

KDDI Knowledge Suite

GRIDY SSO（シングルサインオン）

操作マニュアル

（1.4 版）

2020 年 6 月 1 日

KDDI 株式会社

本書の読み方

本書は以下の構成になっています。

第1部 アドミニストレーター用

第1部はアドミニストレーターに必要な操作を解説しております。アドミニストレーターは GRIDY SSO（以下 SSO）の管理者のことです。アドミニストレーターの方は、初めにこの第1部をお読みになり、引き続き「第2部 メンバー用」もあわせてお読みください。

第2部 メンバー用

第2部は一般のメンバーに必要な操作を解説しています。この第2部は、メンバーの方はもちろん、アドミニストレーターの方もお読みください。

※本マニュアル中のキャプチャ画像は、実際の画面と異なる場合がありますのでご了承ください。

目次

第1部 アドミニストレータ用

■1-1 SSO とは.....	2
■1-2 SSO 設定.....	3
1-2-1 KDDI Knowledge Suite 専用ログイン URL を設定する.....	3
1-2-2 認証方式を設定する.....	4
1-2-3 SSO 結果を確認する.....	6

第2部 メンバー用

■2-1 SSO を利用する（ブラウザ版）.....	2
■2-2 SSO を利用する（iOS 版）.....	3
■2-3 SSO を利用する（Android 版）.....	5

■巻末資料

- JIT プロビジョニングを利用して連携可能な項目

アドミニストレータ用 目次

■1-1 SSO とは.....	2
■1-2 SSO 設定.....	3
1-2-1 KDDI Knowledge Suite 専用ログイン URL を設定 する.....	3
1-2-2 認証方式を設定する.....	4
1-2-3 SSO 結果を確認する.....	6

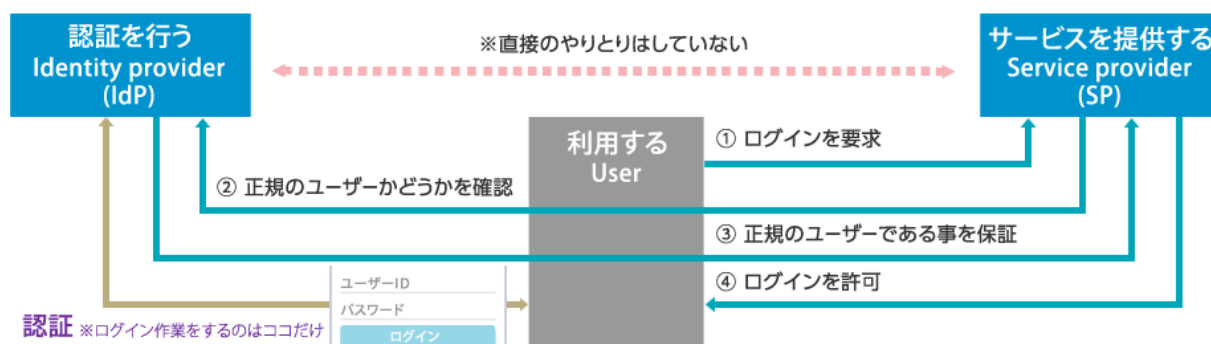
■1-1 SSO とは

SSO(シングルサインオン)は、複数のシステム・クラウドサービスを利用している場合でも SAML2.0に対応している認証プロバイダ (IdP) を通じて、1つの ID で「KDDI Knowledge Suite」にログイン可能となる認証機能です。これにより、ユーザーは都度ログイン認証する必要がなくなり、また多くのログイン ID・パスワードの管理も不要となります。SSO をご利用いただくことで、スマートデバイスからも安全にログインできるようになりセキュリティも強化されます。

