Soliton®

“データ漏えい防止×次世代認証”で テレワークの利便性とセキュリティをともに高める

ニューノーマルに備えゼロトラストへ

テレワークを推進するうえで、セキュリティの確保は最も重要なテーマの一つだ。
その課題解決に向けて、ソリトンシステムズが提供しているのが、次世代認証サービス「Soliton OneGate」と、
テレワーク端末からのデータ漏えいを防ぐ「Soliton SecureAccess」だ。
ソリトンシステムズの話を基に、これらのソリューションによってテレワークセキュリティの何がどう変わるのかを明らかにする。

テレワーク端末にデータを残さない 3つのアプローチ

テレワークを推進するうえで、企業・組織が解決しなければならない課題は少なくない。なかでも大きな課題の一つは、テレワーカーが使う端末（以下、テレワーク端末）からのデータ漏えいリスクをいかにしてゼロに近づけるかだ。そのための手法としては、仮想デスクトップ基盤のVDI（Virtual Desktop Infrastructure）を導入して、テレワーク端末のシンクライアント化を図り、端末にデータが残らないようにするソリューションが広く知られている。ただし、VDIの導入は初期コストが高く、システムの保守・運用管理にも相応の手間がかかる。ゆえにVDIには、全ての企業・組織にとっての最適解とは成りえないというネックがある。

こうした中で、多くの企業・組織に必要とされているのが、VDIよりも安価に、かつ手軽にVDIと同様のテレワーク環境を実現できるソリューションだ。そうしたソリューションの一つが、ソリトンシステムズの「Soliton SecureAccess」（以下、SecureAccess）である。

同ソリューションは、「Soliton SecureDesktop」（以下、SecureDesktop）と「Soliton SecureBrowser」（以下、SecureBrowser）、そして「WrappingBox」という3つのプロダクトによって構成されている。

これらのプロダクトのうち、SecureDesktopは、オフィス内にある自席のパソコンを、テレワーク端末から遠隔操作するリモートデスクトップのソリューションだ。オフィス内のパソコンからテレワーク端末に送られるのは、パソコンの画面のみとなる。ゆえに、端末側にはデータは残らない。

加えて、SecureDesktopの場合、デジタル証明書を使った二要素認証を標準サポートしている。そのため、万が一、ID・パスワードが盗まれても、オフィス内のパソコンが不正に操作される心配はない。

一方、SecureBrowserは、Webベースの社内システムやクラウドサービスを、テレワークで安全に使うためのブラウザだ。このブラウザを使うことでVPNに頼ることなく、社内やクラウドのWebシステムとの通信を全て暗号化することが可能になるほか、Webシステム上にあるデータをテレワーク端末のローカルディスクに保存したり、端末内の他のアプリケーションに渡したりすることを禁止できる。これにより、テレワーク端末にはデータが残らなくなり、テレワーカーが個人的に使用するSNSやメールを通じて会社のデータが外部に流出してしまうといったリスクも低減できる。

