# AgileWorks R3

# SSO 設定ガイド

R3.3 第 1 版(2026/07/15)

ATLED

目次／索引


1. 概要 ..... 4
1.1. ログイン認証 ..... 4
1.2. SSO とは ..... 5
1.3. ログイン URL ..... 6
AgileWorks 標準のログイン画面 URL ..... 6
外部認証（SSO）時の URL ..... 6
SAML 時の URL ..... 6
1.4. ドキュメントビューア URL ..... 7
新規でドキュメントビューアを開くための URL ..... 7
保存された書類を開くための URL ..... 7
「既定のログイン」以外で書類を開くための URL ..... 7
1.5. 書類作成時のフィールド値指定 ..... 8
利用するにあたって ..... 8
利用可能なフィールド ..... 8
指定するフィールド値 ..... 8
書類を表示する際の動作 ..... 8
1.6. ガジェットの利用 ..... 9
1.7. ガジェット利用時のユニークログインユーザー数の考え方 ..... 11
1.8. ガジェットにおける制限事項 ..... 12
1.9. 書類を直接開いた状態でログアウトする ..... 13
1.10. ログイン認証設定のアクセス権限 ..... 13
2. SSO 実現例 ..... 14
2.1. 代表的な方式 ..... 14
2.2. エージェント型 SSO の構成 ..... 14
2.3. エージェント型 SSO 構成での設定方法例 ..... 15
2.4. リバースプロキシ型 SSO の構成 ..... 16
2.5. リバースプロキシ型 SSO 構成での設定方法例 ..... 17
2.6. SAML の構成 ..... 18
AgileWorks の設定 ..... 18
Identity Provider の設定 ..... 18
2.7. 別アプリケーションからの SSO（SSO 製品無し） ..... 19
3. ログイン画面のカスタマイズ ..... 20
3.1. 独自ログイン画面を用意 ..... 20
POST 認証用「ログイン認証」設定を作成 ..... 20
独自ログイン画面の HTML を準備 ..... 21
3.2. ログイン成功後、任意のアドオン画面へ遷移 ..... 22
4. 高度なログイン認証設定 ..... 23
4.1. クエリー記法例 ..... 23
4.2. 組込変数 ..... 24
4.3. 組込識別子 ..... 24
5. 制限事項 ..... 25
5.1. 既存のセッションが存在する場合の動作 ..... 25

## ◆ 改版履歴

| 版数 | 年月日 | 改版内容 |
|---|---|---|
| 第 1 版 | 2026 年 07 月 15 日 | 第 1 版作成 |

# 1. 概要

## 1.1. ログイン認証

AgileWorks では、ログイン認証に関する設定を管理サイトから行ないます。
設定画面は、管理サイト⇒【サイト管理】⇒【サイト共通設定】ワークベンチ⇒【認証・セキュリティ】⇒【ログイン認証】です。

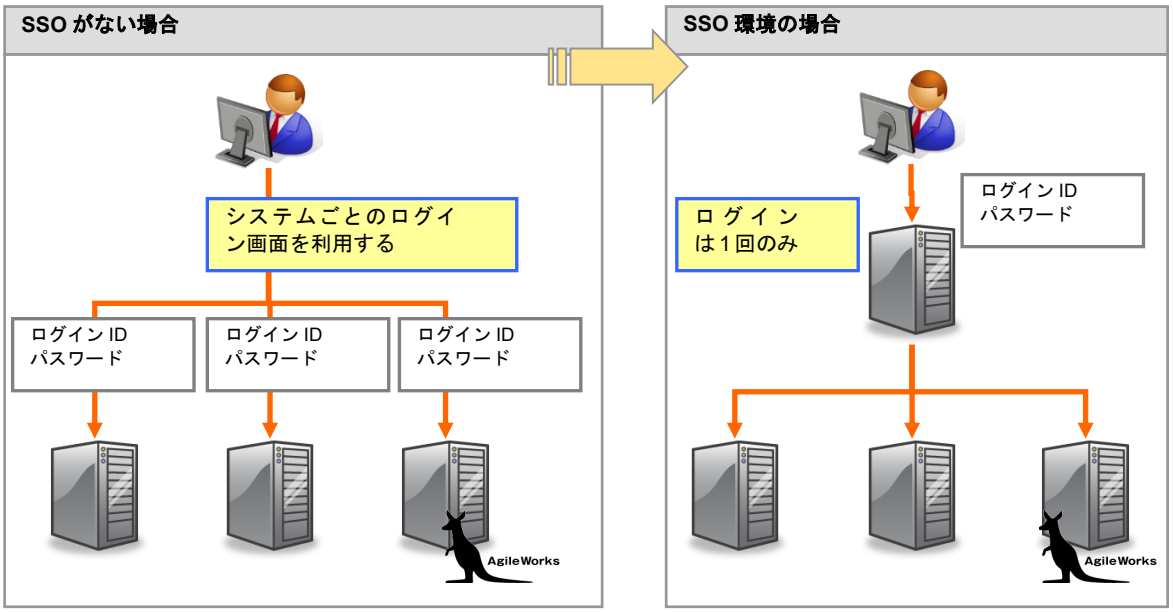
初期状態では、管理サイト／ユーザーサイトそれぞれの AgileWorks 標準ログイン画面からのログインが許可されています。
外部システム（SSO サーバー等）と連携して AgileWorks にシングルサインオンさせたい場合は、ログイン認証設定の追加を行って、ログイン方式に関する設定を行う必要があります。

AgileWorks が提供するログイン認証方式には、大きく以下の種類があります。

| ログイン認証の種類 | 説明 |
|---|---|
| 既定のログイン | AgileWorks 標準ログイン画面からログインする認証方式 |
| 外部連携 | SSO サーバーや外部システムで認証された状態を元に、AgileWorks に対してログインする認証方式<br>※「外部認証オプション」が必要です。 |
| SAML 連携 | SAML v2.0 の認証プロトコルに対応した認証方式<br>※「SAML 連携オプション」が必要です。 |
| Google Apps 連携 | Google Apps の OpenID 認証に対応した方式。<br>※「Google Apps 連携オプション」が必要です。 |
| サイボウズ オープン統合認証 ver.2 連携 | サイボウズのガルーン に対応した方式。<br>※「サイボウズ ガルーン連携オプション」が必要です。 |
| desknet's NEO 連携 | desknet's NEO に対応した認証方式。<br>※「desknet's NEO 連携オプション」が必要です。 |
| SharePoint 連携 | SharePoint に対応した認証方式。<br>※「SharePoint 連携オプション」が必要です。 |

## 1.2. SSO とは

ユーザーが一度認証を受けるだけで、異なるシステムやアプリケーションにログイン無しでアクセスできることを SSO（シングルサインオン）といいます。
AgileWorks の SSO 認証設定を行なうと、外部システムで認証されれば、AgileWorks にはログイン無しで利用できるようになります。（内部的には外部システムからの認証情報を元に認証処理は行なわれています）




補足
上の図のように、AgileWorks が SSO 製品の機能を補うものではなく、SSO 製品や IdentityProvider の配下として AgileWorks が存在するイメージとなります。AgileWorks から他システムへ認証情報を連携する機能はございません。

