
# 激化する現代のサイバー脅威を克服する

新しい Windows 11 Pro 搭載デバイス とセキュリティ対策を初期状態から有効にした戦略

Windows 11 Pro

目次

# あらゆるビジネスチャンスを獲得

絶え間なく進化するセキュリティ脅威状況は前代未聞の規模で課題を生み出しています。企業は、フィシングやランサムウェア、DDoS (分散型サービス拒否攻撃)などの複雑な脅威と格闘しています。これらの脅威は激化を続け、ますます強固な防御態勢を必要としています。

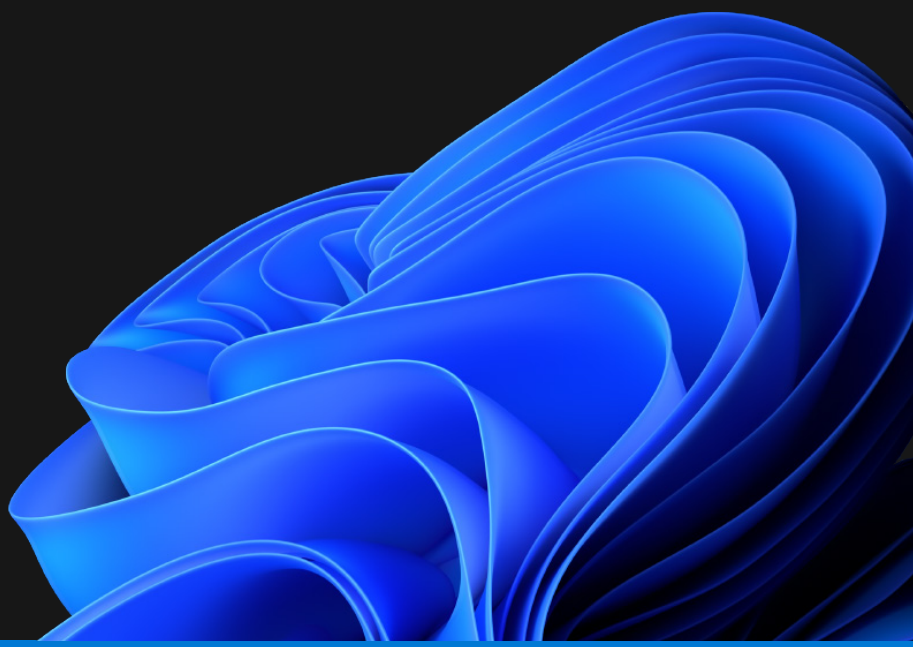
ヒューマンエラーもこの課題をさらに複雑にしています。サイバーセキュリティ障害の 46% が人的ミスによるもので、[2] さらに、働き方の多様性や柔軟な作業環境が普及したことから、潜在的な脆弱性が拡散され、リスクが大幅に増幅されています。

それでも事業はセキュリティの懸念を乗り越えて成長していかなければなりません。あらゆるビジネスチャンスをあらゆる場合に獲得する必要があります。このような状況を受けて、現在、「デフォルトでセキュア」な対策に向けた世界的な動きが台頭しつつあります。企業は、脅威を攻撃未遂の時点で阻止するように設計されたソリューションを実装して、アタックサーフェスを最小化しています。この先行的なアプローチは、脆弱性を最小化し、侵害の可能性を抑えます。

> Windows 11 Pro は何層もの強力な保護機能に支えられているので、**セキュリティ障害が 58% 削減されたと報告されています。**[1]

セキュアに設計され、初期状態からセキュアな Windows 11 Pro は、史上最も強固に防御された Windows で、現代の多面的な驚異環境にある企業を力づける Microsoft のコミットメントに基づいて構築されています。

現在のサイバーセキュリティ状況、多様性の進む働き方や業務環境について続きを読んで詳細をご覧ください。これらの傾向がイノベーションを促進し、同時に新しいセキュリティ上の課題の原因になっていることについて内容をご覧ください。そして、セキュリティ優先の観点から構築されている Windows 11 Pro 搭載のデバイスが、デフォルトで保護機能を提供し、チップからクラウドまでのセキュリティ設計によって企業のセキュリティ態勢を改善し、先行的にリスクを軽減することについてご覧ください。



# サイバーセキュリティ脅威環境をナビゲートする

急速なデジタル トランスフォーメーションに働き方の傾向が変わったことが組み合わさって、従来の仕事場を根本的に見直す結果が生じました。従業員はどこからでも滞りなく共同作業ができて生産性が維持できることを求めるのですが、改革されたより柔軟な働き方は、複雑で困難なサイバーセキュリティ環境を作り出しています。

企業の 23% がサイバーセキュリティ障害を経験したことがあるのは驚くべきことで、[3] そのほぼ半数が人的または従業員のミスによるものでした。[2] この事実は、テクノロジーによる防御態勢だけでなく強力なセキュリティハイジーンも必要であることを明らかにしています。

> **このデータは警告に値する次のような傾向を示しています:**Microsoft の社内データによれば、パスワード攻撃はここ 1 年で 3 倍近く増加し、現在は毎秒 4,000 件となっています。[4]

フィッシング攻撃は毎日 1 億 100 万件を超え、[2] ランサムウェア攻撃は年々 130% 上昇しています。[5] また、DDoS 攻撃も引き続き急増しており、毎日 2,000 件近くが報告されています。[2] (年々 40% 上昇[2]).これらの傾向は、総合的にサービスやビジネスの操業を混乱に陥れる脅威となっています。

