未来を拓くチカラと技術。

NTT AT

News Release

2021 年 10 月 29 日
NTTアドバンステクノロジ株式会社

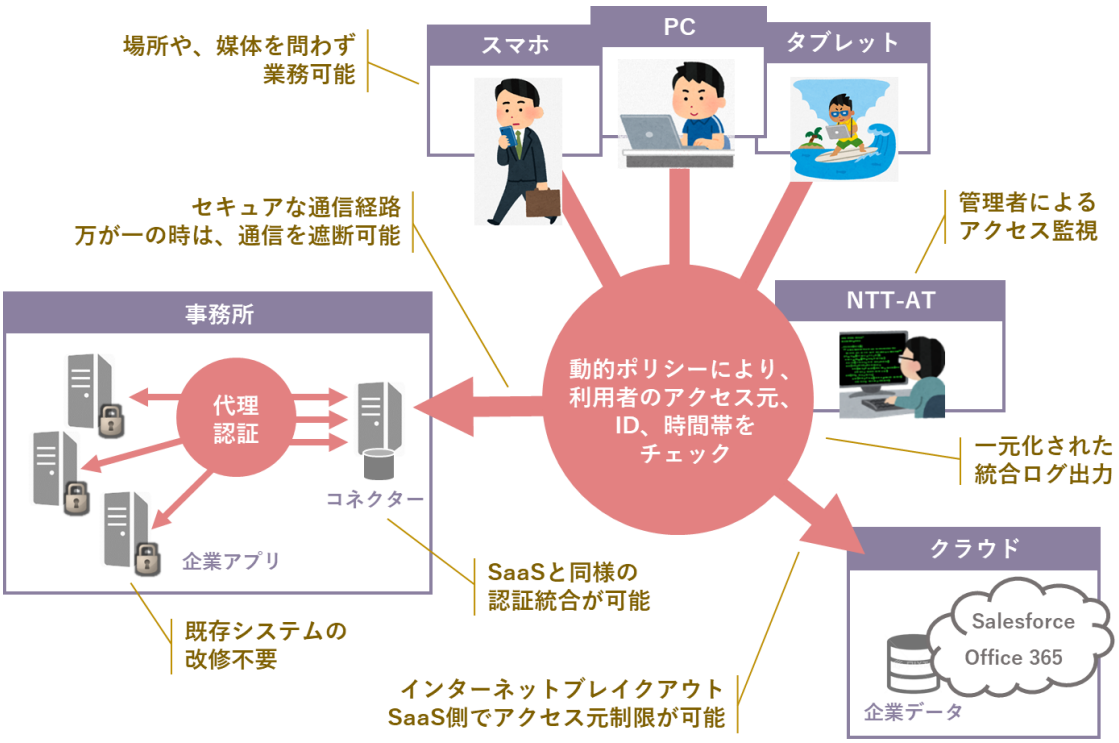
社内システム・クラウドサービスへ安全に接続する リモート接続サービスの提供開始
～ゼロトラストモデルに基づいたリモート接続サービス～

NTT アドバンステクノロジ株式会社（以下：NTT-AT、本社：東京都新宿区、代表取締役社長：木村丈治）はテレワークを実施中および導入を検討している企業向けに、さまざまな端末（PC、スマホ、タブレット、BYOD 端末）と社内システムやクラウドサービスとの接続を、社外からでもエージェントレスでセキュアに実現するリモート接続サービス（以下：本サービス）の提供を 2021 年 11 月 16 日から開始します。

本サービスは、ゼロトラストモデルに基づき、利用場所や利用時間等の設定によるきめ細やかな認証・認可を用いてセキュリティを強化します。また、クラウドサービスには直接接続することで社内ネットワークの負荷増大を回避できます。さらに、リモート接続に特化することで、月額 550 円～／ユーザー（税込）で提供します。

NTT-AT は、本サービスに関するコンサルティングから構築・導入支援・運用・監視までをワンストップ提供し、外出先やテレワークでの業務を望まれるお客様に安全かつ利便性の高いリモート接続環境の実現を支援します。

1．サービス・ソリューションの全体像



２．提供開始の背景・ねらい

昨今、働き方改革や新型コロナウイルス感染症への対応策としてテレワークを導入する企業が増えています。従来、テレワークの導入にはVPNを用いることが一般的でしたが、VPNには専用アプリがインストールされた端末（通常、社給端末）が必要であることや、端末種別が限定される等の制約がありました。しかし、社給端末の持ち出しには紛失の懸念があり、働き方の自由度が高まる現状ではスマホやタブレット等、多様な端末での業務実施が必要になります。リモートアクセスの対象としては、DX（デジタルトランスフォーメーション）によりWebベースでアクセスできる社内システムやSaaS等のクラウドサービスの利用も多くなっています。

