AgileWorks R3

LDAP 認証設定ガイド

R3.2 第 1 版(2025/10/31)

ATLED

目次／索引

◆ 改版履歴

版数	年月日	改版内容
第 1 版	2025 年 10 月 31 日	第 1 版作成

1. はじめに

1.1. 対象読者

本ガイドは、AgileWorks のログイン認証や LDAP に関する基本知識を持つ方を対象としています。ログイン認証に関する詳細な情報についてはガイド資料「Aw02-ログイン認証ガイド」「AwOp01-SSO 設定ガイド」をご参照ください。

1.2. 前提条件

LDAP サーバー	LDAP v3 準拠
認証方式	ID・パスワードによる認証（簡易認証）に対応
セキュリティ	SSL 通信／非 SSL 通信のどちらにも対応
その他	AgileWorks で認証を行いたい全てのユーザーを検索できる LDAP ユーザーが存在する ※Anonymous 認証はサポートしておりません

1.3. ライセンスについて

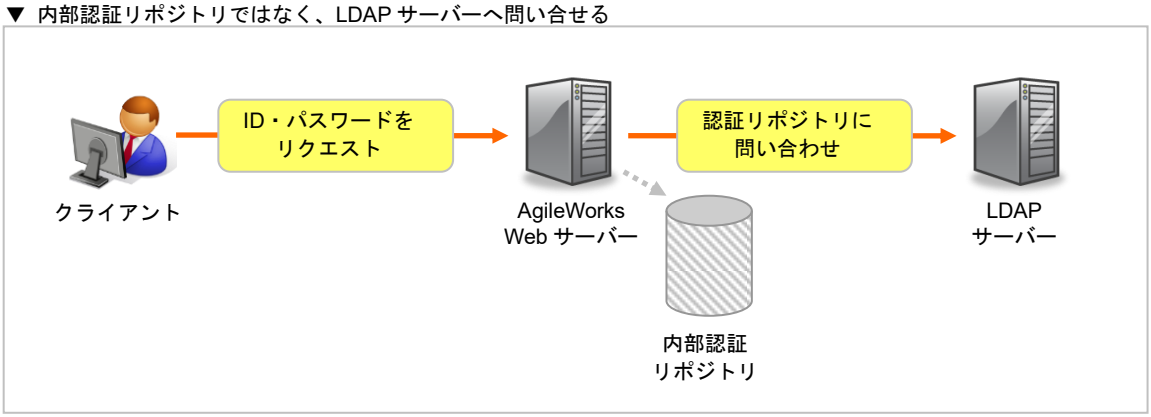
本ガイドで説明する LDAP 認証機能を利用にするには、LDAP 認証連携オプションが別途必要となります。詳細につきましては、AgileWorks 販売代理店までお問い合わせください。

