デジタルテクノロジー株式会社

Telework

オフィスでも、自宅でも、どこででも。
多様な働き方を、最適なアプローチで実現できる

テレワークソリューション

～そのVPNは安全ですか?～

テレワーク未導入のお客様

何がそのハードルになっていますか?

新型コロナウイルス感染症拡大によって、多くの企業が導入したテレワーク。この新たな働き方は、今後も重要な選択肢の1つになると考えられています。優秀な人材の中には、毎日通勤ラッシュにもまれるよりも自宅で作業したほうが効率がいい、と考える人も多く、育児や家族の介護、病気など従業員の様々な生活背景に対し働き方の選択肢が増えることは、従業員満足度の向上にもつながります。企業側も人材の確保や生産性向上のために、従業員の希望に応じてテレワークが可能な体制を整えておく必要があります。
しかし中堅・中小企業の中には、その必要性を理解しているにもかかわらず、テレワーク導入に踏み切れていないところが少なくありません。

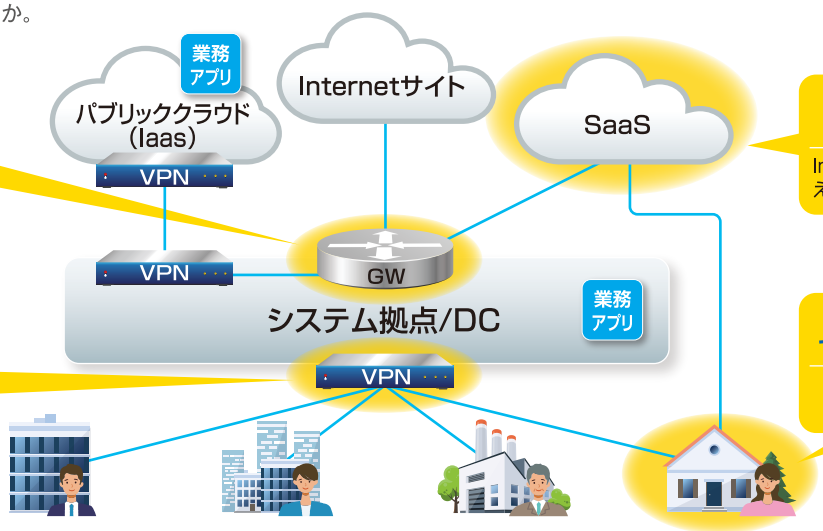
すでにVPNをご活用のお客様

その仕組みにも新たな課題が見えていませんか?

その一方で、すでにテレワークのためにVPNを導入し、社外から社内システムにアクセスできるようにしている企業でも、以下のような複数の問題に直面しているのではないでしょうか。

一極集中問題❶
回線帯域逼迫

一極集中問題❷
VPNユーザ急増による
パフォーマンス不足



シャドウIT問題
Internetにアクセスできれば使えてしまう未許可SaaSの制御

**持ち出しPC
セキュリティリスク問題**
データ漏洩リスク、
端末管理強化

これらの**問題の解決方法**、次のページでご説明します。

解決策1 持ち出しPCセキュリティ対策

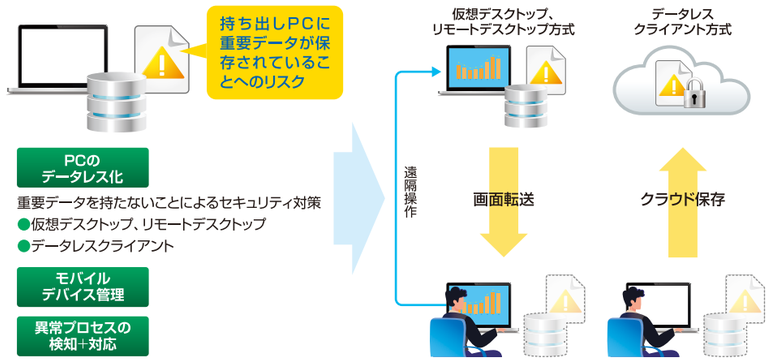
テレワーク化で多くのIT担当者が懸念するのがテレワーク用PCにデータを入れて持ち出し、それが紛失することで発生する情報漏洩ではないでしょうか。またPCを社外に持ち出されると、管理を徹底することが難しいと感じているIT管理者も多いはずです。

このような問題に直面しているのであれば、「**PCのデータレス化**」と「**端末セキュリティの管理**」、「**端末の異常プロセス(挙動・通信)が発生していないかの監視**」を徹底することが効果的です。

「PCのデータレス化」は、持ち出しPCに重要データを保存しないことにより情報漏洩リスクを低減させます。

「端末セキュリティの管理」は、セキュリティソフトがインストールされているか・有効になっているか・バージョンが最新かなどのモバイル端末のセキュリティ設定や、IT管理者が指定するアプリケーションのみ利用許可、などの集中管理を実施しセキュリティを高めます。

また、マルウェア感染を前提とした対策も重要となります。セキュリティソフトのチェックをすり抜けたマルウェアに感染してしまった場合でも、「端末の異常プロセス(マルウェアのふるまい)が発生していないかの監視」を行うことで攻撃を検出し、早期対応を実施することが可能です。

