IIJ IDサービス カスタムアプリケーション 連携マニュアル Jooto

> 2021年04月26日時点での情報で掲載しています。

目次

はじめに

- 本書で説明するカスタムアプリケーションの追加手順は参考例です。
  実際の作業においては、お客様の環境に合わせて設定をしてください。
- 外部サービスとの連携に関するご質問は、IIJ IDサービスのサポート窓口にて対応することはできません。
  対象の外部サービス側のマニュアルをご覧になるか、弊社担当営業までご相談ください。
- 対象の外部サービス自体の操作内容や仕様に関するご質問は弊社では承れません。
  製品マニュアルをご確認いただくか販売元にお問合わせください。
- IIJ IDサービスまたは連携するサービス側での変更によって、実際の設定方法・表示が異なってしまう場合があります。

用語説明

用語	内容
SAML (Security Assertion Markup Language)	異なるドメイン間でユーザ認証情報を交換できるXMLベースの標準規格 IIJ IDサービスは、SAML 2.0をサポートします
SAML SP (Service Provider)	ユーザにサービスを提供するエンティティ
SAML IDプロバイダ (Identity Provider)	ユーザの認証を行い、SPに認証情報を提供するエンティティ
エンティティID (Entity ID)	エンティティを一意に識別するID
SSOエンドポイントURL	SPからIDプロバイダにSAMLリクエストを行う場合にアクセスするURL
SPメタデータ	SPに関する情報を含んだXMLファイル SPがSPメタデータを提供している場合、 IIJ IDサービスでのアプリケーション登録にSPメタデータを利用できます
IDプロバイダのメタデータ	IDプロバイダに関する情報を含んだXMLファイル SPがIDプロバイダのメタデータによってSAML連携が設定出来る場合、 IIJ IDサービスが提供するIDプロバイダのメタデータを利用できます
IDプロバイダ Initiated SSO	IDプロバイダがSPからのSAMLリクエストを受け取らずにユーザの認証を開始し、 認証後にIDプロバイダがSPにSAMLレスポンスを渡してシングルサインオンを行うこと
SP Initiated SSO	SPがSAMLリクエストをIDプロバイダに渡してユーザの認証を開始し、 認証後にIDプロバイダがSPにSAMLレスポンスを渡してシングルサインオンを行うこと

SAML Just-In-Provisioning	該当ユーザが連携先サービスへSAML連携時に IIJ IDサービスからの認証連携情報に含まれるID情報に基づいて、 SAML連携に合わせて連携先サービス側のID情報を更新する 連携先サービス側のSAML機能 連携先サービス側のSAML機能であるため、 本機能が利用できるかどうかは連携先サービス側に依存します
ユーザ識別子(NameID)	認証済みユーザのID 連携先サービスによってはここに連携先サービス側のIDを指定する必要があります
SAML属性ステートメント (SAML Attribute Statement)	SAMLレスポンスに含まれる特有の識別情報

Jootoとの連携

連携にあたっては下記にご注意ください。

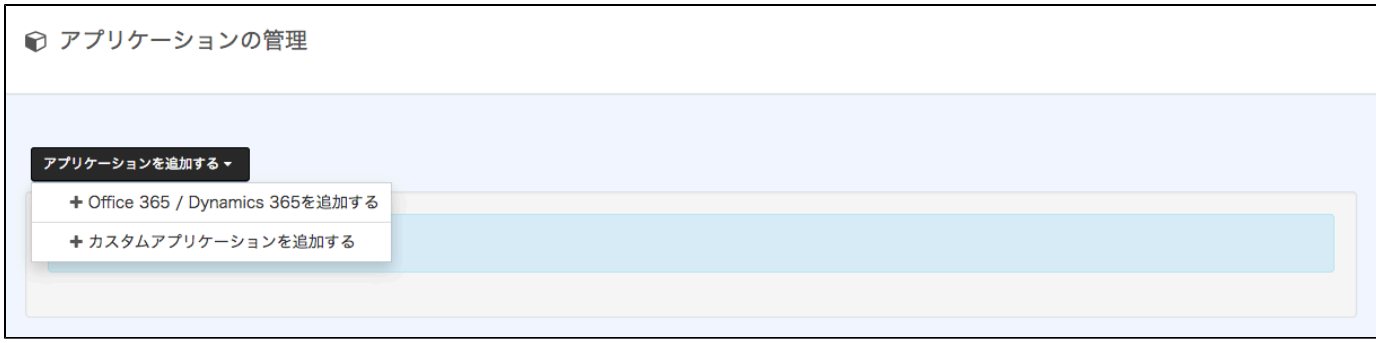
注意事項

1. JootoがSAMLで認証するキーは「ユーザID」、つまり、「メールアドレス」となります。
   IIJ IDサービス内の各ユーザ共通のユーザ属性にJootoの「ユーザID」と同一の値を保持しておく必要があります。
2. 作業前にJootoの管理者のユーザIDの値を保持するアカウントをIIJ IDサービスに用意しておいてください。
   そのアカウントの組み合わせでJootoとIIJ IDサービスにおいてそれぞれ作業を実施するとスムーズです。
3. Jootoでは SAML Just-In-Provisioning 機能が有効になっており、
   IIJ IDサービス側にアカウントあり、Jooto側に該当アカウントが存在していない状態で
   そのアカウントでSAML連携を行いますと、Jooto側に該当アカウントが自動で作成されてしまいます。
   Jooto側に不用意にアカウントを作成させないように、
   4.6.の「利用者設定」において、必要なアカウントのみがJootoにSAML連携させるように制限をかけることを検討してください。

