

# SAML設定方法

AzureAD編

Ver 2.1



Azure Active Directory(以下、AzureAD)とムービーライブラリはSAML認証を用いて、連携することができます。

SAML認証をご利用いただくには、あらかじめサービスを提供するムービーライブラリ(SP)と認証情報を提供するAzureAD(IdP)間で信頼関係を結ぶ必要があります。

信頼関係を結ぶに当たって、下記を実施いただく必要があります。

1. AzureADへ「アプリケーション」の追加
2. AzureADアプリケーションプロパティ設定
3. フェデレーションメタデータドキュメントURLの取得
4. フェデレーションメタデータドキュメントURLの提供

※IdPによって信頼関係を結ぶ正確なプロセスは異なります。詳細については、ご利用のID管理ソフトウェアのドキュメントを参照して下さい。





AzurePortalへログインし、連携を行いたいAzureADテナントにて、  
[アプリの登録] - [新規登録] を選択します。

検索 (Ctrl+/) << ②+ 新規登録 ①+ エンドポイント トラブルシューティング

新しく改良されたアプリの登録 (一般提供になりました) へようこそ。

すべてのアプリケーション 所有しているアプリケーション

名前またはアプリケーション ID を入力し始めると結果がフィルタ

表示名

ML	ML
Mラ	Mライブラリ

①+ アプリの登録

Identity Governance





表示されるアプリケーションの作成画面にて、以下の情報を入力し、登録します。

名前: **任意のアプリケーション名 (例、ムービーライブラリ)**

リダイレクトURL選択: **Web** URL: **https://ml.visuamall.com/(システムID)/saml**

## アプリケーションの登録

\* 名前

このアプリケーションのユーザー向け表示名 (後で変更できます)。

①

サポートされているアカウントの種類

このアプリケーションを使用したりAPIにアクセスしたりできるのはだれですか?

- この組織ディレクトリのみに含まれるアカウント (ソフトバンク株式会社TU 技術管理本部ビジネスモデルのみ - シングルテナント)
- 任意の組織ディレクトリ内のアカウント (任意の Azure AD ディレクトリ - マルチテナント)
- 任意の組織ディレクトリ内のアカウント (任意の Azure AD ディレクトリ - マルチテナント) と個人の Microsoft アカウント (Skype, Xbox など)

[選択に関する詳細。](#)

リダイレクト URI (省略可能)

ユーザー認証が成功すると、この URI に認証応答を送ります。この時点での指定は省略可能で、後ほど変更できますが、ほとんどの認証シナリオで値が必要となります。

②

※システムIDはご利用環境のURLの以下の部分と同じ値です。  
https://ml.visuamall.com/**システムID**/クライアントID/xxx/xxx/

続行すると、Microsoft プラットフォームポリシーに同意したことになります。

③

アプリケーションIDのURIを設定を行います。  
【アプリケーションID URIの追加】をクリックします。

The screenshot shows the Azure AD application properties page for an application named 'ムービーライブラリ' (Movie Library). The page is divided into a left-hand navigation pane and a main content area. The navigation pane includes sections for '概要' (Overview), '管理' (Management), and 'サポート + トラブルシューティング' (Support + Troubleshooting). The main content area features a search bar, a list of actions (Delete, End Point), and a table of properties. A red dashed box highlights the 'アプリケーションIDのURI' (Application ID URI) property, which is currently set to 'アプリケーションID URIの追加' (Add Application ID URI). A red circle with the number '1' is placed next to this property. Below the table, there is a message about app registration and a section for 'APIの呼び出し' (API Calls) with various Microsoft service icons. On the right side, there is a 'ドキュメント' (Documents) section with links to various resources.

