

# **KDDI Knowledge Suite**

**GRIDY SSO (シングルサインオン)**

---

**操作マニュアル**

**(1.3 版)**

2020 年 1 月 22 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

■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ー用 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

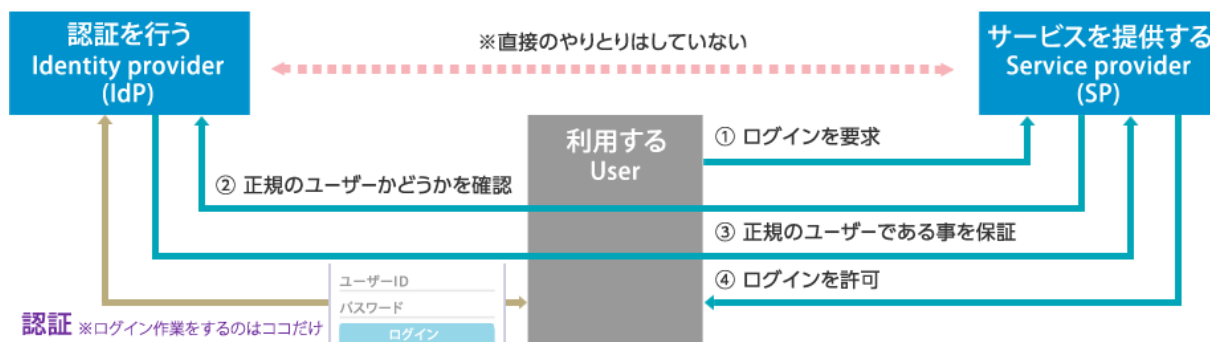
## ■ 1-1 SSO とは

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。

#### 【認証プロバイダー (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。

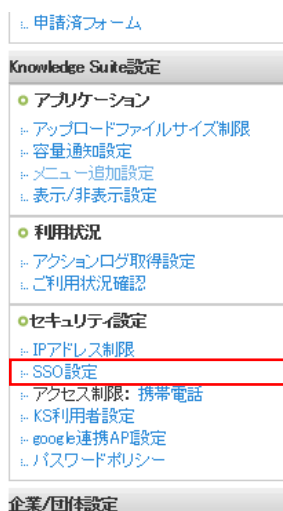
## 1-2 SSO 設定

「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。



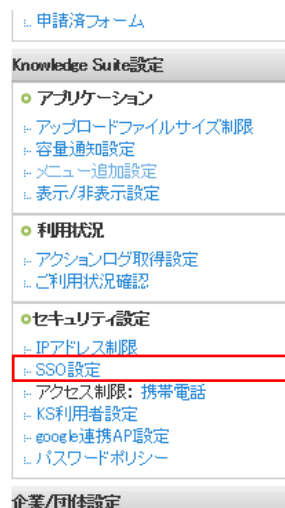
2. 「KDDI Knowledge Suite 設定」の「SSO 設定」をクリックします。

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。

 A screenshot of the 'SSO 設定' (SSO Settings) configuration page. The page contains several configuration items, each with a description and a control element. The following items are highlighted with red rectangular boxes:
 

- 'SSO 利用設定 \*': Includes radio buttons for '有効' (checked) and '無効'.
- 'SSO 利用時の通常ログイン許可設定 \*': Includes radio buttons for 'アドミニストレーターのみ可能' (checked) and '全員可能'.
- 'JIT 連携の利用設定 \*': Includes radio buttons for '有効' and '無効' (checked).
- 'SSO 利用時の URL \*': Includes a text input field with the value 'https://[ ] .saml.gridy.jp'.
- '識別子のフォーマット \*': Includes a dropdown menu with the value 'urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified'.
- 'ID プロバイダーログイン URL \*': Includes a text input field and a '接続確認' (Check Connection) button.
- 'ID プロバイダーログアウト URL': Includes a text input field and a '接続確認' (Check Connection) button.
- 'ID プロバイダー証明書 \*': Includes a '参照...' (Reference) button.

 At the bottom left, there is an orange '設定保存' (Save Settings) button.

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。

<b>JIT 連携の利用設定 *</b> 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。	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
--	--

**設定 ?**

**SSO設定**

\*は必須項目です。

<b>SSO利用設定 *</b> <small>無効時は通常のURL(https://gridy.jp)を、有効時は下記「SSO利用時のURL」でご指定いただいたURLをご利用ください。</small>	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
<b>SSO利用時の通常ログイン許可設定 *</b> <small>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。</small>	<input checked="" type="radio"/> アドミニストレーターのみ可能 <input type="radio"/> 全員可能
<b>JIT 連携の利用設定 *</b> <small>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。</small>	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
<b>SSO利用時のURL *</b> <small>ご利用になるサブドメインを指定してください。  <small>*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。</small></small>	https:// <input type="text"/> .saml.gridy.jp
<b>識別子のフォーマット *</b> <small>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。</small>	<input type="text" value="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified"/>
<b>IDプロバイダーログインURL *</b> <small>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。</small>	<input type="text"/> <input type="button" value="接続確認"/>
<b>IDプロバイダーログアウトURL</b> <small>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。</small>	<input type="text"/> <input type="button" value="接続確認"/>
<b>IDプロバイダー証明書 *</b> <small>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。  <small>*証明書ファイルは以下の形式で作成してください。</small></small>	<input type="text"/> <input type="button" value="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。

