セキュアアクセス
ソリューション

フォーティネットのソリューションを導入することで、大学や専門学校などの高等教育機関は、数千台のデバイスの効率的な統合、アプリケーション使用の管理と優先度の設定、処理能力の容易な拡張が可能となり、新たな脅威からの最高レベルの保護を実現できるようになります。

高等教育機関におけるセキュアアクセスの実現

高品質の Wi-Fi 環境と脅威保護

何千人もの学生が無線ネットワークに初めて接続する新学期は、帯域幅の需要が急増し、新しいアプリケーションや新しいサイバー脅威が出現する時期でもあります。

従来は、「信頼できるノート PC」によるネットワークアクセスが大半でしたが、今ではスマートフォン、タブレット、電子ブックなどへと使用するデバイスが次々と変化し、また同時に何台も使うことも多く、学生たちは Wi-Fi やクラウドに完全に依存するようになりました。学生たちは信頼性の高い接続を要求しており、強力なセキュリティやアプリケーションの優先度付けが必要とされています。

フォーティネットのセキュアアクセスアーキテクチャによってトップクラスの体感品質の WLAN 環境を補完することで、高等教育機関が業界で最も容易な方法で最新の脅威から完全に保護された世界水準のサイバーセキュリティを導入し、統合を合理化できるようになります。

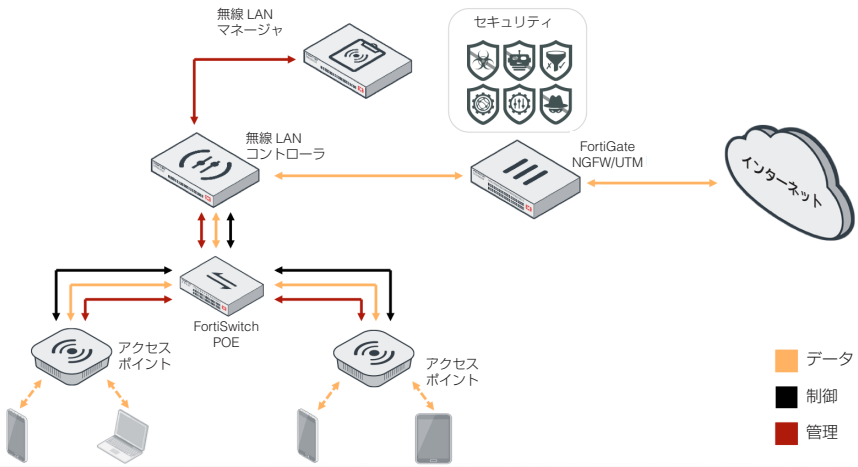

図 1：フォーティネットのインフラ型セキュアアクセスソリューション

- 業界で最も容易な導入と処理能力の拡張が可能
- 高速で信頼性の高いローミングでトップクラスの体感品質を実現
- Bonjour プロトコルのマルチキャストを抑制し、非効率的な帯域幅の使用を解消
- サイト全体のチャネルボンディングによる優れた 802.11ac パフォーマンス
- 脅威に対する包括的な保護を 1 台のアプライアンスに統合
- アプリケーションと利用状況の高度な可視化と制御
- FortiGuard Labs からのシグネチャの定期更新によって、セキュリティは常に最新の状態を維持

高等教育機関におけるアクセスの課題

ネットワークへの依存

オフライン環境が主流だった時代は終わりを迎え、学生や教員はネットワークに常時接続された環境でクラウドのリソースを使って作業するようになりました。米国では、学生の 50%以上がモバイルデバイスの学習アプリを使用し、世界中で 50 万人の学生が Google Apps for Education、さらには、Office 365 の電子メール、予定表、PowerPoint などを使用しています。何億もの人々が、iCloud、Dropbox、Google Drive などのクラウドストレージ上の音楽やファイルへのアクセスなしには生活できない状況になっています。

