安全なキャンパス ネットワークの構築： 成功のための 4 つの重要なステップ

目次

概要

現代のキャンパスネットワークの構築は、実に大変な業務です。組織がデジタルイノベーションを加速させるにつれて、企業ネットワークの複雑化と分散化がさらに進み、エッジ数も増え続けています[1]。組織がネットワークに求める役割は次第に増えていくため、現時点でのあらゆる需要に対応できるネットワークを構築するだけでは不十分です。今後の情勢を考慮することも重要であり、それには慎重な計画が求められます。この eBook で紹介するステップを実行すると、円滑に動作するネットワークで安全な接続を実現でき、その信頼性は将来にわたって持続します。

「組織には、セキュリティとネットワークが統合型フレームワークとして機能し、ネットワーク上のどこででも信頼できる接続を提供するための戦略が必要です」[2]

ステップ 1：環境を理解する

すべてのネットワークは、それが動作する物理的環境に応じて構築する必要があります。この環境とは建物だけではなく、ユーザーが誰で、そのユーザーが使用するデバイスや実行する必要のあるアプリケーションは何か、ということも意味します。

場所

建物はそれぞれ異なり、時間の経過と共にその利用方法も変化します。ネットワークを新設または更新する場合は、事前に物理的環境の特性を理解しておきます。会議室以外にユーザーが集まる場所を確認してください。管理者のオフィス、休憩室、談話室など、共同作業でよく利用されている場所は他にありますか？そうした場所に容量を追加することを、必ず計画に組み込んでください。

さらに、建物や備品に使用されている材質も知っておく必要があります。金属製のものは、Wi-Fi 信号の伝播に重大な影響を与える可能性があります。容量の追加が必要な場所と RF 障害物（またはその他の干渉減）の場所を確認したら、堅実なアクセスポイント（AP）配置計画を立てることができます。その後、上流側のスイッチング容量が、AP 数および AP に必要な PoE（Power over Ethernet）に十分対応できることを確認します。

利用者

大半の企業には、従業員、来訪者、契約業者などさまざまなユーザーが存在します。これらのユーザーが誰で、どの程度のネットワークアクセスを利用できる（またはすべき）か、さらにはどこでネットワークにアクセスできる（またはすべき）かを理解しておくことは非常に重要です。ネットワークの構築は、ネットワークを保護することでもあります。したがって、来訪者や契約業者がネットワークアクセスできる場所とできない場所を計画しておく必要があります。ユーザーグループに応じて異なるアクセスレベルが適用されるようにネットワークを構築してください。

デバイス

ネットワークユーザーは、多数のデバイスをネットワークに接続します。そして、IoT デバイスが増加している現在、デバイスの数や種類はサイトによって大きく異なる可能性があります。それらがどのようなデバイスで、どういった機能を（ネットワーク技術とセキュリティの両面で）備えているかを把握することが必要不可欠です。これを理解していなければ、どのような接続デバイスでも適切にサポートできるネットワークを計画することは非常に困難です。セキュリティ機能の少ないデバイスやヘッドレスデバイスの場合は、ネットワーク内で追加のセキュリティ対策が必要になることもあります。

顧客が入れ替わる標準的な頻度を考慮することも重要です。新規デバイスが頻繁にネットワークに接続する場合や、デバイスの交換サイクルが 3 年を超える傾向がある場合などは、ネットワーク規格やセキュリティ対策の面で異なる判断が必要になります。

方法

主な検討事項には、誰がどのアプリケーションを使用し、どのような方法でアクセスするかを理解することも含まれます。アプリケーションのカタログを作成し、利用予定者とアプリケーションを比較検討してください。アプリケーションセットに遅延やジッターの影響を受けやすいものが含まれている場合は、それらをサポートするようネットワークを設計します。

新規または現行の企業イニシアチブでは、どのようなアプリケーションと利用形態が推奨されるかを考えてください。これらは現在のネットワークのニーズを変えるものではありませんが、将来のネットワークに影響する可能性があります。そして、現在展開されているネットワークは、将来のイニシアチブに対応しなければならないのです。このようなアプリケーションのニーズは、後述するステップのネットワークとセキュリティの計画に影響します。

「インターネットに接続されたデバイスは、個人情報の収集、ID の窃取、金融データの流出、ユーザーの盗聴や監視のために悪意のある組織に利用される可能性があります」[3]

ステップ 2：ネットワーク計画の作成

すべての情報を収集し理解したら、ネットワーク計画を作成します。まずは最も一般的なアクセスレイヤー（無線）から始め、そこから重要項目へと進んでいきましょう。

無線レイヤー

ユーザーとデバイスを対応づけたカタログに基づいて、最も適切な無線ネットワーク技術を選択します。採用する Wi-Fi 規格を検討する際、考慮すべき点は価格です。新世代の規格は高額になりがちですが、通常は旧世代よりも大幅に値上がりすることはありません。クライアントデバイスの入れ替わりが激しい場合や、今後数年間のネットワーク利用で大きな変化が予想される場合は、最新技術によって将来性を確保することに価値を見出せます。ネットワークと利用形態が安定している場合は、最新規格を求める必要性は低いため、予算を温存しておくことができます。