ムービーライブラリ

検索 (Ctrl+F)

削除 エンドポイント

少しお時間があれば、Microsoft ID プラットフォーム (以前は開発者向け Azure AD) に関するフィードバックをぜひお寄せください。 →

表示名	: ムービーライブラリ	サポートされているアカウント...	: 所属する組織のみ
アプリケーション (クライアント)...	:	リダイレクト URI	: 1 Web, 0 パブリック クライアント
ディレクトリ (テナント) ID	:	アプリケーション ID の URI	: <b>アプリケーション ID URI の追加</b>
オブジェクト ID	:	ローカルクライアント向けのマネ...	: ムービーライブラリ

新しく強化されたアプリの登録へようこそ。アプリの登録 (レガシ) からの変更点を確認することをご希望ですか? [詳細情報](#)

### API の呼び出し

Microsoft サービスと自社の独自のデータ ソースからの豊富なユーザー データおよびビジネス データを使用して、より強力なアプリを作成します。

[API アクセス許可の表示](#)

### ドキュメント

- Microsoft ID プラットフォーム
- 認証シナリオ
- 認証ライブラリ
- コード サンプル
- Microsoft Graph
- 用語集
- ヘルプとサポート

【アプリケーションIDのURI設定】をクリックして、以下情報を保存します。

アプリケーションIDのURI: `api://xxxxxxx`

※xxxxxx部分はAzureより自動で払い出される文字列となります

ムービーライブラリ - API の公開

検索 (Ctrl+/) **1** アプリケーション ID の URI の設定

この API で定義されているスコープ

API によって保護されているデータと機能に対するアクセスを制限するために、この API の一部にアクセスする必要があるアプリケーションで、スコープを定義します。この API の一部にアクセスする必要があるアプリケーション

ムービーライブラリ | API の公開

検索 (Ctrl+/) << フィードバックがある場合

アプリ ID の URI の設定

アプリケーション ID の URI

api:// [REDACTED]

**2** **3** 保存 破棄

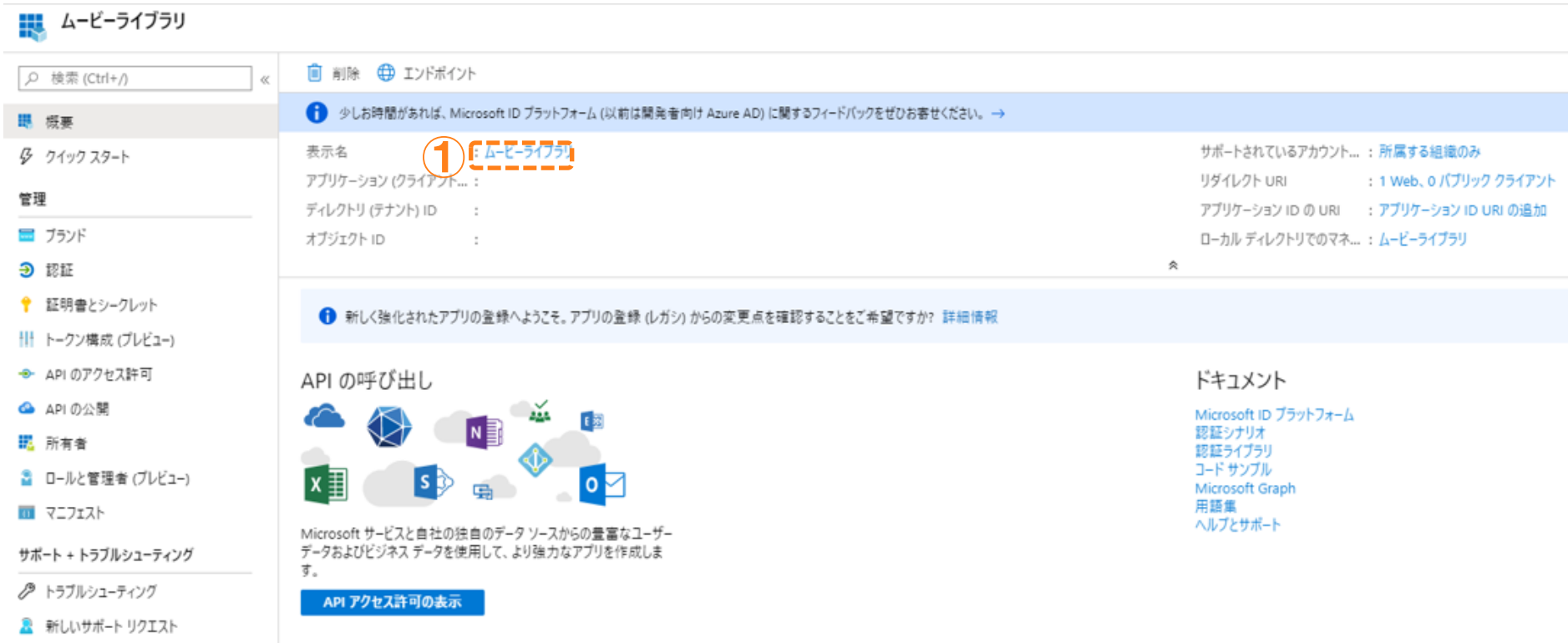
こちらにスコープを追加すると、委任されたアクセス許可のみが作成されます。アプリケーション専用スコープを作成可能なアプリ ロールを定義してください。[アプリ ロール] に移動します。

