



2025年10月14日

非サポート環境の運用リスク VS アップデートの生産性向上と競争力強化!

# Windows 10サポートが終了しました。

## すでに現在、Windows10のアップデートもサポート受けられません。

つまりセキュリティインシデントやOSの障害・不具合にはMicrosoftは責任を持たないということです。

アップデートにより 脆弱性リスクを抑制しつつ、日々の業務を速く・正確に!



### 日経新聞の記事から引用!



**「Windows10サポート終了 企業PCなお1割が利用、高まる攻撃リスク」**日経新聞は10月14日付で上記の見出しの記事を掲載しました。(以下記事の要約)

10月14日にWindows 10のサポートが終了し、以後は脆弱性修正が出ないため攻撃リスクが急増します。国内では企業PCの約1割(全体で約2割弱)が依然Win10のままで、対応は「Windows 11へ迅速に移行」か「有償の拡張セキュリティ更新」の二択ですが、2017年以前のPCは11非対応が多い点に注意が必要です。日本企業へのランサム攻撃が増加・巧妙化しているなか、OS更新を軸に資産の最新化と常時監視を組み合わせた総合防御への早急な転換が求められます。

参照元: 日本経済新聞10月14日掲載(有料会員記事) <https://www.nikkei.com/article/DGXZQUC10AY40Q5A011C2000000/>



### OSサポート終了を“経営改革の起点”に



OSのサポート終了を単なる「パソコンの入れ替え」としてではなく、お客様の将来にも関わる大切な「経営課題」としてお考えいただくためにお届けします。サポートが終了したOSを使い続けることの具体的なリスクと、これを機に新しい環境へ移行することで得られる経営上のメリット(セキュリティ強化、業務の効率化、コスト最適化)について、分かりやすくご説明いたします。

#### 1.サイバー攻撃への最大のリスク

- サイバー攻撃の標的が、大企業から「私たち中小企業」へと移っています。  
昨今、日本企業が海外の攻撃者によって、被害を受けたニュースは記憶に新しいと思いますし、まだ完全な復旧ができていないと聞いています。
- サイバー脅威は質的に変化し、攻撃が日常的になっています。  
2025年の調査(帝国データバンク)によれば、日本企業の3社に1社にあたる32.0%が、過去に何らかのサイバー攻撃の被害を経験していることが明らかになりました。同調査レポートは「**足元では中小企業のサイバー攻撃に対するリスクが急速に高まっている**」と明確に警鐘を鳴らしています。
- 「**うちは規模が小さいから狙われない**」という認識が、もはや全く通用しない現実を示しています。  
警察庁の発表でも、中小企業のランサムウェア(身代金要求ウイルス)被害が前年比で37%も増加したと報告されており、攻撃者はセキュリティ対策が手薄な中小企業をあえて狙っていることが強く示唆されます。
- お客様自身が「**最終的な標的**」となる場合、あるいは大手取引先へ侵入するための「**踏み台**」(サプライチェーン攻撃)として悪用される場合に関わらず、サポート切れのOSを使い続けることは非常に危険です。  
これは、自社だけでなく、大切な取引先全体を危険に晒す重大な経営リスクとなることをご理解ください。



#### もう一度!! リスクの再確認 Windows 10を「このまま使い続ける」ことの 本当の代償

- サポート終了で、パソコンの「セキュリティの穴」は絶対に塞げなくなります
- 2025年10月14日を過ぎると、Windows 10には、新しい危険からパソコンを守るための「修理プログラム(セキュリティの更新)」が原則として届かなくなります。
- たとえ最新のウイルス対策ソフトを入れていても、OSそのものに見つかった「設計上の欠陥(セキュリティの穴)」が直されないまま放置されることを意味します。
- IPA(情報処理推進機構)の調査でも、企業を狙う危険の第1位は「ランサムウェア(身代金要求)による被害」です。サポート切れのOSは、新たに発見された「穴」を狙うランサムウェアや、被害の多くを占めるフィッシング攻撃にとって、これ以上ない格好のターゲットとなってしまいます。
- 例えるなら、「**玄関の鍵が壊れているのを知りながら、その鍵を使い続ける**」のと同じ状態です。攻撃者に「どうぞ入ってください」と侵入を誘っているのと同じく、極めて危険な経営判断となります。



## 2.「守り」の進化

●Windows 11と最新パソコンで実現する、何重もの強力な防御！  
Windows 10を使い続ける危険性が明らかになる一方で、Windows 11と新しいパソコンへの切り替えは、単にリスクを避けるだけでなく、将来の攻撃にも負けない、頑丈な「守り」の土台を作り上げます。

●OSが土台から守る:Windows 11が義務付けた、パソコン自体の安全機能  
Windows 11は、単なる見た目や機能が変わる「表面的な更新」ではありません。TPM 2.0(パスワードなどをパソコン内の専用チップで保護)や、VBS(OSの中心部分を特別な技術で隔離して守る)といった機能を、必ず備えていることを条件にしています。

パソコンの電源を入れる前から電源を切るまで、OSとパソコンの部品が一体(一つのチーム)となって安全を守る「頑丈な土台」を強制的に作るようになります。従来のWindows 10のように、後からウイルス対策ソフトを「付け足すだけの防御」とは、考え方自体が根本的に違うのです。



