# WebOTX 運用編(ユーザ管理)

WebOTX 運用編

バージョン: 7.1

版数: 第 3 版

リリース: 2008 年 11 月

# 目次


1　はじめに ..... 1

2　ユーザ管理の概要 ..... 2
2.1　ユーザ ..... 2
2.2　グループ ..... 2
2.3　ロール ..... 2
2.4　ユーザ、グループ、ロールの関係 ..... 2
2.5　レルム ..... 3

3　レルムの設定 ..... 4
3.1　Fileレルム ..... 4
3.1.1　運用管理コマンドから設定 ..... 4
3.1.2　統合運用管理ツールから設定 ..... 5
3.1.3　Fileレルムで設定可能なオプション一覧 ..... 10
3.2　LDAPレルム ..... 10
3.2.1　運用管理コマンドから設定 ..... 10
3.2.2　統合運用管理ツールから設定 ..... 12
3.2.3　LDAPレルムで設定可能なオプション一覧 ..... 16
3.3　JDBCレルム ..... 17
3.3.1　運用管理コマンドから設定 ..... 17
3.3.2　統合運用管理ツールから設定 ..... 19
3.3.3　JDBCレルムで設定可能なオプション一覧 ..... 23

4　ユーザ管理 ..... 26
4.1　Fileレルムを使用する場合 ..... 26
4.1.1　ユーザの追加、削除 ..... 26
4.1.2　グループの追加、削除 ..... 29
4.2　LDAPレルムを使用する場合 ..... 30
4.2.1　ユーザの追加、削除 ..... 30
4.2.2　グループの作成、削除 ..... 34
4.2.3　ユーザをグループに登録 ..... 38
4.3　JDBCレルムを使用する場合 ..... 40
4.3.1　データベーステーブルの作成、削除 ..... 40
4.3.2　ユーザの追加、削除 ..... 41
4.3.3　グループの追加、削除 ..... 42

5　ロールの設定 ..... 42
5.1　アプリケーションへのロールの設定 ..... 42

5.1.1 配備記述子にロールの定義を追加 ..... 42
5.1.2 ユーザ認証を行うWebアプリケーションの作成方法 ..... 45

# 1 はじめに

本書は WebOTX 実行環境を運用するための運用操作法について概要や具体的な設定項目や設定方法について記載しています。

## 対象読者

このマニュアルは WebOTX Application Server Web Edition、Standard-J Edition、Standard Edition、Enterprise Edition を使って運用環境を構築するシステムエンジニア、日々の運用を行うオペレータを対象としています。

## 表記について

### パス名表記

本書ではパス名の表記については特に OS を限定しない限りセパレータはスラッシュ'/'で統一しています。Windows 環境においては'¥'に置き換えてください。

### 環境変数表記

インストールディレクトリやドメインルートディレクトリなど環境によって値の異なるものについては環境変数を用いて表します。

${*env*} または $(*env*)で表しています。

例)
${AS_INSTALL} : インストールディレクトリ
${INSTANCE_ROOT}: ドメインルートディレクトリ

### コマンド操作について

本書中では運用操作に用いるコマンドの詳細についての説明は省略しています。

コマンドの詳細は「運用管理コマンド」、「運用管理コマンドリファレンス」を参照してください。

# 2 ユーザ管理の概要

## 2.1 ユーザ

ユーザとは、アプリケーションサーバが個人、アプリケーションに割り当てる ID のことです。ユーザは一つのグループに所属することができます。

- WebOTX では？

WebOTX では、ドメイン作成時に 3 つのデフォルトユーザ(admin、system、guest)が作成されます。これらの 3 つのアカウントのうち、admin のみを WebOTX 運用管理に利用します。system は、WebOTX 内部で使用し、ユーザが利用することはできません。また、変更、削除も行わないでください。guest は JMS の運用ユーザです。

ユーザを新しく追加する場合は、4 章を参照してください。

## 2.2 グループ

グループは共通の特性で分類されたユーザのカテゴリです。ユーザをグループに分類すると、ユーザからの大量のアクセスを制御することが容易になります。

- WebOTX では？

WebOTX では 2.1 節で述べたように、ドメイン作成直後には admin,system,guest ユーザが作成されます。これらのユーザのうち、admin と system は otxadmin グループに所属し、guest は anonymous グループに所属しています。WebOTX では、2.3 節で説明していますが、WebOTX の運用管理を行うユーザは otxadmin グループに所属していなければなりません。グループの作成方法については、4 章を参照してください。

## 2.3 ロール

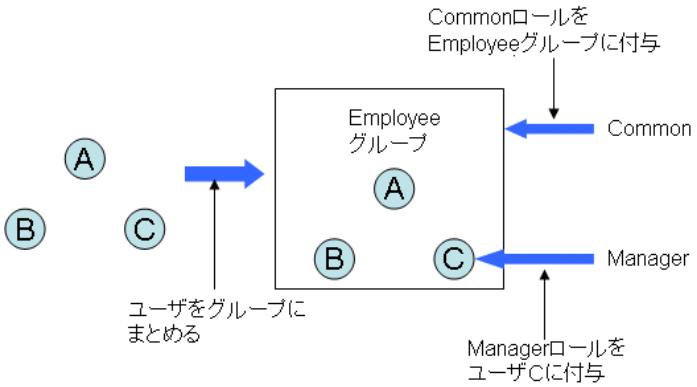
ロールとは、ユーザがどのアプリケーションを利用することができるか、アプリケーションのどの部分にアクセスすることができるかを決定します。

WebOTX 上で動作するアプリケーション(WebAP、EJB)を実行するためのロールは、WebOTX が提供している配備ツールを利用することにより、細かくロールの設定を行うことができます。ロールの設定方法については 5 章を参照してください。

## 2.4 ユーザ、グループ、ロールの関係

ユーザは共通の特性によってグループ単位に分けることができます。複数のユーザをグループとしてまとめることで、ユーザの管理がしやすくなります。また、ロールはユーザ個人、またはグループに付与することができます。グループにロールを付与することは、そのグループに所属しているユーザ全員に同じロールを割り当てることと同じことになります。

例えば勤務管理システムでは、利用者(ユーザ、図では A,B,C)は全員、Employee(従業員)というグループに所属していなければなりません。Employee グループには毎日の勤務時間の登録、変更を行うことができるロールである一般という意味の common というロールが付与されています。common に加えて、管理職である C には Manager というロールが付与されていて、勤務時間の登録、変更に加えて、承認作業を行うことができます。




## 2.5 レルム

レルムとは、ユーザおよびグループの情報を格納しているレポジトリを意味しています。WebOTX ではこのレルムを利用し、ユーザの認証を行います。

WebOTX で使用できるレルムについて説明します。

WebOTX では、次の3つのレルムをサポートしています。ドメイン作成直後のデフォルトで File レルムを使用する設定になっています。

- File レルム
  File レルムを使用する場合、WebOTX はユーザに関する情報(ユーザ ID、パスワード、グループ名)を keyfile と呼ばれるファイルに書き込み、ローカルに保存しておきます。keyfile は ${INSTANCE_ROOT}/config 以下に保存されています。ドメイン作成直後の設定では、デフォルトで File レルムを使用する設定になっています。File レルムの設定が不要な場合、または再設定を行う場合は、3.1 章を参照してください。運用管理コマンド、ツールを利用してユーザの管理を行うことができます。File レルムを利用する場合のユーザの追加、削除の方法は、4.1 章を参照してください。
- LDAP レルム
  LDAP レルムを使用する場合、WebOTX は LDAP サーバからユーザ情報を取得します。WebOTX では、以下の二つの LDAP サーバと連携することができます。
  - Enterprise Directory Server Ver5(Windows,Linux) Ver4.1(HP-UX)(*1)
  - OpenLDAP Ver2.0

  LDAP レルムを使用するための設定方法は 3.2 章、Enterprise Directory Server(以下 EDS)でのユーザ、グループ管理の方法については、4.2 章を参照してください。OpenLDAP を利用する場合は、OpenLDAP のマニュアルを参照してください。
- JDBC レルム
  JDBC レルムを使用する場合、WebOTX は、JDBC ドライバがアクセスするデータベースから、ユーザ情報を取得します。JDBC レルムを使用するための設定方法は、3.3 章、データベースでユーザ、パスワード等を管理するための表については、4.3 章を参照してください。

(*1)
Enterprise Directory Server とは NEC が提供している LDAP サーバです。WebOTX の CD4 枚目(Linux は 3 枚目)からインストールすることができます。利用する場合は、セットアップカード(EDS_SetupCard.pdf)を参照して、WebOTX がインストールされている環境にインストールしてください。セットアップカードは CD4 枚目(Linux は 3 枚目)に含まれています。

# 3 レルムの設定

## 3.1 File レルム

File レルムの設定方法について説明します。File レルムの設定は、運用管理コマンド、または統合運用管理ツールから行います。

### 3.1.1 運用管理コマンドから設定

本節では運用管理コマンド(otxadmin コマンド)を利用してFileレルムの設定を行う方法について説明します。以下の例では設定するドメイン名を domain1、運用ユーザの ID を admin、パスワードを xxxxxx とします。適宜環境に合わせて読み替えてください。

#### 設定手順

1. ドメイン起動
   ドメインが起動していない場合は起動します。
   ${AS_INSTALL}/bin/otxadmin start-domain domain1

2. File レルムの設定
   create-auth-realm コマンドを利用し、File レルムの設定を行います。以下にコマンド例を記載します。create-auth-realm コマンドの詳しい使い方はマニュアルの[運用管理コマンドリファレンス]―[運用管理エージェント運用管理コマンド(otxadmin)]の create-auth-realm を参照してください。

   {AS_INSTALL}/bin/otxadmin
   otxadmin > login --user admin --password xxxxxx --port 6212
   otxadmin > create-auth-realm --classname
   com.nec.webotx.enterprise.security.auth.realm.file.FileRealm --property
   "file=${INSTANCE_ROOT}/config/keyfile:jaas-context=fileRealm" filesample

   - 注意 : classname オプションで指定する値は必ず以下の値にしてください。
     **com.nec.webotx.enterprise.security.auth.realm.file.FileRealm**

   なお、property オプションで指定する項目は 3.1.3 節の File レルムで設定可能なオプション一覧を参照してください。

3. 使用するレルムの指定
   ・アプリケーションを利用するユーザの認証に使用するレルムを設定する場合
   otxadmin > set server.security-service.default-realm=filesample
   ・WebOTX 運用ユーザの認証に使用するレルムを設定する場合
   otxadmin > set server.admin-service.admin-realm=filesample

4. ドメインの再起動
   ドメインを再起動することにより、設定が反映されます。
   otxadmin > exit
   (停止)　${AS_INSTALL}/bin/otxadmin stop-domain domain1
   (起動)　${AS_INSTALL}/bin/otxadmin start-domain domain1

#### 削除手順

1. ドメイン起動
   ドメインが起動してない場合は起動します。
   ${AS_INSTALL}/bin/otxadmin start-domain domain1

2. 使用するレルムの変更
   削除するレルムを default-realm に設定していると削除を行うことができません。そのため、使用するレルムを変更する必要があります。以下にレルム名 filesample を削除するために、レルム名が ldap というレルムに変更する例を記載します。適宜環境に合わせて変更してください。

{AS_INSTALL}/bin/otxadmin
otxadmin > login --user admin --password xxxxxx --port 6212
・AP ユーザの認証を行うレルムの変更を行う場合
otxadmin > set server.security-service.default-realm=ldap
・運用ユーザの認証を行うレルムの変更を行う場合
otxdmin > set server.admin-service.admin-realm=ldap

3. File レルムの設定を削除(必要がある場合)
delete-auth-realm コマンドを利用して、File レルムの設定を削除します。以下にコマンド例を記載します。ただし 2 の手順を行うだけで、使用するレルムを変更することができるので必須ではありません。delete-auth-realm コマンドの詳しい使い方は、マニュアルの[運用管理コマンドリファレンス]―[運用管理エージェント運用管理コマンド(otxadmin)]の delete-auth-realm を参照してください。

otxadmin > delete-auth-realm filesample

注意:ドメイン作成時に設定されるデフォルトの File レルムである、レルム名 file は削除しないでください。

4. ドメイン再起動
ドメインを再起動することにより、設定が反映されます。
otxadmin > exit
(停止)　${AS_INSTALL}/bin/otxadmin stop-domain domain1
(起動)　${AS_INSTALL}/bin/otxadmin start-domain domain1

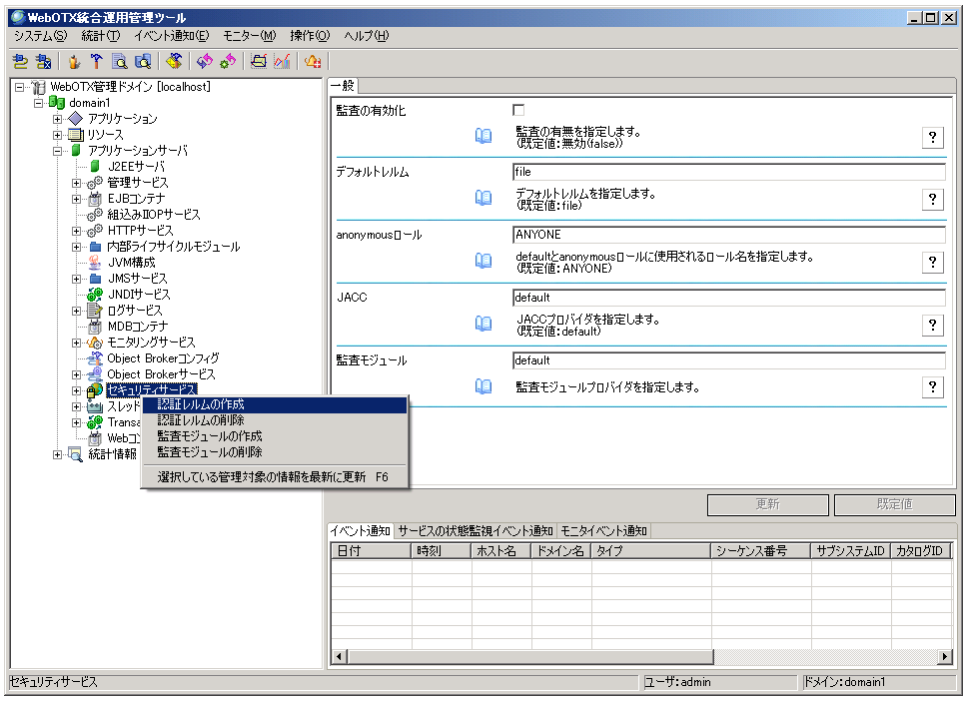
### 3.1.2 統合運用管理ツールから設定

本節では統合運用管理ツールを利用して File レルムの設定を行う方法について説明します。以下の例では設定するドメイン名を domain1、運用ユーザの ID を admin、パスワードを xxxxxx とします。適宜環境に合わせて読み替えてください。

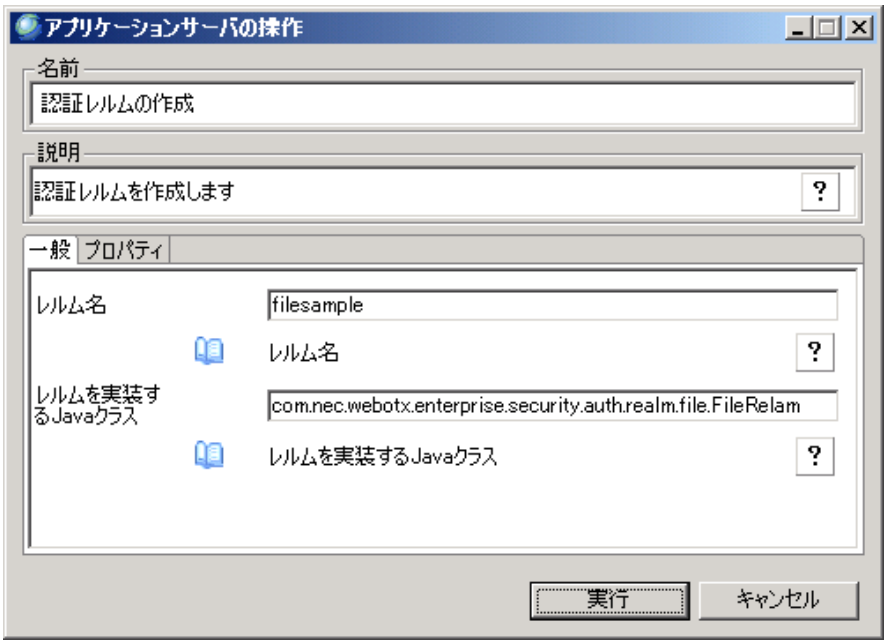
#### 設定手順

1. ドメイン起動
ドメインが起動していない場合はコマンドから起動します。
${AS_INSTALL}/bin/otxadmin start-domain domain1

2. File レルムの設定
統合運用管理ツールを domain1 に接続します。統合運用管理ツールの[domain1]-[アプリケーションサーバ]-[セキュリティサービス]を右クリックします。表示されたメニューから[認証レルムの作成]を選択します。

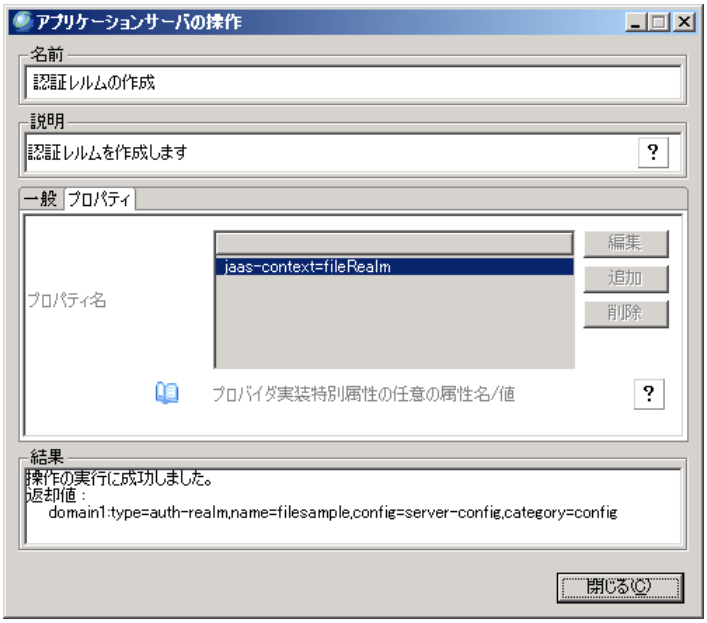



一般タブを選択し、レルム名に任意の名前を入力します。レルム名は任意に設定できます(本例では file とします)。また、クラス名には **com.nec.webotx.enterprise.security.auth.realm.file.FileRealm** を入力してください。




