SONICWALL

SonicWall Cloud Edge Secure Access

ゼロトラストセキュリティを数分で導入

SonicWall Cloud Edge Secure Access は、サイト間や AWS、Azure、Google クラウドなどのハイブリッドクラウドへの接続性を向上させ、サイト向けにシンプルなサービスとしてのネットワーク（NaaS）を提供する強力なクラウドサービスです。このプロセスでは、ゼロトラストと最小権限のセキュリティアプローチを1つの統合されたサービスとして組み合わせます。

最小権限アクセスのアプローチでは、特定のユーザーのアクセスを必要なものだけに制限し、それ以上は何も与えられず、これは「知る必要のある人に限定して知らせる」という概念に似ています。ネットワークの他の機密領域へのアクセスを制限することで、組織は運用の柔軟性を犠牲にすることなく、リソースを保護することができます。

SonicWall Cloud Edge Secure Access は、4つの主要なセキュリティアクションに基づいてゼロトラストセキュリティを適用します。

- 内部トラフィックであっても、ユーザーとデバイスの認証情報を検証する
- 出所の正しさと企業ガイドラインへの準拠を保証するために、リクエストの文脈を判断する
- ネットワークアクセスのマイクロセグメント化を促進し、脅威の 横への移動を防止
- 要求されたアプリケーションだけにアクセスを限定し、それ以上のアクセスを認めない

Cloud Edge Secure Access のインフラの中核を形成するのは、最新の設計によるセキュリティの SDP（Software-Defined Perimeter）アーキテクチャです。

SDP は、ユーザーやデバイスを認証するコントローラをトラストブローカーとして機能するゲートウェイから分離します。ゲートウェイをエンドユーザーの近くに分散させることで、Cloud Edge Secure Access サービスは素早くスケールアップして高性能を維持し、最高のクラウド体験を提供することができます。

また、機能の分離により、DDoS、公衆無線LANの乗っ取り、SYN フラッド、Slowlorisなどの一般的なサイバー攻撃の脅威を効果的に阻止し、SonicWall は高度に統合されたゼロトラストセキュリティプラットフォームを提供することができます。

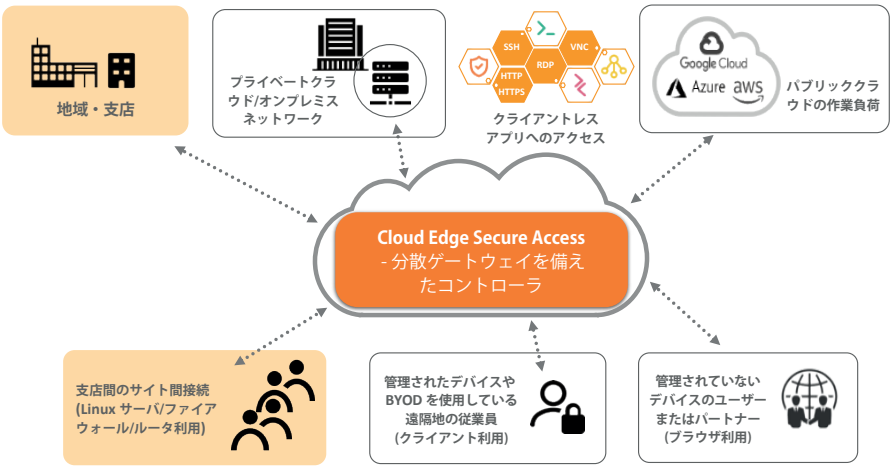

図 1 – SonicWall Cloud Edge Secure Access

メリット

- 分散型企業、リモートワークを行う社員向けのセキュリティソリューション
- ハイブリッドクラウド上のあらゆるサイトやリソースへの即時の安全なアクセス
- ネットワーク、アプリケーション、ユーザー、デバイスプロファイルによるゼロトラストポリシー
- マイクロセグメンテーションを内蔵し、不正の横への移動を防止
- 100人から数千人規模のユーザーに対応
- IT 管理者は15分で設定可能
- エンドユーザーは5分で導入可能
- 使用量・帯域制限なし
- 公衆無線 LAN セキュリティ
- 高性能 WireGuard の暗号化
- クラウド アイデンティティプロバイダーとの統合
- 最新の SSO と MFA の統合
- DDoS、Slowloris、SYN フラッドを阻止
- MSSP 向けのマルチテナント
- コンプライアンス監査のための完全なモニタリングとレポート機能
- 専用のクラウドゲートウェイと顧客ごとのIPアドレス
- サービスは、米国、ヨーロッパ、中東、アジアで利用可能

