

まなびポケット

～外部IdP連携オプションをお申し込みの方対象～

Microsoft Entra ID(旧Azure AD) 連携ログイン設定マニュアル

2024.9.20

NTTコミュニケーションズ

Microsoft Entra ID連携ログインとは？

※「Microsoft Azure AD」から「Microsoft Entra ID」に名称が変更されております。

■ まなびポケット Microsoft Entra ID連携ログインとは？

まなびポケットをご利用の際に、Microsoft Entra IDアカウントでログインすることです。

■ Microsoft Entra ID連携ログインをするためには？

Microsoft Entra ID 連携ログインを希望の学校は、本マニュアルの手順でのお申し込みと設定が必要です。お申し込みの際には、事前にMicrosoft Entra ID アカウントを取得いただく必要があります。

■ Microsoft Entra ID 連携ログインをすると？

まなびポケットにログインする際にMicrosoft Entra ID アカウントを使用できるようになります。

設定前の確認

以下のいずれかに該当する場合はP.21の注意事項をご確認ください。

- ・複数市区町村でMicrosoft Entra IDを共有利用している場合
- ・Microsoft Entra ID連携をお申し込み済みの自治体/学校法人が学校を追加お申し込みする場合

※アプリの再作成やアプリを複数作成するとメタデータが更新されてしまい、Microsoft Entra ID連携を設定済の学校でまなびポケットにログインができなくなってしまうため、ご注意ください。

目次

Microsoft Entra ID 連携ログインとは？ (P.2)

設定前の確認 (P.2)

目次 (P.3)

登録の流れ (P.4)

1. Azure Portalの設定 (P.5～16)

1.1 Azure Portalの設定 (P.5～16)

2. お申し込み (P.17)

2.1 申込書とフェデレーション メタデータ XMLの送付 (P.17)

3. まなびポケットにログイン (P.18～20)

3.1 まなびポケット サービスデスクから開通案内の受領 (P.18)

3.2 学校管理者でログイン (P.18～20)

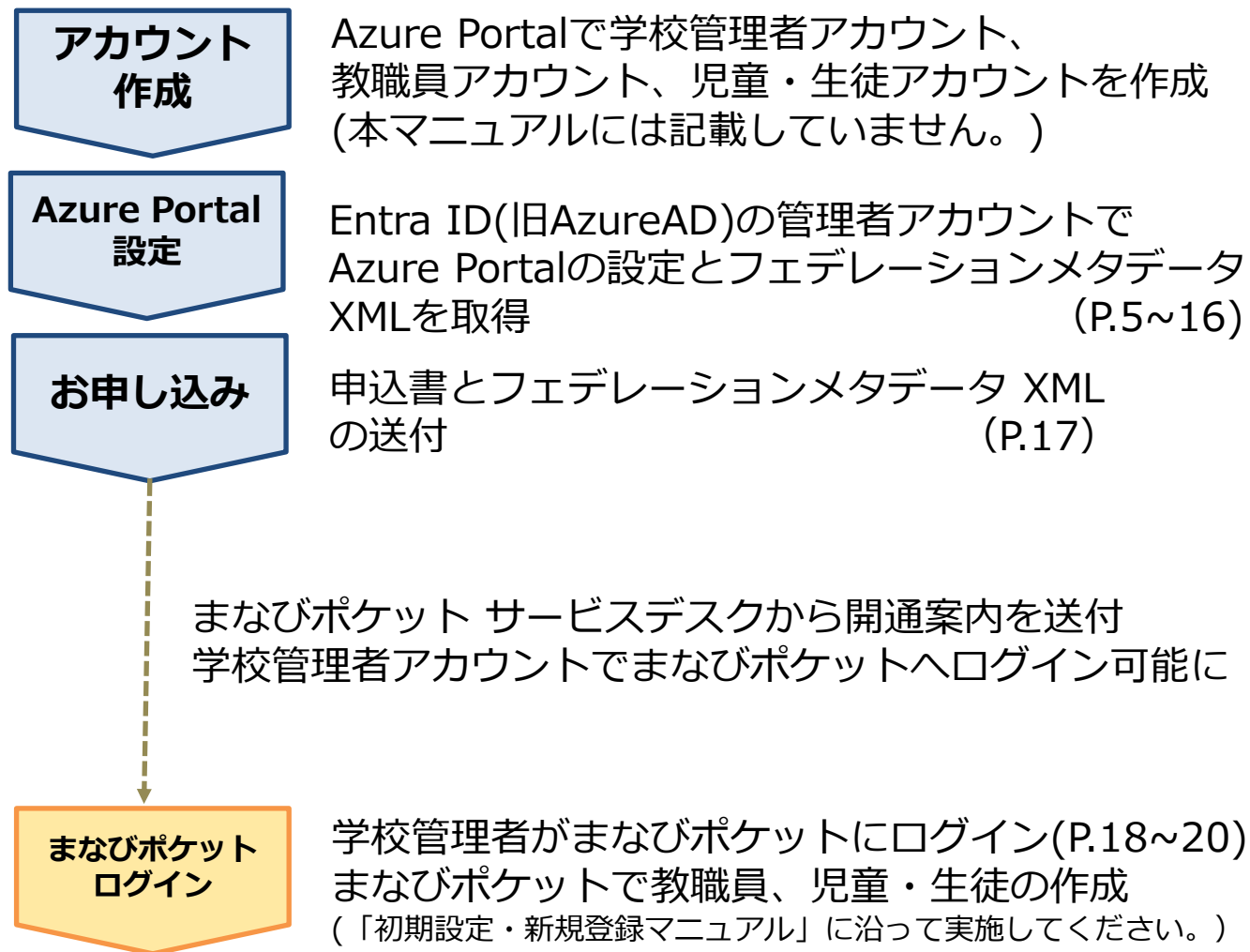
4. 注意事項 (P.21)

