Windows helloとWindows hello for businessの違い

Microsoftが考える多要素認証

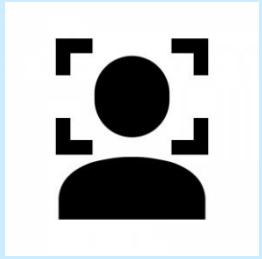
認証方法と機能 - Microsoft Entra ID | Microsoft Learn

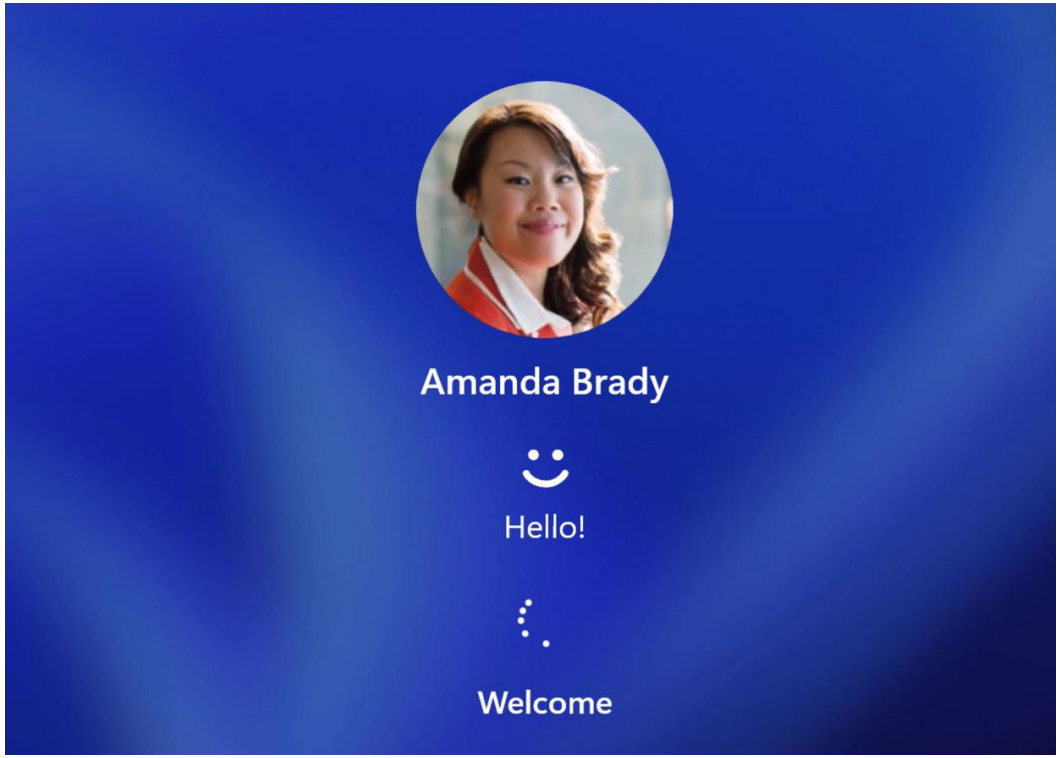
そもそもWindows hello/Windows hello for businessって

