



# LISM

**管理者ガイド Ver.1.0.0**

**2016 年 11 月 株式会社セシオス**



# 目次

---

1	概要.....	4
2	インストールと設定.....	5
2.1	事前準備.....	5
2.2	インストール.....	6
2.3	セットアップツールによる初期設定.....	6
2.3.1	FQDN の設定.....	8
2.3.2	visudo の設定変更.....	8
2.3.3	パスワード辞書ファイルの作成.....	8
2.3.4	LDAP サーバへの接続設定.....	8
2.3.5	Memcached サーバへの接続確認.....	9
2.3.6	管理者パスワードの設定.....	9
2.3.7	サービスの再起動.....	9
2.3.8	サービスの停止.....	10
2.3.9	終了.....	10
3	LISM WEB 管理コンソール.....	11
4	ユーザ.....	13
4.1	新規登録.....	13
4.2	一覧表示・変更・削除.....	15
4.3	CSV 登録・変更・削除.....	16
5	組織.....	18
5.1	新規登録.....	18
5.2	組織の一覧表示・変更・削除.....	18
5.3	CSV 登録・変更・削除.....	19
6	ユーザグループ.....	20
6.1	新規登録.....	20
6.2	一覧表示・変更・削除.....	20
6.3	CSV 登録・変更.....	22
7	統合 ID 管理.....	23
7.1	同期システム一覧.....	23
7.2	マスタ LDAP サーバ設定.....	24

7.3	マスタ DB 設定 .....	25
7.4	LDAP サーバ設定 .....	26
7.4.1	連携先 LDAP サーバの設定項目 .....	26
7.4.2	Active Directory との連携設定例 .....	28
7.4.3	動作確認 .....	30
7.5	DB 設定 .....	31
7.6	CSV インポート設定 .....	32
7.6.1	独自 CSV フォーマットと LISM の属性マッピング .....	32
7.6.2	動作確認 .....	33
7.6.3	CSV ファイルのインポート実行 .....	33
7.7	CSV エクスポート設定 .....	34
7.7.1	エクスポートする CSV フォーマット設定 .....	34
7.7.1	動作確認 .....	35
7.7.2	エクスポート実行 .....	35
7.8	RESTFUL API 設定 .....	36
7.8.1	RESTFUL API の設定項目 .....	36
7.8.2	SeciossLink との連携設定例 .....	37
7.9	追加属性 .....	39
7.10	関数一覧 .....	39
<b>8</b>	<b>システム設定 .....</b>	<b>41</b>
8.1	システム設定 .....	41
8.2	パスワードポリシー設定 .....	41
8.3	メールテンプレート設定 .....	42
<b>9</b>	<b>参考 .....</b>	<b>42</b>
9.1	OPENLDAP の構築 .....	42
9.1.1	OpenLDAP のインストール・設定 .....	42
9.1.2	LDAPS 接続用の自己証明書作成 .....	43
9.1.3	LISM 管理用の OpenLDAP 設定 .....	43
<b>表 1</b>	<b>LISM サーバスペック .....</b>	<b>5</b>
<b>表 2</b>	<b>LISM メニュー .....</b>	<b>12</b>
<b>表 3</b>	<b>ユーザメニュー .....</b>	<b>13</b>
<b>表 4</b>	<b>ユーザ情報項目一覧 .....</b>	<b>13</b>
<b>表 5</b>	<b>ユーザー一覧操作機能 .....</b>	<b>15</b>

表 6 CSV ユーザ登録フォーマット一覧	16
表 7 組織メニュー	18
表 8 組織項目一覧	18
表 9 組織一覧操作機能	19
表 10 CSV 組織登録フォーマット	19
表 11 CSV 組織削除フォーマット	19
表 12 ユーザグループメニュー	20
表 13 ユーザグループ項目一覧	20
表 14 ユーザグループ操作機能一覧	21
表 15 グループメンバータブ	22
表 16 CSV によるグループメンバー登録・削除	22
表 17 CSV グループ登録フォーマット	22
表 18 統合 ID 管理メニュー	23
表 19 マスタ LDAP サーバの設定項目	24
表 20 マスタ DB 設定項目	25
表 21 連携先 LDAP 設定項目一覧	26
表 22 AD へ同期設定例	28
表 23 DB 連携設定項目	31
表 24 CSV インポート設定項目一覧	32
表 25 CSV エクスポート設定項目一覧	34
表 26 RESTFUL 設定一覧	36
表 27 SeciossLink への同期設定例	38
表 27 利用可能な関数一覧	39
表 28 システム設定項目一覧	41
表 29 パスワードポリシー設定	41
表 30 メールテンプレート設定項目	42

# 1 概要

統合 ID 管理ソフトウェア「LISM」は、様々なシステムに分散した ID 情報や役割（ロール）情報を一元的に管理することができるソフトウェアです。

LISM は、システムの情報を 1 つの LDAP ディレクトリツリーとして管理し、連携先の各システムの情報はそれぞれサブツリーに分かれて管理されています。マスタデータとなる LDAP サーバの情報については、ou=LDAP と ou=Master の配下に表示され、ou=Master 配下の情報がマスタデータとして扱われます。

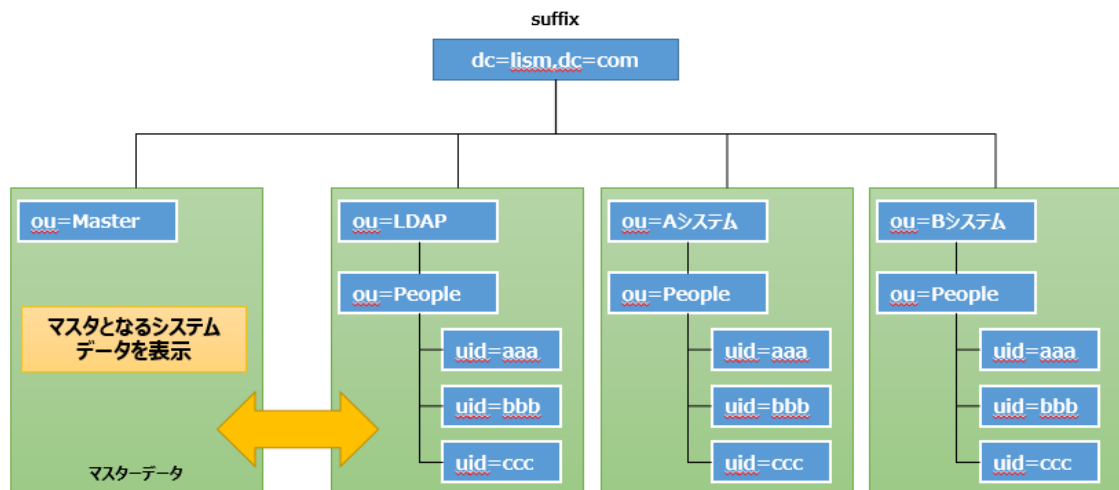


図 1 LISM LDAP 構成イメージ

そのため、LISM のマスタデータ（OpenLDAP）に対して更新を行うことで、連携されている Active Directory、LDAP、RDBMS や、CSV ファイル出力、RESTful API、SOAP API を持った Web サービスに対して ID 情報の更新内容をリアルタイムで同期することができます。ID 情報の管理は、基本的にマスタデータに対して操作のみの一元管理を実現します。

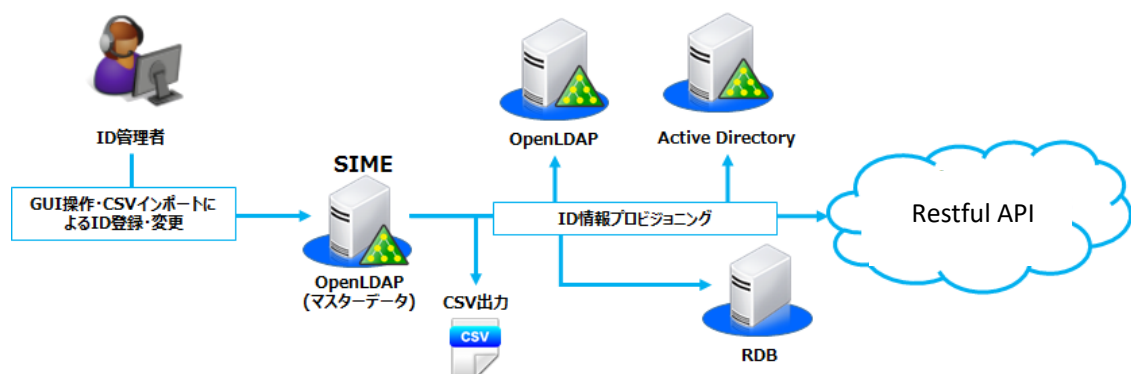


図 2 LISM 連携イメージ

## 2 インストールと設定

### 2.1 事前準備

LISM のシステム要件は以下の通りです。

表 1 LISM サーバスペック

環境	スペック
OS	CentOS7 / Redhat Enterprise Linux v7
ミドルウェア	Apache / OpenLDAP / PHP / Perl MariaDB / Memcached
ハードウェアスペック (最少スペック)	CPU : : 1CPU (2core) 以上 メモリ : 2GB 以上 ディスク空き容量 : 20GB 以上の空き

※ ハードウェアスペックは参考値です。利用 ID 数によって変わります。

LISM が必要とするパッケージは、インストール中に全て自動的に導入することが可能です（対話形式）。ただし、標準では含まれないパッケージを yum コマンド、或は rpm コマンドでインストールするため、EPEL リポジトリを導入する必要があります。

CentOS7 の場合

```
# yum install epel-release
```

Redhat Enterprise Linux v7 の場合

```
# rpm -ivh http://ftp.riken.jp/Linux/fedora/epel/epel-release-latest-7.noarch.rpm
```

LISM のご利用に当たり、OpenLDAP, MariaDB が必要なため、「9 参考」を参照していただき、事前に構築してください。また、LISM のインストールツールを実行する前に、必ず SELinux の無効化を実施してください。

## 2.2 インストール

LISM のパッケージファイルを展開し、インストールスクリプト (install.sh) を用いて以下のオプションでインストールします。

```
# ./install.sh install    (LISM をインストールします)
# ./install.sh update     (LISM をアップデートします)
# ./install.sh uninstall  (LISM をアンインストールします)
```

LISM アップデート、アンインストールを実施する場合、以下のフォルダをバックアップしてください。

- /opt/secioss
- /usr/share/seciossadmin
- /var/www

必要なパッケージが不足している場合、一覧表示され、自動的にインストールします。

```
eventlog が必要です。
httpd が必要です。
. . . .
yum リポジトリから必須パッケージをインストールします。よろしいですか？ [yes]
yes
```

## 2.3 セットアップツールによる初期設定

インストールが正常に完了すると、引き続き解凍された LISM パッケージフォルダの下にあるセットアップツール (setup.pl) が自動に起動し、設定項目に進めます。なお、セットアップツールの実行により再設定が可能です。

```
LISM のインストールが完了しました。
引き続き初期設定ツールを起動します。よろしいですか？ [yes]
```



