



教育機関向け Azure AD のパスワード考慮

日本マイクロソフト株式会社

2020 年 9 月版



Windows 端末へのサインイン

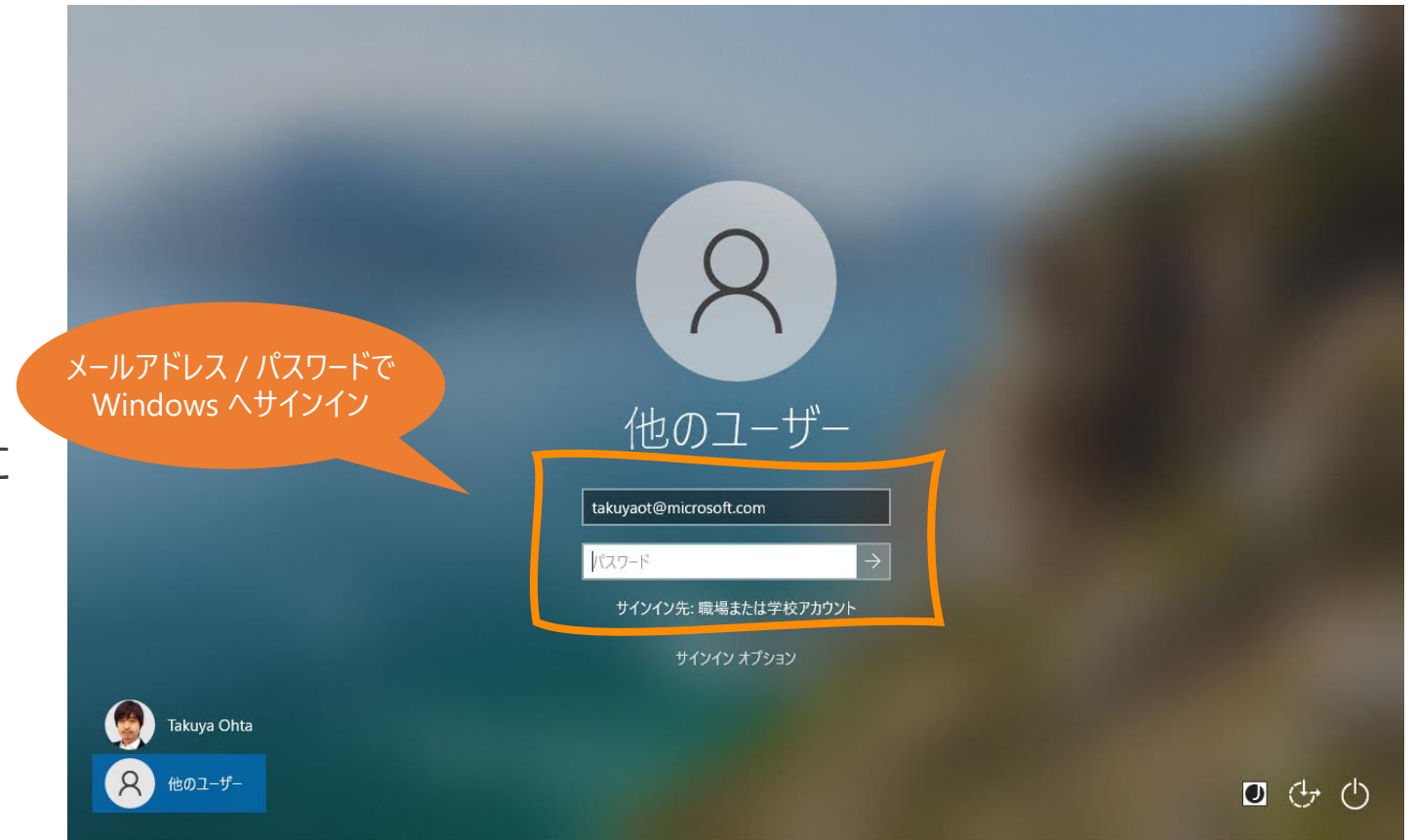
Azure AD 参加した状態の Windows では、作成した ID とパスワードでサインインを行う

Windows へサインインをすることで、ID 認証が完了
その後クラウドサービスやリソースにアクセスする際には
シングルサインオン (SSO) が可能になる

つまり、PC を起動し Windows へサインインする際に
パスワードの入力が必要となる。

Azure AD 参加済みデバイスとは

<https://docs.microsoft.com/ja-jp/azure/active-directory/devices/concept-azure-ad-join>



