NII 次世代認証基盤連携検討部会

Microsoft

Windows enables security by design from chip to cloud

MicrosoftにおけるAAL2以上の対応について

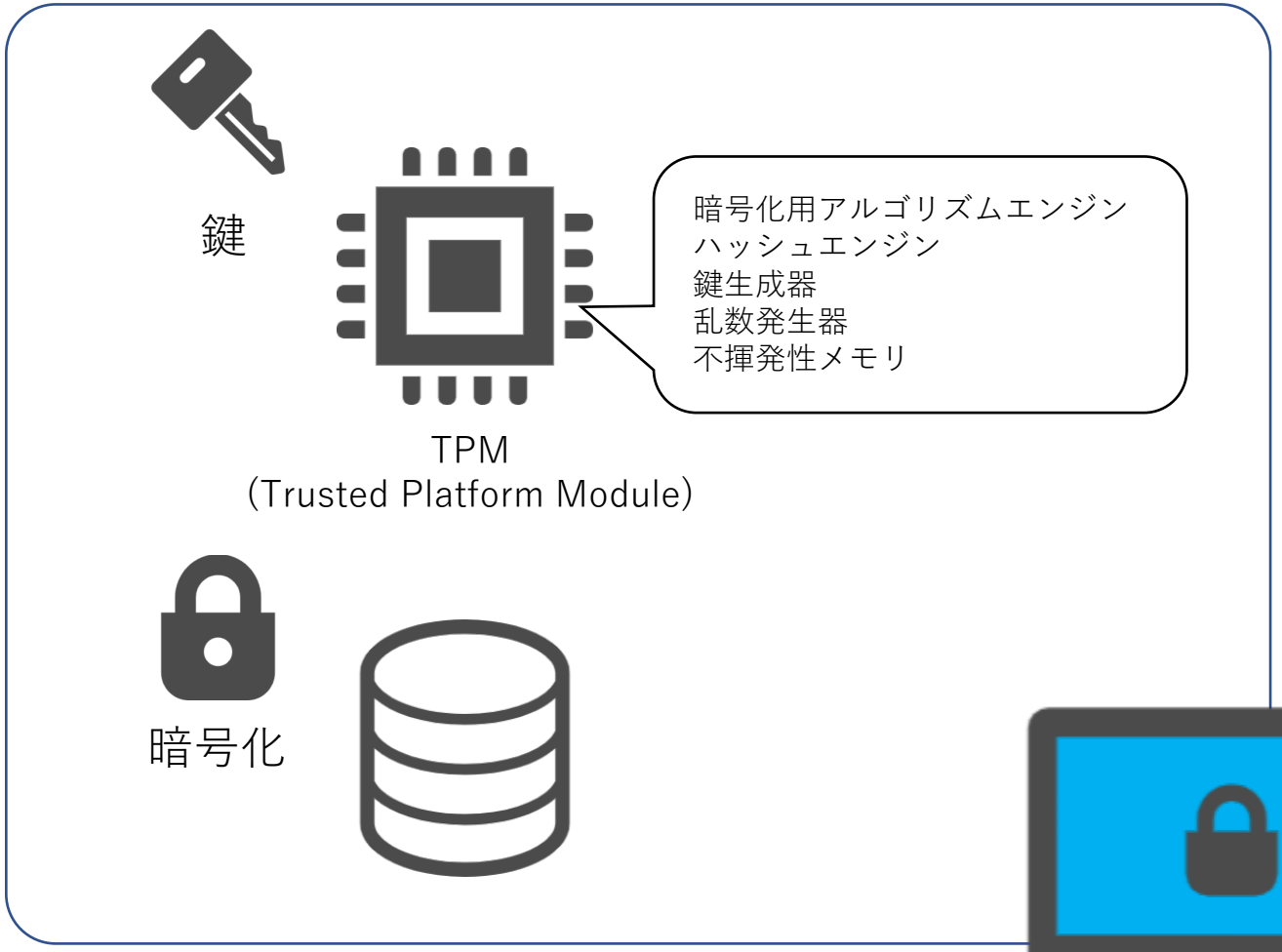
2021年9月10日

日本マイクロソフト株式会社

中田　寿穂

2021年10月5日 リリース

Windows 11 で必須になった「TPM 2.0」って何？



TPM 1.2 → TPM 2.0

- 暗号化アルゴリズム: RCA に加え ECCが利用可能に
- 鍵を管理するための階層が1階層→3階層に

利用用途

- ブートプロセスの監視
- BitLocker によるドライブの暗号化
- Credential Guard
- Windows Hello for Business

など

Windows 11、チップからクラウドまでのセキュリティ バイ デザインを実現

June 25, 2021

Windows 11 enables security by design from the chip to the cloud

David Weston　Director of Enterprise and OS Security

- ✓ TPM 2.0 の搭載を義務付けることで、ルートオブトラストが必須となり、ハードウェアセキュリティの基準を高めることができる。
- ✓ TPM 2.0 は、Windows Hello や BitLocker でセキュリティを提供する際の重要な構成要素でデバイスの健全性を証明する際の安全な要素となり、TMP によるゼロトラストセキュリティの促進が可能。
- ✓ Windows 11 では、Azure ベースの Microsoft Azure Attestation (MAA) がデフォルトでサポートされ、認証によって信頼性が証明することでハードウェアベースのゼロトラストをセキュリティが実現できる。
- ✓ Windows Hello によってパスワードを廃止し、情報を保護。

https://www.microsoft.com/security/blog/2021/06/25/windows-11-enables-security-by-design-from-the-chip-to-the-cloud/

