

SURVEY WHITE PAPER 2024

Windows 10 サポート終了に
向けた対応動向と中小企業の
IT環境動向について



中小企業のPC・IT動向調査2024

Windows 10 サポート終了に向けた
対応動向と中小企業のIT環境動向について

IT環境アンケート2024 Windows 10 サポート終了に向けて 調査概要

- 調査期間: 2024年8月中旬～2024年8月下旬 (2024/8/21～2024/8/28)
- 回答社数: 755社
- アンケート項目: 全30項目(お客様基礎情報は除く)

第 1 部

迫る Windows 10 サポート終了への対応と
PC運用に関わる動向

1. Windows 11 対応状況
2. Windows 11 対応にあたっての課題
3. Windows 11 対応とIT投資
4. パソコンの運用管理

第 2 部

人材不足時代の

中小企業におけるITインフラ動向

1. 中小企業が直面するビジネスの課題
2. 中小企業におけるサーバー利用の動向
3. 中小企業におけるセキュリティ対策動向

“ COLUMN ”

もはや企業規模は関係ない
セキュリティリスク
サブライチエーション攻撃の脅威

4. 中小企業におけるITインフラの運用管理

第 3 部

生成AIへの取り組み

1. 生成AIへの取組状況
2. 生成AIの活用動向
3. 生成AI導入・活用に向けての課題

総 括

● 企業動向 (2問)

ビジネスにおける現状の課題

● PCの運用・Windows 10 サポート終了対応 (8問)

社内のPC台数、Windows 10 サポート終了対応動向、PCのライフサイクル、
PC運用動向 等

● IT全般 (12問)

IT投資動向、IT投資額、サーバーの導入動向・クラウド利用状況、ITインフラ運用
の課題 等

● セキュリティ (2問)

セキュリティリスク、セキュリティ対策状況

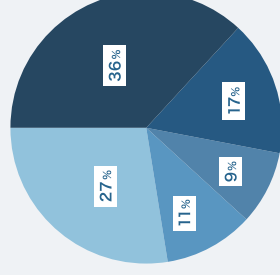
● 生成AIのビジネスへの導入 (4問)

生成AIへの取り組み動向、活用方針、活用への課題 等

● その他 (2問)

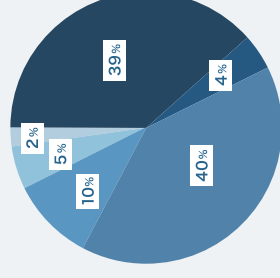
デル・テクノロジーズが提供する中小企業プログラムへの関心度、デル・テクノロ
ジーズへの期待度

企業規模別社数



■ 1-9名
■ 10-29名
■ 30-49名
■ 50-99名
■ 100名以上

IT機器導入に関する立場



■ 決断権がある
■ 決断権はないが、製品もしくはメーカー企業を選定している
■ 決断権はない
■ 関与していない/わからない
■ 顧客に提案・販売する



迫る Windows 10 サポート終了への 対応とPC運用に関わる動向

Windows 10 のサポートが終了する2025年10月まで、残すところ1年を切りました。Windows OS はサポートが終了するとセキュリティパッチが提供されなくなるため、サイバー攻撃を受けるリスクが高まるといふ課題があります。特に最近ではランサムウェアなど、OSの脆弱性を狙ったサイバー攻撃が多いため、セキュリティ対策としても Windows 11 への移行は必須です。

そこで、今回の Windows 10 → Windows 11 への移行について、各企業の対応状況と、移行にあたっての課題等の調査を行いました。

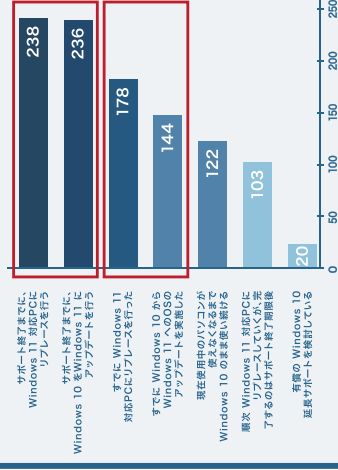
さらに、PCのリプレースやOSのアップデートとも密接に関わる、ライフサイクルやPCの運用についてもあわせて調査をしました。

