eSecu FIDO ボタンキー
FD200/202/203 ユーザーマニュアル
(V2.2)

Excelsecu Data Technology Co., Ltd.

ACOT Electronics Inc.

株式会社エクセルセクデータテクノロジーの機密情報

本マニュアル、いかなる性質の保証を行うものではありません。すべての製品および関連文書に開示されている資料は、正式に締結されたプログラム製品のライセンスまたは機器の購入またはリースに関する契約の条件に従ってのみ提供されます。

このマニュアルに記載されている製品に関して、ExcelsecuTechnology が行う唯一の保証は、あるとすれば、当該ライセンス、または契約書に記載されている物のみです。

Excelsecu テクノロジーは、お客様が本情報またはソフトウェアを使用した結果として生じる直接的、間接的、特別または結果的な損害を含む金銭的またはその他の責任を受け入れることができません。

この情報および/またはソフトウェア資料の使用が、使用されている管轄区の規則および規制に準拠していることを確認するように注意してください。無断転載を禁じます。

目次

1. マニュアル

名前

eSecu FIDO ボタンキーは、ExcelSecu 社では、eSecu FIDO2/FIDO・U2F セキュリティキー FD200, FD202, FD203 と呼ばれています。ACOT 社では感嘆のため、FIDO ボタンキーと呼び、ExcelSecu FIDO2セキュリティキー FD210、FD213 と合わせて FIDO キーと呼んでいます。FIDO ボタンキーと FIDO2 セキュリティキーの違いは、前者はスイッチ、後者は指紋認証システムが本人確認のキー内認証である点です。

FIDO ボタンキーと FIDO2 セキュリティキー
ボタンタッチは、人間の存在を示すだけで、本人確認ができません。そのため、4桁、6桁、8桁などの数字の暗証番号 PIN と併用されています。つまり、FIDO ボタンキーの PIN とボタンタッチと、FIDO2 セキュリティキーの指紋認証が対応しています。また、それらの認証処理は、FIDO キー内部で行われます。そのため、その点を除くと登録や認証操作では両者に大きな差はありません。

有線・無線
また、FIDO キーはコンピュータの周辺機器として、コンピュータに接続して利用します。FD200 や FD210 は、USB TypeA のインタフェースで、ディスクトップパソコンに接続します。スマートフォンには、NFC(近距離通信)や BLE(BlueTooth 低エネルギー)無線で接続します。NFC は、タッチするほど近くでのみ利用可能ですが、BLE は何メートルも離れていても通信可能です。

2. 製品概要

eSecu FD200 は、FIDO2 標準と FIDO・U2F 標準および HOTP アルゴリズムをサポートするハードウェア認証器です。二要素認証、多要素認証として、またはパスワードなし認証の要素、および OTP デバイスとして、ログイン保護が必要なネットワークアカウントへの安全なログインに利用できます。

- FIDO・U2F 対応のサービスとアプリケーションに対して、2段階認証の第2段階の認証として利用できます。1段階認証にはパスワードや暗証番号 PIN が使われます。Google Chrome ブラウザや Microsoft Edge ブラウザからのクラウドアカウントへの安全なログ

インに利用できます。また、OTP デバイスとして利用も可能です。

- ❑ FIDO2にも対応が可能で、Microsoft Edge ブラウザからクラウドアカウントへのパスワードなしログイン認証や Windows パスワードなしログインにも利用できます。

3. 製品写真

ボタンの点灯状態は次のとおりです。

- 白色光の点灯：FD200 キーをコンピュータの USB ポートに挿入され、動作していること示しています。

- 白色光の点滅：FD200 キーは、認証要求の受信時に白色光が点滅します。ボタンを押してサインインを完了します。

4. FD200 キーの基本操作

4.1 登録(初回のみ)

1) ユーザー名とパスワードを入力して、 FIDO2/FIDO・U2F をサポートするアプリケーションにログインします。
2) FD200 キーを USB-A ポートに挿入します。
3) アカウントに FD200 キーを追加します。

4.2 サインイン(登録完了後)

1) ログインする Web サイトを開きます。
2) 通常のユーザー名とパスワードを入力します。
3) 登録済みの FD200キーをコンピューターに接続します。キーのボタンを押すだけで認証します。

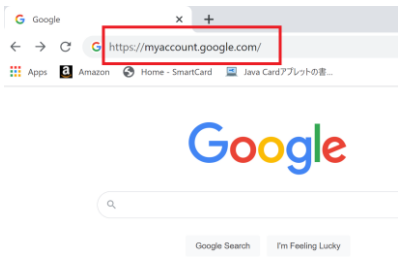
5. Google アカウントへの2段階認証ログイン

5.1 Google 登録

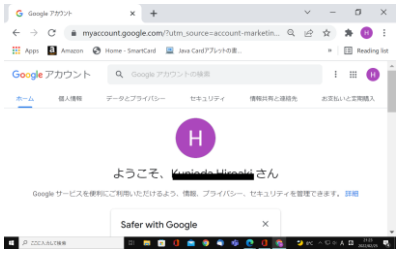
1) Web サイト https://www.google.com/に移動します。画面上の右上隅にある[ログイン]をクリックします。

2) アカウント名とパスワードを入力して、ログインします。

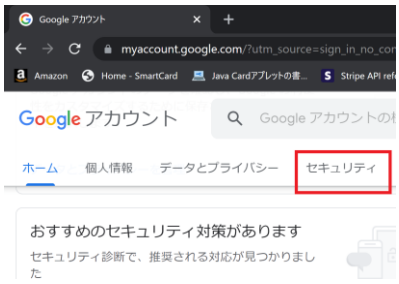
3) 正常にログインしたら、Google アカウント https://myaccount.google.com.へ移動します。



4) Google アカウントのセキュリティへ移動します。



5) Google アカウントのセキュリティへ移動します。



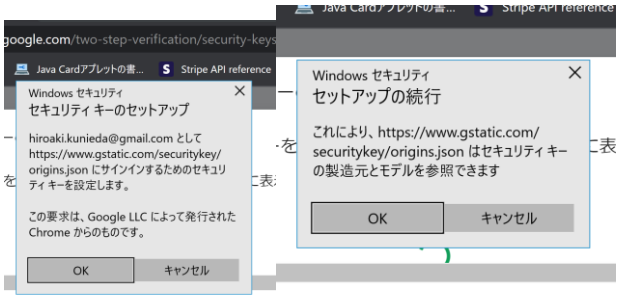
6) [セキュリティ]モードで、[2 段階認証プロセス]を選択します。

7) 再度確認のためのユーザー確認が求められます。

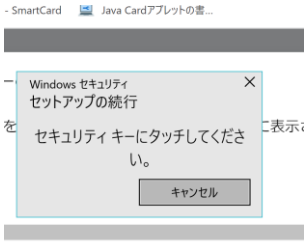
8) 利用できる 2 つ目の手順として [セキュリティキー]をクリックします。

9) 既存のセキュリティ キーが表示されますので、[セキュリティキーの追加]をクリックします。

10) セキュリティキーのセットアップ情報のポップアップが現れます。FD200キーをコンピュータの USB 端子に挿入して、OK をクリックします。



11) FD200 キーの白色光が点滅しているときに、FD200キーのボタンを押します。



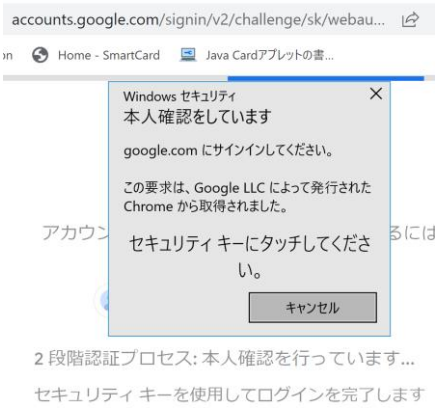
12) FD200 キーの適当な名前を付け、[完了]をクリックして終了します。

13) 登録が完了したメッセージが表示されます。

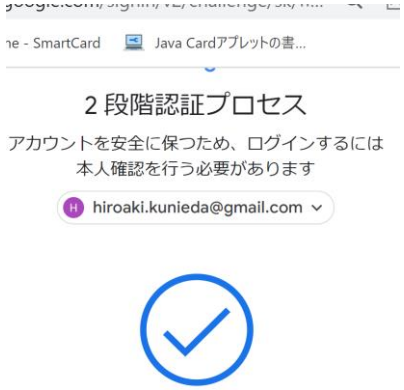
5.2　Google サインイン

1)　次の Web サイトにログインします：https://www.google.com/そして右上隅にある[ログイン]をクリックします。アカウント名とパスワードを入力し、「次へ」をクリックします。

