eBook

ZTNAが満たすべき10の要件

netskope

目次

はじめに

クラウドの普及、インフラの分散化、リモートワークの拡大により、従来の境界型セキュリティは限界を迎えつつあります。VPNを中心とした従来のアクセス制御では、現代のIT環境に十分対応できないケースが増えています。現在のVPN環境では、アタックサーフェス（攻撃対象領域）の拡大、コスト増大、レイテンシーの増加、アプリケーション性能の可視性不足など、さまざまな課題が顕在化しています。そのため、従来のVPNだけでは十分な対策にならないケースも少なくありません。

クラウドベースでその代替ソリューションとなる「ZTNA（Zero Trust Network Access）」は、現代のセキュリティのニーズを満たしてくれます。ZTNAは、ユーザーのアイデンティティやデバイスのコンテキストを基に、役割に応じたアプリケーションアクセスを制御します。これにより、リスクを最小化し、アタックサーフェスを縮小するとともに、ネットワーク内部でのラテラルムーブメント（横移動）を防止します。VPNとは異なり、ZTNAは信頼性高いブローカーを介してユーザーをアプリケーションに接続し、パブリックインターネットにさらすことなくアクセスを可能にします。SSE（Security Service Edge）ソリューションへのシームレスな統合により、ZTNAはオンプレミス、クラウド、ハイブリッド環境全体で安全かつ柔軟な接続性を確保し、セキュリティとパフォーマンスの両方を強化します。

とはいえ、すべてのZTNAソリューションが同じではありません。優れたZTNAソリューションの要件10項目をここでご紹介します。

基本のおさらい：ZTNAとは？

ZTNAは、ユーザーの役割に基づいてアプリケーションやリソースへのアクセスを最小権限で許可する仕組みです。アクセス許可はユーザーとデバイスのアイデンティティだけでなく、日時、地理的位置、デバイスの状態（デバイスポスチャ）といったコンテキストの評価も通じて制御します。アクセス先の資産の周りに安全な境界を構築して、ネットワークフローを管理します。

デバイスポスチャの変化などが検知された場合でも、ほぼリアルタイムでアクセス権限を取り消すことができます。ZTNAはデフォルトでアクセス拒否をする方式で、例えば特定リソースへはジャストインタイムアクセスを許可するなど、ゼロトラスト原則に則っています。ユーザーは許可されたアプリケーションのみへのアクセス権限が与えられますが、このアクセス権限は常に監視と再評価がされています。この方式は、アタックサーフェスを縮小し、保護対象リソースに近い位置でセキュリティ制御を行うことでリスクを低減することを目的としています。

さらにZTNAであれば、アプリケーションをパブリックインターネットへ直接さらす必要がありません。直接接続する代わりに、信頼性高いブローカーがユーザーとアプリケーション間の接続を仲介します。このブローカーとは、管理型クラウドサービス、データセンター内のセルフホスト型サービス、またはIaaSクラウド内の仮想アプライアンスなどです。

