高等教育機関における WiFi に関する 9 つの誤った通念

Ruckus
Simply Better Wireless.

WiFi は絶えず成長し続けているように見えます。10 年以上も前に「WiFi」という用語 (この用語を承認した Wi-Fi Alliance メンバーによれば、特に何かの省略形というわけではない) が誕生して以来、WiFi は急速に拡張し続けるテクノロジーとして常にもてはやされてきたように見えます。

しかし数年前までは、大学で WiFi は新しいテクノロジーでした。多くの機関は、確実な導入を行うための予算がありませんでした。また、セキュリティや教育上の理由でこのテクノロジーの導入を見送った機関もありました。

今日、WiFi は大部分のキャンパスで利用可能です。現時点で WiFi がないキャンパスでも、近いうちに導入されるでしょう。大学生の親は、子供の学生生活が「自宅のように感じられる」ものであることを願っています。それには、机の上に飾る写真 (というよりはスクリーンセーバー) から、電子機器やお気に入りのアプリをすべて使用できる環境が含まれます。WiFi は、最新の教育環境を使用し、世界的ニュースを把握し、ときにはホームランダービー ゲームで上級者レベルに達するために必要なテクノロジーです。WiFi は、比較的安価で、一般デバイス用に普及していて、便利です。

あるいは、少なくとも便利に使用できるはずのものです。

残念ながら、一部の人々の間では、キャンパス環境での WiFi の評判はあまり芳しくありません。率直に言えば、大勢の人が多数の WiFi ネットワークに大金をつぎ込んだにもかかわらず、満足なパフォーマンスを得られていません。

このドキュメントでは、この問題に対処するためのソリューションを提案します。私たちはキャンパスでの WiFi 導入における 9 つの誤った通念を特定しました。こうした誤りを回避すれば、キャンパス WiFi が期待どおりに動作する可能性が格段に高まります。また、現在の WiFi ネットワークが、ここで述べる誤りの大部分に該当しないとしても、WiFi を最適な状態に高めるために、何かしら閃くことがあるかもしれません。

では、キャンパス教育環境における WiFi 導入で一般的になっている、誤った通念をいくつか見ていきましょう。

#1 平均的な大学生はキャンパスに 3 つのデバイスを持ち込む

学生のカバンをひっくり返してみれば、おそらくラップトップとスマートフォンが出てくるでしょう。タブレットを持っている学生も大勢います。寮の部屋には、ゲーム機、ワイヤレス プリンター、AppleTV、スマート TV、Blue-ray プレイヤー、e リーダーなどがあるかもしれません。また、スマート ウォッチやフィットネス バンドなどのウエアラブル デバイスの増加に伴い、キャンパスに持ち込まれるデバイスの数も増加します。

Re:fuel Agency の 2014 年 College Explorer レポートによれば、平均的な大学生がキャンパスに持ち込むインターネット接続デバイスは 7 個です。

これらすべてのデバイスが WiFi に対応しています。すべてのデバイスがキャンパス WiFi アクセス ポイントに接続しようとします。

学生がネットワークに接続する目的が、ラボでの調査研究から寮でのマルチプレイヤー ゲームまでますます多様化するのに伴い、IT チームにとっては、毎日 24 時間の接続を求めて増大する期待に応えることが困難になっています。管理を怠れば、ネットワーク コストは膨れ上がり、コンプライアンスに失敗し、必須アプリケーションへに確実に対応することが難しくなります。

#2 高密度エリアのアクセス ポイント数を増やせばワイヤレス信号到達範囲が改善する

WiFi に限らず、人生の多くのシーンにおいて、お金をつぎ込めば問題が解決するという考えは間違いです。たとえば 1990 年代初めのニューヨーク ヤンキーズはプロ野球界で最高の報酬を選手に支払っていたにもかかわらず、成績はそれに見合うものではありませんでした。同様に、高額な WiFi を導入しても、綿密に計算された導入には太刀打ちできません。

