目次

改訂情報

変更年月日	変更内容
2016-04-01	初版
2016-08-01	第2版 下記を追加・変更しました。 ▪ 「*OpenAM*」の「*バージョン*」を修正 ▪ 「*OpenAM*」に「*使用可能な署名アルゴリズム*」を追加 ▪ 「*Microsoft Entra ID*」の「*シングルログアウトについて*」を修正 ▪ 「*Microsoft Entra ID*」に「*Microsoft Entra ID に送信するリクエストの署名について*」を追加 ▪ 「*Microsoft Entra ID*」に「*Microsoft Entra ID の暗号処理について*」を追加 ▪ 「*Active Directory Federation Services*」に「*使用可能な署名アルゴリズム*」を追加 ▪ 「*salesforce.com*」に「*使用可能な署名アルゴリズム*」を追加
2017-04-01	第3版 下記を追加・変更しました。 ▪ 「*操作*」の「*SAML認証環境設定*」に表示タイプに関するコラムを追加 ▪ 「*操作*」に「*IdP一覧*」を追加 ▪ 「*操作*」の「*IdP新規作成*」にIdP表示方法とテナント解決方法に関するコラムを追加 ▪ 「*操作*」に「*IdP更新*」を追加 ▪ 「*操作*」の「*SAMLユーザマッピング(管理)*」にインポートモードに関するコラムを追加 ▪ 「*操作*」に「*一般ユーザログイン画面を経由せずSAML 認証してログインする方法*」を追加 ▪ 「*Microsoft Entra ID*」の「*Microsoft Entra ID にアプリケーションを追加*」にある入力値に関するコラムを修正
2019-08-01	第4版 下記を追加・変更しました。 ▪ 「*Microsoft Entra ID*」の手順を修正
2020-12-01	第5版 下記を追加・変更しました。 ▪ 「*注意事項*」 のエンティティIDの説明を修正 ▪ 「*注意事項*」 にバインディングURLの説明を追加 ▪ 「*注意事項*」 にベースURLの変更についての説明を追加
2022-06-01	第6版 下記を追加・変更しました。 ▪ 「*Microsoft Entra ID*」の手順を修正 ▪ 「*Okta*」の設定例を追加
2024-04-01	第7版 下記を追加・変更しました。 ▪ 「*Microsoft Entra ID*」の「Azure Active Directory (AzureAD)」の名称を「Microsoft Entra ID」に修正
2025-04-01	第8版 下記を追加・変更しました。 ▪ 「*注意事項*」 のエンティティIDの説明を変更 ▪ 「*注意事項*」 のバインディングURLの説明を変更 ▪ 「*注意事項*」 のベースURLの変更についての説明を変更 ▪ 「*Okta*」の「*intra-mart Accel Platform に Okta で追加したアプリケーションを登録*」を変更

はじめに

本書の目的

本書ではSAML認証機能のIdP に関するセットアップ方法および注意点について解説します。

対象読者

- SAML 認証機能のセットアップを行う方

本書の構成

本書は、以下のような内容で構成されています。

- *SAML 認証設定*
- *IdP 別の設定方法*

注意事項

本書内「*IdP 別の設定方法*」に記載されているIdP に関する説明は 2016年4月1日 現在のものとなります。

SAML 認証設定

ここでは、SAML 認証の設定について解説します。

操作

項目

SAML認証環境設定

intra-mart Accel Platform の一般ユーザログイン画面にある通常のログインフォームを表示するかどうかを変更する場合、システム管理者でログインして「システム管理」→「SAML認証設定」→「SAML認証環境設定」を選択してください。

コラム

- **「表示タイプ」に「動的に判定する」を選択した場合**
  「クラス名」の入力が必須です。入力するクラスの詳細は「SAML認証プログラミングガイド 」の「 ログインフォームの表示方法を制御する 」を参照してください。

IdP一覧

intra-mart Accel Platform に登録したIdP を確認する場合、システム管理者でログインして「システム管理」→「SAML認証設定」→「IdP一覧」を選択してください。「SPメタデータダウンロード」のアイコンをクリックすると intra-mart Accel Platform のメタデータをダウンロードできます。

IdP新規作成

intra-mart Accel Platform にIdP を登録する場合、システム管理者でログインして「システム管理」→「SAML認証設定」→「IdP一覧」を選択してください。一覧画面の「新規登録」ボタンからIdP 情報を登録します。
登録後、IdP を一意に識別するための「プロバイダID」が発行されます。「プロバイダID」は一般ユーザログイン画面を経由せずSAML認証して intra-mart Accel Platform にログインする際に使用します。詳細は「 *一般ユーザログイン画面を経由せずSAML 認証してログインする方法* 」を参照してください。

コラム

「IdP表示方法」に「動的に判定する」を選択した場合
「クラス名」の入力が必須です。入力するクラスの詳細は「SAML認証プログラミングガイド 」の「 SAML認証のボタン表示方法を制御する 」を参照してください。

コラム

バーチャルテナントによる複数テナント の場合、IdP で認証済みのユーザが intra-mart Accel Platform にログインするテナントを決定するため、「テナント解決方法」の「クラス名」の入力が必須です。入力するクラスの詳細は「SAML認証プログラミングガイド 」の「 SAML認証時のテナントIDの解決方法をカスタマイズする 」を参照してください。

IdP更新

intra-mart Accel Platform に登録したIdP の情報を更新か削除する場合、システム管理者でログインして「システム管理」→「SAML認証設定」→「IdP一覧」から「IdP名」のリンクを選択してください。

SAMLユーザマッピング(管理)

IdP で認証したユーザが intra-mart Accel Platform ではどのユーザでログインするかのマッピングをテナント毎に一括して登録・更新・削除する場合、テナント管理者でログインして「サイトマップ」→「SAML認証」→「SAMLユーザマッピング(管理)」を選択してください。
「新規作成」ボタンからマッピング情報を1件ずつ登録できます。「インポート」ボタンからはCSV ファイルでマッピング情報を一括登録できます。また、「エクスポート」ボタンから登録済みのマッピング情報をCSV ファイルでダウンロードできます。

> コラム
> - **「インポートモード」に「全件削除してインポート」を選択した場合**
> 対象のIdP のマッピング情報を全て削除後、CSV ファイルのマッピング情報を登録します。
> - **「インポートモード」に「更新モードでインポート」を選択した場合**
> CSV ファイル内のIdP ユーザと iAP ユーザのマッピング情報を削除後、CSV ファイルのマッピング情報を登録します。

SAMLユーザマッピングCSV フォーマット

インポートするCSV のフォーマットは1列目にはIdP のユーザコード、2列目には intra-mart Accel Platform のユーザコードを指定します。ユーザコードにダブルコーテーションまたはカンマが含まれていればエスケープします。以下はCSV ファイルの例です。

```
aoyagi@domainname,aoyagi
ikuta@domainname,ikuta
hayashi@domainname,hayashi
katayama@domainname,katayama
maruyama@domainname,maruyama
"sekine""domainname",sekine
"ueda,domainname",ueda
```

SAMLユーザマッピング

ログインしている intra-mart Accel Platform ユーザとIdP ユーザをマッピングする場合、「サイトマップ」→「SAML認証」→「SAMLマッピング」を選択してください。「新規作成」ボタンからマッピング情報を登録します。

一般ユーザログイン

登録したIdP の「状態」と「シングルサインオン」が「有効」であり、「IdP表示方法」の表示条件を満たすと一般ユーザログイン画面にSAML 認証でログインするボタンが表示されます。
ボタンを押下した先のIdP ログイン画面でログインすると intra-mart Accel Platform のログイン後のページへ遷移します。

> コラム
> - **IdP 登録時、「マッピング未検出対応」に「エラーとする」を選択した場合**
> SAMLユーザマッピングを登録する必要があります。
> マッピング情報が見つからなければログインエラー画面に遷移します。
> - **IdP 登録時、「マッピング未検出対応」に「IdPのユーザコードでログインを試みる」を選択した場合**
> マッピング情報が見つからず、IdP のユーザコードに一致するユーザが intra-mart Accel Platform に存在すれば一致したユーザでログインします。
> IdP のユーザコードに一致するユーザが存在しなければログインエラー画面に遷移します。

ログアウト(認証元からもログアウト)

登録したIdP の「シングルログアウト」が「有効」であり、SAML認証で intra-mart Accel Platform にログインした場合
通常の「ログアウト」と「ログアウト(認証元からもログアウト)」の二種類のログアウト方法を選ぶことが可能です。

- **通常のログアウト**
  intra-mart Accel Platform からのみログアウトします。
  一般ユーザログイン画面のSAML 認証でログインするボタンを押下するとIdP でユーザコードを入力することなく intra-mart Accel Platform にログインします。
- **ログアウト(認証元からもログアウト)**
  intra-mart Accel Platform とIdP 両方からログアウトします。
  一般ユーザログイン画面のSAML 認証でログインするボタンを押下すると再びIdP でユーザコードの入力を求められます。

一般ユーザログイン画面を経由せずSAML 認証してログインする方法

注意

この機能を利用するには認可設定画面で認可ポリシーの許可を行う必要があります。デフォルトの設定では許可していません。ポリシーを設定するリソースと対象者は下記の通りです。

認可ポリシーの許可を行うリソース	「SAML認証済みユーザリダイレクトサービス」
ポリシーを設定する対象者	「ゲストユーザ」 「認証済みユーザ」

- 下記URL から intra-mart Accel Platform の一般ユーザログイン画面を経由せずSAML 認証してログインできます。
  <SAML 認証するIdP のプロバイダID> はIdP 一覧画面から確認できます。<SAML 認証後の遷移先パス> にはコンテキストパス以降のURLを指定してください。指定がない場合はホーム画面に遷移します。
  - **IdP を1件のみ登録している場合**
    http://<HOST>:<PORT>/<CONTEXT_PATH>/samlsso/<SAML 認証後の遷移先パス>
  - **IdP を2件以上登録している場合**
    http://<HOST>:<PORT>/<CONTEXT_PATH>/samlsso/<SAML 認証するIdP のプロバイダID>/<SAML 認証後の遷移先パス>

コラム

下記構築例でSAML 認証後に「サイトマップ」→「個人設定」→「パスワード」のパスワード画面へ遷移する場合、URL は次の通りです。

- IdP を1件のみ登録している場合：
  http://localhost:8080/imart/samlsso/user/settings/password
- IdP を2件以上登録している場合：
  http://localhost:8080/imart/samlsso/8eb1m9psf19lxwv/user/settings/password

項目	例
<HOST>	「ローカル環境（localhost）」
<PORT>	「8080」ポート
<CONTEXT_PATH>	「imart」
<SAML 認証するIdP のプロバイダID>	「8eb1m9psf19lxwv」

注意事項

ここでは、SAML 認証設定時の注意事項について解説します。

エンティティID

IdP はエンティティID と呼ばれる識別子でSP(intra-mart Accel Platform) を認識します。
エンティティID は ベースURLと識別子で構成されます。

ベースURLは、IDP新規作成画面で以下の規則に従って初期表示されます。

1. BaseUrlProviderが実装されている場合、その実装クラスが返却するベースURL（返却値が null の場合は次の規則）
2. 設定ファイル(conf/server-context-config.xml)に定義したベースURL
3. ベースURLが定義されていない場合は「http://server:port/path」

識別子の初期表示は空欄ですが、任意のIDを設定できます。ここでは例としてテナントIDを設定しています。

以下はSPメタデータの抜粋です。
ハイライトされた行の entityID 属性に ベースURLと識別子から構成されたエンティティIDを使用します。

```
<?xml version="1.0" encoding="UTF-8"?>
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" entityID="https://example.org/imart/default"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      .....
</md:EntityDescriptor>
```

バインディングURL

バインディングURL はシングルサインオンやシングルログアウトの時に IdP から SP(intra-mart Accel Platform) にリダイレクトされるURLです。
これらのURLに使用されるベースURL は エンティティIDに使用されるベースURLと同じです。

SPメタデータのバインディングURLは IdP 新規登録または更新時に設定されます。

以下はSPメタデータの抜粋です。

ハイライトされた行の Location 属性に ベースURLを使用します。

```
<?xml version="1.0" encoding="UTF-8"?>
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" entityID="https://example.org/imart/default"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
   <md:SPSSODescriptor AuthnRequestsSigned="false" WantAssertionsSigned="false"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
      <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
Location="https://example.org/imart/saml/profile/slo_response/redirect"/>
      <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://example.org/imart/saml/profile/slo_response/post"/>
       .....
      <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://example.org/imart/saml/profile/sso_response/post" index="0"/>
   </md:SPSSODescriptor>
</md:EntityDescriptor>
```

ベースURLの変更について

ベースURLを変更した場合、SPメタデータのエンティティID および バインディングURL の変更が必要です。
変更を反映するためには、以下の作業が必要です。

1. IdPの更新画面からベースURLを変更します（必要に応じて識別子を設定してください）。
   SPメタデータが更新されます。
2. SPメタデータをダウンロードします。
   SPメタデータのエンティティID および バインディングURLに対して、ベースURLが反映されているか確認してください。
3. SPメタデータをIdPへインポートします。

署名

署名アルゴリズム

証明書情報に登録可能な署名アルゴリズムは以下の通りです。

- RSA
- DSA

シングルサインオンの署名処理

登録するIdP メタデータの「IDPSSODescriptor」要素に「WantAuthnRequestsSigned=”true”」の設定がある場合
シングルサインオンのリクエストには署名が必須となるため「署名しない」を選択していても署名処理を行います。

暗号化

AES256の使用

JDK8 を利用している場合に、標準のままでは AES の鍵の長さが 128bit までしか使用できません。
256bit を使用する場合は JCE(Java Cryptography Extension) を差し替える必要があります。

