Part3 知ってるつもり？

ワイヤレスLAN環境構築の落とし穴

シスコシステムズ合同会社
前原 朋実 *Maehara Tomomi*
パートナー・ビジネス　パートナー・システムズエンジニアリング
シニアシステムエンジニア
李 奇 *Richard Li*
ボーダーレスネットワークシステムズエンジニアリング
シニアシステムエンジニア

快適なワイヤレス（無線）LAN環境を構築するためには、多面的に考察することが大事です。本章では、無線LANアクセスポイント製品を選ぶときのコツ、そしてユーザ管理の方法や、実際に導入するときに見落としがちなポイントを紹介します。

無線LAN環境の利用が向いている業務、向いてない業務

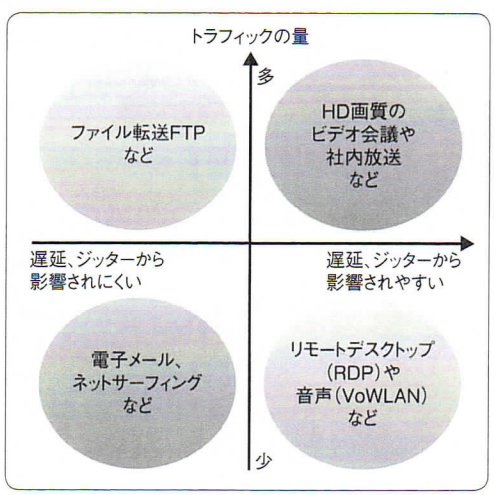
正しく無線LAN環境を設計していますか？

たとえ無線LANといえども、ネットワークですから、企業内の業務で生じるトラフィックの特徴がわかれば、注意すべきポイントが見えてきます。

分類するために**図1**のように簡単なマトリックスを作ってみました。縦軸はトラフィック量を示し、横軸はトラフィックが遅延やジッターなどに敏感かどうかです。

遅延とは名前のとおりパケットの到着が遅れることです。ジッターは、パケットの到着時間にバラつきがあることです。たとえば、1番目のパケットは10ms（ミリ秒）で到着したのに、2番目のパケットは何らかの理由で1000msがかかって届くといったことが挙げられます。

▼図1　ワイヤレス環境の利用が適しているか否か？



●マトリックスで考える無線LAN

では、図1のマトリックスにどんなトラフィックが当てはまるかを見ましょう。たとえば、FTPでファイルをアップロード／ダウンロードする場合、トラフィックの量は多いですが、パケットに多少遅延があってもあまり気になるものではありません。メールやWebサーフィンの場合も同様です。

しかし、RDP（Remote Desktop Protocol）の場合は、そのトラフィック自体は重くないですが、遅延が問題になります。遅延が発生すると、マウスを移動させても画面上にすぐ反映されなくなり、いろいろな操作の時間がかかり、ストレスが溜まります。

また、IP電話（Voice Over IP）を導入する会社が年々増えています。その延長として、無線LANで実現できるVoWLAN（Voice Over WLAN）も、さまざまな会社で検討され始めています。音声データの場合、RDPと同様にトラフィックは重くないですが、遅延やジッターがあると、相手の音声がいつも遅れて聞こえてきたり、急に途切れたりして会話に障害が出ます。

●帯域も用途に合わせて変更していますか？

1つ注意してほしいのは、オフィスの環境では通常複数の業務が共存していることです。無線LANでファイル伝送サービスを利用しながら、VoWLANも利用するケースも少なくありません。その場合はトラフィックの特性を考慮し、それぞれの帯域を分けて使う方法があります。ファイル伝送は2.4GHz帯を使い、音声トラフィックは5 GHz帯で使うというものです。また、状況によっては、企業で独自開発した無線端末や業務アプリケーションもあります。それらのトラフィックの特徴、そしてほかの端末やアプリケーションへの影響を事前に確認しておく必要があります。

