ホワイトペーパー

Always Secure. Always Available.

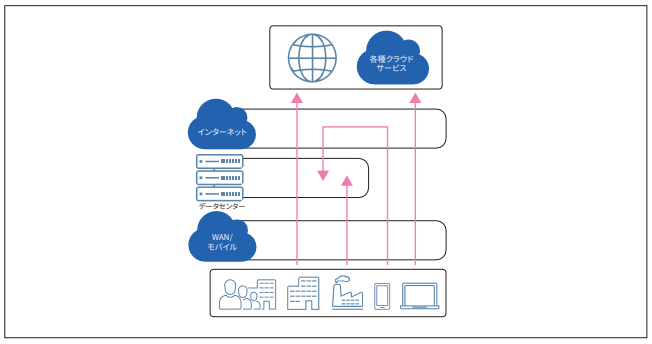
ゼロトラスト実現への最初の一歩
「A10 Cloud Access Controller」

いま「ゼロトラストセキュリティ」が注目されています。ただしゼロトラストセキュリティとは概念のことであり、特定の製品やソリューションを指すわけではありません。そのため「どこから始めれば良いのかわからない」「コスト（時間、費用、稼働）がかかるのは困る」といった懸念をお持ちではないでしょうか。A10 Cloud Access Controllerはそうした懸念を払拭するA10ネットワークスの新しいクラウドサービスです。長年培ってきた実績と技術により、ネットワークの最適化とセキュリティをご提供します。

どこからでも安心・安全に働くための課題

デジタルトランスフォーメーション（DX）推進への機運が高まるとともに、コロナ禍による在宅勤務・テレワークが急速に普及したことにより、多くの企業がセキュリティ対策を見直そうとしています。特に、どこからでも安心・安全に働ける環境を提供するために、従来の境界型防御を前提としていたネットワークセキュリティは大きく変化する必要に迫られています。従来のようなVPN（仮想プライベートネットワーク）経由で社内へアクセスし、そこから複数のクラウドサービスを利用するといったネットワーク構成では、インターネットやWANなど通信回線のひっ迫、プロキシやファイアウォールなどネットワーク／セキュリティ機器の負荷増大によって遅延の発生を招き、業務に支障を来すおそれがあります。そうした負荷を軽減するためにクラウドサービスを直接利用するように経路を変更すると、今度はセキュリティ対策が難しくなり、ガバナンスの効いていない「シャドーIT」の問題も発生します。

■クラウド時代のネットワークの課題

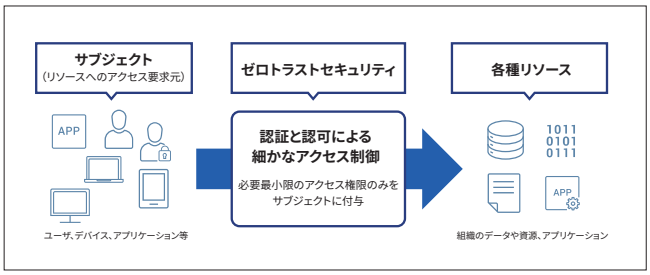


企業ネットワークの守り方を変える

クラウドサービスを快適に利用しながら、どこからでも安心・安全に働ける環境を実現するには、ネットワークの境界にセキュリティゲートウェイを設置する従来の「境界防御型セキュリティ」だけでは十分な対策ができません。なぜなら社内だけでなく社外にも守るべき資産が存在し、その場所へのアクセス方法も多様なためです。こうしたセキュリティ事故の発生を最小化する対策として注目されているのが「ゼロトラストセキュリティ」です。これは「社内ネットワークは安全」のような暗黙の信頼をなくし、すべてのアクセスを認証・認可機能でそのつど検証し、詳細に設定した権限ごとに制御を行うことにより、データやアプリケーションの利用の安全性と情報保護を実現しよう、という考え方です。

ちなみに、日本政府のCIOポータルで公開されている「クラウドサービス（SaaS）活用のためのネットワーク設計」でも、IPアドレス・ドメイン名・アプリケーション識別に基づいたトラフィック制御技術を取り入れ、既存の境界防御型セキュリティに依存しないゼロトラストセキュリティを実現していくことが示されています。場所を問わない働き方とクラウドサービスの利用が一般化するこれからの時代、ゼロトラストセキュリティを意識してネットワークを設計することが潮流となるのは間違いありません。