1 Windows 11 対応状況

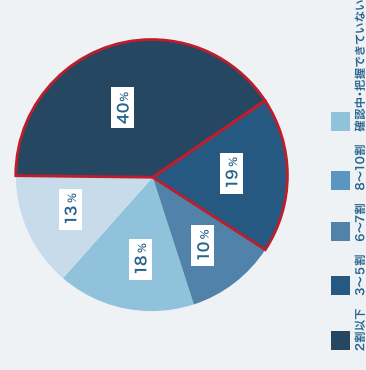
約7割の企業が Windows 10 サポート終了までに Windows 11 対応を計画

- 全体の7割強^{*}の企業がサポート終了までには Windows 11 へのアップデート、もしくは Windows 11 PC への移行を実行、もしくは計画している。
※便益なくなくなるまで使え:122社、サポート終了後に完了予定:103社、重複回答17社を除く208社全体の27.5%を差し引いた547社
- 後述するセキュリティ対策への関心度等の背景もあり、多くの企業が積極的に、Windows 10 サポート終了までに、Windows 11 対応に取り組んでいることが伺える。

Windows 11 への移行対応の状況・予定 (複数回答可)



リプレースが必要なPC台数の割合



6割の企業が、社内の半数以上のPCの Windows 11 への移行をすでに実施

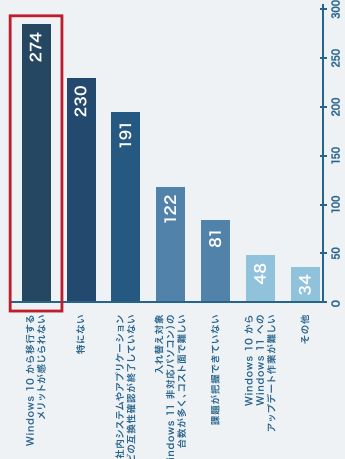
- 59%の企業が、すでに5割以上の社内PCを Windows 11 へ移行していると回答。積極的な移行を裏付ける結果となっている。
- 一方で、移行があまり進んでいない企業も全体で3割程度存在している。
特に企業規模が大きな企業ほどその傾向が強くなり、PC台数の多さに伴う、コストや移行工数の多さが背景にあると考えられる。

2 Windows 11 対応にあたっての課題

特に課題はないと回答する企業が多数
一方で、互換性やコスト、工数を課題とする企業も

- 全体の3割程度の企業は Windows 11 対応にあたって特に課題はないと回答した
- 一方で、既存のシステムやアプリケーションの互換性、台数の多さによるコスト、アップグレード作業の難しさなどを課題として挙げる企業も少なくない。これらの課題は、影響を受けやすく、比較的規模の大きな企業で移行が進んでいないという現在の状況の裏付けと言えるだろう。
- Windows 10 から移行するメリットが感じられないという声もあるが、前述した6割の企業が社内半数以上のPCを移行済みという移行状況や、今後の移行計画を見ると、Windows 11 対応の大きな障壁にはなっていないと思われる。

Windows 11 対応にあたっての課題
(複数回答可)

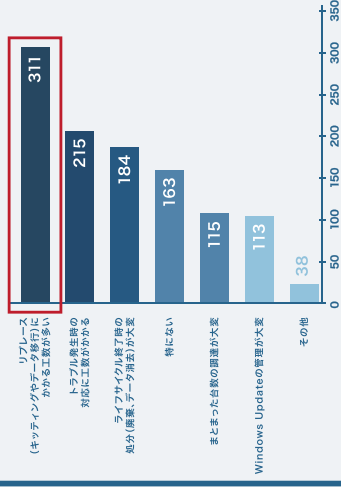


4 パソコンの運用管理

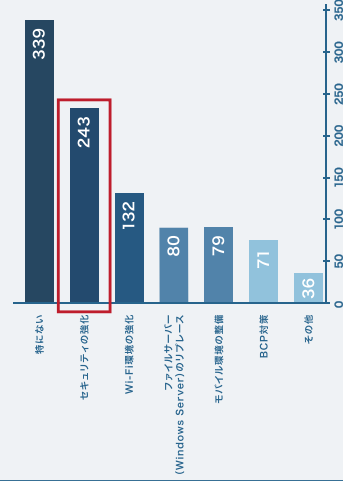
パソコン運用管理で負担感が大きいのは
リプレース関連業務とトラブル対応

- パソコンの運用管理において負担感が大きいものとしてあげられているのが、リプレースの工数、パソコン廃棄関連業務、調達といったリプレースに関わる業務である。これらは Windows 11 対応でも発生する業務であり、その負担感が伺われる。
- また、トラブル発生時の対応工数への負担感も高い。リプレース関連業務とあわせて、PC台数に比例して負担は増えるため、規模の大きな企業ほど、この傾向は強い。
- 一方で兼任や一人で担当するなど、システム管理に十分な人を割くことができないのもこの規模の企業の課題である。DX推進などのより生産性の高い業務を求められる中、ある一定規模の企業であれば、LMS(ライフサイクルマネジメントサービス)など、システム管理業務をアウトソーシングすることも検討すべきだろう。

