株式会社オウケイウェイヴ GRATICA 用シングルサインオン設定マニュアル

第一章 SSO を対応させるグループの作成とユーザの選択 --- P.1 第二章 AzureAD にアプリケーションを登録する ----- P.3 第三章シングルサインオン (SSO) の設定 ----- P.5



第一章 SSO を対応させるグループの作成とユーザの選択

1. AzureAD を開きグループを開きます



2. 新しいグループを開きます



p. 1



- 3. 以下のように設定して作成をクリックします
 - ・ グループの種類:セキュリティ
 - ・ グループ名:任意
 - ・ グループの説明:任意
 - ・ 所有者:システム管理者アカウントを選択
 - ・ メンバー: SSO をさせたい個人アカウント全てを登録

Azure Active Directory 管理セン	9-		Q Q ©	0 R	
≪ ఔ1 ళిッシュポ−ド ⋿ すべてのサ−ビス	ダッシュポード >				×
★ お知EスU ◆ Azure Active Directory ▲ ユーザー Щ エンターブライズ アプリケーション	アライードバックがある場合 クルーブの提供 * ① セキュリティ クルーブの * ① GATICA_SSO クルーブの説明 ① GRATICA_SSO クルーブの説明 ② GRATICA_SSO ブルーブの説明 ③ GRATICA_SSO ブルーブ プルーブ アルーブ クルーブ アルーブ アルーブ アルーブ アルーブ アルーブ アルーブ アルーブ ア	× × ×			
	1 人の所有者 1 人の所有者が読むました メンバー 1 人のメンバーを選択しました 作成				

4. グループの作成は完了です



第二章 AzureAD にアプリケーションを登録する

1. AzureAD でエンタープライズアプリケーションを開きます

Azure Active Directory 管理セ	ンター			G	K
※ ダッシュボード Ⅲ ダッシュボード Ⅲ すべてのサービス	ダッシュポード > 林式会社 : Azure Active Directory	概要 …			×
★ お気に入り ◆ Azure Active Directory ユーザー 戦 エンタープライズ アプリケーション	 ● 概要 ■ フレビュー機能 ※ 問題の診断と解決 	★ + ibin ◇ ② テナントの管理 ② 新名柄板 図 ブレ ○ Microsoft Entra EEL, D.およびアクセス管理のすべてのニー ニ(プレビュー)をお話しください。 ③	ビュー機能 ズを管理するた	アノードバックがある場合 ∨ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・	×
	管理 ▲ ユーザー み グループ ● External identities ▲ ロールに容積者 画 容積単位	 概要 監視中 プロバティ チュートリッル ターテナントの検索 基本情報 名前 		7-17-	
	 モンターフライズ アフリケーション デバイス アプリの登録 Identity Governance アプリケーションプロキシ Custom security attributes 	テナントロ プライマリドメイン ライゼンス アラート	LD.	クルーフ アプリケーショー デバイス	
	(Preview) <p< th=""><th>今後のTLS 1.0. 1.1、3055の廃止予定 サービスへの影響を迎けるために、クライアントワ[*] プリケーシュンォルにはプラットフメーム)でTLS 12 のリポートを有効にしてください。 詳細 C</th><th></th><th></th><th></th></p<>	今後のTLS 1.0. 1.1、3055の廃止予定 サービスへの影響を迎けるために、クライアントワ [*] プリケーシュンォルにはプラットフメーム)でTLS 12 のリポートを有効にしてください。 詳細 C			
	↑ バスワードリセット ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	マイフィード			

2. 新しいアプリケーションを開きます





3. 独自のアプリケーションの作成を開きます



- 4. 右メニューで以下のように設定して作成をクリックします
 - ・ お使いのアプリの名前は何ですか?:任意 ※「GRATICA」とするとわかりやすいです
 - ・ ギャラリーに見つからないその他のアプリバージョンを統合しますのラジオボタンにチェック

