# **KDDI** Knowledge Suite

GRIDY SSO (シングルサインオン)

操作マニュアル (1.1版)

2018 年 5 月 16 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。

※ご利用ブラウザ、端末のバージョン等により表示画面が異なる場合がございます。予めご了承ください。

目次										
第1部 アドミニストレーター用	第2部 メンバー用									
■1-1 SSO とは 4	■2-1 SSO を利用する(ブラウザ版)10									
■1-2 SSO 設定5	■2-2 SSO を利用する(iOS 版)11									
	■2-3 SSO を利用する(Android 版)13									

# GRIDY SSO (シングルサインオン)

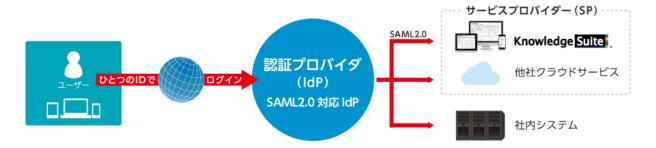
# アドミニストレータ一用

<b>■</b> 1-1	SSO Er	ţ														4
<b>■</b> 1-2	SSO 設定	<u> </u>														ļ

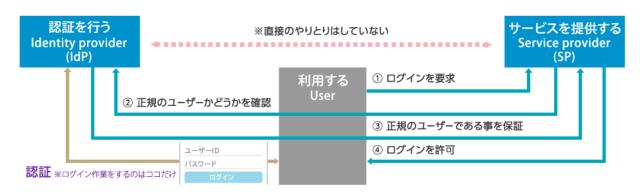
# ■1-1 SSO とは

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

「Knowledge Suite」にて、専用ログイン設定を行います。

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

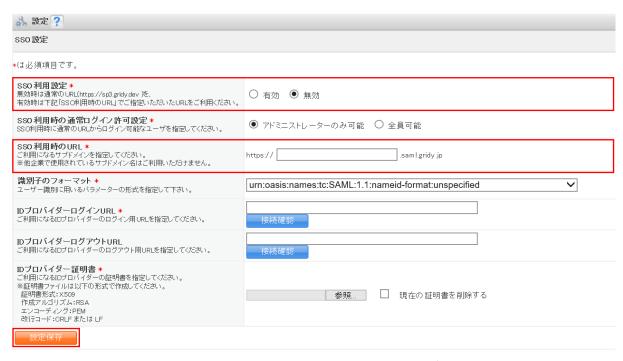


1. Knowledge Suite にログインし、画面上部の[設定]をクリックします。



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

### GRIDY SSO (シングルサインオン)



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。

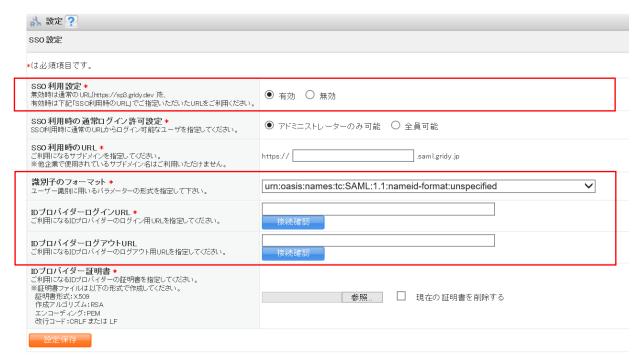
# 1-2-2 認証方式を設定する



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



2. 「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。

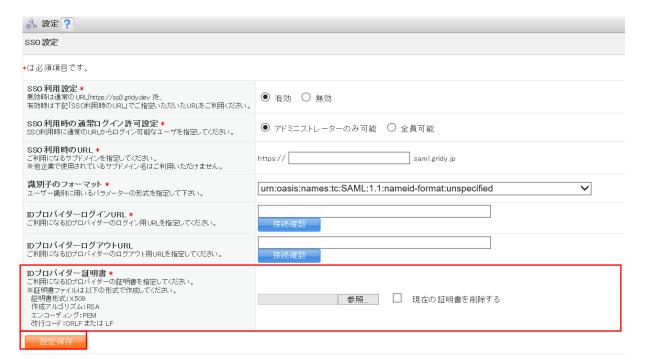
# POINT

「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:to:SAML:2.0:nameid-format:Kerberos urn:oasis:names:to:SAML:2.0:nameid-format:entity



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。

# GRIDY SSO (シングルサインオン)

# メンバー用

<b>■</b> 2-1	SSO を利用する	(ブラウザ版)	10
■2-2	SSO を利用する	(iOS版)	11
<b>2</b> -3	SSO を利用する	(Android 版)	13

# ■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。



2. 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。



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