

## Safie Manager SSO・ディレクトリ連携設定マニュアル

Microsoft Entra ID編

セーフィー株式会社



#### はじめに



- 本書はSafie 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Safie 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。
- 多くの手順でMicrosoft Azure ADとSafie Managerを行き来しながら 設定します。両方の画面を開いた状態で作業してください。
- 設定に際しては必ず本書の手順通りに行ってください。異なる手順で行った場合、連携に失敗する場合があります。





## • シングルサインオン

- 設定の流れ
- Safie Managerの初期設定
- Microsoft Entra IDの設定
- Safie Managerの設定
- 動作確認





### ディレクトリ連携

- 設定の流れ
- Safie Managerの初期設定
- Microsoft Entra IDの設定
- 動作確認





## シングルサインオン



#### シングルサインオンの設定は以下の手順で行います。

- 1. Safie Managerの初期設定
  - 1.1. Safie 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. Safie 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
  - 3.3. SSO有効化
- 4. SSOの動作テスト



## Safie Managerの初期設定



- 以下のURLにアクセスし、Safie Managerにログインしてください <u>https://safie.link/manager/#/login</u>
- ログイン後、画面右上の赤枠部が「全体管理者」であることを確認してください
  - ※「管理者」となっている場合、以降の手順が行えません





- サイドメニューの管理設定の画面からSSO・ディレクトリ連携設定タ ブをクリック
- 「企業別認証IDの発行」をクリック
- 確認のダイアログが表示されるので「続行」をクリック





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

<	権限	ログイン履歴	接続/切断履歴	SSO・ディレクトリ連携設定	
♠ ホーム			AND A CONTRACT		
デバイス	IdPへの登録	清報			
🗈 デバイスグループ	SSO URL(ACS)				
▲ ユーザー					<i>@</i> コピー
😫 ユーザーチーム	SSO Entity ID				
🎤 運用設定 🔹 🔨					<i>@</i> コピー
✿ 管理設定	SCIM用URL				
					<i>®</i> コピー
	シークレットト	ークン			
	未発行				発行
	IdP情報				
	IDプロバイダー	のログインページのURL 👸			
					8
© Safie Inc.	IDプロバイダー	の識別子のURL 必須			

**Safie** 



## Microsoft Entra IDの設定



以下のURLにアクセスし、Azureにログインしてください
 <u>https://portal.azure.com/#home</u>

 上部の検索フォームに「エンタープライズ」と入力し、「エンタープ

ライズアプリケーション」のメニューに遷移してください



#### 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

遷移先の画面で「独自のアプリケーションの作成」をクリック

≡ Microsoft Azure	ノロ リソース、サービス、ドキュメントの検索 (G+/)		⊵ Ç Q	© ©	ନ		
ホーム > エンタープライズ アプリク	<b>ノーション</b>						
エンタープライフ セーフィー株式会社 - Azure /	<b>、アプリケーション</b>  すべてのアフ Active Directory	プリケーション …					
概要	≪ + 新しいアプリケーション ひ 更	匣新 🚽 ダウンロード (エクスオ	ポート)   🚺 プレと	ニーの情報 🕴	■■ 列		
<ol> <li>概要</li> </ol>	Azure AD テナントを ID プロ	Microsoft Azure	P リソース、サ	ービス、ドキュメント(	の検索 (G+/)		Q 🚳
🗙 問題の診断と解決	▶ アプリケーションの名前または	> エンタープライズ アプ	リケーション >				
管理	アプリケーションの種類 == エ	Azure AD ギャラ	リーの参照				
🗰 すべてのアプリケーション	6 個のアプリケーションが見つかりま	and a set of second a	_				
🐻 アプリケーション プロキシ	名前 ↑↓ オブ	名前 ↑→ オブ 十 独自のアプリケーションの作成 🖗 フィードバックがある場合					
🔅 ユーザー設定	SA 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タログです。アプリ ギー						
🍱 コレクション	SA SA この記事。 されたナソノレートを活用して、ユーサーをより安全にアノリに接続することかできます。ここで独自のアノリゲーションを参照または作成してくたさい。他の組織が ンを Azure AD ギャラリーに公開する場合は、次に説明されているプロセスを使用して要求を提出できます。この記事。						
セキュリティ	SA	₽ アプリケーションを検索		シングル	サインオン・すべて	フーザー アカウントの管理: All	カテゴリ・す/
🔩 条件付きアクセス	SA					- / ///////////////////////////////////	
		クラウド プラットフォーム					
		Amazon Web S	Services (AWS)		Google Clo	ud Platform	
		av	VS		6	3	(





