テレワーク関連ツールの特徴比較

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業務システムの形態、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、「リモートデスクトップ方式」により社内サーバに接続し、併せて「クラウドアプリ利用方式」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。

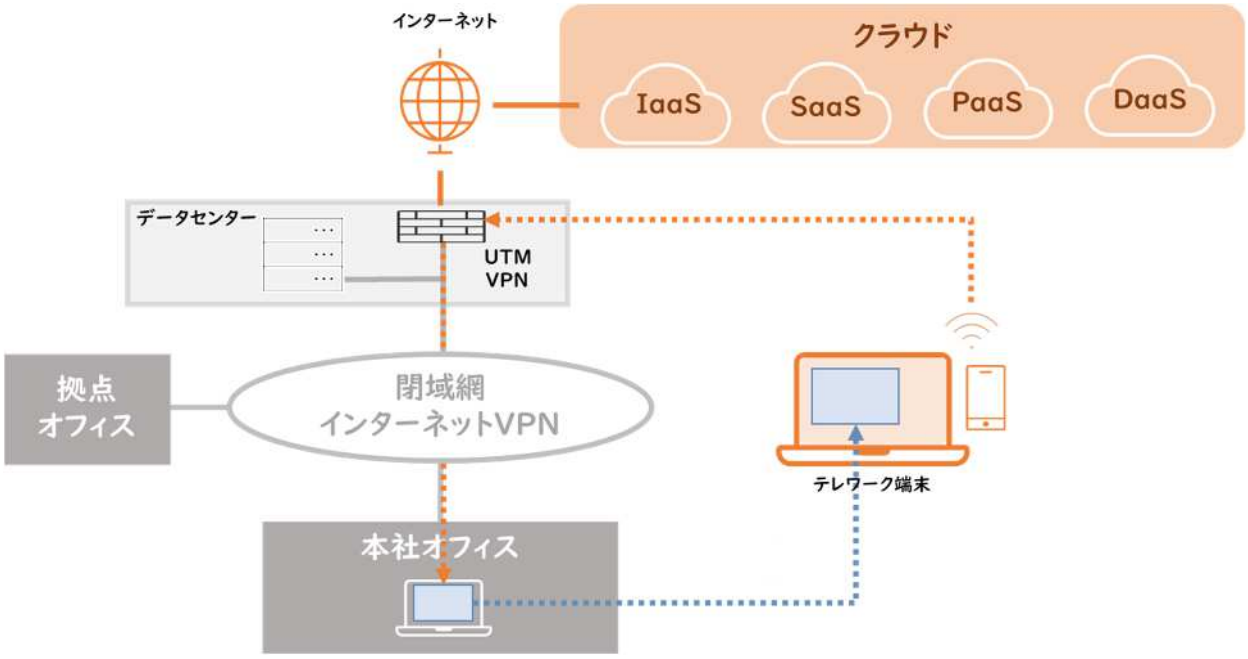
図表 3-1　システム方式

No	ツール	概要	TW 形態	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、導入も容易。	すべて タブレットやスマホ からの接続・利用も可能。	magicConnect/NTT テクノクロス㈱ Splashtop Business/スプラッシュトップ㈱ Remote View/RSUPPORT㈱ DoMobile/㈱日立ソリューションズ・クリエイト CACHATTO リモートデスクトップ Box/e-Jan ネットワークス㈱
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 台から提供するものも出てきている。 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。管理者も必要になることから、中堅・大企業で の導入事例が多い。	すべて	Citrix XenDesktop/シトリックス・システムズ・ジャパン㈱ VMware Horizon 8/ヴイエムウェア㈱ Microsoft VDI/日本マイクロソフト㈱ Amazon WorkSpaces/アマゾンウェブサービスジャパン㈱
3	クラウドアプリ利用方式	業務システムが SaaS や PaaS で構築されている場合にブラウザアクセスのみで処理を行う方式。 但し、多くのシステムではファイルのダウンロード機能があり、ブラウザのキャッシュも残ることから、PC 紛失時の対策は必須となる。	すべて	後述の各種ツールが該当するため省略
4	安全ファイル持ち出し方式	業務ファイルを外部 PC に安全に持ち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。	すべて	CACHATTO SecureContainer/e-Jan ネットワークス㈱ WrappingBox/㈱ソリトンシステムズ Flex Work Place/横河レンタ・リース㈱ ZENMU for PC/㈱ ZenmuTech
5	ファイル持ち出し方式 （VPN 接続）	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、クラウドストレージや 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。	すべて	Dropbox、Google ドライブ、Box、OneDrive 等のクラウドストレージ PacketiX VPN/ソフトイーサ㈱、 Verona/㈱網屋、beat/富士フイルムビジネスイノベー ションジャパン㈱等の VPN 経由

