Manager
SSO・ディレクトリ連携設定マニュアル

2026/08/13　更新

はじめに

- 本書はManagerでMicrosoft Entra IDとのシングルサインオン（SSO）およびディレクトリ連携の設定に関するマニュアルです。
- 本設定には**Managerは全体管理者、Microsoft Entra IDは管理者相当の権限**を持つアカウントが必要です。
- 設定の多くはMicrosoft Entra IDとManagerを行き来するため、両方の画面を開いた状態で作業してください。
- 連携失敗を防ぐため、設定は**必ず本書の手順通りに行ってください。**

もくじ

SSO利用

1	既にSSOをご利用の方	･･･04
2	SSO設定方法	･･･07
3	Managerの初期設定	･･･10
4	Microsoft Entra IDの設定	･･･14
5	Managerの設定	･･･27
6	SSOの動作テスト	･･･32

ディレクトリ連携

7	ディレクトリ連携	･･･35
8	Managerの設定	･･･38
9	Microsoft Entra IDの設定	･･･41
10	動作確認	･･･67
11	ディレクトリ連携で取り込まれたユーザー・チームについて	･･･72
12	ディレクトリ連携における運用時の留意事項	･･･74
13	ログイン設定	･･･76
14	SSO必須化時ログイン情報でのログイン	･･･78
15	運用時の留意事項	･･･83
16	Appendix	･･･86

既にSSOをご利用の方

2026年７月以降の変更点

ログイン設定の変更点

- SSO設定が有効 / 無効の二段階から、
  SSO無効 / SSO有効(ログイン情報利用可) / SSO有効(必須)の三段階に変わっています。
- すでに有効をご利用頂いていた方は以降、**SSO有効(必須)の設定** となっています。
- **パスワード利用のユーザー**は**SSO必須化対象外ユーザー一覧**に入っています。



旧Managerの画面



新Managerの画面

推奨はしませんが、SSOログインと、ログイン情報(メールアドレスとパスワード)を併用して使う事も設定可能です。

【新機能】SSO必須化対象外ユーザー一覧について

- パスワード利用のユーザー、または2026年7月以前一度もSSOログインをしていないユーザーは**SSO必須化対象外ユーザー一覧**に入っています。
  - このリストに入っているユーザーはSSO有効(必須化)の設定でもログイン情報(メールアドレスとパスワード)でのログインができます。
  - SSO必須化対象外ユーザー一覧の詳しい使い方（ページに移動します）



SSO必須化対象外ユーザー一覧

SSO設定方法

前提

- シングルサインオン（SSO）のみを利用する場合
  - 本マニュアルの35ページまでの手順を完了してください。

- ディレクトリ連携も利用する場合
  - ディレクトリ連携にはSSO設定（11～35ページ）が必須です。SSO設定完了後、36ページ以降の設定を実施してください。

設定の流れ

シングルサインオンの設定は以下の手順で行います。

1. Managerの初期設定
    1.1. Managerに「全体管理者」のアカウントでログイン
    1.2. 管理設定 > SSO設定タブから「企業別認証ID」を発行

2. Microsoft Entra IDの設定
    2.1. Microsoft Azureに管理者アカウントでログインし、Microsoft Entra ID設定画面へ
    2.2. エンタープライズアプリケーションの作成
    2.3. シングルサインオンの設定
    2.4. ユーザーの割り当て

3. Managerの設定
    3.1. Microsoft Entra ID側情報の入力
    3.2. SAML署名証明書のアップロード / Entra IDの入力
    3.3. SSO有効化

4. SSOの動作テスト

Managerの初期設定

Managerにログイン

- 以下のURLにアクセスし、Managerにログインしてください。
- ログイン後、画面右上のアイコンをクリックし、赤枠部が「全体管理者」であることを確認してください。
  - **※「管理者」や「部門管理者」となっている場合、12ページ以降の手順が行えません。**





企業別認証IDの発行

- サイドメニューの管理設定からSSO・ディレクトリ連携設定タブを選択し、「IdP連携を設定」ボタンをクリックします。
- 確認のダイアログが表示されるので「発行」ボタンをクリックします。



初期設定の完了

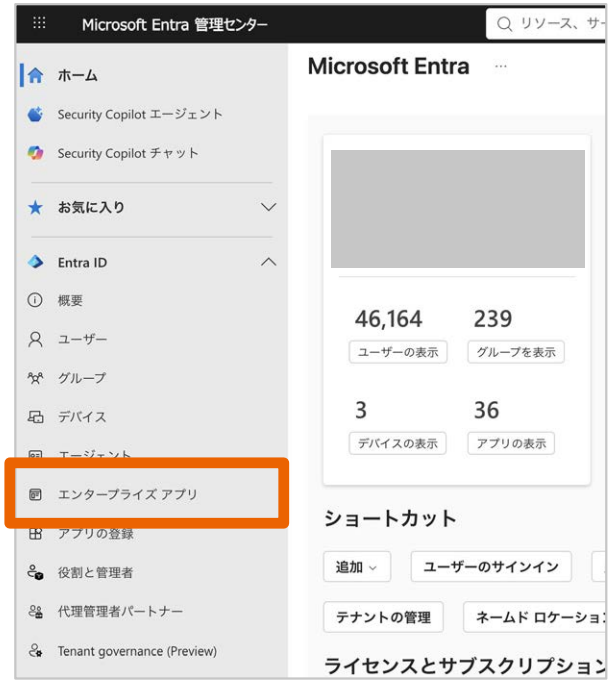
- 以下の画面が表示されたらManagerのシングルサインオン初期設定は完了です。
- この画面は以降の手順で参照するので**画面を閉じずに**次の手順に進んでください。



Microsoft Entra IDの設定

Microsoft Azureにログイン

- 以下のURLにアクセスし、ログインしてください。
  - https://entra.microsoft.com/#home
- 左のメニューから「エンタープライズ アプリ」をクリックします。



エンタープライズアプリケーションの作成（1/3）

- 画面上部の「新しいアプリケーション」をクリックします。



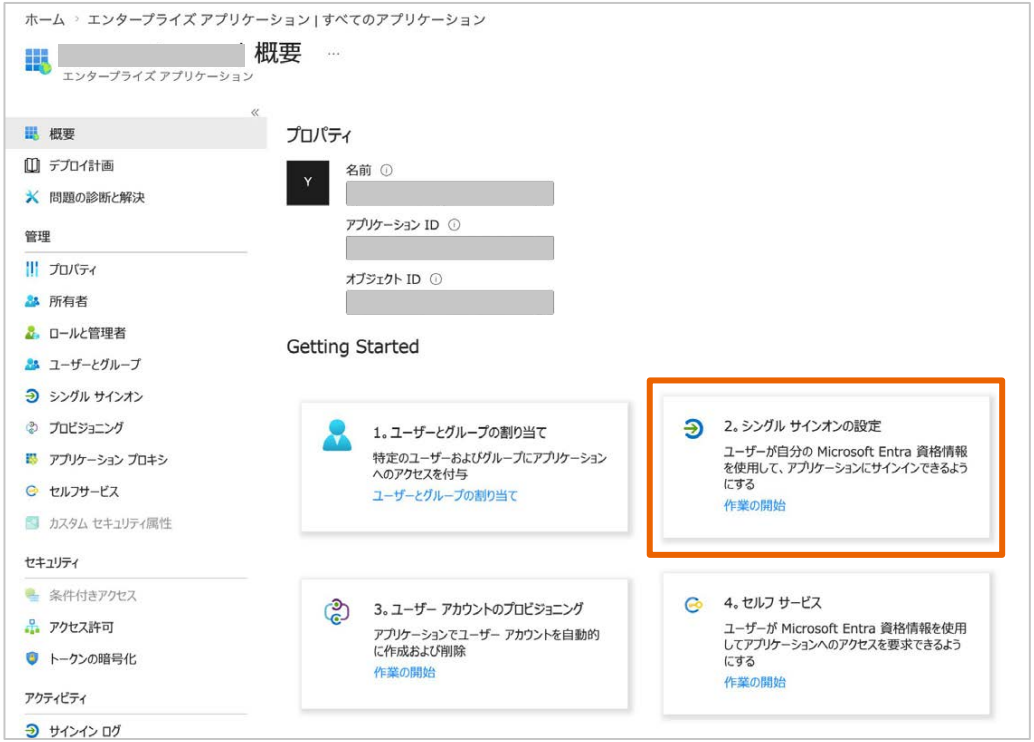
エンタープライズアプリケーションの作成（2/3）

- 「独自のアプリケーションの作成」をクリックすると、画面右に作成画面が表示されるので、以下の情報を入力します。
  - アプリケーション名：任意の文字列を入力
  - 操作の種類：一番下を選択
- 「作成」ボタンをクリックします。