●無線LANのほうがセキュア！

企業での機密性の高い情報を無線LANに流していいのかと、心配されている人もいまだにたくさんいます。電波が漏れるからセキュアじゃない、という主張も昔から多くあります。MAC認証やWEP暗号化方式は、MACアドレスは簡単に改ざんできるし、WEPも脆弱性があるので簡単に解読できます。確かに無線LANがセキュアではないと思われてもしかたありません。

しかし、それは遠い昔のことです。今はEAP(PPP Extensible Authentication Protocol：拡張認証プロトコル／IEEE802.1X)で証明書やユーザIDなどを使い、正しく身分が証明されて、初めて無線LANに接続できるようになっています。もちろん無線空間で流すデータもしっかりAES(Advanced Encryption Standard)で暗号化されています。

さて、逆に有線ネットワークを見てみると、認証と暗号化をしているでしょうか。この意味で無線LANは有線よりセキュリティが高いとも言えます。そもそも、暗号化方式ではAESにしないと、802.11nは動作せず高いデータレートが実現できません。

また、ほかのレイヤでも認証・暗号化がきちんと行われているので(たとえば、https)、ネットワーク全体のセキュリティは、昔と比べて飛躍的に進歩しています。正しく認証スキームを構築し、強固なAES暗号化方式を利用すれば、セキュアになります。

あなたの知らないアクセスポイント選択のコツ

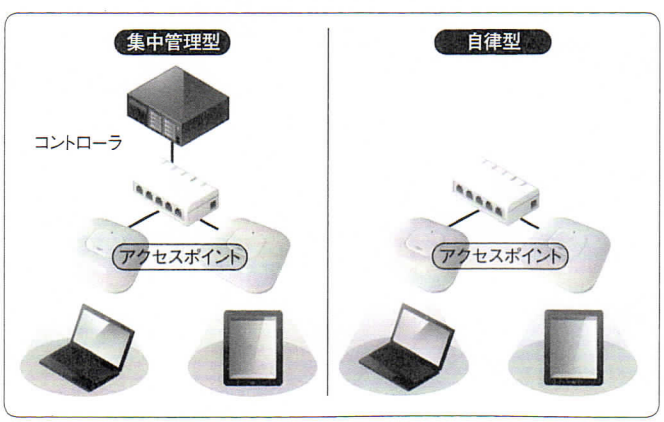
コツその1「自律型 vs. 集中管理型」

企業向け無線LANのしくみとして、まずは「自律型と集中管理型」がキーワードです。自律型は、分散管理型、Autonomousとも言いますが同じ意味です。現在の企業向け無線LANの主流は集中管理型です。その違いは、**図2**に示すように無線LANのアクセスポイントをコントロールする機材が他にあるかどうかです。コントローラと呼ばれるハードウェアなどでアクセスポイントが一括管理・コントロールされるのが集中管理型、自律型は読んで字のごとく何にもコントロールされずスタンドアローンでこなすタイプです。

●その違いがLAN環境の効率に影響

集中管理型では、コントローラと呼ばれる機材(もしくはアプリケーションソフトウェア)が、

▼図2　アクセスポイントは、集中管理型と自律型に分類される



アクセスポイント本来の機能に余る処理を行います。コントローラは、次の処理を担います。

・セキュリティ
・QoS
・ポリシー適用

とくにポリシー適用は、リアルタイム電波環境管理で最も重要な処理です。

一方、アクセスポイントは、次のようなタイミングが重要とされるアクティビティを処理します。

・ビーコンの処理
・端末とのハンドシェーク

つまり、コントローラとアクセスポイントが役割分担することにより、処理能率が上がるのです。たとえば、1台ですべてこなす自律型に比べ、集中管理型はリアルタイムアプリケーションの安定性に欠かせない「ファーストローミングの切り替え時間が各段に短くなる」などのメリットが生まれます。コントローラが必須です。

