



Microsoft Entra ID (旧 : Azure Active Directory) SSO連携手順書



アジェンダ

Agenda

- 01 連携概要
- 02 連携操作手順
- 03 よくあるご質問
- 04 お問い合わせ先

01

Chapter

連携概要

Microsoft Entra ID × ミキワメ SSO設定 概要



Microsoft Entra IDを利用してミキワメにSSO設定を行うことで、ミキワメにログインする際のミキワメ上のパスワード認証が不要になります。

ログインの手間が減るだけでなく、パスワード漏洩のリスクも軽減され、セキュリティと利便性を両立することが可能です。

本マニュアルでは具体的な操作手順についてご案内いたします。

なお、本マニュアル記載のミキワメ側の操作については、「管理者」または「管理者+ストレスチェック事務」権限の管理アカウントでのみ操作が可能です。

02

Chapter

連携操作手順

Microsoft Entra ID×ミキワメ SSO設定 連携操作手順



SSOを設定する大まかな流れは以下5ステップです。
SSO設定は、可能な限り貴社のセキュリティ担当者様・情報システム担当者様にて操作いただくことを推奨いたします。

手順	操作対象	操作内容
事前準備	-	ミキワメのカスタマーサポートへ、SSO設定ご希望の旨ご連絡ください。< お問い合わせフォーム >
ステップ1	ミキワメ	IdPに登録する情報をコピーする
ステップ2	Microsoft Entra ID	必要項目を設定する
ステップ3	ミキワメ	必要項目を設定し、ログイン方法を設定する
ステップ4	ミキワメ	社員アカウントに対して、Microsoft Entra IDのSSOを有効化する
ステップ5	Microsoft Entra ID	社員アカウントに対して、ミキワメのSSOを有効化する

1

2

3

4

https://   

成る URL の通知

2. シングル サインオンの設定
ユーザーが自分の Microsoft En
輯を使用して、アプリケーションに
きるようにする
[作業の開始](#)

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](#)

連携操作手順 ステップ2：Microsoft Entra IDに必要項目を設定する

5

「属性とクレーム」の編集を押下→「必要な要求」→
「一意のユーザー識別子(名前ID)」を選択

ホーム > Mikiwame | 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.mail [nameid-for... ***

6

「ソース属性」から「user.mail」を選択し保存

ホーム > 属性とクレーム >

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	nameidentifier
名前空間	http://
名前識別子の形式の選択	
名前識別子の形式 *	電子メール アドレス
ソース *	<input checked="" type="radio"/> 属性 <input type="radio"/> 変換 <input type="radio"/> ディレクトリスキーマ拡張
ソース属性 *	user.mail
要求条件	
SAML クレームの詳細オプション	

7

「SAML 証明書」内の「フェデレーション メタデータXML」をダウンロード

Mikiwame | 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 モーデルの破棄 このアプリケーションをTest フィードバック

属性とクレーム

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

SAML 証明書

トーン署名証明書	アクティブ
証明	04B5367808442D8B2ACB046E30160A62181
有効期限	2028/7/7 14:53:06
発行元	com
アプのフェデレーション メタデータ URL	https://login.microsoftonline.com/0012258f-...
証明書 (Base64)	ダウンロード
証明書 (Base64)	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

検証証明書 (オプション)

必須	はい/いいえ
アクティブ	はい/いいえ
有効期限切れ	はい/いいえ

連携操作手順 ステップ3：ミキワメに必要な項目を設定し、ログイン方法を設定する

1

ミキワメ管理画面にアクセスし、サイドメニュー「設定」→「SSOを管理する」→
IdP情報「IdPを管理する」を押下し、右上の「新規作成」を押下

SSO管理

SSO管理

サービスプロバイダ情報

IdPとの連携に必要な、ミキワメのサービスプロバイダ情報を確認します。

確認する

IdP管理

IdPの新規登録や、登録済みIdPの確認・更新を行います。

IdPを管理する

新規作成

IdP管理

登録済みIdP一覧

ご利用のIdPを登録・管理することができます。

登録したIdPを利用する場合、SAML SSOの有効化からステータスを有効化にしてください。

IdPが登録されていません。

3

サイドメニュー「設定」→「SSOを管理する」→SAML SSOの有効化「設定する」
→SAML SSOの利用設定の「有効化」にチェックを入れる

SAML SSOの有効化

IdPサービス適用者のログイン設定

☐ SSOでのログインのみ許可する

SAML SSOの利用設定

IdP名称	Entity ID	有効化
test	http://[redacted]	<input type="checkbox"/>
azure	https://[redacted]	<input checked="" type="checkbox"/>