ユーザーの認証情報とデバイスコンテキストの確認後、ブローカーがアプリケーションの近くに位置するアプリコネクタと通信します。

アプリコネクタはその後、プライベートアプリケーションへのセキュアな接続とブローカーへのアウトバウンド通信経路を確立します。

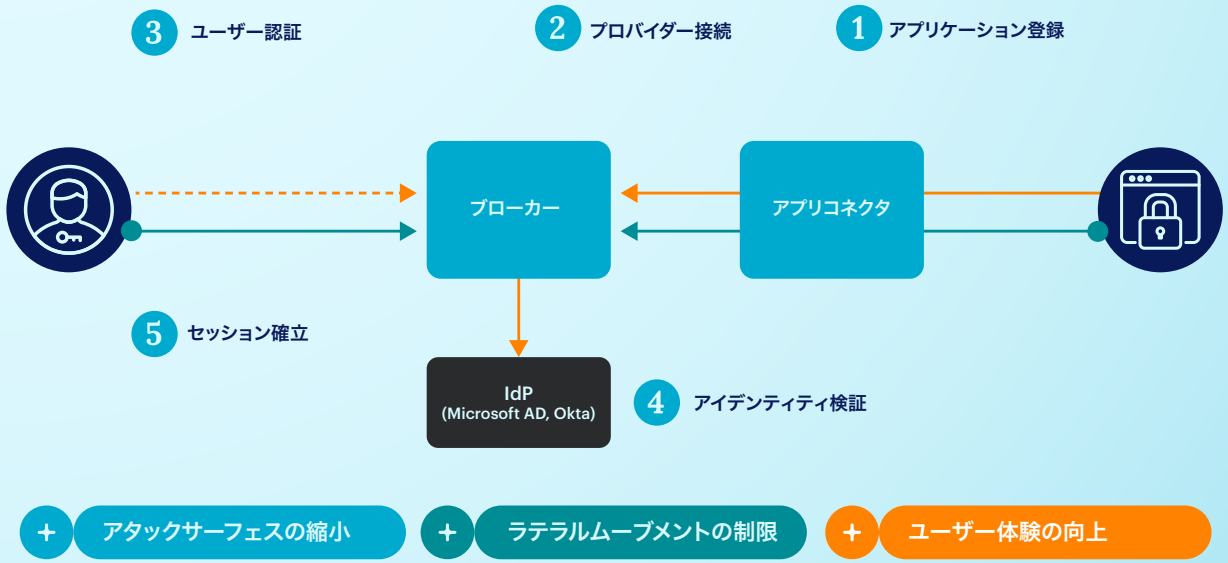


図1：ZTNA（ゼロトラストネットワークアクセス）の仕組み

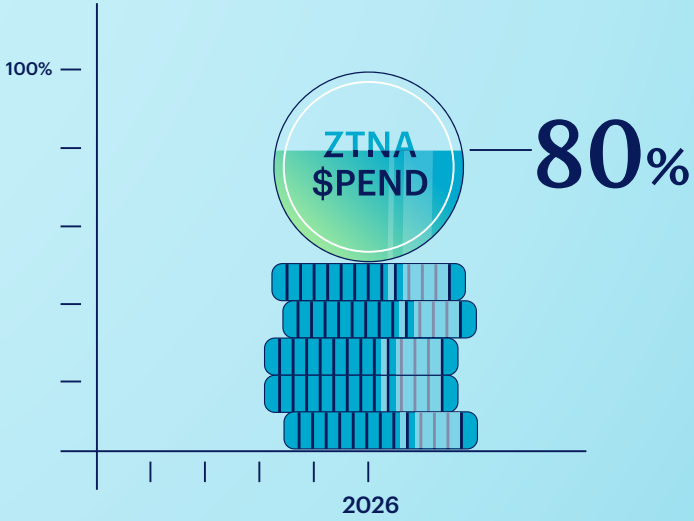
ZTNAのSSEにおける役割と ZTNA統合が顧客にもたらすメリット

SSEは、ZTNA、SWG（Secure Web Gateway）、CASB（Cloud Access Security Broker）、DLP（Data Loss Prevention）などの主要なセキュリティサービスをクラウドから提供する統合プラットフォームです。

SSEの中核となるZTNAは、アプリケーションやサービスへの安全かつ詳細な条件付きアクセスを実現します。オンプレミスとクラウドベースの両方のリソースに対するアクセスの制御と認証を管理します。またZTNAは、ユーザーの行動、デバイスの健全性、位置情報、その他のリスク指標に基づくコンテキストベースのアダプティブアクセス制御を適用し、SSEフレームワーク内すべてのセキュリティサービスに一貫した保護を確実にします。Gartner社の調査によると、ZTNA関連支出の80%は、より広範なSASE、管理型SASE、またはSSEの購入の一部として2026年までに発生すると予測されています。これは2022年と比較して40%の増加です。[1]

SSEはZTNAから得られるリアルタイムデータを活用し、セキュリティレベルを動的に調整します。例えば、デバイスが侵害された場合、SSEは自動的にアクセス制御を変更し、DLPなどのサービスを追加適用して、データ漏洩や不正アクセスを防止します。

SSE内でZTNAを活用することで、セキュリティを強化しながらユーザーエクスペリエンスを向上させることができます。さらに、管理の簡素化や拡張性の向上も実現できます。このようにZTNAをSSEと統合することで、企業はゼロトラストセキュリティモデルを導入し、自社リソースを保護しながら進化する脅威に対応できるようになります。



> Gartner社の調査によると、ZTNA関連支出の80%は、より広範なSASE、管理型SASE、またはSSEの購入の一部として2026年までに発生すると予測されています。これは2022年と比較して40%の増加です。[1]

[1] Gartner社「Competitive Behaviors in the ZTNA Platform Market,」、Evan Zeng, Charanpal Bhogal著、2024年8月12日

1 | アイデンティティに基づく最小権限認証

01

認証はセキュリティの基本的な仕組みの一つです。しかし、静的な認証だけではセキュリティのギャップを生み、コンプライアンス上の問題やユーザーの不満、さらには組織全体のセキュリティ低下につながる可能性があります。