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。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	メーカ	特徴	価格	納期
1	magic Connect	NTT テクノクロス㈱	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。	初期 15,000 円、年額 18,000 円	約 1 週間
2	Splashtop Business/スプラッシュトップ㈱	スプラッシュトップ㈱	画面を高速に動画配信する技術を採用。但し本プランは 30 フレーム/秒。 MacOS 対応、リモートマイク、マルチモニタ、GPU エンコードは上位プランのみ	初期費用 0 円。年額 15,000 円～	3 営業日程度
3	Remote View	RSUPPORT㈱	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。 MacOS 対応 RemoteWOL は別売 36,000 円	月額プラン 1,100 円 / 月 年額プラン 12,000 円 / 年	3 営業日
4	DoMobile	日立ソリューションズ・クリエイト	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。Web 会議は音声のみ WOL サーバ要 画面ロック・BlackOut D 証明書・二段階認証	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
5	CACHATTO リモートデスクトップ Box	e-Jan ネットワークス㈱	専用コネクタを社内 LAN につなぐだけで導入完了。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	初期費用 0 円。 同時接続数 3 ユーザ 7,500 円/月	最大 5 営業日

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。

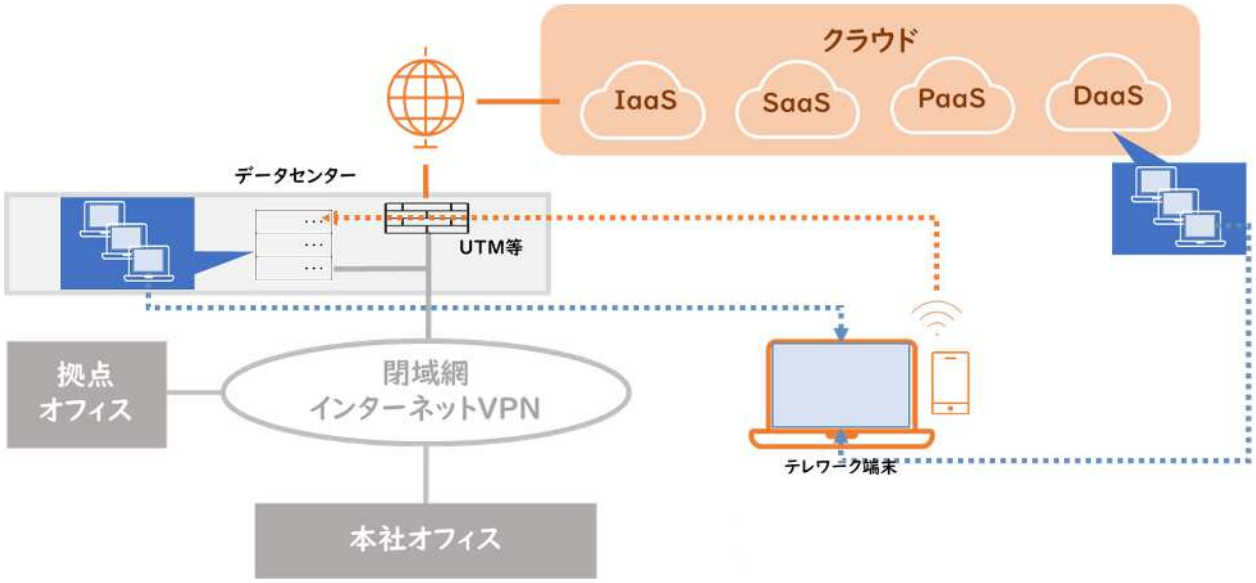
仮想デスクトップ方式については、従業員人数分の数十人、数百人単位で導入し、業務中のサーバ停止が多額の損失に繋がりかねないこともあり、導入コストは高額になるケースが多い。

