

「Cisco Webex」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. Cisco Webex との SAML 連携

音声会議、ビデオ会議、Web 会議をすべてひとつに統合する「Cisco Webex」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、シンプルな認証で安全なサービス利用を実現します。

2. Cisco Webex について

「Cisco Webex」は、世界で最も利用されている Web 会議システムです。インターネット経由であるにもかかわらず複数人での高品質なコミュニケーションが可能のため、毎月 2,000 万件以上ものミーティングに活用されています。

3. 連携イメージ

スマートフォン連携認証 (スマートフォンで認証を肩代わり)

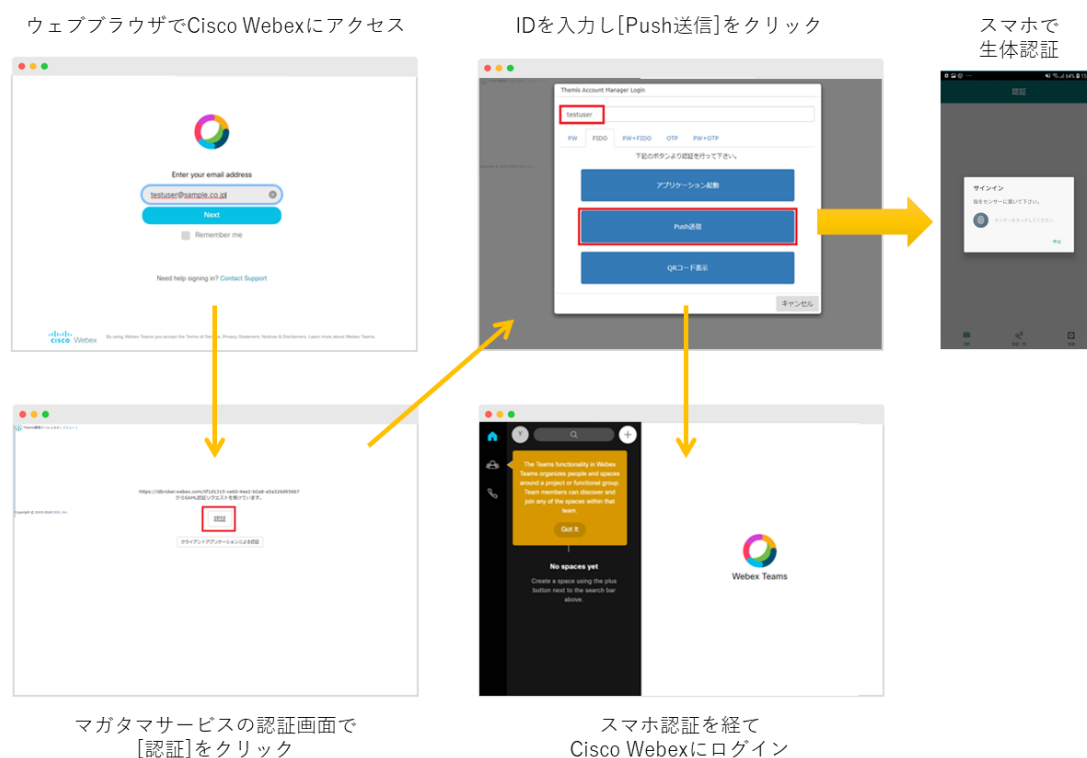
プッシュ通知認証 (認証サーバー経由でプッシュ通知をスマートフォンに送り、代理で認証)



Cisco Webex では、様々な PC での Web ブラウザでのアクセスから、Windows、macOS、iOS、Android デバイスでのアプリケーションからの認証でマガタマサービスがご利用いただけます。

