【J-MOTTO 会員ログイン】

SAML 認証ログインマニュアル

[Microsoft365 用]

目次

1　はじめに

【概要】
Azure（Microsoft365）の SAML 認証の仕組みを使い J-MOTTO サイトに通常は「会員 ID」「ユーザーID」「パスワード」の 3 要素でログインして頂いたものを Microsoft365 のログイン方法に統一できます。
本書では前提条件や注意事項、管理者による設定の手順について説明します。

【前提条件】
SAML によるログイン連携を行うには、「Azure」の「エンタープライズアプリ」機能に当社専用のアプリケーション（SAML 認証用）を設定頂く必要があります。

その為、Microsoft365 のご契約においてもこの「Azure」および「エンタープライズアプリ」の設定が可能であることがご利用の条件になります。

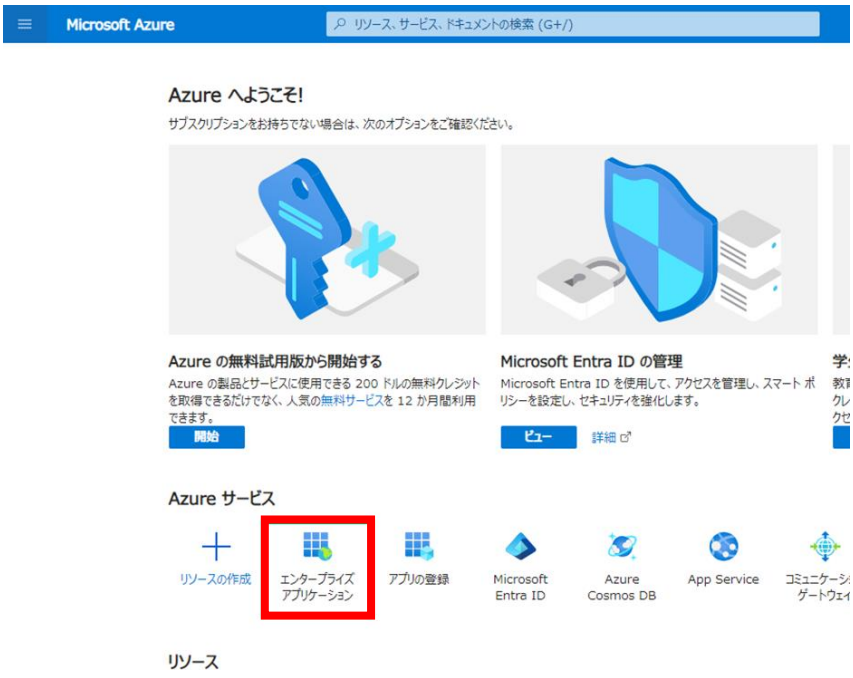
【行程概要】
① Azure 側のエンタープライズアプリケーションに SAML 設定をおこなう
② Azure 側の SAML 設定から必要ファイルを二つダウンロードする
③ J-MOTTO サイト上の会員情報管理の専用設定画面からダウンロードしたファイルをアップロードする
④ SAML ログインさせたいユーザーに対して、Azure 側のエンタープライズアプリケーションの利用権限を付与する
⑤ J-MOTTO 会員情報管理のユーザー情報「メールアドレス」を Azure 側の UPN と対応させる
※例：00001 のメールアドレス設定を（00001 を使うユーザーの）UPN に変更し、他に重複がないか確認する
⑥ SAML ログインさせたいユーザーに SAML ログイン専用の URL を伝える

2　初期設定（Azure）

エンタープライズアプリケーションの作成

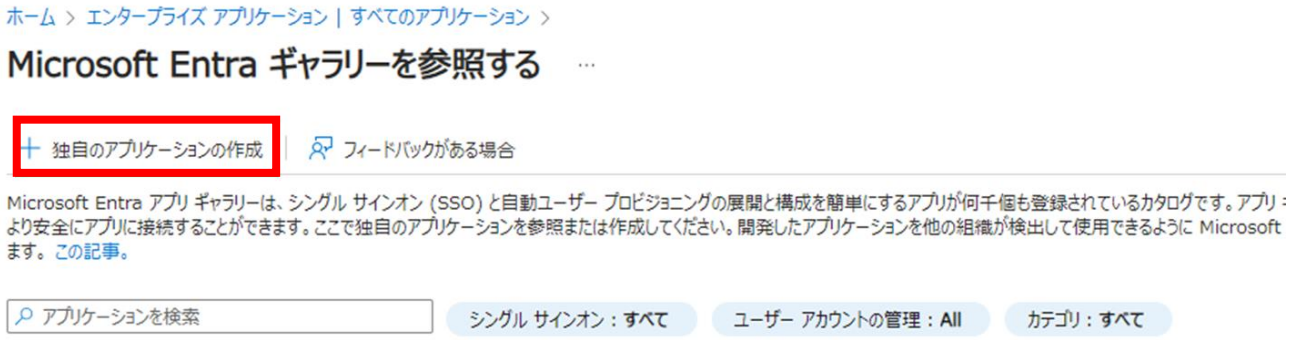
本操作では Microsoft365（Azure）における管理者権限で設定してください。
SAML 認証が利用できるように Azure に「エンタープライズアプリケーション」を設定します。