2)　.FIDO2 セキュリティキーを USB ポートに挿入するように求められます。キーの白色光が点滅しているときに、FIDO2 セキュリティキーのボタンを押します。



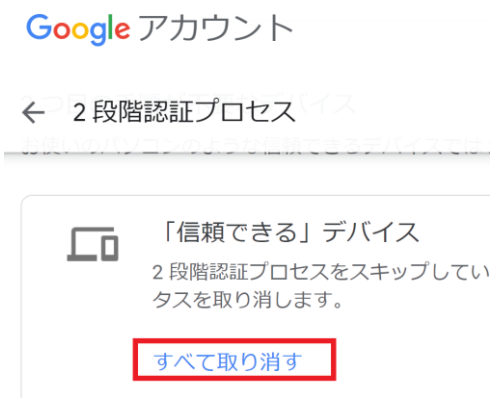
3)　[次へ]をクリックしてログインします。



注：

1) **デフォルトでは、「このコンピューターで再度質問しない」がオンになっています。チェックボックスをオンにすると、次のログインで 2 段階の確認がスキップされ、ユーザー名とパスワードを使用して直接ログインします。**

2) **日常で使用している信頼できるデバイスでは、2 段階認証の第2段階の認証が省略されます。見た目はパスワード認証だけのように見えます。[Google アカウント/セキュリティ/2段階認証プロセス]の最後尾には、**「信頼できる」デバイス欄があります。下の **「すべて取り消す」をクリックして、信頼できるデバイスをクリアしますと、2段階目のスキップのない2段階認証を行います。**



6. Microsoft アカウントへのパスワードなしログイン

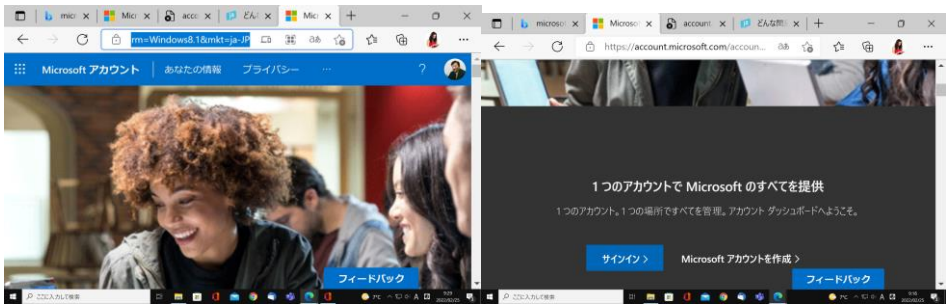
Microsoft Edge ブラウザと Windows10 オペレーティングシステム(システムバージョン 1809 以上)を使用する必要があります。
https://support.microsoft.com/ja-jp/windows/windows-hello-またはセキュリティ-キーで-microsoft-アカウントにサインインする-800a8c01-6b61-49f5-0660-c2159bea4d84

Microsoft アカウントは、事前に作成しておく必要があります。ここでは記述していません。そのアカウントにセキュリティキーを利用したパスワードなしログイン機能を追加する形になります。

6.1 Microsoft 登録

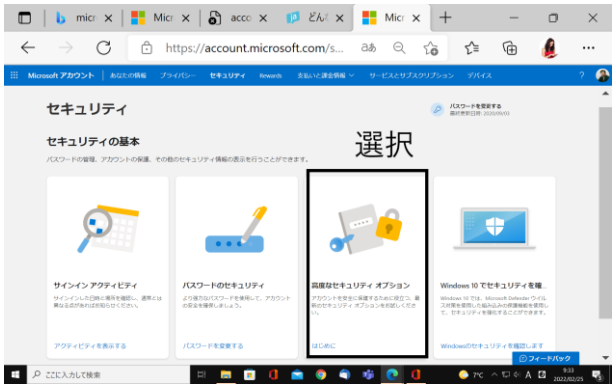
1) 既存の方法でサインインし、[マイ Microsoft アカウント]をクリックします。

https://account.microsoft.com/account/Account?ref=settings&Platform=Windows8.1&mkt=ja-JP



2) [セキュリティ]をクリックし、ポップアップ画面で「セキュリティ ダッシュボード」をクリックします。

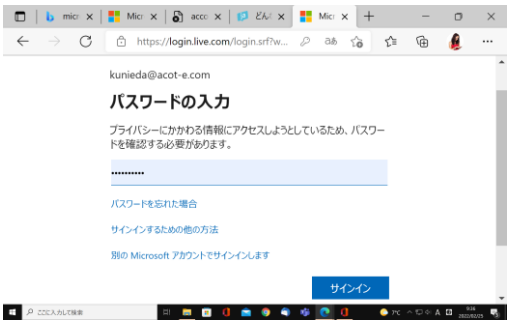
3) 「高度なセキュリティオプション」をクリックします。



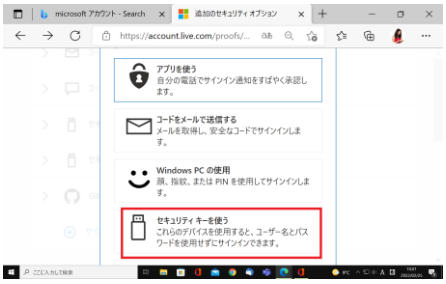
4) [サインインまたは確認の新しい方法を追加]をクリックします。 このとき、その下の設定が以下になっていることを確認してください。

- パスワードレスアカウント：オン
- 2段階認証：オフ

5) 本人確認を求められます。

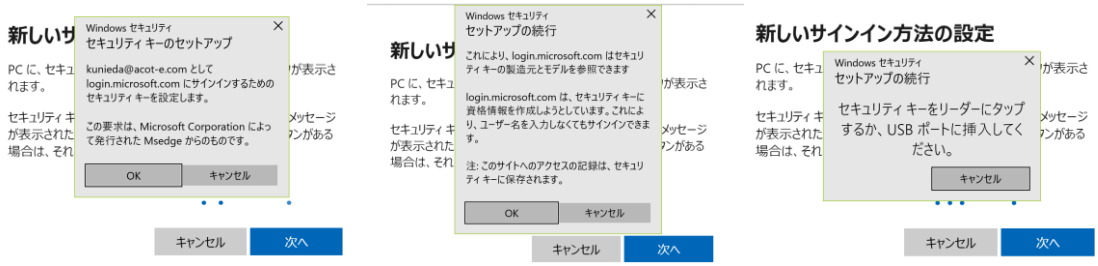


6) 認証に合格したら、[確認またはサインインのための追加の方法の選択]ページに入り、[セキュリティ キーを使う]をクリックします。

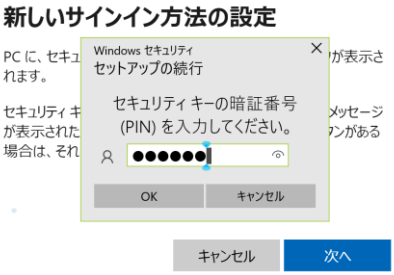


7) [セキュリティ キーの設定]に従って、FD200 キーを挿入します。 そして、次へをクリックします。

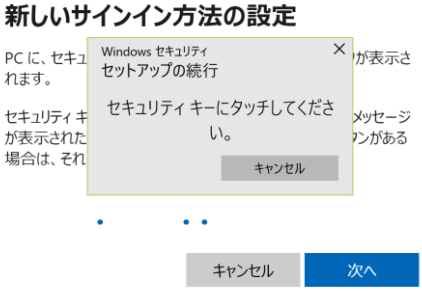
8) 以下のポップアップ画面で[セットアップの設定]の説明があり、次へをクリックします。