●パソコン自体の防御力:AIが危険を見つけて閉じ込める「自分で守れるPC」  
新しいビジネス用パソコンは、OSでは守りきれない部分、特に電源を入れた直後の基本ソフト(BIOS)の段階や、私たちが使うアプリのレベルでの防御機能を、パソコンの部品自体に最初から組み込んでいます。例えば、HPのビジネス向けAI PCに入っている「HP Wolf Security」という仕組みは、パソコンの隅々まで(基本ソフト、アプリ、外部機器まで)何重にも保護します。



参照元:日本HP\_Webサイト <https://jp.ext.hp.com/business-solution/security/?msocid=2d51b0dfbfc61ee0ba3a32bbe6f6085>

●クラウドとの協力体制:いつでもどこでも安全な「ゼロトラスト」の仕組み  
Windows 11と新しいパソコンへの切り替えは、「ゼロトラストセキュリティ」の1つです。

## 3.「攻め」の基盤:AI時代の仕事のやり方を変える、最新パソコンの力

■AI活用競争の本格化:生産性向上のチャンスと、セキュリティ上の新たな課題  
生成AIによる業務革新の波です。AI活用はもはや大企業の特権ではありません。例えば、専門知識がない社員でもAIを活用できるよう「ひな形(テンプレート)」の活用や、社内ドキュメントとの連携を進めることで、実際にメール作成時間を大幅に短縮したり、資料作成時間を約半減させたりといった、高い生産性向上の効果が報告されています。

AIの利便性を追求すると、機密情報の漏えいリスクが高まるというトレードオフの関係が生まれます。

AIに業務を任せると、「入力したデータが外部に流出しないか」という不安は、中小企業が抱える大きな懸念です。このため、一部のサービスでは「入力情報を学習に利用しない」「データは国内で管理する」といったセキュリティ対策が講じられています。



### まとめ

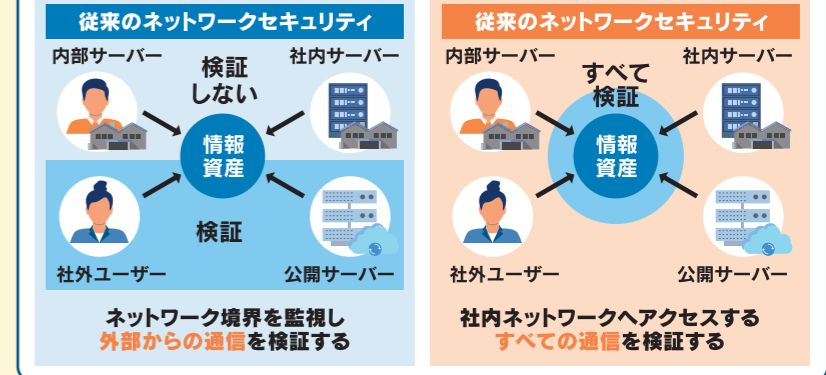
「いま決める」ことが最大のリスク対策であり、未来への投資です!  
Windows 10のサポート終了は、単なる入れ替えではありません。

「放置はリスク!移行は投資!」とお考え下さい。  
ランサムウェア等のサイバー攻撃の被害という大きな危険を回避し、AI時代に生産性を上げるためのスタート地点に立つための、会社全体の「重要な経営課題(将来のための投資)」として捉える必要があるのです。



## ゼロトラストセキュリティとは?

### ●ゼロトラストとは



「何も信用しない」を前提にした新しい安全対策  
これまでのセキュリティ対策は、「会社のネットワークの中に入ってしまう安全」という考え方が中心でした。

ゼロトラストの核は、「何も信用しない、常にすべての安全を確認する」という原則です。

アクセスが社内の人からであっても、会社のパソコンからであっても、すべてのアクセスに対して「このアクセスは本当に安全か?」と厳しくチェックすることを徹底します。現代のビジネスでは、クラウドサービスを利用し、オフィス外で仕事をするのが当たり前になりました。ゼロトラストは、このような多様な働き方(どこからでもアクセスできる環境)を安全に保つための、最も強力な土台となります。

「Windows 11」や最新のAI PCは、このゼロトラストに必要な機能を複数備えており、さらにID管理も徹底することで、ゼロトラストセキュリティの実現に1歩も2歩も近づきます!

最近話題の「AI PC」(AIパソコン)とは、AI(人工知能)の処理を専門的に行う「NPU(AI専用チップ)」を搭載した新しいタイプのパソコンのことです。

このチップのおかげで、インターネット上のクラウドに頼らず、パソコンの中でAIを高速かつ低電力で動かすことができます。

これは、仕事の進め方を大きく変えるための新しい土台となります。

OS・デバイスの更新は、単なる「守り」の費用で終わりません。それは、AIを使った今までにない大きな生産性向上の波に乗るための、「攻め」の土台(プラットフォーム)を手に入れることを意味します。

### NPU搭載PCがもたらす4つのメリット

- AIアプリケーションの処理速度向上
- CPUの負荷軽減によるシステム全体の快適化
- 省電力化によるバッテリー駆動時間の延長
- オフライン環境でのAI処理によるセキュリティ強化

ぜひ、ご相談ください!  
御社のDX伴走パートナーであり続けます。