お客様ご契約の Microsoft365（Azure）にログインします。
Azure のサイドメニューから「エンタープライズ　アプリケーション」を選択します。



「新しいアプリケーション」をクリックします。

「独自のアプリケーションの作成」をクリックします。クリック後、作成用のメニューが開きます。



「お使いのアプリの名前は何ですか？」に対して弊社用の SAML 設定であることがわかる名前を自由につけてください。
ただし、Azure 内で公開されている他のアプリケーション名称と同じにはできません。
「Integrate any other application you don't find in the gallery (Non-gallery)」を選択し、メニュー最下段の「作成」ボタンを押してください。（「作成」ボタンが離れているため、押し忘れないようにご注意ください）

「⑥」の作成後に付けて頂いたアプリケーションの名前のプロパティが表示されれば準備は完了です。そのまま次の設定をおこないます。

エンタープライズアプリケーションの設定

「シングルサインオンの設定」の「作業の開始」リンクをクリックします。

初回はシングルサインオン方式を選択しますので、「SAML」を選択します。

SAML 設定画面になりますので「識別子（エンティティ ID）」と「応答 URL」を設定します。
まずは「編集」のボタンをクリックします。

専用のメニューが表示されます。
「識別子（エンティティ ID）」には 「j-motto.co.jp/login」 と設定してください。
j-motto.co.jp/login　以外が設定されている場合には SAML 機能が働かず、ログインできません。

「応答 URL」には「**https://www2.j-motto.co.jp/saml/sso**」を設定してください。
設定できましたら「保存」してください。
※識別子や応答 URL は Azure 設定上、複数設定できますが必ず一つずつです。

保存後、このような状態になっていればエンタープライズアプリケーションの設定は完了です。
※ほかの項目はデフォルト（変更なし）のままとしてください。

3　初期設定（J-MOTTO／会員情報管理画面への設定）

本操作では Microsoft365（Azure）における管理者権限　および
J-MOTTO の会員情報管理に管理者でアクセスできる方で設定してください。
※J-MOTTO「グループウェア」の管理者権限は必要ありません。