今や学生は、昼夜を問わず信頼性の高いインターネットアクセスを必要としていますが、単にアクセスできれば良いということではありません。多数のデバイスすべてをどこからでも確実に接続でき、接続が途切れることなくローミングされて、リソースを使ってあらゆる作業を実行できなければなりません。つまり、授業の合間に急いで講義ノートをダウンロードしたり、学食で Skype したり、寮で Facebook と映画を同時に見たり、そのすべてが中断なく行うことができる必要があるのです。

アプリケーション利用の急増

学生たちは、授業がない時間に寮、学食、教室の外などのさまざまな場所で遊んだり、ゲームを楽しんだり、オンラインチャットをしたりするものです。マルチメディア教材や Netflix などの普及によって、ビデオのストリーミングが毎年 40 ～ 60% も増加しており、利用者が最も多いのは 2000 年前後に生まれた 14 ～ 25 才の世代です。

現在のネットワークには、さまざまな帯域幅の要件が混在しており、多様なウェアラブルデバイス（時計、追跡、拡張現実などの装置）や Wi-Fi Calling の増加により、ネットワークの負荷はますます高まっています。古いアクセスポイントの 20 ～ 25% 程度を毎年入れ替える予算しか確保できない状況の多くの大学には、帯域幅の適切な管理以外に選択肢はなく、バースト性のある Bonjour や帯域幅を多用するリッチメディアなどのアプリケーションの利用を制限するとともに、重要なアプリケーションが優先的に処理されるようにして授業の妨げにならないようにしなければなりません。

ユーザーやデバイスの統合

新たな大量のユーザーやデバイスを安全に統合することは容易ではありません。新しいデバイスが追加されるたびに、学生の不正行為や知らぬ間に感染してしまったマルウェアによってネットワークが脅威にさらされる危険性があります。

セルフサービスによる高度な統合機能と AAA クラスのセキュリティフレームワークが連携されていない場合、大量の学生のデバイスが統合された途端、膨大なサポート業務に負われる可能性があります。

また、課題はデバイスの統合だけにとどまらず、アクセスセキュリティの全体図から見れば、1 つの問題を解決したに過ぎません。あらゆる教育機関は、ネットワークで送受信されるリアルタイムデータの保護、既知の不正サイトの遮断、施設内ネットワークのセグメント化によって感染の拡大を防止あるいは遅らせる対策をとり、ハッカーやウイルスの侵入に備えることが不可欠です。

新たな脅威のベクトル

サイバー攻撃の件数はますます増加し、高度化しています。WPA2、802.1X、各種 EAP タイプ、不正 AP 検出、WIP（無線侵入防止）などの標準無線セキュリティ機能は、どれも有効で価値のあるものです。しかしながら、完全な保護対策には通常ファイアウォール、IPS、アンチマルウェア、Web フィルタリング、アプリケーション制御などの多様なセキュリティアプライアンスが必要であり、導入がかなり複雑になる可能性があります。

モバイルオペレーティングシステム、ゲーム機器、ウェアラブルデバイス、そしてその他のヘッドレスデバイスは、攻撃の格好の標的になることで知られています。多くの場合、デバイスへの攻撃は内部にあるはるかに価値の高いシステムに侵入するための手段に過ぎません。次世代ファイアウォール（NGFW）や内部セグメンテーションファイアウォール（ISFW）が不可欠になっているのはそのためです。

フォーティネットのセキュアアクセスアーキテクチャ

受信可能範囲、パフォーマンス、信頼性、BYOD の統合、サイバーセキュリティなど、アクセスに関する課題はほとんどの組織に共通するものですが、その対策は一様ではありません。採用するネットワークアーキテクチャやトポロジはもちろん、IT が果たす役割や責任範囲も組織によって異なります。

他の WLAN ベンダーはどの問題にも同じソリューションを提案しますが、単一のソリューションが万能でないことを誰もが理解しています。このため、フォーティネットのセキュアアクセスアーキテクチャは、業界で最も強力なアクセスセキュリティによって実証されている、すべての共通な WLAN トポロジと導入モデルに対応しています。