#### 画面右に作成画面が表示されるので、以下の情報を入力

- 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
- 入力が終わったら「作成」をクリック

E Microsoft Azure アリソース、サービ	「ス、ドキュメントの検索 (G+/) ・・・・ 🤐
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 …	独自のアプリケーションの作成 ×
	🔗 フィードバックがある場合
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	独自のアプリケーションを開発している場合、アプリケーション プロキシを使用している場合、またはギャラリーに ないアプリケーションを統合する必要がある場合は、ここで独自のアプリケーションを作成できます。
19 るとさに、争前に構築されたナプノレートを活用して、ユーザーをより 織が検出して使用できるように、開発したアプリケーションを Azure Al	お使いのアプリの名前は何ですか? アプリケーション名
クラウド プラットフォーム	アフリケーションでどのような操作を行いたいですか?
Amazon Web Services (AWS)	○ アプリケーションを登録して Azure AD と統合します (開発中のアプリ)
aws	<ul> <li>ギャラリーに見つからないその他のアプリケーションを統合します (ギャラリー以外)</li> </ul>

#### 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

三 Microsoft Azure Pリソー	ス、サービス、ドキュメントの検索 (G+/)	$\mathbf{\Sigma}$	Ŗ	Q	٢	0	ন্দ		セーフィー	 株式会社
ホーム >										
エンタープライズ アプリケーション	概要 …									)
«										
14 税要	プロパティ									
🛄 デプロイ計画	名前①									
管理	JA D									
11 วือパティ	アプリケーション ID ③									
🎎 所有者										
歳 ロールと管理者										
🎎 ユーザーとグループ	Catting Stantad									
∋ シングル サインオン	Getting Started									
⑦ プロビジョニング										
🐯 アプリケーション プロキシ	1。ユーザーとグループの割り当て			Э	2。シン	グルサ	インオン	の設定		11
☺ セルフサービス	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	7			ユーザーて、アフ	が自分 リケーシ	の Azure ョンにサイ	AD 資格帽 ンインできる	青報を使用し ようにする	
🧾 カスタム セキュリティ属性 (プレビュー)	ユーザーとグループの割り当て				作業の	開始				
セキュリティ			_							

#### 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

	ス、サービス、ドキュメントの検索 (G+/)	区 頃 Q 懲 ⑦ タ <sup>-</sup> t-74-株5					
$\pi - 4 > $ safie-manager-sso-test-frontend							
ションタープライズ アプリケーション	シングル サインオン	/					
≪ ■ 概要 ① デブロイ計画 管理	シングルサインオン (SSO) により、組織内のユーザーが、自分が低め、ユーザーが Azure Active Directory のアプリケーションにサイログインすると、その資格情報は、そのユーザーがアクセスする必要ださい。	使用しているすべてのアブリケーションに、1 つのアカウントでサインインできるようにな 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 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					
プロパティ & 所有者	シングル サインオン方式の選択 判断	行に役立つヘルプの表示					
<ol> <li>ロールと管理者</li> <li>ユーザーとグループ</li> </ol>	魚 無効	C SAML					
<ul> <li>シングルサインオン</li> <li>プロビジョニング</li> </ul>	シングル サインオンか有効になっていません。 ユーザーは、[マイ アブリ] からアブリを起動で きません。	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。					
<ul> <li>アプリケーション ブロキシ</li> <li>セルフサービス</li> </ul>							
🧾 カスタム セキュリティ属性 (ブレビュー)							
セキュリティ 	パスワードベース Web ブラウザーの拡張機能またはモバイルア プリを使用したパスワードの保存と再生。	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。					

#### 基本的なSAML構成の右上にある編集ボタンをクリックして編集画面 を表示します

ホーム > エンタープライズ アプリケーシ	ν=Υ >
エンタープライズ アプリケーション	SAML ベースのサインオン … ×
👪 概要	≪ ▼ メタデータ ファイルをアップロードする り シングル サインオン モードの変更 ・・・
🛄 デプロイ計画	SAML によるシングル サインオンのセットアップ
管理	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
プロパティ	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。
🏞 所有者	以下をお読みください 構成ガイド 🗗 🥼 を統合するためのヘルプ。
🚨 ロールと管理者	
🎎 ユーザーとグループ	● 基本的な SAML 構成 ② 編集
Э シングル サインオン	識別子 (エンティティ ID) 広答 LIRL (Assertion Consumer S
🖏 プロビジョニング	ervice URL)
🐻 アプリケーション プロキシ	サインオン URL 「レー状態 (首略可能) 首略可能
😔 セルフサービス	ログアウト URL (省略可能) <i>省略可能</i>
🧾 カスタム セキュリティ属性 (ブレビュー	
++11ティ	■ 属性とクレーム   ② 編集