●集中管理型のメリット①
――設定が容易になる

役割分担をすることで導入時・運用時に管理者が「楽」になるというメリットがあります。1つは、アクセスポイントをネットワークに接続するだけで自動的にサービス提供を始める「ゼロタッチコンフィギュレーション」です。アクセスポイントは、ネットワークに接続されると、ネットワーク上のコントローラを自分で見つけてきて、そこからOSや設定などをダウンロードします。DHCPサーバがあるならば、アクセスポイントにケーブルを挿したら、ダウンロードが完了するのを待つだけです（もちろん最初にコントローラの設定をします）。

これが自律型の場合、ひとつひとつ自力で設定することになります。数が増加すればするほど、それがいかにたいへんかは想像に難くありません。

●集中管理型のメリット②
――電波環境の自動調整

もう1つの「楽」ポイントは、電波環境の自動調整です。

・チャネルを変える
・電波出力を上げる／下げる

これらの機能により、チャネルが干渉したら切り替える、ほかのアクセスポイントの故障などにより電波が届かなくなった個所を検出したら、周りのアクセスポイントが出力上げる、逆にお互いの出力が強すぎれば下げる、といった調整がされます。これは複数のアクセスポイントから集めた情報をもとにコントローラが定期的に自己判断します。

故障は想定範囲外で、最初にサイトサーベイをするのだから必要ないのでは？――隣の会社が導入すれば、干渉する可能性が出てきます。また、レーダーなどの干渉源によって、いつ影響を受けるかもわかりません。

●集中管理型のメリット③
――運用コストの削減

ただし自動調整機能は、実績あるメーカーのものを選んだほうが良いでしょう。未熟な製品の場合、かえって悪くなることもあります。不安定になったり、調整タイミング間隔が長すぎて意味をなさないこともあり得ます。

複数のアクセスポイントが、コントローラによって一括でコントロールされることでゼロタッチコンフィギュレーションや電波環境の自動調整といった自動化が可能になります。アクセスポイントを増やす、減らす、設置場所を変える、といったあとあとの変更も管理者は簡単にできるようになるので運用コストも下がります。そのため集中管理型を選ぶ企業が増えています。

コツその2「2.4GHz＋5GHzデュアルバンド対応か？」

●2.4GHz帯だけで十分か

2.4GHz帯を利用するIEEE 802.11gと5GHz

帯を利用するIEEE 802.11aは規格上同じ通信速度の54Mbpsです。IEEE 802.11nは2.4G/5GHz帯のどちらでも使えます。また2.4GHz帯(b/g/n)だけに対応しているアクセスポイント製品が安い場合も多いので、2.4GHz帯だけでかまわないと考えていませんか。

無線LANが使える周波数帯は、それ専用ではありません。テレビや携帯電話網のように特定の会社専用というものでなく、簡単なルールを守れば誰でも使用可能な周波数帯です。そのため、とくに2.4GHz帯はBluetoothや電子レンジなど無線LAN(WiFi)ではない製品も多く利用します。さらにコンシューマ向けPCやスマートフォンの多くは2.4GHz帯しかサポートしていないため、利用者が多いのです。「2.4GHz帯は汚れている、混雑している」とよく言われるのはこのためです。それに対して5GHz帯は比較的きれいです。2.4GHz帯だけを使うのはあまりお勧めできません。

● 2.4GHz帯のデメリット、5GHz帯のメリット

また、2.4GHz帯は同時に使えるチャネルが3つしかありません。これに対して5GHz帯は最低でも4つ、最高で19チャネルが使えます。チャネルが多ければ多いほど、アクセスポイント同士の干渉が減るので、セル設計が楽になります。

5GHz帯のチャネル数は「W52, 53, 56」という表記で判断できます。W52が4チャネル、W53も4チャネル、W56は11チャネルです。また、W56は屋外でも利用できますので敷地内の建物間なども無線LANを敷いて、屋内・屋外関係なく使えるなど利用法が広がります(もちろん、2.4GHz帯でも屋外で利用可能です)。

