

## Citrix Virtual Apps and Desktops へのタブレット顔認証利用について

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

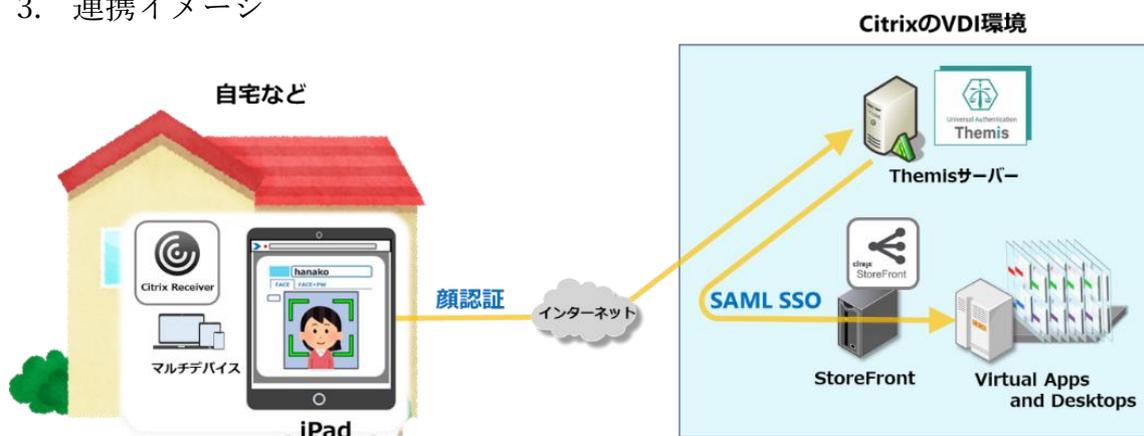
### 1. 万能認証基盤 Themis による iPad 顔認証で Citrix の VDI 環境へログイン

セキュアな仮想アプリケーションと仮想デスクトップを配信するソリューション Citrix Virtual Apps and Desktops の Citrix StoreFront と万能認証基盤 Themis を連携することで、Citrix Virtual Apps and Desktops の環境に iPad のカメラを利用した Themis の顔認証でシームレスなログインが可能となります。これにより、データセンターなどへ集約された仮想化環境に対して、自宅や外出先で iPad の顔認証を利用して安全かつ便利にアクセスして業務を行うことができます。

### 2. Citrix StoreFront について

Citrix StoreFront は、セキュリティを向上させ、導入を簡素化するエンタープライズアプリストアであり、あらゆるプラットフォーム上の Citrix Workspace App で、比類のない最新のユーザーエクスペリエンスを提供します。Citrix StoreFront を使えば、マルチサイト、マルチバージョンの Citrix Virtual Apps and Desktops 環境を簡単に管理することができます。これにより、組織は特定のビジネスニーズに合わせてブランディングと展開をカスタマイズすることができます。また、Citrix StoreFront は、ユーザーがどこにいても、どんなデバイスからでも仕事ができるように、モビリティへの取り組みを可能にしています。

### 3. 連携イメージ



## 4. SAML 登録方法

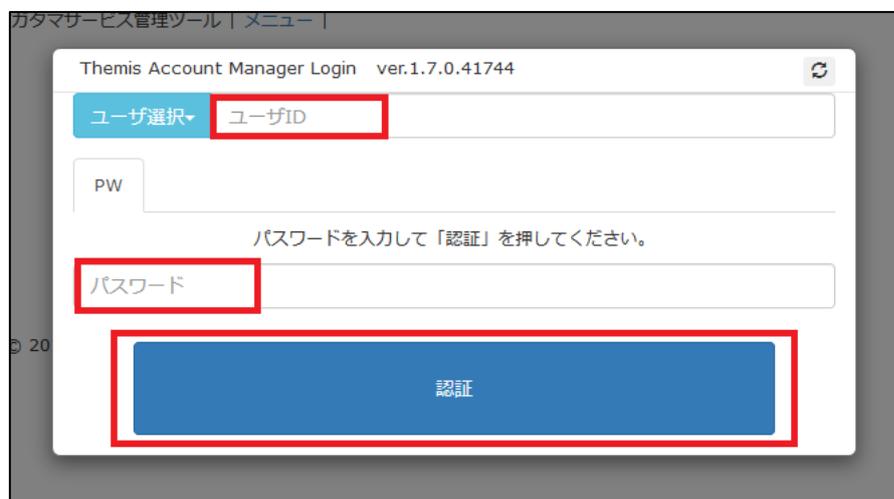
### (1) サービスプロバイダー情報（以下 SP と記述）の登録

#### i. アプリケーションの登録

Citrix StoreFront 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）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 | メニュー | ログアウト

◎ユーザー ○グループ

ユーザー ID  検索

全体

**DEMO CUSTOMER**

グループ

- MAAdministrators [管理者]

