3 テレワーク関連ツールの特徴比較

3.1 システム方式

図表 3-1では、データやソフトウェアにネットワーク経由で接続する代表的な方式について5つに区分して記載している。

1～5のいずれの方式で接続するかについては、テレワークの形態や社内のセキュリティポリシーに沿って検討する。

例えば、在宅でのテレワークでは、「1 リモートデスクトップ方式」により社内の業務ソフト等を利用し、併せて「3 クラウドアプリ方式」で提供されるグループウェアを利用すること等を検討する。

図表 3-1　システム方式

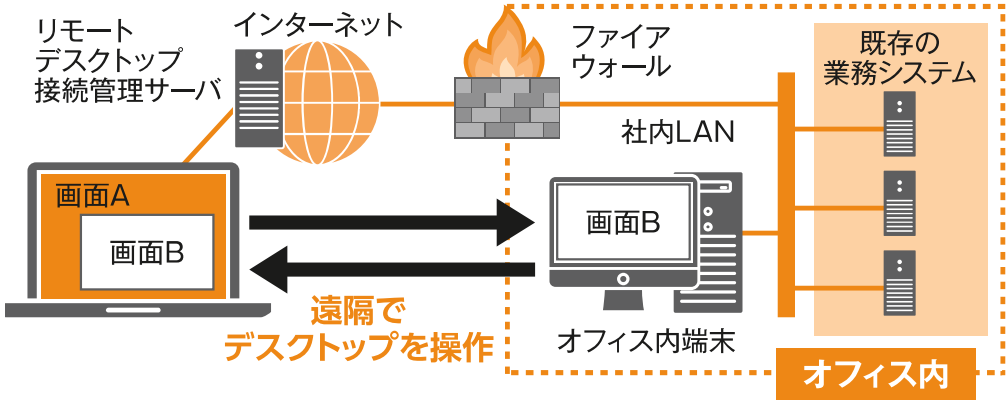
No	ツール	概略	テレワーク形態との関係	製品例
1	リモートデスクトップ方式	社内の通常のPCに外部のPC等からリモートログインする方式（画面転送）。 処理は社内のPCで実行される。 社内のPCにソフトウェアを導入することで実現が可能であり、仮想デスクトップ方式と比較して、導入までの障壁が少ない。 既存のPCやタブレットを流用することで1台あたり月額800円～1,500円程度のコストでの導入も可能であり、導入も容易。	形態にかかわらず、社内PCへの接続が必要なケースでは導入を検討する。 在宅勤務のみではなく、モバイルワークでのタブレットからの接続・利用も可能。	magicConnect/ NTTテクノクロス(株) Splashtop Business/ スプラッシュトップ(株) Remote View/ RSUPPORT(株) DoMobile／(株)日立ソリューションズ・クリエイト
2	仮想デスクトップ方式	サーバ内の仮想PCにリモートログインする方式（画面転送）。　処理は仮想PCで実行される。 新規システムの構築が必要であり、計画的な取り組みが必要となる。サーバが停止した場合の業務への影響が大きいため、慎重な対策が必要。 SIベンダー等に導入を依頼するのが一般的。 最近は、Amazon WorkSpacesのように　クラウドサービスとして1台から仮想デスクトップを提供するものも出てきている。	形態にかかわらず、サーバ側でPCの一元管理を重視する場合には、導入を検討する。 管理者等も必要になることから、中堅企業・大企業での導入事例が多い。	Citrix XenDesktop/シトリックス・システムズ・ジャパン(株) VMware Horizon 8/ ヴイエムウェア(株) Microsoft VDI/日本マイクロソフト(株) Amazon WorkSpaces/アマゾンウェブサービスジャパン(株)
3	クラウド型アプリ方式	外部業者の提供するサーバ及びソフトウェアをインターネット経由で利用する方式。 処理はサーバで実行される。自社で開発した既存の業務ソフト等多くのアプリは社内で稼動しており、この方式では利用できない。 クラウド型でも業務ファイルを持出す場合は、安全持出方式を併用することが望ましい。	形態にかかわらず、それぞれのセキュリティポリシーに応じて導入を検討する。	後述するグループウェアや会議システム等の製品の多くは、この方式で提供される。
4	安全ファイル持出方式	業務ファイルを外部PCに安全に持出して処理を行う方式。 処理は外部PCで実行されるが、業務ファイルは、外部PCのメモリ等に展開するだけで、終了時は安全な場所に書き戻す、あるいは秘密分散暗号化等を用いることで、安全性が高い。	形態にかかわらず、それぞれのセキュリティポリシーに応じて導入を検討する。	CACHATTO Desktop/e-Janネットワークス(株) WrappingBox/(株)ソリトンシステムズ Flex Work Place/横河レンタ・リース(株) @割符plus、ZENMU for PC
5	ファイル持出方式（ネットドライブやVPN経由持出）	社内で使用しているPCやタブレットを社外に持ち出す、あるいは、ネットドライブやVPNを用いて、社外のPC等に業務ファイル等をダウンロードして社外のPCで業務アプリを実行する。 使い慣れた端末の利用が可能。社内LANへの不正侵入対策や、PC紛失時のデータ漏洩対策等を慎重に行う必要がある。	形態にかかわらず、それぞれのセキュリティポリシーに応じて導入を検討する。	Dropbox、Googleドライブ、BOX、OneDrive等のネットドライブ経由 PacketiX VPN/ソフトイーサ(株)、Verona/(株)網屋、beat/富士フイルムビジネスイノベーションジャパン(株)等のVPN経由

