

「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。



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「DEMO CUSTOMER」（名称は任意で設定いただけます）

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。

The screenshot shows the 'Authentication Information' tab for 'DEMO CUSTOMER'. The left sidebar lists 'DEMO CUSTOMER' and several groups. The main content area displays a table of applications and a table of authentication sets.

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

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。

The screenshot shows the 'New Application Creation' form. The 'Application Name' field is filled with 'Citrix ADC'. The 'Summary' field is empty. Under 'Utilizable Authentication Sets', several checkboxes are visible, with '9016 PW', '9051 FIDO', and '9205 PW+FACE' highlighted with red boxes. The 'SAML Relay First' dropdown is set to 'その他' (Others), and the 'Save' button is also highlighted with a red box.

「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 | inituser4732d275 | 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

アプリケーション情報を作成しました。

全体

- DEMO CUSTOMER

グループ

- Group A
- Group B
- Group C
- MAAdministrators [管理者]

どのグループにも属していないユーザー

- DDS 太郎

DEMO 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	Citrix ADC	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	

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 | inituser4732d275 | 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

アプリケーション情報を作成しました。

全体

- DEMO CUSTOMER

グループ

- Group A
- Group B
- Group C
- MAAdministrators [管理者]

どのグループにも属していないユーザー

DEMO 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	Citrix ADC	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、XXXX の SP としての情報を登録します。

Service Provider 情報の設定

SP の名前: Citrix ADC

Issuer: [Redacted]

SSO エンドポイント: [Redacted]

SLO エンドポイント: [Redacted]

メタデータ URL: [Redacted]

フィンガープリント: [Redacted]

RelayState: [Redacted]

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: 1 時間

ログイン時に必ず認証を行う

属性の設定

ユーザー ID

名

姓

Eメール

更新

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	※1
メタデータ URL	※1
フィンガープリント	-

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