■SSO（シングルサインオン）とは



■SAML2.0 シングルサインオンの仕組み



【シングルサインオン (SSO)】

1 回の認証で複数の異なるアプリケーション・システムの利用を可能にする仕組み。

【SAML】

異なる認証情報を連携するための、XML ベースの標準仕様・ルール。「Security Assertion Markup Language」の略称。

【認証プロバイダ (IdP)】

ユーザーがSSOを使用して他のWebサイトにアクセス、ログイン認証できるようにする信頼済みプロバイダ。

【サービスプロバイダー (SP)】

KDDI Knowledge Suite 等、クラウドサービスを提供する事業者。

POINT

SSO をご利用いただくには、IdP のご契約及び証明書のダウンロードが必須となります。

名刺取り込みアプリ（名刺 CRM、24/365）は、SSO 非対応です。

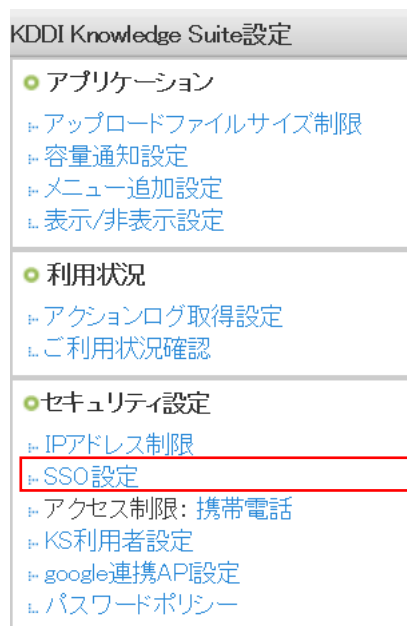
■ 1-2 SSO 設定

「KDDI Knowledge Suite」にて、専用ログイン設定を行います。

1-2-1 KDDI Knowledge Suite 専用ログイン URL を設定する



1. KDDI Knowledge Suite にログインし、画面上部の「設定」をクリックします。



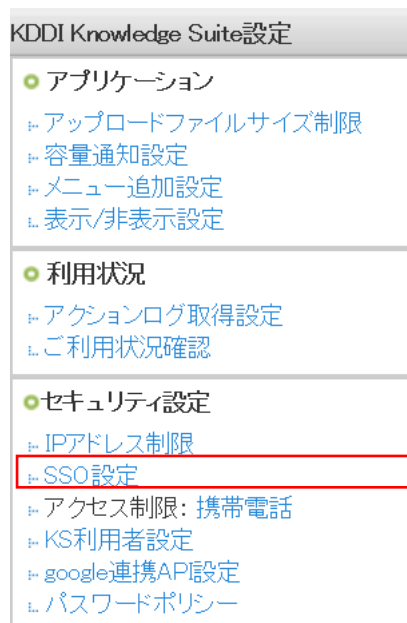
2. 「KDDI Knowledge Suite 設定」の「SSO 設定」をクリックします。

3. 「SSO 利用設定」は「無効」を選択し、「SSO 利用時の URL」に任意のサブドメインを入力して「設定保存」をクリックします。

1-2-2 認証方式を設定する



1. KDDI Knowledge Suite にログインし、画面上部の「設定」をクリックします。



2. 「KDDI Knowledge Suite 設定」の「SSO 設定」をクリックします。

設定 ?

SSO 設定

*は必須項目です。

SSO 利用設定 *	無効時は通常の URL (https://gridy.jp) 並、有効時は下記「SSO 利用時の URL」で指定いただいた URL をご利用ください。	☒ 有効 ☐ 無効
SSO 利用時の通常ログイン許可設定 *	SSO 利用時に通常の URL からログイン可能なユーザを指定してください。	☒ アドミニストレータのみ可能 ☐ 全員可能
JIT 連携の利用設定 *	有効にすると、SAML の Just-in-time プロビジョニングを、ご利用いただけます。	☐ 有効 ☒ 無効
SSO 利用時の URL *	ご利用になるサブドメインを指定してください。 ※他企業で使用されているサブドメイン名はご利用いただけません。	https:// [] .saml.gridy.jp
識別子のフォーマット *	ユーザー識別に用いるパラメータの形式を指定して下さい。	urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
IDプロバイダーログインURL *	ご利用になるIDプロバイダーのログインURLを指定してください。	[] 接続確認
IDプロバイダーログアウトURL	ご利用になるIDプロバイダーのログアウトURLを指定してください。	[] 接続確認
IDプロバイダー証明書 *	ご利用になるIDプロバイダーの証明書を指定してください。 ※証明書ファイルは以下の形式で作成してください。 証明書形式: X.509 作成アルゴリズム: RSA エンコーディング: PEM 改行コード: CRLF または LF	[] 参照...

