

「Box」と「マガタマサービス」の SAML 連携

株式会社ディー・ディー・エス

1. 「Box」との SAML 連携

クラウド・コンテンツ・マネジメントプラットフォームである「Box」と次世代オンライン認証規格 FIDO (Fast Identity Online) に対応したクラウド本人認証「マガタマサービス」を連携します。これにより、指紋認証や顔認証、セキュリティキー認証、ワンタイムパスワード認証を利用して、Box に格納したコンテンツにパスワードレスでアクセスすることが可能になります。

2. 「Box」について

Box はモバイルデバイスでのファイル共有やアクセスから、企業全体のデータ管理やガバナンスなどの洗練されたビジネスプロセスまで、単純なものから複雑なものまで、企業が持つあらゆるコンテンツの課題を解決する、クラウド・コンテンツ・マネジメントプラットフォームです。場所やデバイスを問わず、様々なコンテンツへのセキュアなアクセスと情報の共有・活用を可能にするクラウドサービスです。

3. 連携イメージ



4. SAML 登録方法

(1) サービスプロバイダー情報（以下 SP と記述）の登録

i. アプリケーションの登録

Box の SP としての情報をマガタマサービス管理ツールへ登録します。ウェブブラウザ（Chrome や Internet Explorer 等）で管理ツールへアクセスし、「管理ツールにログイン」をクリックします。



管理者用のユーザー名とパスワードを入力して「認証」をクリックし、管理者としてログインします。



全体で設定されている「Sample Customer」（名称は任意で設定いただけます）を選択し、「認証情報」タブをクリックします。アプリケーションの「50010 SAML application」の「追加」をクリックしてアプリケーションの新規作成を行います。

Themis & マカタマサービス管理ツール | admin | メニュー | ログアウト

●ユーザー ○グループ

基本情報 **認証情報** ログビューアー

ユーザー ID 検索

全体

- Sample Customer**

グループ

- MAAdministrators [管理者]
- SampleGroup

どのグループにも属していないユーザー

なし

Sample Customer

アプリケーション

ID	アプリケーション名	設定
50002	Management tool Logon	設定 詳細
50010	SAML application	設定 追加

認証セット

No.	ID	認証セット名	設定
1	39016	PW	
2	39051	FIDO	

「アプリケーション名」と「概要」を入力し、必要な認証要素にチェックを入れて「保存」をクリックします。

Themis & マカタマサービス管理ツール | admin | メニュー | ログアウト

●ユーザー ○グループ

基本情報 認証情報 ログビューアー

ユーザー ID 検索

全体

- Sample Customer

グループ

- MAAdministrators [管理者]
- SampleGroup

どのグループにも属していないユーザー

なし

アプリケーションの新規作成

アプリケーション名

概要

利用可能な認証セット

- 39016 PW
- 39051 FIDO
- 39202 PW+FIDO
- 39052 WebAuthn
- 39204 PW+WebAuthn

保存

Copyright © 2018-2019 DDS, Inc.

「アプリケーション情報を作成しました。」と表示されます。登録した名前のアプリケーションが作成されていればアプリケーションの登録が完了となります。

Themis & マガタマサービス管理ツール | admin | メニュー | ログアウト

◎ユーザー ○グループ

基本情報 認証情報 ログビューアー

アプリケーション情報を作成しました。

全体

- Sample Customer

グループ

- MAAdministrators [管理者]
- SampleGroup

どのグループにも属していないユーザー

なし

Sample Customer

アプリケーション

ID	アプリケーション名	設定
50002	Management tool Logon	設定 詳細
50010	SAML application	設定 追加
70000	Box	設定 詳細 削除 SSO

認証セット

No.	ID	認証セット名	設定
1	39016	PW	
2	39051	FIDO	
3	39052	WebAuthn	

ii. Box の SP 情報の登録

管理ツール画面で全体の「Sample Customer」を選択し、「認証情報」タブをクリックします。その後、アプリケーションの「Box」の「詳細」をクリックします。

Themis & マガタマサービス管理ツール | admin | メニュー | ログアウト

◎ユーザー ○グループ

基本情報 認証情報 ログビューアー

アプリケーション情報を作成しました。

全体

- Sample Customer

グループ

- MAAdministrators [管理者]
- SampleGroup

どのグループにも属していないユーザー

なし

Sample Customer

アプリケーション

ID	アプリケーション名	設定
50002	Management tool Logon	設定 詳細
50010	SAML application	設定 追加
70000	Box	設定 詳細 削除 SSO

「Service Provider 情報の設定」の画面に遷移します。ここに、Box の SP としての情報を登録します。

The screenshot shows the 'Service Provider Information Settings' page. The 'SP Name' field is set to 'Box'. The 'Issuer' and 'SSO End Point' fields are highlighted with a red box. The 'SAML Settings' section includes a checkbox for 'SAML Request Signature Verification' (unchecked), a dropdown for 'Signature Algorithm' (SHA-256), and a dropdown for 'Session Timeout' (infinite). A red box highlights the '更新' (Update) button at the bottom.

Service Provider 情報の設定

設定変数	値
SP の名前	任意の名称を設定ください
Issuer	※1
SSO エンドポイント	※1
SLO エンドポイント	-
メタデータ URL	-
フィンガープリント	-
RelayState	-

※1 担当者にお問い合わせください。

(2) ID プロバイダー（以下 Idp と記述）情報の登録

マガタマサービスの Idp としての情報を Box へ登録します。管理ツール画面で全体の「Sample Customer」を選択し、「認証情報」タブをクリックします。その後、アプリケーションの「Box」の「SSO」をクリックします。



「SSO 設定情報」が表示されます。ここで表示される「SSO エンドポイント」、「SLO エンドポイント」、「メタデータ」、「X.509 証明書」の情報を Box のフェデレーションサーバに登録します。

(例) SSO 設定情報ページ



ここまでの登録手順を実施することで、次回ログイン以降、「Box」の SAML 専用ログイン URL から「マガタマサービス」の認証ページにリダイレクトされ、FIDO 認証を利用しフェデレーションを行うことができるようになります。

以上