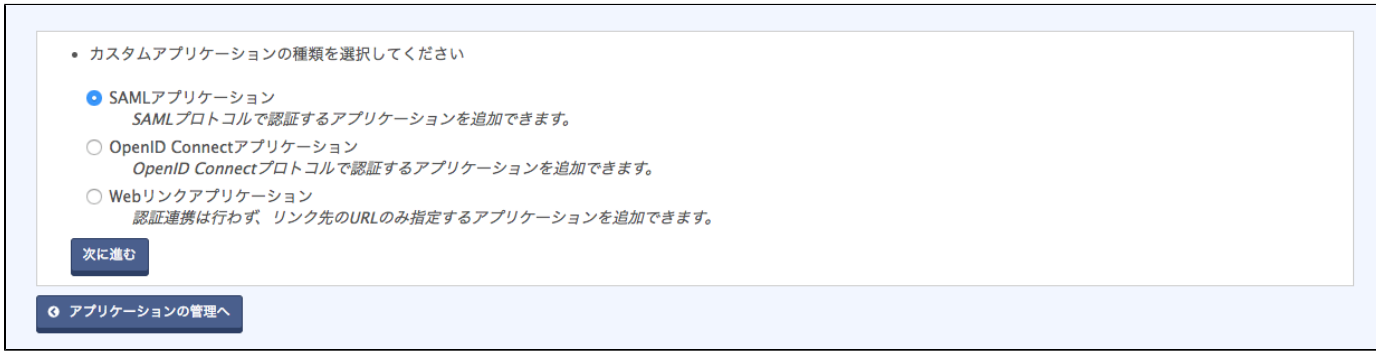
1. IIJ IDサービスにSAMLアプリケーションを登録する

1. IIJ IDコンソールに管理者アカウントとしてログインし、「アプリケーション」>「アプリケーションの管理」をクリックします。

2.「アプリケーションを追加する」>「カスタムアプリケーションを追加する」をクリックします。



3.「SAMLアプリケーション」を選択して、「次に進む」をクリックします。



4. アプリケーション情報を入力して、「アプリケーションを追加する」をクリックします。

項目	内容	備考
アプリケーション名	例) Jooto	必須
アプリケーションの説明	例) カンバン方式のタスク・プロジェクト管理ツール「Jooto」	任意
アプリケーションロゴ	（ファイルアップロード）	任意
IDプロバイダの選択	「アプリケーション専用のエンティティIDを利用」を選択	必須