(1)リモートデスクトップ方式

リモートデスクトップ方式のサービスでは、接続を認証するサーバが必要であり、サービスが使用できない場合に損失する時間・人件費等を勘案すれば、特にサーバの稼動・安定性を重視する必要がある。運用実績の面では、magicConnectが優れている。また、タブレットでの利用を重視する場合には、画面更新速度の速いSplashtop Businessが優れていると思われる。リモートWOL機能※を利用した場合、社内PCへの電源投入を外部から可能にし、電気代を節約できる。その他、それぞれの価格・特徴・試用時の画面更新スピード等を検討して選択を行う。

※リモートWOL機能とは、ネットワーク経由でのPCの電源投入機能。

図表 3-2 リモートデスクトップの仕組み



図表 3-3　リモートデスクトップ方式の製品例

No	製品名	比較項目						
		ファイル転送制限	タブレット対応	USBキーの使用	リモートWOL機能	価格(税別)	所要導入工程	特徴
1	magic Connect/ NTTテクノクロス(株)	設定可	指タッチ＋仮想マウス	可	可（オプション）	USB1台+タブレット初期費用15,000円、年額18,000円～	約1週間	2004年のサービス開始以来、トラブルによる停止の実績がない。国内導入企業数では最も多い。
2	Splashtop Business/ スプラッシュトップ(株)	禁止設定のみ	指タッチ	―	―	初期費用0円。年額15,000円～	3営業日程度	PC画面を高速に動画配信する技術を採用。(株)ソリトンシステムズ等から販売。
3	Remote View/ RSUPPORT (株)	設定可	指タッチ＋仮想マウス	―	可（オプション）	お問い合わせください	オンライン決済:即時振込等:3営業日	低回線速度(128kbps)からも利用可能。接続ログと統計情報を一度に確認。
4	DoMobile/ 日立ソリューションズ・クリエイト	設定可	指タッチ＋仮想マウス	可	可	初期:10,000円＋1,000円×ユーザ数。年額:18,000円/ユーザ	3営業日程度	強固なセキュリティに加えて導入の容易性を兼ね備えている。
5	Ninja Connect / e-Janネットワークス(株)		―	―		同時接続数 3ユーザ 7,500円/月	発注後営業日	Webブラウザからアクセスするので、USBの利用や新たなアプリのインストールは不要
6	シン・テレワークシステム/ IPA(情報処理推進機構)	設定可	―	―	可	無料	即日	新型コロナウイルス対策実証実験（IPA+NTT東日本）高性能。自治体利用実績あり。

※全ての方式で通信の暗号化は行われている。
※全て画面転送型。社内ファイルのダウンロード制限、コピー&ペースト制限については、いずれの製品でも可能。
※全てのサービスがタブレットにも対応。

(2)仮想デスクトップ方式

「Citrix XenDesktop」「VMware Horizon 8」「Microsoft VDI/Microsoft Virtual Desktop Infrastructure」の3製品が国内市場におけるシェアのほとんどを占めており、3製品で機能的には大きな差はみられないため、特に比較は行わない。