● 帯域ごとに振り分けをしてますか？

このように多くのメリットがある5GHz帯ですが、2.4GHz帯しかサポートしていない端末が5GHz帯を使うというウルトラCはできません。ですので、端末ごとに振り分けることを検討してください。スマートフォンは2.4GHz帯対応がほとんどですが、PCやタブレットは5GHz帯に対応しているものが多いです。

振り分けをすると、結果として1つの周波数帯に端末が集中しないので、余計な混雑も避けられます。ただ振り分ける方法をあれこれ考えるのは面倒です。たとえばシスコ製品ならば、バンドセレクト機能を使用すれば、2.4/5GHz帯両サポート端末は優先的に5GHz帯で接続できます。

コツその3「接続ユーザ数だけで決めていませんか？」

● メーカーの公表値は当てにならない

「1アクセスポイントあたり何ユーザまで可能か」という質問をよく受けますが、あいまいに答えざるを得ません。なぜかといえば、どのように無線LANを利用するかでその数は大きく異なってくるからです。また、安定性にもつながる無線LAN品質の最低ラインをどこにするかというメーカーの考え方もあるので、一概にメーカーが回答するサポートユーザ数が多ければ良いわけではありません。今後、スマートフォンのようなWiFi対応端末はどんどん増えていくので、1人で複数の端末を持つのが当たり前になってきます。そのため、ユーザがどのようなWiFi端末をどれだけ所有しているのかを把握し、端末ベースで設計していく必要があります。

● 干渉源に強いかどうか

それ以外にも、無線LAN最大の敵「干渉源」に対処できる機能を持ったアクセスポイントや、端末などの場所を表示するシステムやセキュリティ面で重要なWireless IPSのシステムの一部としてのアクセスポイントがあります。

無線LANがどこでも普通に使われるようになったからこそ、企業では無線LANの安定性やコンプライアンスを含めたセキュリティ面が重要な検討課題となっています。とくにネットワーク利用が当たり前な今、安定性は大前提です。有線と同じに使えることが期待されています。

単につながればよいという時代ではありません。

コツその4「無線LANはすべて規格どおりではない!」

●メーカーの独自実装もチェックしていますか

無線LANには、a/b/g/n以外にも多くのIEEE規格が存在します。それだけでもう十分と思うかもしれませんが、メーカー独自の実装も存在します。IEEEに提案した規格なのに結論が出ないため、似たしくみで先にリリースする場合や、規格だけでは物足りず、機能を追加する場合などがあります。

コツその5「アクセスポイントとクライアントとの相性もある」

●WiFi認定の落とし穴

IEEEの規格には、オプション部分があり、IEEE 802.11nが相当します。そのせいで同じIEEE 802.11n対応とうたっていてもアクセスポイントにより実装がかなり異なります。さらに、メーカー間の相互接続性を確認するWi-Fi Allianceという組織がありますが、ここでIEEE規格のオプションを含めた全機能の相互接続性を確認しているわけではありません。そのため、あれだけ規格がそろっていて、WiFi認定と表示されて同じアクセスポイントを使っても、端末が異なると動作が違うことがよくあります。

●機能比較表だけではわからない

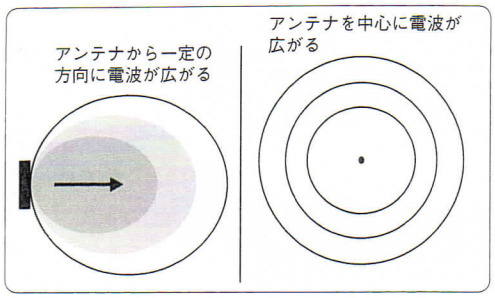
IEEE 802.11nの場合だと、端末によってスループットが違ったり、逆もしかりで、同じ端末なのにアクセスポイントごとにスループットに差がある場合があります。スループットだけなら良いですが、一規格の中のいくつかの機能をアクセスポイント・端末のどちらかが実装しておらず、結局その機能が使えなかったという場合もあり得ます。

