ITA_システム構成/環境構築ガイド

SSO(シングルサインオン)編

―第1.6版 ―

免責事項

本書の内容はすべて日本電気株式会社が所有する著作権に保護されています。
本書の内容の一部または全部を無断で転載および複写することは禁止されています。
本書の内容は将来予告なしに変更することがあります。
日本電気株式会社は、本書の技術的もしくは編集上の間違い、欠落について、一切責任を負いません。
日本電気株式会社は、本書の内容に関し、その正確性、有用性、確実性その他いかなる保証もいたしません。

商標

- LinuxはLinus Torvalds氏の米国およびその他の国における登録商標または商標です。
- Red Hatは、Red Hat, Inc.の米国およびその他の国における登録商標または商標です。
- Apache、Apache Tomcat、Tomcatは、Apache Software Foundationの登録商標または商標です。
- Oracle、MySQLは、Oracle Corporation およびその子会社、関連会社の米国およびその他の国における登録商標です。
- MariaDBは、MariaDB Foundationの登録商標または商標です。
- Ansibleは、Red Hat, Inc.の登録商標または商標です。
- Active Directoryは、米国Microsoft Corporationの米国およびその他の国における登録商標または商標です。

その他、本書に記載のシステム名、会社名、製品名は、各社の登録商標もしくは商標です。
なお、® マーク、TMマークは本書に明記しておりません。
※本書では「Exastro IT Automation」を「ITA」として記載します。

目次

はじめに

本書では、ITA でシングルサインオン認証（以下、「SSO 認証」）機能を利用頂く為に必要なシステム構成について説明します。

SSO 認証機能を利用するにあたっては、ITA 基本機能が構築済であることが前提です。ITA 基本機能の構築に関しては、「システム構成／環境構築ガイド_基本編」をご覧ください。

1 機能

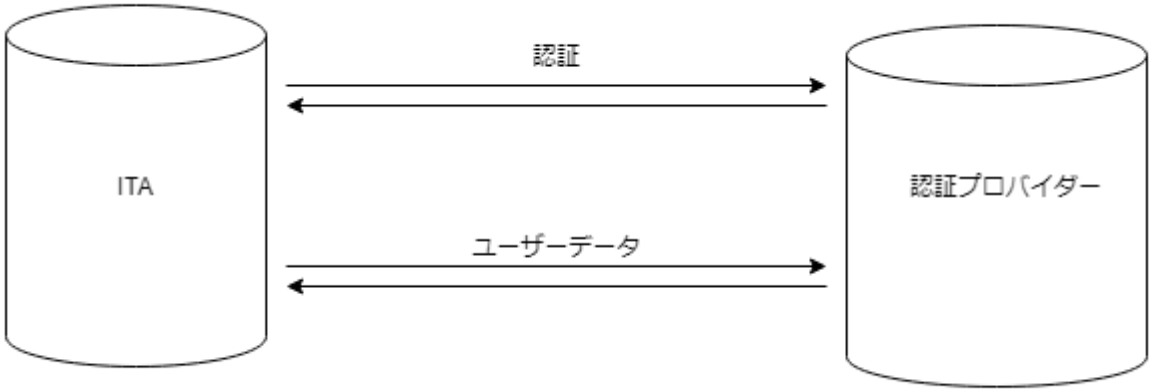
SSO 認証機能は、以下の機能を提供します。

表 1-1 機能名

No	機能名	概要	WEB コンテンツ	BackYard コンテンツ
1	SSO 認証機能	外部認証プロバイダーを使用して ITA の認証を行います。	○	―

2　システム構成

SSOの概念



3 システム要件

SSO 認証機能は ITA システムのシステム要件に準拠するため、「システム構成／環境構築ガイド_基本編」を参照してください。
SSO 認証機能を利用するには、ITA システムがインストールされているシステム及び利用者のクライアントデバイスが SSO 認証プロバイダーと HTTP/HTTPS 通信可能であることが必要です。
ITA システム側の HTTP/HTTPS 通信は直接または PROXY を使用しての通信をサポートしております。ただし認証が必要な PROXY はサポートしておりません。
利用者のクライアント側の HTTP/HTTPS 通信は SSO 認証プロバイダーに SSO 認証とは関係なく正常に認証できることが必要です。

