



# BlueBean SSO認証 説明書

## Azure SAML編

# 目次

1

Azure SAML情報作成

2

BlueBean設定

# Azure SAML情報作成 エンタープライズアプリケーション作成

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をクリックする

Microsoft Azure リソース、サービス、ドキュメントの検索 (G+)

ホーム > エンタープライズ アプリケーション

**エンタープライズ アプリケーション** | すべてのアプリケーション ...  
Default Directory - Azure Active Directory

概要

新しいアプリケーション 更新 ダウンロード (エクスポート) プレビューの情報 列 プレビュー機能 フィー

概要  
Azure AD テナントを ID プロバイダーとして使用するよう設定されている、ご自身の組織内のアプリケーションを表示、フィルター処理、検索します。

問題の診断と解決  
組織で管理されているアプリケーションのリストは、アプリケーションの登録にあります。

管理

すべてのアプリケーション  
アプリケーション プロキシ  
ユーザー設定  
アプリ起動ツール  
カスタム認証拡張機能 (プレビュー)

セキュリティ  
条件付きアクセス

アプリケーションの名前またはオ... アプリケーションの種類 == エンタープライズ アプリケーション × アプリケーション ID 次の値で始ま

5 個のアプリケーションが見つかりました

名前	オブジェクト ID	アプリケーション ID	ホームページ URL	作成日
BL bluebean-saml-dev				
BL bluebean-saml-sample				
BL bluebean				
TE test				
テス テスト-OIDC				

# Azure SAML情報作成 エンタープライズアプリケーション作成

## 独自のアプリケーションの作成

ホーム > Default Directory | エンタープライズアプリケーション > エンタープライズアプリケーション | すべてのアプリケーション

### Azure AD ギャラリーの参照

①

+ 独自のアプリケーションの作成 フィードバックがある場合

Azure AD アプリ ギャラリーは、シングルサインオン (SSO) と自動ユーザー プロビジョニングの展開と構成を簡単にする数千のアプリのカタログとして、ユーザーをより安全にアプリに接続することができます。ここで独自のアプリケーションを参照または作成してください。他の組織の場合は、次に説明されているプロセスを使用して要求を提出できます。 [この記事](#)。

アプリケーションを検索

シングルサインオン: **すべて** ユーザー アカウントの管理: **All** カテゴリ:

#### クラウド プラットフォーム

Amazon Web Services (AWS)



Google Cloud Platform



Oracle



#### オンプレミスのアプリケーション

**オンプレミスのアプリケーションの追加**

Azure AD アプリケーション プロキシを構成し、セキュアなリモートアクセスを実現します。

**アプリケーション プロキシの詳細情報**

アプリケーション プロキシを使用してオンプレミスのアプリケーションへの安全なリモートアクセスを提供する方法について説明します。

### 独自のアプリケーションの作成

フィードバックがある場合

独自のアプリケーションを開発している場合、アプリケーション プロキシを使用している場合、またはギャラリーにないアプリケーションを統合する必要がある場合は、ここで独自のアプリケーションを作成できます。

②

お使いのアプリの名前は何か?

入力名

アプリケーションでどのような操作を行いたいですか?

- オンプレミスのアプリケーションへのセキュリティで保護されたリモート アクセス用のアプリケーション プロキシを構成します
- アプリケーションを登録して Azure AD と統合します (開発中のアプリ)
- 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)

③

④

作成

# Azure SAML情報作成 シングルサインオン作成

## アプリケーション詳細画面 > シングリサインオン

ホーム > Default Directory | エンタープライズ アプリケーション > エンタープライズ アプリケーション | すべてのアプリケーション > bluebean-saml-sample

### bluebean-saml-sample | シングル サインオン ...

エンタープライズ アプリケーション

<<

- 概要
- デプロイ計画
- 問題の診断と解決

シングルサインオン (SSO) により、組織内のユーザーが、自分が使用しているすべてのアプリケーションに、1つのアカウントでサインインできるようになるため、ユーザーが Azure Active Directory のアプリケーションにサインオンするときのセキュリティと利便性を向上します。一度ユーザーがアプリケーションにログインすると、その資格情報は、そのユーザーがアクセスする必要がある他のすべてのアプリケーションに使用されます。[詳細については、こちらをご覧ください。](#)

#### 管理

- プロパティ
- 所有者
- ロールと管理者
- ユーザーとグループ
- シングル サインオン
- プロビジョニング
- アプリケーション プロキシ
- セルフサービス