認証情報の侵害は一般的な脅威の一つです。従来型セキュリティでは、すべてのユーザーに一律の保護を適用することが多く、高リスク状況では脆弱性を、低リスク状況では不要な制限を生むことがあります。認証は極めて重要ですが、その価値を最大化するには柔軟性とコンテキスト認識が不可欠です。適切なアダプティブ認証が導入されていない場合、コンテキストに基づくリアルタイムの対応が困難となり、セキュリティ侵害、アカウント侵害、インサイダー脅威のリスクが高まります。

アイデンティティベースの最小権限認証は、動的かつコンテキスト認識型のアプローチを認証に適用して、これらの課題を解決します。セキュリティレベルは、ユーザーのログイン試行におけるリスク評価に基づいて調整されます。ZTNAソリューションにおいては、この仕組みにより各アクセス要求のリスクを継続的に評価し、リスクに応じた認証要件を課すことでセキュリティを強化します。リアルタイムでのリスク評価にアクセス制御を統合したこのアプローチは、強固なゼロトラストセキュリティを実現します。

ZTNAでアイデンティティベースの最小権限の原則を実装するには、セキュリティポリシーの定義、多要素認証（MFA）の統合、およびコンテキストに応じたリスク評価の設定が必要です。ZTNAには、アイデンティティベースの最小権限認証が必須で、アクセス許可はユーザーのアイデンティティとアクセスコンテキストに基づいて、必要なときに必要なアクセスのみを許可します。これにより、リスクを最小化し、アタックサーフェスを縮小しながらセキュリティを強化します。

NETSKOPEのソリューション

Netskope One Private Accessがアイデンティティベースのアクセス制御を厳格に行い、ユーザーが必要な権限のみを付与します。また管理対象デバイス（エージェントベース）と非管理対象デバイス（エージェントレス）の両方をサポートします。

2 | デバイスポスチャの総合評価

02

デバイスの状態管理が不十分な場合、サイバー攻撃、データ侵害、コンプライアンス違反のリスクが著しく高まり、セキュリティ運用が非効率になりかねません。

リモートワークとBYOD（Bring Your Own Device）の普及に伴い、デバイスポスチャ（デバイスの状態）の管理の重要性がますます高まっています。セキュリティ基準を継続的に監視し適用しなければ、組織は十分に保護されていないデバイスからの脅威にさらされる可能性があります。デバイスポスチャ管理は、管理対象か否かを問わずあらゆるデバイスが、機密リソースにアクセスする前にセキュリティポリシーを満たしていることを確認します。

ZTNAでは、デバイスポスチャ管理機能がネットワーク上のリソースへのアクセスを許可する前に、デバイスのコンプライアンスを検証します。アクセス許可前にデバイスの健全性とコンテキストを動的に評価することで、安全なデバイスのみが重要なデータにアクセスを許される仕組みになっています。このアプローチはリスクを低減し、ネットワーク全体のセキュリティを強化します。

あらゆるZTNAソリューションに必須の機能であるデバイスポスチャ管理が、ゼロトラストの原則に基づきながらセキュリティ、コンプライアンス、脅威の軽減、インシデント対応を支援します。例えば、会社の資格情報が入ったデバイスが盗難に遭った場合、ポスチャチェックによりコンプライアンス違反を検知し、アクセス試行時にアラートを発生させることができます。

安全なデバイスのみがネットワークにアクセスできることを確実にすることで、組織は強固なゼロトラストセキュリティ体制を維持できるのです。

NETSKOPEのソリューション

Netskope One Private Accessは、管理端末と非管理端末両方についてデバイス健全性とコンプライアンスを継続的に評価することで、アクセス許可前のリアルタイムリスク評価を行っています。

3 | アイデンティティベースのポリシーによる高度なマイクロセグメンテーション

03

従来のネットワークセキュリティモデルやセグメンテーション手法では、現代のIT環境の複雑さに対応しきれず、しばしばリスクと脆弱性の増加につながることがあります。

高度なセキュリティ対策が不足している組織は、データ漏洩、不正アクセス、非効率的なネットワークリソース利用などのリスクが高まり、機密データの保護、規制コンプライアンス、進化する脅威への防御が困難になります。アイデンティティベースのポリシーによる高度なマイクロセグメンテーションは、ネットワークアクセスを正確に制御し、ユーザーアイデンティティ、デバイスポスチャ、アプリケーションのコンテキストに基づいてセキュリティを実行し、これらのリスクや課題に対応します。

