

「BioPass FIDO2」を使用したマガタマサービスの WebAuthn

株式会社ディー・ディー・エス
飛天ジャパン株式会社

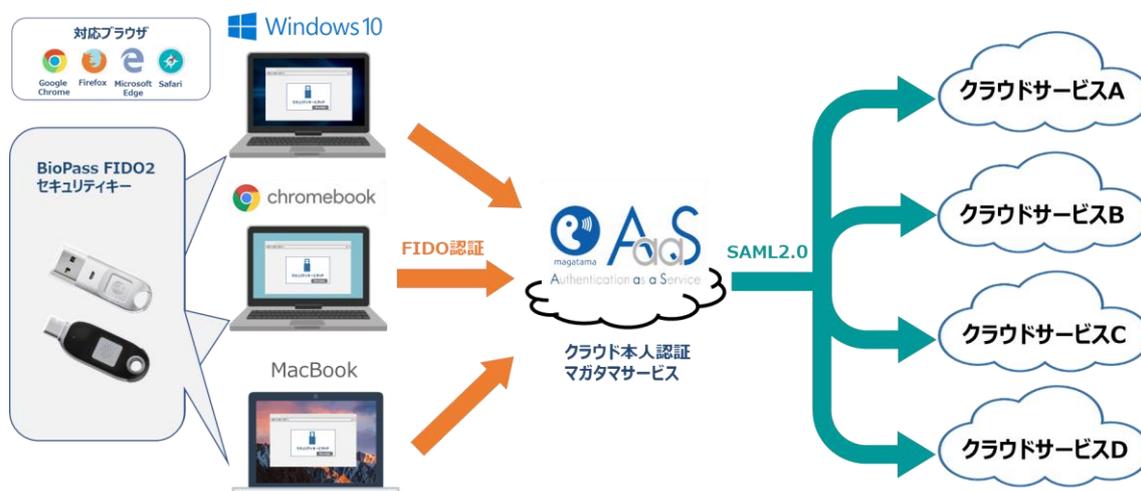
1. 「BioPass FIDO2」を使用したマガタマサービスの FIDO 認証について

次世代オンライン認証規格 FIDO (Fast IDentity Online) に対応した「BioPass FIDO2」セキュリティキーを、同じく FIDO に対応したクラウド本人認証「マガタマサービス」の認証デバイスとして使用できます。これにより、ユーザーは場所やプラットフォームによる制約を受けることなく、複数のクラウドサービスへのログオンに、生体情報と所持の二要素によるパスワードレス認証を実現します。

2. 「BioPass FIDO2」について

「BioPass FIDO2」は、生体情報と所持の二要素認証を実現する次世代認証デバイスです。生体情報はデバイス内にセキュアに格納され、流出することはありません。この指紋認証デバイス「BioPass FIDO2」と FIDO に対応したサービスで、シンプルで強固なパスワードレス認証を実現します。

3. 使用イメージ



[クラウドサービスへのログオン]



マガタマサービスと連携したクラウドサービスへのログオンについて、マガタマサービスの WebAuthn の認証時に「BioPass FIDO2」セキュリティキーを用いた指紋認証を利用することができます。

[Chrome OS 端末へのログオン]



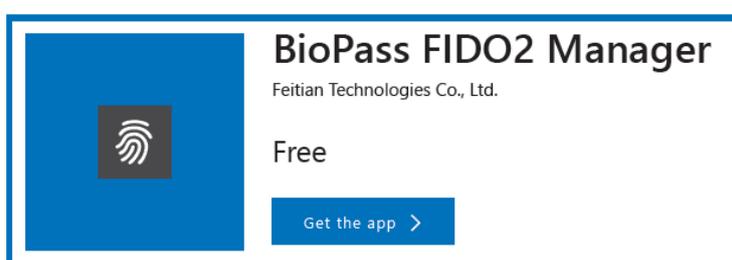
G Suiteとマガタマサービスを連携し、Google Chrome のデバイス制御設定を行うことで WebAuthn の認証時に「BioPass FIDO2」セキュリティキーを用いた指紋認証を利用して Chrome OS 端末にログオンを行うことができます。

4. BioPass FIDO2 への指紋登録

■ アプリのダウンロード

BioPass FIDO2 セキュリティキーを初めて使用する場合、BioPassFIDO2 マネージャーアプリを介して指紋登録をする必要があります。アプリは Microsoft ストアまたは弊社 Web サイトからダウンロードできます。

Microsoft store (英語版) : <https://www.microsoft.com/store/productId/9P2ZJPWK3PXW>



飛天ジャパン Web サイト (日本語版) : <https://ftsafte.co.jp/products/fido2/>

指紋登録アプリ	BioPass FIDO2 Manager (for Windows)	BioPass FIDO2 Manager (for Mac)	BioPass FIDO2 Manager (for Linux)
---------	---	---	---

ご注意 :