ここで明確なことは:脅威に対する戦いは単に外部に対するものではなく、企業内でのセキュリティ認識を強固にすることが明らかに重要であること。サイバーセキュリティに対する包括的なアプローチが必要不可欠であり、そのアプローチは人的な意識、警戒、テクノロジーがシナジーを奏功して現在と将来の企業の運用を守れるものであること。多様性と新たな働き方がセキュリティのリスクプロファイルを変える可能性があることを理解するのも非常に重要です。

Windows 11 Pro 搭載の PC を配備することは、この容赦ない脅威の真っただ中、作業場所にかかわらず従業員のセキュリティに対する心配の重荷を取り除き、企業にはセキュリティ態勢を強化する方策となる、重要な進歩となります。

**23%**
サイバーセキュリティ障害を経験したことのある事業の割合[3]

**46%**
すべてのサイバーセキュリティ障害の内、人的または従業員によるミスが原因なものの割合[2]

**3 億 4,500 万以上**
1 日当たりのパスワード攻撃[4]

**1 億 100 万以上**
1 日当たりのフィッシング攻撃[2]

**130%**
ランサムウェア攻撃の年々増加率[5]

**1,955**
1 日当たりの DDoS 攻撃[2]

**40%**
DDoS 攻撃の年々増加率[2]

# 働き方によって変わるデバイスと OS のニーズ

Microsoft は LinkedIn と GitHub と協働して、今までで最も広範囲な調査プロジェクトを実施しました。「新しい仕事の未来」と呼ばれるイニシアティブです。調査の結果、新しいデバイスやオペレーティングシステムが仕事の将来を形作り、進化の絶えないサイバーセキュリティ状況に対抗するのにどのような役割りを果たすかについて非常に重要な洞察を得ることができました。

柔軟な働き方と働き場所がますます一般的になり、市場動向ばかりでなく、従業員が本当に何を好んでいるかが変化していることが反映されています。従業員はより高度な自律性と利便性を求め、多くの企業はその意向を受け入れることが生み出す利点 (生産性や仕事に対する満足度の向上) を認識しています。[6]

これらの常に変化する働き方は、特に柔軟な作業環境ではセキュリティに対する新たな課題となります。その一方、仕事とテクノロジーは同列的に進化するので、より優れた業務プラクティスを導入すれば生産性をさらに高めることができます。新しいデバイスを導入すれば、ミーティングや戦略的管理がより効果的になるばかりでなく、より広範囲な生産性向上の結果にもつながります。たとえば、ウェルビーイングやワークライフバランスの向上、仕事での従業員の全体的な経験がより良くなることが含まれます。

働き方を変えるのは単に仕事をする場所を変えるだけではありません。どのように仕事が実行されるかが大きく変わります。Windows Copilot と Microsoft 365 Copilot[7] などを含む人工知能 (AI) が業務環境の改革に果たす役割りがますます大きくなっているのはそのためです。仕事に関するデータ生成が今までにない速度で加速されると、老朽化したデバイスや古いバージョンの OS がこれらのテクノロジーが約束するイノベーションを阻む障害となります。

急速に変化する市場で事業が繁栄するには、どこからでも繁栄できるようなセキュリティが確保された、イノベーションを育むことのできる適切なツールを使う必要があります。Windows 11 Pro 搭載デバイスは、セキュリティが設計に組み込まれたフレームワークによって構築されているので、新出の業務テクノロジーのパワーを活用してこれらの課題に立ち向かうことができます。

このセクションでは、多様な働き方が従業員個人の働き方だけでなく、共同作業するチーム内部、企業、そして社会構造そのものの力学を変えていることについて探索します。

# 大規模な環境での柔軟な働き方: 年齢構成による違いの理解

## 個人への影響

柔軟な働き方は、リモートとオフィスで行う作業が混合されて、個人にはより高度な柔軟性と自律性を提供します。さまざまな場所から仕事ができるということはワークライフバランスをさらに高めることができますが、異なる環境に合ったツール、テクノロジー、セキュリティ対策が必要になります。

Windows 11 Pro はセキュリティ強化対策とユーザー中心機能を設計に組み込んで以上の懸念事項に対処しています。容易に利用できる、直感的なユーザーエクスペリエンスと新しいサイバーセキュリティ脅威に対する防御を提供して、従業員の満足度とウェルビーイングをさらに高めます。

## 共同作業をするチームへの影響

柔軟な働き方に移行するにはチーム同士の協働のし方について考えなおす必要があります。柔軟な働き方は、より多様で世界各地から人材を求めることを助長しますが、物理的にどこにいても滞りのないコミュニケーションとコーディネーションが可能な、堅牢で安全なコラボレーション プラットフォームやツールが必要となります。

Microsoft Teams を使ってシームレスに仕事ができる Windows 11 Pro の包括的なセキュリティ機能は作業を保護し、同時に、ノイズ キャンセルや背景ぼかし、ファイル共有、タスクバーからミュート・アンミュート、などのスマートなビデオ会議機能が、共同作業をよりしやすくします。スナップ レイアウトも場所を移動したときの仕事の整理を簡単にしてくれます。

## 企業内部での広範囲な影響

企業は部門間のコミュニケーション、構造的な孤独感、大がかりな従業員の移動などの複雑な問題にも取り組んでいます。組織全体に影響のある潜在的な脅威には、ネットワーク全体に支障をきたす巧妙なランサムウェア攻撃などがあります。

Windows 11 Pro は、さまざまな作業環境間のコミュニケーションを安全にし、システム全体を保護して操業継続を確保する、なくてはならない資産であることが明らかになります。