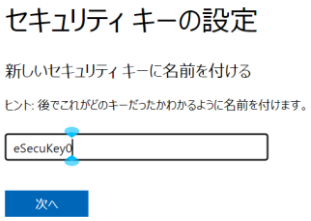
9) FD200 キーの暗証番号 PIN の入力が要求されます。PIN 入力の上、次へをクリックします。



10) プロンプトが表示されたら、FD200 キーのボタンを押します。



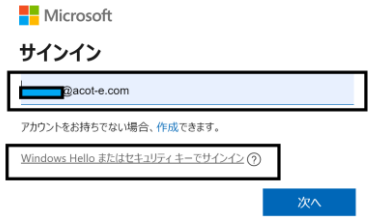
11) FD200 キーに名前を付けて、次へを押します。



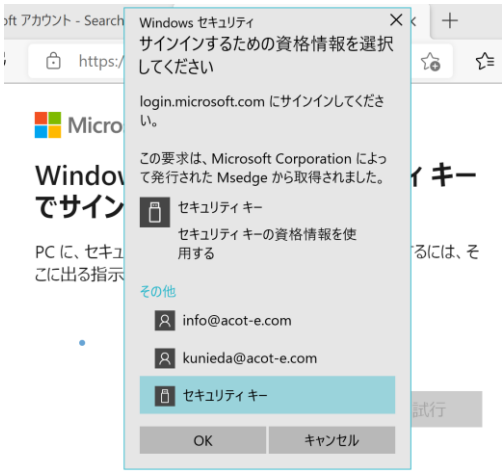
12) 登録が完了して、アカウントサイトに戻ります。

6.2 Microsoft サインイン

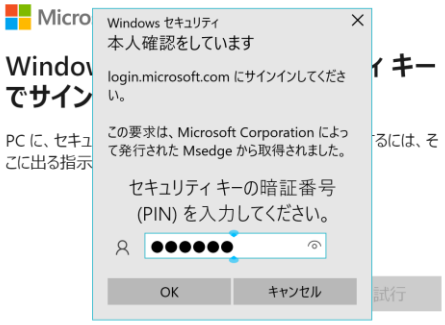
1) マイクロソフトアカウントの「サインイン」サイトに移動します。
アカウント名の入力し、「Windows Hello またはセキュリティキーでサインイン」をクリックします。



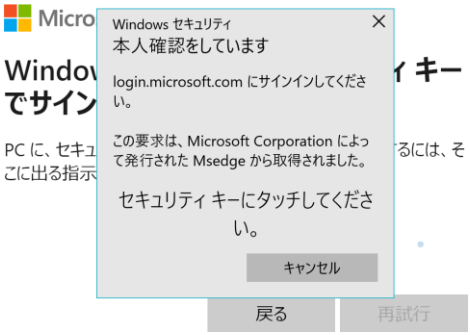
2) 「セキュリティキー」をクリックします。



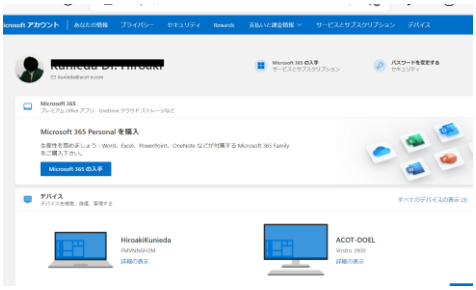
3) セキュリティキーの暗証番号 PIN を入力します。



4) プロンプトが表示されたら、FD200 キーを USB 端子に挿入します。更に、FD200 キーのボタンを押します。



5) 正常にサインインすると、アカウントへログイン完了します。



7. Windows へのサインイン

前提条件

- Windows 10 1903 バージョン以降の最新バージョン
- Azure Active Directory (Azure AD)の管理者
- Azure AD の会社アカウント
- デバイス設定用データの保存用 USB メモリ

A.管理者の設定作業

1. Azure の設定
2. プロビジョニングパッケージの作成
3. PC デバイスの設定

B.ユーザーの設定作業

1. 暗証番号 PIN
2. Azure への FIDO キーの登録

7.1 管理者の設定作業

7.1.1 Azure の設定

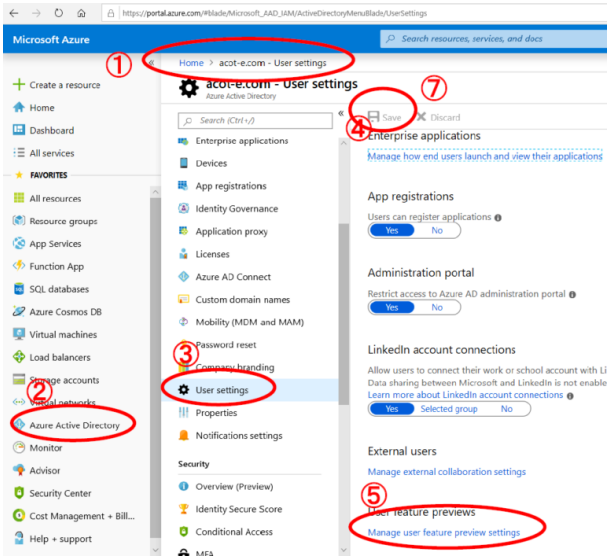
Azure の設定として、Windows と Azure AD に同時ログインするユーザーやグループと FIDO2 ログイン方法を設定します。Azure は、企業や学校などの Azure テナントと呼ばれる組織が利用するマイクロソフトのクラウドサービスです。これとは別に Office365 なども有名です。Azure ユーザーは、Azure AD アカウントまたは職場または学校アカウントと呼ばれるアカウントを持ちます。マイクロソフトと呼ばれる個人アカウントとは異なります。職場アカウントで Azure ログインにパスワードなし FIDO2 認証を利用するには、Azure の設定とキーの設定が必要です。ここでは Azure の設定を示しています。

1) 職場アカウントで Azure ポータルへサインインします。(①)その上で、Azure Active Directory (Azure AD)を選択し、その中でユーザー設定を選択します。ここの例では、acot-e.com は Azure AD の登録組織のドメインです。

1. **アプリ、管理者ポータル、LinkedIn アカウント、外部ユーザーなどのアクセス設定**
2. **User feature previews として、ユーザー特徴設定をクリック**
3. **変更したときは変更を保存**

を行います。

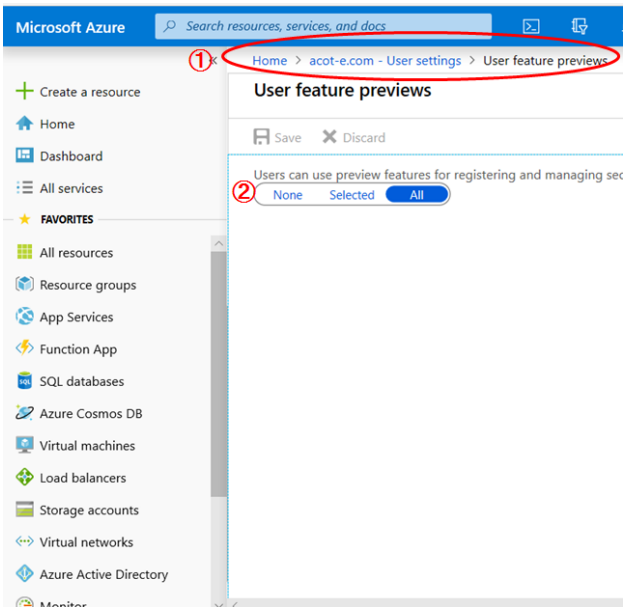
Azure > Azure AD> acot-e.com > ユーザー設定



2)上の続きとして

4. ユーザー特徴を利用に関する選択(クリックして次へ)

