CISOのプレイブック

ユニバーサルZTNAでネットワークセキュリティの課題　トップ４を克服する方法

appgate

要旨

高度なデジタル環境と変容するサイバー脅威は、CISOとそのチームにかつてない課題を突きつけています。セキュリティの目的がビジネスの目標と衝突することが多い中、「簡単なボタン」を押さなければならないという絶え間ないプレッシャーと、適切なバランスを見つけることは至難の業です。

間違いなく、CISOは戦略的なビジネスリーダーとして、イノベーションとデジタルトランスフォーメーションを妨げることなく、複雑なハイブリッドネットワークとコアリソースを保護することを任されています。このようなシフトが起きているのは、リスクを軽減することがもはやデータやシステムの安全性だけでなく、組織のブランド、財務的安定性、市場での地位を守ることだからです。

CISOがコントロールできないビジネス面が多い中、影響力が鍵となります。主要な利害関係者と関係を築き、サイバーセキュリティ計画をビジネスストーリーに組み込むことが重要です。CISO として、以下の質問を検討してください：何が分かっているのか？何を知りたいか？何を理解していないのか？ビジネスの俊敏性を実現するセキュリティ戦略によってリスクとギャップを最小化することは、信頼を構築し、インパクトのある変化をもたらすために不可欠です。

CISOは、セキュリティ目標と企業の願望を両立させるために、即効性のある解決策がないことを知っています。では、決して簡単にはいかないのであれば、せめてもっと簡単にできないものでしょうか。

多くのCISOは、ユニバーサル・ゼロ・トラスト・ネットワーク・アクセス（ZTNA）を礎石とするゼロ・トラスト・セキュリティのフレームワークで、この質問に肯定的に答えています。このアプローチでは、過剰な特権ユーザー・アクセスを排除し、攻撃面を最小化し、ネットワークを遮蔽し、ハイブリッド環境全体でエンドツーエンドの監視と可視化を優先します。そして、適切なZTNAソリューションは、運用上の大きなメリットと運営費用の節約をもたらします。結局のところ、ビジネスを可能にし、収益に貢献しながら、サイバーの複雑さを克服することが、今日のデジタル世界におけるCISOの成功の新たな特徴なのです。

目次

ビジネスイネーブラーとしてのCISO: 権限、所有権、説明責任

近年、CISO の役割は、コスト・センター・マネージャーから、ビジネスの成長を促進する戦略的パートナーへと進化しています。この変化は、サイバーセキュリティが単なる防御手段ではなく、イノベーション、俊敏性、競争優位性を実現する重要な手段であるという事実を浮き彫りにしています。

しかし、CISO は依然として予算や権限の制約に直面することが多く、そのため経営幹部 の同僚や取締役会との信頼関係を築き、影響力を行使することが重要になります。業務上のニーズ、イノベーション、時間的制約、その他のビジネス上の優先事項のバランスを取る方法を知ることは、強力な交渉術となります。

CISOの権限は組織によって異なります。通常、CISO は、一定の閾値までのサイバーセキュリティ・リスクの評価と受け入れ、セキュリティ・ポリシーの設定と実施、リソースの割り当て、サイバーセキュリティ予算と優先事項の調整を行うことができます。リスク評価を主導し、脅威緩和戦略を策定し、従業員に対するセキュリティ期待とトレーニングを確立します。また、CISO には、セキュリティ・インシデントを防止するためのギャップを特定し、対処する任務があります。侵害が発生した場合は、インシデント対応と復旧作業を指揮し、レジリエンスを構築します。

CISOの影響力と権限が大きくなるにつれて、ビジネスに対する説明責任も大きくなります。そのためには、ITとサイバーセキュリティの市場、規制の状況、競争圧力などを理解する必要があります。CISO は、セキュリティの有効性とビジネスへの影響を測定するための主要業績評価指標を確立する必要があります。また、サイバーセキュリティ投資の ROI（投資収益率）を伝える能力も重要であり、サイバーセキュリティ投資がどのようにビジネスの実現を支援し、運用コストを削減できるかを強調する必要があります。

