トレンドワードから効率化を読む（第24回）

リモートアクセスサービスとは？サービス選定のコツ

2020.12.21

新型コロナウイルスの影響もあり、近年、多くの企業がテレワークの導入を急いでいます。これから導入をお考えの方は「リモートアクセスサービス」というサービスをご存じでしょうか。

遠隔地から会社のパソコンなどにアクセスするサービスですが、テレワークを実現する方法としては比較的容易に利用できるサービスです。

今回は、リモートアクセスサービスの概要からメリット・デメリット、導入する際の選定ポイントについて解説します。

リモートアクセスサービスとは？

リモートアクセスサービスは、自宅や外出先など、社外から会社のパソコンに接続して遠隔操作を実現するサービスです。

手元のパソコンやスマートフォンを使って、会社のパソコンに接続することができるので、あたかも会社の自席で作業するように仕事ができます。

リモートアクセスサービスの仕組みは、サービスの提供会社によって異なりますが、大まかには次の流れで実現しています。

1.自宅などの手元の端末（パソコン、スマートフォン）で専用ソフトを起動する
2.暗号化された通信を用いて、会社のパソコンに接続する
3.手元の端末から会社のパソコンを遠隔操作する

リモートアクセスサービスは、あくまでも会社のパソコンでの作業を遠隔地から実現するサービスなので、重要な情報などを社外に持ち出さずに仕事を行える点が特徴です。

リモートアクセスサービスのメリット・デメリットについて

リモートアクセスサービスを利用する際のメリット・デメリットについてご紹介します。1つずつ見ていきましょう。

＜メリット＞

・テレワークのセキュリティ対策になる
テレワークでは、セキュリティ対策が大きな課題の1つに挙げられます。テレワークを実施するうえで最も気を付けるけるべきセキュリティ事故は、業務情報が保存された接続端末の紛失などから発生する情報漏えいといえるでしょう。

しかし、リモートアクセスサービスを利用する際は、あくまでも社内のパソコンに接続しているだけなので、端末にデータを保存する必要性がありません。また、業務情報を社外に持ち出すことなく業務を行えます。そのため、情報漏えいのリスクを低減できるのです。

・リモートワークの推進
リモートワークを効率的に実施するには常に作業が行える端末を準備する必要があります。例えば、会社で利用しているパソコンにデータがある場合、リモートワークをする際には会社から許可を得てそのパソコンを持ち出して作業をするケースもあります。

しかし、リモートアクセスサービスを利用すれば、決められた端末ではなくても構いません。自宅などにある手元の端末から社内のパソコンに接続でき、リモートワークをしやすくなるメリットがあります。決められた端末が常に必要にならず、さまざまな場所での業務もしやすくなるため、リモートワークの推進につながります。

・緊急時に備えた体制の強化
リモートアクセスサービスの利用で、緊急時に備えた体制の強化も図れます。

例えば、新型コロナウイルスの感染拡大や、地震などの災害で外出や出社が難しくなったときに、自宅から社内のパソコンに接続すれば、緊急時でも業務を継続することができます。

＜デメリット＞

・利用するインターネット環境、端末の性能に左右されやすい
リモートアクセスサービスはインターネット回線を通じて社内のパソコンを操作します。利用するインターネット環境（回線）が悪いと、リモートでの操作性に影響を及ぼします。それ以外にも、手元の端末の性能もリモートでの操作性に影響を及ぼす可能性があります。インターネット環境や端末の性能に左右されやすい点がデメリットとして挙げられるでしょう。

・社内パソコンの電源を入れっ放しにする必要がある
リモートアクセスサービスを利用する際には、接続先となる社内パソコンの電源は入れっ放しにしておく必要があります。電源が入っていないとリモートアクセスはできません。電源を入れたままにしたときのコストの増加は、デメリットといえるでしょう。また、社内パソコンのOSアップデートなどで再起動をしなければならないときや、社内パソコンに何らかの問題が生じたときに、リモートアクセスは利用できなくなります。