2. 概要

2.1. LDAP 認証とは

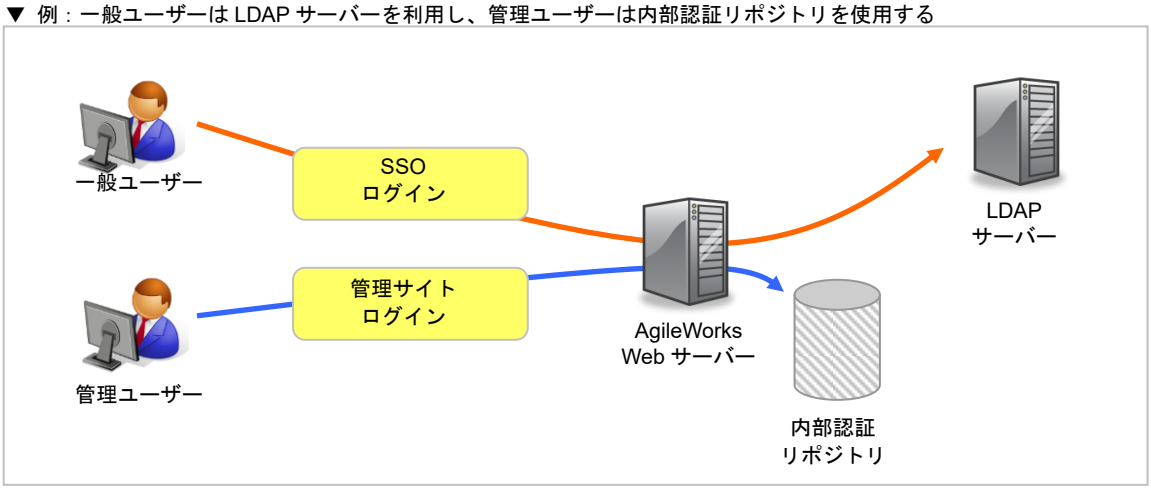
AgileWorks の認証処理では、リクエストから受け取った ID・パスワード等の情報が正しいものかどうかを確認するために、認証リポジトリに問い合わせます。この認証リポジトリは通常 AgileWorks に登録されているユーザー情報（内部認証リポジトリ）となりますが、LDAP サーバーを認証リポジトリとして指定することで、LDAP サーバー上に登録されているユーザー情報・パスワードを元に認証を行うことが可能となります。

▼ 内部認証リポジトリではなく、LDAP サーバーへ問い合せる



また、AgileWorks では通常のログイン画面からの認証だけでなく、SSO 認証・SAML 認証といった様々なログイン認証方式が利用できます。認証リポジトリはこれらのログイン認証設定毎に切り替えることが可能なため、認証方式に合わせて柔軟に認証リポジトリを切り替えることも可能です。例えば、管理ユーザーが LDAP サーバー上に存在しないケースでは、管理サイトのログイン認証のみ内部認証リポジトリとすることも可能です。

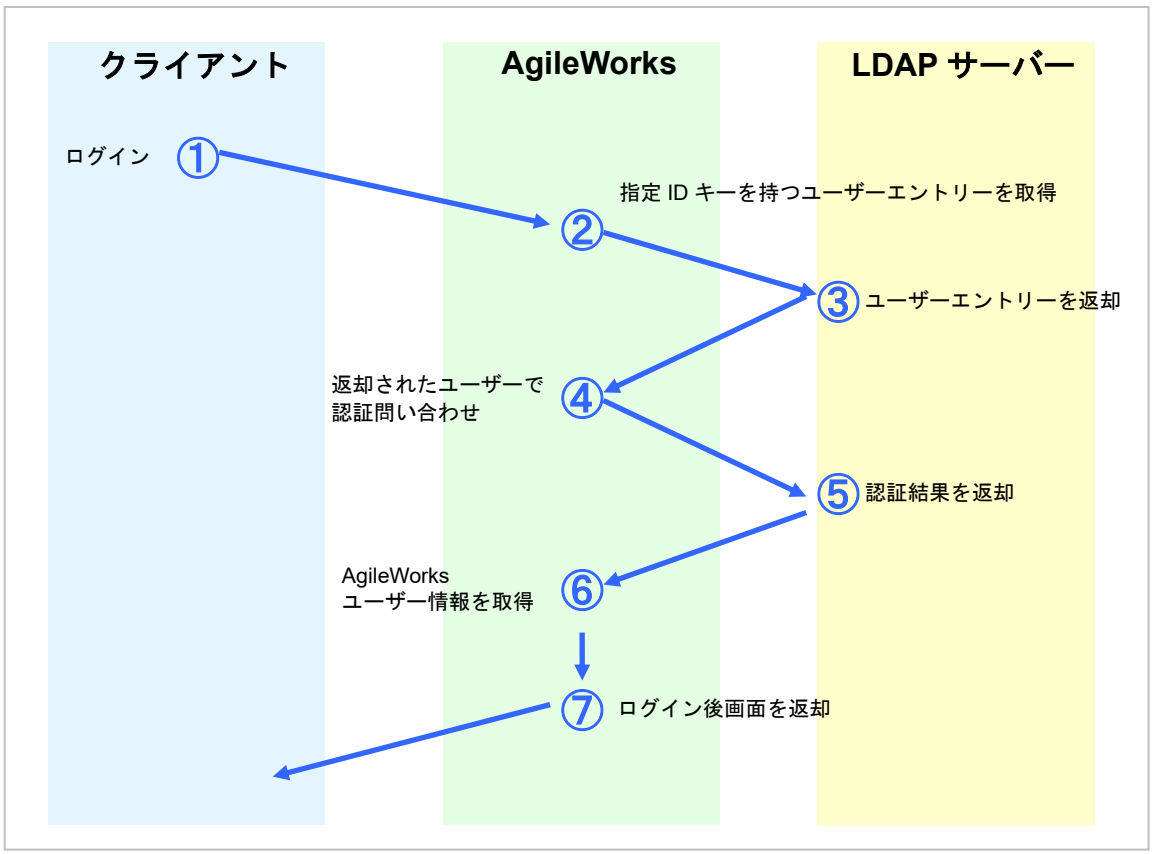
▼ 例：一般ユーザーは LDAP サーバーを利用し、管理ユーザーは内部認証リポジトリを使用する



