

——アフターコロナ時代、本当にVDIのままで大丈夫？

コスト、パフォーマンスからセキュリティまで 調査で見えた、意外に多いVDIの課題とは

年間IT関連支出の1/4が VDIに費やされている

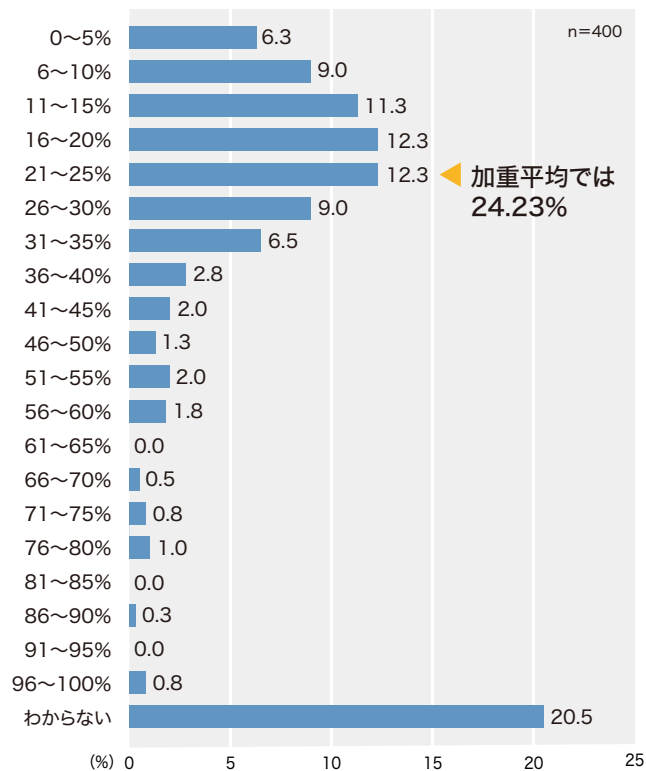
ローカルPCにデータを保管せず、画面情報のみを転送するVDI(Virtual Desktop Infrastructure)。テレワークの業務環境として、コロナ禍で導入が進んだこのVDIだが、その後の状況の変化に伴い様々な課題が見え始めている。

そこでZenmuTechは、2023年12月に「VDI市場動向調査」*を実施。今回は、この調査で見えてきたVDIの課題をひも解くことで、これからの時代に求められる業務インフラの姿を考えてみたい。

まず、多くの企業が気にかけているのがコストだ。年間のIT関連支出のうち、VDIのサーバー／ライセンスコストが占める割合は平均24.23%と、実に全体の1/4を占めることが分かった(図1)。

安定的なVDIの実施には、CPUやメモリに余裕のある高性能サーバーや高速・広帯域なネットワーク環境が必要になる。

図1 VDIのコストが年間のIT費用に占める割合



VDIを実施するコストは、年間のIT費用のうち、平均で24%に上る。ライセンス費用のほか、オンプレミス(自社サーバーなど)またはクラウド基盤の費用、シンクライアントPCなどのコストが必要だ。

そのため多くの投資が必要になるが、この状況がDX推進のボトルネックになっている企業は、決して少なくないだろう。

66%が「稼働しないアプリ」を経験 情報漏えい対策も十分とはいえない

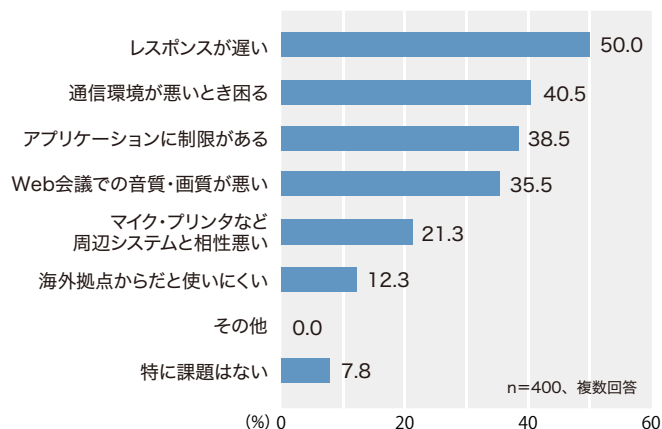
パフォーマンスの面でも課題が見えてきた。「VDIで稼働しないアプリケーションがあるかどうか」を尋ねた質問には66%が「ある」と回答。具体的には、会計・経理・総務系アプリ、自社開発アプリ、業務系アプリなどがその例として挙げた。

原因はVDIとアプリの相性が合わない、サーバーやネットワークのスペック不足などいくつか考えられるが、いずれにせよアプリが使えなければ業務効率は大きく下がる。これを防ぐには、VDI導入時に十分な検証を行う必要があるが、IT部門としてはそこに多くの工数をかけるのも避けたいところだろう。

さらに、アプリ自体は動くが便利に使えていない企業も多かった。「レスポンスが遅い」(50%)、「通信環境が悪いとき困る」(40.5%)などは、いずれもVDIのサーバーやネットワーク環境に起因する課題といえる(図2)。

加えて、コロナ禍以降はWeb会議ツールが広く普及したが、これをVDIで使う際は、動作を安定させるために映像をOFFにする運用がよくみられる。その背景にあるのが「Web会議での音質・画質が悪い」(35.5%)という実情だろう。ツール本来の価値を引き出せないことも、無視できないVDIの課題といえる。