#### 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Safie Manager側の情報を転記します
- 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

<		🔛 保存 🛛 🔗 フィードバックがある場合
★ ホーム	権限 ロクイン腹歴 技術/切断腹歴	🚯 SAML 構成エクスペリエンスのこのプレビューを終了しますか? ここをクリックすると、プレビューが終了します。 →
デバイス	IdPへの登録情報	識別子 (エンティティ ID) * ①
デバイスグループ	SSO URL(ACS)	Azure Active Directory に対してアプリケーションを識別する一意の ID。この値は、Azure Active Directory テ ナント内のすべてのアプリケーションで一意である必要があります。既定の識別子は、IDP で開始された SSO の
▲ ユーザー	https://app.st.safie.link/user/sso/ /authorize	SAML 応答の対象ユーザーになります。
ユーザーチーム	SSO Entity ID	既定
▶ 運用設定 >	https://app.st.safie.link/api/sso/ /meta	■ 「「」 一 ① ■ 識別子の追加
✿ 管理設定	IdP情報	応答 URL (Assertion Consumer Service URL) * ① 応答 URL は、アブリケーションが認証トークンを受け取る場所です。これは、SAML では \*Assertion Consumer Service\* (ACS) とも呼ばれます。
		イン 既定
	IDプロバイダーの識別子のURL 🛛 👸	▶ ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●
		サインオン URI (省略可能)

¶safie

×

シングルサインオン設定から「属性とクレーム」の画面の編集ボタン
 をクリックしてください



#### 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

😑 Microsoft Azure 🔎 リソース、サービス、ドキュメン	/トの検索(G+/) 🖸 🖟 🗳 🕜 🎗	9
ホーム > アイトレート		~
属性とグレーム		~
+ 新しいクレームの追加 + グループ要求を追加する ΞΞ 列	🔀 フィードバックがある場合	
必要な要求		
クレーム名	値	
一意のユーザー識別子 (名前 ID)	user.userprincipalname [nameid-format:emailAddress]	
追加の要求		
クレーム名	値	
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailadd	user.mail ····	

#### 「ソース属性」を[user.objectid]に変更し、画面上部の「保存」ボ タンをクリックしてください

Microsoft Azure	🔎 リソース、サービス、ドキュメントの検索(G+/) 🗵 😡 🖓 🛞 🕜 🔗	8			
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://schemas.xmlsoap.org/ws/2005/05/identity/claims				
へ 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*	<ul> <li>属性 〇 変換</li> </ul>				
ソース属性*	user.objectid	~			

#### ■ 右上の「新しいクレームの追加」をクリック

■ Microsoft Azure	、、ドキュメントの検索 (G+/)	🙆
ホーム > エンタープライズ アプリケーション >	> SAML ペースのサインオン >	
属性とクレーム		$\times$
+ 新しいクレームの追加 + グルーブ要求を追加する ■■	列 🛛 🔗 フィードバックがある場合	
必要な要求		
クレーム名	値	
효지기 또 한미기 / 수준 지정	· · · · · · · · · · · · · · · · · · ·	

#### ■ 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。

### 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」を選択します

≡ Microsoft Azure		
ホーム > エンタープライズ アプリク		
	■ · · · · · · · · · · · · · · · · · · ·	×
エノターノライス アノリソーション	, «	
₩ 概要	^ プロパティ	
∭ デプロイ計画	名前①	
管理	SA Ф	
1 วือパティ	アブリケーション ID ①	
🎥 所有者		
🎝 ロールと管理者	D	
🎥 ユーザーとグループ	Getting Started	
Э シングル サインオン		
プロビジョニング		
🐻 アブリケーション プロキシ	1。ユーザーとグループの割り当て	Э 2。シングル サインオンの設定
☺ セルフサービス	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
🔝 カスタム セキュリティ属性 (プレ	ビュー) ユーザーとグループの割り当て	作業の開始
セキュリティ		
💺 条件付きアクセス		
🔒 アクセス許可	3。ユーザー アカウントのプロビジョニング	🛀 4。条件付きアクセス

#### ユーザーの割り当て(1/2)



- 「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でセーフィーのサービスを利用でき るようになります