エンタープライズアプリケーションの作成（3/3）

- 作成が無事に完了すると以下の画面に遷移します。
- 下部のメニューから「2.シングルサインオンの設定」をクリックします。



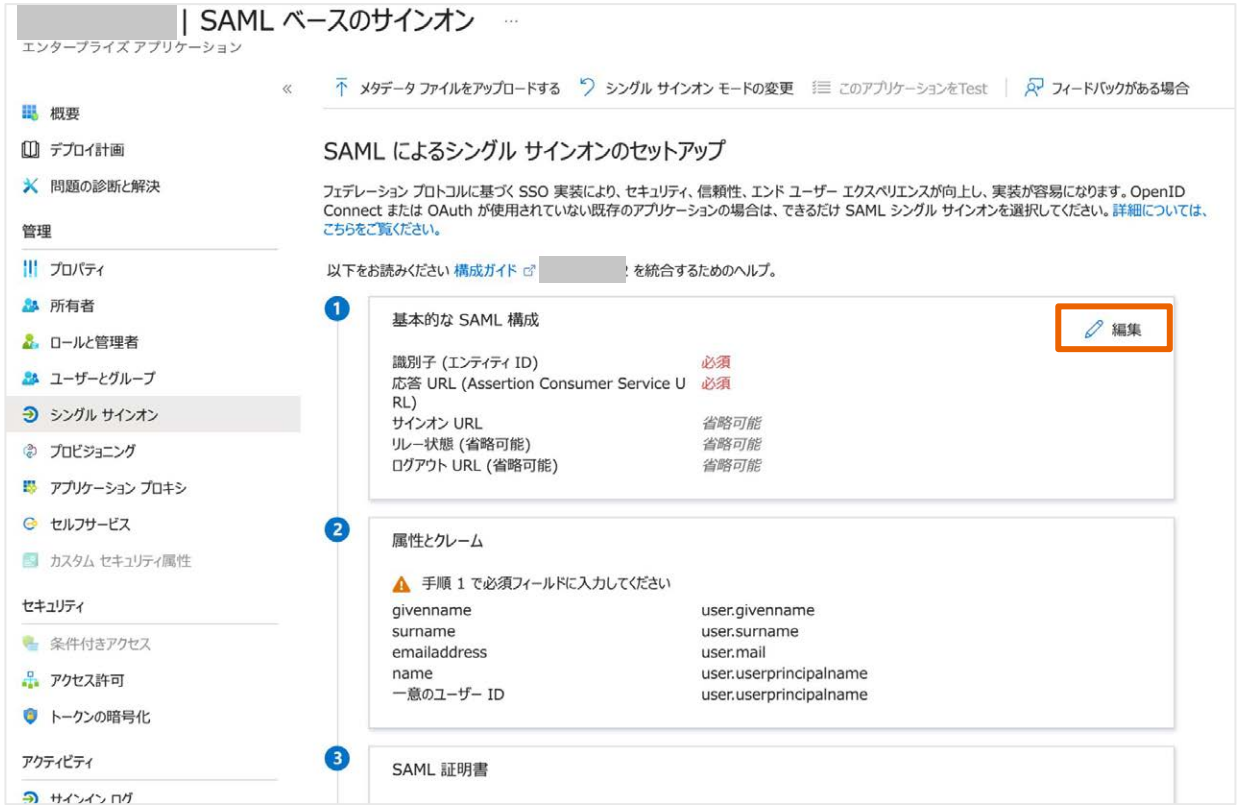
シングルサインオンの設定（1/6）

- シングルサインオン方式の設定画面が表示されます。
- 下部の選択欄の中から「SAML」をクリックします。



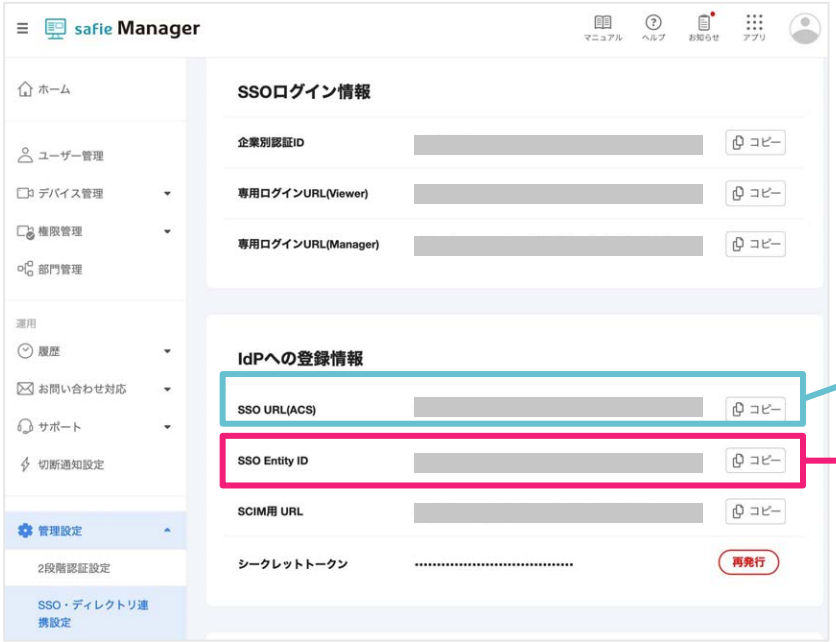
シングルサインオンの設定（2/6）

- 基本的なSAML構成の右上にある「編集」をクリックして、編集画面を表示します。



シングルサインオンの設定（3/6）

- 識別子（エンティティID）と応答URL（Assertion Consumer Service URL）にManager側のIdPへの登録情報を設定します。
- 入力が完了したら画面上部の「保存」ボタンをクリックしてください。



Managerの画面



Microsoft Azureの画面

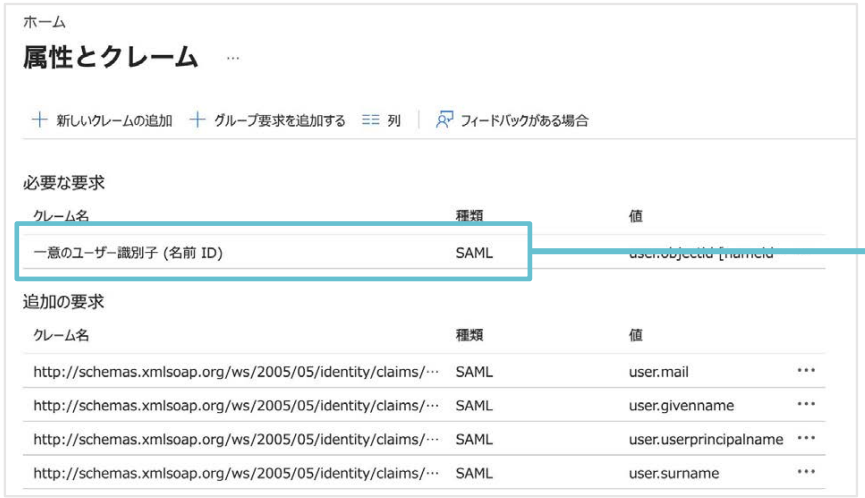
シングルサインオンの設定（4/6）

- シングルサインオン設定から「属性とクレーム」の画面の「編集」をクリックします。



シングルサインオンの設定（5/6）

- 画面中央の「一意のユーザー識別子（名前 ID）」をクリックします。
- **「ソース属性」を[user.objectid]に変更**し、画面上部の「保存」をクリックします。





シングルサインオンの設定（6/6）

- 右上の「新しいクレームの追加」をクリックします。
  - 下表の２項目を新たに追加します。



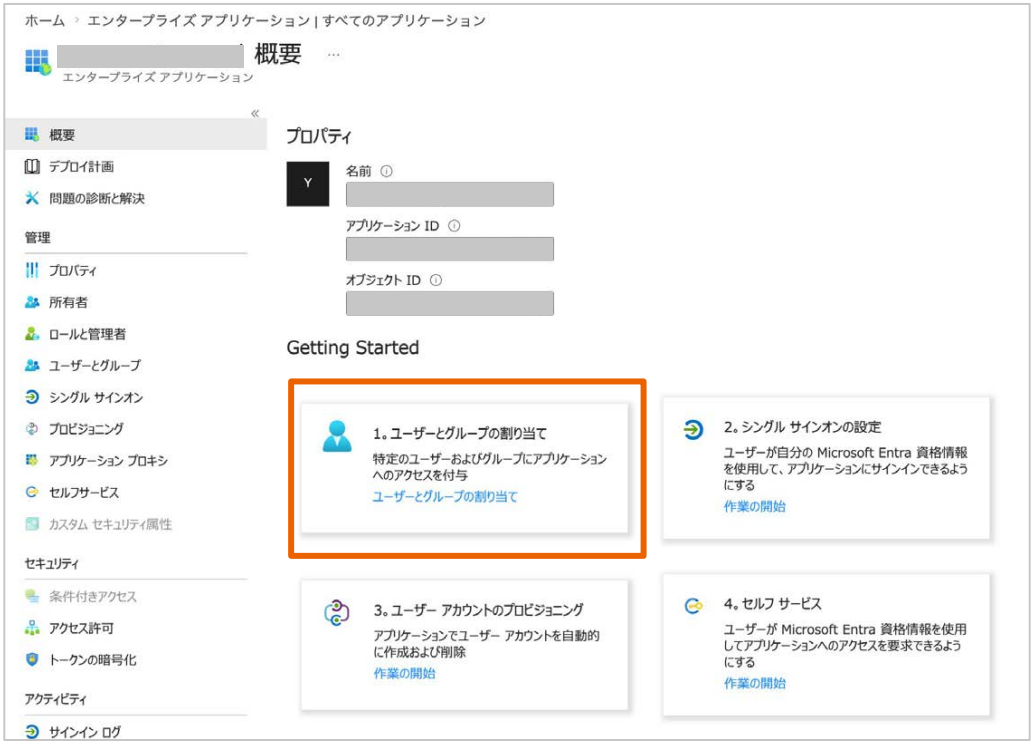


名前	名前空間	ソース	ソース属性
mail_address	なし	属性	user.mail
user_name	なし	属性	user.displayname

※要求条件は設定不要です。

ユーザーの割り当て（1/3）

- アプリケーションのトップに戻って「ユーザーとグループの割り当て」をクリックします。



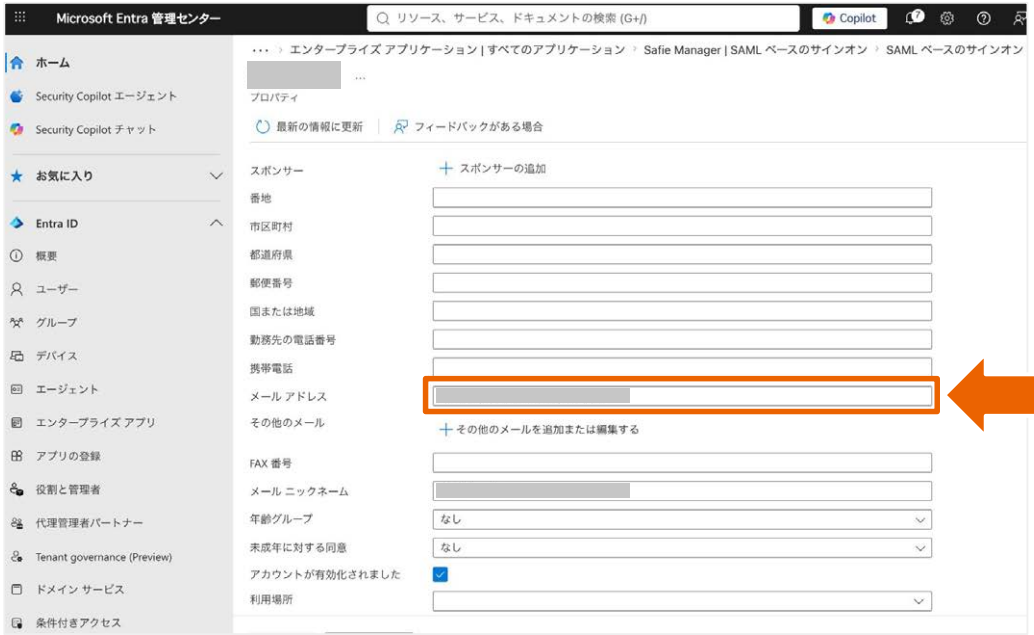
ユーザーの割り当て（2/3）

- 「ユーザーまたはグループの追加」をクリックし、ユーザーを追加します。
- ここで追加したアカウントがSSOでのサービスを利用できるようになります。



ユーザーの割り当て（3/3）

エンタープライズアプリケーションに割り当てられたユーザーは**「メールアドレス」が識別子として利用されます。**
ユーザーのプロパティの**「メール アドレス」にメールアドレスを設定してください。**