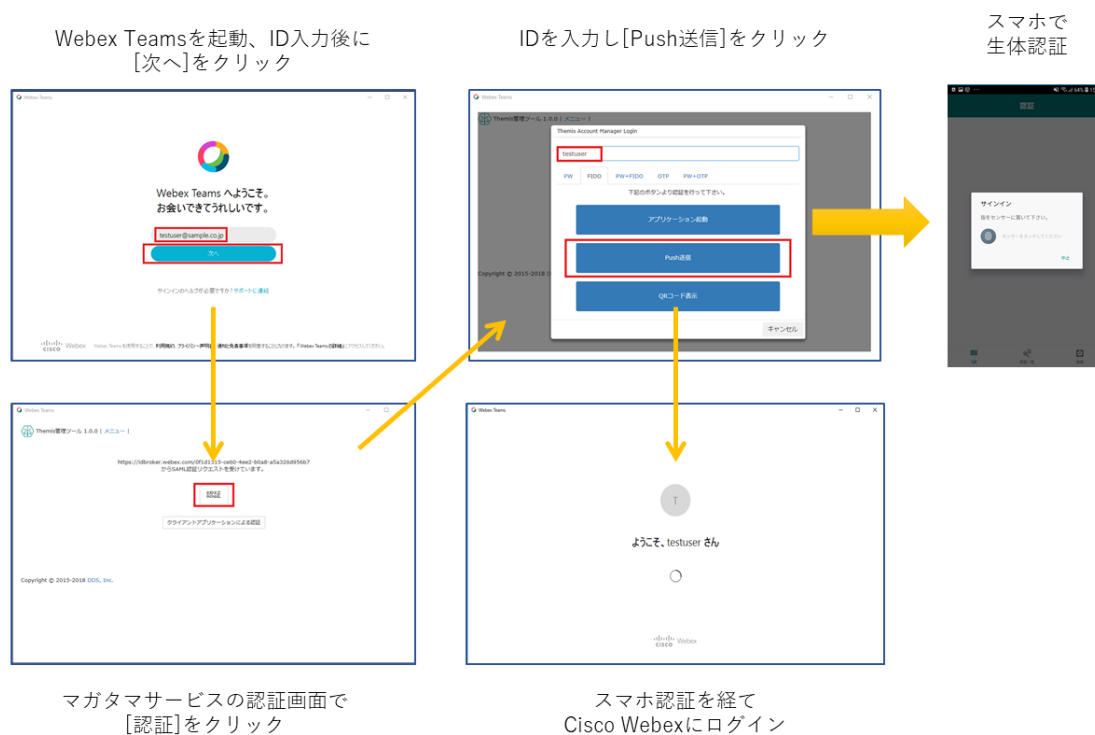
(1) Web ブラウザ経由の場合

ブラウザで「Cisco Webex」へアクセス（ログインIDを入力して[Next]をクリック）するとマガタマサービスの認証にリダイレクトされます。マガタマサービスの認証でスマートフォンへの「Push 送信」を選択することで、スマートフォンの生体認証で認証が可能となります。通知を受けたスマートフォンで生体認証をすることで、「Cisco Webex」へログインします。



(2) Windows/macOS アプリケーションの場合

アプリケーション「Webex Teams」を起動し、ログイン ID を入力して[次へ]をクリックすると、マガタマサービスの認証にリダイレクトされます。マガタマサービスの認証でスマートフォンへの [Push 送信] を選択することで、スマートフォンの生体認証で認証が可能となります。通知を受けたスマートフォンで生体認証をすることで、「Webex Teams」へログインします。



(3) Android アプリケーションの場合

Android のアプリケーション（「Webex Teams」アプリ）を起動し、ログイン ID を入力して[次へ]をクリックすると、マガタマサービスの認証にリダイレクトされます。マガタマサービスの認証でスマートフォンへの [Push 送信] を選択することで、スマートフォンの生体認証で認証が可能となります。スマートフォンで生体認証を行うことで「Webex Teams」アプリへログインします。