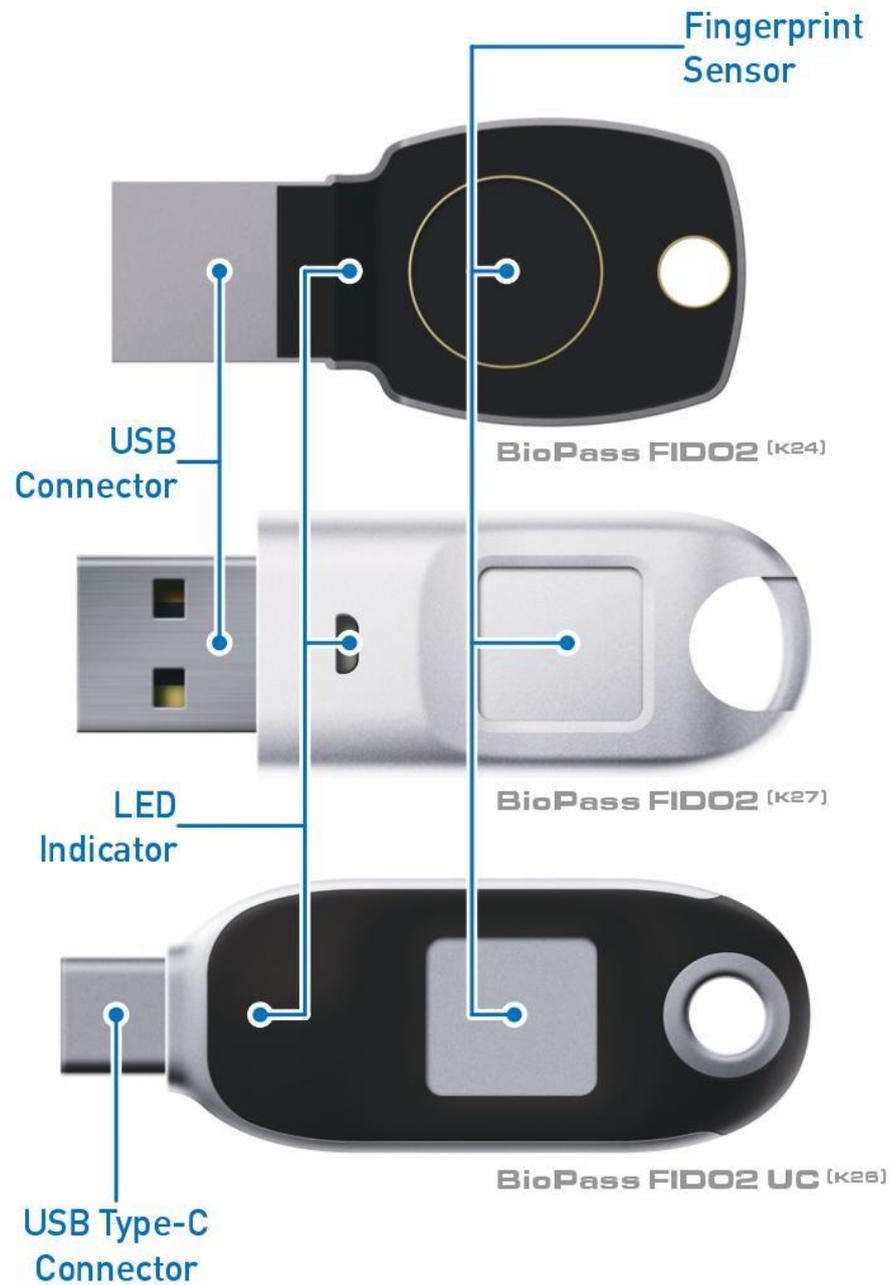
セキュリティ上の理由から、指紋確認を 15 回あるいは PIN 確認を 8 回連続で失敗した場合、セキュリティキーはブロックされます。

PIN が設定されていない場合は、指紋確認よりブロックされたデバイスをリセットするとブロックを解除できます (保存されているデータはすべて失われます)。

PIN が設定されている場合は、指紋確認よりブロックされたデバイスを PIN 入力でブロックを解除できます (保存されているデータに影響がありません)。

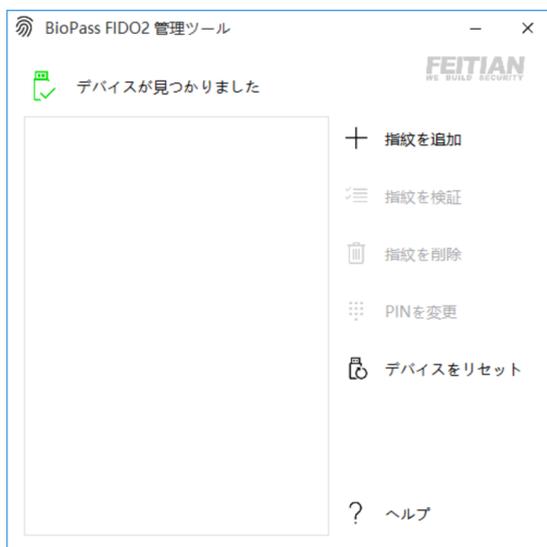
PIN が設定されている場合でもブロックされたデバイスをリセットするとブロックを解除できますが、保存されているデータはすべて失われます (一度リセットするとセキュリティキーに保管されたあなたの認証情報を含むすべてのデータが削除されます)。

Diagram



■ 指紋の登録

① BioPass FIDO2 マネージャーアプリを起動し、BioPass FIDO2 セキュリティキーを差し込むと、次のウィンドウが表示されます。



② 「指紋を追加」をクリックしてください。セキュリティキーを初めて利用する場合、またはリセット後の場合、「PIN+指紋」で利用するか、あるいは「指紋のみ」で利用するかを選択するため、下記のウィンドウが表示されます。



ご注意：

1つのオプションを選択したら、デバイスをリセットしない限り別のオプションに変更することはできません。

「PIN+指紋」を選択した場合、新しい PIN を設定するように通知されます。PIN に含めることができるのは、数字、文字および記号です。

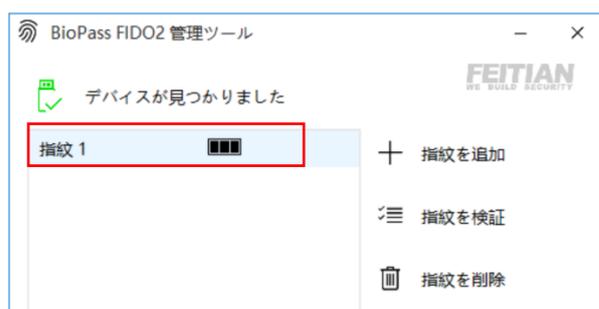
PIN には少なくとも 4 文字使用する必要があり、最大 63 文字までになります。