次にプロパティの設定を行います。[プロパティ]タブを選択します。[追加]ボタンを押してプロパティの追加を行います。[プロパティ名の追加]ダイアログが表示されるので、「プロパティ名=値」の形式で入力を行ってください。入力が完了した場合は[OK]ボタンを押します。
設定するプロパティの一覧については 3.1.3 節を参照してください。

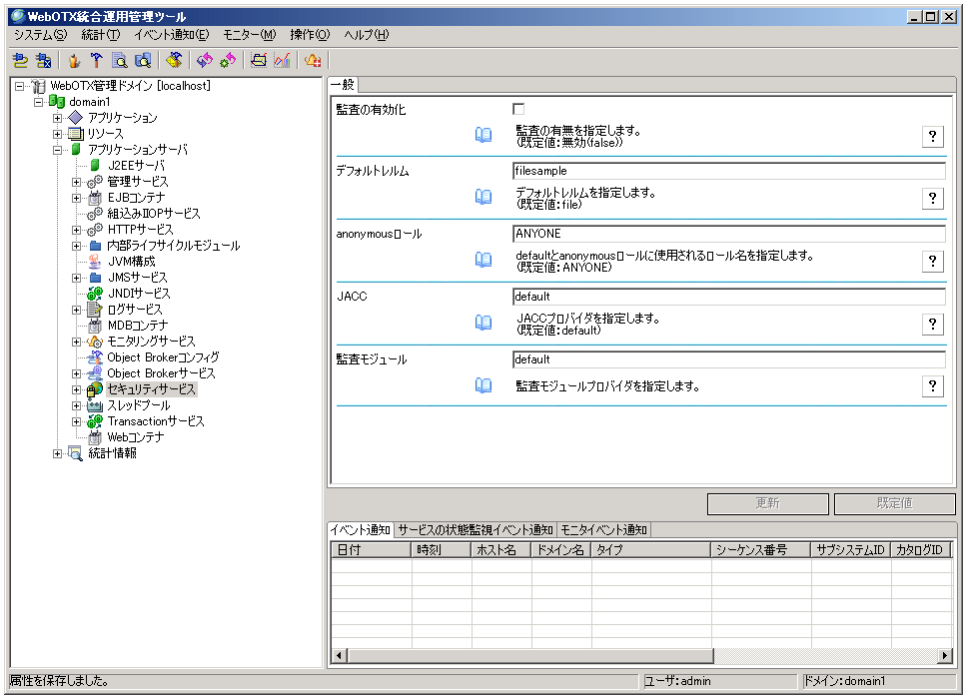
プロパティの設定が終わったら[実行]ボタンを押して、レルムの作成を行います。




3. 使用するレルムの変更

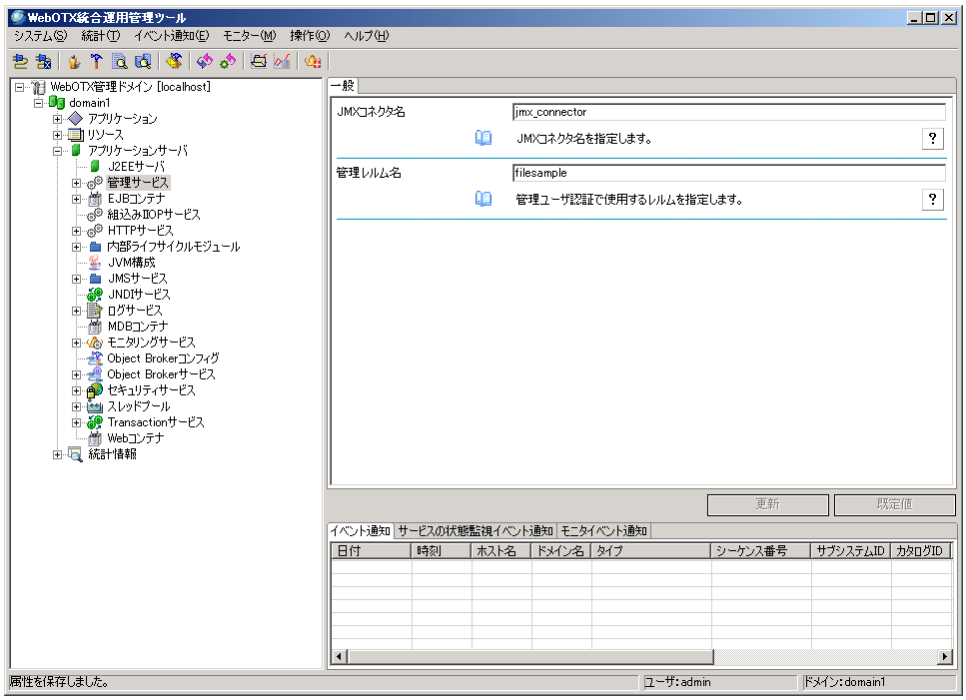
・AP ユーザの認証に使用するレルムを変更する場合

使用するレルムの変更を行います。[domain1]-[アプリケーションサーバ]-[セキュリティサービス]ををクリックします。デフォルトレルムの値を 2 のレルム名で指定した名前(本例では filesample)に変更し、[更新]ボタンを押します。




・運用ユーザの認証を行うレルムの変更を行う場合

[domain1]-[アプリケーションサーバ]-[管理サービス]をクリックします。[管理レルム名]を 2 で指定した名前(本例では filesample)に変更し、[更新]ボタンを押します。

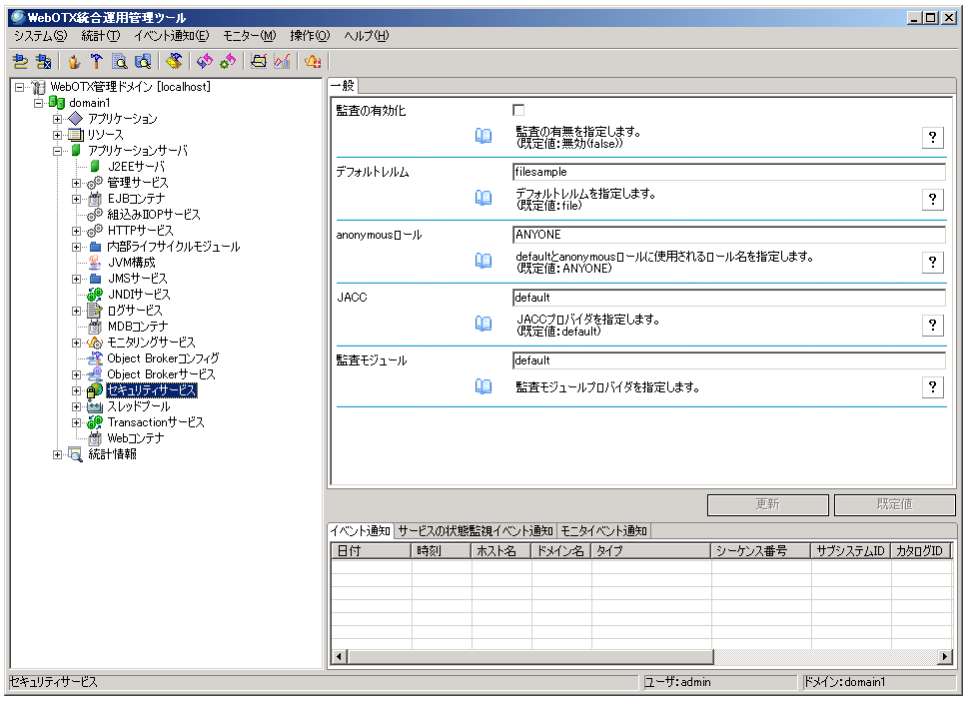



4. ドメイン再起動
   2,3 の変更を反映させるため、ドメインの再起動をおこなってください。以下のコマンドから行います。
   (停止) ${AS_INSTALL}/bin/otxadmin stop-domain domain1
   (起動) ${AS_INSTALL}/bin/otxadmin start-domain domain1

## 削除手順

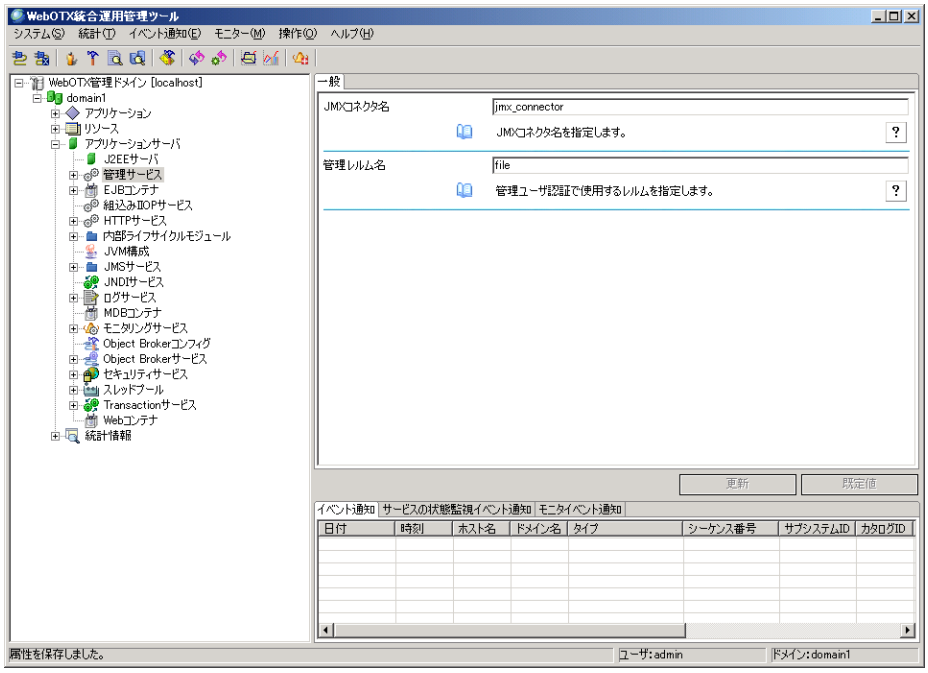
1. ドメイン起動
   ドメインが起動していない場合はドメインを起動します。
   ${AS_INSTALL}/bin/otxadmin start-domain domain1

2. 使用するレルムの変更
   削除を行うレルムをデフォルトレルムに設定していると、削除を行うことができません。まず、使用するレルムを変更します。
   ・AP ユーザの認証に使用するレルムを変更する場合
   使用するレルムの変更を行います。[domain1]-[アプリケーションサーバ]-[セキュリティサービス]ををクリックします。デフォルトレルムの値を作成手順の 2 でレルム名で指定した名前以外(本例では ldap に変更)に変更し、[更新]ボタンを押します。



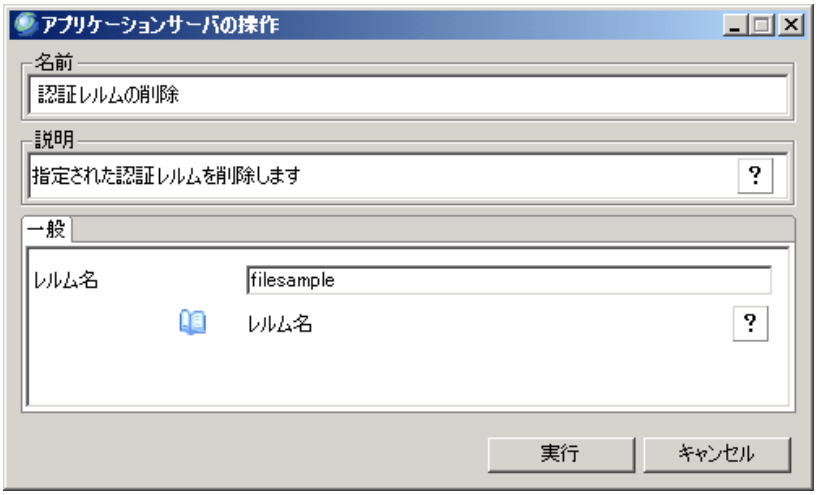

・運用ユーザの認証を行うレルムの変更を行う場合

[domain1]-[アプリケーションサーバ]-[管理サービス]をクリックします。[管理レルム名]に作成手順の 2 で指定した名前以外(本例では ldap に変更)に変更し、[更新]ボタンを押します。




3. レルムの削除(必要がある場合)

2 の設定を行うことで使用するレルムを変更することができます。レルムの設定を完全に削除する場合は次の手順を行ってください。[domain1]-[アプリケーションサーバ]-[セキュリティサービス]を右クリックし、[認証レルムの削除]を選択してください。レルム名に削除するレルムの名前(本例では filesample)を入力し、[実行]ボタンをおしてください。




4. ドメイン再起動
   設定を反映するためにドメインの再起動をおこなってください。
   (停止) ${AS_INSTALL}/bin/otxadmin stop-domain domain1
   (起動) ${AS_INSTALL}/bin/otxadmin start-domain domain1

### 3.1.3 File レルムで設定可能なオプション一覧

create-auth-realm コマンドの property オプションで指定するプロパティについて説明します。File レルムでは以下のオプションを必ず設定してください。

- 必須オプション

File レルムの設定では以下のプロパティが必須となります。

| プロパティ名 | 説明 | 値 |
|---|---|---|
| file | ユーザ情報が格納されている keyfile の完全パスおよび keyfile の名前 | ${INSTANCE_ROOT}/config/keyfile (keyfile の配置箇所、名前を変更した場合は適宜上記の値を変更してください。) |
| jaas-context | このレルムに使用するログインモジュールタイプ | **fileRealm** |

## 3.2 LDAP レルム

LDAP レルムの設定方法について説明します。LDAP レルムの設定は、運用管理コマンド、または統合運用管理ツールから行います。

### 3.2.1 運用管理コマンドから設定

本節では運用管理コマンド(otxadmin コマンド)を利用して LDAP レルムの設定を行う方法について説明します。以下の例では設定するドメイン名を domain1、運用ユーザの ID を admin、パスワードを xxxxxx とします。適宜環境に合わせて読み替えてください。

#### 設定手順

1. ドメイン起動
   ドメインが起動していない場合は起動します。
   ${AS_INSTALL}/bin/otxadmin start-domain domain1

2. LDAP レルムの設定
create-auth-realm コマンドを利用し、LDAP レルムの設定を行います。以下にコマンド例を記載します。create-auth-realm コマンドの詳しい使い方はマニュアルの[運用管理コマンドリファレンス]―[運用管理エージェント運用管理コマンド(otxadmin)]の create-auth-realm を参照してください。

```
${AS_INSTALL}/bin/otxadmin
otxadmin > login --user admin --password xxxxxx --port 6212
otxadmin > create-auth-realm
--classname com.nec.webotx.enterprise.security.auth.realm.ldap.LDAPRealm
--property "directory=ldap¥://localhost¥:389:base-dn=c¥=JP:jaas-context=ldapRealm" ldap
```

上記の例の¥は Unix/Linux 環境ではバックスラッシュに読み替えてください。

- 注意：classname オプションで指定する値は必ず以下の値にしてください。
  **com.nec.webotx.enterprise.security.auth.realm.ldap.LDAPRealm**

なお、property オプションで指定する項目は 3.2.3 節の LDAP レルムで設定可能なオプション一覧を参照してください。

3. 使用するレルムの指定
・AP ユーザの認証を行うレルムの変更を行う場合
otxadmin > set server.security-service.default-realm=ldap
・WebOTX 運用ユーザの認証を行うレルムの変更を行う場合
otxadmin > set server.admin-service.admin-realm=ldap

4. ドメインの再起動
ドメインを再起動することにより、設定が反映されます。
otxadmin > exit
(停止)　${AS_INSTALL}/bin/otxadmin stop-domain domain1
(起動)　${AS_INSTALL}/bin/otxadmin start-domain domain1

## 削除手順

1. ドメイン起動
ドメインが起動してない場合は起動します。
${AS_INSTALL}/bin/otxadmin start-domain domain1

2. 使用するレルムの変更
削除するレルムを security-service.default-realm に設定していると削除を行うことができません。そのため、使用するレルムを変更する必要があります。以下にレルム名が file というレルムを使用する例を記載します。適宜環境に合わせて変更してください。

```
{AS_INSTALL}/bin/otxadmin
otxadmin > login --user admin --password xxxxxx
```

・AP ユーザの認証を行うレルムの変更を行う場合
otxadmin > set server.security-service.default-realm=file
・WebOTX 運用ユーザの認証を行うレルムの変更を行う場合
otxadmin > set server.admin-service.admin-realm=file

3. LDAP レルムの設定を削除(必要がある場合)
delete-auth-realm コマンドを利用して、LDAP レルムの設定を削除します。以下にコマンド例を記載します。ただし 2 の手順を行うだけで、使用するレルムを変更することができるので必須ではありません。delete-auth-realm コマンドの詳しい使い方は、マニュアルの[運用管理コマンドリファレンス]―[運用管理エージェント運用管理コマンド(otxadmin)]の delete-auth-realm を参照してください。

```
otxadmin > delete-auth-realm ldap
```

4. ドメイン再起動
ドメインを再起動することにより、設定が反映されます。
otxadmin > exit

（停止）　${AS_INSTALL}/bin/otxadmin stop-domain domain1
（起動）　${AS_INSTALL}/bin/otxadmin start-domain domain1

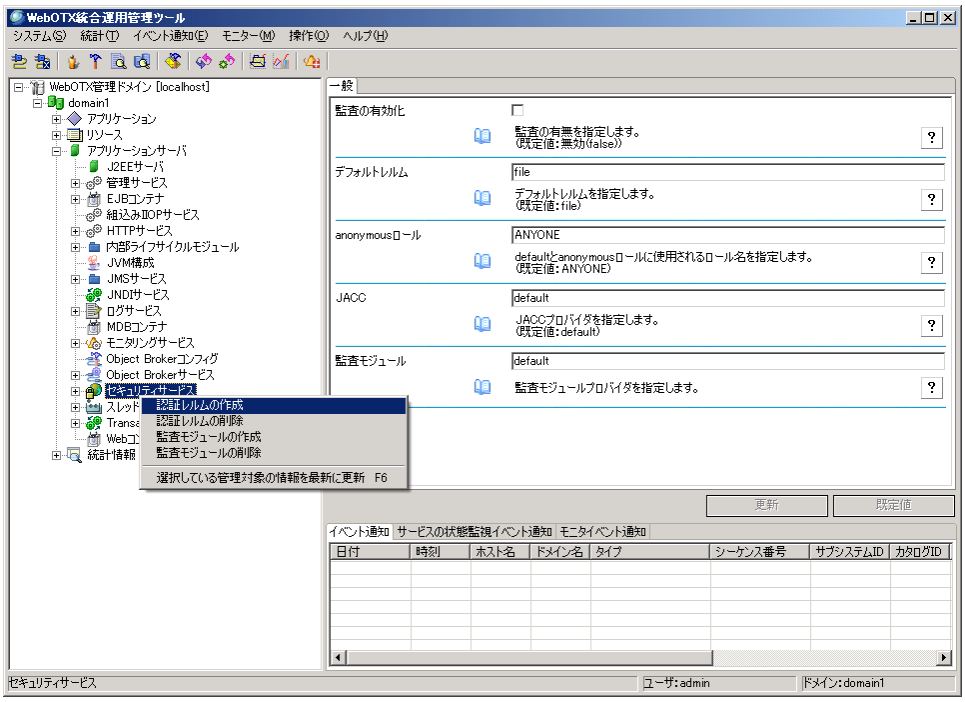
### 3.2.2 統合運用管理ツールから設定

本節では統合運用管理ツールを利用して LDAP レルムの設定を行う方法について説明します。以下の例では設定するドメイン名を domain1、運用ユーザの ID を admin、パスワードを xxxxxx とします。適宜環境に合わせて読み替えてください。