“Enter”をクリックし、次へ進みます。

LISM は SELinux に対応していません。

SELinux を無効化してください。

SELinux が有効になっている場合には以下の画面が表示されます。

SELinux を一時的に無効にする場合以下実行してください。

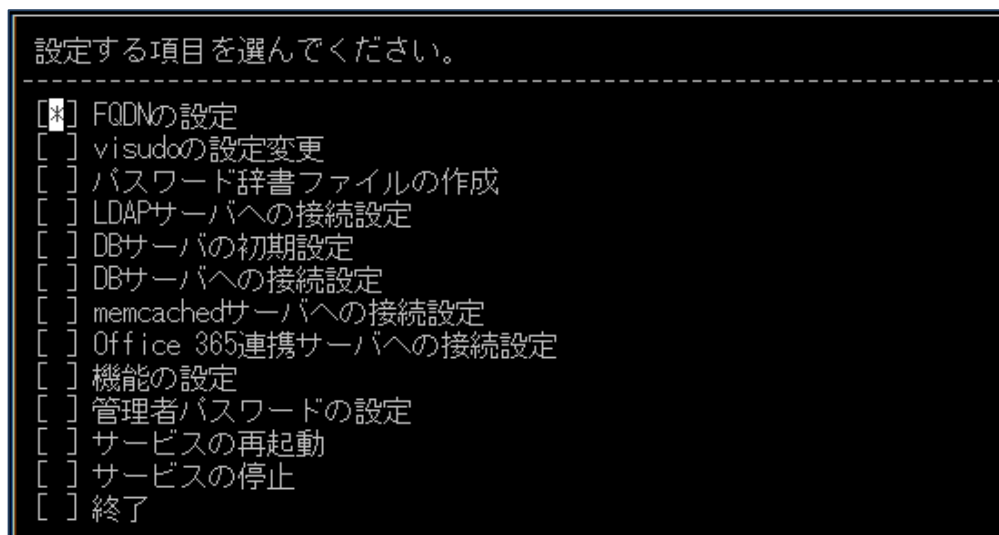
**# setenforce 0**

CentOS の場合、「/etc/sysconfig/selinux」ファイルの「SELINUX=」パラメータに「disabled」を設定するとコンピュータの再起動後も SELinux も無効になります。

SELINUXTYPE=disabled

以下のコマンドと設定に用いて、サーバの SELinux を無効化してください。

SELinux が無効化されている場合、以下の画面で各設定を行います。





### 2.3.1 FQDN の設定

ユーザがアクセスするサーバのホスト名を入力してください。

FQDN の設定を行います。

FQDN を入力してください。 (default: ...)

**LISM.secioss.com**

FQDN の設定が完了しました。

### 2.3.2 visudo の設定変更

sudo コマンドを利用するための設定を行います。

sudo の設定変更を行います。

requiretty を無効にします。よろしいですか？ [yes/no](default: yes)

**yes**

apache ユーザにコマンド実行時の昇格権限を付与します。よろしいですか？ [yes/no](default: yes)

**yes**

visudo の設定変更が完了しました。

### 2.3.3 パスワード辞書ファイルの作成

この辞書ファイルにはよくあるパスワード文字列や使用禁止文字列などが格納されており、パスワードポリシーのチェック時に利用されます。

パスワード辞書ファイルを作成します。

yum リポジトリから最新の辞書ファイルをインストールします。よろしいですか？ [yes/no](default: yes)

**yes**

パスワード辞書ファイルの作成が完了しました。

### 2.3.4 LDAP サーバへの接続設定

OpenLDAP サーバとの接続情報を入力し、設定を行います。

LDAP サーバの設定を行います。

LDAP-path を入力してください。 (default: ldap://localhost)

**ldaps://LISM.ldap.com**

BaseDN を入力してください。 (default: dc=example,dc=com)

**dc=LISM,dc=ldap,dc=com**

BindDN を入力してください。 (default: cn=Manager,dc=example,dc=com)

**cn=Manager,dc=LISM,dc=ldap,dc=com**

Password を入力してください。

\*\*\*\*\*

LDAP サーバへの接続設定が完了しました。

- LDAP-path: OpenLDAP の接続 URI
- BaseDN: 接続する OpenLDAP BaseDN
- BindDN: OpenLDAP に接続用アカウントの DN
- Password: BindDN のパスワード

接続する OpenLDAP サーバとの接続できない場合、LISM は動きません。構築された OpenLDAP に合わせて入力してください。OpenLDAP サーバが未構築の場合、本ドキュメント「9.1 OpenLDAP の構築」を参照して構築してください。

### 2.3.5 Memcached サーバへの接続確認

Memcached は LISM のセッション情報を管理するために利用するミドルウェアです。LISM インストール時に yum でインストールされます。本設定を行う前に、Memcached を起動してください。

#### #systemctl start memcached

Memcached は LISM と同一サーバに導入する場合「localhost:11211」を入力してください。

memcached サーバの設定をします。

memcached サーバを入力してください。カンマ区切りで複数指定できます。(default: localhost:11211)

**enter**

memcached サーバへの接続設定が完了しました。

### 2.3.6 管理者パスワードの設定

LISM Web 管理コンソールに接続する管理アカウント「admin」のパスワードを設定します。初期では本設定を行わない場合、「admin」ユーザでログインできません。必ず実施してください。

Secioss Identity Manager 管理者パスワードを設定します。

管理者パスワードを入力してください。

管理者パスワード(再入力)を入力してください。

\*\*\*\*\*

管理者パスワードの設定が完了しました。

### 2.3.7 サービスの再起動

LISM が利用するデーモンサービス（プロセス）の再起動を行います。初回設定あるいは、設定変更した場合必ず実行してください。

通常運用では再起動を行う必要はありませんが、設定変更や、メンテナンスなどによる OS の再起動や、LISM を一時停止するなどの場合、セットアップツールを起動し、本設定により必要とする全サービスを再起動することが可能です。

サービスの再起動を行います。

httpd を再起動しますか？ [yes/no](default: yes)

**yes**

syslog-ng を再起動しますか？ [yes/no](default: yes)

**yes**

openldap-lism を再起動しますか？ [yes/no](default: yes)

**yes**

sim-server を再起動しますか？ [yes/no](default: yes)

**yes**

sitaskctrl を再起動しますか？ [yes/no](default: yes)

**yes**

sitaskmgr を再起動しますか？ [yes/no](default: yes)

**yes**

httpd を再起動しています。

syslog-ng を再起動しています。

openldap-lism を再起動しています。

sim-server を再起動しています。

sitaskctrl を再起動しています。

sitaskmgr を再起動しています。

サービスの再起動が完了しました。

### 2.3.8 サービスの停止

LISM が利用するデーモンサービス（プロセス）を停止します。通常運用ではサービス停止を行うことはありませんが、LISM を一時的に停止する必要がある場合には、本設定を利用してください。

また、LISM 関連サービスの再起動は「サービスの再起動」を実施してください。

### 2.3.9 終了

初期設定ツールを終了します。

### 3 LISM WEB 管理コンソール

ID 管理者は LISM の Web 管理コンソールにアクセスし、ユーザ、グループの登録や ID 連携先システムの登録、ID の同期条件などを設定する必要があります。

Web 管理コンソールへのアクセス先 URL :

<https://<サーバホスト名>/seciossadmin/>

例) <https://IDM-Server.local/seciossadmin/>

Web 管理コンソールへアクセスするとログイン画面が表示されます。入力するユーザ ID は「admin」で、パスワードはセットアップツールの「管理者パスワードの設定」で設定したパスワードです。

図 3 LISM 管理コンソールログイン画面

この「admin」ユーザは Web 管理コンソールの「ユーザ」には表示されません。このまま「admin」ユーザを利用して運用するか、Web 管理コンソールから別途管理者アカウント作成した後、「admin」ユーザを削除するか、何れかの方法があります。






「admin」ユーザを削除する場合には、以下のファイル `/usr/share/seciossadmin/etc/passwd` を削除してください。

ログイン後、「ユーザー一覧」画面が表示されます。メニューは画面左側に、各種詳細情報が画面中央に表示されます。画面上部の折り畳みアイコンをクリックするとメニューの開閉ができます。また、表示フィルタアイコンをクリックすると表示する情報をフィルタすることができます。



図 4 ユーザー一覧表示

表 2 LISM メニュー

メニューアイコン	機能概要
 ユーザ	新規ユーザの登録や変更を行うことができます。CSV ファイルから一括で登録、更新、削除することもできます。登録された情報は連携先システムに同期することができます。
 組織	組織情報を登録することができます。CSV ファイルから一括で登録、更新、削除することもできます。
 ユーザグループ	グループ情報を登録することができます。CSV ファイルから一括で登録、更新、削除することもできます。
 統合ID管理	連携先システムの登録、同期条件などの登録を行います。本機能が統合 ID 管理の中核機能となります。Active Directory や LDAP、各種クラウドサービスの設定画面があります。
 システム	パスワードポリシーやメール送信時（パスワード期限切れ通知など）のフォーマットなどを設定することができます。

メニューにある機能について以降の各章で説明します。

## 4 ユーザ

メニューの「ユーザ」をクリックすると、ユーザー一覧表示や新規登録メニューが表示されます。

LISM で管理を行うユーザ情報が源泉となり、Active Directory やクラウドサービスなど、連携しているシステム、サービスに必要な情報を同期します。

表 3 ユーザメニュー

ユーザ	
一覧	登録されているユーザを一覧で表示します。操作アイコンによるユーザ情報の変更や削除もできます。
新規登録	ユーザの新規登録を行います。
csv 登録	CSV ファイルからユーザの一括登録、変更、削除します。

### 4.1 新規登録

メニューの「ユーザ」-「新規登録」をクリックすると画面からユーザの新規登録を行うことができます。必須項目、各属性に情報を入力し、画面下の「登録」ボタンをクリックしてください。

なお、ユーザをグループに所属させることや、追加情報として会社名や電話番号などの「連絡先情報」も入力することができますが、「グループ」への追加や「連絡先情報」はユーザ作成後に追加することが可能になります。

表 4 ユーザ情報項目一覧

項目名	説明
ユーザ ID	ユーザ ID は LISM で一意の値となります。
社員番号	ユーザの社員番号です。任意の値を入力してください。
氏名	ユーザの氏名です。
氏名 (かな)	ユーザの氏名のかな表記です。任意の値を入力してください。
別名	ユーザの別名です。任意の値を入力してください。
メールアドレス	ユーザのメールアドレスです。
メールエイリアス	ユーザのメールエイリアスです。
組織	ユーザの所属する組織を指定します。リストには、メニューの「組織」機能にて登録したものが表示されます。
地域	ユーザの地域です。リストから選択をしてください。
言語	ユーザの言語です。リストから選択をしてください。「日本語」、「英語」、「中国語」を設定した場合には LISM の Web 管理コンソールもそれぞれの言語に表示が変わります。 ※変更したユーザでログインすると設定した言語で表示されます。
パスワード	ユーザのパスワードです。LISM のパスワードポリシー（デフォルト:OFF）を設定している場合には、ポリシーに従ったチェックが行われます。
ユーザ状態	ユーザアカウントの状態です。「有効」、「無効」の設定ができます。