2. IIJ IDサービスのIDプロバイダ情報を確認する

1. 引き続き、作成されたアプリケーションに対して「編集する」をクリックします。

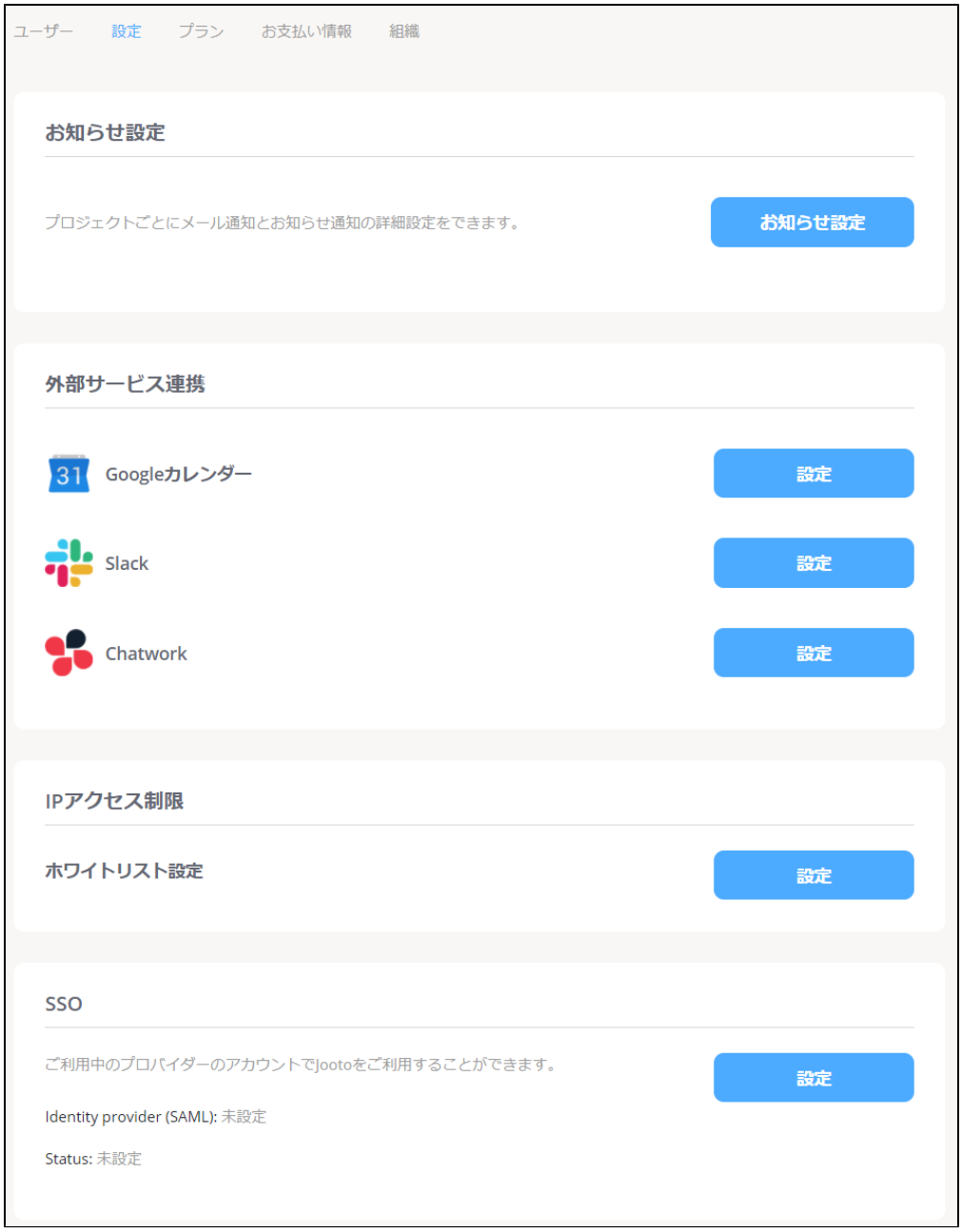
2. 「IDプロバイダ情報」のタブをクリックします。

3. 表示された「メタデータ」の箇所にある「ダウンロードする」をクリックし、IDプロバイダのメタデータをダウンロードします。

3. Jootoの設定を実施する

1. Jootoに管理者としてログインし、上部にあるメニューより「お客様の組織名」>「設定」をクリックします。

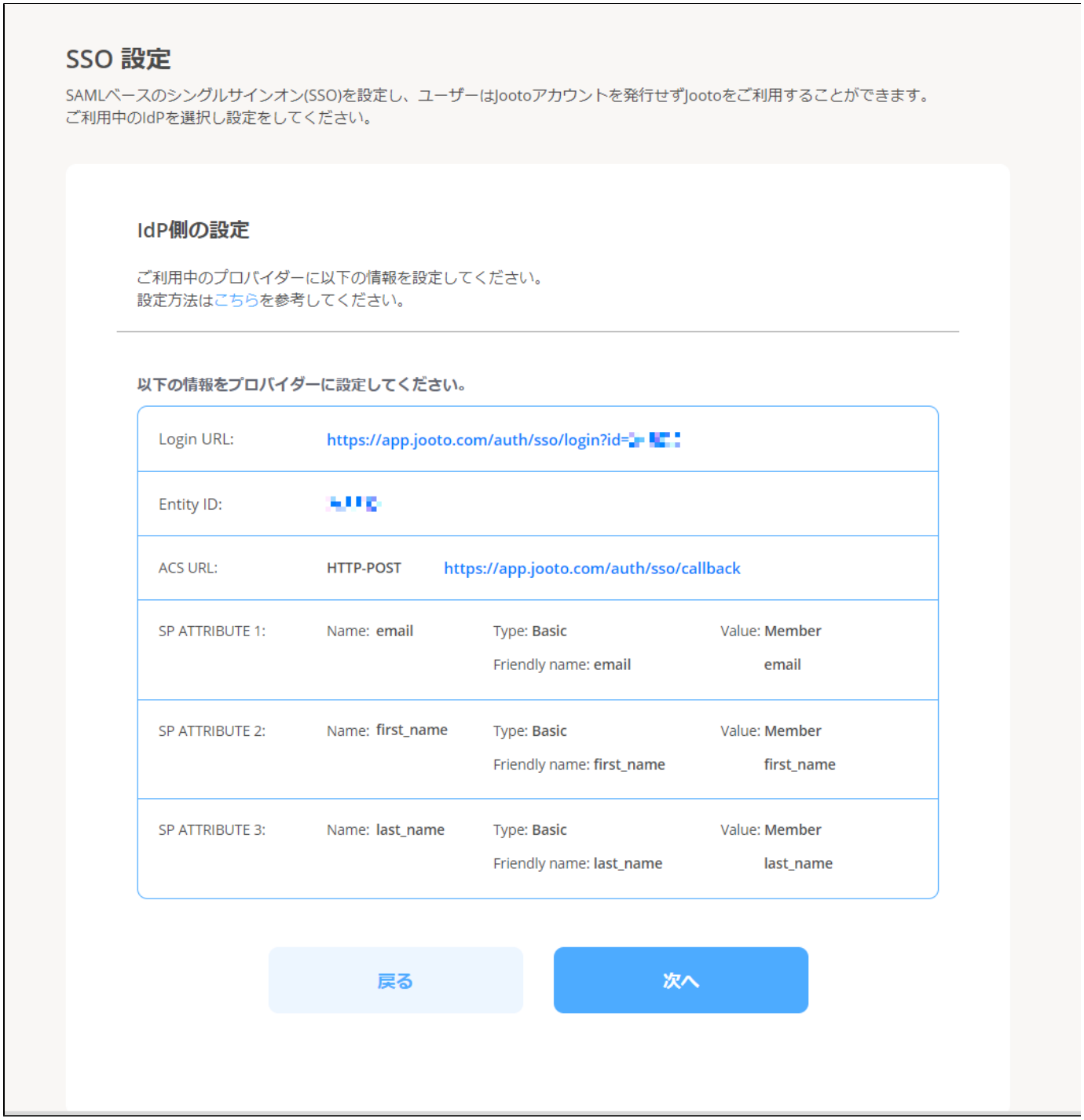
2. 表示された組織設定画面にて、SSOの項目より「設定」をクリックします。



3. 表示されたSSO設定で、以下の通り入力し「次へ」をクリックします。

項目	内容	備考
IdP選択	Other	必須
ドメイン名	例) example.com	必須 IIJ IDサービスと連携するドメインを入力
説明	例) IIJ IDサービス	任意