## 社会への波紋

社会的規模では、仕事の場所が変わることとその影響が現在調査されています。このような混乱のなか、サイバーセキュリティ脅威は業種全体を危機に陥れる可能性があります。

Windows 11 Pro は、これらのグローバルな変動のなか、企業が安全に適応できるような装備を提供し、事業の継続と生産性を維持し、同時にますます増大するサイバーセキュリティの脅威に対する堅牢な保護態勢を確保します。

# 新しい働き方の時代における 3 つのリスク要因

企業の使命は明確です:現在ならびに将来の業務環境と不確定さを見極めながら方向を定めていくには、堅牢なサイバーセキュリティ戦略と最新のシステムとデバイスが中核にある操業計画を策定しなければなりません。次の 3 つのリスク要因は、実世界の影響がその根本にあり、先行的に対処しない場合、企業のセキュリティ態勢と事業の成功に深刻な影響を与える可能性があります。

## 1.イノベーションの行き詰り

> CIO の **95%** が、自分の役職について、従来の IT の責務を超えて拡大していると示唆しました。[8]
>
> CIO の **71%** は、新しい考え方を促進するためにより多様性のあるインクルージブなチームを創設しており、**38%** は新しいテクノロジーに投資してビジネス イノベーションを促進しています。[9]

古いシステムやデバイスは、企業がイノベーションに取り組み、急速に進化する事業環境で競争する力を阻止する場合があります。老朽化したテクノロジーは、高度のアプリケーションやサービスをサポートできない場合が多く、変革的な技術の導入の障害になります。

さらに、古いシステムは故障しやすく、操業を中断するダウンタイムとなり、生産性を下げ、クライアントとの関係や事業機会を妨げることもあります。同時に、最も望ましい人材の採用と保持が影響されることもあります。従業員 1 人ひとりがつながって、企業のイノベーション計画に寄与できるような、セキュアでアクセス可能なテクノロジーを確実に提供することは必要不可欠です。

**リーダーが検討すべき項目:**

- 時代遅れのテクノロジーが自社のイノベーションと競争力にどのような影響を与えているか。
- 老朽化しつつあるハードウェアやソフトウェアが起因となるシステムのダウンタイムのコストはどのくらいか。
- 現在使用中のテクノロジーは、自社の多様性のある働き方とどのように連携しているか。
- 現在のインフラストラクチャは新しい動的な業務環境で求められる人材を集めて維持することができるか。

# 2.過負荷な状態の IT リソース

セキュリティ部門の担当者の **66%** が職場で強度のストレスを感じています。**64%** の担当者は仕事のストレスが**精神的にも健康に影響を与えています。**[10]

現職に留まることを強く意思表明している IT 担当者は全体の **29.1%** に過ぎず、これは IT 以外の従業員と比べて **10.2%** 低い値です。[11]

データ侵害の平均コストは大規模企業の場合 **445 万ドルです。**[12]

古いシステムにはより多くのメンテナンス作業が必要になり、IT 担当者の酷使につながることが多く、戦略的作業に注力できない状態が起きます。新しい IT 管理ツールとの互換性がないことも、堅牢なセキュリティとコンプライアンスの維持の問題となります。また、老朽化するシステムには最新のセキュリティアップデートがない場合が多く、その結果、サイバーセキュリティ脅威にさらされ、お客様の信頼を損ねる可能性のある、コストの高いデータ侵害につながる可能性があります。

**リーダーが検討すべき項目:**

- IT リソースの何 % が老朽化しつつあるデバイスの維持に費やされ、それが戦略的フォーカスにどのような影響を与えたか。
- 古いシステムは、セキュリティとコンプライアンスにおいて新しい IT 管理ツールと互換性があるか。
- 老朽化しつつあるデバイスは、パスワード攻撃やランサムウェアなどのサイバーセキュリティ脅威に対してどの程度脆弱な状態か。
- 時代遅れのセキュリティがもたらすデータ侵害の潜在的な財務、風評コストはどのくらいか。

# 3.従業員の自信と生産性の崩壊

職務の実行をサポートするテクノロジーがあると感じている従業員は **230% よりやる気があり**、3 年以上現職に留まる傾向が **85% 高くなっています** 。[13]

テクノロジーならびに事業リーダーの **60%** が、従業員の職場のあり方を改善することが IT の最優先事項だと示唆しています。[14]

技術的な面において従業員が職場のあり方がよいと感じている企業は、弱いと感じている企業に比べて **25% 高い利益** を計上しています。[15]

老朽化しつつあるデバイスは、従業員の生産性と満足度を阻害する可能性があります。パフォーマンスが遅い、新しいツールとの互換性がない、などはフラストレーションにつながる場合が多く、士気や収益を影響します。古いシステムは狙われやすいソフトターゲットなのでサイバー脅威のリスクが高まり、機密データの侵害につながり、さらに従業員の自信の低下や風評被害を起こすことにもなります。

**リーダーが検討すべき項目:**

- 古いデバイスの性能の問題は従業員の生産性と満足度をどのように影響してるか。
- 従業員は必要なツールを使用できているか、それとも互換性が問題となって思うように使えていないか。
- 古いシステムによるサイバー脅威へのエクスポージャーは従業員の自信にどのように影響しているか。
- 従業員や顧客の機密データにかかわる財務的、風評的なコストはどのようなものか。

# 人工知能の時代に備える

「新しい仕事の未来」が発展するに従って、AI がその強力な指南役となります。

基礎を構成する言語モデルの進歩、AI 技術の躍進、パンデミックにより飛躍したデジタルトランスフォーメーションが、企業を極めて重要な岐路に立たせます。私達の働き方を再構築するうえでこれほど重要な機会はかつてありません。