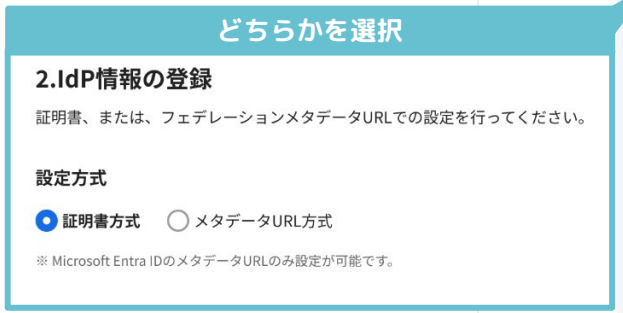
適切なメールアドレスが
設定されているご確認ください

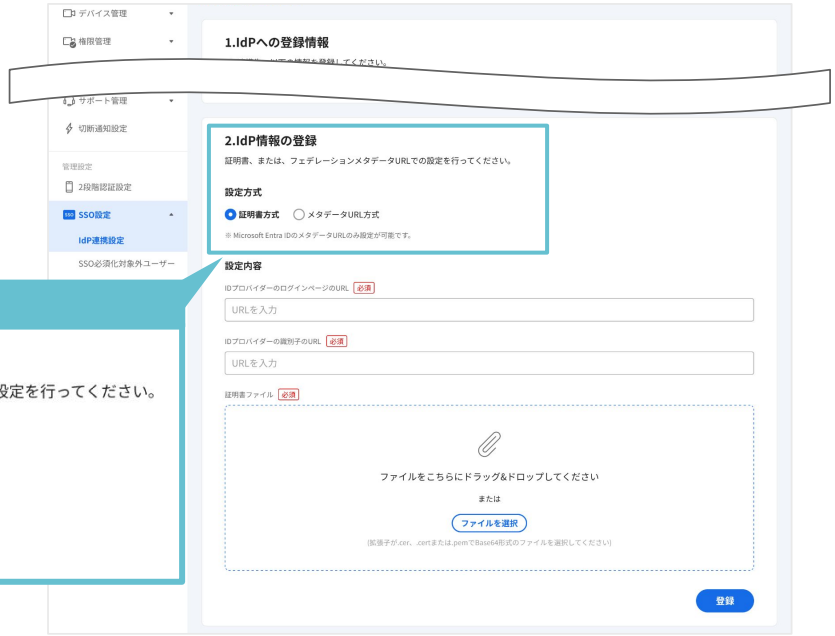
Managerの設定

ManagerでのSSO設定方法

- 管理設定のメニューから「SSO・ディレクトリ連携設定」をクリックして下部の2.IdP情報の登録から情報の入力をしてください。
- 以下2つのうちどちらかを選択する必要があります。
  - 証明書方式
    - ※SAML証明書の設定
  - メタデータURL方式
    - ※Microsoft Entra IDのみ対応

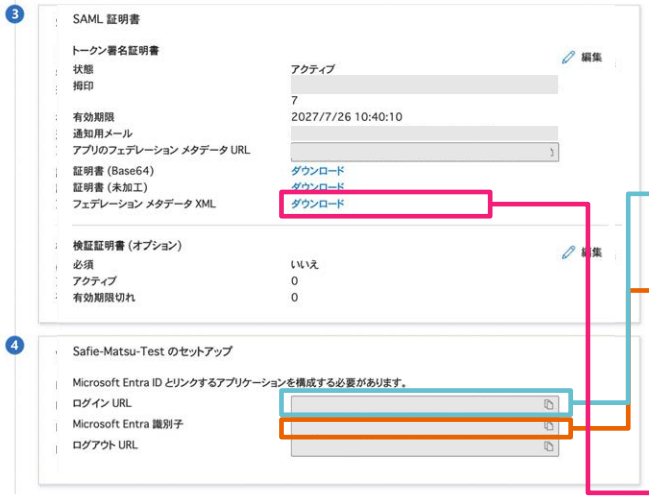




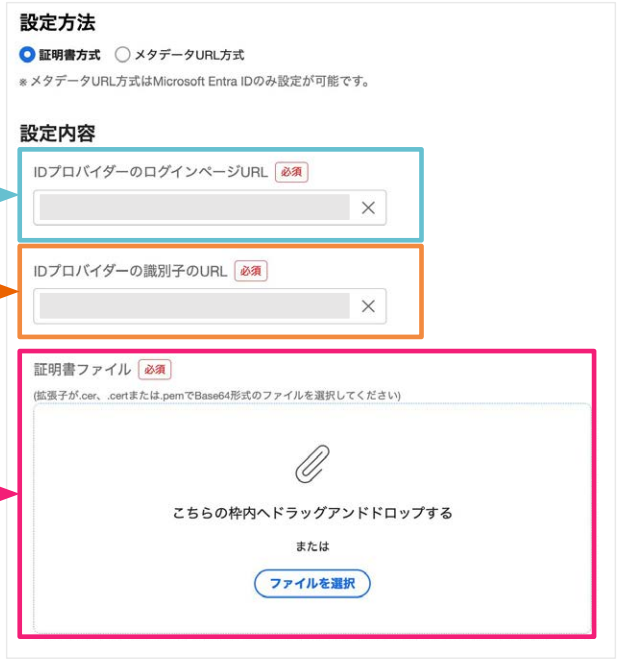


「証明書方式」を選択した場合

- Manager側の設定方法で「証明書方式」を選択します。以下の通りMicrosoft Entra ID側のログインURL、識別子情報を入力します。
- SAML署名証明書のファイルをMicrosoft Azureでダウンロードして、同ファイルをアップロードし登録します。



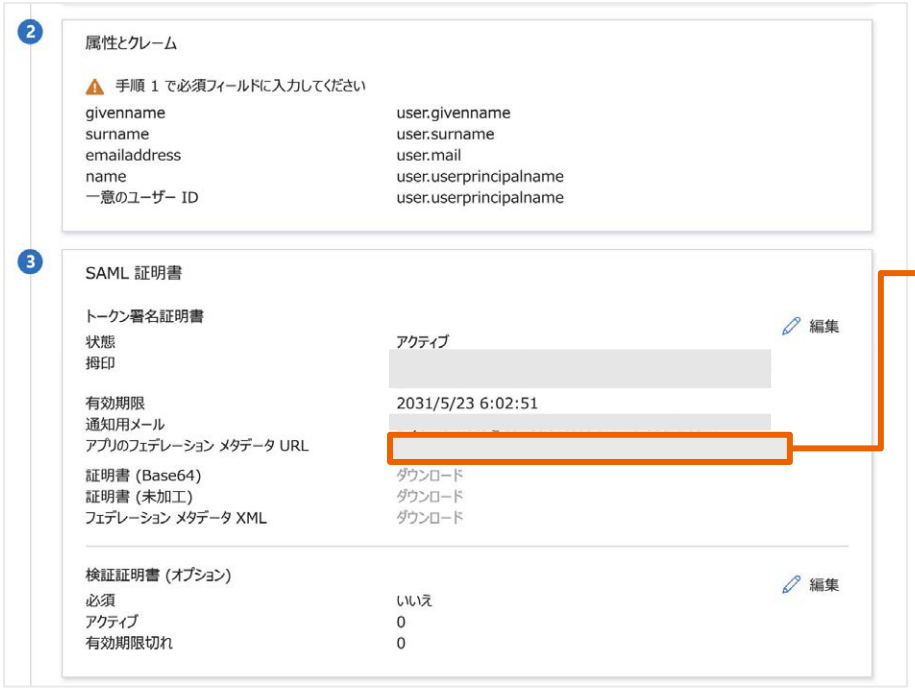
Microsoft Azureの画面



Managerの画面

「メタデータURL方式」を選択した場合

- Manager側の設定方法で「メタデータURL方式」を選択し、メタデータURLを登録します。
  - ※Microsoft Entra IDのみ対応



Microsoft Azureの画面



Managerの画面

SSO有効化

- IdP連携設定が完了すると以下のような画面になります。
- 設定直後は「SSO無効」状態なので、ログイン設定の「変更」ボタンをクリックし、設定を変更してください。
    - ○ ログイン設定について（ページに移動します）