	₽ リソース、サービス、ドキュメントの検索	i (G+/)	🙆
ホーム > エンターブライズ アブリケー	23X >		
IVタープライズ アプリケーション		ユーザーとグループ …	×
👪 概要	≪ + ユーザーまたはグループの	2 編集 🔟 削除 🖉 資	格情報の更新
🛄 デプロイ計画	アプリケーションは、割り るには、プロパティの中で	当てられたユーザーのマイ アプリ内に表示され? ? [ユーザーに表示しますか?] を [いいえ] に設定	ます。これを表示しないようにす → Eします。
管理	● 最初の 200 件を表示し	ています。すべてのユーザーとグループを検索	するには、表示名を入力して
11 วือパティ	表示名	オブジェクトの種類	割り当てられたロール
🎎 所有者		ユーザー	User
👃 ロールと管理者		ユーザー	User
🎥 ユーザーとグループ		ユーザー	User
∋ シングル サインオン		7_#_	User
🔹 プロビジョニング		ಹಾಗ	
🐯 アプリケーション プロキシ			



## Safie Managerの設定

#### Safie ManagerのSSO設定画面で以下の通りAzure AD側のログイン URL、識別子情報を入力します

Ξ	Microsoft Azure ア・リソース、サービス、ドキュメントの検索 (G+/) ···· 🧏	r
	SAML ベー ×	権限 ログイン履歴 接続/切断履歴 SSO・ディレクトリ連携設定
199-	ソフキスアンリケーション	シークレットトークン
	>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>	
3	SAML 署名証明書	
	状態 アクティブ 拇印	IdP情報
	有効期限 2025/6/27 11:28:42 通知用メール アプリのフェデレーション メタデータ URL	
	証明書 (Base64)     ダウンロード       証明書 (未加工)     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	IDプロバイダーの識別子のURL 必須
4	safie-manager-sso-test-frontend のセットアップ	証明書ファイル 必須 (拡張子が.cer、.certまたは.pemでBase64形式のファイルを選択してください)
	Azure AD とリンクするアプリケーションを構成する必要があります。	ファイルを選択 選択されていません
	ログイン URL ①	■ 設定と同時にSSOを有効にする
	Azure AD 識別子	
	ロクアンド URL   ステップ バイ ステップの手順を表示	

- 🕫 safie
- Azure ADからSAML署名証明書のファイルをダウンロードして、Safie ManagerのSSO設定画面で同ファイルをアップロードします

Microsoft Azure P リソース、サービス、ドキュメントの検索 (G+	+/) ···· 🌾 r		
J SAM	Lベー ··· × 権限	ログイン履歴	接続/切断履歴 SSO・ディレクト
イズ アプリケーション	シークレッ	トトークン	
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			
SAML 署名証明書			
状態 アクティブ	IdP情報		
拇印	IDプロバイ	ダーのログインページのURL 必須	
有効期限 2025/6/27 11:28:42			
通知用メール			
デ印書 (Race64) ダウンロード	IDプロバイ	ダーの識別子のURL <mark>必須</mark>	
証明書 (あいこの) 証明書 (未加工) 9ワンロート			
フェデレーション メタデータ XML ダウンロード			
		イル 必須	
safie-manager-sso-test-frontend のセットアップ	(拡張子が、	.er、.certまたは.pemでBase64形式の	ファイルを選択してください)
Azure AD とリンクするアプリケーションを構成する必要があります。	ファイル	を選択 選択されていません	
ログイン URL		同時に200を右効にする	
Azure AD 識別子	〕 設定C	INTE A COOLE IL MILE A S	
ログアウト URL	D 21	录	





Azure AD側の情報や証明書ファイルが正しいことを確認したら、「設定と同時にSSOを有効にする」にチェックを入れて「登録」をクリックしてください

	権限 ログイン履歴	接続/切断履歴	SSO設定	
ホーム	É.			
ト デバイス	- en			814-
3 デバイスグループ				
ユーザー	IdP情報			
1 ユーザーチーム	IDプロバイダーのログインページのURL	必須		
	https://login.microsoftonline.com/		/saml2	0
・ 連用設定 ~	IDプロバイダーの識別子のURL 👸			
管理設定	https://sts.windows.net/	1		٥
	証明書ファイル <mark>必須</mark> (拡張子が.cerまたは.pemでBase64形式の	りものを選択してください)		
	ファイルを選択	.cer		
	✓ 設定と同時にSSOを有効にする			



