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

GRIDY SSO（シングルサインオン）

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ー用

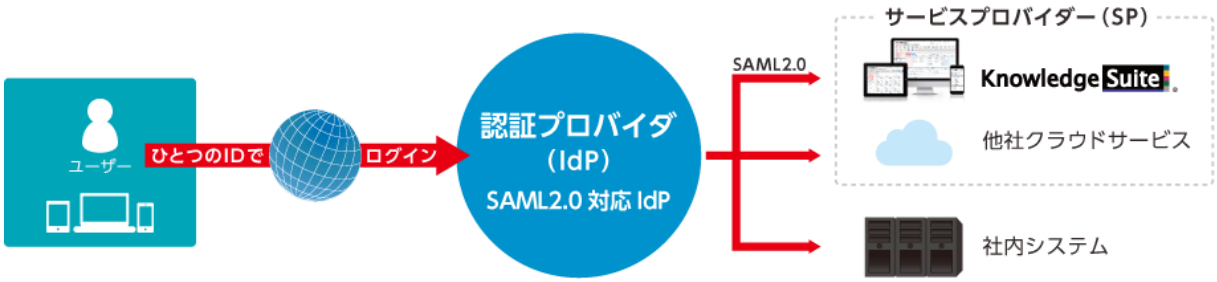
第２部　メンバー用

アドミニストレーター用　目次

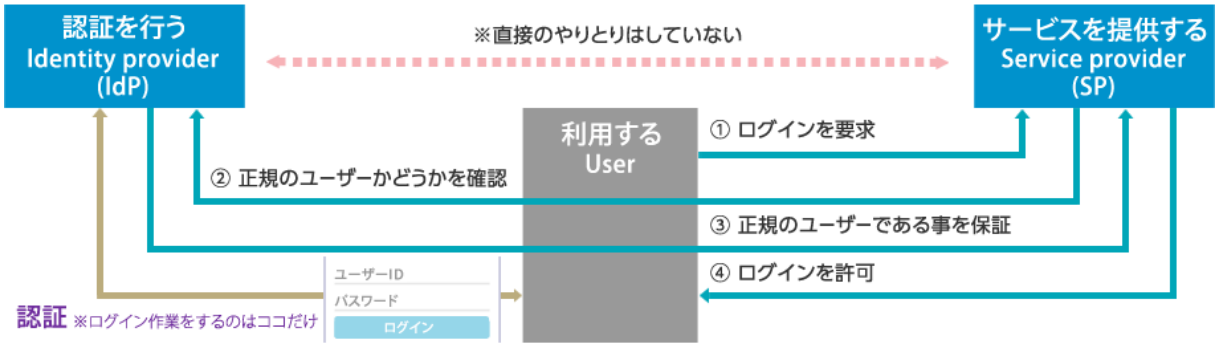
■1-1　SSO とは

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。

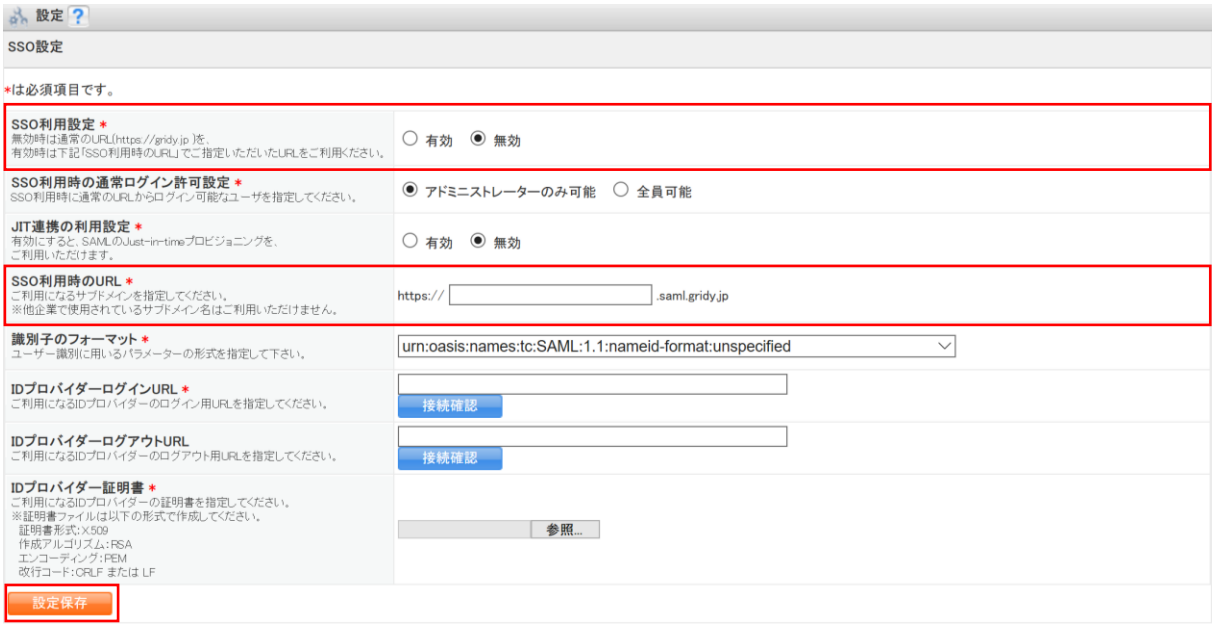
