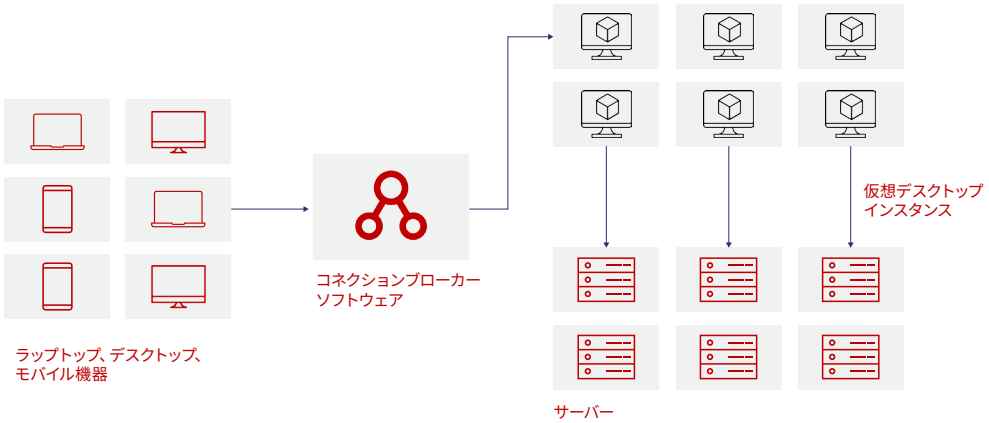
MENLO SECURITY

WhitePaper

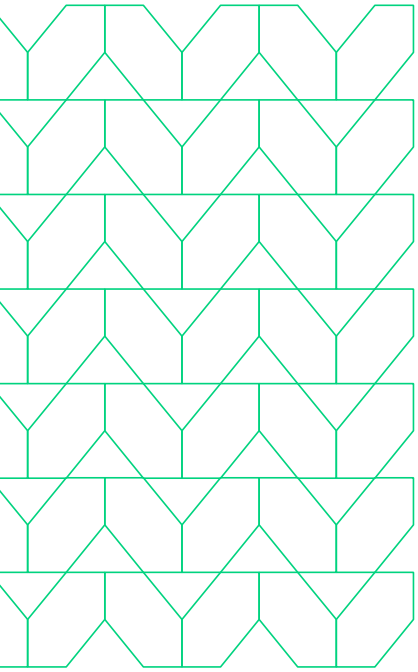
今日の企業における VDIの再考

仮想デスクトップ技術は長い歴史を持ち、広く知られています。シンクライアントを使ったリモートデスクトップ技術の始まりは1990年代にまで遡りますが、仮想デスクトップインフラストラクチャ（VDI：Virtual Desktop Infrastructure）という用語はVMwareが2006年に最初に使いました。それにシトリックスやマイクロソフトが追従することで、この用語が一般化しました。VDIはデータセキュリティおよびコンプライアンス、そして災害復旧と事業継続性を可能にするもので、開発された当時は非常に魅力的なソリューションでした。しかし、その後状況は大きく変わりました。ネットワークペリメータは消滅し、SaaSモデルの登場によって最新のアプリケーションがクラウド上に置かれるようになり、その多くにブラウザ経由でアクセスするようになったのです。

これらの技術は、コロナ禍の下で利用が急拡大しました。多くの企業が、ほとんど一夜にして、安全なリモートアクセスソリューションを構築する必要に迫られたのです。Computerworld誌は2020年に「…企業のすべての従業員が自宅から企業ネットワークに接続するようになりましたが、従業員はVPNを備え安全なアクセスのために設定済みの会社支給のデバイスを使わない場合もあるため、VDIが見直されています。」と書いています。[1]



[1] Pandemic gives VDI a new lease on life, Computerworld, Sept 23, 2020, https://www.computerworld.com/article/3574938/pandemic-gives-vdi-a-new-lease-on-life.html

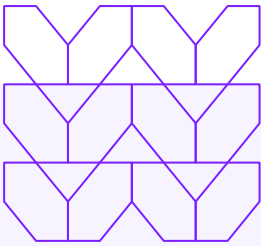


クラウドであれオンプレミスであれ、VDIソリューションをサポートするインフラストラクチャには、クライアント、コネクションブローカー、仮想マシン、ハイパーバイザーが含まれます。ユーザーはクライアント（エンドユーザーデバイス）から、仮想マシン上の仮想デスクトップやアプリケーションにアクセスします。

コネクションブローカーは、エンドユーザーデバイスと仮想マシンおよびハイパーバイザーの間を接続します。コネクションブローカーはまた、認証と認可に加え、デスクトップセッションとプール、またはデスクトップを管理します。