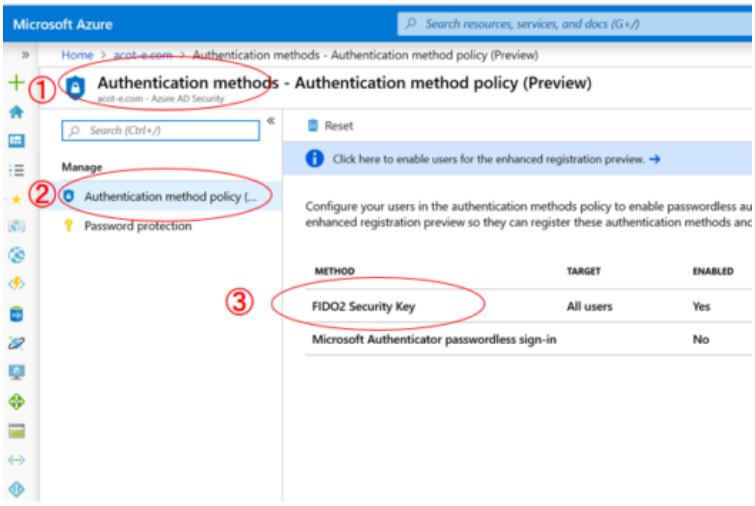
を行います。



3) 認証方法の設定

②認証方法として、③FIDO2 セキュリティキーを選択します。

Azure ポータル＞Azure AD ＞ セキュリティ ＞ 認証方法(①)



4)FIDO2 セキュリティキー

認証方法として FIDO2 セキュリティキーを利用を有効にします。対象とするユーザーをすべてに設定してください。

Azure ポータル＞Azure AD ＞ セキュリティ ＞ 認証方法 ＞FIDO2 セキュリティキー

5) 全般的なパラメータを設定します。

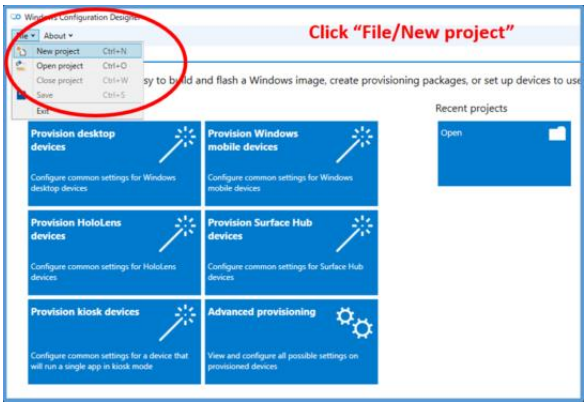
7.1.2 プロビジョニングパッケージの作成

マイクロソフトが無料で提供する専用プログラム(Windoes Configuration Designer)を使用します。クラウドからダウンロードしてみてください。このプログラムで、職場アカウントを PC デバイスに紐づけるプロビジョニングパッケージを作成して。外付けの USB メモリに保存します。プログラムは、マイクロソフトの"Microsoft Store"から入手できます。

https://docs.micro ＝ soft.com/jajp/windows/configuration/provisioning-packages/provisioning-create-package

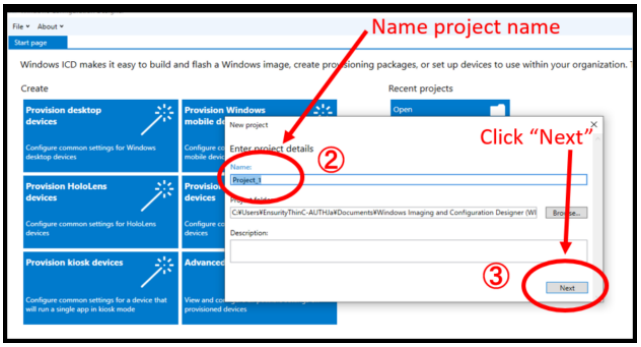
① File/New project をクリック

Windows Configuration Designer > File > New project



2)① File/New project をクリックします。

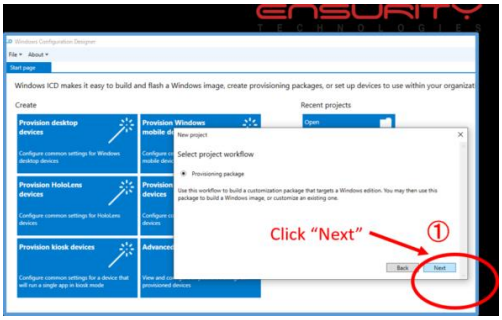
Windows Configuration Designer > File > New project



3)① セキュリティの設定(何も設定しないのも OK)

"Next"をクリック

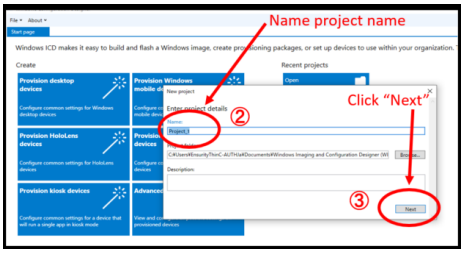
Windows Configuration Designer > File > New project > Next



4)② 設定対象のデバイスの選択

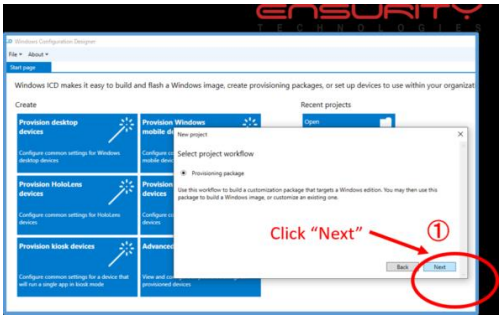
All Windows desktop editions を選択(重要: Runtime settings に UseSecurityKeyfor Signin の項がなくなる) ③ "Next をクリック

Windows Configuration Designer > File > New project > Next > Next

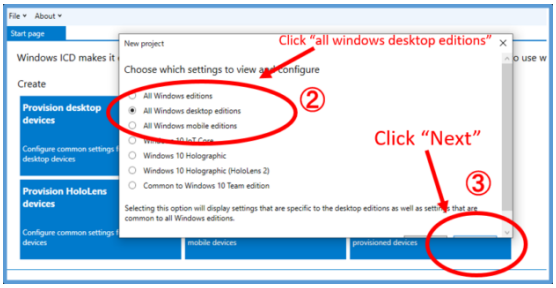


5)① セキュリティの設定(何も設定しないのも OK) "Next"をクリック

Windows Configuration Designer > File > New project > Next

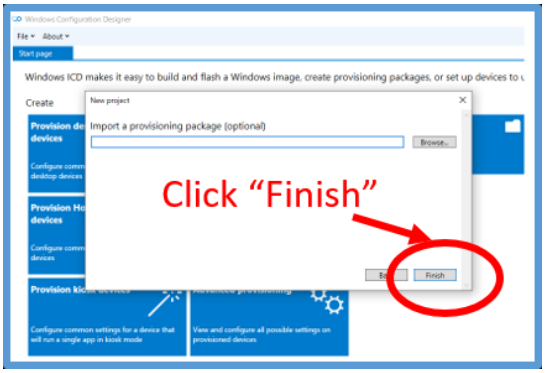


6)Windows Configuration Designer > File > New project >　Next > Next



7) 終了をクリック

Windows Configuration Designer > File > New project >　Next > Next > Next

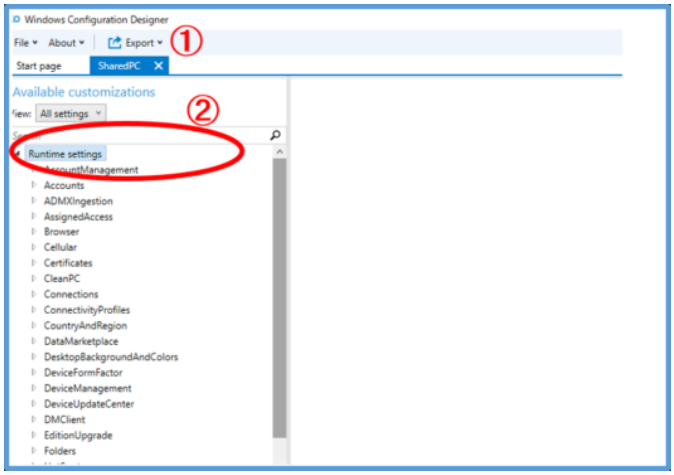


8)