設定保存

3. 「SSO 利用設定」は「有効」を選択し、「識別子のフォーマット」をプルダウンから設定します。「ID プロバイダーログイン URL」、「ID プロバイダーログアウト URL」を入力します。

POINT

「識別子のフォーマット」にて設定していただけるパラメーター形式は以下となります。

urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
urn:oasis:names:tc:SAML:2.0:nameid-format:persistent
urn:oasis:names:tc:SAML:2.0:nameid-format:transient
urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName
urn:oasis:names:tc:SAML:1.1:nameid-format:WindowsDomainQualifiedNames
urn:oasis:names:tc:SAML:2.0:nameid-format:Kerberos
urn:oasis:names:tc:SAML:2.0:nameid-format:entity

POINT

Just In Time（JIT）プロビジョニングを利用する場合、「JIT 連携の利用設定」は「有効」を選択します。
連携可能な項目は巻末資料の「[JIT プロビジョニングを利用して連携可能な項目](#)」をご参照ください。

JIT連携の利用設定 * 有効にすると、SAMLのJust-in-timeプロビジョニングを、ご利用いただけます。	☒ 有効 ☐ 無効
--	--



SSO設定

*は必須項目です。

SSO利用設定 * 無効時は通常のURL(https://gridy.jp)を、有効時は下記「SSO利用時のURL」をご指定いただいたURLをご利用ください。	☒ 有効 ☐ 無効
SSO利用時の通常ログイン許可設定 * SSO利用時に通常のURLからログイン可能なユーザを指定してください。	☒ アドミニストレーターのみ可能 ☐ 全員可能
JIT連携の利用設定 * 有効にすると、SAMLのJust-in-timeプロビジョニングを、ご利用いただけます。	☐ 有効 ☒ 無効
SSO利用時のURL * ご利用になるサブドメインを指定してください。 ※他企業で使用されているサブドメイン名はご利用いただけません。	https:// .saml.gridy.jp
識別子のフォーマット * ユーザー識別に用いるパラメーターの形式を指定して下さい。	urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
IDプロバイダーログインURL * ご利用になるIDプロバイダーのログインURLを指定してください。	 接続確認
IDプロバイダーログアウトURL ご利用になるIDプロバイダーのログアウトURLを指定してください。	 接続確認
IDプロバイダー証明書 * ご利用になるIDプロバイダーの証明書を指定してください。 ※証明書ファイルは以下の形式で作成してください。 証明書形式:X.509 作成アルゴリズム:RSA エンコーディング:PEM 改行コード:CRLF または LF	 参照...

4. 「ID プロバイダー証明書」に IdP 側で入手したプロバイダー証明書のファイルを選択し、[設定保存] をクリックします。

POINT

「ID プロバイダー証明書」については、以下の形式で作成してください。

証明書形式 : X.509

作成アルゴリズム : RSA

エンコーディング：PEM

改行コード：CRLF または LF

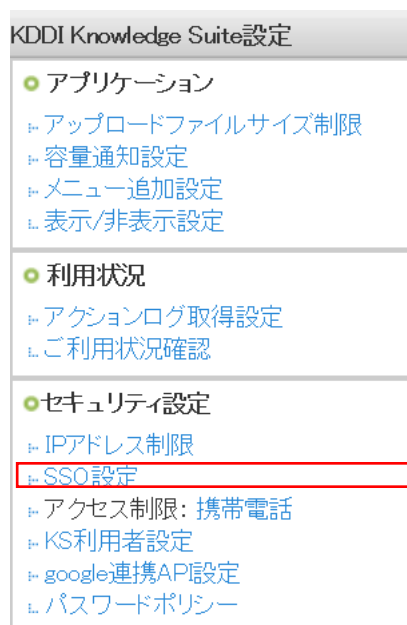
※「Azure Active Directory」等、証明書がファイルとして取得できない場合は、
-----BEGIN CERTIFICATE----- から -----END CERTIFICATE-----までをコピーし
そのままテキストエディタに貼り付けて作成してください。