フォーティネットは唯一、明確に異なる 3 つの無線ソリューション、すなわちトップクラスの無線、スイッチング、およびセキュリティコンポーネントで構成されるインフラ型ソリューション、WLAN の制御とセキュリティが 1 台の高性能アプライアンスに組み込まれた統合型ソリューション、そして、セキュリティインテリジェンスがクラウド管理型アクセスポイントに組み込まれたクラウド型ソリューションを提供しています。

フォーティネットのインフラ型無線ソリューション

フォーティネットが高等教育機関に推奨するのは、インフラ型無線ソリューションです。このソリューションは、高スループットであると同時に他の競合 WLAN ソリューションに比べて容易な導入が可能で、数千台のデバイスの統合、アプリケーションの利用状況の管理、そして脅威に対するワールドクラスの保護の実現に必要な機能がすべて提供されます。

このソリューションは、クラストップレベルのスイッチング、WLAN（旧メルー・ネットワークス製品）、サイバーセキュリティのコンポーネントで構成されています。WLAN コンポーネントは、802.11n と 802.11ac 対応の広範なアクセスポイント（AP）による高性能のオンプレミス管理型 Wi-Fi ネットワークを提供します。

また、WLAN コンポーネントで採用されているバーチャルセルと呼ばれる独自のチャネル管理アーキテクチャには、他のすべてのベンダーが採用している従来型のチャネル導入アプローチにはない優れた利点があります。

バーチャルセルは、独自のシングルチャネルデプロイメントによってチャネルプランニングのプロセスを最小化します。同一チャネル干渉の課題を回避できるため、大規模導入環境では数か月を要することもある、複雑で時間のかかるプロセスが最小限に短縮されます。

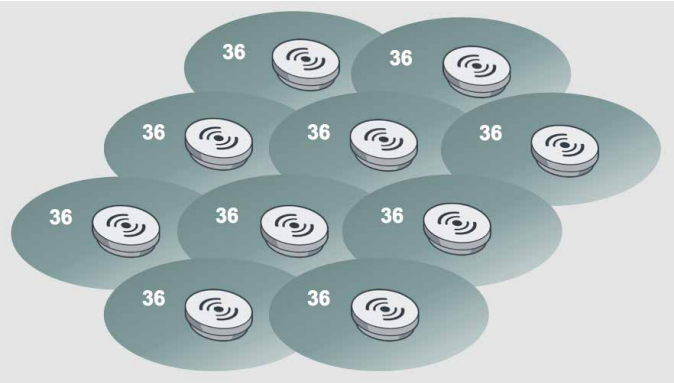

図 2：フォーティネットのバーチャルセル導入モデル

バーチャルセルでは、すべてのラジオが同一チャネルで動作し、キャンパス内の受信可能範囲を階層化できるため、クライアントがどこに移動しても単一のラジオとして認識できます。また、クライアントではなくネットワークが、クライアントのローミングの方法と時期を制御します。

この独自のアプローチによって同一チャネル干渉が解消されるため、クライアント向けに常に最適な接続の使用が保証され、シームレスなゼロハンドオフローミングが実現します。これにより、学生が接続を維持しながらキャンパス内を自由に移動できるようになります。

迅速な導入と拡張

フォーティネットのインフラ型セキュアアクセスソリューションは、サイトサーベイ、チャネルプランニング、セルサイズや送信出力の調整が不要であるため、容易な導入が可能です。受信可能範囲や処理能力を拡張する場合でも、必要な場所に AP を設置して電源を入れるだけで作業が完了し、既存の AP のすぐ隣に増設することも可能です。チャネルの調整やサイトサーベイはまったく必要ありません。