## 1.3. ログイン URL

AgileWorks へのログイン URL について説明します。

### AgileWorks標準のログイン画面URL

▼ ユーザーサイト

http://{Server}/AgileWorks/Broker/Picus

▼ 管理サイト

http://{Server}/AgileWorks/Broker/EMMA

※ 上記 URL は、インストーラーからインストールした時の標準的な URL です。
　インストール時にコンテキスト名を AgileWorks 以外に指定した場合は、以下の{ContextName}を指定したコンテキスト名に置き換えてください。

http://{Server}/{ContextName}/Broker/EMMA

### 外部認証（SSO）時のURL

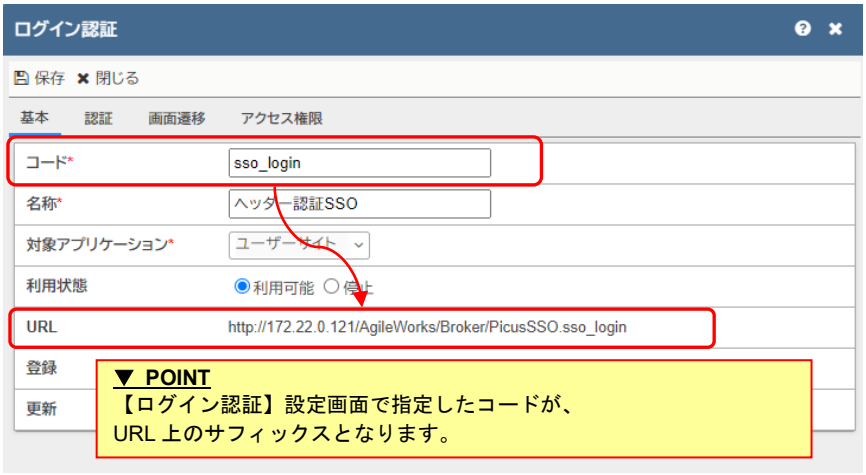
▼ ユーザーサイト

http://{Server}/AgileWorks/Broker/PicusSSO.{$Code}

▼ 管理サイト

http://{Server}/AgileWorks/Broker/EMMASSO.{$Code}

【重要】$Code について
$Code には、【ログイン認証】設定で指定したコードを指定します。




注意事項
SSO を利用する場合、R2.0 までの URL と、R2.1 からの URL が変更となっています。
R2.0 からマイナーバージョンアップした場合は、上記仕様に合わせて SSO 側の URL 設定変更が必要となります。

### SAML時のURL

▼ ユーザーサイト

http://{Server}/AgileWorks/Broker/PicusSAML

▼ 管理サイト

http://{Server}/AgileWorks/Broker/EMMASAML

▼ ガジェット

書類件数ガジェット: http://{Server}/AgileWorks/Broker/GadgetSAML?Code=$portlet.count
書類作成ガジェット: http://{Server}/AgileWorks/Broker/GadgetSAML?Code=$portlet.new
書類一覧ガジェット: http://{Server}/AgileWorks/Broker/GadgetSAML?Code=$portlet.list

▼ モバイルサイト

http://{Server}/AgileWorks/Broker/MobileSAML

## 1.4. ドキュメントビューア URL

AgileWorks の書類表示ビューアである「ドキュメントビューア」を外部システム等から直接開く場合、以下で説明する URL をリンクします。

### 新規でドキュメントビューアを開くためのURL

例えばグループウェアやポータルから AgileWorks の書類を新規で開くためのリンクを設置するには、以下形式の URL をリンクします。

```
http://{Server}/AgileWorks/Broker/Document?FormCode={$FormCode}&RuleCode={$RuleCode}
```

・$FormCode : 管理サイトで指定したフォームコード
・$RuleCode : 管理サイトで指定した回付ルールコード

### 保存された書類を開くためのURL

保存された書類を他システムや、通知メール文面等から直接開くには、以下形式の URL をリンクします。

```
http://{Server}/AgileWorks/Broker/Document?DocId={$DocId}
```

・$DocId : AgileWorks の書類 ID
※「書類 ID」は、AgileWorks が自動的に採番した、書類を識別する為の一意の値です。

### 「既定のログイン」以外で書類を開くためのURL

AgileWorks ではログイン認証設定を複数設定できます。
「既定のログイン」以外に SSO 用のログイン認証設定を追加しており、その SSO 用ログイン設定を利用して書類をダイレクトに開く場合は、下記のような URL を指定します。

▼ 新規で書類を開く URL

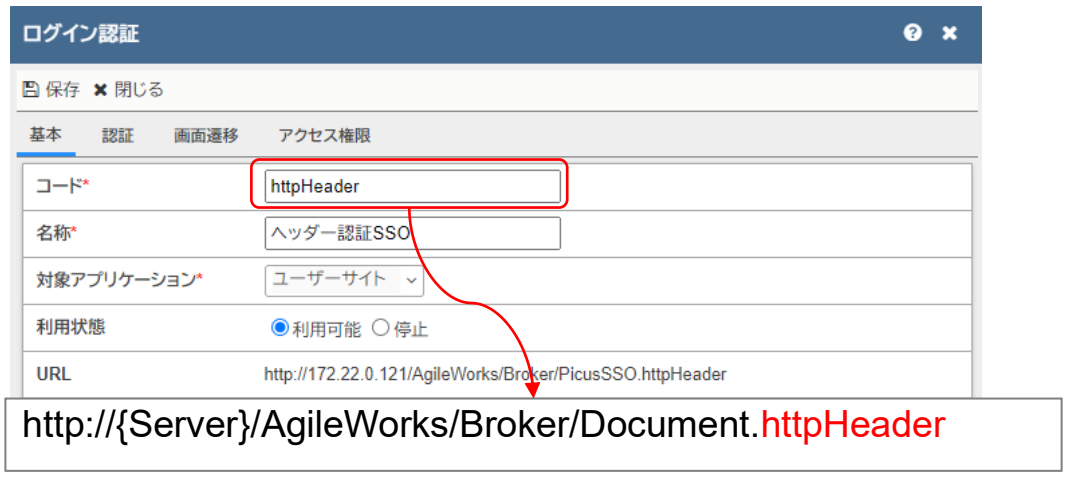
```
http://{Server}/AgileWorks/Broker/Document.{$LoginCode}?FormCode={$FormCode}&RuleCode={$RuleCode}
```

▼ 保存された書類を開く URL

```
http://{Server}/AgileWorks/Broker/Document.{$LoginCode}?DocId={$DocId}
```

・$ LoginCode: AgileWorks のログイン認証設定コード

▼ SSO 用ログイン認証で、書類を直接表示する時の URL 例



## 1.5. 書類作成時のフィールド値指定

「新規でドキュメントビューアを開くための URL」にて書類を作成する際に、任意のフィールドに指定した値をセットすることができます。
{フィールド ID}={フィールド値} のように指定し、GET と POST の両方に対応しています。

例）GET を利用する場合

```
http://・・・/Document?FormCode=RINGI&RuleCode=RINGI&title=doc_title&item_0=item_name&price_0=100
```

### 利用するにあたって

本機能は全フォームに対して利用することが可能です。

本機能は外部システムの情報を元に書類を作成するような場合に手入力の手間を削減するための機能です。
利用する際には書類URL を配置しているポータルや外部システム側でフィールドIDとフィールド値を指定する仕組みを構築する必要があります。

### 利用可能なフィールド

文字フィールドやコンボボックスなど、入力フィールドに対して利用することができます。
表明細のフィールドでも利用可能です。
表明細のフィールドを指定する際には「フィールド ID_行番号」のように指定してください。行番号は「0」から始まります。

ただし、「不可視」「編集禁止」「無効」の何れかの属性が有効なフィールドでは利用できません。

### 指定するフィールド値

フィールド値は URL エンコードされている必要があります。

コンボボックスやチェックボックスなどの書類上に表示される値（表示値）と DB に保存される値（DB 登録値）が異なる場合のあるフィールドでは、「DB 登録値」を指定してください。

### 書類を表示する際の動作

本機能によって値をセットした場合、書類の表示時に入力チェックなどが動作します。
そのため、X-WebForm にて設定した最大入力文字数を超える値をセットするようなことはできません。

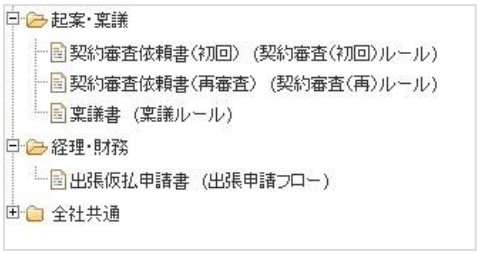
値のセットはサーバー側で行われるため、ブラウザ上で動作する OnLoad イベントなどでセットした値を利用することが可能です。

> 注意事項
> フィールド値の指定に GET を利用する場合はフィールド数とフィールド値の文字数が多くならないように注意してください。
> 上記要素が多いと URL が長くなり、ブラウザによってはアクセスできない場合があります。

## 1.6. ガジェットの利用

AgileWorks が提供するガジェットの利用方法について説明します。
AgileWorks 製品内部に組み込まれる形で 3 種類のガジェットを用意しています。