このアプローチでは、ネットワークを安全なマイクロセグメントに分割し、ユーザーアイデンティティとコンテキスト要因に基づいて各セグメントへのアクセスを制御します。最小権限の原則を遵守し、ユーザー、デバイス、アプリケーションに対して動的できめ細かなアクセス制御を適用することで、セキュリティを強化します。これによりラテラルムーブメントを防止し、信頼の過剰付与を抑制し、コンプライアンスを維持しながら第三者リスクを低減できます。また、ハイブリッド環境やマルチクラウド環境の保護にも有効です。

ZTNAと組み合わせることで、マイクロセグメンテーションはゼロトラストアーキテクチャの重要な構成要素となります。ZTNAがネットワーク境界でアイデンティティを検証する一方、マイクロセグメンテーションはネットワーク内部での相互作用を制御します。アクセス許可後もユーザーの行動をアイデンティティや役割に基づいて制限することで、より強固なセキュリティを実現します。

高度なマイクロセグメンテーションの実装には、複数技術の組み合わせ、ベストプラクティス、そして継続的な管理が求められます。組織がZTNAソリューションでこれを最大限に活用するには、アイデンティティベースのアクセス制御、継続的監視、自動化、定期的なポリシー更新を統合し、セグメンテーションを安全に保つとともに、ユーザーとデバイスのアイデンティティに基づく動的ポリシーを適用する必要があります。

NETSKOPEのソリューション

Netskope One Private Accessは、アイデンティティベースのポリシーを適用し、そのなかでアクセス制限の対象をネットワーク全体ではなく特定のアプリケーションに限定します。

4 | ユニバーサルZTNA

04

従来のZTNAソリューションは、Webアプリケーションやクラウドアプリケーションへのアクセスを中心に設計されていることが多く、レガシーシステム、非Webアプリケーション、管理対象外のデバイスに対するセキュリティ対策が不十分な場合があります。その結果、オンプレミス、クラウド、ハイブリッド環境全体でアクセス制御が統一されず、ユーザーエクスペリエンスが低下します。

ZTNAソリューションは、レガシーアプリケーションの課題にも対応する必要があります。というのも、これらのアプリケーションは往々にして時代遅れのVPN技術に依存しており、セキュリティリスクを高め、ユーザーエクスペリエンスを低下させているからです。多くのZTNAソリューションは、レガシーまたはオンプレミスアプリケーションのトラフィックを集中型VPNゲートウェイ経由でルーティングしています。すると、ボトルネックやレイテンシーを引き起こし、直接的なアイデンティティベースのアクセスというZTNAの利点が十分に活かされません。さらに、ゼロトラスト原則の適用に(特にレガシーシステムにおいて)ばらつきが生じ、組織がセキュリティ上の脆弱性にさらされてしまいます。