+ Scope の追加

スコープ	同意できるユーザー	管理者

スコープは定義されませんので、か

ホームページURLの設定を行います。  
【任意のアプリケーション名】をクリックします。



ムービーライブラリ

検索 (Ctrl+/) <<

削除 エンドポイント

少しお時間があれば、Microsoft ID プラットフォーム (以前は開発者向け Azure AD) に関するフィードバックをぜひお寄せください。 →

表示名 **1** **ムービーライブラリ**

アプリケーション (クライアント)... :

ディレクトリ (テナント) ID :

オブジェクト ID :

サポートされているアカウント... : 所属する組織のみ

リダイレクト URI : 1 Web、0 パブリック クライアント

アプリケーション ID の URI : アプリケーション ID URI の追加

ローカル ディレクトリでのマネ... : ムービーライブラリ

新しく強化されたアプリの登録へようこそ。アプリの登録 (レガシ) からの変更点を確認することをご希望ですか? [詳細情報](#)

API の呼び出し

Microsoft サービスと自社の独自のデータ ソースからの豊富なユーザー データおよびビジネス データを使用して、より強力なアプリを作成します。

[API アクセス許可の表示](#)

ドキュメント

- Microsoft ID プラットフォーム
- 認証シナリオ
- 認証ライブラリ
- コード サンプル
- Microsoft Graph
- 用語集
- ヘルプとサポート

以下情報を入力して保存します。

ホームページURL(推奨値・・・ムービーライブラリのログインページURL):

[https://ml.visuamall.com/\(システムID\)/\(クライアントID\)/login/login.php?c=xx](https://ml.visuamall.com/(システムID)/(クライアントID)/login/login.php?c=xx)

※システムID・クライアントIDはご利用環境のURLの以下の部分と同じ値です。

<https://ml.visuamall.com/システムID/クライアントID/xxx/xxx/>

ムービーライブラリ - ブランド

検索 (Ctrl+/) 3 保存 ✕ 破棄

**概要**

クイックスタート

管理

- ブランド
- 認証
- 証明書とシークレット
- トークン構成 (プレビュー)
- API のアクセス許可
- API の公開
- 所有者
- ロールと管理者 (プレビュー)
- マニフェスト