### シングル サインオン方式の選択 [判断に役立つヘルプの表示](#)



#### 無効

シングル サインオンが有効になっていません。ユーザーは、[マイ アプリ] からアプリを起動できません。



#### SAML

SAML (Security Assertion Markup Language) プロトコルを使用した、アプリケーションに対する多機能かつセキュリティで保護された認証。

クリックする



#### パスワードベース

Web ブラウザーの拡張機能  
イル アプリを使用したノ  
存と再生。

# Azure SAML情報作成 シングルサインオン作成

SAMLセットアップ画面で「編集」ボタンをクリックする

↑ メタデータ ファイルをアップロードする
 ↶ シングル サインオン モードの変更
 ☰ このアプリケーションをTest
 🔍

## SAML によるシングル サインオンのセットアップ

フェデレーション プロトコルに基づく SSO 実装により、セキュリティ、信頼性、エンド ユーザー エクスペリエンスが向上し、実装容易になります。OpenID Connect または OAuth が使用されていない既存のアプリケーションの場合は、できるだけ SAML シングルサインオンを選択してください。[詳細については、こちらをご覧ください。](#)

以下をお読みください [構成ガイド](#) test を統合するためのヘルプ。

1

### 基本的な SAML 構成

識別子 (エンティティ ID)	<b>必須</b>
応答 URL (Assertion Consumer Service URL)	<b>必須</b>
サインオン URL	省略可能
リレー状態 (省略可能)	省略可能
ログアウト URL (省略可能)	省略可能

 編集

# Azure SAML情報作成 シングルサインオン作成

SAMLセットアップ画面で「編集」ボタンをクリックする

↑ メタデータ ファイルをアップロードする 
 ↶ シングル サインオン モードの変更 
 ☰ このアプリケーションをTest 
 🔍

## SAML によるシングル サインオンのセットアップ

フェデレーション プロトコルに基づく SSO 実装により、セキュリティ、信頼性、エンド ユーザー エクスペリエンスが向上し、実装容易になります。OpenID Connect または OAuth が使用されていない既存のアプリケーションの場合は、できるだけ SAML シングルサインオンを選択してください。[詳細については、こちらをご覧ください。](#)

以下をお読みください [構成ガイド](#) test を統合するためのヘルプ。

1

### 基本的な SAML 構成

識別子 (エンティティ ID)	必須
応答 URL (Assertion Consumer Service URL)	必須
サインオン URL	省略可能
リレー状態 (省略可能)	省略可能
ログアウト URL (省略可能)	省略可能

 編集

# Azure SAML情報作成 シングルサインオン作成

## 識別子の追加ボタンを押します

タープライズ アプリケーション > 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 ...

「 < ↑ メタデータ ファイルをアップロードする ↓ >」

### SAML によるシングル サインオン

フェデレーション プロトコルに基づく SSO 実装に容易になります。OpenID Connect または OAuth がシングルサインオンを選択してください。詳細については、このドキュメントを参照してください。

以下をお読みください [構成ガイド](#) test を統合する

- 1 基本的な SAML 構成
  - 識別子 (エンティティ ID)
  - 応答 URL (Assertion Consumer Service URL)
  - サインオン URL
  - リレー状態 (省略可能)
  - ログアウト URL (省略可能)

- 2 属性とクレーム
  - 手順 1 で必須フィールドに入力してください
  - givenname
  - surname
  - emailaddress

## 基本的な SAML 構成

保存 | フィードバックがある場合

### 識別子 (エンティティ ID) \* ⓘ

Azure Active Directory に対してアプリケーションを識別する一意の ID。この値は、Azure Active Directory テナント内のすべてのアプリケーションで一意である必要があります。既定の識別子は、IDP で開始された SSO の SAML 応答の対象ユーザーになります。

既定

識別子を入力してください

✓ ⓘ 🗑️

識別子の追加

任意の文字列 例: bluebean-saml

### 応答 URL (Assertion Consumer Service URL) \* ⓘ

応答 URL は、アプリケーションが認証トークンを受け取る場所です。これは、SAML では "Assertion Consumer Service" (ACS) とも呼ばれます。

イ... 既定

応答 URL を入力してください

✓ ⓘ 🗑️

応答 URL の追加

認証後BlueBean戻るURLです。

https://{domain}/sso\_auths/saml\_acs

※{domain}は実際に払い出したBlueBeanサーバのドメインに書き換えてください

### サインオン URL (省略可能)

サービス プロバイダーによって開始されたシングル サインオンを実行する場合は、サインオン URL が使用されます。この値は、アプリケーションのサインイン ページの URL です。ID プロバイダーによって開始されたシングル サインオンを実行する