■ゼロトラストセキュリティの働き



ゼロトラストセキュリティを実現するには？

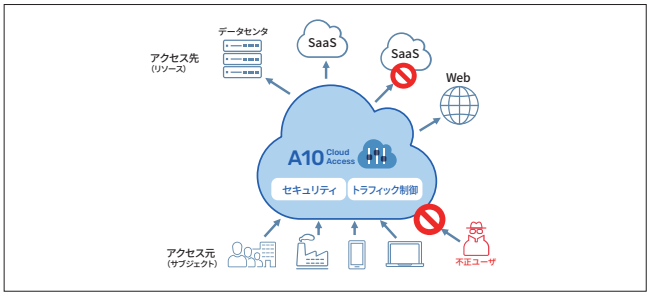
では、ゼロトラストセキュリティという概念を実現する新しいネットワークへと変えていくには、どのような製品・ソリューションを導入すればよいのでしょうか。そうした製品・ソリューションの中でも、多くの企業や官公庁から絶大な支持を得ているのが、A10ネットワークスの「A10 Cloud Access Controller」です。

A10 Cloud Access Controllerは、クラウドサービスと社内のオンプレミス環境、そして社外のリモート環境といった様々なネットワーク経路、例えるならそれぞれに張り巡らされた道路の交通整理や舗装することで安全性と利便性を両立させる機能をクラウドサービスとして提供します。

ゼロトラスト環境の導入の大きな誤解の一つに、既存のインフラをすべてクラウドに移行する必要がある、というものがあります。実際に全てを移行するには企業のセキュリティポリシーや費用・時間などの面からも非常に困難です。

それに対しA10 Cloud Access Controllerは、従来のネットワークやデータセンター設備を変更したり、新たな通信回線や機器を導入したりする必要はありません。ユーザーやデバイスなどアクセス元（サブジェクト）と各種クラウドサービスや自社データセンターなどアクセス先（リソース）の間にクラウドサービスのA10 Cloud Access Controllerを挟み込むだけで、ネットワークのトラフィック管理・制御・最適化と、IDベースの認証・認可を含むゼロトラストセキュリティを実現できます。例えば、在宅テレワークのユーザーだけをA10 Cloud Access Controller経由に変更することで、データセンターや社内ネットワークの負荷を軽減し、快適なアクセス環境を入手できます。

■A10 Cloud Access Controllerの役割



■A10 Cloud Access Controller の位置づけ

	境界防御指向	ゼロトラスト指向
クラウド	クラウド型セキュリティサービス（SASE、SSEなど）	A10 Cloud Access Controller Zero Trust Network Access型サービス
オンプレミス	プロキシ、ファイアウォール、UTM、IPS、IDS	A10 Cloud Access Proxy、ローカルブレイクアウトソリューション

■他社SASE/SSE製品・サービスとの違い

	A10 Cloud Access Controller	他社SASE／SSE製品・サービス
トラフィック制御	・全てのトラフィックをサービスに渡す必要が無い ・ドメイン名による正確な通信のブレイクアウト（DPIや宛先IPアドレスを利用しない） ・サービスアクセス時の送信元IPの固定が可能	・基本的には全てのトラフィックを通す前提 ・ローカルブレークアウトはクライアントソフトのアプリケーション認識機能による ・送信元IPアドレスの固定は困難
リモートアクセス	・リバースプロキシを用いたリモートアクセス ✓基本ライセンスにバンドル ・お客様のID基盤と連携したZTNAの実現 ✓高度なADC機能も利用可能	・クライアント側に、IPsec-VPNを利用するためのソフトウェアインストールが必要 ✓多くのベンダ製品では追加ライセンスが必要 ・お客様のID基盤と連携したZTNAの実現
セキュリティ	・提供元が明らかなベンダ製品群から、お客様にとって最適なセキュリティ機能を選択・提供	・独自技術または単一ベンダによるセキュリティソリューション
SaaSのテナント制御	・SSL/TLS可視化による柔軟なテナント制御（多くのSaaSに適用可能）	・限定的なSaaSに対するテナント制御機能の提供
ハイブリッドアプローチへの対応	・クラウドサービスとオンプレミスの共存が可能（例：SSL/TLS可視化はクラウド上で実施せずにオンプレミスで実施し、セキュリティを担保	・全ての通信をクラウドサービスに流す前提（サービスへの全幅の信頼が前提）
ライセンス	・通信量に依存しないライセンス ・Basic,Standard,Advancedのシンプルな包括ライセンス ・クライアント数単位でのサブスクリプション	・製品によっては通信量でライセンス料が変わる場合あり ・機能ごとにライセンスが必要な場合あり