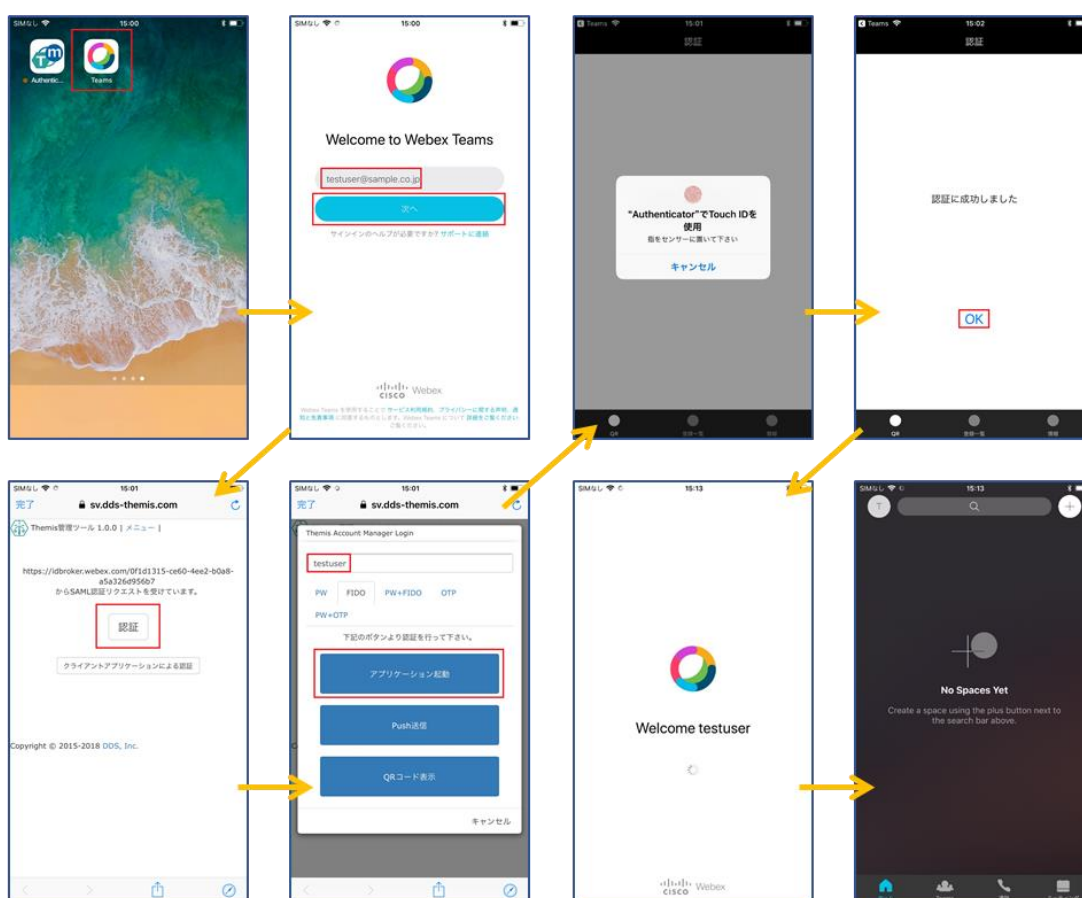


(4) iOS アプリケーションの場合

iOS のアプリケーション（「Webex Teams」アプリ）を起動し、ログイン ID を入力して[次へ]をクリックすると、マガタマサービスの認証にリダイレクトされます。マガタマサービスの認証でスマートフォンでの認証を行う [アプリケーション起動] を選択することで、iOS の生体認証（Touch ID など）での認証が可能となります。スマートフォンで生体認証を行うことで「Webex Teams」アプリへログインします。

Webex Teamsを起動、ID入力後に
[次へ]をクリック

スマホで生体認証後、
表示される画面で[OK]をクリック



マガタマサービスの認証画面で
[認証]をクリックし、表示された画面で
IDを入力し[アプリケーション起動]をクリック

Webex Teamsにログイン
(ホーム画面からTeamsを起動すると
ログイン処理を実行)