■1-2　SSO 設定

「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。

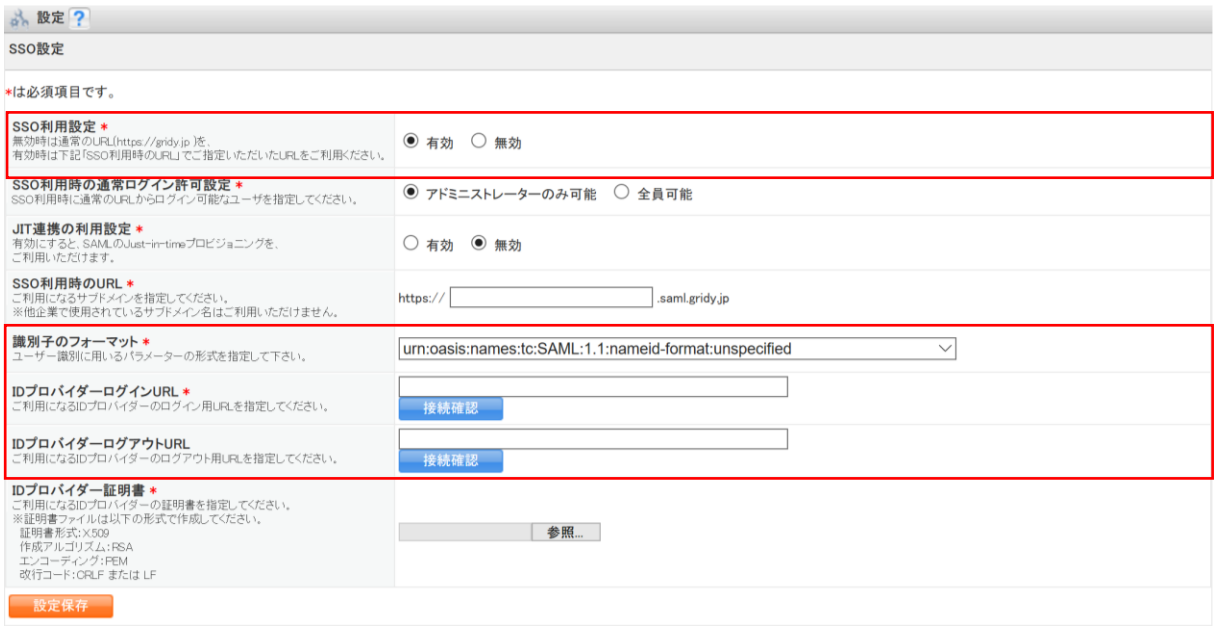


3. 「SSO 利用設定」は「無効」を選択し、「SSO 利用時の URL」に任意のサブドメインを入力して［設定保存］をクリックします。

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。



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。

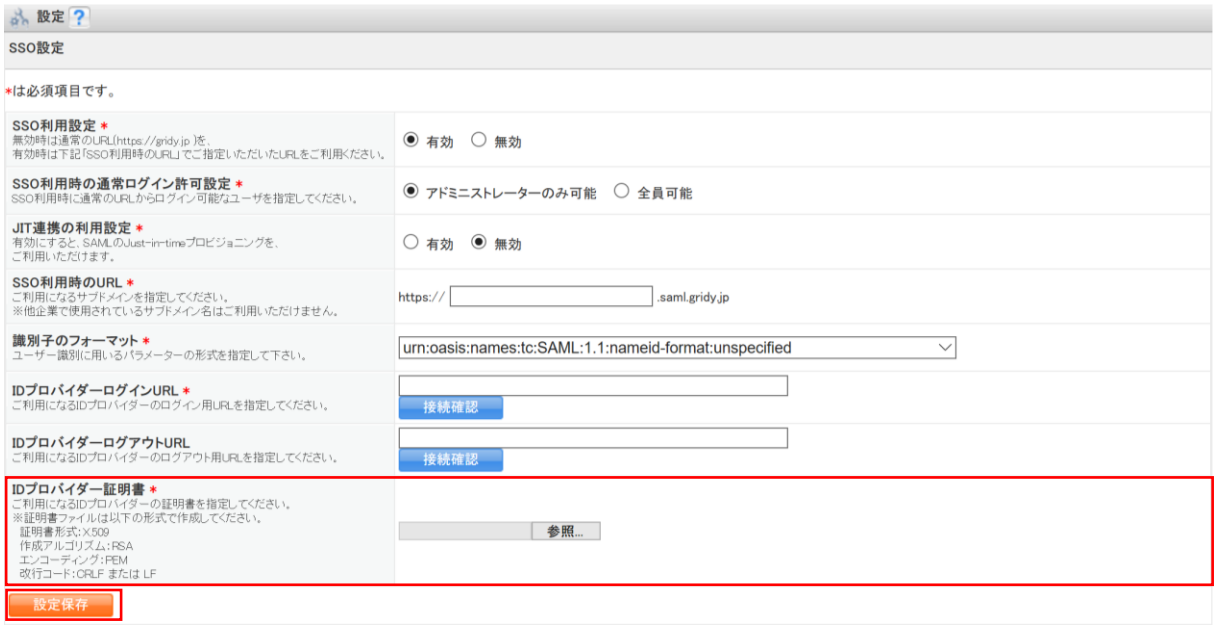
POINT