WiFi の世界における典型的な過剰の一例は、過剰な数の AP を導入することです。WiFi の導入で AP の数を増やすと、容量はある程度増加しますが、数を増やし過ぎると生産性が低下し始めます。

AP を過剰に導入すると、複数の AP が同じデバイスの同じチャネルにサービスを提供しようとしてパフォーマンスが低下します。つまり、iPad で Airport Utility アプリケーション [iOS 設定で Airport Utility アプリケーション用にスキャン機能が有効になっている必要があります] を実行したときに、複数台のキャンパス AP が、-80 dBm 超の信号で、同じチャネルで動作している場合です。北米では 2.4 GHz 周波数帯を使用しているときに利用できる非干渉チャネルは 3 つしかありません (一般デバイスに最も広く対応する周波数帯です)。

AP が各教室、または寮の各部屋にも設置されている場合、スマートフォン、タブレット、ラップトップからは、ほぼ確実に、同じチャネルでサービスを提供する複数の AP が「見えます」。

一部の WiFi 導入では、過剰導入されていないように見せかけるため、AP の通信速度が低く設定されています。このようなまやかしに引っかかってはなりません。WiFi は双方向通信技術であるため、AP の通信速度を下げると、ユーザーが密集している環境でチャネルの渋滞という問題が発生したときに対応できません。

「1 教室に 1 台の AP」という誤った通念によって悪影響を受けないよう、AP の設置場所を選択する前に現場を適切に調査することが必要です。各教室に AP を設置することが有効な場合もありますが、現

場を適切に調査しなければわかりません。現場調査は複雑で時間がかかりますが、熟練した導入業者に現場調査を依頼することで、長期的には時間と資金を節約できます。

警告 : ラッカス マーケティング コンテンツ

ラッカス ワイヤレスでは BeamFlex という独自のアンテナ システムを提供していますが、これは、指向性アンテナを動的に形成すると同時に全方向パターンでのデバイス接続にも対応するアンテナ アレイを使用します。このため、廊下に設置された AP は学生と教師の目に触れず気になることもありませんが、教室の壁さえも通り抜ける十分な強度の信号を送受信できます。また、AP 設置を複雑でコスト高にする外部指向性アンテナは不要です。ラッカス AP に内蔵された独自の特許取得 BeamFlex アンテナによって、廊下に取り付けることが現実的なオプションになります。

#3 Wave 2 クライアントを使用していなければ Wave 2 AP を活用できない

WiFi において規格は常に大きな意味を持ってきましたが、現在最も注目されているのは 802.11ac Wave 2 です。802.11ac 規格は 2013 年に IEEE によって正式に承認されましたが、802.11ac AP とデバイスはそれよりかなり前に利用可能になっていました。問題は、最近まで何もかもが 802.11ac Wave 1 だったことです。802.11ac Wave 1 は多少の複雑さを伴いますが、基本的には通常の 802.11n (以前の IEEE 規格で、2009 年まで遡る) に一般向け WiFi 用の改善点がわずかに加えられているだけです。ただし、802.11n と 802.11ac Wave 1 のハードウェアが互いに同等であるというわけではありません。802.11ac Wave 1 用のチップセットは 802.11n 用のチップセットより新しくなっています。チップセットは重要な要素です。ですので、最新チップセットを使用することの重要性については、後ほど詳しく説明します。

現在は 802.11ac Wave 2 が使用されていますが、その対象はアクセス ポイントだけです。大部分のスマートフォン、タブレット、ラップトップは現時点では 802.11ac Wave 2 に対応しておらず、一部の機器が対応するのは少し先のことになりそうです。たとえば Apple は、WiFi 規格に対応するデバイスの生産になかなか踏み切らないことで知られています。他のデバイス メーカーが 802.11ac Wave 1 スマートフォンを 2013 年初頭までに製造開始していたのに対し、Apple 初の 802.11ac Wave 1 スマートフォンである iPhone 6 は 2014 年末までリリースされませんでした。

