools-14.x.x-xx.el7.noarch.rpm
```

{OPENAM_RPMS} は OpenAM を展開したディレクトリです。OpenAM14 インストールガイドの通りであれば/srv/osstech-work/software/RPMS です。

5.1 設定ファイルの作成

ssoconfigurator コマンドは OpenAM の初期設定内容をファイルから読み込みます。まずは設定ファイルのテンプレートから設定ファイルを作成します。

```
# cp /opt/osstech/share/openam14/ssoConfigTools/conf/server1.conf.template \
oam1.conf
```

以下のように内容を編集します。「#」から始まる行はコメントです。

```
# OpenAM server configuration
SERVER_URL=http://openam01.example.co.jp:8080
DEPLOYMENT_URI=/openam
BASE_DIR=/opt/osstech/var/lib/tomcat/data/openam
locale=en_US
PLATFORM_LOCALE=en_US
AM_ENC_KEY=
ADMIN_PWD=password
AMLDAPUSERPASSWD=agent-password
COOKIE_DOMAIN=example.co.jp

# Configuration data store
DATA_STORE=embedded
DIRECTORY_SSL=SIMPLE
DIRECTORY_SERVER=localhost
DIRECTORY_PORT=50389
DIRECTORY_ADMIN_PORT=4444
```

```
DIRECTORY_JMX_PORT=1689
ROOT_SUFFIX=dc=openam,dc=osstech,dc=co,dc=jp
DS_DIRMGRDN=cn=Directory Manager
DS_DIRMGRPASSWD=password
```

各設定項目について説明します。

5.1.1 OpenAM 設定

項目	値	説明
SERVER_URL	http://openam01.example.co.jp:8080	※ 1
DEPLOYMENT_URI	/openam	※ 2
BASE_DIR	/opt/osstech/var/lib/tomcat/data/openam	※ 3
locale	en_US	ユーザーロケールです。 変更不要です。
PLATFORM_LOCALE	en_US	OpenAM に設定するロケールです。 変更しないでください。
AM_ENC_KEY		※ 4
ADMIN_PWD	password	amAdmin のパスワード
AMLDAPUSERPASSWD	agent-password	ポリシーエージェントのパスワード
COOKIE_DOMAIN	example.co.jp	Cookie ドメインです。

- ※ 1: OpenAM サーバー本体の URL です。
- ※ 2: OpenAM のコンテキスト名です。先頭に「/(スラッシュ)」が必要です。
- ※ 3: OpenAM 設定情報ディレクトリです。
- ※ 4: OpenAM のパスワード暗号化鍵です。値を設定しない場合、自動で生成された値が設定されます。冗長構成にする場合は 1 号機と 2 号機の設定ファイルにこの値を指定するか、 1 号機で自動生成された値を 2 号機の設定ファイルに指定してください。

5.1.2 設定データストア (OpenDJ) 設定

(通常は、設定値をデフォルトから変更する必要はありません)

項目	値	説明
DATA_STORE	embedded	※ 1
DIRECTORY_SSL	SIMPLE	※ 2
DIRECTORY_SERVER	localhost	※ 3
DIRECTORY_PORT	50389	※ 4
DIRECTORY_ADMIN_PORT	4444	※ 5
DIRECTORY_JMX_PORT	1689	※ 6
ROOT_SUFFIX	dc=openam,dc=osstech,dc=co,dc=jp	※ 7
DS_DIRMGRDN	cn=Directory Manager	※ 8
DS_DIRMGRPASSWD	password	※ 9

- ※ 1: 設定データストアの種類です。「embedded」は OpenAM 内蔵の OpenDJ を意味します。 通常は「embedded」を指定します。
- ※ 2: 設定データストアにおける SSL の使用有無を指定します。デフォルト値は「SIMPLE」です。
  - 値:
    - SSL : SSL を有効化
    - SIMPLE : SSL を無効化 (デフォルト)
- ※ 3: 設定データストアが稼働しているホストを指定します。デフォルト値は「localhost」です。
- ※ 4: 設定データストアのポート番号です。デフォルト値は「50389」です。
- ※ 5: 設定データストアの管理用ポート番号です。デフォルト値は「4444」です。
- ※ 6: 設定データストアの JMX 用ポート番号です。デフォルト値は「1689」です。
- ※ 7: 設定データストアのルートサフィックスです。 OSSTech 版 OpenAM のデフォルト値は「dc=openam,dc=osstech,dc=co,dc=jp」です。
- ※ 8: 設定データストアの管理者の DN です。デフォルト値は「cn=Directory Manager」です。
- ※ 9: 設定データストアの管理者のパスワードを指定します。 OpenAM の初期設定を GUI(Web インタフェース) から実行した場合、このパスワードは amadmin と同じになりますが、コマンドで初期設定する場合は異なるパスワードを指定可能です。

5.1.3 サイト構成設定項目

項目	値	説明
LB_SITE_NAME	site1	※ 1
LB_PRIMARY_URL	https://openam.sso.example.co.jp/openam	※ 2

- ※ 1: サイト構成設定の親サイト名を指定します。
- ※ 2: サイトの URL を指定します。1 台目にのみ必要です。

5.2 コマンドの実行

設定ファイルを作成したら、ssoconfigurator コマンドを実行して初期設定を行います。 設定ファイルのファイル名を openam-init.conf と仮定します。OpenAM(Tomcat) が起動した状態でコマンドを実行します。

```
# /opt/osstech/bin/ssoconfigurator -f openam-init.conf

COMMON DEVELOPMENT AND DISTRIBUTION LICENSE (CDDL) Version 1.0

1. Definitions.

1.1. Contributor means each individual or entity that creates or contributes to
the creation of Modifications.
...
(省略)
...
Do you accept the license?
```

ライセンスが表示され、同意するかどうかの入力を求められます。同意する場合には「y」を入力し、Enter キーを押してください。

```
Checking license acceptance...License terms accepted.
Checking configuration directory
/opt/osstech/var/lib/tomcat/data/openam....Success.
Installing OpenAM configuration store...Success
RSA/ECB/OAEPWithSHA1AndMGF1Padding.
Extracting OpenDJ, please wait...Complete
...
(省略)
...
Configuration complete!
```

最後に「Configuration complete! 」と表示されれば正常に終了しています。初期設定完了後に OpenAM を再起動してください。 以上で初期設定は完了です。

5.3 冗長化構成

OpenAM を冗長化する場合、2 号機以降の設定ファイルには冗長構成用の設定が必要になります。まずは、テンプレートから設定ファイルを作成します。

```
# cp /opt/osstech/share/openam14/ssoConfigTools/conf/server2.conf.template \
oam2.conf
```

以下のように内容を編集します。AM_ENC_KEY を 1 号機のパスワード暗号化鍵と合わせる必要があります。[*3]

```
# OpenAM server configuration
SERVER_URL=http://openam02.example.co.jp:8080
DEPLOYMENT_URI=/openam
BASE_DIR=/opt/osstech/var/lib/tomcat/data/openam
locale=en_US
PLATFORM_LOCALE=en_US
AM_ENC_KEY={1 号機のパスワード暗号化鍵}
ADMIN_PWD=password
AMLDAPUSERPASSWD=agent-password
COOKIE_DOMAIN=example.co.jp

# Configuration data store
DATA_STORE=embedded
DIRECTORY_SSL=SIMPLE
DIRECTORY_SERVER=localhost
DIRECTORY_PORT=50389
DIRECTORY_ADMIN_PORT=4444
DIRECTORY_JMX_PORT=1689
ROOT_SUFFIX=dc=openam,dc=osstech,dc=co,dc=jp
DS_DIRMGRDN=cn=Directory Manager
DS_DIRMGRPASSWD=password
```

OpenAM が冗長化構成の場合、以下の内容も編集します。

[*3] 管理コンソールの [デプロイメント]-[サーバー]-[サーバー名を選択]-[セキュリティ]-[暗号化]-[パスワード暗号化鍵] で確認可能です。

```
# http://server2.example.com:8080/openam
DS_EMB_REPL_FLAG=embReplFlag
DS_EMB_REPL_REPLPORT1=58989
DS_EMB_REPL_HOST2=openam01.example.co.jp
DS_EMB_REPL_ADMINPORT2=4444
DS_EMB_REPL_REPLPORT2=50889
existingserverid=http://openam01.example.co.jp:8080/openam
```

冗長構成用の設定項目について説明します。

- DS_EMB_REPL_FLAG
  - 設定値例: embReplFlag
  - 設定データストアを冗長化構成にするためのパラメーターです。「embReplFlag」を指定します。
- DS_EMB_REPL_REPLPORT1
  - 設定値例: 58989
  - 自サーバーの設定データストアのレプリケーションポート番号です。デフォルト値は「58989」です。
- DS_EMB_REPL_HOST2
  - 設定値例: openam01.example.co.jp
  - 1 台目の OpenAM のホスト名です。
- DS_EMB_REPL_ADMINPORT2
  - 設定値例: 4444
  - 1 台目の OpenAM の設定データストアの管理用ポート番号です。1 台目 OpenAM の「DIRECTORY_ADMIN_PORT」のポート番号を指定します。
- DS_EMB_REPL_REPLPORT2
  - 設定値例: 50889
  - 1 台目の OpenAM の設定データストアのレプリケーションポート番号です。デフォルト値は「50889」です。
- existingserverid
  - 設定値例: http://openam01.example.co.jp:8080/openam
  - 1 台目の OpenAM の URL です。1 台目の OpenAM のフルパスを指定します。

6 OpenAM 全体の設定

本章では、ssoadm コマンドで OpenAM 全体の動作設定を管理する方法を説明します。

6.1 サーバーの設定

6.1.1 サーバーの設定変更

OpenAM 管理コンソールの以下の画面の設定を変更します。

- 「デプロイメント」タブ→「サーバー」
  - 「サーバー」欄の各サーバー

書式は以下になります。

```
ssoadm update-server-cfg
    -u|--adminid OpenAM 管理者ユーザー名
    -f|--password-file OpenAM 管理者パスワード記述ファイル
    -s|--servername サーバー名
   [-a|--attributevalues 設定属性値]
   [-D|--datafile 設定属性値記述ファイル]
```

サブコマンド共通のオプションの説明は「オプション」をご参照ください。ここでは、このサブコマンドに特有のオプションについて説明します。

- -s, --servername サーバー名
  - 設定を変更するサーバー名を指定します。
    - 例「http://openam01.example.co.jp:8080/openam」
  - 「デフォルトのサーバー設定値」を変更する場合は「default」を指定します。[*4]
  - 属性値については「属性」をご参照ください。

実行例は以下になります。