Windows Hello とは？

AAL3

Windows Helloとは、Windowsへログインする際に顔認証や指紋認証といった**生体認証機能**を提供する機能。Windows 10のパソコンに標準搭載されており、Windows Hello対応のウェブカメラや指紋リーダーなどを使うことで利用が可能。リモートワークの広がりとともに高まるセキュリティ強化のニーズを受け、近年発売されるノートパソコンには、こうした機器があらかじめ組み込まれ、Windows Helloがそのまま利用できるモデルが増えている。

Windows Hello が目指すもの

IDやパスワードの代替手段、パスワードレスの実現

Windows Hello の機能

a. 生体認証

https://docs.microsoft.com/ja-jp/windows-hardware/design/device-experiences/windows-hello-biometric-requirements

体認証の性能を測る要件として、他人を誤認する「他人受入率（FAR）」と、本人を間違う「本人拒否率（FRR）」が挙げられる。Windows Helloにおける指紋認証の要件は、**FARが0.002%以下、FRRが10%以下**。

顔認証の要件は**FARが0.001%以下、FRRが5%以下または10%以下**となっている。

b. PIN認証

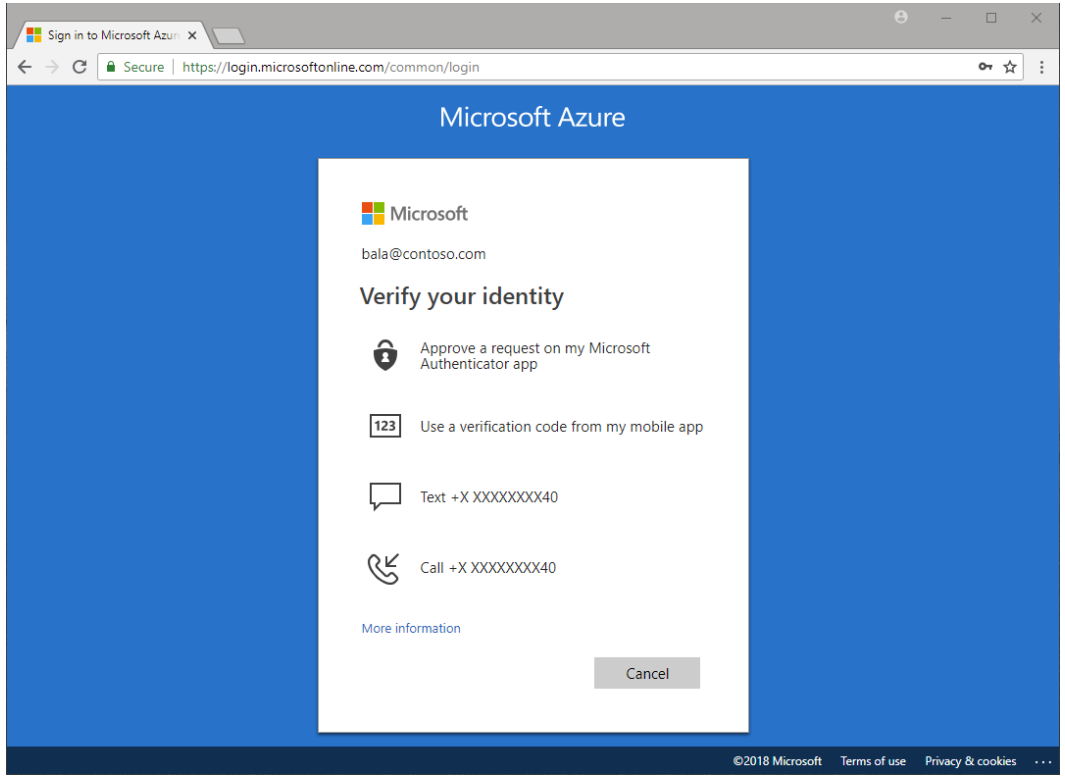
生体認証がうまくいかなかった際の代替手段として、PINが用意されている

Azure AD Multi-Factor Authentication

AAL2 AAL3

Azure AD Multi-Factor Authentication は、次の認証方法のうち 2 つ以上を要求することで機能します。

- ユーザーが知っているもの (通常はパスワード)。
- ユーザーが持っているもの (携帯電話やハードウェア キーのように、簡単には複製できない信頼できるデバイスなど)。
- ユーザー自身 (指紋スキャンや顔面認識などの生体認証)。



Azure AD Multi-Factor Authentication で追加できる検証形式

- Microsoft Authenticator アプリ
- OATH ハードウェア トークン (プレビュー)
- OATH ソフトウェア トークン
- SMS
- 音声通話

Azure AD Multi-Factor Authentication

AAL2 AAL3

Microsoft Authenticator をすべてのユーザーに対してすぐに有効にするために、すべての Azure AD テナントでセキュリティの既定値群を使用できます。 サインイン イベント時に追加の検証を要求するように、Azure AD Multi-Factor Authentication に対してユーザーとグループを有効にすることができます。

より詳細な制御を行うために、条件付きアクセス ポリシーを使用して、MFA を必要とするイベントやアプリケーションを定義できます。 これらのポリシーにより、ユーザーが企業ネットワークまたは登録済みデバイスを使用中の場合は通常のサインイン イベントを許可しますが、リモートまたは個人用デバイスを使用中の場合は追加の検証要素を求めることができます。