サイバー・イニシアチブをより広範なビジネス目標に整合させることは極めて重要です。CISO はリスクの軽減を超越し、ビジネスのニーズを理解し、全体的な成功を促進し、万一侵害が発生した場合の影響を最小限に抑えるセキュリティ戦略を活用することによって、戦略的目標に積極的に貢献しなければなりません。

ユニバーサルZTNAは、リスクを管理し、複雑さを軽減し、コンプライアンスに対応し、ビジネスへのROIを証明するための強力なフレームワークとして登場しました。ゼロ・トラスト・アプローチを採用することで、CISOは暗黙の信頼を排除し、組織全体のすべてのユーザー、デバイス、アプリケーションの継続的な認証と認可を確保します。このきめ細かな管理により、不正アクセスや横移動のリスクが大幅に低減されるため、企業と連邦政府機関の両方で全体的なセキュリティ態勢が強化されます。

また、ベスト・オブ・ブリードのユニバーサルZTNAは、IAM、AV、SIEM、SOAR、EDR、XDR、SWG、CASB、DLPなどの異種ソリューションのアルファベットスープを統一プラットフォームに統合するAPIリッチ機能により、コストのかかるリッピング＆リプレースシナリオを最小限に抑えることができます。この合理化されたアプローチにより、複雑さが軽減され、可視性が向上し、より効果的な脅威の特定と対応が可能になります。さらに、ZTNAのきめ細かなアクセス制御と詳細な監査証跡は、企業が厳しいコンプライアンス要件を満たすのに役立ちます。

> CISO は、セキュリティの有効性とビジネスへの影響を測定するための主要指標を確立しなければなりません。

ネットワーク セキュリティの課題 トップ4

#1 複雑性への挑戦

現代のネットワークは、クラウドからエッジ、そしてその間のあらゆる場所にリソースが散在する、広大なエコシステムです。この複雑さは、CISOやセキュリティ・チームにとって大きな課題であり、複雑なネットワーク・トポロジー全体に死角や脆弱性を生み出しています。エンドポイントの急増、クラウドの採用、遅れているレガシーの統合の必要性により、攻撃対象が拡大し、セキュリティ体制を強化することがますます難しくなっています。さらに、組織再編、従業員の入れ替わり、合併買収、デジタルトランスフォーメーション・イニシアチブのような変化が、この複雑さに拍車をかけています。

#2 安全でないVPNの課題

インターネットに面したVPNのような伝統的なセキュリティ・ソリューションは、安全でないオープン・ポートのために、脅威行為者の人気のターゲットとなっています。では、セキュリティ・アプライアンスが攻撃のベクトルになってしまったらどうなるのでしょう?サイバーセキュリティ101：CISOは、セキュリティ・アプライアンスが攻撃経路にならないようにしなければなりません。

公開されたCVEやVPNのゼロデイ・エクスプロイトがサイバー業界のヘッドラインを飾ることはよくあることで、最近ではIvantiの複数のセキュリティ欠陥に関する数カ月に及ぶ報道が記憶に新しいでしょう。これらのCVEは、VPNの弱点と露出したインフラの危険性を思い起こさせるものです。

しかし、VPNベンダーがパッチを発行できるようにエクスプロイトが発見されるのを待つのが答えではありません。持続的なVPNの悪用は、ある傾向を浮き彫りにする警鐘です。敵が使用する高度な持続的脅威の手口は、エンドポイントを標的とするものから、露出したインフラを標的とするものへと変化しています。なぜなら、ほとんどの組織は、敵対者、特に莫大なリソースを使用する国家に支援された敵対者ほど迅速には対応できないからです。