# Azure SAML情報作成 BlueBeanに渡す情報設定

シングルサインオン画面で「属性とクレーム」の編集ボタンをクリックする

[-プライズ アプリケーション](#) > [エンタープライズ アプリケーション](#) | [すべてのアプリケーション](#) > [bluebean-saml-dev](#)

## SAML ベースのサインオン ...

[メタデータ ファイルをアップロードする](#)
[シングル サインオン モードの変更](#)
[このアプリケーションをTest](#)
[フィードバックがある場合](#)

ログアウト URL (省略可能) 省略可能

2

### 属性とクレーム

 編集

givenname	user.givenname
surname	user.surname
name	user.userprincipalname
mail	user.mail
一意のユーザー ID	user.userprincipalname

3

### SAML 証明書

#### トークン署名証明書

 編集

状態	アクティブ
拇印	E725CF5D5C6A7F6F84EE8593F11331CFEC22FB8B
有効期限	2026/6/22 18:10:34
通知用メール	ayechanphyo8@outlook.com
アプリのフェデレーション メタデータ URL	<input type="text" value="https://login.microsoftonline.com/a5dfbeb0-6d7e..."/>

証明書 (Base64) [ダウンロード](#)

証明書 (未加工) [ダウンロード](#)

フェデレーション メタデータ XML [ダウンロード](#)

# Azure SAML情報作成 BlueBeanに渡す情報設定

## 属性とクレーム画面

... > エンタープライズ アプリケーション | すべてのアプリケーション > bluebean-saml-dev | SAML ベースのサインオン > SAML ベースのサインオン >

### 属性とクレーム ...

+ 新しいクレームの追加 + グループ要求を追加する ≡ 列 | フィードバックがある場合

#### 必要な要求

クレーム名	種類	値
一意のユーザー識別子 (名前 ID)	SAML	user.userprincipalname [...]

#### 追加の要求

クレーム名	種類	値
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	SAML	user.givenname ...
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	SAML	user.userprincipalname ...
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	SAML	user.surname ...
mail	SAML	user.mail ...

▽ 詳細設定

# Azure SAML情報作成 BlueBeanに渡す情報設定

識別子の追加ボタンを押します

... > エンタープライズ アプリケーション | すべてのアプリケーション > bluebean-saml-dev | SAML ベースのサインオン > SAML ベースのサインオン

## 要求の管理 ...

 保存  変更の破棄 |  フィードバックがある場合

名前 \*

**mail 必ず mailを記入してください**

名前空間

名前空間の URI を入力してください

▼ 名前の形式を選択する

ソース \*

属性  変換  ディレクトリ スキーマ拡張 (プレビュー)

ソース属性 \*

ドロップダウンから選択するか、定数を入力してください **必ず user.mailを選択してください**

▼ 要求条件

▼ SAML クレームの詳細オプション

## Azure SAML情報作成 証明書発行

シングルサインオン画面で「SAML証明書」の編集ボタンをクリックする

↑ メタデータ ファイルをアップロードする    ↶ シングル サインオン モードの変更    ☰ このアプリケーションをTest    |    👤

3

### SAML 証明書

#### トークン署名証明書

状態

アクティブ

 編集

拇印

E725CF5D5C6A7F6F84EE8593F11331CFEC22FB8B

有効期限

2026/6/22 18:10:34

通知用メール

ayechanphyo8@outlook.com

アプリのフェデレーション メタデータ URL



証明書 (Base64)

[ダウンロード](#)

証明書 (未加工)

[ダウンロード](#)

フェデレーション メタデータ XML

[ダウンロード](#)

# Azure SAML情報作成 証明書発行

PEM証明書をダウンロードする

## SAML 署名証明書



アプリに対して発行される SAML トークンに署名するために Azure AD によって使用される証明書を管理します

保存
 新しい証明書
 証明書のインポート
 | 
 フィードバックがある場合

状態	有効期限	拇印
アクティブ	2026/6/22 18:10:34	E725CF5D5C6A7F6F84EE8593F11331...
署名オプション	SAML 応答とアサーションへの署名	
署名アルゴリズム	SHA-256	
通知の電子メール アドレス	[redacted]@outlook.com	

...をクリック

- 証明書をアクティブにする
- Base64 証明書のダウンロード
- PEM 証明書のダウンロード
- 未加工の証明書のダウンロード
- フェデレーション証明書 XML をダウンロード