更新する

2

登録するIdPの名称を入力し「ファイルを選択」→ダウンロードしたフェデレーション メタデータXMLを選択→「ファイルを読み込む」を押下し「IdPを登録する」を押下する

IdPの新規登録

IdP情報の入力

登録するIdPの名称

IdP一意に表す名称

XMLファイルの読み込み・入力

IdPからダウンロードしたXMLファイルを選択し、読み込ませてください。メタデータが自動で検出されます。
XMLファイルの読み込みができない場合、フォームに直接入力してください。

ファイルを選択

SAMLファイルを選択して下さい

ファイルを読み込む

IdPの新規登録

IdP情報の入力

登録するIdPの名称

IdP一意に表す名称

XMLファイルの読み込み・入力

IdPからダウンロードしたXMLファイルを選択し、読み込ませてください。メタデータが自動で検出されます。
XMLファイルの読み込みができない場合、フォームに直接入力してください。

ファイルを選択

SAMLファイルを選択して下さい

ファイルを読み込む

IdPの新規登録

IdP情報の入力

登録するIdPの名称

IdP一意に表す名称

XMLファイルの読み込み・入力

IdPからダウンロードしたXMLファイルを選択し、読み込ませてください。メタデータが自動で検出されます。
XMLファイルの読み込みができない場合、フォームに直接入力してください。

ファイルを選択

SAMLファイルを選択して下さい

ファイルを読み込む

IdPの新規登録

IdP情報の入力

登録するIdPの名称

IdP一意に表す名称

XMLファイルの読み込み・入力

IdPからダウンロードしたXMLファイルを選択し、読み込ませてください。メタデータが自動で検出されます。
XMLファイルの読み込みができない場合、フォームに直接入力してください。

ファイルを選択

SAMLファイルを選択して下さい

ファイルを読み込む

IdPの新規登録

IdP情報の入力

登録するIdPの名称

IdP一意に表す名称

XMLファイルの読み込み・入力

IdPからダウンロードしたXMLファイルを選択し、読み込ませてください。メタデータが自動で検出されます。
XMLファイルの読み込みができない場合、フォームに直接入力してください。

ファイルを選択

SAMLファイルを選択して下さい

ファイルを読み込む

IdPの新規登録

IdP情報の入力

登録するIdPの名称

IdP一意に表す名称

XMLファイルの読み込み・入力

IdPからダウンロードしたXMLファイルを選択し、読み込ませてください。メタデータが自動で検出されます。
XMLファイルの読み込みができない場合、フォームに直接入力してください。

ファイルを選択

SAMLファイルを選択して下さい

ファイルを読み込む

IdPの新規登録

IdP情報の入力

登録するIdPの名称

IdP一意に表す名称

XMLファイルの読み込み・入力

IdPからダウンロードしたXMLファイルを選択し、読み込ませてください。メタデータが自動で検出されます。
XMLファイルの読み込みができない場合、フォームに直接入力してください。

ファイルを選択

4

SSOでのログインのみ許可する場合は「SSOでのログインのみ許可する」に
チェックを入れ「更新する」を押下する
注) 次ページの SSOでのログインのみ許可する場合の注意事項をご参照
ください。

SAML SSOの有効化

IdPサービス適用者のログイン設定

☒ SSOでのログインのみ許可する

SAML SSOの利用設定

IdP名称	Entity ID	有効化
test	http://localhost:18080/realms/test	<input type="checkbox"/>
azure	https://sts.windows.net/d017258f-d1fd-48ab-8e2c-319e5d4b96a/	<input checked="" type="checkbox"/>

更新する

連携操作手順 SSOでのログインのみ許可する場合の注意事項

「SSOでのログインのみ許可する」を有効化する場合、パスワード認証によるログインができなくなります。

※IdPとミキワメの連携に障害が発生した場合などを考慮し、管理者権限と管理者 + ストレスチェック事務権限のみパスワード認証を利用するログインが可能です。

SSOでのログインのみ許可する場合と、SSOでのログインとパスワード認証によるログインいずれも許可する場合の違いについて、以下の表をご参照ください。

なお、SSOを有効化している社員に対して一括制御となりますので、個別で制御方法を変えることはできません。

例)【マネージャー権限は SSOでのログインのみ許可し、一般社員は SSOでのログインとパスワード認証によるログインいずれも許可する】設定は不可。

SSOでのログインのみ許可する場合

アカウントの種別	アカウントの権限	パスワード認証を利用する サインイン	SSOを利用する サインイン
管理アカウント	管理者	○	○
	管理者 + ストレスチェック事務	○	○
	マネージャー	×	○
	利用者	×	○
	運用担当者	×	○
	カスタム権限	×	○
	ストレスチェック事務従事者	×	○
一般社員アカウント	-	×	○