コツその6「アンテナは内蔵か外付けか?」

●設置場所のほうが大事です！

メーカーによってはアンテナが内蔵タイプと外付けタイプのアクセスポイントを用意しています。どちらが良いかはケースバイケースです。内蔵タイプはアンテナが動かせないので、どこにどう置くかで決まります。また、アクセスポイントそのものがアンテナですので、丸ごと天井の表側や壁に設置する必要があります。その代わり、多くの場合見た目がすっきりしていて天井の表側に設置しても目立ちません。

▼図3　指向性アンテナ（左）と無指向性アンテナ（右）



●アンテナの指向性も応用

外付けタイプはアンテナを選べるというメリットがあります。アンテナには上から見るとアンテナを中心にして円を描くように電波を出す全方向性（無指向性）アンテナと特定の方向に電波を出す指向性アンテナがあります（図3）。指向性の場合、エネルギーを特定の方向に集中して長い距離を飛ばせますが、その分カバーする角度が狭くなります。これらのアンテナを組み合わせることで、外に電波が漏れないように細長い場所には指向性アンテナを配置するなど、きめ細やかな対応ができます。アンテナだけを外に出して、アクセスポイント自体は天井裏などに隠すといったことも可能です。また、外付けタイプはアクセスポイントの強度や密閉性を高め、工場などオフィスより厳しい環境に対応させている製品もあります。

無線LANのユーザ管理はどうしていますか？

アカウント管理だけでは対応できない現在

昨今のスマートフォンやタブレットの爆発的

な普及により1人で何台も無線LAN端末を持つようになりました。最近ではBYOD(Bring Your Own Device)とか私物解禁などの単語が飛び交っています。筆者の周りでもスマートフォンはもちろんのこと、打ち合わせの席にPCの代わりにタブレットを使う人が増えています。そのため、これまではユーザ単位での管理でも問題なかったのですが、これからは違ってきます。ユーザにとっては時と場所によって端末を選ぶことができるのはうれしいことですが、IT管理者にとってはたまりません。これらをユーザID単位で管理するのでは1ユーザのすべての所有端末が同じアクセス権を持つということになります。

セキュリティの観点から、PC以外の端末利用を制限してきた管理者からすると、ユーザの利便性を考えセキュリティをある程度犠牲にするか、利便性を無視してセキュリティを優先させるかという選択肢になりかねません。しかし、どちらもこの時代にふさわしい管理方法ではありません。

次世代管理はポリシーベースで

BYOD時代に向かって主流になっていくと思われる管理方法は、ユーザ単位だけではなく、端末の種類や場所などの情報をベースにその都度アクセスできる範囲を変えていく方法です。端末がネットワーク接続しようとするたび、管理ツールがこれらの情報を集めてアクセス範囲をインターネットのみ、社内ネットワークの特定のサイトはOKという判断をあらかじめ決めておいたポリシーベースで実施し制御するのです。実際にこのような製品はでてきていますが、その際、管理者にとって重要なのはこのポリシー作成になります。スマートフォンでもiPhoneかAndroidか、社内からの接続かVPN経由なのかといったよりきめ細やかな設定ができることが重要ですが、一方でゼロからすべてのパターンを作成していくのはたいへんな作業です。そのため、あらかじめポリシーのテンプレートが豊富にあるほうが使い勝手はよくなります。また、これらの接続は無線LANからとは限りません。スマートフォンやタブレットに気を取られて無線LAN側だけでこのような管理を進めても、効果は半減します。有線・無線アクセスをトータルで考慮する必要があります。