このように利用可能な Wave 2 デバイスが少なかったことが理由で、この誤った通念が拡散してしまったのです。「Wave 2 デバイスがなければ、Wave 2 AP 導入する意味がない」というような考え方がまかり通っています。ただし、半分は真実です。確かに Wave 2 の利点を完全に活用できるのは、Wave 2 デバイスが利用可能になってからです。一方で、接続されているデバイスがすべて 802.11ac Wave 1 (または 802.11n) だとしても、Wave 1 AP は Wave 2 AP と同じパフォーマンスを実現することはできません。

まず、不利な点は、現時点ではあまり多くの 802.11 Wave 2 デバイスが市場に出回っていないことです。Wave 2 AP が教室に導入されても、学生や教授陣が使用するスマートフォンやタブレットは、Wave 1 AP が導入された場合と同じ最大データ速度しか使用できません。また、一部のデバイスでは、より強力なパフォーマンス向上プロトコルがまったく使用されないかもしれません。これは、トランスミット ビームフォーミング (TxBF) および マルチユーザー マルチ入出力 (MU-MIMO) で、チャネル オーバーヘッドの増大や電池寿命の消耗といった副作用を引き起こすことがあるからです。

人気の高い一般デバイスに WiFi 技術が追いついていないことは残念ですが、スマートフォンやタブレットで 802.11ac Wave 2 の改善された性能をすべて活用できないからといって、スマートフォンやタブレットが Wave 2 アップグレードの恩恵を受けないというわけではありません。802.11ac Wave 2 AP ではより新しいチップセットが使用されており、 Wave 1 AP よりも受信感度が高くなります。このため、煩わしい半接続 (デバイスには接続済みと表示されるが、ネットワークへのアクセスが安定しない) 状態

が低減され、最終的に、信号到達範囲が広がります。Wave 2 AP はアンテナ数も多いため受信ダイバシティが改善されて、接続デバイスが 802.11ac Wave 1 または 802.11n にしか対応していない場合でも、WiFi の状態が向上します。つまり、ユーザーのデバイスが Wave 2 に対応するようになるまでは Wave 2 を全面的に実現することはできませんが、Wave 2 AP はいくつかの点で Wave 1 AP より優れています。

警告 : ラッカス マーケティング コンテンツ

もうひとつ考慮すべきは、将来に備えることです。キャパス ワイヤレス ネットワークのアップグレードが 5 年に一度ほどしか実施されない場合、Wave 2 を導入しておけば、次回に予算が下りるまでキャンパス ユーザーをサポートできます。クライアント デバイスの 98% が 802.11ac に対応していなかった 802.11n から 802.11ac への過渡期にも同じ問題が提起されましたが、当時 802.11ac へのアップグレードに投資した教育機関は、新しいクライアントが台頭してきたときに体制が整っていました。学生の要求に先回りして応え、不満の声を聞かないで済めば、それに越したことはないと思いませんか？

#4

WiFi は IT セキュリティの最弱点である

WiFi を追加しても IT セキュリティにまったく影響はないといったらウソになります。確かに影響はあります。学生、スタッフ、管理者は、ワイヤレス認証を行う必要があります。オンプレミスのハッカーは、罠を仕掛け、注意を怠ったユーザーを脆弱な状況にに誘い込むことができます。その気になれば、オンラインのウォードライビング サイトから、学生と教師が所在する学校の位置を突き止めることができます。そのどれもが IT 担当者にとって頭痛の種であり、最悪のケースでは窮地に陥ることになります。

ただし率直に言って、WiFi リンクが原因となる、重大なネットワーク攻撃が現実に起こる時代は終わっています。WiFi セキュリティは強力になり、標準化され、広く普及しています。

全米でチェーン展開しているデパートが WiFi からハッキングされた事件を覚えていますか？このような事件は現在は起こっていません。

犯人は WEP 経由で侵入しましたが、最新のキャンパス導入では WPA2 が必須になっています。

また、全米でチェーン展開する別のデパートが、空調設備修理作業員のミスでハッキングされた事件を覚えていますか？このような事件も起こっていません。今日のキャンパスでの導入ではゲスト アクセス用に別の VLAN を使用するため、ベンダー、修理作業員、その他のユーザーは、内部の機密データから切り離されています。