SSOでのログインとパスワード認証によるログイン
いずれも許可する場合

アカウントの種別	アカウントの権限	パスワード認証を利用する サインイン	SSOを利用する サインイン
管理アカウント	管理者	○	○
	管理者 + ストレスチェック事務	○	○
	マネージャー	○	○
	利用者	○	○
	運用担当者	○	○
	カスタム権限	○	○
	ストレスチェック事務従事者	○	○
一般社員アカウント	-	○	○

連携操作手順 ステップ4：社員アカウントに対して、Microsoft Entra IDのSSOを有効化する -CSV編-

1

サイドメニュー「設定」→「SSOを管理する」→
SAML SSOのアカウント紐付け設定「設定する」を押下

SSO管理

SSO管理

サービスプロバイダ情報
IdPとの連携に必要な、ミキワメのサービスプロバイダ情報を確認します。

確認する

IdP管理
IdPの新規登録や、登録済みIdPの確認・更新を行います。

IdPを管理する

SAML SSOの有効化
SAML SSO適用者のログイン設定や、IdPの有効 / 無効化の設定ができます。

設定する

SAML SSOのアカウント紐付け設定
社員アカウントに対してSAML SSOを有効化し、紐づけるIdPサービスを設定します。

設定する

2

SAML SSO設定をCSVで一括更新を押下 →SAML SSO設定CSVをダウンロードを押下し、テンプレートをダウンロード

SAML SSO設定可能アカウント一覧

SAML SSO設定を一括更新

検索条件

姓
姓を入力

名
名を入力

セイ
セイを入力

メイ
メイを入力

SAML SSO設定をCSVで一括更新
[CSVテンプレートのダウンロード](#)
CSV形式でSAML SSO設定を一括で追加・更新することが出来ます。
追加・更新用のCSVデータを作成する場合は、こちらからSAML SSO設定CSVをダウンロードしてください。
[SAML SSO設定CSVをダウンロードする](#)

CSVテンプレートの各項目の説明

3

SSOを有効化したい社員アカウントの D列に「1」を入力、E列に利用するIdPサービス名([ステップ3手順2](#) で登録した名称)を入力し、CSVを保存

	A	B	C	D	E
1	メールアドレス	氏名	所属部署	SSO有効化	利用するIdPサービス
2	sample20250	ミキワメ 太郎	部署A/部署A	1	azure
3	sample20250	ミキワメ 太郎	部署A/部署A	1	azure
4	sample20250	ミキワメ 太郎	部署A/部署A	1	azure
5	sample20250	ミキワメ 太郎	部署A/部署A	1	azure
6	sample20250	ミキワメ 太郎	部署A/部署A	1	azure
7	sample20250	ミキワメ 太郎	部署A	1	azure
8	sample20250	ミキワメ 太郎	部署B	0	
9	sample20250	ミキワメ 太郎	部署B	0	

CSV作成時の注意点

- ・D列に「1」を入力した行の E列は入力必須となります。
- ・E列に入力する名称はミキワメに登録した名称です。※ [ステップ3手順2](#) で登録した名称
- ・A～C列変更できません。
- ・テンプレートCSVから不要な行を削除した上でインポートすることが可能です。

4

「ファイルを選択」を押下し作成した CSVを選択の上、「アップロード」を押下

CSVテンプレートをアップロード

ファイルを選択

sample_sso_setting_2025-07-11 (1).csv

アップロードする

連携操作手順 ステップ4：社員アカウントに対して、Microsoft Entra IDのSSOを有効化する -手動登録編-

1

サイドメニュー「設定」→「SSOを管理する」→
SAML SSOのアカウント紐付け設定「設定する」を押下

SSO管理

SSO管理

サービスプロバイダ情報

IdPとの連携に必要な、ミキワメのサービスプロバイダ情報を確認します。

確認する

IdP管理

IdPの新規登録や、登録済みIdPの確認・更新を行います。

IdPを管理する

SAML SSOの有効化

SAML SSO適用者のログイン設定や、IdPの有効 / 無効化の設定ができます。

設定する

SAML SSOのアカウント紐付け設定

社員アカウントに対してSAML SSOを有効化し、紐づけるIdPサービスを設定します。

設定する

2

対象者の「編集」を押下

SAML SSO設定可能アカウント一覧

SAML SSO設定を一括更新

検索条件

姓

名

セイ

メイ

ミキワメ

名を入力

セイを入力

メイを入力

詳細検索を開く

条件をクリア

検索する

全 8 件

1ページに表示する件数: 25

氏名	メールアドレス	部署	連携IdPサービス	操作
ミキワメ 太郎	sample2025062001@sample.mikiwame.com	-	未連携	編集
ミキワメ 太郎	sample2025060603@sample.mikiwame.com	-	azure	編集