■改訂履歴 (P.23)

登録の流れ

初回登録の流れは下記の通りです。

Azure Portalでの学校管理者アカウントや教職員、児童・生徒アカウントの作成については本マニュアルに記載していません。事前に作成をお願い致します。



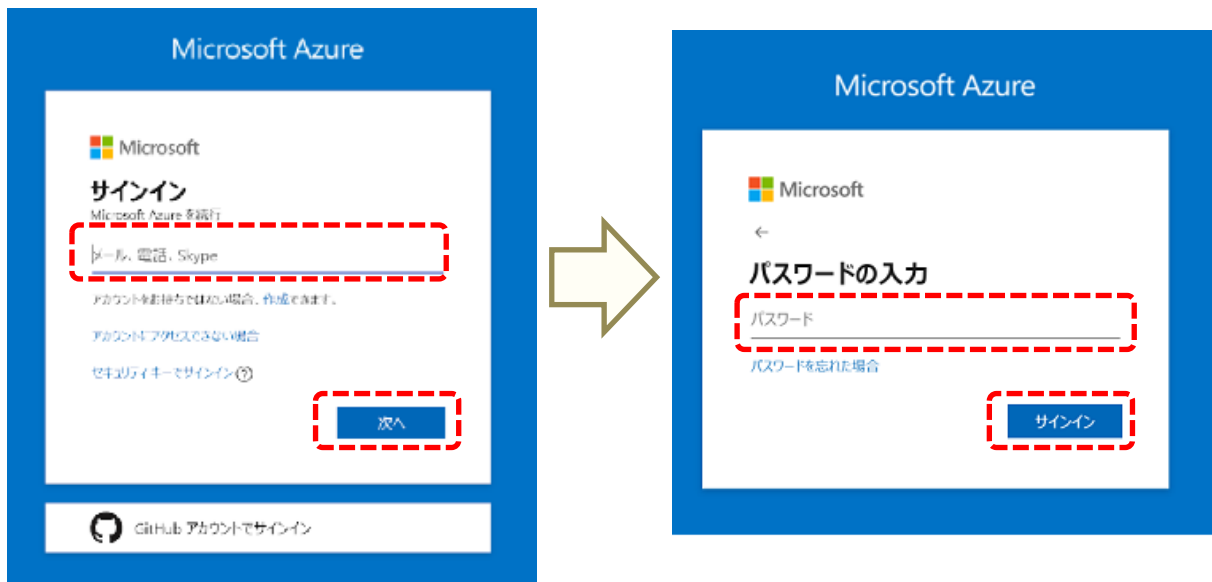
1. Azure Portalの設定

Microsoft Entra ID連携(旧Azure AD)ログインをご利用いただくためには、お申し込み時に、Azure Portalの設定と、「申込書」と「フェデレーション メタデータ XML」の2つを送付いただく必要があります。
この項目では、Azure Portalの設定について説明します。