パソコンの管理・運用で負担が大きい業務
(複数回答可)



Windows 11 対応とともに行いたいIT投資
(複数回答可)



多くの企業がセキュリティ対策に関心
モバイル対応を進める企業も

- 3割の企業がセキュリティ強化を行うとしており、セキュリティに対する関心度の高さが伺われる。
- 次の多いWi-Fi環境の強化やモバイル環境の整備は、在宅勤務やリモートワーク対応に伴うモバイルPCへの移行に伴うものと見られる。



人材不足時代の中小企業における ITインフラ動向

少子高齢化、そして人口減少局面に入ったわが国では、いよいよ人材不足が現実化しつつあります。企業規模を問わず人材確保に苦戦している企業が多くなってきました。一方で、わが国の生産性は先進国の中ではもっとも低いとされており、この生産性の低さを改善することにより、ある程度、人材不足を補うことが期待できます。生産性向上を実現する一つの方法として今日注目されているのがDX（デジタル・トランスフォーメーション）です。これまで人が担ってきた業務を根本的に見直し、デジタル技術を活用した新たな手法で業務改革を行い、生産性を高めるDXは、人材不足対策の一つとして期待されています。同様に人に代わって、ある領域に関しては人と同等以上に業務をこなすことができるAIも急激に発展しつつあります。特に生成AIはこの数年で飛躍的に機能が向上し、ビジネス利用において実用的な局面に入りつつあります。そこで、中小企業におけるビジネスの課題とIT投資、そしてAIへの取り組みについて調査してみました。

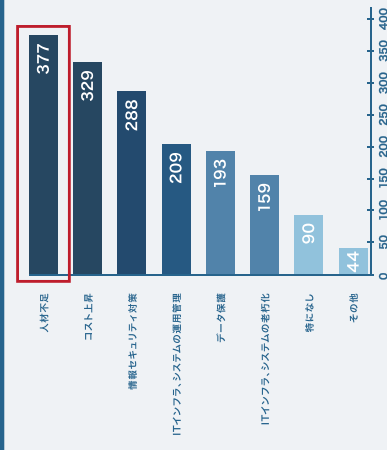
1 中小企業が直面するビジネスの課題

約半数の企業が人材不足を挙げる コスト上昇、情報セキュリティ対策も上位に

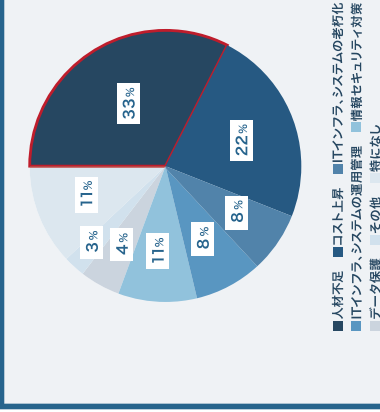
- 経営に大きなインパクトを与えるコストの上昇を押さえて、約5割(755社中377社)の企業が人材不足を直面するビジネス課題として挙げています。人材不足を重要課題とする企業も多く、深刻な課題になりつつあることが読み取ることができる。

- IT関連では、情報セキュリティ対策が多く挙げられており、関心度の高さが伺われる。次いでITインフラ・システムの運用管理やデータ保護など、日々のIT利用に関わることについて課題感が強い。これらは人材不足やコストの上昇とは異なり内因的割合が高いので、企業自身、課題感を持つことも、有効な手立てができていないことが推測される。

ビジネスにおける現状の課題 (複数回答可)



ビジネスにおける最重要課題



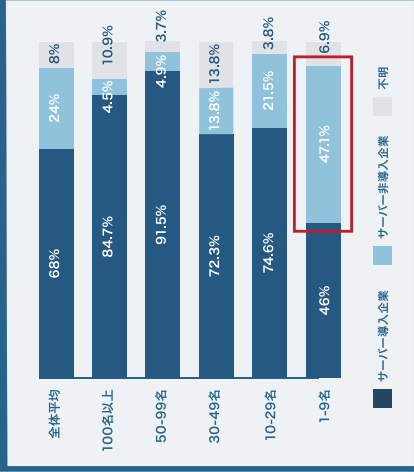
2 中小企業におけるサーバー利用の動向

サーバーの導入状況:

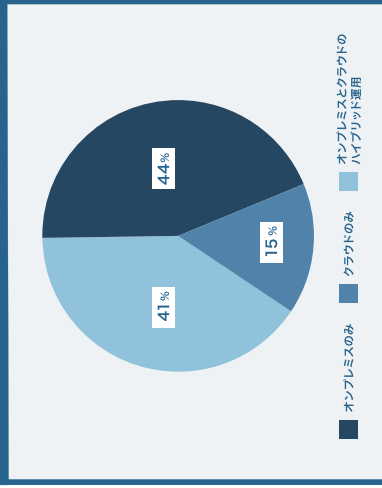
企業規模に比例してサーバー導入企業が増える根強いオンプレミスサーバーのニーズ

- 約7割の517社がオンプレミス、クラウド、もしくは両方のサーバーを導入している。
- 一方で、企業規模が小さな企業では未導入企業も多いことがわかる。特に9名以下の企業では半数が未導入。

サーバー導入企業と非導入企業の割合 (企業規模別)



サーバー導入企業における オンプレミスとクラウドの割合 (サーバー導入済み企業517社)



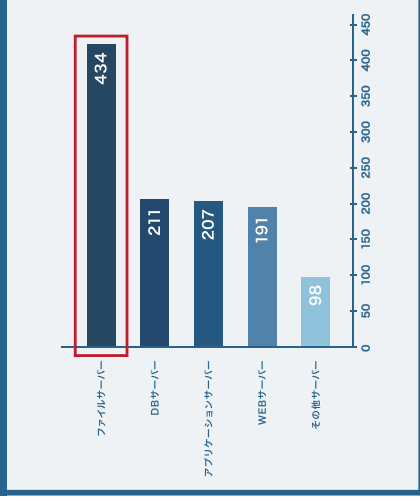
導入サーバーの種類: サーバー導入企業の8割が ファイルサーバーを利用

- サーバー導入企業517社中、8割の434社がファイルサーバーを導入。
- ファイルサーバー導入企業に絞ってサーバーの形態を調べてみると、ほとんどがオンプレミスサーバーを利用していることがわかる。これらから、ファイルサーバーの多数はオンプレミスサーバーで運用されていることがみ取れる。
- 当然ながらDBサーバー、Webサーバー、アプリケーションサーバーを導入している企業の割合は企業規模に比例するが、3種以上のサーバーを導入している企業は全て100名以上で、202社の約1/4にあたる45社に上る。一概には言えないが、これらの企業では業務のシステム化を強力に推進していることが伺われる。

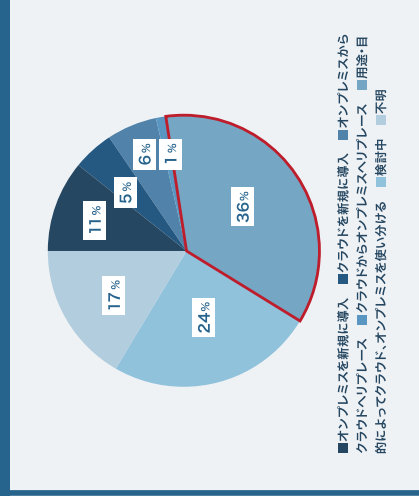
今後のサーバー運用形態: クラウドソフトより クラウド・オンプレミスの適材適所へ

- サーバー未導入企業を除いた574社に今後のサーバー運用形態を聞くと、約4割の企業がクラウドとオンプレミスを使い分けると回答。
- 一方でクラウド新規導入・オンプレからクラウドのようなクラウドのみといったいわゆるクラウドソフト的な運用に関しては消極的な結果が出た。
- 最近の円安によるクラウドサービスの値上げなどの影響もあり、全てをクラウドソフトするという考え方より、ファイルサーバーのようなクラウドでは割高なサーバーは従来通りのオンプレミス、Webなどのクラウドとの親和性が高いサーバーはクラウドサーバーを選択するという「適材適所」の使い分けが進んでいくとみられる。

導入サーバーの利用用途 (母数:サーバー導入済み企業517社複数回答可)



今後のサーバー運用形態 (母数:サーバー導入済み企業517社)



もはや企業規模は関係ないセキュリティリスク サブライチエーン攻撃の脅威

中小企業こそが狙われるサブライチエーン攻撃

サブライチエーン攻撃は年々増加傾向にあり、毎年大規模な被害が報告されています。IPA(独立行政法人情報処理機構)が毎年発表している情報セキュリティ10大脅威[組織編]でも6年連続で10大脅威として選定されており、最新の2024年度版では、ランサムウェアに次いで2位に位置づけられています。