1. 「JCE Unlimited Strength Jurisdiction Policy Files」をダウンロードしてください。
2. zip ファイルを解凍してファイル内の「US_export_policy.jar」と「local_policy.jar」を以下のパスに上書きコピーしてください。
   - <%JAVA_HOME%>/jre/lib/security

コラム

URL（2016年4月現在）

- JDK8：https://www.oracle.com/java/technologies/javase-jce8-downloads.html

IdP から intra-mart Accel Platform へのシングルサインオンを開始する場合

IdP によっては、IdP から intra-mart Accel Platform にシングルサインオンする機能があります。
この機能を利用する場合、同じエンティティID のIdP を複数登録しないでください。IdP を特定できずに正しく動作しません。

IdP からのログアウトリクエストについて

IdP によっては、IdP からSP にログアウトするようにリクエストを送信する機能がありますが intra-mart Accel Platform は対応していません。

IdP 別の設定方法

ここでは、検証済みのIdP 毎に設定方法および注意点について解説します。

OpenAM

OpenAM をIdP としてSAML 認証を行うための設定例を説明します。

項目

バージョン

以下のバージョンを前提として説明します。

- Tomcat Ver 8.x
- OpenAM Ver 12.x.x あるいは 13.x.x

前提条件

- Tomcat にOpenAM のデプロイが完了していること
- OpenAM の初期設定が完了していること

設定方法

OpenAM をIdP に設定

OpenAM に管理者でログインしてホストアイデンティティプロバイダの作成を行います。

アイデンティティープロバイダ新規登録時の設定例

署名鍵	OpenAM のkeystore に登録したエイリアス名
トラストサークル	intra-mart Accel Platform
属性マッピング 表明内の名前	usercd
属性マッピング ローカル属性名	uid

コラム
- 「属性マッピング ローカル属性名」の「uid」とはOpenAM のユーザコードのことです。
- 署名、暗号化に関する設定はホストアイデンティティプロバイダ登録完了後、「連携」タブのエンティティープロバイダ項目のリンク先で設定可能です。

OpenAM のメタデータをダウンロード

OpenAM のメタデータをダウンロードします。以下のURL からメタデータを表示できます。
- http://<ホスト名>:<ポート番号>/<OpenAM コンテキストパス>/saml2/jsp/exportmetadata.jsp

intra-mart Accel Platform にOpenAM を登録

IdP 新規登録画面からOpenAM を以下の設定で新規登録します。
記載のない項目はIdP の設定に応じて変更してください。

IdP 新規登録時の設定例

状態	有効
IdPメタデータ	OpenAM からダウンロードしたメタデータの内容
ユーザコード取得方法	属性名を指定して取得する
属性名	usercd
シングルサインオン	有効

コラム
- 「属性名」にはOpenAM で登録した「属性マッピング 表明内の名前」の値と同じにしてください。

intra-mart Accel Platform のメタデータをダウンロード

IdP新規登録後、IdP 一覧画面からメタデータをダウンロードします。

OpenAM にメタデータをインポート

OpenAM の管理者でログインして intra-mart Accel Platform からダウンロードしたメタデータをインポートします。

- メタデータのインポート
  「連携」タブにあるエンティティープロバイダ項目の「エンティティーのインポート」からインポート可能です。

トラストサークルの設定

OpenAM の管理者でログインして intra-mart Accel Platform をOpenAM と同じトラストサークルに設定してください。

- トラストサークルの設定
  「連携」タブに登録されているトラストサークルのリンク先で設定可能です。

intra-mart Accel Platform ユーザとOpenAM ユーザをマッピング

テナント管理者でログインしてSAMLユーザマッピング(管理)画面から intra-mart Accel Platform のユーザコードとOpenAM のユーザコードをマッピングしてください。

OpenAM のユーザで intra-mart Accel Platform にログイン

上記設定が完了すると intra-mart Accel Platform の一般ユーザログイン画面にOpenAM のログイン画面に遷移するボタンが表示されます。
ボタンを押下してOpenAM のログイン画面でログインすると intra-mart Accel Platform にログインします。

注意事項

使用可能な署名アルゴリズム

2016年8月現在、intra-mart Accel Platform とOpenAM 間のSAML認証で使用可能な署名アルゴリズムを各鍵長、各バインディングごとに表した一覧は以下になります。

OpenAM Ver 12.x.x

		HTTP-REDIRECTバインディング	HTTP-POSTバインディング
SHA1withDSA	**1024bit**	○	○
	2048bit以上	○	×
SHA1withRSA	**1024bit**	○	○
	2048bit以上	○	○
SHA256withRSA	**1024bit**	×	○
	2048bit以上	×	○

OpenAM Ver 13.x.x

		HTTP-REDIRECTバインディング	HTTP-POSTバインディング
SHA1withDSA	**1024bit**	○	○
	2048bit以上	○	×
SHA1withRSA	**1024bit**	○	○
	2048bit以上	○	○
SHA256withRSA	**1024bit**	○	○
	2048bit以上	○	○

intra-mart Accel Platform のメタデータが変更された場合

IdPの設定を更新して intra-mart Accel Platform のメタデータに変更があった場合はOpenAM でメタデータのインポートとトラストサークルの設定を再度実行する必要があります。

Microsoft Entra ID

Microsoft Entra ID をIdP としてSAML 認証を行うための設定例を説明します。

項目

> **コラム**
>
> 「Azure Active Directory (AzureAD)」 の名称は 「Microsoft Entra ID」 に変更されました。
> 詳細については、Microsoft社のドキュメントを参照してください。
> https://learn.microsoft.com/entra/fundamentals/new-name

前提条件

- intra-mart Accel Platform が SSL/TLS に対応していること（httpsでアクセスできること）
- intra-mart Accel Platform に連携対象のユーザが存在すること
- Microsoft Entra ID のディレクトリ作成が完了していること
- 作成したディレクトリにユーザが存在すること

設定方法

Microsoft Entra ID にアプリケーションを追加

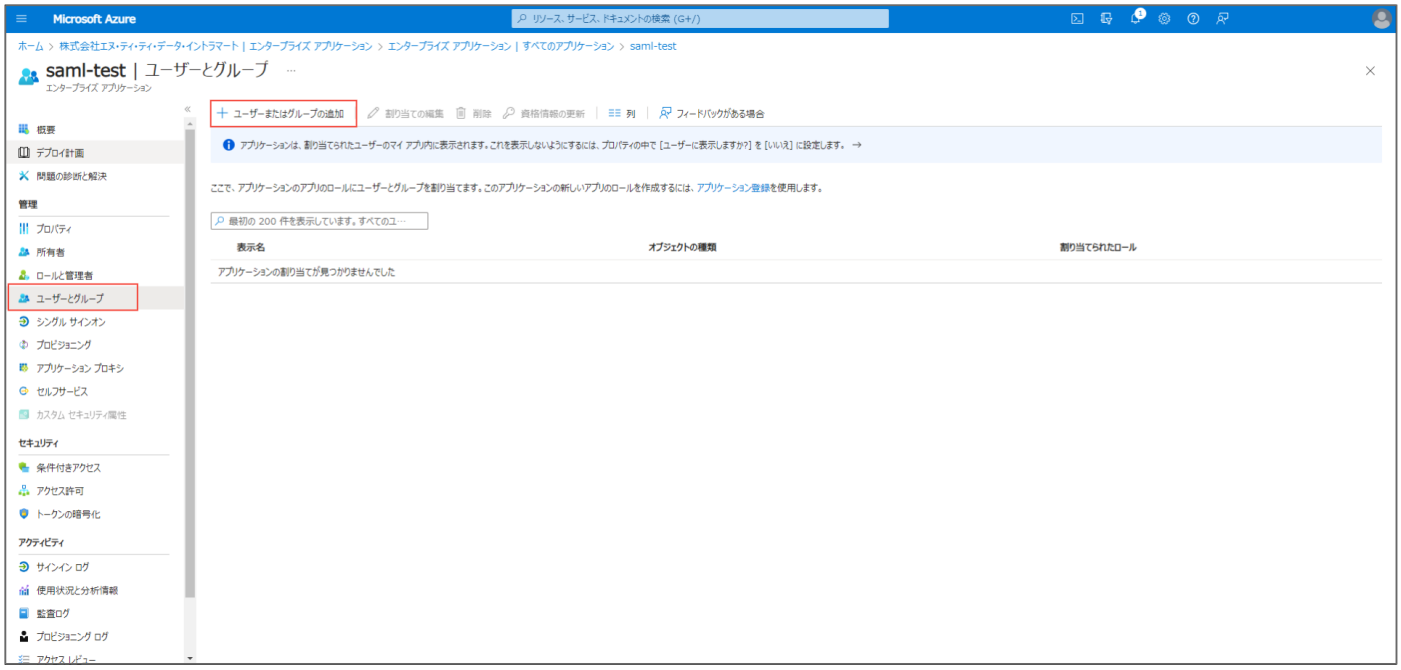
Microsoft Entra ID の管理画面から intra-mart Accel Platform をアプリケーションとして登録します。

「Microsoft Entra ID」→「エンタープライズ アプリケーション」→「新しいアプリケーション」→「独自のアプリケーションの作成」をクリックします。
アプリケーションの名前を入力し、「アプリケーションでどのような操作を行いたいですか？」のラジオボタンは「ギャラリーに見つからないその他のアプリケーションを統合します (ギャラリー以外)」を選択して、作成ボタンをクリックします（本書では saml-test と名前を入力）。

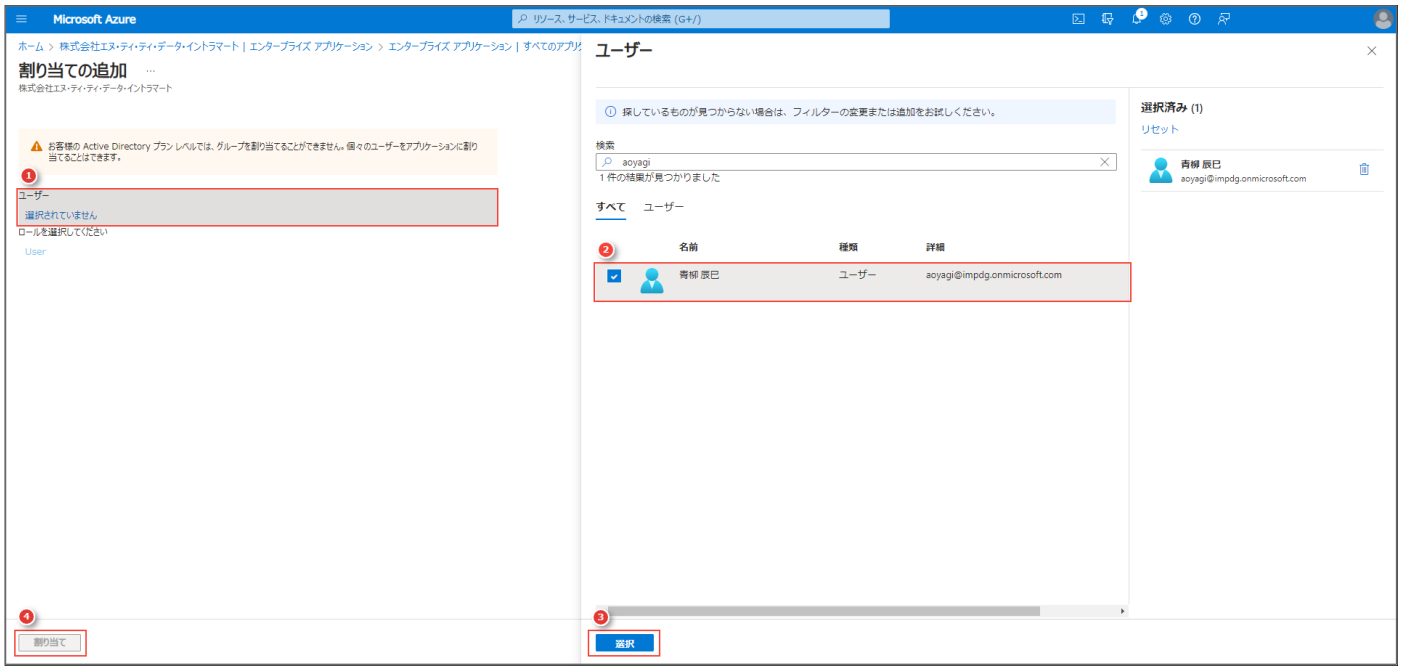
登録したアプリケーションにユーザを割り当て

登録したアプリケーションの管理メニューから、SAML認証を利用するユーザを追加します。

「Microsoft Entra ID」→「エンタープライズ アプリケーション」→ 登録したアプリケーションを選択 → メニューより「ユーザとグループ」をクリックします。
「ユーザまたはグループの追加」ボタンから追加したいユーザを選択します。