▼ 書類作成ガジェット




▼ 書類件数ガジェット




▼ 書類一覧ガジェット




ガジェットを利用するには、管理サイト⇒【サイト管理】⇒【サイト共通設定】ワークベンチ⇒【認証・セキュリティ】⇒【ログイン認証】から設定します。

1) "外部連携"用の設定を追加
2) 「対象アプリケーション」に"ガジェット"を選択
3) 「AgileWorks ユーザーとの引当方法」を指定



**▼書類作成ガジェット URL**

http://{Server}/AgileWorks/Broker/GadgetSSO.{$Code}?Code=$portlet.create

書類作成ガジェットでは自動更新などのクエリパラメーターは利用できません。

**▼書類件数ガジェット URL**

http://{Server}/AgileWorks/Broker/GadgetSSO.{$Code}?$Code=portlet.count

書類件数ガジェット URL の受付パラメータ（R2.5.0 にて追加、変更がありました。）

| パラメータ | 説明 |
|---|---|
| aw_target | リンククリック時のユーザーサイト遷移先ウィンドウターゲット。<br>A 要素の TARGET 要素にあたる値を指定する(_blank/_top 等)<br>デフォルトは_blank。 |
| aw_reload | 自動更新間隔を秒で指定。<br>デフォルトは 600(＝10 分)。0 を指定すると自動更新されません。 |
| aw_css | 任意の CSS ファイルを読み込みます。<br>URL を相対、又は絶対指定してください。 |
| aw_wrap | 書類状態を 1 列に何個配置するかを 1～7 の範囲で指定します。<br>1 を指定した場合：1 列に 1 つだけ（縦に並ぶ）<br>2 を指定した場合：1 列に 2 つずつ並ぶ |

パラメータ指定例） ウィンドウターゲットを_top、自動更新間隔を 5 分
http://{Server}/AgileWorks/Broker/GadgetSSO.{$Code}?Code=$portlet.count&aw_target=_top&aw_reload=300

**▼書類一覧ガジェット URL**

http://{Server}/AgileWorks/Broker/GadgetSSO.{$Code}?Code=$portlet.list

書類一覧ガジェット URL の受付パラメータ（R2.5.0 にて追加、変更がありました。）

| パラメータ | 説明 |
|---|---|
| aw_target | リンククリック時のユーザーサイト遷移先ウィンドウターゲット。<br>A 要素の TARGET 要素にあたる値を指定する(_blank/_top 等)<br>デフォルトは_blank。 |
| aw_reload | 自動更新間隔を秒で指定。<br>デフォルトは 600(＝10 分)。0 を指定すると自動更新されません。 |
| aw_css | 任意の CSS ファイルを読み込みます。<br>URL を相対、又は絶対指定してください。 |
| aw_rows | 書類一覧の最大表示件数。<br>デフォルトは 20。0～99999999 の整数を指定してください。 |
| aw_height | 書類一覧の高さを指定します。<br>単位を px として、0～9999 の整数を指定してください。 |
| aw_heading | 書類一覧ガジェット上部のボタンを表示するかどうかを指定します。<br>on、又は off を指定します。デフォルトは on です。 |
| aw_selected | 初回表示時に選択されているタブを指定します。<br>1～5 までの整数を指定してください。左から順番に番号が振られています。<br>下書 ＝ 1、申請依頼 ＝2、・・・<br>デフォルトは承認依頼（2）です。 |
| aw_width | 書類一覧の幅を指定します。<br>単位を px として、1～9999 の整数を指定してください。<br>上記の範囲外、又は未指定の場合はガジェットを表示する領域に合わせて表示されます。<br>デフォルトは未指定。 |
| aw_fit | 「aw_width」で指定した書類一覧を表示する幅に、項目全体が納まるように各項目の幅を調節するかどうかを指定します。<br>（共通一覧ビューで指定した幅を割合として調節します）<br>yes を指定します。デフォルトは未指定。<br>未指定、又は yes 以外の場合は共通一覧ビューで指定した幅(px)で表示します。 |

パラメータ指定例）自動更新間隔を 5 分、最大表示件数を 40 件
http://{Server}/AgileWorks/Broker/GadgetSSO.{$Code}?Code=$portlet.list& aw_reload=300&aw_rows=40

- $Code には、【ログイン認証】設定で指定したコードを指定します。
- インストール時にコンテキスト名を AgileWorks 以外に指定した場合は、上記 URL 部分をコンテキスト名に置き換えてください。

注意事項
・ガジェットを利用するには「外部認証オプション」「Google Apps 認証連携オプション」「サイボウズ ガルーン連携オプション」「desknet's NEO 連携オプション」「SharePoint 連携オプション」のいずれかが必要です。
・ガジェットのパラメータはどの連携方式でも共通です。
・ガジェットは AgileWorks 製品内部組込型の HTML ファイルであるため、画面デザイン等のカスタマイズはできません。

書類作成ガジェット、書類一覧ガジェットからの書類表示に関する仕様

ガジェットからの書類表示は、AgileWorks 仕事・検索画面からの表示とは以下の点で異なります。

・AgileWorks 側の設定「ダブルクリックによる書類表示方式」に関わらず、必ず別ウィンドウによる表示となります。
・「書類一覧ガジェット」からドキュメントビューアを開いた場合、次へ(→)、前へ(←)機能は利用できません。
・「書類一覧ガジェット」からドキュメントビューアを開いて【承認】操作等を行って閉じた場合、
ガジェット側の件数・一覧表示は更新されません。(ガジェット側で「更新」を手動実行すると更新されます)
・「書類一覧ガジェット」の報告確認からドキュメントビューアを開いた場合、
本人が複数ステップを兼務していると「確認」メニューが表示されないことがあります。
その場合は「回付状況」画面から、確認ステップ上の自分の名称をクリックし、
確認ステップの立場で書類を再表示してください。

## 1.7. ガジェット利用時のユニークログインユーザー数の考え方

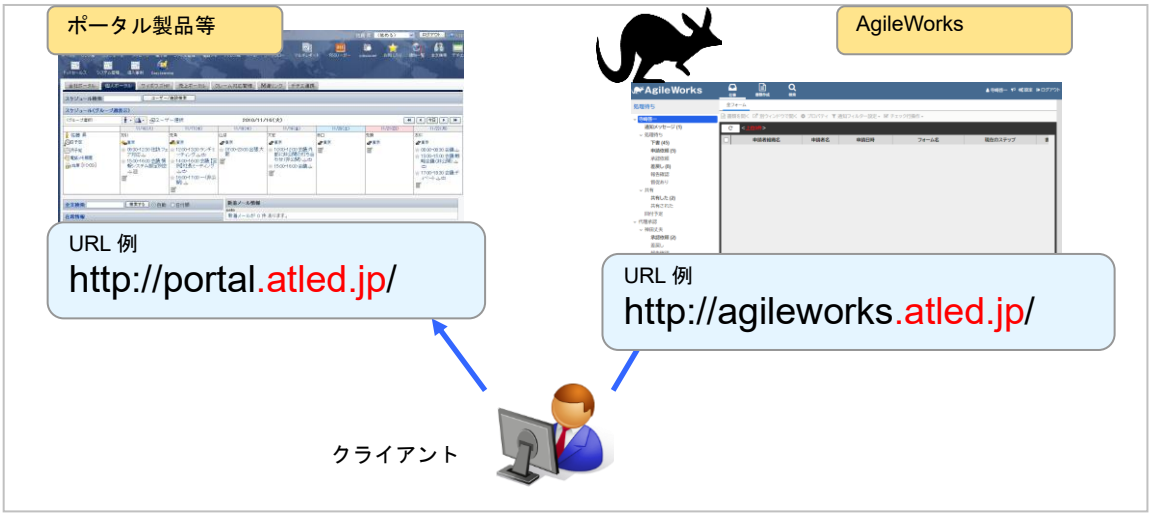
ガジェットにてログイン(SSO)を行った直後は AgileWorks のライセンスにてカウントされる同時ログインユーザー数にはカウントされません。
ガジェットから「ユーザーサイト」や「書類(ドキュメントビューア)」を開いたタイミングで同時ログインユーザー数にカウントされるセッションに変化します。