同様の事例は多数あります。パスワードが空中を飛び交うことはありません。どの認定 WiFi デバイスも (最初の iPhone が発表された 1 年前である 2006 年以降) AES 暗号化への対応が義務付けられているからです。
偽の AP が内部のユーザーを誘うことはありません。今日の WiFi デバイスは、AP が同一の WPA2 ログイン情報を使用していない限り、ローミングしないからです。不正な AP はもはや脅威ではありません。有線ポートが開きっ放しになることがないからです。まだまだ、多数の例があります。

WiFi はネットワーク セキュリティに影響しますが、これはネットワークに何を追加した場合でも同じです。ただ、WiFi が弱点となる日々は遠い過去の話になりました。少なくともそのはずです。セキュアなワイヤレス ネットワークの導入はシンプルです。ただし、ユーザーをオープン ネットワークからセキュア ネットワークに移行させるのには、多少手間がかかります。パスワード、ログインの繰り返し、IT トラブル チケットの発行は、誰もが煩わしく感じることです。

警告 : ラッカス マーケティング コンテンツ

パスワードの問題を回避するために推奨されるひとつの方法は、Ruckus Cloudpath などの、自動証明書配信システムと公開鍵インフラストラクチャ (PKI) です。

- 各デバイスの構成とプロビジョニングを有効にすることで、各デバイスでまったく同じ手順を使用でき、デバイスの構成における IT の関与を最低限にできます。これによって IT スタッフはデバイスを操作する責任から解放され、より戦略的な IT 目標を達成することが可能になります。
- 管理者はデバイスや OS の種類にかかわらず単一のポリシーを作成できるため、セキュリティの設定に必要な IT 時間が最小限に短縮されます。キャンパス全体のセキュリティを設定するために要する時間が劇的に減少するため、より戦略的な IT 目標を達成することが可能になります。
- 証明書の有効期限が切れるまでセキュア ネットワークに自動的に繰り返し接続されるようデバイスを登録することによって、いったんセキュアにしたデバイスを再度セキュアにする手続きを最小化できます。IT スタッフは同じデバイスに同じ手続きを 1 年に何度も行うことに時間を費やす必要がなくなるため、より戦略的な IT 目標を達成することが可能になります。聞いたことのある話ではありませんか？

#5 AP をアップグレードする際には PoE をアップグレードする必要がある

最初に、誤った通念でない (真実の) 話をしましょう。新しい規格では、電力の要件も高くなっています。802.11a が普及したとき、デュアル無線 AP が使用され始めました。無線が増えると、必要な電力も多くなりました。802.11n 規格に MIMO が追加されたときには、複数の無線チェーンが一般的になり、AP 電力の要件はさらに高くなりました。

802.11ac Wave 1 で 3 ストリーム MIMO が一般的になると、AP はますます大きな電力を要求するようになりました。802.11ac Wave 2 が登場し、4 つの MIMO ストリーム (そして将来的には最大 8 ストリーム) に対応するようになったため、AP 電力のニーズは再び上昇しました。

誤解を生む原因は、新 PoE 規格に対応するためにスイッチのアップグレードが提案されることです。確かに最新の 802.3at (PoE Plus) は 1 ポートにつき 12W の追加供給電力 (正確には 25W) に対応していますが、旧型の 802.3af (PoE) 規格 (12.95W の供給電力) にしか対応していないスイッチ ポートに接続されている場合でも AP は動作します。

警告 : ラッカス マーケティング コンテンツ

多くの場合 PoE Plus へのアップグレードは不要ですが、デスクトップやラップトップが密集している学校では、オリジナルの PoE にしか対応していないスイッチ ポートに AP が接続されていると WiFi 速度が低下する場合があることは事実です。ラップトップやデスクトップは 3 ストリーム MIMO に対応していることもあり、大部分のエンタープライズ AP は、電力が不足している場合に、利用可能な MIMO ストリームの数を減らします。

