SECURITY REPORT

2021 DEC

CyberFortress

このレポートは、株式会社サイバーフォートレスの独自の調査にて収集されたデータに基づき作成しています。

Windows 11の必須条件、TPMとは？

01. 概要

マイクロソフト(MS)が日本時刻2021年10月5日、日本を含めた全世界の190国以上に新しいOS「Windows11」を正式に発表した。前のWindows10が発表されてからおよそ6年ぶりに新しい製品を出した。新規PCはもちろん、既存のWindows10基盤のPCからは無料のアップグレードができるため、大勢のユーザーがアップグレードの計画を立てている。しかし、Windows11をインストールための最初仕様でさらに強化されたセキュリティ要求事項が公開され、混乱している。どのような問題なのかまとめました。

【▲ 最近全世界に新たに公開されたWindows11 (参考：デジタルデイリー)】

Windows 11の必須条件、TPMとは？

02. Windows11をインストールするための仕様

1) 最小インストール仕様

まずマイクロソフト(MS)が公式に発表したWindows11をインストールするためのシステム要求事項はホームページで確認できるが、内容を整理してみると▲ 64Bit及び1GHz以上のデュアルコアプロセス(またはSoC)、▲64GB以上のストレージ、▲UEFI/Secure Bootをサポートするbios、▲DirectX 12以上をサポートするグラフィックカード、▲9インチ以上のHDディスプレー、そして最後に▲TPM2.0サポートなどがある。

＊Windows仕様及びシステム要求事項
- https://www.microsoft.com/ja-jp/windows/windows-11-specifications

プロセッサ	1 **ギガヘルツ** (GHz) 以上で 2 コア以上の **64 ビット互換プロセッサ** または System on a Chip (SoC)。
メモリ	4 ギガバイト (GB)。
ストレージ	64 GB 以上の記憶装置 注: 詳細は下記の「Windows 11 を最新状態に維持するために必要な空き領域についての詳細情報」をご覧ください。
システム ファームウェア	UEFI、セキュア ブート対応。お使いの PC がこの要件を満たすようにする方法については、**こちら**をご覧ください。
TPM	**トラステッド プラットフォーム モジュール** (TPM) バージョン 2.0。お使いの PC がこの要件を満たすようにする方法については、**こちら**をご覧ください。
グラフィックス カード	DirectX 12 以上 (WDDM 2.0 ドライバー) に対応。
ディスプレイ	対角サイズ 9 インチ以上で 8 ビット カラーの高解像度 (720p) ディスプレイ。