1-2-3 SSO 結果を確認する

SSO によるユーザーのログイン結果を確認します。ログイン結果は直近 10 件分が表示されます。また JIT 連携の利用設定を有効にしている場合は、JIT 連携の結果も表示します。



1. KDDI Knowledge Suite にログインし、画面上部の「設定」をクリックします。



2. 「KDDI Knowledge Suite 設定」の「SSO 設定」をクリックします。

設定

SSO設定

*は必須項目です。

SSO利用設定 * 無効時は通常のURL(https://gridy.jp)を、有効時は下記「SSO利用時のURL」で指定いただいたURLをご利用ください。	☒ 有効 ☐ 無効
SSO利用時の通常ログイン許可設定 * SSO利用時に通常のURLからログイン可能なユーザーを指定してください。	☒ アドミニストレーターのみ可能 ☐ 全員可能
JIT連携の利用設定 * 有効にすると、SAMLのJust-in-timeプロビジョニングを、ご利用いただけます。	☒ 有効 ☐ 無効
SSO利用時のURL * ご利用になるサブドメインを指定してください。 ※他企業で使用されているサブドメイン名はご利用いただけません。	https:// ***** .saml.gridy.jp
識別子のフォーマット * ユーザー識別に用いるパラメーターの形式を指定して下さい。	urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
IDプロバイダーログインURL * ご利用になるIDプロバイダーのログイン用URLを指定してください。	https://robotid.jp/idaas/f/saml2/***** 接続確認
IDプロバイダーログアウトURL * ご利用になるIDプロバイダーのログアウト用URLを指定してください。	https://robotid.jp/idaas/f/main/index.xhtml 接続確認
IDプロバイダー証明書 * ご利用になるIDプロバイダーの証明書を指定してください。 ※証明書ファイルは以下の形式で作成してください。 証明書形式: X509 作成アルゴリズム: RSA エンコーディング: PEM 改行コード: CRLF または LF	ファイルを選択 選択されていません 証明書は既に設定済みです。 ☐ 設定済みの証明書を削除する

[設定保存](#)

SSO結果					
SAML認証				JIT連携	
日時	結果	識別子	SAMLレスポンス	結果	連携データ
2020-04-13 09:50:57	成功	c.yamashita@example.com	<?xml version="1.0" encoding="UTF-8"?><saml:Response xmlns:saml="urn:oasis:names:tc:SAML:2.0:protocol" Destination="https://knowledge-suite.saml.gridy.jp/login" ID="53d634097c38496f8987158e4827a45e" InResponseTo="N0xJEgVQgET1qWDnuJRKSSoJYKwMG" IssueInstant="2020-04-13T09:50:57.227Z" Version="2.0"><saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">https://robotid.jp/idaas/f/saml2/*****</saml:Issuer><saml:Status><saml:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/></saml:Status><saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"><saml:Subject><saml:NameID value="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified" Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified"/></saml:Subject><saml:Authn><saml:AuthnContext class="urn:oasis:names:tc:SAML:2.0:authn-context-class:unspecified"></saml:AuthnContext></saml:Authn></saml:Assertion></saml:Response>	成功	last_name:山下 first_name:千佳 last_kana:やました first_kana:ちか
2020-04-13 08:55:03	成功	k.maezono@example.com	<?xml version="1.0" encoding="UTF-8"?><saml:Response xmlns:saml="urn:oasis:names:tc:SAML:2.0:protocol" Destination="https://knowledge-suite.saml.gridy.jp/login" ID="B88ce116362143b88127a0680440c02c" InResponseTo="ywdElybnLpnXdBrXjkShOhClRgDpL" IssueInstant="2020-04-13T08:55:03.347Z" Version="2.0"><saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">https://robotid.jp/idaas/f/saml2/*****</saml:Issuer><saml:Status><saml:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/></saml:Status><saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"><saml:Subject><saml:NameID value="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified" Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified"/></saml:Subject><saml:Authn><saml:AuthnContext class="urn:oasis:names:tc:SAML:2.0:authn-context-class:unspecified"></saml:AuthnContext></saml:Authn></saml:Assertion></saml:Response>	無効	