ところでサブライチエーン攻撃とはどのようなものなのでしょうか。ご存じの方も多いとは思いますが、おさらいとして簡単に説明します。

サブライチエーン攻撃とは標的とする大企業を攻撃するために、その子会社や比較的規模の小さな取引先企業を踏み台として使う攻撃手法です。一般的に大企業は情報セキュリティ対策がしっかり行われ、攻撃に対する守りが堅固ですが、その子会社や取引先企業では、大企業ほど情報セキュリティが十分ではない場合があります。攻撃者はそこを狙って攻撃をかけて来ます。セキュリティ的に弱い会社の情報システムに侵入することで、サブライチエーンの内部に入り込み、比較的防御が薄い内側のネットワークやシステムを使って大企業を狙います。このことからサブライチエーン攻撃と呼ばれるままです。つまり、今は中小企業こそがサイバー攻撃の対象にならざるを得ないということです。

ウイルス対策ソフトだけでは守りきれない

ウイルス対策ソフトは今や Windows 10 / 11 にも標準でインストール (Windows Defender) されており、もはや入っていないパソコンは皆無ですが、アンケート結果にもあったように、ウイルス対策ソフト以外は何も対策していない企業も数多くありました。

しかし、高度化、巧妙化するマルウェアの全てをウイルス対策ソフトで防ぐことはほぼ不可能となっています。そこで現在では何段階も防御手段を講じる、多層防御が情報セキュリティの常識となりつつあります。

これは「スイスチーズモデル」とも呼ばれています。大きな穴の空いているスイスチーズでも、スライスして穴の位置をずらして重ねることで、穴を通り抜けることが難しくなることから名前がつけられており、このスライスしたチーズ1枚1枚がセキュリティ対策を意味しています。

このように、複数のセキュリティ対策を講じることが、サブライチエーン攻撃を含めた情報セキュリティ対策として重要だということを確認する必要があります。

攻撃者は常に脆弱性を狙っている。対策として重要な Windows Update。

もう一つ確実にしておきたい情報セキュリティ対策が Windows Update の品質向上アップデート (QU) です。実は、サイバー攻撃の多くは既知の脆弱性を狙ったものです。その理由は、知られている脆弱性のほうが攻撃しやすいからという単純なものです。とはいえ、意外と Windows Update を行っていない企業は少なくないようです。2017年に世界的な被害をもたらしたランサムウェア WannaCry は、その数か月前にMicrosoftから脆弱性を解消するセキュリティパッチが配布されていたものの、それをインストールしていないPCが次々と感染して被害を広げました。この事例からもわかるように、脆弱ではありますが、Windows Update をしっかり実施することもサイバー攻撃対策として重要です。もちろん、これらの対策を行っても100%確実にサイバー攻撃からシステムやパソコンを守ることはできませんが、可能な限り情報セキュリティリスクを低減するために欠かせない対策と言えるでしょう。

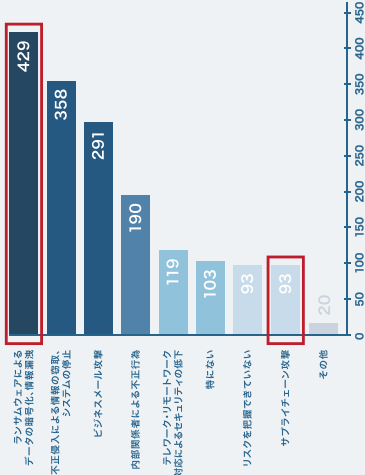
3 中小企業におけるセキュリティ対策動向

セキュリティリスクへの認識

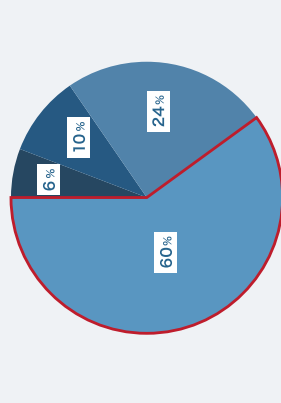
ランサムウェアやサイバー攻撃、ビジネスメール攻撃に高い懸念

- ランサムウェア攻撃や不正アクセスによる侵入はメディアで報道されることも多いことから関心度が高いと思われる。ビジネスメール攻撃についても同様と推察される。
- 一方で、近年中小企業が標的とされることが多いサブライチエーン攻撃への関心度の低さが気にかかる。よりリスク意識を高める必要があると考えられる。
- また、企業規模が大きくなると増えてくるのが、内部関係者による不正行為。情報システムに関わる人員が増えるとそれに比例してリスクも高まることから、セキュリティマネジメントの難しさを感じさせる。