サポート + トラブルシューティング

- トラブルシューティング
- 新しいサポート リクエスト

名前 \* 1

ロゴ 指定されていません

新しいロゴのアップロード

ホームページ URL 2  ✓

サービス利用規約 URL

プライバシーに関する声明の URL

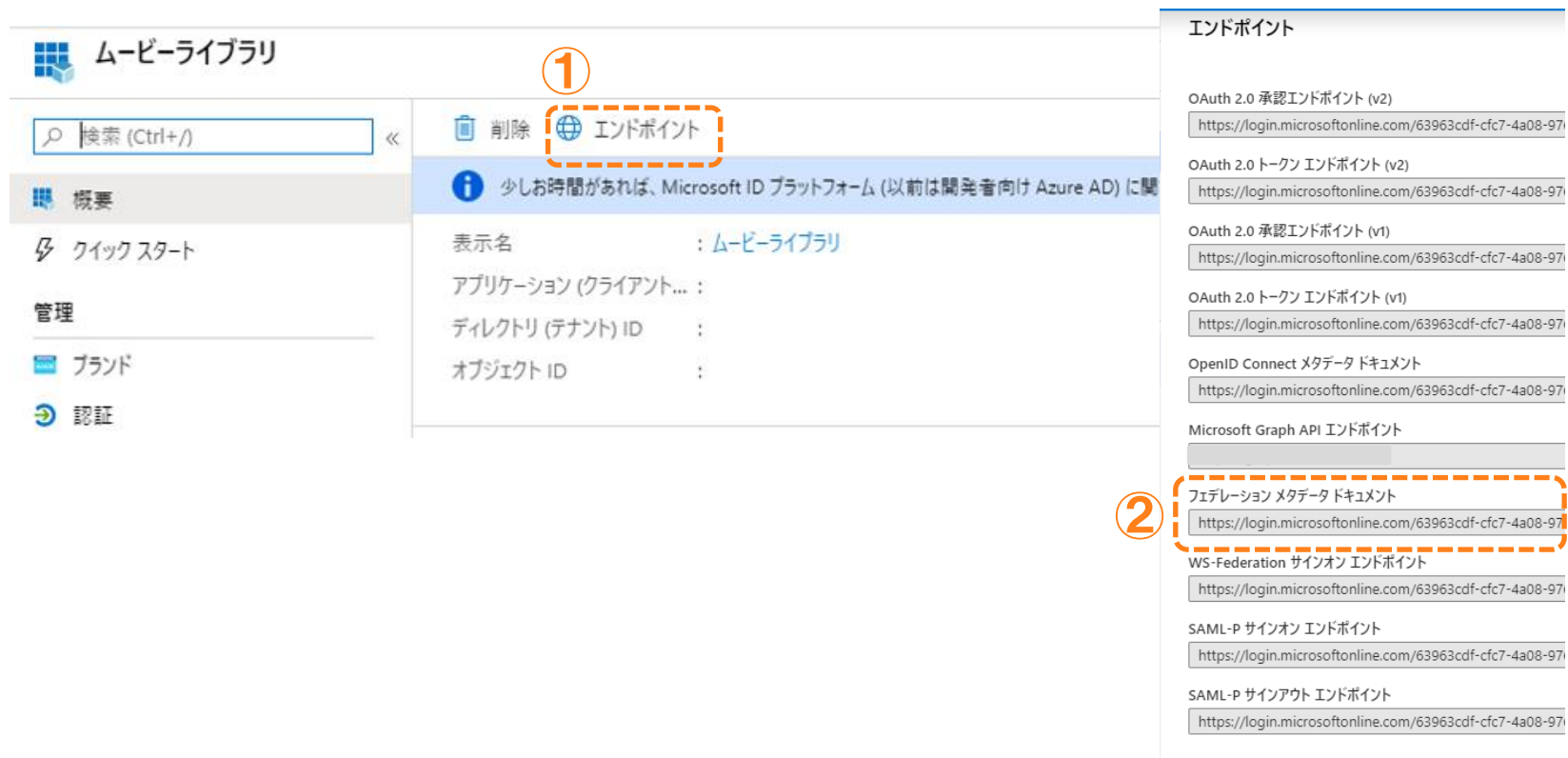
パブリッシャー ドメイン ⚠  ドメインを更新します

アプリケーションの同意画面に [未確認] と表示されます。  
パブリッシャー ドメインの詳細をご確認ください



アプリ登録後、ムービライブラリへSSOするために必要な、  
フェデレーションメタデータドキュメントURLを取得します。

[エンドポイント] - [フェデレーションメタデータドキュメント] よりURLをコピーします。



ムービライブラリ

① エンドポイント

削除

② フェデレーションメタデータドキュメント

https://login.microsoftonline.com/63963cdf-cfc7-4a08-97...

OAuth 2.0 承認エンドポイント (v2)  
https://login.microsoftonline.com/63963cdf-cfc7-4a08-97...