## 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。

	P リソース、サービス、ドキュメントの検索 (G+/) ・・・・ 人
ホーム > エンタープライズ アプリケーション	>
エンタープライズ アプリケーション	SAML ベースのサインオン ···· ×
<ul> <li>● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●</li></ul>	
<ul> <li>パティ</li> <li>が有者</li> </ul>	
<ol> <li>ロールと管理者</li> <li>ユーザーとグループ</li> </ol>	Azure AD とリンクするアプリケ
<ul> <li>シングルサインオン</li> <li>プロビジョニング</li> </ul>	Azure AD 識別子 ログアウト URL フーマゴ いく フーマゴの デリテト ログアウト URL コーマゴ いく フーマゴの デリテト
<ul> <li>アノリケーション ノロキシ</li> <li>セルフサービス</li> <li>カスタム セキュリティ属性 (ブレビュー)</li> </ul>	
<b>セキュリティ</b>	ここでサインインして、のシングルサインオン構成を Test します。 Azure Active Directory 構成とそのもシングルサインオンが機能してのの両方を構成したことを確認してください。
♣ アクセス許可 ▲ かいの映画ル	Test       サインインをテストする方法を選択         ● 現在のユーザーとしてサインイン         ● 他のユーザーとしてサインインする (ブラウザーの拡張機能が必要)
	サインインのテスト

#### SSOの動作テスト(2/2)

- 🕫 safie
- しばらくたって、Safie Viewerの利用規約画面(またはログイン後の トップページ)に遷移したら設定は正常に完了しています。
   エラーが表示された場合は入力したURL情報や証明書情報に誤りがな いか確認して再度お試しください。





## ディレクトリ連携





シングルサインオンの機能のみをご利用されたい場合、ディレクトリ連携 設定については必須ではありません。 P30までの設定を行なっていただければご利用いただけるため、これ以降 の設定は不要となります。

逆に、ディレクトリ連携の設定を行うにはシングルサインオンの設定は必 須となるため、P5-P30までの設定は完了いただくようお願いいたしま す。



- ディレクトリ連携の設定は以下の手順で行います。
- 1. Safie Managerの初期設定
  - 1.1. Safie 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
  - 1.3. 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



## Safie Managerの初期設定



- 以下のURLにアクセスし、Saafie Managerにログインしてください <u>https://safie.link/manager/#/login</u>
- ログイン後、画面右上の赤枠部が「全体管理者」であることを確認してください
  - ※「管理者」となっている場合、以降の手順が行えません





- サイドメニューの管理設定の画面からSSO・ディレクトリ連携設定タ ブをクリック
- 「企業別認証IDの発行」をクリック
- 確認のダイアログが表示されるので「続行」をクリック



#### シークレットトークンの発行

- **F**safie
- 以下の画面が表示されたら、「IdPへの登録情報」内の「シークレット トークン」蘭の横にある「発行」ボタンをクリック
- 表示されたシークレットトークンを手元に控える ※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
   本画面は以降の手順でも参照するので画面を閉じずに次の手順に進ん

本首面は以降の」派でし<u>ジボッゼので</u>直面で<u>月の」に</u>次の」派で定べ でください。

<b>Fsafie</b> Safie Manag	er	シークレットトークン発行
ホーム	権限 ログイン履歴 接続/切断履歴	シークレットトークンを発行しました。 この画面を閉じるとシークレットトークンを確認することができ なくなります。
デバイス	IdPへの登録情報	<i>®</i> ⊐ピー
🖻 デバイスグループ	SSO URL(ACS)	
▲ ユーザー		閉じる
🖻 ユーザーチーム	SSO Entity ID	
運用設定		
✿ 管理設定	SCIM用URL シークレットトークン 未発行	ビー 発行



## Microsoft Entra IDの設定



 本マニュアルのP12~P14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います



# 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

≡ Microsoft Azure		Σ	Ŗ	Q	٢	0	ন্দ		 セーフィー株式会社
ホーム >									
エンタープライズ アプリケーション	∞								
₩ 概要	≪ 								
<ul> <li>ロ デブロイ計画</li> <li>管理</li> </ul>	A前① SA								
プロパティ 🏜 所有者	アプリケーション ID ① . ① オブジェクト ID ①								
<ol> <li>2. ロールと管理者</li> <li>2 ザーとグループ</li> </ol>	Getting Started								
<ul> <li>シングルサインオン</li> <li>プロビジョニング</li> </ul>									
🐯 アプリケーション プロキシ	1。ユーザーとグループの割り当て			Э	2。シン	グルサ	インオン	の設定	
☺ セルフサービス	特定のユーザーおよびグループにアプリケーショ へのアクセスを付与	2			ユーザー	が自分	の Azure ョンにサイ	e AD 資格情報 (ソインできるよ	服を使用し ;うにする
🔝 カスタム セキュリティ属性 (プレ	ビュー) ユーザーとグループの割り当て				作業の	開始			
セキュリティ									