> ⚠ 注意事項
> LDAP 認証を利用するためには、事前に AgileWorks と LDAP サーバーとでユーザー情報の同期を行っておく必要があります。また、AgileWorks ユーザーと LDAP ユーザー間を 1 対 1 で紐付ける引当キー項目をお互いに持つ必要があります。この項目には、例えばログイン ID やメールアドレス等が使用されます。

2.2. LDAP 認証処理の流れ

LDAP 認証を行う際に、AgileWorks がどのようなステップで LDAP サーバーへの問い合わせを行っているかを説明します。下記の図では、クライアントから渡された ID・パスワードを受け取り、外部認証リポジトリである LDAP サーバーへ問い合わせを行い、クライアントに結果を返すプロセスを示しています。



各処理の詳細は以下の通りです。

手順	詳細
① ログイン	ログイン画面または SSO 認証により、AgileWorks へログインします。 この際、ユーザーを特定する ID・パスワード情報がリクエスト情報として渡されます。
② 指定 ID を持つユーザーエントリーを取得	リクエスト情報を元に問い合わせ先となる認証リポジトリが決定します。 認証リポジトリが LDAP サーバーの場合は、リクエストから受け取った ID を持つユーザーのエントリを返すよう LDAP サーバーに問い合せます。この際、LDAP サーバーへアクセスするユーザーは、これからログインしようとしているユーザーとは異なる、ユーザーDN ディレクトリにアクセス可能なユーザーとなります。 このユーザーは外部認証リポジトリの情報として、事前に設定しておくことになります。
③ ユーザーエントリーを返却	該当ユーザーが LDAP サーバー上に存在する場合、LDAP サーバーは AgileWorks に対してユーザーエントリーを返却します。
④ 返却されたユーザーで認証問い合わせ	③で返却されたユーザー情報とパスワード情報を用いて、LDAP サーバーに対して認証問い合わせを行います。
⑤ 認証結果を返却	LDAP サーバーは AgileWorks に対して認証結果を返却します。
⑥ AgileWorks ユーザー情報を取得	認証が成功した場合、ユーザーエントリーの属性を引当キーとし、AgileWorks ユーザー情報を取得します。 引当キーには、例えばログイン ID やメールアドレス等が使用されます。 引当キーは外部認証リポジトリの情報として、事前に設定しておくことになります。
⑦ ログイン後画面を返却	クライアントにログイン後画面を返却します。