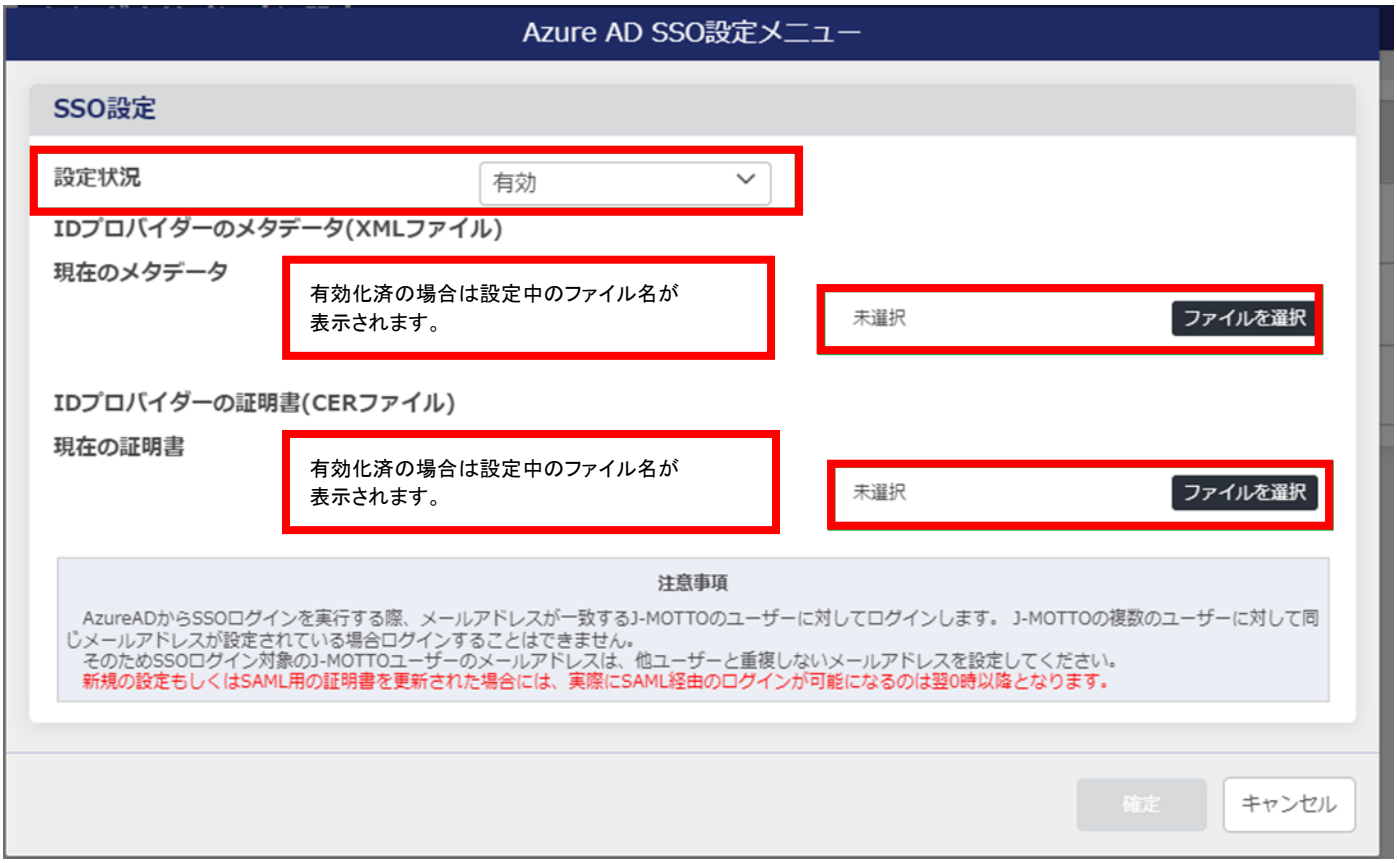
Azure から会員情報管理で使うファイルをダウンロード

エンタープライズアプリケーションの設定（識別子や応答 URL の設定）で利用した SAML 設定画面を表示します。
その画面上の項目③にある「SAML 署名証明書」の項目にダウンロードのリンクが3つあります。
「証明書（BASE64）」と「フェデレーションメタデータ XML」の二つをダウンロードします。
※「証明書（未加工）」は利用しません。誤ってこのファイルを利用した場合は正常にログインできません。

会員情報管理画面に証明書とフェデレーションメタデータ XML をアップロード

J-MOTTO の管理者権限でログインすると、管理者メニューに専用のメニューがありますので「設定一覧」をクリックすると、Azure の項目が出ますので変更ボタンをクリックします。

設定メニューが表示されます。
Azure から会員情報管理で使うファイルをダウンロードした二つのファイル（XML 形式、CER 形式）をアップロードします。
「現在のメタデータ」に XML 形式のファイルを、「現在の証明書」に CER 形式のファイルを選択、アップロードし、最後に確定ボタンを押してください。実際にファイルがアップロードされ、設定が完了します。



SAML 認証はこれでいつでも利用できる状態になりました。
次は実際に一般ユーザーで利用を開始するまでをご案内します。

4　ログイン許可について

SAML の仕組みと制限事項

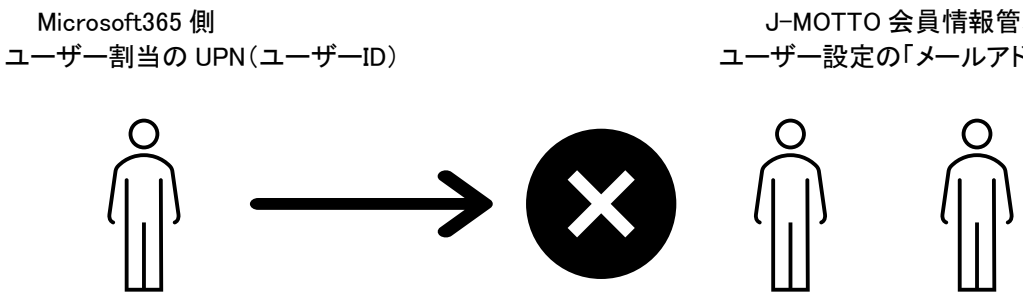
SAML 認証は Azure 上ではアプリケーションの形になっており、そのアプリケーションの利用許可の形で J-MOTTO へのシングルサインオンの利用／利用不可を制御可能です。

設定完了の直後はアプリケーションの利用許可がありませんので、許可するユーザーに対しては本手順書で作成したアプリケーションの利用許可を与えてください。
※J-MOTTO「グループウェア」の管理者権限は必要ありません。

なお、ログイン許可するユーザーについては、事前に J-MOTTO 側のユーザー設定において Microsoft365 からそのユーザーに割り当てられている「UPN」（メールアドレス形式で、お客様によっては UPN＝メールアドレスの場合もあり）を J-MOTTO ユーザー設定の「メールアドレス」に設定してください。
※グループウェア内の通知先メールアドレスではありません。