#### ■ 「作業の開始」をクリック

$\equiv$ Microsoft Azure	ク リソース、サー	ビス、ドキュメントの検索 (G+/)	N 🖓 🍪 🕐	R 8
<b>ホーム</b> >	エンタープライズ アプリケーション > エンタープ	ライズ アプリケーション すべてのアプリケーション > Microsoft Entra	ギャラリーを参照する >   プロビジ	ヨニング >
0	一一一概要			×
	※  □ フィードバックがある場合			
(1) 概要				
♀ オンデマンドでプロビジョニン	ヴ			
管理		10		
プロビジョニング		<b>.</b>		
モニター				
プロビジョニング ログ				
<ul> <li>監査ログ</li> </ul>				
分析情報		Microsoft Entra を使用して ID ライフナ	オイクル管理を目動化する	
トラブルシューティング		ユーザーが組織内で参加、脱退、移動するときに、アカウントを	自動的に作成、更新、削除します。詳細情報。	
🧟 新しいサポート リクエスト		1 1995 20041	1	
	プロビジョニングとは何ですか?	アプリケーションのデプロイを計	画します。	自動プロビジョニングを構成します。

#### プロビジョニング設定(2/7)

- プロビジョニングモードについて「自動」を選択します。
- 「自動」を選ぶと「管理者資格情報」の中に「テナントのURL」と「シークレットトークン」の入力 項目が表示されます。こちらに、Safie Manager側の情報を転記します
- 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

			$\equiv$ Microsoft Azure	
er			・・・・ 〉 エンタープライズ アプリケーション   すべ	、てのアプリケーション > Microsoft Entra ギャラリーを参照する >
権限	ログイン履歴	接続/切断履歴	プロビジョニング	
TELA			🔄 保存 🗙 破棄	
IdPへの登録情	青報		プロビジョニング モード	
SSO URL(ACS)			自動	~
			Microsoft Entra を使用して、ユーザーとグループ 期を管理します。	の割り当てに基づいたでのユーザーアカウントの作成と同
SSO Entity ID				
			∧ 管理者資格情報	
			管理者資格情報	
SCIM用URL			Microsoft Entra がの /	API に接続してユーザー データを同期するには、次の情報が必要です。
			<del>アナントの URL * ①</del>	
シークレットトー	-クン		シークレットトークン	
未発行				
			テスト接続	

- ¶safie
- 保存を行うと、「マッピング」という設定項目が表示されるようになります。
   こちらよりユーザー情報・グループ情報のマッピング設定を行います
   ユーザー情報「Provision Azure Active Directory Users」をクリック

#### プロビジョニング

□ 保存 × 破棄
 成と同期を管理します。
 ◇ 管理者資格情報
 > マッピング
 マッピング
 マッピングでは、Azure Active Directory と customappsso の間でのデータのフロー方法を定義できます。
 名前 有効
 Provision Azure Active Directory Users
 はい

既定のマッピングを復元する

#### プロビジョニング設定(4/7)



- 「属性マッピング」内の設定をデフォルト設定から変更します
- customappsso属性の「externalId」をMicrosoft Entra ID属性の 「objectId」に紐付け、照合の優先順位を1としてください
- 「displayName」を「displayName」に紐付けてください
- 「emails[type eq "work"].value」を「mail」に紐付けてください

■ (任意)

「urn:ietf:params:scim:schemas:extension:enterprise:2.0:User:employeeNumber」を「employeeId」に紐付けてください

属性マッピングでは、Microsoft Entra ID と customappssoの間で属性をどの	ように同期するかを定義します			
customappsso 属性	Microsoft Entra ID 属性	照合の優先順位	編集	削除
externalld	objectId	1	編集	削除
active	Switch([issortDeleted], raise, rue, rue, raise)		和表	रत्नाएस
displayName	displayName		編集	削除
τιτιε	ומסן		相未	HURK
emails[type eq "work"].value	mail		編集	削除
preterredLanguage	preterredLanguage		編業	削原
name.givenName	givenName		編集	削除
urn:ietf:params:scim:schemas:extension:enterprise:2.0:User:empl···	employeeld		編集	削除

- 「属性マッピング」内の設定のデフォルト値として、Microsoft Entra ID属性の 「userPrincipalName」の照合の優先順位が1となっています。本設定ではcustomappsso属性の 「externalId」をMicrosoft Entra ID属性の「objectId」に紐付け、照合の優先順位を1とする必要 があるため、以下の手順で設定を行なってください。
- customappsso属性の「externalId」をMIcrosoft Entra ID属性の「objectId」に紐付けた段階で 「この属性を使用してオブジェクトを照合する」を「はい」に設定し、照合の優先順位を「2」で設 定する