AI 革命の生先端にある企業は、今、次のように問いかけています:どのようにしたら AI を使ってイノベーションの障害を乗り越え、IT リソースが酷使されている状態を緩和し、従業員の自信と生産性を高めることができるだろうか。その答えは明確になりつつあります。

Windows 11 Pro によって Microsoft はその道を歩み始めています。Bing Chat Enterprise を伴った Windows Copilot の導入は、インテリジェントなツールを一緒にデスクトップに導入して、仕事で使う AI に簡単で安全なアクセスを提供します。この機能には生産性を強化する計り知れないほどの潜在性があり、クラウドや Edge 全体で Windows アプリケーションを改革する、AI をくまなく活用したエクスペリエンスにつながる段取りとなります。

Windows 11 Pro 搭載デバイスに切り替えることは、企業にとって、働き方の次の時代の複雑な対流を巧みにナビゲートすることを可能にする触媒と言えます。AI の改革的な力を活用する企業は、この革新的な技術が提供する広大な潜在性を利用して、単に仕事の未来に適応するのではなく、それを積極的に形作るのです。

# Windows 11 Pro 搭載 PC:
# 現代のビジネスを支える多層保護

セキュリティの意思決定者を対象とした調査結果によると、ほぼ 90% の回答者が、時代遅れのハードウェアは攻撃に対する脆弱性を高め、現代のハードウェアが将来の保護に必要不可欠であると考えています。[16] Windows 10 のイノベーションを基に、Windows 11 Pro は、デバイス製造とチップ製造のパートナーとの協働により、ハードウェアセキュリティ機能を追加し、現代の働き方を支え、変化しつつある脅威状況に応答しています。

## 強化されたハードウェアとオペレーティング システムのセキュリティ

Windows 11 Pro は TPM 2.0 などのハードウェアベースのセキュリティによって保護機能を次のレベルに押し上げ、暗号キーやユーザーの資格情報の不正アクセスやかいざんを防いでいます。強化されたカーネル保護を提供するために、Windows 11 Pro 搭載のデバイスは、仮想化ベースのセキュリティ (VBS) やハイパーバイザーコード統一性 (HVCI) などを含む隔離技術をデフォルトで有効にするようになりました。

## 堅牢なアプリケーションセキュリティとプライバシー制御

実行可能ファイルを使ったマルウェアに対する最も効果的な防御対策はアプリケーションの制御であると多くの企業が提示しています。App Control for Business (旧称 Windows Defender Application Control) は、Windows のための次世代のアプリケーション制御ソリューションで、IT は環境内で実行するアプリを決定して強力にコントロールできるようになります。Microsoft Intune[17] を使ってデバイスを管理しているお客様は、管理コンソールから App Control for Business を設定することができるようになり、 そこから Intune[17] をマネージド インストーラーとしてセットアップすることもできます。

個人データとビジネスデータの両方の安全を確保するために、Windows 11 Pro は多層のアプリケーションセキュリティを使用しています。アプリケーションの隔離、コードの完全性、プライバシー制御、最少権限などの原則により、開発者は最初からセキュリティとプライバシーを埋め込むことができます。

Windows 11 Pro は位置、カメラ、マイクへのアクセスなどのプライバシー機能もより高度に制御できるようにしてユーザーの力を高めています。

## 保護されたアイデンティティ

サイバー犯罪者は頻繁にパスワードを狙っているので、Windows 11 Pro は、資格情報の盗取に対する堅牢な保護機能を使っています。Windows Hello for Business で多要素承認と資格情報保護を有効にすれば、暗唱番号、顔や指紋認証による簡単で安全なパスワードレスのサインインが実現されます。Microsoft Defender SmartScreen は資格情報盗取に対する先行的な保護を強化された作り込みのフィッシング対策によって提供する一方、Windows Presence はデスクを離れると自動的にロックし、戻ったときに再起動するので安心です。[18]

## クラウド サービスに接続

Windows Update for Business は費用のかからないクラウドサービスです。IT 管理者は社内の Windows のクライアントデバイスを Windows Update サービスに直接接続すれば、最新の Windows 機能とセキュリティ保護対策が常に提供去れている状態を維持できます。Windows 11 Pro にはデバイス登録と管理クライアントも作り込みで提供されているので、企業のセキュリティポリシーの施行、Microsoft Intune のような最新のデバイス管理 (MDM) ツールの優位点の利用などが可能です。[17] Windows 11 Pro はオンプレミス、クラウドベースのどちらの管理ソリューションとでも機能します。

クラウドの管理をお考えの場合には、Windows 11 Pro と Microsoft 365 Business Premium の組み合わせをお勧めします。[7] 現在のセキュリティと柔軟性の要件を満たす Windows 11 Pro 搭載の最新の PC と Microsoft 365 Business Premium[7] のペアリングは、より強靭で効率のよい作業環境の構築に欠かせない手段となります。