「フェデレーション メタデータ XML」は、**【1.1 Azure Portal】** の設定のステップ14で取得します。

1.1 Azure Portalの設定（所要時間目安：10分）

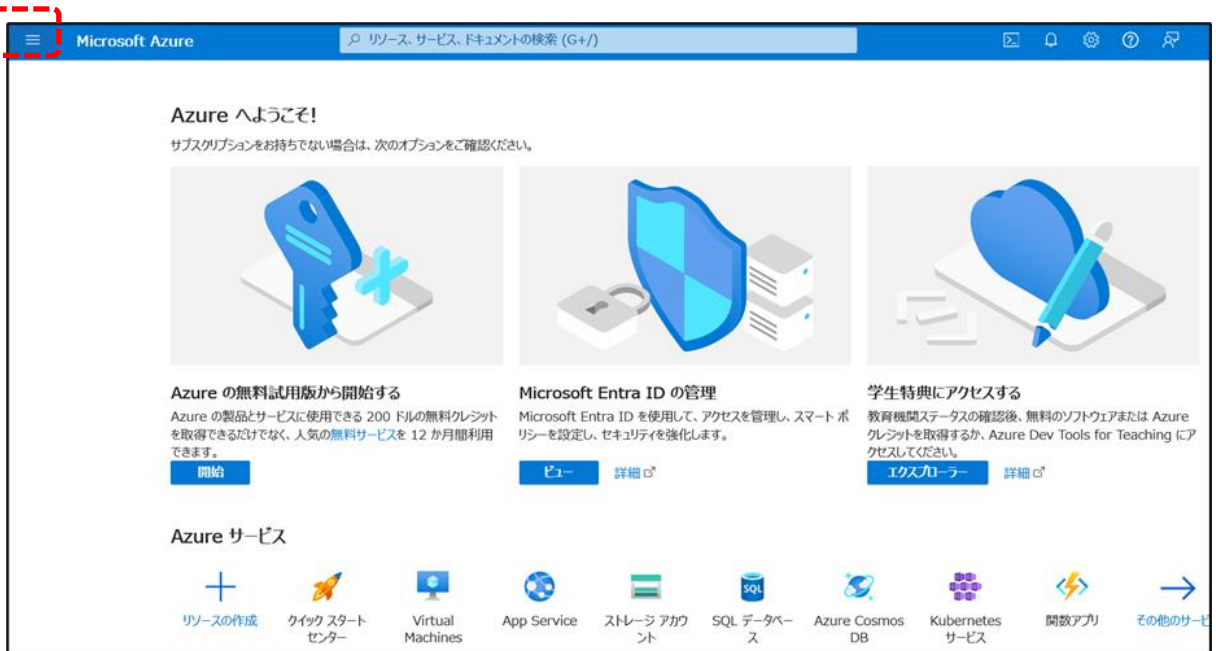
●ステップ1：Azure Portalへログイン




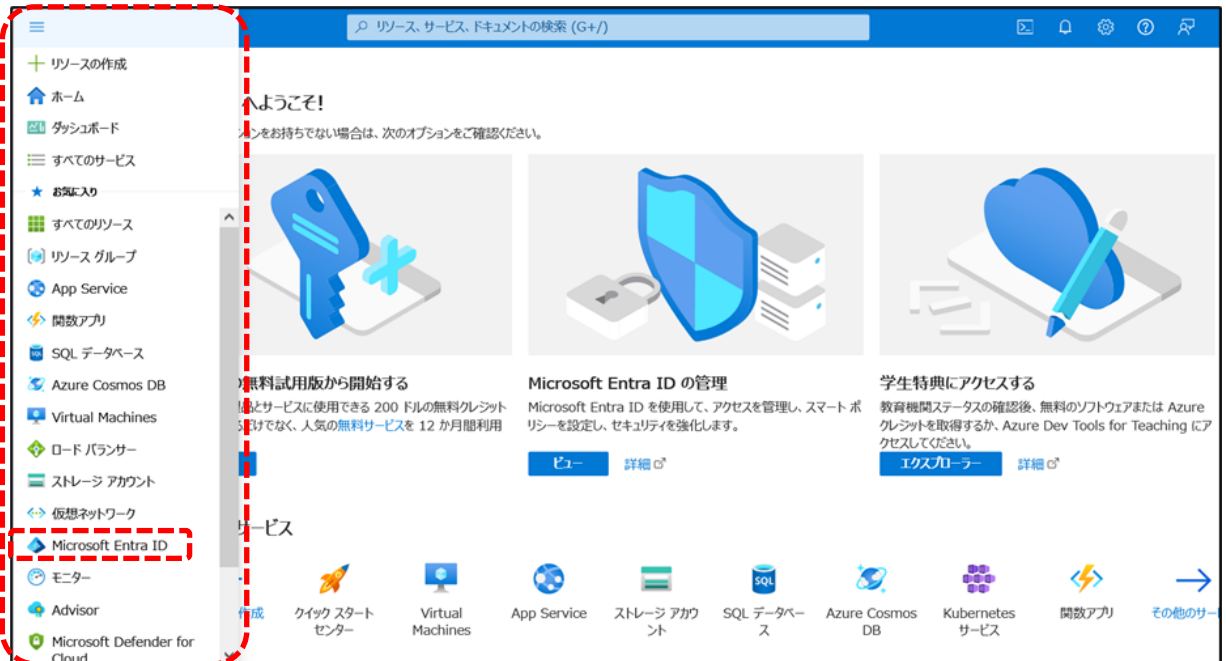
<https://portal.azure.com/>へアクセスしてください。
AzureADの管理者アカウントのメールアドレスとパスワードを入力し、ログインしてください。