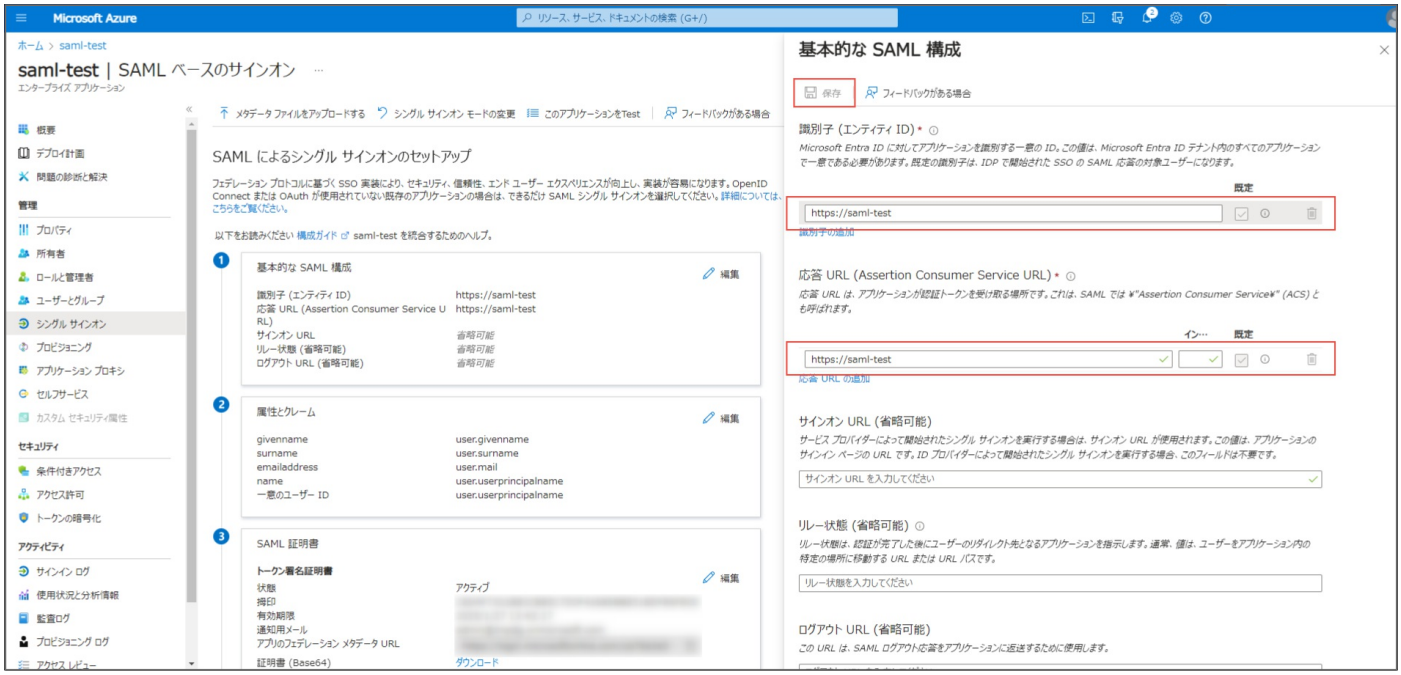
「選択されていません」と表示されている箇所をクリックすると、ユーザの検索フォームが表示されるので、割り当てたいユーザを検索し選択します。
選択したユーザがいる状態で右下の「選択」ボタンをクリックします。
左下の「割り当て」ボタンをクリックします。



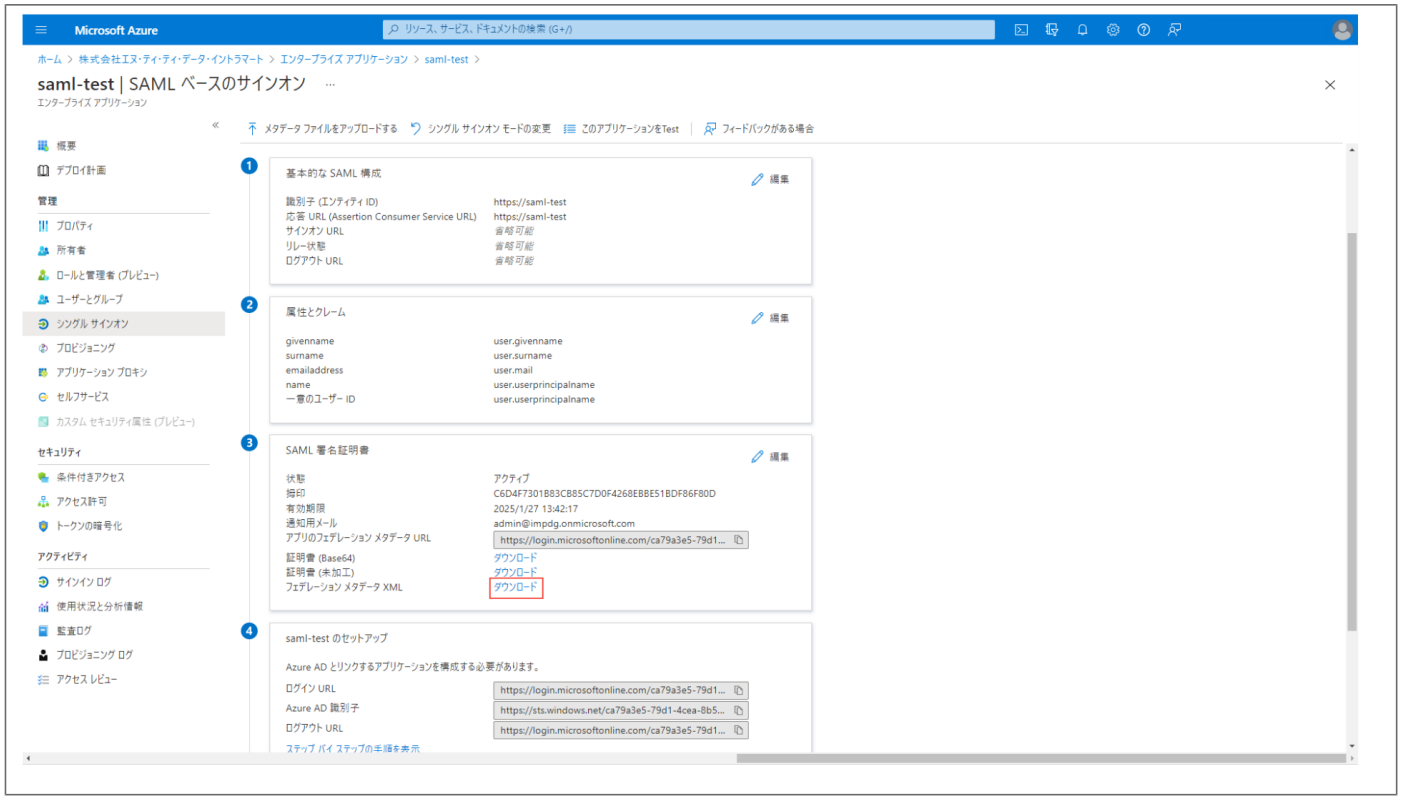
登録したアプリケーションのフェデレーション メタデータをダウンロード

登録したアプリケーションの管理メニューより「シングル サインオン」を選択します。シングル サインオン方式は SAML を選択します。
「基本的な SAML 構成」の編集ボタンをクリックします。入力項目「識別子 (エンティティ ID)」と「応答 URL (Assertion Consumer Service URL)」に仮の値を入力して、保存ボタンをクリックします（本書ではどちらも https://saml-test と入力）。

> **コラム**
>
> 入力項目「識別子 (エンティティ ID)」と「応答 URL (Assertion Consumer Service URL)」の正式な値は、「*Microsoft Entra ID にメタデータをアップロード*」で設定されます。



「SAML 署名証明書」の項目「フェデレーション メタデータ XML」をダウンロードします。



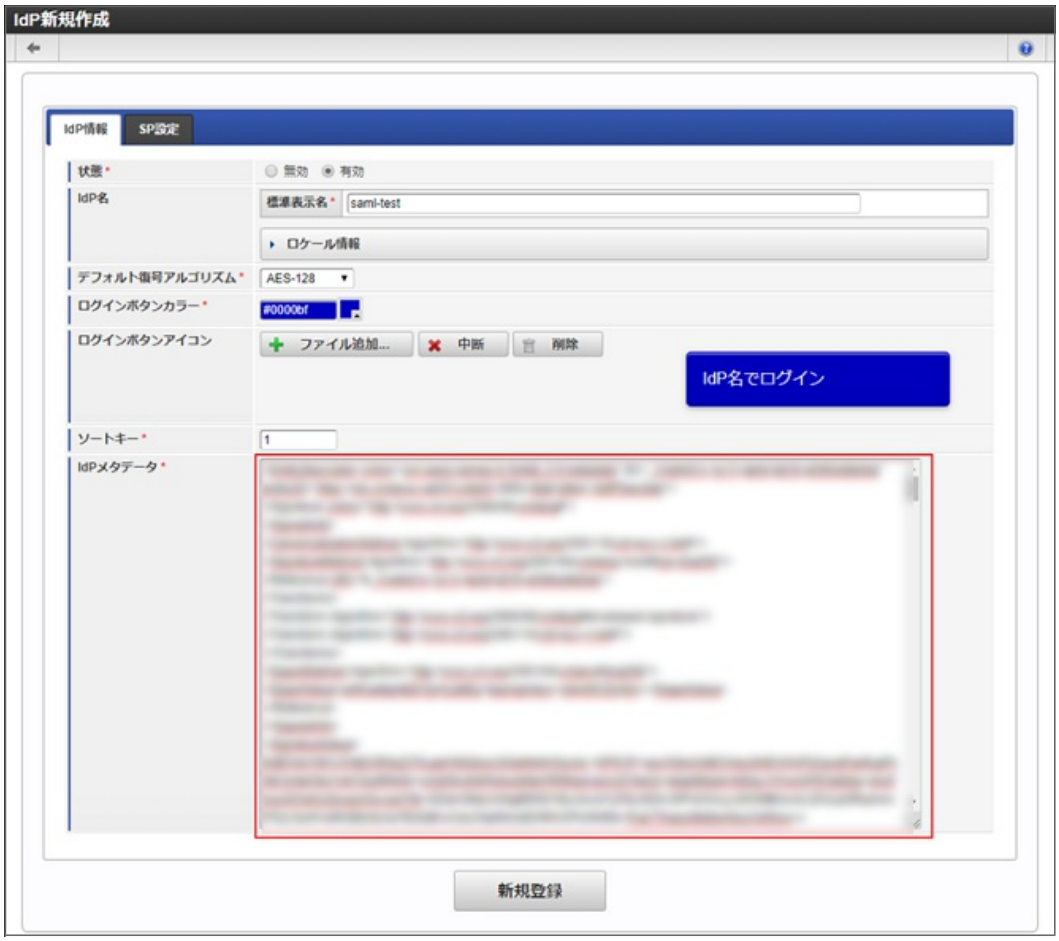
intra-mart Accel Platform に Microsoft Entra ID を登録

intra-mart Accel Platform にてシステム管理者でログインし、「システム管理」→「SAML認証設定」→「IdP一覧」をクリックします。「新規作成」ボタンをクリックし、新規登録画面に遷移します。
「IdPメタデータ」に「*登録したアプリケーションのフェデレーション メタデータをダウンロード*」でダウンロードしたフェデレーション メタデータ XML の内容を貼り付けます。
その他必要な項目を入力し「新規登録」ボタンをクリックします。

IdP 新規登録時の設定例（IdP設定タブ）

状態	有効
IdP名	任意の値
ソートキー	任意の値

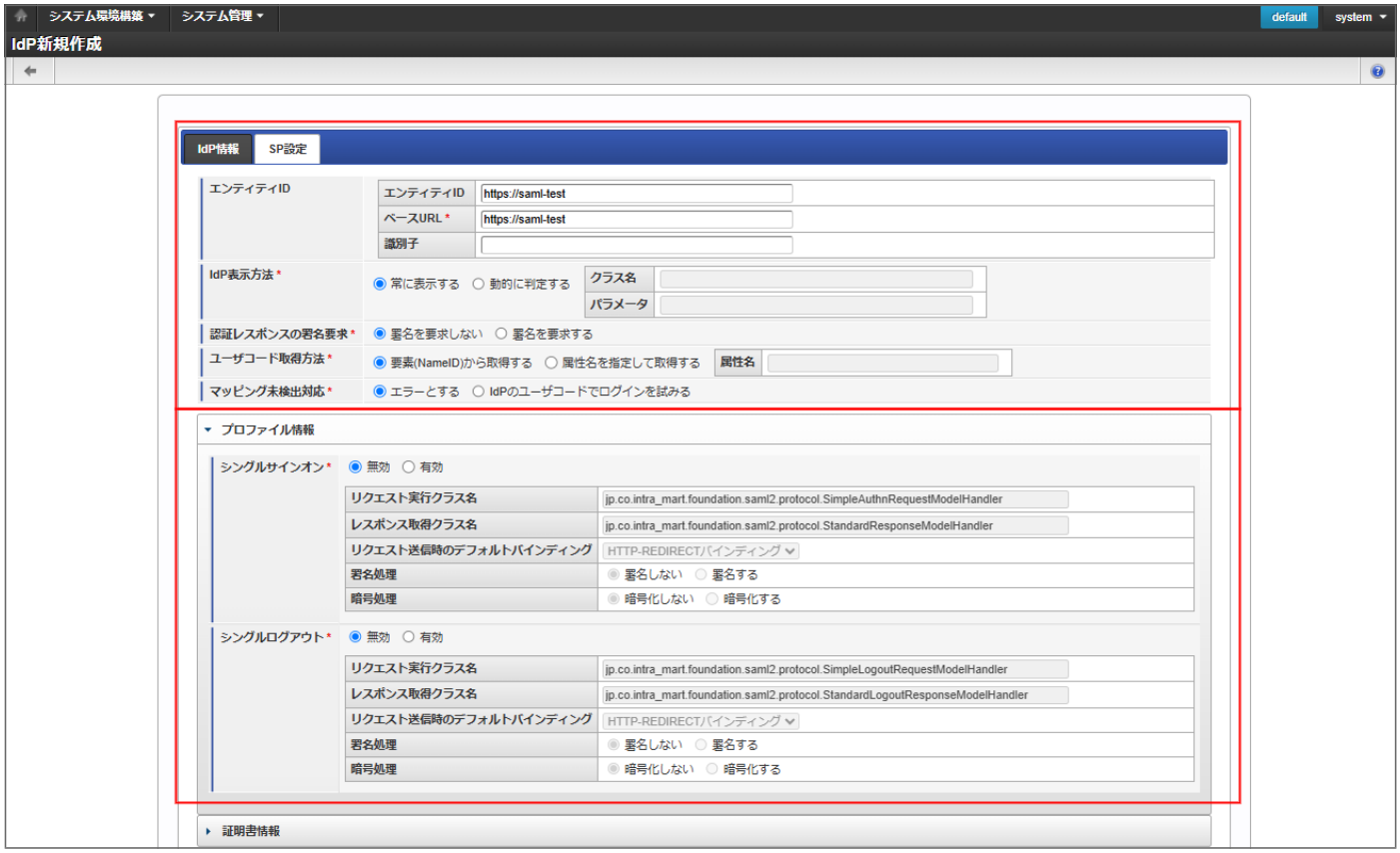
IdPメタデータ	Microsoft Entra ID からダウンロードしたフェデレーション メタデータの内容