「 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（t 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



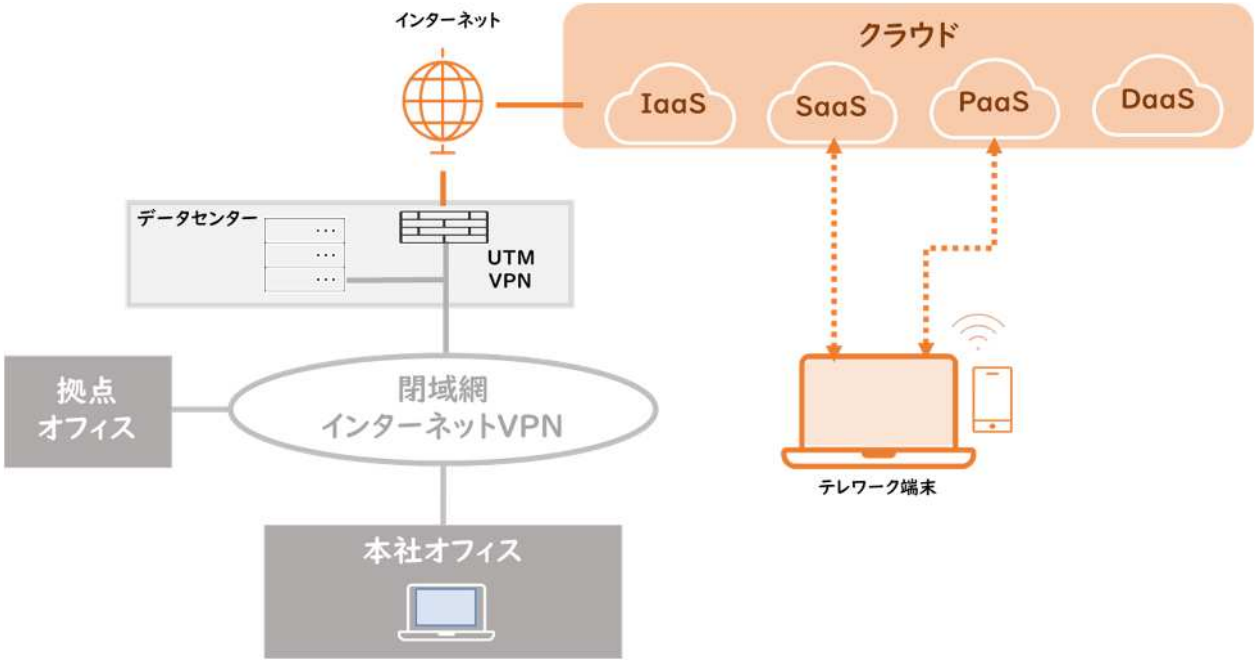
クラウド型アプリ方式

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。

何も設定されていない場合は、インターネットに接続できる端末であれば直接アクセス可能だが、IP アドレス制限やデジタル証明書等で端末制限をかけることも可能。特に重要なデータがクラウド型である場合や、複数のクラウド型アプリの一元管理をしたい場合は、CloudGateUNO（㈱インターナショナルシステムリサーチ）等のサービス利用を検討する。