1. Azure Portalの設定

●ステップ2：メニューを表示



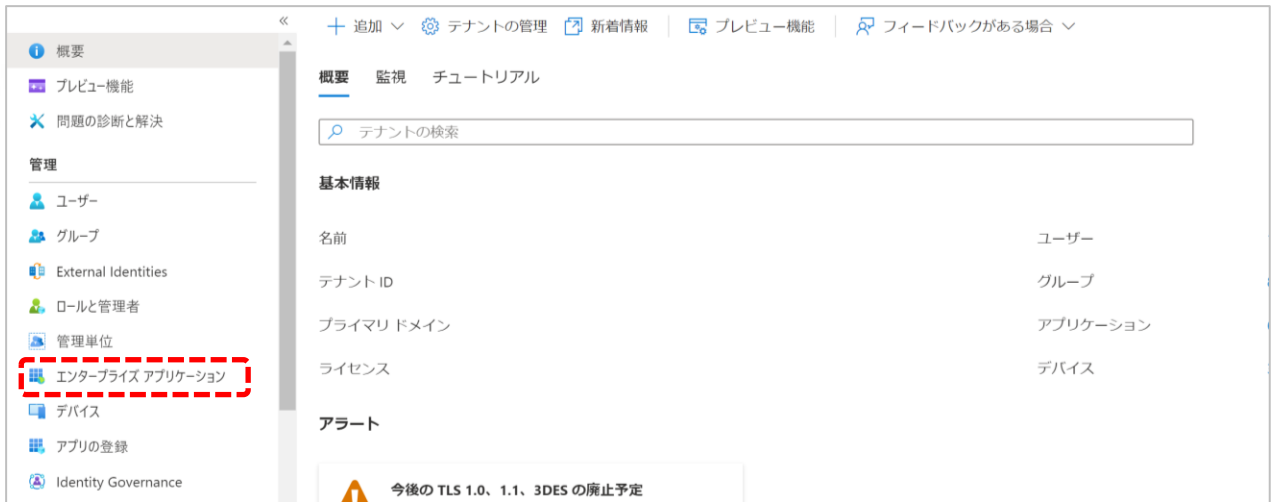
ログイン後上記のような画面が表示されますので、
左上のハンバーガーボタン  をクリックしてください。



左側にメニューが表示されますので、その中から「Microsoft Entra ID(旧Azure Active Directory)」をクリックしてください。

1. Azure Portalの設定

●ステップ3：「エンタープライズアプリケーション」をクリック



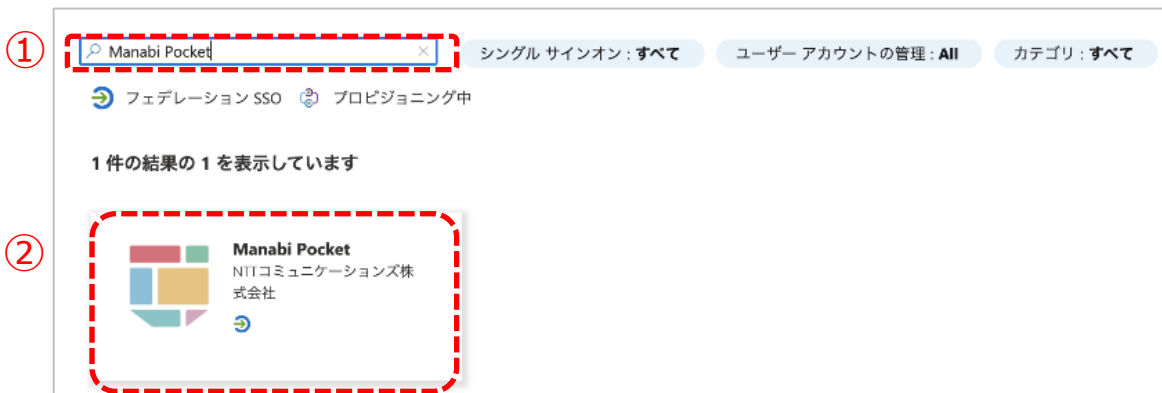
左のメニューの中の「エンタープライズアプリケーション」をクリックしてください。

●ステップ4：「+新しいアプリケーション」をクリック



「+新しいアプリケーション」をクリックしてください。

●ステップ5：まなびポケットのアプリケーションを追加



①の検索窓に「Manabi Pocket」と入力してください。

②「Manabi Pocket」のアプリケーションが表示されますので、クリックしてください。

1. Azure Portalの設定

●ステップ6：「作成」をクリック

ホーム > エンタープライズ アプリケーション > Azure AD ギャラリーの参照 ...