【▲ Windows11のインストールするためのシステム要求事項 (参考：Microsoftホームページ)】

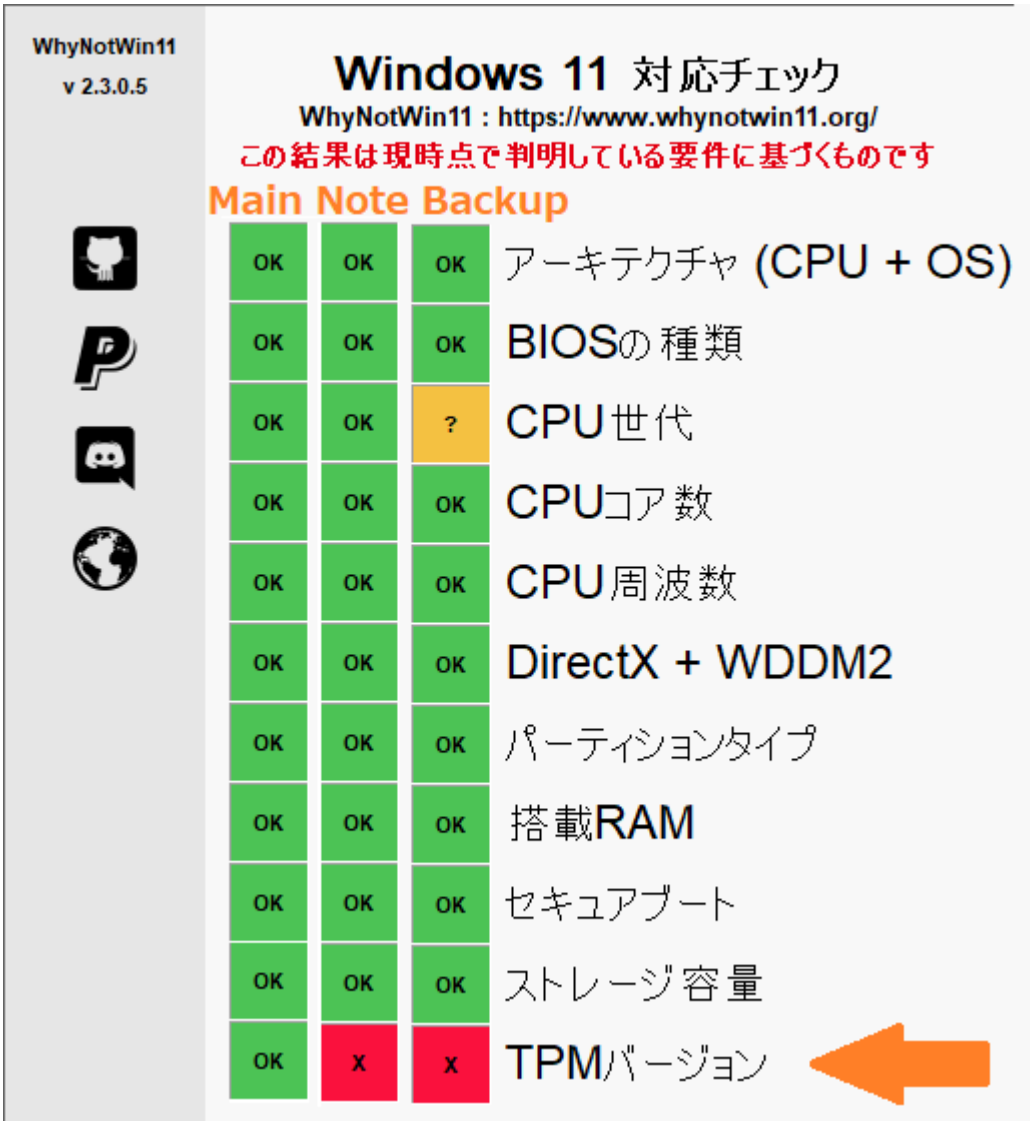
Windows 11の必須条件、TPMとは？

2) なにが話題になっているのか？

マイクロソフトから発表した公式の仕様でもWindows11を使うためにすごい性能のハードウェアは求められていない。仕様には特に問題はなく、既存Windows10を使用していたPCであればWindows11をインストールすることには問題がないと思われる。

しかしながら、一つややこしい要求事項がある。それは「TPM(信頼できるプラットフォームモジュール)バージョン2.0サポート」である。この条件で思ったより多くのユーザーのPCがWindows11のインストールができないと思う。

Windows11の発売とともに一番話題になっているのがTPM要求によるユーザーの混乱である。



【▲ Windows11をインストールためのシステム互換性(要求事項)確認結果 (参考：IoT MCUのHappyTech)】

Windows 11の必須条件、TPMとは？

03. TPMとはなんだろう？

1) TPMとは？

まず、TPMとはなんでしょう。どのようなものでWindows11のインストールに必須仕様として要求されているのでしょうか。TPMはTrusted Platform Moduleの略で、翻訳すると信頼できるプラットフォームモジュール(装置)を意味する。ハードウェア的はセキュリティ装置で、コンピューター内部に内蔵されていてセキュリティ機能を提供する暗号化専用プロセスである。このプロセスは暗号化作業を遂行するように設計されていてる。OS環境の改ざんなどを防止する様々なセキュリティメカニズムが含まれていてマルウェアがTPMのセキュリティ機能の改ざんができないようになっている。

【▲ Trusted Platform Module (Discrete TPM) (参考：https://www.ieiworld.com) 】

10年も超えたTPMプロジェクトはPC、サーバ、ネットワーク機器、スマートフォン内部に別途チップを作り、そこに暗号化機能のための公開鍵、秘密鍵、パスワード、電子証明などを全て入れようとするアイデアから始まった。ハッカーは当該のチップを物理的に盗まない限りハッキングができないようにしてセキュリティ問題をハードウェア(HW)的な方法で解決しようとする。簡単な例としてスマートフォンのUSIMをセキュリティ用で活用することと似ている。

Windows 11の必須条件、TPMとは？

2) TPMの規格及び違い

TPMは1.2と2.0の規格が存在する。TPMは2007年7月9日に1.2(rev.1030)が発表されて、現在の最新バージョンは2.0である。TPM2.0は1.2と比べて機能が大幅に追加されており仕様も違う。
TPM2.0はより多様な暗号化アルゴリズムをサポートし、柔軟性を高めた。具体的にTPM1.2ではRSA及びSHA-1 HASHアルゴリズムだけ仕様されていたが、TPM2.0からはECCとSHA-2も追加サポートされてドライブ証明及びキー作成機能が改善した。また暗号化キー管理階層も1つから3つに増えて、コンピューター(PC)以外にもモバイル機器及び組込みシステムまでサポートできるようになった。
整理すると、TPM2.0はより強力な暗号化ともっと多いセキュリティ及び最新アルゴリズムに対するサポートを提供する最新技術である。