③下記の指示に従い、指紋登録をします。



④正常に登録されると、指紋がメインウィンドウに表示されます。

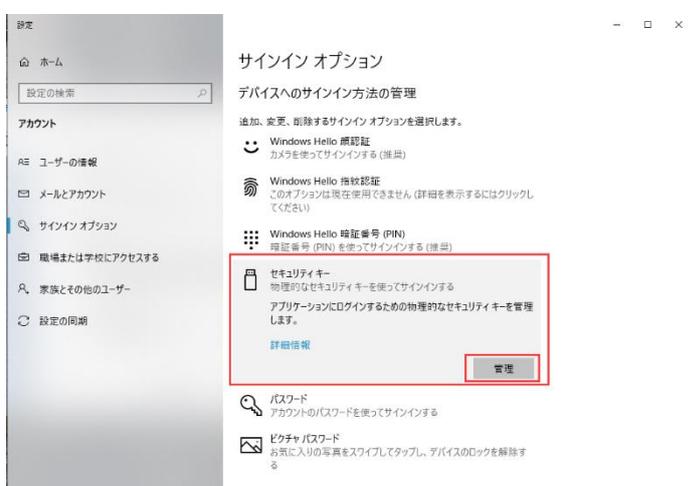


■ Windows10 1903 標準機能での指紋登録

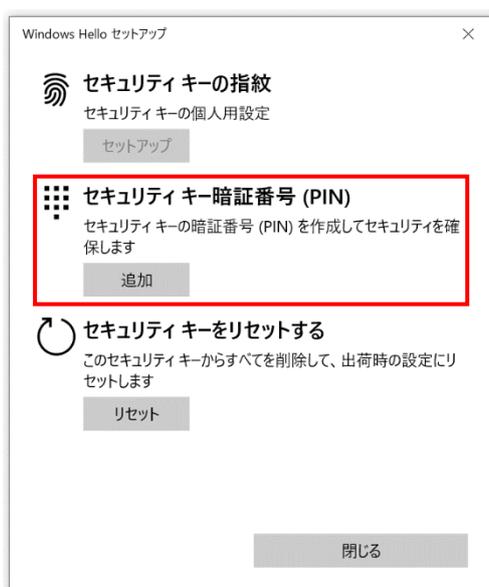
BioPass FIDO2 は Windows 10 バージョン 1903 より備えている「セキュリティキー」に対応しています。「セキュリティキー」にて BioPass FIDO2 を用いて管理することができます。

■ 指紋の登録

- ① Windows 設定画面サインオプションより「セキュリティキー」をクリックした後、「管理」をクリックしてください。

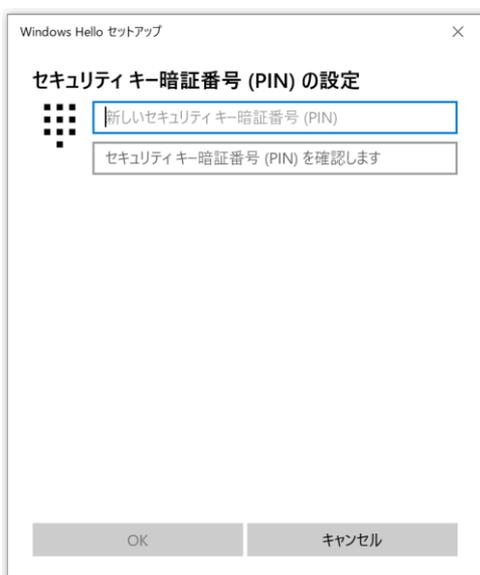


- ② BioPass FIDO2 セキュリティキーを差し込みデバイスをタッチすると、次のウィンドウが表示されます。セキュリティキー暗証番号 (PIN) の「追加」をクリックしてください。

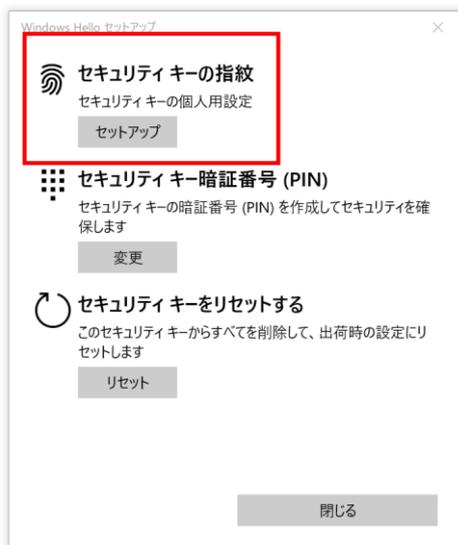


③ PIN を設定し、「OK」をクリックしてください。

※セキュリティキーを初めて利用する場合、PIN の登録は必須です。



④ PIN の登録が完了すると、セキュリティキーの指紋「セットアップ」を選択できますので、クリックしてください。



- ⑤ 先ほど登録した PIN を入力してください。



- ⑥ 下記の指示に従い、指紋登録をします。



⑦ こちらで登録は完了です。



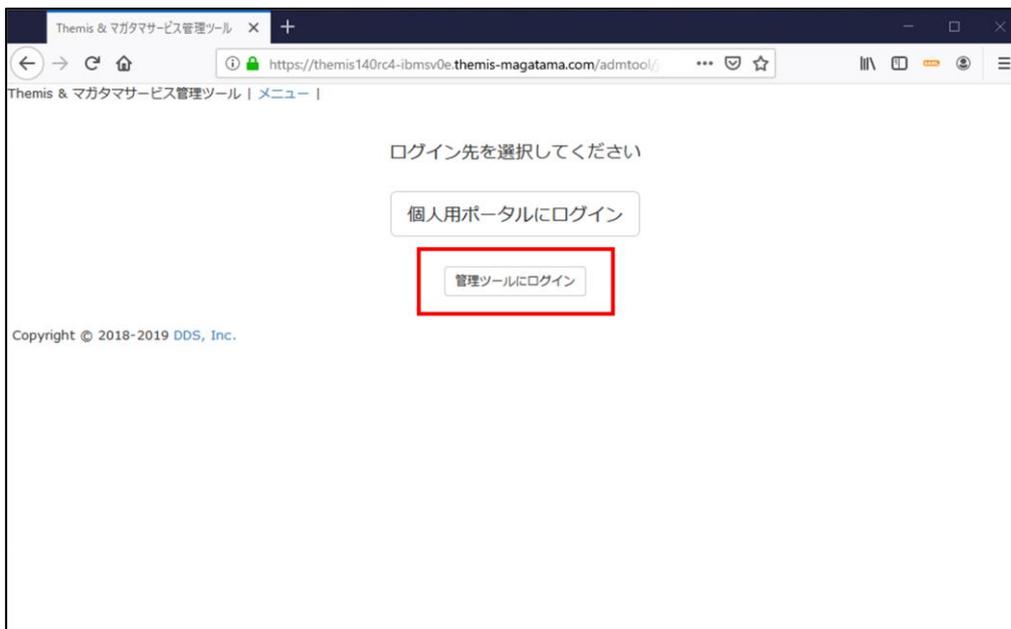
詳細情報について、後段の Microsoft 公式ホームページを参照してください。