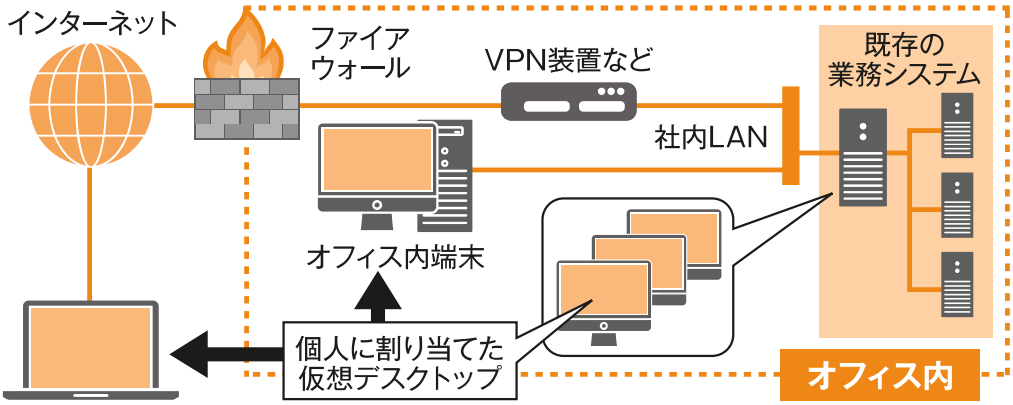
仮想デスクトップ方式については、従業員人数分の数十人、数百人単位で導入し、業務中のサーバ停止が多額の損失に繋がりかねないこともあり、導入コストは高額になるケースが多い。

「Citrix XenDesktop」「VMware Horizon 8」「Microsoft VDI/Microsoft Virtual Desktop Infrastructure」等の導入を手がけるSIベンダー等に対して、見積りやデモンストレーションを依頼し、処理スピードや導入料金・ライセンス料、継続してシステムを稼働させる能力・対策等を比較して導入を検討する。また、仮想デスクトップの画面制御の負荷が大きくなるので、仮想化されたGPUとして、NVIDIA社のvGPUも必要に応じて検討する。

新しい流れとして、Amazon WorkSpaces等のクラウドサービスでは、クラウドベースの仮想デスクトップを1台から実現できる。また実際に使用した分の料金を払う時間料金制も選べるので、小規模からの利用にも適している。

また、オンプレミス型の低価格の仮想デスクトップとして、SKYDIV Desktop Client（5ライセンスパック¥100,000から：ただし別途Microsoft社ライセンスが必要）などもある。

図表 3-4　仮想デスクトップの仕組み



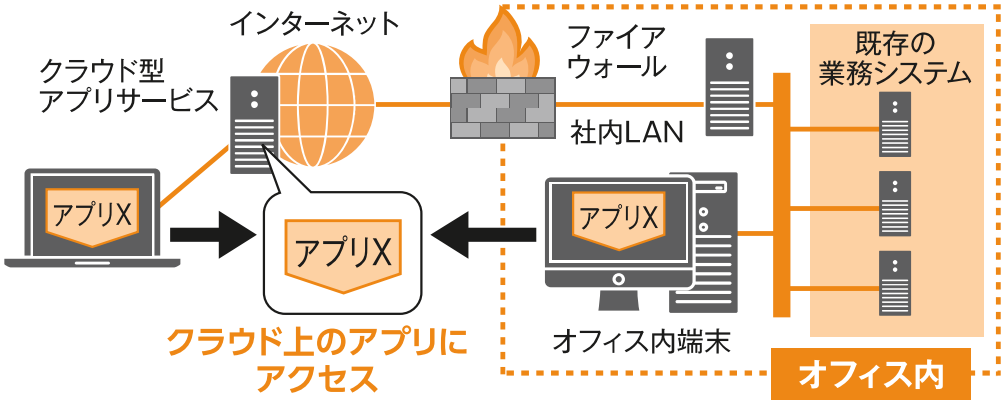
(3)クラウド型アプリ方式

外部業者の提供するサーバ及びソフトウェアをインターネット経由で利用する方式。

後述するグループウェアや会議システム等の製品の多くは、この方式で提供される。

なお、グループウェアや会議システム等については、労務管理ツールやコミュニケーションツールとして取りあげているため、ここでは記載しない。

図表 3-5　クラウド型アプリ方式の仕組み



(4)安全にファイルを持出す方式

業務ファイルを外部のPCに持ち出して、業務アプリも外部のPCで実行するが、安全のために、業務ファイルは、外部PCのメモリや一時ファイルの特定エリアに展開するだけに留め、終了時には元の安全な場所に書き戻し、外部PC上は全てを削除する。 ラッピング、セキュアブラウザ／コンテナ、ディスクレスPC、仮想データルームなどがこれに相当する。
(セキュアブラウザ／コンテナについては、「3.6 安全なモバイルテレワークツール」の項目を参照。)
また、暗号化や秘密分散技術により、安全に持ち出す方式もある。