```
# /opt/osstech/bin/ssoadm update-server-cfg -u amadmin -f password.txt \
-s default -a "com.iplanet.am.cookie.secure=true"

default の設定が更新されました。
```

[*4] 冗長化構成で全ての号機に反映させるため、原則として default を指定します。

6.1.2 属性

設定項目の属性について説明します。

設定値は OpenDJ の以下のエントリに保存されます。

- 「デフォルトのサーバー設定値」
  - ou=server-default,ou=com-sun-identityservers,ou=default,ou=GlobalConfig,ou=1.0,ou=iPlanetAMPlatformService,ou=services,dc=openam,dc=osstech,dc=co,dc=jp
- 各サーバーの設定値
  - ou=http://openam01.example.co.jp:8080/openam,ou=com-sun-identity-servers,ou=default,ou=GlobalConfig,ou=1.0,ou=iPlanetAMPlatformService,ou=services,dc=openam,dc=osstech,dc=co,dc=jp
  - ou=http://openam02.example.co.jp:8080/openam,ou=com-sun-identity-servers,ou=default,ou=GlobalConfig,ou=1.0,ou=iPlanetAMPlatformService,ou=services,dc=openam,dc=osstech,dc=co,dc=jp

属性の例を下表に示します。

属性値	説明
com.iplanet.am.cookie.name	※ 1
com.iplanet.am.cookie.secure	※ 2
com.iplanet.am.cookie.encode	※ 3
com.sun.identity.cookie.httponly	※ 4
com.iplanet.am.session.maxSessions	※ 5
com.sun.identity.idm.cache.entry.expire.enabled	※ 6
com.sun.identity.idm.cache.entry.default.expire.time	ユーザーデーターストア属性のキャッシュ時間 (分)
com.sun.identity.idm.cache.entry.user.expire.time	ユーザーデーターストア属性のキャッシュ時間 (分)
com.iplanet.services.stats.state=off	※ 7

- ※ 1: 「セキュリティ」 → 「Cookie」 → 「Cookie 名」
  - 例: oamSession
- ※ 2: 「セキュリティ」 → 「Cookie」 → 「セキュリティー保護された Cookie」
  - 値
    - true (チェックボックスオン)

        * false (チェックボックスオフ)
- ※ 3: 「セキュリティ」 → 「Cookie」 → 「Cookie 値のエンコード」
  - 値
    * true (チェックボックスオン)
    * false (チェックボックスオフ)
- ※ 4: Cookie の HTTPOnly 属性の有効/無効を指定
  - 値
    * true (有効)
    * false (無効)
- ※ 5: 「セッション」 → 「セッションの制限」 → 「最大セッション数」
  - 例: 100000
- ※ 6: ユーザーデーターストア属性のキャッシュの有効/無効を指定
  - 値
    * true (キャッシュ有効)
    * false (キャッシュ無効)
  - ※ false にしても、ユーザーデーターストアで更新した属性が即時に OpenAM に反映されるわけではないため、この値を true にし、キャッシュ時間を短くするという対応をとります。
- ※ 7: 「セッション」 → 「統計情報」 →「状態」。統計情報ログの有効/無効を指定。
  - 値
    * off (無効化)
    * file (OpenAM のログファイルに出力)
    * console (Web サーバーのログとして出力)

6.2 サイト設定

OpenAM 管理コンソールの以下の画面の設定を変更します。

- 「デプロイメント」タブ → 「サイト」

6.2.1 サイトの追加

サイトを新規に追加します。書式は以下になります。

```
ssoadm create-site
    -u|--adminid OpenAM 管理者ユーザー名
```

```
    -f|--password-file OpenAM 管理者パスワード記述ファイル
    -s|--sitename サイト名
    -i|--siteurl プライマリ URL
   [-a|--secondaryurls セカンダリ URL]
```

サブコマンド共通のオプションの説明は「オプション」をご参照ください。ここでは、このサブコマンドに特有のオプションについて説明します。

- -s, --sitename サイト名
  - サイト名を指定します。
- -i, --siteurl プライマリ URL
  - サイトのプライマリ URL を指定します。
- -a, --secondaryurls セカンダリ URL
  - サイトのセカンダリ URL を指定します。

実行例は以下になります。

```
# /opt/osstech/bin/ssoadm create-site -u amadmin -f password.txt -s site01 -i \
http://sso.example.co.jp/openam

サイトが作成されました。
```

6.2.2 サイトメンバーの追加

サイトにメンバー (「割り当てられたサーバー」) を追加します。書式は以下になります。

```
ssoadm add-site-members
    -u|--adminid OpenAM 管理者ユーザー名
    -f|--password-file OpenAM 管理者パスワード記述ファイル
    -s|--sitename サイト名
    -e|--servernames サーバー (複数指定可能)
```

サブコマンド共通のオプションの説明は「オプション」をご参照ください。ここでは、このサブオプションに特有のオプションについて説明します。

- -s, --sitename サイト名
  - サイト名を指定します。
- -e, --servernames サーバー (複数指定可能)
  - サイトに追加するサーバーを指定します。
  - 例えば、「http://openam01.example.co.jp:8080/openam」などです。

  - 複数のサーバーを追加する場合は、サーバー名を半角スペースで区切って指定します。
  - http://openam01.example.co.jp:8080/openam http://openam02.example.co.jp:8080/openam

実行例は以下になります。

```
# /opt/osstech/bin/ssoadm add-site-members -u amadmin -f password.txt -s site01 \
-e http://openam01.example.co.jp:8080/openam \
http://openam02.example.co.jp:8080/openam

サーバーがサイトに追加されました。
```

6.3 Cookie ドメイン設定

OpenAM 管理コンソールの以下の画面の設定を変更します。

- 「設定」タブ →「グローバルサービス」 →「システム」タブ →「プラットフォーム」 →「Cookie ドメイン」

6.3.1 Cookie ドメインの追加

Cookie ドメインを追加します。書式は以下になります。

```
ssoadm add-attr-defs
    -u|--adminid OpenAM 管理者ユーザー名
    -f|--password-file OpenAM 管理者パスワード記述ファイル
    -s|--servicename サービス名
    -t|--schematype スキーマタイプ
   [-a|--attributevalues 設定属性値]
   [-D|--datafile 設定属性値記述ファイル]
```

サブコマンド共通のオプションの説明は「オプション」をご参照ください。ここでは、このサブオプションに特有のオプションについて説明します。

- -s, --servicename サービス名
  - サービス名を指定します。
- -t, --schematype スキーマタイプ
  - スキーマタイプを指定します。
- サービス名、スキーマタイプ、設定属性値については「サービス名、スキーマタイプ、属性」をご参照ください。

実行例は以下になります。

```
# /opt/osstech/bin/ssoadm add-attr-defs -u amadmin -f password.txt -t Global \
-s iPlanetAMPlatformService \
-a "iplanet-am-platform-cookie-domains=sso.example.co.jp"

スキーマのデフォルト属性値が追加されました。
```

6.3.2 Cookie ドメインの変更

Cookie ドメインを変更します。既存の設定値は上書きされます。書式は以下になります。

```
ssoadm set-attr-defs
    -u|--adminid OpenAM 管理者ユーザー名
    -f|--password-file OpenAM 管理者パスワード記述ファイル
    -s|--servicename サービス名
    -t|--schematype スキーマタイプ
   [-a|--attributevalues 設定属性値]
   [-D|--datafile 設定属性値記述ファイル]
```

オプションの説明は「Cookie ドメインの追加」をご参照ください。実行例は以下になります。

```
# /opt/osstech/bin/ssoadm set-attr-defs -u amadmin -f password.txt -t Global \
-s iPlanetAMPlatformService \
-a "iplanet-am-platform-cookie-domains=sso.example.co.jp"

スキーマのデフォルト属性値が設定されました。
```

6.3.3 Cookie ドメインの削除

Cookie ドメインを変更します。すべての値が削除されます。書式は以下のとおりです。

```
ssoadm remove-attr-defs
    -u|--adminid OpenAM 管理者ユーザー名
    -f|--password-file OpenAM 管理者パスワード記述ファイル
    -s|--servicename サービス名
    -t|--schematype スキーマタイプ
    -a|--attributenames 属性名
```

オプションの説明は「Cookie ドメインの追加」をご参照ください。ここでは、このサブコ

マンドに特有のオプションについて説明します。

- -a, --attributenames 属性名
  - 削除する属性の名前を指定します。

実行例は以下になります。

```
# /opt/osstech/bin/ssoadm remove-attr-defs -u amadmin -f password.txt -t Global \
-s iPlanetAMPlatformService -a "iplanet-am-platform-cookie-domains"

スキーマのデフォルト属性値が消去されました。
```

6.3.4 サービス名、スキーマタイプ、属性

サービス名、スキーマタイプ、属性について説明します。設定値は OpenDJ の以下のエントリに保存されます。

- ou=1.0,ou=iPlanetAMPlatformService,ou=services,dc=openam
  - 「sunServiceSchema」属性の値に XML として保存されます。LDIF 出力すると、属性値が base64 エンコードされて出力されます。

サービス名、スキーマタイプ、属性は以下のとおりです。

サービス名	iPlanetAMPlatformService
スキーマタイプ	Global
属性	iplanet-am-platform-cookie-domains 値の例: iplanet-am-platform-cookie-domains=sso.example.co.jp

6.4 セッション設定

OpenAM 管理コンソールの以下の画面の設定を変更します。

- 「設定」タブ → 「グローバルサービス」 → 「セッション」

設定の変更は ssoadm コマンドの「set-attr-defs」サブコマンドで行います。コマンドの利用方法については「Cookie ドメインの変更」をご参照ください。

サービス名、スキーマタイプ、設定属性値については後述します。実行例は以下になります。

```
# /opt/osstech/bin/ssoadm set-attr-defs -u amadmin -f password.txt -t Global \
-s iPlanetAMSessionService -a "iplanet-am-session-constraint-handler=org\
.forgerock.openam.session.service.DestroyNextExpiringAction"