詳細は Windows 11 Security Book をダウンロードしてご覧ください。

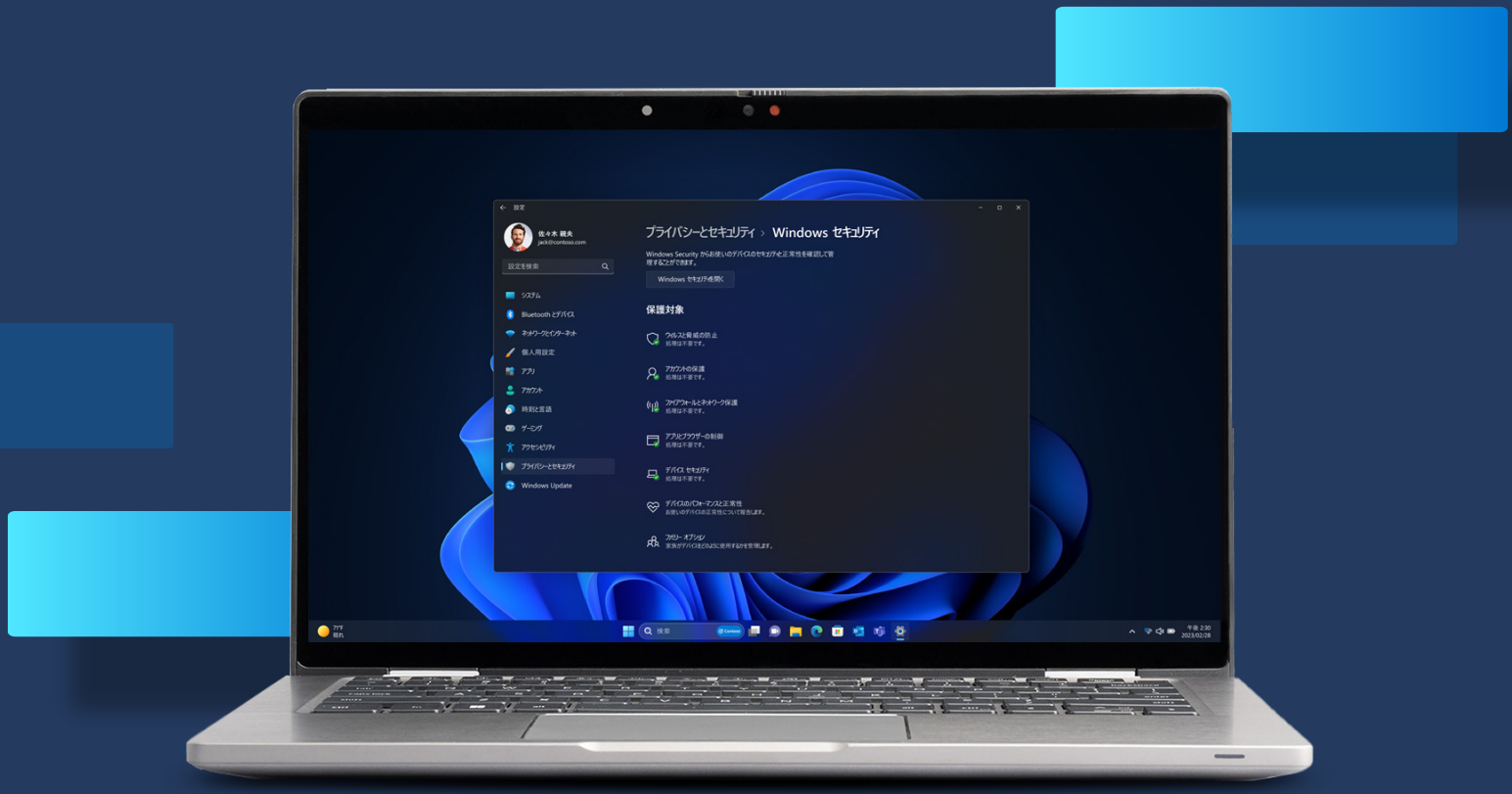
# Windows 11 Pro 搭載 PC:
# 新しい業務環境でのセキュリティ

変革的な業務環境に適応する企業には、堅牢なセキュリティ、手間のかからない管理機能、多様な働き方の支援を統合するプラットフォームが必要になります。Windows 11 Pro 搭載デバイスの展開は、従来の IT セキュリティの域を超えた高度のソリューションを提供し、保護ばかりでなく、生産性、共同作業、操業効率の向上にも対応します。

Windows 11 Pro 搭載デバイスはセキュリティ対策だけが取り柄ではありません。生産性や共同作業を強化し、動的な職場環境に適応します。

この適応性が従業員の自信を向上させ、潜在的な生産性の降下を相殺します。展開とプロビジョニングを簡素化した Windows 11 Pro 搭載のデバイスは、逼迫した IT リソースの負荷を緩和し、イノベーションを助長してコストを引き下げます。

Windows 11 Pro 搭載デバイスは将来のための地ならしの役割りを果たします。クラウドを基盤とした運用に移行して新しいテクノロジーを活用する企業はビジネスチャンスを捉え、リスクから身を守り、成長の機運に乗ることができ、変化の絶えない事業環境において一貫して卓越した結果を出すための準備が整います。



# セキュリティが向上。コスト削減。

## 標準搭載された確実なセキュリティ

Windows 11 Pro は堅牢なセキュリティをすべてのレベルで確保し、ファームウェア攻撃の件数を 3.1 倍削減しています。[1] 多層保護機能、TPM 2.0 を含むハードウェアベースの資格情報保護、VBS によるカーネル保護の強化などが作り込みで提供され、デフォルトで有効になっています。

## 進化し続ける脅威を先回り

Microsoft Defender SmartScreen による強化されたフィッシング対策は資格情報盗取件数を 2.8 倍削減したと報告されています。[1] さらに、 Windows Hello はパスワードレスでサインインすることを可能にして使いやすさの向上とセキュリティ強化を提供します。Windows Presence は、デバイスを離れるときにロック、戻ると再起動する機能でユーザーを保護します。作り込みで提供されている脆弱なドライバーのブロック リストはデフォルトで有効になっており、潜在的なリスクのあるドライバーを避けるための機能です。

## ミッション クリティカルなアプリの保護

Windows 11 Pro は Windows デスクトップのアプリケーションを Win32 アプリを介して隔離させて実行することによって、強化されたマルウェア対策を提供します。AppControl for Business (旧称 Windows Defender Application Control) を新型のデバイス管理機能と合わせて利用すると、信頼されたアプリケーションのみをデバイスで実行させることができます。