Azure Active Directory 管理セ	コンター		\$\$ \$\$ \$\$ \$\$ \$\$ \$\$ \$\$	
« 🏧 97921R-F	ダッシュボード > III III III III III III III III III	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	独自のアプリケーションの作成	×
E 4KT09-EX			尺 フィードバックがある場合	
* BREAU	+ 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	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
2-9-	Azure AD アフリ キャラリーは、シンクル サインオン (SSO) と自動 り安全にアプリに接続することができます。ここで独自のアプリケー: て要求を提出できます。この記事。	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シ ションを参照または作成してください。他の組織が検出して使用できるよう!	ないアプリプーションを統合する必要がある場合は、ここで残日のアプリプーションを作成できます お値いのアプリの条部け何ですか?	w.
🛄 エンタープライズ アプリケーション	Q アプリケ-ペョンを絵本	20/20 HZ0000 HZ97 T H THOMA MEMORAL	GRATICA V	
	/ //// / wixm	シンジル リインオン:9へて ユーリー アカソンドの皆様:All	アプリケーションでどのような操作を行いたいですか?	
	クラウド ブラットフォーム		オンプレミスのアプリケーションへのセキュリティで保護されたリモート アクセス用のアプリケーションへのセキュリティで保護されたリモート アクセス用のアプリケーションのセキュリティで保護されたリモート アクセス用のアプリケーションのセキュリティで保護されたリモート アクセス用のアプリケーションのセキュリティで保護されたリモート	ション プロキシ
	Amazon Web Services (AWS)	Google Cloud Platform	⑦ 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)	
			 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) 	
	aws	<u> </u>	エントリと一致する可能性がある次のアプリケーションが見つかりました 可能な場合はギャラリー アプリケーションを使用することをお勧めします。	
	60	Google Cloud	linformatica Platform	
			Clarity	
		L	lean Lean	
	SAP		Mind Tools Toolkit	
	SAD		OpenForms	
	SIAP		-	
			作成	
		[作成	

5. アプリケーションの登録は完了です



第三章シングルサインオン(SSO)の設定

1. 第二章で登録したアプリケーションを開きユーザとグループを開きます(上記で作成をクリックすると自動的に開きます)

※AzureAD \rightarrow エンタープライズアプリケーション \rightarrow GRATICA (任意の名前) で検索でも開けます



2. ユーザまたはグループの追加をクリックします





3. ユーザとグループ下の選択されていませんをクリックします

Azure Active Directory 管理セン	79-	Ę ♥ @ Ø ₽	
Azure Active Directory 管理セン ※ 第 グッシュポード 第 オバズのサービス ★ お気に入り ▲ Azure Active Directory ▲ ユーザー ■ エンターブライズ アブリケーション	ジター ダッシュボード: 割り当ての追加 … ユーザーとグループ 星沢をれていまさん ローアルを見かしていたさい User	日 🕑 💿 🔊	×
	割り当て		

4. 第一章で作成したグループを検索して選択し、下の選択をクリックします

Azure Active Directory 管理セン	/9	lig li @ @ R	
≪ 型 ダッシュポード		ユーザーとグループ	×
 ■ すべてのサービス ★ お気に入り ◆ Azure Active Directory 	ユーザーとグループ 		×
💄 ユーザー 🔜 エンタープライズ アプリケーション	ロールを選択してください User		
		選択したアイテム 浜目が注訳されていません	
	割り当て	選択	



5.1個のグループが選択されましたと表示されたことを確認して割り当てをクリックします

※ここで選択したグループに属するアカウントしか SSO が有効になりませんのでご注意ください

Azure Active Directory 管理セ	2 /9- \$ © \$	
«	ジッシュボード > Iンターブライズ アブリケーション > Iンターブライズ アブリケーション すべてのアブリケーション > Azure AD ギャラリーの参照 > GRATICA_ コーザーとグループ >	
── ダッシュボード	割り当ての追加	×
E 4~(07-KX		
* 8%LAU	▲ アプリケージョンにプループを削り当てると、そのプループ内の声機のコーゲーだけがアクセスできるようになります。割り当ては、入れ × スペンシュークループマルージマルージマルージマルージマルージマルージマルージマルージマルージマルージ	
2 1-9-	1.669.16.2.1072762020-1120166204	
📕 エンタープライズ アプリケーション	コーザーとグループ	
	1 (m07/k-77/#34/2412.L.)	
	User	
	¥1087	

6. シングルサインオンをクリックし、右の SAML をクリックします





7. GRATICA のサービスプロバイダ情報を控えます

$\%$ GRATICA \rightarrow	詳細設定	→ セキ	ユリティ ー	SAML	SS0	設定で開けます
----------------------------	------	------	--------	------	-----	---------

🔘 株式会社オウケイウェイヴ ┃	仲理内病 ような ような しょう こうしょう しょう しょう しょう しょう しょう しょう しょう しょう しょう	
ダッシュボード		
ソーシャルグラフ	SAML SSO 設定	
カード送受信データ	SAML SSO 設定 サードスプロバイダ情報	
カード削除	サービスブロバイダ情報に記載されている情報をお使いのIDブロバイダ(IdP)に設定します。	
	Entity ID 8ff6456ee4 [18956b	
ユーザー管理 ~	Single SignOn Post URL https:// /samt2/100/acs	
ギフト管理 ~	Single Logout URL https:// Isami2/100/sis	
グループ設定	i metadataをダウンロード	
オリジナルテンプレート 〜		
セキュリティ ヘ		6
SAML SSO 没有		
IPアドレス制限		