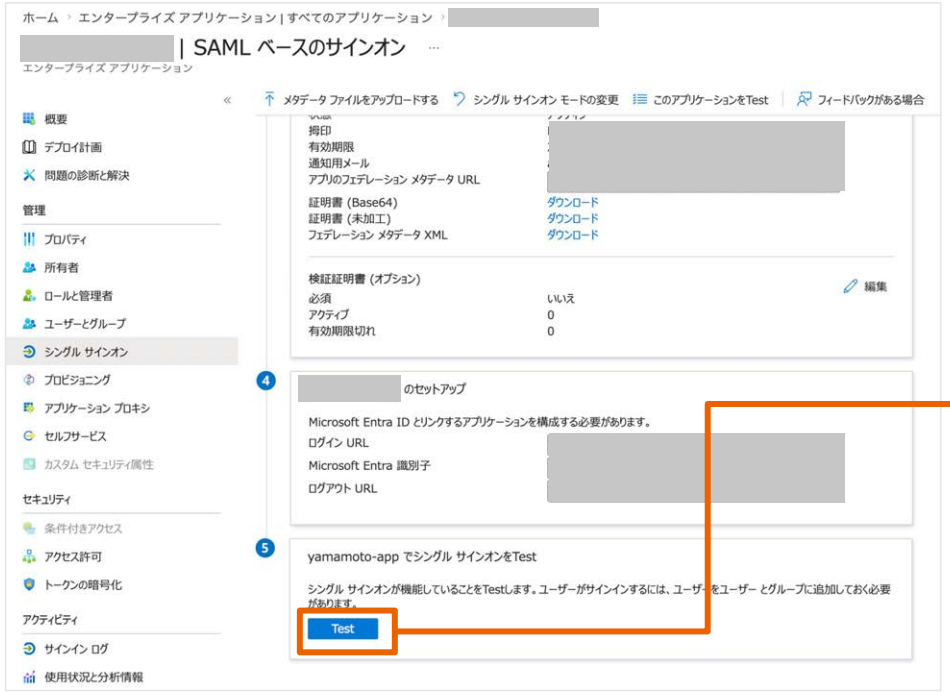


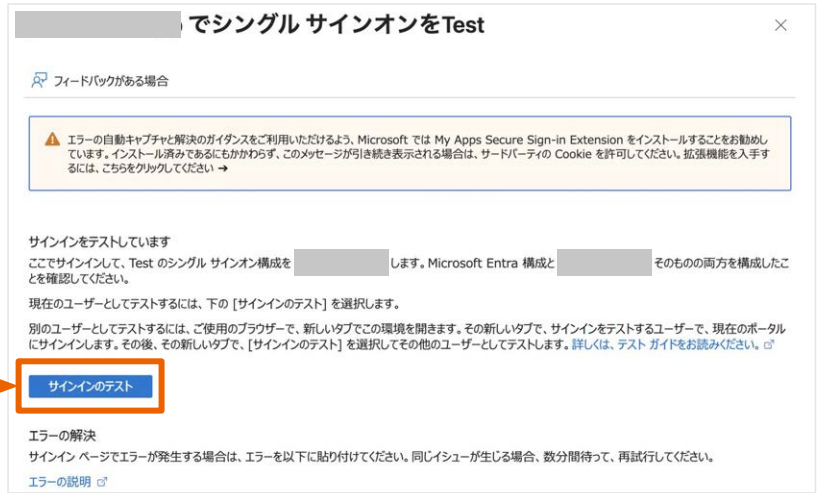
ログイン設定変更画面

SSOの動作テスト

SSOの動作テスト（1/2）

- 画面下部のテストのエリアにある「Test」のボタンをクリックし、遷移後の画面にある「サインインのテスト」をクリックしてください。





SSOの動作テスト（2/2）

- 設定完了の確認
  - しばらくするとViewerの利用規約画面（またはログイン後のトップページ）が表示されます。この画面に遷移すれば設定は正常に完了しています。
- エラーが表示された場合
  - エラーが表示された場合は、登録したURLや証明書に誤りがある可能性があります。登録情報をご確認の上、再度お試しください。

ディレクトリ連携

設定の流れ

ディレクトリ連携について
ディレクトリ連携にはSSO設定（本マニュアルの35ページまで）が必須です。SSO設定完了後にディレクトリ連携を行ってください。

ディレクトリ連携の設定は以下の手順で行います。

1. Managerの初期設定
    1.1. シークレットトークンの発行
2. Microsoft Entra IDの設定
    2.1. Microsoft Azureに管理者アカウントでログイン&エンタープライズアプリケーションの作成
    2.2. ディレクトリ連携の設定
    2.3. ユーザーの割り当て
3. 動作確認
4. プロビジョニングの停止

Managerの設定

シークレットトークンの発行(1/2)

- SSO設定 > IdP連携 >「IdPへの登録情報」内の「シークレットトークン」欄の横にある**「発行」ボタンをクリック**します。





※ シークレットトークンを再発行するとプロビジョニングエラーになります。

シークレットトークンの発行(2/2)

- 確認画面がでるので、下部の**「発行」ボタン**をクリックします。
- 表示されたシークレットトークンは**ここでしか表示されないため、必ず手元に控えてください。**
  - **この画面は以降の手順でも参照するため、画面を閉じずに次の手順に進んでください。**





シークレットトークンはここでしか表示されないため、必ず手元に控えてください

※ シークレットトークンを再発行するとプロビジョニングエラーになります。

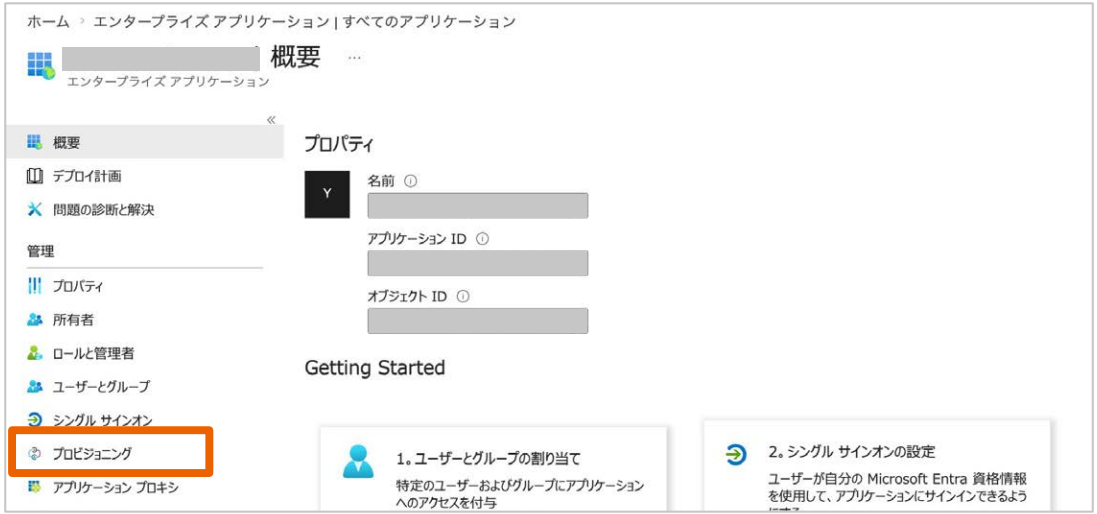
Microsoft Entra IDの設定

プロビジョニング設定画面への遷移

ディレクトリ連携について

本マニュアルの15～17ページを参照し、Microsoft Azureへのログインおよびエンタープライズアプリケーションの作成を行ってください。

- エンタープライズアプリケーションの作成が無事に完了すると以下の画面に遷移します。
- サイドメニューから「プロビジョニング」をクリックします。



プロビジョニング設定（1/22）

- 「アプリケーションの接続」をクリックします。



プロビジョニング設定（2/22）

- プロビジョニングモードについて「ベアラー認証」であることを確認してください。
- ManagerのSCIM用 URLをコピーして「テナントのURL」にペーストしてください。



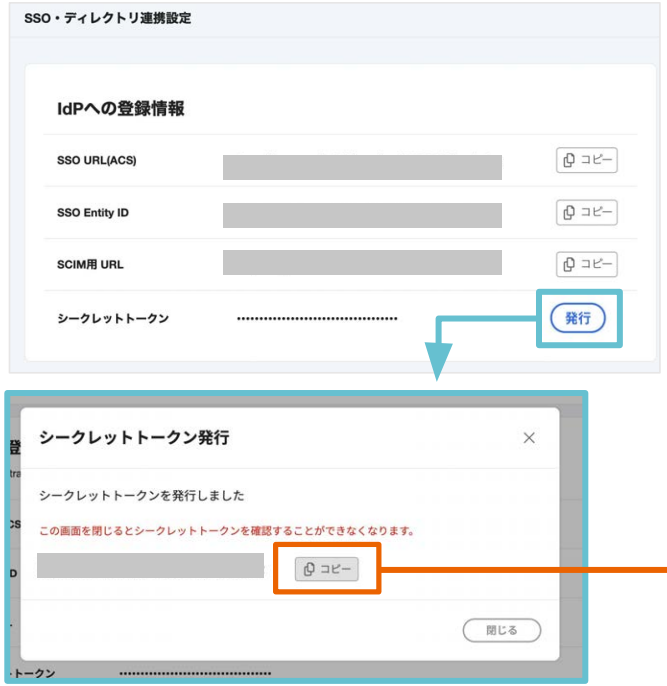
Managerの画面



Microsoft Azureの画面

プロビジョニング設定（3/22）

- Managerのシークレットトークンを発行します。
  - シークレットトークン発行の確認画面は割愛します。
- Managerのシークレットトークンをコピーして「シークレットトークン」にペーストしてください。