仮想マシンは、それぞれ独自のOSとアプリケーションを持ち、個別に設定されています。最終的なコンポーネントには、物理サーバーとハイパーバイザー（サーバーのコンテンツを仮想マシンに分割する）が含まれます。

VDIは、企業のデータセンターでオンプレミスでホストされるように設計されていますが、この技術のクラウドベースのバージョンも存在します。VDIシステムがどこに導入展開されたとしても、企業側はハードウェア/ソフトウェアライセンス、およびネットワークインフラストラクチャに取り組まなければなりません。そしてそのためには、仮想化やネットワークエンジニアリング、そしてコンピューターシステムおよびセキュリティの各分野でクロストレーニングを受けた熟練スタッフのような、ただでさえ不足しているリソースを継続的に確保する必要があります。さらに、VDIソリューションのさまざまな要素をインストールし、導入展開して管理/運用するためのスタッフも必要で、それにも多大なコストがかかります。これらのスタッフはまた、ハードウェアのプロビジョニング、ソフトウェアのアップデート、セキュリティのアップグレードのような日常的なメンテナンスを行うよう依頼される場合もあります。



Desktop as a Service (DaaS)

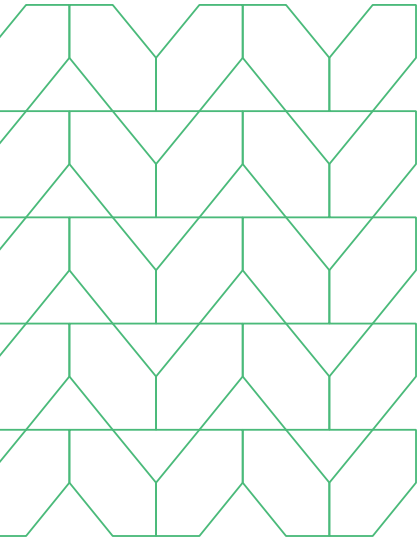
エンドユーザーにとって、VDIとDaaSの違いはほとんどありません。しかし、セキュリティ、IT、およびインフラストラクチャチームにとっては、その差は非常に大きなものです。VDIはシングルテナントとして設計されていますが、DaaSソリューションは管理されたマルチテナントです。

しかし、違いはそれだけではありません。DaaSの本質は、第3者によって管理されているVDIであるということができます。VDIは、たとえば従来型のコールセンターのユーザーなど、限られたアプリケーションを使用するような一部のユーザープロファイルには有効です。一方でDaaSは、企業の管理負担を軽減し、その分を従量制の運用料金と引き換えにしているだけという見方もできます。ハードウェアとソフトウェアは第3者によって提供されるため、選択肢が限られます。さらにこの第3者は、コンプライアンスとデータ主権に加えて、管理、メンテナンス、バックアップ、アップグレード、セキュリティポスチャ、脅威への対応も監視します。しかし、一般的な企業ではこれらの責任をクラウドサービスに委譲することができないため、DaaSは多くの場合選択肢になりません。

現時点では、VDIとDaaSのどちらを選ぶべきなのでしょうか?

現時点でVDIを導入することが適切な選択なのかどうかを判断するために、VDIが何のために設計されたのかを考えてみましょう:

- シンクライアントやBYODのエンドポイントを使用することにより、全従業員に専用のPCを提供するよりもコストを削減できる
- 企業のインフラストラクチャを一元的に監視/管理/バックアップできる
- エンドユーザーに安全なリモートアクセスを提供できる



コスト

コストの削減は、VDIベンダーが当初から主張していた重要なポイントでした。この主張の根拠は、VDIには次のようなメリットがあるというものでした:

- **管理およびサポートコストを削減できる:** しかし、このメリットを享受できるのは、企業に十分な規模のエンドユーザーが存在し、VDIを実装するための多額のコストと労力を正当化できる場合に限られます。VDIを正当化できる状況は現在でも存在しますが、ユーザー数は以前よりもはるかに少なくなるでしょう。また、VDIはどのような形態であっても「one-and-done (一度で終わり)」というものではない、ということを認識することも重要です。VDIの世界では、ネットワークやコンピューティングの他の側面と同様に、状況は常に変化するからです。
  もうひとつの重要な、そして見落とされがちな要素は、一元化されたインフラストラクチャのメンテナンスには、一般的なデスクトップの管理に必要なスキルセットとはまったく異なるスキルセットが必要であるということです。VDIソリューションを構築したことのある管理者なら誰でもわかっているのは、適切なエンドユーザーエクスペリエンスを提供するためには最初のインフラストラクチャの選択時をはるかに上回る要素が必要であり、セットアップやメンテナンスが予測できないものになる可能性があるということです。さらにやっかいなのは、エンドユーザーの満足度に最も大きく影響する要素の中に、企業が制御できない要素があることです。このシステムには、広い帯域幅や低遅延のインターネット接続、十分なコンピューティングリソース、高速なストレージ、安全なセットアップ、そして絶え間ないパッチ適用が必要なのです。