✓生体認証（顔認証・指紋認証）、PINコードでWindowsのPCにサインインできる技術のこと。

生体認証

Windows Helloによる顔認証によりログイン



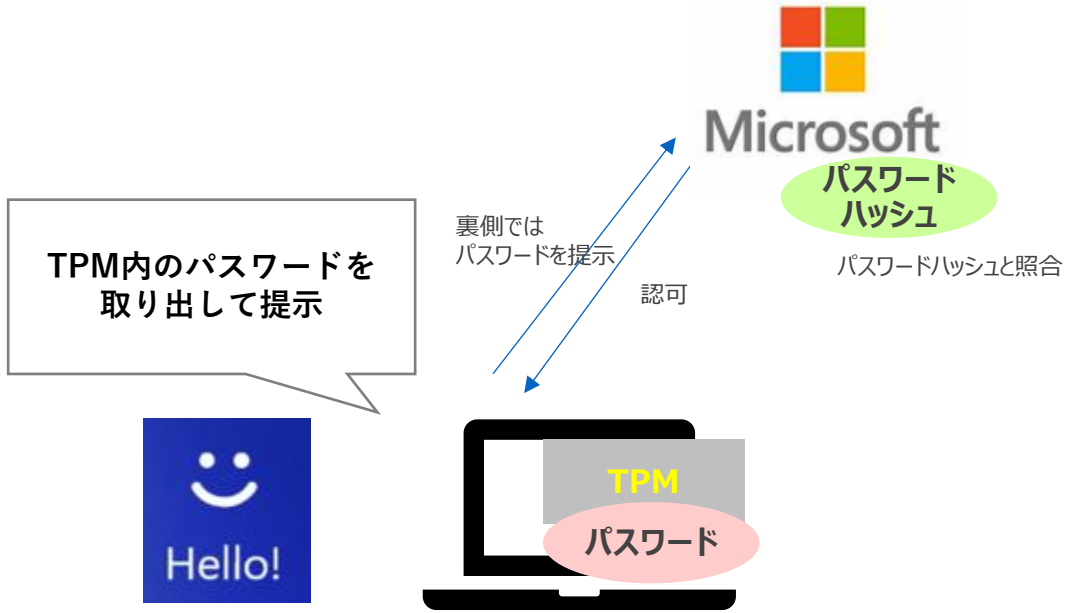


Windows Hello for Business の概要 | Microsoft Learn

Windows helloとWindows hello for businessの違い

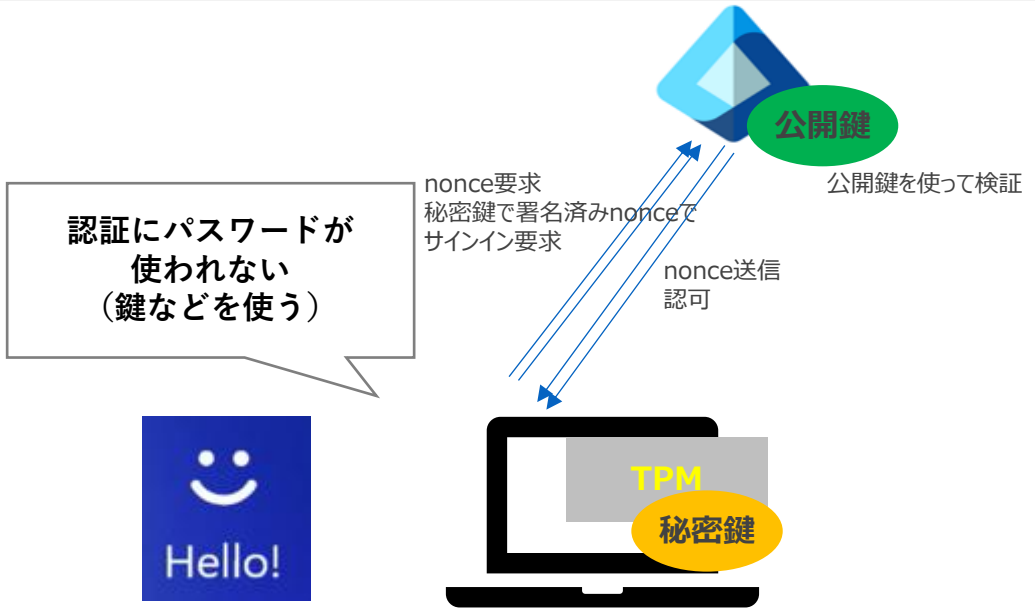
- ✓ Windows helloは見かけ上パスワードレスっぽいが、実態としてはパスワードを使って認証している
- ✓ Windows hello for businessは、公開鍵/秘密鍵を利用し、一切パスワードを使わない仕組み
- ✓ Windows hello for business は多要素認証とみなされる

Windows hello



PIN(知識情報)
or
指紋・顔(生体情報)

Windows hello for business（クラウド単独展開）



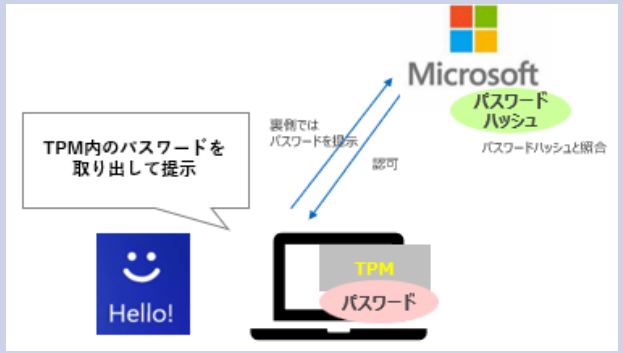
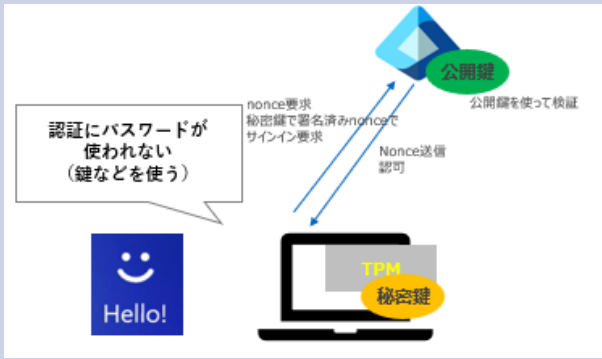
①PIN(知識情報)
or
指紋・顔(生体情報)