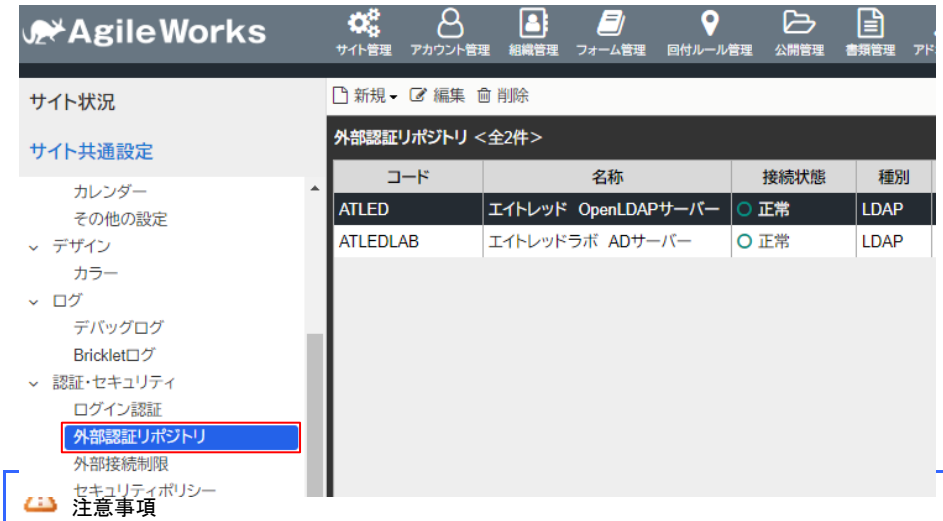
3. LDAP認証設定の流れ

この章では、実際に LDAP 認証を行う際に設定手順や、認証が正常に動作しているかの確認手順について説明します。

3.1. 外部認証リポジトリ設定

LDAP 認証を利用する場合、まずは利用する LDAP サーバーを外部認証リポジトリとして登録する必要があります。管理サイトにログインし、[サイト管理]-[サイト共通設定]-[認証・セキュリティ]-[外部認証リポジトリ]にアクセスしてください。