## シンプルになったエンドツーエンドの保護

Windows 11 Pro の合理化されたチップからクラウドまでのセキュリティは、 Intune Endpoint Privilege Management (EPM) を使ったシステムアクセスの保護を提供する一方、[17] 従業員には Mobile Application Management (MAM) for Windows. を使って管理対象外のコンテンツにアクセスできるようにします。そのうえ、Windows 11 Pro は Local Administrator Password Solution (LAPS) with Microsoft Entra (旧称 Azure AD) を使ったサインインのセッションで使われるトークンの保護、ローカル管理者のパスワードアカウントの自動管理などの機能によって堅牢なセキュリティを確保します。

# 必要なときに保護を追加

Windows 11 Pro 搭載のデバイスには一連のセキュリティ機能が装備されています。オプションとして **Microsoft Pluton セキュリティ プロセッサ**を介したハードウェアベースの RoT 保護機能,と **BitLocker** や **Windows Hello for Business**、**TPM 2.0** などの統合された要素があります。

Advanced Hardware-Enforced Stack Protection はソフトウェアとハードウェアによる防御機能を同期化してメモリ破損、ゼロデイ攻撃などの脅威に対抗します。定期的な RoT ファームウェアのアップデートにより、デバイス環境をしっかりと保護した状態が維持されます。

Windows 11 Pro 搭載デバイスを展開している企業は、アタックサーフェスを格段に削減させることができ、セキュリティを妥協せずに適応性と成長の両方を強化できます。

## Windows 11 Pro の主な利点

### **企業:**堅牢なセキュリティの基盤

Windows 11 Pro はサイバー脅威を最大 58% 削減するのに貢献できます。[1] セキュリティを妥協せずに自信を持って事業成長の機会を追求することができます。

### **IT 部門:**障害を減らしてデータを守る

ハードウェアベースの信頼されたルート (RoT) から BitLocker や Windows Hello などの統合保護機能によって、IT 部門は Windows 11 Pro の包括的なセキュリティ機能のメリットを享受します。

### **従業員:**安全に効率よく働く

Windows 11 Pro 搭載のデバイスには定期的な自動ファームウェアアップデートが提供されるので、従業員はデータが保護されていることに自信が持て、生産性に注力できます。

# 変化の絶えない脅威状況における高度の保護

Windows 11 Pro 搭載のデバイスには最新の CPU に加えて、TPM 2.0 によるハードウェアベースの信頼されたルート、安全なブート機能、ドライブの暗号化をする BitLocker などのセキュリティ機能がデフォルトで装備されているので、セキュリティ態勢が強化されます。他社のセキュリティ ソフトウェアと統合させた場合、セキュリティ攻撃の成功例が 20% 減少したことが実証されています。[19]

> Windows 11 Pro 搭載デバイスではセキュリティ攻撃が成功する確率が**最大 20% 減少**。[19]

新しい、アップグレードされたデバイスに含まれている TPM 2.0 は、ストレージの保護、暗号化、キー生成、ブートの完全性などの Windows Hello や Windows Defender System Guard などの機能の基盤となる主要機能を支えています。このしくみは一貫性のあるハードウェアによる信頼されたルートを確立させ、将来のセキュリティ機能に対応できる段取りとなります。

## Windows 11 Pro の主な利点

### **企業:**事業改革を躍進させる

チップからクラウドまでカバーする包括的なセキュリティが提供されているので、企業は自信を持って新しい機会に取り組み将来の方向を定めていきます。性能の強化、セキュリティ機能の進歩、AI との統合によってどこからでも操業でき、妥協なしで躍進することができます。

### **IT 部門:**管理と互換性の合理化

既存のソフトウェアとハードウェアに対する互換性が展開を簡素化する一方、最新の管理機能によって IT 業務の効率化が実現できます。Windows 11 Pro はコストと労力の削減のマイルストーンであり、企業を成功に導くシームレスで安全な効率のよい環境を実現します。

### **従業員:**どこからでも卓越した仕事を実現

AI を活用した操作環境、インテリジェントなワークフロー、パーソナライズ設定によって、従業員は好みにあった方法で仕事ができるので、ウェルビーイングと生産性が促進されます。Windows 11 Pro は、単なる機能性を超越した共感的なアプローチを提供し、従業員の満足感と事業業績の両方を高めます。

# 生産性と共同作業のために開発

Windows 11 Pro の新しい機能と現代のデバイスを組み合わせると、従業員の生産性向上の可能性が創出され、より迅速に、より多くの仕事を完了できます。事業成長の目的のために構築された現代の Windows 11 Pro 搭載デバイスは、最高級の性能と堅牢な柔軟性を持ち合わせています。従業員が箱を受け取ったとき、そのまま使用できてセキュリティも確保されている Windows 11 Pro 搭載デバイスは、ファームウェア攻撃件数が 3.1 倍削減されたという報告の基となるハードウェアベースの保護が組み合わされており、[1] システムのパフォーマンスや従業員の生産性を阻害することもありません。

> 調査対象企業は、以前の Windows デバイスに比べて生産性と共同作業が **50% 上昇** したと報告されています。[20]

スナップ レイアウトなどの機能はデスクトップの整理を効率化して生産性を促進してマルチタスクをシンプルに実行できるようにします。これらの機能は AI によって強化されたシームレスなビデオ会議機能と組み合わされ、新しいデバイスに統合されている高品質カメラとスピーカーによってさらに強力なものになります。ユーザーに馴染みのある Windows インターフェイスのおかげで中断されないワークフローが使用できるので、Windows 11 Pro 搭載デバイスは最大 15% の生産性向上に寄与します。[19]