従来のVPNからゼロトラストセキュリティへの進化

社員がどこにいても仕事ができ、リソースがクラウドにあるデジタルトランスフォーメーションの時代には、従来の VPN ソリューションは導入が複雑で、制約が多すぎる傾向があります。

典型的な VPN の導入には、数日から数週間かかることもあり、備品の入手可能性により、稼働停止を計画するのが困難な場合もあります。

従来の VPN は、ログインに成功した場合、ユーザーに広範囲のネットワークアクセスを提供し、サブネット内での側方移動が可能なため、潜在的な侵入のためのバックドアを開く可能性があります。

さらに、VPN は、ユーザーのトラフィックがクラウドに直接送られるのではなく、オンプレミスの VPN コンセントレーターを経由するため、追加のレイテンシーが発生し、ユーザーのクラウド体験を低下させる原因となります。

Gartner の調査によると、2023 年までに、60% の企業が自社のリモートアクセス仮想プライベートネットワーク（VPN）の大半をゼロトラストネットワークアクセス（ZTNA）に移行すると予測しています。

SonicWall Cloud Edge Secure Access は、前述の問題点を克服し、このような3つの必須の機能を備えた ZTNA を提供します。

企業資産を保護するための最小特権アクセス

セルフサービスによる迅速な導入

どこからでもクラウドにダイレクトに信頼性の高いアクセス

図 2 – SonicWall Cloud Edge Secure Access 機能

主な使用事例

セルフサービスによる迅速な導入

- **迅速な導入** – IT マネージャーは、サインアップ、ゲートウェイのインスタンス化、ネットワークとユーザーのコンテキストに基づいたきめ細かなポリシーの構成を 15 分以内に行うことができます。
- **迅速なユーザーオンボーディング** – エンドユーザーは、モバイルまたはデスクトップのクライアントアプリを介して接続するか、またはブラウザを備えた公共のコンピュータを使用している場合、クライアントのインストールを完全に回避するという選択肢があります。セルフサービスの導入モデルでは、ユーザーは 5 分で設定し、立ち上げることができます。
- **ハイブリッドクラウドへの信頼性の高いアクセス** – 完了すると、ユーザーは世界中のどこからでも、オンプレミスやパブリッククラウドのリソースに素早く、簡単に、かつ安全にアクセスします。

信頼されたホットスポットでも公衆無線LANでも接続を保護

- **自動 Wi-Fi セキュリティ** – Windows および Mac OS 用の Cloud Edge Secure Access エージェントアプリケーションは、環境をプロアクティブに監視し、公衆無線 LAN でのセキュアアクセスによる接続を自動的に有効化します。それによりデータの盗難やコンプライアンス違反を引き起こす可能性のある、ありふれた Wi-Fi の傍受からユーザーを保護します。
- **非常停止スイッチ** – 潜在的なサイバー攻撃を阻止するために、セキュアアクセス接続が中断されると、デバイスのインターネット接続が即座に停止し、デバイスからのデータの流出を防ぎます。
- **信頼できるWi-Fiネットワーク** – SSID が信頼できると指定されている場合、自動Wi-Fiセキュリティ機能は作動しません。
- **常時接続型 VPN/アプリケーション** – この便利な機能は、再ログインまたは再認証を必要とせずに、ユーザーやデバイスを1つのアプリケーションまたは一連のアプリケーションに自動的に再接続します。

図 3 – Apple iOS用 SonicWall Cloud Edge Secure Access管理コンソールとモバイルエージェントアプリケーション

ゼロトラストアプリケーションアクセス

Cloud Edge Secure Access は、デジタル組織が切望していた機能を提供し、企業のリソースを保護すると同時に、リモートワークを可能にし、担当社員に権限を与えるためのツールです。

Secure Accessのゼロトラストポリシーを使用することで、適切なコンテキストを持つ外部ユーザーは、企業ネットワークをサイバー攻撃の脅威にさらすことなく、リモートデスクトップやウェブアプリケーションのホストに安全にアクセスすることができます。