3. 「SSO 結果」を確認します。

POINT

SSO ログイン時にエラーが発生した場合、「SAML 認証」の「結果」欄にエラー内容が表示されます。
また、JIT 連携でエラーが発生した場合は、「JIT 連携」の「結果」欄にエラー内容が表示されます。

SSO結果					
SAML認証				JIT連携	
日時	結果	識別子	SAMLレスポンス	結果	連携データ
2020-04-01 15:52:11	失敗 内部エラーが発生しました	c.yamashita@example.com	<?xml version="1.0" encoding="UTF-8"?><saml:Response xmlns:saml="urn:oasis:names:tc:SAML:2.0:protocol" Destination="https://knowledge-suite.saml.gridy.jp/login" ID="7f4051e326344cd2bec9a1467ea6bfff" InResponseTo="fBdcRoAOzDcGpwbAmtzckIVPpHE" IssueInstant="2020-04-01T06:52:09.969Z" Version="2.0"><saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">https://robotid.jp/idaas/f/saml2/*****</saml:Issuer><saml:Status><saml:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/></saml:Status><saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"><saml:Subject><saml:NameID value="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified" Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified"/></saml:Subject><saml:Authn><saml:AuthnContext class="urn:oasis:names:tc:SAML:2.0:authn-context-class:unspecified"></saml:AuthnContext></saml:Authn></saml:Assertion></saml:Response>	失敗 携帯電話番号を正しく入力してください	cell_phone_number : 080-0000-0000

メンバー用 目次

■2-1 SSO を利用する（ブラウザ版）	2
■2-2 SSO を利用する（iOS 版）	3
■2-3 SSO を利用する（Android 版）	5

■2-1 SSO を利用する（ブラウザ版）

ブラウザからのご利用方法です。

https://●●●●.saml.ks.kddi.ne.jp <http://saml.ks.kddi.ne.jp/>

1. 管理者が設定した「SSO 利用時の URL」にアクセスし、ログインします。

※お客様側でご契約された IdP のログイン画面が表示されます。

The screenshot displays the GRIDY SSO interface. At the top, there's a header with the GRIDY logo, a user profile section for 'Knowledge Suite, inc. 取締役会 前園 清治', and links for '設定', 'ヘルプ', and 'ログアウト'. Below the header is a navigation bar with tabs: 'グループウェア', 'SFA', 'リードフォーム', 'CENTER', and 'メールビューコン'. A grid of application icons follows, including 'マイページ', 'スケジュール', '設備予約', '部署/グループ', 'プロジェクト管理', '掲示板', 'トピック', 'メール', 'アドレス帳', '電話メモ', 'メッセージ', 'タイムカード', 'ToDo', 'ファイル', and 'メモパッド'. The main content area is divided into sections: 'お知らせ' (Notifications) with a list of alerts, 'スケジュール' (Calendar) showing a monthly view for April 2018, and '新着掲示板' (New Bulletin Board) with a table of recent posts.

日曜日	月曜日	火曜日	水曜日	木曜日	金曜日	土曜日
1	2	3	4	5	6	7

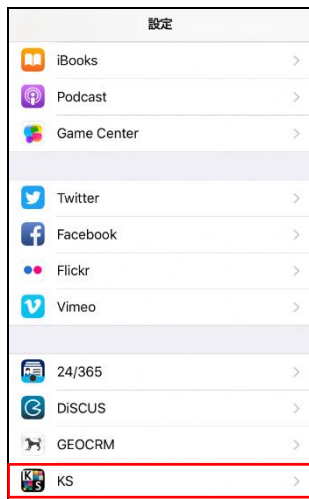
投稿時間	掲示板名 (コメント数)
05/20	健康診断のご案内(1)

投稿時間	トピック名 (コメント数) (グループ名)
03/23	社員旅行 (0) (取締役会)

2. KDDI Knowledge Suite のログイン後の画面（マイページ）に遷移します。

■2-2 SSO を利用する（iOS 版）

スマートフォン（iOS端末）でアプリケーションを利用する前に必要となる初期設定およびご利用方法です。事前準備として、App Store からご利用端末へアプリケーション「Knowledge Suite」をインストールしてください。