スキーマのデフォルト属性値が設定されました。
```

サービス名、スキーマタイプ、属性について説明します。 設定値は OpenDJ の以下のエントリに保存されます。

- ou=1.0,ou=iPlanetAMSessionService,ou=services,dc=openam,dc=osstech,dc=co,dc=jp
  - 「sunServiceSchema」属性の値に XML として保存されます。LDIF 出力すると、属性値が base64 エンコードされて出力されます。

サービス名は「iPlanetAMSessionService」を指定します。スキーマタイプ、属性の例を以下に示します。

- スキーマタイプ: Global (画面の「グローバル属性」)
  - 設定項目: 割り当て制限を有効
    - 属性名: iplanet-am-session-enable-sessionconstraint
    - 値: ON (オン) / OFF (オフ)
  - 設定項目: セッション制限がいっぱいになった場合に生じる動作
    - 属性名: iplanet-am-session-constraint-handler
    - 値: 後述
- スキーマタイプ: Dynamic (画面の「動的属性」)
  - 設定項目: 最大セッション時間
    - 属性名: iplanet-am-session-max-session-time
    - 値: 360(分)
  - 設定項目: 最大アイドル時間
    - 属性名: iplanet-am-session-max-idle-time
    - 値: 360(分)
  - 設定項目: アクティブなユーザーセッション
    - 属性名: iplanet-am-session-quota-limit
    - 値: 2

「セッション制限がいっぱいになった場合に生じる動作 (iplanet-am-session-constraint-handler)」に指定可能な値を以下に示します。

- 設定: DENY_ACCESS(新しいセッションの作成要求が拒否される)
  - 値: org.forgerock.openam.session.service.DenyAccessAction
- 設定: DESTROY_NEXT_EXPIRING(次の有効期限切れセッションが破棄される)
  - 値: org.forgerock.openam.session.service.DestroyNextExpiringAction
- 設定: DESTROY_OLDEST_SESSION(最も古いセッションが破棄される)
  - 値: org.forgerock.openam.session.service.DestroyOldestAction
- 設定: DESTROY_OLD_SESSIONS(以前のすべてのセッションが破棄される)
  - 値: org.forgerock.openam.session.service.DestroyAllAction

7 レルムの設定

本章では、ssoadm コマンドでレルムの設定を管理する方法を説明します。

7.1 レルムの管理

レルムを作成/削除する方法を説明します。

7.1.1 レルムの作成

レルムを新規に作成します。書式は以下のとおりです。

```
ssoadm create-realm
    -u|--adminid OpenAM 管理者ユーザー名
    -f|--password-file OpenAM 管理者パスワード記述ファイル
    -e|--realm レルム名
```

オプションの説明は「オプション」をご参照ください。実行例は以下になります。

```
# /opt/osstech/bin/ssoadm create-realm -u amadmin -f password.txt -e usr

レルムが作成されました。
```

7.1.2 レルムの一覧取得

レルムの一覧を取得します。書式は以下になります。

```
ssoadm list-realms
    -u|--adminid OpenAM 管理者ユーザー名
    -f|--password-file OpenAM 管理者パスワード記述ファイル
    -e|--realm 検索起点のレルム名
   [-r|--recursive]
```

サブコマンド共通のオプションの説明は「オプション」をご参照ください。ここでは、このサブコマンドに特有のオプションについて説明します。

- -r, --recursive
  - 再帰的にレルムを探索します。
  - すべてのレルムを検索する場合は、-e オプションに「/」(最上位のレルム) を指定します。

実行例は以下になります。

```
# /opt/osstech/bin/ssoadm list-realms -u amadmin -f password.txt -e / -r

tenant0001
tenant0002
検索が終了しました。
```

7.1.3 レルムの削除

レルムを削除します。書式は以下のとおりです。

```
ssoadm delete-realm
    -u|--adminid OpenAM 管理者ユーザー名
    -f|--password-file OpenAM 管理者パスワード記述ファイル
    -e|--realm レルム名
```

オプションの説明は「オプション」をご参照ください。実行例は以下になります。

```
# /opt/osstech/bin/ssoadm delete-realm -u amadmin -f password.txt -e usr

レルムが削除されました。
```

7.2 「プロパティ」画面の設定

レルムの以下の画面の設定方法を説明します。

- 「ダッシュボード」→「プロパティ」

コマンドで指定するサービス名と設定属性値については「サービス名と属性 (レルム)」をご参照ください。

7.2.1 設定の追加/変更

設定を追加/変更します。書式は以下になります。

```
ssoadm set-realm-attrs
    -u|--adminid OpenAM 管理者ユーザー名
    -f|--password-file OpenAM 管理者パスワード記述ファイル
    -e|--realm レルム名
    -s|--servicename サービス名
```

```
   [-a|--attributevalues 設定属性値]
   [-D|--datafile 設定属性値記述ファイル]
   [-p|--append]
```

オプションの説明は「オプション」をご参照ください。実行例は以下になります。

```
# /opt/osstech/bin/ssoadm set-realm-attrs -u amadmin -f password.txt -e usr -s \
sunIdentityRepositoryService -a "sunOrganizationAliases=sso.demo.osstech.co.jp"

属性値が設定されました。
```

7.2.2 設定の確認

設定されている属性値を確認します。書式は以下になります。

```
ssoadm get-realm
    -u|--adminid OpenAM 管理者ユーザー名
    -f|--password-file OpenAM 管理者パスワード記述ファイル
    -e|--realm レルム名
    -s|--servicename サービス名
```

オプションの説明は「オプション」をご参照ください。実行例は以下になります。

```
# /opt/osstech/bin/ssoadm get-realm -u amadmin -f password.txt -e usr \
-s sunIdentityRepositoryService

sunOrganizationStatus=Active
sunOrganizationAliases=sso.demo.osstech.co.jp
```

7.2.3 設定の削除

属性値を削除します。書式は以下のとおりです。

```
ssoadm delete-realm-attr
    -u|--adminid OpenAM 管理者ユーザー名
    -f|--password-file OpenAM 管理者パスワード記述ファイル
    -e|--realm レルム名
    -s|--servicename サービス名
    -a|--attributevalues 設定属性値
```

オプションの説明は「オプション」をご参照ください。実行例は以下になります。

```
# /opt/osstech/bin/ssoadm delete-realm-attr -u amadmin -f password.txt -e usr \
-s sunIdentityRepositoryService -a "sunOrganizationAliases"

属性が消去されました。
```

7.2.4 サービス名と属性 (レルム)

設定項目のサービス名と属性について説明します。

- 設定項目: レルムの状態
  - サービス名: sunIdentityRepositoryService
  - 属性名: sunOrganizationStatus
  - 値: Active (アクティブ) / Inactive (非アクティブ)
- 設定項目: レルムまたは DNS のエイリアス
  - サービス名: sunIdentityRepositoryService
  - 属性名: sunOrganizationAliases
  - 値: (例) sso.example.co.jp

7.3 「認証」メニューの設定

レルムの「認証」メニューの設定方法を説明します。コマンドで指定するサービス名と設定属性値については「サービス名と属性 (認証)」をご参照ください。

7.3.1 設定の追加

設定を追加します。複数の属性値を設定可能な設定項目において、既に設定されて値に新たな設定値を追加する場合にこのコマンドを実行します。書式は以下になります。

```
ssoadm add-svc-attrs
    -u|--adminid OpenAM 管理者ユーザー名
    -f|--password-file OpenAM 管理者パスワード記述ファイル
    -e|--realm レルム名
    -s|--servicename サービス名
   [-a|--attributevalues 設定属性値]
   [-D|--datafile 設定属性値記述ファイル]
```

オプションの説明は「オプション」をご参照ください。-D オプションを利用する場合、まず「設定の確認」のコマンドで属性値の一覧を取得し、必要な属性のみ含むファイルを作成すると便利です。実行例は以下になります。

```
# /opt/osstech/bin/ssoadm add-svc-attrs -u amadmin -f password.txt -e usr \
-s iPlanetAMAuthService -a "sunEnableModuleBasedAuth=false"

次の属性が追加されました。

sunEnableModuleBasedAuth=false
```

7.3.2 設定の変更

設定を変更します。書式は以下になります。

```
ssoadm set-svc-attrs
    -u|--adminid OpenAM 管理者ユーザー名
    -f|--password-file OpenAM 管理者パスワード記述ファイル
    -e|--realm レルム名
    -s|--servicename サービス名
   [-a|--attributevalues 設定属性値]
   [-D|--datafile 設定属性値記述ファイル]
```

オプションの説明は「オプション」をご参照ください。既存の設定値は上書きされます。-D オプションを利用する場合、まず「設定の確認」のコマンドで属性値の一覧を取得し、必要な属性のみ含むファイルを作成すると便利です。実行例は以下になります。

```
# /opt/osstech/bin/ssoadm set-svc-attrs -u amadmin -f password.txt -e usr \
-s iPlanetAMAuthService -a "sunEnableModuleBasedAuth=false"

usr 内の iPlanetAMAuthService が変更されました。
```

```
# /opt/osstech/bin/ssoadm set-svc-attrs -u amadmin -f password.txt -e usr \
-s iPlanetAMAuthService -D iPlanetAMAuthService.conf

usr 内の iPlanetAMAuthService が変更されました。
```

7.3.3 設定の確認

設定されている属性値を確認します。書式は以下のとおりです。

```
ssoadm get-realm-svc-attrs
    -u|--adminid OpenAM 管理者ユーザー名
    -f|--password-file OpenAM 管理者パスワード記述ファイル
```

```
    -e|--realm レルム名
    -s|--servicename サービス名
```

オプションの説明は「オプション」をご参照ください。実行例は以下になります。

