

情報システム担当が選ぶ ネットワークインフラ

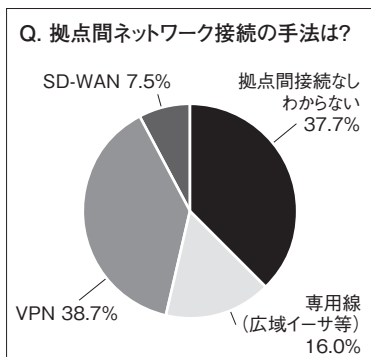
第5回

拠点間接続の実態は、いまだVPNが中心

Virtual Private Network

複数の拠点を持つ企業では、本社／支店／工場／店舗などを、どうつなぐかが業務効率を大きく左右します。今回のアンケートでは、VPN※¹利用が最多だった一方で「接続なし・わからない」もほぼ同水準となりました。拠点間接続は、単に回線を結ぶだけではありません。通信の安定性、セキュリティ、クラウド利用のしやすさにまで関わってくる重要な基盤です。今回は、VPN／専用線／SD-WAN※²の違いを、できるだけわかりやすく整理します。

図1 アンケート結果（回答数 106 票）



拠点間接続は VPN接続が最多

● 拠点間ネットワーク接続では、どんな手法をとっていますか？ 今回のアンケートは、SNS上

で情報システム担当者を対象に実施したもので、106名から回答が寄せられた結果、最多はVPNの38・7%でした。

一方で「拠点間接続なし／わからない」も37・7%と非常に高く、企業によっては拠点同士のネットワーク整備が十分に進んでいない、あるいは現場で接続方式が把握されていない実態もうかがえます。

なお、SNS上でのアンケートであるため、回答者の属性や企業規模には一定の偏りがある可能性があります。この結果は中小企業における拠点間接続の現実をよく表していると考えられます。

コストを抑えながら必要最低限の接続を実現する手段としてVPN

株式会社ピーエスアイ
管理部広報担当

内藤 純一

URL <https://www.psi.co.jp>

E-mail support@psi.co.jp

Nが広く使われている一方、通信品質や運用管理の面では課題を抱えているケースも少なくありません。また、クラウド利用が増えた現在では「本社を経由して各拠点をつなぐ」という従来型の考え方のそのものを見直す必要も出てきています。

ここで注意したいのは「接続できている」と「業務に適した接続になっている」ということは、まったく別であるという点です。

拠点間通信は、普段は意識されにくい存在ですが、遅延や切断が起きた瞬間に「受発注処理／在庫確認／勤怠管理／Web会議／ファイル共有」など、日常業務のさまざまな部分に影響が出ます。

ネットワークは見えにくい設備ですが、会社の働き方を支える交通インフラのようなものです。道が細かったり、信号が整理されていなかったりすれば、どれだけ高性能の車を用意しても目的地にはスムーズにたどり着けません。

拠点間接続も同じで、方式の選び方と設計次第で、業務の快適さと安全性が大きく変わります。

※1 VPN (Virtual private network)：仮想プライベートネットワーク

※2 SD-WAN (Software Defined WAN)：ソフトウェアによってWAN (広域通信網) を効率的に制御・管理する技術

本社／支店などをつなぐ 拠点接続の役割とは

●通信の許可と制限

- 「本社／支店／営業所／工場／店舗」など、拠点が複数の場合はデータや業務システムの共有が大きな課題です。例えば、以下のよう業務は日常的に行われています。
- ・支店から本社の販売管理システムへアクセス
- ・店舗から支店の在庫情報を確認
- ・工場のデータを本社へ集約

こうした情報共有を円滑かつ安全に行うには、拠点間ネットワークの整備が欠かせません。しかし、ネットワークが不安定だと、システムの応答遅延やファイル転送の遅れ、Web会議の途切れなどが発生し、業務効率の低下を招きます。

また昨今は、社内システムだけではなく、Microsoft 365やGoogle Workspaceや会計ソフト、CRM（顧客管理システム）など、クラウドサービスを拠点から直接使うケースが増えています。

つまり、拠点間接続は「本社と

支店をつなぐしくみ」から「各拠点が必要なサービスに快適かつ安全にアクセスするためのしくみ」へと役割が変わってきており、この変化は、ネットワークを考えるレイヤー（ネットワーク階層）にも影響します。

従来は、拠点間をどうつなぐかというレイヤー3、つまりIPネットワークの経路設計が中心でしたが、現在は業務アプリケーションがクラウド側に移り、通信の宛先も本社サーバーだけではありません。