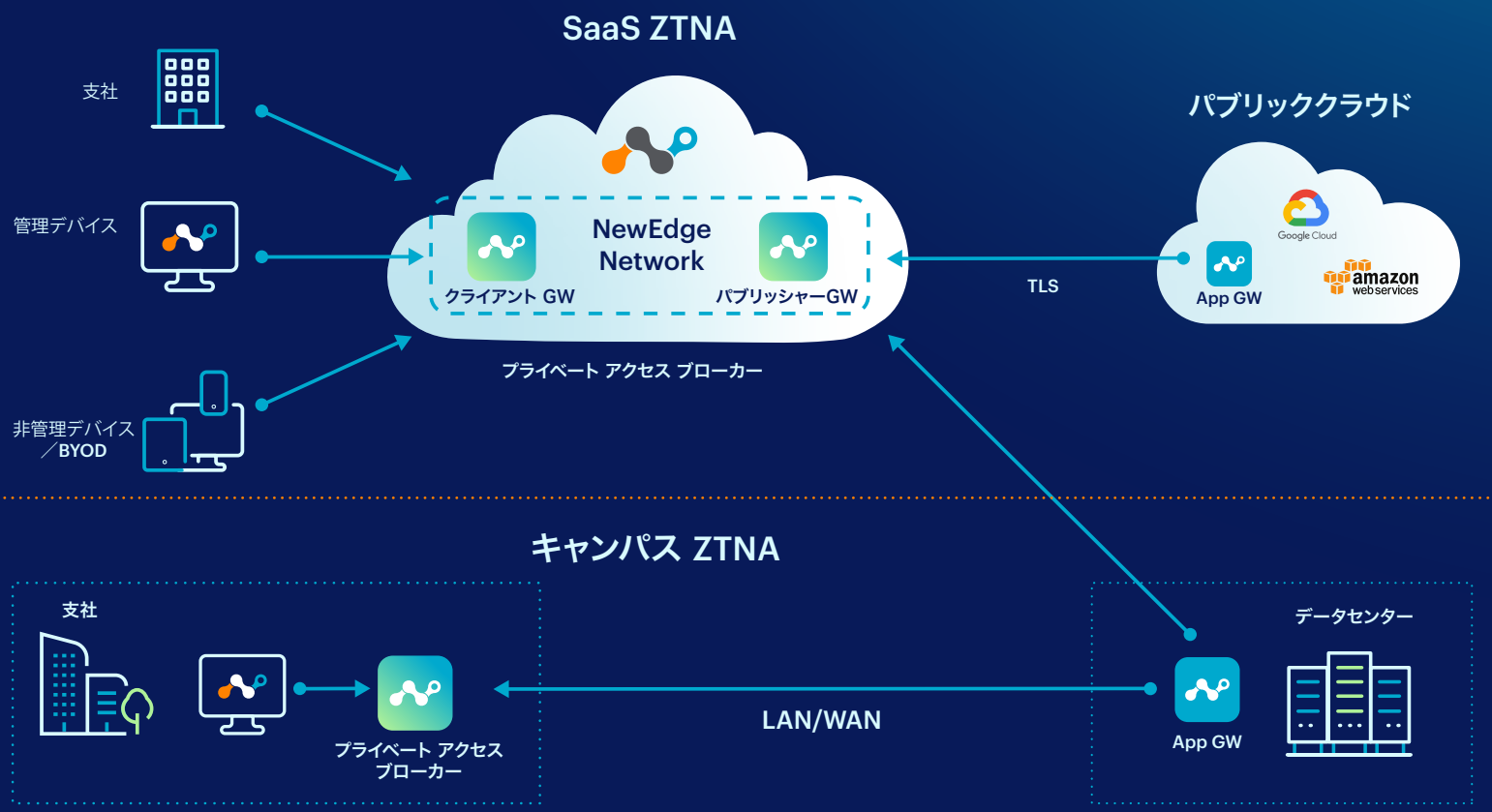
これらの課題解決の鍵をにぎるのがユニバーサルZTNAで、レガシー、最新的、クラウド、オンプレミスなどの属性を問わずあらゆる種類のリソースに対し、ユーザーの場所やデバイスにも関係なく、安全なアクセスを提供します。ユニバーサルZTNAを導入することで、企業はすべてのアプリケーションアクセスを一元管理できるようになり、環境全体で統一されたセキュリティポリシーを維持できます。ゼロトラスト原則の一貫した適用により包括的かつ確実な保護をし、ユーザー活動の完全な可視化やアクセス管理の簡素化も可能になります。このアプローチは、ユーザーにとってはストレスフリーでシームレスなアクセス、管理者とっては環境全体で統一されたポリシーの適用、管理の簡素化、効率よい監視・監査というメリットをもたらします。

NETSKOPEのソリューション

Netskope One Private Accessは、高度なZTNAとコアとなるNAC機能を統合し、リモート環境、キャンパス内、支社拠点、さらにはサードパーティのユーザーに至るまで、あらゆる環境において最小権限アクセスを一貫して適用します。

Netskope One Private Accessのユニバーサル ZTNA

Netskope One Private Accessは、オフィス、自宅、外出先など、ユーザーの場所に関係なくプライベートアプリケーションへの安全なアクセスを提供します。ゼロトラストの原則に基づき、認証、アクセス許可、リスクベースの制御を一貫して適用することで、ラテラルムーブメントのリスクを低減しながら、導入と運用の簡素化を実現します。また、インテリジェントなトラフィック制御によりパフォーマンスを最適化するとともに、統合クライアントによってZTNAとVPN機能を一つのプラットフォームで利用できます。単一のポリシーエンジンが、オンプレミスとリモート両方のユーザーに対してきめ細かなアクセス制御を適用しながら、リスクスコアに基づいてリアルタイムにポリシーを更新します。



5 | レガシーアプリケーションへの対応

05

ZTNAがレガシーアプリケーションに対応していないことで、インフラの最新化とクラウドサービスへの移行が妨げられてしまいます。

包括的なセキュリティ、運用の効率化、そして最新化されたインフラへの円滑な移行を実現するためにも、ZTNAソリューションはレガシーアプリケーションに対応していなければなりません。

