ADVANTECH Microsoft

Windows 11 IoTをアップデートする前に

11 考えておきたいのこと

Index

■ はじめに 01

■ Windows11 IoT アドバンテックによる6つの検証レポート 02

-USB 4.0とWi-Fi 6をサポートし、高速なデータ転送速度を実現。
- TPM 2.0って必要？TPM 2.0を使わずにWindows 11 IoTをインストールする方法は？
-ブートセクターに変更は？/ Linuxアプリの実行には対応しているの？
-包括的なデータセキュリティとアップグレードプログラム
-Gatekeeperでセキュリティ強化、Teamsも活用できる！

■ エキスパートが答える！選ぶ前に確認したい5つの質問 08

-ハードウェアとソフトウェアの基本的な環境要件は？
- Windows 10 IoTからWindows 11 IoTへの更新はどんな時におすすめ？
- Windows 11 IoTの導入で最も恩恵を受ける具体的な業種とその理由とは？
-アドバンテックのWindows向けのキオスクモードの使用感について教えて。
-導入前に、サポート期間など気をつけるべきことはありますか？

■ Windows 11 IoTのfTPMアクティベーションを行うには？ 14

はじめに

Windows 11 IoTへアップグレードしなきゃいけないの？

産業デバイスへWindows 11 IoTを導入したいと考えている方は多いと思いますが、
「新機能をどのように活用するのか」「自分のデバイスが対応しているのか」といった疑問が生じています。そのため、Windows 11 IoTには、どのような新機能や制約があるのか？
また、Windows 11 IoTを用いる上で、アドバンテックはどのような検証を行い、
お客様にどのようなアドバイスをしているのでしょうか？

アドバンテックは、こうした疑問に答えるべく、自社のIPCプラットフォームへ
Windows 11 IoTを採用し、検証テストを実施しました。

このカタログでは、Windows 11 IoTの性能や規約や検証内容、Windows 11 IoTを実際に使用する企業へアドバンテックがどのようなアドバイスをしているのかを含む、6つの検証レポート・Windows 11 IoTを採用する前に確認しておきたい5ポイントをまとめています。

Windows 11 IoT

6 アドバンテックによる つの検証レポート

【検証レポート①】

USB 4.0とWi-Fi 6をサポートし、高速なデータ転送速度を実現。

この新しいリリースでは、最大 40 Gbps のデータ転送速度を提供できる最新世代の USB 4.0をサポートしています。
また、無線ネットワークも大幅にパワーアップし、6GHz帯のWi-Fi 6E を正式にサポートしています。
これにより、コンピューティングデバイスは 前世代の Wi-Fi 6 よりも高速な伝送速度を提供でいるようになります。

さらに、インターフェースのデザインを一新し、よりすっきりとしたモダンなデザイン・操作性を実現しています。

USB通信比較マップ

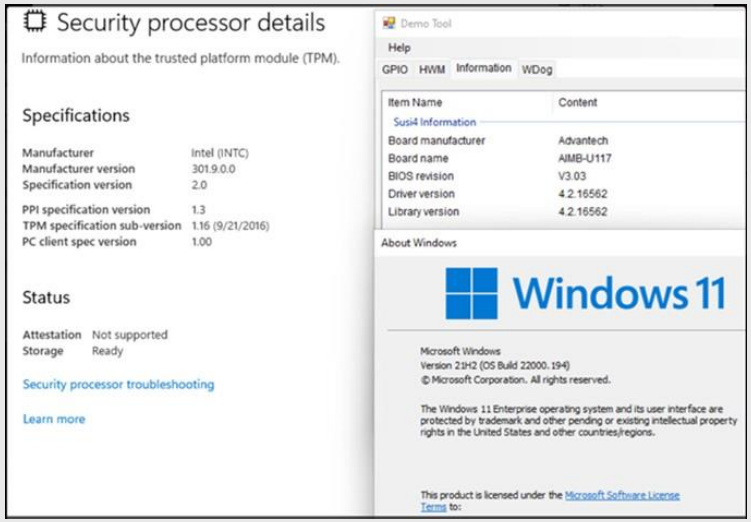
USB規格	最大スループット	ブランド/ロゴ総称
USB 2.0	480 Mbps	High Speed
USB 3.0	5 Gbps	Super Speed USB3.1 Gen1/USB3.2 1x1
USB 3.1	10 Gbps	Super Speed USB3.1 Gen1/USB3.2 1x1
USB 3.2	20 Gbps	Super Speed USB3.1 Gen1/USB3.2 1x1
USB 4	40 Gbps	Undisclosed

