



Copyright © 2016 NTT DATA INTRAMART CORPORATION

目次

- 1. 改訂情報
- 2. はじめに
 - 2.1. 本書の目的
 - 2.2. 対象読者
 - 2.3. 本書の構成
 - 2.4. 注意事項
- 3. SAML 認証設定
 - 3.1. 操作
 - 3.2. 注意事項
- 4. IdP 別の設定方法
 - 4.1. OpenAM
 - 4.2. AzureAD
 - 4.3. Active Directory Federation Services
 - 4.4. salesforce.com
 - 4.5. PingFederate

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 ▪ 「AzureAD」の「シングルログアウトについて」を修正 ▪ 「AzureAD」に「AzureAD に送信するリクエストの署名について」を追加 ▪ 「AzureAD」に「AzureAD 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 ▪ 「AzureAD」の「AzureAD にWeb 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

はじめに

項目

- [本書の目的](#)
- [対象読者](#)
- [本書の構成](#)
- [注意事項](#)

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](#)
- [IdP一覧](#)
- [IdP新規作成](#)
- [IdP更新](#)
- [SAMLユーザマッピング\(管理\)](#)
 - [SAMLユーザマッピングCSV フォーマット](#)
- [SAMLユーザマッピング](#)
- [一般ユーザログイン](#)
- [ログアウト\(認証元からもログアウト\)](#)
- [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](#)

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

intra-mart Accel Platform — SAML認証セットアップガイド 第3版 2017-04-01
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」→「管理用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>/samlss/<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>/samlss/<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/samlss/user/settings/password`
- IdP を2件以上登録している場合：
`http://localhost:8080/imart/samlss/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。

項目

- [エンティティID](#)
- [署名](#)
 - [署名アルゴリズム](#)
 - [シングルサインオンの署名処理](#)
- [暗号化](#)
 - [AES256の使用](#)
- [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 からのログアウトリクエストについて](#)

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。
intra-mart Accel Platform のエンティティIDは以下の規則に従ってIdP 新規登録または更新時に設定されます。

- 設定ファイル(conf/server-context-config.xml)に定義したベースURL
- ベースURLが定義されていない場合は「http://server:port/path」

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

Javaは標準のままではAES の鍵の長さは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)

- JDK1.8 : <http://www.oracle.com/technetwork/java/javase/downloads/jce8-download-2133166.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](#)
- [前提条件](#)
- [設定方法](#)
 - [OpenAM をIdP に設定](#)
 - [OpenAM のメタデータをダウンロード](#)
 - [intra-mart Accel Platform にOpenAM を登録](#)
 - [intra-mart Accel Platform のメタデータをダウンロード](#)
 - [OpenAM にメタデータをインポート](#)
 - [トラストサークルの設定](#)
 - [intra-mart Accel Platform ユーザとOpenAM ユーザをマッピング](#)
- [OpenAM のユーザで intra-mart Accel Platform にログイン](#)
- [注意事項](#)
 - [使用可能な署名アルゴリズム](#)
 - [intra-mart Accel Platform のメタデータが変更された場合](#)

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 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プロバイダ項目の「エンティティのインポート」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	○	○

		HTTP-REDIRECTバインディング	HTTP-POSTバインディング
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。

AzureAD

AzureAD 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
- 設定方法
 - AzureAD にWeb アプリケーションを追加
 - AzureAD のメタデータをダウンロード
 - intra-mart Accel Platform にAzureAD を登録
 - intra-mart Accel Platform ユーザとAzureAD ユーザをマッピング
- AzureAD のユーザで intra-mart Accel Platform にログイン
- 注意事項
 - AzureAD に送信するリクエストの署名について
 - AzureAD の暗号処理について
 - シングルログアウトについて

前提条件

- AzureAD 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

AzureAD にWeb アプリケーションを追加

Azure AD の管理コンソールから intra-mart Accel Platform をWeb アプリケーションとして登録します。

「ACTIVE DIRECTORY」→「作成したディレクトリ名」→「アプリケーション」→「追加」から登録可能です。

Web アプリケーション登録時の設定例

実行する作業	組織で開発中のアプリケーションを追加
種類	WEB アプリケーションや WEB API
サインオン URL	http://<ホスト名>:<ポート番号>/< intra-mart Accel Platform コンテキストパス>/saml/profile/sso_response/post
アプリケーション ID/URI	http://<ホスト名>:<ポート番号>/< intra-mart Accel Platform コンテキストパス>