OAuth 2.0 トークン エンドポイント (v2)  
https://login.microsoftonline.com/63963cdf-cfc7-4a08-97...

OAuth 2.0 承認エンドポイント (v1)  
https://login.microsoftonline.com/63963cdf-cfc7-4a08-97...

OAuth 2.0 トークン エンドポイント (v1)  
https://login.microsoftonline.com/63963cdf-cfc7-4a08-97...

OpenID Connect メタデータドキュメント  
https://login.microsoftonline.com/63963cdf-cfc7-4a08-97...

Microsoft Graph API エンドポイント

WS-Federation サインオン エンドポイント  
https://login.microsoftonline.com/63963cdf-cfc7-4a08-97...

SAML-P サインオン エンドポイント  
https://login.microsoftonline.com/63963cdf-cfc7-4a08-97...

SAML-P サインアウト エンドポイント  
https://login.microsoftonline.com/63963cdf-cfc7-4a08-97...



以下2点をお申込書に記載いただき、弊社営業へご連絡下さい。

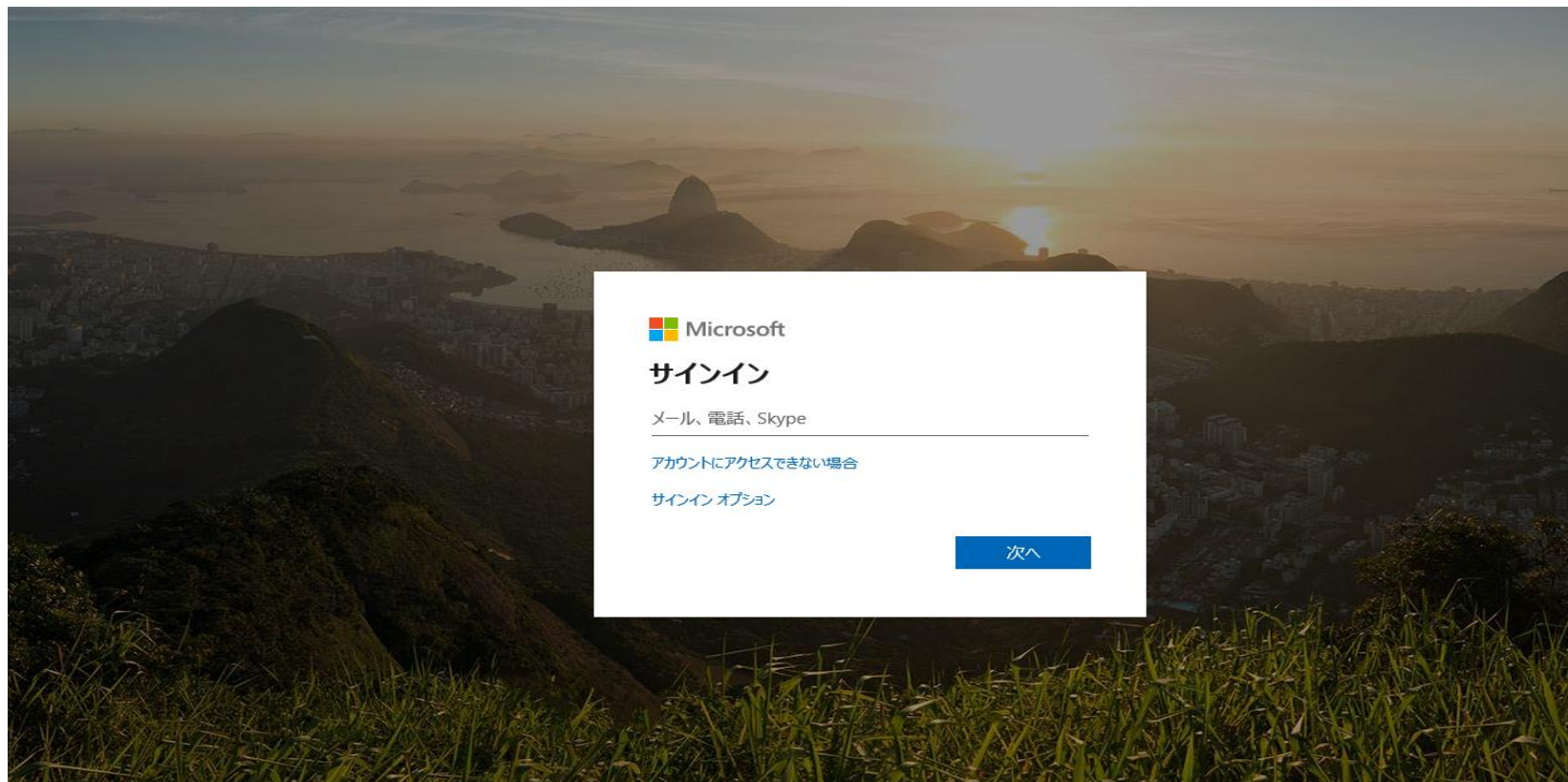
- ・アプリケーションIDのURI(項目番号2-1-2)
- ・フェデレーションメタデータドキュメントURL(項目番号3)