<b>権限</b>	<p>LISM に対する管理者権限の設定を行います。</p> <p>管理者権限を付加されたユーザのみ LISM の Web 管理コンソールにログインできます。</p> <p>管理者権限には 2 種類あります。</p> <p>1・特権管理者：全ての機能を使用することができます。</p> <p>2・ユーザ管理者：ユーザの管理機能のみ利用できます。</p> <p>「ユーザ管理者」権限は、管理対象の「組織」を指定することで、例えば各部署の責任者が自部署のメンバのみ操作する、というような要件に対応することができます。リストには、メニューの「組織」機能にて登録したものが表示されます。</p>
<b>許可するサービス</b>	<p>同期を行う対象システム、サービスを指定します。例えば、Active Direcotry、DB2 つのサービスにチェックが入っているユーザはそれぞれのサービスに ID 情報が同期されます。</p> <p>※統合 ID 機能にて、連携するシステム、サービスを設定していない場合には何も表示されません。</p>
<b>通知用メールアドレス</b>	<p>パスワードの初期化、パスワード有効期限の警告メール等の通知メールの送り先メールアドレスを設定します。</p> <p>※設定されない場合、通知メールはメールアドレスに登録されている宛先に送信されます。</p>

## 4.2 一覧表示・変更・削除

メニュー「ユーザ」をクリックすると登録されているユーザー一覧表示されます。



図 5 ユーザー一覧操作

表 5 ユーザー一覧操作機能

機能	詳細
表示フィルタ	指定した条件で表示する情報をフィルタすることができます。
操作アイコン	<div>✎</div> 該当ユーザ情報を変更します。詳細な「連絡先情報」や「グループ」への追加ができます。
	<div>✕</div> 該当ユーザを削除します。
削除ボタン	選択欄にチェックを行ったユーザを一括削除します。
ファイル出力ボタン	登録されている全ユーザを CSV ファイルで出力します。

ユーザ情報から、画面右上のタブにてユーザ「連絡先情報」の編集、グループ追加も可能です。



図 6 ユーザの連絡先情報、グループタブ



### 4.3 CSV 登録・変更・削除

CSV ファイルを利用することで一括してユーザを登録、変更、削除することができます。特に LISM への初期ユーザ登録作業時に有用な機能です。

メニューの「ユーザ」-「csv 登録」をクリックし、利用する csv ファイルをアップロード後、画面下の「登録」ボタンをクリックしてください。なお、ユーザを登録、更新する場合と削除する場合ではアップロードする画面が異なります。画面右上の「登録」タブ、「削除」タブを切り替えて、csv ファイルを登録してください。



図 7 CSV による「登録」「削除」タブ

以下に登録・変更用 csv ファイルのフォーマットを記載します（csv 登録画面にも表示されています）。ただし、連携サービスによって項目が増えるものもありますので、必ずしもカラム数は固定されません。例えば Office365 との連携設定が完了していると「簡易表示名」や「アドレス帳表示」の項目が追加されます。

必須項目には必ず値を入力してください。また、ユーザ ID がキーとなっているため、既に存在する場合には上書き更新となります。

表 6 CSV ユーザ登録フォーマット一覧

No	項目名	説明
1	ユーザ ID※必須	例) Test_User_001
2	社員番号	例) 001
3	姓※必須	例) テスト
4	名※必須	例) ユーザ 0 1
5	姓 (かな)	例) てすと
6	名 (かな)	例) ゆーざ

7	メールアドレス※必須	例) Test_User@secioss.co.jp
8	メールエイリアス	例) Test_User_001@secioss.co.jp
9	地域※必須	言語と国名を表す 2 文字のコードを"_"で連結した値を登録します。日本の場合「ja_JP」
10	言語※必須	CSV ファイル登録では日本語(ja)、英語(en)、中国語(zh)のうち 1 つを指定してください。
11	パスワード※必須	例) Password CSV ファイル上のカラムが空白の場合、変更なし。
12	ユーザ状態※必須	有効・・・active 無効・・・inactive
13	管理権限	特権管理者・・・system_admin ユーザ管理者・・・user_admin ユーザ管理者の場合、管理する組織を指定することができます（指定しない「全て」となります）。組織は登録されたものを指定してください。設定方法は「user_admin=上位組織/組織」です。例) user_admin=本社/開発部
14	サービス	ユーザに許可するサービスを「サービス名=ルール 1&ルール 2&...」の形式で登録して下さい。ルールはサービス毎の権限です。設定可能なサービスについて CSV 登録画面を参考してください。 例) Office365=Exchange Online&SharePoint Online
15	組織	「上位組織/組織」の形式で指定してください。 例) 本社/開発部
16	別名	例) セシオステストユーザ
31	通知用メールアドレス	例) secioss@gmail.com

CSV によるユーザの削除の場合、CSV ファイルフォーマットは「ユーザ ID」のみとなります。

## 5 組織

Web 管理コンソールのメニュー「組織」をクリックすると、メニュー一覧が表示されます。

表 7 組織メニュー

組織	
一覧	登録されている組織を一覧表示します。表示画面から、組織情報の変更や削除を行うこともできます。
新規登録	組織の新規登録を行います。
CSV 登録	CSV ファイルから組織情報の一括登録、変更、削除します。

### 5.1 新規登録

メニューの「組織」-「新規登録」をクリックすると画面から組織の新規登録を行うことができます。必須項目、各属性に情報を入力し、画面下の「登録」ボタンをクリックしてください。

表 8 組織項目一覧

項目名	詳細
上位組織	上位組織がある場合、上位となる組織を選択してください。
組織名	組織を識別する一意の名称を入力してください。
説明	組織の説明欄です。



### 5.2 組織の一覧表示・変更・削除

メニューの「組織」をクリックすると登録されている組織が一覧表示されます。



図 8 組織一覧操作

表 9 組織一覧操作機能

機能	詳細
表示フィルタ	指定した条件で表示する情報をフィルタすることができます。
操作アイコン	 該当組織の情報を変更します。
	 該当組織を削除します。
削除ボタン	選択された組織を一括削除します。下位の組織が所属している場合削除できません。
ファイル出力ボタン	登録されている全組織を csv ファイルで出力します。

### 5.3 CSV 登録・変更・削除

CSV ファイルから一括して組織を登録、変更、削除することができます。メニューの「組織」-「CSV 登録」をクリックし、利用する CSV ファイルをアップロード後、画面下の「登録」ボタン、或は「削除」ボタンをクリックしてください。

以下に登録・変更・削除用 CSV ファイルのフォーマットを記載します（CSV 登録画面にも表示されています）。必須項目には必ず値を入力してください。また、組織名がキーとなっているため、既に存在する場合には上書き更新となります。

【登録・変更用 CSV ファイルフォーマット】

表 10 CSV 組織登録フォーマット

No	項目名	詳細
1	組織名 ※必須項目	例) 開発部
2	説明	例) 開発業務を行う部署
3	上位組織	例) 本社 （値がない場合には上位組織は空白となります。）

【削除用 CSV ファイルフォーマット】

表 11 CSV 組織削除フォーマット

No	項目名	詳細
1	組織名 ※必須項目	例) 開発部
2	上位組織	例) 本社

## 6 ユーザグループ

Web 管理コンソールのメニュー「ユーザグループ」から、グループ一覧表示やフラット構造のユーザグループを新規登録できます。

ユーザグループ及びメンバ情報は Active Directory のセキュリティグループや、クラウドサービスのメーリングリストとして情報を同期することができます。

表 12 ユーザグループメニュー

ユーザグループ	
一覧	登録されているユーザグループを一覧表示します。表示画面から、ユーザグループ情報の変更や削除を行うこともできます。
新規登録	ユーザグループの新規登録を行います。
CSV 登録	CSV ファイルからユーザグループ情報の一括登録、変更、削除します。

### 6.1 新規登録

メニュー「ユーザグループ」-「新規登録」をクリックすると画面からユーザグループの新規登録を行うことができます。各項目に情報を入力し、画面下の「登録」ボタンをクリックしてください。

なお、一部の項目は連携先サービスの設定を行っていると表示されます。ユーザグループへのメンバ追加や削除、メンバの一覧表示はユーザグループ作成後の設定となります。また、ユーザグループ項目がサービス側のどの属性に同期されるかは、「**エラー! 参照元が見つかりません。エラー! 参照元が見つかりません。**」を参照してください。

表 13 ユーザグループ項目一覧

項目名	詳細
グループ名	グループ名で、一意の値を入力してください。
表示名	Google Apps のグループ名、Office 365 の表示名になります。
メールアドレス	Google Apps にはメールアドレスを登録した場合のみグループが同期されます。Office 365 にはメールアドレスを登録した場合、「配布グループ」または「セキュリティグループ」として、メールアドレスを登録していない場合には「セキュリティグループ」として同期します。
説明	任意の値を入力してください。

### 6.2 一覧表示・変更・削除

メニューの「ユーザグループ」-「一覧」をクリックするとユーザグループが一覧表示されます。



図 9 ユーザグループ操作一覧

表 14 ユーザグループ操作機能一覧

機能	詳細
表示フィルタ	指定した条件で表示する情報をフィルタすることができます。
操作アイコン	該当ユーザグループの情報を変更します。
	該当ユーザグループを削除します。
削除ボタン	選択欄にチェックを行ったユーザグループを一括削除します。
ファイル出力ボタン	登録されている全ユーザグループを csv ファイルで出力します。

※「上位グループ」に所属されたグループ ID が表示されます。所属する上位グループが削除された場合、暫く「上位グループ」に表示される場合があります。

ユーザグループ情報の変更中、メンバー一覧の表示やメンバ追加、削除が可能です。画面右上のタブをクリックしてください。

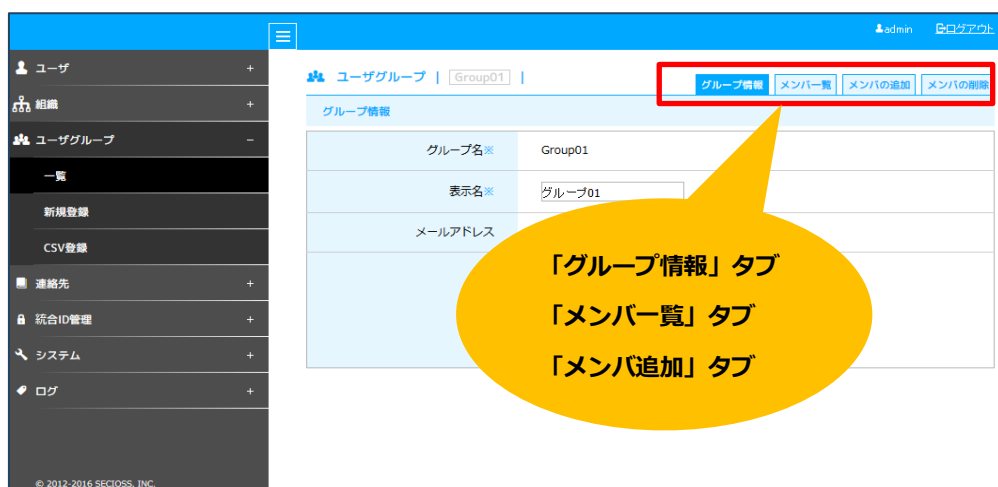


図 10 メンバー一覧、追加、削除タブ

表 15 グループメンバータブ

機能	詳細
グループ情報	グループ情報の変更ができます。
メンバー一覧	<p>所属しているメンバー一覧を表示します。</p> <div> <div>サービスへ強制同期</div> <div>・・・メンバ情報を強制同期する機能です。本機能は同期しているサービスに対して、強制的にメンバ情報を上書きします。例えば、サービス側のグループを直接操作するなど、LISM 側と差異が発生した場合に利用します。</div> </div>
メンバ追加	メンバの追加を行います。ユーザ、グループ、連絡先からメンバを検索し、追加してください。また、CSV ファイルからメンバを一括登録することができます。
メンバ削除	メンバの削除を行います。現在、所属しているメンバを表示し、削除してください。また、CSV ファイルからメンバを一括削除することができます。

