

# IJ 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
- 用語説明
- Jootoとの連携
  - 1. IJ IDサービスにSAMLアプリケーションを登録する
  - 2. IJ IDサービスのIDプロバイダ情報を確認する
  - 3. Jootoの設定を実施する
  - 4. IJ IDサービスのSAMLアプリケーションを設定する
  - 5. SSOの開始設定

## 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、IJ 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。
- IJ 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 IJ 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、 IJ 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、 IJ 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	<p>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</p> <p>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</p>
ユーザ識別子(NamID)	<p>認証済みユーザのID</p> <p>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</p>
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

- 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。
- 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。
- 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

- 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。



- 「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。

## アプリケーションの管理

アプリケーションを追加する

- + Office 365 / Dynamics 365を追加する
- + カスタムアプリケーションを追加する

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。

- カスタムアプリケーションの種類を選択してください
  - SAMLアプリケーション  
SAMLプロトコルで認証するアプリケーションを追加できます。
  - OpenID Connectアプリケーション  
OpenID Connectプロトコルで認証するアプリケーションを追加できます。
  - Webリンクアプリケーション  
認証連携は行わず、リンク先のURLのみ指定するアプリケーションを追加できます。

次に進む

アプリケーションの管理へ

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

### アプリケーション情報

■ アプリケーション名 **必須**

Jooto

■ アプリケーションの説明

カンバン方式のタスク・プロジェクト管理ツール「Jooto」

■ アプリケーションロゴ

+ ファイルを選択

■ 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
- システムで共通のエンティティIDを利用

アプリケーションを追加する

2. IJ 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。

### お知らせ設定

プロジェクトごとにメール通知とお知らせ通知の詳細設定をできます。

お知らせ設定

### 外部サービス連携

 Googleカレンダー

設定

 Slack

設定

 Chatwork

設定

### IPアクセス制限

ホワイトリスト設定

設定

### SSO

ご利用中のプロバイダーのアカウントでJootoをご利用することができます。

設定

Identity provider (SAML): 未設定

Status: 未設定

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

## SAML Identity Providerを選択してください

ご希望のIdPを選択してください。IdP名は現在ご利用中のサービス名を選択し、ドメイン名はご自身が所属している企業のドメイン名を入力してください。

### IdP 選択

Other

ご利用されているIdPを選択してください。

### ドメイン名



ドメイン名を入力してください。例 user1@example.com の場合 example.com になります。

### 説明 (任意)

クラウド型のID管理・認証管理サービスIDサービス

設定時に記載しておきたい情報を入力してください。(必須ではありません。)

戻る

次へ

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。

## SSO 設定

SAMLベースのシングルサインオン(SSO)を設定し、ユーザーはJootoアカウントを発行せずJootoをご利用することができます。  
ご利用中のIdPを選択し設定をしてください。

### IdP側の設定

ご利用中のプロバイダーに以下の情報を設定してください。  
設定方法は[こちら](#)を参考してください。

以下の情報をプロバイダーに設定してください。

Login URL:	<a href="https://app.jooto.com/auth/sso/login?id=">https://app.jooto.com/auth/sso/login?id=</a>		
Entity ID:	<a href="#"></a>		
ACS URL:	HTTP-POST	<a href="https://app.jooto.com/auth/sso/callback">https://app.jooto.com/auth/sso/callback</a>	
SP ATTRIBUTE 1:	Name: email	Type: Basic Friendly name: email	Value: Member email
SP ATTRIBUTE 2:	Name: first_name	Type: Basic Friendly name: first_name	Value: Member first_name
SP ATTRIBUTE 3:	Name: last_name	Type: Basic Friendly name: last_name	Value: Member last_name

戻る

次へ

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。

## SAML IdP メタデータをインポート

IdP側にてJootoの設定を行ったあと発行されるXMLメタデータを入力してください。

XML メタデータ



戻る

完了

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。

SSOの設定が正常に完了しました。 [SSOを開始する](#)

## 4. IJ IDサービスのSAMLアプリケーションを設定する

1. IJ 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との連携ではこの値は評価されないで、「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。