Azure AD 参加した状態への Windows 10 へのサインイン画面

Azure AD のユーザーのパスワード

Azure AD のユーザーでサインインする際のパスワードの要件・設定可能値は以下の通り
下記の 2 つのうちのいずれかの手段で設定することが必要

種類	要件	サンプル	考慮事項
① 既定のパスワード ポリシー	<div>セキュリティ上推奨</div> <ul style="list-style-type: none">■ 8 文字以上 256 文字以下■ 次の 4 つのうち、3 つが必要<ul style="list-style-type: none">・ 小文字・ 大文字・ 数字 (0-9)・ 記号	Password1 P@ssw0rd! (ランダムなど)	<ul style="list-style-type: none">■ 既定の推奨のパスワード■ 入力には手間がかかるがセキュリティ上推奨
② 複雑ではないパスワード	<ul style="list-style-type: none">■ 8 文字以上 256 文字以下	12345678 password (ランダムなど)	<ul style="list-style-type: none">■ セキュリティ上推奨はできないパスワード■ 低学年向けなどどうしても使わざるを得ない場合 <p>※ 条件付きアクセスなど追加機能でセキュリティを高めることを推奨</p>

※ パスワードを 8 文字未満の短さに設定することはできません。

複雑でないパスワードを利用するには

PowerShell を使ったアカウント登録時に

- ① 複雑でないパスワードを有効にする(-StrongPasswordRequired)
- ② 初回パスワードの強制変更を無効にする(-ForceChangePassword)

NAME

addo365user1.ps1

SYNOPSIS

addo365user1.ps1 <Input file> <Output file>

addo365user1.ps1

Connect-MsolService

```
Import-Csv -Path $Args[0] -Encoding UTF8 | foreach {New-MsolUser -DisplayName $_.DisplayName -UserPrincipalName $_.UserPrincipalName -Title $_.JobTitle -
Department $_.Department -PostalCode $_.PostalCode -City $_.City -State $_.State -Country $_.Country -UsageLocation $_.UsageLocation -
LicenseAssignment $_.AccountSkuId -StrongPasswordRequired $false -ForceChangePassword $false} | Export-Csv -Path $Args[1] -Encoding UTF8
```

NAME

addo365user2.ps1

SYNOPSIS

addo365user2.ps1 <Input file directory> <Output file directory>

addo365user2.ps1

Connect-MsolService

```
Get-ChildItem -Recurse -File $Args[0] | ForEach-Object {Import-Csv -Path .¥Input¥$_ -Encoding UTF8 | foreach {New-MsolUser -DisplayName $_.DisplayName -
FirstName $_.GivenName -LastName $_.SurName -UserPrincipalName $_.UserPrincipalName -Title $_.JobTitle -Office $_.PhysicalDeliveryOfficeName -
Department $_.Department -PostalCode $_.PostalCode -StreetAddress $_.StreetAddress -MobilePhone $_.Mobile -City $_.City -State $_.State -Country $_.Country -
UsageLocation $_.UsageLocation -LicenseAssignment $_.AccountSkuId -StrongPasswordRequired $false -ForceChangePassword $false} | Export-Csv -Path $Args[1]¥$_ -
Encoding UTF8}
```

Windows へのパスワードレス サインイン手段 (オプション)

Windows Hello for Business を利用することで、Windows へのログオンの際にパスワードを使用しないことは可能。
しかしながら多要素認証を利用して本人確認が必要なため、小中学校等の生徒に対しては非現実的な手段となる。


※ 多要素認証 (Azure MFA) では、電話やスマートフォンなどのモバイルデバイスが必要

種類	デバイス要件	考慮事項
③ Hello の生体認証	<ul style="list-style-type: none">■ Windows Hello 対応の生体認証デバイス■ 多要素認証で利用できるデバイス	<ul style="list-style-type: none">■ 初回登録時に多要素認証での本人確認■ 2 回目以降は生体認証でサインイン可能
④ Hello の PIN (暗証番号)	<ul style="list-style-type: none">■ 特にデバイスは必要なし■ 多要素認証で利用できるデバイス	<ul style="list-style-type: none">■ 初回登録時に多要素認証での本人確認■ 2 回目以降は PIN でサインイン可能
⑤ FIDO2 セキュリティ キー	<ul style="list-style-type: none">■ FIDO2 セキュリティ キー デバイス	<ul style="list-style-type: none">■ 初回にセキュリティ キーの登録が必要■ 2 回目以降はキーへのタッチでサインイン可能