＊TPMに使用されている多様なアルゴリズムリスト(TCG Algorithm Registry)
- http://www.trustedcomputinggroup.org/resources/tcg_algorithm_registry
＊TPM2.0に対する必須アルゴリズムリスト(PC Client Platform TPM Profile)
- http://www.trustedcomputinggroup.org/resources/pc_client_platform_tpm_profile_ptp_specification

アルゴリズムタイプ	アルゴリズム名	TPM 1.2	TPM 2.0
非対称	RSA 1024	はい	オプション
	RSA 2048	はい	はい
	ECC P256	いいえ	はい
	ECC BN256	いいえ	はい
対称	AES 128	オプション	はい
	AES 256	オプション	オプション
HASH	SHA-1	はい	はい
	SHA-2 256	いいえ	はい
HMAC	SHA-1	はい	はい
	SHA-2 256	いいえ	はい

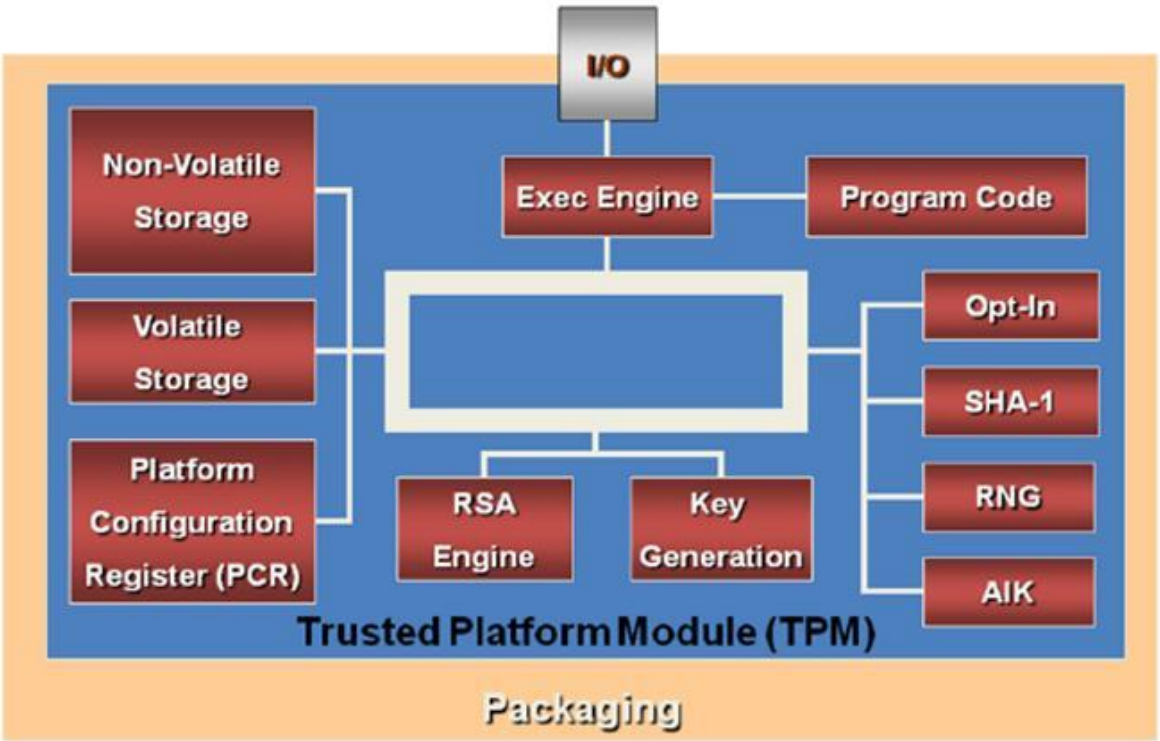
OS区分		TPM 1.2	TPM 2.0
Windows	7	はい	いいえ
	8	はい	はい
	8.1	はい	はい
	10	はい	はい
Linux	RHEL	いいえ	はい
	Ubuntu	いいえ	はい

【▲ TPM1.2とTPM2.0の比較】

Windows 11の必須条件、TPMとは？

3) TPMの構造(アーキテクチャ)