【検証レポート②】

TPM 2.0って必要？TPM 2.0を使わずに Windows 11 IoTをインストールする方法は？

Microsoftのサポート ドキュメントによると、ユーザーがレジストリに簡単な変更を加えて Windows 11 IoT デバイスをアップグレードし、TPM セキュリティ チェック メカニズムをスキップすると、デバイスがハードウェア標準を満たしていないことを示す警告を表示します。
この警告はさらに、サポートされていないデバイスで Windows 11 IoT を実行すると互換性の問題が発生すること、および問題が発生した場合、そのような問題によりメーカーの保証が無効になる可能性があることを示しています。

しかし、アドバンテックの検証結果によると、 Windows 11はハードウェアTPM2.0だけでなく、
ファームウェアTPM 2.0でも正常に動作することが確認されています。
つまり、第8世代Intel CPU及びそれ以降のバージョン、AMD Ryzen 2000及びそれ以降のバージョンを搭載したコンピュータデバイスでは、BIOS設定からファームウェアTPM 2.0機能を有効にするだけで、スムーズに実行でき、警告メッセージは全く表示されなくなるのです。

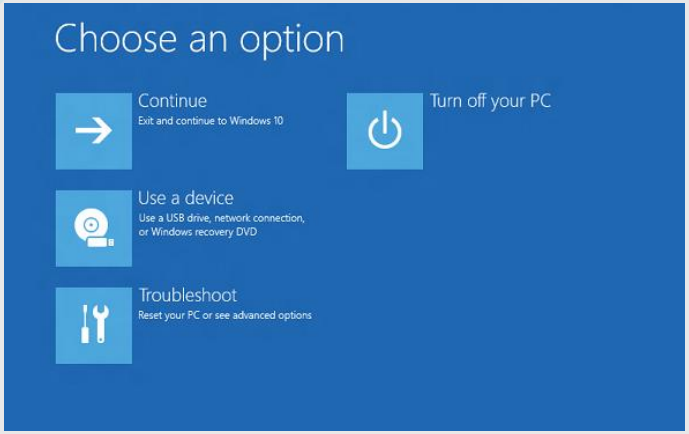


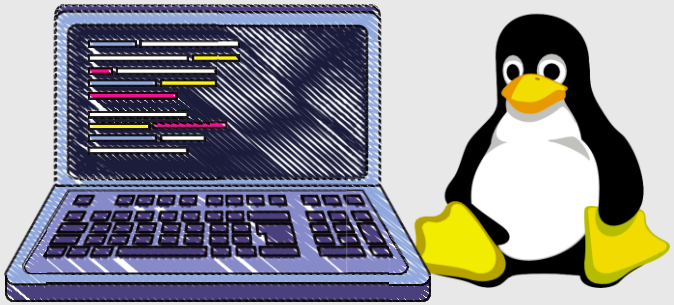
【検証レポート③】
ブートセクターに変更は？

バックアップ/リカバリーソフトウェアが既にインストールされている場合、Windows 11 IoT は UEFI 起動モードをサポートするために、MSR と呼ばれる新たなパーティションを作成します。
しかし、Windows回復環境(Windows RE)を使用していた方は、新しいパーティションがブートローダーの誤動作を引き起こす可能性があることに注意する必要があります。

【検証レポート④】
Linuxアプリの実行には対応しているの？

Windows 11 IoT は、Windows Subsystem for Linux GUI (WSLg)をサポートしており、Linuxで開発されたアプリケーションをソースコードを変更することなく実行することができます。





【検証レポート⑤】
包括的なデータセキュリティとアップグレードプログラム

Windows 11 IoT は、VBS、HVCI、およびセキュア ブート機能を強化し、ユーザーのプログラムとデータの整合性とセキュリティを保証します。

VBS（仮想化ベースのセキュリティ） は、ハードウェア仮想化機能を使用して、OSから分離された安全なメモリ領域を作成します。また、「仮想セーフ モード」は、分離されたメモリ領域の保護を強化するいくつかのセキュリティ ソリューションを読み込むことができます。この仮想セーフ モードを用いることでOSの弱点を軽減し、ハッカーによる悪意のあるコードや実行可能なコードの使用を防止することが可能です。

HVCI（Hypervisor-enforced Code Integrity、メモリの整合性) は、VBS を活用しコードの整合性を強化します。Kernel-Mode Code Integrityは、カーネル モード ドライバーとバイナリを有効にする前にチェックすることで機能します。 これにより、承認された署名者によって署名された実行可能ファイルのみを有効にし、未署名のドライバーやシステム ファイルがシステムメモリにロードされるのを防止します。