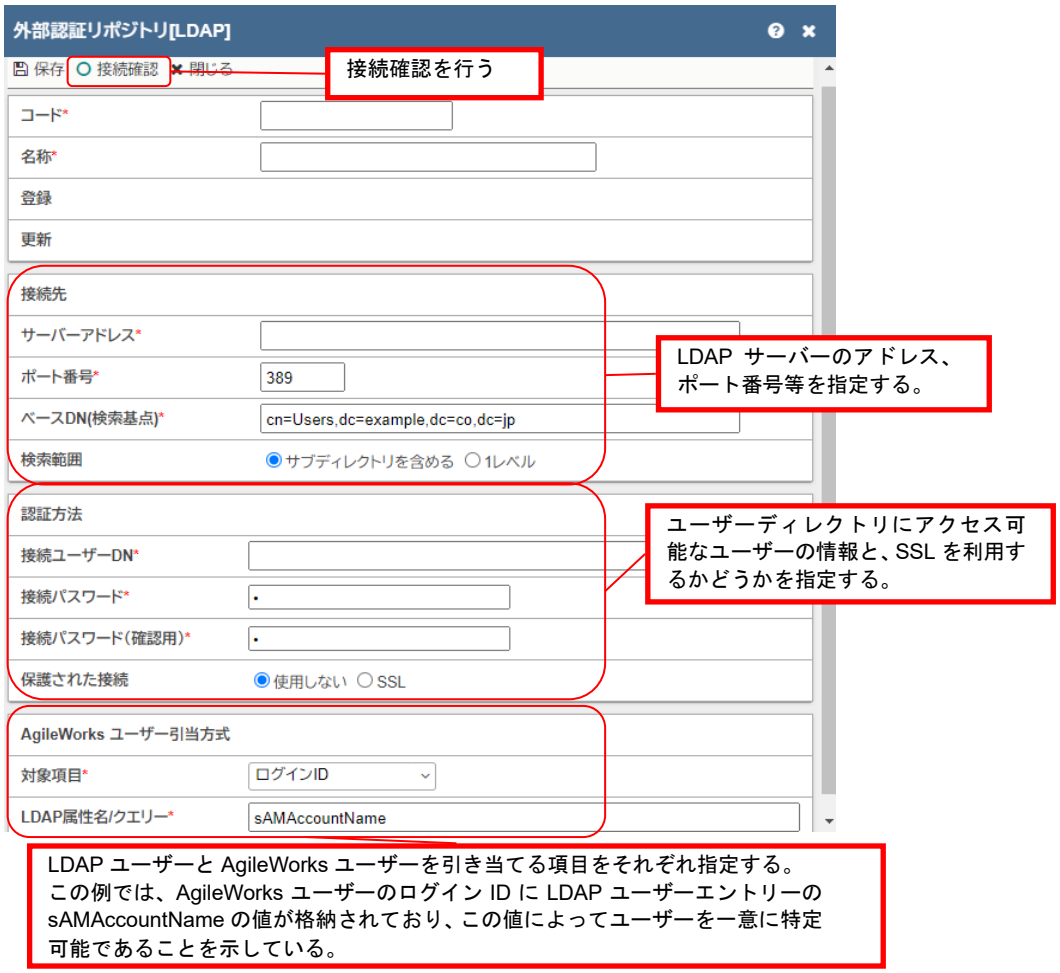
▼サイト共通設定画面



注意事項

LDAP 認証オプションが適用されていない場合、本メニューは表示されません。

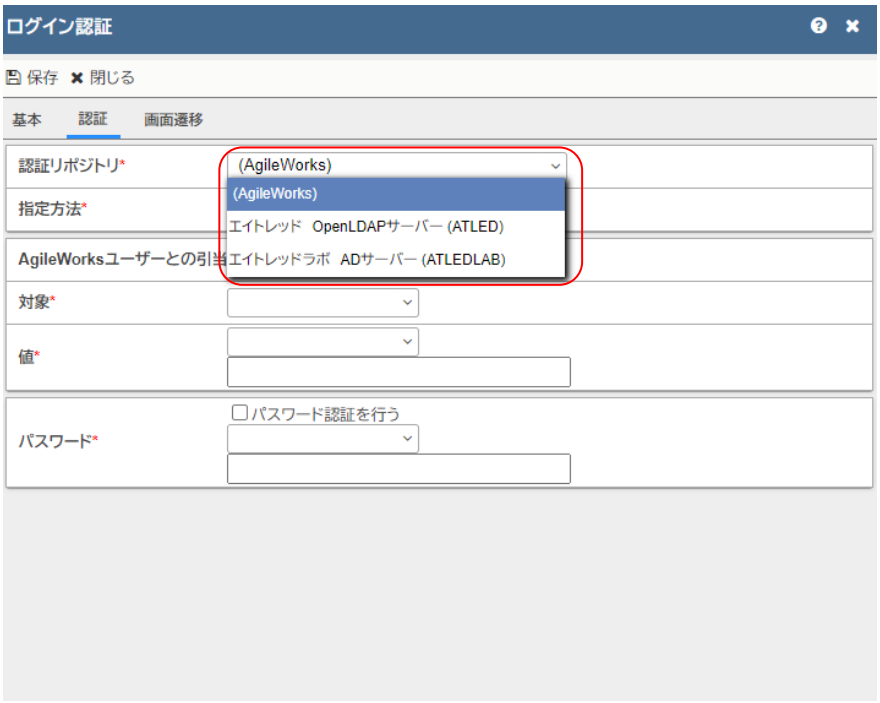
[新規]-[LDAP 認証リポジトリ]から、新規に外部認証リポジトリの設定画面を開きます。ご利用の LDAP サーバーに合わせて各項目を入力してください。設定が完了したら[接続確認]メニューより、LDAP サーバーへの接続が可能かどうか確認してください。
https://zaoraru.atledcloud.jp/AgileWorks/Broker/Picus