<https://support.microsoft.com/ja-jp/help/4463210/windows-10-sign-in-microsoft-account-windows-hello-security-key>

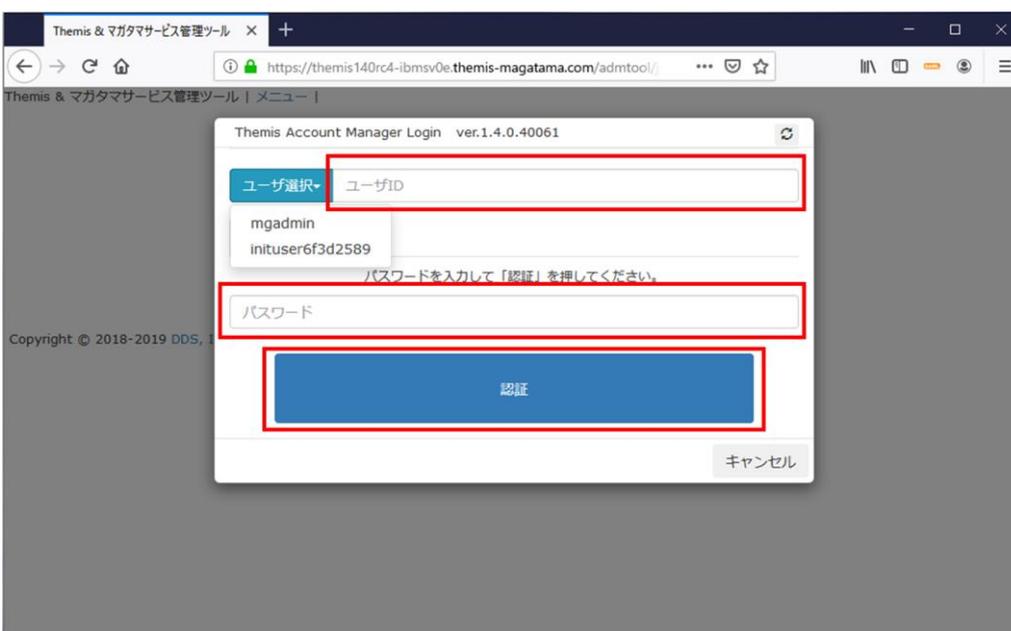
5. マガタマサービスへの BioPass FIDO2 セキュリティキーの登録

■ 認証セット WebAuthn (FIDO2) の有効化 (管理者の場合)