特に注意頂きたいこと

一つの UPN を、複数の J-MOTTO ユーザーの「メールアドレス」に設定しないでください。
グループウェア内の「プロフィール」は SAML 認証で利用しておりませんので重複しても問題ありません。



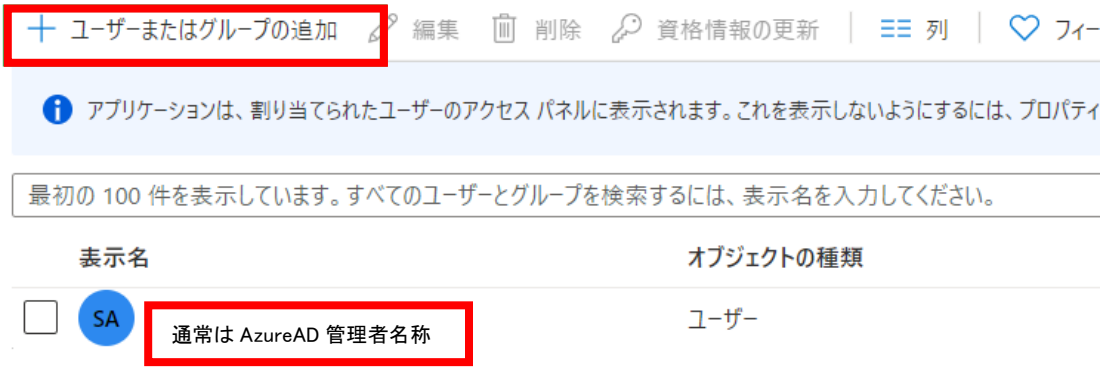
J-MOTTO においてはこの「UPN」の情報と会員情報管理上のユーザー情報「メールアドレス」を照合してユーザーID（数字五桁）の部分を特定し、ログイン済情報をログイン者（ブラウザ）に渡します。
そのため、Microsoft365 の一つの UPN を J-MOTTO 側の複数アカウントに同時に設定された場合には、SAML 認証としてはどのユーザーID がログイン対象者か特定ができないため、J-MOTTO 画面ではログインエラーとなりますのでご注意ください。

例：一つの UPN を会員情報管理画面の複数のユーザー情報に登録していた場合のエラー画面例

Azure での実際の許可設定

Azure にログインし、エンタープライズアプリケーションから作成して頂いたアプリケーションの名前をクリックして設定に入ります。今回は「ユーザーとグループの割り当て」をクリックします。

ユーザー追加（削除）画面になりますので、Azure（Microsoft365）としてこの SAML 認証アプリケーションの利用許可を追加、削除してください。
削除の場合はユーザーを選択してから「削除」のアイコンをクリックします。
※Microsoft365 の契約プランにより Azure 側の制限として「グループ単位」での設定ができない場合があります。その場合はお手数でもユーザー単位での設定をお願いします。



管理者側の設定は以上になります。

5　一般ユーザー向け（ログインの仕方について）

本操作で Microsoft365 のログイン画面を利用した J-MOTTO グループウェアログインの方法をご案内します。

手順1
以下の URL にブラウザで直接アクセスします。
（ブラウザのお気に入りなどに登録されても構いません）
https://www2.j-motto.co.jp/web/doLogin/（会員 ID）

例：
https://www2.j-motto.co.jp/web/doLogin/JM0000000

手順2
J-MOTTO サイトからのログインとは異なり、（手順1の URL に対応した）会員 ID が表示されたページになりますので、会員 ID をご確認の上、「Microsoft365 ログイン」をクリックしてください。

手順3
Microsoft365 のログイン画面になるので「Microsoft365 ログイン」で普段利用されている ID と PW でログインをしてください。ログイン成功後はグループウェアの画面となります。

注意点
Microsoft365 のログイン画面でエラーが出て場合は普段ご利用中の Microsoft365 の ID、パスワードの入力に誤りがないかご確認ください。
J-MOTTO のサイト画面でエラーが出た場合は、管理者による利用許可がされていない場合がありますので、お客様で Microsoft365 を管理されている管理者にご相談ください。

お客様ご契約の Microsoft365 のパスワードについては、J-MOTTO お客様サポートセンターではお答えできませんのでご注意ください。

お問合せ

J-MOTTO お客様サポートセンター	
TEL	0120-70-4515（通話料無料） 平日 10:00～17:00（土・日・祝日休）
チャット	https://www.j-motto.co.jp/00000000/manual/ （上記 WEB サイト内右下部） 平日 09:00～18:00（土・日・祝日休）
メール	support@j-motto.co.jp

ご不明な点がございましたら、お気軽にお問合せください。