「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:WindowsDomainQualifiedName
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。



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

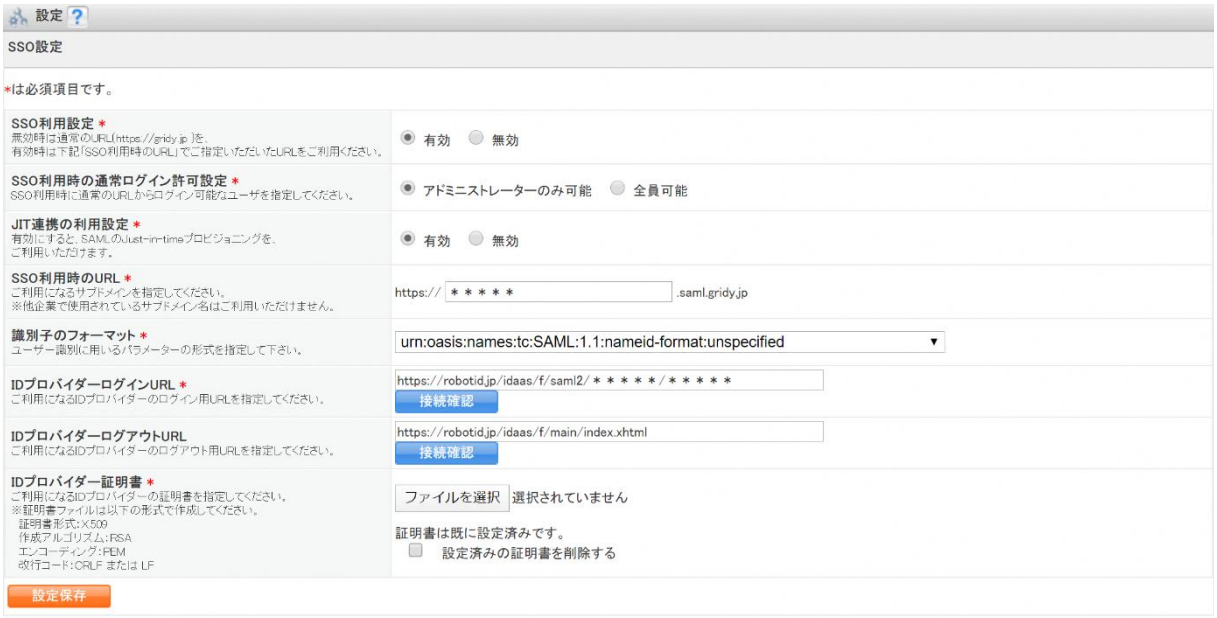
※「Azure Active Directory」等、証明書がファイルとして取得できない場合は、
-----BEGIN CERTIFICATE----- から -----END CERTIFICATE-----までをコピーし
そのままテキストエディタに貼り付けて作成してください。