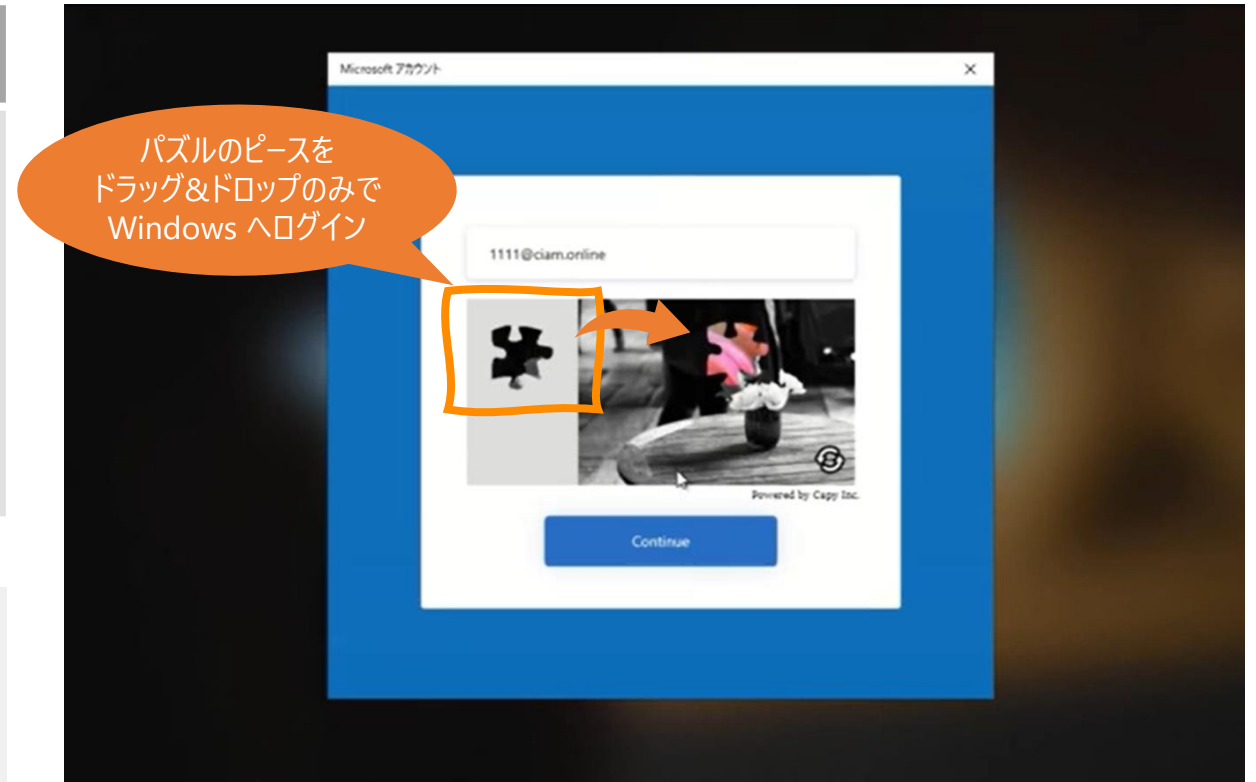


3rd Party ソリューション (オプション)

伊藤忠テクノソリューションズ (CTC) が提供するサービスを利用することで、様々な認証に拡張して対応が可能
※ 別途有償での契約が必要となります。

種類	概要
⑥ CTC – SELMID  	CTC が提供する IDaaS。 Azure AD の認証を拡張し、LINE や facebook の認証なども利用可能。 小学校低学年にはパズル CAPTCHA を利用した実績もあり。

B2C事業者様向けIDaaS「SELMID」
<https://ctc-insight.com/selmid>



パズル CAPTCHA による Windows へのサインイン
<https://youtu.be/WGAOiQB3LDU>

参考資料 1

Windows Hello for Business 関連資料

Windows Hello とは？

Windows 10 デバイスに素早く安全にアクセスする代替手段

特徴

デバイス ロック解除を PIN もしくはパスワードレス化
PIN、生体認証情報利用時はローカルのみに保存

メリット

のぞき見や使いまわしなどによるパスワード流出を防止
素早い認証、パスワード入力の手間から解放

Windows Hello で可能な認証

- Microsoft アカウント
- Active Directory アカウント
- Azure AD アカウント
- FIDO v2.0 認証をサポートする ID プロバイダー サービス
または証明書利用者サービス (進行中)