- ① マガタマサービス管理ツール URL へアクセスし、「管理ツールにログイン」をクリックします。



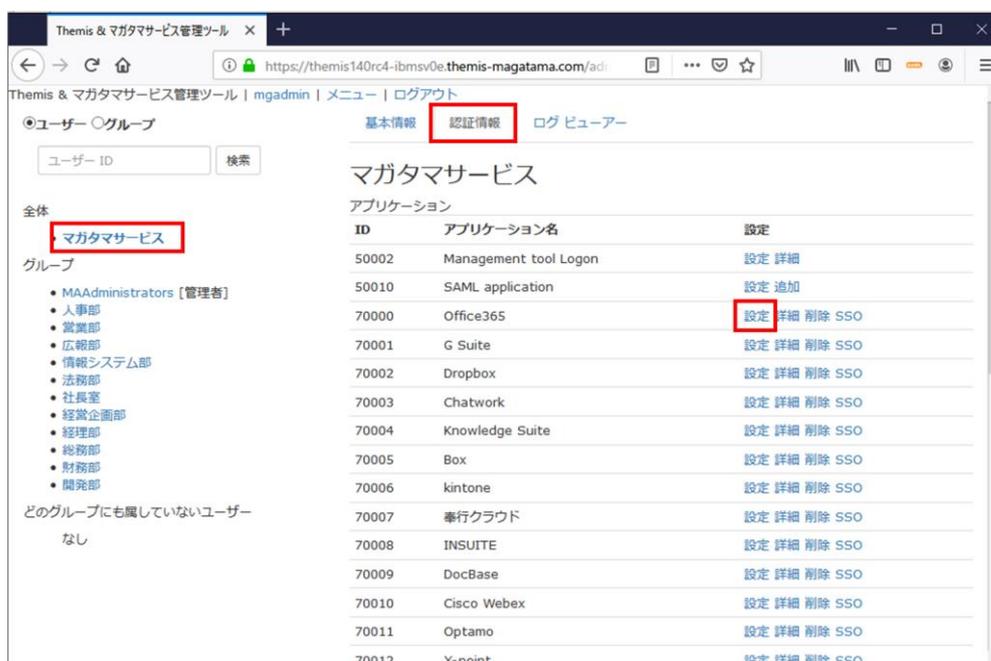
- ② 管理者の ID とパスワードを入力し、「認証」ボタンをクリックします。



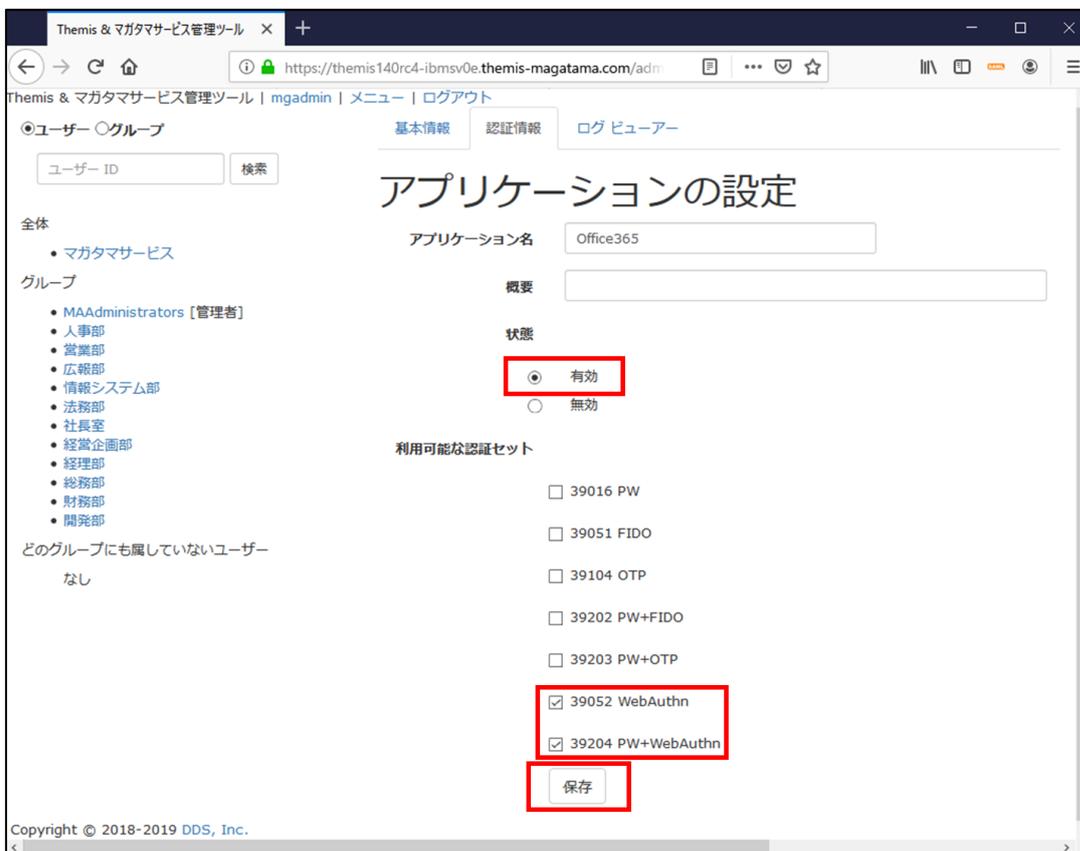
- ③ ログインに成功すると以下の画面が表示されます。



- ④ 左ペインの「全体」に表示される本テナント名を選択した状態で「認証情報」タブをクリックします。表示されているアプリケーション一覧から WebAuthn (FIDO2) の認証を使いたいアプリケーションの「設定」をクリックします。



- ⑤ アプリケーションの「状態」の「有効」を選択し、「利用可能な認証セット」について WebAuthn を含む認証要素にチェックを入れて、「保存」ボタンをクリックします。