ユーザグループへメンバ追加、削除を行う場合、以下 CSV フォーマットで、それぞれ「メンバ追加」、「メンバの削除」のタブ画面で行います。

表 16 CSV によるグループメンバー登録・削除

項目名	詳細
ユーザ ID で登録・削除する場合	ユーザ ID,user 例) test001,user
グループ名で登録・削除する場合	グループ名,group 例) Group01,group

### 6.3 CSV 登録・変更

メニューの「ユーザグループ」-「CSV 登録」から、CSV ファイルから一括してユーザグループを登録、変更できます。

以下に登録・変更用 CSV ファイルのフォーマットを記載します（CSV 登録画面にも表示されています）。必須項目には必ず値を入力してください。また、グループ名がキーとなっているため、既に存在する場合には上書き更新となります。

表 17 CSV グループ登録フォーマット

No	項目名	詳細
1	グループ名 ※必須項目	例) Group01
2	表示名 ※必須項目	例) メーリングリスト 01
3	メールアドレス	例) Group01@secioss.co.jp
4	説明	例) 部門メーリングリストで利用

## 7 統合 ID 管理

メニュー「統合 ID 管理」をクリックすると、LISM と連携するシステム、サービスの設定を行います。

「統合 ID 管理」は LISM の中核機能であり、LISM の管理用 OpenLDAP に登録された情報を、どのシステムにどのような条件で同期するか、細かく設定できます。インポート、エクスポートの CSV フォーマットを自由に設計でき、LDAP や DB から ID 情報を取得し、LISM に取り込む設定なども可能です。

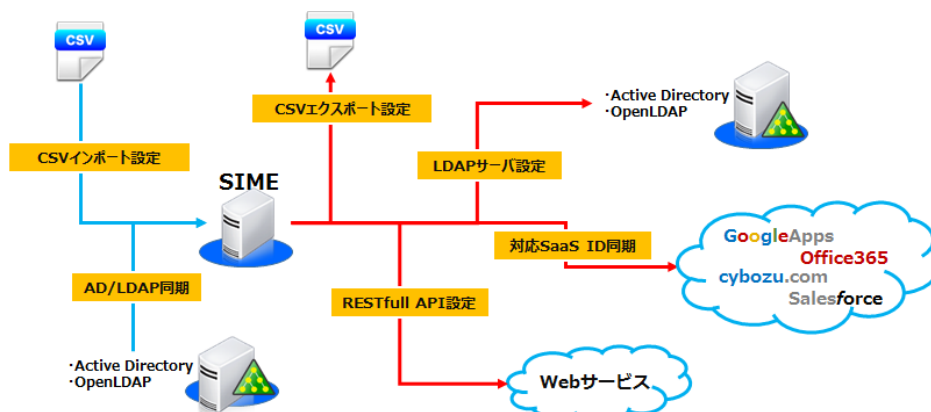


図 11 LISM 連携イメージ

表 18 統合 ID 管理メニュー

統合 ID 管理	
同期システム一覧	連携しているシステム、サービスが一覧で表示されます。 該当登録システムを編集します。 該当登録システムを削除します。 システムを複数選択し、「削除」ボタンで一括削除ができます。 ※メニューに表示されているシステムは削除できません。
マスタ LDAP サーバ設定	マスタデータとする LDAP サーバと連携し、定期的に LISM がデータ情報を取得します。
マスタ DB 設定	マスタデータとする DB サーバと連携し、定期的に LISM がデータ情報を取得します。
CSV インポート設定	LISM に取り込む CSV ファイルのフォーマットを規定します。
LDAP サーバ設定	LISM をマスタデータとして、ID 情報を Active Directory、OpenLDAP へ同期を行います。
DB 設定	LISM をマスタデータとして、ID 情報を DB へ同期を行います。
CSV エクスポート設定	LISM から出力する CSV ファイルのフォーマットを規定します。
RESTful API 設定	REST API を備えた Web サービスに対して API を実行する設定を行います。具体的な設定は Web サービス側の仕様に依存します。
追加属性	各設定項目を増やす場合、ここで追加設定を行います。

以降、各設定の詳細について記載します。

### 7.1 同期システム一覧

同期設定が行われ連携システムの一覧になります。すでに、設定が行われた場合この項目をクリックし、操作アイコンにより、設定内容の詳細を表示し、削除、変更などを行ってください。



## 7.2 マスタ LDAP サーバ設定

左メニューの「統合 ID 管理」 - 「マスタ LDAP サーバ設定」をクリックすると LISM にデータを同期するマスタ LDAP サーバを登録することができます。マスタ LDAP サーバのユーザ情報、グループ情報、組織情報は、定期的 LISM に同期されます。

表 19 マスタ LDAP サーバの設定項目

項目名	説明
システム ID	システムを識別する ID
LDAP サーバの種類	LDAP サーバの週類 (Active Directory LDAP サーバ)
LDAP サーバの URI	LDAP サーバの URI 例 : ldaps://192.168.1.100
LDAP サーバのベース DN	LDAP サーバの同期対象となるエントリのベース DN 例 : dc=example,dc=com
LDAP サーバユーザ名	LDAP サーバに接続するユーザの DN 例 : cn=Manager,dc=example,dc=com
LDAP サーバパスワード	LDAP サーバに接続するパスワード
同期の実行※1	同期を実行するかどうか
同期条件※1	同期対象となるエントリの条件 (LDAP の検索フィルタ形式) 例 : (objectClass=inetOrgPerson)
更新の種類※1	同期を実行する更新の種類 (追加 変更 削除)
ベース DN※1	LDAP サーバから同期するエントリのベース DN 例 : ou=Users
属性※1	LDAP サーバから同期する属性 “同期元”は LDAP サーバの属性名、“同期先”は LISM 側の属性名です。
デフォルト値※1	LISM にエントリを追加する際のデフォルト値 “属性名”に LISM の属性名、“値”にデフォルト値を設定して下さい。 “値”には、“%(関数名(引数))”の形式で関数を実行した値を設定することができます。引数には LDIF 形式の更新データを%0 として使用することができます。
属性値変換	LISM に同期する属性値の変換を行うことができます。  <ul style="list-style-type: none"> <li>変換条件 属性名: 変換対象の属性名 例 : mail</li> <li>変換条件 フィルタ : 変換対象となるエントリを LDAP の検索フィルタで指定 例 : (seciossAccountStatus=active)</li> <li>変換前 : 変換前の値</li> <li>変換後 : 変換後の値 “変換後”には、パターングループにマッチした値を“%数字”の形式で設定するこ</li> </ul>

	とや、“%{関数名(引数)}”の形式で関数を実行した値を設定することができます。 また、LDIF 形式の更新データを%0 として使用することができます。
--	---

※1：ユーザ情報、グループ情報、組織情報についてそれぞれ設定を行います。

## 7.3 マスタ DB 設定

左メニューの「統合 ID 管理」-「マスタ DB 設定」をクリックすると LISM にデータを同期するデータベースを登録することができます。マスタ DB のユーザ情報、グループ情報、組織情報は、定期的に LISM に同期されます。

表 20 マスタ DB 設定項目

項目名	説明
システム ID	システムを識別する ID
DB サーバの種類	データベースサーバの種類（MySQL PostgreSQL）
DB サーバのホスト名	データベースサーバのホスト名
データベース名	接続するデータベース名
DB サーバユーザ名	データベースサーバに接続するユーザ名
DB サーバパスワード	データベースサーバに接続するパスワード
同期の実行※1	データの同期を行うかどうか
同期の条件※1	同期対象となるエントリの条件（LDAP の検索フィルタ形式） 例：(objectClass=inetOrgPerson)
更新の種類※1	同期を実行する更新の種類（追加 変更 削除）
テーブル名※1	データベースのテーブル名 例：users
ID のカラム名※1	テーブル内の ID のカラム名 例：user_id
検索条件 SQL※1	同期対象となるレコードを検索する際の検索条件（SQL 形式） 例：deleted = 0
属性※1	登録する属性 “カラム名”はテーブルのカラム名、属性名は LISM の属性名です。
属性(SQL)※1	登録する属性。属性値をデータベースに対して SELECT を実行して取得します。 ・属性名：LISM の属性名 ・カラム：SELECT 文のカラム名 ・FROM：SELECT 文の FROM 句 ・WHERE：SELECT 文の WHERE 句 %o は“ID のカラム名”で設定したカラムの値に変換されます。

デフォルト値※ <sup>1</sup>	LISM にデータを登録する際のデフォルト値 “属性名”に LISM の属性名、“値”にデフォルト値を設定して下さい。 “値”には、“%{関数名(引数)}”の形式で、関数を実行した値を設定することもできます。
属性値変換※ <sup>1</sup>	LISM にインポートするエントリの属性名、値の変換を行うことができます。 <ul style="list-style-type: none"> <li>変換条件 属性名：変換対象の属性名 例：mail</li> <li>変換条件 フィルタ：変換対象となるエントリを LDAP の検索フィルタで指定 例：(objectClass=inetOrgPerson)</li> <li>変換前：変換前の値</li> <li>変換後：変換後の値</li> </ul> “変換後”には、“%{関数名(引数)}”の形式で、関数を実行した値を設定することもできます。

※<sup>1</sup>：ユーザ情報、グループ情報、組織情報についてそれぞれ設定を行います。

## 7.4 LDAP サーバ設定

メニューの「統合 ID 管理」-「LDAP サーバ設定」をクリックすると連携先ディレクトリサーバの新規設定を行います。

### 7.4.1 連携先 LDAP サーバの設定項目

連携先ディレクトリサーバの設定を行います。対象となるディレクトリサーバは、Active Directory と OpenLDAP です。

連携先システム設定を行ってから最大 20 分で設定内容が反映されます。その後、「ユーザ」、「グループ」、「組織」の管理を行い、情報の追加、変更、削除が行われたタイミングで連携先へ同期されます。

表 21 連携先 LDAP 設定項目一覧

項目名	詳細
システム ID	連携先システムを識別する一意の ID です。(半角英数のみの入力になります)
LDAP サーバの種類	LDAP サーバの種類を選択します。
LDAP サーバの URI	LDAP サーバの URI を入力します。 例) ldaps://192.168.1.100
LDAP サーバのベース DN	同期先に同期されるベース DN を指定します。 例) ou=sync,dc=example,dc=com
LDAP サーバユーザ名	LDAP サーバに接続するユーザの DN です。例) cn=Administrator,cn=Users,dc=example,dc=com
LDAP サーバパスワード	LDAP サーバに接続するユーザのパスワードを入力します。
パスワードハッシュ形式	LDAP サーバにパスワードを格納するときのハッシュ形式を選択します。 Active Directory の場合は「Active Directory」 LDAP サーバの場合：PAAINIEXT CRYPT MD5 SHA
同期の実行※ <sup>1</sup>	更新のタイミングで、同期を実行するかどうか設定します。
同期条件※ <sup>1</sup>	<ul style="list-style-type: none"> <li>「許可するサービスに表示」をチェックする場合：システム ID はユーザ情報「許可するサービス」項目に表示され、ユーザの「許可するサービス」としてチェックされれば、エクスポート対象となります。</li> <li>「許可するサービスに表示」をチェックしない場合：同期対象となるエントリの条件を LDAP の検索フィルタ形式で設定します。LISM が持つ OpenLDAP から同期対象となるエントリを絞り込む。例えば、アカウントステータスが「active」のユーザが同期対象とする場合“(seciossAccountStatus=active)” と入力します。</li> </ul>
更新の種類※ <sup>1</sup>	同期を行う処理（追加 変更 削除）を選択します。例えば削除は手動で行うような運用の場合には「削除」のチェックを外してください。