① プロジェクト名(例えば SharedPC)を入力してください。

② "Runtime Settings"をクリック

Windows Configuration Designer > (project name) > Runtime settings



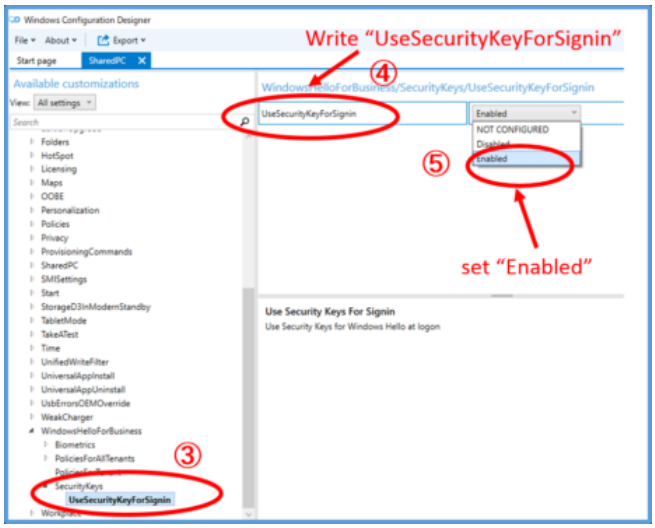
9)Windows Configuration Designer > (project name) > Runtime settings >

③ WindowsHelloForBusiness > UseSecurityKeyForSignin をクリック

④ "UseSecurityKeyForSignin"を記述して、"Enable"を選択

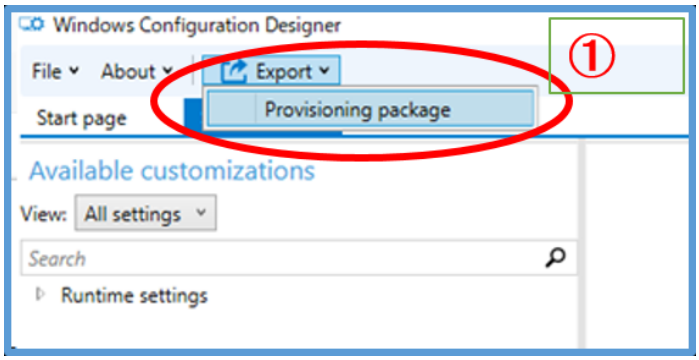
⑤ 設定データの生成

WindowsHelloForBusiness > UseSecurityKeyForSignin

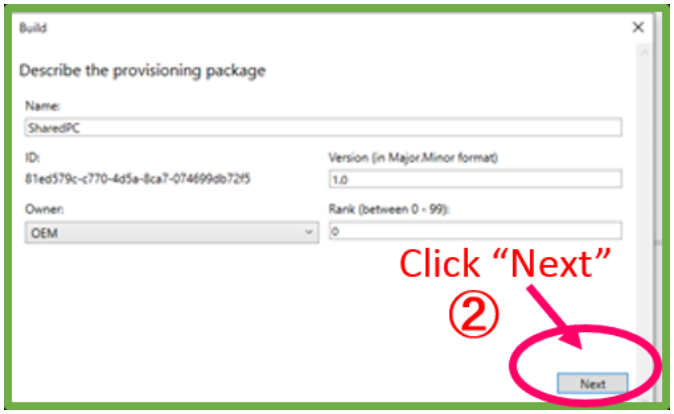


10)①Export/Provisioning Package をクリック(5つのウインドウへ)

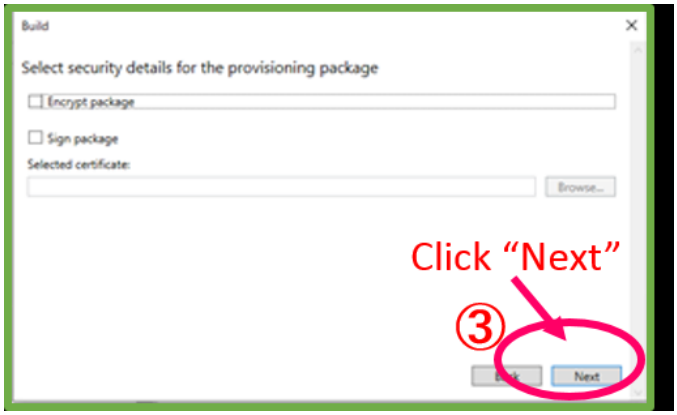
Windows Configuration Designer > Export > Provisioning Package



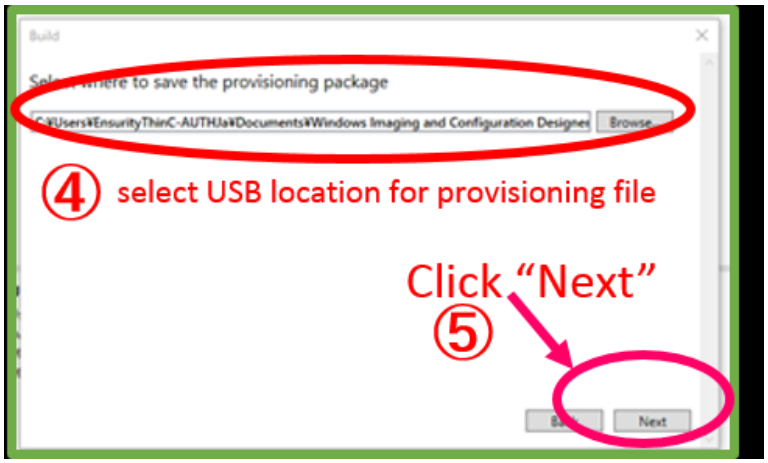
11)② 設定データ(Provisioning package)の記述



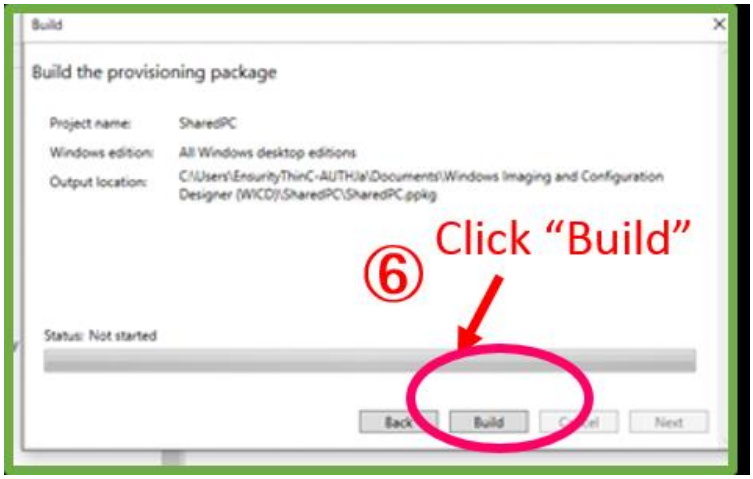
12) データ保護の選定



13)④ 設定データの保存場所(USBメモリへ)