3.2. ログイン認証設定

次に LDAP 認証を行いたい認証方式に対して、先ほど登録した LDAP 認証リポジトリを外部認証リポジトリとして指定します。[サイト管理]-[サイト共通設定]-[認証・セキュリティ]-[ログイン認証]にアクセスしてください。

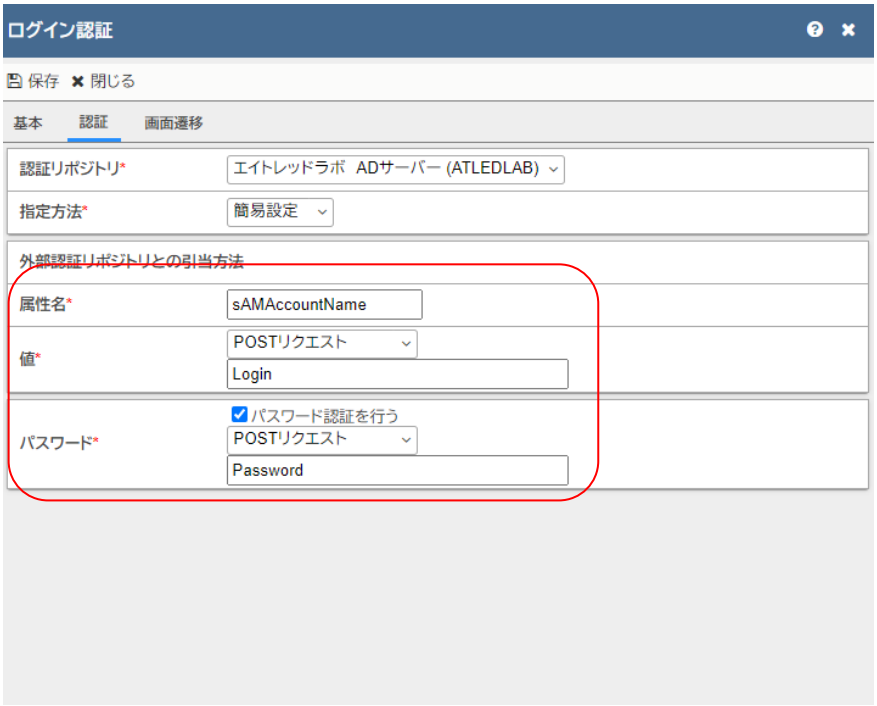
次にログイン認証の編集画面を開き、[認証]タブを表示します。認証リポジトリ項目のプルダウンを表示すると、先ほど登録した外部認証リポジトリが候補に表示されます。



認証リポジトリを外部認証リポジトリに変更すると、引当方法に関する設定項目が表示されます。ここでは、クライアントから受け取ったリクエストのどのパラメータをキーとして用いるか、またそのパラメータとユーザーエントリーのどの属性とを引き当てるかを指定します。

下記の図の例では、POST リクエストで渡されたパラメータ"Login"を用いて、ユーザーエントリーの"sAMAccountName"属性と引き当て、ユーザーエントリーを特定することになります。

本設定の詳細については、管理サイトのヘルプまたはガイド資料「ログイン認証／SSO ガイド」をご参照ください。



3.3. 動作確認方法

以上で LDAP 認証の設定は完了です。実際にログイン画面等からログインし、指定した認証リポジトリにアクセスし、認証が成功することを確認しましょう。

認証に失敗する場合は、[サイト管理]-[サイト共通設定]-[ログ]-[デバッグログ]にアクセスし、"認証情報のトレース"を有効にしてください。

有効にした状態で認証に失敗すると、原因がデバッグログに出力されるようになります。原因を確認し、設定内容の見直し等を行ってください。

▼ デバッグログ画面に認証結果が表示される

```
34 2022/03/24 13:18:44 DEBUG - LDAP: user not found by query. [sAMAccountName=test0000]
35 2022/03/24 13:18:44 DEBUG - AuthenticationResponse: SSO[ATLED] => fail [EXTERNAL_REPOSITORY_ERROR]
36 2022/03/24 13:18:52 DEBUG - AuthenticationResponse: AW[AgileWorks] => fail [EMPTY_LOGIN_ID]
```