情報セキュリティでリスクと感じているサイバー攻撃 (複数回答可)



情報セキュリティ対策に対する取組状況



■セキュリティ専任チーム・部門を設置して対応している
 ■サイバーセキュリティセンターなどを選定して導入している
 ■外部のセキュリティベンダーを利用している
 ■セキュリティ対策ソフトは導入しているが、それ以外は特に対応していない

情報セキュリティ対策の現状 リスク意識が高い一方で、 不十分なセキュリティ対策

- 情報セキュリティ対策として圧倒的に多いのがウイルス対策ソフトの導入のみ」という回答。全体でも60%の企業が、50名以上の企業に限っても4割近い企業がこのように回答している。
- 多くの企業がリスクと考えているランサムウェアや不正侵入、ビジネスメール攻撃はいずれもウイルス対策ソフトのみでの対策では不十分とされており、少なくともセキュリティ機器の導入など、いわゆる多層防御のセキュリティ体制を整える必要があるが、社内にもその知識やノウハウが不足している点が見られる。

4 中小企業におけるITインフラの運用管理

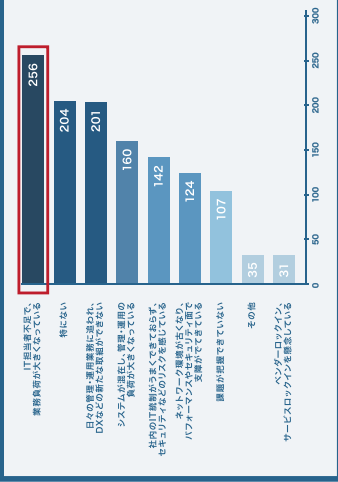
IT人材の不足がDX推進への妨げに
一方で運用管理業務は
負担の大きな自前主義が主流

- 多くの企業でIT人材の不足によるシステム管理担当者の業務負担の増大や、DXへの取り組みができないうという課題感を持っている。
- 一方で特に課題はないという企業も多い。特に9名以下の企業は44.2%が特に問題ないと回答している。9名以下の規模では、専属のシステム管理担当者が不在の可能性もあり、ITインフラと呼ばれるものが導入されていないなどという見方が可能と思われる。セキユリティやネットワークなどに対し「こんなものだろう」「これでもいい」というような課題が顕在化できていないことも推測される。

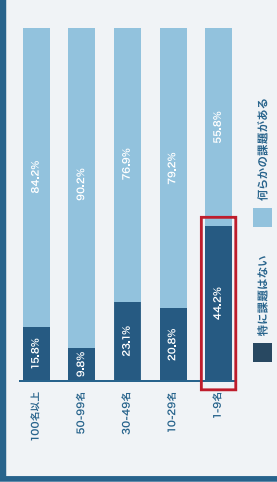
- IT人材不足が顕在化する中で、その解決法の一つとして考えられるアウトソーシングサービスを利用している企業がどれほどあるのか、パソコンの運用管理業務を例に取ってみると、実に全体の約65%にあたる489社が、特ににも利用していないと回答、自前主義が多いことが伺われる。

慢性的なIT人材の不足は長く言われており、決定的な解消策がない中で、これらのサービスの活用により、システム管理担当者の業務負担を軽減し、DX推進へのシフトが可能になる。特に比較的規模の大きな企業では導入検討の余地があるだろう。

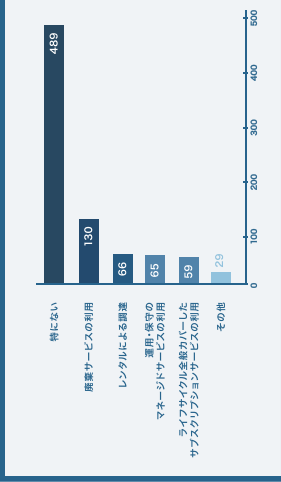
ITインフラの管理・運用に対する課題
(複数回答可)



ITインフラ運用管理の課題感の有無
(企業規模別)



パソコンの運用管理負担を軽減する
サービスの活用状況



生成AIへの取り組み

生成AIの登場と急激な普及により、ビジネスへのAI導入が身近なものになってきました。生成AIを始めとするAI技術の成熟により、これまでパソコンが苦手としてきた非定型業務のシステム化や、既存の概念を覆した発想に基づく新たなクリエイティブの実現が可能となってきています。