Windows Hello を利用した Windows へのサインイン

Windows Hello の使用方法

対応デバイスの準備

- Windows 10
- TPM チップ搭載を推奨
- Windows Hello 対応生体認証デバイス

※ PIN だけであれば Hello 対応デバイスが無くても使用可能

Windows Hello の使用

Windows サインイン時に以下を実施

- A) カメラに対して顔をみせる
- B) 指紋リーダーをなぞる
- C) サインイン画面にて PIN を入力する



現在の Surface は全て Windows Hello 対応済み

Windows Hello の概要とセットアップ

<https://support.microsoft.com/ja-jp/help/4028017/windows-learn-about-windows-hello-and-set-it-up>

生体認証デバイス

Windows Hello でサポートされる 3 種類の生体認証



指紋

最新の指紋センサー付きデバイスをサポート



顔

最新の Intel® RealSense™ (f200) 以降のバージョン仕様に準拠した IR センサーを搭載しているデバイス



虹彩

現在は Hololens 2 のみで使用



※ Windows Hello 対応デバイスかどうかを購入時にご確認ください！

Windows Hello 生体認証の企業利用

<https://docs.microsoft.com/ja-jp/windows/security/identity-protection/hello-for-business/hello-biometrics-in-enterprise>

PIN (暗証番号)

Windows Hello では PIN の利用も想定

PIN は一見セキュリティ強度が低いように思われがちなもの。しかしデバイスに対して設定するもので、そのデバイスだけで有効。試行できる回数や入力できる時間が制限されている。

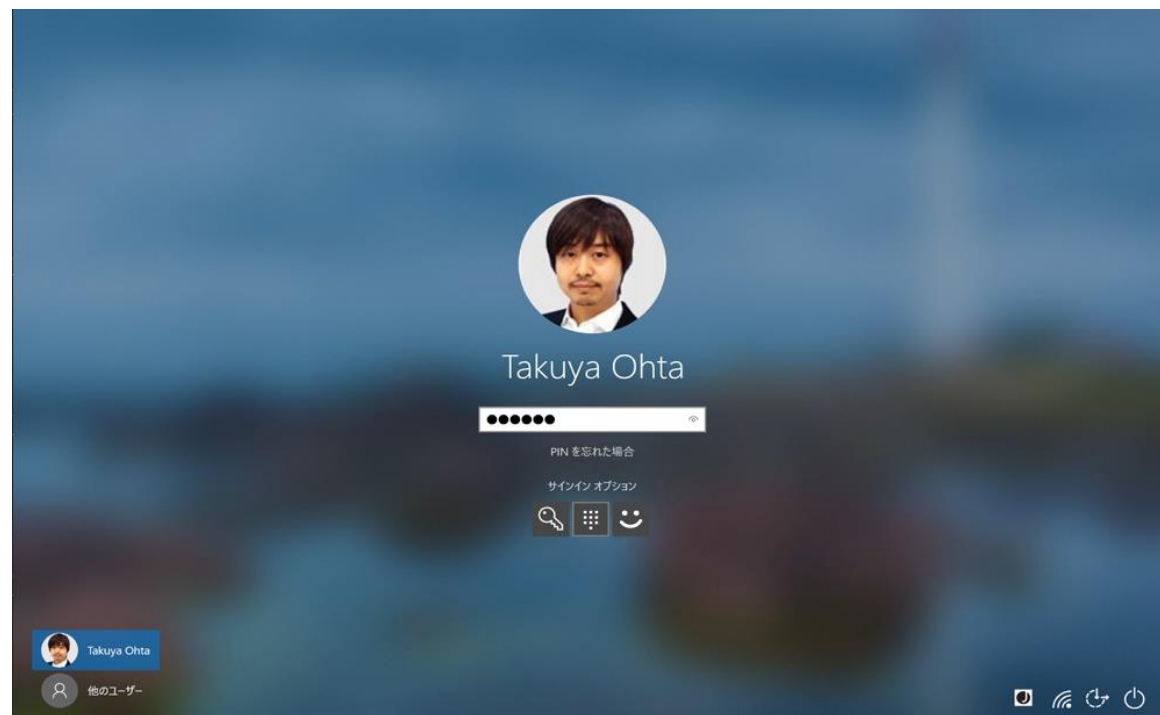
また、けがのためやセンサーの不調・故障などに備えて、PIN を使ってサインインできるように設定が必要。