端末そのものの管理も重要です。PCと同じようにOSなどのバージョン管理、セキュリティの観点から一部アプリケーションのダウンロード禁止といったことから、紛失時の情報漏洩を防ぐために遠隔からデータを削除したりロックをかけたりする必要もでてきます。これらはMDM(Mobile Device Management)と呼ばれるツール／サービスで利用できます。

通信速度と安定性、どちらを選びますか？

通信速度はインフラだけでは決まらない

ほんとうに300Mbps出ますか？

ネットワークを構築するときに、通信速度を評価基準にするケースが多いです。無線LANの場合も同じです。とくに802.11nが普及し、すべてのメーカーが300Mbpsを広告するので「高速」ばかり注目されます。そして、802.11nのアクセスポイントを購入したら、一気に300Mbpsで通信できると思ってしまいます。

しかし、無線LANの場合、通信速度はインフラだけでは決められないのです。ユーザの利用するクライアント／端末に依存していることを忘れてはなりません。たとえば、iPhoneやGalaxyなどのスマートフォンの場合、端末のサイズや電池時間などの制限があって、802.11n対応と言っても、最大72Mbpsのデータレートしかサポートできません。その場合300Mbpsは無理でしょう。

遅い端末で通信速度が低下する！

また、無線LANの場合、端末が同じ周波数資源を共有しているので、従来の802.11a/b/g規

格のクライアント端末が混在すれば、802.11nクライアントもそれに引っ張られ、システム全体のパフォーマンスが低下する場合もあります。

つまり、通信速度はインフラだけではなく、クライアント端末のスペック、クライアント端末の割合(802.11n vs. 802.11a/b/g)に依存するこ

Column

干渉源は、どのように影響するのか？

○電子レンジ、Bluetoothも干渉源

無線LANの敵「干渉源」。それはいったい何でどんな悪さをするのでしょうか。干渉源には、大きく分けて3種類あります。1つはWiFi干渉源。これはWiFi機器であるアクセスポイントです。2つ目はレーダー。気象レーダーや船舶レーダーなど、普段の我々の生活ではみないものですがこれも干渉源になります。最後にNon-WiFi干渉源です。WiFi認定を取っていない(取る必要のない)製品群、たとえばBluetoothや電子レンジなどです。

○アクセスポイントの電波干渉

まずはアクセスポイント同士の電波干渉について。隣り合うアクセスポイント同士が同じチャネルを使っている場合に発生します。また、アクセスポイントですので2.4GHz帯／5GHz帯両方で考慮しておく必要があります。

WiFi同士の場合、同じタイミングで電波信号を送り打ち消しあうことを防ぐために、譲り合いの精神が組み込まれています。電波信号を出したいときにその空間が空いているかどうかを確認し、空いていれば電波信号を出します。一方別のWiFiはほかから電波信号が出ている間はひたすら待ち、しばらくして空いているかどうか再確認し空いていれば送信、ダメならまた我慢する、というしくみです。これをCSMA/CAと言います。端末が増えれば増えるほど、ほかの機器に空間を占拠される確率が上がるので、この我慢の時間が長くなります。つまりスループットが落ちるわけですが、2つのアクセスポイントが干渉していると、1つの空間に存在する端末が2倍になり我慢の時間が2倍になる、つまりスループットが半分になってしまうのです。2.4GHz帯では使えるチャネルが実質3つのため、アクセスポイントが4つ以上になると気を付ける必要があります。5GHz帯ではこの設計が楽になると書きましたが、使えるチャネル数が多いためあまりこのWiFi干渉を気にする必要がないからです。

○レーダー干渉源

次に気象レーダーや船舶レーダーなどのレーダー干渉ですが、これは5GHz帯のW53とW56と呼ばれるチャネルに影響します。このレーダーに無線LANが悪影響を与えないようアクセスポイントへの「DFS」というしくみの搭載が義務付けられています。これは、レーダーが出ていないかをアクセスポイントが常に監視し、検出した場合は即座に通信をストップしてほかのチャネルに移動するのです。さらに、レーダーを検出したチャネルはその後30分間使えないようになっています。ここではレーダーが最優先になるのです。