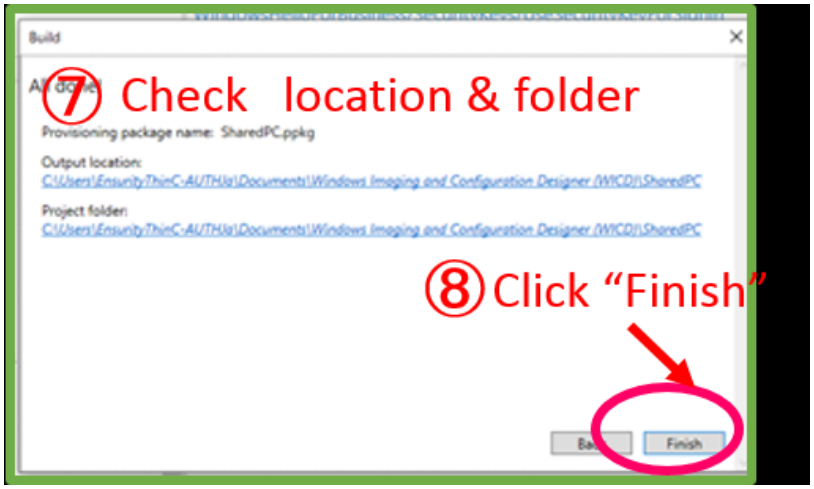
14⑤ 設定データの生成



15)⑦ 保存場所とプロジェクトのフォルダーを確認して、"終了"をクリック

⑧ 接続したUSBメモリに設定データファイルが 2 つ生成されています。(と)

このファイルを利用して複数のデバイスにFIDO2認証を設定できます。



7.1.3 PC デバイスの設定

PC デバイスごとに共通のプロビジョニングパッケージを USB メモリから読み込ませ、職場アカウントの設定を行います

新たな職場アカウントを Windows のローカルアカウントに設定することはユーザープロビジョニングと呼ばれています。

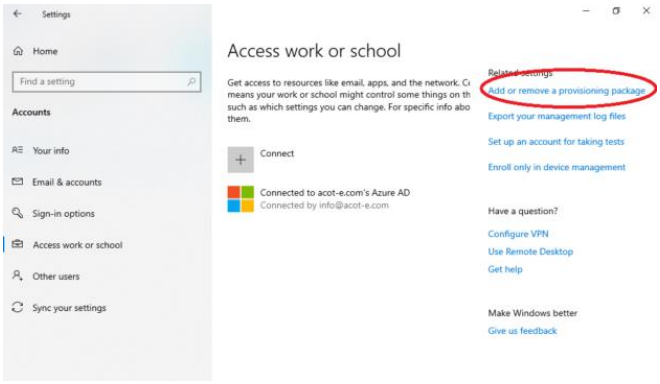
従来のディスクイメージによるクローニング展開は、PC 購入時にプリインストールされている OS や各種アプリケーションを全て消去し、新規に OS や各種アプリケーションをインストールし直して作成したディスクイメージをもとに、複数の PC にクローニング展開を行う方法でした。

ここで使用するプロビジョニングパッケージは、プリインストールされている OS やアプリケーションを利用し、その上で必要な設定だけを加えることで業務用 PC として利用できます。プロビジョニングパッケージの ppkg ファイルをダブルクリックするだけで、ホスト名やアカウント作成を始めとする初期設定が実施できます。特にここでは、PC デバイスを Active Directory へ登録したり、Azure AD に登録します。また、ローカル管理者を作成することもできます

7.1.3.1 プロビジョニング パッケージの適用

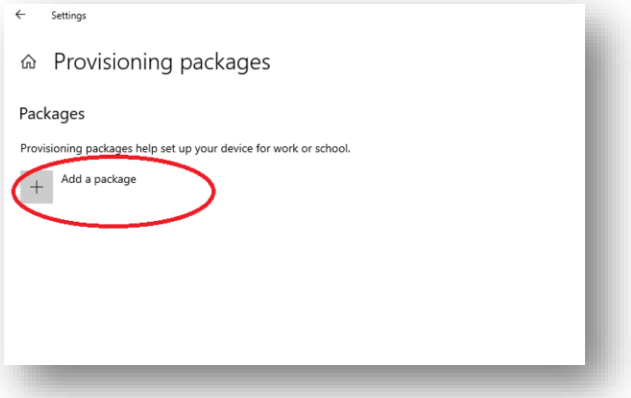
1)① Windows 左下の Windows 10 ロゴから設定を選び、さらにアカウント>会社または学校アカウントに入ってください。右の関連設定項目の"プロビジョニングパッケージを追加または削除する"をクリックします。

> 設定 > アカウント > 職場にアクセス



2)② 設定データの画面が現れますので、データ(package)を追加をクリック。

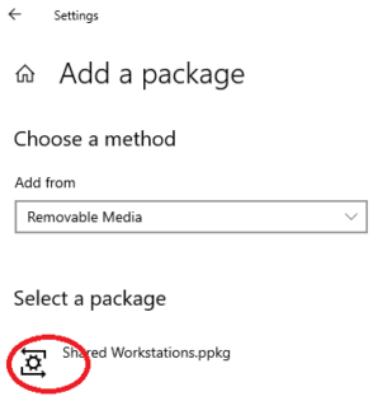
> 設定 > アカウント > 職場にアクセス



3) USB メモリの接続

③ 設定データを保存した USB メモリを USB 端子に接続すると、画面にデータファイル名が表示されます。クリック

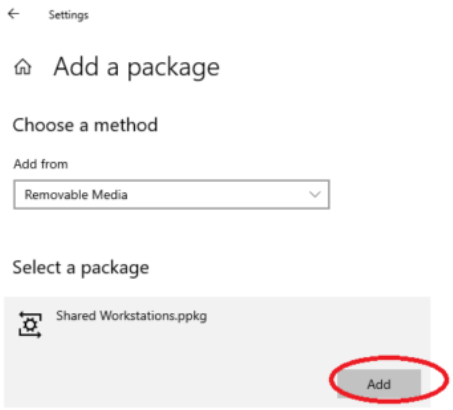
> 設定 > アカウント > 職場にアクセス



4) **パッケージをセットアップ**

④ **追加が表示。クリック simasu.**

› 設定 › アカウント › 職場にアクセス



5)プロビジョニング準備完了

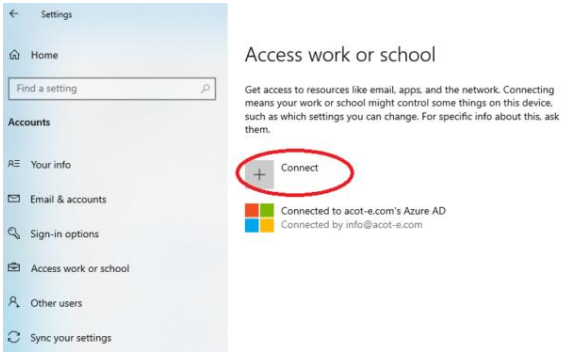
⑤　確認のためのウィンドウが表示されます。クリックで終了です。

7.1.3.2 職場アカウントの追加

1)① 職場アカウントの追加

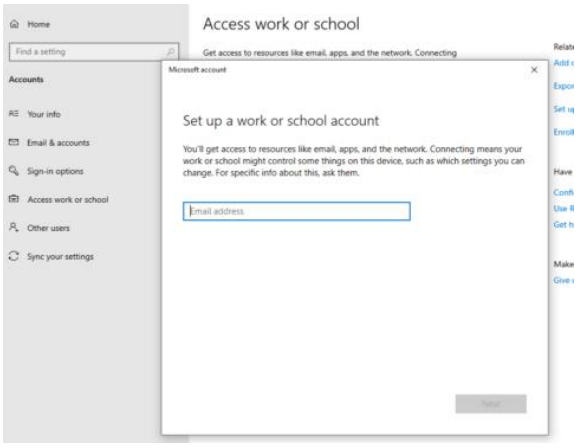
Windows 左下の Windows 10 ロゴから設定を選び、さらにアカウント>会社または学校アカウントに移動してください。