4. 表示された下記情報から「Login URL」と「ACS URL」の値を控え、「次へ」をクリックします。



5.「XMLメタデータ」の入力欄に、2.3. で入手したxmlファイルの中身を張り付け、「完了」をクリックします。

6.Jootoページの上部に緑のバーで「SSOの設定が正常に完了しました。」が表示されたことを確認します。

4. IIJ IDサービスのSAMLアプリケーションを設定する

1. IIJ IDコンソールにログインし、「アプリケーション」>「アプリケーションの管理」をクリックします。

2. 引き続き、作成されたアプリケーションに対して「編集する」をクリックします。

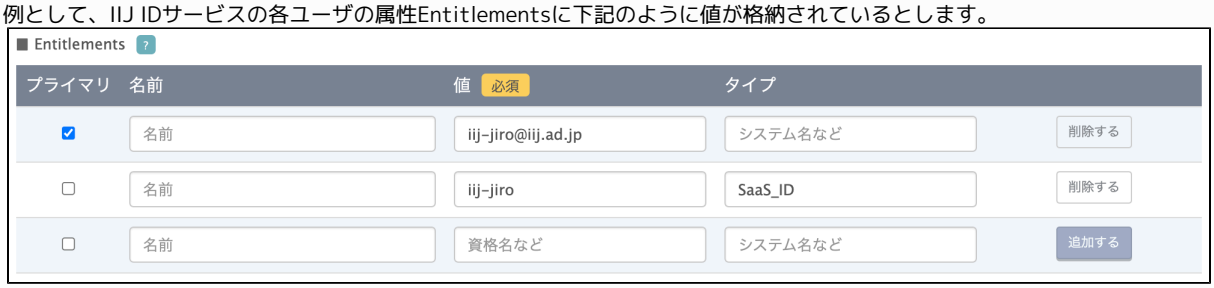
3.「フェデレーション設定」のタブをクリックします。

4.「SAML基本情報」を以下の通り設定して、「変更を適用する」をクリックします。

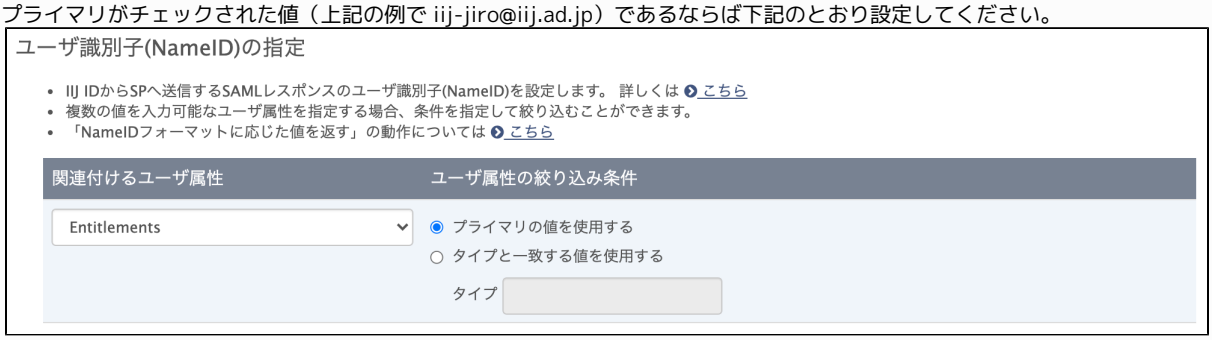
項目		内容		備考
SAML基本情報	「SAML情報を入力する」を選択			
	シングルサインオンURL	3.4.で控えた「ACS URL」を入力 https://app.jooto.com/auth/sso/callback		
	エンティティ ID	「https://app.jooto.com/」を入力		3.4.の「Entity ID」ではなく、 「https://app.jooto.com/」と 入力してください
	NameIDフォーマット	「urn:oasis:names:tc:SAML:1.1: nameid-format:unspecified」を選択		
	検証後の遷移先 (RelayState)	（空欄）		
	アプリケーションの トップページURL	3.4.で控えた「Login URL」を入力 例) https://app.jooto.com/auth/sso/login?id=XXXXX		「XXXXX」の部分は、 3.4.で控えた値に基づいて 入力してください
ユーザ識別子 (NameID)の指定	関連付けるユーザ属性	例) 「ID」		Jootoとの連携では ここの値は評価されないので、 「ID」をそのまま 指定しておくことをおすすめします。
属性値関連付け（ユーザ属性）		email	例） ID	Jootoの 各ユーザの「ログインID」の値が 格納されている属性を指定します。
		last_name	例） 姓	Jootoの 各ユーザの「姓」の値が 格納されている属性を指定します。
		first_name	例） 名	Jootoの 各ユーザの「名」の値が 格納されている属性を指定します。