○Non-WiFi干渉源

最後に無線LANにとって最も厄介な干渉源がNon-WiFi干渉源です。これらには、WiFi干渉源で書いた譲り合い精神がありません。WiFiの規格にのっとっているわけではないので当然ですが……このエリアは、電子レンジ、Bluetooth、コードレスフォン、無線カメラ、無線マウスなど種類も多く、今後も増えていくかもしれない未知の世界です。また、それぞれの動きは同じではありません。1つのチャネルをずっと占拠して無線LANの通信がまったく入り込めないものや、チャネル間をホップして、ちょっとずつチャネルを間借りしながら空間リソースを使うものなど、どれだけ無線LANに影響するのか、またはあまり影響がないのかは調べてみないとわからないのです。また、1つだけならたいした影響がなくても、多くの人が使えば厄介者になる可能性は十分にあります。

とを理解しないといけません。

ビームフォーミングで802.11a/b/g端末もスピードアップ!

ビームフォーミングのしくみ

802.11nのネットワークを導入しても、ユーザの利用する端末を一度に802.11n対応に入れ替えわけにはいかないでしょう。そのため、既存の802.11a/b/gクライアントにも802.11nのメリットを享受させられればとても魅力的です。

802.11nでは、MIMO(Multiple Input Multiple Output)という技術を利用して、複数の送受信機(アンテナ)を利用して電波を送っています。クライアントからの信号を複数の受信機で受信するので、それぞれの受信信号の位相の違いを利用し高い確率でクライアント端末の方向を推測できます。その情報を活用して、送信するときに複数の送信機から出す信号に位相差を付けて送ります。その電波信号がクライアント端末に届いたときに、同じ位相になって、高い受信レベルを維持できます。つまり、電波の一番強い部分を端末がいる場所で重ね合わせるよう調整するのです。これをビームフォーミングと言います。高い受信レベルを維持できれば、高いデータレート、つまり高い通信速度が実現できます。802.11nのクライアントにも効果がありますが、802.11a/b/gの端末にも効果があります。このようなビームフォーミング技術を利用することによって、低速クライアント端末による通信速度の低下を改善できます。

セルを小さくして通信速度向上

通信速度はアクセスポイントとクライアント端末との距離にも依存します。アクセスポイントと端末が離れている場合、お互いに受信レベルが低くなり、通信に低いデータレートしか使えなくなります。つまり、アクセスポイントの届く距離と実際の通信速度がトレードオフ関係になります。

高い通信速度を維持したい場合、アクセスポイントをさらに密に配置し、アクセスポイントごとのカバレッジを狭く絞る必要があります。アクセスポイントの出力レベルを低く抑えて、カバレッジを狭く絞るメリットはもう1つあります。セルが狭くなれば、同じ周波数資源をシェアするクライアント端末の数も減り、それぞれの端末が高いスループットを得られます。

安定性を忘れてはならない!

ネットが不安定になる原因とは？

無線LANの場合、安定性こそ高速通信技術を活かす重要なポイントです。アクセスポイントの近くで300Mbpsのデータレートを得られても、少しアクセスポイントから離れると、激しく劣化したり、安定せず通信が切れたりすることは論外です。

そうは言っても、802.11nの技術で無線LANの安定性もかなり改善されてきて、昔のように端末を少し動かしたら通信速度が激しく落ちるとか、切れたりすることはほとんどなくなりました。では、無線LANの安定性を脅かす原因はどこにあるのでしょうか。

思わぬ電波の干渉

ほとんどの場合は、電波の干渉です。1つにはWiFi信号の干渉です。自社の設置したアクセスポイントから発した電波の干渉や、周囲の会社の設置した無線LANからの電波干渉などが考えられます。WiFi信号からの干渉に関しては、前述したように電波の自動管理機能でお互いの干渉を最小限に抑えて、システム全体の最適化ができます。