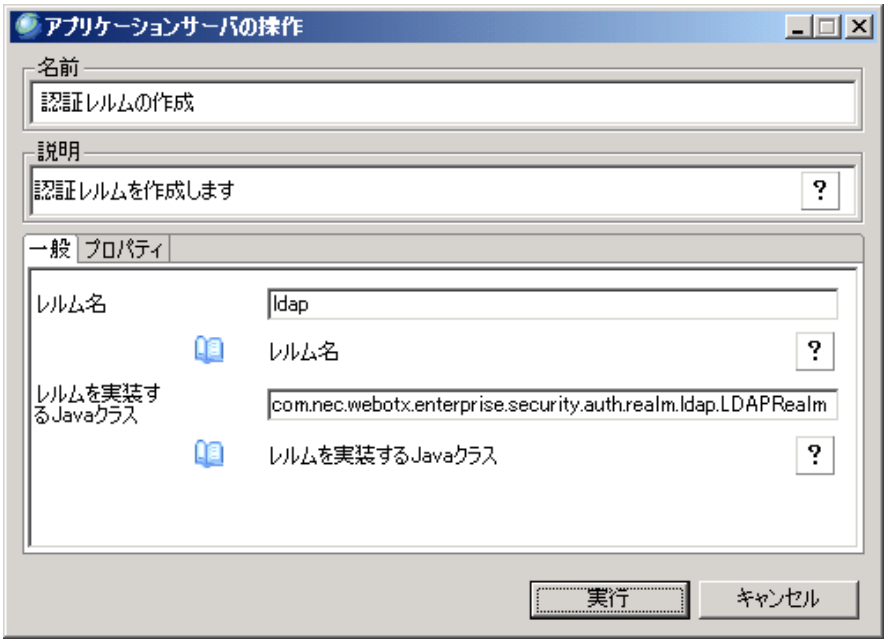
#### 設定手順

1. ドメイン起動
   ドメインが起動していない場合はコマンドから起動します。
   ${AS_INSTALL}/bin/otxadmin start-domain domain1

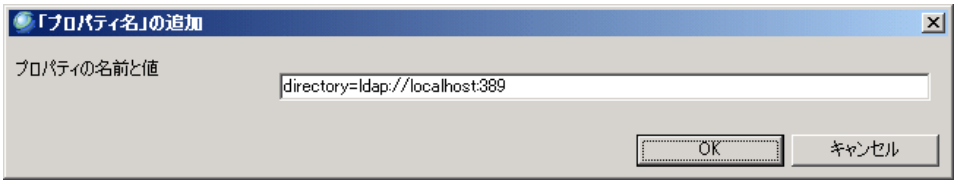
2. LDAP レルムの設定
   統合運用管理ツールを domain1 に接続します。統合運用管理ツールの[domain1]-[アプリケーションサーバ]-[セキュリティサービス]を右クリックします。表示されたメニューから認証レルムの作成を選択します。



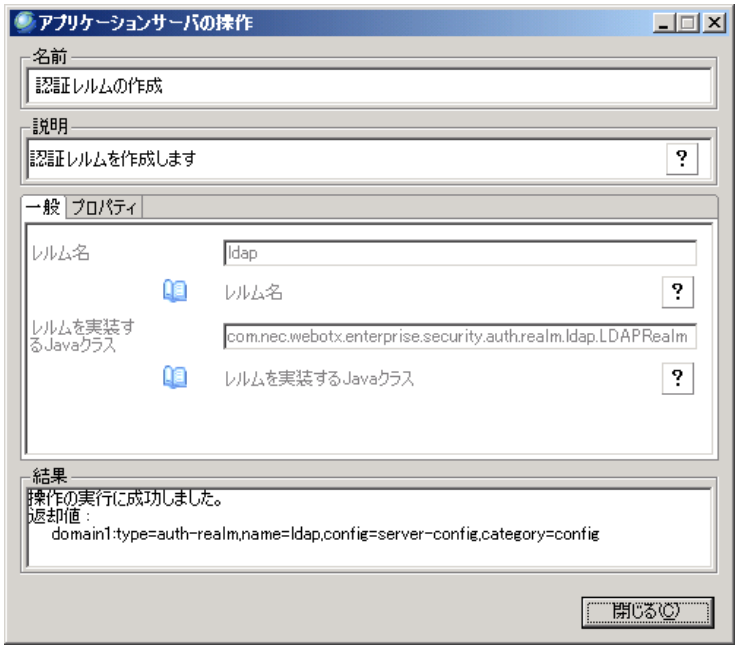

3. 一般タブを選択し、レルム名に任意の名前を入力します。レルム名は任意に設定できます。また、クラス名には **com.nec.webotx.enterprise.security.auth.realm.ldap.LDAPRealm** を入力してください。




4. 追加ボタンを押してプロパティの追加を行います。[プロパティ名の追加]ダイアログが表示されるので、「プロパティ名=値」の形式で入力を行ってください。入力が完了した場合は OK ボタンを押します。プロパティの設定一覧は、3.2.3 節に記載してあります。必須オプションは必ず指定してください。

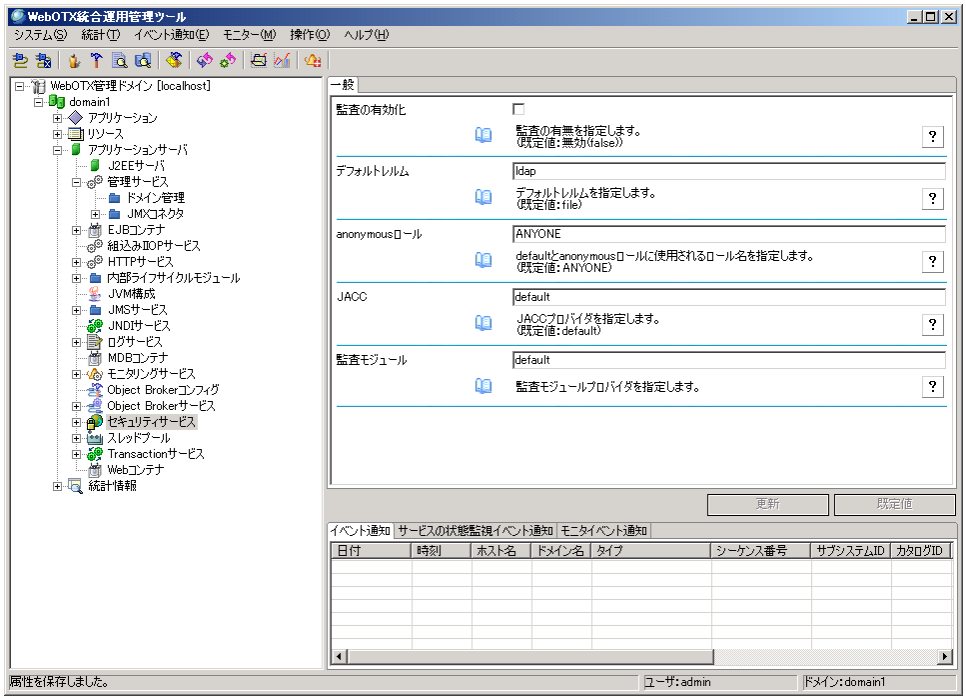



プロパティの設定が終わったら[実行]ボタンを押して、レルムの作成を行います。

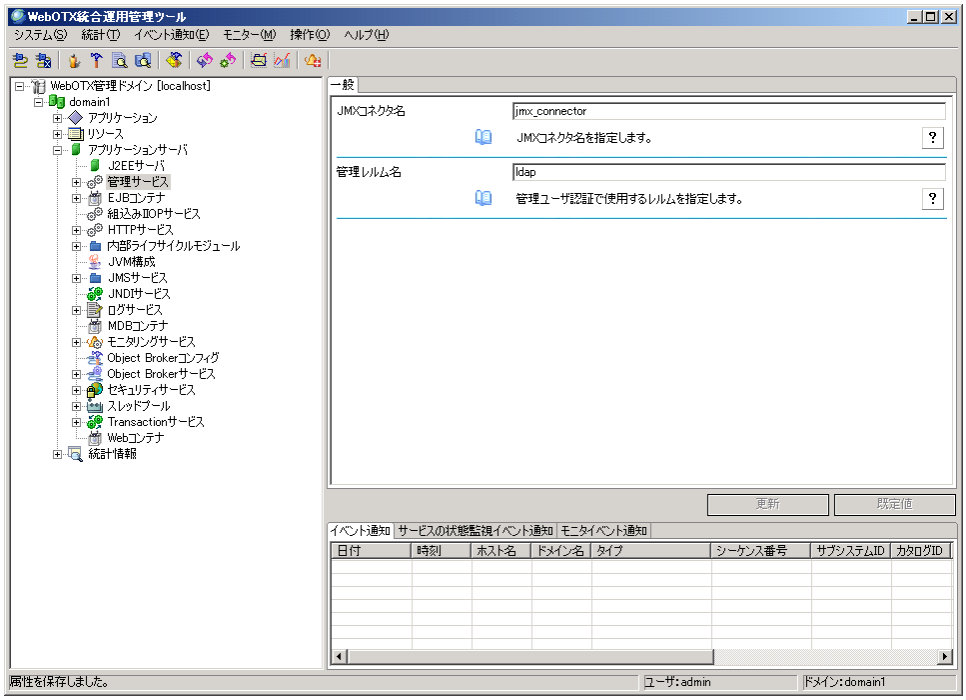



5. 使用するレルムの変更

・AP ユーザの認証を行うレルムの変更を行う場合
使用するレルムの変更を行います。[domain1]-[アプリケーションサーバ]-[セキュリティサービス]ををクリックします。適当な名前(本例では ldap)に変更し、[更新]ボタンを押します。




・運用ユーザの認証を行うレルムの変更を行う場合
[domain1]-[アプリケーションサーバ]-[管理サービス]をクリックします。[管理レルム名]に 3 で指定した名前(本例では ldap)に変更し、[更新]ボタンを押します。

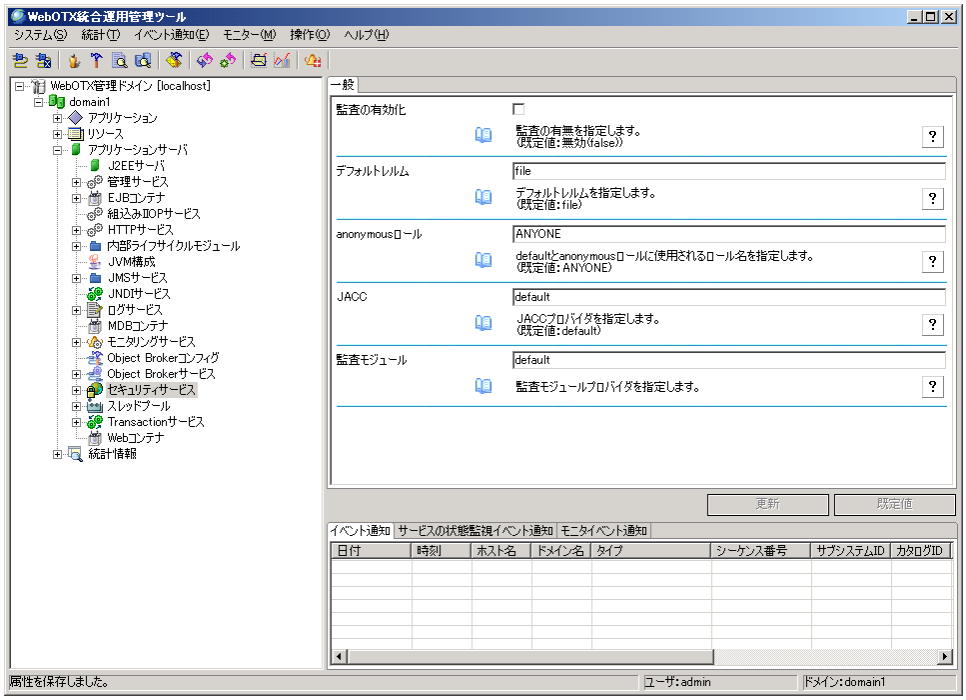



6. ドメイン再起動
3～5 の変更を反映させるため、ドメインの再起動をおこなってください。
(停止) ${AS_INSTALL}/bin/otxadmin stop-domain domain1
(起動) ${AS_INSTALL}/bin/otxadmin start-domain domain1

## 削除手順

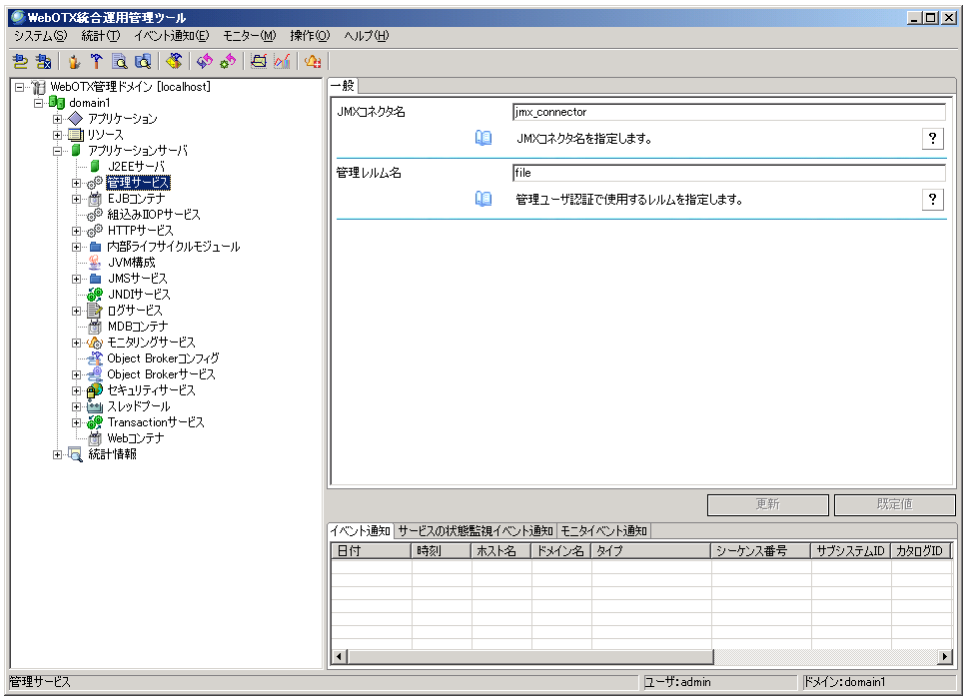
1. ドメイン起動
   ドメインが起動していない場合はドメインを起動します。
   ${AS_INSTALL}/bin/otxadmin start-domain domain1

2. 使用するレルムの変更
   削除を行うレルムを使用する設定になっていると、削除を行うことができません。まず、使用するレルムを変更します。
   ・AP ユーザの認証に使用するレルムを変更する場合
   使用するレルムの変更を行います。[domain1]-[アプリケーションサーバ]-[セキュリティサービス]ををクリックします。デフォルトレルムの値を適当な名前(本例では file)に変更し、[更新]ボタンを押します。

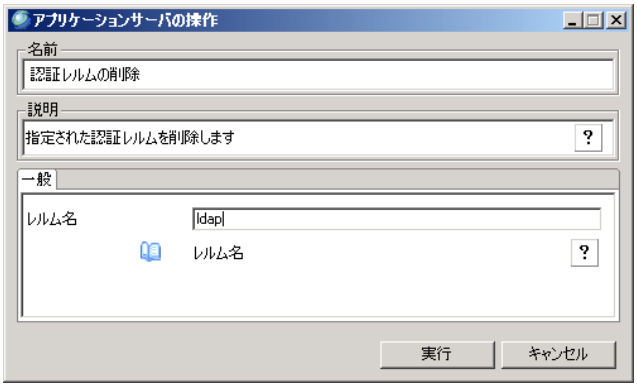



・運用ユーザの認証を行うレルムの変更を行う場合

[domain1]-[アプリケーションサーバ]-[管理サービス]をクリックします。[管理レルム名]に 2 で指定した名前(本例では file)に変更し、[更新]ボタンを押します。




3. レルムの削除(必要がある場合)
   2 の設定を行うことで使用するレルムを変更することができます。レルムの設定を完全に削除する場合は次の手順を行ってください。[domain1]-[アプリケーションサーバ]-[セキュリティサービス]を右クリックし、[認証レルムの削除]を選択してください。レルム名に削除する作成手順 2 で指定したレルムの名前(本例では ldap)を入力し、[実行]ボタンをおしてください。




4. ドメイン再起動
   設定を反映するためにドメインの再起動をおこなってください。
   (停止) ${AS_INSTALL}/bin/otxadmin stop-domain domain1
   (起動) ${AS_INSTALL}/bin/otxadmin start-domain domain1

### 3.2.3 LDAP レルムで設定可能なオプション一覧

create-auth-realm コマンドの property オプションで指定するプロパティについて説明します。LDAP レルムの設定では、必須オプションと、任意に設定するオプションがあります。

- 必須オプション

LDAP レルムの設定では以下のプロパティが必須となります。

| プロパティ名 | 説明 | 指定する値 |
|---|---|---|

| | | |
|---|---|---|
| base-dn | ユーザ情報が格納されているエントリを DN 形式で指定します。 | 例：dc=users,dc=domains, dc=webotx,o=NEC, c=JP |
| directory | LDAP サーバが動作しているホスト名を LDAP URL 形式で指定します。 | 以下のように指定してください。<br>ldap://hostname:port<br>例：ldap://localhost:389 |
| jaas-context | 使用するログインモジュールのタイプです。 | **ldapRealm** |