その後、ユーザーサイトや書類の操作を続けている限り、同時ログインユーザー数にカウントされ続けますが、
必要な操作(書類の申請や承認など)を終え、ガジェットのリロード、または自動リロードのみの時間が一定時間続くとそのセッションはライセンスの同時ログインユーザー数にカウントされなくなります。
※ガジェットにログインした直後と同じ扱いに戻ります。
R3.1.1a 以降での動作です。

本動作の詳細につきましてはサポートサイトの「ガジェット利用時のセッションについて」をご参照ください。

## 1.8. ガジェットにおける制限事項

ガジェットは、AgileWorks 側で認証が成功した際の情報を Web ブラウザの Cookie に書き出し、該当情報を参照することで連携を実現しています。
Cookie はセキュリティやプライバシーの観点から、Cookie を発行したドメイン内または Cookie に書き出された domain 属性で指定された範囲内でのみ読み出すことができる為、基本的にはガジェットを利用するポータル製品等と AgileWorks の接続 URL は、同一ドメインにする必要があります。




注意事項
ガジェットを利用するポータル製品等と AgileWorks の接続 URL を同一ドメインにすることができない場合は、AgileWorks の AP サーバー上で稼働している Apache に設定を追加することでガジェットを表示させることが可能です。(2025/11/28 現在)

詳細は以下 FAQ をご参照ください。

▼[FAQ00320]グループウェア連携で Chromium 派生ブラウザを利用すると、AgileWorks へのシングルサインオンやガジェット表示が行えない
https://support.atled.jp/agileworks?id=kb_article_view&sysparm_article=KB0173795

## 1.9. 書類を直接開いた状態でログアウトする

ドキュメントビューアやガジェットから直接書類を開いた場合、ドキュメントビューアに「ログアウト」ボタンが表示されます。
この「ログアウト」ボタンを押下すると、AgileWorks からログアウトし、ログイン認証設定の「画面遷移 > ログアウト時」に従って画面が遷移します。

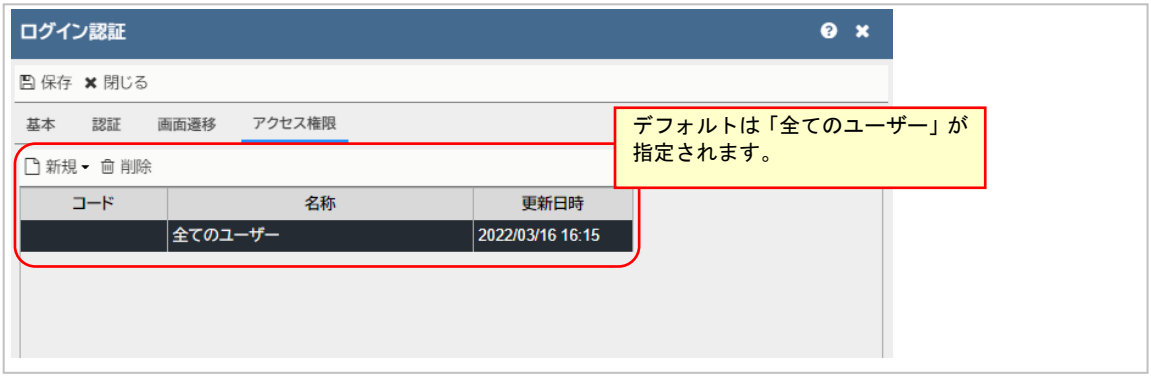



※ユーザーサイトの仕事や検索画面から開いた場合は表示されません。

## 1.10. ログイン認証設定のアクセス権限

ログイン認証設定は、設定毎に利用できるユーザーを限定することができます。
設定は、ユーザーや組織、ユニバーサルロール単位で指定可能です。

▼対象のログイン認証設定の【アクセス権限】タブに指定したユーザーのみ利用できます。



# 2. SSO実現例

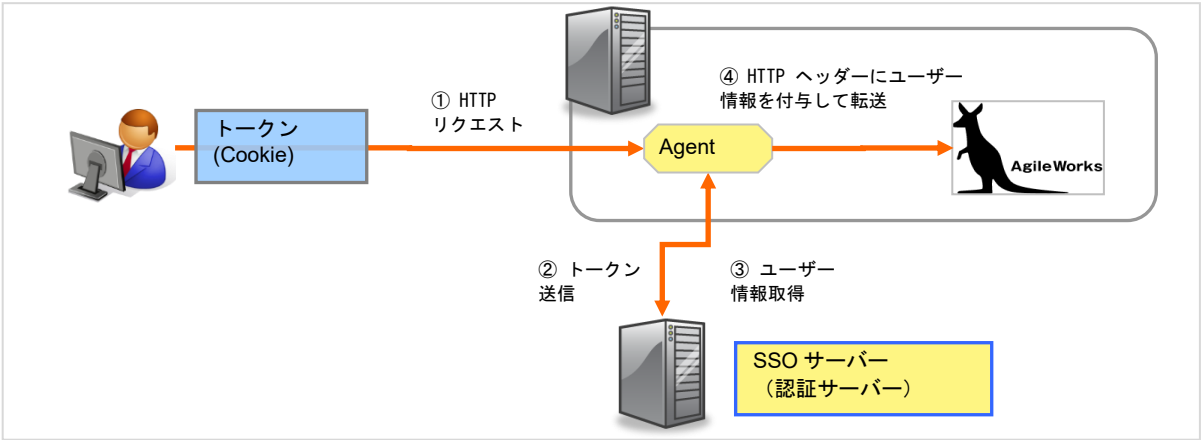
この章では、AgileWorks を SSO 配下のシステムとして動作させる場合のよくある構成と設定例について説明します。

## 2.1. 代表的な方式

SSO 構成の代表的なものには、「エージェント型」と「リバースプロキシ型」があります。
また、クラウドコンピューティングの台頭により、インターネット上のアプリケーション間 SSO をセキュアに実現するための方式として、標準化団体「OASIS」が策定した SAML という仕様も存在します。
AgileWorks ではそれぞれの SSO 方式を想定した SSO 認証の仕組みに、管理サイトからの設定で対応できるようになっています。

## 2.2. エージェント型 SSO の構成

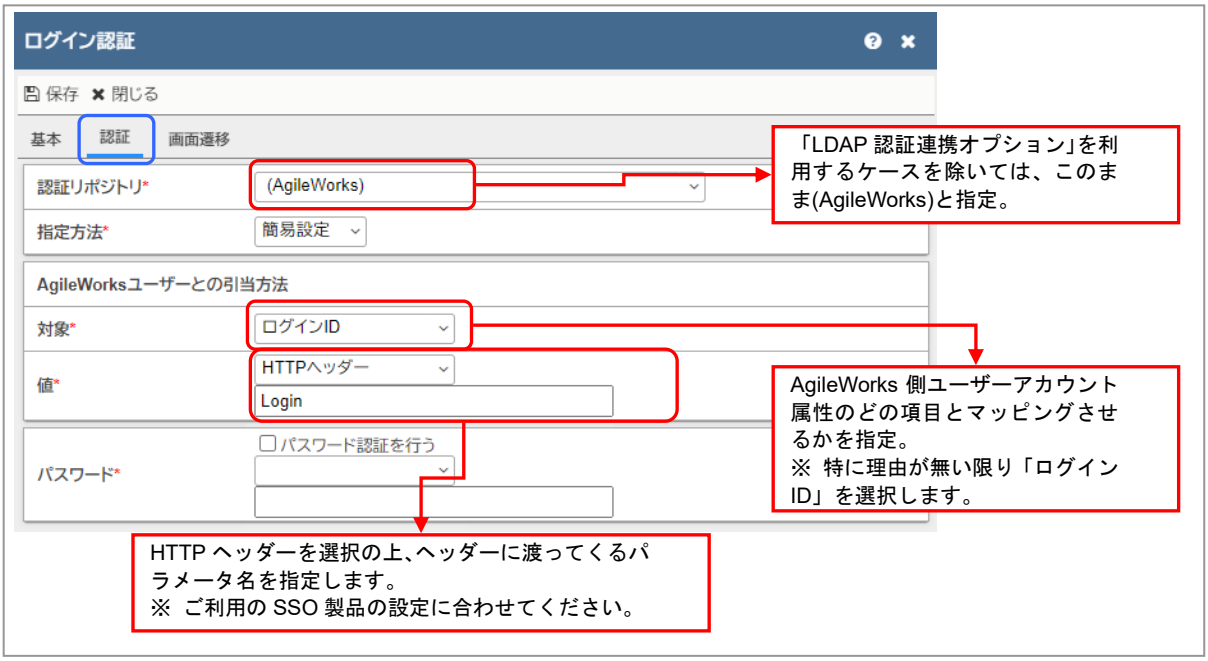
エージェント型 SSO の場合、AgileWorks の Web サーバーに、SSO 製品が提供するエージェントモジュール（ポリシーエージェント等と呼ばれます）を組み込む必要があります。通常、エージェントモジュールは Web サーバーApache 等の module としてインストールします。
エージェント型 SSO では、AgileWorks への認証リクエストには HTTP ヘッダー内にユーザー情報（認証情報）が入ってくるケースが多い為、その場合、AgileWorks 側 SSO 設定では、HTTP ヘッダーからログイン情報を取得して認証する為の設定を行ないます。