- SPがメタデータを提供している場合は「SPのメタデータをアップロードする」を選択してください。
- それ以外の場合は「SAML情報を入力する」を選択してください。

## SAML基本情報

- SPのメタデータをアップロードする
- SAML情報を入力する

■ シングルサインオンURL **必須**■ エンティティ ID **必須**■ NameIDフォーマット **必須**■ 検証後の遷移先(RelayState) **?**■ アプリケーションのトップページ URL **?**

## ユーザ識別子(NameID)の指定

- IJ IDからSPへ送信するSAMLレスポンスのユーザ識別子(NameID)を設定します。詳しくは [こちら](#)
- 複数の値を入力可能なユーザ属性を指定する場合、条件を指定して絞り込むことができます。
- 「NameIDフォーマットに応じた値を返す」の動作については [こちら](#)

関連付けるユーザ属性

ユーザ属性の絞り込み条件

## 属性値関連付け (ユーザ属性)

- IJ IDのユーザ属性値をSAMLレスポンスに付与して、SPへ送信することができます。詳しくは [こちら](#)
- 複数の値が入力可能なユーザ属性を指定した場合、条件を指定して絞り込むことができます。

SAML属性名

関連付けるユーザ属性

ユーザ属性の絞り込み条件

関連付けを削除する

関連付けを削除する

関連付けを削除する

[+ 関連付けを追加する](#)

## 属性値関連付け (所属グループ名)

- ユーザが所属するグループの名前をSAMLレスポンスに付与して、SPへ送信することができます。詳しくは [こちら](#)

[+ 関連付けを追加する](#)[変更を適用する](#)

- 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、IJ 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。

プライマリ	名前	値	必須	タイプ	
<input checked="" type="checkbox"/>	名前	ijj-jiro@ijj.ad.jp		システム名など	削除する
<input type="checkbox"/>	名前	ijj-jiro		SaaS_ID	削除する
<input type="checkbox"/>	名前	資格名など		システム名など	追加する

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 ijj-jiro@ijj.ad.jp）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)の指定

- IJ IDからSPへ送信するSAMLレスポンスのユーザ識別子(NameID)を設定します。詳しくは [こちら](#)
- 複数の値を入力可能なユーザ属性を指定する場合、条件を指定して絞り込むことができます。
- 「NameIDフォーマットに応じた値を返す」の動作については [こちら](#)

関連付けるユーザ属性	ユーザ属性の絞り込み条件
Entitlements	<input checked="" type="radio"/> プライマリの値を使用する <input type="radio"/> タイプと一致する値を使用する タイプ <input type="text"/>

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 ijj-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)の指定

- IJ IDからSPへ送信するSAMLレスポンスのユーザ識別子(NameID)を設定します。詳しくは [こちら](#)
- 複数の値を入力可能なユーザ属性を指定する場合、条件を指定して絞り込むことができます。
- 「NameIDフォーマットに応じた値を返す」の動作については [こちら](#)

関連付けるユーザ属性	ユーザ属性の絞り込み条件
Entitlements	<input type="radio"/> プライマリの値を使用する <input checked="" type="radio"/> タイプと一致する値を使用する タイプ <input type="text" value="SaaS_ID"/>

- 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IJ 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う可能性があります。  
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。

プライマリ	名前	値 <span style="background-color: #ffc107;">必須</span>	タイプ	
<input checked="" type="checkbox"/>	名前	ijj-jiro@ijj.ad.jp	システム名など	削除する
<input type="checkbox"/>	名前	ijj-jiro	SaaS_ID	削除する
<input type="checkbox"/>	名前	jiro	SaaS_ID	削除する
<input type="checkbox"/>	名前	資格名など	システム名など	追加する

- 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、IJ 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。

プライマリ	名前	値 <span style="background-color: #ffc107;">必須</span>	タイプ	
<input checked="" type="checkbox"/>	名前	abc	システム名など	削除する
<input type="checkbox"/>	名前	1234	SaaS_Attr1	削除する
<input type="checkbox"/>	名前	multi1	SaaS_MultiAttr1	削除する
<input type="checkbox"/>	名前	multi2	SaaS_MultiAttr1	削除する
<input type="checkbox"/>	名前	資格名など	システム名など	追加する