4 ITA でサポートしている SSO 認証方式

No	ITA 上の認証方式名	概要
1	OAuth2	OAuth version2.0

5 設定フロー

① 認証プロバイダーへのクライアント登録

利用したい認証プロバイダーを利用するために ITA でサポートされている認証方法に必要なクライアント登録を行い認証に必要な情報を取得します。

No	認証方式	認証に必要な情報
1	OAuth2	・clientId ・clinentSecret

プロバイダーに設定するコールバック URL(またはリダイレクト URL)は以下を設定してください。

No	認証方式	コールバック URL(リダイレクト URL)
1	oauth2	https//(ITA の FQDN)/common/common_sso_auth.php?oauth2&callback

※ITA の設定が http(非 SSL)の場合はコールバック URL も http://・・としてください(非推奨)

② ITA の SSO 基本情報の登録

メインメニュー >> 管理コンソール >> SSO 基本情報管理

主にログイン画面への表示情報と認証方法を設定します。

No	項目名	設定内容	必須	備考
1	プロバイダーID	自動採番	○	
2	プロバイダー名	プロバイダー名	○	ログイン画面に表示するプロバイダー名
3	認証方式	認証方式を選択	○	OAuth2 のみ
4	ロゴ	画像ファイルをアップロード		ログイン画面に表示するプロバイダーのロゴ
5	表示フラグ	ログイン画面への表示フラグ	○	選択肢：表示 or 非表示 ※認証に必要な情報が不足している場合は表示されません 「④ログイン画面への表示について」を参照

③ ITA の SSO 属性情報の登録

メインメニュー >> 管理コンソール >> SSO 属性情報管理

主に認証設定とプロバイダーからのユーザー情報取得に関する設定します。

No	項目名	設定内容	必須	備考
1	属性 ID	自動採番	○	
2	プロバイダー名	プロバイダー名	○	「SSO 基本情報管理」に登録済みのプロバイダーをプルダウンから選択
3	設定項目	設定項目	○	設定する項目をプルダウンから選択する ※設定項目は下記の「設定項目一覧」を参照
4	設定値	設定値		設定項目に対する設定値

※プロバイダーと設定項目は重複登録できません。

設定項目一覧

認証方式	項目名	設定内容	必須	備考
OAuth2	clientId	認証クライアント識別子	○	認証プロバイダーから払出された値を設定します
	clientSecret	認証クライアントシークレット	○	認証プロバイダーから払出された値を設定します
	authorizationUri	ユーザー認証エンドポイント	○	認証プロバイダーの仕様を確認して設定してください
	accessTokenUri	accessToken 取得エンドポイント	○	認証プロバイダーの仕様を確認して設定してください
	resourceOwnerUri	ユーザー情報取得エンドポイント	○	認証プロバイダーの仕様を確認して設定してください
	scope	ユーザー情報の開示(取得)範囲		認証プロバイダーの仕様を確認して設定してください
	id	ユーザーID キー名	○	resourceOwnerUri で取得するユーザーデータ内のキー名
	name	ユーザー名キー名	○	resourceOwnerUri で取得するユーザーデータ内のキー名
	email	ユーザーメールアドレスキー名		resourceOwnerUri で取得するユーザーデータ内のキー名
	imageUrl	ユーザー画像 URL キー名		resourceOwnerUri で取得するユーザーデータ内のキー名 ※キーが配列になっている場合は “>”で区切る
その他	proxy	外部と通信する際の proxy を指定する		tcp:///(ホスト名 or IP アドレス):(ポート番号) または http:///(ホスト名 or IP アドレス):(ポート番号)
その他	debug	デバッグフラグ		SSO ログイン失敗時に失敗時の詳細情報を画面に表示する ※”1”を設定することでデバッグフラグが on になります