- **最小権限アクセス制御を厳格に実施** – 組織は、ユーザーやグループの IDやアクセスされるデータの機密性といった関連属性に基づいて、リソースとのやりとりをコントロールすることができます。
- **コンテキスト主導** – このソリューションは、オンプレミスとクラウドでホスティングされているリソースに対しユーザーを重視したポリシーベースのアクセスを確保します。
- **クラウドベースの主要なID管理プロバイダーを活用し統合** – 組織は、オンプレミスのレガシー IT 資産のサービス寿命を延長するか、Azure AD、Google Authenticator、Okta などのプロバイダーが提供する最新のクラウドベースのID管理サービスに移行することができます。
- **マイクロセグメンテーション** – 各インバウンド トラフィックを正確なセグメントに分割することで、マルウェアや不正なユーザーが横方向に移動するのを防ぎ、攻撃の対象となる場所を減らし、サイバー攻撃の全体的な脅威にさらされるのを低減します。
- **シングルサインオンと多要素認証の連携** – この組み合わせは、単一のポータルから、ユーザーをハイブリッドのIT環境へと認証することにより、一貫性のあるシームレスなユーザー体験を実現します。
- **コンプライアンス監査の利便性** – すべてのゼロトラストアクセス活動は、将来の監査のために完全にモニタリングされ、記録されています。

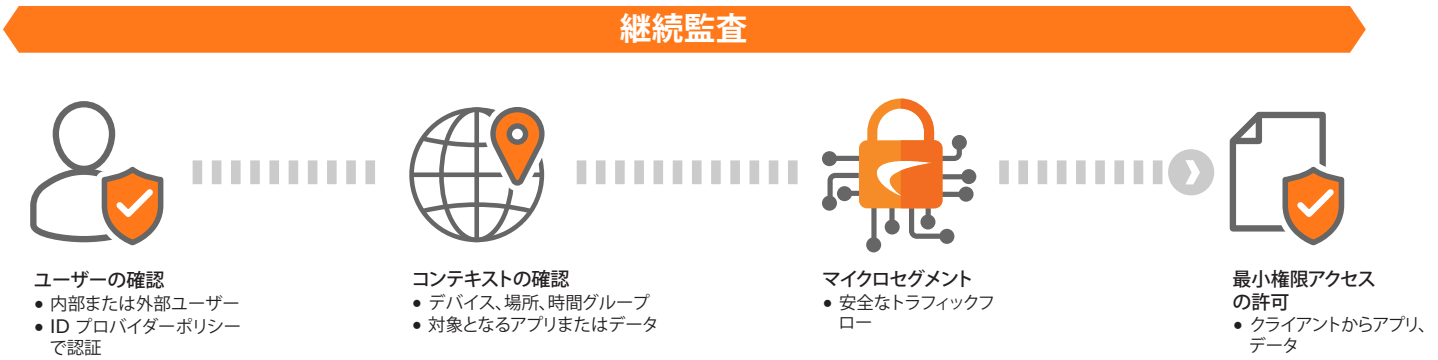

図 4 – SonicWall Cloud Edge Secure Access ZTNA プロセス

サイト間の相互接続性またはサービスとしてのネットワーク（NaaS）

Cloud Edge Secure Access は、サイト間接続サービスまたはサービスとしてのネットワーク (NaaS) を提供し、地理的に分散した場所にある支店を迅速なオンボーディングを可能にします。

NaaS を利用することで、IT 管理者は、コストのかかる MPLS に依存することなく、キオスク端末、小売店、セールスポイントをクラウド型リソースに迅速かつ安全に接続することができます。

- **サイト間またはサイトからクラウドへの相互接続サービス** – このソリューションは、AWS、Azure、Google Cloud などの一般的なクラウド環境に簡単に接続したり、異なるサイトにある2つの異なるネットワーク間の安全な通信リンクを作成します。
- **複数の地域での導入** – 管理者は、専用の Cloud Edge ゲートウェイをさまざまな場所に導入して、国際的な支店と社員に最適なサービスを提供することができます。
- **高性能なグローバルバックボーン** – SonicWall Cloud Edge サービスは、グローバルで利用可能で、お客様の拠点に近い場所にゲートウェイを分散し、サーバー全体のトラフィックの負荷を分散させることで、レイテンシーを最小限に抑えます。
- **最先端の WireGuard トンネル** – IT マネージャーは、IPsec を搭載したすべてのブランチルーターやファイアウォールを駆使して、最寄りのCloud Edge ゲートウェイに接続することが可能です。

最高のパフォーマンスを実現するために、SonicWall は、最寄りのゲートウェイへの WireGuard トンネルサービスを実行するブランチ Linux サーバーを使った WireGuard コネクター機能を推奨します。

- **ネットワークの監査とモニタリング** – グループやサーバーの作成、チームメンバーの認証、パスワードの変更などの可視性を含めてネットワークの健全性、アクティビティ、セキュリティについてより多くの情報を得ることができます。