## 2.3. エージェント型 SSO 構成での設定方法例

エージェント型 SSO を利用する場合の設定例を説明します。

管理サイト⇒【サイト管理】⇒【サイト共通設定】ワークベンチ⇒【認証セキュリティ】⇒【ログイン認証】画面
メニューバー「新規」⇒「外部連携」を選択し、
「ログイン認証」画面の「認証」タブを、以下の要領で設定します。




AgileWorks の一部のユーザーサイト機能や管理機能はエージェント型 SSO 構成に対応していません。そのため、SSO 製品の管理下に置く URL を以下に限定する必要があります。

▼ SSO 製品の管理下に置く URL
[製品固定の URL]
・http://{サーバー名}/AgileWorks/Broker/Picus
・http://{サーバー名}/AgileWorks/Broker/EMMA
・http://{サーバー名}/AgileWorks/Broker/Gadget
・http://{サーバー名}/AgileWorks/Broker/Mobile
・http://{サーバー名}/AgileWorks/Broker/Document
[ログイン認証毎の URL]
・http://{サーバー名}/AgileWorks/Broker/PicusSSO.{$Code}
・http://{サーバー名}/AgileWorks/Broker/EMMASSO.{$Code}
・http://{サーバー名}/AgileWorks/Broker/GadgetSSO.{$Code}
・http://{サーバー名}/AgileWorks/Broker/MobileSSO.{$Code}
※ログイン認証設定画面に表示されている URL
・http://{サーバー名}/AgileWorks/Broker/Document.{$Code}
※ユーザーサイト用のログイン認証設定時のみ

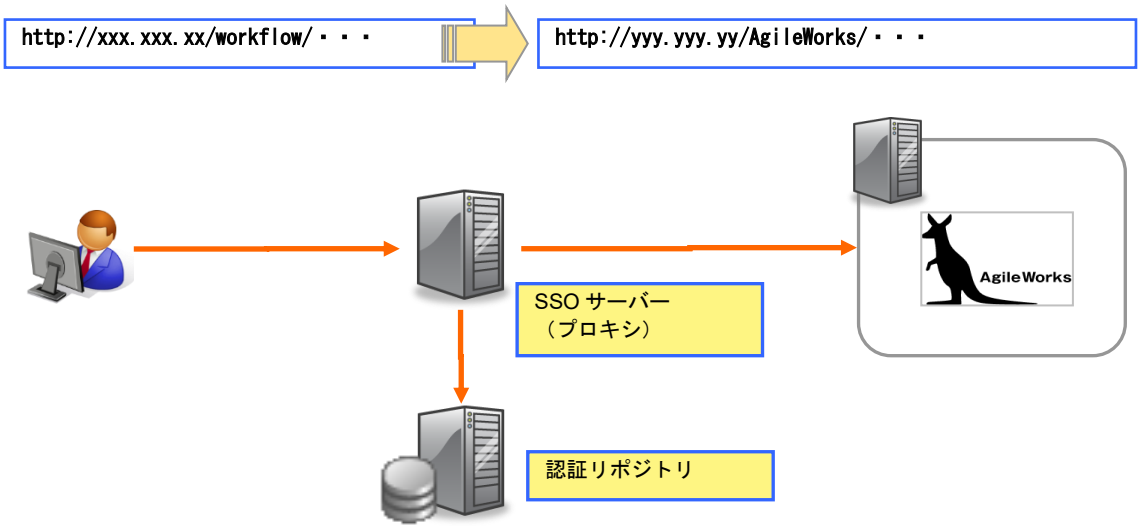
【重要】$Code について
$Code には、【ログイン認証】設定で指定したコードを指定します。

▼ SSO 製品の管理下から除外する URL
・上記以外の URL

注意事項
エージェント型 SSO の場合、AgileWorks の Web サーバーに SSO エージェントモジュールをインストールする必要がある為、AgileWorks を Cloud として利用するなど Web サーバーApache の設定を変更できない構成では、エージェント型 SSO の実現はできません。Cloud 型構成では SAML 認証を利用してください。

## 2.4. リバースプロキシ型 SSO の構成

リバースプロキシ型 SSO の場合、AgileWorks の Web サーバーにエージェントモジュールをインストールする必要はありません。クライアント Web ブラウザから AgileWorks へのリクエストは必ずプロキシサーバーを経由し、プロキシサーバーが認可・認証した後に、AgileWorks へリクエストを転送します。

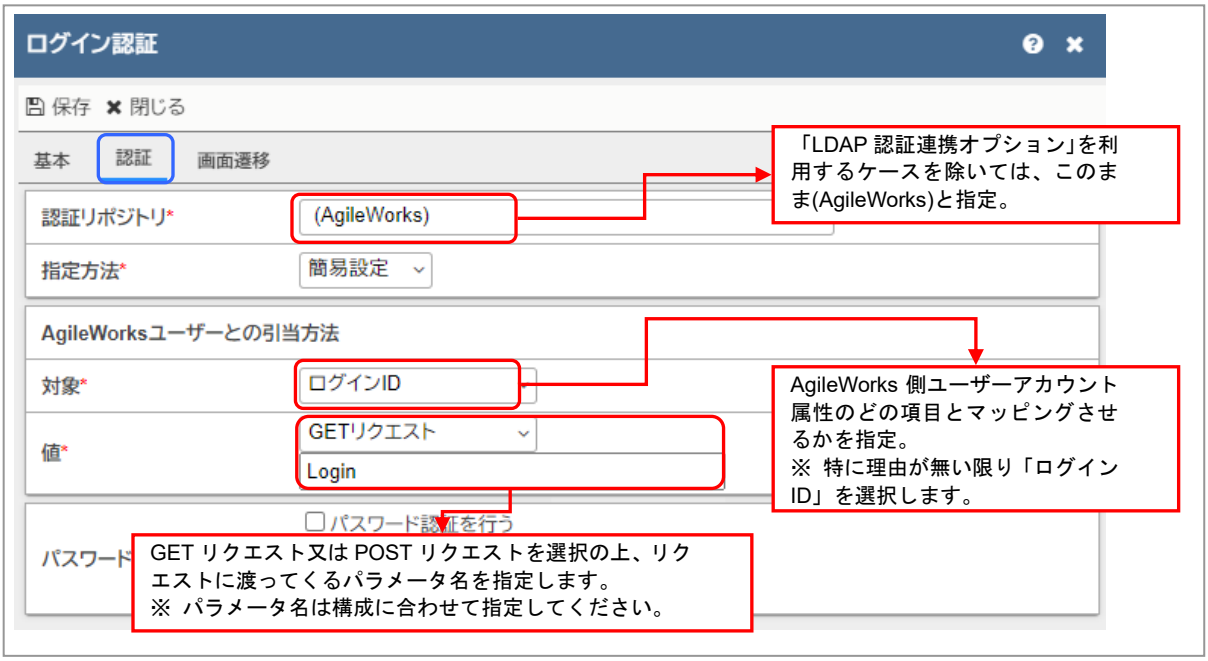



プロキシサーバーから転送されたリクエスト等に AgileWorks 側認証に必要な情報が付与されています。
認証情報を付与する方式は SSO 製品や設定により異なり、HTTP ヘッダーに認証情報を付与したり、HTTP リクエストの GET パラメータに認証情報を付与したりと様々ですが、ここでは、プロキシサーバーから転送された HTTP リクエストの GET or POST パラメータにユーザー情報（認証情報）が入ってくる事を想定し、AgileWorks 側 SSO の設定例を説明します。