TPMは大きくコマンド処理エンジン(Exec Engine)、暗号化エンジン、非揮発性及び揮発性メモリに構成されている。非揮発性メモリにはTPMチップが作られるとき付与された固有なキー(EK, SRK)などが保存されていて、このキーは外部に漏出されないようになっている。コマンド処理エンジンからはチップOSとTPMコマンドを遂行し、その際、揮発性メモリに保存されている暗号化キーと暗号化エンジンを使用してデータを暗号化・複号化及び各種の認証を行う。このようにTPMはハードウェア的にメインシステムと分離されて外部からのアクセスを遮断することでマルウェア(Malware)のようなソフトウェア攻撃から暗号化キーとデータを安全に管理することができる。整理すると、TPMチップはハードウェアであるため、システムのメモリに情報が漏出されないため、ハッカーの攻撃が難しいである。



【▲ Trusted Platform Module Architecture (参考：https://resources.infosecinstitute.com)】

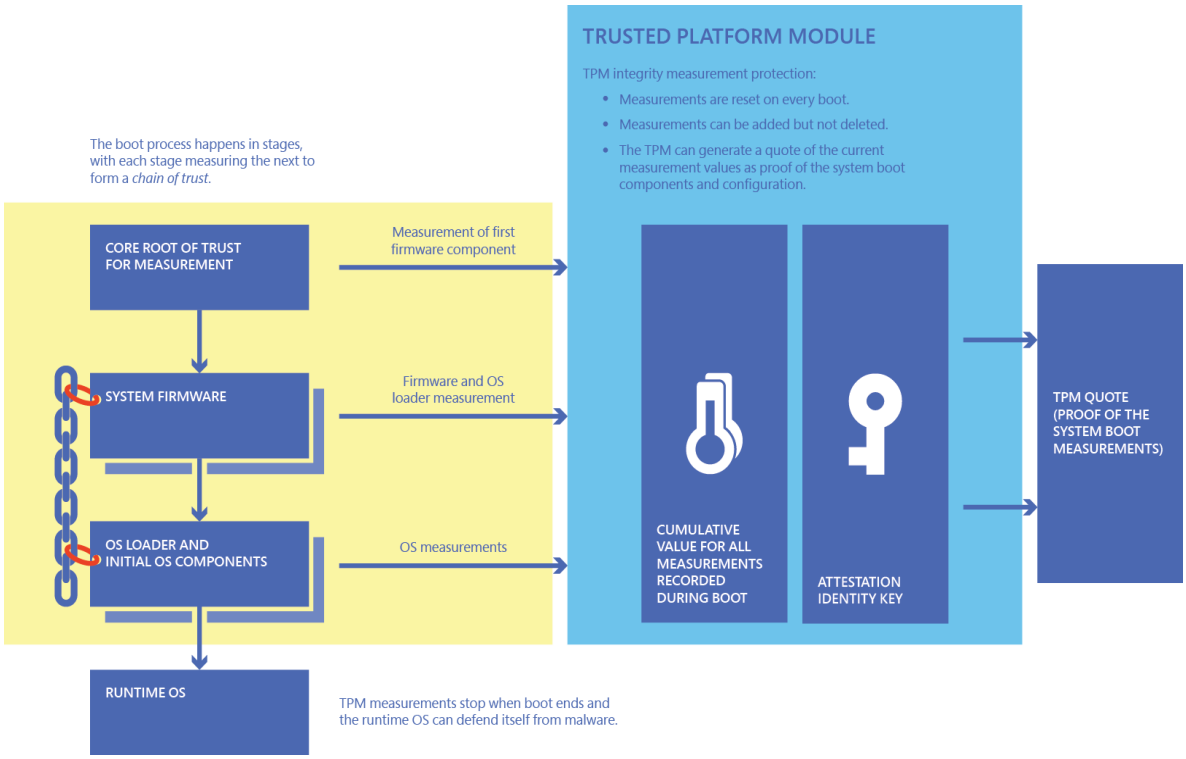
Windows 11の必須条件、TPMとは？

4) TPMの主要機能

TPMは外部からアクセスができない安全な場所にキーを保管し、内部から暗号化演算を遂行するように設計されたハードウェア装置(チップ)である。TPMの内部に暗号化されたデータは暗号キーを持っているTPMだけ複合化ができる。この特徴を利用して暗号化キーを作成し、管理してBIOS及びOSを修正(改ざん)できないように保護する補助プロセスの役割をする。TPMは色々なセキュリティ機能を提供し、用途が広範囲で主に機器の識別、認証、暗号化及び機器の整合性の検証などに使用される。主要機能は以下になる。