コラム

「サインオン URL」と「アプリケーション ID/URI」は後から変更できます。

「[intra-mart Accel Platform にAzureAD を登録](#)」が完了するまでは任意のURL を入力しておき、完了後に intra-mart Accel Platform のメタデータにある正しいURL を確認してからの変更が可能です。

- 「サインオン URL」は intra-mart Accel Platform のメタデータにある「AssertionConsumerService」要素の「Location」属性の値と一致します。
- 「アプリケーション ID/URI」は intra-mart Accel Platform のメタデータにある「EntityDescriptor」要素の「entityID」属性の値と一致します。

AzureAD のメタデータをダウンロード

「フェデレーション メタデータ ドキュメント URL」からAzureAD のメタデータをダウンロードします。

intra-mart Accel Platform にAzureAD を登録

IdP 新規登録画面からAzureAD 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	AzureAD 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	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name
シングルサインオン	有効



コラム

- 「属性名」の
「http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name」とは
AzureAD のユーザ名（メールアドレス形式）のことです。

intra-mart Accel Platform ユーザとAzureAD 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AzureAD のユーザ名をマッピングしてください。

AzureAD 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AzureAD 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AzureAD 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

AzureAD 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AzureAD 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。

AzureAD の暗号処理について

2016年8月現在、intra-mart Accel Platform とAzureAD 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う必要があります。

1. AzureAD で作成したWeb アプリケーションからマニフェストをダウンロードします。

2. マニフェストの「logoutUrl」に intra-mart Accel Platform のメタデータにあるシングルログアウト用のURL を設定します。
「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。
3. 編集したマニフェストをアップロードします。

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。

項目

- バージョン
- 前提条件
- 設定方法
 - Active Directory Federation Services のメタデータをダウンロード
 - intra-mart Accel Platform にActive Directory Federation Services を登録
 - intra-mart Accel Platform のメタデータをダウンロード
 - Active Directory Federation Services にメタデータをインポート
 - 要求規則の編集
 - intra-mart Accel Platform ユーザとActive Directory Federation Services ユーザをマッピング
- Active Directory Federation Services のユーザで intra-mart Accel Platform にログイン
- 注意事項
 - 使用可能な署名アルゴリズム
 - intra-mart Accel Platform のメタデータが変更された場合
 - シングルログアウトについて

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

- <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	○	○
SHA256withRSA	1024bit	○	○
	2048bit以上	○	○

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

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。

項目

- 前提条件
- 設定方法
 - salesforce.com のメタデータをダウンロード
 - intra-mart Accel Platform にsalesforce.com を登録
 - intra-mart Accel Platform のメタデータをダウンロード
 - 接続アプリケーションの新規作成
 - 接続アプリケーションのカスタム属性設定
 - 接続アプリケーションのプロファイル設定
 - intra-mart Accel Platform ユーザとsalesforce.com ユーザをマッピング
- salesforce.com のユーザで intra-mart Accel Platform にログイン
- 注意事項
 - 使用可能な署名アルゴリズム
 - intra-mart Accel Platform のメタデータが変更された場合
 - シングルログアウトについて

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

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	○	×

		HTTP-REDIRECTバインディング	HTTP-POSTバインディング
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。

項目

- バージョン
- 前提条件
- 設定方法
 - PingFederate のメタデータ（テンプレート）をダウンロード
 - intra-mart Accel Platform にPingFederate を登録
 - intra-mart Accel Platform のメタデータをダウンロード
 - PingFederate に intra-mart Accel Platform を登録
 - PingFederate のメタデータをダウンロード
 - intra-mart Accel Platform のPingFederate を更新
 - intra-mart Accel Platform ユーザとPingFederate ユーザをマッピング
- PingFederate のユーザで intra-mart Accel Platform にログイン
- 注意事項
 - intra-mart Accel Platform のメタデータが変更された場合
 - SAML Profiles について
 - Protocol Settings のAllowable SAML Bindings について
 - 署名アルゴリズムについて

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
 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

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。