- 任意オプション

ldapレルムの設定では以下のプロパティを任意に設定することができます。設定しない場合はデフォルトの値が自動的に設定されます。

| プロパティ名 | 説明 | 既定値 |
|---|---|---|
| search-filter | ユーザ検索に使用されるフィルタ。 | uid=%s<br>(%s はシステム内部で指定したユーザ名に変換されます。) |
| group-base-dn | グループの情報が格納されているエントリを DN 形式で指定します。 | base-dn と同じです。 |
| group-search-filter | グループ検索に使用するフィルタです。 | uniquemember=%d<br>(%d はシステム内部で指定した DN に変換されます。) |
| group-target | グループ名のエントリを含む属性名 | CN |
| search-bind-dn | search-filter 検索を実行するために必要なオプション DN です。 | なし |
| search-bind-password | search-bind-dn で指定した DN のパスワードです。*1 | なし |
| authentification | LDAP サーバとの認証方式を指定します。利用できる認証方式は、simple(平文認証)、CRAM-MD5、DIGEST-MD5 です。 | simple |

DN 形式、CN 等 LDAP に関する表現については EDS のマニュアルを参照してください。

*1 V6.50.02 より、パスワードの暗号化を行うことができるようになりました。暗号化の方法については、マニュアル「運用編(コンフィグレーション) 3.2 章エージェント設定項目一覧」を参照してください。

## 3.3 JDBC レルム

JDBCレルムの設定方法について説明します。 JDBCレルムの設定は、運用管理コマンド、または統合運用管理ツールから行います。

### 3.3.1 運用管理コマンドから設定

本節では運用管理コマンド(otxadminコマンド)を利用してJDBCレルムの設定を行う方法について説明します。以下の例では設定するドメイン名を domain1、運用ユーザの ID を admin、パスワードを xxxxxx とし、データベースにはOracleを使用します。適宜環境に合わせて読み替えてください。

#### 設定手順

1. ドメイン起動
   ドメインが起動していない場合は起動します。
   ${AS_INSTALL}/bin/otxadmin start-domain domain1

2. JDBC レルムの設定
   create-auth-realm コマンドを利用し、JDBC レルムの設定を行います。以下にコマンド例を記載します。create-auth-realm コマンドの詳しい使い方はマニュアルの[運用管理コマンドリファレンス]―[運用管理エージェント運用管理コマンド(otxadmin)]の create-auth-realm を参照してください。

   {AS_INSTALL}/bin/otxadmin

otxadmin > login --user admin --password xxxxxx --port 6212
otxadmin > create-auth-realm --classname
com.nec.webotx.enterprise.security.auth.realm.jdbc.JDBCRealm --property
"driverName=oracle.jdbc.driver.OracleDriver:jaas-context=JDBCRealm

:connectionURL=jdbc¥:oracle¥:thin¥:@ntserver¥:1521¥:ORCL:connectionName=scott

:connectionPassword=tiger:userTable=jdbc_user:userNameCol=userid:userCredCol=passwd

:userRoleTable=jdbc_role:roleNameCol=role" JDBCrealm

- 注意：classname オプションで指定する値は必ず以下の値にしてください。
  **com.nec.webotx.enterprise.security.auth.realm.jdbc.JDBCRealm**

なお、property オプションで指定する項目は 3.3.3 節の JDBC レルムで設定可能なオプション一覧を参照してください。

3. 使用するレルムの指定
・AP ユーザの認証を行うレルムの変更を行う場合
otxadmin > set server.security-service.default-realm=JDBCrealm
・WebOTX 運用ユーザの認証を行うレルムの変更を行う場合
otxadmin > set server.admin-service.admin-realm= JDBCrealm

4. JDBC ドライバの配置
JDBCドライバをディレクトリ ${INSTANCE_ROOT}/lib/ext に置く、もしくは ドメインのクラスパスに追加します。 JDBC データソースを利用する場合は、ドメイン起動後に運用編コンフィグレーション「9.JDBC データソースに関する設定」も参照して、設定してください。

5. ドメインの再起動
ドメインを再起動することにより、設定が反映されます。
otxadmin > exit
(停止) ${AS_INSTALL}/bin/otxadmin stop-domain domain1
(起動) ${AS_INSTALL}/bin/otxadmin start-domain domain1

## 削除手順

1. ドメイン起動
ドメインが起動してない場合は起動します。
${AS_INSTALL}/bin/otxadmin start-domain domain1

2. 使用するレルムの変更
削除するレルムを security-service.default-realm に設定していると削除を行うことができません。そのため、使用するレルムを変更する必要があります。以下にレルム名が file というレルムを使用する例を記載します。適宜環境に合わせて変更してください。

{AS_INSTALL}/bin/otxadmin
otxadmin > login --user admin --password xxxxxx
・AP ユーザの認証を行うレルムの変更を行う場合
otxadmin > set server.security-service.default-realm=file
・WebOTX 運用ユーザの認証を行うレルムの変更を行う場合
otxadmin > set server.admin-service.admin-realm=file

3. JDBCレルムの設定を削除(必要がある場合)
delete-auth-realm コマンドを利用して、JDBCレルムの設定を削除します。以下にコマンド例を記載します。ただし 2 の手順を行うだけで、使用するレルムを変更することがでるので必須ではありません。delete-auth-realm コマンドの詳しい使い方は、マニュアルの[運用管理コマンドリファレンス]—[運用管理エージェント運用管理コマンド(otxadmin)]の delete-auth-realm を参照してください。

otxadmin > delete-auth-realm JDBCrealm

4. ドメイン再起動
ドメインを再起動することにより、設定が反映されます。

otxadmin > exit

（停止）　${AS_INSTALL}/bin/otxadmin stop-domain domain1
（起動）　${AS_INSTALL}/bin/otxadmin start-domain domain1

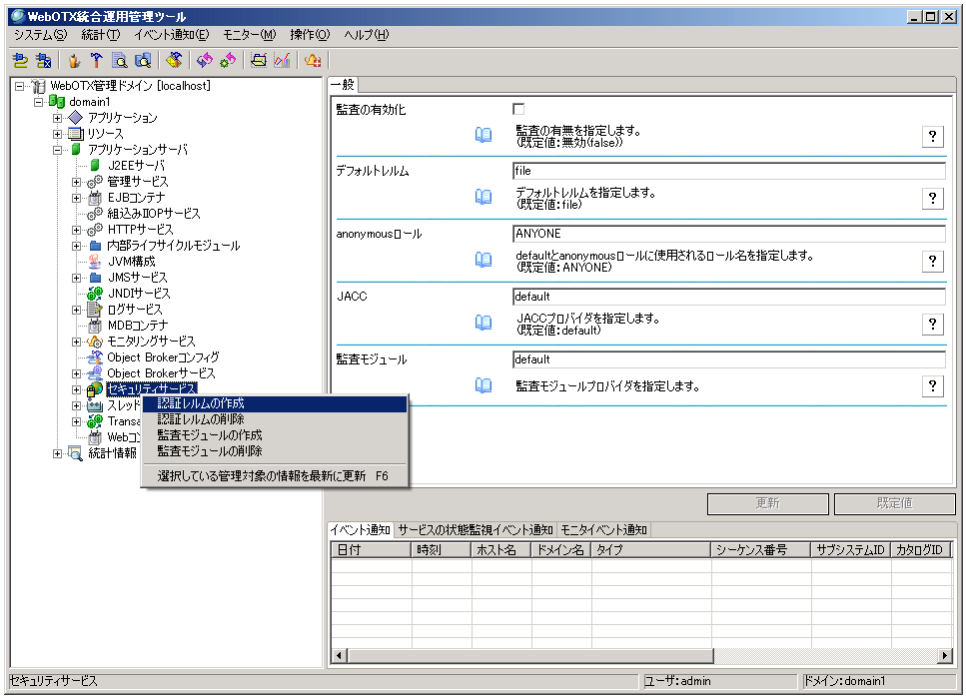
## 3.3.2 統合運用管理ツールから設定

本節では統合運用管理ツールを利用して JDBC レルムの設定を行う方法について説明します。以下の例では設定するドメイン名を domain1、運用ユーザの ID を admin、パスワードを xxxxxx とします。適宜環境に合わせて読み替えてください。

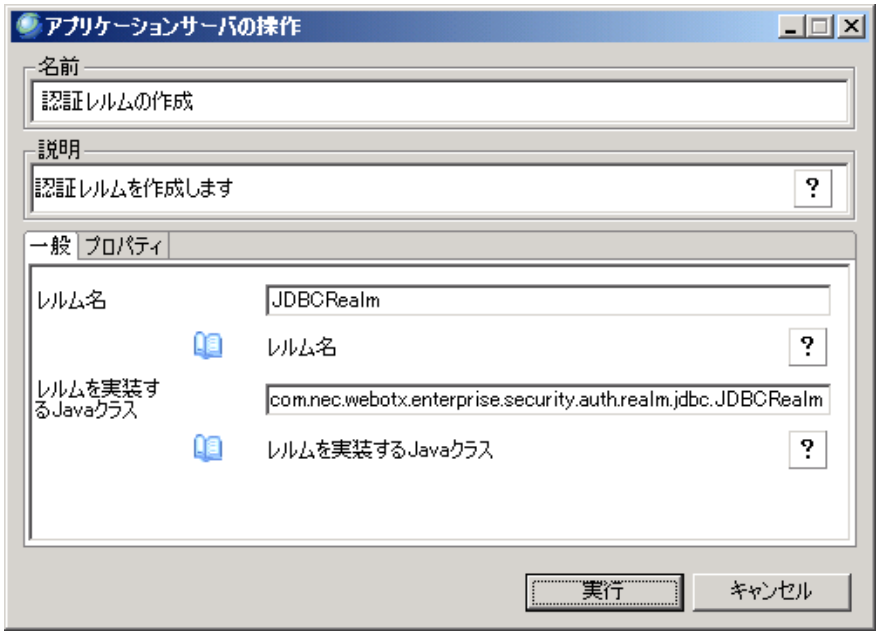
### 設定手順

1. ドメイン起動
   ドメインが起動していない場合はコマンドから起動します。
   ${AS_INSTALL}/bin/otxadmin start-domain domain1

2. JDBC レルムの設定
   統合運用管理ツールを domain1 に接続します。統合運用管理ツールの[domain1]-[アプリケーションサーバ]を右クリックします。表示されたメニューから認証レルムの作成を選択します。

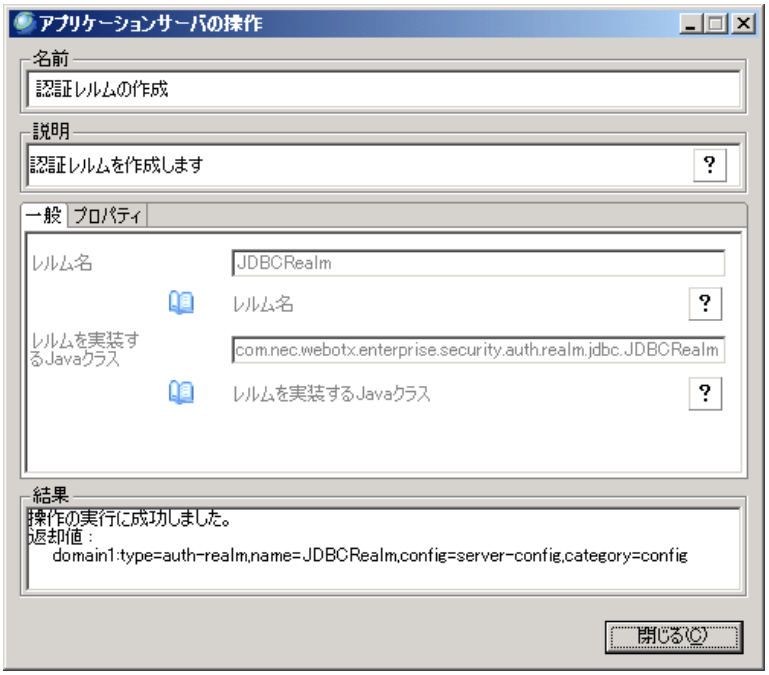



3. 一般タブを選択し、レルム名に任意の名前を入力します。レルム名は任意に設定できます。また、クラス名には **com.nec.webotx.enterprise.security.auth.realm.jdbc.JDBCRealm** を入力してください。




4. 追加ボタンを押してプロパティの追加を行います。[プロパティ名の追加]ダイアログが表示されるので、「プロパティ名=値」の形式で入力を行ってください。入力が完了した場合は OK ボタンを押します。プロパティの設定一覧は、3.3.3 節に記載してあります。必須オプションは必ず指定してください。

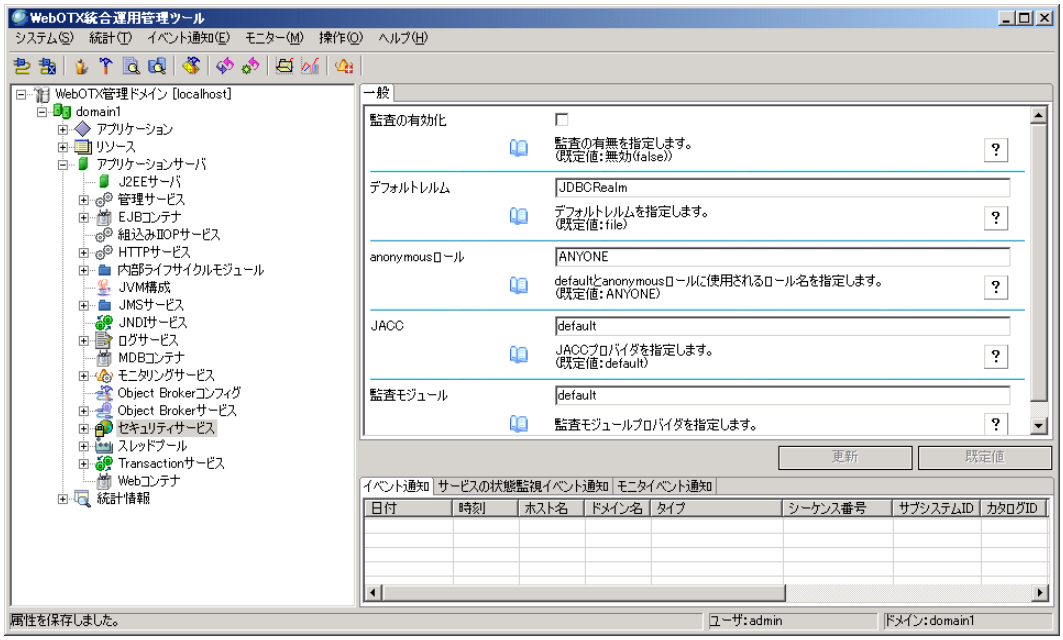

プロパティの設定が終わったら[実行]ボタンを押して、レルムの作成を行います。



5. 使用するレルムの変更

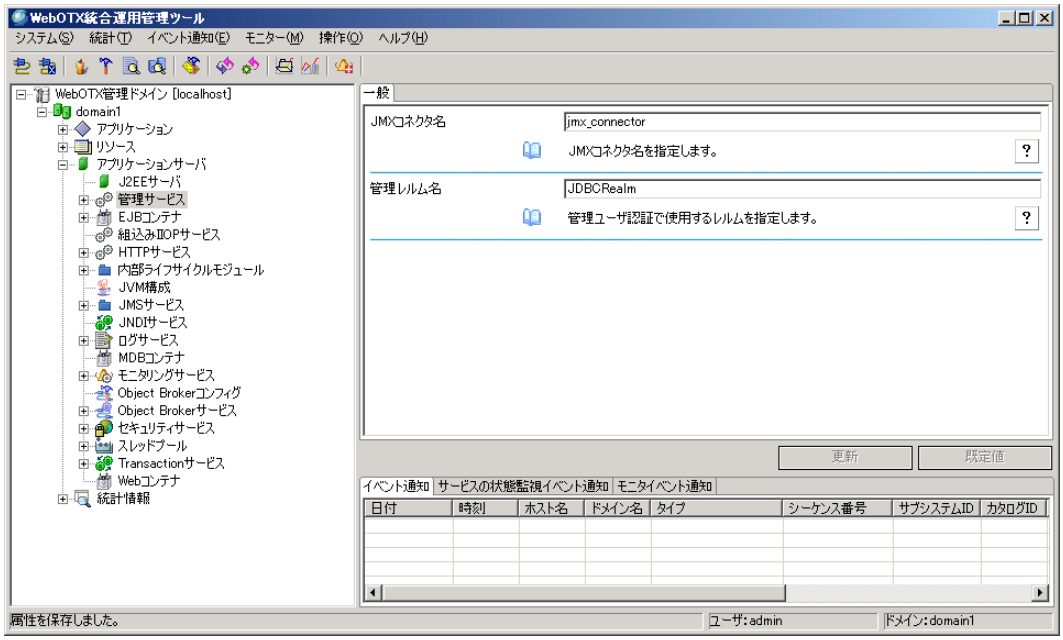
・AP ユーザの認証を行うレルムの変更を行う場合

使用するレルムの変更を行います。[domain1]-[アプリケーションサーバ]-[セキュリティサービス]ををクリックします。デフォルトレルムの値を 2 のレルム名で指定した名前(本例では JDBCrealm)に変更し、[更新]ボタンを押します。




・運用ユーザの認証を行うレルムの変更を行う場合

[domain1]-[アプリケーションサーバ]-[管理サービス]をクリックします。[管理レルム名]に 3 で指定した名前(本例では JDBCrealm)に変更し、[更新]ボタンを押します。




6. ドメイン再起動

2,3 の変更を反映させるため、ドメインの再起動をおこなってください。

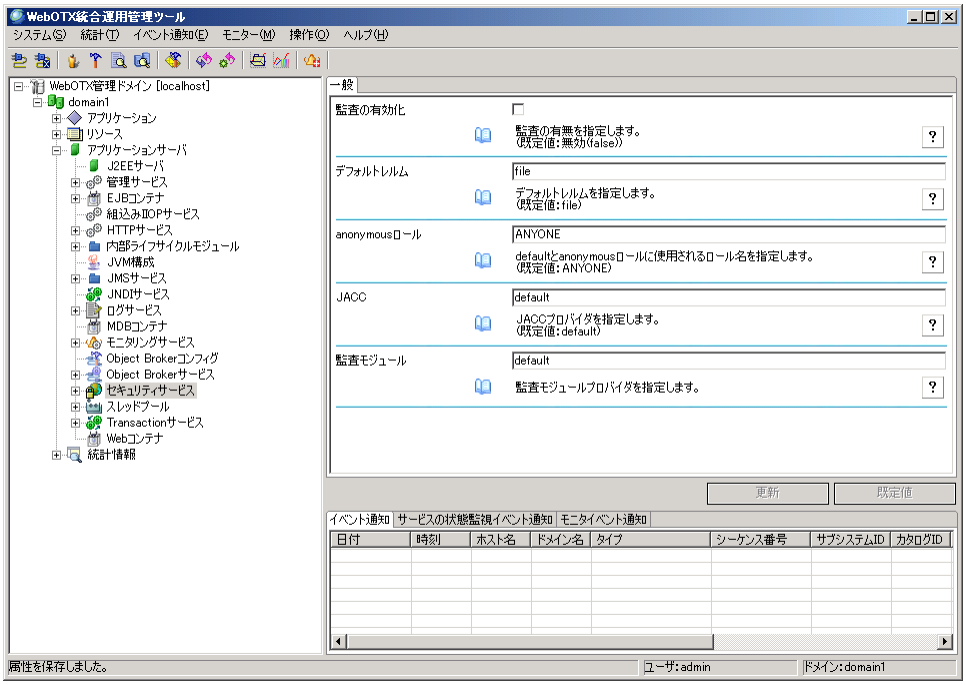
(停止) ${AS_INSTALL}/bin/otxadmin stop-domain domain1