8. 基本的な SAML 構成の右にある編集をクリックします

Azure Active Directory 管理セ	2ンター		1	R 🗳 🐵 🕐 🖉
*	ダッシュボード >	エンタープライズ アプリケーション > エンタープライズ 7	アプリケーション すべてのアプリケーション > Azure AD ギャラリーの:	参照 > GRATICA_ >
 ダッシュボード すべてのサービス 	GRATICA_ SAML ベ エンタープライズ アプリケーション	ースのサインオン		
 ★ お知に入り ◆ Azure Active Directory ▲ ユーザー ■ エンターフライズ アプリケーション 	 転 数要 デナロイ計画 管理 11 プロ(ティー) 20(ディー) 20(ディー) 	ベ 주 メタダータ ファイルモアップロードする う シ SAML によるシングル サインオンの フェデレーション フロトコルに基づく SSO 実装により、 Connect または OAUM が使用されていない原件の られていたかたという。	ングルサインオンモードの変更 巨 このアブリケーションをText ズ レセットアップ 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し、実施が のアブリケーションの場合は、できるだり SAML シングル サインスンを選択 いたってストルのトリコ	² フィードバックがある場合 診断になります。OpenID パでください。詳細については、こち
	C ロールと言称者 ユーザーとグループ シングル サインオン アバビジョニング アブリケーション プロキシ レード レフ	K T E CLERK (LCL) (第20/17 B UKAILCA, E	(表面 音 らん2000-719-2)。 ※現 (vice URL) 参規 資料可能 資料可能 資料可能	
	 はたり ビオコリティ属性 (フレビュー) セオコリティ 条件付きアクセス 条件付きアクセス アクセス計画 トーククの納予化 アクラレチェー 	る 属性とクレーム ▲ 予用 T で必須フィールドに入力して givenname surname emailaddress name ー売のユーザー ID	CCC2U user.givenname user.amane user.mail user.userprincipalname user.userprincipalname	
	 ● サインインログ 論 使用状況と分析情報 ■ 監査ログ ▲ フロビジョニングログ 	3 SAML 署名証明書 ▲ 手順 1 で必須フィールドに入力して 状態 例印 本い純時時	てください アクライブ D 9994932775296530185D819ASC4265F255744CE2 2017パル3 ちか248	



- 9. 以下のように入力して保存をクリックします
 - ・ 識別子の追加をクリックし 識別子 (エンティティ ID) : GRATICA 管理画面の Entity ID を入力
 - 応答 URL の追加をクリックし 応答 URL: GRATICA 管理画面の Single Sign On Post URL を入力
 - ・ サインオン URL: GRATICA 管理画面の Single Sign On Post URLを入力

Azure Active Directory 管理センター						
«	ダッシュボード >	エンタープラ	イズ アプリケーション :	基本的な SAML 構成	×	
= 1<705-EX	GRATICA_ SAML ~- エンタープライズ アプリターション	スのサイ	ンオン …	🗟 保存 🗌 💀 フィードバックがある場合		
★ お気に入り ◆ Azure Active Directory	11. 祝要	< <u></u> ↑ ×	タデータ ファイルをアップ	🚯 SAML 構成エクスペリエンスのこのプレビューを持了しますか? ここをクリックすると、プレビューが除了します。 →		
🚨 1-1-	🛄 デブロイ計画	SAM	L によるシングノ	識別子 (エンディティ ID)* の	1	
📕 エンタープライズ アプリケーション	管理	フェデレ	-ション プロトコルに基立	Azure Active Directory に対してアプリケーションを減別する一意の ID。この値は、Azure Active Directory テナント内のすべてのアプリケーシ	- 1	
	プロバティ	Connect または OAut らをご覧ください。		ョンで一意である必要があります。既定の裁別子は、IDP で開始された SSO の SAML 応答の対象ユーザーになります。	- 1	
	🚨 所有者	い下を	おきみください、展示	既定	- 1	
	🍰 ロールと管理者	 基本的な SA IL	DBU/ GCCV MAN	8ff6456ee4315af3f189561		
	🎎 ユーザーとグループ		識別子の進加	- 1		
	อ ขวตีม ชาวหว		応答 URL (Assertion Consumer Service URL) * ②			
	プロビジョニング					
	🐻 アブリケーション ブロキシ		リレー状態 (省略司 ログアウト URL (省	応答 URL は、アフリケーションが認証トージンを受け取る場所です。これは、SAML では ("Assertion Consumer Service(" (ACS) とわせばれま す。	- 1	
	⊙ セルフサービス			イン 既定	- 1	
	🗐 カスタム セキュリティ属性 (プレビュー)	2	属性とクレーム	https://gratica.xxxxxxxxip/sami2/100/acs	- 1	
	セキュリティ		givenname	応答 URL の迫加	- 1	
	🔩 条件付きアクセス		surname		- 1	
	🔒 アクセス許可		name	サインオン URL (省略可能)	- 1	
	🟮 トークンの暗号化		一旅のユーザー ID	サービスプロバイシーにように開始されたシングル サイブオンを実行する場合は、サイブオン URL が使用されよす。この地は、アノリサーションのサイ ンイン ページの URL です。ID プロバイサーによって開た <mark></mark> されたシングル サインオンを実行する場合、このフィールドは不要です。	- 1	
	アクティビティ	8	CAMI W 2 17 18	https://gratica.xxxxxxxip/sami2/100/acs		
	サインイン ログ		SAML名名证明			
	前 使用状況と分析情報		状態 細印	リレー状態 (省略可能) ①		
	※音ログ		有効期限	リレー状態は、認証が完了した後にユーザーのリダイレクト先となるアプリケーションを指示します。満定、値は、ユーザーをアプリケーション内の特 室の場応に終発するJRP エトイナリPI パスアオ		
	🔓 วัตชีชีละพุที ตุที	-	アプリのフェデレーシ	リレー状態を入力してください	-	