- ユーザ識別子(NameID)の指定は、ユーザ単位ではなくSAMLアプリケーション単位でしかできません。

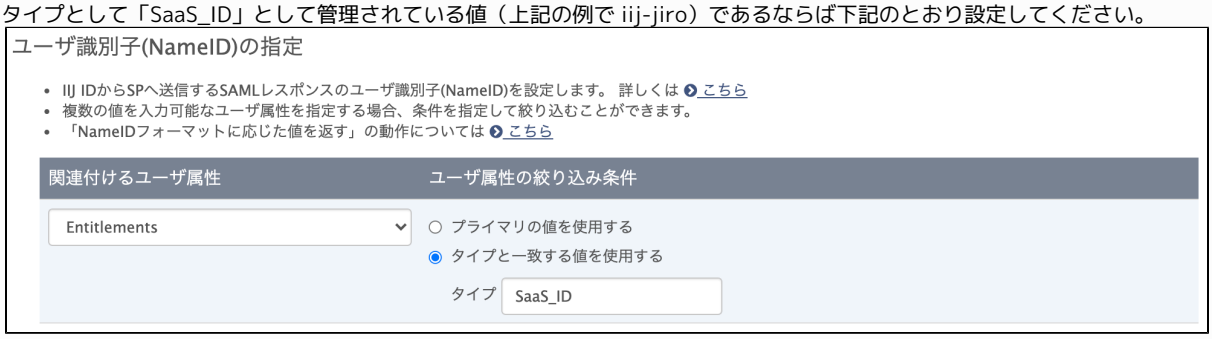
- ユーザ識別子(NameID)の指定した属性にユーザが値を保持していない場合は SAML連携は失敗します。
- 以下、ユーザ識別子(NameID)でID以外で複数値を持つ属性での指定方法を説明します。
  例として、IIJ IDサービスの各ユーザの属性Entitlementsに下記のように値が格納されているとします。



そして、連携先サービス側にユーザ識別子(NameID)として渡したい値が
プライマリがチェックされた値（上記の例で iij-jiro@iij.ad.jp）であるならば下記のとおり設定してください。

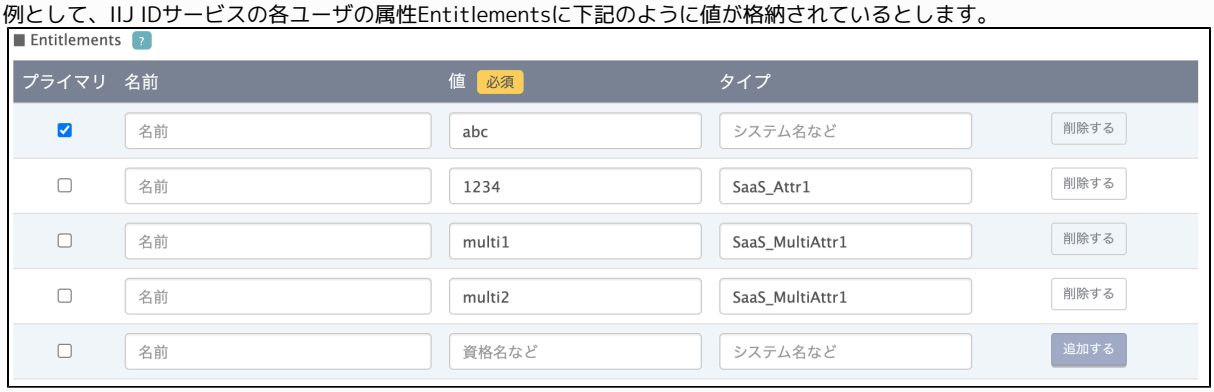


連携先サービス側にユーザ識別子(NameID)として渡したい値が
タイプとして「SaaS_ID」として管理されている値（上記の例で iij-jiro）であるならば下記のとおり設定してください。

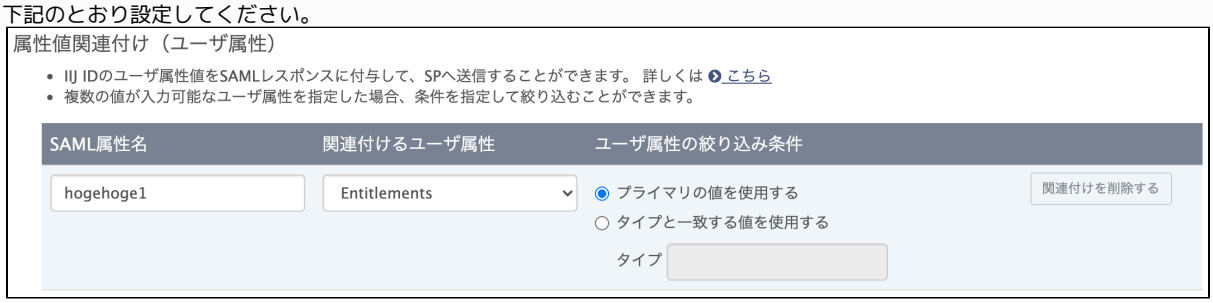


- ユーザ識別子(NameID)としてID以外の属性を指定している場合、
  基本IIJ IDサービスに対する更新処理で該当属性の値を更新される可能性があります。
  しかし、その更新が連携先サービスまで伝搬されることはありませんので、
  該当属性の値が更新されてしまうとそれまで連携先サービスで連携していたアカウントに接続できなくなってしまいます。
  よって、ユーザ識別子(NameID)としている属性の値が更新される場合には、
  連携先サービス側でもそれに紐づく属性（多くの場合、ユーザID）に対して忘れずに更新をかけてください。
- あるユーザではタイプとして「SaaS_ID」が複数エントリーがある状態で設定されていて、
  それをユーザ識別子(NameID)として指定している場合、
  サービスマニュアルに記載されている所定のルールに基づいていずれかの単数値だけが採用される結果となり、
  連携対象のサービスに対して管理者の意図しないアカウント同士でSAML連携されてしまう危険性があります。
  よって、必ず対象となる各ユーザにおいて、
  ユーザ識別子(NameID)として指定するタイプのエントリーが複数個存在させないようにご注意ください。