Windows 11 Pro 搭載のデバイスには、そのほか、バッテリー駆動時間の最大 61% 延長[20,21]、応答性の高いパフォーマンス、複数の 4K モニターで高品質なプレゼンができる機能強化も提供されています。従来のキーボードとマウスに加えて、ペン、インク、タッチ、音声などの周辺機器によって可能になるさまざまな作業モード[18] が柔軟な作業方法を実現します。

## Windows 11 Pro の主な利点

**企業:**成長促進のためのエンジニアリング

Windows 11 Pro 搭載デバイスは、マルウェアに対する抵抗力を向上させてファームウェア攻撃の成功率を削減していますが、そのすべてをパフォーマンスに影響を与えずに実現しています。[1] 複数の 4K モニターでプレゼンができるので生産性が向上でき、Windows 11 Pro は事業目標と整合され、容易にビジネスチャンスを捉えることができます。

**IT 部門:**比類のないコントロールとセキュリティ機能

合理的な統合ができるように構築された Windows 11 Pro 搭載デバイスは、ハードウェアベースの保護や応答性の高いパフォーマンスを提供するばかりでなく、アプリとの互換性も 99.7% と高く、プリンター、ディスプレイ、その他のハードウェアの使用がしやすくなっています。[22] Windows 11 Pro があればシステムは安全で信頼でき、簡単に使用できるので、 IT 部門はイノベーションに注力できます。

**従業員:**あらゆる働き方に適応する設計

スナップ レイアウトと AI により強化されたビデオ会議機能が共同作業とマルチタスクを簡単にします。そして 61% 長いバッテリー駆動時間[20,21] と統合されている高品質のカメラと応答性の高いパフォーマンスによって、Windows 11 Pro 搭載デバイスは 1 つひとつのタスクの柔軟性と利便性を優先しています。

# セキュリティと IT 部門のための生産性向上

Microsoft が委託した Forrester 社によるレポートによれば、Microsoft, Windows 11 Pro 搭載デバイスは、膨大な仕事の量に耐えかねている IT リソースの重荷を緩和します。デバイスには **仮想化ベースのセキュリティ** (VBS)、**ハイパーバイザーによるコードの整合化** (HVCI)、**Windows Hello for Business**、**Trusted Boot**などのセキュリティ機能が標準装備されているので、IT 部門はセキュリティ設定よりも戦略的な作業に焦点をあてることができます。

> **3 年間でヘルプデスクへのリクエストが 80%** 削減された報告。[19]

VBS はハードウェアの仮想化によって、オペレーティングシステムからカーネルを隔離して安全にホストします。従って、例えオペレーティング システムが侵害されてもカーネルは安全に保護されています。HVCI は、VBS と合わせて、ドライバーなどのカーネルモードのコードを変更する目的で仕掛けられた攻撃の防止に使われ、ハードウェアレベルのコードの完全性を維持し、不正な変更を防ぎます。

この高度で先行的なセキュリティのしくみは、IT 部門の生産性を大幅に向上させます。その例には Forrester 社グループをサポートする セキュリティ部門で 20% の生産性向上が見られたことが挙げられます。[19] そのうえ、Windows 11 Pro 搭載デバイス内部に装備され、デフォルトで有効になっているセキュリティ機能は、セルフサービス機能と組み合わされてるので、ヘルプデスクへの問い合わせが 3 年間で 80% 削減されたことの一因となっています。[19]

## Windows 11 Pro の主な利点

### **企業:**最小限のオーバーヘッドで成長

仮想化ベースのセキュリティ (VBS) やハイパーバイザー保護によるコード整合性 (HVCI) などのセキュリティ機能によって、Windows 11 Pro 搭載デバイスは脅威に対する露呈を削減することに役立ち、機密データを安全に保ちます。これらのシステムは、生産性を 20% 向上させるというすばらしい結果を出しています。[19]

### **IT 部門:**毎日繰り返す作業をシンプルに

Windows 11 Pro 搭載デバイスは機能の有効化を自動的に行うので、常時行うトラブルシューティング作業を減らし、先行的なシステム強化のための時間を創出し、同時にヘルプデスク対応時間も削減します。[19] 従って IT 担当者は事後処理よりも、新しい技術の実装や戦略の実施に注力することができます。

### **従業員:**毎日がスムーズに動く

Windows 11 Pro 搭載デバイスはどのような働き方にも適用する、ユーザーフレンドリーで安全な作業環境を提供します。高度なセキュリティ機能が作り込まれているので、従業員はデータやシステムが保護されていることを確信して、自信を持って仕事に専念できます。

# 展開、プロビジョニング、セキュリティを躍進

Windows 11 Pro 搭載デバイスの導入は、展開とプロビジョニングのプロセスを加速するばかりでなく、デバイスと今日の事業の運用に欠かせないアプリケーションの両方に堅牢な保護を提供します。

シームレスにハードウェアとソフトウェアが統合されているので、広範囲にわたるハードウェアのチェックや互換性評価の必要性が削減されます。この効率的な展開プロセスの所要時間は 25% 短縮されると報告されています。[19]

> **Windows 11 Pro 搭載デバイスを展開した場合に最大 25%** の効率向上が報告されています。[19]

**Microsoft Intune**、[17] **Microsoft Configuration Manager**、**Windows Autopilot** などのテクノロジーがデバイスのプロビジョニング、構成管理、ソフトウェアアップデートを全社的に簡素化して、経費削減とコンプライアンスの向上に貢献します。[23] また、Windows Autopilot は、事前に設定されているデバイスをリモートで働く従業員に対してゼロタッチで展開できるので、効率がさらに改善され、大幅な時間とコストの節約につながります。[23]

## Windows 11 Pro の主な利点

### **企業:**ビジネス イノベーションのためのプラットフォーム

Windows 11 Pro 搭載デバイスと現代のクラウド管理を組み合わせると、セキュリティを強化し、新しい効率向上項目を実施してどこからでも事業が展開できます。.