一方、セキュリティの側面からは、ランサムウェアに代表される標的型攻撃により端末内に保管したパスワードの流出などの影響を最小化するために、境界型セキュリティ防御モデルに加え、“ゼロトラスト”というセキュリティモデルが普及してきました。

ゼロトラストでは、情報リソースを本当に必要とする利用者に対して限定的にアクセスを許可します。利用者の認証結果から無条件にアクセスを許可するものではなく、アクセス場所や時刻などをベースにリスクベースの動的ポリシーに則って認可を行うことで、不正アクセスのリスクを軽減します。

３．本サービスの概要・効果

本サービスは、ビジネス環境の変化によりDXが浸透し、Webベースの社内システムやクラウドサービスが多くなったことから、アクセス先をWebベースのシステムに限定することで、VPN接続の際に必要とされていた端末エージェントが不要となり、ブラウザーのみでリモート接続できるようにいたしました。これにより、スマートフォンやタブレット、さらにはBYOD端末などの社給端末以外からも社内システムやクラウドサービスに接続することが可能となりました。

本サービスは、ゼロトラストモデルに基づき、社外からアクセスできるプロキシサーバーで強固な利用者認証を実施し、利用者単位でアクセスできるサーバーを制限します。さらに、実際に社内やクラウドのサーバーにアクセスする際には利用者のアクセス場所や時刻などをベースにリスクベースの動的ポリシーに則ったきめ細やかなアクセス制御を行い高度なセキュリティを担保します。

また、社内に設置するコネクターにおいて社内システムの認証を代理で実施することにより、利用者がID・パスワード管理を行う必要がなくなるため、標的型攻撃により端末内に保管した ID・パスワード情報の漏えいリスクを軽減することができます。

NTT-ATは、テレワークの推進とともに安心して利用できる環境作りを支援してまいります。

４．本サービスの主な機能・特長

機能	特長
リモート端末からの社内システム、クラウドサービスへの接続	**導入時**
	SAML[*2]に対応していないオンプレミス社内システムも、IDaaS[*3]と連携させることでSaaSと同様に利用可能
	独自認証方式を利用している社内 Web サーバーも社内にコネクターを設置することで改修不要
	クラウドサービスに接続して利用するため、端末にエージェントツール不要
	利用時
	ゼロトラストモデルに基づいており、アクセスの度に毎回認証・認可を行うことで高度なセキュリティを担保

	代理認証機能により、各システムに存在するパスワードを利用者に管理させないことで標的型攻撃などによるパスワード漏えいリスクを大幅低減
	ブラウザー一つで利用可能とすることで利用端末を限定しない
	社内を経由せず直接クラウドサービスへ接続（インターネットブレイクアウト）可能
	運用時
	万が一の時は通信を遮断可能
	セキュリティインシデント発生時の調査・対応をより迅速に行うために、プロキシサーバーに各社内システムへのアクセスログを一元管理

５．提供開始

2021 年 11 月 16 日

６．提供価格

1ID　550 円～/月額（100ID から）＊税込。サポート費用を含みます。

*別途、初期導入費用・社内システム連携費用が掛かります。

７．今後の展望

NTT-AT は本サービスについて、端末監視制御や可視化機能など、さまざまな提供ソリューションの拡張により、お客様に安心・安全なテレワーク環境を提供してまいります。

*1：ゼロトラストモデル

⇒ 2010 年にアメリカの調査会社であるフォレスターリサーチのジョン・キンダーバーグ（John Kindervag）調査員によって提唱された、「信頼せず攻撃されることを前提とする」という考え方に基づいた、セキュリティのコンセプト。

*2：SAML

⇒ 「Security Assertion Markup Language」の略で、シングルサインオンを実現する仕組みの一つ。

*3：IDaaS

⇒ 「Identity as a Service」の略で、クラウド経由で ID 認証ならびに ID パスワード管理、シングルサインオン、アクセス制御などを提供するサービス。

本件に関するお問い合わせ先

【商品に関するお問い合わせ先】
NTTアドバンステクノロジ株式会社
セキュリティ事業本部
セキュリティサービス&ソリューションビジネスユニット
ゼロトラストサービス担当
https://www.ntt-at.co.jp/product/zerotrust-ztna/

【報道関係のお問い合わせ先】
NTTアドバンステクノロジ株式会社
ビジネス推進部
コーポレート・コミュニケーション部門
担当：加藤・増田
E-Mail：inquiry@ml.ntt-at.co.jp