どのグループにも属していないユーザー  
なし

基本情報 **認証情報** ログ ビューアー

## DEMO CUSTOMER

オフライン認証の許可 許可する

[編集](#)

アプリケーション

ID	アプリケーション名	設定
50002	Management tool Logon	<a href="#">設定 詳細</a>
50005	Offline Caching	<a href="#">設定 詳細</a>
50006	ID Manager application	<a href="#">設定 詳細 追加</a>
50008	Windows Logon	<a href="#">設定 詳細</a>
50010	SAML application	<a href="#">設定 追加</a>

認証セット

No.	ID	認証セット名	設定
1	39016	PW	
2	39066	FACE	

「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

ユーザー ID  検索

全体

- DEMO CUSTOMER

グループ

- MAAdministrators [管理者]

どのグループにも属していないユーザー  
なし

基本情報 認証情報 ログ ビューアー

## 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

39066 FACE

39205 PW+FACE

SAML連携先

「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

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

- MAAdministrators [管理者]

どのグループにも属していないユーザー  
なし

## DEMO CUSTOMER

オフライン認証の許可 許可する [編集](#)

アプリケーション

ID	アプリケーション名	設定
50002	Management tool Logon	<a href="#">設定 詳細</a>
50005	Offline Caching	<a href="#">設定 詳細</a>
50006	ID Manager application	<a href="#">設定 詳細 追加</a>
50008	Windows Logon	<a href="#">設定 詳細</a>
50010	SAML application	<a href="#">設定 追加</a>
70000	Citrix StoreFront	<a href="#">設定 詳細 削除 SSO</a>

## ii. Citrix StoreFront 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 StoreFront」の「詳細」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

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

- MAAdministrators [管理者]

どのグループにも属していないユーザー  
なし

## DEMO CUSTOMER

オフライン認証の許可 許可する [編集](#)

アプリケーション

ID	アプリケーション名	設定
50002	Management tool Logon	<a href="#">設定 詳細</a>
50005	Offline Caching	<a href="#">設定 詳細</a>
50006	ID Manager application	<a href="#">設定 詳細 追加</a>
50008	Windows Logon	<a href="#">設定 詳細</a>
50010	SAML application	<a href="#">設定 追加</a>
70000	Citrix StoreFront	<a href="#">設定 <b>詳細</b> 削除 SSO</a>

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

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

### Service Provider情報の設定

全体

- DEMO CUSTOMER

グループ

- MAAdministrators [管理者]

どのグループにも属していないユーザー

なし

SPの名前: Citrix StoreFront

Issuer: http://localhost:8080/citrix/storefront/

SSOエンドポイント: http://localhost:8080/citrix/storefront/

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

### 属性の設定

ユーザーID

名

姓

Eメール

#### 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

Themis の Idp としての情報を Citrix StoreFront 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 StoreFront」の「SSO」をクリックします。

The screenshot shows the 'DEMO CUSTOMER' configuration page in the Themis & Magatama Service Management Tool. The 'Authentication Information' tab is active, displaying a table of applications. The 'Citrix StoreFront' application (ID 70000) is listed, and the 'SSO' link in the 'Settings' column is highlighted with a red box.

ID	アプリケーション名	設定
50002	Management tool Logon	設定 詳細
50005	Offline Caching	設定 詳細
50006	ID Manager application	設定 詳細 追加
50008	Windows Logon	設定 詳細
50010	SAML application	設定 追加
70000	Citrix StoreFront	設定 詳細 削除 <b>SSO</b>

「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 XXXX 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

### SSO設定情報

**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**

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiMCEHvFtfCQ/AE4KBECQqwSAAwwDQYJKoZIhvcNAQELBQAwXDELMakG
A1UEBhMCSIAxEjAQBgNVBAGMCFpY2hpLlUtlbjETMBEGA1UEBwwKTmFnb3lhLXNo
aTESMBAGA1UECgwJRERTLCBjbmMuMRAwDgYDVQQDDAdERFMgU1NPMB4XDTIwMDYx
NTA2MDc1N1oXDTMwMDYxNTA2MDc1N1owXDELMakGA1UEBhMCSIAxEjAQBgNVBAGM
CUFpY2hpLlUtlbjETMBEGA1UEBwwKTmFnb3lhLXNoaTESMBAGA1UECgwJRERTLCBj
bmMuMRAwDgYDVQQDDAdERFMgU1NPMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAYt1H/5Yk7UObVSTu3uGNkdBkkFb2anDI95XYSm
t3ySuKt1NkqMEIzc/U
ahX4S1CNII//gkC6Jm2ygTeOgIyGtYgxfFUPBnpTZ+nMaxq
-----
```

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」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、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

Citrixロゴおよびその他のマークは、Citrix Systems, Inc. および／またはその一もしくは複数の子会社の商標であり、米国の特許商標庁および他の国において登録されている場合があります。その他の社名、商品名はそれぞれの所有者の登録商標または商標です。