- **メンテナンスコストを削減できる:** VDIを導入しても、アップグレードやメンテナンスの作業が不要になるわけではありません。それらは単に、インフラストラクチャの他の部分に移動されるだけです。メンテナンスとアップグレード、およびそれらを実装するためのスタッフが、全体のコストを大幅に上昇させる可能性があります。他の一元化モデルと同様に、インフラストラクチャの一部に問題が発生するとすべてのエンドユーザーに影響がおよぶため、VDIの導入展開の状況を常に把握しておくことが特に重要です。

- **ハードウェアコストを削減できる:** 当初のアイデアは、大量のエンドユーザーデバイスを購入する代わりに、堅牢な中央のインフラストラクチャに投資するというものでした。この考え方は、この技術が開発された当時は正しかったかもしれませんし、今でも当てはまる部分があるかもしれません。しかし、これまでVDIを利用してきて明らかになったのは、エンドユーザーをサポートするために必要なサーバーのコストは、多くの場合、デバイスを購入するよりも高くつくということです。程度の差はありますが、クラウドベースのVDIにも同じことがいえます。

セキュリティ

- **セキュリティを強化できる：**セキュリティの強化は、昔からVDIを導入する理由のひとつです。資産を一元管理し、エンドユーザーのデスクトップを制御してバックエンドシステムへのアクセスを強化できるため、企業の資産はより安全になるという考え方でした。盗難や紛失の可能性があるエンドユーザーデバイスが存在しないということも重要なポイントです。しかし、VDIシステムそのものがハッキングされる可能性があるということも忘れてはいけません。攻撃者が一元管理された資産へのアクセスに成功した場合、より大きな標的が狙われる可能性があります。バックエンドシステムに侵入しなくても、エンドポイントとの間のデータ転送を介してデータの流出やその他のリスクが発生するかもしれません。そして、ソリューションのいずれかの要素がハッキングされた場合、事実上すべての要素がハッキングされることになります。

エンドユーザー

VDIが最終的に成功するか否かは、多くの場合エンドユーザープロファイルの分配にかかっています。ユーザーが特定のアプリケーションやパーソナライズされた設定、そして平均以上の計算能力を必要とする場合、VDIの管理は多数の企業向けワークステーションを管理するよりも遙かに難しくなる恐れがあります。もうひとつの懸念は、技術的に洗練されたユーザーほど、VDIの実装がロックダウンされていることに反発する可能性が高いことです。

- **リモートワーカー：**コロナ禍においてVDIがこれほどまでに普及した最大の理由のひとつは、リモートワークの急増です。企業はリモートワークを可能にするためにVDIを採用しましたが、ハイブリッド/リモートワークが定着し、多くの企業はその環境を維持しています。VDIはリモートワークを技術的にはサポートできますが、ユーザーはそのエクスペリエンスに満足しないことが多く、これらのデバイス上の管理されていないブラウザがもたらすセキュリティリスクが脅威となっています。特にモバイルのユースケースで、VDIはパフォーマンスが低いことが知られており、アプリケーションの動作が遅くなったり完全に停止したりするため、ユーザーに敬遠されることがあります。

- **柔軟性：**VDIインフラストラクチャは企業の俊敏さを高めると考えられており、過去には実際にそういった例もありました。たとえば、キャンパス内または固定された物流環境で派遣契約社員向けにアプリケーションをプロビジョニングする場合、この技術は期待どおりに機能しました。しかし、ソリューションの実装対象である社員のプロファイルが全体と適合していなければ、これらのメリットは簡単に損なわれてしまいます。VDIが実際に提供しているシート数を正確に把握するのは難しい場合があり、VDIインフラストラクチャとエンドユーザーデバイスの管理がどちらも必要になるという、最悪の事態に陥る可能性があります。

仮想化デスクトップの復活

VDIは、コロナ禍によってアプリケーションやリソースへの安全なアクセスを（突如として）必要とするようになったリモートワーカーからのニーズによって第2の人生を歩み始めましたが、この技術は数十年前から存在していたものです。DaaSは本質的には第3者によって実装され管理されているVDIということができ、VDIと同じメリットを見かけ上低価格で提供するものです。クラウドベースのアプリケーションへの移行がそれほど進んでいなかったことを考えれば、これらが求められたのは当然のことでした。しかし、現代の企業が優先すべき事項と、今ではほとんどのクラウドベースのアプリケーションがブラウザ経由でアクセスできるようになったことを考えた場合、仮想デスクトップの一元的な導入展開は本当に費用対効果が高いのでしょうか？ また、必要なのでしょうか?