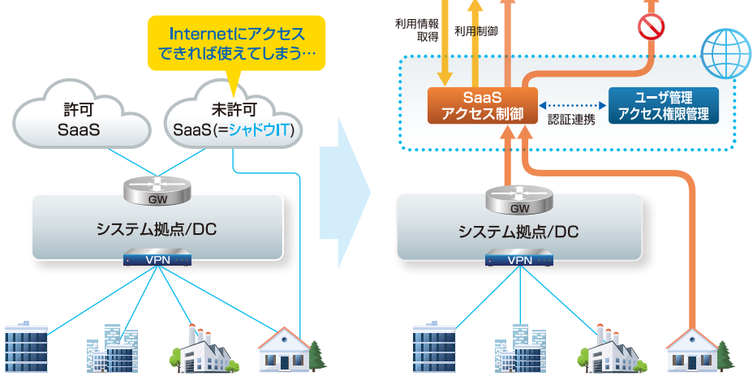


解決策2 シャドウIT対策

テレワークを効率的に行う上で、クラウドサービスの活用は不可欠です。しかし、従業員が勝手にIT管理者の把握していないクラウドサービスを利用するとシャドウITの温床となります。シャドウITが横行すると、企業のセキュリティレベルは大幅に低下し、情報漏洩発生の危険性が高まります。

この問題を回避するため、社内ネットワークを経由させてクラウドサービスの利用を制御する方法もありますが、インターネット経由でクラウドサービスへの接続が可能であれば、このルートをバイパスされる危険性があります。

これらの問題を解決できるのが、クラウドアクセス制御のソリューションです。ユーザとクラウドサービスの間に制御ポイントを設けることで、ユーザ管理・アクセス権限管理の仕組みと連携しながら、**クラウドサービス利用状況の可視化、不正アクセスや不正なデータ移動の抑止、許可されていないクラウドサービスの利用禁止**などを制御することが可能です。

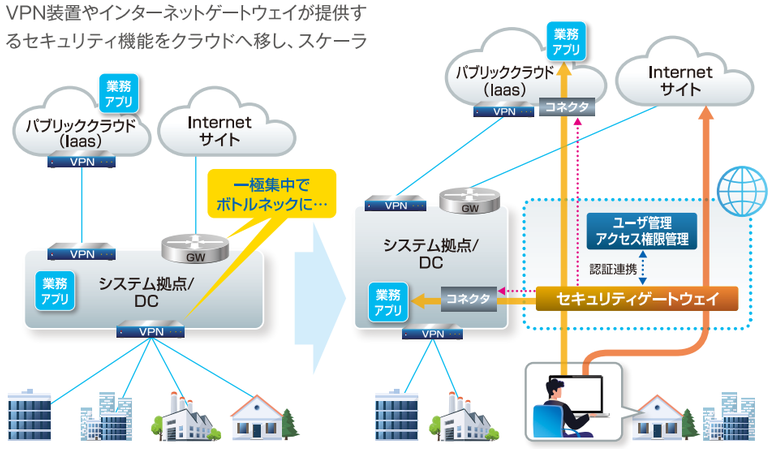


解決策3 システム拠点一極集中対策

社内にVPN装置を設置し、社内システムやクラウドサービスへのアクセスをVPN経由で行うようにすることは、セキュリティ確保を行う上で大きな効果があります。しかし、既にVPNを導入している多くの企業が経験しているように、この方法はテレワーク利用者が増えるとVPNにアクセスが集中し、ボトルネックが生じやすいという問題を抱えています。安全性は確保しやすいものの、アクセスの低速化によってユーザの利便性を損なう危険性があるのです。

この問題を解決できるのが、オンプレミス環境のVPN装置やインターネットゲートウェイが提供するセキュリティ機能をクラウドへ移し、スケーラビリティを確保するというアプローチです。

クラウドサービスとして提供されるセキュリティゲートウェイを介したセキュアな通信経路の構築、Webアクセスのセキュリティチェックなどを組み合わせることで実現できます。セキュリティチェックでは、URLフィルタ、アンチウィルス、サンドボックスなどの機能が統合されているものも多く、ユーザが社外にいても社内と同様に不正なWebサイトによって行われるサイバー攻撃から守ることが可能です。