リモートアクセスサービスを導入する際のシステム選定のポイント

リモートアクセスサービスは、さまざまな企業からサービスが提供されています。リモートアクセスサービスを導入する際にどのような点に注目すればいいのか、その選定ポイントをしっかり押さえておきましょう。

ここでは、リモートアクセスサービスを導入する際に押さえておきたい3つの選定ポイントをご紹介します。

＜セキュリティ対策がしっかり施されているか＞
リモートアクセスサービスを検討する際に、最も気をつけなければならないのがセキュリティ対策です。リモートアクセスが実現できても、セキュリティが甘ければ利便性以上にリスクが大きくなってしまいます。

リモートアクセスを行うネットワークの暗号化や、アクセスの際の認証方式を基準に、セキュリティ対策がしっかりと施されているかを確認しましょう。

特に不正アクセスのリスクに備えて、IDとパスワードを使った認証方式だけでなく、デバイス認証やワンタイムパスワードなどの異なる認証方式を組み合わせた「2段階認証」「多要素認証」を採用するサービスを選ぶようにしましょう。

＜対応するOSと端末種類＞
リモートアクセスサービスは、どのような環境下でも利用できるとは限りません。サービスによっては、利用できるOSや端末の種類（パソコン・スマートフォン・タブレットなど）が制限される場合もあります。

例えば、macOSの社内パソコンにスマートフォンからアクセスしたい場合に、導入するリモートアクセスサービスが対応していなければ意味がありません。自社の環境に合わせて、対応するOSと端末の確認は選定時のポイントの1つです。

＜リモートでの操作性＞
リモートアクセスサービスを利用するうえで、リモートでの操作性は選定に欠かせません。リモートアクセスを実現しても、リモートでの操作性が悪ければまともに作業できないでしょう。

リモートでの操作性は、インターネット環境や利用する端末の性能に左右されますが、アクセス環境にばらつきがあっても快適に作業を行えるかを確認したうえで、サービスを選定しましょう。

テレワークの導入にはクラウド型リモートアクセスサービス「マジックコネクト」

リモートアクセスサービスは、社外から会社のパソコンに接続して遠隔操作を実現するサービスです。手元のパソコンやスマートフォンなどの端末を利用し、あたかも会社の自席で作業をしているかのように仕事ができます。

テレワークを手軽に実現する手段としても注目されており、リモートワークの推進や緊急時に備えた体制の強化にも効果が得られます。

しかし、利用するインターネット環境や端末の性能に左右されやすく、社内パソコンの電源を入れっ放しにする必要があるなどの点はデメリットとして覚えておきましょう。

リモートアクセスサービスはさまざまなシステムが提供されていますが、「セキュリティ対策」「対応OSと端末種類」「リモートでの操作性」の観点から選定するのがポイントです。

NTT西日本グループでは、まだテレワークの導入が進んでいない企業のために、クラウド型リモートアクセスサービス「マジックコネクト」を提供しています。

マジックコネクトはマルチデバイスに対応し、多要素認証を採用したセキュリティ対策や、USBキー1本でリモートアクセスできるようになっています。

マジックコネクトならファイルやメールは会社に置いたまま、外出先から会社の端末画面を手元の端末に呼び出し、インターネット環境ならどこからでもマイデスク・マイオフィスを実現できます。

テレワークの導　でお困りの際は、ぜひリモートアクセスサービスをご検討ください。

※「MagicConnect（マジックコネクト）」は、セキュリティ脅威に対するリスクを低減させるものであり、脅威そのものを完全に取り除くものではありません
※「MagicConnect」は、NTT テクノクロス（株）が運営するサービスです
※「Biz ひかりクラウドMagicConnect」は、エヌ・ティ・ティ・スマートコネクト（株）が提供するサービスです
※NTT　　本は、本サービスの販売取り次ぎを実施します
※「MagicConnect」は、NTT テクノクロス（株）の登録商標です
※macOS は、Apple Inc.の商標です

※掲載している情報は、記事執筆時点のものです