④ ログイン画面への表示について

ログイン画面に表示するには以下のすべての条件を満たしていなければなりません。

・「②ITA の SSO 基本情報」の「表示フラグ」が「表示」となっていること

・「③ITA の SSO 属性情報の登録該当認証方式」で該当認証方式の必須項目が全て設定されていること

・エンドポイントの各 Uri については“https://”または“http://”で始まっている文字列で設定されていること

・proxy を設定している場合、備考欄に記載のフォーマットで入力されていること

⑤ ログイン画面には表示せずに設定内容が正しいのかを確認する方法

ログイン画面に表示してしまうと設定が正しいのかわからない状態でもログイン操作がされてしまいます。

ログイン可能なのかを最終確認してから「②ITA の SSO 基本情報」の「表示フラグ」を「表示」に設定することを推奨します。

ログイン画面への表示フラグを「非表示」としている場合は下記 URL を直接ブラウザに入力することで動作検証することができます。

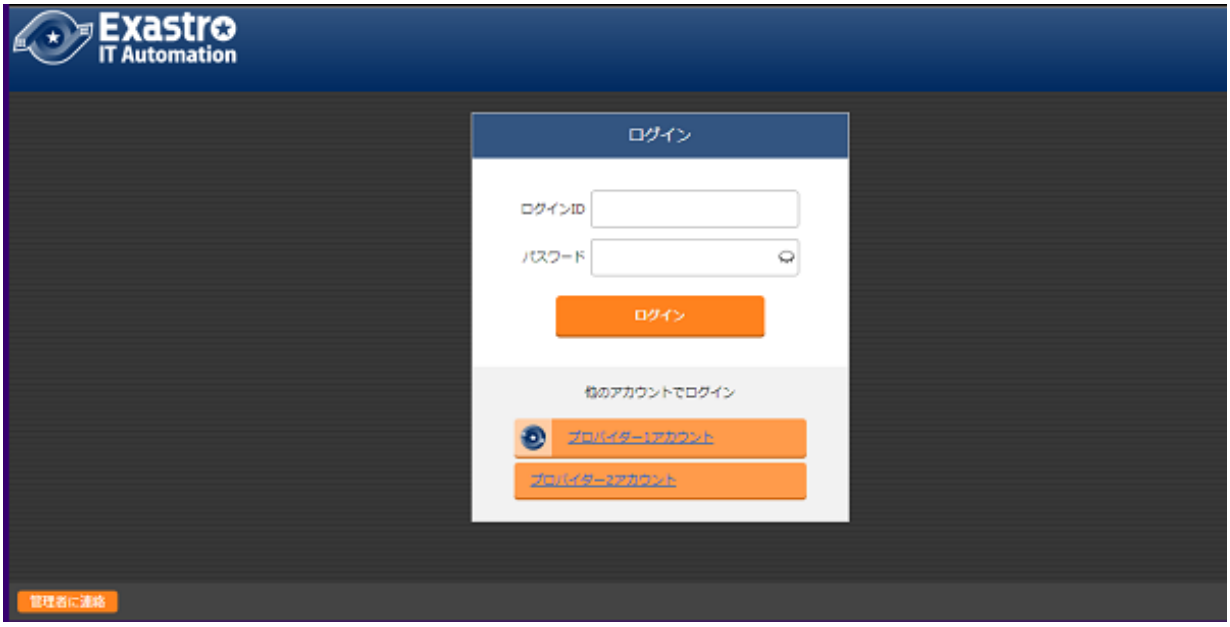
No	認証方式	動作確認 URL
1	oauth2	https://(ITA の FQDN)/common/common_sso_auth.php?oauth2&providerId=(プロバイダーID) ※プロバイダーID は「SSO 基本情報管理」メニューの項目

6 ロールについて

SSO 認証されたユーザーは ITA ユーザーとして自動作成されます。
また、初回ログイン時に SSO デフォルトロール(ロール ID:2100000001)に自動的に紐づけされます。
※割り当ては初回のみです。
このロールには初期状態ではどのメニューにも紐づいていないため必ず事前に適切なメニューと紐づけを行ってください。紐づけは
メインメニュー >> 管理コンソール >> ロール・メニュー紐付管理
で設定可能です。