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。

#### 属性値関連付け（ユーザ属性）

- IJ IDのユーザ属性値をSAMLレスポンスに付与して、SPへ送信することができます。詳しくは [こちら](#)
- 複数の値が入力可能なユーザ属性を指定した場合、条件を指定して絞り込むことができます。

SAML属性名	関連付けるユーザ属性	ユーザ属性の絞り込み条件	
hogehoge1	Entitlements	<input checked="" type="radio"/> プライマリの値を使用する <input type="radio"/> タイプと一致する値を使用する タイプ <input type="text"/>	関連付けを削除する

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。

#### 属性値関連付け（ユーザ属性）

- IJ IDのユーザ属性値をSAMLレスポンスに付与して、SPへ送信することができます。詳しくは [こちら](#)
- 複数の値が入力可能なユーザ属性を指定した場合、条件を指定して絞り込むことができます。

SAML属性名	関連付けるユーザ属性	ユーザ属性の絞り込み条件	
hogehoge1	Entitlements	<input type="radio"/> プライマリの値を使用する <input checked="" type="radio"/> タイプと一致する値を使用する タイプ <input type="text" value="SaaS_Attr1"/>	関連付けを削除する

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。

属性値関連付け (ユーザ属性)

- IJ IDのユーザ属性値をSAMLレスポンスに付与して、SPへ送信することができます。詳しくは [こちら](#)
- 複数の値が入力可能なユーザ属性を指定した場合、条件を指定して絞り込むことができます。

SAML属性名	関連付けるユーザ属性	ユーザ属性の絞り込み条件	
hogehoge1	Entitlements	<input type="radio"/> プライマリの値を使用する <input checked="" type="radio"/> タイプと一致する値を使用する	関連付けを削除する
		タイプ SaaS_MultiAttr1	

5. 引き続き、「利用者設定」のタブをクリックします。

[ダッシュボード](#)
[基本設定](#)
[IDプロバイダ情報](#)
[フェデレーション設定](#)
[プロビジョニング設定](#)
[利用者設定](#)
[グループ設定](#)

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。

[ダッシュボード](#)
[基本設定](#)
[IDプロバイダ情報](#)
[フェデレーション設定](#)
[プロビジョニング設定](#)
[利用者設定](#)
[グループ設定](#)

- アプリケーションの利用者を設定できます。
- 利用者はグループまたはユーザを指定できます。グループを指定した場合はグループメンバーが利用者になります。
- 利用者のマイアプリケーションにアイコンを表示することができます。
- プロビジョニング設定が有効になっている場合は、グループのメンバーあるいはユーザをアプリケーションにエクスポートできます。

■ アプリケーションへのログイン 利用者であるユーザのみ、アプリケーションへのログインを許可する [編集](#)

---

[+ 利用者を追加する](#)

利用者が存在しません

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。

**👤 アプリケーションへのログイン許可**

利用者であるユーザのみ、アプリケーションへのログインを許可する  
 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

キャンセル
変更を適用する

## 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。

**お知らせ設定**

---

プロジェクトごとにメール通知とお知らせ通知の詳細設定ができます。

[お知らせ設定](#)

**外部サービス連携**

---

 Googleカレンダー [設定](#)

 Slack [設定](#)

 Chatwork [設定](#)

**IPアクセス制限**

---

ホワイトリスト設定 [設定](#)

**SSO**

---

ご利用中のプロバイダーのアカウントでjootoをご利用することができます。

[SSO設定詳細](#)

Identity provider (SAML): Other

Status: 停止 / [SSO開始する](#)

[編集](#)

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。

×

**注意**

SSO利用開始前に現在組織にいるユーザーの確認状態を行います。  
ユーザーはこの組織以外に参加することはできません。また、別ドメインメールでの参加もできなくなります。

[キャンセル](#) [確認する](#)

4. 以下の画面が表示されるため、「OK」をクリックします。

## SSO利用開始

この組織に所属している全てのユーザーがSSOをご利用する準備が整いました。  
OKボタンを押して利用を開始してください。



戻る

OK

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