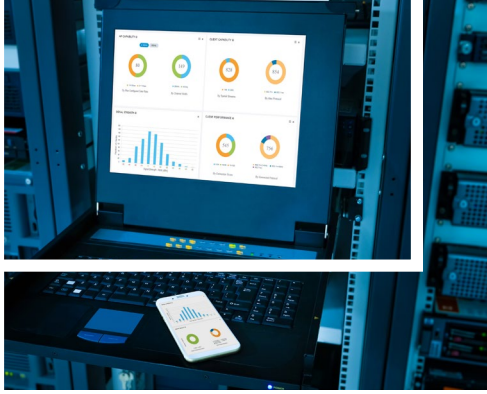
次世代のITインフラ - ゼロトラスト・アーキテクチャ
ネットワーク視点で捉えるゼロトラストの必要性



PwCコンサルティング合同会社　シニアマネージャー　田村 郷司

1. ネットワーク視点で捉えるゼロトラスト

社内のネットワーク構築においては、これまでデータセンターを中心に設計をしてきた企業や組織が多いのではないでしょうか。しかし近年、クラウドサービスの利用が急激に進み、これからはクラウド環境を中心にした設計にシフトする必要が出てきています。

こうした環境下、企業のIT担当者はクラウド向けのトラフィックのマネジメントに苦慮してきたことかと思います。これに加えて、新型コロナウイルス感染症（COVID-19）をきっかけにする在宅勤務（リモートワーク）の増加で社外から自社のデータセンターやクラウドサービスへ接続するといった、管理するべきトラフィックの経路が増えてきています。企業においては、従来のデータセンター中心のトラフィックマネジメントのやり方を再考する時期に来ているのではないかと考えています。

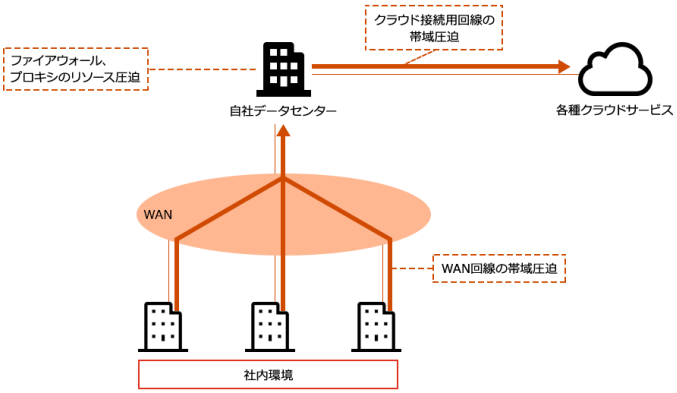
今回は、近年顕著になっている企業ネットワークの課題とリモートワーク推進により新たに生じた課題をピックアップし、ゼロトラスト化の必要性について、ネットワークの観点で解説します。

2. クラウド利用の急増が与えた企業ネットワークへの影響

データセンター上で稼働していた業務アプリケーションをクラウド上のサービスに切り替える動きが増えています。一方でクラウド利用に伴い、いくつかの問題が生じている企業が出てきています。例えば、通信トラフィックが多く発生するコラボレーション系のソフトウェアをクラウドに移行することで、データセンターとクラウドサービスをつなぐ回線が混雑し、利用者のユーザビリティを著しく低下させるという問題が発生しています。

またデータセンター内のサーバー環境、ネットワーク環境を仮想化しクラウドのIaaS（Infrastructure as a Service）基盤とシームレスに連携するハイブリッドな環境の構築も進んできています。クラウド環境向けネットワークに対して求められる可用性やパフォーマンスは、ますます高くなってきています。

図表1:クラウド利用の急増による通信のボトルネック



この問題を解消するために、多くの企業は回線帯域の増強を行ってきたのではないでしょうか。この対策はセキュリティのガバナンスを維持しつつ至急打てる策の一つではありますが、長い目で見た時に、データセンター内の他のリソース（通信機器、プロキシサーバーなど）も消費し、各拠点をつなぐアクセス回線の帯域も圧迫させるため、恒久的な策とは言えません。

3. リモートワークがもたらした新たな課題 - 境界型アーキテクチャの限界

COVID-19をきっかけに、リモート環境でPCを利用するのが当たり前になりました。リモート環境でPCを利用するにはこれまで、業務上必要な場合、社内の申請手続きを経る必要がありました。そのため、利用されるPCの台数は多くありませんでした。しかし、リモートワークが推奨されるようになり、社内で利用されるPC台数よりリモート環境で使われるPCのほうが多くなりました。社員のほとんどがリモート環境でPCを利用する場合、ネットワークに求められる新たな要件を考察すると、大きく以下の2つが言えるかと思います。