ワールドワイドで豊富な実績がある機能をクラウドサービスで提供

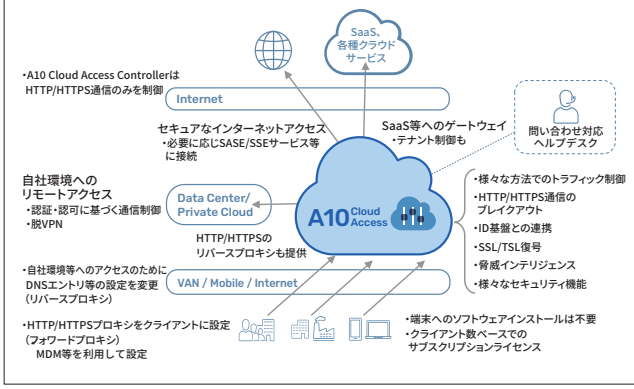
A10 Cloud Access Controllerの概要は下図のとおりです。A10 Cloud Access Controllerが実現・提供する機能自体は、グローバルで豊富な実績があるA10のプロキシ技術、ADC（Application Delivery Controller）技術がベースです。通信キャリアやISP、企業ネットワーク、官公庁・自治体など様々な分野への導入で培ったノウハウとともに、トラフィックの最適化や様々なセキュリティ機能をA10のクラウドサービスとして安心してご利用いただけるものになっています。オンプレミス側の機能との共存・連携ができ、既存の設備等と組み合わせて分散セキュリティ環境を構築することもできます。さらに、ゼロトラスト環境そのものも必要に応じて随時拡張や変更が必要ですが、その基盤ともなります。

また、テレワークで利用するデバイスなどクライアント側にはエージェントなど特別なソフトウェアをインストールする必要がないことも特徴となっています。SSLを復号し脅威を可視化する「SSLインサイト機能」も有しています。この機能により詳細ログの取得や高度なトラフィック制御、セキュリティ機能との連携が可能です。ID管理基盤や既存のA10ソリューションとも容易に連携して利用できます。

A10ネットワークスでは、これらの機能を備えたA10 Cloud Access Controllerを、シンプルなライセンス体系で提供しています。提供機能の違いによる「Basic」「Standard」「Advanced」という3種類の包括ライセンスが基本で、必要に応じて選べる追加オプション、といった形式です。クライアント数に応じた課金体系を採用しているので、たとえトラフィックが増えたとしても追加コストを支払う必要はありません。

例えば、Zero Trust Network Access (ZTNA) やSecure Web Gateway (SWG) といった、ゼロトラスト環境の検討時のキーワードがありますが、A10 Cloud Access Controllerによって実現することも可能です。

■A10 Cloud Access Controllerの概要

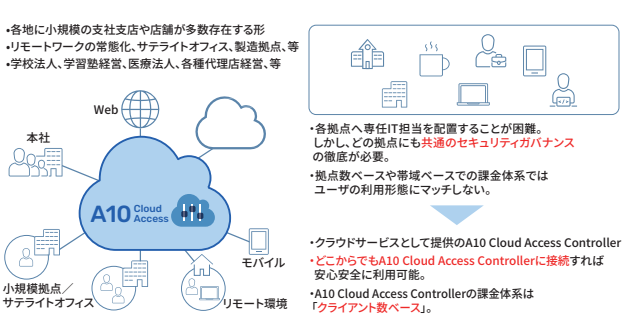


■主な提供機能とライセンス

機能	ライセンス種別			
	Basic	Standard	Advanced	追加オプション
フォワードプロキシ	○	○	○	
リバースプロキシ	○	○	○	
トラフィック制御機能	○	○	○	
認証基盤連携	○	○	○	
アクセスログ保管	○	○	○	
URLフィルタリング	○	○	○	
SSL/TLS復号		○	○	○
SaaSサービスのテナント制御		○	○	○
IPアドレスレピュテーション			○	○
アプリケーション可視化と制御			○	○
アンチマルウェア				○
コンテンツ無害化				○
データ損失防止				○
Site-to-Site IPsec VPNによる接続				○

A10 Cloud Access Controllerのユースケース

■① 小規模多拠点



■② IoTデバイス、エッジでの処理後のネットワーク接続

Learn More

About A10 Networks

お問い合わせ
a10networks.co.jp/contact

A10ネットワークス株式会社

www.a10networks.co.jp
a10networks.co.jp/contact

Part Number: A10_SB_Proxy MAR 2022