Managerの画面



Microsoft Azureの画面

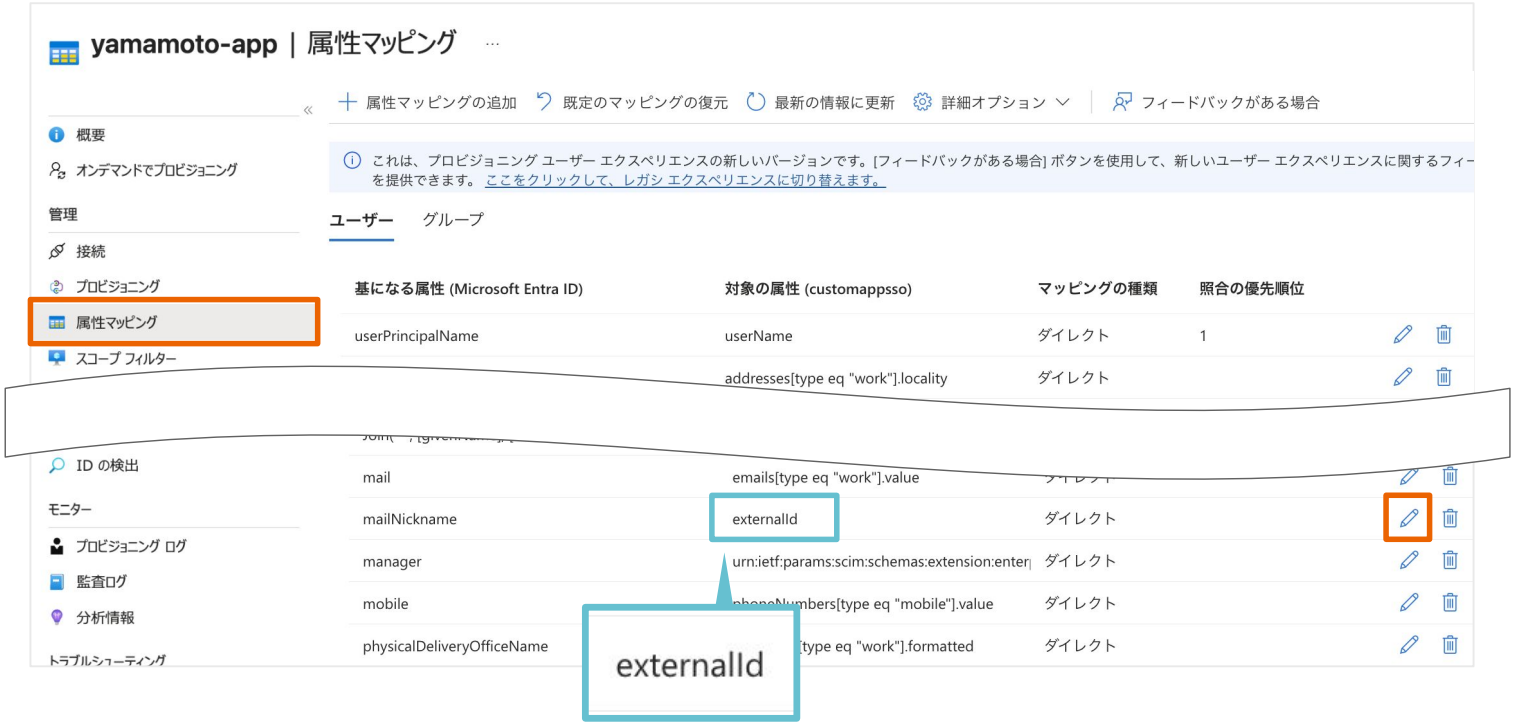
プロビジョニング設定（4/22）

- 「テナントURL」と「シークレットトークン」の入力をしたら、**「テスト接続」ボタンをクリック**します。
- テスト接続が完了すると、下部の**「作成」ボタンが青くなるので、クリック**します。



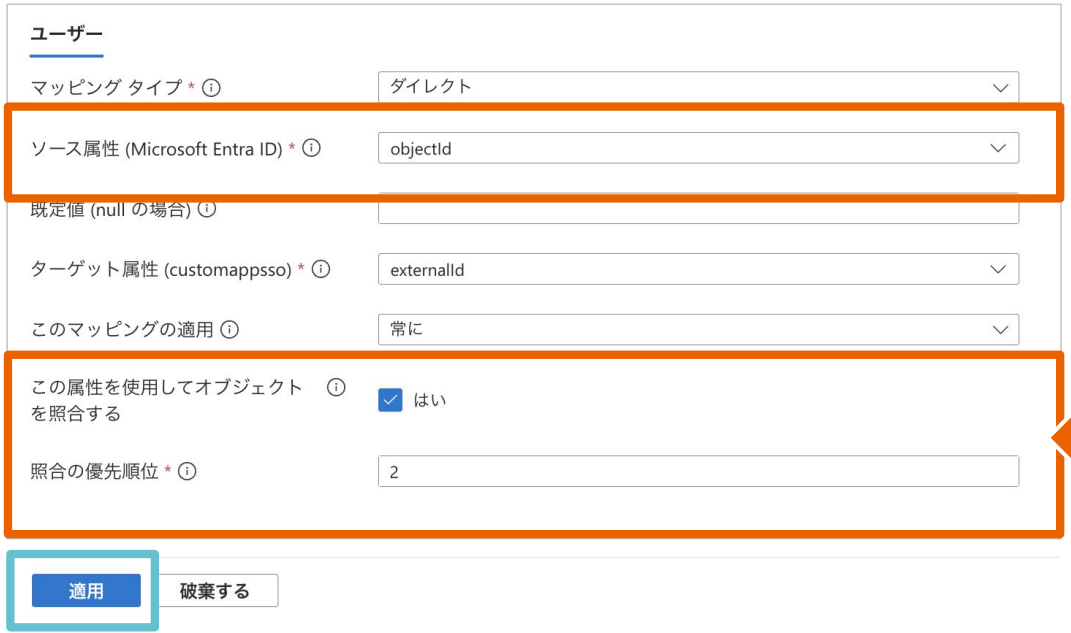
プロビジョニング設定（5/22）

- サイドメニューの**「属性マッピング」**をクリック。
  - もしこの画面が出ない場合は「Provision Microsoft Entra ID Users」をクリック。
- customappsso属性の**「externalId」のペンアイコン（編集）**をクリックします。



プロビジョニング設定（6/22）

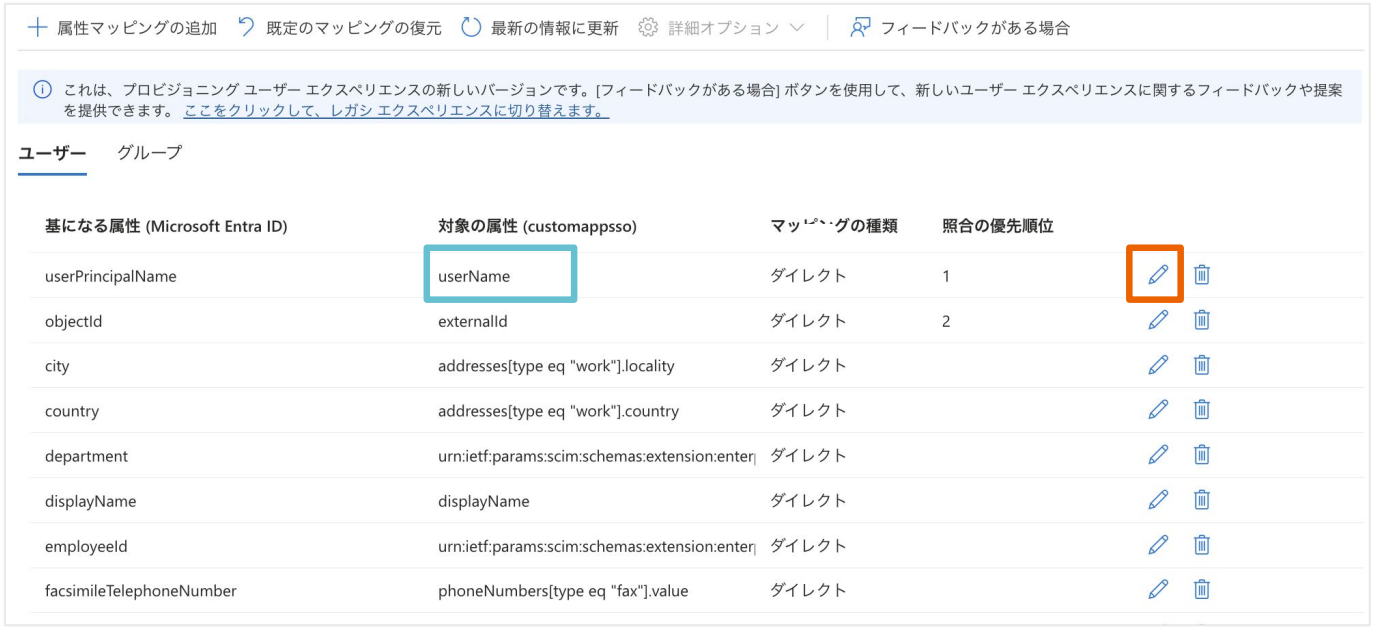
- 「ソース属性(Microsoft Entra ID)」を**「objectId」へ変更**します。
- 「この属性を使用してオブジェクトを照合する」に**チェックを入れます。**
- **「照合の優先順位」を「２」と入力します。**
    - 最終的に「externalId」と「objectId」を照合優先順位1にするための手順です。
- 左下の「適用」ボタンをクリックします。



「はい」を選択し「2」と入力

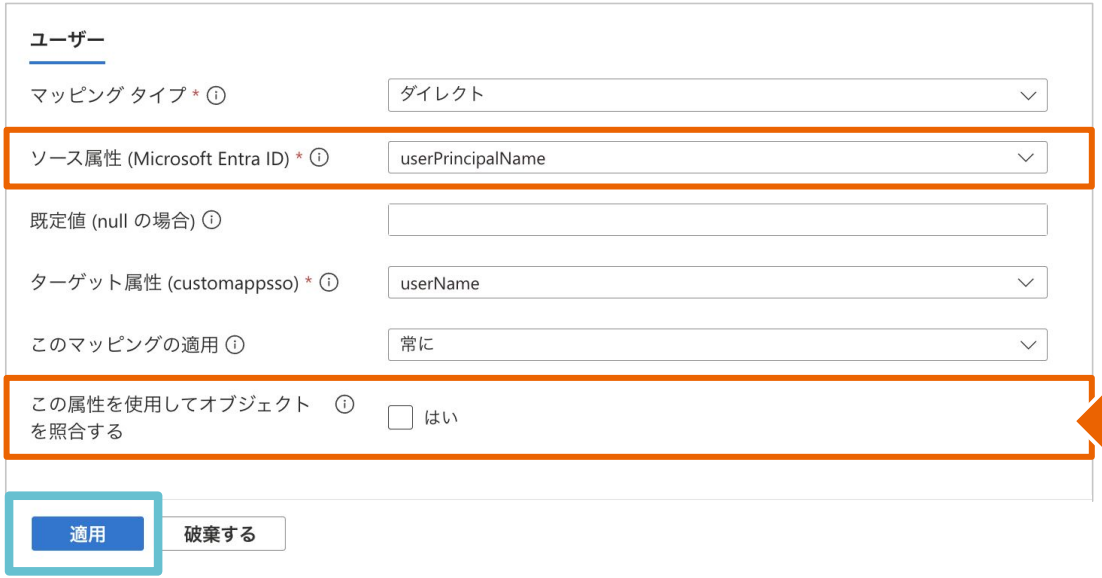
プロビジョニング設定（7/22）

- 「属性マッピング」のトップに戻るので、対象の属性(customappsso)が**「userName」のペンアイコン（編集）**をクリックします。



プロビジョニング設定（8/22）

- 「ソース属性(Microsoft Entra ID)」が「userPrincipalName」になっていることを確認してください。
- 「この属性を使用してオブジェクトを照合する」の**チェックを外します**。
- 左下の「適用」ボタンをクリックします。