その一方で、その活用にはまだまだハードルが高く、実際のビジネスにおけるAI活用の事例は極限られた物となっています。

今回の調査では、中小企業におけるAI導入の現状とその課題について調査を行い、ビジネスへのAI導入推進の糸口を探りました。

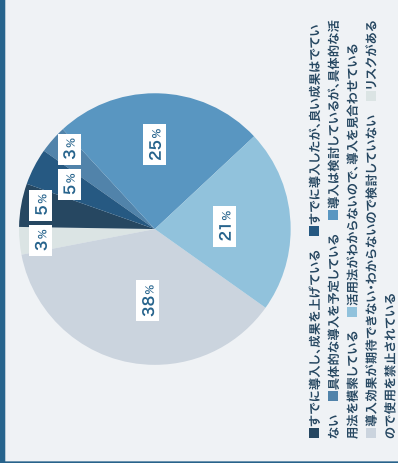


1 生成 AI への取組状況

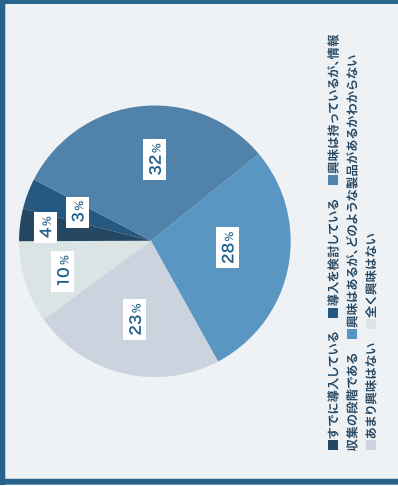
6割の企業がAI導入に興味・関心を持ち、4割の企業が導入・検討中 具体的な活用に関する情報不足が導入の障壁に

- AI製品に対する興味・関心度は高く、6割強の企業が何らかの形で興味を持っているが、活用方法が見いだせない企業も多い。
- 生成AIは10%の企業がすでに導入を開始。ただし実際の導入成果を上げることができていない企業はその半数程度。
- 一方で活用方法がわからない、効果が期待できないということ
で生成AI導入に消極的な企業も約6割あり、AI活用製品同
様に具体的な活用方法や導入事例が求められていることがわ
かる。

生成AIの導入状況



AI活用製品への関心度

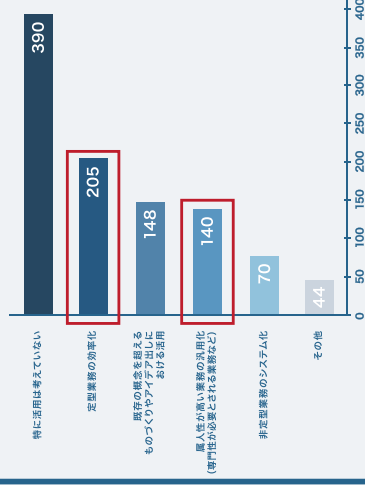


2 生成 AI の活用動向

人材不足を補う業務への活用に期待

- 生成AIを活用、もしくは活用を検討している業務として期待されているのは、定型業務の効率化や、属人性の高い業務など、現在生産性が課題になっている実務への導入であることがわかる。また、AIが得意とする非定型業務のシステム化も期待されている。これらへの導入・活用が進むことで、人材不足を補う効果が期待される。
- 一方で生成AIが得意とされるクリエイティブ性の高い業務への活用も期待されている。チャット型の生成AIは「アイデア出しの壁打ち役」としてすでに活用している人も多く、他方、CADなどで生成AIによる斬新な設計を支援するツールもできており、今後はこの分野の発展も期待できる。

生成AIの活用業務領域 (複数回答可)

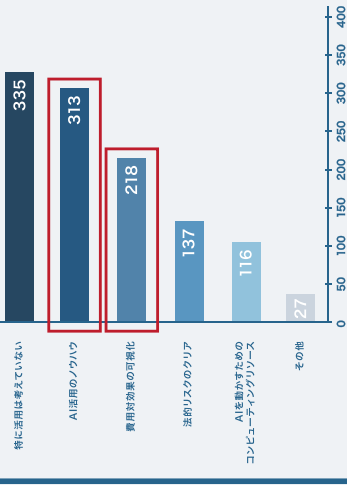


3 生成 AI 導入・活用に向けての課題

生成AI導入のノウハウや効果の情報を渴望

- これまでの設問と同様に、ビジネスにおける生成AIの普及には、活用のノウハウや、費用対効果の可視化が多く求められていることがわかる。活用を考えていない企業も一定数いるが、AIに対する興味・関心度の高さを踏まえると、これらの情報が充実することで、より導入への機運は高まると見られる。
- 2024年秋よりAI処理プロセッサNPUを搭載したパソコンが登場し、Windows 11にも生成AI Copilotが統合されたことから、より生成AIを始めとするAI環境は身近になってくる。これらが活用されることで、今後AI導入へのハードルは低くなっていくだろう。