ラッカスでは、別の (より優れた PoE を提供する) 方法で対応します。他社の多くの AP では、AP の数を減らして、対応する送受信機器の数を減らします。たとえば、高電力 PoE (802.3at) は 4x4:4 に対応できますが、古い PoE (802.3af) では 2 つの無線をシャットダウンして AP を減らし、2x2:2 にします。
ラッカスの R710 (Wave 2 11ac) では、完全な運用のために必要な電力が不足しているときには USB ポートとセカンダリ イーサネット ポートのみをシャットダウンするため、WiFi 速度を最高レベルに保つために十分な電力を温存しておけます。

#6

AP 送信出力を増加させると信号到達範囲が広がる

802.11g が「超高速」であった WiFi 黎明期には、WLAN プロフェッショナルはアクセス ポイントを中心とした「円」で信号到達範囲を示しました。円がオーバーラップしない場所は、信号が届かないギャップでした。このギャップを閉じるために、AP 間の距離を狭めたり、最低データ速度を下げたり、送信出力を上げたりしていました。

しかし、802.11n の出現により、一筋縄では行かなくなり、複雑さが増して、理解することが難しくなりました。RF の基本的な課題のひとつである多重反射を克服するために、IEEE は多重反射の建設的干渉を活用してこのやっかいな問題を解決する仕組みを規格に組み込みました。しかし、その結果、信号到達範囲のパターンは、マップ上の円というよりは、まるでロールシャッハ テストのような形になりました。AP 送信出力を増加させると信号到達範囲を広げることはできますが、各 AP が設置されている場所の環境によって多重特性が異なるため、信号にばらつきが生じました。このため、サービス提供範囲の計画が複雑さを増し、現場の調査が大変重要になりました。

第 6 の誤った通念を真に理解するためには、「信号到達範囲」という用語を最初に定義する必要があります。可能な定義は 3 つありますが、「信号到達範囲」の意味として適切なものはどれであるかは、あなたが決めてください。

1. 「信号到達範囲」とは、デバイスから WiFi ネットワークが見えることである。
2. 「信号到達範囲」とは、デバイスから WiFi ネットワークが見え、そのネットワークに接続できることである。
3. 「信号到達範囲」とは、デバイスから WiFi ネットワークが見え、そのネットワークに接続でき、安定してアクセスできることである。

さあ、どれでしょう。申し訳ありませんが、実は、あなたに決めていただくことはできません。「信号到達範囲」の定義は 3 番です。

WiFi 「信号到達範囲」は、デバイスから WiFi ネットワークに安定してアクセスできるのでなければ、信号到達範囲とは言えません。また、AP の送信出力を上げると AP がデバイスにデータをより安定して送信できる可能性は高まりますが、デバイスから AP がデータを受信できる可能性が高まるかどうかとはまったく無関係です。これは、AP の送信出力を上げてもデバイスの送信出力は上がらないからです。そして、AP とデバイスの両方の送信出力を上げなければ、(3 つ目の定義で言うところの) 真の信号到達範囲は向上しません。(実際は、より強力な AP に接続された場合に送信出力が低下してしまうデバイスもあり、この場合は信号到達範囲が狭まります。極めて強力な信号を検出したデバイスは、当然のことながら、電池の寿命を延ばそうとして送信出力を下げます)。

警告 : ラッカス マーケティングコンテンツ

デバイスよりも強い送信出力を持つ AP がある場合は、AP の受信感度がデバイスの受信感度よりも高い場合に限り、信号到達範囲の向上が望めます。ラッカスの AP は、WiFi ビジネスで最高の受信感度を誇ります。このため、他の殆どのベンダーの WiFi では、AP 送信出力を 14 ～ 17 dBm の範囲に設定したときに動作が最適になりますが、ラッカスの AP は AP 送信出力を 19 ～ 20 dBm にまで高めても最大の効果を得られます。

AP の受信感度をどのように向上させたかをお教えすることはできませんよ。それは当社の企業秘密です。しかし、証明することは簡単です。ラッカスの AP を他社製品と比較してみてください。ラッカス AP は聞く力に優れているため、接続とデータ送信を、ずっと離れた場所から行えます。ラッカスの受信性能は決して他の追随を許しません。