チェックを外します
（もしくは「いいえ」を選択）

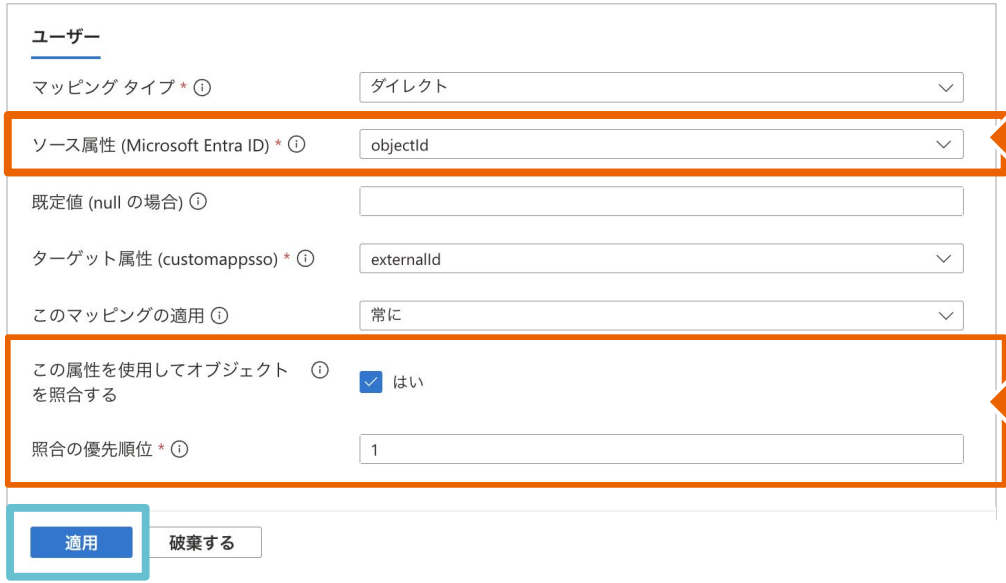
プロビジョニング設定（9/22）

- 「属性マッピング」のトップに戻るので、対象の属性(customappsso)が**「externalId」のペンアイコン（編集）**をクリックします。



プロビジョニング設定（10/22）

- **「ソース属性(Microsoft Entra ID)」が「objectId」**になっていることを確認してください。
- **「照合の優先順位」が「1」**になっていることを確認してください。
  - 「1」ではない場合は「1」を入力してください。
- 左下の「適用」ボタンをクリックします。



objectId以外で設定すると正しく動作しません。

「はい」を選択し「１」と入力

プロビジョニング設定（11/22）

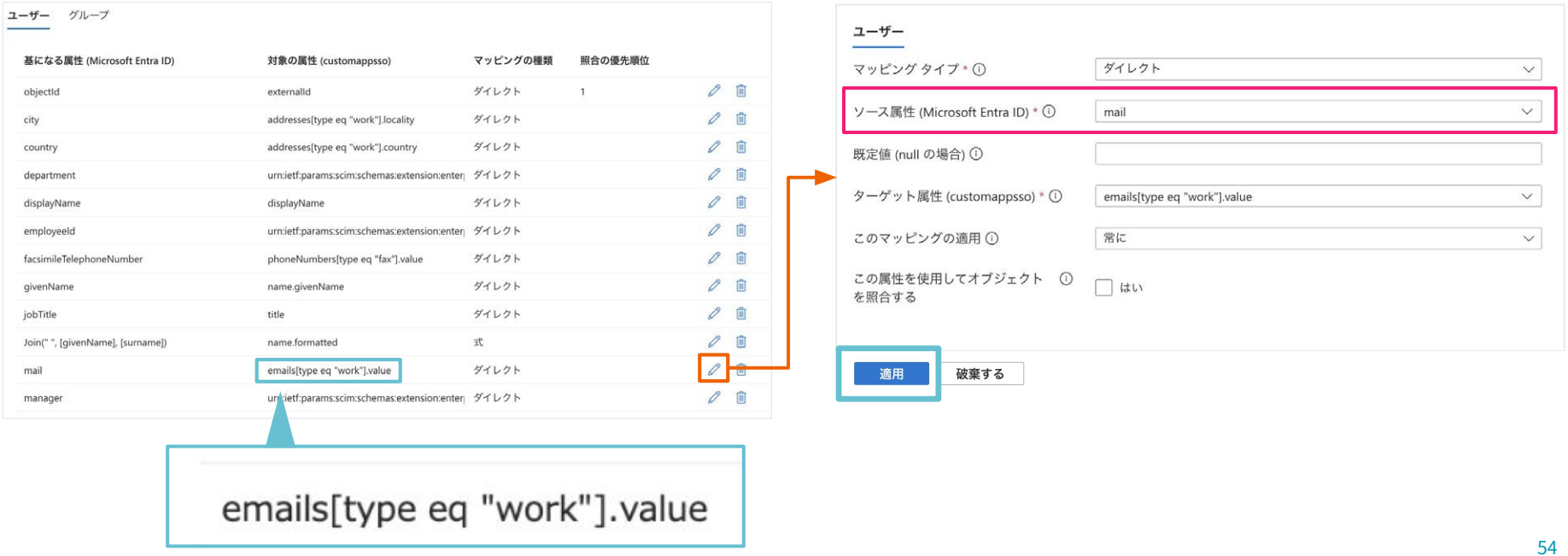
- 「属性マッピング」のトップに戻るので、対象の属性(customappsso)が「displayName」のペンアイコン（編集）をクリックします。
- 「ソース属性(Microsoft Entra ID)」と「対象の属性」が「displayName」になっていることを確認してください。
- 左下の「適用」ボタンをクリックします。





プロビジョニング設定（12/22）

- 「属性マッピング」のトップに戻るので、対象の属性(customappsso)が「emails[type eq "work"].value」のペンアイコン（編集）をクリックします。
- 「ソース属性(Microsoft Entra ID)」が「mail」になっていることを確認してください。
- 左下の「適用」ボタンをクリックします。



プロビジョニング設定（13/22）

- 「属性マッピング」のトップに戻るので、対象の属性(customappsso)が「urn:ietf:params:scim:schemas:extension:enterprise:2.0:User:employeeNumber」のペンアイコン（編集）をクリックします。
- 「ソース属性(Microsoft Entra ID)」が「employeeId」になっていることを確認してください。
- 左下の「適用」ボタンをクリックします。





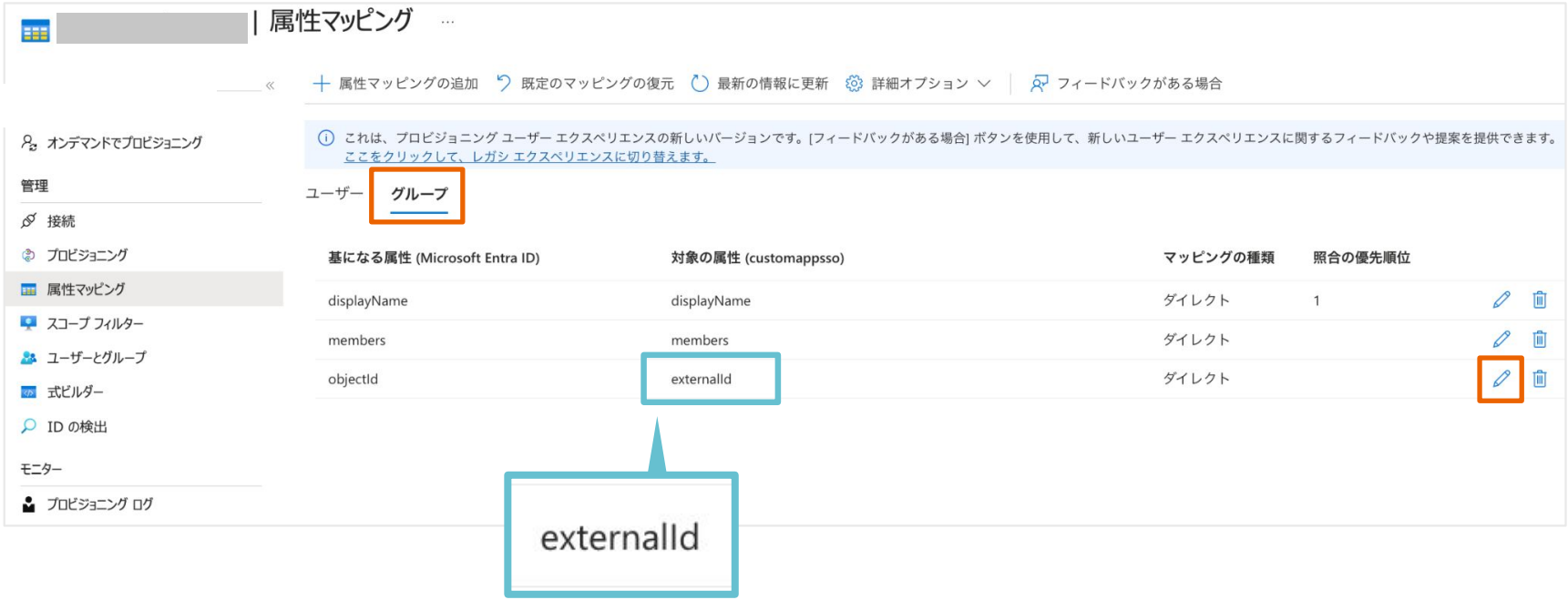
プロビジョニング設定（14/22）

- 「属性マッピング」のトップに戻るので、**左下の保存**をクリックします。



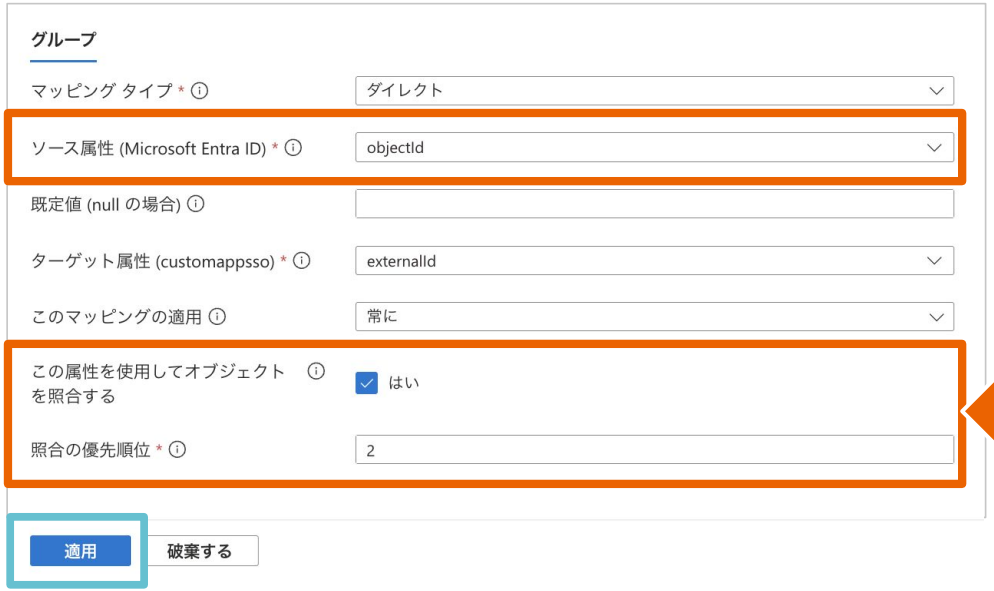
プロビジョニング設定（15/22）

- **「グループ」のタブをクリック**します。
  - もしこの画面が出ない場合は「Provision Microsoft Entra ID Groups」をクリック。
- 対象の属性(customappsso)が**「externalId」のペンアイコン（編集）**をクリックします。