4. SAML 登録方法

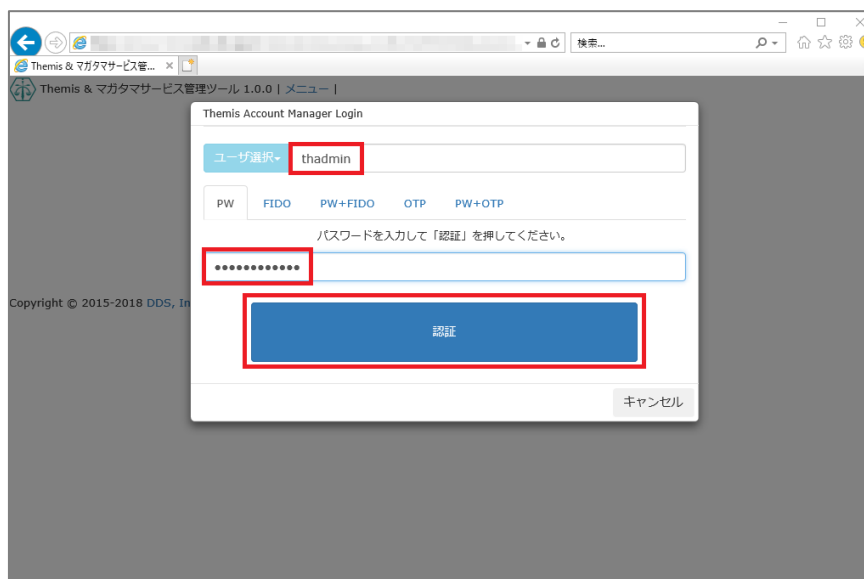
(5) サービスプロバイダー情報（以下 SP と記述）の登録

i. アプリケーションの登録

Cisco Webex 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。
Internet Explorer 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 & マガタサーバー管理ツール 1.0.0 | thadmin | 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

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	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 & マガタサーバー管理ツール 1.0.0 | thadmin | 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

アプリケーションの新規作成

アプリケーション名 Webex

概要 WebexへのSAMLログイン

利用可能な認証セット

- 39016 PW
- 39051 FIDO
- 39104 OTP
- 39202 PW+FIDO
- 39203 PW+OTP
- 39031 FeliCa
- 39105 Credential Cache

保存

Copyright © 2015-2018 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。

The screenshot shows the 'Application Information' page for 'DEMO CUSTOMER'. The 'Application Information' tab is active, and a green message states 'Application information was created successfully.' The 'Applications' table lists three entries: 'Management tool Logon' (ID 50002), 'SAML application' (ID 50010), and 'Webex' (ID 70000). The 'Webex' entry is highlighted with a red box, and its 'Settings' link is also highlighted. The 'Authentication Sets' table below shows one set with ID 39016 and name 'PW'.

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	Webex	設定 詳細 削除 SSO

No.	ID	認証セット名	設定
1	39016	PW	

ii. Cisco Webex 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「Cisco Webex」の「詳細」をクリックします。

The screenshot shows the 'Authentication Information' page for 'DEMO CUSTOMER'. The 'Authentication Information' tab is active. The 'Applications' table lists three entries: 'Management tool Logon' (ID 50002), 'SAML application' (ID 50010), and 'Webex' (ID 70000). The 'Webex' entry is highlighted with a red box, and its 'Details' link is also highlighted. The 'Authentication Sets' table below shows two sets: one with ID 39016 and name 'PW', and another with ID 39051 and name 'FIDO'.

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	Webex	設定 詳細 削除 SSO

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

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

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 詳細は Cisco Webex の SAML 認証ガイドを御覧ください。

- (6) 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 INSUITE 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「Cisco Webex」の「SSO」をクリックします。

The screenshot shows the user management interface for 'DEMO CUSTOMER'. The 'Authentication Information' tab is active. Under the 'Applications' section, the 'Webex' application is listed with an 'SSO' link highlighted in a red box. The 'Authentication Sets' table below shows two sets: 'PW' and 'FIDO'.

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	Webex	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「Cisco Webex」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

The screenshot shows the 'SSO 設定情報' page with the following fields and values:

- SSOエンドポイント: `https://sv.dds-themis.com:10443/admtool/saml/` [Copy]
- SLOエンドポイント: `https://sv.dds-themis.com:10443/admtool/saml/` [Copy]
- メタデータ: `https://sv.dds-themis.com:10443/admtool/saml/` [Copy]
- X.509証明書: [表示] button

The X.509 Certificate field contains a large block of text starting with '-----BEGIN CERTIFICATE-----' and ending with '-----END CERTIFICATE-----'. A 'Copy' button is located at the bottom right of the certificate text area.

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、「Cisco Webex」のログイン 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