(起動) ${AS_INSTALL}/bin/otxadmin start-domain domain1

## 削除手順

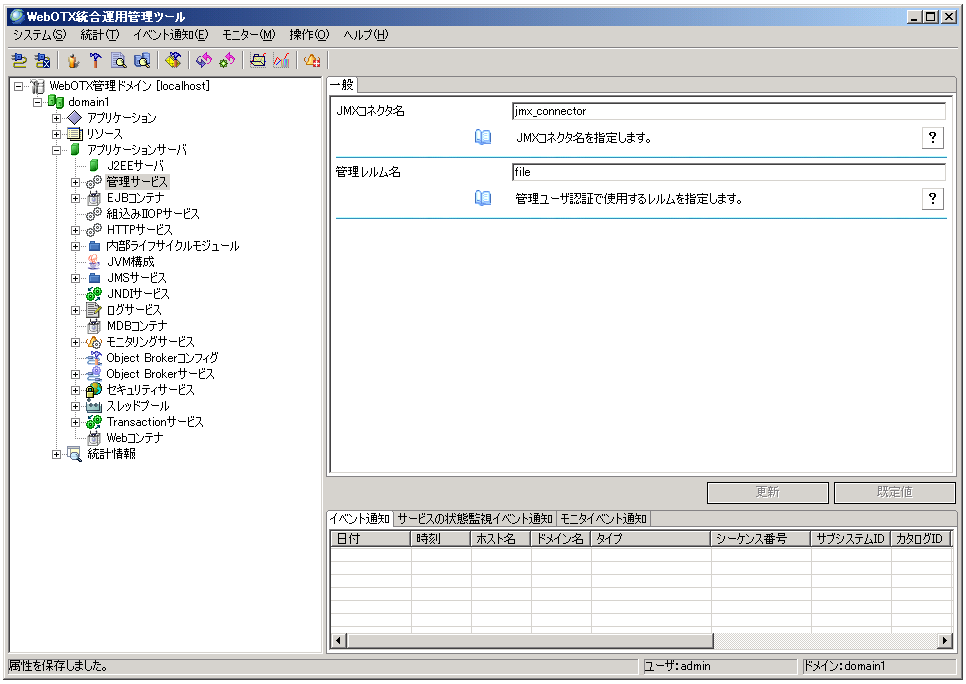
1. ドメイン起動
   ドメインが起動していない場合はドメインを起動します。
   ${AS_INSTALL}/bin/otxadmin start-domain domain1

2. 使用するレルムの変更
   削除を行うレルムを使用する設定になっていると、削除を行うことができません。まず、使用するレルムを変更します。
   ・AP ユーザの認証に使用するレルムを変更する場合
   使用するレルムの変更を行います。[domain1]-[アプリケーションサーバ]-[セキュリティサービス]ををクリックします。デフォルトレルムの値を適当な名前(本例では file)に変更し、[更新]ボタンを押します。

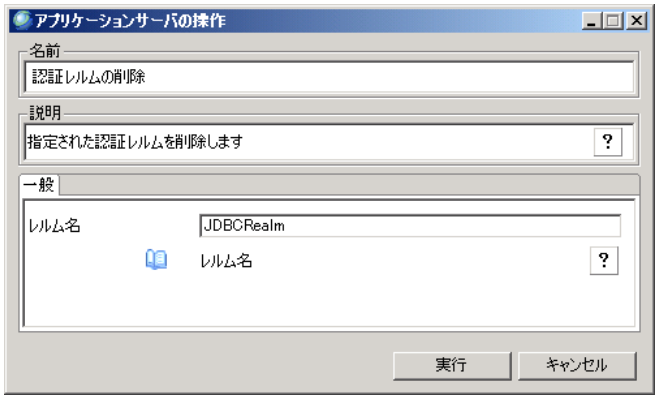



・運用ユーザの認証を行うレルムの変更を行う場合

[domain1]-[アプリケーションサーバ]-[管理サービス]をクリックします。[管理レルム名]に 2 で指定した名前(本例では file)に変更し、[更新]ボタンを押します。




3. レルムの削除(必要がある場合)
   2 の設定を行うことで使用するレルムを変更することができます。レルムの設定を完全に削除する場合は次の手順を行ってください。[domain1]-[アプリケーションサーバ]-[セキュリティサービス]を右クリックし、[認証レルムの削除]を選択してください。レルム名に削除する作成手順 2 で指定したレルムの名前(本例では JDBCrealm)を入力し、[実行]ボタンをおしてください。




4. ドメイン再起動
   設定を反映するためにドメインの再起動を行ってください。
   (停止) ${AS_INSTALL}/bin/otxadmin stop-domain domain1
   (起動) ${AS_INSTALL}/bin/otxadmin start-domain domain1

### 3.3.3 JDBC レルムで設定可能なオプション一覧

create-auth-realm コマンドの property オプションで指定するプロパティについて説明します。JDBC レルムの設定では、必須オプションと、任意に設定するオプションがあります。

- 必須オプション

JDBC レルムの設定では以下のプロパティが必須となります。 JDBC ドライバと JDBC データソースのど

ちらを使うかで必須オプションが変わります。また、両方の設定がある場合は、JDBC データソースの設定が優先されます。

| プロパティ名 | 説明 | 指定する値 |
|---|---|---|
| jaas-context | 使用するログインモジュールのタイプです。 | JDBCRealm |
| JDBCdatasource | 使用する JDBC データソース名を指定します。 JDBC ドライバを指定する設定より優先して使用します。<br>*JDBC ドライバを指定する際は不要です。 | JNDI 名で指定してください。 |
| driverName | データベース接続時に使用する JDBC ドライバ(完全修飾名)を指定します。<br>* JDBC データソースを指定する際は不要です。 | 以下のように指定してください。<br>例:oracle.jdbc.driver.OracleDriver |
| connectionURL | データベースへの接続文字列を指定します。<br>* JDBC データソースを指定する際は不要です。 | 以下のように指定してください。<br>jdbc:<db>:<server>:<port>:databaseName<br>例:<br>jdbc:oracle:thin:@ntserver:1521:ORCL<br>※運用管理コマンドでは":"の前に"¥"を入れます。 |
| connectionName | データベース接続時に使用されるユーザ名を指定します。<br>* JDBC データソースを指定する際は不要です。 | データベースを使用するユーザ名を指定してください。 |
| connectionPassword | データベース接続時に使用されるパスワード<br>* JDBC データソースを指定する際は不要です。 | データベースを使用するユーザのパスワードを指定してください。 |
| userTable | ユーザ情報テーブルの名前 | 例:jdbc_user |
| userNameCol | ユーザ名を格納するフィールドの名前を指定します。 | 例: userid |
| userCredCol | パスワードを格納するフィールドの名前を指定します。 | 例: passwd |
| userRoleTable | ユーザ権限(ロール)情報テーブルの名前を指定します。 | 例: jdbc_role |
| roleNameCol | 権限名(ロール)を格納するフィールドの名前を指定します。 | 例: role |

- 任意オプション

JDBC レルムの設定では以下のプロパティを任意に設定することができます。設定しない場合はデフォルトの値が自動的に設定されます。

| プロパティ名 | 説明 | 既定値 |
|---|---|---|
| digest | データベースに保存するパスワードのダイジェスト方式を指定します。ダイジェスト方式には MD5 、SHA-1 、SHA-256 、SHA-384 、SHA-512 のいずれかを指定することができます。 | NULL<br>(平文を使用) |
| useA1Digest | userCredCol に示されるフィールドに格納される値が、DIGEST 認証専用のダイジェスト値か否かを指定します。<br>※true を指定すると DIGEST 認証専用のレルムとなり、BASIC 認証用には使用できなくなります | true : userCredCol に格納する情報は DIGEST 認証用のダイジェスト値。<br>false(既定値) : userCredCol に格納する情報は平文パスワード。 |
| realmNameCol | 複数の JDBC レルムが 1 つのテーブルを参照する場合に、realm 名を格納するフィールドの名前を指定します。 | 例: realm |

**※digest プロパティを設定すると DIGEST 認証ができなくなります。**

# 4 ユーザ管理

## 4.1 File レルムを使用する場合

本節では、WebOTX 運用ユーザの管理に File レルムを利用する場合の、ユーザの追加、削除の方法について説明します。以下の例では、ドメイン名を domain1、運用ユーザの ID を admin、パスワードを xxxxxx、File レルム名を filesample とします。

### 4.1.1 ユーザの追加、削除

#### 運用管理コマンドを利用する場合

運用管理コマンド(otxadmin コマンド)を利用して、ユーザの追加を行う方法について説明します。

- ユーザの追加

1. ドメイン起動
   ドメインが起動していない場合は起動してください。
   ${AS_INSTALL}/bin/otxadmin start-domain domain1

2. ユーザの追加
   ユーザを追加する場合、create-file-user コマンドを利用します。create-file-user コマンドの詳しい使い方は、[運用管理コマンド(otxadmin)]-[create-file-user]を参照してください。作成するユーザは、ユーザ ID testuser、パスワード userpass、グループ testgrp とします。

   ```
   ${AS_INSTALL}/bin/otxadmin
   otxadmin > login -- user admin --password xxxxxx --port 6212
   otxadmin > create-file-user --userpass admpass --groups testgrp testuser
   ```

   - 注意 1:ユーザ ID に使える文字は、英数字と “-“(ハイフン)、”_”(アンダースコア)になります。文字数の制限はありません。
   - 注意 2:パスワードに使える文字は、英数字と記号が利用できますが、「¥」、「”」文字は利用できません。パスワードを省略することはできません。1 文字以上指定してください。
   - 注意 3:WebOTX 運用ユーザを作成する場合は groups オプションで指定する値は **otxadmin** としてください。
   - 注意 4:domain.xml の jvm-config に com.nec.webotx.admin.password.complexity=true を設定した場合、ユーザのパスワードは 8 文字以上、英数字、大文字小文字を含めなければなりません。

3. ドメイン再起動
   作成したユーザが WebOTX 運用ユーザの場合、設定を反映させるためにドメインを再起動してください。**作成したユーザを AP で利用する場合、ドメインの再起動は必要ありません。**

   ```
   otxadmin > exit
   (停止)  ${AS_INSTALL}/bin/otxadmin stop-domain domain1
   (起動)  ${AS_INSTALL}/bin/otxadmin start-domain domain1
   ```

- ユーザの削除
  ユーザの追加で作成したユーザ testuser を削除する手順を説明します。

1. ドメイン起動
   ドメインが起動していない場合は起動してください。
   ${AS_INSTALL}/bin/otxadmin start-domain domain1

2. ユーザの削除

   ```
   ${AS_INSTALL}/bin/otxadmin
   otxadmin > login --user admin --password admin
   ```

otxadmin > delete-file-user --authrealmname file testuser

3. ドメイン再起動
削除したユーザが WebOTX 運用ユーザの場合、設定を反映させるためにドメインを再起動してください。**削除したユーザを AP で利用される場合、ドメインの再起動は必要ありません。**
otxadmin > exit
(停止)　${AS_INSTALL}/bin/otxadmin stop-domain domain1
(起動)　${AS_INSTALL}/bin/otxadmin start-domain domain1

## 統合運用管理ツールを利用する場合

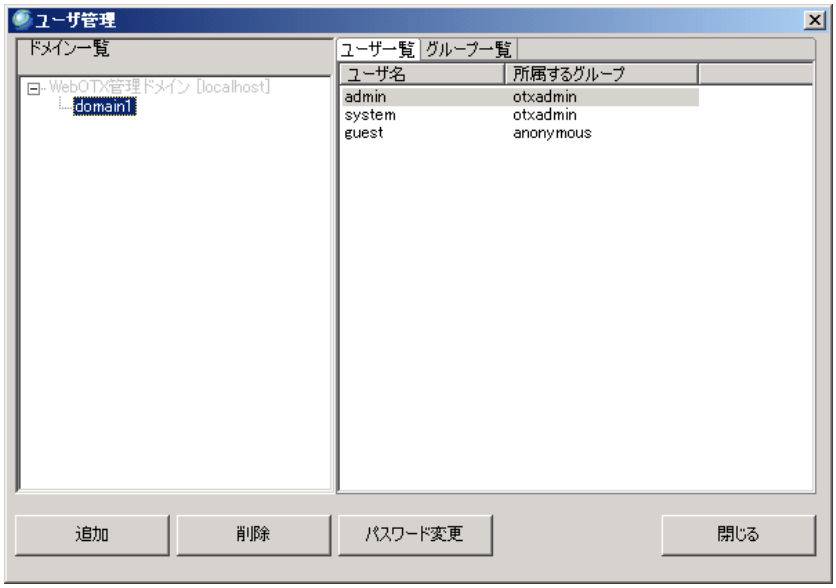
統合運用管理ツールを利用して、ユーザの追加を行う方法について説明します。

- ユーザの追加

1. ドメイン起動
ドメインが起動していない場合は起動してください。
${AS_INSTALL}/bin/otxadmin start-domain domain1

2. 統合運用管理ツールの接続
統合運用管理ツールを起動し、ドメインに接続してください。

3. ユーザの追加
統合運用管理ツールのメニューバーの[ユーザ管理]ボタンをクリックしてください。[ユーザ管理]画面が表示されるので、ユーザを追加したいドメインを選択した後、[追加]ボタンを選択してください。




[ユーザ追加]画面に、ユーザ名、グループ名、パスワードを入力してください。


- 注意 1:ユーザ ID に使える文字は、英数字と “-“(ハイフン)、”_”(アンダースコア)になりま

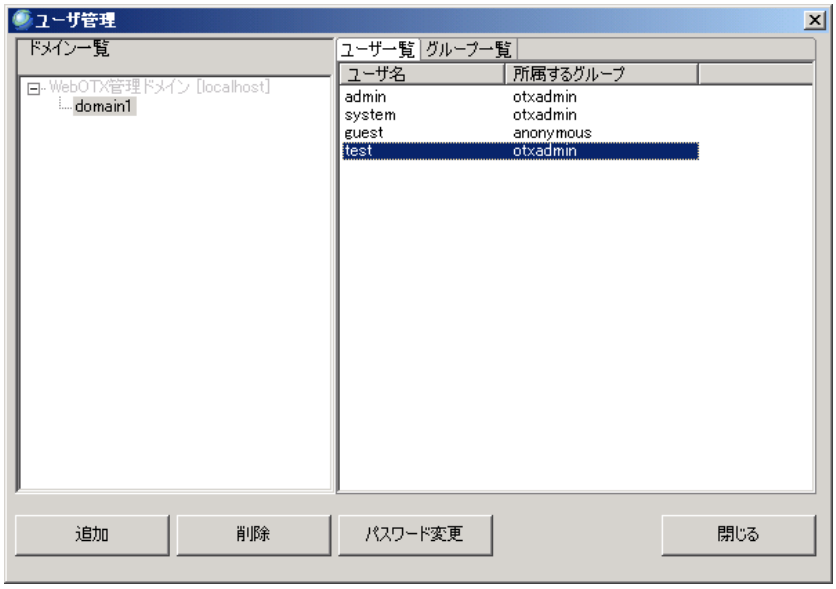
す。文字数の制限はありません。

- 注意 2：パスワードに使える文字は、英数字と記号が利用できますが、「¥」、「”」文字は利用できません。パスワードを省略することはできません。1文字以上指定してください。
- 注意 3：WebOTX 運用ユーザを追加する場合は、グループ名は必ず **otxadmin** を入力してください。
- 注意 4：domain.xml の jvm-config に com.nec.webotx.admin.password.complexity=true を設定した場合、ユーザのパスワードは 8 文字以上、英数字、大文字小文字を含めなければなりません。

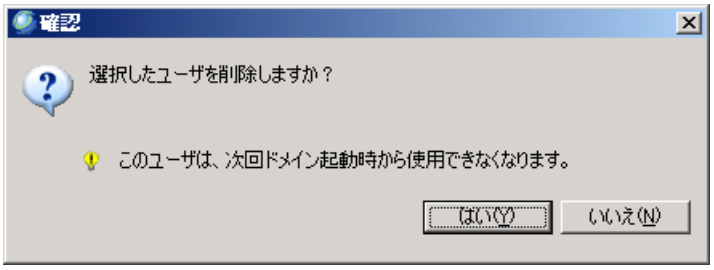
4. ドメイン再起動
作成したユーザが WebOTX 運用ユーザの場合、設定を反映させるためにドメインを再起動してください。作成したユーザが AP で利用する場合、ドメインの再起動は必要ありません。
(停止)　${AS_INSTALL}/bin/otxadmin stop-domain domain1
(起動)　${AS_INSTALL}/bin/otxadmin start-domain domain1

- ユーザの削除

1. ドメイン起動
ドメインが起動していない場合は、起動してください
${AS_INSTALL}/bin/otxadmin start-domain domain1
2. 統合運用管理ツールの接続
統合運用管理ツールを起動し、ドメインに接続してください。
3. ユーザの削除
統合運用管理ツールのメニューバーの[ユーザ管理]ボタンをクリックしてください。[ユーザ管理]画面が表示されるので、ユーザを削除したいドメインを選択し、削除したいユーザ名をクリックした後、[削除]ボタンをクリックしてください。




[確認]画面が表示されるので、正しければ[はい]を選択してください。




4. ドメイン再起動
削除したユーザが WebOTX 運用ユーザの場合、設定を反映させるためにドメインを再起動してください。**削除したユーザが AP で利用される場合、ドメインの再起動は必要ありません。**
(停止)　${AS_INSTALL}/bin/otxadmin stop-domain domain1
(起動)　${AS_INSTALL}/bin/otxadmin start-domain domain1

### 4.1.2 グループの追加、削除

#### 運用管理コマンドを利用する場合

- 追加
4.1.1 節の運用管理コマンドでユーザを作成する際にに指定する groups オプションで指定したグループが、ユーザ作成と同時に作られます。例えば、ユーザ test1 を作成するときに、groups オプションで testgrp を指定したときに初めて、グループ testgrp が作成されます。最後に変更を反映させるためにドメインを再起動してください。

・グループ作成(4.1.1 の 2 と同じ)
${AS_INSTALL}/bin/otxadmin
otxadmin > login -- user admin --password xxxxxx --port 6212
otxadmin > create-file-user --userpass admpass --groups testgrp testuser