IdP 新規登録時の設定例（SP設定タブ）

ユーザコード取得方法	要素(NameID)から取得する ※ SAML認証された Microsoft Entra ID のユーザコードを取得する場合「属性名を指定して取得する」を選択します。属性名は 「 http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name 」 とします。
マッピング未検出対応	エラーとする
シングルサインオン	無効 ※ シングルサインオンを利用する場合は「有効」、暗号処理は「暗号化しない」を選択
シングルログアウト	無効 ※ シングルログアウトを利用する場合は「有効」、暗号処理は「暗号化しない」を選択

ユーザコード取得方法を「要素(NameID)から取得する」に指定し、マッピング未検出対応のラジオボタンを「エラーとする」を設定してください。
SAML認証された Microsoft Entra ID のユーザコードとログインさせたい intra-mart Accel Platform ユーザをマッピングする場合は、「*intra-mart Accel Platform ユーザとMicrosoft Entra ID ユーザをマッピング*」のノートを参照してください。



IdPを新規登録すると、「IdP一覧」画面に登録したIdPが表示されます。
「SPメタデータダウンロード」のアイコンをクリックし、SPメタデータをダウンロードしてください。

コラム

「*intra-mart Accel Platform に Microsoft Entra ID を登録*」の操作方法は、サイトツアー機能を利用して参照できます。

シングルサインオン、シングルログアウトを利用する場合は「SP設定」タブをクリックし、「プロファイル情報」のラジオボタンを「有効」に設定してください。シングルログアウトの詳細は「*シングルログアウトについて*」を参照してください。
「*Microsoft Entra ID の暗号処理について*」に記載の通り、暗号処理は「暗号化しない」を選択してください。

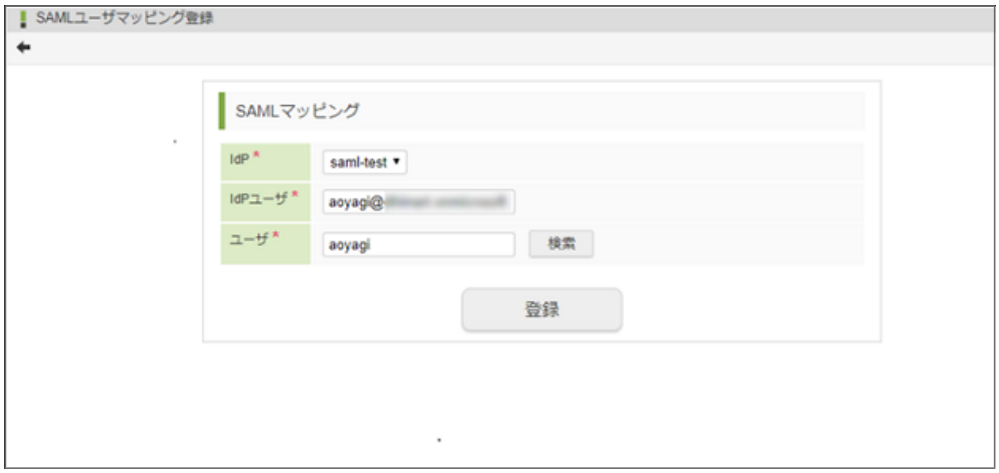
intra-mart Accel Platform ユーザとMicrosoft Entra ID ユーザをマッピング

intra-mart Accel Platform にてテナント管理者でログインし、「サイトマップ」→「SAML認証」→「SAMLユーザマッピング（管

理）」をクリックします。
「新規作成」ボタンをクリックし、以下のように設定し登録します。

新規登録時の設定例

IdPユーザ	Microsoft Entra ID でアプリケーションに割り当てたユーザのアドレス
ユーザ	intra-mart Accel Platform で連携させたいユーザのユーザコード



コラム

SAML認証後のユーザコード取得方法を変更することで、「*intra-mart Accel Platform ユーザとMicrosoft Entra ID ユーザをマッピング*」の手順を省略できます。
以下の方法を利用するには、Microsoft Entra IDアカウントのメールアドレスの@の前がIMのアカウント名と一致することが前提です。

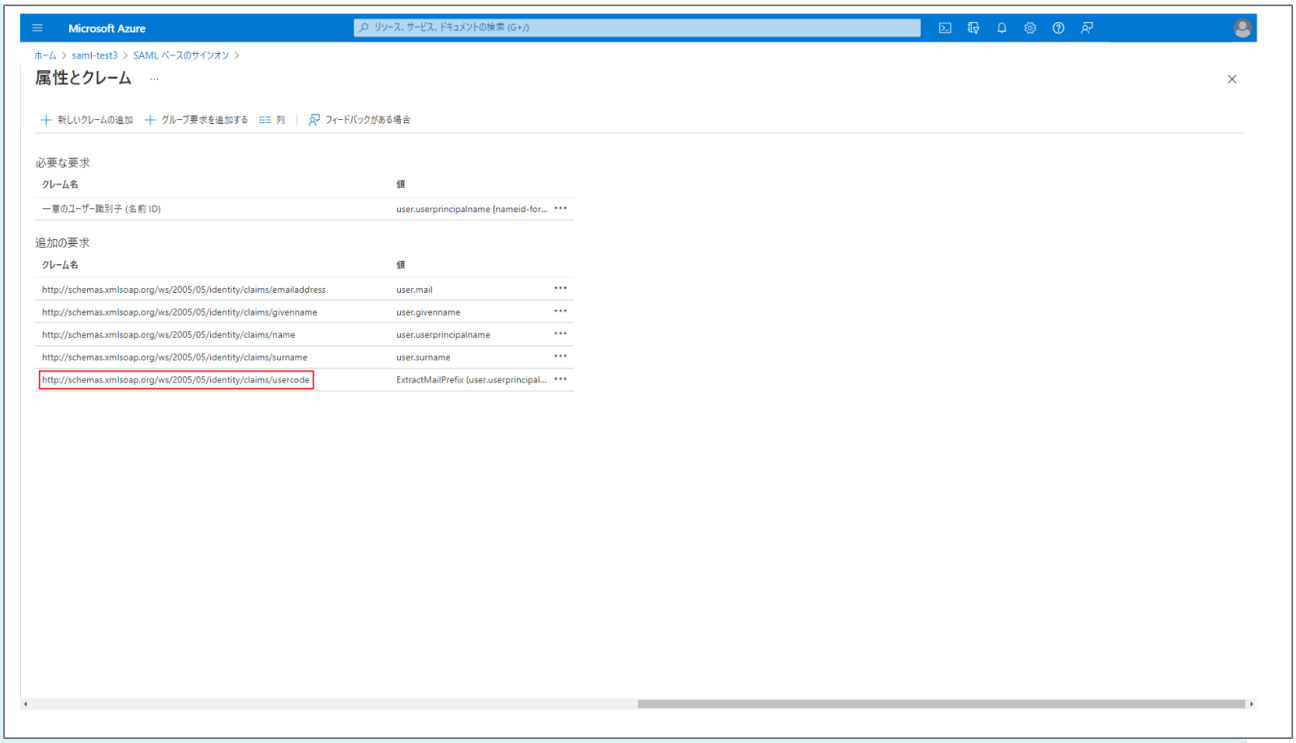
1. Microsoft Entra ID の 「Microsoft Entra ID」→「エンタープライズ アプリケーション」→「シングル サインオン」 で「属性とクレーム」の編集ボタンをクリックします。
2. 「新しいクレームの追加」をクリックします。
3. 「要求の管理」の各入力項目を入力します。

- 名前 ： 任意の値
- 名前空間 ： 任意の値
- ソース ： 変換

4. 「変換の管理」の各入力項目を入力し、「変換を通知する」をクリックします。

- 変換 ： ExtractMailPrefix() - メールアドレスまたはユーザプリンシパル名からドメインサフィックスを除去（aoyagi@domain.com の場合 “aoyagi” を抽出）
- パラメータ1 ：user.userprincipalname - UPNプレフィックスとUPNサフィックスからなるログイン名

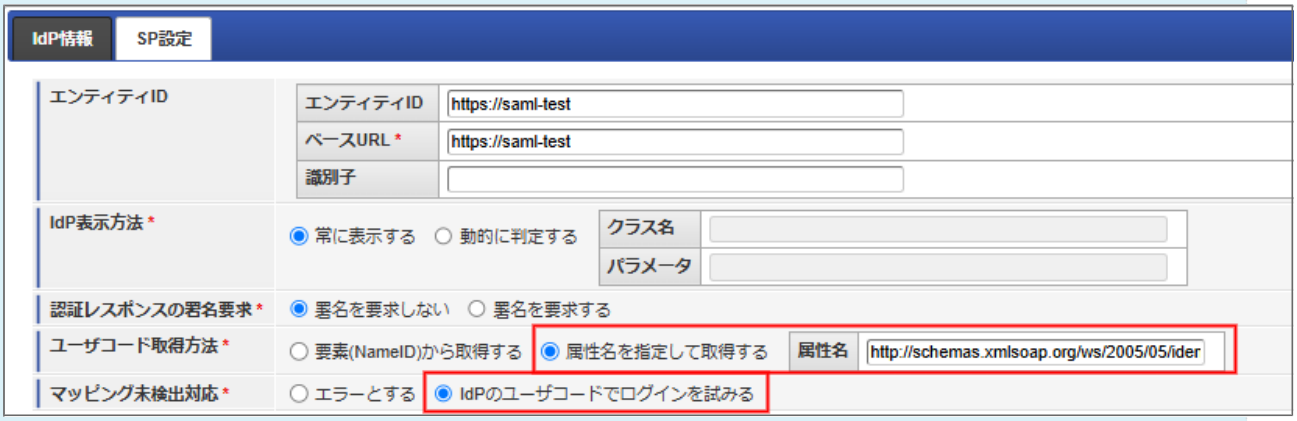
5. 「保存」をクリックします。
6. 「ユーザ属性とクレーム」に追加したクレームのクレーム名（赤枠部分）をコピーします。



7. intra-mart Accel Platform にてシステム管理者でログインし、「システム管理」→「SAML認証設定」→「IdP一覧」をクリックします。

8. 「SP設定」タブの「ユーザコード取得方法」のラジオボタンを「属性名を指定して取得する」に設定の上、属性名に 手順4. でコピーしたクレーム名を入力します。

9. 「SP設定」タブの「マッピング未検証対応」のラジオボタンを「IdPのユーザコードでログインを試みる」に設定します。



10. 更新ボタンをクリックします。

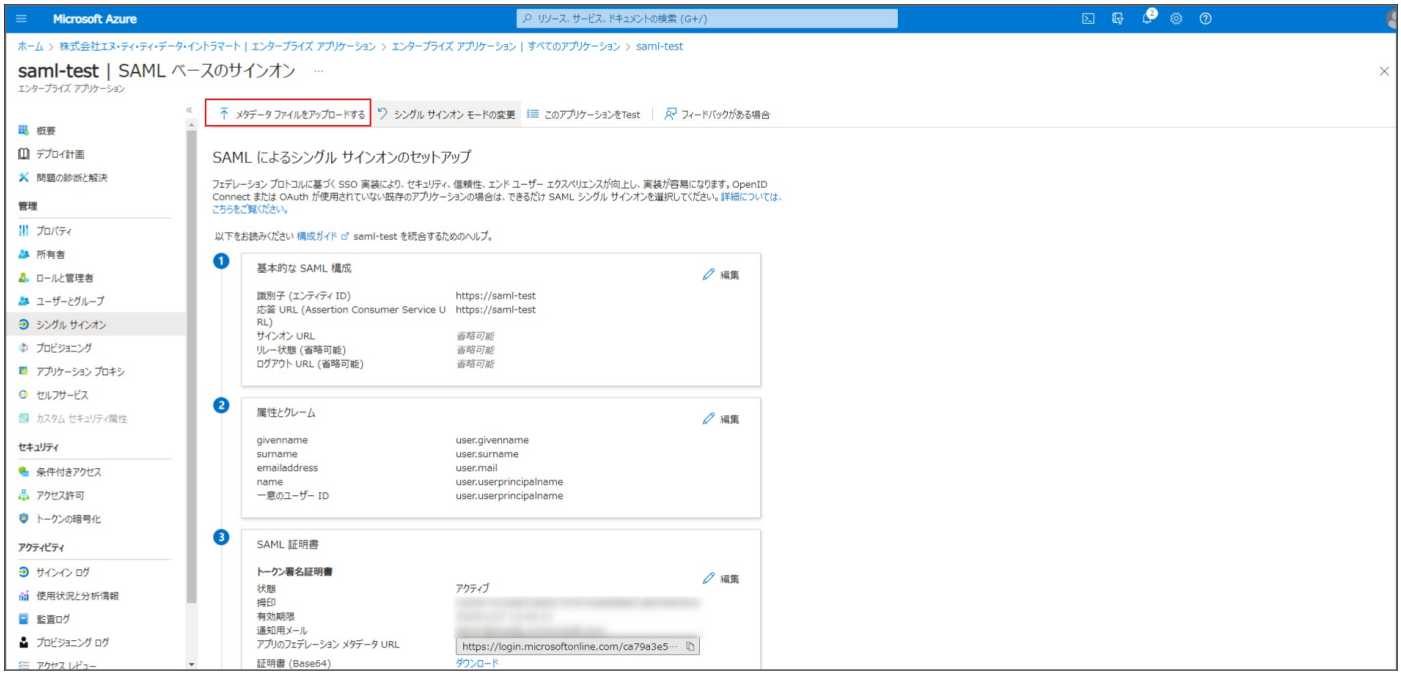
Microsoft Entra ID にメタデータをアップロード

Microsoft Entra ID の管理画面から「Microsoft Entra ID」→「エンタープライズ アプリケーション」 で 「*Microsoft Entra ID にアプリケーションを追加*」 で設定したアプリケーションを検索します。
登録したアプリケーションの管理メニューより「シングル サインオン」を選択します。