ネットワークセキュリティの課題トップ4

#3 レガシーシステムのセキュリティ確保という課題

技術革新は、顧客、規制、従業員、パートナー、競争相手など、需要に応じて行われます。バックオフィス機能、ネットワークインフラストラクチャ、データベース、その他の機能で、あまり動的でなかったり、ユーザーと対面していなかったりするものは、それが必須となるまで近代化が遅れる傾向があります。

レガシーシステムの技術的負債によって生じるセキュリティギャップは、CISOにとって継続的な懸念事項です。ネットワーク・デバイスは、インフラやすべての王冠につながる経路であるため、特に魅力的なターゲットです。これらの容易に悪用可能なインターネットに面したリソースは、修復、パッチ適用、アップデートの負担でセキュリティ・チームを忙しくさせています。パッチやアップデートのたびに、システムが正常に動作し続けることを確認するための大規模なテストが必要になることは言うまでもありません。

#4 露出したインフラ・コンポーネントへの攻撃戦術の転換という課題

CISOの優先課題は、サイバー攻撃のトレンドを先取りし、防御の脆弱性を迅速に特定することであることは間違いありません。サイバーニュースをざっとスキャンしてみると、ハッカーがエンドポイントを標的にすることから、露出したインフラ・コンポーネントを標的にすることへとシフトしていることがわかります。このシフトにはいくつかの要因があります：

攻撃対象の拡大：インターネットに面したインフラ・コンポーネントは、膨大かつ急速に拡大する攻撃対象となります。また、リース機能（SaaSなど）の採用も、攻撃対象領域を変化させ、組織のコントロールから外すことになります。

脆弱性の露出：パッチチューズデー、メジャーアップデート、CISAアドバイザリーのたびに、CISOの「やるべきこと」リストが追加されます。サーバーやその他のエンドユーザー以外のデバイスにパッチを適用するのは、困難で時間がかかるため、遅れがちです。このため、組織の重要なバックエンド業務システムは、影響を受けやすい魅力的な標的となってしまいます。

効率性と費用対効果：攻撃者がインフラを標的にするのは、フィッシングよりも迅速かつ容易な侵入方法だからです。インターネットに接続されたシステムの脆弱性を利用することは容易であり、攻撃者はユーザーや電子メールによる防御を効率的かつコスト効率よく回避し、そのままデータ侵害に移行することができます。

ユニバーサルZTNAのケーススタディ:
レガシーネットワークデバイスの保護

ユニバーサルZTNAは、ネットワーク・セキュリティの焦点を、静的な境界から、ユーザーからリソース、リソースからリソースへの各接続を保護する「1つのセグメント」に変更します。これにより、レガシー・ネットワーク・デバイスへのアクセスを保護するという問題がテーブルから取り除かれます。例を挙げましょう。

AppgateのFortune 50の顧客の1社は、Appgate SDPを使用して、18,000台以上のサーバの99%（約12億ポート相当）をクローキングしています。残りの1%未満は、シフトがノイズに紛れないようにするプロトコルを介して、ポートステータスの変更を即座にアラートすることで積極的に防御されています。

Appgate SDPはまた、約2億200万個のSMBポートをブロックし、ファイルサーバ、プリンタ、システムへのアクセスを制御するために使用されます。これらのSMBポートは不可視であり、脅威行為者が魅力的なネットワーク・ターゲットを探し出す能力を排除します。そして、この世界的な巨大企業は、1年の間に、Appgate SDPを使用して、リスクの高いポートへのトラフィックを7,500万回ブロックしました。この種のサービス拒否は、データを盗んだりネットワークに感染させようとする未知のソースや悪意のある行為者から組織を安全に保つための中核となるものです。