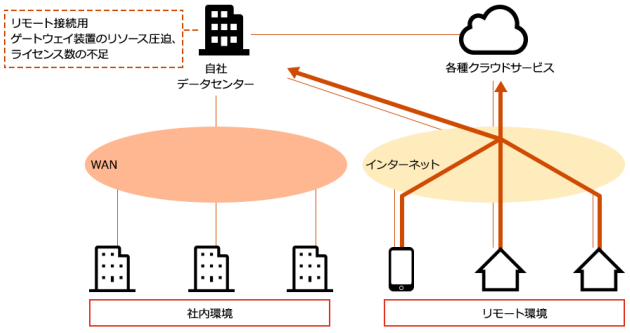
(1)セキュアにクラウド環境にアクセスできること

これまでのようなオンプレミスの境界型のセキュリティ装置で担保されていた仕組みが効かない、オープンなインターネットの領域からクラウド環境にアクセスすることになるため、ウイルス感染やデータ漏えいへの対策をネットワーク上の新たな仕組みで補う必要が出てきます。

(2)社内システムに一斉にアクセスしても耐えられるキャパシティを用意すること

これまでは、業務で必要となる社員が申請してPCを利用するといった対応をしていたため、接続台数はある程度予測でき、急激に変化するということはありませんでした。しかし、社員の多くがリモートワークに切り替わることにより、これまでの想定より多くのPCがリモートアクセス用のゲートウェイ装置などに接続してくるという状態になってしまいました。これにより多くの企業は、装置の処理性能や接続用のライセンスが不足するといった状況に陥りました。

図表2:リモート環境の利用増による通信のボトルネック

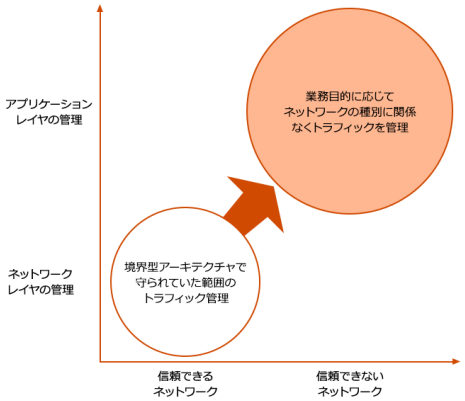


この2つの要件を、境界型のアーキテクチャで数日から長くて数週間で対応することは、極めて困難です。企業のIT担当者にとっては、境界型のアーキテクチャの限界を肌で感じる象徴的な出来事だったのではないでしょうか。

4. 今後、どうするべきか - 変革を実現する重要な論点

これからのネットワークに求められる要件に応えるためには、従来の境界型で守られていた範囲を管理するという考え方から、社員の働き方を中心に捉えて、業務の目的に応じてネットワークの種別に関係なくトラフィックを管理する、という考え方に変える必要があります。そのためには、これまで閉域網におけるIPベースでの管理から、業務内容により近いアプリケーションレベルでトラフィックを管理していくこと、さらにリモート環境でPC利用することを前提としたセキュリティリスクなどを管理していく必要が出てきます。

図表3:今後のトラフィック管理の方向性



アプリケーションレベルでトラフィック管理を行うには、SDN（Software Defined Network）の技術が必要になってきます。IPベースで設計された物理的なネットワーク（アンダーレイネットワーク）による制約を受けずにコントロールできるため、オーバーレイネットワークとも呼ばれます。SDNの技術を用いたWAN（Wide Area Network）のソリューションが、SD-WANです。アプリケーションを識別する機能を持ったSD-WANルータでクラウドサービス向けのトラフィックを集中的にコントロールすることができ、企業のネットワークを支える技術の大きな柱になってきています。

次に、インターネットのような必ずしも信頼できないネットワークを利用する場合のリスクを管理するために必要となってくるのが、ゼロトラスト・アーキテクチャの概念です。全てのトラフィックを信頼しないことを前提に検証することで、ネットワークを脅威から守るというアプローチです。デバイス、ユーザー、アプリケーション、トラフィックそれぞれの視点でリスクが存在しないか検証を行い、安全との確認が取れたもののみ利用を許可します。ゼロトラスト・アーキテクチャは概念であるため、自社の要件をもとに、どの製品ベンダーのソリューションが最適なのか、評価を行った上で導入を進めていく必要があります。自社に最適なゼロトラストのソリューションを採用することで、安全にリモートワークができるようになります。

今後、ビジネス環境はさらに急激に変化していくことが想定されます。企業はそれに対応するために、ゼロトラストなネットワークになるための準備を今から進めていく必要があるでしょう。

お問い合わせ

PwCコンサルティング合同会社
〒100-6921　東京都千代田区丸の内2-6-1 丸の内パークビルディング
Tel : 03-6250-1200（代表）　Mail : jp_cyber_inquiry@pwc.com