「メタデータ ファイルをアップロードする」を選択し、「 *intra-mart Accel Platform に Microsoft Entra ID を登録*」でダウンロードしたメタデータを追加し保存します。

注意

- 一連の設定が完了したら Microsoft Entra ID からサインアウトしてください。認証時にエラーが発生するためです。



Microsoft Entra ID のユーザで intra-mart Accel Platform にログイン

上記設定が完了すると、 intra-mart Accel Platform の「一般ユーザログイン」画面に SAML 認証を行うボタンが表示されます。
ボタンをクリックすると、Microsoft Entra ID の認証画面に遷移します。アプリケーションに割り当てを行ったユーザの認証情報を入力します。
認証に成功すると intra-mart Accel Platform にログインできます。

注意事項

Microsoft Entra ID に送信するリクエストの署名について

2016年8月現在、 intra-mart Accel Platform からMicrosoft Entra ID に送信するリクエストに署名してもエラーが発生することはありませんが、署名チェックは行われずに無視されます。

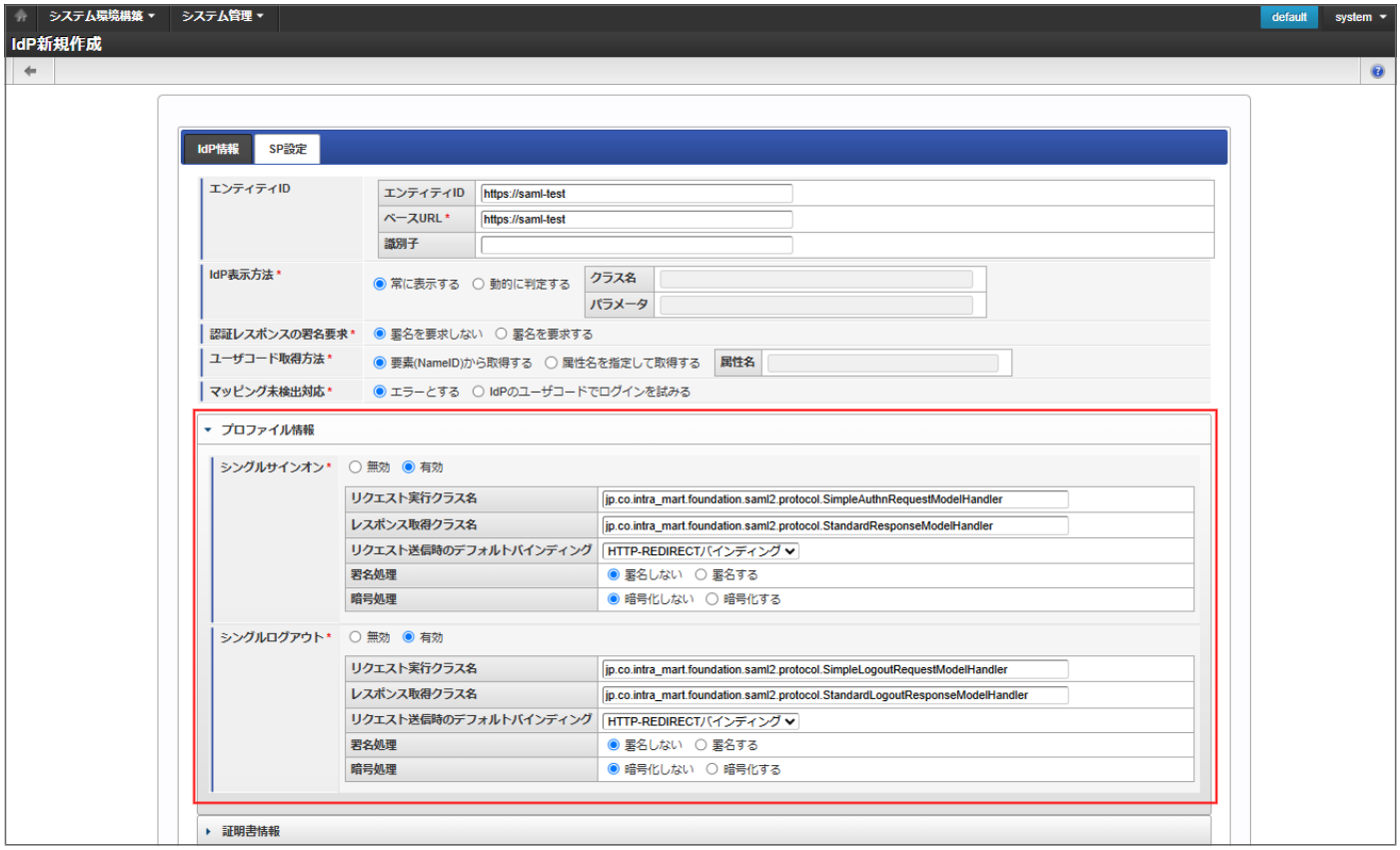
Microsoft Entra ID の暗号処理について

2016年8月現在、intra-mart Accel Platform とMicrosoft Entra ID 間のSAML認証は暗号化に対応していません。IdP新規作成またはIdP更新時にプロファイル情報の暗号処理は「暗号化しない」を選択してください。

シングルログアウトについて

シングルログアウトを有効にするには以下の手順を行います。

1. intra-mart Accel Platform の 「SAML認証設定」 内の画面 「IdP一覧」 のSP設定タブにて、「プロファイル情報」のラジオボタンを「有効」に設定します。



2. 作成したSPメタデータをダウンロードします。

3. Microsoft Entra IDにアクセスし、「Microsoft Entra ID」→「エンタープライズ アプリケーション」→ 登録したアプリケーションを選択 → メニューより「シングルサインオン」をクリックします。

4. 「基本的な SAML 構成」の編集ボタンをクリックします。

5. 入力項目「ログアウト URL」に、ダウンロードしたSPメタデータ内の「Binding=”urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect”」属性をもつ「SingleLogoutService」要素の「Location」属性のURL を設定してください。

6. 「保存」をクリックします。

Active Directory Federation Services

Active Directory Federation Services をIdP としてSAML 認証を行うための設定例を説明します。

バージョン

以下のバージョンを前提として説明します。

- Windows Server 2012 R2

前提条件

- Active Directory Federation Services の初期設定まで完了していること

設定方法

Active Directory Federation Services のメタデータをダウンロード

Active Directory Federation Services のメタデータをダウンロードします。以下のURL からメタデータを表示できます。

- https://<server name>/federationmetadata/2007-06/federationmetadata.xml

intra-mart Accel Platform にActive Directory Federation Services を登録

IdP 新規登録画面からActive Directory Federation Services を以下の設定で新規登録します。
記載のない項目はIdP の設定に応じて変更してください。

IdP 新規登録時の設定例

状態	有効
IdPメタデータ	Active Directory Federation Services からダウンロードしたメタデータの内容
ユーザコード取得方法	要素(NameID)から取得する
シングルサインオン	有効

注意

- Active Directory Federation Services に登録する intra-mart Accel Platform のURL はSSL(https)である必要があります。
  IdP 登録時はシステム管理者にSSL(https)でログインして登録処理を行ってください。

intra-mart Accel Platform のメタデータをダウンロード

IdP新規登録後、IdP 一覧画面からメタデータをダウンロードします。

Active Directory Federation Services にメタデータをインポート

AD FS の「信頼関係」→「証明書利用者信頼」→「証明書利用者信頼の追加」から intra-mart Accel Platform のメタデータをインポートしてください。

要求規則の編集

メタデータインポート後、規則の追加を行います。

要求規則の設定例

要求規則テンプレート	LDAP 属性を要求として送信
属性ストア	Active Directory
LDAP属性	User-Principal-Name
出力方向の要求の種類	名前ID

注意

- 「出力方向の要求の種類」が「名前ID」となる規則を必ず含めてください。
  レスポンスの要素が不足して認証エラーとなります。

コラム

- 「User-Principal-Name」は「ユーザ名@ドメイン名」となります。

intra-mart Accel Platform ユーザとActive Directory Federation Services ユーザをマッピング

テナント管理者でログインしてSAMLユーザマッピング(管理)画面から intra-mart Accel Platform のユーザコードとActive Directory Federation Services のユーザ名をマッピングしてください。

Active Directory Federation Services のユーザで intra-mart Accel Platform にログイン

上記設定が完了すると intra-mart Accel Platform の一般ユーザログイン画面にActive Directory Federation Services のログイン画面に遷移するボタンが表示されます。
ボタンを押下してActive Directory Federation Services のログイン画面でログインすると intra-mart Accel Platform にログインします。

注意事項

使用可能な署名アルゴリズム

2016年8月現在、intra-mart Accel Platform とActive Directory Federation Services 間のSAML認証で使用可能な署名アルゴリズムを各鍵長、各バインディングごとに表した一覧は以下になります。

Active Directory Federation Services

		HTTP-REDIRECTバインディング	**HTTP-POSTバインディング**
SHA1withDSA	**1024bit**	×	×
	2048bit以上	×	×
SHA1withRSA	**1024bit**	○	○
	2048bit以上	○	○

		HTTP-REDIRECTバインディング	HTTP-POSTバインディング
SHA256withRSA	1024bit	○	○
	2048bit以上	○	○

intra-mart Accel Platform のメタデータが変更された場合

IdPの設定を更新して intra-mart Accel Platform のメタデータに変更があった場合はActive Directory Federation Services でメタデータのインポートと要求規則の編集を再度実行する必要があります。

シングルログアウトについて

Active Directory Federation Services のシングルログアウトは署名が必須となります。
IdP登録時に署名処理に「署名する」を選択して証明書を登録してください。

salesforce.com

salesforce.com をIdP としてSAML 認証を行うための設定例を説明します。

前提条件

- salesforce.com のドメイン登録が完了していること
- salesforce.com をIdP として有効化していること

設定方法

salesforce.com のメタデータをダウンロード

salesforce.com のメタデータをダウンロードします。
「管理」→「セキュリティのコントロール」→「ID プロバイダ」からダウンロード可能です。

intra-mart Accel Platform にsalesforce.com を登録

IdP 新規登録画面からsalesforce.com を以下の設定で新規登録します。
記載のない項目はIdP の設定に応じて変更してください。

IdP 新規登録時の設定例

状態	有効
IdPメタデータ	salesforce.com からダウンロードしたメタデータの内容
ユーザコード取得方法	属性名を指定して取得する
属性名	usercd
シングルサインオン	有効
シングルログアウト	無効

intra-mart Accel Platform のメタデータをダウンロード

IdP新規登録後、IdP 一覧画面からメタデータをダウンロードします。

接続アプリケーションの新規作成

salesforce.com の接続アプリケーションに intra-mart Accel Platform を登録します。
「ビルド」→「作成」→「アプリケーション」から登録可能です。

「Web アプリケーション設定」項目の設定例

SAML の有効化	チェック
エンティティ ID	intra-mart Accel Platform のメタデータにある「EntityDescriptor」要素の「entityID」属性の値
ACS URL	intra-mart Accel Platform のメタデータにある「AssertionConsumerService」要素の「Location」属性の値
件名種別	ユーザ名
名前 ID 形式	urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
発行者	初期入力されている値
要求署名を確認	IdP 登録時に署名するように設定した場合はチェックを入れます。 IdP 登録時と同じ証明書をアップロードします。
SAML レスポンスを暗号化	IdP 登録時に暗号化するように設定した場合はチェックを入れます。 IdP 登録時と同じ証明書をアップロードします。
暗号化アルゴリズムをブロック	IdP 登録時に設定した「デフォルト復号アルゴリズム」と同じアルゴリズムを設定します。

接続アプリケーションのカスタム属性設定

登録後、接続アプリケーションの詳細画面からカスタム属性を設定します。

カスタム属性の設定例

属性キー	usercd
属性値	$User.Username

コラム

- 「属性キー」にはIdP 新規登録時の「属性名」の値と同じにしてください。
- 「属性値」の「$User.Username」とはsalesforce.com のユーザ名(メールアドレス形式)のことです。

接続アプリケーションのプロファイル設定

登録後、接続アプリケーションの詳細画面からプロファイルを設定します。
アプリケーションへのアクセス権を持つユーザを選択してください。

intra-mart Accel Platform ユーザとsalesforce.com ユーザをマッピング

テナント管理者でログインしてSAMLユーザマッピング(管理)画面から intra-mart Accel Platform のユーザコードとsalesforce.com のユーザ名をマッピングしてください。

salesforce.com のユーザで intra-mart Accel Platform にログイン

上記設定が完了すると intra-mart Accel Platform の一般ユーザログイン画面にsalesforce.com のログイン画面に遷移するボタンが表示されます。
ボタンを押下してsalesforce.com のログイン画面でログインすると intra-mart Accel Platform にログインします。