> 設定 > アカウント > 職場にアクセス



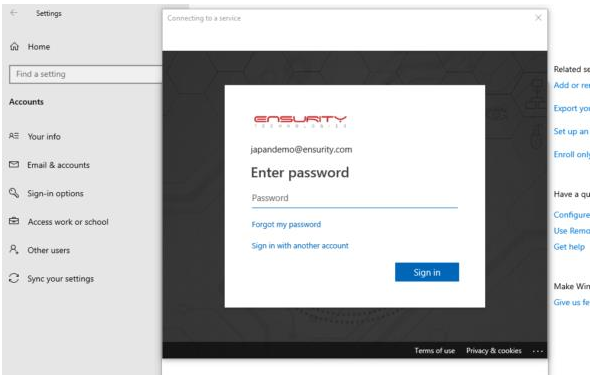
2)② E メールアドレスの入力をします。

> 設定 > アカウント > 職場にアクセス



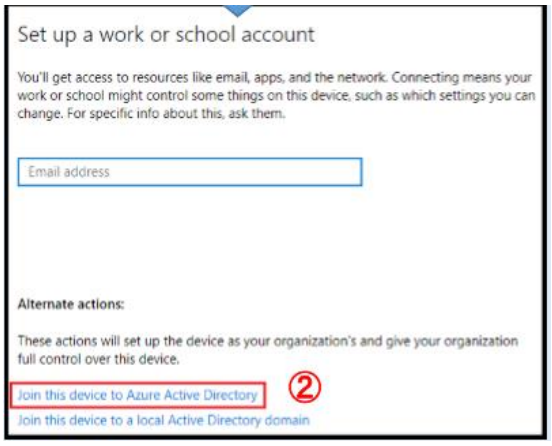
3)③ パスワードの入力をします。

設定 > アカウント > 職場にアクセス



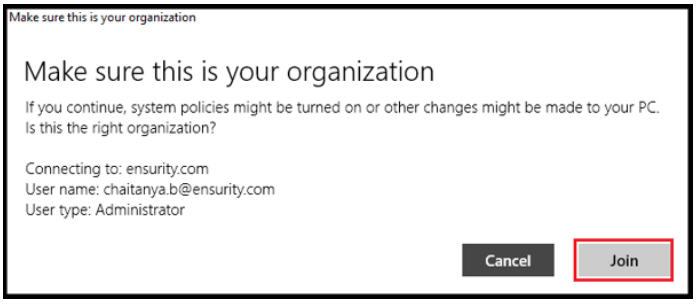
4)④ デバイスの Azure AD への参加

> 設定 > アカウント > 職場にアクセス



5)⑤ 組織を確認して終了します。

> 設定 > アカウント > 職場にアクセス



7.1.3.3 ローカルアカウントの設定

PC デバイスに紐づけられた職場アカウントを PC デバイスの Windows のローカルアカウントに設定します。それによって、その PC デバイスの Windows にログインに設定された FIDO キーによるパスワードなしログインが可能になります。Azure　AD の FIDO2 サーバーによるユーザー認証されますので、Azure AD にも同時にログイン認証されています。そのため、Windows から認証なしで AzureAD に移行できます

1)職場アカウントの追加

① ″他のユーザー″の″職場または学校アカウントユーザー″で職場または学校アカウントの追加をクリックします。

その時のローカルアカウントが標準ユーザーのときは他のユーザーが表示されません。アカウント > ユーザーの情報欄には。現在のローカルアカウントが表示されます。

Windows システムツール > コントロールパネル> ユーザーアカウント欄には、ローカルアカウントが表示されます。現在のローカルアカウントを選択して、″アカウントの種類の変更″をクリックして、″管理者″の種類を選択する必要があります

> 設定 > アカウント > 職場にアクセス

2) Windows 再起動して、新しい職場アカウントを使用して、″サインインオプション″でセ ›
キュリティキーを選択します。PIN+FIDO ボタンキータッチか、FIDO2 セキュリティキータッチで Windows ログインを行います。Windows ログイン後、Azure AD portal にユーザー認証なしで移動できることを確認して下さい。

ローカルアカウントが、新しい職場アカウントに自動的に変更されていることを確認ください。

› 設定 › アカウント › ユーザーの情報

7.2 ユーザーの設定作業

7.2.1 暗証番号 PIN の登録

Excelsecu 社の FIDO Manager ソフトウエアの FIDO ページで暗証番号 PIN を設定できます。また、Windows 10 のアカウント設定機能を利用して、暗証番号 PIN や指紋を各自の FIDO キーに登録します。

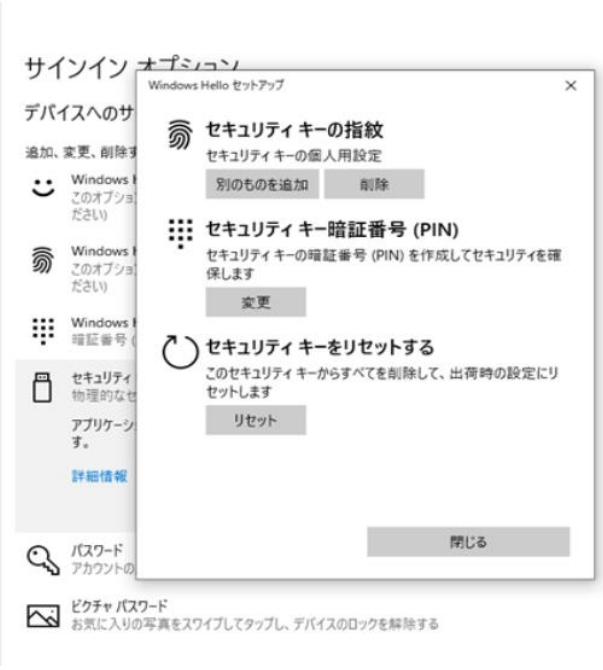
Windows > 設定 > アカウント > サインインオプション > 暗証番号 PIN にて

初めてのときは、暗証番号を記入します。暗証番号を変更したいときは、以下の3つのコードを入力します。

古いセキュリティキーの暗証番号、

古いセキュリティキーの暗証番号

古いセキュリティキーの暗証番号



7.2.2 Azure への FIDO キーの登録

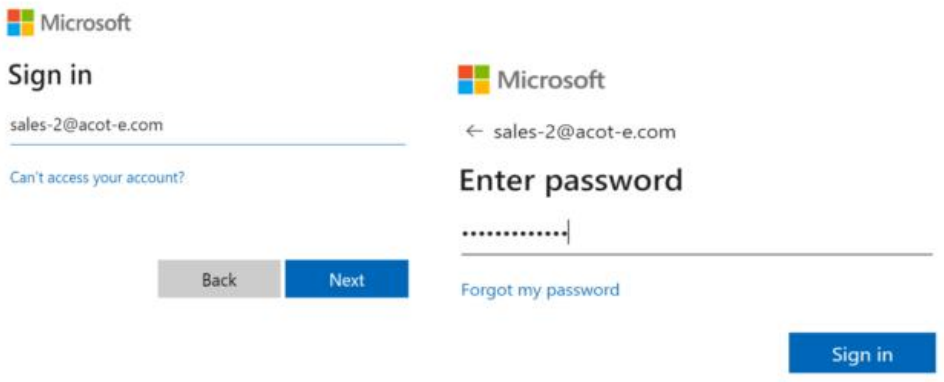
自分の FIDO キーに鍵のペアを生成して、Azure AD に公開鍵とともに鍵名を登録します。Azure AD に関連した My Profile のマイ プロファイルポータルで、FIDO キー（FIDO ボタンキーFD200-203 または FIDO2 セキュリティキーFD210-213）によるパスワードなし FIDO2 認証を登録します。

職場アカウントを使用して、マイプロファイルポータル(https://myprofile.Microsoft.com)にパスワードを利用したユーザー認証を実行してしてログインします。そこでは、職場または学校アカウントを管理するために、セキュリティ情報の設定と管理や、接続されている組織とデバイスの管理を行うことができるほか、所属する組織で自分のデータがどのように使用されているかを確認することができます。