マッピングの種類 ①	
直接	~
ソース属性 * ①	
objectId	$\checkmark$
null の場合の既定値 (オプション) ①	]
対象の属性* ①	
externalld	~
この属性を使用してオブジェクトを照合する	
はい	~
照合の優先順位* ①	
2	✓
このマッピングを適用する ①	
常時	$\sim$

- **F**safie
- MIcrosoft Entra ID属性の「userPrincipalName」の「この属性を使 用してオブジェクトを照合する」を「いいえ」に設定する

マッピングの種類 ①	
直接	$\sim$
ソース属性 * ①	
userPrincipalName	$\checkmark$
null の場合の既定値 (オプション) ①	
対象の属性*①	
userName	$\checkmark$
この属性を使用してオブジェクトを照合する	
いいえ	$\checkmark$
照合の優先順位①	
このマッピングを適用する ①	

 $\sim$ 

#### MIcrosoft Entra ID属性の「objectId」をの照合の優先順位を「1」で 設定する

マッピングの種類 ①	
直接	$\checkmark$
ソース属性* ()	
objectId	$\sim$
null の場合の既定値 (オプション) <sup>①</sup>	
対象の属性*①	
externalld	$\checkmark$
この属性を使用してオブジェクトを照合する	
はい	$\checkmark$
照合の優先順位* ①	
1	~

このマッピングを適用する ①

常時

 $\sim$ 



## 「マッピング」よりグループ情報「Provision Azure Active Directory Groups」をクリック

#### プロビジョニング

□ 保存 × 破棄

成と同期を管理します。

∨ 管理者資格情報

へ マッピング

マッピング

マッピングでは、Azure Active Directory と customappssoの間でのデータのフロー方法を定義できます。

名前	有効
Provision Azure Active Directory Groups	はい
Provision Azure Active Directory Users	はい

] 既定のマッピングを復元する

#### プロビジョニング設定(6/7)



- 「属性マッピング」内の設定をデフォルト設定から変更します
- customappsso属性の「externalId」をMicrosoft Entra ID 属性の 「objectId」に紐付け、照合の優先順位を1としてください
- 「displayName」を「displayName」に紐付けてください
- 「members」を「members」に紐付けてください

#### 属性マッピング

属性マッピングでは、Microsoft Entra ID と customappsso の間で属性をどのように同期するかを定義します

customappsso 属性	Microsoft Entra ID 属性	照合の優先順位	編集	削除
externalld	objectId	1	編集	削除
displayName	displayName		編集	削除
members	members		編集	削除

#### プロビジョニング設定(7/7)

# プロビジョニング画面に戻り、「プロビジョニングの開始」をクリックすることでプロビジョニングが開始されます



#### プロビジョニングの編集

### 再度設定を変更したい場合は、「プロビジョニングの編集」をクリッ クし設定の変更を行なってください

	ス、サービス、ドキュメントの検索 (G+/)		📃 🛛 🖓 🖗 🕐 /	रु 🚺 🕘
ホーム >  エンター	プライズ アプリケーション 〉 エンタープライズ ア	プリケーション   すべてのアプリケーション >		
٢	プロビジョニング …			×
エンタープライズ アプリケーション 《	プロビジョニングの開始 フロビジョニン	グの停止 🤇 プロビジョニングの再開 🖉 プロビジョニ:	ングの編集 👂 要求時にプロビジョニン?	ブする 🛛 💍 更新 🗌 …
■ ഡ女				
★ 問題の診断と解決	現在のサイクルの状態	現在までの統計情報		
等理	増分サイクルが停止しました。	◇ プロビジョニングの詳細の表示		
■生     プロパティ	0% 75 ]	~ 技術情報の表示		
A 所有者	ユーザー グループ			
🛃 ロールと管理者	6,246 151			
🎥 ユーザーとグループ	プロビジョニング ログの表示			
∋ シングル サインオン				
② プロビジョニング	プロビジョニングの管理			
以 アプリケーション プロキシ	資格情報の更新 属性マッピングの編集			
📀 セルフサービス	スコープ フィルターの追加 要求時にプロビジョニングする			
カスタム セキュリティ属性 (プレ ビュー)				
セキュリティ				
Network Contraction (1997) (19977) (19977) (1997) (1997) (1997) (1997) (1997)				