1. スマートフォンの「設定」より「KS」を選択し、Knowledge Suite の設定画面を表示します。



2. 「SSO サブドメイン」に設定値を入力し、「設定」をタップします。
※接続先 URL を「https://ks.kddi.ne.jp」に変更してください。
※設定値につきましては管理者様にお問い合わせください。
※お客様のご契約により、「接続先 URL」は異なります。
※手順 1～2 は初期設定時のみの手順です。

The image shows the login screen of the KDDI Knowledge Suite application. At the top is the logo "KDDI Knowledge Suite". Below it are two input fields: "ログインID" (Login ID) and "パスワード" (Password). Under the password field is a toggle switch labeled "ログインIDを保存" (Save login ID), which is currently turned on. A red rectangular box highlights the "ログイン" (Login) button. At the bottom, there is a small copyright notice: "copyright (C) KDDI CORPORATION. All RIGHTS RESERVED."

3. Knowledge Suite アプリを起動し、何も入力せず「ログイン」をタップします。
4. お客様側でご契約された IdP のログイン画面が表示されるので、IdP の ID とパスワードでログインします。（IdP で認証済みの場合は IdP のログイン画面は表示されません。）



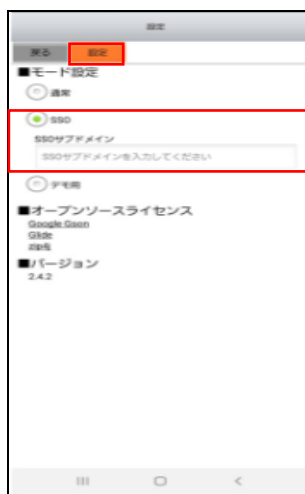
5. KDDI Knowledge Suite のログイン後の画面（トップページ）に遷移します。

■2-3 SSO を利用する（Android 版）

スマートフォン(Android端末)でアプリケーションを利用する前に必要となる初期設定および利用方法です。事前準備として Google Play Store からご利用端末へアプリケーション「KDDI Knowledge Suite」をインストールしてください。



1. KDDI Knowledge Suite アプリを起動し、「設定」をタップします。



2. 「■モード設定」にて「SSO」を選択後、「SSO サブドメイン」に設定値を入力し、「設定」をタップします。

※設定値につきましては管理者様にお問い合わせください。

※初回時のみ本設定が必要です。



The image shows the login screen for KDDI Knowledge Suite. At the top is the logo 'KDDI Knowledge Suite'. Below it are two input fields: 'ログインID' (Login ID) with the example 'example@example.co.jp' and 'パスワード' (Password). There is a checkbox for 'ログインIDを保存' (Save login ID). A red box highlights the 'ログイン' (Login) button. Below the button is a blue link 'Knowledge Suiteとは？' (What is Knowledge Suite?). At the bottom are links for '設定' (Settings), '障害・メンテナンス情報' (Incident/Maintenance Information), 'ヘルプ' (Help), and 'プライバシーポリシー' (Privacy Policy). A copyright notice 'Copyright © KnowledgeSuite Inc. All Rights Reserved.' is at the very bottom.

3. ログイン画面にて何も入力せず「ログイン」をタップします。
4. お客様側でご契約された IdP のログイン画面が表示されるので、IdP の ID とパスワードでログインします。（IdP で認証済みの場合は IdP のログイン画面は表示されません。）



5. KDDI Knowledge Suite のログイン後の画面（トップページ）に遷移します。

■ 巻末資料

■ JIT プロビジョニングを利用して連携可能な項目

JIT プロビジョニングを「有効」とした場合に IdP と連携可能な Knowledge Suite のメンバーインポート項目は以下です。

Knowledge Suite の メンバーインポート項目名	IdP 側の 属性マッピングに登録する設定値
名前・姓	last_name
名前・名	first_name
ふりがな・姓	last_kana
ふりがな・名	first_kana
社員 ID	employee_id
電話番号（会社）	phone_number
電話番号（内線）	extension
電話番号（携帯電話）	cell_phone_number
部署名（表示用）	department
役職（表示用）	position

POINT

設定値を設定しない場合は、Knowledge Suite のメンバー招待時と同じ設定で登録されます。