① 運用環境(プラットフォーム)の整合性

OSと関係なく、すべてのコンピューター装置の整合性を保障する機能を遂行する。ブートプロセスからハードウェアとソフトウェアの信頼できる組み合わせで起動されているかを確認及び記録し、以前に保存した内容と比較して情報が一致しているか検証する。その結果、改ざんされていない場合だけシステムを使用できるようにする。



【▲ TPMを活用したOS(Windows)整合性検証機能 (参考：Microsoftホームページ)】

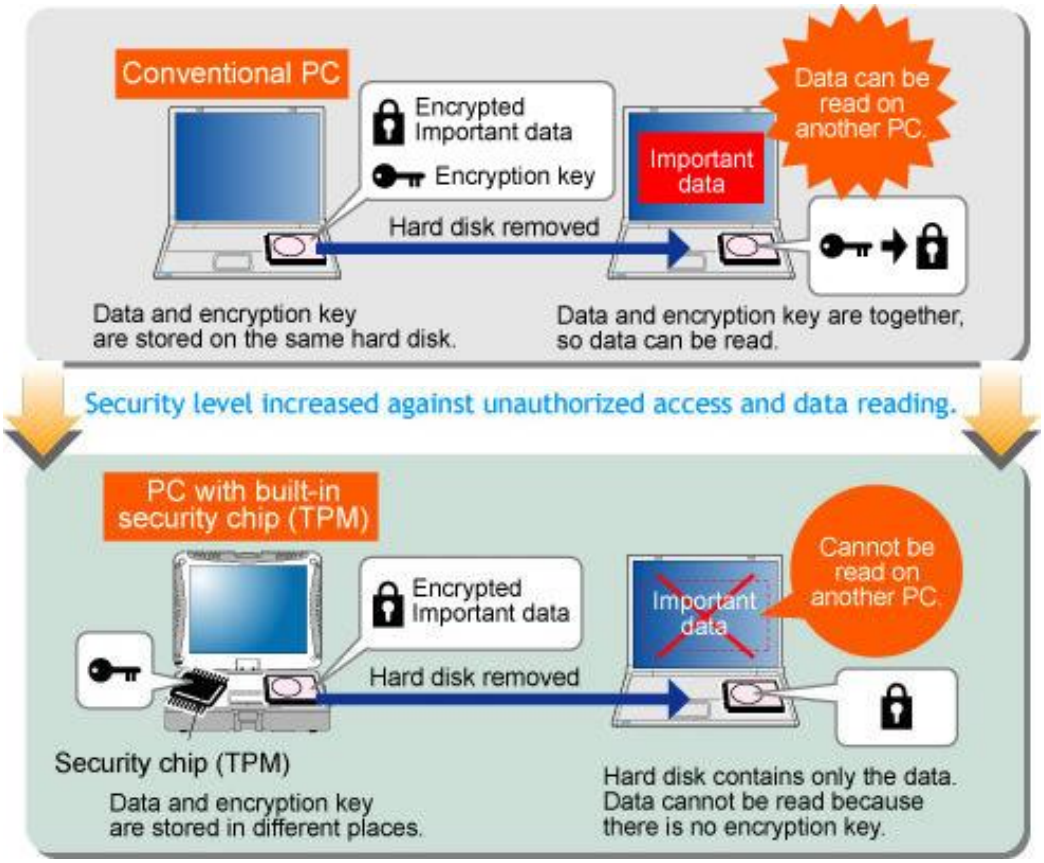
Windows 11の必須条件、TPMとは？

② 記憶装置(ハードディスクなど)の暗号化

TPMの技術で装置(PC)の全てのハードディス、USBのような記憶装置を暗号化してデータを保護することができる。一番代表的な例としてWindowsのBitLocker(ビットロッカー)機能である。Full Disk Encryption(FDE)技術と呼ばれて特定のフォルダやファイルではない記憶装置(デバイス)もしくは、パーティション全体を暗号化することが特徴で、ここで使用される暗号化キーを保護するためにTPMを利用している。

③ 資格証明(認証情報)の保存及び管理

OSから一般的にキー、データまたはシステムを保護するための認証(暗号やその他の方法を含め)が必要であるが、このような認証情報(暗号)を保存する際、使用される資格証明、認証書及び暗号化キーを保存する物理的に安全な場所を提供する。TPMはメモリ(シェル)に保存され、情報の損失がなく、プロセスと得点的に通信することが可能で、他のハードウェアの構成要素がプロセスの許可なしでアクセスすることができないため、安全である。



【▲ TPMを活用したデータ(ディスク)の暗号化及びキー保存機能 (参考：個人ブログ- kthan.tistory.com)】

Windows 11の必須条件、TPMとは？

5) TPMのタイプ

TPMはタイプごとに5種類があって、それぞれの動作方法は以下になる。

① Discrete TPM(分離型)