企業には、特定の業界に合わせてカスタマイズでき、新たなコンプライアンスとデータ主導のニーズを考慮した安全なソリューションが必要です。完全なフォレンジックを行う能力とともに、エンドツーエンドの可視性が不可欠です。そして、企業資産を意図的または不注意による侵害から保護する必要があります。

最後に重要なのは、これらのソリューションが、それを使用する必要があるエンドユーザーにどの程度受け入れられるかということです。パーソナライズされたデバイスが最適と考えるユーザーにとっては、新しいオペレーティングシステムを習得しなければならないことが問題に映るかもしれません。さらに、VDIとDaaSの両方共に、パフォーマンスの問題に悩まされているという事実があります。仮想化デスクトップは利用のピーク時にアプリケーションの動作が遅くなることが多く、ユーザーはフラストレーションを感じています。

もっと良い方法とは

今なら、もっとシンプルなソリューションがあります：SAA（Secure Application Access）を備えたMenlo SecurityのSecure Cloud Browserです。協力会社やパートナーなどのユーザーは、会社支給のデスクトップや自身のBYODデバイスで作業することができます。SAAはSSHやRDPプロトコルを含む一般的なアプリケーションへのアクセスを提供し、企業データを保護して、アプリケーションを侵害されたエンドポイントから守ります。また、SAAはユーザー自身のエンドポイントに加えて、ユーザーがすでに

使っているブラウザとも連携するため、ユーザーの生産性も大幅に向上します。

SAAは、エンドユーザー以外にもメリットをもたらします。アプリケーションがブラウザベースのため、エージェントの導入や証明書のインポート、DNSの変更が不要となり、導入展開が容易です。さらにセキュリティおよびITチームは、読み取り/書き込み、アップロード/ダウンロード、コピー/ペーストなど、データやアプリケーションのきめ細かなコントロールが可能になります。その他のメリットとしては、ラストワンマイルまでのデータ漏洩防止（DLP）、コンテンツへの電子透かし適用、サンドボックス化などがあらかじめ組み込まれていることなどが挙げられます。SAAは、許可されたユーザーがアプリケーションを完全に利用できるようにすると同時に、インターネットの脅威から保護します。

Menlo Secure Cloud Browserは、最新の検知回避型脅威（HEAT：Highly Evasive Adaptive Threats）に対する保護をさらに強化し、信頼されたWebサイトから送信される高度なフィッシング攻撃などを阻止します。従来型のペリメータセキュリティやエンドポイントセキュリティではこれらの攻撃を検知できませんが、Menlo Secure Cloud Browserはゼロアワー攻撃も含め、毎日のように攻撃を捉えています。Menlo HEAT Shieldが導入展開されていれば、侵入される前でもアラートを簡単に調査できます。また、Menlo Browsing Forensicsにより、エンドユーザーブラウザの不適切な挙動を簡単に調査できるようになりました。これは、どの企業にとっても大幅なリスク軽減となります。

受賞歴のあるSecure Cloud BrowserをベースにしたMenlo Secure Application Accessソリューションは、コストを節約するだけでなく、ITチームの負担も軽減できる完全なソリューションを提供します。監視と管理を一元化することで、VDIが持つ複雑さを排除して安全なリモートアクセスを実現します。エンドユーザーは優れたエクスペリエンスを享受し、ITチームは問題に迅速かつ容易に対応することができます。

現在のアプリケーションアクセスの問題を、過去の技術で解決しようとしないでください。Menlo Secure Cloud BrowserとSecure Application Accessがお客様にとって最適かどうか、是非ご確認ください。

MENLO SECURITY

お問い合わせ：
www.MenloSecurity.jp
japan@MenloSecurity.com

Menlo Securityについて

Menlo Securityは、Menlo Secure Cloud Browserによって高度に回避的な脅威を排除し、生産性を維持します。Menlo Securityは、クラウドベースのセキュリティが目指す、導入展開が容易なゼロトラストアクセスを実現します。Menlo Secure Cloud Browserは、エンドユーザーがオンラインで業務を行う間、ユーザーからは見えない形でサイバー攻撃から防御し、同時にセキュリティチームの運用負担を軽減します。

Menlo Securityは、ユーザーを保護してアプリケーションへのアクセスを確保し、完全なエンタープライズブラウザソリューションを提供します。Menlo Securityなら、ワンクリックでブラウザセキュリティポリシーを導入することができ、SaaSやプライベートアプリケーションへのアクセスを保護して、ラストワンマイルまで企業データを守ります。信頼と実績のあるサイバー防御により、あらゆるブラウザでデジタルトランスフォーメーションを保護します。Menlo Securityと共に、安心してビジネスを前進させましょう。