ユニバーサルZTNAで課題を克服

正直なところ、多様なネットワーク環境へのアクセスを保護することは、ほとんどのCISOにとって綱渡りのように感じられるかもしれません。クラウドのデプロイメント、レガシーシステム、データセンター、オンプレミスのインフラは共存しなければなりません。攻撃対象や死角は増え続けます。別々のセキュア・アクセス・ソリューションが、ポリシー管理をロジスティカルな悪夢にしています。また、あらゆる場所にある企業リソースにアクセスする必要のある従業員は、ネットワーク・セキュリティにさらなる複雑さをもたらします。多様な環境のセキュリティ確保に悩むCISOは、セキュリティ体制を強化し、進化するITランドスケープに適応できることが証明されているゼロ・トラスト・ネットワーク・アクセス（ZTNA）にますます注目するようになっています。しかし、すべてのZTNAソリューションが同じように作られているわけではありません。また、ハイブリッドITが複雑化しているため、CISOは、現在および将来のネットワーク・セキュリティ・ニーズに対応できる最善のZTNAを選択する際には、見極めが必要です。ZTNA ソリューションを比較する際には、以下の点を考慮してください：

- リモートアクセス以上の接続を効果的に処理できますか？ZTNAソリューションの大半はクラウドルート型で、主にリモートアクセス用に設計されています。レガシーシステムとの統合やオンプレミスインフラの保護に苦労するだけでなく、ベンダーのマルチテナントクラウドを経由させるため、遅延、スループット、スケールの制限が加わります。
- シームレスな統合と相互運用性を提供しますか？選択するZTNAソリューションが、他のセキュリティツールやビジネスツールと効果的に接続できることを確認し、サイロ化を回避することが重要です。
- 包括的な可視性を提供しますか。ロギングやアクセス情報など、多様なユーザーとデバイスの活動に関する完全な洞察を提供できますか。
- 将来のニーズに対応できる拡張性と適応性を備えていますか？全体的な成長計画や新たなテクノロジーとの統合をサポートするための強力な適応性と拡張性を備えている必要があります。

普遍的なZTNAの優位性

ユニバーサル・ゼロトラスト・ネットワーク・アクセスは、セキュアなアクセス管理のパラダイムシフトです。包括的なポリシーフレームワークにより、企業はデバイスや場所（オンプレミスまたはリモート）に関係なく、すべてのユーザーに対してゼロトラスト原則の厳格かつ一貫した適用を保証できます。合理的なアプローチは、VPN、MPLS、NACのような従来の技術に取って代わり、複雑なネットワーク・トポロジーにわたるセキュアなアクセス管理を簡素化します。また、ユニバーサルZTNAソリューションは、CISOが堅牢なネットワークセキュリティ、ユーザーエクスペリエンス、ビジネス目標を健全にバランスさせるのに役立ちます。その結果、セキュリティは劇的に向上し、エンドユーザーはシームレスなアクセスを享受し、ビジネスは効率性の向上と運用コストおよび資本コストの削減によって利益を得ることができます。

DXCテクノロジー・ストーリー

M&Aによって設立されたフォーチュン500のDXCテクノロジーは、複雑なVPNの数々、不必要なオーバーヘッド、運用上の障害、セキュリティギャップといった共通の課題に直面していました。問題を克服し、ゼロトラストセキュリティ原則に沿うために、**DXC**はわずか**120**日で**Appgate SDP** ユニバーサル **ZTNA**を導入し、膨大な統合インフラと13万人以上のユーザーを保護する統一プラットフォームを構築しました。

スタッフの管理時間を大幅に削減し、ユーザーエクスペリエンスを向上させただけでなく、DXCは600以上のサイトからMPLS接続を削減し、Appgate SDPのダイレクトルートアーキテクチャとマルチトンネル機能を活用したカフェスタイルのWi-Fiネットワークを構築しました。これにより、接続コストが67%削減され、年間数百万ドルの節約につながりました。また、Appgate SDPは、DXCの重複するIPスペースに対応しました。これは、M&A後の統合や分割で頻繁に発生するハードルです。