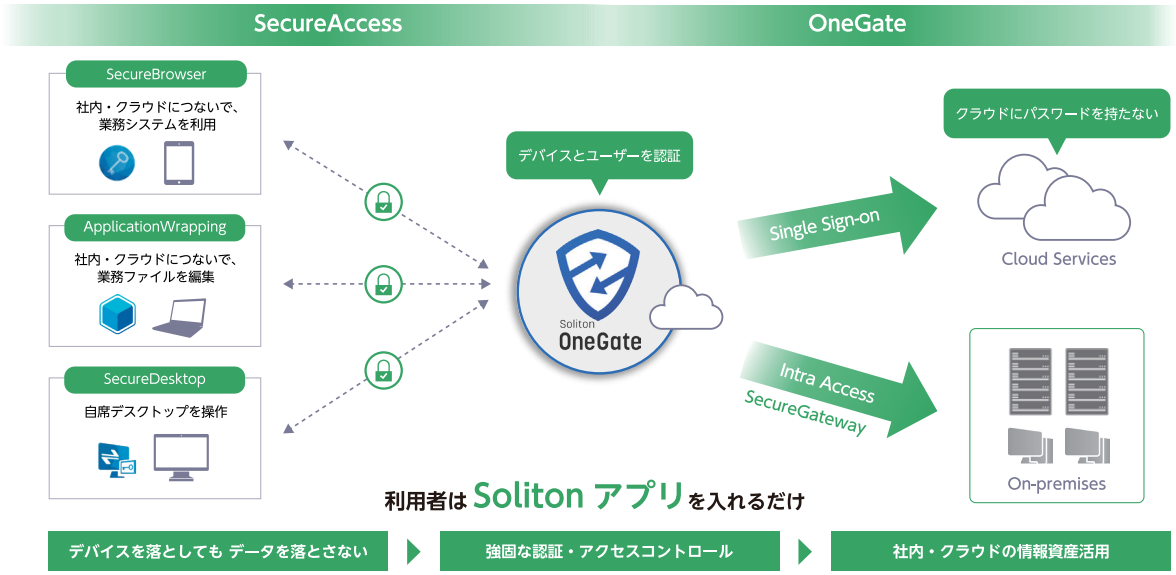
株式会社ソリトンシステムズ
プロダクト & サービス統括本部
新井 ひとみ 氏

株式会社ソリトンシステムズ
プロダクト & サービス統括本部
佐野 誠治 氏

さらに、WrappingBoxは、テレワーク端末にインストールされているWindowsネイティブのアプリケーションをセキュアに利用するための仕組みである。WrappingBoxがテレワーク端末内で、ローカルから論理的に分離されたセキュアなワークスペースを形成し、そこでマイクロソフトのワード（Word）やエクセル（Excel）、Microsoft Teamsなどのアプリケーションを動作させることができる。利用者は、パソコン内蔵のカメラを使ったビデオ会議やチャットを通じたファイルの共有、チャットで受け取ったファイルの編集、クラウドストレージへのアップロードなど、ネイティブアプリとパソコンのリソースをフル活用したさまざまな業務が行える。業務終了時にはワークスペース上で扱ったデータは全てローカルな環境から消去されるため、自宅ネットワークからの情報流出が防止できる。データを消去する前には社内のファイルサーバーへのデータの保存を促すメッセージが表示されるので、うっかり必要なデータが消えてしまう心配もない。

「同じ企業でも部門・部署によって、テレワーク時に利用する業務システムのタイプはさまざまです。業務や端末環境に応じてSecureAccessは3つのタイプが選べます。また全てクラウドサービスでも提供しているため、パンデミックなどの緊急時でも、すぐにテレワーク環境を整える必要がある場合にも、SecureAccessを採用いただくことで、多くの手間とコストをかけずに、セキュアなテレワーク環境を実現いただけます」（ソリトンシステムズ プロダクト & サービス統括本部、新井 ひとみ氏）。

図：ソリトンシステムズが提供するテレワーク・セキュリティソリューション



社内システムとクラウドサービスの「認証」を統合する

ソリトンシステムズでは、SecureAccess に加えて、テレワークのセキュリティを巡る企業・組織の現状を直視したソリューションも提供している。それは、「Soliton OneGate」（以下、OneGate）と呼ばれる次世代認証サービスだ。

周知のとおり、今日の企業・組織では、クラウドサービスの活用が進み、業務の現場では、Office 365 や Salesforce、G Suite、box をはじめとする多種多様なクラウドサービスが使われている。また、こうしたクラウド活用の潮流は、新型コロナウイルス感染性の流行をきっかけにしたテレワークの普及に伴い、さらに勢いを増すことが予想されている。

このようなクラウドシフトの中で、企業・組織の情報セキュリティを脅かす問題として深刻化しているのが、クラウドサービス上の情報資産に対する不正侵入だ。その背景には、業務の現場で使われるクラウドサービスの種類が増えたことで、ログイン ID・パスワードがクラウド上に散在するようになり、情報システム担当者によるアカウント管理が煩雑になっている現実がある。

「クラウドサービスのアカウント管理が行き届かなくなると、例えば、退職者のログイン ID が消去されずにそのまま残され、それが不正に利用されるなどのリスクが膨らみます。このような状況を打破するために、クラウドサービスと社内システムの認証情報を 1 つにまとめる役割を担うのが、OneGate です」と、ソリトンシステムズ プロダクト & サービス統括本部の佐野 誠治氏は言う。

佐野氏の言うように、OneGate は、クラウドと社内にまたがる業務システムの ID と認証を統合し、アカウント管理の自動化とシングルサインオン（SSO）、そして多要素認証を提供するサービスだ。社内の Active Directory（AD）で管理されているユーザー情報を読み取り、各クラウドサービス用に情報を整形して投入する機能を備えている。これによって、情報システム部門の担当者は AD のメンテナンスだけを行えばよくなり、各クラウドサービスに対するアカウントの作成・変更・削除運用は OneGate によって自動化されるようになる。また、この仕組みの中ではクラウド上にユーザーの認証情報を保管する必要がなくなり、パスワードが各所に散在し管理が行き届かなくなる、といった心配も不要となる。

脱 VPN、ゼロトラストに向けた第一歩

OneGate サービスは、デジタル証明書配布アプリ「Soliton KeyManager」を包含しており、AD のアカウントに基づきながら、デジタル証明書を安全かつ容易に配布する機能を提供している。また、FIDO2 認証にも対応し、パスワードレスの多要素認証環境が実現できる。これによって、クラウド活用のセキュリティレベルと利便性をともに高められると、佐野氏は説明を加える。

テレワークの継続検討やクラウドシフトの加速に伴い、ますます注目を集める「脱 VPN、ゼロトラスト」の実現に向けて、まず取り組むべきは ID 認証基盤の整備だ。ゼロトラストモデルでは、業務システムの利用を、信頼できる社内ネットワークではなく、信頼できるユーザーとデバイスに限定することが前提になるためだ。

「デジタル証明書を安全に運用できる OneGate なら、利用ユーザーに加えて利用デバイスの特定も容易となり、社内からのアクセスに限定していたクラウドの利用を自宅ネットワークからの利用に開放することが可能となります。さらに、デバイスからのデータ漏えいを防止する SecureAccess を活用すれば BYOD 活用も可能となり、今ある環境を活かしながら、テレワークを推進することが可能となります」（佐野氏）。

ソリトンシステムズでは、そうした OneGate と SecureAccess を中心に、運用負荷がかからず、安全で利便性の高いテレワークのセキュリティソリューションを提供していく考えだ（図）。

株式会社ソリトンシステムズ（Soliton Systems K.K.）

住所 …… 東京都新宿区新宿 2-4-3
URL …… https://www.soliton.co.jp/
メール …… natsales@soliton.co.jp