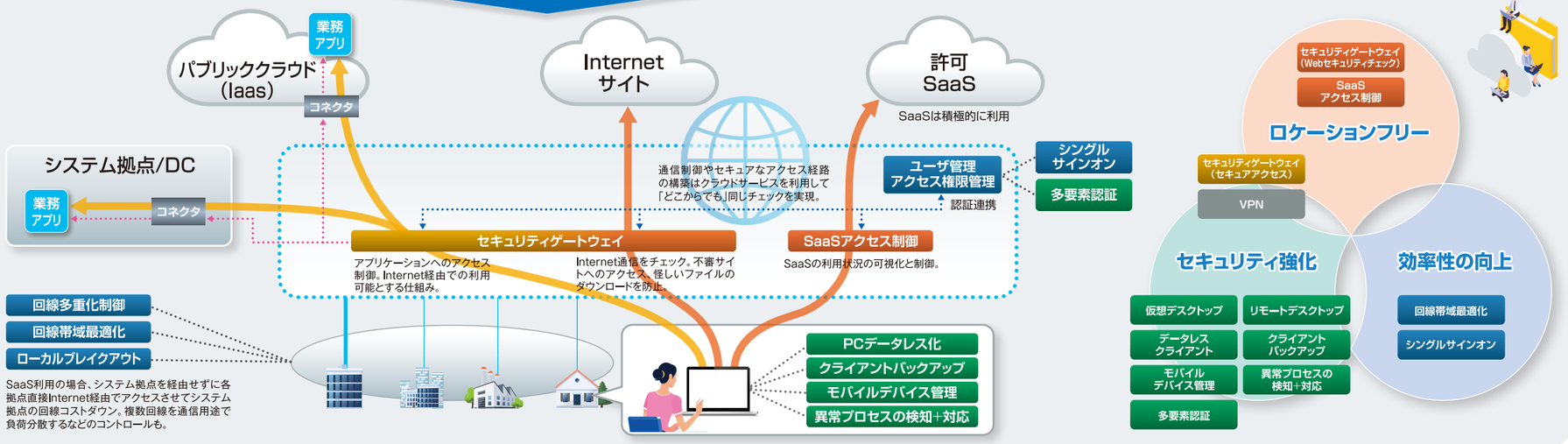
最終的なゴール

めざせ、脱・VPN!

これら3つの解決策のどれから着手すべきかは、その企業が直面している喫緊の課題やセキュリティポリシー、テレワーク対象の従業員の職種や割合などによって変わってきます。デジタルテクノロジーはお客様の状況に合わせて、これらの解決策を柔軟に提案し、その実現をお手伝いします。

しかし、どの解決策から着手するかにかかわらず、最終的なゴールは同じです。**目指すべきは、レガシーなVPNからの脱却であり、テレワークを前提とした新しく安全なネットワークの実現**なのです。

デジタルテクノロジーは、その最終ゴールに到達するまで、お客様とともに走り続けます。



テレワーク化への様々なアプローチ方法

前ページで説明した解決策の他にも、様々なアプローチが考えられます。
デジタルテクノロジーではお客様のテレワーク化をご支援するため、以下のようなソリューションをご提供しています。

クライアントが業務アプリ/データにアクセスする際の経路をセキュアにしたい	セキュリティゲートウェイ（セキュアアクセス）	VPN	
クライアント端末にデータ保存しないことで情報漏洩リスクを減らしたい	仮想デスクトップ	リモートデスクトップ	データレスクライアント
SaaSやWebサイトへのアクセスチェックと制御を、ユーザーの利用環境にかかわらず実行したい	セキュリティゲートウェイ（Webセキュリティチェック）	SaaSアクセス制御	
SaaS利用等によるインターネット向け通信増加に対策を打ちたい	回線多重化制御	回線帯域最適化	ローカルブレイクアウト
クライアント端末の保護、管理をより強化したい	クライアントバックアップ	モバイルデバイス管理	異常プロセスの検知＋対応
SaaS活用時代だからこそ、便利な認証×強固な認証の両立を目指したい	シングルサインオン	多要素認証	
利用しているSaaS内に保存されたデータを保護したい	SaaSのバックアップ（Microsoft 365、Google Workspace、Slackなど）		
テレワーク環境でもオフィスと同様に社員の就業状態を見守りたい	テレワーク就業時間取得システム		

オンプレミスからクラウドファーストへ

テレワークの生産性と安全性の向上は、オンプレミスシステムでは限界があります。そこでおすすめしたいのが「クラウドファースト」の考え方です。これはシステム構築・更改の際に、独自でインフラ構築やアプリケーション開発を行うのではなく、事業者が提供するクラウドサービスの利用を第一に考えるというもの。テレワークでは必然的にインターネットを使った通信が発生するため、SaaSなどのクラウドサービスとの親和性が非常に高いのです。クラウドサービスを積極的に活用することで、以下のメリットが享受できます。

- 管理対象の削減
- システム導入の迅速化
- システム拡張 / 縮退の柔軟性向上
- 運用コストの低減

デジタルテクノロジーでは、クラウド環境に特化したサービスメニュー「D-Cloud」もご用意しています。またお客様のご要望に合わせ、様々なメーカーの製品やサービスを組み合わせてご提案しており、ご予算や優先度に合わせた「段階を踏んだシステム構築」も承っております。さらに、検討計画・導入・運用の各フェーズでのお手伝いができ、お客様のご希望に合わせてそれら全部、もしくは一部のご提供も可能です。

生産性が高く、安心安全なテレワークの実現方法は、ぜひデジタルテクノロジーにご相談ください。

デジタルテクノロジー株式会社

https://www.dtc.co.jp/

［東 京］ 〒104-0032 東京都中央区八丁堀 2-23-1 エンパイヤビル
MAIL：sales@dtc.co.jp

［大 阪］ 〒530-0001 大阪市北区梅田1-13-1
大阪梅田ツインタワーズ・サウス 15F
MAIL：osaka@dtc.co.jp

2024.02