D210070

「Citrix ADC」と「Themis」の SAML 連携

株式会社ディー・ディー・エス

シトリックス・システムズ・ジャパン株式会社

1. 「Citrix ADC」との SAML 連携

アプリケーションデリバリーと負荷分散機能を提供する「Citrix ADC」と多要素認 証を可能とする「万能認証基盤 Themis」を連携することで、顔認証などの多要素認 証を利用して、目的のリソースにセキュアにリモートアクセスできるようになりま す。

2. 「Citrix ADC」について

Citrix ADC (旧称 NetScaler ADC) は包括的なアプリケーションデリバリーソリュ ーションであり、ハイブリッドマルチクラウド環境において負荷分散を含む柔軟なト ラフィックコントロールによりサイトパフォーマンスを最大化するとともに、認証連 携、暗号化、リモートアクセス、アプリケーションファイアウォールなど、近年のサ ービスに不可欠なセキュリティ機能を提供します。

アプリケーションサーバ単体では実装できない付加機能も、物理/仮想アプライアン スもしくはクラウド上にインスタンスを配置する事で容易に構成する事が可能になり ます。

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

Citrix ADC の SP としての情報を Themis 管理ツールへ登録します。ブラウザで 管理ツールを開き、「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	ツール 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	ESE	
	キャンセル	

全体で設定されている「DEMO 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 inituser4732	2d275 メニュ	- ログアウト		
◉ユーザー ◎グループ	基本情報	認証情報 [コグビューアー	
ユーザー ID 検索	DEMO アプリケー:	CUSTOME	R	
• DEMO CUSTOMER	ID	アプリケーシ	ョン名	設定
グループ	50002	Managemer	nt tool Logon	設定 詳細
Group A Group B	50010	SAML applie	cation	設定 <mark>追加</mark>
Group C	認証セット			
• MAAdministrators [管理者]	No.	ID	認証セット名	設定
どのグループにも属していないユーザー	1	39016	PW	
• DDS 太郎	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)	レ 1.7.1 (c0be8db) pocuser1 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	*** アプリ	」ケー	ションの新規作成
全体			
DemoCenter	アプリケー	ーション名	Citrix ADC
グループ		概要	
 MAAdministrators [管理者] どのグループにも属していないユー 	ザー 利用可能な	認証セット	
なし			9016 PW
			9051 FIDO
			9104 OTP
			9202 PW+FIDO
			9203 PW+OTP
			9105 Credential Cache
			9066 FACE
			9205 PW+FACE
	SA	ML連携先	
			その地 ~
			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 inituser	4732d275 メニュ	- ログアウト			
●ユーザー ○グループ	基本情報	認証情報 🛛	コグ 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 • DEMO CUSTOMER	DEMO アプリケー:	CUSTOME	R		
91L-J	ID	アプリケーション	冶	設定	
Group A Group B	50002	Management to	ool Logon	設定 詳細	
Group C MAAdministrators [管理委]	50010	SAML applicati	on	設定 追加	
どのグループにも厚していないユーザー	70000	Citrix ADC		設定 詳細 削除 SS(0
• DDS 太郎	認証セット				
	No.	ID	認証セット名		設定
	1	39016	PW		
	2	39051	FIDO		
	2	00050			

ii. Citrix ADC の SP 情報の登録

管理ツール画面で全体の「DEMO 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「Citrix ADC」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 inituser473	32d275 メニュ-	- 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	ーション情報を作成しました。	
全体 ・ DEMO CUSTOMER	DEMO アプリケーシ		
	ID	アプリケーション名	設定
Group A Group B	50002	Management tool Logon	設定 詳細
• Group C • MAAdministrators [管理者]	50010	SAML application	設定 追加
どのグループにも属していないユーザー	70000	Citrix ADC	設定 <mark>詳細</mark> 削除 SSO

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

基本情報 認証情報 ログ ビューアー	
Service Provider情報の設定	
SPの名前	Citrix ADC
Issuer	
SSOエンドポイント	
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	185700
	□ ログイン時に必ず認証を行う
属性の設定	
	□ ユーザーID
	0 名
	□ 姓
	□ EX−JL
	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	*1
メタデータ URL	*1
フィンガープリント	-

RelayState	-	
····································	カンマイン	- 一川白ノンショ

※1 お使いの Citrix ADC のメタデータに従って設定ください。

(2) ID プロバイダー(以下 Idp と記述)情報の登録
 Themis の Idp としての情報を Citrix ADC へ登録します。

管理ツール画面で全体の「DEMO 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「Citrix ADC」の「SSO」をクリ ックします。

Themis & マガタマサービス管理ツール inituser4732	d275 メニュー	ログアウト			
®ユ −ザ − [©] グル−プ	基本情報	認証情報	コグビューアー		
ユーザー ID 検索	SP情報を更	新しました。			
全体 ・ DEMO CUSTOMER	DEMO アプリケーショ	CUSTOM	ER		
クループ	ID	アプリケーショ	ン名	設定	
Group A Group B	50002	Management	cool Logon	設定 詳細	
• Group C	50010	SAML applicat	ion	設定 追加	
どのグループにも属していないユーザー	70000	Citrix ADC		設定 詳細 削除 <mark>SSO</mark>	
• DDS 太郎	認証セット				
	No.	ID	認証セット名	10	婝
	1	39016	PW		
	2	39051	FIDO		

「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 Citrix ADC のポータルサイトに登録します。

(例) SSO 設定情報ページ

基本情報認証情報	ログ ビューアー	
SSO設定情報		
SSOエンドポイント	https://sv.dds-themis.com:10443/admtool/saml/	Сору
SLOエンドポイント	https://sv.dds-themis.com:10443/admtool/saml/	Сору
メタデータ	https://sv.dds-themis.com:10443/admtool/saml/	Сору
X.509証明書	表示	
	BEGIN CERTIFICATE	^
	Read on payment provides with provident and services and the set	
	A DATE OF A DESCRIPTION OF A DATE OF	
		-
	and the statement of the second statement of the secon	
	Co	ру

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、「Citrix ADC」の SAML 専用 ログイン URL から「Themis」の認証ページにリダイレクトされ、Themis 認証を利用し て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