▼ 主なエラーメッセージとその原因

エラーメッセージ	原因
user not found by query	LDAP サーバーに、指定されたキーのユーザーエントリーが存在しない
invalid password	指定されたパスワードによる認証に失敗した

この時、エラーログに LDAP サーバーから返却されたエラーコード・エラーメッセージが出力されている場合があります。これらのエラーコード・メッセージの詳細につきましては、ご利用の LDAP 製品のサポート窓口等へお問い合わせください。

4. 複数のLDAPサーバーを利用した構成例

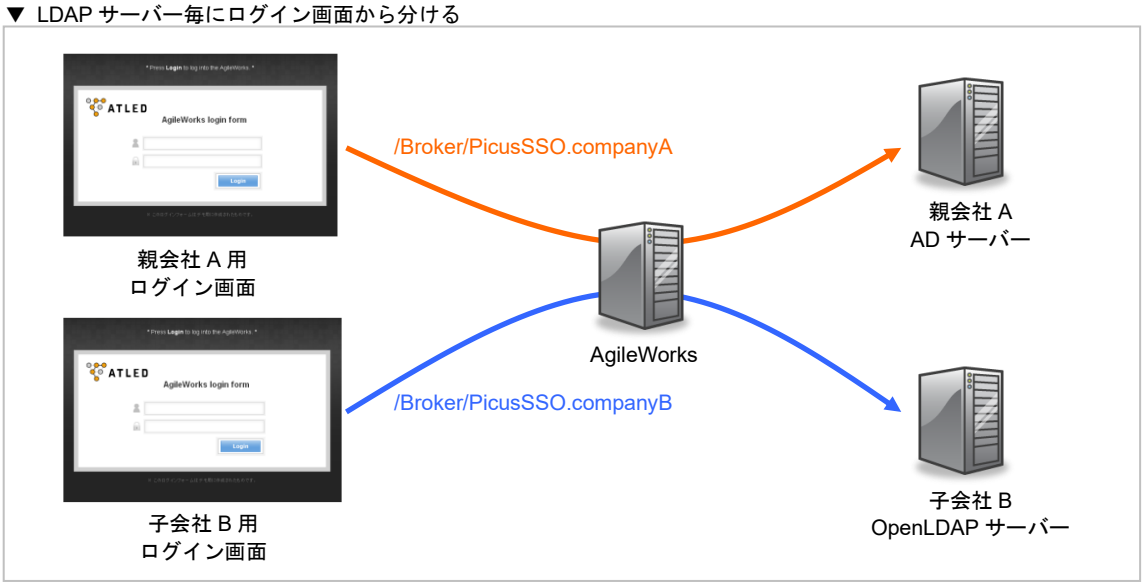
企業の子会社化、合併などに伴い、自社内に複数の LDAP サーバーが構築されているケースがあります。
本章では、そのようなケースにおいて SSO 認証を利用することで、現在の構成を変更することなく複数の LDAP サーバーに対応した認証環境を構築する例を説明します。

4.1. 構成

LDAP サーバー毎にログイン画面、ログイン認証設定、外部認証リポジトリの一式を用意することで、複数 LDAP サーバーに対応した認証を実現します。

下記の図は、親会社 A とその子会社 B にそれぞれ LDAP サーバーが構築されている場合の構成例となります。実現のために SSO 認証を利用するため、各会社のログイン画面、ログイン URL が異なることになります。