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

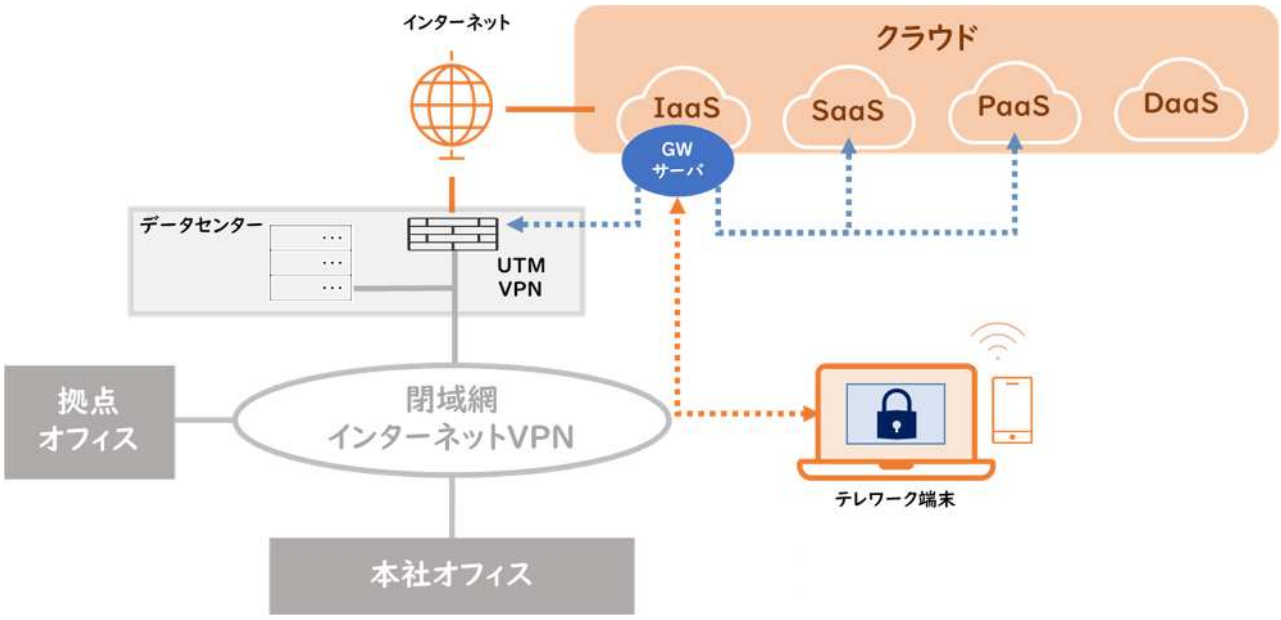


安全にファイルを持ち出す方式

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　安全持ち出し方式の仕組み



図表 3-7　安全持ち出し方式の製品例

No	製品名	メーカ	特徴	価格
1	CACHATTO SecureContainer	e-Jan ネットワークス ㈱	外部領域からのアクセスを制限したセキュアな遠隔業務領域。VPN サーバ不要で既存の社内サーバや Microsoft 365 などのクラウドサービスへのアクセスができる。業務終了時に領域内はデータ削除される。	要問合せ
2	WrappingBox	㈱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へ保存する。Microsoft365 などが利用可能。	ユーザライセンス 月額 1,000 円/ユーザ
3	Flex Work Place	横河レンタ・リース㈱	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。 OneDrive 連携版もあり。	レンタル： 月 780 円/ユーザ 購入（最小構成）：520,000 円+18,000 円/ユーザ
4	ZENMU for PC	㈱ 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ち出しせる。AONT（All or Nothing Transform）方式でデータを無意味化する。	年 9,600 円/ユーザ