一方、Non-WiFiの干渉からの影響は今まで以上に注目されています。無線LAN、とくに2.4GHz帯を利用する場合、同じ周波数帯域を利用するほかの端末も多くあります。たとえば、Bluetooth、コードレス電話そして電子レンジなどが挙げられます。それらのデバイスから発する電波が無線LANの信号に干渉を与えて、通信パフォーマンス低下につながります。さらに、常に電波を発するNon-WiFiの無線監視カメラ

などが周囲に存在すれば、WiFiの無線信号が完全に遮断されて、クライアント端末の接続が切れる事態も発生し得るのです。それらの干渉デバイスの存在が無線LANにとっては不安要素です。そういう意味では、無線LANを構築するときに、己を知るだけではなく、敵(Non-WiFiの干渉源)を知る必要もあります。

● 主動的(Proactive)対応で問題解決

数年前にシスコはアクセスポイントに専用のスペクトラムアナライザチップを載せて、干渉源を検知・回避する機能を実装しました。受信した電波を専用のチップで解析することによって、どんな干渉源が存在して、その干渉電波からどれくらい影響を受けるのかを高い精度で把握できます。今まで検知できなかったNon-WiFiの干渉源を見える化することによって、初めて無線LANで安定した高いパフォーマンスを維持できるようになります。

また、特定の干渉デバイスが現れた場合、直ちに無線LAN管理者にその存在を通知し、位置を特定する機能もあります。これにより干渉によって、安定性が劣化しスループットが低下する前に、主動的(Proactive)に対応できます。

ほかの無線LANベンダもそのトレンドに追従して、各社のアクセスポイントに干渉検知機能を実装し始めていますが、ソフトウェアで電波の処理を行うので、専用チップを利用するケースと比べて検知の精度が劣るようになり、スループットに影響を与えるのではないかとの懸念が残ります。SD

Column

SSID数とスループットの関係をご存じですか？

無線LAN選定のRFPによく「SSID数は16個」などと書いてあります。ただし、SSIDが多ければ多いほど良いということではありません。SSIDが多くあれば、それなりにビーコンパケットやProbe Responseパケットが多く送信されます。ビーコンやProbe Responseは遠くまで飛び、多くのクライアント端末に届けるために、最も低いデータレートで送信されます。低いデータレートで送信されるパケットが多ければ多いほど、高いデータレートの通信がかなり足を引っ張られ、全体的な通信速度が低下してしまうことになります。

ですから、高速通信を望んでいるなら、SSID数を最低限に抑えることが必要ですね。

Column

低いデータレートを無効にしていますか？

無線LANの通信で利用するデータレートはさまざまです。一般的に1 Mbps、2 Mbps、5.5 Mbpsなどの低いデータレートを無効にすることを推奨しています。低いデータレートを有効にする場合、左記コラムでも述べたようにビーコンなどのパケットがそのデータレートで送信されてしまいます。それはとても効率の悪いことです。たとえば、250バイトのビーコンを送信するために、1Mbpsのデータレートなら2096 μs(マイクロ秒)かかりますが、6Mbpsなら353 μs、さらに24Mbpsのデータレートを使うなら、103 μsしかかからないのです。低いデータレートを無効にして、高いデータレートだけを使えば効率が良いことがわかります。

また、低いデータレートを有効にする場合、端末が遠いところに移動しても、新しいアクセスポイントにつなぎ直さず、前のアクセスポイントに低いデータレートで通信を維持することがあります。せっかく近くにほかのアクセスポイントがあり、それにつなげば高い速度で通信できるのに、前のアクセスポイントを忘れられず、引っ張られてしまいます。そんな状況を防ぐために、低いデータレートを無効にするのは有効です。

もちろん端末との相性を事前に確認しないといけないですが、一般的に12Mbps以下のデータレートを無効にすることをお勧めします。