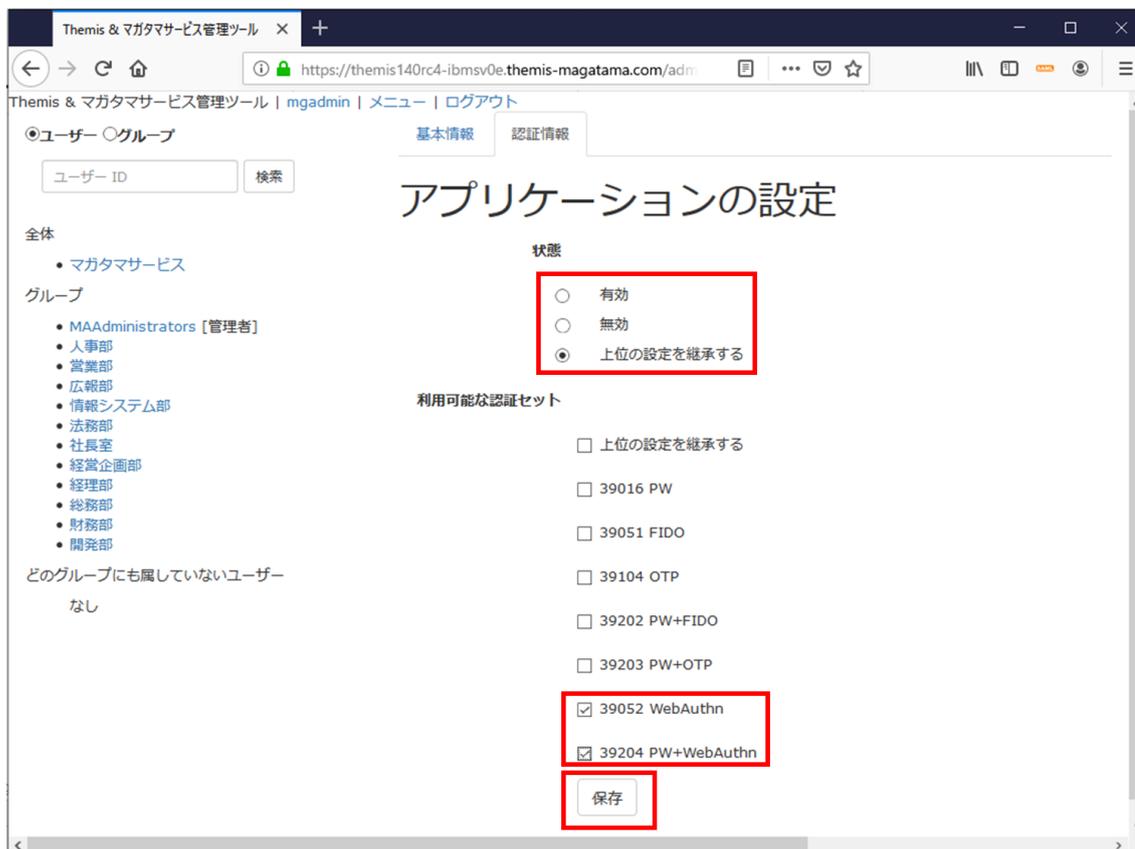


- ⑥ グループ毎に認証要素の設定を行いたい場合は、以下の設定を行います。
左ペインで登録を行いたいグループ名を選択した状態で「認証情報」タブをクリックします。表示されているアプリケーション一覧から WebAuthn (FIDO2) の認証を使いたいアプリケーションの「設定」をクリックします。

The screenshot shows the 'Themis & Magatama Service Management Tool' interface. The left sidebar shows a tree view of groups, with '情報システム部' (Information Systems Department) selected and highlighted with a red box. The main content area is titled '情報システム部' and shows a table of applications. The '認証情報' (Authentication Information) tab is selected and highlighted with a red box. The table lists various applications with their IDs and names, and a '設定' (Settings) link for each. The '設定' link for the 'Office365' application (ID 70000) is highlighted with a red box.

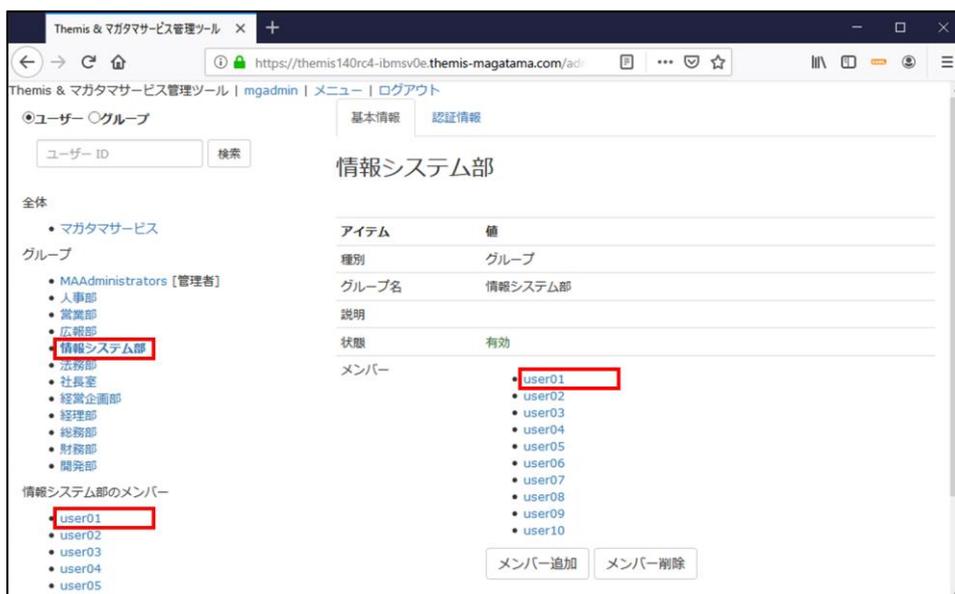
ID	アプリケーション名	設定
50002	Management tool Logon	設定 詳細
50010	SAML application	設定
70000	Office365	設定
70001	G Suite	設定
70002	Dropbox	設定
70003	Chatwork	設定
70004	Knowledge Suite	設定
70005	Box	設定
70006	kintone	設定
70007	奉行クラウド	設定
70008	INSUITE	設定
70009	DocBase	設定
70010	Cisco Webex	設定
70011	Optamo	設定

- ⑦ アプリケーションの「状態」を選択し、「利用可能な認証セット」について WebAuthn を含む認証要素にチェックを入れて、「保存」ボタンをクリックします。