ファイル持ち出し方式

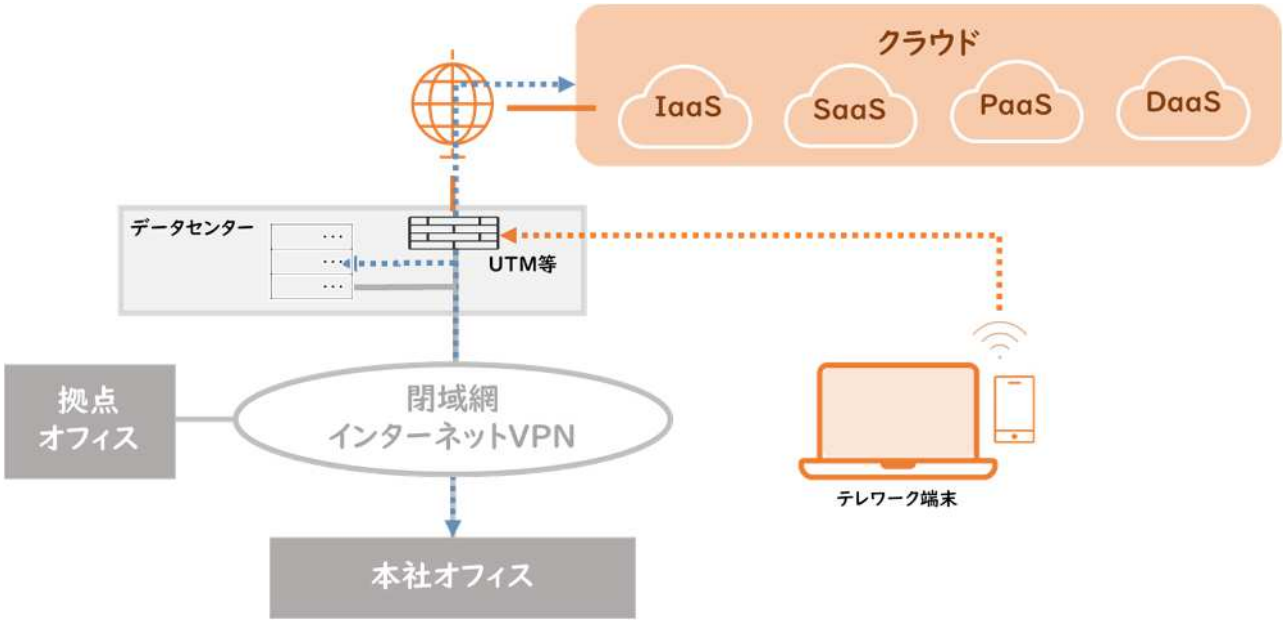
社内で使用している PC やタブレットを社外に持ち出す、あるいは、クラウドストレージや VPN を用いて、社外の PC 等に業務ファイル等をダウンロードして社外の PC で業務アプリを実行する方式。使い慣れた端末の利用が可能。

外部に持ち出された端末がマルウェアに感染し、それを社内に再び持ち込む場合、全ての社内端末にマルウェア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、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。また、近年 VPN 機器の脆弱性を狙ったサイバー攻撃が増えているため、機器の脆弱性対策は必須となる。

クラウドストレージ（Dropbox、Google ドライブ、Box、OneDrive 等）や VPN を用いて、ファイルを社外の PC 等に持ち出す場合は、(4) の安全ファイル持ち出し方式の利用を検討する。

図表 3-7　ファイル持ち出し方式の仕組み



図表 3-8　VPN 接続製品例

No	製品名	メーカ	特徴	価格	納期
1	VPN ルータ等	Cisco、 YAMAHA、BUFFALO 等	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 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。	—
2	PacketiX VPN	ソフトイーサ ㈱	9 年間で 5,500 社に採用の VPN 製品の最新版。ソフトウェアによる VPN 接続。ユーザが体験版で 動作検証してから 導入を行う。	Standard Edition（小規模企業向け）95,000 円～	検証用ソフトは Web 入手。
3	Verona	㈱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。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。	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 営業日以内に機器送付。
4	beat/active	富士フイルムビジネスイノベーションジャパン㈱	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。各事業所に専用の装置（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。	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	注文から 1～2 週間

（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ち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、境界で防御するものが主流で、「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（持ち出しリスク）に問題があると考えられている。前頁の表のツールは、その持ち出し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、「決して信頼せず常に確認せよ」という考え方です。NIST SP800-207 では、7つの原則が定義されています。

- すべてのデータソースとサービスをリソースとみなす
- ネットワークの場所に関係なくすべての通信を保護する
- リソースへのアクセスはセッション単位で付与する
- リソースへのアクセスは ID や各種属性を含めた動的ポリシにより決定する
- すべての資産の整合性とセキュリティ動作を監視・測定する
- すべての認証と認可は動的に行われ、アクセスが許可される前に厳格に実施する
- 収集した情報をセキュリティ対策の改善に利用する

具体的には、下記のような構成技術ごとにソリューションがあり、ネットワークセキュリティでは、Zscaler、PrismaAccess、Cato などが代表的である。

- SASE（Secure Access Service Edge）
- SWG（Secure Web Gateway）
- ZTNA（Zero Trust Network Access）
- CASB（Cloud Access Security Broker）
- IAM（Identity and Access Management）
- SIEM（Security Information and Event Management）
- EMM（Enterprise Mobility Management）
- EDR（Endpoint Detection & Response）