機密データや重要なプロセスを扱う業務上不可欠な機能について、依然としてレガシーアプリケーションに依存している企業は少なくありません。リモートデスクトッププロトコル（RDP）、SAPやOracleなどのオンプレミスERPシステム、産業用IoTシステム、VoIPプラットフォームなどがその例です。これらの古いシステムは、クラウドコンピューティングや現代的なセキュリティプロトコルの多くが広く普及する前に構築されており、そのコスト、複雑さ、あるいは技術的な依存関係から更新やアップグレードが困難なケースも少なくありません。

ZTNAがレガシーアプリケーションに対応していない場合、VPNなど従来型のアクセス方法に依存せざるを得ず、結果、脆弱性が増し、セキュリティのギャップが生じ、ゼロトラストモデルが弱体化してしまいます。集中型VPNアクセスも、特にリモートユーザーにとってネットワークのボトルネックやレイテンシーが生じ、業務の効率や生産性の低下につながります。

さらに、最新アプリケーションとレガシーアプリケーションでアクセス方法が異なると、セキュリティ管理が複雑化し、運用コストの増加やポリシー適用の不整合を招く可能性があります。レガシーアプリケーションに対応するZTNAソリューションでは、すべての環境で一貫したセキュリティポリシーを適用できるため、管理が簡素になり、ITの最新化の過程でも重要な業務を中断することなく維持できます。これにより、組織は強固なセキュリティと運用の継続性を確保しながら、新しいシステムへ段階的に移行できます。

NETSKOPEのソリューション

Netskope One Private Accessは 、ZTNAにSD-WAN機能をもたらし、すべてのプライベートアプリケーションへの安全で最適化された接続を実現します。これにより、組織はリモートアクセスVPNソリューションを完全に置き換えるとともに、ハイブリッドワーク環境にのコネクティビティを最新化できます。

6 | ユーザーとアプリケーションに近い位置でのセキュリティ制御

06

ZTNAにおいて、ユーザーやアプリケーションの近くにセキュリティ制御が配置されていない場合、レイテンシーやボトルネックを生じ、ゼロトラストの適用が弱まります。その結果、ユーザーエクスペリエンスが低下し、セキュリティの脆弱性が生じます。

セキュリティ制御を1カ所に集約すると、特にリモートユーザーにとってクラウドアプリケーションのパフォーマンスが低下、レイテンシーが増大、さらにセキュリティがより脆弱になる可能性があります。分散型のセキュリティが導入されていない場合、トラフィックは中央のゲートウェイを経由することになり、アクセスの遅延やポリシー適用の複雑化を招きます。

ZTNAソリューションでは、ユーザーとアプリケーションの接続ポイントでセキュリティ制御をすることが重要で、これにより広範なネットワークを露出させることなくアプリケーションごとのポリシーを確実に適用できます。このアプローチは、ユーザー数やサービス需要の増加にともなう拡張性を高めます。同時に、アイデンティティやデバイスの状態といった要素に基づいて、リアルタイムでアクセス許可の判断ができます。レイテンシーを低減しパフォーマンスを向上させる戦略の例には、オンプレミス環境へのローカルブローカーの配置、主要拠点へのZTNAゲートウェイの設置、クラウドへのセキュリティ制御の組み込み、およびZTNAとSSEの統合などがあります。さらに、エッジコンピューティングやローカルなPoP（Point of Presence）を活用することで、パフォーマンスとコンプライアンスの最適化を図ることができます。

主要なZTNAベンダー各社は、これらの課題解決のためにグローバルにPoPを展開し、レイテンシーに影響を受けやすい要求や地域ごとのコンプライアンス要件に対応しています。

NETSKOPEのソリューション

Netskope One Private Accessは、ローカルまたはクラウド上に配置されたブローカーを通じてポリシーを適用します。このブローカーはユーザーの近くに配置されており、アプリケーションへの迅速な接続を可能にすることで、レイテンシー低減とパフォーマンス向上を両立しています。

7 | より広範なセキュリティエコシステムとの統合

07

ZTNAイベントが、ネットワーク全体の通信状況やエンドポイントの挙動に関連付けられていない場合、セキュリティチームは侵害の初期兆候を見逃してしまう可能性があり、攻撃者がネットワーク内で活動を拡大したり、データを窃取したりする時間の余裕を与えてしまいます。この検知の遅れが、侵害リスクと被害の拡大を著しく増加させてしまいます。