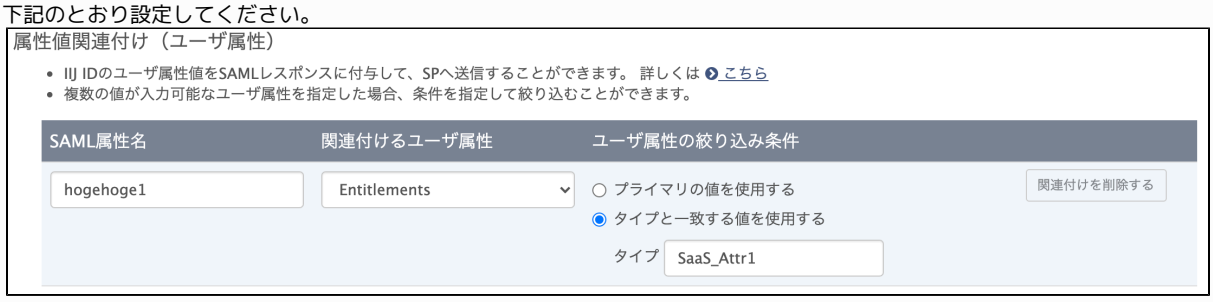
- 属性値関連付け（ユーザ属性）は、ユーザ単位ではなくSAMLアプリケーション単位でしかできません。
- 以下、属性値関連付け（ユーザ属性）で複数値を持つ属性での指定方法を説明します。
例として、IIJ IDサービスの各ユーザの属性Entitlementsに下記のように値が格納されているとします。



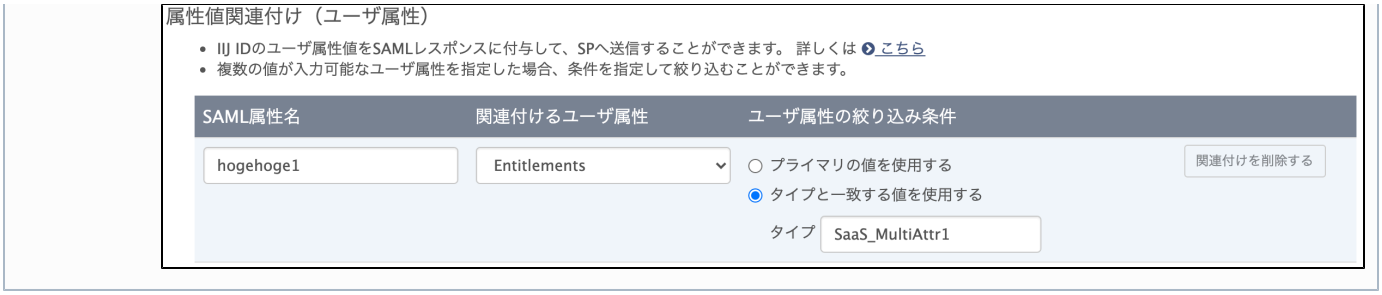
そして、連携先サービス側に属性値関連付け（ユーザ属性）として「hogehoge1」という属性名として、
渡したい値についてはプライマリがチェックされた値（上記の例で abc）であるならば
下記のとおり設定してください。



連携先サービス側に属性値関連付け（ユーザ属性）として「hogehoge1」という属性名として、
渡したい値についてはタイプとして「SaaS_Attr1」として管理されている値（上記の例で 1234）であるならば
下記のとおり設定してください。