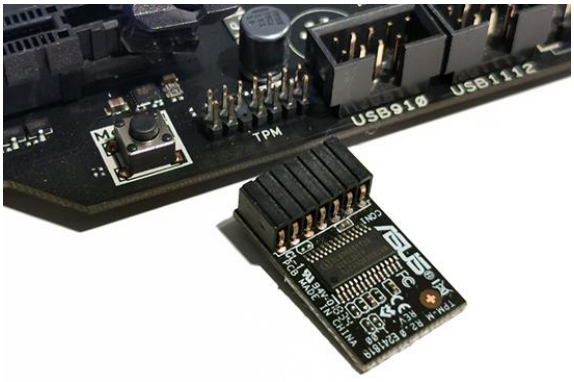
dTPMは別途、分離されたモジュールの形で出てる製品の中で最も使用されるタイプで装置(ボード)の専用ピンヘッダーにTPMモジュールを装着する方法である。装置メーカーから大体デフォルトではなく、オプションとして提供しているため、別途購入して装着すると使用できる。一般のPCによく使われている方法である。

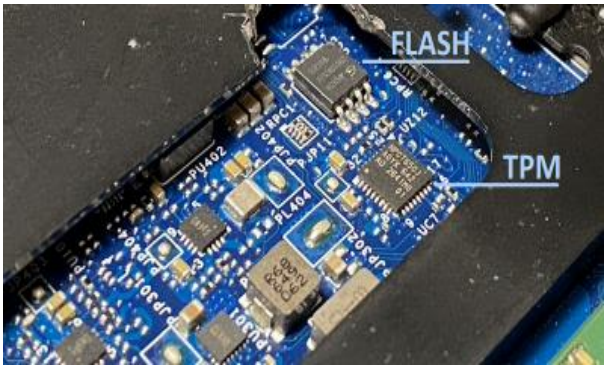
② Integrated TPM(統合型)

iTPMは別途分離さているのではなく、TPMモジュールをデフォルト的に装着し、作られて統合されたタイプで、主に企業用のノートパソコンに使用される。

③ Firmware TPM(ファームウェア型)

fTPMはマザーボードのファームウェアを利用するソフトウェアの方法でTPMを利用する方法でCPUの信頼できる環境から実行される。従って、ソフトウェアバグに脆弱性が発生する可能性がある。





【▲ Discrete TPM(右) / Integrated TPM(左) / Firmware TPM(下) (参考：Googleイメージ検索)】

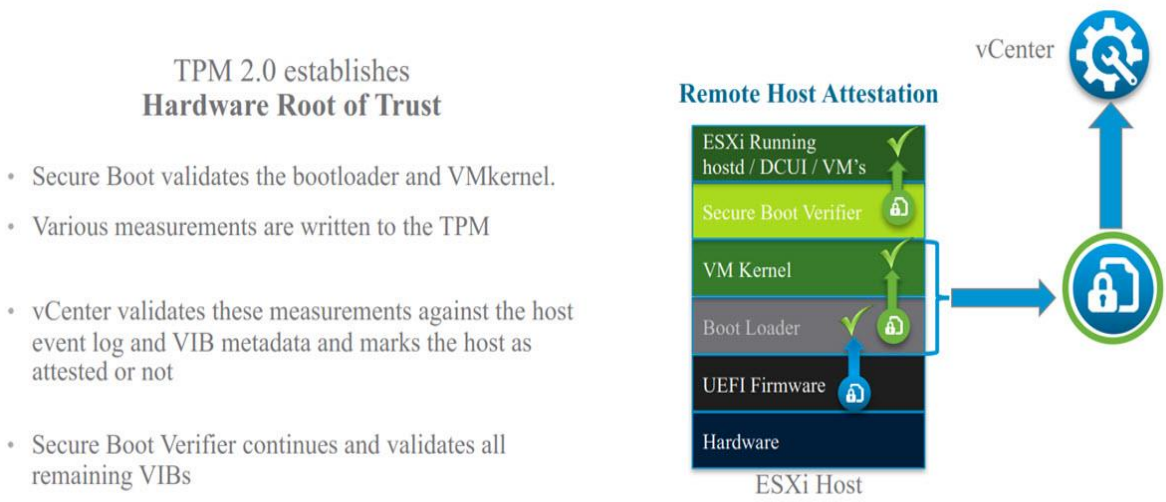
Windows 11の必須条件、TPMとは？

④ Software TPM(ソフトウェア型)

sTPMはソフトウェアで似たような動作をするように作られたエミュレーター方法のTPMである。OS内から一般プログラムとして動作し、実行される環境に完全依存する。一般実行環境から提供するセキュリティより機能が少なく、ソフトウェアのバグやマルウェアなどの攻撃に脆弱である。主にTPMを開発するための目的として使用される。