・ドメイン再起動
削除したグループが WebOTX 運用ユーザの場合、設定を反映させるためにドメインを再起動してください。**削除したグループが AP で利用される場合、ドメインの再起動は必要ありません。**
(停止)　${AS_INSTALL}/bin/otxadmin stop-domain domain1
(起動)　${AS_INSTALL}/bin/otxadmin start-domain domain1

- 削除
削除したいグループに所属しているユーザをすべて削除することにより、グループを削除することができます。例えば、グループ testgrp にユーザ test1、test2 が属している場合、test1、test2 を削除したときに初めて、グループ testgrp が削除されます。最後に、変更を反映させるためにドメインを再起動してください。

・グループ削除(4.1.1 のユーザの削除の 2 と同じ)
${AS_INSTALL}/bin/otxadmin
otxadmin > login --user admin --password xxxxxx --port 6212
otxadmin > delete-file-user --authrealmname file testuser

・ドメイン再起動
削除したグループが WebOTX 運用ユーザの場合、設定を反映させるためにドメインを再起動してください。**削除したグループが AP で利用される場合、ドメインの再起動は必要ありません。**
(停止)　${AS_INSTALL}/bin/otxadmin stop-domain domain1
(起動)　${AS_INSTALL}/bin/otxadmin start-domain domain1

#### 統合運用管理ツールを利用する場合

- 追加
統合運用管理ツールから、グループを追加する場合、ユーザを作成する際にグループの作成を行います。グループ名が新規の場合は、新しいグループを作成され、既存のグ

ループ名を指定する場合は、指定したグループにユーザを追加します。

変更を反映させるためにドメインを再起動します。
(停止)　${AS_INSTALL}/bin/otxadmin stop-domain domain1
(起動)　${AS_INSTALL}/bin/otxadmin start-domain domain1

- 削除
  削除したいグループに所属しているユーザをすべて削除することにより、グループを削除することができます。統合運用管理ツールを利用してのユーザの削除手順は、4.1.1 節を参照してください。削除したいグループにユーザが所属している場合は、グループを削除することができません。グループの削除は、所属しているユーザが存在しない場合に行われます。

  変更を反映させるためにドメインを再起動します。
  (停止)　${AS_INSTALL}/bin/otxadmin stop-domain domain1
  (起動)　${AS_INSTALL}/bin/otxadmin start-domain domain1

## 4.2　LDAP レルムを使用する場合

LDAP サーバとして Enterprise Directory Server(以下 EDS)を利用する場合について説明します。
WebOTX と EDS を連携させる場合は、WebOTX のセットアップカードに記載されている EDS 初期化を行ってください。LDAP サーバに OpenLDAP を利用する場合は、OpenLDAP のマニュアルを参照してください。

注意：LDAP サーバに運用管理ユーザを作成する場合、ユーザ名が admin、system のユーザを作成する必要はありません。admin、system は File レルムのユーザを利用します。

### 4.2.1　ユーザの追加、削除

EDS にユーザを追加、削除する方法は EDS の運用管理ツールから行うか、EDS の edload コマンドを利用し、ldif ファイルを読み込む方法があります。edload コマンドを利用してユーザの追加、削除を行う方法については、EDS のマニュアル(ユーティリティ利用の手引 1 章)を参照してください。今回、運用管理ツールから追加を行う方法について説明します。

#### ユーザ登録

1. EDS Protocol Server の起動
   EDS Protocol Server が起動していない場合は起動してください。
   - Windows の場合
     サービスマネージャから[EDS Protocol Server]を起動、またはコマンドプロンプトで
     net start “EDS Protocol Server”を実行してください。
   - Linux の場合
     /opt/nec/eds/bin/EDAGENT start
   - HP-UX の場合
     /opt/eds/bin/EDAGENT start
2. EDS の運用管理ツールの接続
   EDS の運用管理ツールを起動してください。
   - Windows の場合
     スタートメニューの[Enterprise Directory Server]-[運用管理ツール]を選択してください。
   - HP-UX、Linux の場合
     /opt/nec/eds/client/edsconsole を実行してください。HP-UX、Linux で運用管理ツールを起動する場合、環境ファイルの作成が必要となります。環境ファイルの作成方法は、それぞれの OS に対応した EDS のセットアップカードを参照してください。

   運用管理ツールを起動後、以下の情報を入力してください。

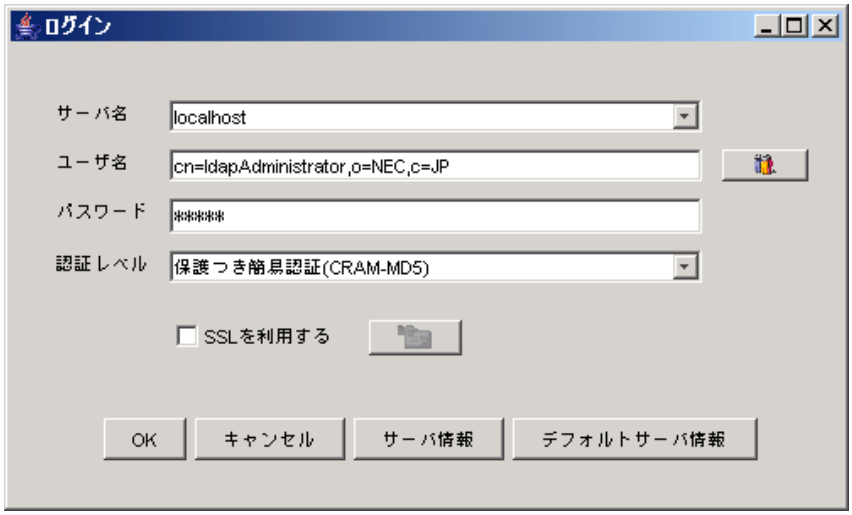
| 項目 | 説明 |
|---|---|
| サーバ名 | EDS が起動しているマシン名 |

| | |
|---|---|
| ユーザ名 | EDS に登録されているユーザ名をDN形式で入力 |
| パスワード | EDS インストール時に設定した管理者パスワード |
| 認証レベル | 保護つき簡易認証(CRAM-MD5) |

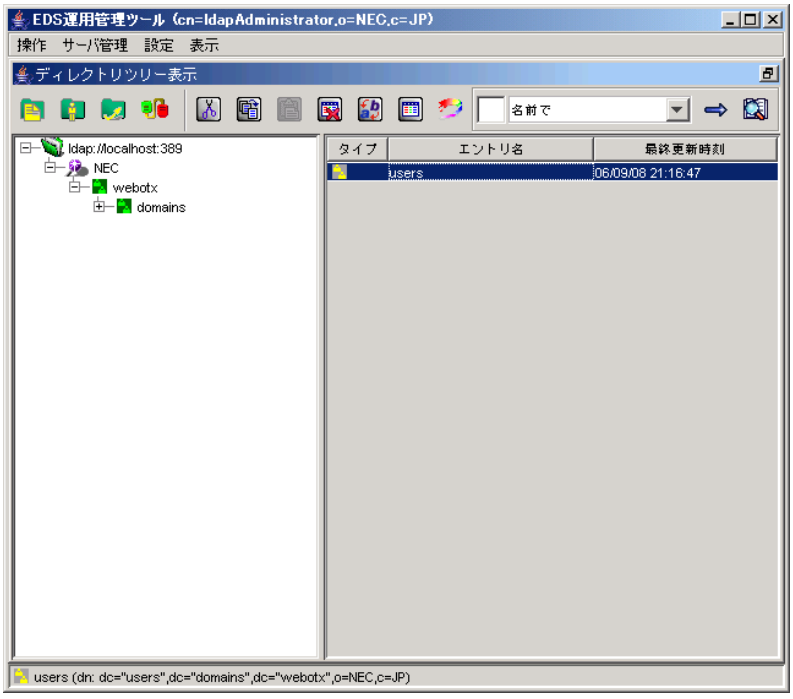
ユーザ名の例

EDS インストール直後にログインを行う場合は、管理ユーザを利用してください。DN は以下のようになります。
cn=ldapAdministrator,${ROOT_ENTRY}

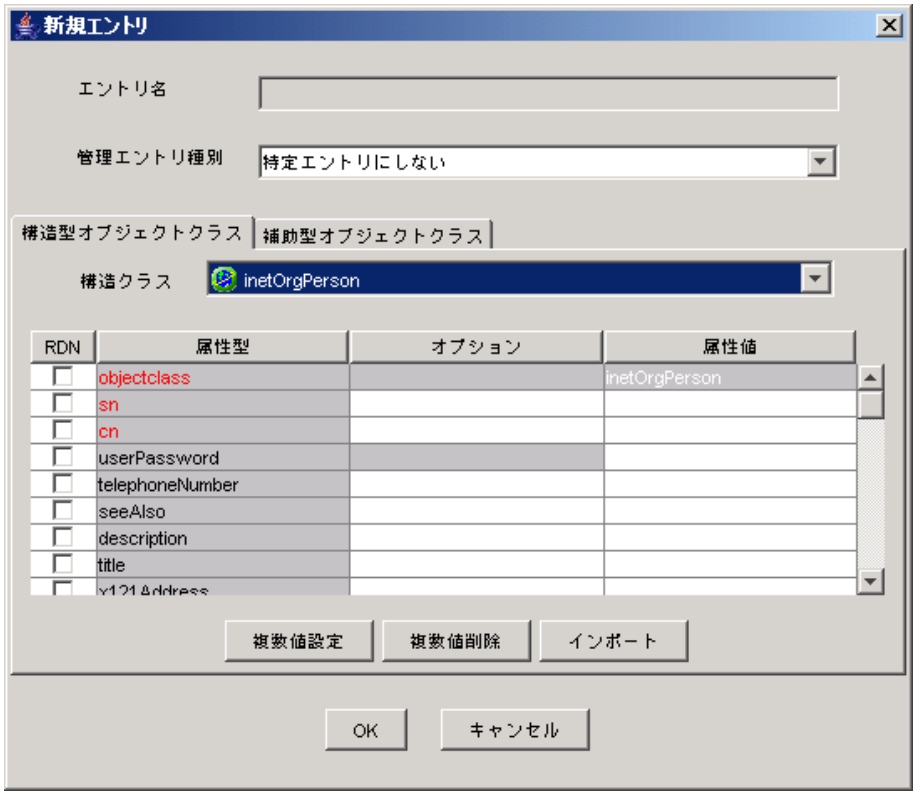
注意：${ROOT_ENTRY}は EDS インストール後の作業時に指定したルートエントリを指定してください。
Windows の場合：EDS データベース初期化ツール実行時
HP-UX/Linux の場合：/opt/eds/bin/edinit(HP-UX),/opt/nec/eds/bin/edinit(Linux)実行時




3. ユーザ登録
EDS 初期化スクリプトを実行していない場合は以下のコマンドを実行してください。
${AS_INSTALL}/config/eds/edsinit.bat(edsinit) ${ROOT_ENTRY}
上記コマンドを実行すると、運用管理ツールには以下のように表示されます。



users を右クリックし、表示されるメニューから[利用者登録]を選択すると、[新規エントリ]が表示されます。


新規エントリ画面では**構造クラスに inetOrgPerson** を必ず指定してください。また、以下の属性値は必ず指定してください。

| 属性名 | 説明 |
|---|---|
| cn | 一般名。氏名、社員番号など |
| sn | 姓 |
| userPassword | 登録するユーザのパスワード。アプリケーション等の認証に利用 |
| uid | 登録するユーザの ID。アプリケーション等の認証に利用 |

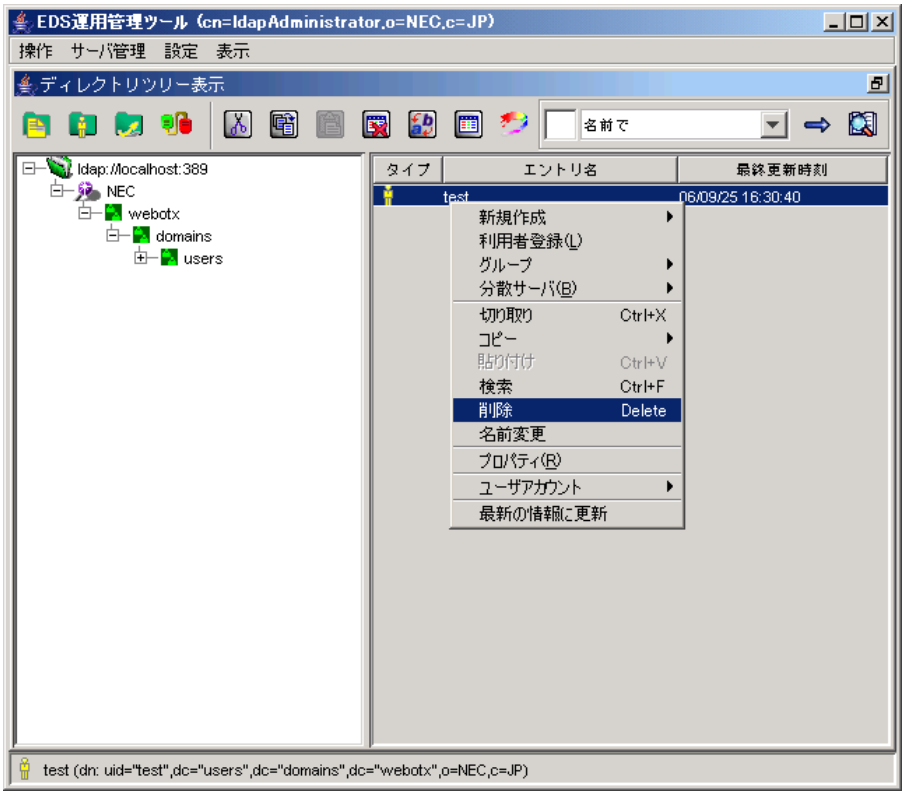
その他の属性については必要に応じて設定してください。

## ユーザの削除

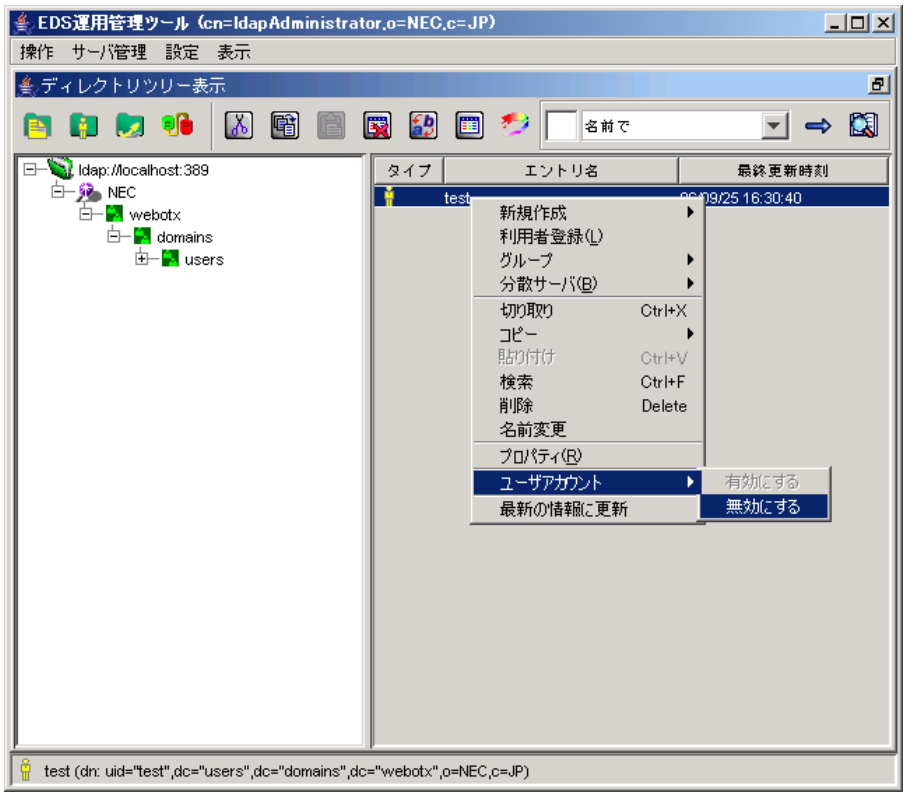
EDS サーバ、運用管理ツールの接続方法は、ユーザ作成を参照して、運用管理ツールの接続まで完了してください。

1. ユーザ削除
   運用管理ツールにおいて、削除したいユーザ名を右クリックします。本例ではユーザ名 test を利用します。

   - サーバから完全にユーザ情報を削除する場合
     右クリックメニューから[削除]を選択します。




   - ユーザアカウントを無効にする場合
     右クリックメニューから[ユーザアカウント]-[無効にする]を選択します。




## 4.2.2 グループの作成、削除

EDS に新たにグループを作成、削除する方法について説明します。グループの作成、削除には EDS の運用管理ツールを利用して行います。本例では、ユーザとして、ユーザ名:[test]を予め作成しているものとします。

### グループの作成

1. EDS Protocol Server の起動
   EDS Protocol Server が起動していない場合は起動してください。
   - Windows の場合
     サービスマネージャから[EDS Protocol Server]を起動、またはコマンドプロンプトで net start “EDS Protocol Server”を実行してください。
   - HP-UX,Linux の場合
     /opt/nec/eds/bin/EDAGENT start
   - HP-UX の場合
     /opt/eds/bin/EDAGENT start
2. EDS の運用管理ツールの接続
   EDS の運用管理ツールを起動してください。
   - Windows の場合
     スタートメニューの[Enterprise Directory Server]-[運用管理ツール]を選択してください。
   - HP-UX、Linux の場合
     /opt/nec/eds/client/edsconsole を実行してください。HP-UX、Linux で運用管理ツールを起動する場合、環境ファイルの作成が必要となります。環境ファイルの作成方法は、それぞれの OS に対応したセットアップカードを参照してください。