注意事項

使用可能な署名アルゴリズム

2016年8月現在、intra-mart Accel Platform とsalesforce.com 間のSAML認証で使用可能な署名アルゴリズムを各鍵長、各バインディングごとに表した一覧は以下になります。

		salesforce.com	
		HTTP-REDIRECTバインディング	**HTTP-POSTバインディング**
SHA1withDSA	**1024bit**	○	○
	2048bit以上	○	×
SHA1withRSA	**1024bit**	○	○
	2048bit以上	○	○
SHA256withRSA	**1024bit**	○	○
	2048bit以上	○	○

intra-mart Accel Platform のメタデータが変更された場合

IdPの設定を更新して intra-mart Accel Platform のメタデータに変更があった場合は接続アプリケーションの設定を更新してください。

シングルログアウトについて

salesforce.com はシングルログアウトに対応していません。
IdP登録時にシングルログアウトを有効にしないでください。

PingFederate

PingFederate をIdP としてSAML 認証を行うための設定例を説明します。

バージョン

以下のバージョンを前提として説明します。

- PingFederate Ver 8.x.x

前提条件

- PingFederate の初期設定が完了していること
- PingFederate が使用する証明書を登録していること
  以下の説明では署名アルゴリズムが「RSA SHA256」の証明書を前提として説明します。
- PingFederate のアダプタを登録していること
  以下の説明ではLDAP(Active Directory) 連携するアダプタを前提として説明します。

設定方法

PingFederate のメタデータ（テンプレート）をダウンロード

- PingFederate の管理者でログインしてPingFederate のメタデータをダウンロードします。
  「Server Configuration」→「Metadata Export」からダウンロード可能です。

> **注意**
> - この時点でダウンロードしたメタデータは intra-mart Accel Platform で対応できない情報を含んだテンプレートです。
>   IdP 新規作成およびPingFederate に intra-mart Accel Platform 登録完了後、メタデータを再ダウンロードしてIdP 情報を更新します。

intra-mart Accel Platform にPingFederate を登録

IdP 新規登録画面からPingFederate を以下の設定で新規登録します。
記載のない項目はIdP の設定に応じて変更してください。

IdP 新規登録時の設定例

状態	有効
IdPメタデータ	PingFederate からダウンロードしたメタデータの内容

ユーザコード取得方法	要素(NameID)から取得する
シングルサインオン	有効
証明書設定	署名と暗号化で同じ証明書を使用する
証明書	証明書情報の内容
秘密鍵のパスフレーズ	秘密鍵のパスフレーズ
秘密鍵	秘密鍵情報の内容

コラム

- PingFederate に intra-mart Accel Platform を登録する場合、署名処理の設定に関わらず証明書情報を求められます。
  署名しない場合も証明書情報を登録してください。

intra-mart Accel Platform のメタデータをダウンロード

IdP新規登録後、IdP 一覧画面からメタデータをダウンロードします。

PingFederate に intra-mart Accel Platform を登録

PingFederate の管理者でログインして intra-mart Accel Platform を登録します。
「IdP Configuration」→「SP CONNECTIONS」→「Create New」から登録可能です。

SP Connection の設定例

Connection Type	BROWSER SSO PROFILES
Connection Options	BROWSER SSO
Import Metadata	ダウンロードした intra-mart Accel Platform のメタデータをインポート
General Info	初期入力されている値

Browser SSO の設定例

SAML Profiles	SP-INITIATED SSO, SP-INITIATED SLO, IDP-INITIATED SSO
Assertion Lifetime	初期入力されている値

Assertion Creation の設定例

Identity Mapping	STANDARD
Attribute Contract	初期入力されている値
Authentication Source Mapping	事前に登録したアダプター

IdP Adapter Mapping の設定例

ADAPTER INSTANCE	事前に登録したアダプター
Mapping Method	USE ONLY THE ADAPTER CONTRACT VALUES IN THE SAML ASSERTION
Attribute Contract Fulfillment	**Attribute Contract** : SAML_SUBJECT **Source** : Adapter **Value** : username
Issuance Criteria	設定なし

Protocol Settings の設定例

Assertion Consumer Service URL	初期入力されている値
SLO Service URLs	初期入力されている値
Allowable SAML Bindings	POST, REDIRECT
Signature Policy	初期入力されている値
Encryption Policy	初期入力されている値

Credentials の設定例

Digital Signature Settings	**SIGNING CERTIFICATE**：事前に登録した証明書 **SIGNING ALGORITHM**：RSA SHA256
Signature Verification Settings	設定なし

Activation & Summary の設定例

Connection Status	ACTIVE

PingFederate のメタデータをダウンロード

- PingFederate のメタデータをダウンロードします。
  「IdP Configuration」→「SP CONNECTIONS」→「Export Metadata」からダウンロード可能です。

intra-mart Accel Platform のPingFederate を更新

改めてダウンロードしたメタデータの内容を「IdPメタデータ」に貼り付けて更新します。

intra-mart Accel Platform ユーザとPingFederate ユーザをマッピング

テナント管理者でログインしてSAMLユーザマッピング(管理)画面から intra-mart Accel Platform のユーザコードとPingFederate のユーザ名をマッピングしてください。

コラム
- LDAP(Active Directory)連携アダプタを使用する場合
  PingFederate のログイン画面でユーザ名を「Administrator」と入力したとするとレスポンスにも「Administrator」が返却されます。

PingFederate のユーザで intra-mart Accel Platform にログイン

上記設定が完了すると intra-mart Accel Platform の一般ユーザログイン画面にPingFederate のログイン画面に遷移するボタンが表示されます。
ボタンを押下してPingFederate のログイン画面でログインすると intra-mart Accel Platform にログインします。

注意事項

intra-mart Accel Platform のメタデータが変更された場合

IdPの設定を更新して intra-mart Accel Platform のメタデータに変更があった場合はPingFederate に再登録する必要があります。

SAML Profiles について

intra-mart Accel Platform のSAML 認証は「IDP-INITIATED SLO」に対応していません。
「SAML Profiles」設定時にはチェックをはずしてください。

Protocol Settings のAllowable SAML Bindings について

intra-mart Accel Platform のSAML 認証は「ARTIFACT」、「SOAP」バインディングに対応していません。
「Allowable SAML Bindings」設定時にはチェックをはずしてください。

署名アルゴリズムについて

- intra-mart Accel Platform のSAML 認証は署名アルゴリズム「EC」に対応していません。
  署名アルゴリズム「RSA」を選択してください。
- intra-mart Accel Platform のSAML 認証は署名アルゴリズム「RSA」のうち「RSA SHA384」、「RSA SHA512」に対応していません。
  「RSA SHA1」または「RSA SHA256」を選択してください。

Okta

Okta を IdP として SAML 認証を行うための設定例を説明します。

項目

前提条件

- intra-mart Accel Platform に HTTPS でアクセスできること
- intra-mart Accel Platform に連携対象のユーザが存在すること
- Okta に連携対象のユーザが存在すること
- シングルログアウトを利用する場合は、事前に秘密鍵と証明書のペアを用意していること

> **注意**
>
> このドキュメントでは、Okta に Developer アカウントでログインした場合の操作方法を記載しています。
> 操作方法は、ログインするアカウントの契約によって、異なる場合があります。

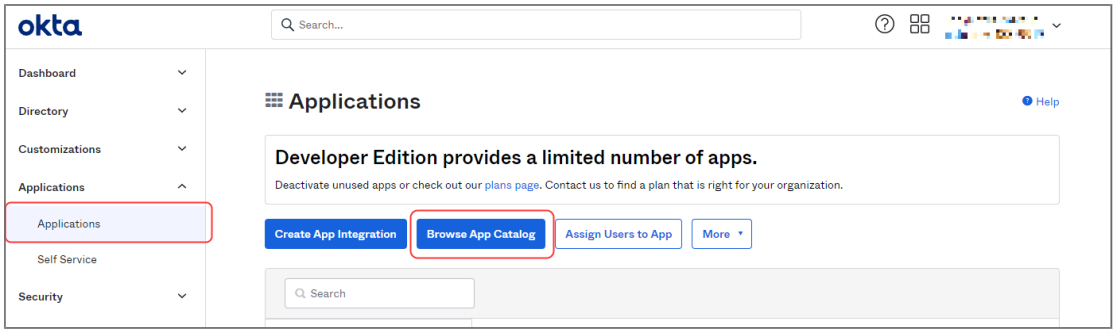
シングルサインオンの設定方法

シングルサインオンを設定します。

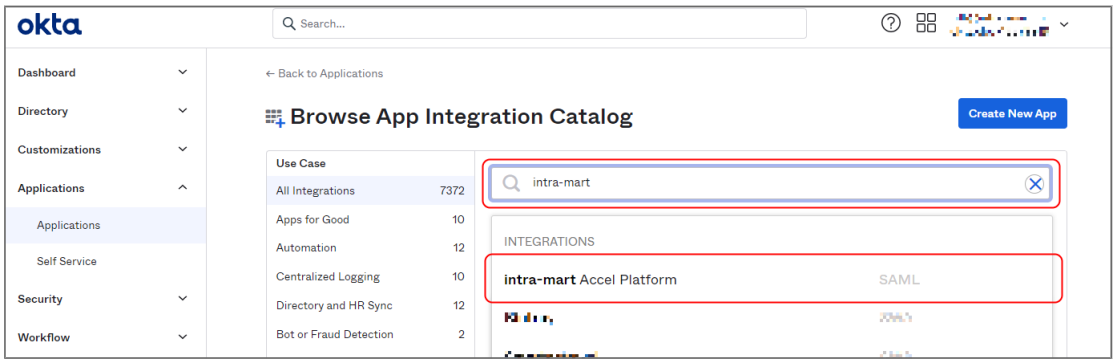
Okta にアプリケーションを追加

Okta の管理画面から intra-mart Accel Platform をアプリケーションとして登録します。

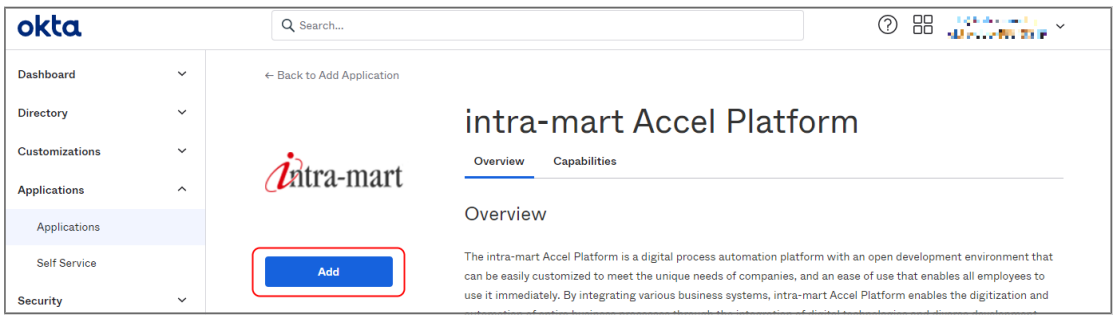
1. 左側のメニューから「Applications」→「Applications」→「Browse App Catalog」をクリックします。



2. 検索テキストボックスに「intra-mart」と入力し、「intra-mart Accel Platform」を選択します。



3. 「Add」をクリックします。

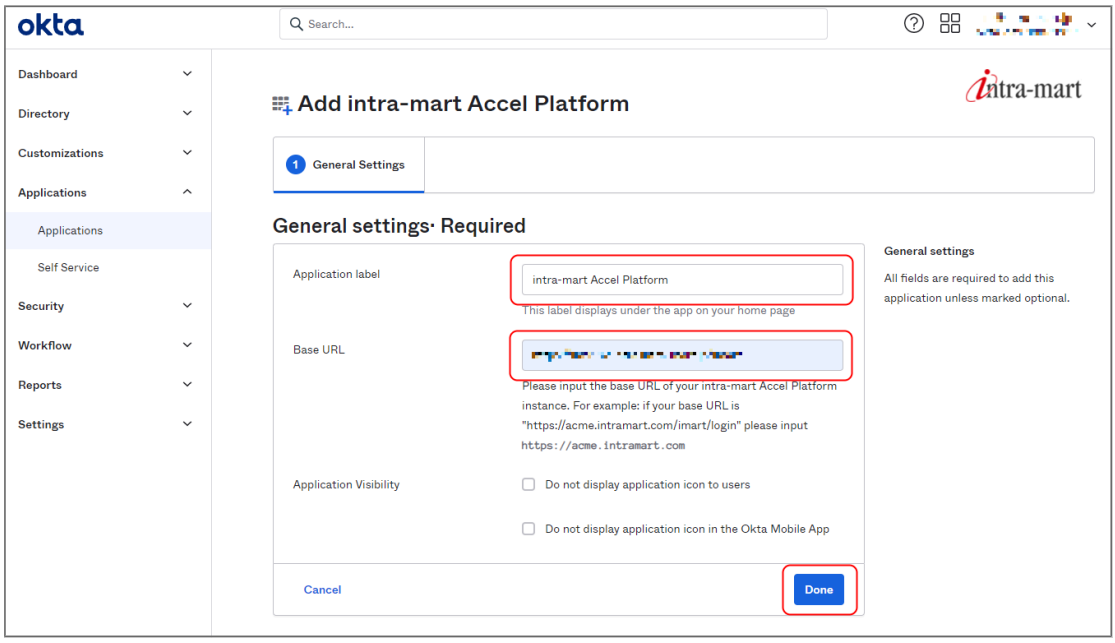


4. 「Application label」に任意のアプリケーションの名前を入力し、「Base URL」に intra-mart Accel Platform のベース URL を入力し、「Done」をクリックします。