Web会議の質、SaaSへの応答速度、ファイル同期の安定性など、レイヤー7に近いアプリケーション体験までが必須です。

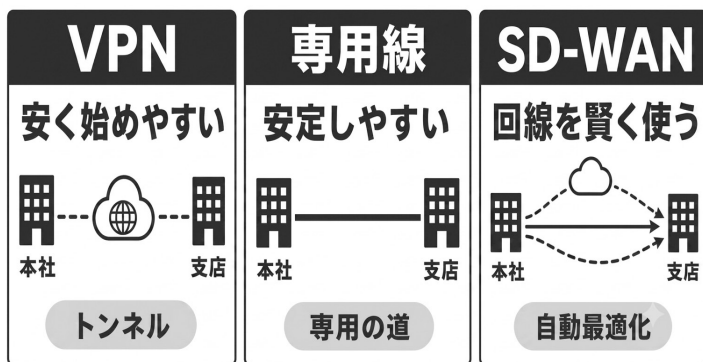
拠点間接続のセキュリティも重要で、ウイルスに感染した端末がVPN経由で本社や他拠点へ到達できる構成になっていれば、被害が広がる可能性があります。

拠点同士をつなぐことは便利な一方で、攻撃者の移動経路にもなり得ます。したがって、どの通信を許可し、どの通信を制限するかという設計が大切であり、ネットワークの利便性とセキュリティ

は拠点間接続の設計段階から一体で考える必要があります。

3つの接続方式 それぞれの向き・不向き

拠点間接続には、大きく分けて3つの方式があり、今回のアンケートで取り上げた「VPN／専用線／SD-WAN」です（図2）。それぞれにある「向き・不向き」を解説していきます。



●「VPN」の特徴

VPNは、インターネット回線を使いながら、通信内容を暗号化してやり取りするしくみです。

拠点間接続ではIPsec VPN※3などがよく使われます。比較的低コストで導入がしやすく、多くの企業で採用されています。中小企業にとっては最も現実的な選択肢のひとつといえます。

今回の調査で最も多かったVPNが選ばれる理由は、導入のしやすさとコストのバランスにあります。新たに高額な専用線を引かなくても、既存のインターネット回線を使って本社と支店を比較的短期間でつなぐことが可能です。

VPNは、通信内容を暗号化しながら拠点間を接続でき、適切な設計・運用を前提に高い安全性を確保できる点も利点です。また、しくみとしてイメージしやすく「支店から本社へ安全なトンネルをつくる」と考えると理解しやすいでしょう。

一般的な中小企業が、まずVPNから始めるという流れは自然ですが、VPNは万能ではなく、イン

※3 IPsecVPN：IPsecという暗号化・認証プロトコルを使って、拠点間やリモート端末と社内ネットワークの間に安全な仮想専用線（VPN トンネル）を構成する仕組み

ターネット回線を前提とするために、利用回線の品質や混雑状況の影響を受けます。また拠点が増えると設定や運用が複雑になり「拠点同士がどのようにつながっているのか」がわかりにくくなります。

加えて、VPN機器そのものの脆弱性や設定ミス、認証情報の管理不備が外部からの侵入経路になることもあります。VPNを導入しているから安心という考え方はなく、機器の更新、不要な接続の停止、多要素認証、ログ監視などを含めた運用が重要です。

●「専用線」の特徴

専用線は、通信事業者が企業のために専用の回線や閉域網を用意する方式です。一般的なインターネット回線より通信品質を安定させやすく、重要な拠点間通信に向いています。一方、高費用で回線手配にも時間がかかる傾向があります。

専用線というと「昔ながらの高価なしくみ」という印象を持つ方もいるかもしれませんが、現状でも用途によっては有力な選択肢で

す。重要な業務システムを常時利用する拠点、工場の制御系データを扱う環境など、遅延や切断が業務に大きく影響する場所では、安定性の価値は大きくなります。

例えば、受発注処理が1日に何度も止まる、映像監視が頻繁に途切れる、工場の拠点データ連携が不安定になる。こうしたトラブルは、単なる「少し不便」では済みません。これらの事象は業務停止や顧客対応の遅れに直結します。

また、専用線は「全拠点に入れるべきもの」ではありません。拠点の重要度や通信量に応じて、本来に必要な場所に絞って使うのが現実的です。重要拠点だけ専用線を使い、その他はVPNやインターネット回線と組み合わせるという考え方も一般的です。

●「SD・WAN」の特徴

SD・WANは、複数の回線をソフトウェアで統合・制御しながら、拠点間通信やクラウドアクセスを最適化する考え方です。

難しそうに感じますが、要するに「複数の道路を見比べて、混雑

状況や目的地に応じて最適な道を自動で選ぶ交通整理システム」のようなものです。

今回のアンケートでSD・WANは75%と少数派で、まだ中小企業では普及途上といえます。ただし今後は、注目度が高まる分野であることは間違いありません。

例えば、

- ・通常業務…安価なインターネット回線を使用
- ・重要な通信…品質の安定した回線を優先
- ・回線障害が起きたとき…別回線へ自動で切り替える

といった制御が可能になり、さらにクラウドサービスでは、本社を経由せずに直接アクセスするといった設計も容易になります。

もちろん、すべての企業にSD・WANが必要というわけではありません。拠点数が少なく、通信要件もシンプルであれば、VPNで十分なケースもあります。一方で、拠点数の増加やクラウド利用の拡大、回線障害の影響をできるだけ抑えたいといった課題を抱