```
# /opt/osstech/bin/ssoadm get-realm-svc-attrs -u amadmin -f password.txt \
-e usr -s iPlanetAMAuthService

openam-auth-stateless-sessions=false
iplanet-am-auth-login-failure-lockout-mode=false
sunLockoutDurationMultiplier=1
iplanet-am-auth-lockout-warn-user=0
sunEnableModuleBasedAuth=true
iplanet-am-auth-org-config=ldapService
openam.auth.zero.page.login.allow.null.referer=true
iplanet-am-auth-login-failure-url=https://test.example.co.jp/error.html
iplanet-am-auth-lockout-attribute-name=
sunAMIdentityType=agent
sunAMIdentityType=user
sunAMUserAttributesSessionMapping=
iplanet-am-auth-admin-auth-module=ldapService
iplanet-am-auth-default-auth-level=0
sunAMAuthInvalidAttemptsDataAttrName=
openam.auth.zero.page.login.enabled=false
iplanet-am-auth-login-failure-duration=300
openam.auth.zero.page.login.referer.whitelist=
sunStoreInvalidAttemptsInDS=true
iplanet-am-auth-lockout-duration=0
iplanet-am-auth-locale=en_US
iplanet-am-auth-lockout-email-address=
iplanet-am-auth-user-container=ou=People
iplanet-am-auth-allowed-modules=
iplanet-am-auth-default-role=
sunAMUserStatusCallbackPlugins=
iplanet-am-auth-lockout-attribute-value=
iplanet-am-auth-username-generator-class=
iplanet-am-auth-hmac-signing-shared-secret=********
iplanet-am-auth-alias-attr-name=uid
iplanet-am-auth-valid-goto-domains=
iplanet-am-auth-login-failure-count=5
iplanet-am-auth-key-alias=test
iplanet-am-auth-post-login-process-class=
iplanet-am-auth-dynamic-profile-creation=false
iplanet-am-auth-username-generator-enabled=true
```

```
iplanet-am-auth-user-naming-attr=uid
forgerockTwoFactorAuthMandatory=false
iplanet-am-auth-login-success-url=/openam/console
```

7.3.4 設定の削除

設定されている属性値を削除します。 書式は以下になります。

```
ssoadm remove-svc-attrs
    -u|--adminid OpenAM 管理者ユーザー名
    -f|--password-file OpenAM 管理者パスワード記述ファイル
    -e|--realm レルム名
    -s|--servicename サービス名
   [-a|--attributevalues 設定属性値]
   [-D|--datafile 設定属性値記述ファイル]
```

オプションの説明は「オプション」をご参照ください。実行例は以下になります。

```
# /opt/osstech/bin/ssoadm remove-svc-attrs -u amadmin -f password.txt -e usr \
-s iPlanetAMAuthService \
-a "iplanet-am-auth-login-failure-url=https://test.example.co.jp/error.html"

次の属性が消去されました。

iplanet-am-auth-login-failure-url=https://test.example.co.jp/error.html
```

7.3.5 サービス名と属性 (認証)

設定項目のサービス名と属性について説明します。

- 設定項目: 組織認証設定
  - サービス名: iPlanetAMAuthService
  - 属性名: iplanet-am-auth-org-config
  - 値: 認証連鎖の名前デフォルトは「ldapService」
- 設定項目: 管理者認証設定
  - サービス名: iPlanetAMAuthService
  - 属性名: iplanet-am-auth-admin-authmodule
  - 値: 認証連鎖の名前デフォルトは「ldapService」
- 設定項目: ログイン成功時に返すデフォルトの URL
  - サービス名: iPlanetAMAuthService

  - 属性名: iplanet-am-auth-login-success-url
  - 値: (例) http://www.example.co.jp/
- 設定項目: モジュールベースの認証
  - サービス名: iPlanetAMAuthService
  - 属性名: sunEnableModuleBasedAuth
  - 値: true(有効) / false(無効)

7.4 ユーザーデータストアの設定

レルムの「データストア」メニューの設定方法を説明します。コマンドで指定する設定属性値については「属性値」をご参照ください。

7.4.1 ユーザーデータストアの追加

レルムにユーザーデータストア設定を追加します。書式は以下になります。

```
ssoadm create-datastore
    -u|--adminid OpenAM 管理者ユーザー名
    -f|--password-file OpenAM 管理者パスワード記述ファイル
    -e|--realm レルム名
    -m|--name ユーザーデータストア名
    -t|--datatype データストアタイプ
   [-a|--attributevalues 設定属性値]
   [-D|--datafile 設定属性値記述ファイル]
```

サブコマンド共通のオプションの説明は「オプション」をご参照ください。ここでは、このサブコマンドに特有のオプションについて説明します。

- -m, --name ユーザーデータストア名
  - ユーザーデータストアの名前 (画面の表示名) を指定します。
- -t, --datatype データストアタイプ
  - ユーザーデータストアのタイプを指定します。タイプは以下のものから選択します。

データストアタイプ	説明
OpenLDAP	OpenLDAP (OSSTech 版 OpenAM のみ指定可能)
LDAPv3ForAD	Active Directory

データストアタイプ	説明
LDAPv3ForADAM	Active Directory アプリケーションモード (ADAM)
LDAPv3ForOpenDS	OpenDJ
LDAPv3ForAMDS	OpenAM スキーマを含んだ Sun Directory Server
LDAPv3ForTivoli	Tivoli Directory Server
LDAPv3	汎用 LDAPv3
Database	データベースリポジトリ (実験的機能)

- -a, --attributevalues 設定属性値
  - 設定属性値を指定します。指定されなかった属性値はデフォルト値が設定されます。
- -D, --datafile 設定属性値記述ファイル
  - 設定属性値をファイルに記述します。指定されなかった属性値はデフォルト値が設定されます。ファイルの内容が空でもコマンドを実行可能です。ファイルの例を以下に示します。

```
sun-idrepo-ldapv3-config-ldap-server=ldap.example.co.jp:389
sun-idrepo-ldapv3-config-authid=cn=admin,dc=example,dc=jp
sun-idrepo-ldapv3-config-authpw=admin
sun-idrepo-ldapv3-config-organization_name=dc=example,dc=jp
sun-idrepo-ldapv3-config-ssl-enabled=false
sun-idrepo-ldapv3-config-referrals=false
sun-idrepo-ldapv3-config-people-container-name=ou
sun-idrepo-ldapv3-config-people-container-value=Users
sun-idrepo-ldapv3-config-group-container-name=ou
sun-idrepo-ldapv3-config-group-container-value=groups
```

実行例は以下になります。

```
# /opt/osstech/bin/ssoadm create-datastore -u amadmin -f password.txt -e usr \
-m openldap -t OpenLDAP -D openldap.conf

データストアが作成されました。
```

```
# /opt/osstech/bin/ssoadm create-datastore -u amadmin -f password.txt -e usr \
-m openldap -t OpenLDAP -a "sun-idrepo-ldapv3-config-ldap-server=localhost:389"
```

```
データストアが作成されました。
```

7.4.2 ユーザーデータストアの設定変更

作成済みのユーザーデータストアの設定を変更します。書式は以下になります。

```
ssoadm update-datastore
    -u|--adminid OpenAM 管理者ユーザー名
    -f|--password-file OpenAM 管理者パスワード記述ファイル
    -e|--realm レルム名
    -m|--name ユーザーデータストア名
   [-a|--attributevalues 設定属性値]
   [-D|--datafile 設定属性値記述ファイル]
```

オプションの意味は「ユーザーデータストアの追加」をご参照ください。実行例は以下になります。

```
# /opt/osstech/bin/ssoadm update-datastore -u amadmin -f password.txt -e usr \
-m openldap -D openldap.conf

データストアプロファイルが更新されました。
```

7.4.3 ユーザーデータストアの一覧取得

作成済みのユーザーデータストアの一覧を取得します。書式は以下になります。

```
ssoadm list-datastores
    -u|--adminid OpenAM 管理者ユーザー名
    -f|--password-file OpenAM 管理者パスワード記述ファイル
    -e|--realm レルム名
```

オプションの意味は「ユーザーデータストアの追加」をご参照ください。実行例は以下になります。

```
# /opt/osstech/bin/ssoadm list-datastores -u amadmin -f password.txt -e usr

データストア:
openldap
```

7.4.4 ユーザーデータストアの設定属性値取得

作成済みのユーザーデータストアの全ての設定属性値を取得します。書式は以下のとおりです。

```
ssoadm show-datastore
    -u|--adminid OpenAM 管理者ユーザー名
    -f|--password-file OpenAM 管理者パスワード記述ファイル
    -e|--realm レルム名
    -m|--name ユーザーデータストア名
```

オプションの意味は「ユーザーデータストアの追加」をご参照ください。取得したユーザーデータストア設定属性値のうち、データベースへの接続パスワードは伏字になっています。LDAP 系のユーザーデータストアの場合、 LDPA への接続パスワードの属性名は「sunidrepo-ldapv3-config-authpw」です。

```
sun-idrepo-ldapv3-config-authpw=********
```

実行例は以下になります。

```
# /opt/osstech/bin/ssoadm show-datastore -u amadmin -f password.txt -e usr \
-m openldap

sun-idrepo-ldapv3-config-ldap-server=ldap.example.co.jp:389
sun-idrepo-ldapv3-config-authid=cn=admin,dc=example,dc=jp
sun-idrepo-ldapv3-config-organization_name=dc=example,dc=jp
sun-idrepo-ldapv3-config-ssl-enabled=false
(省略)
```

7.4.5 ユーザーデータストアの削除

ユーザーデータストア設定を削除します。書式は以下になります。

```
ssoadm delete-datastores
    -u|--adminid OpenAM 管理者ユーザー名
    -f|--password-file OpenAM 管理者パスワード記述ファイル
    -e|--realm レルム名
    -m|--name ユーザーデータストア名
```

オプションの意味は「ユーザーデータストアの追加」をご参照ください。実行例は以下になります。

```
# /opt/osstech/bin/ssoadm delete-datastores -u amadmin -f password.txt -e usr \
-m openldap