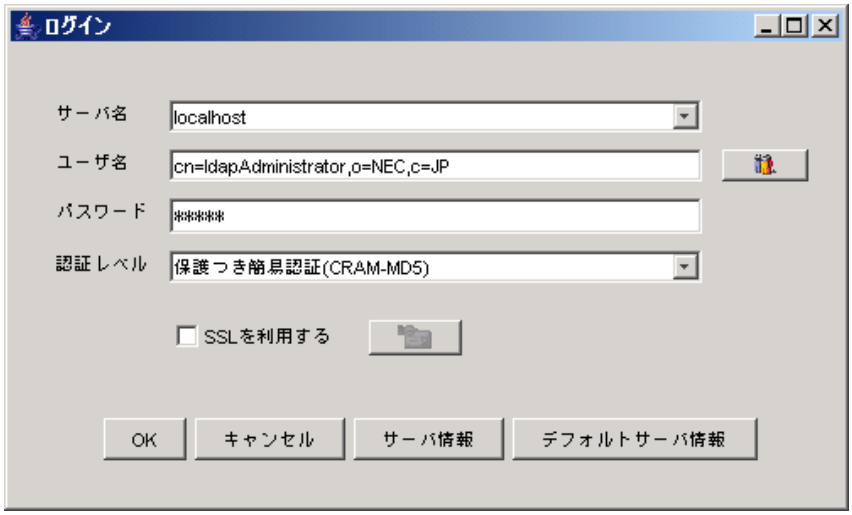
運用管理ツールを起動後、以下の情報を入力してください。

| 項目 | 説明 |
| --- | --- |
| サーバ名 | EDS が起動しているマシン名 |
| ユーザ名 | EDSに登録されているユーザ名をDN形式で入力 |
| パスワード | EDSインストール時に設定した管理者パスワード |
| 認証レベル | 保護つき簡易認証(CRAM-MD5) |

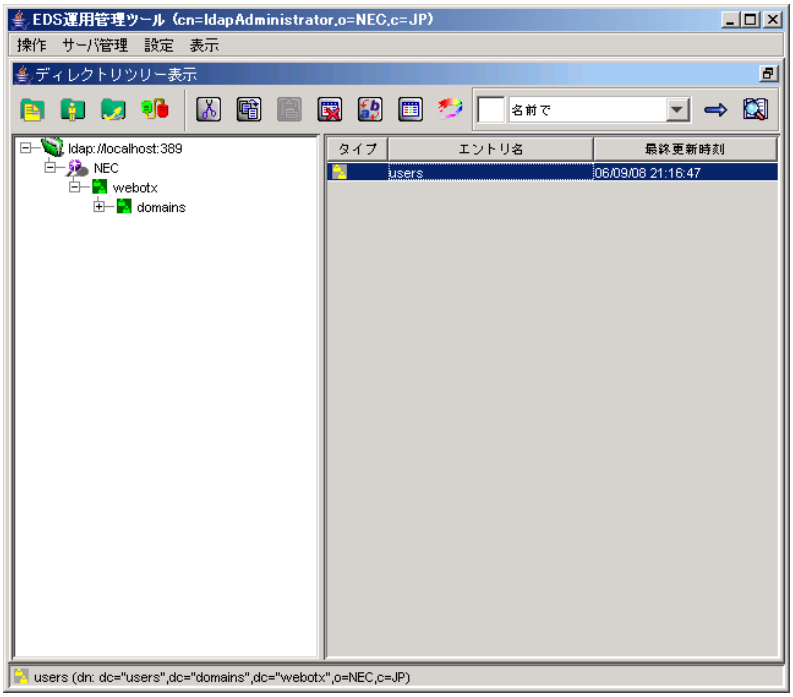
ユーザ名の例

EDS インストール直後にログインを行う場合は、管理ユーザを利用してください。DN は以下のようになります。
cn=ldapAdministrator,${ROOT_ENTRY}

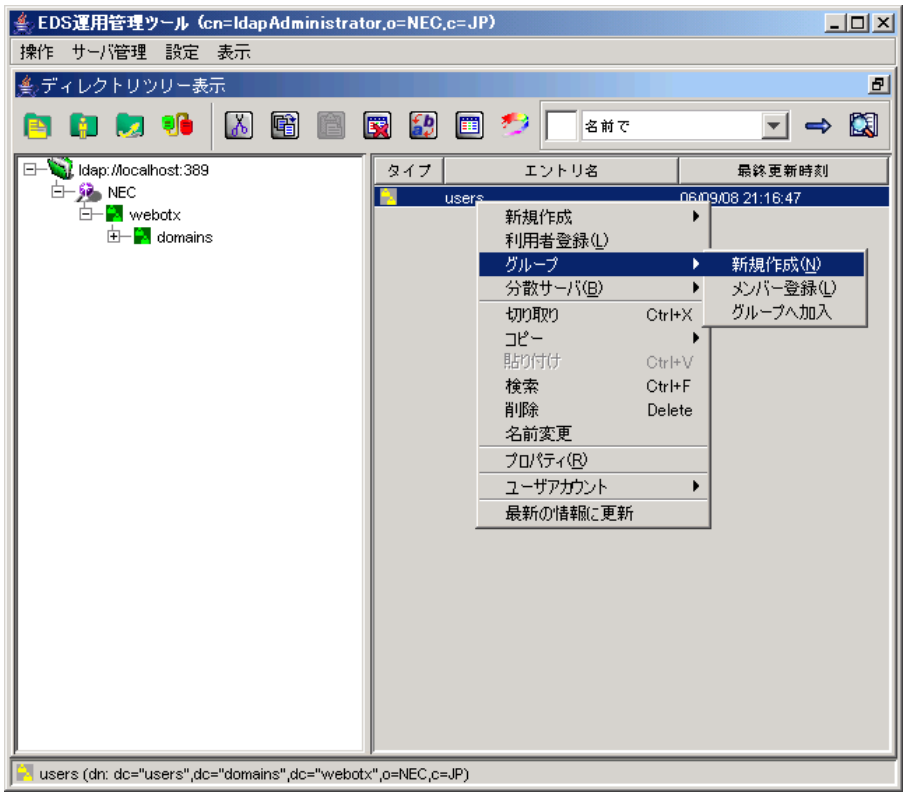
注意：${ROOT_ENTRY}は EDS インストール後の作業時に指定したルートエントリを指定してください。
Windows の場合：EDS データベース初期化ツール実行時
HP-UX/Linux の場合：/opt/eds/bin/edinit(HP-UX),/opt/nec/eds/bin/edinit(Linux)実行時




3. グループ作成
EDS 初期化スクリプトを実行していない場合は以下のコマンドを実行してください。
${AS_INSTALL}/config/eds/edsinit.bat(edsinit) ${ROOT_ENTRY}
上記コマンドを実行すると、運用管理ツールには以下のように表示されます。




users を右クリックし、表示されるメニューから[グループ]-[新規作成]を選択すると、[新規エントリ]が表示されます。



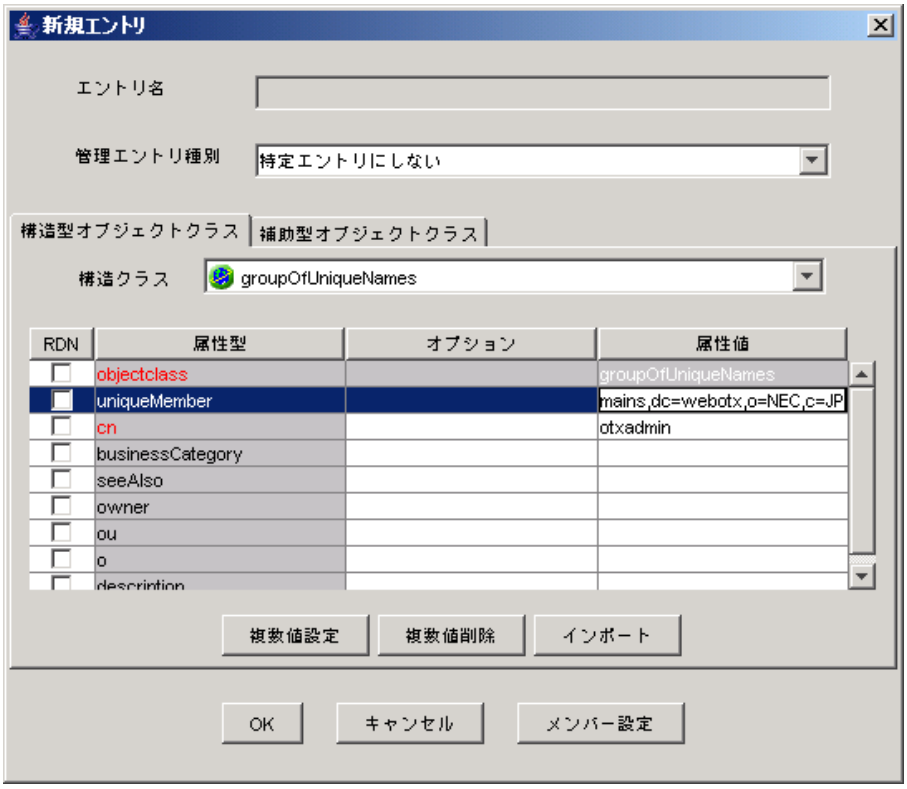

新規エントリ画面では**構造クラスには、groupOfUniqueNames** を必ず指定してください。また、以下の属性値は必ず指定してください。

運用管理ツールを起動後、以下の情報を入力してください。

| 属性名 | 説明 |
|---|---|

| | |
|---|---|
| uniqueMember | グループを作成する場合は、作成時に必ず 1 ユーザをグループ所属させる必要がある。<br>作成時に所属させるユーザの DN |
| cn | グループ名 |

その他の属性については必要に応じて指定してください。



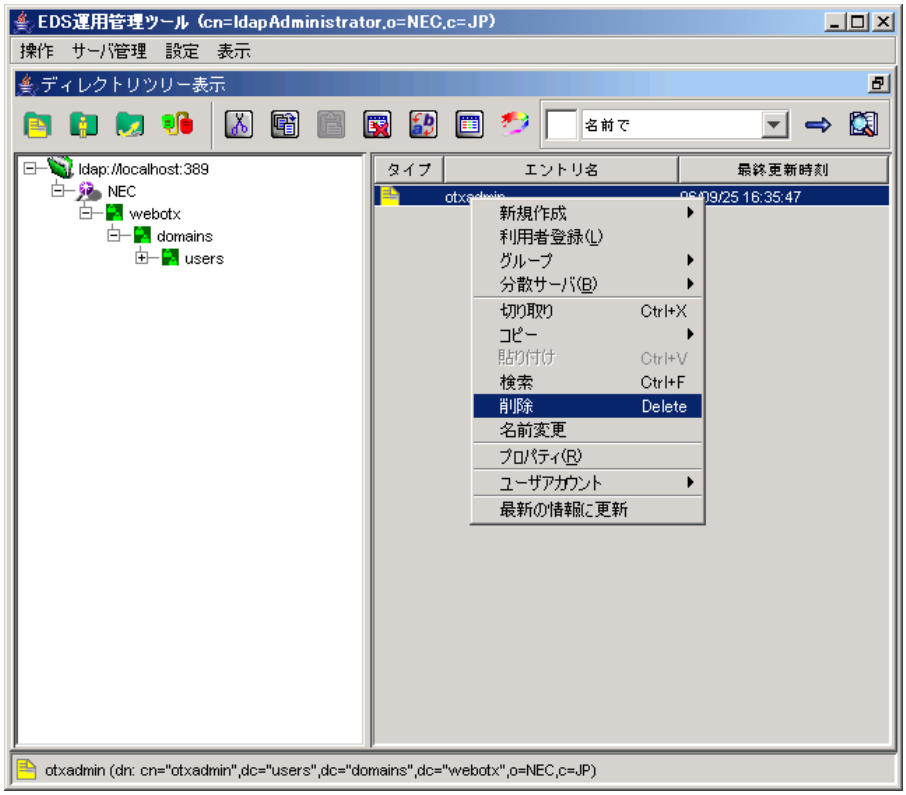

4. グループのアクセス権の設定
   グループのアクセス権の設定をします。アクセス権の設定方法については EDS のマニュアル(運用の手引 5 章)を参照してください。

## グループの削除

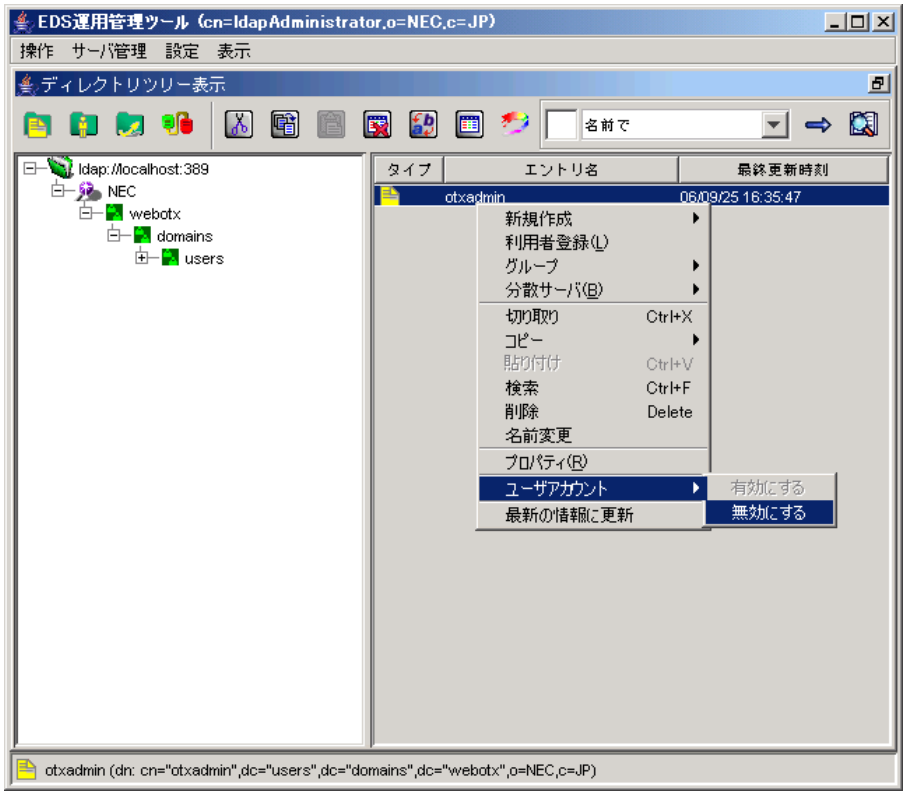
EDS サーバ、運用管理ツールの接続方法は、グループ作成を参照して、運用管理ツールの接続まで完了してください。

1. グループ削除
   運用管理ツールにおいて、削除したいユーザ名を右クリックします。

   - サーバから完全にグループ情報を削除する場合
     右クリックメニューから[削除]を選択します。




- グループを無効にする場合
  右クリックメニューから[ユーザアカウント]-[無効にする]を選択します。

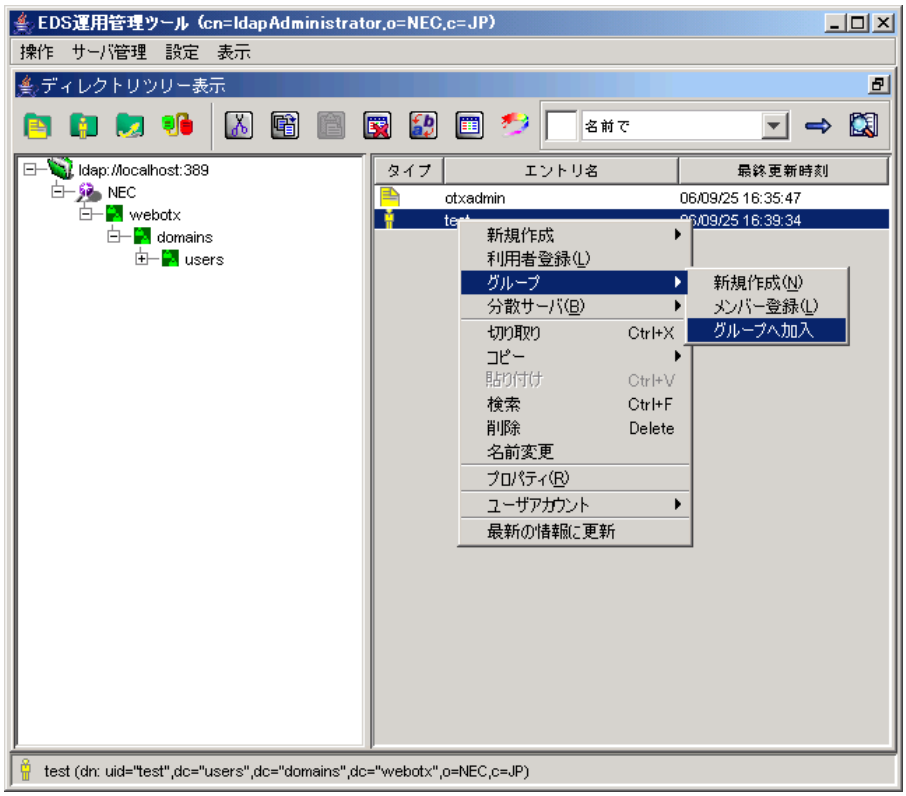



### 4.2.3 ユーザをグループに登録

## ユーザをグループに登録

作成したユーザをグループに登録します。グループの作成方法は 4.2.2 節を参照してください。ここでは、予め otxadmin グループが作成されているとします。

1. 作成したユーザ名を右クリックし、[グループ]-[グループへ加入]を選択します。




2. [グループ選択]画面で登録したいグループを選択し[←追加]ボタンを押します。最後に[OK]ボタンを押すことで、グループへの追加は完了です。本例では otxadmin グループに追加しています。

## 4.3 JDBC レルムを使用する場合

本節では、JDBC レルムを利用する場合の、ユーザの追加、削除の方法について説明します。ここではデータベースに Oracle を使用することを前提としますが、操作は SQL で記述しますので、その他のデータベースでも利用することが可能です。

データベースのアプリケーションのインストール、データベースの作成方法、ログイン方法については、利用するデータベースのマニュアルを参照してください。

注意：JDBC に運用管理ユーザを作成する場合、ユーザ名が admin、system のユーザを作成する必要はありません。admin、system は File レルムのユーザを利用します。

### 4.3.1 データベーステーブルの作成、削除

ユーザおよびグループを登録するために、事前に次のようなテーブルを作成しておきます。

テーブル名 :jdbc_user (任意)

| フィールド名 | データ型 | 内容 |
|---|---|---|
| userid(任意) | VARCHAR(10) | ユーザ名を登録します。 |
| passwd(任意) | VARCHAR(30) | パスワードを登録します。 |
| realm(任意) | VARCHAR(30) | レルム名を登録します。<br>DIGEST 認証を行い、かつ複数のレルムがこのテーブルを参照する場合のみ必須フィールドとなります。<br>※レルム名には JDBC レルムの name 値を登録します。 |

テーブル名 :jdbc_role (任意)

| フィールド名 | データ型 | 内容 |
|---|---|---|
| userid(任意) | VARCHAR(10) | ユーザ名を登録します。 |
| role(任意) | VARCHAR(10) | ロール名を登録します。 |

コマンドを利用して、テーブルを作成する方法について説明します。

- テーブルの作成

次のコマンドを実行します。

CREATE TABLE jdbc_user(userid VARCHAR(10), passwd VARCHAR(30) , *realm VARCHAR(30)*);

CREATE TABLE jdbc_role(userid VARCHAR(10), role VARCHAR(10));