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。



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"?><samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" Destination="https://knowledgesuite.saml.gridy.jp/login" ID="_53d634097c38496f8987158e4827a45e" InResponseTo="NQxJEgVOgETTlqWDnuJRKSSoJYKwMG" 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><samlp:Status><samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/></samlp:Status><saml:Assertion xmlns:saml="urn:oasi	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"?><samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" Destination="https://knowledgesuite.saml.gridy.jp/login" ID="_888ce116362143b88127a0680440c02c" InResponseTo="ywdElYbnLlpnXdBrXjkShOhClRgDpL" 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><samlp:Status><samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/></samlp:Status><saml:Assertion xmlns:saml="urn:oasi	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@exmple.com	<?xml version="1.0" encoding="UTF-8"?><samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" Destination="https://knowledgesuite.saml.gridy.jp/login" ID="_7f4051e326344cd2bec9a1467ea6bfff" InResponseTo="fBdicRoAOzjDcGpwbAmtzcklVfPpHE" 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><samlp:Status><samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/></samlp:Status><saml:Asse	失敗 携帯電話番号は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）

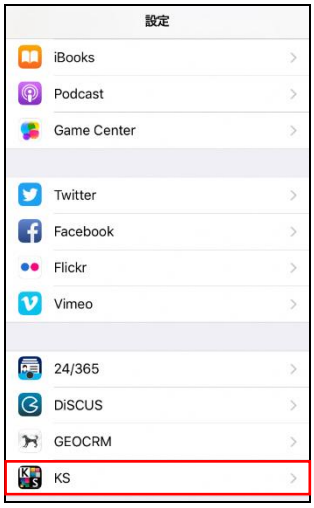
ブラウザからのご利用方法です。

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。

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。

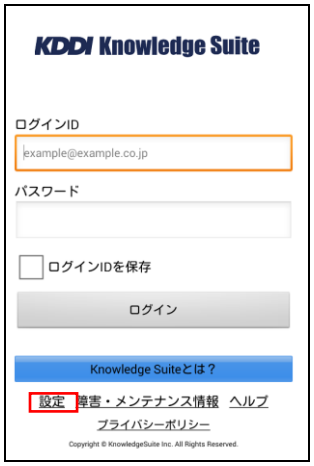
3. Knowledge Suite アプリを起動し、何も入力せず［ログイン］をタップします。

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。）

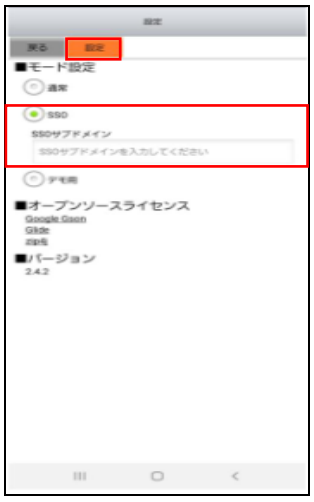
5. KDDI Knowledge Suite のログイン後の画面（トップページ）に遷移します。

■2-3　SSO を利用する（Android 版）

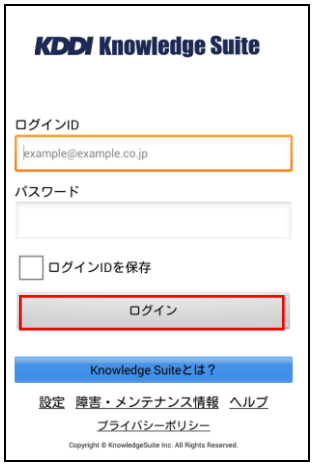
スマートフォン(Android端末)でアプリケーションを利用する前に必要となる初期設定および利用方法です。
事前準備として Google Play Store からご利用端末へアプリケーション「KDDI Knowledge Suite」をインストールしてください。



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。



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。