プロビジョニング設定（16/22）

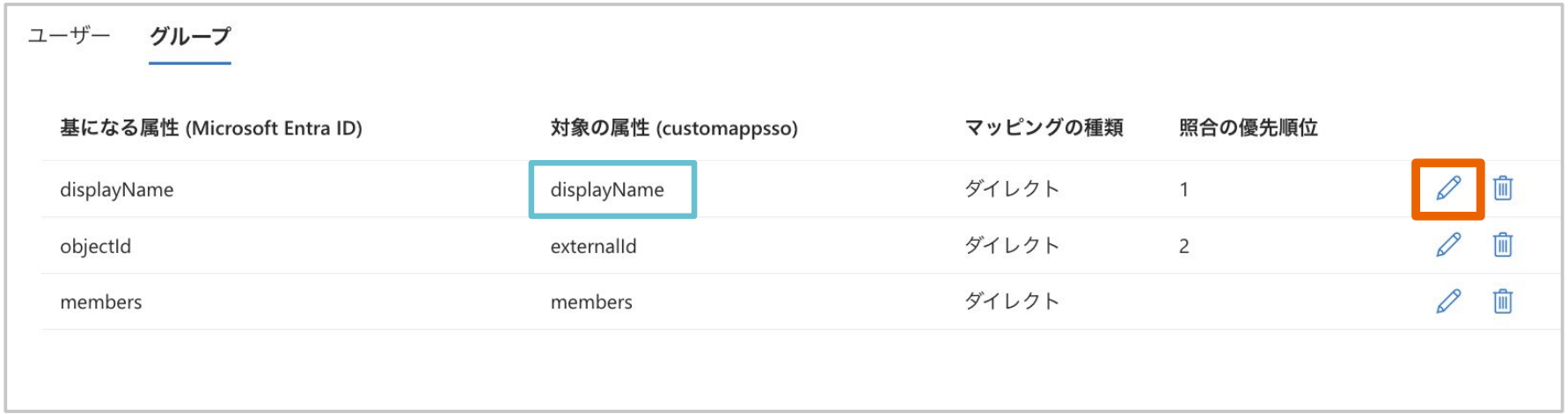
- 「ソース属性(Microsoft Entra ID)」を「objectId」になっていることを確認してください。
  - 「objectId」でない場合、「objectId」へ変更します。
- 「この属性を使用してオブジェクトを照合する」に**チェックを入れます。**
- **「照合の優先順位」を「２」と入力します。**
  - 最終的に「externalId」と「objectId」を照合優先順位1にするための手順です。
- 左下の「適用」ボタンをクリックします。



「はい」を選択し「2」と入力

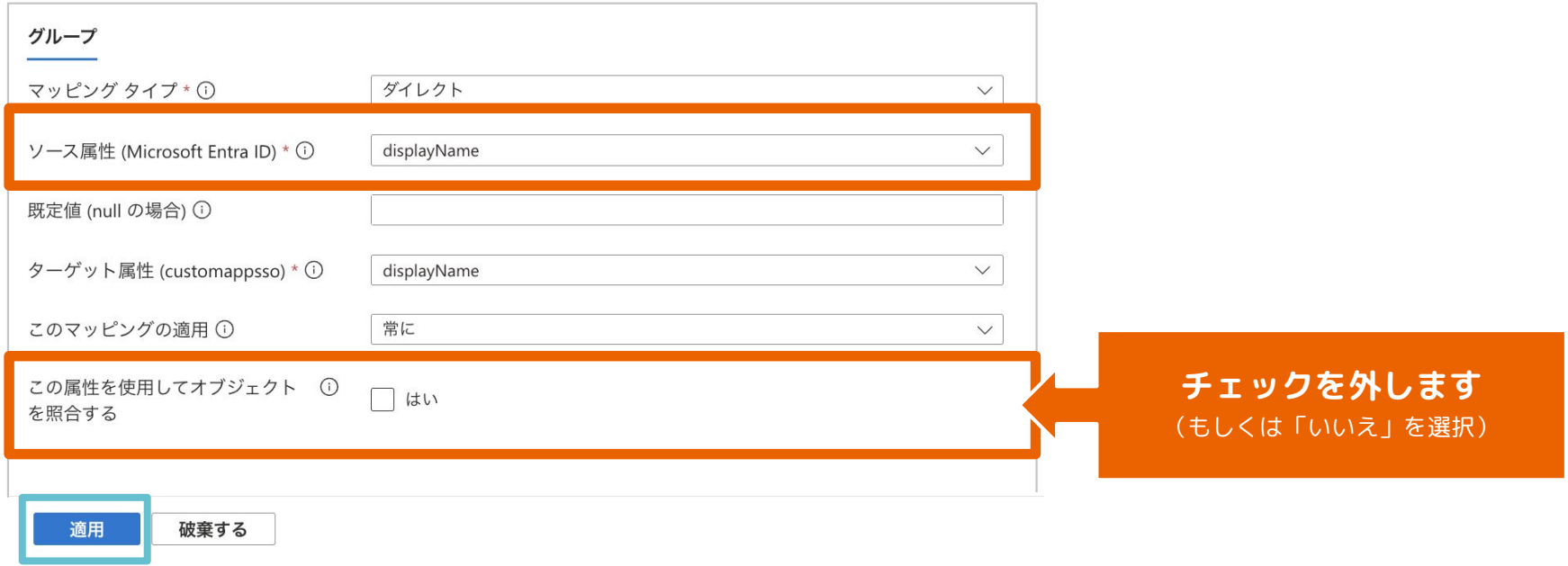
プロビジョニング設定（17/22）

- 「属性マッピング」のトップに戻るので、対象の属性(customappsso)が**「displayName」のペンアイコン（編集）**をクリックします。



プロビジョニング設定（18/22）

- 「ソース属性(Microsoft Entra ID)」が「userPrincipalName」になっていることを確認してください。
- 「この属性を使用してオブジェクトを照合する」の**チェックを外します**。
- 左下の「適用」ボタンをクリックします。



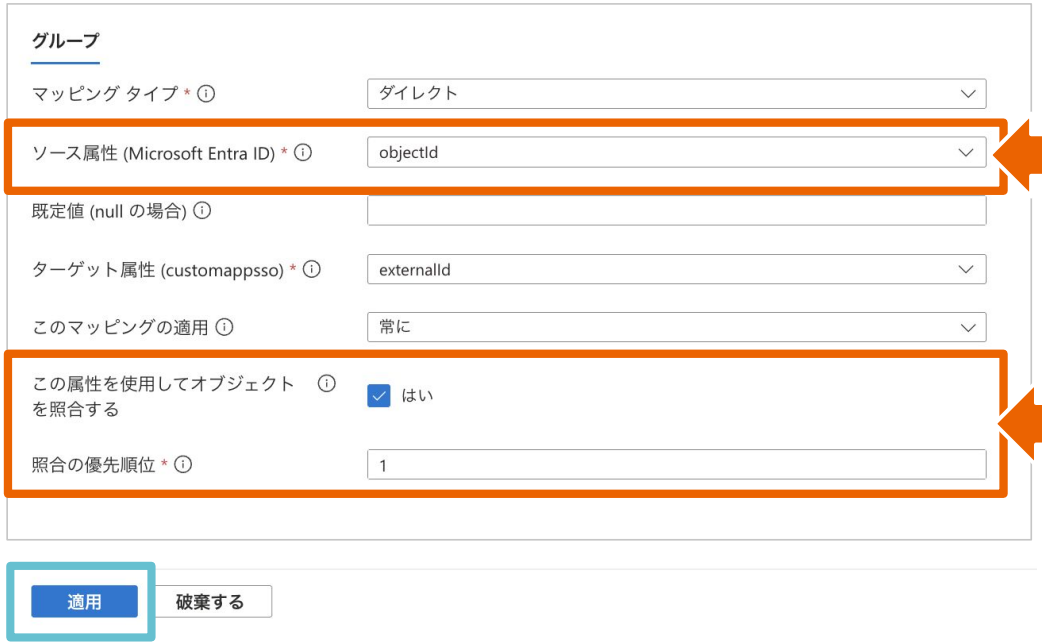
プロビジョニング設定（19/22）

- 「属性マッピング」のトップに戻るので、対象の属性(customappsso)が**「externalId」のペンアイコン（編集）**をクリックします。



プロビジョニング設定（20/22）

- **「ソース属性(Microsoft Entra ID)」が「objectId」**になっていることを確認してください。
- **「照合の優先順位」が「1」**になっていることを確認してください。
  - 「1」ではない場合は「1」を入力してください。
- 左下の「適用」ボタンをクリックします。



objectId以外で設定すると正しく動作しません。

「はい」を選択し「1」と入力

プロビジョニング設定（21/22）

- 「属性マッピング」のトップに戻るので、**左下の保存**をクリックします。



プロビジョニング設定（22/22）

- **サイドメニューから「概要」へ戻り、「プロビジョニングの開始」**をクリックすると、プロビジョニングが開始されます。



プロビジョニングの停止

- **「プロビジョニングを一時停止」をクリック**することでプロビジョニングが停止されます。



ユーザーの割り当て

- 25、26ページを参照し、エンタープライズアプリケーションへのユーザーの割り当てを行います。

動作確認

プロビジョニングログの確認

- **サイドメニューから「プロビジョニングログ」をクリック**します。
- プロビジョニングログを確認する画面に遷移することができます。
- ユーザー・グループ情報の同期成功・失敗について、こちらのログから確認することができます。



