D191080

「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。

Themis & マガタマサービス管理ツール 1.0.0 メニュー
ログイン先を選択してください
個人用ポータルにログイン
管理ツールにログイン
Copyright © 2015-2018 DDS, Inc.

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。

Themis & マガタマサービス管理	ピール 1.0.0 メニュー	
	Themis Account Manager Login	
	ユーザ選択・ ユーザID]
	PW FIDO OTP PW+FIDO PW+OTP	
	パスワードを入力して「認証」を押してください。	_
	パスワード]
Copyright © 2015-2018 DDS		-
	認証	
	キャンセ	าน

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 & マガタマサービス管理ツール admin > ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・	ニュー ログアウト 基本情報	認証情報 □	グ ビューアー	
ユーザー ID 検索	Samp	e Custome	er	
Sample Customer	ID	アプリケーシ	ヨン名	設定
グループ	50002	Managemer	nt tool Logon	設定 詳細
 MAAdministrators [管理者] SampleGroup 	50010	SAML applic	cation	設定 <mark>追加</mark>
・ ・ ・ どのグループにも風していないユーザー	認証セット			
	No.	ID	認証セット名	設定
-50	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
ユーザー ID 検索	アプリケーションの新規作成
全体 • Sample Customer	アプリケーション名 Box
グループ	概要
 MAAdministrators [管理者] SampleGroup 	利用可能な認証セット
どのグループにも属していないユーザー	
なし	⊠ 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。

iemis & マガダマリーと大管理ツール admin メ					
●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	アプリケー	ション情報を作	「成しました。		
全体 • Sample Customer	Sample	e Custo ∍>	mer		
グループ	ID	アプリケー	ション名	設定	
 MAAdministrators [管理者] SampleGroup 	50002	Managem	ent tool Logon	設定 詳細	
どのグループにも属していないユーザー	50010	SAML app	lication	設定 追加	
なし	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−ザ− ○グル−プ	基本情報	認証情報 ログビュ	ーアー	
ユーザー ID 検索	アプリケ-	ーション情報を作成しました。		
全体 • Sample Customer	Samp アプリケージ	le Customer		
	ID	アプリケーション名	1	安定
MAAdministrators [50002	Management tool Log	on 1	殳定 詳細
どのグループにも属していないユーザー	50010	SAML application	1	殳定 追加
なし	70000	Box		殳定 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。

シューザー ○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	Service Provid	der情報の設定
全体			
Sample Customer	10	SPの名前	Box
ヴループ		Issuer	ACCURATE A
 MAAdministrators SampleGroup 	[管理者]		
どのグループにも騙してい	ないユーザー	22017FW47F	
なし		SLOエンドポイント	
		メタデータURL	
		フィンガープリント	
		RelayState	
		SAMLの設定	
			□ SAMLリクエストの署名検証を行う
		署名アルゴリズム	SHA-256 ~
		セッション有効期間	無期限
			□ ログイン時に必ず認証を行う
			更新

Service Provider 情報の設定

設定変数	值
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。

Themis & マガタマサービス管理ツール admin メニュ	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	Sampl	e Custo	mer	
全体	アプリケーシ	ヨン		
Sample Customer	ID	アプリケー	ション名	設定
グループ	50002	Manageme	ent tool Logon	設定 詳細
• MAAdministrators [管理者]	50010	SAML appl	ication	設定 追加
• SampleGroup	70000	Box		設定 詳細 削除 SSO

「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

		7752552252		
ユーザー 〇グループ	基本情報	認証情報	ログビューアー	
ユーザー ID 検索	SSO設定	宦情報		
体				
Sample Customer				Con.
ループ	SSOID	F#42F		Сору
 MAAdministrators [管理者] SampleGroup 	SLOID	ドボイント		Сору
のグループにも罵していないユーザー				
なし		メタデータ		Сору
	x.:	509証明書	表示	
		1		^
				_
				÷
				-
				Сору

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