▼ LDAP サーバー毎にログイン画面から分ける



4.2. 構築手順

本構成を実現するための構築手順を以下に示します。

1) 外部認証リポジトリを登録

[サイト管理]-[サイト共通設定]-[認証・セキュリティ]-[外部認証リポジトリ]にアクセスし、親会社 A が利用する Active Directory サーバー、子会社 B が利用する OpenLDAP サーバーを、それぞれ外部認証リポジトリとして登録します。

2) SSO 認証設定を登録

[サイト管理]-[サイト共通設定]-[認証・セキュリティ]-[ログイン認証]にアクセスし、親会社 A 用の SSO 認証設定、子会社 B 用のログイン認証設定をそれぞれ登録します。

今回はログイン画面を HTML で作成するため、POST リクエストによる認証とします。また、ここで指定した値の名称はログインフォームのログイン ID フィールドの名称となります。ここではログイン ID の名称を"Login"、パスワードの名称を"Password"とします。

3) HTML で各画面を作成

親会社 A、子会社 B 用のログインフォームをそれぞれ作成します。先ほど登録した SSO 認証設定の URL に対して、パラメータ名称を POST する HTML を作成してください。

▼ POST リクエストを行うための HTML 例

```
<form action="http://{ServerAddress}/AgileWorks/Broker/PicusSSO.companyB" method="post">
  <input type="text" name='Login' value=""/><br/>
  <input type="password" name='Password' value=""/><br/>
  <input type="submit" value="Login">
</form>
```

SSO 認証の URL は編集画面の基本タブで確認することができます。

続けて、認証失敗時・ログアウト時の画面を作成します。この画面には特別なロジックは必要なく、ログイン画面へ遷移するための URL を含めた HTML を用意するだけで充分です。

ここまでで、全部で以下の 6 つの HTML が用意されました。

対象	ファイル名	用途
親会社 A	login.html	ログイン用画面
	loginfailed.html	認証失敗時の画面
	logout.html	ログアウト時の画面
子会社 B	login.html	ログイン用画面
	loginfailed.html	認証失敗時の画面
	logout.html	ログアウト時の画面

4)　作成した HTML をホストする

3)で作成した HTML を、Web サーバーでホストしてください。ここでは Web サーバーのルート直下に親会社 A、子会社 B のディレクトリを作成し、その中に各 HTML を配置します。

ディレクトリ名	ファイル名	URL
companyB	login.html	http://{ServerAddress}/companyA/login.html
	loginfailed.html	http://{ServerAddress}/companyA/loginfailed.html
	logout.html	http://{ServerAddress}/companyA/logout.html
companyB	login.html	http://{ServerAddress}/companyB/login.html
	loginfailed.html	http://{ServerAddress}/companyB/loginfailed.html
	logout.html	http://{ServerAddress}/companyB/logout.html

5)　画面遷移の設定

4)でホストした HTML のうち、ログイン・ログアウト・認証失敗の URL を画面遷移タブから指定してください。今回、セッションタイムアウトした際はログイン画面に遷移するよう設定します。

以上で設定は完了です。
実際にログイン画面にアクセスし、各リポジトリを利用した認証が行われているかを確認してください。

4.3. 注意事項

- 通知メールからの書類直接表示機能の利用

複数の LDAP サーバーを利用した構成を採用する場合、ログイン認証 URL がユーザーごとに異なる為、通知メールからの書類表示 URL はサポートされません。
通知メールからはログイン画面へ遷移（誘導）するようなメール文面にしてください。

＜補足説明＞
通知メールに記載された書類直接表示用の URL をクリックすると、まだ認証が成功していない場合はログイン画面にリダイレクトされ、利用ユーザーはログイン ID・パスワードを入力し認証を行うことになります。この時の認証では、ユーザーサイト（既定）のログイン認証設定を採用する仕様となっております。

そのため、本構成のようなログイン認証設定が複数登録されている場合においては、まだ認証が成功していない場合のリダイレクトや、その後にログインした後に書類 URL へ遷移させる動きが実現できません。