アプリケーションの設定例

Application label	任意のアプリケーション名

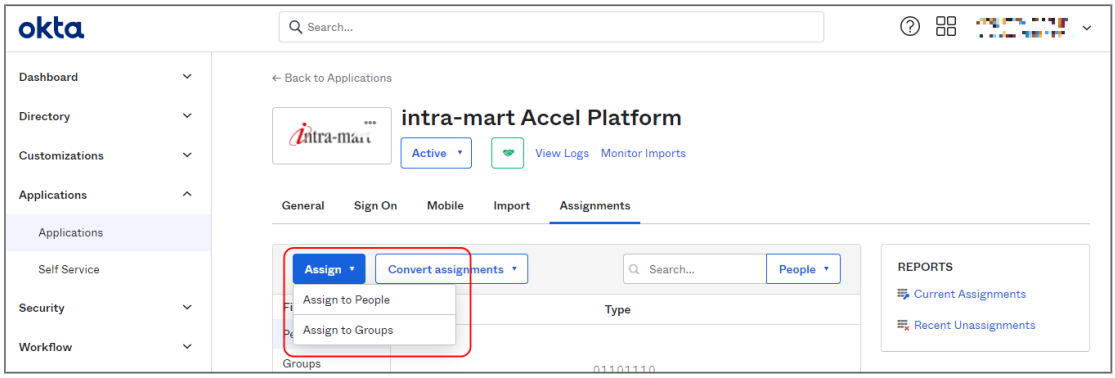
Base URL	intra-mart Accel Platform のベース URL



アプリケーションを利用するユーザまたはグループを割り当て

アプリケーションを利用するユーザまたはグループを割り当てます。

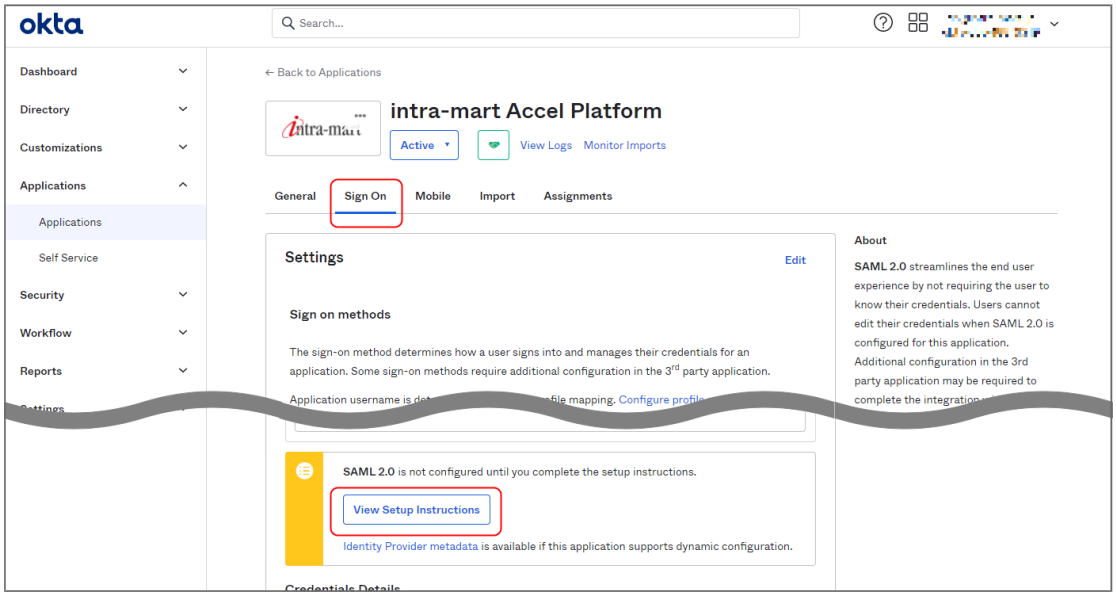
1. 「Assignments」タブで「Assign」をクリックし、「Assign to People」または「Assign to Group」から追加したアプリケーションを利用するユーザまたはグループを割り当てます。



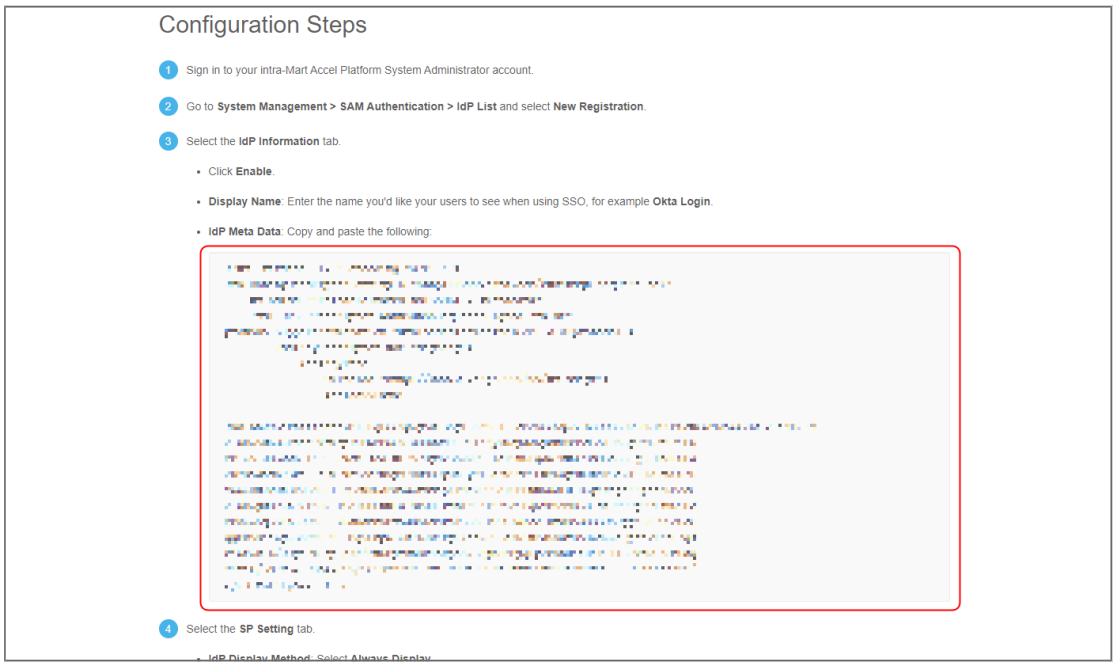
IdP メタデータを取得

IdP メタデータを取得します。

1. 「Sign On」タブをクリックし、「View Setup Instructions」をクリックします。



2. 表示された「IdP Metadata」をコピーします。



intra-mart Accel Platform に Okta で追加したアプリケーションを登録

intra-mart Accel Platform に登録します。

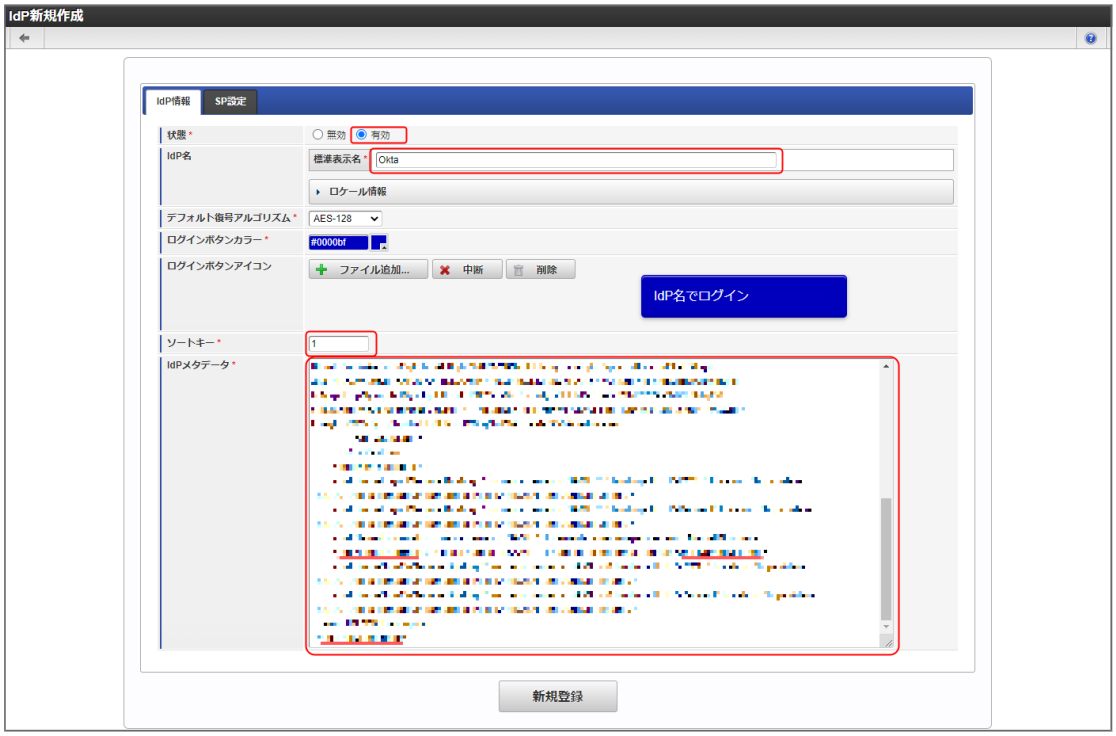
1. intra-mart Accel Platform にてシステム管理者でログインし、「システム管理」→「SAML認証設定」→「IdP一覧」をクリックします。
2. 「新規作成」ボタンをクリックし、新規登録画面に遷移します。
3. 「IdPメタデータ」に「*IdP メタデータを取得*」でコピーしたメタデータを貼り付け、その他必要な項目を入力し「新規登録」ボタンをクリックします。

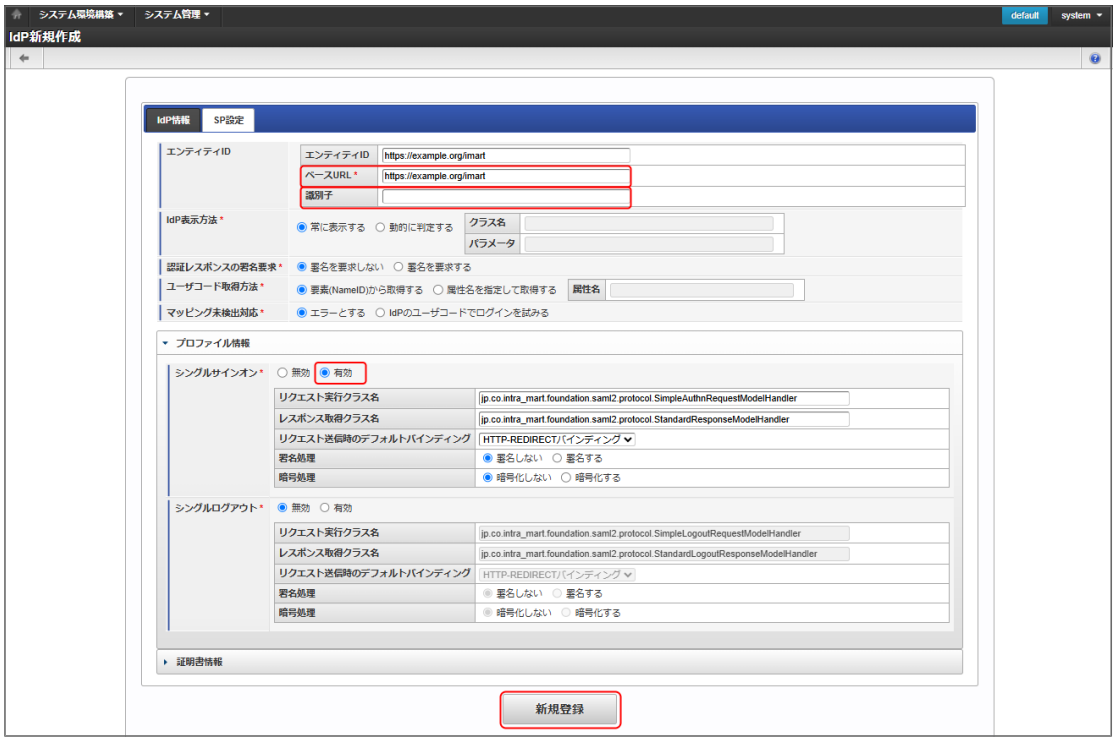
IdP 新規登録時の設定例（IdP設定タブ）

状態	有効
IdP名	任意の値
ソートキー	任意の値
IdPメタデータ	Okta からコピーしたメタデータ

IdP 新規登録時の設定例（SP設定タブ）

ベースURL	Oktaに登録した intra-mart Accel Platform のベースURL
識別子	なし
シングルサインオン	有効





注意

エンティティIDで設定するベースURLは、Oktaに登録したアプリケーションの「Base URL」と同じにする必要があります。
またOktaではSPのエンティティIDは上記の「Base URL」が設定されます。そのためSP設定タブでエンティティIDを設定する際は、識別子を入力しないでください。

intra-mart Accel Platform ユーザと Okta ユーザをマッピング

intra-mart Accel Platform ユーザと Okta ユーザをマッピングします。

1. intra-mart Accel Platform にてテナント管理者でログインし、「サイトマップ」→「SAML認証」→「SAMLユーザマッピング（管理）」をクリックします。
2. 「新規作成」ボタンをクリックし、以下のように設定し登録します。

新規登録時の設定例

IdPユーザ	Okta でアプリケーションに割り当てたユーザのアドレス
ユーザ	intra-mart Accel Platform で連携させたいユーザのユーザコード

intra-mart Accel Platform にログイン

Okta のユーザで intra-mart Accel Platform にログインします。
「*シングルサインオンの設定方法*」に記載された設定が完了すると、intra-mart Accel Platform の「一般ユーザログイン」画面に SAML 認証を行うボタンが表示されます。