②デバイスに登録された秘密鍵
（デバイスそのものの所持情報）

Windows Hello for Business の概要 | Microsoft Learn

Windows hello とWindows hello for business　対象アカウントの違い

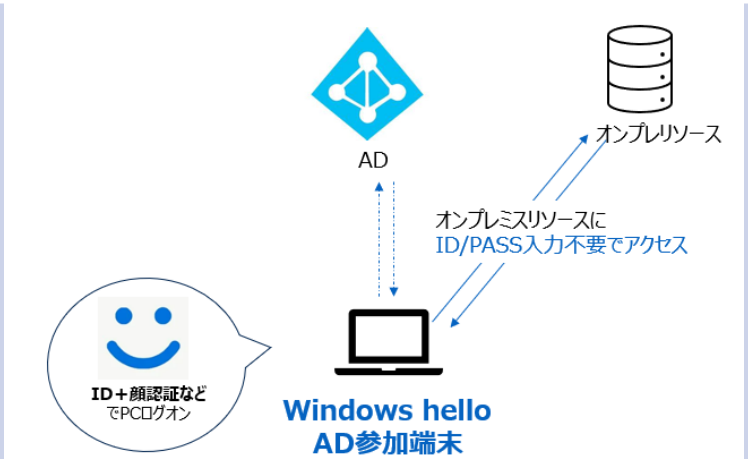
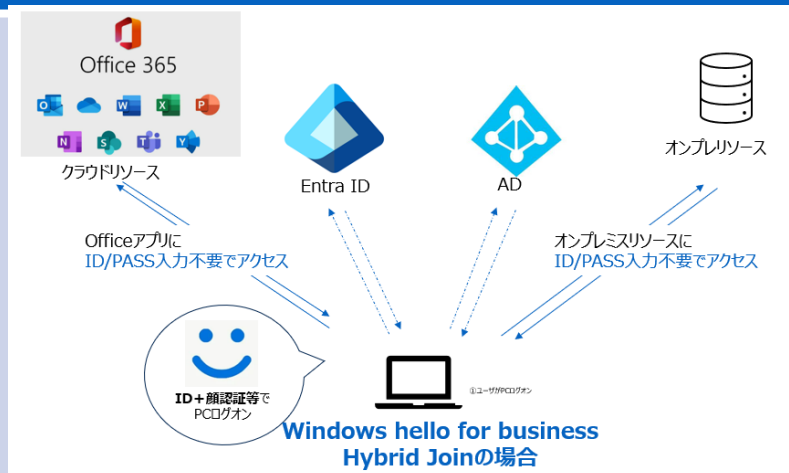
- ✓ 顔や指紋などのデータは端末のみに保存されるため、クラウド上等には保存されない。
- ✓ ユーザエクスペリエンスには変わりはない。セキュリテイ面、実装できるアカウント/端末に違いがある。
- ✓ Windows hello for businessの方が、**実際の認証時にパスワード情報が送信されないので、**よりセキュア。

	Windows hello	Windows hello for business
		
裏の仕組み	TPM内に**パスワード**を保存している 生体認証/PINで、TPMからパスワードを取り出して認証。 **見かけ上パスワードを使っていないように見えるが、** **認証フローではパスワードを利用されている**	TPMにて**秘密鍵**を保存し、Entra ID に公開鍵保存 TPM内に秘密鍵が保管されている。生体認証/PINで認証後、一回限り有効なnonce(ランダムデータ）に秘密鍵で署名したものをEntraに送信する。 **認証フローにおいて一切パスワードは利用されない。** **傍受されても再利用できないため、よりセキュアな仕組み。**
利用で想定されているアカウント	・ローカルアカウント ・Microsoft アカウント ・ADアカウント ×**EntraIDアカウント　サポート対象外**	・ADアカウント ・EntraIDアカウント
利用で想定されるPC	・Workgroup端末 ・ドメイン(AD)参加端末 ×Entra Hybrid Join端末 ×Entra Join端末	・ドメイン(AD)参加端末（方式名：オンプレミス単独展開） ・Entra Hybrid Join端末（方式名：ハイブリッド展開） ・Entra Join端末（方式名：クラウド単独展開）
WindowsOS	Home含むすべてのエディション	Professional/Enterprise/Education ※Homeは対象外