Azure AD ギャラリーの参照 ...

+ 独自のアプリケーションの作成 ○ 新しいギャラリー アプリを要求する | フィードバックがある場合

1 改良された新しいアプリ ギャラリー エクスプレィエンスをご利用いただけます。従来のアプリ ギャラリー エクスプレィエンスに戻すには、こちらをクリックしてください。

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テゴリです。アプリを閲覧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。

Manabi Pocket

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: 3

フェデレーション SSO プロビジョニング中

1 件の結果の 1 を表示しています

Manabi Pocket
NTTコミュニケーションズ株式会社

Manabi Pocket

名前 * ○
Manabi Pocket

発行元 ○
NTTコミュニケーションズ株式会社

プロビジョニング ○
自動プロビジョニングはサポートされていません

シングル サインオン モード ○ URL ○
SAML ベースのサインオン リンクされたサインオン
https://www.ntt.com/index.htm

Manabi Pocket 統合の手順に関するチュートリアルを読む

まなびポケットは、デジタル教材とコミュニケーション機能を利用することができるプラットフォームです。クラウドサービスのため、インターネットが利用できる環境があれば、いつでもどこでも利用することができます。デジタル教材は、無料と有料のものがあり、無料のものだけでは、初期費用/月額費用ともに完全無料ではないポケットを使うことができます。

作成

①の名前欄に「Manabi Pocket」と入力されていることを確認して、下部にある②の「作成」をクリックしてください。

●ステップ7：「2. シングルサインオンの設定」をクリック

ホーム > エンタープライズ アプリケーション > Azure AD ギャラリーの参照 > Manabi Pocket | 概要 ...

Manabi Pocket | 概要 ...

Manabi Pocket

概要

デプロイ計画

管理

プロパティ

所有者

ロールと管理者 (プレビュー)

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

セルフサービス

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

使用状況と分析情報

プロパティ

名前 ○
Manabi Pocket

アプリケーション ID ○
84b56b0a-d182-468f-bcb8-...

オブジェクト ID ○
da7858c0-9eec-4549-be52-...

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

2. シングル サインオンの設定
ユーザーが自分の Azure AD 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 アカウントの作成が必要
詳細情報

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

アプリケーションの追加
アプリケーション Manabi Pocket が正常に追加されました

①ステップ6が正しく実行されると「アプリケーション Manabi Pocketが正しく追加されました」と表示されます。

②「シングルサインオンの設定」をクリックしてください。

1. Azure Portalの設定

●ステップ8：「SAML」をクリック

ホーム > エンタープライズ アプリケーション > Azure AD ギャラリーの参照 > Manabi Pocket

Manabi Pocket | 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 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 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。	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。
--	---	---

セキュリティ

「シングルサインオン方式の選択」という画面が表示されるので、「SAML」をクリックしてください。

●ステップ9：「基本的なSAML構成」の「編集」をクリック

ホーム > エンタープライズ アプリケーション > Azure AD ギャラリーの参照 > Manabi Pocket >

Manabi Pocket | 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

管理

プロパティ

所有者

ロールと管理者 (プレビュー)

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

セルフサービス

カスタム セキュリティ属性 (プレビュー)

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

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](#) Manabi Pocket 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
	ログアウト URL	省略可能

「基本的なSAML構成」の項目の中の「編集」をクリックしてください。

1. Azure Portalの設定

●ステップ10：「基本的なSAML構成」を設定

①右側に画面が表示されるので、「識別子の追加」と「応答URLの追加」をクリックしてください。

②右側に画面が表示されるので、「識別子(エンティティID)」と「応答URL」に下記のURLを入力してください。

識別子：<https://idp1.ed-cl.com/idpop/provider>

応答URL：https://idp1.ed-cl.com/idpop/assertion_post

③「保存」をクリックしてください。

1. Azure Portalの設定

※ステップ10「基本的なSAML構成」を設定時の注意点

(注意)