<b>オブジェクトクラス※1</b>	同期したエントリのオブジェクトクラスを指定します。例えば Active Directory の場合、ユーザ：user、グループ：group、組織：organizationalUnit
<b>RDN の属性※1</b>	同期先 RDN の属性を指定します。例えば Active Directory の場合、ユーザ、グループ：cn、組織：ou
<b>属性※1</b>	LDAP サーバに同期する属性をマッピングします。“同期元”は LISM の管理用 OpenLDAP に格納されている属性名で、“同期先”は連携先 LDAP サーバの属性名です。
<b>デフォルト値※1</b>	LDAP サーバにエントリを追加する際、指定した属性名にデフォルト値を設定できます。例えば Active Directory の場合、「userAccountControl」属性に値を設定しないと無効状態で作成されるため、デフォルト値として「512」を設定します。 “属性名”に連携先 LDAP サーバの属性名、“値”にデフォルト値を設定して下さい。値には、固定値以外に、“%(関数名(引数))”の形式で関数※2を用いて値をセットできます。。 例えば Active Directory の「userPrincipalName」に値を設定する場合“%{getValue(\$entryStr, 'uid')}@example.com”とすることで uid 属性とドメインを組み合わせた値を AD ユーザ情報に設定し、AD に同期します。
<b>変換ルール</b>	LISM の管理 LDAP から連携先 LDAP サーバに同期する際、エントリの DN、属性名、属性値を連携先の構成に合わせて変換を行うことができます。 ・変換条件 DN：変換対象となるエントリの DN を正規表現で指定 例) ou=People, ・変換条件 フィルタ：変換対象となるエントリを LDAP の検索フィルタで指定 例) objectClass=inetOrgPerson ・変換前：変換前の正規表現値 ・変換後：変換後の正規表現値 “変換後”には、パターングループにマッチした値を“%数字”の形式で設定することや、“%(関数名(引数))”の形式で関数を実行した値を設定することができます。また、LDIF 形式の更新データを%0 として使用することができます。 例：LISM 側のユーザを AD の ou=user, ou=sync,dc=example,dc=com の配下に同期したい場合以下の設定になります。 変換条件 DN：ou=People, 変換前：ou=People, 変換後：ou=user,
<b>コマンド実行</b>	連携先 LDAP サーバへのエントリの更新後に実行するコマンドを設定できます。例えば、ユーザ作成時にホームディレクトリを作成するプログラムを起動するといった場合 ・実行条件 DN：変換対象となるエントリの DN を正規表現で指定 例) ou=People, ・実行条件 属性値：変換対象となるエントリの属性値を正規表現で指定 例) mail:.*@example.com ・追加 コマンドライン：LDAP サーバへエントリ追加時に実行するコマンドライン ・変更 コマンドライン：LDAP サーバのエントリ変更時に実行するコマンドライン ・削除 コマンドライン：LDAP サーバのエントリ削除時に実行するコマンドライン ※コマンドは 1 エントリの更新毎に実行されます。

※1 ユーザ、グループ、組織共通設定になります ※2 使用可能な関数は「7.10 関数一覧」を参照ください

7.4.2 Active Directory との連携設定例

本節では、「7.4.1」を基に、Active Directory と連携する場合の基本的な同期設定例を記述します。LISM 側の組織、ユーザ、ユーザグループ及びそのメンバー情報を AD に同期します。AD 側との同期ツリー構造は以下のようなイメージになります。

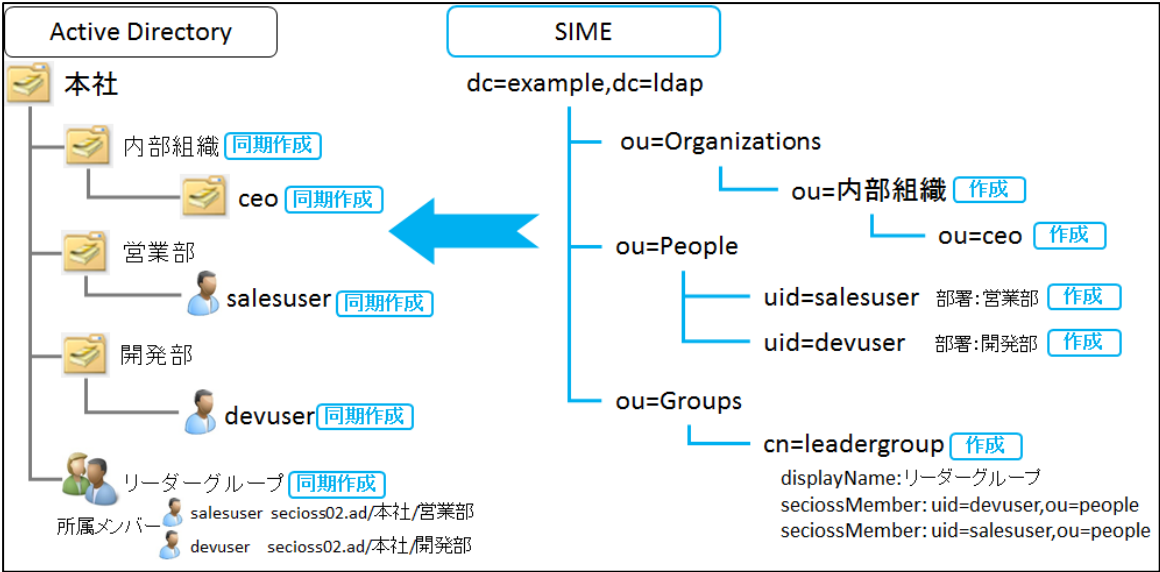


図 12 AD と LISM の連携イメージ

AD 側既存組織は「本社」「営業部」「開発部」の三つとなります。LISM 側で作成された組織、ユーザ、ユーザグループ及びメンバ情報が下記表の同期設定により、AD 側に作成されます。

表 22 AD へ同期設定例

LDAP サーバ設定					
システム ID		AD138			
LDAP サーバの種類		Active Directory			
LDAP サーバの URI		ldaps://192.168.1.138			
LDAP サーバのベース DN		DC=secioss02,DC=ad			
LDAP サーバユーザ名		CN=Administrator,CN=Users,DC=secioss02,DC=ad			
LDAP サーバパスワード		****			
パスワードハッシュ形式		Active Directory			
ユーザ	同期の実行	「許可するサービスに表示」をチェック			
	同期条件	(objectClass=inetOrgPerson)			
	更新の種類	追加、変更、削除 全チェック			
	オブジェクトクラス	user			
	RDN の属性	cn			
	属性	同期元	uid	同期先	cn
		同期元	uid	同期先	sAMAccountName
		同期元	sn	同期先	sn
		同期元	givenName	同期先	giveName
		同期元	userPassword	同期先	unicodePwd

	デフォルト値	属性名	userAccountControl	値	512※1
		属性名	userPrincipalName	値	%{getValue(\$entryStr, 'uid')}}@secioss02.ad ※2
		属性名	displayname	値	%{getValue(\$entryStr, 'sn')}} %{getValue(\$entryStr, 'givenName')}
グループ	同期の実行	有効チェック			
	同期条件	(objectClass=seciossGroup)			
	更新の種類	追加、変更、削除 全チェック			
	オブジェクトクラス	group			
	RDN の属性	cn			
	属性	同期元	cn	同期先	sAMAccountName
		同期元	displayname	同期先	cn
		同期元	description	同期先	description
		同期元	seciossMember	同期先	member
	デフォルト値	属性名		値	
組織	同期の実行	有効チェック			
	同期条件	(objectClass=organizationalUnit)			
	更新の種類	追加、変更、削除 全チェック			
	オブジェクトクラス	organizationalUnit			
	RDN の属性	ou			
	属性	同期元	ou	同期先	ou
		同期元	description	同期先	description
	デフォルト値	属性名		値	
変換ルール	変換条件 DN	ou=People,		フィルタ	
	変更前	cn=([^\,]+),ou=people,		変更後	cn=%1,ou=%{searchAttr('seciossDepartment', '(uid=%1')}}),ou=本社, ※3
	変換条件 DN	ou=Groups,		フィルタ	
	変更前	sAMAccountName=([^\,]+),ou=Groups,		変更後	cn=%{searchAttr('displayName', '(cn=%1')}}),ou=本社,
	変換条件 DN			フィルタ	
	変更前	member: [^=]+=([^\,]+),ou=groups,.*		変更後	member: %{searchdn('(cn=%1')}})
	変換条件 DN			フィルタ	
	変更前	member: [^=]+=([^\,]+),ou=people,.*		変更後	member: %{searchdn('(cn=%1')}})
	変換条件 DN	ou=Organizations,		フィルタ	
	変更前	ou=Organizations,		変更後	ou=本社,

※1 この設定は必須になります。設定されない場合ログインできません。設定値 512 の場合、AD 側の一般ユーザになります。設定値 66048 の場合、パスワード無期限のユーザとなります。※2 “secioss02.ad”は AD ドメインとなります。環境に合わせて変更してください。※3 “本社”は AD 側同期先の ou となります。環境に合わせて設定してください。語尾にあるカンマに注意してください。

OpenLDAP と Active Directory の構造は異なるため、変換ルールの項目にて、正規表現を利用して AD 側ツリー構造、対象 DN を合わせます。

例えば、LISM 側 LDAP の DN に「uid=devuser,ou=people」があり、AD 側の属性設定の「同期元：uid ⇒ 同期先：cn」により、変更前の正規表現以下となります。

**`cn=([^\,]+),ou=people,`**

AD 側の対象 DN に合わせるため、変更後は以下の正規表現で書き直します。

**`cn=%1,ou=%{searchAttr('seciossDepartment', 'uid=%1')},ou=本社,`**

設定完了後、LISM の管理コンソールにて、ID 管理を行い、更新情報は AD へ同期されます。

### 7.4.3 動作確認

設定保存後、「保存」ボタンの横にある「動作確認」から、同期する予定のデータ情報を確認できます。ここでは、データ構成をチェックすることによって、同期項目は正しく設定されたか否かを確認する目的になります。

動作確認	
同期対象	devuser    種類 ユーザ    更新の種類 追加
結果	<pre>dn: cn=devuser,ou=開発部,ou=本社,DC=secioss02,DC=a changetype: add cn: devuser sAMAccountName: devuser sn: 開発 givenname: 太郎 unicodePwd: [SHA]IRxUJG6PL3x8zgB2bT+I0I+CcAE= userAccountControl: 512 userPrincipalName: devuser@secioss02.ad displayName: 開発 太郎 objectClass: user</pre>

実行    戻る

図 13 LDAP サーバ設定動作確認

同期対象の種類（ユーザ | グループ | 組織）、及び更新種類（追加 | 変更 | 削除）を選択し、ターゲットとなる対象の ID を入力し、実行をクリックしますと、設定内容に従って同期する予定のデータ内容が結果に出力されます。