ZTNAを他のIT、セキュリティ、ネットワークシステムとシームレスに統合することで、セキュリティを強化し、運用を効率化するとともに、ユーザーエクスペリエンスの向上を実現できます。主要な統合対象には、IAM（SSOとMFA）、EDR（Endpoint Detection and Response）、SIEM、CASB、SD-WAN、VPN、従来型ファイアウォール、脅威インテリジェンス、アプリケーションやクラウドインフラ関連ツールなどがあります。

SIEMやログ管理システムなどの広範な監視ツールをZTNAと統合することは、ZTNAトラフィックとユーザー行動を包括的に可視化するために不可欠です。これらを統合しなければ、セキュリティチームは異常なアクセスパターンや脅威を見逃す恐れがあり、侵害リスクが高まります。ZTNAをネットワークセキュリティ、エンドポイント保護などの他のシステムと統合することで、セキュリティチームはイベントの関連性をより効率的に把握できるため、インシデントの検知や対応までの時間を短縮できます。また、IAMやSSOを統合することで、ユーザーアイデンティティとアクセスの管理も簡素化できます。

このような統合により、ZTNAはその効率性や拡張性を高め、現代のビジネスニーズに迅速に対応できるようになり、セキュリティ、柔軟性、ユーザーエクスペリエンスのすべてが改善できます。

NETSKOPEのソリューション

Netskope One SASEの一部として、CASB、SWG、DLPを統合、さらにはセキュリティ、ID管理、ITSM、モバイル、セキュリティ運用分野の主要パートナーとも連携し、一貫したポリシー適用、リアルタイムの脅威防御、データとアプリケーション全体にわたる可視性を実現します。

8 | ネットワーク全体の可視化と分析

08

ネットワーク全体の可視化が不十分な場合、セキュリティ上の死角、コンプライアンス問題、非効率性が生じ、組織のゼロトラストセキュリティ体制が弱体化し、潜在的な脅威に対する脆弱性が増大します。

ZTNAフレームワークにおいて、ネットワーク全体を可視化し分析し続けることは、組織をセキュリティリスクから保護するうえで不可欠です。これが実現できていない場合、ゼロトラストの適用が十分に機能せず、内部脅威の検出が困難になるほか、BYODやリモートワークのリスク管理に課題が生じます。

すべてのネットワークトラフィックをリアルタイムで監視することで、異常な挙動やセキュリティ侵害、進化する脅威の早期検知が可能になります。包括的なネットワーク可視化により、セキュリティチームはラテラルムーブメントや悪意のある行動を特定し、高度な検知アルゴリズムを活用できます。さらに、ネットワーク分析と機械学習により、さらなる検知精度の向上、コンプライアンスの強化、パフォーマンスの最適化にもつながります。

継続的な監視、リアルタイム分析、動的なポリシー適用は、進化する脅威に対応するための鍵であり、ZTNAソリューションには不可欠です。これを実現するためには、監視ツール、行動分析、アクセス制御を導入し、SIEM、CASB、脅威インテリジェンスなどの既存のセキュリティ基盤と統合する必要があります。

NETSKOPEのソリューション

Netskope One DEMは、ユーザーからアプリケーションに至るまでのデジタルエクスペリエンスを360度あらゆる角度から可視化します。ユーザースコア、デバイスの健全性、ローカル接続（Wi-Fi）、SD-WAN OnRamp、SSEサービスなど、あらゆる要素をカバーします。

9 | 拡張性と俊敏性の確保

09

組織の成長やリモートアクセスの需要増加に伴い、十分な拡張性を備えたZTNAソリューションがない場合、ユーザー数が限定され、接続が妨げられ、クラウドアプリケーションへのアクセスにも制約が生じる可能性があります。その結果、組織のセキュリティや運用効率が低下する恐れがあります。

今日の組織の多くは、オンプレミスのインフラ、パブリッククラウドとプライベートクラウド、そしてさまざまなSaaSアプリケーションが混在する環境で運用が行われています。環境ごとに個別のセキュリティソリューションを管理していては、管理が複雑でコストもかかり、ポリシーの不整合を招く原因にもなります。ZTNAは、すべての環境におけるユーザーアクセスを統一的に可視化・制御することで、管理をシンプルにし、セキュリティを強化します。

オンプレミスとクラウドの両方にアプリケーションやデータが存在するハイブリッド環境において、ZTNAソリューションは一貫したセキュリティポリシーを適用し、変化するワークロードにも柔軟に対応する必要があります。ユーザの一増加や新規アプリケーションにあわせた拡張には、クラウドネイティブなZTNAソリューションが重要であり、これにより物理的なインフラ変更を加えずに柔軟なスケール拡張が可能になります。