「識別子 (エンティティ)」と「応答URL」の欄には、ステップ10に記載のURLのみ設定されている状態にしてください。

○正しい設定

識別子 (エンティティ ID) * ⓘ
既定の識別子は、IDP-initiated SSO の SAML 応答の対象となります

既定

https://idp1.ed-cl.com/idpop/provider ✓


パターン: https://idp1.ed-cl.com/*

応答 URL (Assertion Consumer Service URL) * ⓘ
既定の応答 URL は、IDP-initiated SSO の SAML 応答の宛先となります

既定


https://idp1.ed-cl.com/idpop/assertion_post ✓

パターン: https://<SERVER-NAME>.ed-cl.com/<TENANTID>/idp/assertion_post

ステップ10実施時に、「識別子 (エンティティID)」と「応答URL」の欄にステップ10に記載したURL以外のURLが設定されている場合は、①ステップ10に記載のURLを入力した後、②  ゴミ箱マークをクリックして、その他のURLを削除してください。

識別子 (エンティティ ID) * ⓘ
既定の識別子は、IDP-initiated SSO の SAML 応答の対象となります

既定

https://idp1.ed-cl.com/* ✓ ⓘ  ②

① https://idp1.ed-cl.com/idpop/provider ✓

パターン: https://idp1.ed-cl.com/*

応答 URL (Assertion Consumer Service URL) * ⓘ
既定の応答 URL は、IDP-initiated SSO の SAML 応答の宛先となります

既定

① https://idp1.ed-cl.com/idpop/assertion_post ✓

パターン: https://<SERVER-NAME>.ed-cl.com/<TENANTID>/idp/assertion_post

1. Azure Portalの設定

●ステップ11：「基本的なSAML構成」の設定の完了



ステップ10が完了すると、画面右上に「シングルサインオン構成が正常に保存されました」と表示されます。



「Manabi PocketでシングルサインオンをTest」という画面が表示されることがありますが、まだ設定が完了していないため「いいえ、後でtestします」をクリックしてください。

続いて、「新しい証明書」の追加および「フェデレーションメタデータXML」のダウンロードを行います。ステップ12に進んでください。

1. Azure Portalの設定

●ステップ12：「新しい証明書」を追加

Manabi Pocket | 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

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](#) Manabi Pocket を統合するためのヘルプ。

- 1 基本的な SAML 構成
- 2 属性とクレーム
- 3 SAML 署名証明書

項目	値
識別子 (エンティティ ID)	https://idp.1.ed-cl.com/idpop/provider
応答 URL (Assertion Consumer Service URL)	https://idp.1.ed-cl.com/idpop/assertion_post
サインオン URL	省略可能
リレー状態	省略可能
ログアウト URL	省略可能

属性とクレーム	値
givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
一意のユーザー ID	user.userprincipalname

SAML 署名証明書	状態	アクティブ
状態	アクティブ	F5C15EDA95F63534F8E467A24D71DA0DB659DC4A
拇印		703413272-10-31-27

① 「SAML署名証明書」の項目の中の「編集」をクリックしてください。

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	2025/6/21 12:10:00	DE7525DA773BEA9D22E2F0574E287C7FF6B2F275

署名オプション: SAML アサーションへの署名

署名アルゴリズム: SHA-256

② 「新しい証明書」をクリックしてください。

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	2025/6/21 12:10:00	DE7525DA773BEA9D22E2F0574E287C7FF6B2F275
N/A	2025/6/21 15:24:17	保存時に表示されます

署名オプション: SAML アサーションへの署名

署名アルゴリズム: SHA-256

③ 「保存」をクリックしてください。

※クリック後、状態「N/A」が「非アクティブ」となったことを確認してください。

1. Azure Portalの設定

●ステップ13：追加した証明書を「アクティブ」に設定



①ステップ12で追加した証明書の「…」をクリックしてください。



②「証明書をアクティブにする」をクリックしてください。



③「はい」をクリックしてください。



④ステップ12で追加した証明書の状態が「アクティブ」になっていることを確認してください。

1. Azure Portalの設定

⚠ 注意

右図のように証明書が3つ以上存在している場合、有効期限が古く「非アクティブ」になっている証明書を削除してください。

※1 証明書は2つまでになるようにしてください。

※2 「アクティブ」になっている証明書は削除しないでください。

<手順>

- (a) 「…」をクリック
- (b) 「証明書の削除」をクリック
- (c) 画面右上に「証明書が正常に削除されました」と表示されたら削除完了



●ステップ14：「フェデレーションメタデータXML」のダウンロード



- ① アクティブになったことが確認できたら、「x」をクリックしてください。



- ② 「フェデレーションメタデータXML」という項目の横の「ダウンロード」をクリックしてください。ダウンロードしたファイルは保存しておいてください。

ここで取得した「フェデレーションメタデータXML」は、**【2. お申し込み】**で利用します。

1. Azure Portalの設定

●ステップ15：証明書の有効期限の確認



SAML署名証明書の中に「有効期限」が記載されているので記載された有効期限にご注意ください。

●ステップ16：ユーザーの割り当ての変更



- ①左のメニューから「プロパティ」をクリックしてください。
- ②「割り当てが必要ですか?」の箇所「いいえ」を選択してください。
- ③「保存」をクリックしてください。