## 2.5.　リバースプロキシ型 SSO 構成での設定方法例

リバースプロキシ型を利用する場合の設定例を説明します。

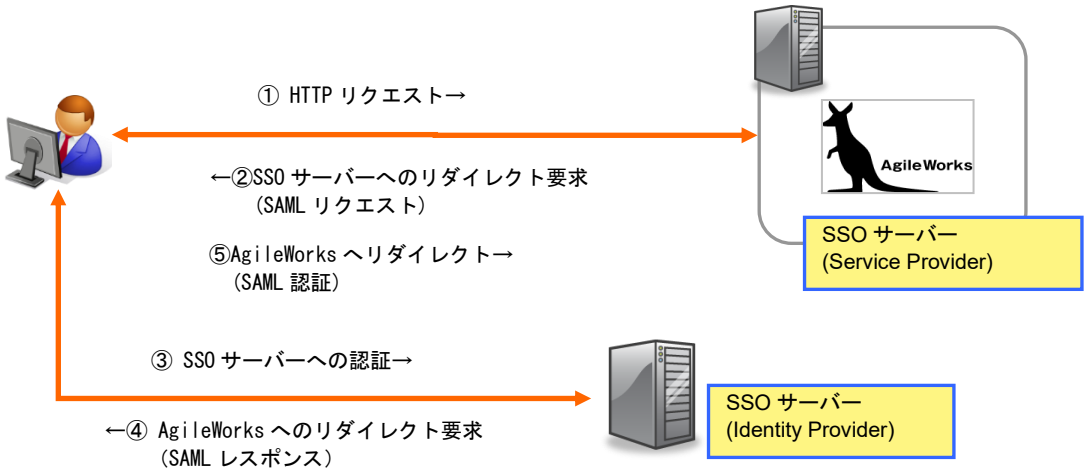
管理サイト⇒【サイト管理】⇒【サイト共通設定】ワークベンチ⇒【認証セキュリティ】⇒【ログイン認証】画面
メニューバー「新規」⇒「外部連携」を選択し、
「ログイン認証」画面の「認証」タブを、以下の要領で設定します。



## 2.6. SAML の構成

SAML(Security Assertion Markup Language) は、クロスドメインでユーザーの認証と認可のデータ交換をサポートする XML ベースの標準規格です。
AgileWorks は、SAML v2.0 の仕様に基づいた SSO サービスプロバイダーとして動作することが可能です。

AgileWorks は SP-Initiated-SSO のみに対応しており、
SAML v2.0 で SSO を実現した場合、以下①～⑤の流れで認証リクエストのやり取りがされます。

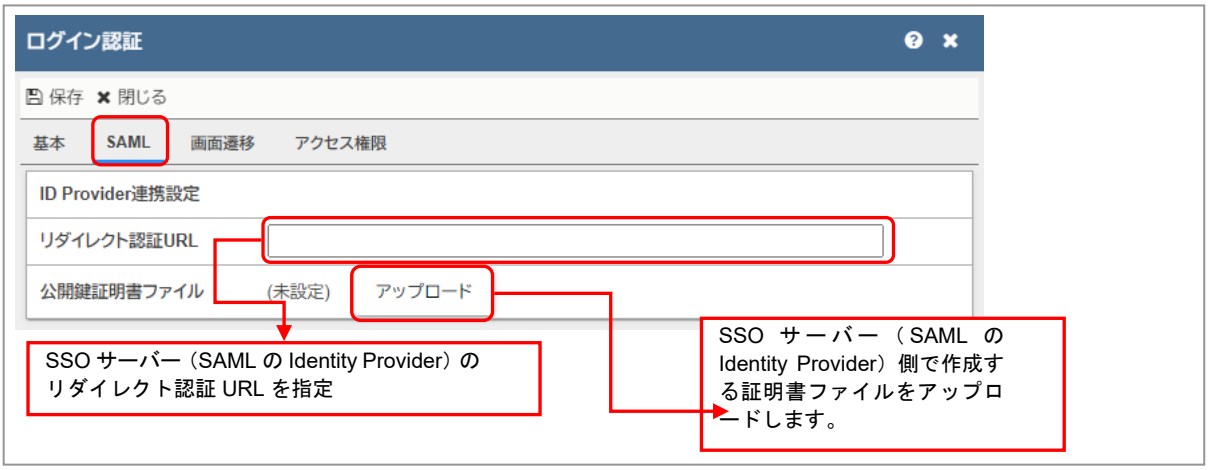



SAML を使用して SSO を実現するには、事前に SSO サーバー(SAML の Identity Provider)から、URL と公開鍵(X509 証明書)を取得し、管理サイトへアップロードします。

URL と公開鍵(X509 証明書)を取得した上で、AgileWorks 管理サイトから以下の要領で設定を行ないます。

### AgileWorksの設定

管理サイト⇒【サイト管理】⇒【サイト共通設定】ワークベンチ⇒【認証セキュリティ】⇒【ログイン認証】画面
ログイン認証の一覧に「SAML 認証」の設定が初めから登録されていますので、「SAML 認証」の行を選択してメニューバー「編集」をクリックします。
※初期状態では「利用状態」が"停止"になっていますので、利用する場合は"利用可能"に変更する必要があります。




### Identity Providerの設定

| 一般的な項目名 | 設定内容 |
|---|---|
| EntityID、識別子 | atled.jp |
| リダイレクト URL、<br>アサーションコンシューマエンドポイント、<br>エンドポイント URL | ユーザーサイト：https://{サーバー名}/AgileWorks/Broker/PicusSAML<br>管理サイト：　https://{サーバー名}/AgileWorks/Broker/EMMASAML<br>ガジェット：　https://{サーバー名}/AgileWorks/Broker/GadgetSAML |
| NameIDFormat | urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified<br>※返却値は AgileWorks 側ユーザーの「ログイン ID」の値とします |
| AssertionConsumerService Binding | POST |

## 2.7. 別アプリケーションからの SSO（SSO 製品無し）

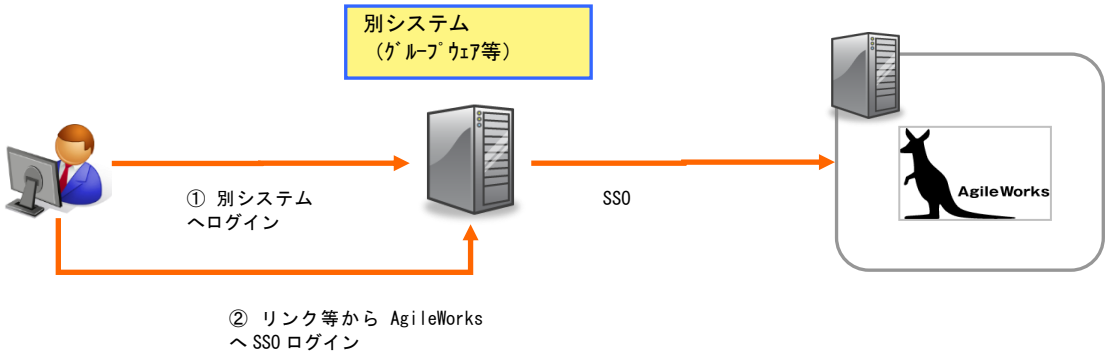
SSO 製品が無い構成で、別システムから AgileWorks へ SSO する為の実現例を説明します。

この場合は、企業内各システムを SSO で統合する方式ではなく、システム対システムの 1 対 1 または 1 対多でのシングルサインオンとなります。

方法案 1) GET リクエストでの SSO
以下のような URL(例)を送信することで、他システムから AgileWorks への SSO が実現できます。

1) http://{Server}/AgileWorks/Broker/PicusSSO.{$Code}?LoginId=ABC1111
2) http://{Server}/AgileWorks/Broker/PicusSSO.{$Code}?LoginId=ABC1111&Password=hoge