#7 パスワードベースの WiFi ネットワークはセキュアである

かつては贅沢であった WiFi ネットワークは一般的なものになり、WiFi 接続の価値は何倍にもなり、eduroam のような常時接続の方向に向かっています。一方、デバイスの数と種類は拡大の一途をたどり、学生、スタッフ、ゲストが最初から円滑に接続を確立することは難しくなっています。

パスワードベース (PEAP、TTLS) のネットワークでは、パスワードが変更されるごとにユーザーへのサービスが中断されます。切断されたデバイスがネットワークに再度接続を試みることによる認証要求の回数は、学生 1 人に換算すると 1 日 30,000 回にも及びます。

ヘルプ デスクへの対応の平均 20% ～ 50% は、パスワードのリセットを求めるものです。高等教育機関の WiFi におけるこのやっかいな課題に対するソリューションは、長い間利用可能でした。それは、EAP-TLS を使用する WPA2-Enterprise という証明書ベースの WiFi です。

証明書を使用すると WiFi でパスワードが不要になります。つまり、パスワードがデバイスにキャッシュされたり、接続を試みるたびに送信されたりすることはなく、パスワードが変更されても接続は途切れません。基本的に、一度登録したデバイスは、中断なしに一年中動作し続けることになります。

これによってユーザーの満足度が高まり、サポート チケットの数が減ります。

警告 : ラッカス マーケティングコンテンツ

セキュリティがこれほどまでにシンプルであれば、訪問者にセキュリティ保護されていない WiFi の利用を強要する理由はありません。弊社の Cloudpath Enrollment System (ES) では、あらゆる訪問者にセキュアな WiFi を、驚くほどシンプルに提供できます。Cloudpath ES は、従来のゲスト サーバーと異なり、IT の関与なしに WPA2- エンタープライズ ワイヤレス ネットワークにゲストをオンボーディングします。

面倒なウェブ ログインやセキュリティ保護されていないワイヤレスを利用する心配は無用です。訪問者、ネットワーク、
そして評判は、すべて保護されます。

Cloudpath Enrollment System は、スポンサーシップや自己検証など、さまざまな従来型認証・承認オプションを提供します。従来の機能以外に、Cloudpath ES は、業界初となる、セキュアな WiFi と Google、Facebook、LinkedIn などの外部 ID サービスとの統合により、特許を取得しています。

#8 すべてのアクセス ポイントは同じように設計されている

多くの購買部長にとって、WiFi は単なる WiFi です。ユーティリティであり、1 つのアクセス ポイントは別のアクセス ポイントと変わりません。苦情に対応し、問題のトラブルシューティングを行うスタッフは、そうでないことを知っています。しかしここには、半分の真実があります。大手ブランドのエンタープライズ AP はすべて標準のチップセットに基いており、多くが OEM リファレンス デザインを採用し、IEEE 802.11 規格に準拠し、WiFi アライアンスによるテストで相互互換性が証明されています。

しかし、標準のその先に改善の余地はあるのでしょうか？

では、典型的な大学のキャンパスと、導入の影に潜む固有の課題について見ていきましょう。

WiFi の課題はキャンパス全体に及ぶ

キャンパスの敷地 - 学生やスタッフは最新の優れたデバイスで、ますます多くのクラウド アプリケーション、オンライン データ ストレージを使用するようになっています。彼らは、いつでもどこでも最大の信号強度を確保できることをキャンパス WiFi ネットワークに期待しています。これを達成するには、ポイントツーポイント ブリッジング、メッシュ ネットワーク、堅牢な屋外 AP ハードウェアと取り付けオプションが必要です。

スタジアム - 友人や家族、ソーシャルメディアとつながったままでいることは、ファン体験の一環です。スタジアム用に設計された AP は、チャンネル プランニングと実装に役立つように、高密度に対応し、干渉を抑制し、屋外用に耐性が高められ、セクター化されたアンテナが内蔵されています。