以上で【1. Azure Portalの設定】は完了です。

2. お申し込み

2.1 申込書とフェデレーションメタデータXMLの送付 (所要時間目安：5分)

下記の2つの資料をセットにしてお申し込みください。

- 申込書

- ※「エクセルの原本」と「印または署名したエクセルの申込書シートをPDFにしたもの」を送付してください。

- ※必ず外部IdP連携に関する項目に記入をしてください。

- 1.1 で取得した「フェデレーションメタデータXML」のファイル

お申し込み先は下記の通りです。

お申し込みパッケージ	お申し込み先
無料お申し込み（新規）	https://manabipocket.ed-cl.com/input-select （Webフォーム）
有料お申し込み（新規）	営業担当者に送付
GIGAスクールパック	営業担当者に送付
外部IdP連携への変更 お申し込み	https://manabipocket.ed-cl.com/input-select （Webフォーム）

以上で【2.お申し込み】は完了です。

3. まなびポケットにログイン

3.1 まなびポケット サービスデスクから開通案内の受領

まなびポケット サービスデスクから開通案内をお送りします。
開通案内が届きましたら、記載の学校コードを利用して、まなびポケットにログインすることができます。

3.2 学校管理者でログイン

ログインに必要な設定は完了しましたので、
Azureアカウントでまなびポケットにログインします。
ログインには3つのステップが存在します。

●ステップ1：ログイン画面へアクセスする



まなびポケットのトップページで、「ログイン」をクリックしてください。

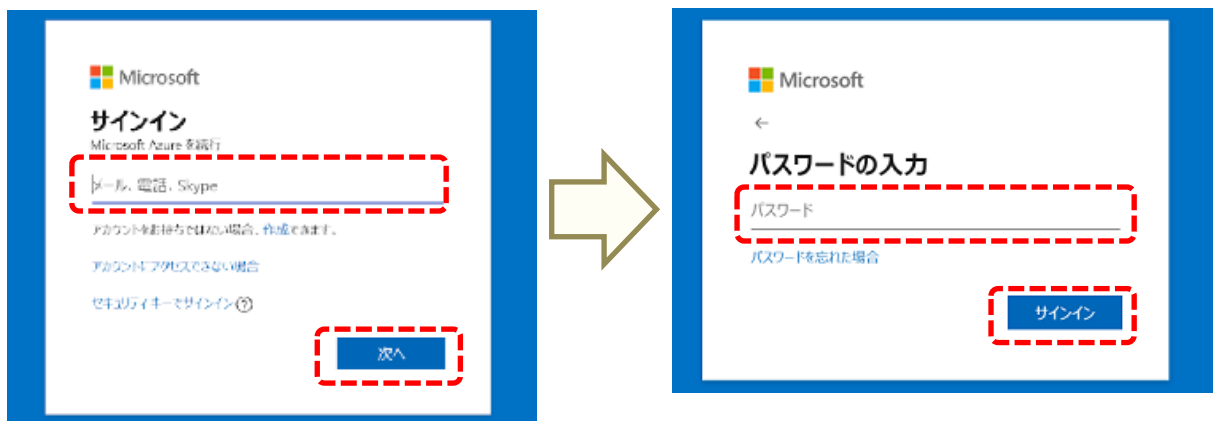
3. まなびポケットにログイン

●ステップ2：学校コードを入力する



「学校コード」の入力欄に、開通案内情報に記載の学校コードを入力してください。
入力したら「次へ」をクリックしてください。

●ステップ3：Azureアカウントでログインする



Microsoftのサインイン画面が表示されますので、
学校管理者（申込書に記載したアカウント）のメールアドレスを入力
してください。続いてパスワードも入力してください。