方法案 2) POST リクエストでの SSO
AgileWorks のシングルサインオン用 URL に対して、POST で認証に必要な情報を SUBMIT する事で、他システムから AgileWorks への SSO が実現できます。
http://{Server}/AgileWorks/Broker/PicusSSO.{$Code}




注意事項
本章で説明する実現方式は、SSO 製品を利用した方式に比べるとセキュリティが低下する恐れがあります。
なぜなら、クライアントブラウザと AgileWorks サーバー間のリクエスト通信、URL、HTML ソース等に、ログイン認証に必要な情報が含まれてしまうからです。
IT 統制の視点でセキュリティ的な強度を求める場合は、SSO 製品を利用した方式を推奨します。

# 3. ログイン画面のカスタマイズ

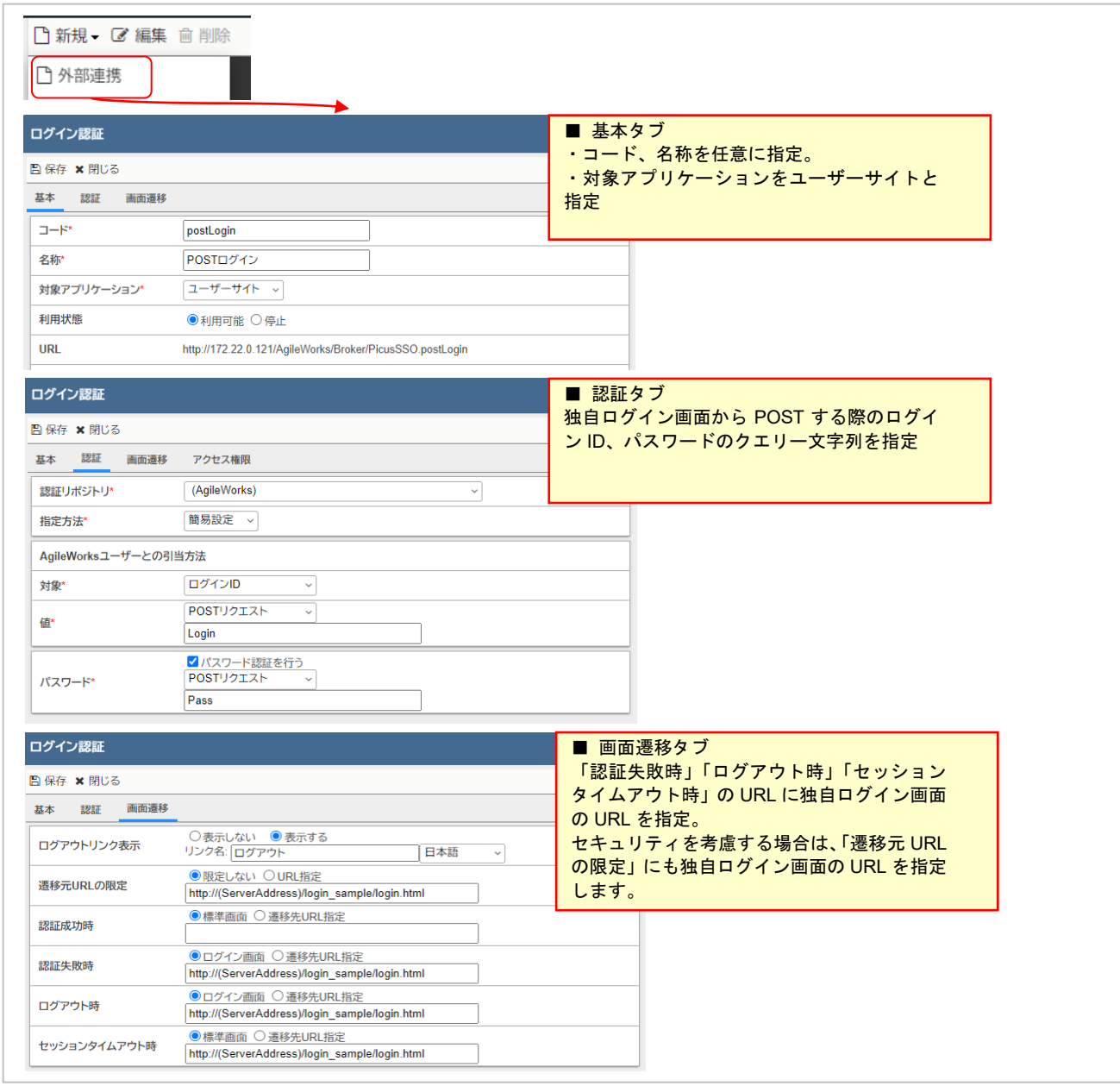
ログイン画面をカスタマイズする方法について説明します。

## 3.1. 独自ログイン画面を用意

AgileWorks 標準のログイン画面ではなく、固有のログイン画面を用意するための手順を説明します。

### POST認証用「ログイン認証」設定を作成

管理サイト⇒【サイト管理】⇒【サイト共通設定】ワークベンチ⇒【認証・セキュリティ】⇒【ログイン認証】




続けて、上記設定に合わせた独自ログイン画面の HTML を準備します。

## 独自ログイン画面のHTMLを準備

独自ログイン画面のサンプル HTML と JavaScript を示します。
準備した HTML は利用者から接続できる Web サーバー（Apache）に配置して、利用してください。

▼ サンプル HTML

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
        "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
        <meta http-equiv="content-type" content="text/html; charset=utf-8" />
        <script type="text/javascript" src="sample.js"></script>
        <title>AgileWorks Sample Login</title>
</head>
<body onload="initMessage();">
<form action="http://{Server}/AgileWorks/Broker/PicusSSO.postLogin" method="post">
ログイン ID :
<input type="text" id='Login' name='Login' value="" maxlength="255" style=" ime-mode:disabled;"/>
<br>
パスワード :
<input type="password" id='Pass' name='Pass' value="" maxlength="255" style="ime-mode: disabled;"/>
<br>
<input type="submit" value="ログイン" />
<br>
<div id="message" />
</form>
</body>
</html>
```

・POST 先(form action の値)には、AgileWorks ログイン認証設定の SSO 用ログイン URL を指定します。
・ログイン ID の name には、AgileWorks ログイン認証設定のログイン ID の値を指定します。
・パスワードの name には、AgileWorks ログイン認証設定のパスワードの値を指定します。

補足
このサンプル HTML ではデザインは考慮していない為、デザインは独自に準備してください。また、セキュリティ的には input タグに autocomplete="off"要素を追加する等の考慮も必要です。ここで提示する HTML は、あくまでサンプルという位置付けとなりますので、HTML の準備と利用は構築担当者の責任の上で実施・テストしてください。

▼ サンプル JavaScript
この JavaScript では、ログイン失敗時のエラーコードを取得して、message エリアに値を表示する処理をしています。

```
function initMessage() {
   var messageLabel = document.getElementById('message');
   var errorCode = getErrorCode();
   if ( errorCode ) {
      switch (errorCode) {
         case "BRKCMN-W0002":
               messageLabel.innerHTML = 'ログイン ID またはパスワードに誤りがあります。';
               break;
         case "BRKCMN-E0009":
               messageLabel.innerHTML = 'ライセンスが適用されていません。システム管理者へ連絡してください。';
               break;
         case "BRKCMN-E0018":
               messageLabel.innerHTML = 'メンテナンス中のため、ログインできません。';
               break;
         default:
               break;
      }
   }
   if (document.forms[0].Login && focus) {
      document.forms[0].Login.focus();
   }
}

function getErrorCode() {
   var queryString = document.location.search;
   if ( !queryString ) return "";

   // ?を除いたクエリストリング取得
   var queryStringNotQuestion = document.location.search.substring( 1 );
   var parameters = queryStringNotQuestion.split('&');

   for ( var i = 0; i < parameters.length; i++ ) {
      var element = parameters[i].split('=');
```