7　ログイン画面

上記の設定フローを完了してログイン画面への表示フラグを「表示」と設定したらログイン画面の下部に表示されます。
このプロバイダーをクリックすることで SSO 認証が実施されます。
「SSO 基本情報管理」でロゴを登録していた場合はプロバイダー名の前にロゴが表示される。



8　ログイン後の画面

SSO でログイン後は右上のログインユーザー情報に SSO プロバイダー情報が表示されます。
「SSO　基本情報管理」でロゴを登録していた場合ロゴが表示されます。登録していない場合はプロバイダー名が表示されます。
「SSO　属性情報管理」で「iimageUrl」(ユーザー画像　URL)を登録していてプロバイダーから取得できた場合はユーザーの画像がプロバイダー情報の右側に表示します。

プロバイダーロゴを登録している、ユーザー画像を取得できた場合

プロバイダーロゴを登録していない、ユーザー画像を取得しない場合

9　SSO 認証ユーザーの管理について

SSO 認証ユーザーは名前、メールアドレスは認証プロバイダーで設定されたものをそのまま使用します。
ITA の管理画面で変更することは可能ですが、次回ログインしたときに自動的にプロバイダーから取得した最新の情報で再設定されます。
なお、ログイン ID については ITA のユーザー管理で再設定した場合その後再変更されることはありません。
また、ITA の管理画面でユーザーの廃止を行ったとしてもそのユーザーがプロバイダー側でログイン可能であれば ITA にログイン時に自動的に復活します。ただし、SSO デフォルトロールへの紐付は行われません。
特定ユーザーを利用させたくない場合はプロバイダー側でユーザー削除またはログインできないようにするか、ITA 側でロールに割り当てないことで ITA の利用を制限してください。

10 AD(ActiveDirectory)との併用について

SSO 認証と AD 認証は併用可能です。
通常 ITA で AD 認証を有効にしている場合はシステム管理者(ユーザーID:1)およびシステム管理者ロール(ロール ID:1)以外のユーザーおよびロールは ActiveDirectory 設定ファイルに記載していない場合自動的に廃止されますが、SSO 認証ユーザー(認証方式:sso)および SSO デフォルトロール(ロール ID：2100000001)は廃止されません。

11 リバース PROXY 環境においての注意点

※リバース PROXY を利用していない場合、本項の問題は生じません。

ユーザーが ITA にアクセスする際に負荷分散等のためにリバース PROXY を利用している場合、SSO 認証において以下に該当する場合にリバース PROXY サーバーへの追加設定が必要になります。

- HTTPS を使用していない。(クライアント(ブラウザ)⇔リバース PROXY サーバー間)
- AWS の ELB(ALB,CLB)を利用していない。
  ※AWS の ELB(ALB、CLB)ではこの問題は発生しません。
- リバース PROXY⇒ITA サーバー間でリクエスト元プロトコル情報のヘッダー
  (X_FORWARDED_PROTO)を送信していない。

上記全ての条件を満たす場合、SSO 認証のフローの際に元のプロトコルではないプロトコルに代わってしまう可能性があります。また、切り替わる際にどちらか片方のみで運用していた場合はその時点でエラーが発生してしまいます。
apache などのオープンソースソフトウェアでのリバース PROXY を行うことは可能ですが、標準でリクエスト元のプロトコル情報を送っていない場合があります。

下記に apache でのリバース PROXY での追加ヘッダーの設定例を示します。
※その他の場合については割愛させていただきます。

アクセスする URL: http://example.com
リバース PROXY する URL: http://192.168.100.1

```
<VirtualHost *:80>
    ServerName   example.com
    ErrorLog     (省略)
    CustomLog    (省略)
    ProxyRequests Off
    ProxyPass / http://192.168.100.1/
    ProxyPassReverse / http://192.168.100.1/
    RequestHeader set X-Forwarded-Proto http
</VirtualHost>
```

※下線の行の設定を追加してください。