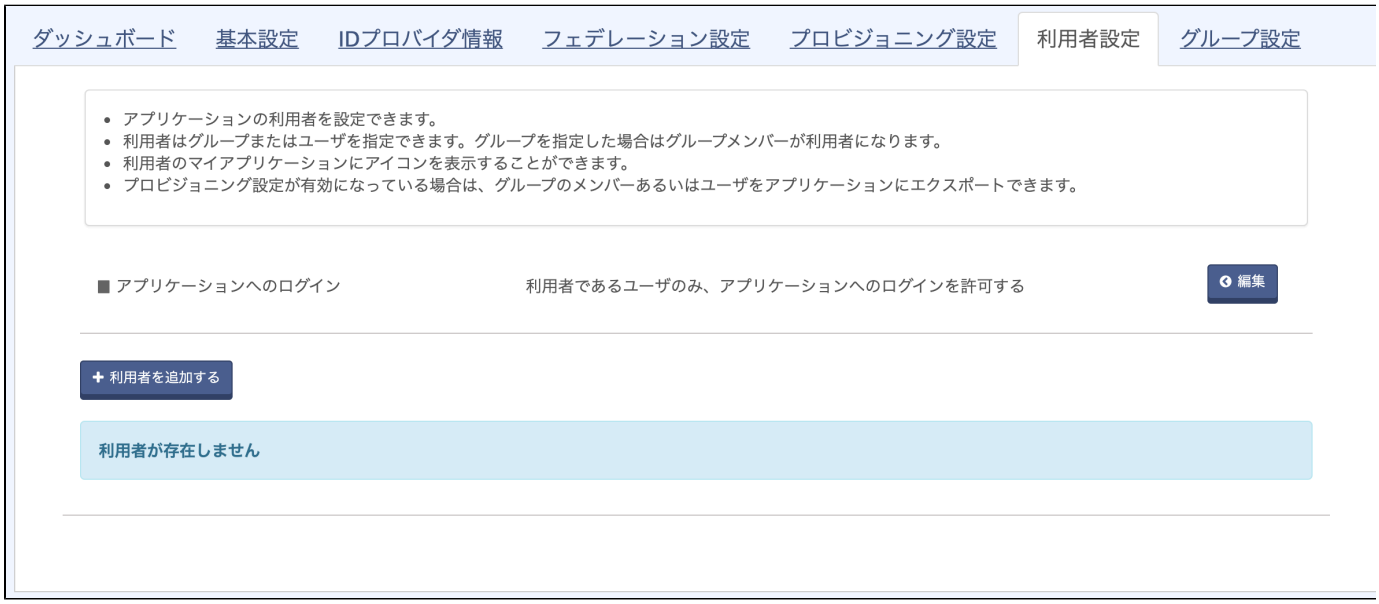


連携先サービス側に属性値関連付け（ユーザ属性）として「hogehoge1」という属性名として、
渡したい値についてはタイプとして「SaaS_MultiAttr1」として管理されている値（上記の例で multi1 と multi2 の複数値）であるならば
下記のとおり設定してください。



5. 引き続き、「利用者設定」のタブをクリックします。

6.「利用者を追加する」をクリックし、アプリケーションにシングルサインオンさせたいグループ or ユーザを指定します。

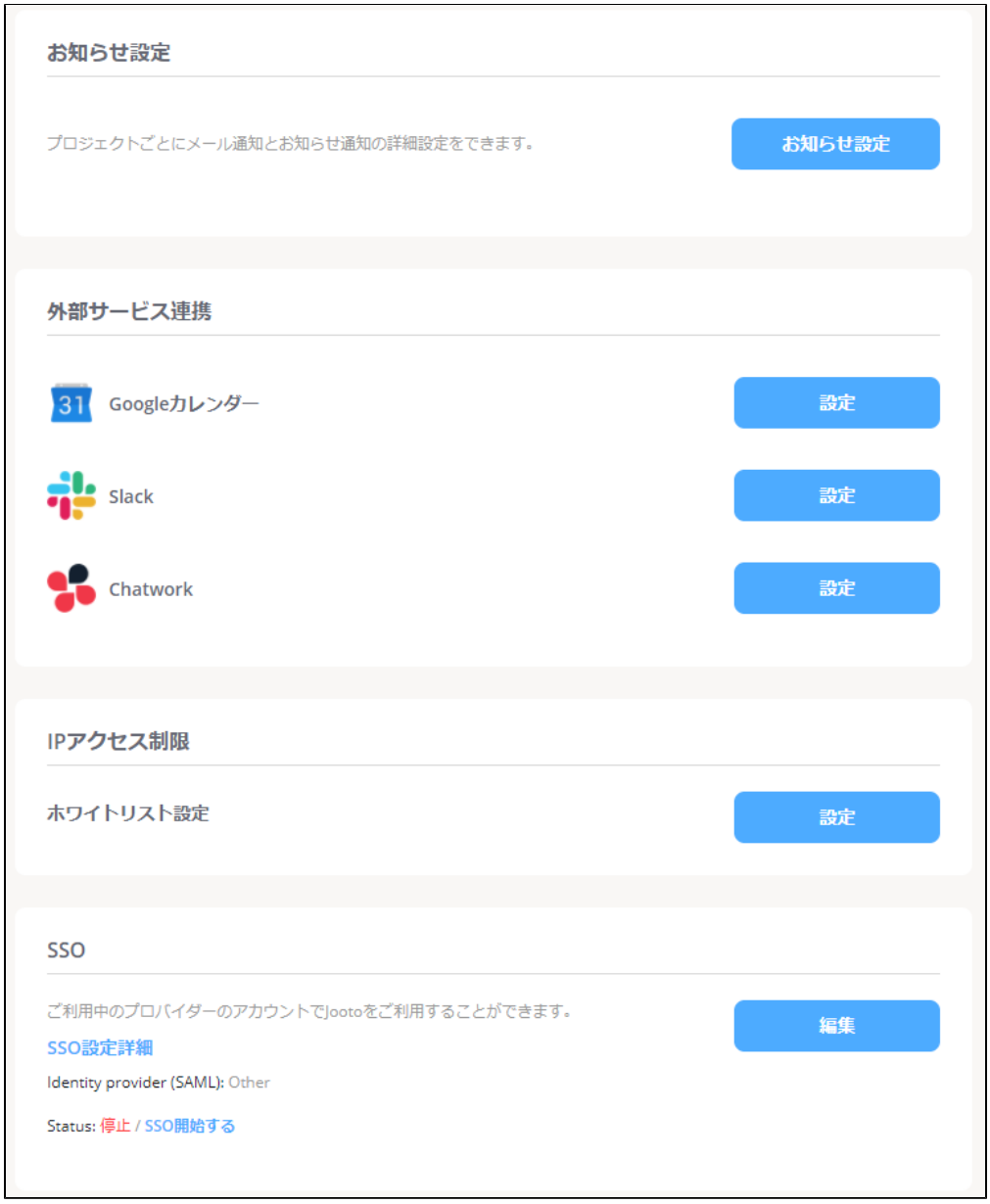


利用者に登録したグループ or ユーザ以外のユーザにもこのアプリケーションを利用させたい場合は、
「アプリケーションへのログイン」のところにある「編集」をクリックし、
「利用者でないユーザも、アプリケーションへのログインを許可する」を選択し、「変更を適用する」をクリックしてください。