図表 3-6　安全持出方式の製品例

No	製品名	比較項目		
		概要	価格(税別)	特徴
1	CACHATTO Desktop/e-Jan ネットワークス(株)	外部領域からのアクセスを制限したセキュアな仮想ワークスペース。社内のメールやスケジューラー、ファイルサーバーに社外から安全にアクセスできる。	お問合せ下さい	既存のファルサーバーやMicrosoft 365などのクラウドサービスとの連携もできる。
2	WrappingBox/ (株)ソリトンシステムズ	端末上に安全な「保護領域」を作り、その中でファイルの編集などのアプリを起動する。編集したファイルは会社のサーバーへ保存する。	WrappingBox ユーザライセンス 月額　1,000円／ユーザー	Microsoft365などが利用可能。
3	Flex Work Place/ 横河レンタ・リース(株)	デバイスからユーザデータを分離する「データレスPC」 PCのローカルキャッシュデータは自動的に削除される。	レンタル: 780円/月・ユーザ 購入(最小構成): 520,000円+18,000円／ユーザ	OneDriveなど Microsoft 365と連携可能。
4	＠割符plus (Tally To Go)/ ネクスト・シェアリング(株)	秘密分散暗号化技術を用いて分散管理する。通常の暗号化よりさらに安全にファイルを持出せる。	お問合せ下さい	紛失しても、重要インシデントとならない。
5	ZENMU for PC/ (株) ZenmuTech	秘密分散暗号化技術を用いて分散管理する。通常の暗号化よりさらに安全にファイルを持出せる。	お問合せ下さい	AONT(All or Nothing Transform)方式

(参考)ゼロトラスト アーキテクチャー

安全にファイルを持出す方式の新しい流れとして、「ゼロトラスト アーキテクチャー」という考え方がある。
現状のテレワークのセキュリティの考え方は、危険な「社外」から安全な「社内」を完全に分離して、
「社内」に閉じて作業を行うものが主流で、「リモートデスクトップ方式」や「仮想デスクトップ方式」が
その典型的な例である。
一方「クラウドアプリ方式」は、「社外」でのファイルのダウンロードなどが可能なものが多く、セキュリティ
(持出リスク)に問題があると考えられている。上の表のツールは、その持出リスクを少なくする技術を用いている。

「ゼロトラストアーキテクチャー」とは、性悪説によるもので、自由に(危険な)クラウドサービスを利用を許すが、
「監視」と「制御」によって(さらにＡＩ学習によって)、セキュリティを担保する考え方である。
具体的には、デバイス、ユーザ、ネットワークフローをひとつ残らず認証し、内容を監視することで認可する。
CASB(Cloud Access Security Broker)、UEM(Unified Endpoint Management)、
EDR(Endpoint Detection & Response)などの技術を用いる

(5)ファイル持出方式

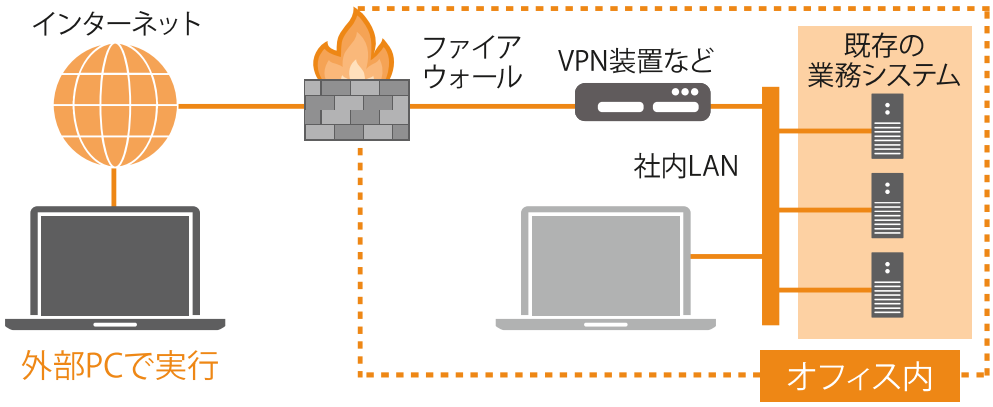
社内で使用しているPCやタブレットを社外に持ち出す、あるいは、ネットドライブやVPNを用いて、社外のPC等に業務ファイル等をダウンロードして社外のPCで業務アプリを実行する方式。使い慣れた端末の利用が可能。