## 7.5 DB 設定

左メニューの「統合 ID 管理」 - 「DB 設定」をクリックすると同期対象のデータベースを登録します。

表 23 DB 連携設定項目

項目名	説明
システム ID	システムを識別する ID
DB サーバの種類	データベースサーバの種類 (MySQL PostgreSQL)
DB サーバのホスト名	データベースサーバのホスト名
データベース名	接続するデータベース名
DB サーバユーザ名	データベースサーバに接続するユーザ名
DB サーバパスワード	データベースサーバに接続するパスワード
文字コード	データベースの文字コード
パスワードハッシュ形式	ユーザ情報のパスワードのハッシュ形式
同期の実行※ <sup>1</sup>	データの同期を行うかどうか
同期条件※ <sup>1</sup>	同期対象となるエントリの条件 (LDAP の検索フィルタ形式) 例 : (objectClass=inetOrgPerson)
更新の種類※ <sup>1</sup>	同期を実行する更新の種類 (追加 変更 削除)
テーブル名※ <sup>1</sup>	データベースのテーブル名 例 : users
ID のカラム名※ <sup>1</sup>	テーブル内の ID のカラム名 例 : user_id
属性※ <sup>1</sup>	登録する属性。属性名は LISM の属性名、“カラム名”はテーブルのカラム名です。
属性(SQL)※ <sup>1</sup>	登録する属性。属性値の登録、取得を行う際にデータベースに対して SQL を実行します。 <ul style="list-style-type: none"><li>・ 属性名 : LISM の属性名</li><li>・ 追加 SQL : 値を追加する SQL 文</li><li>・ 削除 SQL : 値を削除する SQL 文</li><li>・ 検索カラム : SELECT 分のカラム名</li><li>・ FROM : SELECT 文の FROM 句</li><li>・ WHERE : SELECT 文の WHERE 句</li></ul> %o は“ID のカラム名”で設定したカラムの値に、%a は属性値に変換されます。
デフォルト値※ <sup>1</sup>	データを登録する際のデフォルト値 “カラム名”にテーブルのカラム名、“値”にデフォルト値を設定して下さい。 “値”には、“%(関数名(引数))”の形式で関数を実行した値を設定することができます。 引数には LDIF 形式の更新データを%0 として使用することができます。
デフォルト値(SQL)※ <sup>1</sup>	データを登録する際のデフォルト値 “SQL”に実行する SQL 文、“値”にデフォルト値を設定して下さい。 %o は“ID のカラム名”で設定したカラムの値に、%a はデフォルト値に変換されます。
属性値変換※ <sup>1</sup>	LISM からエクスポートするエントリの属性値の変換を行うことができます。



	<ul style="list-style-type: none"> <li>・変換条件 属性名：変換対象の属性名 例：mail</li> <li>・変換条件 フィルタ：変換対象となるエントリを LDAP の検索フィルタで指定 例：(objectClass=inetOrgPerson)</li> <li>・変換前：変換前の値</li> <li>・変換後：変換後の値</li> </ul> <p>“変換後”には、“%(関数名(引数))”の形式で関数を実行した値を設定することができます。引数には LDIF 形式の更新データを%0 として使用することができます。</p>
論理削除	<p>削除の際にレコードを削除せずに、設定したカラムの値を変更します。</p> <ul style="list-style-type: none"> <li>・有効：論理削除を行う場合にチェック</li> <li>・カラム名：削除時に変更するカラム名</li> <li>・値：削除時に変更する値</li> </ul>

※1：ユーザ情報、グループ情報、組織情報についてそれぞれ設定を行います。

## 7.6 CSV インポート設定

本機能の設定により、複数の独自 CSV フォーマットを用いて「ユーザ」、「グループ」、「組織」情報を一括してデータを投入することが可能になります。

### 7.6.1 独自 CSV フォーマットと LISM の属性マッピング

メニューの「統合 ID 管理」-「CSV インポート設定」をクリックすると独自フォーマット CSV ファイルに対する設定を新規で作成します。すでに作成した設定内容の表示、変更については「同期システム一覧」から行ってください。

表 24 CSV インポート設定項目一覧

項目名	詳細
システム ID	連携先システムを識別する一意の ID です。(半角英数のみの入力になります)
同期の実行※1	データのインポートを実行するかどうか設定します。
追加/変更の条件※1	インポートする CSV ファイル中の属性値に従って、追加・変更を実施します。例えば、“seciossAccountStatus=active”と入力した場合、属性名「seciossAccountStatus」の属性値が「active」の場合、該当レコードのユーザの追加・変更が可能となります。
削除の条件※1	「追加/変更の条件」項目同様、例えば、“seciossAccountStatus=delete”と入力した場合、属性名「seciossAccountStatus」の属性値が「delete」のユーザを削除します。
属性※1	インポートする CSV のカラム番号と LISM 側属性とマッピングします。
デフォルト値※1	LISM 側の属性にデフォルト値を設定します。固定値以外に、“%(関数名(引数))” ※2 の形式で、CSV から値を取得することもできます。 例えば「displayName」の値は CSV ファイルカラム 1 番と 2 番を合わせた値にする場合 %{getValue(\$entryStr, 'column1')} %{getValue(\$entryStr, 'column2')}
属性値変換※1	インポートするエントリの属性名、値の変換を行うことができます。 <ul style="list-style-type: none"> <li>・属性名：変換対象の属性名 例)mail</li> <li>・フィルタ：変換対象となるエントリを LDAP の検索フィルタで指定 例) objectClass=inetOrgPerson</li> <li>・変換前：変換前の値</li> <li>・変換後：変換後の値 (“%(関数名(引数))”の形式で、関数を実行した値で設定できます。</li> </ul>

※1 ユーザ、グループ、組織共通設定になります。 ※2 使用可能な関数は「7.10 関数一覧」を参照ください。

### 7.6.2 動作確認

設定保存後、「保存」ボタンの横にある「動作確認」から、インポートする予定のデータ情報を確認できます。ここでは、データ構成をチェックすることによって、同期項目は正しく設定されたか否かを確認する目的になります。

動作確認	
種類	ユーザ
CSV レコード	devuser02,開発,次郎,jiro@mail.com,active,ja,JP_ja>Password
結果	<pre>dn: uid=devuser02,ou=People,ou=importouri,dc=sime,dc=ldap,dc=net objectclass: person objectclass: organizationalperson objectclass: inetorgperson objectclass: seciossperson objectclass: seciossiamaccount seciossaccountstatus: active userpassword: Password uid: devuser02 seciossContactAttribute1: sime_import givenname: 次郎 preferredlanguage: ja sn: 開発 mail: jiro@mail.com seciosslocalecode: JP_ja</pre>

実行 戻る

図 14 CSV インポート設定動作確認

インポートする種類（ユーザ | グループ | 組織）を選択し、設定されたカラム順にテスト用の csv レコードを入力し、実行をクリックしますと、設定内容に従ってインポートする予定のデータ内容が結果に出力されます。

### 7.6.3 csv ファイルのインポート実行

SSH 接続、WINSXP など LISM サーバに接続し、インポートする CSV ファイルをディレクトリ

「**/data/csv/import**」配下に配置してください。また、CSV ファイルは **LF 改行**、**文字コードは UTF8** であることを予め確認してください。

手動でインポートを実行する場合、スクリプト「**/opt/secioss/sbin/csvimport**」を実行してください。運用上、定期的にインポートさせたい場合、スクリプトの cron 設定を行ってください。

また、インポートするスクリプトを実行後、実行された csv ファイルを“ファイル名.年月日時刻”の形式で「**/data/csv/import\_backup**」配下にバックアップされます。

## 7.7 CSV エクスポート設定

「ユーザ」、「グループ」、「組織」情報を独自の CSV フォーマットでエクスポートできます。

メニューの「統合 ID 管理」-「CSV エクスポート設定」をクリックするとエクスポートする CSV ファイルのフォーマット形式や、出力時にデフォルト値をセット、値を変換することができます。

### 7.7.1 エクスポートする CSV フォーマット設定

LISM にあるユーザ、グループ、組織それぞれの属性名を設定したカラム番号順に属性値を出力し、独自のフォーマット CSV ファイルをエクスポートします。

表 25 CSV エクスポート設定項目一覧

項目名	詳細
システム ID	連携先システムを識別する一意の ID です。任意の値を入力してください。
文字コード	出力する CSV ファイルの文字コードを指定します。
区切り文字	出力するカラム間の区切り文字指定
パスワード ハッシュ形式	PLAINTEXT   CRYPT   MD5   SHA (パスワードを出力するハッシュ形式)
同期の実行※1	データのエクスポートを行うかどうか設定します。
同期条件※1	<ul style="list-style-type: none"><li>・「許可するサービスに表示」をチェックします。システム ID はユーザ情報「許可するサービス」項目に表示され、ユーザの「許可するサービス」としてチェックされれば、エクスポート対象となります。</li><li>・「許可するサービスに表示」をチェックせず、エクスポートするエントリを LDAP の検索フィルタ形式で指定できます。例えば、「有効」アカウントのみ出力したい場合には、“(seciossAccountStatus=active)”</li></ul>
属性※1	エクスポートする LDAP 属性を CSV の何カラム目に出力するかをマッピングします。
デフォルト値 ※1	エクスポートするデータのデフォルト値を設定します。“カラム番号”に CSV ファイルのカラム番号、“値”にデフォルト値を設定して下さい。 “値”には、“%(関数名(引数))”の形式で関数※2を実行した値を設定することができます。引数には LDIF 形式の更新データを%0 として使用することができます。
属性値変換※1	エクスポートするエントリの属性名、値の変換を行うことができます。 <ul style="list-style-type: none"><li>・属性名：変換対象の属性名 例) mail</li><li>・フィルタ：変換対象となるエントリを LDAP の検索フィルタで指定 例) objectClass=inetOrgPerson</li><li>・変換前：変換前の値</li><li>・変換後：変換後の値</li></ul> “変換後”には、“%(関数名(引数))”の形式で関数を実行した値を設定することができます。引数には LDIF 形式の更新データを%0 として使用することができます。
自動登録	LISM がエクスポートした CSV ファイルを他のシステムで取り込む操作を自動化する機能です。利用できる条件として、Web 画面から CSV ファイルをインポートすることができる機能を持った Web サービスです。 ファイルの自動取り込みを行うために、Selenium を利用しています。CSV ファイルの自動取り込みを行うための Selenium シナリオファイルをお客様にて作成する必要があります。 <ul style="list-style-type: none"><li>・登録用シナリオファイル：Selenium により作成した Web 画面から CSV インポートを行うシナリオファイルを登録します。</li><li>・登録用ユーザ：CSV インポート時に Web 画面にログインするユーザ（取り込み先 Web サービスのアカウント）を指定します。</li></ul>

	<ul style="list-style-type: none"> <li>・登録用パスワード：登録用ユーザのパスワードを入力します。</li> <li>・成功時のメッセージ：CSV インポートが成功した場合表示されるメッセージを入力します。</li> </ul> <p>※シナリオファイル内で、ログインするユーザ、パスワード、インポートする CSV ファイル名は、それぞれ USERNAME、PASSWORD、CSVFILE に置換して下さい。</p>
--	--