仕様

区分	特徴	メリット
スケールと性能	ユーザー数	100-10000+
	性能	顧客ゲートウェイごとに　1G bps、より多くのゲートウェイを使用したクラウドの水平スケーリング
クラウドプラットフォーム	クラウド管理プラットフォーム	組織のネットワークを簡単に構築できるクラウド管理プラットフォームオンプレミスとクラウドを含む
	迅速で簡単なネットワーク導入	15分以内にネットワークを自動的に導入
	可用性と稼働時間	サービスによって自動的に管理されます。最新の Cloud Edge サービス状況は https://status.sonicwall.com/ で提供されています
	負荷分散	SonicWall がホストおよび管理する世界中の30以上の POP に渡って存在する共有/専用ゲートウェイにより提供される
	サイト間の相互接続	2つのサイト間（オンサイト、オフサイト、またはクラウドベース）の接続。IPsecとWireGuard をサポート
	カスタム DNS	内部 DNS サーバーを使用するために、一度トンネルを定義すると、デフォルトの DNS を使用する代わりにカスタム DNS サーバーを定義することも可能。
	クライアントレスアプリケーションアクセス	HTTP, HTTPS, RDP, VNC, SSH へのゼロトラストアプリケーション
	アクセスクライアントベースアクセス	Windows, Mac, iOS, Android プラットフォームで利用可能
	アプリと環境	ハイブリッド環境やクラウドのワークロードに最適
ゼロトラスト機能	Always-onアプリケーション	Always-onアプリケーションは、信頼されていないネットワークに接続している時にインターネットへの安全なアクセスを提供し、セキュリティの脅威から保護
	ポリシーベースのセグメンテーション	ポリシーは、ユーザーとアプリケーションごとに適用
	詳細なアクセス制御ポリシー	ユーザー、アプリケーション、Geo IP、地理的位置（国）、ブラウザの種類、OS と日時に基づく
	スプリットトンネリング	トラフィックを疎通させるサブネットの指定が可能
	非常停止スイッチ	潜在的なサイバー攻撃を妨害するために、セキュアアクセス接続が中断されると、デバイスのインターネット接続が即座に停止し、デバイスからのデータの流出を防止する
	自動 Wi-Fi セキュリティ	保護されていない公衆無線 LAN に接続した際に、社員のデバイスを自動的に保護する特許取得済みの機能
	DNS フィルタリング	ネットワーク内のユーザーがインターネットブラウザを使用して特定のウェブサイト、サイトカテゴリ、および IP アドレスにアクセスするのを阻止
認証	シングルサインオン機能	Okta、G Suite、Azure AD、Active Directory LDAP などのシングルサインオンプロバイダを介して統一されたログインを導入
	2 要素認証	組込みSMS, DUO Security およびGoogle Authenticator 二要素認証を統合しリモート攻撃を予防
モニタリングとロギング、サポート	24 時間 365 日のサポート	サポート付きのフルマネージドクラウドソリューション
	アクティビティの監査とレポート	ログイン、ゲートウェイの展開とアプリ接続のモニタリング
	SIEM 統合	セキュリティ情報とイベントをリアルタイムで保存・保持し、Splunk との簡単なクリックスルー統合を含むすべてのSIEM アプリケーションに配信
	クラウドサービスの状況	https://www.sonicwall.com/support を確認
相互運用性	エンタープライズファイアウォール	SonicWall、Check Point、Fortinet、Palo Alto Networks、WatchGuard、Sophos Xyxel、UniFi、pfSense、Cisco、Untangle
カスタム統合	API 利用可能	当社の包括的な REST ベースのAPIは、サードパーティの管理、自動化、およびオーケストレーションツールを使用して、迅速かつ簡単な統合を可能にし、新たにプロビジョニングされた、または新たに移転されたアプリケーショの仮想化を確実に保護
コンプライアンス	ISO27001＆27002、SOC-2 type 2	クラウドインフラストラクチャに準拠したSOC-2 type 2
お申込み方法	サブスクリプション制	Cloud Edge Secure Access の定期サービスのお申込みは、MSSP、再販業者、および代理店に連絡してください。

SonicWallについて

SonicWall は、Boundless Cybersecurity を提供することにより誰もがリモートで、モバイルで、危険にさらされながら仕事をするという超分散化時代のビジネスの現実に対処します。未知領域を探求し、リアルタイムの可視性を提供しながら経済の躍進に貢献している SonicWall はサイバーセキュリティの課題を解決して世界中の企業や政府、SMB をサポートします。詳しくは、www.sonicwall.com をご覧ください。

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
その他の情報については当社のウェブサイトをご覧ください。
www.sonicwall.com

Datasheet-CloudEdge-US-VG-2807