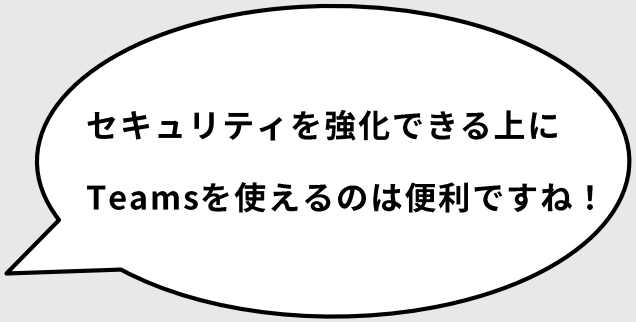
セキュア ブートは、PCの起動時にマルウェアがロードされるのを防止する重要なセキュリティ機能です。
ほとんどの新しいPCはセキュア ブートを実行できますが、設定によってはPCが安全に起動できない場合があります。
これらの設定は、PCで初めて Windows を実行する前に、BIOS セットアップを使用して起動時に調整できます。
ユーザーは、PCの起動モードを UEFI/BIOS に切り替え、セキュリティを強化するためにセキュア ブート オプションをオンにする必要があります。

【検証レポート⑥】

Gatekeeperでセキュリティ強化、Teamsも活用できる！

ユーザー アクセス ポイントにゲートキーパーを設定することは、クラウドのセキュリティにとって重要なポイントです。 ゲートキーパーは、不正なログイン試行をブロックし、AzureDPSでTPM X.509 認証情報を活用し安全なスタートアップ ネットワーキングを実現します。また、 ID 認証とプライバシーの観点から、Windows 11 IoT はパスワードなしのエントリを強化しました。 そのため、音声や指紋ログイン メカニズムがサポートされています。

さらに、Microsoft Teams などの数多くのアプリケーションをサポートしています。web会議機能やビジネスチャット、ファイル共有、ドキュメントの共同編集など、さまざまな機能が集約されているTeamsを活用できます。



エキスパートが答える！

5 選ぶ前に確認したい つの質問

【質問①】
ハードウェアとソフトウェアの基本的な環境要件は？

【回答】

基本的なハードウェア要件と、マッピング表です。
是非参考にしてみてください。

	CPU	RAM	Storage
Win 11 IoT	1Ghz, 2 cores	4GB	64GB
Win 10 IoT	1Ghz	1GB/32-bit, 2G/64-bit	16GB/32-bit, 20G/64-bit

【質問②】

Windows 10 IoTからWindows 11 IoTへの更新はどんな時におすすめ？

【回答】

基本的にソフトウェア更新は、TPMを活用してセキュリティを向上したいときにおすすめです。
また、顧客とのやり取りを行うアプリケーションをお持ちのユーザーにもアップグレードは必須です。
Windows 11 IoTでは、AIやUIもパワーアップされているので、おすすめですよ。

※現在、Windows 11 IoTは、LTSCの10年サポート版ではありません。サポート期間が短くなっています。

【質問③】

Windows 11 IoTの導入で最も恩恵を受ける具体的な業種とその理由とは？

【回答】

産業用タブレットやPOS サービス ソリューション、
HMI インタラクティブ市場向けに設計されたその他の
コンピュータデバイスなど、顧客とやり取りを行う業務で
これらのコンピュータデバイスを活用している業界は、
セキュリティ機能やUIが強化されたWindows 11 IoT の恩恵
を特に受けますね。

【質問④】

アドバンテックのWindows向けの キオスクモードの使用感について教えて。

【回答】

Windows 10 IoTのマルチキオスクモードは、複数のモードを同時に保存することができるので、状況に応じて異なるアプリケーションを実行することができます。
アドバンテックは、異なるシナリオに対応したマルチキオスクモードを素早く起動できる、付加価値の高いソフトウェアを提供していますが、Windows 11 IoTでは、マルチキオスクモードが提供されていません。Lockdown Utilityソフトウェアを提供し、単一アプリケーションのみを実行するユーザーのニーズをサポートするキオスクモードを可能にします。

【質問⑤】
導入前に、サポート期間など気をつけるべきことはありますか？

【回答】
Windows 11 IoTの組込み機能の多くは、
まだカスタマイズができません。
また、マルチキオスクモードやOSの長期サポートが必要な場合は、Windows 11 IoTを採用しないほうがよいでしょう。
また、周辺機器のドライバが Windows 11 IoT をサポートしているかどうかもあらかじめ確認してみてください。