※1 ユーザ、グループ、組織共通設定になります。※2 使用可能な関数は「7.10 関数一覧」を参照ください。

### 7.7.1 動作確認

設定保存後、「保存」ボタンの横にある「動作確認」から、エクスポートする予定のデータ情報を確認できます。ここでは、データ構成をチェックすることによって、エクスポート項目は正しく設定されたか否かを確認する目的になります。

図 15 CSV エクスポート設定動作確認

エクスポートする種類（ユーザ | グループ | 組織）を選択し、ターゲットとなる対象の ID を入力し、実行をクリックすると、エクスポートする予定のレコードが結果に出力されます。

### 7.7.2 エクスポート実行

CSV ファイルを出力するには、「保存」ボタンの横にある（保存後に出現する）「ダウンロード」ボタンで行います。ただし、最新のデータをエクスポートしたい場合、以下のバッチを実行する必要があります。

「/opt/seciooss/sbin/csvexport」

バッチスクリプトの実行により、エクスポートした最新の CSV ファイルは LISM サーバの

「/data/csv/export」ディレクトリに出力されます。「ダウンロード」をクリックする前バッチスクリプトの実行を推奨します。運用上、常に「ダウンロード」ボタンから取得したい場合、バッチスクリプトの事項を cron で設定し、定期的に行うようにしてください。

## 7.8 RESTful API 設定

### 7.8.1 RESTful API の設定項目

RESTful API を持つ Web サービスへの ID 同期のための設定を行います。

最近の Web サービスは RESTful API インターフェースを標準で備えているため、特別な仕組みを用意することなく、外部から HTTP(S)で操作をすることが可能になっています。例えば、Box や Dropbox などです。具体的な設定については Web サービス側 API の仕様に依存します。

表 26 RESTFUL 設定一覧

項目名	詳細
システム ID	システムを識別する ID です。任意の値を入力してください。
URL	システムの URL を設定してください。
認証方式	システムに接続する認証方式（OAuth Basic POST）を選択してください。
OAuth 認証 Authorize URL	OAuth の Authorize URL を設定してください。
OAuth 認証 Token URL	OAuth の Token URL を設定してください。
OAuth 認証クライアント ID	OAuth のクライアント ID を設定してください。
OAuth 認証クライアントシークレット	OAuth のクライアントシークレットを設定してください。
OAuth 認証アクセストークン	OAuth のアクセストークンを設定してください。固定のアクセストークンを発行するシステムの場合、設定して下さい。
OAuth 認証 Authorization ヘッダ	Authorization ヘッダ（Bearer OAuth）を選択してください。
ログイン認証ユーザ名	認証方式 Basic、POST でシステムに接続するユーザ名を設定してください。認証方式 POST の場合は POST するパラメータ名も設定して下さい。
ログイン認証パスワード	認証方式 Basic、POST でシステムに接続するパスワードを設定してください。認証方式 POST の場合は POST するパラメータ名も設定して下さい。
ログイン認証パラメータ	認証方式 POST でシステムに送信するパラメータ名と値を設定してください。
ログイン認証レスポンス	認証方式 POST でログインした際のレスポンスの形式を設定してください。
リクエストの形式	システムへのリクエストの形式（JSON XML POST）を選択してください。
レスポンスの形式	システムからのレスポンスの形式（JSON XML Text）を選択してください。
メソッド	追加、変更、削除、検索リクエストの HTTP メソッド選択してください。（GET POST PUT DELETE）
同期の実行※1	同期を実行するかどうか設定します。
追加、変更、削除、検索の設定※1	追加、変更、削除、検索リクエストの設定を行います。 ・パス：API のパス（“URL”の後ろに追加）。%r は“一意な属性”で設定した属性の値に変換されます。例) /users/%r ・パラメータ名、値：リクエストに付加する固定のパラメータ名と値 例) パラメータ名 action、値 create ・検索結果のパラメータ名：検索の場合、レスポンスの検索結果が格納されているパラメータ名 例) entries
同期条件※1	同期対象となるエントリの条件（LDAP の検索フィルタ形式）を設定します。 例) seciossAccountStatus=active

<b>IDのパラメータ名※1</b>	システムのデータのIDが格納されているパラメータ名を設定します。例) id
<b>一意な属性※1</b>	システムデータを一意に識別する値が格納されているLISMの属性名を設定します。例) mail
<b>一意な属性 変更リクエスト※1</b>	システムで一意な属性の値を変更可能な場合、変更を行うリクエストボディの設定をします。%rは変更前の値、%aは変更後の値に変換されます。例) {"login": "%a"}
<b>属性※1</b>	システムに同期する属性とパラメータ名をマッピングします。
<b>属性 (API) ※1</b>	<p>システムに同期する属性と更新するAPIの設定をします。</p> <p>%r はデータのID、%a は属性値にに変換されます。</p> <ul style="list-style-type: none"> <li>・属性名：LISMの属性名</li> <li>・追加、削除、検索のパス：値を追加、削除、検索するAPIのパス (“URL”の後ろに追加します。) 例) /users/%r/email_aliases</li> <li>・追加、削除、検索のリクエスト：値を追加、削除、検索するリクエストボディ 例) {"email": "%a"}</li> <li>・検索結果のパラメータ名：検索の場合、属性値が格納されているレスポンスのパラメータ名 例) entries</li> <li>・属性値のパラメータ名：属性値のパラメータ名 例) email</li> <li>・IDのパラメータ名：データのIDのパラメータ名 例) id</li> </ul>
<b>デフォルト値※1</b>	システムにデータを追加する際のデフォルト値を設定します。“パラメータ名”にシステムのパラメータ名、“値”にデフォルト値を設定して下さい。“値”には、“%{関数名(引数)}”の形式で関数を実行した値を設定することができます。引数にはLDIF形式の更新データを%0として使用することができます。
<b>属性値変換※1</b>	<p>LISMにインポートするエントリの属性名、値の変換を行うことができます。</p> <ul style="list-style-type: none"> <li>・属性名：変換対象の属性名 例) mail</li> <li>・フィルタ：変換対象となるエントリをLDAPの検索フィルタで指定 例) objectClass=inetOrgPerson</li> <li>・変換前：変換前の値</li> <li>・変換後：変換後の値</li> </ul> <p>“変換後”には、“%{関数名(引数)}”の形式で関数※2を実行した値を設定することができます。引数にはLDIF形式の更新データを%0として使用することができます。</p>
<b>レスポンス※1</b>	<p>システムのレスポンスの設定を行います。</p> <ul style="list-style-type: none"> <li>・エラーコードのパラメータ名：エラーコードが格納されているパラメータ名 例) code</li> <li>・メッセージのパラメータ名：メッセージが格納されているパラメータ名 例) message</li> <li>・成功の場合のエラーコードまたはメッセージ：リクエストが成功した場合のエラーコードまたはメッセージ 例) 0</li> <li>・既に存在する場合のエラーコードまたはメッセージ：データが既に存在する場合のエラーコードまたはメッセージ。この場合、LISMのデータでシステムのデータを上書きします。例) 68</li> <li>・存在しない場合のエラーコードまたはメッセージ：データが存在しない場合のエラーコードまたはメッセージ。このエラーの場合、LISMのデータでシステムにデータを追加します。例) 32</li> </ul>

※1：ユーザ情報、グループ情報、組織情報についてそれぞれ設定を行います。※2 使用可能な関数は「7.10 関数一覧」を参照ください。

### 7.8.2 SeciossLink との連携設定例

本節では、「7.4.1」を基に、SeciossLink と連携する場合の基本的な同期設定例を記述します。LISM 側のユーザを SeciossLink の検証環境に同期します。検証環境は <https://www.secioss.co.jp/contact2/> から申し込むことができます。

表 27 SeciossLink への同期設定例

LDAP サーバ設定				
システム ID		seciosslink		
URL		https://slinkdev.secioss.net/admin/api/		
認証方式		POST		
ログイン認証 ユーザ名		admin@test.com パラメータ名 : id		
ログイン認証 パスワード		パラメータ名 : password		
ログイン認証 パラメータ		パラメータ名 : action_login 値 : true		
ログイン認証 レスポンス		エラーコードのパラメータ名 : code 成功の場合のエラーコード : 0 セッションのパラメータ名 : sessid		
リクエストの形式		POST		
レスポンスの形式		XML		
メソッド	追加	POST		
	変更	POST		
	削除	POST		
	検索	POST		
ユーザ	同期の実行	有効		
	追加の設定	パラメータ名 : action_user_create 値 : true		
	変更の設定	パラメータ名 : action_user_update 値 : true		
	削除の設定 1	パラメータ名 : action_user_delete 値 : true		
	検索の設定	検索結果のパラメータ名 : entries,entry パラメータ名 : action_user_read 値 : true		
	同期条件	「許可するサービスに表示」をチェック		
	ID のパラメータ名	id		
	一意な属性	uid		
	属性	同期元	uid	同期先 id
		同期元	sn	同期先 sname
		同期元	givenName	同期先 gname
		同期元	mail	同期先 mail
		同期元	seciossLocaleCode	同期先 locale
		同期元	preferredLanguage	同期先 lang
		同期元	userPassword	同期先 password
	レスポンス	エラーコードのパラメータ名 : code メッセージのパラメータ名 : message 成功の場合のエラーコードまたはメッセージ : 0 ユーザが既に存在する場合のエラーコードまたはメッセージ : 68 ユーザが存在しない場合のエラーコードまたはメッセージ : 32		



## 7.9 追加属性

メニューの「統合 ID 管理」-「追加属性」をクリックするとユーザの属性情報を追加することができます。追加された情報は「ユーザ」の編集画面から確認することができます。また、追加できる項目に制限はありませんが、LISM 管理用 OpenLDAP が持つ属性情報のみ追加ができます。

## 7.10 関数一覧

以下は“デフォルト値”、“変換ルール”、“属性値変換”で利用できる関数です。

表 28 利用可能な関数一覧

関数名	説明	記述例	結果例
<b>searchAttr</b>	マスタ LDAP から条件に一致したエントリを指定し、属性値を取得します。 <ul style="list-style-type: none"><li>・ 第一引数：属性名</li><li>・ 第二引数：条件（LDAP 検索フィルタ形式）</li></ul>	<code>searchAttr('mail', 'uid=%1')</code>	<code>user@example.com</code>
<b>date2time</b>	LDAP 形式の日時 UNIX 時間に変換します。 <ul style="list-style-type: none"><li>・ 第一引数：LDAP 形式の日時</li></ul>	<code>date2time('20150101010100Z')</code>	<code>1420041660</code>
<b>time2date</b>	UNIX 時間を LDAP 形式に変換します。 <ul style="list-style-type: none"><li>・ 第一引数：UNIX 時間</li></ul>	<code>time2date('1420041660')</code>	<code>20150101010100Z</code>
<b>getValue</b>	エントリ内の属性値を取得します。 <ul style="list-style-type: none"><li>・ 第一引数：エントリ</li><li>・ 第二引数：属性名</li><li>・ 第三引数：属性値が無い場合この値を返します。</li><li>・ 第四引数：DN 形式の値をエスケープする場合は真にします。</li></ul>	<code>getValue('%0', 'mail')</code>	<code>user@example.com</code>
<b>replace</b>	正規表現にマッチした部分の文字列を変換します。 <ul style="list-style-type: none"><li>・ 第一引数：正規表現</li><li>・ 第二引数：変換後の文字列</li><li>・ 第三引数：変換対象の文字列</li></ul>	<code>replace(';', '%3b', 'S=user01;O=Example;C=JP')</code>	<code>S=user01%3bO=Example%3bC=JP</code>
<b>strmap</b>	指定した文字列を別の文字列に変換します。 <ul style="list-style-type: none"><li>・ 第一引数：変換数文字列（カンマ区切りで複数指定可能）</li><li>・ 第二引数：変換後の文字列（カンマ区切りで複数指定可能）</li></ul> 第一引数の文字列にマッチした文字列を第二引数の同じ順番の文字列に変換します。	<code>strmap('active,inactive,deleted', '0,1,2', 'seciossAccountStatus:active')</code>	<code>seciossAccountStatus:0</code>
<b>randString</b>	ランダムな文字列を生成します。 <ul style="list-style-type: none"><li>・ 第一引数：文字数</li><li>・ 第二引数以降：使用する文字（"a..z"、"A..Z"、"0..9"のような形式も設定可能）</li></ul>	<code>randString(8, 'a..z', 'A..Z', '0..9')</code>	<code>Gho3902h</code>