# Azure SAML情報作成 テナント情報確認

テナント画面でテナントIDを確認します。BlueBeanに登録が必要です

ホーム > Default Directory | 概要

Azure Active Directory

概要 | 監視中 | プロパティ | 推奨設定 | チュートリアル

テナントの検索

名前	Default Directory	ユーザー	2
テナントID	[REDACTED]	グループ	0
プライマリドメイン	[REDACTED]	アプリケーション	5
ライセンス	Azure AD Free	デバイス	0
ワークロード ライセ...	Azure AD ワークロード Free		

アラート

- MFA Server の非推奨化の予定**  
サービスへの影響を回避するために、2024年9月までに MFA Server から Azure AD Multi-Factor Authentication に移行してください。  
詳細は
- 統合型の認証方法ポリシーに移行する**  
サービスへの影響を避けるために、2024年9月までに認証方法を従来の MFA および SSPR ポリシーから移行してください。  
詳細情報は

# Azure SAML情報作成 ユーザ登録

新規作成されたアプリケーションの詳細画面で「ユーザとグループ」画面でユーザを登録します

※登録されたユーザの emailは必ずBlueBeanの管理者とオペレータのログイン IDと一致していないといけません

ホーム > Default Directory | エンタープライズ アプリケーション > エンタープライズ アプリケーション | すべてのアプリケーション > bluebean-saml-dev

**bluebean-saml-dev** | ユーザーとグループ ...  
エンタープライズ アプリケーション

概要  
デプロイ計画  
問題の診断と解決

管理  
プロパティ  
所有者  
ロールと管理者  
**ユーザーとグループ**  
シングル サインオン  
プロビジョニング  
アプリケーション プロキシ  
セルフサービス

「+ ユーザーまたはグループの追加」

割り当ての編集 | 削除 | 資格情報の更新 | 列 | フ

アプリケーションは、割り当てられたユーザーのマイ アプリ内に表示されます。これを表示しないようにするには、プロ

ここで、アプリケーションのアプリのロールにユーザーとグループを割り当てます。このアプリケーションの新しいアプ

最初の 200 件を表示しています。すべて...

表示名	オブジェクトの種類
<input type="checkbox"/> A1	ユーザー
<input type="checkbox"/> PA	ユーザー
<input type="checkbox"/> エー	ユーザー

# BlueBean情報設定 SSOプロバイダ作成

システム設定 > SSOプロバイダー > 新規SSOプロバイダー作成

新規SSOプロバイダー作成

一覧

名前	Microsoft ▾
SSO認証仕組み	<input checked="" type="radio"/> SAML認証 <input type="radio"/> OIDC認証
テナント ID (*必須)	<input type="text"/> Azureに発行されたテナントID
SAML 証明書 (*必須)	<input type="button" value="ファイルを選択"/> <input type="button" value="選択されていません"/> (*.pem) Azureからダウンロードされた証明書
	<input type="button" value="保存"/>

# BlueBean情報設定

[+ 新規作成](#)  [検索](#) [詳細検索](#)

名前 <small>↑↓</small>	テナント ID	クライアントID	クライアントシークレット	登録日 <small>↑↓</small>	更新日 <small>↑↓</small>
Microsoft	a5d*****	4c3*****	6UM*****	2023-07-13 10:09:22	2023-07-13 10:12:11

1ページ表示行数:  1~1/1行 < 1 >

## BlueBean情報設定 管理者作成

### 新規管理者作成

一覧

ログインID (*必須)	<input type="text"/>
パスワード (*必須)	<input type="password"/> (8文字以上32文字以下、英大文字・英小文字・数字・記号それぞれを1文字以上) 確認のためもう一度入力してください。 <input type="password"/>
名前	<input type="text"/>
フリガナ	<input type="text"/>
タイプ	マネージャー ▼
ステータス ②	<input checked="" type="radio"/> 初期有効 <input type="radio"/> 有効 <input type="radio"/> 無効
	<input type="button" value="保存"/>

# BlueBean情報設定 OP登録

## 新規オペレーター作成

一覧

名前 (*必須)	<input type="text"/>
フリガナ	<input type="text"/>
ログインID (*必須)	<input type="text"/>
パスワード (*必須)	<input type="password"/> (8文字以上32文字以下、英大文字・英小文字・数字・記号それぞれを1文字以上) 確認のためもう一度入力してください。 <input type="password"/>
ステータス ②	<input type="radio"/> 初期有効 <input checked="" type="radio"/> 有効 <input type="radio"/> 無効
所属チーム:	--v
作業モード ②	オンラインモードv ※プレディクティブ(自動発信)作業するには、必ず「オンラインモード」を選択してください。
特定のパソコン限定	<input type="checkbox"/> 有効
備考	<input type="text"/>
	<input type="button" value="保存"/>