さらにZTNAは、クラウドプラットフォームと連携するためのAPIやSDKを提供し、制御と可視性を高める必要があります。多様な環境をまたがってリソースを効果的に管理するために、ZTNAには統一されたセキュリティポリシー、適応型のアクセス制御、シームレスなユーザー体験、および各種システムとの統合機能が不可欠です。堅牢なZTNAソリューションは、クラウドネイティブなインフラ、自動プロビジョニング、適応型ポリシーを活用して拡張性とパフォーマンスを確保しており、ユーザー増加、新規のアプリケーション導入、新たな脅威など変化し続ける要求にも対応可能です。これらの機能は、今日のダイナミックなIT環境において、セキュリティと俊敏性の両方を実現するために不可欠です。

NETSKOPEのソリューション

Netskope NewEdge Networkはクラウドネイティブでスケーラブルなアーキテクチャ、そしてグローバルな展開力を備えます。この基盤により、シームレスな拡張、迅速な導入、そしてリモートワーク環境における安全なアクセスを実現します。

10 | 効果的な管理ツール

10

従来のZTNAソリューションには強力な管理ツールが不足しています。そのため、きめ細かなアクセス制御、インシデントの迅速な対応、組織のセキュリティ体制の継続的な強化の面で、セキュリティチームの対応能力の足かせとなっていました。

ZTNAソリューションの管理インターフェースが非効率な場合、管理が複雑化し、監視が断片化し、インシデント対応の遅延を招いてしまいます。また、セキュリティログへのアクセスに遅延があったり、ポリシー管理が煩雑だったりすると、組織全体でポリシーの適用にばらつきが生じるおそれがあります。

ZTNAにおける管理の利便性を最適化するためには、エンドユーザーと管理者の双方にとって使いやすい仕組みを整えることが重要です。ユーザー、デバイス、アプリケーション、ポリシーを一元管理できるコンソールにより、監視、設定、トラブルシューティングを簡素化し、セキュリティポリシーの一貫した適用やスムーズな導入が可能になります。

最小権限モデルを導入することで、役割や条件に基づいてリソースへのアクセスを制限でき、管理をさらに効率化できます。また、ポリシーの導入や監査がよりシンプルに行えるようになります。また、自動検出、分析、およびトラブルシューティングのツールがこのプロセスを強化します。加えて、ポリシーテンプレート、自動化、詳細なダッシュボードを活用することで、ZTNA環境におけるセキュリティと運用の双方を大幅に効率化できます。

NETSKOPEのソリューション

Netskope One Private Accessは、ユーザー、デバイス、ポリシーを一元管理できるコンソールを提供し、環境全体にわたって一貫したセキュリティポリシーの適用と監査を実現します。

ハイブリッドワークの拡大、さらにクラウドやSaaSアプリケーションの導入により現代の企業が変容し、どこから、どのようにして、どのリソースへアクセスすべきかが変わってきました。

クラウドサービスへの移行と、分散した環境でのリモートワーク導入が進むにつれ、企業にとってこれまで以上に拡張性と柔軟性が高く、同時に安全なソリューションの必要性が高まっています。最新のZTNAソリューションは、適応性が高くセキュアなアクセスを提供することで、こうしたニーズに対応し、今日のデジタル環境において進化しつづけるセキュリティ課題の解決を支援します。

Netskope One Private Accessの
トライアルで実際にご体験ください。

トライアルはこちら

Netskope Oneプラットフォーム

Netskope One SSEの基盤となるNetskope Oneプラットフォーム。本プラットフォームは、場所とデバイスを問わず、クラウドサービス、Webサイト、プライベートアプリケーションへのアクセスにおける、類のない可視性、リアルタイムのデータ、さらに脅威からの保護を実現します。

Netskopeについて

SASEのグローバルリーダーであるNetskopeは、企業におけるゼロトラストの原則とAI／機械学習のイノベーションを活用し、企業のデータ保護とサイバー脅威からの防御を支援します。Netskope Oneプラットフォームと特許取得済みのZero Trust Engineは高速かつ簡単に利用でき、ユーザー、デバイス、データの場所を問わず最適化されたアクセスとリアルタイムのセキュリティを提供します。NetskopeとそのパワフルなnewEdge Networkは数千もの顧客企業から信頼されています。あらゆるクラウド、Web、プライベートアプリケーションの活動に対して比類のない高い可視性とリスク低減を達成しており、妥協しないセキュリティ確保とパフォーマンス向上を両立します。詳しくはnetskope.com/jpをご覧ください。

さらにご興味をお持ちですか？

デモをリクエストする

netskope