図2 VDIの利用に関する課題

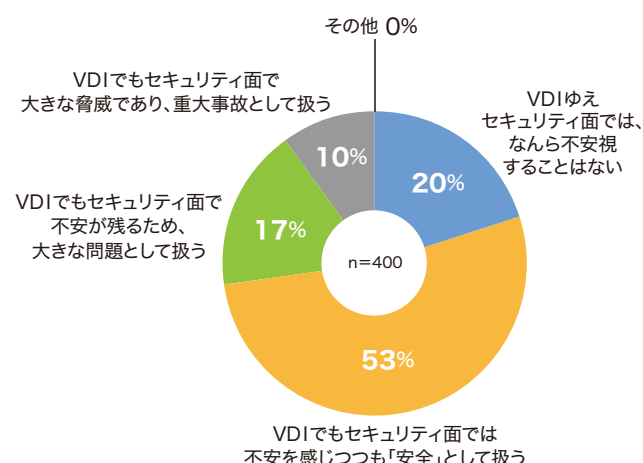


テレワークが当たり前のものになる中、VDIの利用に課題を感じる企業が多い

そして、もう1つ重要なのがセキュリティである。VDIの導入目的に「セキュリティ」を挙げた人は70%に上ったが、一方で、導入後「VDIゆえセキュリティ面では、なんら不安視することはない」と答えた企業は20%に留まった(図3)。

もちろん、シンクライアントを用いるVDIの場合、仮にPCの盗難・紛失が起ころとも情報漏えい事故には直結しないと考えることもできるだろう。だが実際は、ネットワーク接続すればデータにアクセス可能なため、リスクがないわけではない。事実、「VDI環境にあるPCの盗難・紛失を、セキュリティポリシー上どう位置付けるか」を聞いた別の質問では、VDIであっても「大きな問題／重大事故として扱う」が計27%存在した。つまり、情報漏えいを厳格に防ぎたいければ、VDIを使うだけでは不十分だという認識が、既に一定数の企業の間で共有されていることが分かる。

図3 VDI環境にあるPC盗難・紛失時の認識

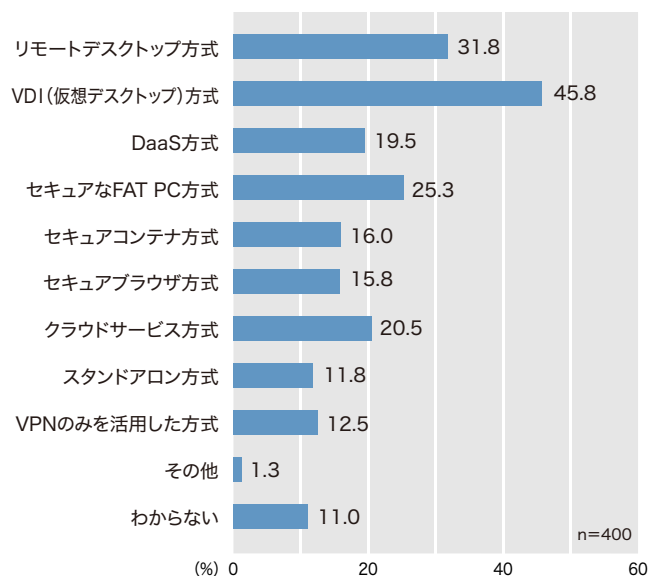


新時代の働き方を模索する中で注目を集めるセキュアFAT PC

また、コロナ禍では緊急時対応の一環としてVDIを導入した企業が少なくない。「業務を止めない」ことが最優先の状況で、仕組みの特徴を精査できなかったケースもあるはずだ。調査でも、「VDIのメリットや内容を理解していない」と答えた人は全体の約40%にのぼっていた。

テレワークとオフィスワークのハイブリッド型の働き方が重要度を増す中、果たしてVDIは今後も継続的に使えるものなのか。改めて、そのメリット／デメリットや投資対効果を精査することが、より一層の業務効率化や、全社のDX推進に向けて不可欠になっている。

図4 VDI導入企業が次回の採用を検討する方式



次回もVDI方式を採用すると答えた企業は多いが、既存のFAT PCを使い、データセキュリティ機能を付加したセキュアFAT PC方式も選択肢の1つとなる

さらに調査では、利用中のVDIが更新時期を迎えた場合、次に採用したい仕組みは何かについても質問した(図4)。ここで注目したいのはVDI(45%)、リモートデスクトップ(31%)に次ぐ3番目に、「セキュアFAT PC」(25%)が挙げたことである。

セキュアFAT PCとは、一般的なPC(FATクライアント)に強力なセキュリティ機能を付加することで、安全に業務を遂行できるようにする方式のこと。FATクライアントならではの利便性と、高い安全性を両立するものだ。

ZenmuTechは、セキュアFAT PCのソリューションである「ZENMU Virtual Drive」を提供している。このソリューションは、独自開発の秘密分散技術によって、ローカルPC内の情報を「無意味化」する。そのため、たとえ業務PCが盗難にあっても、悪意を持つ第三者が重要情報にアクセスすることはできない。また当然、日常的な業務やWeb会議などは一般的なPCと同じ感覚で行える。このようなソリューションへの入れ替えを検討することは、VDIの課題を解決する1つの糸口になるだろう。

アフターコロナ時代に突入し、社会やビジネスの環境変化がますます激しくなっている。時流に即した柔軟かつセキュアな働き方を確立することが企業の重要ミッションといえるだろう。VDI、リモートデスクトップ、そしてセキュアFAT PCなど、様々なツール・ソリューションを幅広く検討することで、自社にとって最適な環境を見出してもらいたい。