```
        if ( element[0] == 'aw.errorCode' ) {
            return element[1];
        }
    }
    return "";
}
```

ログイン認証に失敗すると「認証失敗時の遷移先 URL」のクエリパラメータ「aw.errorCode」に失敗要因を表す AgileWorks 側のエラーコードが付与されます。
本書のサンプル JavaScript では、getErrorCode メソッドでクエリパラメータから aw.errorCode の値を取得して返却するようにしています。

▼ 失敗時のエラーコード

| コード | メッセージ |
|---|---|
| BRKCMN-W0002 | ログイン ID またはパスワードに誤りがあります。 |
| BRKCMN-E0009 | ライセンスが適用されていません。システム管理者へ連絡してください。 |
| BRKCMN-E0018 | メンテナンス中のため、ログインできません。 |

## 3.2. ログイン成功後、任意のアドオン画面へ遷移

ログイン成功後、AgileWorks 標準のユーザーサイトではなく、独自のアドオン画面へ遷移させるには、認証成功時の遷移先 URL をクエリパラメータとして渡すことで実現できます。

▼ クエリパラメータ名
**aw.redirectUrl**

「独自ログイン画面の HTML を準備」で示したサンプル HTML に遷移先 URL に付与するには、以下の要領で hidden フィールド等に aw.redirectUrl を指定します。

```
<input type="hidden" name=”aw.redirectUrl” value="http://hogehoge/" />
```

▼ オープンリダイレクト可能なサイトの制限
aw.redirectUrl による任意の画面への遷移を利用する場合、意図しない外部サイトへのリダイレクト（オープンリダイレクト）を防ぐために、遷移可能なサイトを制限することができます。

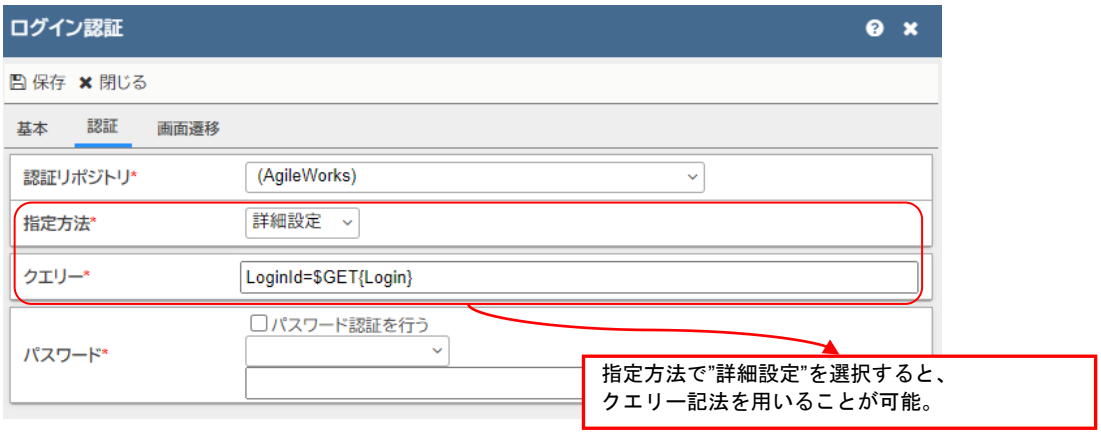
【設定箇所】
管理サイト ⇒ 【サイト管理】 ⇒ 【サイト共通設定】ワークベンチ ⇒ 【認証・セキュリティ】 ⇒ 【セキュリティポリシー】

上記の設定画面にて「オープンリダイレクト可能なサイトの制限」チェックボックスを有効にし、下部の入力欄に許可するサイトのドメインを記載することで、そのサイトへのみリダイレクトを可能とします。

【入力時の条件・注意事項】
・複数のサイトを登録する場合は、サイトごとに改行で区切り、指定してください。
・「システム URL」および「モバイルサイト用システム URL」は、本入力欄が未入力であってもリダイレクト可能です。

# 4. 高度なログイン認証設定

ログイン認証設定では、設定画面の GUI 上だけでは指定できないような複雑な要件に対応する為、「詳細設定」からクエリー記法による設定ができるようになっています。
通常は、ここで説明する記法を用いずとも、GUI 上の「簡易設定」で実現ができますが、
・AgileWorks に渡ってくる複数のパラメータと引当してログインさせたい。
といった要件の場合、クエリー記法による設定を用いる必要があります。




## 4.1. クエリー記法例

1) GET で渡ってくる hoge を、AgileWorks の「ログイン ID」と引当して認証する

```
LoginId=$GET[hoge]
```

2) 認証キーが複数の場合（認証リポジトリが(AgileWorks)）

```
MailAddress=$POST[hoge1], reserveItem2=$POST[hoge2]
```

※上記例では、POST で渡ってくる hoge1 と AgileWorks ユーザーアカウントの「メールアドレス」と引当て、POST で渡ってくる hoge2 と AgileWorks ユーザーアカウントの「拡張項目 2」を引当て、両方が引き当たった場合に認証させる記法例です。

3) 認証キーが複数の場合（認証リポジトリが LDAP）

```
(&(field1=$POST[hoge1])(field2=$POST[hoge2]))
```

※$()()といった文法は、LDAP クエリの記法にのっとっています。
※上記例の field1, field2 には、LDAP 側属性名を指定します。

## 4.2. 組込変数

ログイン認証時に、AgileWorks へ渡ってくる認証パラメータを変数で記述することができます。
指定可能な組込変数は以下の通りです。

▼ログイン方式=”AgileWorks”の場合
AgileWorks ログイン画面からのログイン認証する場合、ログイン画面から渡ってくるログイン ID を以下の変数名で取得します。

| 変数 | 説明 |
|---|---|
| $loginId | AgileWorks 標準ログイン画面から渡ってくる「ログイン ID」 |

▼ ログイン方式=”外部連携”の場合
AgileWorks へ SSO 認証する場合、渡ってくるパラメータを取得するための記法は以下の通りです。

| 変数 | 説明 |
|---|---|
| $GET[hoge] | GET リクエストに”hoge”というパラメータ名で渡ってくる値の取得方法。<br>※hoge 部分は、渡ってくるパラメータ名に合わせて指定します。 |
| $POST[hoge] | POST リクエストに”hoge”というパラメータ名で渡ってくる値の取得方法。<br>※hoge 部分は、渡ってくるパラメータ名に合わせて指定します。 |
| $HEADER[hoge] | HTTP ヘッダーに”hoge”というパラメータ名で渡ってくる値の取得方法。<br>※hoge 部分は、渡ってくるパラメータ名に合わせて指定します。 |
| $COOKIE[hoge] | Cookie に”hoge”というパラメータ名で渡ってくる値の取得方法。<br>※hoge 部分は、渡ってくるパラメータ名に合わせて指定します。 |
| $WWW _AUTH | Web サーバーの環境変数「REMOTE_USER」に渡ってくるパラメータを取得する方法 |

## 4.3. 組込識別子

ログイン認証時に、AgileWorks へ渡ってくる認証パラメータを変数で記述することができます。
指定可能な組込変数は以下の通りです。

▼ログイン方式=”AgileWorks”の場合
AgileWorks ログイン画面からのログイン認証する場合、ログイン画面から渡ってくるログイン ID を以下の変数名で取得します。

| 識別子 | 説明 |
|---|---|
| LoginId | AgileWorks ユーザーアカウントの「ログイン ID」 |
| UserCode | AgileWorks ユーザーアカウントの「ユーザーコード」 |
| MailAddress | AgileWorks ユーザーアカウントの「メールアドレス」 |
| reserveItem1～20 | AgileWorks ユーザーアカウントの「拡張項目 1～20」<br>※拡張項目 3 の場合は、reserveItem3 となります。 |

# 5. 制限事項

## 5.1. 既存のセッションが存在する場合の動作

AgileWorks の認証に成功して既にセッションが存在している環境下において、別ユーザーで新たにログイン認証を行った場合は、既存のセッションが優先されます。

例)
グループウェアに山田太郎でログインして、AgileWorks のガジェットを表示した。
グループウェア側でログアウトして、すぐに佐藤花子でログインし直し、AgileWorks のガジェットを表示した。
→この場合、山田太郎のセッションが存在している為、山田太郎のガジェットが表示される。

この時、以下のセッション破棄 URL を POST/GET リクエストで実行することで、既存セッションは破棄されます。

その為、同一マシンを複数人で利用するケース等が考えられる場合は、
・連携元システムのログアウト処理に組み込む
・AgileWorks への連携前に実行する
といった対応を検討します。

**▼セッション破棄 URL**

| |
|---|
| http://{Server}/AgileWorks/Broker/Picus?logout=1 |