ユーザーの割り当て



 P22、P23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







- プロビジョニング画面から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

≡ Microsoft Azure ♀ リソー	ス、サービス、ドキュメントの検索 (G+/)	ホーム >  エン	タープライズ アプリケーション > エン	タープライズアプ
ホーム >  エンター	プライズ アプリケーション 〉 エンタープライズ	プロビジョニング ロ	グ …	
(2) エンタープライズ アプリケーション	フロビジョニンク …	↓ ダウンロード ∨ (i) 詳細情報	🖒 更新   🎫 列   🔗 フィードル	ヾックがある場合
《	プロビジョニングの開始 □ プロビジョニ	○ D 名または ID		
Ш デプロイ計画	<b>現在のサイクルの状態</b>	許可された時刻 : <b>過去 24 時間</b>	日付を次の基準で表示:: <b>ローカル</b>	状態 : <b>すべて</b>
🗙 問題の診断と解決		許可された時刻 ↑↓	ID	操作
管理	増分サイクルか停止しました。 0% 完 <sup>-</sup>	2023/1/25 15:12:12	表示名 gtm_demo ソース ID 61a8e20b-c609-4a37-8e76-6 ターゲット ID 61a8e20b-c609-4a37-8e	Update
<ul> <li>パープロパティ</li> <li>新有者</li> </ul>	6.246 <sup>9/L-7</sup>	2023/1/25 15:12:12	表示名 SafieManager開発 ソース ID 4b5744d4-c135-43d9-98e5-8 ターゲット ID 4b5744d4-c135-43d9-98	Update
<ul> <li>▲ ロールと管理者</li> <li>▲ ユーザーとグループ</li> <li>▲ ハーザーとグループ</li> </ul>	プロビジョニング ログの表示	2023/1/25 15:12:12	表示名 SafieManager開発 ソース ID 4b5744d4-c135-43d9-98e5-8 ターゲット ID 4b5744d4-c135-43d9-98	Update
<ul> <li>シンクル サインオン</li> <li>プロビジョニング</li> </ul>	プロビジョニングの管理 資格情報の更新	2023/1/25 15:12:12	表示名 SafieManager開発 ソース ID 4b5744d4-c135-43d9-98e5-8 ターゲット ID 4b5744d4-c135-43d9-98	Update
<ul> <li>アプリケーションプロキシ</li> <li>セルフサービス</li> <li>カスタムセキュリティ属性 (プリ)</li> </ul>	属性マッピングの編集 スコープ フィルターの追加 要求時にプロビジョニングする	2023/1/25 15:12:12	表示名 SafieManager開発 ソース ID 4b5744d4-c135-43d9-98e5-8 ターゲット ID 4b5744d4-c135-43d9-98	Update



### プロビジョニング画面の「プロビジョニング編集」をクリックし、 「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

□ 保存 × 破棄

成と回期を管理しま9。

∨ 管理者資格情報

◇ マッピング

へ 設定

~

プロビジョニング状態 ①



- **F**safie
- 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.	AzureAD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。P43を参 考に設定を行ってください。
employee_number is invalid. / invalid employee_number	AzureAD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	AzureAD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。

error_description	エラー内容
Corporation user capacity is full	SafieManager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 AzureAD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.	AzureAD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。



## プロビジョニングの停止

#### プロビジョニングの停止

### プロビジョニング画面から、「プロビジョニングの停止」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

	-ス、サービス、ドキュメントの検索 (G+/) 🛛 🛛 🕞 🖓 🛞 🕐 😥	0
ホーム >  エンター	-プライズ アプリケーション 〉 エンタープライズ アプリケーション   すべてのアプリケーション 〉	
<b>こ</b> エンタープライズ アプリケーション		×
《	▶ プロビジョニングの開始 🗌 プロビジョニングの停止 🤇 プロビジョニングの再開 🖉 プロビジョニングの編集 🤌 要求時にプロビジョニングする │ 🖒 更新 │ …	
🛄 デプロイ計画	現在のサイクルの状態 現在までの統計情報	
🗙 問題の診断と解決	増分サイクルが停止しました。 シープロビジョニングの詳細の表示	
管理		
プロパティ	◇ 技術情報の表示	
🎎 所有者		
🛃 ロールと管理者	10,240 1131	
🎥 ユーザーとグループ	プロビジョニング ログの表示	
Э シングル サインオン		
② プロビジョニング	プロビジョニングの管理	
以 アプリケーション プロキシ	員俗情報の更新 属性マッピングの編集	
📀 セルフサービス	スコープ フィルターの追加 要求時にプロビジョニングする	
カスタム セキュリティ属性 (プレ ビュー)		
セキュリティ		
条件付きアクセス https://portal.azure.com/#		

memory

think

listen

see

speak

混雑状況

気象

# 映像から未来をつくる

「賢くなるカメラ」が人々の第三の目となり 生き方・働き方を豊かにする情報を提供

交通状況

顧客導線



顏認証

店舗データ