学生寮には、すべての最新ガジェットや、スマート TV、ワイヤレス プリンター、Blue-ray プレイヤーなどの WiFi 対応一般電子デバイスが集結しています。さらに今日は、スマート ウォッチ、フィットネス トラッカー、そしてメガネなどのウエアラブルも！こうした硬化コンクリートの建造物の中で WiFi が動作するには、室内用の壁取り付け型 AP が WiFi 信号を至近距離で学生とデバイスに配信できなくてはなりません。

警告 : ラッカス マーケティングコンテンツ

ラッカスはそのさらに先を行きます。弊社のエンジニアは 802.11 規格を基礎とし、AP がどこに導入されてどのように使用されるかに応じて、基盤設計、アンテナ設計、そして工業デザインを最適化します。すべてのアクセス ポイントは同じように設計されているわけではありません。あるベンダーの製品は他社の製品とは異なります。

もちろん予算は重要な検討事項ですが、常に最安値のオプションを選択することは合理的ではありません。要件を満たすソリューションを選択することが重要なのです。

#9

ブロードバンドを増やせば大部分の問題は解決する

確かに、公平に言うならば、これは完全に誤った通念ではありません。ブロードバンドが増えて嬉しくない人はいないでしょう。iPad で速度テストを行ったときにダウンロード速度 100Mbps と表示されたら、その学生はスクリーンショットをキャプチャして Instagram や Tweet に投稿すると思いませんか？

そうは言っても、IT に寄せられる低品質 WiFi に関する苦情のうち、最も多いのはもちろんブロードバンド接続が遅いことです。毎秒何百メガバイトというローカル接続速度をデバイスで利用できるようにする地上最速の WiFi ネットワークがあったとしても、インターネットの分散またはバックホールが十分でなければ、這うような速度になってしまいます。講堂で一握りの AP を使用して何百人もの学生に接続を提供し、その状態を保ちながらエアタイム フェアネスを確保することが困難ならば、100Mbps のインターネット接続でも遅すぎるくらいです。WiFi は遅く安定性が低いと感じられます。WiFi に直接は関係ありませんが、もうひとつの大きな問題は、有線ネットワークの設計そのものです。WiFi ネットワーク接続の爆発的増加に対応できるよう適切に構成されていない、DHCP や DNS などのルーティングおよび高レイヤー機能は、ネットワークの大惨事を引き起こす可能性があるにもかかわらず、WiFi の問題であると見なされています。

しかし、IT プロフェッショナルにとって、ワイヤレス ネットワークの管理と苦情への対応は、ブロードバンドを提供するだけは済みません。最終的には学生の体験に尽きるのであり、おぞましい「#campuswifisucks」ツイートを断ち切って、学長が CIO を叱り、CIO が IT ディレクターを責め、IT ディ

レクターがネットワーク エンジニアに「修正せよ」と命令するような事態を避けなくてはなりません。「問題」は、オンボーディングとパスワード、Bonjour からのネットワーク ストーム、学生寮内での干渉、講堂での不十分な容量、個室への不十分な信号到達などは、すべて、提供される帯域幅と無関係です。

ここまででキャンパス WiFi に関する 9 つの誤った通念を見てきました。これであなたは WiFi を最適な状態に高めることができます。大量の資金をつぎ込まずに WiFi の利点を最大限に活用するための道が見えてきましたね。

そのためのアップグレードを探すときは、「百聞は一見にしかず」の心構えでサプライヤーを試してください。

パフォーマンスには大きな意味があります。そして、誤った通念に関する新たに獲得した知識を使って適切な質問をし、十分な情報に基づいて決定を下すことができます。ネットワークを将来も使い続けられるようにし、最新世代の学生に、壁のない瞬時アクセスを提供してください。

ラッカスワイヤレスジャパン合同会社
〒 103-0027 東京都中央区日本橋 1-18-14
クローバー日本橋ビル 4F
japansales@ruckuswireless.com

Ruckus
Simply Better Wireless.
www.ruckuswireless.com