データストアが削除されました。
```

7.4.6 属性値

設定項目の属性について説明します。

ここでは、OpenLDAP ユーザーデータストアにおける属性設定値を説明します。デフォルト値から変更が必要な属性についてのみ説明します。

属性値	説明
sun-idrepo-ldapv3-config-ldap-server	LDAP サーバー (例: ldap.example.co.jp:389)
sun-idrepo-ldapv3-config-authid	LDAP バインド DN (例: cn=admin,dc=example,dc=jp)
sun-idrepo-ldapv3-config-authpw	LDAP バインドパスワード
sun-idrepo-ldapv3-config-organization_name	LDAP 組織 DN (例: dc=example,dc=jp)
sun-idrepo-ldapv3-config-ssl-enabled	LDAP SSL (例: false(無効)/true(有効))
sun-idrepo-ldapv3-config-referrals	参照先も LDAP 検索する (例: false(無効)/true(有効))
sun-idrepo-ldapv3-config-people-containername	LDAP ピープルコンテナネーミング属性 (例: ou)
sun-idrepo-ldapv3-config-people-containervalue	LDAP ピープルコンテナ値 (例: Users)
sun-idrepo-ldapv3-config-group-containername	LDAP グループコンテナネーミング属性 (例: cn)
sun-idrepo-ldapv3-config-group-containervalue	LDAP グループコンテナ値 (例: groups)
sun-idrepo-ldapv3-config-dftgroupmember	デフォルトグループメンバーのユーザー DN (例: cn=dummy,dc=example,dc=jp)
sun-idrepo-ldapv3-config-memberof	グループメンバーシップの属性名 (例: memberOf)

設定したい項目の属性値が不明な場合は、既に作成済みのユーザーデータストアの設定属性値を参照するなどをして属性値を確認します。作成済みのユーザーデータストアの設定属

性値は、「ユーザーデータストアの一覧取得」の手順で取得可能です。

7.5 認証モジュールの設定

レルムの認証モジュールの設定方法を説明します。コマンドで指定する設定属性値については「属性」をご参照ください。

7.5.1 認証モジュールの追加

レルムに認証モジュールのインスタンスを追加します。書式は以下になります。

```
ssoadm create-auth-instance
    -u|--adminid OpenAM 管理者ユーザー名
    -f|--password-file OpenAM 管理者パスワード記述ファイル
    -e|--realm レルム名
    -t|--authtype 認証モジュールのタイプ
    -m|--name 認証モジュール名
```

サブコマンド共通のオプションの説明は「オプション」をご参照ください。ここでは、このサブコマンドに特有のオプションについて説明します。

- -t, --authtype 認証モジュールのタイプ
  - ユーザーデータストアのタイプを指定します。タイプは以下のものから選択します。大文字小文字を区別します。

タイプ	対応する認証モジュール (日本語)
LDAP	LDAP
OpenLDAP	OpenLDAP
AD	Active Directory
Membership	メンバーシップ
Anonymous	匿名
Cert	証明書
HTTPBasic	HTTP 基本
NT	Windows NT
JDBC	JDBC
WindowsDesktopSSO	Windows デスクトップ SSO
DataStore	データストア

タイプ	対応する認証モジュール (日本語)
RADIUS	RADIUS
HOTP	HOTP
SecureID	SecureID
Adaptive	アダプティブリスク
OAuth	OAuth 2.0/OpenID Connect
SAML2	SAML2
OATH	OATH
MSISDN	MSISDN
PersistentCookie	永続化 Cookie
Federation	連携
SAE	SAE
AuthenticatorOATH	ForgeRock Authenticator (OATH)
DeviceIdMatch	デバイス ID (一致)
DeviceIdSave	デバイス ID (保存)
OpenIdConnect	OpenID Connect ID トークンベアラ
WebAuthnRegister	WebAuthn(登録)
WebAuthnAuthenticate	WebAuthn(認証)
AuthChainSwitch	認証連鎖分岐モジュール (親)
AuthChainSwitchChild	認証連鎖分岐モジュール (子)
SmsOTP	SMS OTP
Id	ID
LineOTP	LINE

- -m, --name 認証モジュール名
  - 認証モジュールの名前を指定します。この名前は OpenAM の管理コンソールで表示されたり、URL のクエリ文字列で指定します。

実行例は以下になります。

```
# /opt/osstech/bin/ssoadm create-auth-instance -u amadmin -f password.txt \
-e usr -t LDAP -m LDAP

認証インスタンスが作成されました。
```

7.5.2 認証モジュールの設定変更

作成済みの認証モジュールの設定属性値を変更します。書式は以下になります。

```
ssoadm update-auth-instance
    -u|--adminid OpenAM 管理者ユーザー名
    -f|--password-file OpenAM 管理者パスワード記述ファイル
    -e|--realm レルム名
    -m|--name 認証モジュール名
   [-a|--attributevalues 設定属性値]
   [-D|--datafile 設定属性値記述ファイル]
```

オプションの意味は「認証モジュールの追加」をご参照ください。実行例は以下になります。

```
# /opt/osstech/bin/ssoadm update-auth-instance -u amadmin -f password.txt \
-e usr -m openldap -D openldap.conf

認証インスタンスが更新されました。
```

作成済みの認証モジュールの一覧を取得します。書式は以下になります。

```
ssoadm list-auth-instances
    -u|--adminid OpenAM 管理者ユーザー名
    -f|--password-file OpenAM 管理者パスワード記述ファイル
    -e|--realm レルム名
```

実行例は以下になります。

```
# /opt/osstech/bin/ssoadm list-auth-instances -u amadmin -f password.txt -e usr

認証インスタンス:
LDAP, [タイプ=LDAP]
HOTP, [タイプ=HOTP]
DataStore, [タイプ=DataStore]
```

7.5.3 認証モジュールの設定属性値取得

作成済みの認証モジュールの設定属性値を取得します。書式は以下になります。

```
ssoadm get-auth-instance
    -u|--adminid OpenAM 管理者ユーザー名
    -f|--password-file OpenAM 管理者パスワード記述ファイル
    -e|--realm レルム名
    -m|--name 認証モジュール名
```

オプションの説明は「認証モジュールの追加」をご参照ください。実行例は以下になります。

```
# /opt/osstech/bin/ssoadm get-auth-instance -u amadmin -f password.txt -e usr \
-m LDAP

認証インスタンスプロファイル:
iplanet-am-auth-ldap-ssl-enabled=false
iplanet-am-auth-ldap-return-user-dn=true
iplanet-am-auth-ldap-base-dn=dc=openam,dc=osstech,dc=co,dc=jp
iplanet-am-ldap-user-creation-attr-list=
iplanet-am-auth-ldap-server=localhost:53389
iplanet-am-auth-ldap-invalid-chars=*|(|)|&|!
iplanet-am-auth-ldap-user-naming-attribute=uid
iplanet-am-auth-ldap-bind-passwd=********
iplanet-am-auth-ldap-server2=
iplanet-am-auth-ldap-auth-level=0
iplanet-am-auth-ldap-ssl-trust-all=false
iplanet-am-auth-ldap-search-scope=SUBTREE
iplanet-am-auth-ldap-search-filter=
iplanet-am-auth-ldap-user-search-attributes=uid
iplanet-am-auth-ldap-behera-password-policy-enabled=true
iplanet-am-auth-ldap-bind-dn=cn=Directory Manager
iplanet-am-auth-ldap-min-password-length=8
iplanet-am-auth-ldap-server-check=15
```

7.5.4 認証モジュールの削除

レルムに登録されている認証モジュールのインスタンスを削除します。書式は以下になります。

```
ssoadm delete-auth-instances
    -u|--adminid OpenAM 管理者ユーザー名
    -f|--password-file OpenAM 管理者パスワード記述ファイル
    -e|--realm レルム名
    -m|--names 認証モジュール名
```

- -m, --names 認証モジュール名
  - 認証モジュールの名前を指定します。
  - スペースで区切ることで、複数の認証モジュールを指定することも可能です。指定した順番に削除されます。指定された認証モジュールが存在しない場合は、その時点でエラー終了します。

```
-m LDAP OpenLDAP
```

その他のオプションの意味は「認証モジュールの追加」をご参照ください。

実行の際はまず、list-auth-instances サブコマンドを実行して、登録されている認証モジュールインスタンスの名前を確認します。

```
# /opt/osstech/bin/ssoadm list-auth-instances -u amadmin -f password.txt -e usr

認証インスタンス:
LDAP, [タイプ=LDAP]
HOTP, [タイプ=HOTP]
DataStore, [タイプ=DataStore]
```

delete-auth-instances サブコマンドを利用して、認証モジュールインスタンスを削除します。

```
# /opt/osstech/bin/ssoadm delete-auth-instances -u amadmin -f password.txt \
-e usr -m LDAP

認証インスタンスが削除されました。
```

7.5.5 属性

設定項目の属性について説明します。ここでは、LDAP 認証モジュールにおける一部の属性値について説明します。設定したい項目の属性値が不明な場合は、既に作成済みの認証モジュールの設定属性値を参照するなどして属性値を確認します。作成済みの認証モジュールの設定属性値は、「認証モジュールの設定属性値取得」の手順で取得可能です。

属性値	説明
iplanet-am-auth-ldap-server	プライマリ LDAP サーバー (例: ldap.example.co.jp:389)

属性値	説明
iplanet-am-auth-ldap-bind-dn	バインドユーザー DN (例: cn=admin,dc=example,dc=jp)
iplanet-am-auth-ldap-bind-passwd	バインドユーザーパスワード
iplanet-am-auth-ldap-base-dn	ユーザー検索の開始 DN
iplanet-am-auth-ldap-behera-password-policy-enabled	LDAP Behera パスワードポリシーサポート

7.6 認証連鎖の設定

レルムの認証連鎖の設定する方法を説明します。

7.6.1 認証連鎖の追加

レルムに認証連鎖を追加します。書式は以下になります。

```
ssoadm create-auth-cfg
    -u|--adminid OpenAM 管理者ユーザー名
    -f|--password-file OpenAM 管理者パスワード記述ファイル
    -e|--realm レルム名
    -m|--name 認証連鎖名
```

サブコマンド共通のオプションの説明は「オプション」をご参照ください。ここでは、このサブコマンドに特有のオプションについて説明します。

- -m, --name 認証連鎖名
  - 認証連鎖の名前を指定します。
  - この名前は OpenAM の管理コンソールで表示されたり、URL のクエリ文字列で指定します。

実行例は以下になります。

```
# /opt/osstech/bin/ssoadm create-auth-cfg -u amadmin -f password.txt -e usr \
-m sample

認証設定が作成されました。
```

7.6.2 認証連鎖に認証モジュールインスタンスを追加する

レルムの認証連鎖に認証モジュールのインスタンスを追加します。書式は以下になります。