ムービーライブラリ(SP)側の設定が完了し、SAML認証をご利用いただける準備が整いましたらご連絡いたします。

# 参考情報



SAML認証を有効にしたムービーライブラリ環境にアクセスすると、下記Azureのログイン画面にリダイレクトされます。  
AzureADにてアクセスを許可されたユーザにてログイン可能です。  
ログイン認証後、ムービーライブラリのトップページへと遷移します。



ムービーライブラリにおけるSAML認証は、シングルサインオン機能のみを提供しており、AzureAD及びムービーライブラリ間でのアカウントの同期を行うことは出来ません。  
あらかじめ、ムービーライブラリ内にご利用になられるADユーザと同等のアカウントを作成いただく必要があります。

アカウントの作成については、ムービーライブラリの管理者機能をご利用いただくか、提供済みのREST APIをご活用いただくことをご検討下さい。

[APIマニュアルはこちら](#)



ご質問内容	回答
Microsoftアカウントでログインしたところ、「申し訳ありませんが、サインイン中に問題が発生しました。正しくない要求を受信しました。」と表示されます。	AzureADの登録済みアプリのプロパティにて、「アプリケーション ID/URI」の値が「 <a href="https://ml.visuamall.com/システムID/saml">https://ml.visuamall.com/システムID/saml</a> 」となっているかご確認ください。(※URLの最後に「スラッシュ(/)」が入っていないこと。) 上記編集後は、Microsoftアカウントを一度ログアウトの上、再度ムービーライブラリのログインURLへアクセスください。
Microsoftアカウントでログイン後、ムービーライブラリへリダイレクトされたが、「お客様のアカウント情報がありません。」と表示されます。	ログインされたMicrosoftアカウントのメールアドレスと同じメールアドレスがムービーライブラリに登録されていない可能性があります。ムービーライブラリへアカウントの登録をお願いします。
SAMLログインを行うにあたって、AzureADに所属済みのMicrosoftアカウントをムービーライブラリへ全て登録する必要がありますか？	ムービーライブラリへSAMLログインを許可するユーザのメールアドレスをムービーライブラリへ登録する必要があります。IdpとSP間でのアカウント同期機能は提供しておりませんので、都度更新いただく必要があります。その際、ムービーライブラリの管理者機能「アカウントExcelデータ取込」をご利用いただくことをオススメします。
Microsoftアカウントのパスワードとムービーライブラリへ登録するアカウントのパスワードは一致させる必要がありますか？	一致させる必要はありません。
AzureAD側でユーザまたはグループへアプリの利用権限を設定することで、ムービーライブラリへのログインを制限できますか？	できません。AzureAD側の権限情報は引き継がれませんので、ムービーライブラリへログインさせたくない場合は、ムービーライブラリ側にアカウントを登録しないようにしてください。
Microsoftアカウントをログアウトすると、ムービーライブラリもログアウトされますか？	ログアウトされません。ログインから24時間が経過するか、ブラウザを全て閉じていただく事でログアウトされます。



# MOVIE LIBRARY

powered by visuamall