AP の正しい配置を判断するには、現在の環境に関する実地調査のデータを使用するか、グリーンフィールド（新規）展開向けの広範囲な計画を立てます。このステップでは、特に新規展開の場合、ステップ 1 で確認した物理的環境の各項目が重要になります。

建物の材質やそこに配置される備品に関する知識があれば、RF 計画ソフトウェアが適切かどうかを判断できます。最新の Wi-Fi ソリューションの大半は、チャネルや電力を調整して欠点を補うことができますが、事前の注意を怠ると、計画面での重大な問題点に何年も悩まされることになります。

有線レイヤー

ネットワークの有線基盤の計画には複数の考慮事項があります。一般的にはポート数（ネットワークに必要な有線ポートの数）、電力バジェット（特に Wi-Fi アクセスポイント、PoE 対応の電話機や産業機器の場合）、全体的な容量を検討します。デバイスの種類やユーザーの数を把握することで、それに応じたスイッチ容量を計画し準備することができます。有線ネットワーク接続が必要な IoT および OT デバイスはすべて対象に含めてください。

WAN 接続

従業員が適切な実績を上げられるようにするには、多くの場合、オフサイトにあるアプリケーションやデータへの安定的で信頼できるアクセスが必要です。冗長性を維持できる WAN 接続を計画し、必要に応じて SD-WAN などの技術を利用して、アプリケーションのパフォーマンス要件を満たしましょう。WAN 接続のサイズは、サイトを通過するデータ量に応じて設定します。さらに、クラウドリソースへの移行計画も考慮に入れます。これにより、WAN の帯域幅と耐障害性の要件が増える場合もあります。

「ハイブリッドメッシュファイアウォールの最重要コンポーネントの一つは、今日のマルチクラウドおよびハイブリッドのデータセンター環境を横断できる機能です。ハイブリッドメッシュファイアウォールは、統合型管理コンソールを使ってすべての IT ドメイン（企業サイト、パブリック / プライベートクラウド、リモートワーカー）を協調的に保護します」[4]

ステップ 3：セキュリティ計画の作成

従来のフラットなネットワークは、たとえネットワークベースのセグメンテーションやマイクロセグメンテーションの技術を使用していたとしても、現代の高度な攻撃を検知または阻止することはできません。この問題の一端は、フラットネットワークの多くが今もなお、認証されたユーザーおよびデバイスに対して、事実上すべてのアプリケーションへの無制限なアクセスを許可することにあります。このように暗黙的な信頼ポリシーには境界がなく、ネットワーク全体、特に暗号化されたパスの可視性を低下させます。

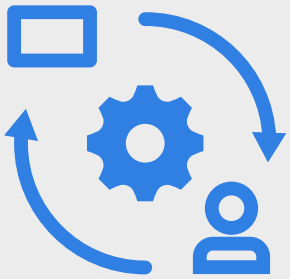
ハイブリッドメッシュファイアウォールのアプローチ

完全に統合され一元的に管理されるセキュリティソリューションは、今日のハイブリッド IT アーキテクチャにおいて、一貫性と適応力に優れた脅威検知とレスポンスを実現できる唯一の方法です。ハイブリッドメッシュファイアウォール（HMF）は、一貫したポリシーの適用と一元管理によって、オンプレミスおよびクラウドインフラストラクチャでネットワークとセキュリティのコンバージェンスを可能にします。こうした統合型セキュリティプラットフォームを用いたアプローチによって、企業 IT のあらゆる領域を協調的に保護できます。

ゼロトラストアクセス

ゼロトラストフレームワークでは、検証されるまでは誰も何も信用されません。これはユーザーがキャンパス内にいようと、あるいはリモートで勤務していようと適用されます。ハイブリッドワークでは、オンサイトとオフサイトの勤務場所がより流動的になるからです。

セキュリティポリシーを作成する際は、必要なアプリケーションへのアクセスをユーザーに許可し、不要なアプリケーションへのアクセスは制限する必要があります。そのための最善の方法は、ゼロトラストネットワークアクセス（ZTNA）を実装し、ゼロトラストフレームワークの中でアプリケーションアクセスを制御することです。



「…組織は『何も信用せず、常に検証する』ゼロトラストモデルを実装する必要があります。これにより、分散ネットワークに厳格なアクセス制御が組み込まれ、ユーザー、デバイス、エンドポイント、クラウド、インフラストラクチャはすべて保護されます」[5]

IoT および OT デバイス

多くの場合、現代のスマートキャンパスにはさまざまな IoT デバイスが配置され、従来で言うところの OT 環境に接続しています。これらのデバイスは、ネットワーク機能が大きく制限されていることがあるため、ZTNA 計画ではしばしば既知の「欠点」と見なされます。ヘッドレスデバイスのオンボードが簡単で、仮想パッチの提供が可能なソリューションを探しましょう。仮想パッチを適用すると、IoT または OT デバイスに既知の脆弱性がある場合に、エコシステム内のセキュリティシステムが自動的に補正的制御を行うことができます。