10. 属性とクレームの右にある編集をクリックします





11. 必要な要求のクレーム名にある一般のユーザの識別子をクリックします



- 12.以下のように選択して保存をクリックします
 - · 名前識別子の形式:永続的
 - ・ ソース:属性
 - ・ ソース属性:user.mail

Azure Active Directory 管理セ	ンター						
≪ 型】ダッシュポード Ⅲ すべてのサービス	···· > エンターフライス ァフリケーション 要求の管理 ···	すべてのアプリケーション > Azure AD ギャラリーの参照	> GRATICA_ SAML ペースのサインオン	' 〉 SAML ベースのサインオン 〉 腐性とクレーム 〉	×		
* 88629	🔚 保存 🗙 変更の破重 🛛 🔗	フィードバックがある場合					
 Azure Active Directory ユーザー エンタープライズ アプリケーション 	名前	名前 nameidentifier					
	名前空間	http://schemas.xmlsoap.org/ws/2005/05/ident	ty/claims				
	へ 名前港別子の形式の選択						
	名前識別子の形式*	水靛的			~		
	у- д *	● 属性 ○ 麦换					
	ソース属性 *	user.mail			\sim		
	へ 要求条件 以下の条件がすべて満たされた場合にのみ	、要求を返します。					
	1 つの要求に複数の条件を適用でき。	ます。条件を追加する場合は投作の順序が重要です。詳細について	は、 <u>ドキュメントをお読みください</u> 。				
	ユーザー タイプ	スコープが設定されたグループ	y-7	插			
	ドロップダウンから選択してください	◇ グループの選択	○ 属性 ○ 変換				



13. 証明書(Base64)のダウンロードをクリックします。 また、その下にある GRATICA のセットアップにある

ログイン URL、AzureAD 識別子、ログアウト URL を控えておいてください。



14. ダウンロードした証明書をテキストで開きます

※改行は全てリセットしてください





1 5. GRATICA の SAML SSO 設定画面に以下を入力して保存し SAML を有効化をクリックします ※GRATICA → 詳細設定 → セキュリティ → SAML SSO 設定で開けます

- ・ Entity ID 欄:項目 13 番のログイン URL をコピー & ペースト
- ・ Single Sign On Post URL 欄:項目 13 番の AzureAD 識別子をコピー&ペースト
- ・ X509 公開鍵欄:項目 14 番のキーをコピー&ペースト

ソーシャルグラフ	SAML SSO 設定	
カード送受信データ	SAML SSO 设定	サービスプロバイダ情報
カード削除	ldPからダウンロードしたmetadata (.xml) のファイルをア ださい。	'ップロードまたは各入力エリアに必要情報を入力してく
ユーザー管理 〜	וזיער	ルを選択
ギフト管理 〜	https://sts.windows.nv	:74/
グループ設定		
オリジナルテンプレート 〜	https://login.mid	:74/semi
セキュリティ ヘ	Single Logout URL	
SAML SSO 設定	MIIC8DCCArdinAw/BAd/OL s8/23bKard4 sFAD/	
IPアドレス制限	kIFNT EwNz cmE0	
パスワードポリシー	OBAM OBAM M8HVd050E/Te172E/21VCDFR0J2///	Ru - NuceavourzecilonvinumichoE3
ログイン・ログアウト履歴		