える企業では、SD・WANが有力な選択肢となります。

クラウド時代に 変化する拠点間接続

●経路の最適化と保守の一貫性

以前は「情報を拠点から本社に集めて、本社からインターネットへ出る」という構成が一般的でした。これは、セキュリティ管理を本社に集中できるため、わかりやすく管理しやすいからです。

しかし今は、各拠点の社員が日常的に使うサービスの多くがクラウド上にあり、クラウド会計やWeb会議を使うたびに、本社を経由してインターネットへ出る構成では、通信が遠回りになり遅延や混雑の原因になります。

この変化は、拠点間接続の考え方をそのものを変えています。重要なのは「すべてを本社に集める」ことではなく「必要な通信を、必要な場所へ、できるだけ無駄なく届ける」ことです。

SD・WANが注目される背景には、このクラウド時代の構造変

化があり、さらに最近では、SD-WAN 単体ではなく、SASE※4 やゼロトラストネットワークアクセスなどと組み合わせて、拠点・端末・クラウドを一体で考える流れも強まっています。

ただし、本社経由をやめれば良くなるという単純な話ではなく、各拠点から直接インターネットへ出る場合、その拠点ごとにセキュリティをどう担保するかという課題が生まれます。本社にだけファイアウォールやログ監視のしくみがある場合、拠点からの直接通信が見えなくなり、かえって管理が難しくなることもあります。

したがって、クラウド時代の拠点間接続は、経路の最適化とセキュリティの一貫性との両立が求められる、どの拠点からどのクラウドサービスへ接続するのか、通信をどこで検査するのか、ログをどこに集約するのかなどが重要です。こうした運用面まで考えた設計が求められ、単に回線を速くするだけではなく、ネットワーク全体を見える化して通信の流れを把握することが出発点になります。

図3 自社の業務要件を整理する

- Q 本社と支店の間で常時大量のデータ通信があるのか
- Q Web会議やクラウドサービスの利用が多いのか
- Q 回線障害が起きたときに、どこまで業務が止まると困るのか
- Q 全拠点で同じレベルの通信品質が必要なのか
- Q 誰が、どの端末で、どのサービスへアクセスするのかを把握できているのか

するなど、現実的な組み合わせが見えてきます。一気に刷新する必

- ・本社と工場間は安定性重視で「専用線」
- ・営業所は「VPN」
- ・主要拠点は将来的に「SD-WAN」を検討

拠点間接続に必要なのは最適化

●接続方式を使い分ける

拠点間接続を見直す際に、単に「VPNか、SD-WANか」という機器や方式の比較だけで考えてしまうと本質を見誤ります。まずは図3のように自社の業務要件を整理します。すると、

要はなく、重要度の高い拠点から見直すだけでも効果があります。

業務上は、最初から大規模な刷新計画を立てるよりも、まず「見える化」から始めるのが現実的です。各拠点で利用している回線、VPN装置、接続先、クラウドサービス、障害時の代替手段を一覧化するだけでも、優先順位はかなり明確になります。

例えば「売上処理や生産管理に関わる拠点は安定性を重視し、営業所や小規模店舗はコストと運用のしやすさを重視する」といった整理ができます。また、障害が起きた際に「誰が復旧判断を行い、どの通信を優先して復旧させるのか」を決めておくのも重要です。

拠点間接続は一度構築すると長く使われるため、導入時だけではなく運用時の確認項目まで設計に含めておく必要があります。そのポイントは、全拠点を同じ構成に揃えることではなく、業務への影響度に応じて接続方式を使い分けることです。

今回のアンケートでは、VPNが最多である一方「接続なし／わ

からない」も非常に高い比率となりました。これは、多くの中小企業にとって拠点間接続の構成がまだ十分に整理されていない、または現場で把握されていない可能性を示しています。

とはいえ、今は単純に「つながっていればよい」時代ではありません。通信の安定性、クラウド利用のしやすさ、障害時の切り替え、セキュリティ管理のしやすさまで含めて考える必要があります。

VPNは今後も有力な選択肢ですし、専用線も重要な場面では有効です。そして、SD-WANやSASE関連技術は、複数の回線とクラウド利用を前提にした新しい最適化の考え方として、今後ますます存在感を高めていきます。

拠点間接続を考えることは、単にネットワークを張ることではありません。会社全体の働き方を支える「交通インフラ」を整えることです。まずは自社の拠点が、どの方式で、どこにつながっており、何に困っているのかを見える化してください。それが見直しの第一歩になります。

※4 SASE (Secure Access Service Edge) : SD-WAN などのネットワーク機能と、SWG・CASB・FWaaS・ZTNA などのセキュリティ機能をクラウド上で統合し、場所を問わずユーザーやデバイスを安全にアプリやデータへ接続させるための次世代ネットワークセキュリティアーキテクチャ。