<b>regmatch</b>	<p>正規表現にマッチした文字列を取得します。</p> <ul style="list-style-type: none"> <li>・ 第一引数：正規表現</li> <li>・ 第二引数：文字列</li> </ul>	<code>regmatch('dn: uid=[^,]+,ou=People,([^\n]+)', '%0')</code>	<code>o=example,dc=secioss,dc=co,dc=jp</code>
<b>dn2oupath</b>	<p>DN に含まれる OU をパスの形式に変換します。</p> <ul style="list-style-type: none"> <li>・ 第一引数：DN</li> <li>・ 第二引数：ベース DN (DN 内のベース DN 配下に対して処理を行います)</li> <li>・ 第三引数：真の場合パスの値を全て小文字に変換</li> </ul>	<code>dn2oupath('uid=user,ou=Sales,ou=Tokyo,ou=People,...', 'ou=People,')</code>	<code>/Tokyo/Sales</code>
<b>path2dn</b>	<p>パス形式の文字列に変換します。</p> <ul style="list-style-type: none"> <li>・ 第一引数：パス</li> <li>・ 第二引数：属性名</li> <li>・ 第三引数：真の場合 DN の並び順を逆にします。</li> </ul>	<code>path2dn('/Tokyo/Sales/', 'ou', 1)</code>	<code>ou=Sales,ou=Tokyo</code>
<b>getAdStatus</b>	<p>Active Directory のステータスを別の文字列に変換します。</p> <ul style="list-style-type: none"> <li>・ 第一引数：Active Directory のステータス</li> <li>・ 第二引数：有効な場合の文字列</li> <li>・ 第二引数：無効な場合の文字列</li> </ul>	<code>getAdStatus(0x200, 'active', 'inactive')</code>	<code>active</code>
<b>hashPasswd</b>	<p>パスワードをハッシュ化します。</p> <ul style="list-style-type: none"> <li>・ 第一引数：パスワード</li> <li>・ 第二引数：ハッシュ形式</li> </ul>	<code>hashPasswd('secret', 'SHA')</code>	<code>{SHA}5en6G6MezRroT3XKqkdPOmY/BfQ=</code>
<b>doFunction</b>	<p>「共通設定」でアップロードしたライブラリの関数を実行した値を返します。</p> <ul style="list-style-type: none"> <li>・ 第一引数：関数名</li> <li>・ 第二引数以降：関数に渡す引数</li> </ul>	<code>doFunction('customFunc', 'arg1', 'arg2')</code>	<code>customFunc('arg1', 'arg2')</code> の実行結果

## 8 システム設定

「システム」から LISM が利用する OpenLDAP の設定や、パスワードポリシー設定やパスワード期限切れのメール文章フォーマットなどをの設定を行うことができます。

### 8.1 システム設定

メニューの「システム」-「システム設定」からメールサーバの設定を行うことができます。

表 29 システム設定項目一覧

項目名	詳細
管理者メールアドレス	管理者のメールアドレスを設定します。
送信メールサーバ名(SMTP)	メールサーバのホスト名、IP アドレスを設定します。
送信ポート番号(SMTP)	SMTP メール送信時のポート番号を設定します。
SMTP 認証 ユーザ名	メール送信時に認証を行う場合のユーザを設定します。
SMTP 認証 パスワード	メール送信時に認証を行う場合に利用するユーザのパスワードを設定します。

### 8.2 パスワードポリシー設定

メニューの「システム」-「パスワードポリシー設定」からユーザのパスワード変更やアカウントのロックアウトに関するポリシーを設定することができます。

表 30 パスワードポリシー設定

項目名	詳細 1
文字数	パスワードの最小、最大文字数を設定します。
使用可能文字	パスワードに使用可能な文字を設定します。
パスワード 強度チェック	推測しやすいパスワードかどうかチェックします。強度の低いパスワードの場合、「警告」では警告メッセージを表示するのみで「変更拒否」では強度の強いパスワードを設定しないとの変更できません。
パスワード 世代管理数	指定した世代数のパスワードは使用できません。 ※ 1

※ 1 : 値が“0”の場合、その項目のポリシーは無効となります。

## 8.3 メールテンプレート設定

ユーザのパスワード初期化・パスワード期限警告・パスワード期限切れの時に、ユーザに対して通知するメールの内容を設定します。メニューの「システム」-「メールテンプレート設定」をクリックしてください。

表 31 メールテンプレート設定項目

項目名	詳細
メールの種類	パスワードメールの種類を選択します。 設定するメールの種類は以下の通りです。 <ul style="list-style-type: none"><li>パスワード初期化</li></ul> 言語は“日本語”、“英語”、“中国語”の3種類です。
差出人メールアドレス	送信するメールの差出人メールアドレスを設定します。
件名	メールの件名を設定します。
本文	メールの本文を設定します。 本文には以下のパラメータを使用することが可能です。 <ul style="list-style-type: none"><li><code>\${id}</code> : ユーザ ID</li><li><code>\${name}</code> : ユーザの氏名</li><li><code>\${password}</code> : 初期化パスワード (パスワード初期化・パスワード期限切れメールのとき)</li></ul>

## 9 参考

### 9.1 OPENLDAP の構築

LISM の管理用に OpenLDAP が必要になります。LISM を導入したサーバに追加で OpenLDAP を導入し、1 台のコンピュータで稼働させることも可能ですが、アカウント数が多い場合には LISM サーバとは別で構築することをお勧め致します。

OpenLDAP は、設定やアカウントなど全ての情報が格納されるため、OpenLDAP のレプリケーション機能を利用し、冗長化することをお勧めします。

#### 9.1.1 OpneLDAP のインストール・設定

以下の手順に従い、OpenLDAP のインストール、初期設定を行ってください。なお、導入環境は OS : CentOS7、OpenLDAP : Ver.2.4 となります。以下のパッケージを yum でインストールします。

```
# yum install -y cyrus-sasl openldap-servers openldap-clients
```

### 9.1.2 LDAPS 接続用の自己証明書作成

LDAPS 接続を行うため、自己証明書を作成します。

```
***秘密鍵の作成***
```

```
# openssl genrsa -out /etc/openldap/certs/openldap.key 2048
```

```
***自己証明書の作成***
```

```
***赤字部分は環境に合わせて変更してください***
```

```
# openssl req -new -x509 -key /etc/openldap/certs/openldap.key -out /etc/openldap/certs/openldap.crt -days 3650 -subj  
'/C=JP/ST=Tokyo/L=shinjuku/O=SECIOSS/CN=example.com'
```

```
***自己証明書のアクセス権限設定***
```

```
# chown ldap:ldap /etc/openldap/certs/openldap.key /etc/openldap/certs/openldap.crt
```

```
# chmod 0400 /etc/openldap/certs/openldap.key /etc/openldap/certs/openldap.crt
```

### 9.1.3 LISM 管理用の OpenLDAP 設定

LISM の管理用 LDAP として利用するための設定を行います。LISM のパッケージファイル内にある

「**secioss\_ldif**」フォルダ以下を OpenLDAP をインストールしたサーバにコピー（ディレクトリは何処でも構いません）してください。

「**secioss\_ldif**」フォルダ内には 3 つの ldif ファイルがあります。これらのファイルを編集し、LDAP の初期設定を行います。

1. admin.ldif
2. schema.ldif
3. module.ldif

【admin.ldif ファイルの編集・適用】

```
***OpenLDAP の管理者パスワード作成***
```

```
# slappasswd -h {SHA} -s <admin password>
```

<admin password>を admin.ldif の「olcRootPW」に記述します。

```
***変更を適用***
```

```
# ldapmodify -Y EXTERNAL -H ldapi:// -f admin.ldif
```

【schema.ldif ファイルの適用】

```
***schema ファイルを適用 ***
```

```
# ldapmodify -Y EXTERNAL -H ldapi:// -f schema.ldif
```

#### 【module.ldif ファイルの適用】

```
***module ファイルを適用 ***
```

```
# ldapmodify -Y EXTERNAL -H ldapi:// -f module.ldif
```

全ての設定が完了したら、OpenLDAP を再起動します。

```
# systemctl restart slapd
```

LDAP サーバに以下の LDIF ファイルを登録して下さい。 suffix の dc=example,dc=com は、OpenLDAP の設定に合わせて変更して下さい。

```
dn: dc=example,dc=com
changetype: add
objectClass: domain
dc: example

dn: o=System,dc=example,dc=com
changetype: add
objectClass: organization
objectClass: seciossTenant
o: System

dn: ou=People,dc=example,dc=com
changetype: add
objectClass: organizationalUnit
ou: People

dn: ou=Groups,dc=example,dc=com
changetype: add
objectClass: organizationalUnit
ou: Groups

dn: ou=Administrators,dc=example,dc=com
changetype: add
objectClass: organizationalUnit
ou: Administrators

dn: ou=Organizations,dc=example,dc=com
changetype: add
objectClass: organizationalUnit
ou: Organizations
businessCategory: invisible

dn: ou=Metadata,dc=example,dc=com
changetype: add
objectClass: organizationalUnit
ou: Metadata

dn: ou=Config,dc=example,dc=com
changetype: add
objectClass: organizationalUnit
ou: Config
```

dn: ou=Autologin,ou=Config,dc=example,dc=com  
changetype: add  
objectClass: organizationalUnit  
ou: Autologin

dn: ou=APIClients,ou=Config,dc=example,dc=com  
changetype: add  
objectClass: organizationalUnit  
ou: APIClients

dn: ou=OAuth,ou=Config,dc=example,dc=com  
changetype: add  
objectClass: organizationalUnit  
ou: OAuth

dn: ou=OpenID,ou=Config,dc=example,dc=com  
changetype: add  
objectClass: organizationalUnit  
ou: OpenID

dn: ou=OpenIDProviders,ou=Config,dc=example,dc=com  
changetype: add  
objectClass: organizationalUnit  
ou: OpenIDProviders

dn: ou=OIDC,ou=Config,dc=example,dc=com  
changetype: add  
objectClass: organizationalUnit  
ou: OIDC

dn: ou=Roles,dc=example,dc=com  
changetype: add  
objectClass: organizationalUnit  
ou: Roles

dn: ou=Profiles,dc=example,dc=com  
changetype: add  
objectClass: organizationalUnit  
ou: Profiles