16. プロパティを開き応答 URL が表示されていることを確認します





17. AzureAD トップからすべてのアプリケーションを開き、GRATICA の右横に現在と緑色のマークが 付いていれば設定は完了です

Azure Active Directory 管理セン	19-	F 🔎 🏾 🖓 🦉	
×	ダッシュポード >	-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	
📶 ダッシュボード	エンタープライズ アプリケ・	ション すべてのアプリケーション …	×
≡ すべてのサービス	- Azure Active Direct	y	
★ お気に入り	<i>«</i>	🕂 新しいアプリケーション 🕚 更新 🚽 ダウンロード (エクスポート) 📔 🗊 プレビューの情報 📄 🎫 列 📗 👼 プレビュー機能 🗌 📈 フィードハ	ックがある場合
🚸 Azure Active Directory	概要		······································
 ▲ 1-9- ■ エンターブライズ アブリケーション 	④ 概要	Salestorce /2018406-1/3c-4/4a-85 SSal/145-atS0-4tee-a89 https://www.salestorce.c 2021/4/1	<u></u>
	🗙 同題の診断と解決	Office 365 Messa 72ddbeca-aa47-477b-85 3a9dd138-8313-4ea1-a3 https://products.office.c 2020/6/25	
	管理	AZ Azure-Sync 73986079-5106-4a09-95 5a735351-d1bc-4c31-b4 2019/11/12	
	# すべてのアプリケーション	D2 dexode 2020 7407ac8e-f87e-4381-9b 4131cfee-a3e7-41ac-890 https://www.microsoft.c 2020/6/5	21
	B 7/17-947 /147	SA Salesforce 78f3a9d4-e16f-426f-bbd 29104cd9-d43e-40db-a 2020/5/22	
		Trello Bot 7bc5a5a1-45ce-4ec6-98 78c16498-0980-4af4-a3f 2020/6/23	2
		Jira Cloud 7e44651e-5c87-4d8e-a3 11cd7f33-594f-4d45-aa2 https://www.msteams-at 2021/6/15	
		DR drawio 866f7fdc-6380-4002-80 45c10911-200f-4e27-a6 https://www.draw.io 2019/10/3	
	セキュリティ	M Mire (formarly Re 8h0d8300.73f6.49ha.82 df49091a.274d.4a90.83 2020/10/27	
	🔩 条件付きアクセス	GR GRATICA 90fa36a; ISf., 7b01; a-af., https://account.activedir., 2021/10/20	● 現在
	☞ 同意とアクセス許可	Atlassian 994/6908.6928.4/fa.h2 /6crlaa36.9339.4/60.hf https://start.atlassian.com 2020/1/20	
	7971871	70 27 Tonior Outlook 90/9E20 MEE 4747 ad 10/9Face 4d2a 4d21 8E2 10/9Face 4d2a 4d21	
	サイソイン Dグ	Zapier Outlook Salasiszo-bios-4/4/ ad	
	2 使用建设2分析情報	HE HDE Email DLP Dr., 9eab50c0-e220-48a5-8a., 597453be-27a3-48df-ba., https://console.mo.hde.,	-
	Reserver	diagrams.net a1267f27-d815-4864-93 b5ff67d6-3155-4fca-965 https://www.diagrams/net 2020/4/6	
	• TOXY	Cisco Webex Mee a4f95d9c-2c6a-4cdf-bbd 7a91e319-a65d-4ceb-90 https://api.webex.com/w 2020/5/13	
	 Desa_20 09 	T TimeRex - Teams a5c30341-473f-476a-84 63d6c652-335d-48e6-9e https://timerex.net 2021/9/15	
	דאר צער און אין אין אין אין אין אין אין אין אין אי	TE TESTOKWAVE a879c9a7-9e98-4204-8c bd93671b-b4a3-41b0-a https://account.activedir 2021/10/20	1
	管理者の同意要求	SurveyMonkey b34f02be-1126-4a6e-a4 07978fee-621a-42df-82 https://www.surveymon	*1
	👶 一括操作の結果	TE test b3c076d5-60d1-4ddd-8 793a7f4d-2183-4a46-9f https://account.activedir 2022/8/12	
	トラブルシューティング + サポート	PC Partner Community b637bda2-d869-44b8-b c0b9c4f9-8f84-48c9-b73 https://www.microsoftp	2

以上