1. ログイン画面を表示して、SAML 認証を行うボタンをクリックし、Okta の認証画面に遷移します。

2. アプリケーションに割り当てを行ったユーザの認証情報を入力し、認証を行います。
3. 認証に成功すると intra-mart Accel Platform にログインできます。

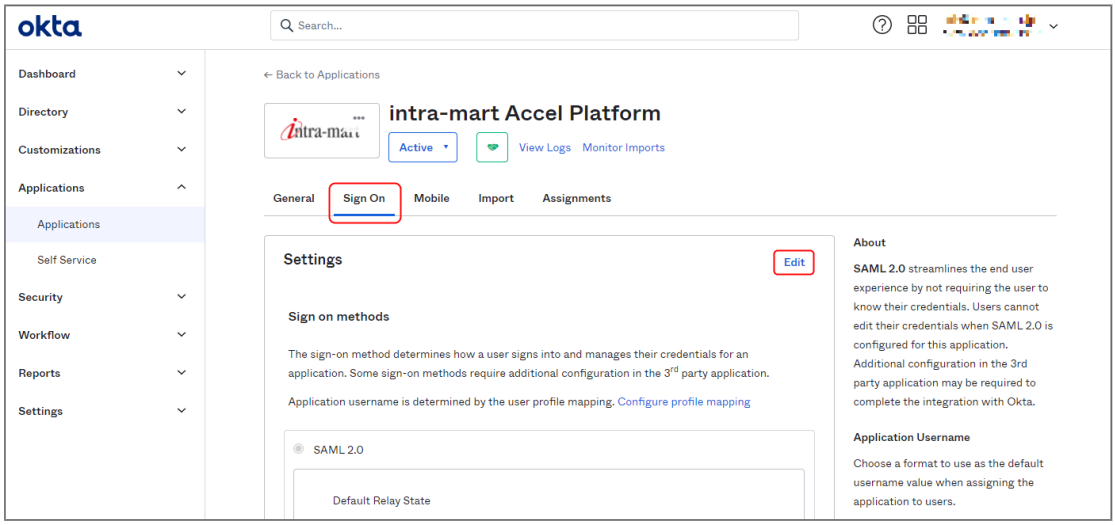
シングルログアウトの設定方法

シングルログアウトを設定します。

Okta のアプリケーションでシングルログアウトの設定

アプリケーションのシングルログアウトを有効にします。

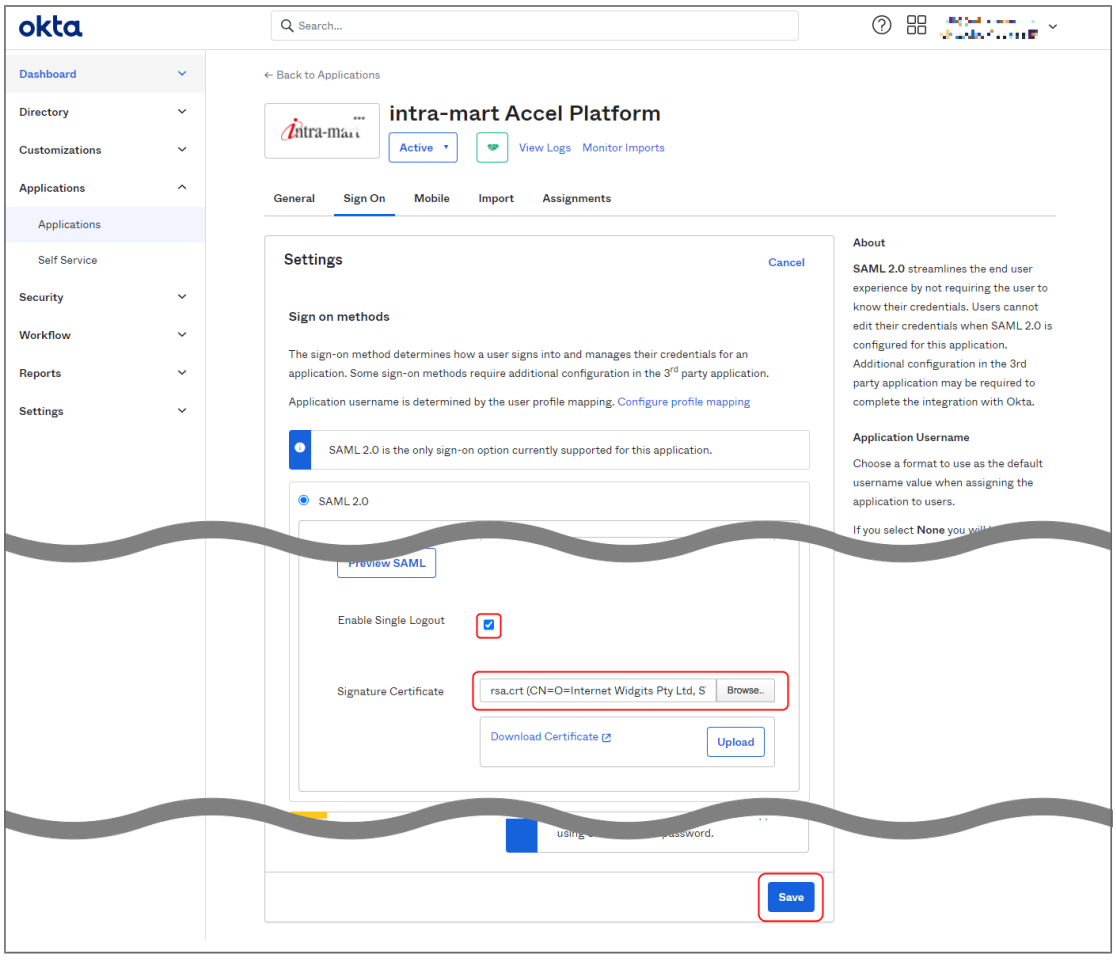
1. 「*Okta にアプリケーションを追加*」で追加したアプリケーションの詳細画面で「Sign On」タブをクリックし、「Settings」の「Edit」をクリックします。



2. 必用な項目を入力し、「Save」をクリックします。

シングルログアウトの設定例

Enable Single Logout	選択
Signature Certificate	事前に準備していた証明書を選択



intra-mart Accel Platform でシングルログアウトの設定

IdP の設定でシングルログアウトを有効にします。

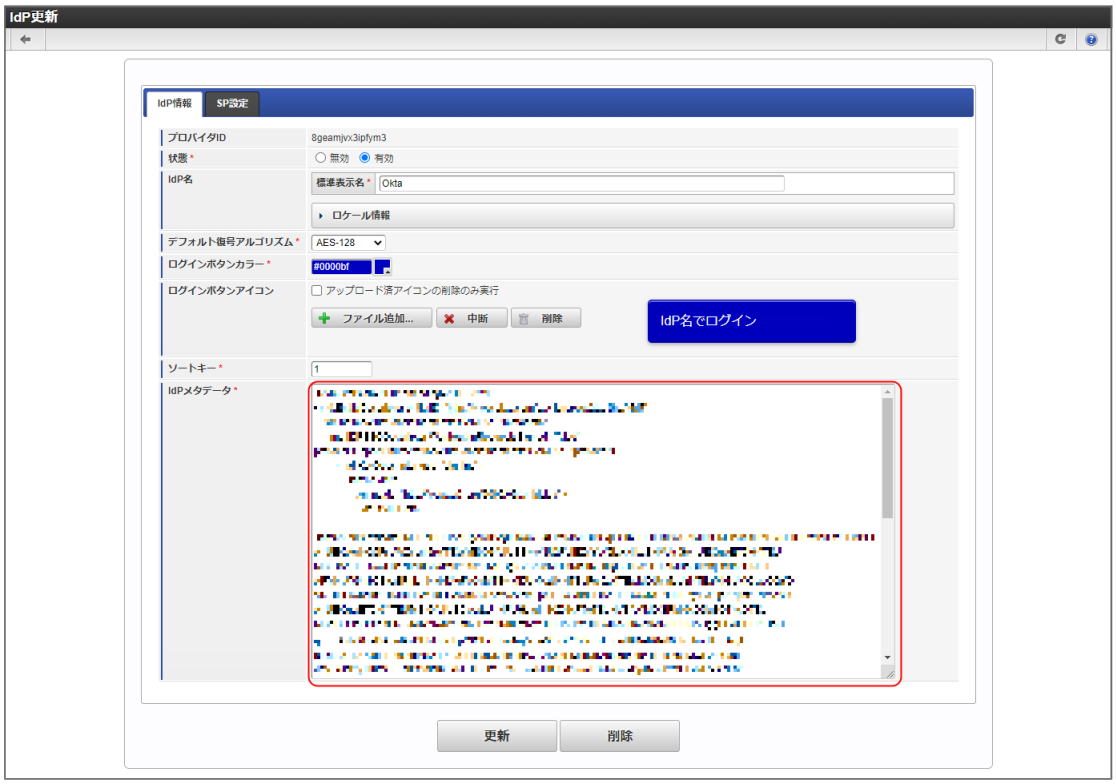
1. 「*IdP メタデータを取得*」に記載された手順で、メタデータを再取得します。
2. intra-mart Accel Platform にてシステム管理者でログインし、「システム管理」→「SAML認証設定」→「IdP一覧」をクリックし、「*intra-mart Accel Platform に Okta で追加したアプリケーションを登録*」で登録した IdP の編集画面に遷移します。
3. 「IdPメタデータ」に取得したメタデータを貼り付け、その他必要な項目を入力し「更新」ボタンをクリックします。

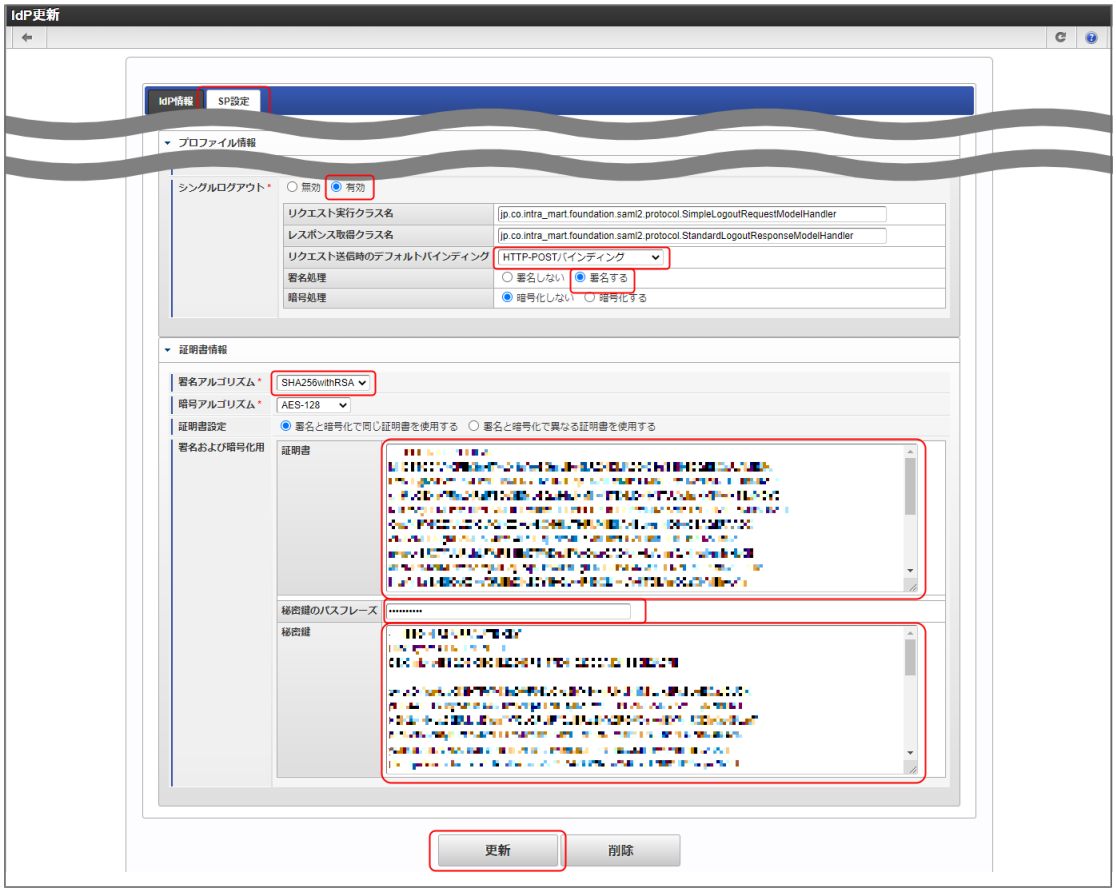
シングルログアウトの設定例（IdP設定タブ）

IdPメタデータ	Okta からコピーしたメタデータ

シングルログアウトの設定例（SP設定タブ）

シングルログアウト	有効
シングルログアウト - リクエスト送信時のデフォルトバインディング	HTTP-POSTバインディング
署名処理	署名する
署名アルゴリズム	SHA256withRSA
証明書	事前に準備していた証明書の内容
秘密鍵のパスフレーズ	事前に準備していた秘密鍵のパスフレーズ
秘密鍵	事前に準備していた秘密鍵の内容





Okta からもログアウト

intra-mart Accel Platform からのログアウトする際に、認証元である Okta からもログアウト（シングルログアウト）します。

1. 「*intra-mart Accel Platform にログイン*」に記載された手順でログインします。
2. ユーティリティメニューから「ログアウト（認証元からもログアウト）」をクリックします。

3. ログアウトに成功すると、intra-mart Accel Platform と Okta からログアウトします。