パスワードの問題点

- 長くないとダメ
- 複雑じゃないとダメ
- 結局使いまわす
- 定期変更が必要
- バレると悪用される

PIN の利点

- PIN はデバイスと密接に関連付け
- PIN はデバイスに対してローカル
- PIN はハードウェアで保護
- PIN は複雑なものも設定可能
- 追加要素の設定も可能



PIN を利用した Windows へのサインイン

PIN がパスワードより安全な理由

<https://docs.microsoft.com/ja-jp/windows/security/identity-protection/hello-for-business/hello-why-pin-is-better-than-password>

Windows Hello のセットアップ

メニューより簡単にセットアップが可能

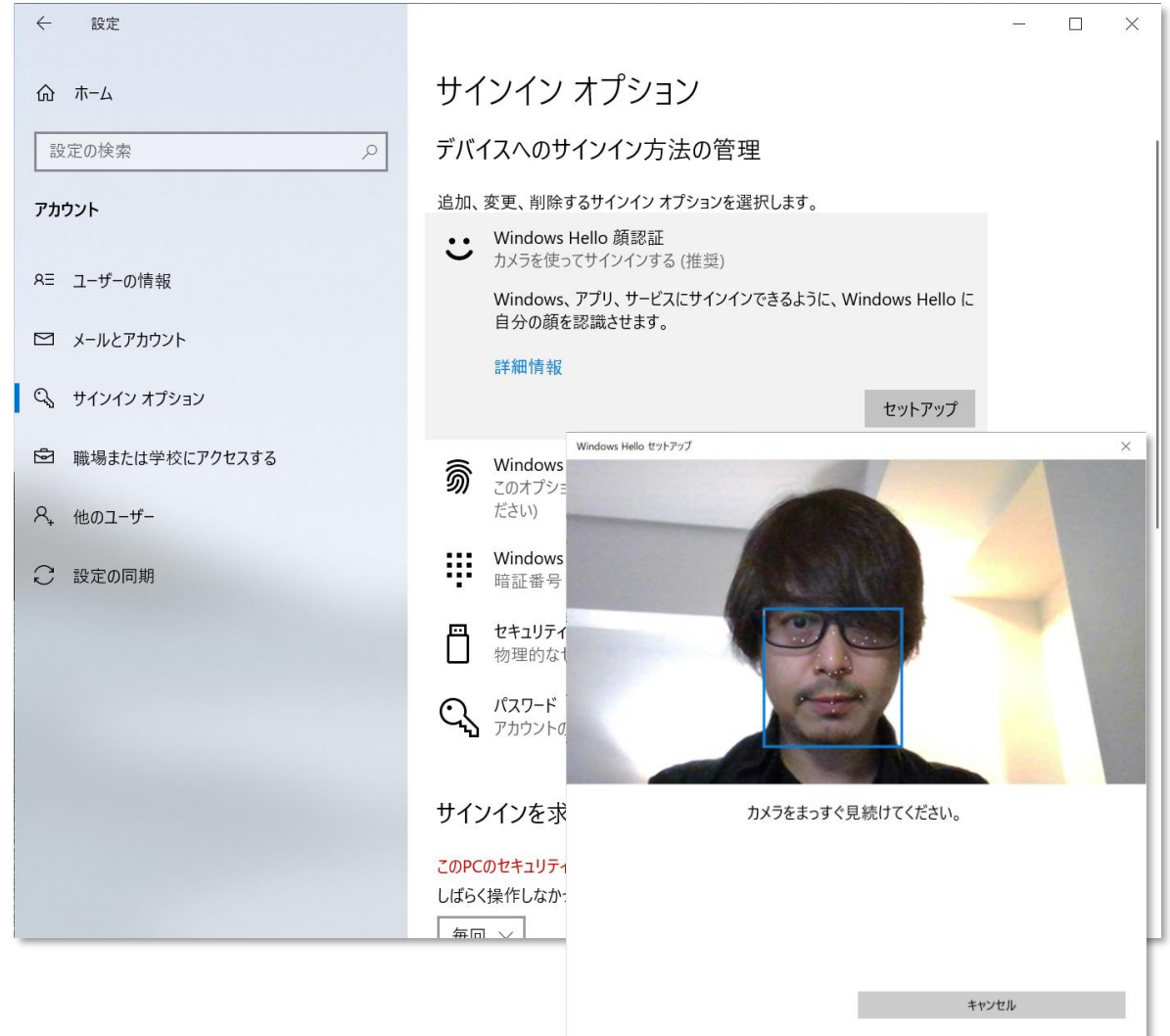
1. [スタート] メニューに移動し、[設定] を選択
2. [アカウント] - [サインイン オプション] を選択
3. 「デバイスへのサインイン方法の管理」にて、Windows Hello の項目を選択