Windows hello とWindows hello for business　動作イメージの違い

✓ 共通して言えることは、**生体認証/PINを利用して、パスワードを入力せずに各リソースにアクセスできる**ようになり、便利。

✓ なおWindows HelloではEntraへのSSOはできず、対話型のサインインが必要。

	Windows hello	Windows hello for business
		
動作イメージ	＜ドメイン(AD)参加端末の場合＞ 生体/PIN認証でPCログオンすると、 ・オンプレリソースにSSOできる（ID,PW不要でアクセスできる） **・EntraにはSSOできない**（端末ログオン後に、ID,PWの入力が必要）	＜Entra Join端末の場合＞ 生体/PIN認証でPCログオンすると、 ・クラウドアプリにSSOできる（ID,PW不要でアクセスできる） ※別途設定を実施することによりオンプレミスリソースにもSSOできる（ID,PW不要でアクセスできる） ＜Hybrid Join端末の場合＞ 生体/PIN認証でPCログオンすると、 ・オンプレリソースにSSOできる（ID,PW不要でアクセスできる） ・クラウドアプリにできる（ID,PW不要でアクセスできる）
参考）MS サポート回答	Microsoft Entra joinもしくは Microsoft Entra hybrid を構成したデバイスに **Entra ID のユーザー (オンプレミス AD から同期されたユーザーも含む) でサインインするシナリオでは Windows Hello (便利な PIN) はサポートされておりません。** https://learn.microsoft.com/ja-jp/windows/security/identity-protection/hello-for-business/faq	

Windows hello とWindows hello for business　実装のための作業の違い

- ✓ Entra Join端末（クラウド単独）の場合、Windows hello for businessは既定で有効になる。
- ✓ ADでは、既定ではWindows hello for businessのパスワードレスの認証に対応していない。そのため、追加の構成が必要。

	Windows hello	Windows hello for business
有効化するための作業	＜ドメイン(AD)参加端末の場合＞ Windows helloを有効化するGPO設定 　コンピューターの構成¥管理用テンプレート¥システム¥ログオン 　便利なPINを使用したサインインをオンにする　・・・有効	＜Entra Join端末の場合＞ ・既定で有効になるため、特に作業は不要 ＜Hybrid Join端末の場合＞ ・既定は有効にならない。下記作業もしくはキー信頼、証明書信頼(証明書の作成等)が必要。 　クラウド Kerberos 信頼 　　①Microsoft Entra Kerberos サーバー オブジェクトの作成 　　②クラウドKerberos信頼有効化のためのGPO/Intune設定 　　参考）クラウド Kerberos 信頼デプロイ方法 | Japan Azure Identity Support Blog ＜ドメイン(AD)参加端末の場合＞ キー信頼、証明書信頼の作業が必要
PINのポリシー設定（複雑さ、生体認証を必須にする/PINだけにするなど）	＜ドメイン(AD)参加端末の場合＞ ・GPOでのポリシー設定 Windowshello for business と同様のGPOで設定する Windows Hello for Business ポリシー設定 | Microsoft Learn	＜Entra Join端末の場合＞ ・Intuneでのポリシー設定 Microsoft Intune を使用してテナント全体の Windows Hello for Business ポリシーを構成する - Microsoft Intune | Microsoft Learn ＜Hybrid Join端末の場合＞ ・GPO/Intuneでのポリシー設定 ※GPOとIntuneいずれも設定がされている場合はGPOが優先される Windows Hello for Business ポリシー設定 | Microsoft Learn ＜ドメイン(AD)参加端末の場合＞ GPOでのポリシー設定
参考）MS サポート回答	Windows Hello (便利な PIN) を使用してオンプレミス AD アカウントで OS にドメイン参加構成のデバイスにサインインした場合、既定でオンプレミス リソースに SSO できます。これは Windows Hello (便利な PIN) では PIN や生体認証で OS にサインインしますが裏ではパスワードで OS にサインインしている動作と同じであり、パスワードで OS にサインインする仕組みではオンプレミス AD から Kerberos チケットを取得できるからです。	Windows Hello for Business は完全にパスワードを排除したよりセキュアな仕組みであり、キーペアを使用して認証を行います。 このキーペアを使用した認証では既定でオンプレミス AD から Kerberos チケットの取得ができないため、追加の構成(クラウド Kerberos 信頼の場合は Microsoft Entra Kerberos サーバーの作成)を行う必要があります。