プロビジョニング失敗時の通知

- サイドメニューから「プロビジョニング」をクリックします。
- 下部の「設定」よりプロビジョニング失敗時にメール通知を行うことができます。



プロビジョニング失敗時のエラー一覧

- プロビジョニング失敗の理由について、プロビジョニングログの「トラブルシューティング」より、SCIMエンドポイントからのエラーレスポンス値を確認することができます。主なエラー内容については下記になります。

error_description	エラー内容
emails is invalid. / Invalid mail address / mail_address is invalid.	Microsoft Entra IDのメールアドレスのマッピング設定が間違っているか、マッピングし取得した情報がメールアドレスの形式となっていない可能性があります。51ページを参考に設定を行ってください。
employee_number is invalid. / invalid employee_number / Max length of employeeNumber is 16	Microsoft Entra IDの社員番号のマッピング設定が間違っているか、社員番号が16文字より大きい情報である、もしくは既に登録されている社員番号である可能性があります。
Max length of displayName is 32	Microsoft Entra IDのユーザー名のマッピング設定が間違っているか、ユーザー名が32文字より大きい情報である可能性があります。

プロビジョニング失敗時のエラー一覧

error_description	エラー内容
Corporation user capacity is full	Managerに登録できるユーザー数の上限を超えています。新たにカメラをご契約いただき上限を増やすか、不要なユーザー情報の削除をご検討ください。
failed to authorize	シークレットトークンによるSCIM用URLでの認証に失敗しています。新たにシークレットトークンを発行しMicrosoft Entra IDへの設定を行うことで解決できる可能性があります。
invalid sso_setting_id.	Microsoft Entra IDの管理者資格情報に設定するSCIM用URLの値が間違っているか、同期対象のユーザーが別企業アカウントに所属している可能性があります。

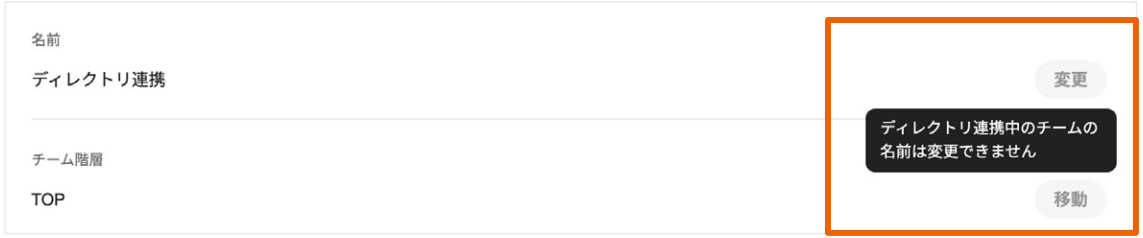
ディレクトリ連携で取り込まれた
ユーザー・チームについて

ディレクトリ連携で取り込まれたユーザー・チームについて

ディレクトリ連携を利用してユーザー管理をする場合、以下の点にご留意ください。

- ディレクトリ連携をした環境のManagerではユーザーやチームにはリンクアイコンが表示されます。
  - 連携済では緑色になり、未連携ではグレーで表示されます。
- 連携済のユーザー
  - ユーザー名の変更や、ユーザーの削除・社員番号の変更がManager上ではできなくなります。
- 連携済のチーム
  - チーム名の変更・移動・ユーザーの追加がManager上ではできなくなります。





ディレクトリ連携における
運用時の留意事項

ディレクトリ連携における運用時の留意事項

- 1度削除したユーザーの再連携
  - Microsoft Entra ID上のグループから削除される等で一度Manager環境から削除されたユーザーをグループ所属によって同じManager環境へ連携することはできません。
- 部署変更、異動などでMicrosoft Entra ID上のグループ変更を行う場合
  - 手順
    - 新グループに該当ユーザーを追加
    - Managerへの同期反映を確認
    - 旧グループから該当ユーザーを削除
  - ユーザーが所属するMicrosoft Entra ID上のグループを変更する場合、一時的にどのグループにも所属しない（未割り当て）状態が発生すると、Managerからユーザーが削除されます。
    意図しないユーザーの削除を防ぐため、操作対象ユーザーを対象のグループだけではなく、エンタープライズアプリケーションに直接ユーザーを紐づけておく運用設定を推奨します。
- 万が一意図せずユーザーが削除となった場合の復旧方法
  - 再連携が行われなくなった場合には、該当グループにそのユーザーを割り当てた後、該当アカウントにてSSOログインを行うと復旧可能です。

ログイン設定

ログイン設定

SSO無効 / SSO有効(ログイン情報利用可) / SSO有効(必須)と三段階あります。
用途に合わせて設定してください

ログイン設定	用途例
SSO無効	SSO運用前・IdPのエラーがあった場合
SSO有効 (ログイン情報利用可)	SSO動作テストでの利用を推奨
SSO有効(必須)	SSO本番運用







SSO必須化時
ログイン情報でのログイン

全体管理者について

- **全体管理者**はログイン設定に関わらず、
  常にログイン情報(メールアドレスとパスワード)でログインできます。

SSO必須化時の注意点

SSO必須化時、Manager操作権限を全体管理者から
他の権限に変更すると、メールアドレスとパスワードでの
ログインできなくなるのでご注意ください。





SSO必須化対象外にするには ①/ ユーザー詳細

- 全体管理者以外のユーザーをSSOログイン対象外に個別設定が可能です。
- ユーザー一覧 > ユーザー情報からSSO必須化の「変更」ボタンをクリックしてください。



ユーザー情報画面

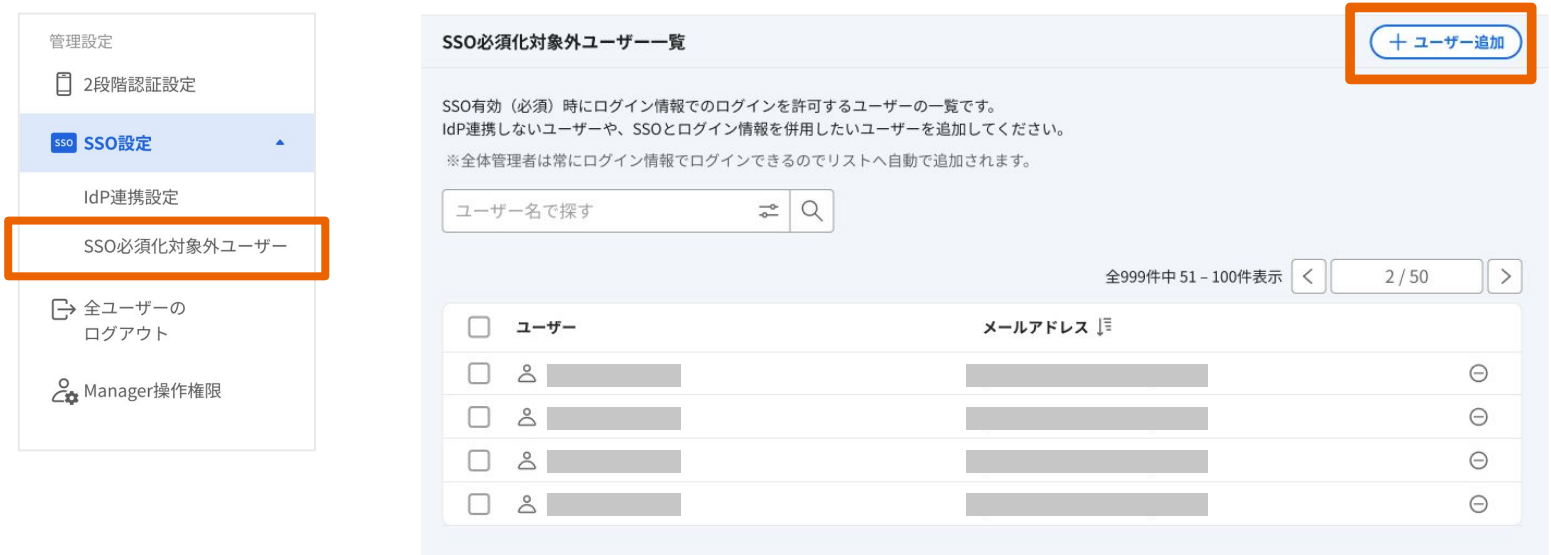
全体管理者をSSO必須化対象に変更することはできません。



SSO必須化変更画面

SSO対象外にするには ② / SSO必須化対象外ユーザー一覧

- SSO必須化対象外ユーザー一覧ページの「ユーザー追加」ボタンをクリックし、対象外にするユーザーを選択してください。
  - SSO必須化対象外ユーザー一覧の詳しい使い方（ページに移動します）



SSO必須化対象外ユーザー一覧

ユーザー作成

- IdP連携後、ユーザー作成時に「SSO必須化」という項目が表示されます。
  - 対象か、対象外かを選択できます。**対象(SSOのみのログイン)の場合はパスワードは入力できません。**
  - **全体管理者の場合はSSO必須化が対象外になります。**



運用時の留意事項

SSO有効（必須化）から無効にした場合の注意点

- SSO有効（必須化）→無効にした場合、SSOログインのみ利用できるユーザーはログインできなくなる可能性があります。
  - その場合、ログイン画面で各自パスワードリセットして、ログインしてください。



部門管理者の編集権限について

- 部門管理者もSSO必須化対象外ユーザー一覧の編集ができます。
  - 権限制限が必要であればカスタム権限をご利用ください。





Appendix

SSO必須化対象外ユーザー一覧

- このリストに入っているユーザーはSSO有効(必須化)の設定でもログイン情報(メールアドレスとパスワード)でのログインができます。
  - 全体管理者は常にログイン情報でログインできるのでリストへ自動で追加されます。
    - **全体管理者を手動で追加/解除はできません。**



SSO必須化対象外ユーザー一覧

SSO必須化対象外ユーザー一覧

- 「まとめて操作」の解除は全体管理者が含まれていると操作できません。
- 検索ボックスの右にある「アイコン」をクリック。ユーザー種別で「全体管理者以外」を選択すると、全体管理者を含まない一覧が表示されます。



全ユーザーのログアウト

- ログイン設定の変更をしたら「ログインセッションのリセット」を推奨します。
- これを実行すると実行者含む全ユーザーが本サービスからログアウトされます。ログイン設定変更後のログイン方法で再度ログインしてください。