認識精度を高める

生体認識の反応が悪いときや、メガネなどをかけて容姿に変化がある場合には、上記の同メニューより **[認識精度を高める]** を選択することで調整可能。

10 要素まで登録が可能

最大で 10 人分の指紋や顔が登録できる。
共有で使用している PC の場合には注意が必要。



セキュリティ キーによるパスワードレス サインイン (プレビュー)

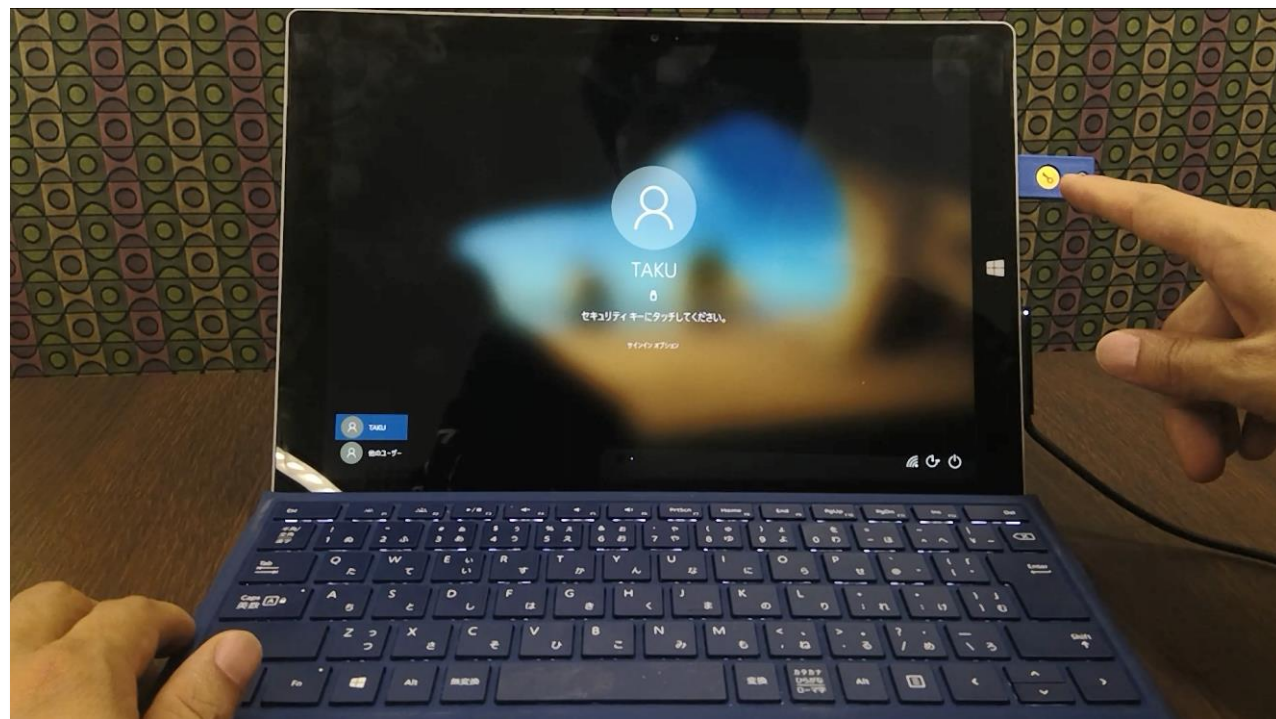
FIDO2 セキュリティ キーに基づくパスワードレス認証

FIDO2 対応デバイスを使用して、Azure AD アカウントで Windows へパスワードレスにサインインが可能に。
低コストでセキュリティ キーによるサインインの実現が可能。

必要条件 (例 : Azure AD 参加の場合)

- Azure MFA
- 互換性のある FIDO2 セキュリティ キー
- Windows 10, version 1903 以降

また制限はあるものの、Windows Hello を使わなくとも、手軽にパスワードレス サインインできる手段の一つに。



Yubico セキュリティキー を利用した Windows へのサインイン

Azure Active Directory を使用して Windows 10 デバイスへのパスワードレス セキュリティ キー サインインを有効にする (プレビュー)
<https://docs.microsoft.com/ja-jp/azure/active-directory/authentication/howto-authentication-passwordless-security-key-windows>