3

連携IdPサービスを選択し、「更新する」を押下

アカウントの編集

IdP適用者情報

以下のアカウントに対して、紐付けるIdPサービスを選択してください。

ご担当省庁氏名 ミキワメ 太郎

メールアドレス sample2025062001@sample.mikiwame.com

連携IdPサービス

azure

更新する

社員アカウントに対して、SSOを無効化する場合

CSV操作:

p.11の操作を行い、手順 3でD列に「0」を入力し、E列を空欄にしたCSVをインポートする

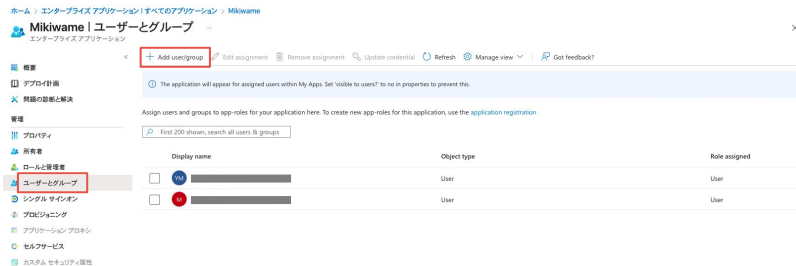
手動操作:

p.12の操作を行い、手順 3で連携IdPサービスを「未連携」にして「更新する」を押下する

連携操作手順 ステップ5：Microsoft Entra IDの社員アカウントに対して、ミキワメのSSOを有効化する

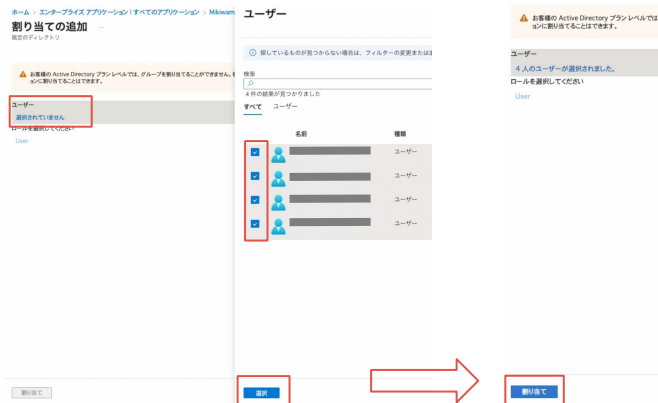
1

Microsoft Entra admin center にアクセスし、すべてのアプリケーション→「Mikiwame（例）」を選択→「ユーザーとグループ」を選択 → 「Add user/group」を押下



2

「ユーザー」を押下 → SSOを有効化したい社員にチェックを入れて、「選択」を押下 → 「割り当て」を押下する



3

招待された社員が Microsoft アカウントにログインすると、「マイアプリ」にアイコンが表示される
※社員がアイコンを押下すると認証完了



04

Chapter

よくあるご質問

よくある質問

Q1 間違って設定するとログインできなくなりますか？

A：はい。リスクはあります。

最初は管理者権限のアカウントでテストし、問題がないことを確認してから全体への適用を推奨いたします。

Q2 SSO設定後も、パスワード認証による通常ログインは使えますか？

A：管理アカウントの権限によって異なります。

管理者権限または管理者+ストレスチェック事務権限の管理者は常時パスワード認証による通常ログインが 使えます。

その他の権限の管理アカウントや一般社員アカウントは、[ステップ3](#)手順4の設定に依存します。

Q3 SSO設定はいつでも取り消せますか？

A：はい。

[ステップ3](#)手順3の操作で、「有効化」チェックを外すことでSSO設定が無効となり、パスワード認証のログイン方法に戻すことが可能です。

05

Chapter

お問い合わせ先

お問い合わせ先

本機能に関してのご質問は下記の問い合わせ窓口あてにご連絡ください。

お問い合わせ窓口：<https://mikiwame-client.zendesk.com/hc/ja/requests/new>

対応時間：平日9時から18時