処理能力を大幅に拡張したり、ユーザーやアプリケーションを無線でセグメント化したりする場合には、複数のバーチャルセルがそれぞれ異なるチャネルを使用するように設定し、AP を何台か追加して同じエリアをカバーするようにすることも可能です。このようなセルの階層化は、小規模ゾーンに限定することも、キャンパス全体を対象にすることもできます。

新しいバーチャルセルの追加にあたって既存のセルを変更する必要がないため、処理能力を拡大しても既存の環境の安定性やパフォーマンスが影響を受けることはありません。

トラフィックの分離

チャネルの階層化を使用するもう 1 つの大きなメリットは、RF レベルでサービスを分離できることにあります。サービスの分離によって、ミッションクリティカルなサービスが専用のスペクトラムを使用でき、他のチャネルの輻輳に影響されることがなくなります。教育機関では、教職員と学生のリソースを分離したり、監視カメラ、音声システム、ビルの管理制御システムなどを異なるチャネルに配置する必要があることも考えられます（図 3 を参照）。

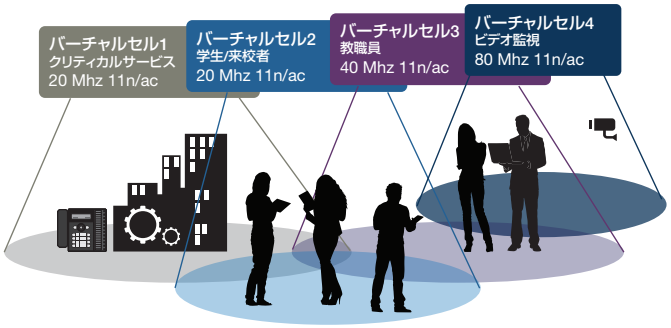

図 3：チャネルの階層化によるキャンパス全域の処理能力の拡張

信頼性の高い接続

もう一つの大きな特長は、クライアントがローミングする最良のタイミングと場所を判断するのは、クライアント自身ではなくネットワークであり、結果として高品質のサービスが実現する点にあります。このアプローチによって、学生のデバイスが常に最適な接続を使用できるようになり、教室を移動しても接続が中断することがありません。

AP から別の AP へはゼロハンドオフのローミングが可能で、従来型のマルチチャネル環境では一般的に 120 ミリ秒以上かかり、802.11k と 802.11r が有効なクライアントであっても最速で 50 ミリ秒とされる再接続時間が、わずか 3 ミリ秒に短縮されます。ロハンドオフローミングであれば、音声や遅延の影響が大きいリアルタイムのセッションで発生する多くの問題が解消され、ローミング中に接続が途切れることがありません。

このネットワークベースのトラフィック制御によって、ステーション数に基づくインテリジェントとはいえないラウンドロビンのアルゴリズムではなく、実際のトラフィックに基づくリアルタイムの AP 負荷分散が可能になります。ステーションの通信時間もネットワークによって管理されるため、すべてのクライアントの無線使用が公正化され、低速のデバイスが通信を占有することがなくなります。

Bonjour マルチキャストの抑制

Apple ユーザーが多い環境では、Apple TV や無線プリンターに学生が接続すると、Apple の Bonjour テクノロジーによって重要性の低いマルチキャストパケットが発生し、大量の帯域幅を使用する問題が発生します。マルチキャストのアドバタイズは小さいかもしれませんが、あらゆる場所に拡がって、すべてのユーザーが影響を受ける可能性もあります。

フォーティネットのサービス制御機能は、Bonjour 経由でサービスをアドバタイズするデバイスの内部テーブルを管理し、検出プロセスを介してマルチキャストのプローブとアドバタイズをユニキャストトラフィックに変換することで、この問題を解決します。このアプローチにより、Bonjour 関連のトラフィックを以前のレベルの 1% 未満に抑制することで、学生寮でまず多く利用される AirPlay や AirPrint の悪影響を完全に緩和します。

セキュリティとアプリケーションの制御

FortiGate アプライアンスによって提供されるセキュリティときめ細かいアプリケーション制御機能は、他のどのセキュリティベンダーよりも効率的で高性能であることが実証されています。