Windows 11 IoTの ファームウェアTPM アクティベーションを行うには？

(第8世代CPU以降に限る）

Windows 11 IoT が登場からかなりの時間が経ちました。

しかし、Windows 11 IoTをインストールするために、システム内のTPMの要件は、

一部のユーザーにとって、非常に分かりにくいものです。

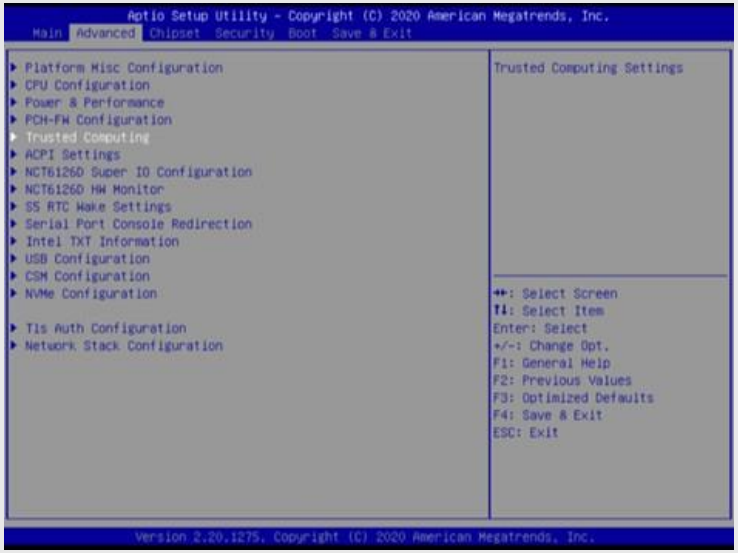
アドバンテックでは、この最新OSをインストールする際に、

お客様がより安心できるように、この状況を明らかにします。

アドバンテックからWindows 11 IoTと一緒にハードウェア製品を購入した場合、BIOS設定でファームウェアTPMを有効にすることができます。この場合、購入した製品に元々ハードウェアTPMが組み込まれていなくても、Windows 11 IoTをスムーズに動作することが可能です。

Windows 11 IoTをインストールする場合、
ファームウェアTPMを手動でアクティベートすることができます。

1. 起動時に“Delete”キーを繰り返し押しBIOS設定へ
2. “Advanced "メニューの "Trusted Computing "に切り替える



3."Security Device Support”を選択し、
「有効」であることを確認。

4. F10キーを押し、”Confirmed”を選択すると、保存され、システムが再起動されます。

キーワード

TPM Explained

Trusted Platform Module(TPM)は、Trusted Computing Group(TCG)というコンピュータ業界のコンソーシアムによって考案されたものである。
2014年4月9日、Trusted Computing Groupは「TPM Library Specification 2.0」と題した仕様のメジャーバージョンアップを発表しました。同グループでは、正誤表やアルゴリズムの追加、新たなコマンドを取り入れた規格の策定作業を続けており、2019年11月にISO/IEC 11889:2015として最新版の2.0を発行しています。

HW TPM Explained

ハードウェアTPM(HW TPM)は下記のベンダーによって実装。
Infineon、Microchip、Nuvoton、STMicroelectronics。

fTPM Explained

ファームウェアTPM(fTPM)は、CPUの信頼された実行環境で動作するファームウェアベース(UEFIなど)のソリューションである。
Intel、AMD、Qualcommが実装。

※Windows 11 IoT が 第8世代Intel CPU以降に余分なハードウェア TPM をインストールせずに対応することは、Intel と MS の両社がそれぞれの文書で発表しています。
インテル社のドキュメント：https://www.intel.com/content/www/us/en/support/articles/000007452/intel- nuc.html
マイクロソフト社のドキュメント：https://docs.microsoft.com/zh-tw/windows/security/information- protection/tpm/tpm-recommendations

東京本社

〒111-0032
東京都台東区浅草6-16-3
TEL:03-6802-1021　FAX:03-6802-1022

名古屋支店

〒460-0008
愛知県名古屋市中区栄4-3-26 昭和ビル 9階
TEL:052-241-2490　FAX:052-241-2491

大阪支店

〒542-0081
大阪市中央区南船場1-10-20 南船場M21ビル 6階
TEL:06-6267-1887　FAX:06-6267-1886

直方事業所

〒822-0006
福岡県直方市上境飛熊2770
TEL:0949-22-2811 FAX:0949-22-2836

Contact Us

E-Mail　：AJP.EIoT.AOL@advantech.com

電話番号　：0800-500-1055 (フリーコール)

オンラインストア

https://buy.advantech.co.jp/

故障・修理に関するお問い合わせ

https://www2.advantech.co.jp/support-AJP/repair.asp

ADVANTECH