### **IT 部門:**デバイス管理の合理化

Windows 11 Pro 搭載デバイスは IT 管理プロセスを簡素化して、時間のかかるハードウェアのチェックや互換性評価を削減することができます。Windows 11 Pro 搭載デバイスを MDM ソリューションとともに導入することによって、IT 部門はオンボーディングのプロセスを加速化でき、手動介入の必要性を削減できます。

### **従業員:**デバイスをすばやく有効化して更新する

Windows 11 Pro 搭載デバイスは定期的にすばやく更新することができるので、より迅速な展開とより堅牢なアプリケーションのセキュリティにつながります。セロタッチ展開が準備されているデバイスなので、従業員は速やかに仕事を開始できます。

# 仕事の将来のセキュリティ

現代の競争の激しい市場で繁栄するには、戦略、レジリエンス、イノベーションの整合性が成功の要となります。Windows 11 Pro 搭載デバイスの導入は主要な戦略的イニシアティブを支える、企業の成長を躍進させる堅牢なプラットフォームでもあり、単なる IT セキュリティのソリューションではありません。

予想不可能な変動の激しいサイバー脅威環境に直面して、Windows 11 Pro はその中核にセキュリティをおいて設計されており、「security-by-default」と「security-by-design」の強固な原則を実装してセキュリティを初期状態から有効にしています。IT 管理者にとって、提供されるコントロール機能は単に強力であるばかりでなく、 的確であり、柔軟性が組み合わされているため、個々の企業特有のニーズに合致した技術環境の構築が可能です。従業員にとっては、比類のないハードウェアベースのセキュリティが保障され、パスワードに縛られないパスワードレスの保護があるので、どのような働き方でもシームレスな統合が促進されます。

Windows 11 Pro 搭載デバイスを使えば、企業は潜在的なサイバーセキュリティ障害の削減のメリットがあるばかりでなく、生産性向上と共同作業の増強により IT インフラストラクチャの負荷を軽減することもできます。エンドツーエンドの保護、柔軟な働き方のサポートが簡単にできること、ワークフローの加速を可能にする革新的なテクノロジーが合わさっているので、Windows 11 Pro 搭載のデバイスはあらゆるビジネスチャンスを獲得することを可能にします。

### Windows 11 Pro 搭載デバイスの紹介

Windows 11 Pro 搭載デバイスの世界をご覧ください。すべてのビジネスのニーズに対応できるように設計されています。革新的な 2 in 1 デバイスから、スタイリッシュで軽量なノート PC、強力なパワーのあるワークステーションまで、企業のあらゆる役割りに適した Windows 11 Pro 搭載デバイスがご利用いただけます。Windows 11 に無料でアップグレードする方法について詳細をご覧ください。

Windows 11 Pro 搭載デバイスを見る >

# 出典と謝辞

1.「SMB Windows 11 Survey Report」. (中小企業 (SMB) を対象とした Windows 11 に関するアンケート調査結果レポート)。Techaisle、2022 年 2 月。Windows 11 の結果を Windows 10 デバイスの結果と比較しています。

2.「Microsoft Digital Defense Report 2022」、Microsoft。

3.Microsoft Research: による「Security in the New Working Environment, 2022」。

4.「Microsoft Security, Microsoft Entra expands into Security Service Edge and Azure AD becomes Microsoft Entra ID」Joy Chik 著、2023/7/11。

5.「Microsoft Security, Protect your organization from ransomware」2023/9/11にアクセス。

6.「Microsoft New Future of Work Report 2022」.(仕事の未来レポート) Microsoft。

7.サブスクリプションが必要です。

8.「IDG, 2020 State of the CIO」に記載のある CIO。

9.「IDG, 2021 State of the CIO」に記載のある CIO。

10.「Predictions 2023:Security Pros Face Greater Internal Risks, 2022」Forrester。

11.「Gartner Global Labor Market Survey, 2022」Gartner。

12.「IBM Cost of a Data Breach Report, 2022」IBM。

13.「In a Hybrid World, Your Tech Defines Employee Experience, 2022」Harvard Business Review。

14.「Digital Workplace Trends To Watch Out For In 2023, 2022」Forrester。

15.「Building Business Value with Employee Experience, 2017」MIT 情報システム研究センター。

16.「Security Signals, March 2021」Microsoft および Hypothesis Group。

17.Microsoft Intune は別売りです。

18.ハードウェアに依存します。

19.Forrester Consulting による委託調査（2022 年 12 月実施）「The Total Economic Impact™ of Windows 11 Pro Device」。定量化されたメリットは、1 つの複合組織が、年間 10 億ドルの収益を計上し、2,000 名の従業員を抱え、4 年に 1 回ハードウェアを更新し、従業員全員を Windows 11 デバイスに移行させた場合の 3 年分の結果を統合したものを反映したものです。

20.Windows 10 デバイスと比較した場合。「Improve your day-to-day experience with Windows 11 Pro laptops」Principled Technologies、2023 年 2 月。

21.バッテリー駆動時間は設定、利用状況、他の要素により異なります。

22.App Assure プログラム データ。

23.Autopilot は Microsoft Intune および Microsoft Entra ID (旧称 Azure Active Directory) が必要です。別売りです。