```
ssoadm add-auth-cfg-entr
    -u|--adminid OpenAM 管理者ユーザー名
    -f|--password-file OpenAM 管理者パスワード記述ファイル
    -e|--realm レルム名
    -m|--name 認証連鎖名
    -o|--modulename 認証モジュール名
    -c|--criteria 基準
   [-t|--options オプション]
   [-p|--position 順序]
```

サブコマンド共通のオプションの説明は「オプション」をご参照ください。ここでは、このサブコマンドに特有のオプションについて説明します。

- -m, --name 認証連鎖名
  - 追加先の認証連鎖の名前を指定します。
- -o, --modulename 認証モジュール名
  - 追加する認証モジュールインスタンスの名前を指定します。
- -c, --criteria 基準
  - 基準を選択します。
  - 以下のうちから選択してください。
    - REQUIRED (必須) / OPTIONAL (任意) / SUFFICIENT (十分) / REQUISITE (必要)
- -t, --options オプション
  - オプションを指定します。
  - オプションはキーと値を”=“でつなぎ、複数指定する場合は”,“で区切ります。
    - 例: key1=value1,key2=value2,key3=value3
- -p, --position 順序
  - 挿入する順序を 0 始まりの数字で指定します。

実行例は以下になります。

```
# /opt/osstech/bin/ssoadm add-auth-cfg-entr -u amadmin -f password.txt -e usr \
-m sample -o LDAP -c REQUIRED -t "key1=value1,key2=value2" -p 0
```

```
認証設定のエントリが作成されました。
```

7.6.3 認証連鎖の設定を更新する

認証連鎖に登録されている認証モジュールインスタンスの設定を更新します。書式は以下になります。

```
ssoadm update-auth-cfg-entr
    -u|--adminid OpenAM 管理者ユーザー名
    -f|--password-file OpenAM 管理者パスワード記述ファイル
    -e|--realm レルム名
    -m|--name 認証連鎖名
  [-a|--entries 認証モジュールインスタンスエントリ]
  [-D|--datafile 認証モジュールインスタンスエントリファイル]
```

サブコマンド共通のオプションの説明は「オプション」をご参照ください。ここでは、このサブコマンドに特有のオプションについて説明します。

- -m, --name 認証連鎖名
  - 更新する認証連鎖の名前を指定します。
- -a, --entries 認証モジュールインスタンスエントリ
  - 一つのエントリを{モジュールインスタンス名}|{基準}|{オプション}の形式で指定します。
    - LDAP|SUFFICIENT|key1=value1,key2=value2
    - 複数のエントリを指定できます。
- -D, --datafile 認証モジュールインスタンスエントリファイル
  - エントリをファイルから読み込みます。
  - 一つのエントリを{モジュールインスタンス名}|{基準}|{オプション}の形式で指定します。
    - LDAP|SUFFICIENT|key1=value1,key2=value2
  - ファイルの各行にエントリを 1 つずつ記載します。

実行例は以下になります。

```
# /opt/osstech/bin/ssoadm update-auth-cfg-entr -u amadmin -f password.txt \
-e usr -m sample -a "LDAP|SUFFICIENT|" "DataStore|REQUIRED|"

LDAP|SUFFICIENT|
```

```
DataStore|REQUIRED|
認証設定のエントリが更新されました。
```

7.6.4 認証連鎖に登録されているエントリの一覧を取得する

認証連鎖に登録されている認証モジュールインスタンスと設定の一覧を所得します。書式は以下になります。

```
ssoadm get-auth-cfg-entr
    -u|--adminid OpenAM 管理者ユーザー名
    -f|--password-file OpenAM 管理者パスワード記述ファイル
    -e|--realm レルム名
    -m|--name 認証連鎖名
```

サブコマンド共通のオプションの説明は「オプション」をご参照ください。ここでは、このサブコマンドに特有のオプションについて説明します。

- -m, --name 認証連鎖名
  - 認証連鎖の名前を指定します。

実行例は以下になります。

```
# /opt/osstech/bin/ssoadm get-auth-cfg-entr -u amadmin -f password.txt -e usr \
-m sample

認証設定のエントリ:
[名前=LDAP] [フラグ=SUFFICIENT] [オプション=]
[名前=DataStore] [フラグ=REQUIRED] [オプション=]
```

7.6.5 認証連鎖の一覧を取得する

レルムに登録されている認証連鎖の一覧を取得します。書式は以下になります。

```
ssoadm list-auth-cfgs
    -u|--adminid OpenAM 管理者ユーザー名
    -f|--password-file OpenAM 管理者パスワード記述ファイル
    -e|--realm レルム名
```

サブコマンド共通のオプションの説明は「オプション」をご参照ください。実行例は以下になります。

```
# /opt/osstech/bin/ssoadm list-auth-cfgs -u amadmin -f password.txt -e usr

認証設定:
ldapService
sample
```

7.6.6 認証連鎖を削除する

認証連鎖をレルムから削除します。 書式は以下になります。

```
ssoadm delete-auth-cfgs
    -u|--adminid OpenAM 管理者ユーザー名
    -f|--password-file OpenAM 管理者パスワード記述ファイル
    -e|--realm レルム名
    -m|--names 認証連鎖名
```

サブコマンド共通のオプションの説明は「オプション」をご参照ください。ここでは、このサブコマンドに特有のオプションについて説明します。

- -m, --name 認証連鎖名
  - 削除する認証連鎖の名前を指定します。
  - 複数指定できます。

実行例は以下になります。

```
/opt/osstech/bin/ssoadm delete-auth-cfgs -u amadmin -f password.txt -e usr \
-m sample1 sample2

認証設定が削除されました。
```

8 SAML 設定

本章では、ssoadm コマンドで SAML の設定を管理する方法を説明します。

8.1 トラストサークルの管理

トラストサークルの設定を管理する方法を説明します。

8.1.1 トラストサークルの作成

トラストサークルを作成します。書式は以下になります。

```
ssoadm create-cot
    -u|--adminid OpenAM 管理者ユーザー名
    -f|--password-file OpenAM 管理者パスワード記述ファイル
    -e|--realm レルム名
    -t|--cot トラストサークル名
```

オプションの説明は「オプション」をご参照ください。ここでは、このサブコマンドに特有のオプションについて説明します。

- -t, --cot トラストサークル名
  - トラストサークルの名前を指定します。

実行例は以下になります。

```
# /opt/osstech/bin/ssoadm create-cot -u amadmin -f password.txt -e usr -t usr-cot

トラストサークル usr-cot が作成されました。
```

8.1.2 トラストサークルの一覧取得

トラストサークルの一覧を取得します。書式は以下になります。

```
ssoadm list-cots
    -u|--adminid OpenAM 管理者ユーザー名
    -f|--password-file OpenAM 管理者パスワード記述ファイル
    -e|--realm レルム名
```

オプションの説明は「オプション」をご参照ください。実行例は以下になります。

```
# /opt/osstech/bin/ssoadm list-cots -u amadmin -f password.txt -e usr

トラストサークルは次のとおりです。
 usr-cot
```

8.1.3 トラストサークルの削除

トラストサークルを削除します。書式は以下になります。

```
ssoadm delete-cot
    -u|--adminid OpenAM 管理者ユーザー名
    -f|--password-file OpenAM 管理者パスワード記述ファイル
    -e|--realm レルム名
    -t|--cot トラストサークル名
```

オプションの説明は「オプション」をご参照ください。実行例は以下になります。

```
# /opt/osstech/bin/ssoadm delete-cot -u amadmin -f password.txt -e usr -t usr-cot

トラストサークル usr-cot が削除されました。
```

8.2 エンティティーの管理

エンティティーの設定を管理する方法を説明します。 エンティティーとは SAML IdP や SAML SP のことを意味します。

8.2.1 エンティティーのインポート

エンティティーをインポートします。 OpenAM に SAML IdP や SAML SP を登録する場合にこのコマンドを使用します。 書式は以下になります。

```
ssoadm import-entity
    -u|--adminid OpenAM 管理者ユーザー名
    -f|--password-file OpenAM 管理者パスワード記述ファイル
   [-e|--realm レルム名]
   [-t|--cot トラストサークル名]
   [-m|--meta-data-file メタデータファイル]
   [-x|--extended-data-file 拡張メタデータファイル]
   [-c|--spec]
```

オプションの説明は「オプション」をご参照ください。ここでは、このサブコマンドに特

有のオプションについて説明します。

- -t, --cot トラストサークル名
  - トラストサークルの名前を指定します。
- -y, --entityid エンティティー ID
  - エンティティー ID を指定します。エンティティー ID は、OpenAM 管理コンソールの「連携」タブ画面の「エンティティープロバイダ」の一覧に表示される「名前」です。
- -m, --meta-data-file メタデータファイル
  - メタデータファイル (XML) を指定します。
  - 登録されるエンティティーの種類 (IdP もしくは SP) はメタデータにより自動的に判断されます。
- -x, --extended_data-file 拡張メタデータファイル
  - 拡張メタデータファイル (XML) を指定します。
  - エンティティーを OpenAM の「ホストアイデンティティプロバイダ」として登録する場合は、このオプションの指定が必要です。このオプションを指定せずにコマンドを実行すると、「リモートアイデンティティプロバイダ」として登録されます。
- -g, --sign
  - メタデータに対してデジタル署名を付加します。
- -c, --spec
  - メタデータのプロトコルを指定します。「saml2」、「idff」、「wsfed」のいずれか一つを指定します。デフォルトは「saml2」です。

インポートに利用するメタデータと拡張メタデータは、「エンティティーのエクスポート」の手順で一旦エクスポートしたメタデータを参考にして作成することができます。メタデータの内容については、「メタデータサンプル」をご参照ください。

- SAML IdP や SAML SP の機能を利用するためには、エンティティーがトラストサークルに所属している必要があります。エンティティーをトラストサークルに所属させるためには、「トラストサークルの作成」の手順で事前にトラストサークルを作成しておき、import-entity サブコマンドの-t オプションでトラストサークルを指定します。

実行例は以下になります。

```
# /opt/osstech/bin/ssoadm import-entity -u amadmin -f password.txt -e usr \
-t usr-cot -m samlsp-metadata.xml -c saml2

ファイル samlsp-metadata.xml をインポートしました。
```

```
# /opt/osstech/bin/ssoadm import-entity -u amadmin -f password.txt -e usr \
-t usr-cot -m samlidp-metadata.xml -x samlidp-ext-metadata.xml -c saml2

ファイル samlidp-metadata.xml をインポートしました。
ファイル samlidp-ext-metadata.xml をインポートしました。
```

8.2.2 エンティティーのエクスポート

エンティティーをエクスポートします。OpenAM に作成されたエンティティーのメタデータを取得する場合に利用します。書式は以下になります。