ダイレクト・ルート・アーキテクチャーで構築されたユニバーサルZTNAの利点

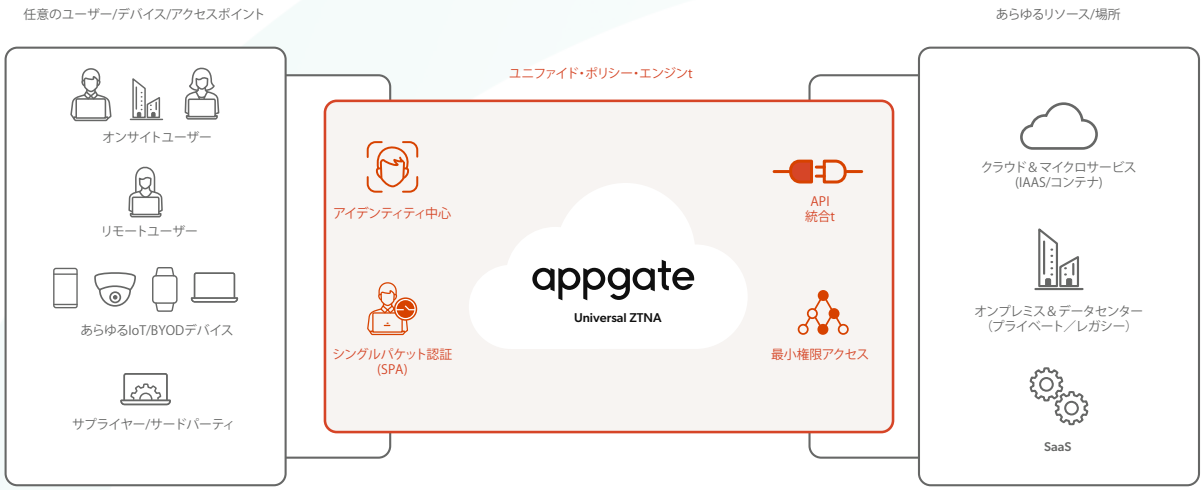
Appgate SDPは、現代のITエコシステムの複雑さを乗り切る組織に堅牢なセキュリティソリューションを提供します。市場で唯一のダイレクトルート型ZTNAソリューションの1つです。これにより、CISOはデータがどのようにネットワークを通過するかをコントロールすることができ、マルチテナントクラウドの暗黙の信頼に依存するクラウドルートのZTNAソリューションの落とし穴を回避することができます。Appgate SDPは、最小限のレイテンシーで最適なパフォーマンスを実現し、すべてのユーザー間およびリソース間の接続を一元的にアクセス制御します。これにより、リモートやオンプレミスのロケーション、マルチクラウドの展開、レガシーインフラストラクチャを含む多様な環境のセキュリティ確保に必要な柔軟性と制御が追加されます。

ユニバーサル**ZTNA**の使用例

- 完全なVPNの代替
- サードパーティ・アクセス
- MPLSからインターネットへのトラフィック移行
- ソフトウェア定義広域ネットワーク（SD-WAN）の排除
- ネットワーク・アクセス・コントロール（NAC）の置き換え
- 企業リソースへのブランチ接続
- レガシーインフラへのセキュアなアクセス

きめ細かく、コンテキストを意識した制御を実施するために、Appgate SDPは、以下を含む多層的な認可を活用しています：

- シングルパケット認証（SPA）：このレイヤでは、インフラストラクチャを隠蔽し、ポートを露出させずに完全に不可視化し、シングルパケットで暗号的に検証されたユーザーのみが通信チャネルにアクセスできるようにします。
- サインイン時の多要素認証（MFA）：ユーザーのデバイスを登録することで、2つ目の認証要素として機能し、盗まれた認証情報による不正アクセスの試みをブロックすることでセキュリティを強化します。
- 認証：このレイヤは、SAML や OIDC などの定義された信頼できるソースに対して、ユーザとデバイスの認証情報を検証します。
- 権限付与：ポリシーの割り当て基準は、ユーザ／デバイスの属性を評価し、各ユーザ／デバイスに特定の権限セットを割り当てることを可能にします。
- アクセス制御：このレイヤでは、ユーザートラフィックをエンタイトルメントと比較し、アクセスポリシーを実施し、アクセス条件を検証し、必要に応じてユーザにアクション（MFAなど）を促します。Appgate SDPは、エンタイトルメントで定義された保護リソースのホスト、ポート、プロトコルに基づき、各ユーザ／デバイスのアクセスを動的に管理します。
- アラートアクション：このレイヤは、潜在的な脅威にプロアクティブに対処するために、未承認のポートスキャンなどのリスクの高い動作をブロックし、アラートとともにログに記録するトリガーシステムとして機能します。