※学校コードやID、パスワードは、初回ログイン以降は一定期間入力せずにログイン
できるようになりますが、ご利用の環境により異なります。

以上で【3. まなびポケットにログイン】は完了です。

3. まなびポケットにログイン

以上でMicrosoft Entra ID連携(旧Azure AD)のログイン設定は完了です。

続いて下記を参考にまなびポケットの教職員、児童・生徒のユーザー情報を作成/更新してください。

▽まなびポケットの初期設定・新規登録を未実施の場合

「[初期設定・新規登録マニュアル](#)」を参考にまなびポケットの教職員、児童・生徒のユーザー情報を作成してください。

※マニュアルおよびユーザー情報登録シートの外部IdP連携に関する設定作業を実施してください。

▽まなびポケットの初期設定・新規登録を実施済の場合

「[アカウント情報変更マニュアル](#)」を参考にまなびポケットの教職員、児童・生徒のユーザー情報「外部認証ID」を更新してください。

4. 注意事項

- ・ 複数市区町村でMicrosoft Entra ID連携(旧Azure AD)を共有利用している場合
 - ・ Microsoft Entra ID連携(旧Azure AD)をお申し込み済みの自治体/学校法人が学校を追加お申し込みする場合
- 上記いずれかに該当する場合、以下の手順で作業してください。

▼手順

①ステップ1～ステップ3 (P.5～7) を実施

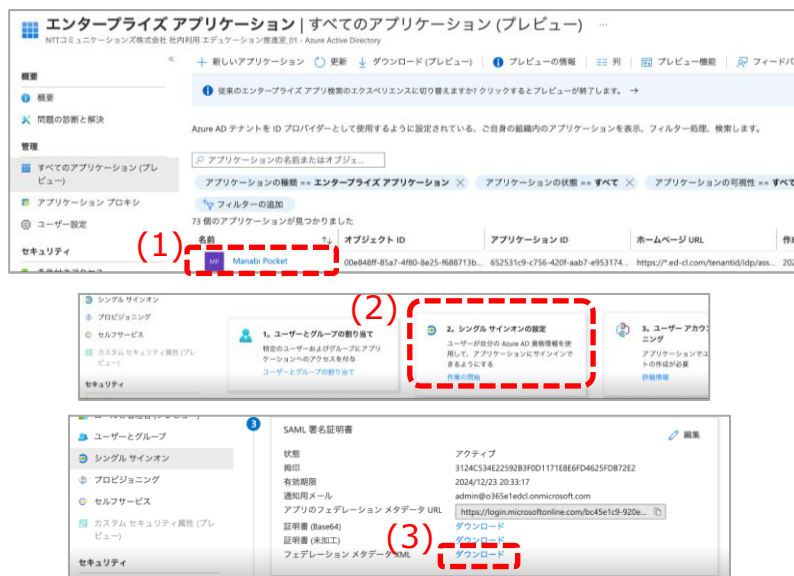
②「フェデレーションメタデータXML」のダウンロード

下記内容で「Manabi Pocket」のアプリがすでに作成済みの場合、「フェデレーションメタデータXML」をダウンロード(アプリの再作成は不要となります。)

識別子 : <https://idp1.ed-cl.com/idpop/provider>

応答URL : https://idp1.ed-cl.com/idpop/assertion_post

- (1) 「Manabi Pocket」をクリック
- (2) 「シングルサインオンの設定」をクリック
- (3) フェデレーションメタデータXMLの「ダウンロード」をクリック



③P.17 申込書と②で取得した「フェデレーションメタデータXML」の送付

サービスデスクに申込書と「フェデレーションメタデータXML」を送付

※アプリの再作成やアプリを複数作成するとメタデータが更新されてしまい、Entra ID連携(旧Azure AD)を設定済の学校でまなびポケットにログインができなくなってしまうため、ご注意ください。

※フェデレーション メタデータ XMLは「メタデータ」や「認証データ」「IdP認証データ」「外部認証データ」などと呼ぶことがあります。

本マニュアルに記載している画面イメージは2024/3/22時点のものです。画面イメージはMicrosoft社によって変更される場合があります。

また、本マニュアルの内容は2024/3/22時点でNTTコミュニケーションズが確認した動作をもとに作成しております。AzureについてはMicrosoft社が提供する機能であり、NTTコミュニケーションズが動作等を保障するものではありませんのでご了承ください。

Azureに関する詳細についてはMicrosoft社へご確認お願いいたします。

本マニュアルに関するお問い合わせ先（Webフォーム）
<https://manabipocket.ed-cl.com/support/contact/>

■ 改訂履歴

※文言修正等の、軽微な修正は改訂履歴に含まない。

改訂年月日	改訂内容
2023年12月12日	改訂履歴追加
2024年4月1日	Entra ID連携（旧Azure AD）名称変更に伴う修正
2024年9月20日	申し込み先の修正