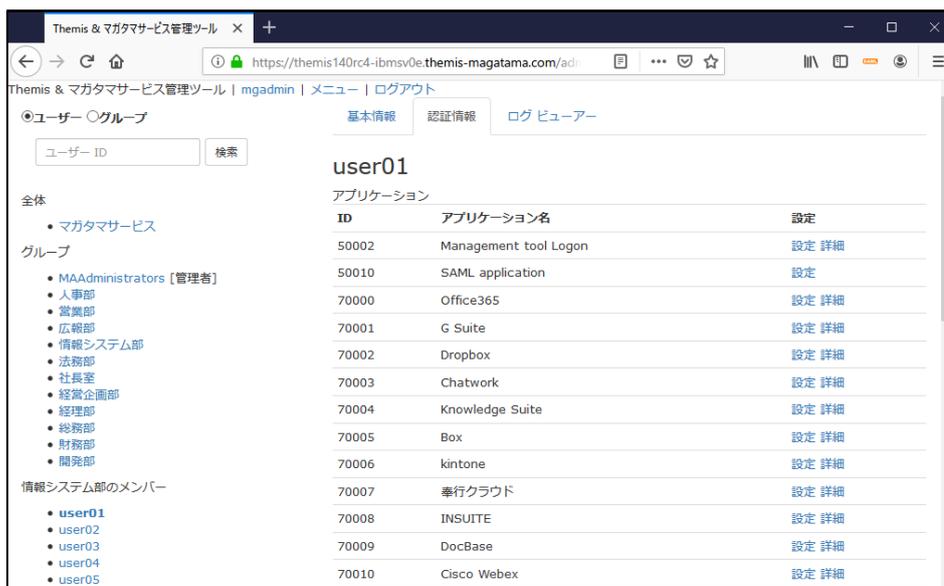


■ 認証要素 WebAuthn (FIDO2) の登録

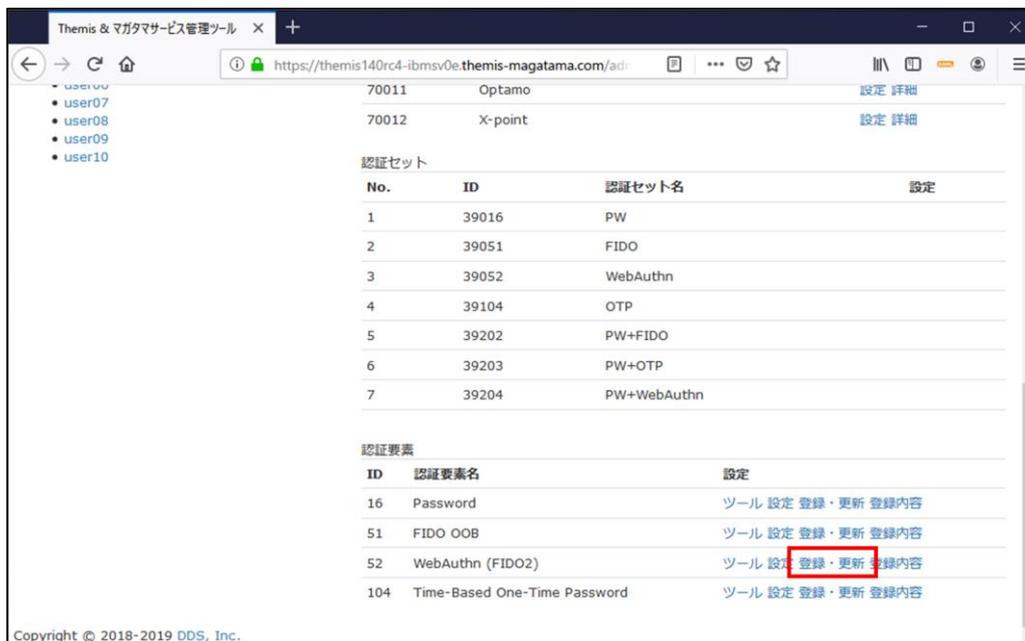
- ① 管理ツールの左のペインから WebAuthn (FIDO2) の登録を行うユーザーが所属するグループをクリックします。その後、左のペインに表示されるユーザーリストまたは基本ユーザーに表示されるユーザーリストから WebAuthn (FIDO2) の登録を行うユーザーをクリックします。