Appgate SDPは、ハイブリッドIT、マルチクラウド、本社、支社、データセンターにまたがるすべてのユーザー、レガシーアプリやカスタムアプリを含むリソース、ロケーションに対してユニバーサルZTNAをサポートする統合ポリシーエンジンを提供します。

未来を確保する：なぜCISOはユニバーサル**ZTNA**を必要とするのか

組織は、クラウドベースのアプリケーション、オンプレミスのインフラ、レガシーシステムを含む異種IT環境の管理をますます強化しています。これらの多様なシステムは、その本質的な設計上、サイバー敵が悪用できる脆弱性を提供し続けることになります。ユニバーサルZTNAは、きめ細かなアクセス制御を実施し、暗黙の信頼の概念を排除することで、これらのリスクを軽減する最も説得力のあるソリューションとして登場しました。

注目すべきことに、Gartner 社は、2026年までサイバー攻撃全体の50%以上が、ゼロトラスト制御ではカバーできず、軽減できない領域を狙ったものになると予測しています。このような攻撃の多くを阻止するためには、場所に関係なく、すべてのユーザーとデバイスにわたってユニバーサルZTNA制御を拡張するセキュリティアプローチが必要です。

その他のCISOリソース

ホワイトペーパーユニバーサル・ゼロ・トラスト・ネットワーク・アクセスの投資収益率分析

ガイドクラウドルートとダイレクトルートのZTNA：その違いは？

電子書籍ゼロ・トラスト成熟度モデルのロードマップ

Appgate SDP ユニバーサル **ZTNA**は、拡大する組織のデジタルフットプリントを保護しようとする**CISO**に強力なソリューションを提供します。以下のようなメリットがあります：

- **すべてのユーザーとデバイスのアクセスを統一：** 複数のソリューションを管理する手間を省き、すべてのユーザーとデバイスに対して一貫性のある統一されたアクセス制御を実現します。
- **適応性と拡張性に優れたセキュリティ：** 多様なユーザーとデバイスに対応するためにアクセスポリシーを動的に適応させ、幅広いユースケースとセキュリティ要件に適合するようにします。
- **生産性の向上：** トラブルチケットを削減し、許可されたユーザーのリソースへのアクセスを迅速化することで、より俊敏で生産性の高い環境を実現します。
- **コンプライアンスの簡素化：** 一貫したアクセス制御を適用することで、報告範囲を縮小し、業界規制へのコンプライアンスを確保します。
- **コスト効率と投資収益率（ROI）：** 複数のアクセス・コントロール・ツールを統合することで、運用効率を高め、大幅なROIを実現します。アクセス制御を統合し、異種のレガシーセキュリティソリューションの必要性を排除することで、ユニバーサルZTNAは、組織が安全で簡素化されたアクセス環境を実現し、セキュリティ体制、ユーザーエクスペリエンス、運用コストを最適化することを支援します。

appgate

Appgateは、組織の最も貴重な資産とアプリケーションを保護します。Appgateは、Zero Trust Network Access（ZTNA）とオンライン詐欺防止におけるマーケットリーダーです。Appgateの製品には、Appgate SDP for Universal ZTNAと360 Fraud Protectionがあります。Appgateのサービスには、脅威アドバイザリ分析およびZTNA実装が含まれます。Appgateは、世界中の企業や政府機関を保護しています。詳細はappgate.comをご覧ください。

SDP – 1993