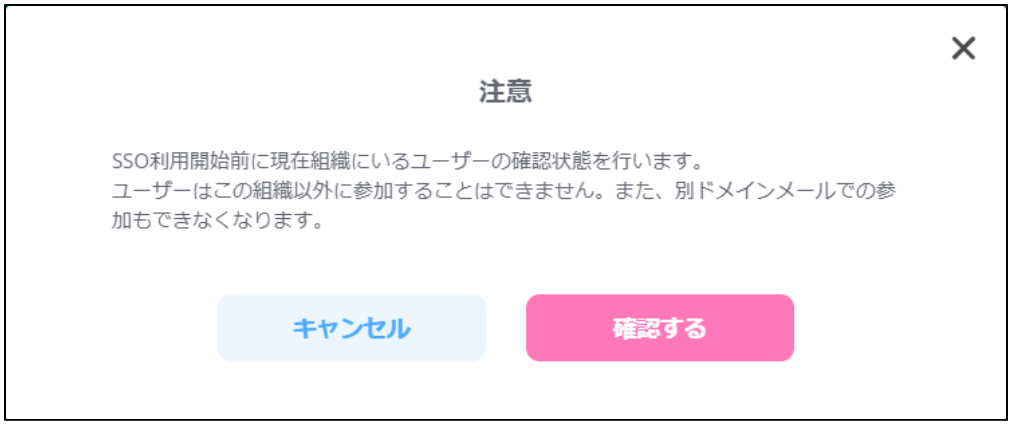
5. SSOの開始設定

1. Jootoに管理者としてログインし、上部にあるメニューより「お客様の組織名」>「設定」をクリックします。

2.表示されたの組織設定画面にて、SSOの項目より「SSO開始する」をクリックします。



3. 以下の画面が表示されるため、「確認する」をクリックします。



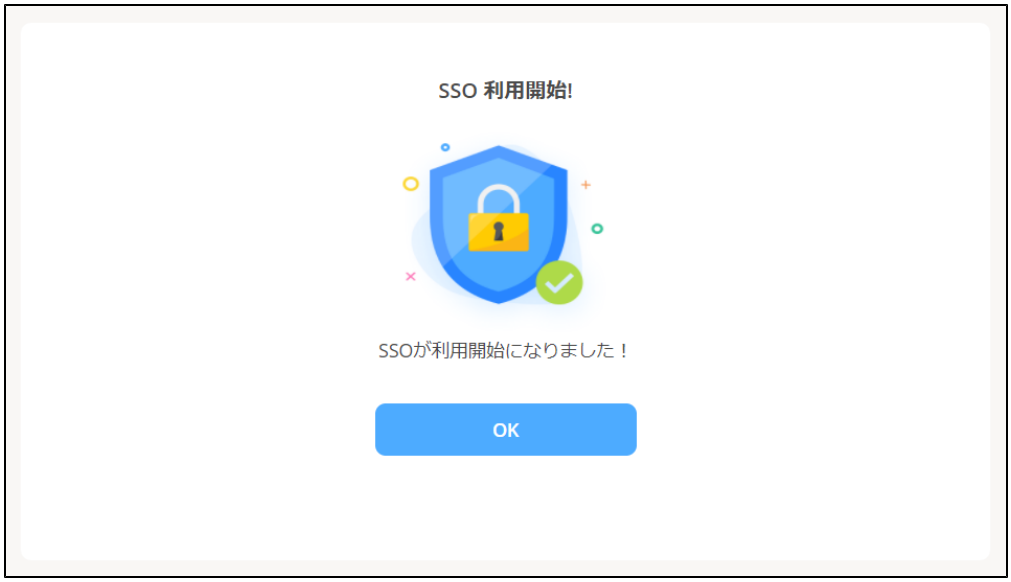
4. 以下の画面が表示されるため、「OK」をクリックします。

IIJ IDサービスでのセットアップをJootoの管理者のユーザIDの値を持つIIJ IDサービスの管理者アカウントで行い、
IIJ IDサービス上ではそのアカウントでログインしたままの状態であることを想定しています。

IIJ IDサービスでのセットアップをJootoの管理者のユーザIDの値を持つIIJ IDサービスの管理者アカウントで行っていない場合は、
IIJ IDサービスのアカウントの登録状況、および、4.6. の「利用者設定」如何では連携エラーとなってしまいます。
また、IIJ IDサービス側でログアウト状態になっている場合には、
IIJ IDサービスの認証が求められる形になりますので、
Jootoの管理者のユーザIDの値を持つIIJ IDサービスのアカウントでログインして認証を行ってください。

5. 以下の画面が表示されるため、「利用開始 」をクリックします。

6. 以下の画面が表示されたら、連携完了になります。


SSO 利用開始!
SSOが利用開始になりました！
OK