外部に持ち出された端末がウイルスに感染し、それを社内に再び持ち込む場合、全ての社内端末にウイルスが広がる危険性があるため、慎重な対策が必要である。また、多くの業務用データを保存した状態のPCを紛失する危険性があるため、PC紛失時の対策も行う必要がある。

VPNは、安全で安価な通信路である。図表3-7に製品例を示す。サテライトオフィスの設置時には拠点間通信にVPNの利用を検討する。しかし、社外のPC等を、VPNを用いて社内のLANに直接接続するのは、セキュリティ上のリスクがある。

ネットドライブ（Dropbox、Googleドライブ、BOX、OneDrive等）やVPNを用いて、ファイルを社外のPC等に持出す場合は、(4)の安全ファイル持出方式の利用を検討する。

図表 3-7　ファイル持出方式の仕組み



図表 3-8　VPN接続製品例

No	製品名	比較項目				
		方式等	サポート等	価格（税別）	所要導入工程	特徴
1	各種VPNルータ等の利用	VPNルータ等のハードウェアのみを使用して、拠点間の接続を行う方式。	VPNルータを購入して設定を行う。基本的には自社で行う作業のため、管理できる人員等が必要。	1台（1拠点あたり）数万円程度の初期費用～。拠点は固定IPである必要があり、プロバイダー費用が高めになる。	機器を自社で購入し、導入するためユーザによる。	自社で設定・管理する能力が必要。月々の利用料等は必要無い。Cisco、YAMAHA、BUFFALO等がVPNルータ製品を販売している。
2	PacketiX VPN/ソフトイーサ(株)	ソフトウェアによるVPN接続。	体験版で動作検証してから導入を行う流れ。サポートサービスが含まれる。	Standard Edition（小規模企業向け）95,000円～1年間のサポートサービスおよびソフトウェアのバージョンアップサービスを含む。	ユーザが体験版で動作検証してから導入を行う。ソフトウェアはWebからダウンロードでき、即日の検証が可能。	9年間で5,500社に採用のVPN 製品の最新版。高額なVPNルータ無しで、ソフトウェアでVPN接続を可能にする。
3	Verona/(株)網屋	VPN機器、IP等の管理サーバ、機器のメンテナンスサービス等を組み合わせた方式。	ルータのOS等については自動的にアップデートが行われる。VPN機器の設定作業は不要。	初期費用 98,000円 月額 8,450円～（1拠点2450円　在宅・外出先10箇所まで6,000円の合計）11拠点での例。	注文から5営業日以内に、機器を届ける。	VPNルータのOSのアップデートや、VPNルータの設定の作業等が不要。メッシュ型のVPNを自動的に構築できる。 拠点ごとの固定IPは不要。
4	beat/active / 富士フイルムビジネスイノベーションジャパン(株)	VPN機器、IP等の管理サーバ、機器のメンテナンスサービス等を組み合わせた方式。	設定済みのVPNルータ（beat-box）が送付され、電話サポートが行われる。	beat/active 初期登録サービス60,000円/拠点 月額12,800円/拠点 beat/active VPN接続設定サービス（初期）30,000円/拠点 月額1,000円/拠点 （上記の双方の契約が必要）	各拠点のネットワークの状況をヒアリングして導入可能かを判断し、その後注文から1～2週間。	複数の事業所に専用のゲートウェイ装置（beat-box）を配置することで、メッシュ型のVPNを自動的に構築できる。 拠点ごとの固定IPは不要。

※ほとんどの製品が、拠点間接続（LANの接続）、PC間接続、PCとLANの接続のそれぞれに対応可能。