自社のビジネスにおいて 生成AI活用に必要なもの (複数回答可)



総括

進みつつある Windows 11 への移行

全体の約5割のPCがすでに何らかの Windows 11 への対応を終えており、また、コストや工数などの理由から対応が進んでいない企業においても、2025年10月の Windows 10 サポート終了までにはほとんどの企業が対応を終えるとしています。全体的に Windows 7 のサポート終了時より速い動きと言えるでしょう。

コラムでも紹介した「WannaCry」のように、サポートを終了したOSほどリスクが高いものはありません。攻撃者は Windows 10 のサポート終了後に Windows 10 の脆弱性を狙ったさまざまなランサムウェアを使っていくことが予測されます。

したがって、サポート終了以降も Windows 10 の利用を考えている方は、ぜひサポート終了前（Windows 11 対応をおすすめします）。

ITインフラはクラウドとオンプレミスの使い分けがキーに

サーバーは企業規模により導入・未導入の差はありましたが、導入企業においては依然オンプレミスサーバーの需要が高いことがわかりました。

主にファイルサーバー用途が多いと想定されますが、クラウドサーバーのコストが上昇傾向にある今、コストが固定化できるオンプレミスサーバーの選択は適切と言えるでしょう。

一方で、クラウドサーバーの利用も一定数あり、またクラウドとオンプレミスを併用している企業も多いことから、使い分けをしているというのも印象的でした。

クラウドとオンプレミスを「適材適所」でうまく使い分けすることで、運用負荷軽減とコストのバランスを取りながら運用するのが理想と言えるでしょう。

DX推進はシステム関連業務の負荷軽減が不可欠

パソコン、ITインフラに限らず、システム管理担当者の負荷が大きいきことが明らかになりました。他の業務との兼務や、社内で一人だけのシステム担当者が多い中小企業において、パソコンのリブレースやトラブル対応、ITインフラの維持管理などの運用管理業務で手一杯という管理担当者も多いでしょう。一方でDX推進役としてのIT人材として期待されるのもシステム管理担当者です。人材不足の今、それを解消する手法としてのDXは企業の存続にも関わるものです。もちろんコストとの兼ね合いもありますが、アウトソーシングサービスなどを活用し、人材確保の難しい貴重な社内IT人材を可能な限りDX推進に当たらせることは経営者の役目ではないでしょうか。

生成AI普及の鍵は活用事例とノウハウの普及

生成AIに関しては事例やノウハウなどの情報不足による「使い控え」があることがわかりました。確かに現状の生成AIは使い方にコツが必要で、また導入効果についても可視化された情報はあまりありません。

一方で、Copilotなど、無料で気軽に使える生成AIも多くあります。またCopilot+ PCのようにAI対応のPCも登場し始め、今後AI対応のアプリケーションも増えてくることでしょう。

人材不足の切り札の一つとして、AI活用による業務効率化は大いに期待できるテクノロジーです。ぜひ怖がらず、まずは無料で使えるチャット型の生成AIから活用を始めてみてはいかがでしょうか。



デル・テクノロジーズ株式会社

〒100-8159 東京都千代田区大手町一丁目 Otemachi One タワー 17 階

●Dell Technologies、Dell、EMC、及びDell EMCが提供する製品及びサービスにかかる商標は米国Dell Inc.又はその関連会社の商標又は登録商標です。●Intel、インテル、Intel ロゴ、Ultrabook、Celeron、Celeron Inside、Core Inside、Intel Atom、Intel Atom Inside、Intel Core、Intel Inside、Intel Inside ロゴ、Intel vPro、Itanium、Itanium Inside、Pentium、Pentium Inside、vPro Inside、Xeon、Xeon Phi、Xeon Inside、Intel Optane は、アメリカ合衆国および / またはその他の国における Intel Corporation またはその子会社の商標です。●Microsoft、Windows、Windows 10、Oce ロゴ、Outlook、Excel、Power-Pointは、米国Microsoft Corporation の米国およびその他の国における登録商標です。●その他の社名および製品名は各社の商標または登録商標です。