⑤ Hypervisor TPM(ハイパーバイザー型)

hTPMはハイパーバイザーから提供してこれに依存する仮想のTPMである。ハイパーバイザーは仮想マシンのソフトウェアからコードを保護するために仮想マシンソフトウェア内部に隠された隔離された環境から実行されて、fTPMと似たようなセキュリティを提供する。



【▲ Hypervisor(vSphere, ESXi, vCenter) TPM (参考：https://blogs.vmware.com)】

Windows 11の必須条件、TPMとは？

04. Windows11はなぜTPMを要求しているのか？

Windows11を使うためにはシステムからTPM2.0を提供しなければならない。ユーザーからするとかなり困ることであるのが、なぜマイクロソフトはこのような難しい条件を要求しているのか。

マイクロソフトがTPM2.0規格を強制化した理由は、フィッシング、ランサムウェアのように持続的に増加している高度化されているサイバー犯罪に対応するためである。公共網攻撃のように日々進化しているサイバー犯罪にTPMを内蔵したPCはレベル高い防御性能をみせるためである。

マイクロソフトは公式ブログから「未来にはランサムウェアのように巧妙で強力なセキュリティ脅威に対応するために信頼できるハードウェアが必要である。」と言いながら「TPMは暗号化キーユーザー資格証明及びその他の重要なデータをハードウェアの壁の後ろから保護すること。」で言った。また、「Windows11がTPM2.0を要求するのは信頼できる内蔵機能からハードウェアのセキュリティレベルを高める意味がある。」と言いながらTPMの重要性を強調した。

マイクロソフトは今まで、仮想化と共にハードウェア及びファームウェアのセキュリティ結合を試したりするなどPCプラットフォーム改善を行っていたが、それを一層発展させることができる丈夫な基盤が必要であり、TPMがそれの回答だと思っている。

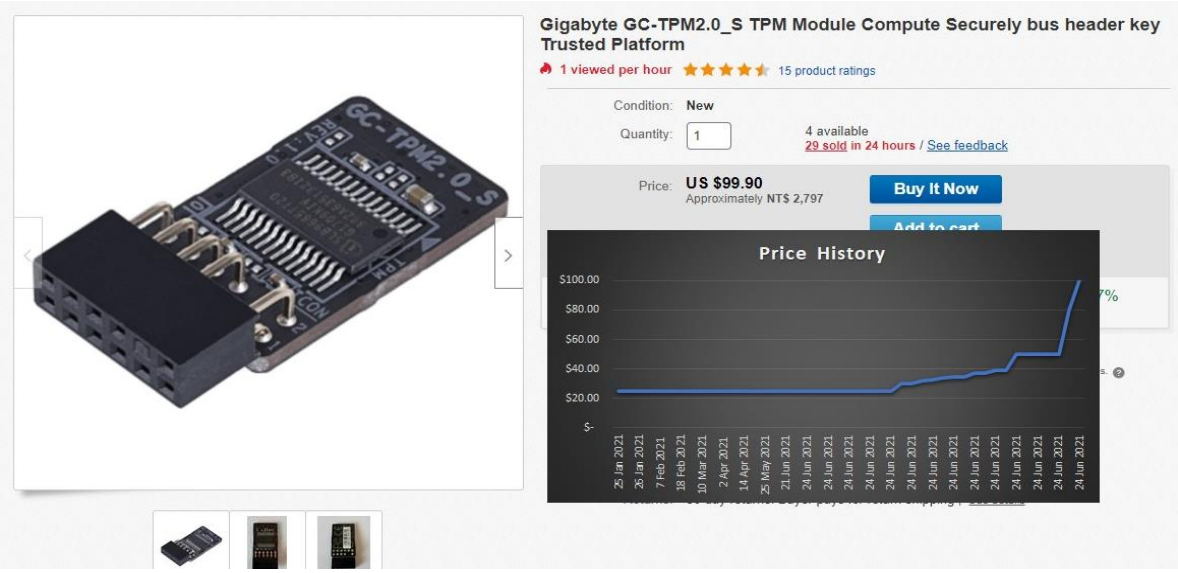
＊Microsoftが公式ブログで発表したTPMの重要性
- https://www.microsoft.com/security/blog/2021/06/25/windows-11-enables-security-by-design-from-the-chip-to-the-cloud/
- https://www.microsoft.com/security/blog/2021/10/04/windows-11-offers-chip-to-cloud protection-to-meet-the-new-security-challenges-of-hybrid-work/