※赤字箇所は任意です

※データの長さは、必要な長さを指定します。

テーブルの作成で、作成したテーブル jdbc_user および jdbc_role を削除する手順を説明します。

- テーブルの削除

次の、コマンドを実行します。

drop table jdbc_user;

drop table jdbc_role;

### 4.3.2 ユーザの追加、削除

データベースに SQL で、ユーザを追加、削除する方法について説明します。

- ユーザの追加

次のコマンドを実行します。(ユーザ名 : user1、パスワード password の登録例です)

INSERT INTO jdbc_user(userid, passwd) values ('user01', 'password');

※ 同一のユーザ名のエントリが複数あった場合は、最初に一致したエントリを使用します。

※パスワードのダイジェストは、次のコマンドで生成することができます。

```
> CD  ${AS_INSTALL}/lib
>          java          -cp          ./webc-catalina.jar;../j2ee.jar;./wosv-rt.jar
  org.apache.catalina.realm.RealmBase -a <ダイジェスト方式> <パスワード>
```

※ ダイジェスト方式は 3.3.1.JDBC レルムの設定で指定した方式を指定します。 ダイジェスト方式には MD5、SHA-1、SHA-256、SHA-384、SHA-512 のいずれかを指定することができます。

※ DIGEST 認証を使用する場合でパスワードのダイジェスト化を行う場合は、JDBC レルムのプロパティに「useA1Digest="true"」を設定し、passwd フィールドには「<user 名> + ":" + <realm 名> + ":" + <パスワード>」の MD5 ダイジェスト値を格納する必要があります。
以下の場合のダイジェスト値を生成する例を示します。
user 名 : "admin"
realm 名 : "JDBCrealm"
パスワード : "adminadmin"

```
… org.apache.catalina.realm.RealmBase –a MD5 admin:JDBCrealm:a
dminadmin
```

ユーザの追加で、登録したユーザ user01 を削除する手順を説明します。

- ユーザの削除

次の、コマンドを実行します。

DELETE from jdbc_user where userid='user01';

SQL を利用して、ユーザの登録状況を確認する方法について説明します。

- ユーザの確認

次の、コマンドを実行します。(ユーザ名 user01 を確認する例です)

select * from jdbc_user where userid='user01';

### 4.3.3 グループの追加、削除

データベースに SQL でグループの追加、削除する方法について説明します。グループは、ユーザ名とグループ名の組を1つエントリとして登録します。

SQL を利用して、グループを追加する行う方法について説明します。

- グループの追加

INSERT INTO jdbc_role(userid, role) values ('user01', 'users');

- グループの削除
  グループの追加で作成したグループ users を削除する手順を説明します。

DELETE from jdbc_role where role='users';

・1人のユーザに複数のグループを設定する場合は、それぞれのグループに対して1つのエントリを作成してください。

# 5 ロールの設定

## 5.1 アプリケーションへのロールの設定

アプリケーションを利用するユーザにロールを設定することで、アプリケーションのどの操作を行うことができるかを定義することができます。本章では、WebOTX が提供している配備ツールを利用し、アプリケーションの配備記述子にロールの定義を追加する方法を説明します。加えて、アプリケーションを利用するユーザとロールを関連付けるためのユーザ認証を行うための設定について説明します。

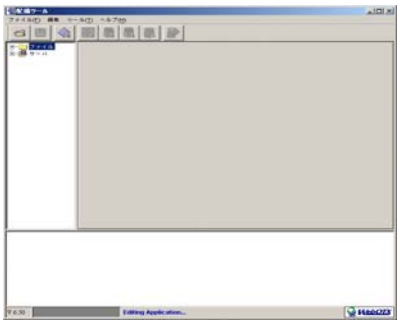
### 5.1.1 配備記述子にロールの定義を追加

配備ツールを利用しての追加方法

1. 配備ツールの起動

   スタートメニューから、配備ツールを起動します。

   起動するとつぎのウインドウが開きます。



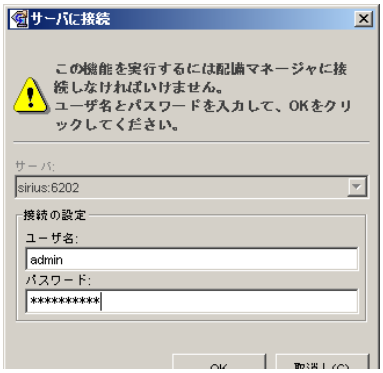
2. 配備ツールの接続

   メニューの「ファイル」－「サーバの追加」をクリックすると、「サーバを追加」ダイアログが表示され

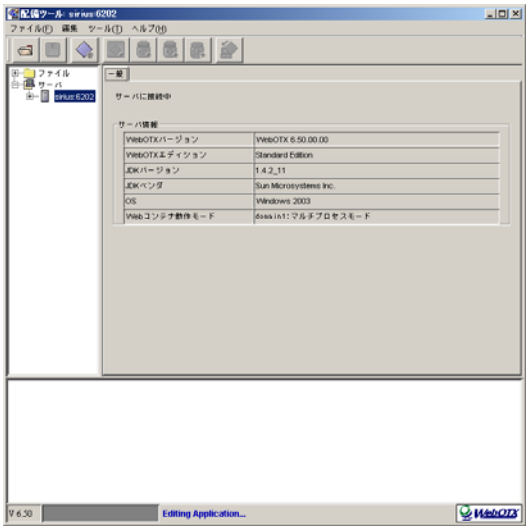
るので、サーバ名とポート番号を入力します。 本例では、デフォルトの localhost の 6202 番ポートを指定しています。


左上にサーバのアイコンが現れます。これを右クリックして、「ドメイン一覧の取得」をクリックします。

「サーバに接続」ダイアログが表示されます。これに、ユーザ名とパスワードを入力します



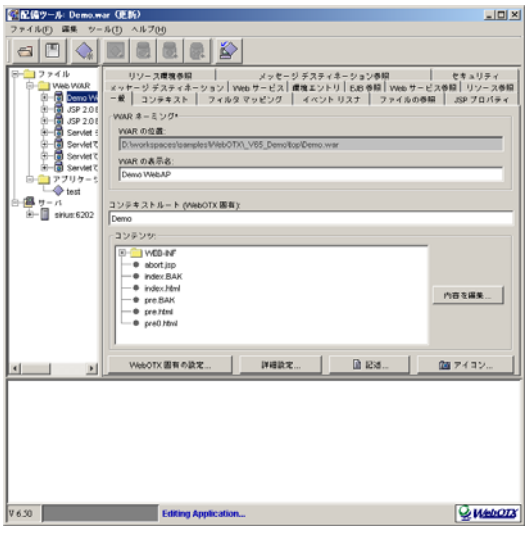

が表示されます。



3. アプリケーションの指定

メニュー「ファイル」ー「開く」をクリックし、アプリケーションファイル（WAR および EAR）を選択し開きます。

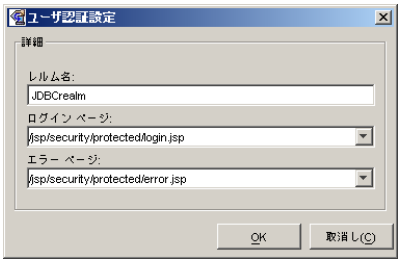
左のアプリケーションをクリックして選択すると、次のようにアプリケーションの設定内容が表示されます。



4.　配備記述子へのロールの追加

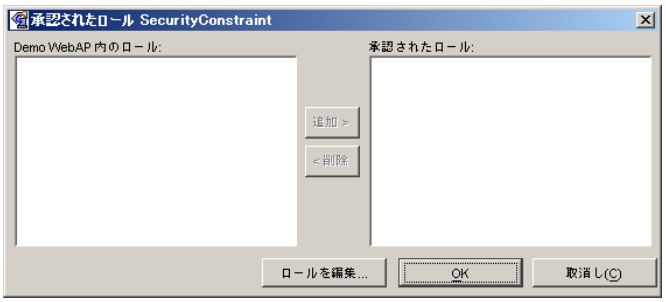
「セキュリティ」タブをクリックして、ユーザ認証方式を選択して、「設定」をクリックすると「ユーザ認証設定」ダイアログが表示されます。 これにレルム名、ログインページ、エラーページを入力します。

基本認証の場合は、レルム名のみを入力します。

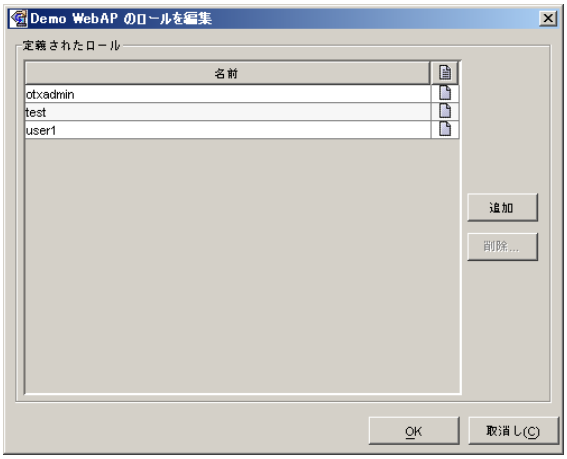



- レルム名には、「3章レルムの設定」で指定したレルム名を指定します。 存在しないレルム名が指定された場合は、デフォルトレルム（file レルム）を使用します。
- ログインページは、ユーザ名、パスワードを入力するためのページです。「5.1.2.ユーザ認証」で説明します。セキュリティがかかったページに未認証のままアクセスするとこのページが表示されます。 エラーページは、認証に失敗した場合に表示されるページです。

「制約の追加」をクリックし、次に「ロールの編集」をクリックします。「承認されたロール SecurityConstraint」ダイアログが表示されます。



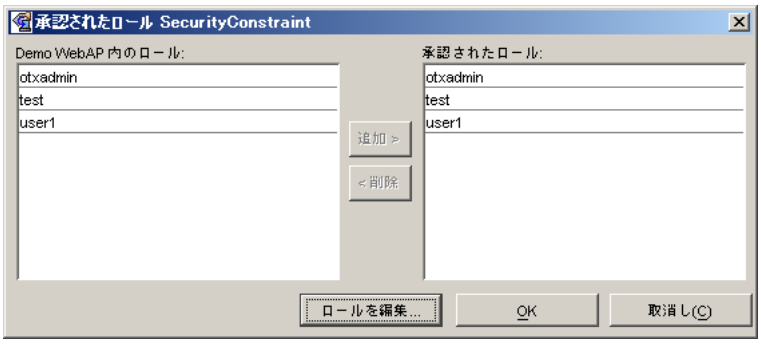

「ロールの編集」をクリックします。「xxxx のロールの編集」ダイアログが表示されます。「追加」をクリックしてロールの入力欄を追加し、名前を入力します。 追加が完了したら「OK」をクリックします。



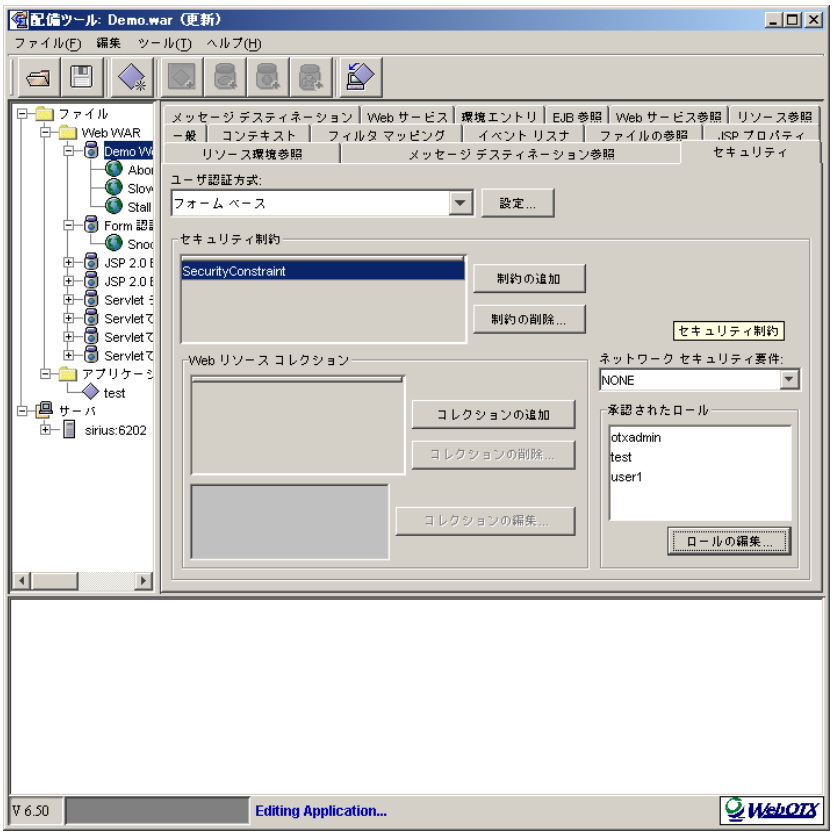
※ここで入力するロール名は、承認するグループ名またはユーザ名です。

「承認されたロール SecurityConstraint」ダイアログに戻ります。「xxx 内のロール」のロール名を選択して「追加＞」をクリックします。 これにより、ロール名のリストから承認されたロールに追加されます。

「OK」をクリックします。




「承認されたロール SecurityConstraint」ダイアログが閉じます。「ファイル」ー「保存」でファイルを保存すると、ロールの設定は完了です。




## 5.1.2 ユーザ認証を行う Web アプリケーションの作成方法

Web アプリケーションを利用するときに、ユーザ認証を行う方法について説明します。

大まかな手順は、次のとおりです。

1） ユーザ認証を除く部分の Web アプリケーションの作成

2） FORM 認証の場合は、ユーザ名、パスワードを入力させるためのログインページおよび認証失敗したときに表示するエラーページの追加

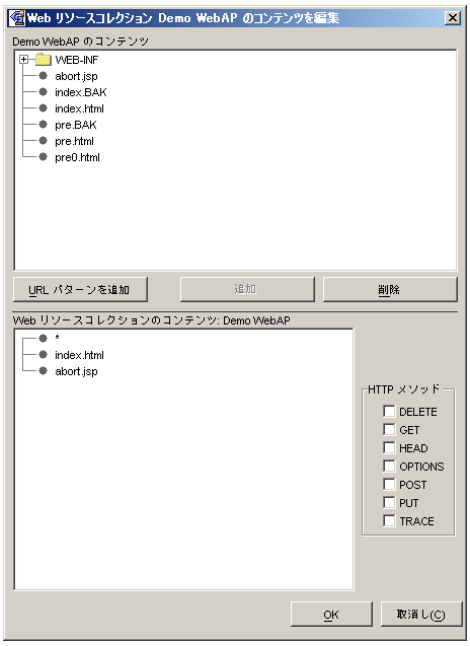
3） 配備記述子へのロールの定義を追加

4） 配備記述子へのセキュリティを適用するページの設定追加

セキュリティを適用するページの設定方法と、FORM 認証の場合に使用するログインページの作成方法について説明します。

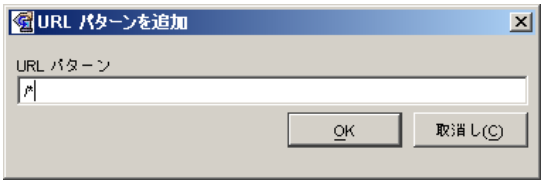
まず、配備ツールから、セキュリティの適用するページを設定する方法を説明します。

「5.1.1 配備記述子にロールの定義を追加」を行ったあとに、「セキュリティ制約」を選択し、「コレクションの追加」をクリックします。次に表示されている Web リソースコレクションを選択し「コレクションの編集」をクリックします。「Web リソースコレクションxxxのコンテンツを編集」ダイアログが表示されます。




「URL パターンを追加」をクリックすると、「URL パターン追加」のダイアログが表示されます。ここにセキュリティを適用するページのコンテキスト名以下の URL を入力し、「OK」をクリックします。

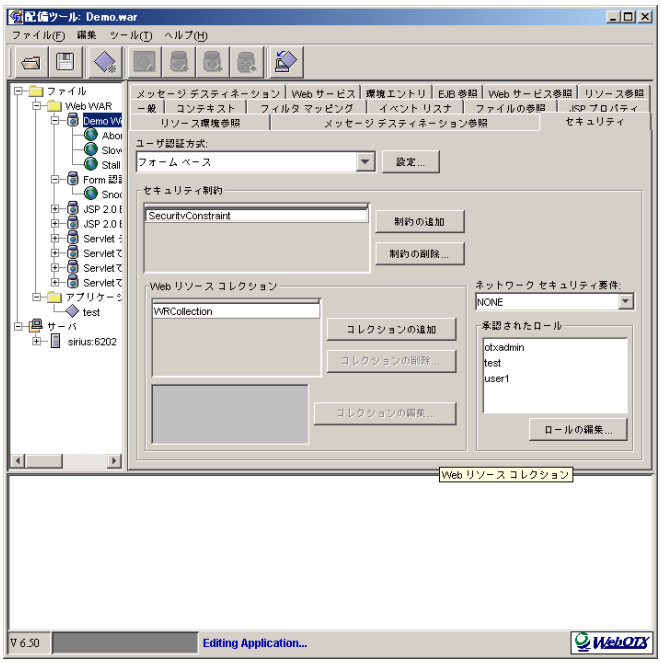
すべてのページにセキュリティをかける場合は“/*”を入力します。 特定のページにかける場合は、“/*jsp”のように記述することができます。また、「xxxxのコンテンツ」のツリーで特定のページを選択し、「追加」をクリックすると「Web リソースコレクションのコンテンツ：xxxx」に登録することができます。



「Web リソースコレクションxxxxのコンテンツを編集」の「OK」をクリックして

ダイアログを閉じます。


「ファイル」ー「保存」でファイルを保存すると、セキュリティを適用するページの設定は完了です。




次に、FORM 認証において、ユーザ名、パスワードを入力させるためのログインページの作成方法について説明します。

ログインページには、ログイン認証させるために、ユーザ名とパスワードを入力させるフォームと、認証に渡すためのアクションを記述する必要があります。

次に、jsp での記述例を示します。

[ログインページ index.jsp の記述の例]

```
<html>
  <head>
    <title>Form Authentication Example Page</title>
<META HTTP-EQUIV="Content-Type" CONTENT="text/html; charset=Shift_JIS">
  </head>
  <h1> Form Authentication Example Page </h1>
<p>
<form method="post" action='<%= response.encodeURL("j_security_check")%>'>
<table>
  <tr>
    <td>ID</td>
    <td> <input type="text" name="j_username"></td>
  </tr>
```

```
  <tr>
    <td>Pass</td>
    <td><input type="password" name="j_password"></td>
  </tr>
</table>
<br>
<input type="submit" value="Login" name="submit">
<input type="reset" value="Reset" name="reset">
</form>

  </blockquote>
  </body>
</html>
```