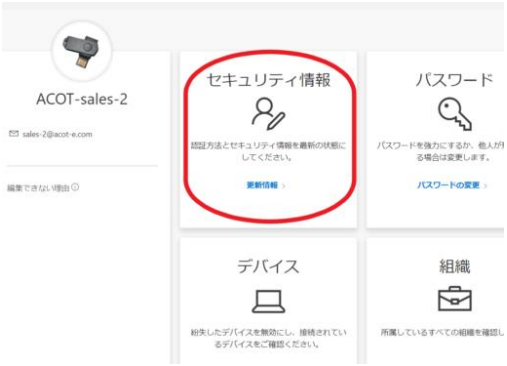
”方法を追加します”のポップアップで、その方法が選択できる項目が現れます。Microsoft Authenticator を指す認証アプリも含まれています。ここではセキュリティキーを選択します。

Azure AD のアカウントを管理するサイトが myprofile です。この職場アカウントに FIDO2 セキュリティキーを登録します。スマートフォンで動作する Microsoft Authintication App を、バックアップのソフトウエア認証器をスマートフォン上に生成してください。

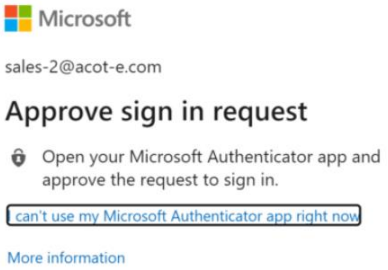
1）＞https://myprofile.microsoft.com/へログインして下さい。職場アカウントをパスワード認証などを利用して,**Azure AD** アカウント管理サイト**(myprofile.microsoft.com)** にログインします。



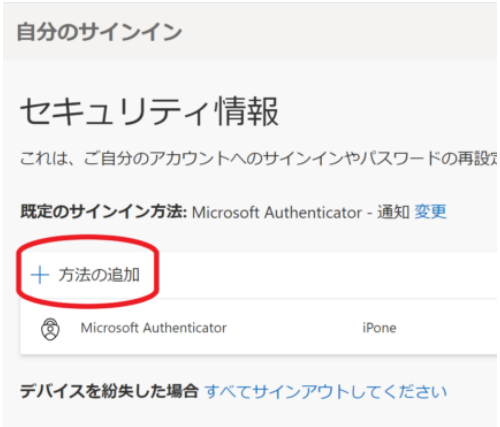
２）”セキュリティ情報"の更新情報をクリックして、セキュリティ情報に移動します。



3)職場アカウントについて再度ユーザー認証が行われます。 Microsoft Authenticator に登録している職場アカウントでは、スマートフォン上に承認するかどうかの問い合わせがありますので、スマートフォンのアプリサイトで承認をクリックします。その結果、情報セキュリティサイトへ移動できます



4)　サインイン方法として、登録済みのサインイン方法が列挙されています。ここでは、”方法の追加”をクリックします。



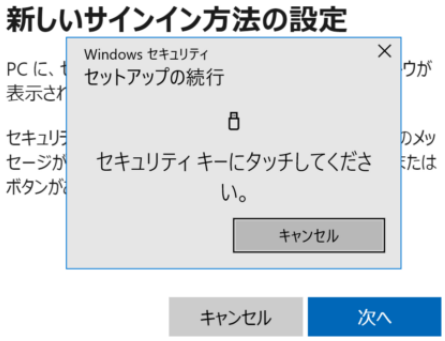
5)”方法を追加します”のホップアップで、方法を選択します。ここではせきゅｒひていキーを選択します。

6)FIDO キーがどのデバイスで利用するキーかを尋ねられます。USB デバイスか NFC デバイスを選択します。次のページで”次へ”をクリックします。FIDO ボタンキーFD200 や FIDO2 セキュリティキーFD210 は、USB デバイスです。対象デバイスは、デスクトップパソコンです。

FIDO ボタンキーFD202 や FIDO2 セキュリティキーFD213 は、NFC デバイスです。対象デバイスは、デスクトップパソコンだけでなく、NFC(近距離無線通信)を使ってスマートフォンでも利用できます。ただし、登録についてはパソコンでの登録に限定されています。

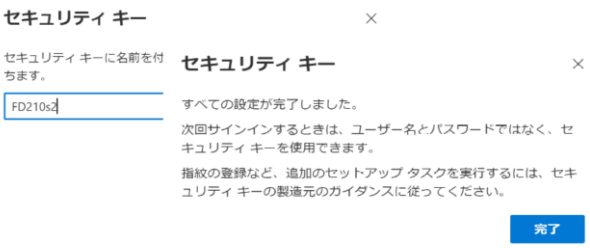
7) FIDO ボタンキーFD200-203 を挿入すると、ボタンタッチの前に暗証番号 PIN の入力を求められます。その後にボタンキーの LED が点滅してボタンタッチが要求されます。暗証番号を新たに入力する場合は、任意の4ケタとか6ケタの数字を入力します。

いずれのキーでも、この登録操作で、公開鍵と秘密鍵が FIDO キーの内部で自動的に生成され、公開鍵は Azure AD 認証サーバーへ送付されます。



8)FIDO キー番号を入力します。この番号は任意の文字で構いません。複数のキーがあるとき、どのキーを登録したか記録するのが目的です。キー番号を入力すると、すべて完了します。

情報セキュリティのサインインの方法に、セキュリティキーの名前が追加されています。同じ列の右端にある”削除”ボタンをクリックすると、登録が削除されます。



8. FIDO Manager および OTP の使用法

FIDO および OTP の構成に使用されるソフトウェア(TOTP / HOTP)は、「Excelsecu Manager ユーザーマニュアル」のドキュメントに記載されています。詳細については、これを参照してください。

9. FAQ

質問	FD200 キーをコンピューターにインストールするにはどうすればよいですか？
回答	インストールする必要はありません。プラグアンドプレイです。 Windows、macOS、Linux、ChromeOS で動作します

質問	2 つの Gmail アカウントを持っています。2 つの Gmail アカウントを保護するために 必要な FD200 キーの数はいくつですか？ 2 つのキーが必要ですか？
回答	複数のアカウントで 1 つの FD200 キーを使用できます。しかし、それはお勧めしません。 1 つまたは 2 つの Gmail アカウントを保護しているかどうかに関係なく、複数のキーを登録することをお勧めします(サービスで許可されている場合)。そうすれば、キーを紛失したり、破損したり、盗まれたりした場合でも、バックアップキーをすぐに使用できます。

質問	FIDO2 セキュリティキーを紛失した場合はどうすればよいですか？
回答	キーがすでに登録されている Web サイトにアクセスするだけです。アカウントなどの Web サイトにリストされているデバイスを削除します。デバイスの利用は停止さ れます。このようなケースを想定して、2 つの FD200 キーをお勧めします。1 つは通常の使用用で、もう 1 つはバックアップ用です。

質問	この FD200 キーには NFC 機能がありますか？
回答	いいえ。FD202 と FD203 キーは、NFC 機能のある FIDO2/FIDO・USF キーです。

質問	この FIDO2 セキュリティキーには Bluetooth 機能がありますか？
回答	いいえ。 FD203キーは、Bluetooth と NFC 機能のある FIDO2/FIDO・USF キーです。

質問	どのアプリケーションが FIDO2 セキュリティキーをサポートしていますか？
回答	FIDO®U2F/ FIDO2 をサポートするアプリケーションには、Google、Microsoft、 Facebook、Dropbox、GitHub、Salesforce、Dashlane などが含まれます。

10.製品仕様

項目	FD200
OS	Windows、macOS、Linux
ブラウザ	Edge、Chrome、Firefox、Opera、Safari
機能	FIDO®U2F、FIDO2、HOTP、TOTP
アルゴリズム	SHA256、AES、HMAC、ECDH、ECDSA
サイズ	44.7x16.0x9.0(mm)
インターフェース	USB-A
プロトコル	HID
データ保持	≥10 年
書き換えサイクル	≥100,000 回
動作電圧	5V±10%
動作電流最大	<40mA
ボタンシングル	シングルボタン
ボタン耐久性	≥100,000 回
動作温度	-10～60℃
動作湿度	10～90%
表示器光	白
材質	AL、 PC
証明書	CE、FCC、RoHS、WEEE、FIDO2 L1