ステップ 4：統合型管理の確立

さまざまなコンソールを使ってネットワークとセキュリティを管理していると、多くの課題が発生し、IT チームの許容範囲を超える量のリソースが消費されます。重要な点は、ネットワーク全体（セキュリティを含むすべて）を 1 つの統合されたものとして管理することです。これにより、管理に費やす手間が簡略化されると共に、信頼できる唯一の情報源を使用してネットワーク内の問題を解決できるようになります。そのためには、共通のフレームワークに統合できるネットワークおよびセキュリティ機器が必要です。

レガシー環境への対処

さまざまな状況において、環境内のテクノロジーが旧式化した場合、ネットワークスタックの全面的な見直しの一環として、それを直ちに交換することはできません。このようなケースでは、古い技術を可視化しながら、新しい技術に移行できるソリューションを探す必要があります。こうした機能は、ネットワーク監視ツールまたは NAC ツール（必要な管理レベルによります）によって実現されます。ネットワーク監視ツールは、マルチベンダー環境を全体的に可視化し、SaaS サービスなど IT チームが管理していないリソースのパフォーマンスを追跡できます。マルチベンダー NAC ソリューションは、機器を安全に接続し、時間と予算に応じたネットワーク展開を可能にします。

損害を回避するためのヒント

よくある落とし穴を回避し、ネットワークの展開と運用を円滑に進めましょう。

自分が建築資材を理解していると思い込まないでください。必要に応じて AP を使った簡単なテストを行い、鉄筋の壁、鉛ガラス、その他の障害物を特定しましょう。

数年後には、新しいアプリケーションやニーズによってネットワークの境界が変化することを想定し、それに応じた計画を立てます。

屋内にある大半の公的空間では、カバレッジではなく容量に合わせて設計します。

スイッチの電力バジェットを確認し、新技術のオーバーヘッドを計画に含めます。

アプリケーションの配置場所（オンプレミス、データセンター、パブリック / プライベートクラウド、SaaS ベースなど）を十分に考慮し、それに適した WAN 接続を計画します。

環境内の IoT および OT デバイスをすべて把握し、それらをどのように保護するかを計画します。

ベンダーの選定後ではなく選択時に管理の容易性を検討します。

設計全体でセキュリティが多層構造になっていることを確認します。また、共通のフレームワーク内でネットワークとセキュリティをコンバージできるソリューションを見つけます。

終わりに

キャンパスネットワークは複雑化し続けているため、ネットワークの新設または更新を計画する場合、IT チームは物理的環境、ユーザーの所在地やデバイス、使用されるアプリケーションなど、さまざまな要素を考慮する必要があります。ただし、最も重要な点は、セキュリティと管理は後回しにできないということです。この eBook のステップに従えば、管理しやすいネットワークで安全な接続を確保し、現在および将来のニーズに対応することができます。

[1]「Zero Trust Access for Dummies」、Lawrence Miller 著、Wiley、2022 年（英語）：
https://www.fortinet.com/content/dam/fortinet/assets/ebook/zero-trust-access-for-dummies.pdf

[2]「How to Secure Your Edges Without Inhibiting Productivity」、Jonathan Nguyen-Duy 著、Fortinet、2022 年 5 月 5 日（英語）：
https://www.fortinet.com/blog/ciso-collective/secure-your-edges-without-inhibiting-productivity

[3]「Securing Wireless Networks」Cybersecurity & Infrastructure Security Agency、2023 年 9 月 5 日アクセス時点の情報（英語）：
https://www.cisa.gov/news-events/news/securing-wireless-networks

[4]「Using a Hybrid Mesh Firewall to Increase Network Security」、Nirav Shah 著、Fortinet、2023 年 8 月 4 日（英語）：
https://www.fortinet.com/blog/ciso-collective/hybrid-mesh-firewall-to-increase-network-security

[5]「Zero Trust Access for Dummies」、Lawrence Miller 著、Wiley、2022 年（英語）：
https://www.fortinet.com/content/dam/fortinet/assets/ebook/zero-trust-access-for-dummies.pdf

フォーティネットジャパン合同会社

〒106-0032
東京都港区六本木 7-7-7　Tri-Seven Roppongi 9 階
www.fortinet.com/jp/contact

お問い合わせ

Copyright© 2023 Fortinet, Inc. All rights reserved. この文書のいかなる部分も、いかなる方法によっても複製、または電子媒体に複写することを禁じます。この文書に記載されている仕様は、予告なしに変更されることがあります。この文書に含まれている情報の正確性および信頼性には万全を期しておりますが、Fortinet, Inc. は、いかなる利用についても一切の責任を負わないものとします。Fortinet®、FortiGate®、FortiCare®、および FortiGuard® は Fortinet, Inc. の登録商標です。その他記載されているフォーティネット製品はフォーティネットの商標です。その他の製品または社名は各社の商標です。

EB-Secure-Campus-Network-202310-R1