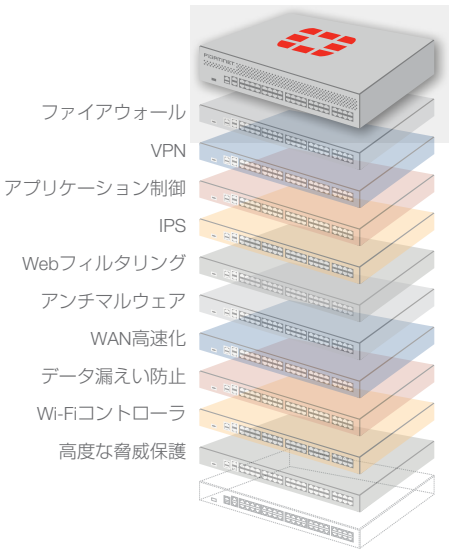

図 4：FortiGate 統合型セキュリティプラットフォーム

FortiGate では、ファイアウォール、VPN ゲートウェイ、ネットワーク IPS、DLP、アンチマルウェア、Web フィルタリング、アプリケーション制御など、7 つ以上のセキュリティデバイスが個別に提供する機能が、1 台の高性能プラットフォームに統合されています。

アプリケーションの負荷に対してリソースが限られている環境では、何らかの対策が必要です。例として、トランシーバーではなく無線 VoIP ハンドセットを職員同士の連絡に使用しているケースを挙げてみましょう。FortiGate であれば、VoIP の通話を学生同士の Skype による通話と区別し、それぞれに独自のポリシーを適用することができます。

また、高画質の YouTube 動画の優先度を下げて、教職員のサーバーからの動画コンテンツのストリーミングが優先されるようにすることもできます。FortiGate は、4,000 以上のアプリケーション用シグネチャを使ってアプリケーションの詳細な利用状況を可視化し、優先度を正確に制御できるほか、事実上あらゆるアプリケーションを制限あるいは遮断することが可能です。

FortiGate では、FortiGuard Labs から高頻度で継続的に提供される最新の自動アップデートによって最新の攻撃の情報が反映されるため、ネットワークは常に保護されます。

内部ネットワークのセグメント化

多くの高等教育機関のネットワークは、極めて単純なフラット型です。ところが、サイバー攻撃はますます高度化しているため、ハッカーに境界を越えて侵入を許してしまうと、公開されている脆弱性が悪用されてフラットなネットワークは即座に侵害されてしまいます。

このため、最近では従来の境界防御だけでなく、高度な攻撃からの保護も実現する多層型の防御が標準的に採用されるようになりました。ユーザーとリソースの間にファイアウォールポリシーを設定し、内部を明示的にセグメント化することで、感染の連鎖を記録して断ち切ることが可能になります。

しかしながら、境界防御を前提に設計されたソフトウェアベースのファイアウォールは、あまりに低速です。フォーティネットは、業界で初めてハードウェアを活用した内部セグメンテーションファイアウォールを開発し、マルチギガビットのラインレートパフォーマンスを実現しました。

まとめ

高等教育機関の WLAN は、受信可能範囲や帯域幅だけが問題だった時代から、セキュリティやアプリケーション管理の優先度が重要な課題とされる、新しい時代へと移行しています。

フォーティネットのインフラ型アクセスソリューションで採用されている独自の Wi-Fi チャネル管理アーキテクチャにより、高等教育機関は、競合 WLAN ソリューションと比較して極めて容易に優れたスループットの高信頼性接続環境を導入し、提供することができます。

さらに、ネットワークセキュリティのパフォーマンスをリードする FortiGate との併用によって、数千台のデバイスを簡単に統合し、アプリケーションの利用状況や優先度の管理、そして最新の脅威からの最高水準の保護の実現に不可欠なすべての機能を利用できるようになります。

FORTINET
フォーティネットジャパン株式会社

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

お問い合わせ