【▲ 多様なサイバー攻撃を防ぐためのMicrosoftno対応方法 (参考：Microsoft公式ブログ)】

Windows 11の必須条件、TPMとは？

05. TPM2.0、私のPCには準備されているのか？

PCを購入してから時間が経っており(TPM1.2のみサポート)TPM2.0が準備されていないのであれば別途、モジュールを購入して装着することができる。しかし、6月上旬には1個で約20ドルであったモジュールが今は約100ドルに暴騰し、一部のメーカーの製品は供給が中止されている。Windows11がTPM2.0を義務化することで品薄現象が起きている。



【▲ TPM2.0強制化により急上昇したモジュール値段 (参考：Amazon.com)】

最近販売されたPCを購入したらTPM2.0モジュールを買う必要はない。今までTPMはPCのマザーボードから分離されたタイプが普通だったが、最近はCPUの中に機能を統合している。5年内に販売されたほぼ全てのCPUがPTT(Intel)、fTPM(AMD)という名前で既にTPMが含まれているため、PCのBIOS設定から有効にすることで機能を使える。

Windows 11の必須条件、TPMとは？

06. Windows11とTPM2.0、今すぐ必要であるのか？

セキュリティ強化のためにはTPM2.0が必要である理由はもう知っていると思う。実はマイクロソフトは2016年、Windows10を販売した時もTPM2.0が必要だと言っていた。しかしこの時はだたの推奨ということだったが、Windows11からはセキュリティ強化のために必須条件になって義務化されただけである。

つまり、TPM2.0をサポートしない旧型PCには別途、モジュールを購入して装着すればいいし、最近購入したPCなら既にTPMが搭載されているため、当該の機能が使えるように有効かすることで必須条件は満たせる。

では、今残っている問題は「すぐ、私にWindows11が必要であるのか？」である。
Windows Hello, BitLocker, Credential Guardなどのハードウェア基盤セキュリティを活用したWindows11の機能が必要であれば今すぐTPMを購入するもしくは、有効化する必要があって、そうではない場合は急いで購入する必要はない。

さらに、Windows10のサポート期間も2025年で、まだ4年も残っているため、無理してハードウェアをアップグレードする必要はない。またWindows11はまだ初期の状況だし、CPU及びアプリケーションの互換性など様々な問題を解決する必要があるため、今すぐWindows11にアップデートするメリットを感じるためにはもう少し時間が必要である。

従って、Windows11のために現在のシステムと互換される別途のTPM購入する必要はないし、混乱を避けるためにはしばらく安心してWindows10を使用するのを推奨する。

07. 参考資料

[1] https://www.microsoft.com/ko-kr/windows/windows-11-specifications
[2] https://www.microsoft.com/security/blog/2020/02/03/guarding-against-supply-chain-attacks-part-2-hardware-risks/
[3] https://www.microsoft.com/security/blog/2021/06/25/windows-11-enables-security-by-design-from-the-chip-to-the-cloud/
[4] https://docs.microsoft.com/en-us/windows/security/information-protection/tpm/how-windows-uses-the-tpm
[5] https://www.microsoft.com/security/blog/2021/10/04/windows-11-offers-chip-to-cloud-protection-to-meet-the-new-security-challenges-of-hybrid-work/
[6] https://zdnet.co.kr/view/?no=20140519124652
[7] https://quasarzone.com/bbs/qc_plan/views/26997
[8] https://byline.network/2021/06/28-149/
[9] https://www.easeus.co.kr/partition-manager-software/tpm-for-windows11-update.html
[10] https://www.itworld.co.kr/opinion/199349
[11] https://www.itworld.co.kr/news/199224
[12] https://www.itworld.co.kr/howto/199874
[13] https://www.itworld.co.kr/news/200024
[14] https://www.itworld.co.kr/news/212664
[15] https://zdnet.co.kr/view/?no=20210706153245
[16] https://www.dell.com/support/kbdoc/ko-kr/000131631/tpm-1-2%EC%99%80-2-0%EC%9D%98-%EA%B8%B0%EB%8A%A5-%EB%B9%84%EA%B5%90
[17] https://www.itfind.or.kr/WZIN/jugidong/1279/127902.pdf
[18] https://www.koreascience.or.kr/article/JAKO201421762413471.pdf
[19] https://happytech.jp/wordpress/2021/07/16/windows-11-shock-and-tpm/