

# Entra ID SAML登録手順

## 1. 「ナレフルチャット」のアプリケーション作成

### 1-1. Microsoft Entra管理センターにアクセスし、ログイン

管理センターのURL

<https://entra.microsoft.com/>

### 1-2. 新しいアプリケーションの作成

サイドメニューの

「ID」⇒「アプリケーション」⇒「エンタープライズ アプリケーション」を選択後

「+ 新しいアプリケーション」をクリック

The screenshot shows the Microsoft Entra Management Center interface. The left sidebar contains a navigation menu with the following items: Home, New information, Troubleshooting, Favorites, ID (highlighted with a red box and a '1' in a red circle), Summary, Users, Groups, Devices, Applications (highlighted with a red box and a '2' in a red circle), and Enterprise Applications. The main content area shows the 'Enterprise Applications' page with the title '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' and 'ナレフルチャット'. Below the title, there is a '+ 新しいアプリケーション' button (highlighted with a red box and a '3' in a red circle), a refresh button, and a download button. The page also displays a search bar, a filter for 'アプリケーションの種類', and a message stating '0 個のアプリケーションが見つかりました' (0 applications found).

### 1-3. アプリケーション名の設定

「+ 独自のアプリケーションの作成」を選択後  
アプリ名に「ナレフルチャット」を入力し、「作成」ボタンをクリック  
必要に応じて、以下より「ナレフルチャットロゴ」をご利用ください。  
**ナレフルチャットロゴ**

<https://drive.google.com/file/d/1LwXniircXTgyV408Myu0RkC6XskgOHgJ/view?usp=sharing>

The screenshot shows the Microsoft Entra Admin Center interface. On the left is a navigation menu with categories like 'Home', 'New information', 'Problem diagnosis and solution', 'Favorites', 'ID', 'Summary', 'Users', 'Groups', 'Devices', 'Applications', 'Security', 'Identity Governance', and 'External Identities'. The main content area is titled 'Microsoft Entra アプリ ギャラリーを参照する' and features a '+ 独自のアプリケーションの作成' button circled in red with a '1' callout. Below this is a search bar and a 'シングルサインオン: すべて' filter. The 'クラウド プラットフォーム' section displays logos for Amazon Web Services (AWS), Google Cloud Platform, and SAP. On the right, a modal window titled '独自のアプリケーションの作成' is open. It contains a 'フィードバックがある場合' link, a warning about application development and proxy usage, and a form. The form has a field 'お使いのアプリの名前は何か?' with 'ナレフルチャット' entered, circled in red with a '2' callout. Below the form are three radio button options for application types. At the bottom of the modal is a '作成' button circled in red with a '3' callout.

## 2. シングルサインオンの設定

### 2-1. シングルサインオンの設定画面にアクセス

アプリケーションの作成が完了したら  
アプリケーションの一覧からナレフルチャットを選択し  
「2. シングルサインオンの設定」をクリック

Microsoft Entra 管理センター

ホーム > 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 > Microsoft Entra ギャラリーを参照する >

### ナレフルチャット | 概要

エンタープライズアプリケーション

- 概要
- プロパティ
- 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
  - カスタムセキュリティ属性
- セキュリティ
  - 条件付きアクセス
  - アクセス許可
  - トークンの暗号化
  - アクティビティ
  - サインインログ

#### Getting Started

1. ユーザーとグループの割り当て  
特定のユーザーおよびグループにアプリケーションへのアクセスを付与  
ユーザーとグループの割り当て  
[作業の開始](#)
2. シングルサインオンの設定  
ユーザーが自分の Microsoft Entra 資格情報を使用して、アプリケーションにサインインできるようにする  
[作業の開始](#)
3. ユーザーアカウントのプロビジョニング  
アプリケーションでユーザーアカウントを自動的に作成および削除  
[作業の開始](#)
4. 条件付きアクセス  
カスタマイズ可能なアクセスポリシーによる、このアプリケーションへの安全なアクセス。  
[ポリシーの作成](#)

### 2-2. サインオン方式の選択

シングルサインオン方式の選択画面で「SAML」をクリック

Microsoft Entra 管理センター

ホーム > ナレフルチャット

### ナレフルチャット | 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

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 Microsoft Entra ID のアプリケーションにサインインするときのセキュリティと利便性が向上します。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。](#)

#### 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。
- パスワードベース  
Web ブラウザーの拡張機能またはモバイルアプリを使用したパスワードの保存と再生。
- リンク  
マイアプリや Office 365 アプリケーション起動プログラム内のアプリケーションへのリンク。

## 2-3. SAML構成の編集

「基本的な SAML 構成」の「**編集**」をクリック

ホーム > ナレフルチャット

### ナレフルチャット | SAML ベースのサインオン

エンタープライズ アプリケーション

×

« [↑](#) 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 | ...