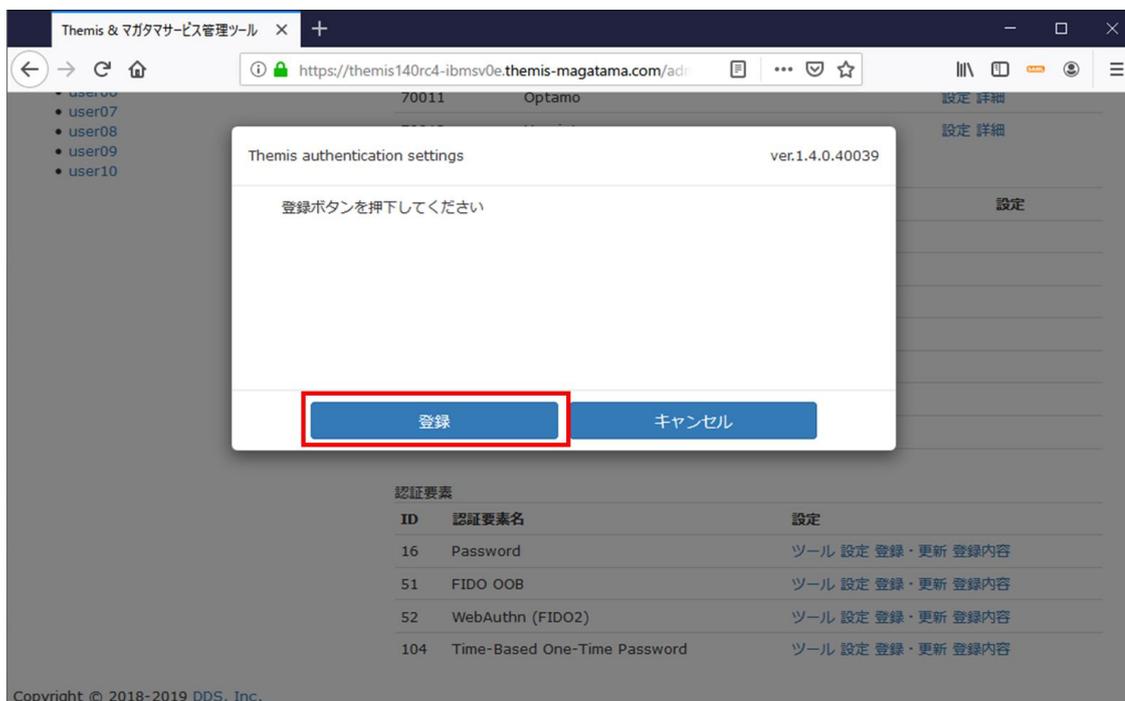
- ② 「認証情報」タブをクリックします。下にスクロールします。



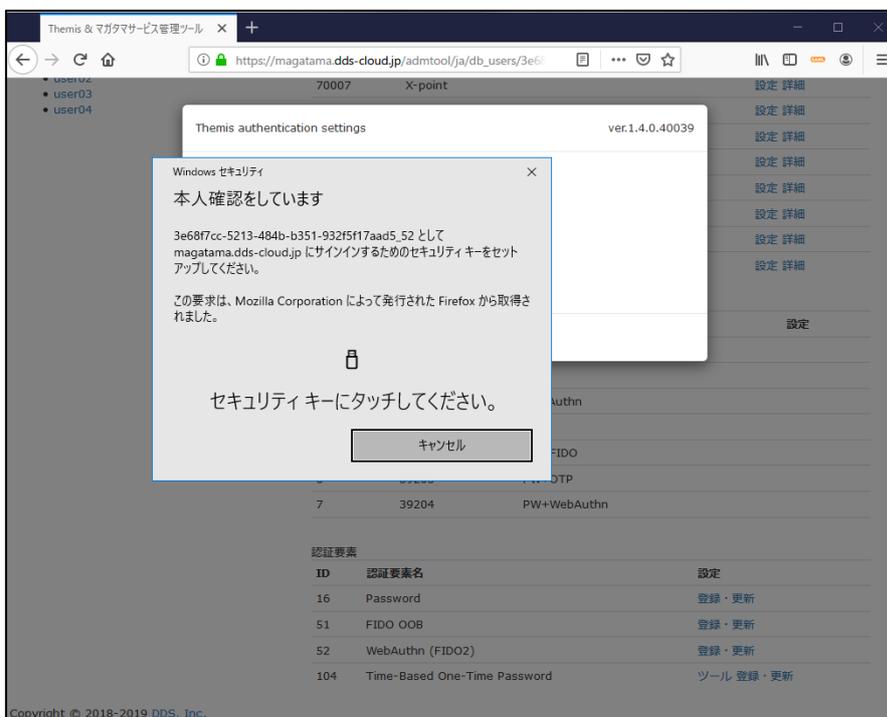
- ③ 「認証要素」リストの「52 WebAuthn (FIDO2)」の「登録・更新」をクリックします。



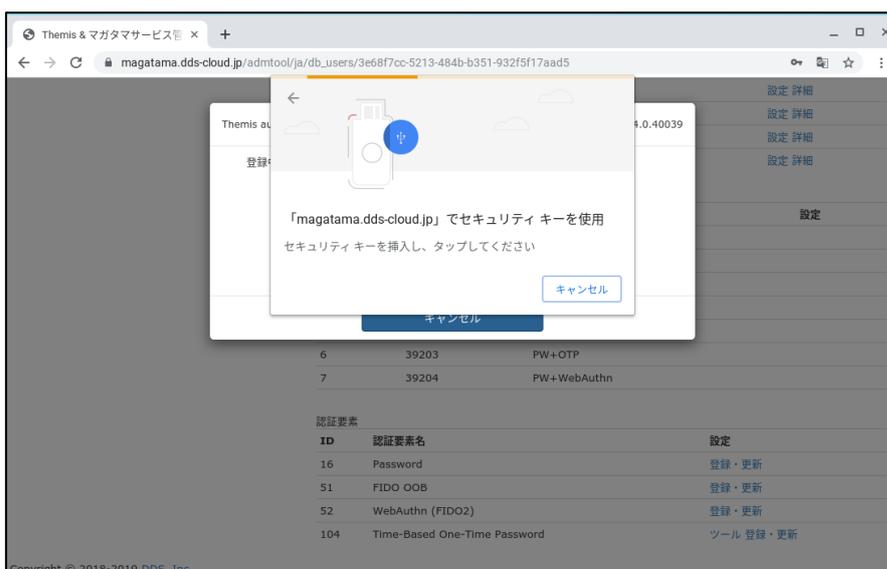
- ④ 「登録」ボタンをクリックします。



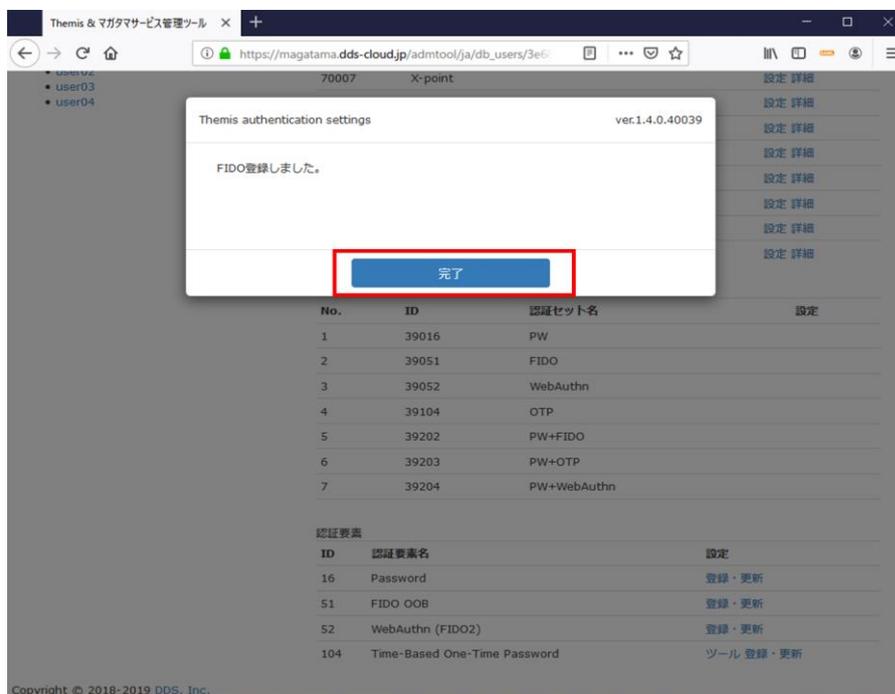
- ⑤ 「BioPass FIDO2」セキュリティキーを PC 端末に挿入し、表示されたメッセージに従い、セキュリティキーにタッチします。



[Google Chrome(Windows Hello を使用しない)の場合、以下のように表示されます。]



⑥ 「完了」ボタンをクリックして登録が完了となります。



■その他

その他ご不明点などございましたら、下記までお問合せください。

「マガタマサービス」について：bio_customer@dds.co.jp ディー・ディー・エスサポート

「Bio Pass FIDO2」について：support@ftsafeco.jp 飛天ジャパン技術サポート

以上

※本書に記載されているロゴ、会社名、製品・サービス名は、各社の登録商標または商標です。

※本書に掲載されている内容、製品・サービスの価格、仕様、お問い合わせ先、その他の情報は、発表時点の情報です。その後予告なしに変更となる場合があります。