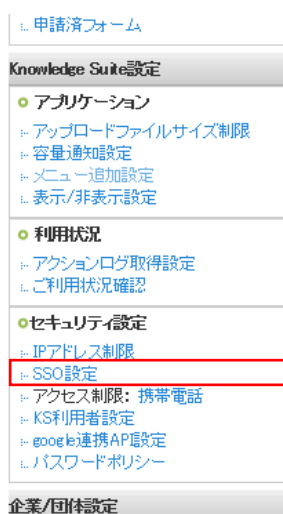


### 1-2-3 SSO 結果を確認する

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  
https://robotid.jp/idaas/f/saml2/\*\*\*\*\*/knowledge suite

**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  
https://robotid.jp/idaas/f/main/index.xhtml

**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...  
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
2019-11-21 16:37:13	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://knowledge.saml.gridy.jp/login" ID="b242580a8b674403bf23efc0f9ba426b" InResponseTo="ZVKTIJULKCDypnCIBADuOyhqFVNfh" IssueInstant="2019-11-21T07:37:12.021Z" Version="2.0"><saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">https://robotid.jp/idaas/f/saml2/*****/	成功	admin_flag: 0 ks_flag: 1 project_id: ***** last_name: 山下 first_name: 千佳 last_kana: ちか first_kana: やました
2019-11-21 16:17:35	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://knowledge.saml.gridy.jp/login" ID="ef32c9fab4b347b29b479cc5c07f6bb" InResponseTo="UsWWInhBEvueiFtpjXffgZpuuMrFMd" IssueInstant="2019-11-21T08:17:34.528Z" Version="2.0"><saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">https://robotid.jp/idaas/f/saml2/*****/	無効	

3. 「SSO 結果」を確認します。

POINT

JIT 連携でエラーが発生した場合は、「JIT 連携」の「結果」欄にエラーメッセージが表示されます。

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
2019-04-04 12:12:59	失敗 内部エラーが発生しました	k.maezono@example.jp	<?xml version="1.0" encoding="UTF-8"?><samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" Destination="https://gridy.jp/login" ID="77b1257efdda4b3c82361c13b73fbae0" InResponseTo="iroJiIGGFsxFyHueAGgNhZJmzMppAf" IssueInstant="2019-04-04T03:12:08.063Z" 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:St	失敗 部署識別情報が正しく指定されていません	extension: 101 project_id: ***** last_name: 前園 cell_phone_number: 090 00000000 phone_number: 0300000000 sort: 1 first_name: 清治 last_kana: まえその first_kana: きよはる

---

## 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。

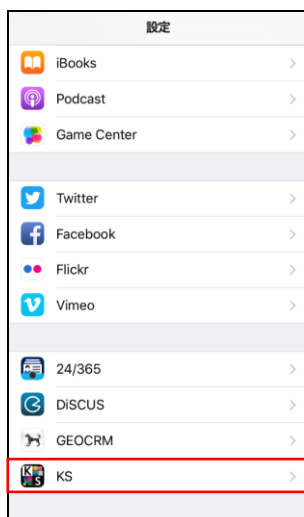
※お客様側でご契約された IdP のログイン画面が表示されます。

The screenshot displays the GRIDY SSO interface. At the top, the user is identified as 'Knowledge Suite, inc. 取締役会 前園 清治'. The main navigation area includes tabs for 'グループウェア', 'SFA', 'リードフォーム', 'CENTER', and 'メールビュー'. A central toolbar contains various application icons such as 'マイページ', 'スケジュール', '設備予約', '部署/グループ', 'フロント外管理', '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'. Below this, there are sections for 'お知らせ' (Notice) with several alerts, a 'スケジュール' (Schedule) calendar for 2018/04/02, and '新着掲示板' (New Bulletin Board) and '新着トピック' (New Topic) sections.

2. KDDI Knowledge Sute 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。



KDDI Knowledge Suite

ログインID  
パスワード

ログインIDを保存

ログイン

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。)



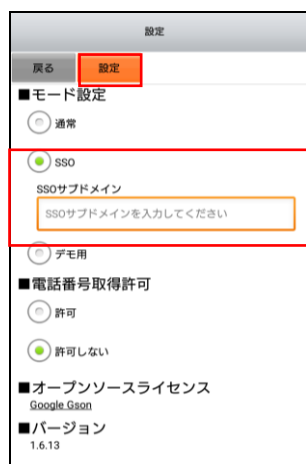
5. KDDI Knowledge Suite のログイン後の画面 (トップページ) に遷移します。

## ■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. モード設定画面にて「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。  
※手順 2 は初期設定時のみの手順です。



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
部署識別情報 (プロジェクト ID)	project_id
部署識別情報 (部署コード)	project_code
表示順	sort
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
アドミニストレーター権限	admin_flag
サブアドミニストレーター権限	sub_admin_flag
グループ管理者権限	group_manager_flag
KS 権限	ks_flag
スマートフォン利用許可	smartphone_flag
スマートフォン利用許可電話番号 1	smartphone_number1
スマートフォン利用許可電話番号 2	smartphone_number2
スマートフォン利用許可電話番号 3	smartphone_number3
SFA エクスポート権限 (営業報告)	sfa_report_export_flag
SFA エクスポート権限 (顧客)	sfa_customer_export_flag
SFA エクスポート権限 (顧客担当者)	sfa_manager_export_flag
SFA エクスポート権限 (商品)	sfa_goods_export_flag
SFA エクスポート権限 (商談)	sfa_negotiation_export_flag
SFA エクスポート権限 (商談商品)	sfa_negotiation_goods_export_flag
タイムカード権限	timecard_flag
ワークフロー権限	workflow_flag
掲示板権限	bulletin_flag

**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。