🏠 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

#### 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、実装が容易になります。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](#) [📖](#) ナレフルチャット を統合するためのヘルプ。

1

##### 基本的な SAML 構成

[✎](#) 編集

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

## 2-4. SAML構成の設定値を入力

「識別子 (エンティティID)」と「応答URL (Assertion Consumer Service URL)」の項目に以下の内容を入力

項目	内容
識別子 (エンティティID)	urn:amazon:cognito:sp:ap-northeast-1_Mc7etfiH6
応答 URL (Assertion Consumer Service URL)	<a href="https://auth.knowledgeful.jp/saml2/idpresponse">https://auth.knowledgeful.jp/saml2/idpresponse</a>

### 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) \* ⓘ

Microsoft Entra ID 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、Microsoft Entra ID 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

 ⓘ 

[識別子の追加](#)

#### 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 の追加](#)

#### 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場合、このフィールドは不要です。

## 2-5. SAML構成の設定を保存

内容の入力が終わったら、画面左上の「保存」をクリック

### 基本的な SAML 構成

×



フィードバックがある場合

識別子 (エンティティ ID) \* ⓘ

Microsoft Entra ID 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、Microsoft Entra ID 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

urn:amazon:cognito:sp:ap-northeast-1\_Mc7etfiH6



識別子の追加

## 3. 連携情報の送信

### 3-1. 必要な情報のコピー

「SAML 証明書」の「アプリのフェデレーション メタデータ URL」をコピー

ホーム > 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 > ナレフルチャット

### ナレフルチャット | SAML ベースのサインオン

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  
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  
カスタムセキュリティ属性  
セキュリティ  
条件付きアクセス  
アクセス許可  
トークンの暗号化  
アクティビティ  
サインインログ

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		編集
状態		
拇印		
有効期限		
通知 URL		
アプリのフェデレーション メタデータ URL	<a href="https://login.microsoftonline.com/345652e...">https://login.microsoftonline.com/345652e...</a>	
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

#### 4 ナレフルチャットのセットアップ

Microsoft Entra ID とリンクするアプリケーションを構成する必要があります。

ログイン URL	
Microsoft Entra 識別子	
ログアウト URL	

### 3-2. フォーム送信

コピーしたURLを、以下URLのGoogleフォームより送信

**フォームURL**

<https://forms.gle/y3SRJsoDvXs4r4JWA>

## 4. 利用ユーザーの追加

アプリ作成直後は、SAML認証を利用するユーザーが一人も追加されていないため必要に応じて、ユーザーを以下手順で追加してください

### 4-1. ユーザーの追加

サイドメニューの「ユーザーとグループ」をクリックし  
「+ ユーザーまたはグループの追加」をクリック

ホーム > ナレフルチャット

ナレフルチャット | 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

カスタムセキュリティ属性

ユーザーとグループ

アプリケーションの割り当てが見つかりませんでした

ここで、アプリケーションのアプリ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に新しいアプリロールを作成するには、[アプリケーションの登録](#)を使用します。

最初の 200 件が表示され、すべてのユーザ...

ユーザーまたはグループの追加

割り当ての編集

割り当ての削除

資格情報の更新

最新の情報に更新

ビューの管理

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、プロパティの中で「ユーザーに表示しますか?」を「いいえ」に設定します。

表示名

オブジェクトの種類

### 4-2. ユーザーの選択画面へアクセス

「ユーザー」の下にある「**選択されていません**」のリンクをクリック

ホーム > ナレフルチャット | ユーザーとグループ >

割り当ての追加 ...

ナレフルチャット

お客様の Active Directory プランレベルでは、グループを割り当てることができません。個々のユーザーをアプリケーションに割り当てることはできます。

ユーザー

**選択されていません**

ロールを選択してください

User

### 4-3. 追加するユーザーを選択

表示されたユーザー選択ウィンドウから

SAML認証を利用できるようにするユーザーもしくはグループを選択し、「**選択**」ボタンをクリック

The screenshot shows a user selection window titled "ユーザー" (Users). At the top, there is a search bar with a message: "探しているものが見つからない場合は、フィルターの変更または追加をお試しください。" (If you can't find what you're looking for, try changing or adding filters). Below the search bar, it says "5件の結果が見つかりました" (5 results found). There are two filter tabs: "すべて" (All) and "ユーザー" (Users), with "ユーザー" being the active tab. A table lists the search results with columns for "名前" (Name), "種類" (Type), and "詳細" (Details). The first row is selected, indicated by a blue checkmark in a box. A red circle with the number "1" is placed over the "名前" column header. Below the table, there are two buttons: "割り当て" (Assign) and "選択" (Select). A red circle with the number "2" is placed over the "選択" button.

	名前	種類	詳細
<input checked="" type="checkbox"/>	[User Icon]	ユーザー	[User Name]
<input type="checkbox"/>	[User Icon]	ユーザー	[User Name]
<input type="checkbox"/>	[User Icon]	ユーザー	[User Name]
<input type="checkbox"/>	[User Icon]	ユーザー	[User Name]
<input type="checkbox"/>	[User Icon]	ユーザー	[User Name]

## 4-4. 選択したユーザーを追加

元の画面に戻ってくるので、「**割り当て**」ボタンをクリック

[ホーム](#) > [ナレフルチャット | ユーザーとグループ](#) >

### 割り当ての追加 ...

ナレフルチャット

 お客様の Active Directory プランレベルでは、グループを割り当てるできません。個々のユーザーをアプリケーションに割り当てることはできます。

ユーザー

1 人のユーザーが選択されました。

ロールを選択してください

User

**割り当て**

#### 注意事項

グループを追加する際は、ユーザーが直接所属しているグループを選択してください。子グループを含む親グループを選択すると、エラーになる場合があります。