```
ssoadm export-entity
    -u|--adminid OpenAM 管理者ユーザー名
    -f|--password-file OpenAM 管理者パスワード記述ファイル
    -y|--entityid エンティティー ID
   [-e|--realm レルム名]
   [-m|--meta-data-file メタデータファイル]
   [-x|--extended-data-file 拡張メタデータファイル]
   [-g|--sign]
   [-c|--spec]
```

オプションの説明は「エンティティーのインポート」のオプションをご参照ください。メタデータの内容については、「メタデータサンプル」をご参照ください。実行例は以下になります。

```
# /opt/osstech/bin/ssoadm export-entity -u amadmin -f password.txt -e usr \
-y "http://sso.example.co.jp/openam/usr" -m saml-metadata.xml -c saml2

エンティティー記述子がファイル saml-metadata.xml にエクスポートされました。
```

```
# /opt/osstech/bin/ssoadm export-entity -u amadmin -f password.txt -e usr \
-y "http://sso.example.co.jp/openam/usr" -m saml-metadata.xml \
-x saml-ext-metadata.xml -c saml2
```

```
エンティティー記述子がファイル saml-metadata.xml にエクスポートされました。
エンティティー設定がファイル saml-ext-metadata.xml にエクスポートされました。
```

8.2.3 エンティティーの一覧取得

エンティティーの一覧を取得します。書式は以下になります。

```
ssoadm list-entities
    -u|--adminid OpenAM 管理者ユーザー名
    -f|--password-file OpenAM 管理者パスワード記述ファイル
   [-e|--realm レルム名]
   [-c|--spec]
```

オプションの説明は「エンティティーのインポート」のオプションをご参照ください。実行例は以下になります。

```
# /opt/osstech/bin/ssoadm list-entities -u amadmin -f password.txt -e usr

エンティティー ID のリスト:
 http://sso.example.co.jp/openam/usr
 http://sp.exmaple.com/
```

8.2.4 エンティティーの削除

エンティティーを削除します。書式は以下になります。

```
ssoadm delete-entity
    -u|--adminid OpenAM 管理者ユーザー名
    -f|--password-file OpenAM 管理者パスワード記述ファイル
    -y|--entityid エンティティー ID
   [-e|--realm レルム名]
   [-c|--spec]
```

オプションの説明は「エンティティーのインポート」のオプションをご参照ください。実行例は以下になります。

```
# /opt/osstech/bin/ssoadm delete-entity -u amadmin -f password.txt -e usr \
-y "http://sso.example.co.jp/openam/usr"

エンティティー http://sso.example.co.jp/openam/usr の記述子が削除されました。
```

8.2.5 メタデータサンプル

メタデータのサンプルです。見やすいように改行しているところがありますが、実際には URL や文字列の途中で改行しないでください。

8.2.5.1 メタデータ

SAML エンティティーのメタデータです。-m(--meta-data-file) オプションで指定します。

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<EntityDescriptor entityID="http://sso.example.co.jp/openam/usr"
  xmlns="urn:oasis:names:tc:SAML:2.0:metadata">
  <IDPSSODescriptor WantAuthnRequestsSigned="false"
    protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <KeyDescriptor use="signing">
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
          <ds:X509Certificate>
            MIICQDCCAakCBEeNB0swDQYJKoZIhvcNAQEEBQAwZzELMAkGA1UEBhMCVVMxEzARBgNVB
            AgTCkNhbGlmb3JuaWExFDASBgNVBAcTC1NhbnRhIENsYXJhMQwwCgYDVQQKEwNTdW4xED
            AOBgNVBAsTB09wZW5TU08xDTALBgNVBAMTBHRlc3QwHhcNMDgwMTE1MTkxOTM5WhcNMTg
            wMTEyMTkxOTM5WjBnMQswCQYDVQQGEwJVUzETMBEGA1UECBMKQ2FsaWZvcm5pYTEUMBIG
            A1UEBxMLU2FudGEgQ2xhcmExDDAKBgNVBAoTA1N1bjEQMA4GA1UECxMHT3BlblNTTzENM
            AsGA1UEAxMEdGVzdDCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEArSQc/U75GB2AtK
            hbGS5piiLkmJzqEsp64rDxbMJ+xDrye0EN/q1U5Of+RkDsaN/igkAvV1cuXEgTL6RlafF
            PcUX7QxDhZBhsYF9pbwtMzi4A4su9hnxIhURebGEmxKW9qJNYJs0Vo5+IgjxuEWnjnnVg
            HTs1+mq5QYTA7E6ZyL8CAwEAATANBgkqhkiG9w0BAQQFAAOBgQB3Pw/UQzPKTPTYi9upb
            FXlrAKMwtFf2OW4yvGWWvlcwcNSZJmTJ8ARvVYOMEVNbsT4OFcfu2/PeYoAdiDAcGy/F2
            Zuj8XJJpuQRSE6PtQqBuDEHjjmOQJ0rV/r8mO1ZCtHRhpZ5zYRjhRC9eCbjx9VrFax0JD
            C/FfwWigmrW0Y0Q==
          </ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </KeyDescriptor>
    <ArtifactResolutionService index="0" isDefault="true"
      Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
      Location="http://sso.example.co.jp/openam/ArtifactResolver/metaAlias/
                usr/idp"/>
    <SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:
                                  HTTP-Redirect"
      Location="http://sso.example.co.jp/openam/IDPSloRedirect/metaAlias/usr/
                idp"
      ResponseLocation="http://sso.example.co.jp/openam/IDPSloRedirect/
                        metaAlias/usr/idp"/>
```

```
    <SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
      Location="http://sso.example.co.jp/openam/IDPSloPOST/metaAlias/usr/idp"
      ResponseLocation="http://sso.example.co.jp/openam/IDPSloPOST/metaAlias/
                        usr/idp"/>
    <SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
      Location="http://sso.example.co.jp/openam/IDPSloSoap/metaAlias/usr/
                idp"/>
    <ManageNameIDService Binding="urn:oasis:names:tc:SAML:2.0:bindings:
                                  HTTP-Redirect"
      Location="http://sso.example.co.jp/openam/IDPMniRedirect/metaAlias/usr/
                idp"
      ResponseLocation="http://sso.example.co.jp/openam/IDPMniRedirect/
                        metaAlias/usr/idp"/>
    <ManageNameIDService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
      Location="http://sso.example.co.jp/openam/IDPMniPOST/metaAlias/usr/idp"
      ResponseLocation="http://sso.example.co.jp/openam/IDPMniPOST/metaAlias/
                        usr/idp"/>
    <ManageNameIDService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
      Location="http://sso.example.co.jp/openam/IDPMniSoap/metaAlias/usr/
                idp"/>
    <NameIDFormat>
      urn:oasis:names:tc:SAML:2.0:nameid-format:persistent
    </NameIDFormat>
    <NameIDFormat>
      urn:oasis:names:tc:SAML:2.0:nameid-format:transient
    </NameIDFormat>
    <NameIDFormat>
      urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
    </NameIDFormat>
    <NameIDFormat>
      urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
    </NameIDFormat>
    <NameIDFormat>
      urn:oasis:names:tc:SAML:1.1:nameidformat:WindowsDomainQualifiedName
    </NameIDFormat>
    <NameIDFormat>
      urn:oasis:names:tc:SAML:2.0:nameid-format:kerberos
    </NameIDFormat>
    <NameIDFormat>
      urn:oasis:names:tc:SAML:1.1:nameidformat:X509SubjectName
    </NameIDFormat>
    <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:
                                  HTTP-Redirect"
      Location="http://sso.example.co.jp/openam/SSORedirect/metaAlias/usr/
```

```
                idp"/>
    <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
      Location="http://sso.example.co.jp/openam/SSOPOST/metaAlias/usr/idp"/>
    <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
      Location="http://sso.example.co.jp/openam/SSOSoap/metaAlias/usr/idp"/>
    <NameIDMappingService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
      Location="http://sso.example.co.jp/openam/NIMSoap/metaAlias/usr/idp"/>
    <AssertionIDRequestService Binding="urn:oasis:names:tc:SAML:2.0:bindings:
                                        SOAP"
      Location="http://sso.example.co.jp/openam/AIDReqSoap/IDPRole/metaAlias/
                usr/idp"/>
    <AssertionIDRequestService Binding="urn:oasis:names:tc:SAML:2.0:bindings:URI"
      Location="http://sso.example.co.jp/openam/AIDReqUri/IDPRole/metaAlias/
                usr/idp"/>
  </IDPSSODescriptor>
</EntityDescriptor>
```

以下の部分を実際の環境に合わせて編集してください。

- 「<EntityDescriptor>」要素の「entityID」属性
  - エンティティー ID を指定してください。
  - 上記の例では「http://sso.example.co.jp/openam/usr」としています。
- 「<ds:X509Certificate> 」要素
  - SAML メッセージのデジタル署名に利用する証明書情報を記述してください。
- 各種サービスの URL
  - 各種サービスの URL に、実際の環境に合わせた値を記述してください。URL は以下のような形式になっています。
    - 「スキーム://ホスト名/OpenAM ディプロイ名/サービス識別子/metaAlias/レルム名/エンティティー種別 (sp/idp)」
  - 「サービス識別子/metaAlias」の部分は変更する必要はありません。それ以外の部分を環境に合わせて変更してください。

8.2.5.2 拡張メタデータ

SAML エンティティーの設定情報を含むメタデータです。-x(--extended-data-file) オプションで指定します。

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<EntityConfig entityID="http://sso.example.co.jp/openam/usr" hosted="true"
  xmlns="urn:sun:fm:SAML:2.0:entityconfig">
```

```
<IDPSSOConfig metaAlias="/usr/idp">
  <Attribute name="idpAuthncontextMapper">
    <Value>com.sun.identity.saml2.plugins.DefaultIDPAuthnContextMapper</Value>
  </Attribute>
  <Attribute name="appLogoutUrl">
    <Value/>
  </Attribute>
  <Attribute name="attributeMap"/>
  <Attribute name="proxyIDPFinderJSP"/>
  <Attribute name="autofedAttribute">
    <Value/>
  </Attribute>
  <Attribute name="proxyIDPFinderClass"/>
  <Attribute name="wantNameIDEncrypted">
    <Value>false</Value>
  </Attribute>
  <Attribute name="signingCertAlias">
    <Value>test</Value>
  </Attribute>
  <Attribute name="idpSessionSyncEnabled">
    <Value>false</Value>
  </Attribute>
  <Attribute name="idpAuthncontextClassrefMapping">
    <Value>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport|0||
    default</Value>
  </Attribute>
  <Attribute name="saeAppSecretList"/>
  <Attribute name="encryptionCertAlias"/>
  <Attribute name="assertionEffectiveTime">
    <Value>600</Value>
  </Attribute>
  <Attribute name="autofedEnabled">
    <Value>false</Value>
  </Attribute>
  <Attribute name="wantMNIResponseSigned">
    <Value>false</Value>
  </Attribute>
  <Attribute name="discoveryBootstrappingEnabled">
    <Value>false</Value>
  </Attribute>
  <Attribute name="wantLogoutRequestSigned">
    <Value>false</Value>
  </Attribute>
  <Attribute name="cotlist">
```

```
    <Value>usr-cot</Value>
  </Attribute>
  <Attribute name="AuthUrl">
    <Value/>
  </Attribute>
  <Attribute name="relayStateUrlList"/>
  <Attribute name="wantArtifactResolveSigned">
    <Value>false</Value>
  </Attribute>
  <Attribute name="idpAccountMapper">
    <Value>com.sun.identity.saml2.plugins.DefaultIDPAccountMapper</Value>
  </Attribute>
  <Attribute name="wantLogoutResponseSigned">
    <Value>false</Value>
  </Attribute>
  <Attribute name="enableProxyIDPFinderForAllSPs"/>
  <Attribute name="idpAdapter"/>
  <Attribute name="basicAuthUser">
    <Value/>
  </Attribute>
  <Attribute name="assertionNotBeforeTimeSkew">
    <Value>600</Value>
  </Attribute>
  <Attribute name="basicAuthPassword">
    <Value/>
  </Attribute>
  <Attribute name="idpECPSessionMapper">
    <Value>com.sun.identity.saml2.plugins.DefaultIDPECPSessionMapper</Value>
  </Attribute>
  <Attribute name="wantMNIRequestSigned">
    <Value>false</Value>
  </Attribute>
  <Attribute name="assertionCacheEnabled">
    <Value>false</Value>
  </Attribute>
  <Attribute name="idpAttributeMapper">
    <Value>com.sun.identity.saml2.plugins.DefaultIDPAttributeMapper</Value>
  </Attribute>
  <Attribute name="nameIDFormatMap">
    <Value>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified=uid</Value>
  </Attribute>
  <Attribute name="metaAlias"/>
  <Attribute name="RpUrl">
    <Value/>
```

```
    </Attribute>
    <Attribute name="basicAuthOn">
      <Value>false</Value>
    </Attribute>
    <Attribute name="saeIDPUrl">
      <Value>http://sso.example.co.jp/openam/idpsaehandler/metaAlias/usr/idp
      </Value>
    </Attribute>
  </IDPSSOConfig>
</EntityConfig>
```

以下の部分を実際の環境に合わせて編集してください。

- 「<EntityDescriptor>」要素の「entityID」属性
  - エンティティー ID を指定してください。
- 各種サービスの URL を「メタデータ」と同じ要領で変更してください。
- 「<Attribute name=“signingCertAlias”> 」の Value を、SAML メッセージへの署名に利用する鍵のエイリアス名に変更してください。デフォルト値は「test」です。
- 「<Attribute name=“nameIDFormatMap”>」の Value を、連携する SAML SP が必要とする NameID の仕様に合わせて適宜変更してください。
- その他の要素は OpenAM の管理コンソールから作成した場合のデフォルト値となっています。必要に応じて適宜変更してください。

9 ユーザー管理

本章では、ssoadm コマンドで OpenAM ユーザーデータストアのユーザー情報を管理する方法を説明します。

9.1 ユーザーの追加

ユーザーデータストアにユーザーを追加します。 書式は以下になります。

```
ssoadm create-identity
    -u|--adminid OpenAM 管理者ユーザー名
    -f|--password-file OpenAM 管理者パスワード記述ファイル
    -e|--realm レルム名
    -t|--idtype アイデンティティのタイプ (User|Role|Group)
    -i|--idname アイデンティティの名前
   [-a|--attributevalues 属性値]
   [-D|--datafile 属性値記述ファイル]
```

サブコマンド共通のオプションの説明は「オプション」をご参照ください。ここでは、このサブコマンドに特有のオプションについて説明します。

- -t, --idtype アイデンティティのタイプ
  - アイデンティティのタイプを指定します。以下の 3 つのタイプのうち、いずれか 1 つを指定します。
    - User : ユーザーエントリ
    - Group : グループエントリ
    - Role : ロールエントリ
- -i, --idname アイデンティティの名前
  - アイデンティティの名前を指定します。ユーザー名やグループ名などです。
- ユーザーエントリの属性 (cn、sn、userPassword など) を指定する場合は、-a オプションか-D オプションを利用し、「属性名=属性値」という形式で指定します。指定可能な属性は、ユーザーデータストア設定の「LDAP ユーザー属性」に設定されている属性です。
- **userPassword 属性は必ず指定する必要があります。**コマンドライン上でのパスワードの指定はセキュリティ上好ましくないため、ファイルに userPassword 属性を記述し、-D オプションで読み込む方法を推奨します。

実行例は以下になります。

```
# cat user.conf
userPassword=*****

# /opt/osstech/bin/ssoadm create-identity -u amadmin -f password.txt -e usr \
-t User -i taro -D user.conf

タイプ User のアイデンティティー taro がレルム usr に作成されました。
```

9.2 ユーザーの変更

ユーザーデータストアのユーザー情報を変更します。 書式は以下になります。

```
ssoadm set-identity-attrs
    -u|--adminid OpenAM 管理者ユーザー名
    -f|--password-file OpenAM 管理者パスワード記述ファイル
    -e|--realm レルム名
    -t|--idtype アイデンティティのタイプ (User|Role|Group)
    -i|--idname アイデンティティの名前
   [-a|--attributevalues 属性値]
   [-D|--datafile 属性値記述ファイル]
```

オプションの意味は「9.1 ユーザーの追加」をご参照ください。実行例は以下になります。

```
# /opt/osstech/bin/ssoadm set-identity-attrs -u amadmin -f password.txt -e usr \
-t User -i taro -a "mail=taro@example.jp"

レルム usr 内のタイプ User のアイデンティティー taro の属性値が変更されました。
```

9.3 ユーザーの削除

ユーザーデータストアのユーザーを削除します。書式は以下になります。

```
ssoadm delete-identities
    -u|--adminid OpenAM 管理者ユーザー名
    -f|--password-file OpenAM 管理者パスワード記述ファイル
    -e|--realm レルム名
    -t|--idtype アイデンティティのタイプ (User|Role|Group)
    -i|--idnames アイデンティティの名前
   [-D|--file アイデンティティー覧ファイル]
```

オプションの意味は「9.1 ユーザーの追加」をご参照ください。ここでは、このサブコマンドに特有のオプションについて説明します。

- -i, --idnames アイデンティティの名前
  - アイデンティティの名前を指定します。半角スペースで区切ることで複数のアイデンティティを指定することも可能です。
  - 複数のアイデンティティを指定した際に、そのうちのいずれかのアイデンティティの削除に失敗した場合は、指定した他のアイデンティティは削除されません。

実行例は以下になります。

```
# /opt/osstech/bin/ssoadm delete-identities -u amadmin -f password.txt -e usr \
-t User -i taro hanako

次の User が usr から削除されました。
    taro
    hanako
```

10 トラブルシューティング

本章では、ssoadm コマンドのトラブルシューティングの方法について説明します。

10.1 エラーメッセージ

ssoadm のエラーメッセージについて説明します。

```
Login failed.
```

- 管理者アカウントの情報 (ユーザー名/パスワード) が間違っています。

```
Service URL not found:session
```

- 最上位のレルムの「モジュールベースの認証」が有効になっていない可能性があります。「サービス (認証連鎖名) の指定」の手順を参照ください。

```
Logging configuration class "com.sun.identity.log.s1is.LogConfigReader" failed
com.sun.identity.security.AMSecurityPropertiesException: AdminTokenAction:
   FATAL ERROR: Cannot obtain Application SSO token.
com.sun.identity.security.AMSecurityPropertiesException: AdminTokenAction:
   FATAL ERROR: Cannot obtain Application SSO token.
```

- セッションの有効性が確認できません。サイト構成の定義を追加が設定されていないか指定している URL が誤っている可能性があります。

```
Cannot bootstrap the system/opt/osstech/var/lib/tomcat/data/openam/bootstrap
  （そのようなファイルやディレクトリはありません）
```

- 設定情報ディレクトリが見つかりません。設定情報ディレクトリの確認が設定されていないか設定しているディレクトリが誤っている可能性があります。

10.2 既知の事象

ssoadm を実行すると稀に下記のメッセージが表示されることがあります。コマンドの実行は成功しており無害なメッセージのため無視して下さい。

```
Exception in thread "SystemTimer" java.lang.Error: java.lang.ExceptionInInitializ
erError
    at com.sun.identity.common.TimerPool$WorkerThread.run(TimerPool.java:542)
Caused by: java.lang.ExceptionInInitializerError
    at com.sun.identity.idm.IdRepoListener.getChangedIds(IdRepoListener.java:278)
    at com.sun.identity.idm.IdRepoListener.objectChanged(IdRepoListener.java:174)
  ～ スタックトレース省略 ～
```

11 改訂履歴

- 2019 年 12 月 23 日 リビジョン 1.0
  - 初版作成。
- 2020 年 11 月 25 日 リビジョン 1.1
  - 初期設定ガイドで構築した場合の URL に変更
  - 「サイト構成の定義を追加」「サービス (認証連鎖名) の指定」「設定情報ディレクトリの確認」を追加
- 2021 年 4 月 28 日 リビジョン 1.2
  - 設定情報ディレクトリのパスを修正
- 2021 年 5 月 6 日 リビジョン 1.3
  - パッケージのバージョン表記の統一
- 2022 年 7 月 14 日 リビジョン 1.4
  - 表紙の社名を OSSTech 株式会社に変更
- 2023 年 1 月 10 日 リビジョン 1.5
  - 「既知の事象」を追加
- 2023 年 5 月 8 日 リビジョン 1.6
  - 「デバッグログのログレベルの変更」に OpenAM のログレベルと連動する旨を追加
  - 「グローバルオプション」の--debug の説明を修正