

# WI-FI ネットワークの保護

DAVID COLEMAN & NEIL DIENER



DAVID COLEMAN および NEIL DIENER 共著

## レイヤ 1 に潜むセキュリティの脅威

### 概要

企業での Wi-Fi の使用が一般的になるにつれて、Wi-Fi インフラストラクチャを構築するための標準的な 3 段階プロセスも確立されてきました。第 1 段階では、特定のサイトの調査を行って、アクセスポイントの最適な数と位置を決定します。第 2 段階では、アクセスポイントおよび他の Wi-Fi 機器を展開し、最適なパフォーマンスが得られるようにネットワークを微調整します。

第 3 段階では、従来のワイヤレス用 Intrusion Detection System (IDS; 侵入検知システム) や Intrusion Prevention System (IPS; 侵入防御システム) などのさまざまなセキュリティソリューションを使用して、ネットワークを継続的に監視します。

多くの人は、このような段階を踏むことによって、順調かつ安全な Wi-Fi 展開が可能であると考えています。ただし、そのように思い込んでしまうと、セキュリティの盲点を突かれる可能性があります。従来の展開プロセスおよび Wi-Fi セキュリティ製品で見過ごされているのが、OSI 参照モデルのレイヤ 1 である物理層です。有線ネットワークでは、レイ

ヤ 1 はトラフィックを伝送するケーブルなどの物理メディアで構成されます。Wi-Fi ネットワークでは、レイヤ 1 は電波のスペクトルで構成されます。

IPS や NAC などのセキュリティソリューションは、レイヤ 2 およびその上位のレイヤで動作します。

レイヤ 1 は完全に無視されています。しかし、レイヤ 1 は Wi-Fi ネットワークの基盤です。基盤であるがゆえに、物理レイヤに対する攻撃は、上位のレイヤに対する攻撃よりも壊滅的な結果を招くおそれがあります。

攻撃には、大きく分けて、「意図的でないもの」と「意図的なもの」の 2 つの種類があります。意図的でない攻撃は、免許不要のスペクトルを Wi-Fi と共有する一般的なデバイス (コードレス電話や Bluetooth デバイスなど) が発生源になります。

このスペクトルでは、電子レンジなどの通信用に使用されないデバイスからも RF が発生し、Wi-Fi 通信を妨害する可能性があります。

この種の RF 干渉により、Wi-Fi ユーザー側では、スループットが低下したり、遅延が増加したり、接続が切断されたりする場合があります。

意図的な攻撃において、悪意のあるユーザは、通常の PC とソフトウェアまたは独自の電波妨害装置を使用して、Wi-Fi 通信を妨害します。この種の攻撃では、Denial Of Service (DoS; サービス拒絶) と、ネットワークへの不正アクセスを可能にする侵犯が行われる可能性があります。

スペクトルの問題を解決するため、ネットワークエンジニアには、RF 干渉を検出および分類し、干渉を起こしているデバイスを特定するためのソリューションが必要です。

サイト調査ツールや Wi-Fi 機器そのものでこれらのタスクを実行することはできません。これらのタスクに適切なソリューションが、スペクトルアナライザです。

個々の独立したデバイスを検出、追跡、特定できる新しい種類のスペクトルアナライザが市場に流通するようになり、このような問題のトラブルシューティングが可能になりました。また、Wi-Fi ネットワーク展開の開始時に行うサイト調査でスペクトルアナライザを使用することにより、ネットワークの初期構築を強化でき、企業での使用に適したネットワークにすることができます。

# レイヤ 1 に潜むセキュリティの脅威

## Wi-Fi のセキュリティ上の懸念事項

WLAN では、実際は RF に関係するセキュリティの脅威についても考慮する必要があります。Wi-Fi データ セキュリティを突破しようとするプロトコルレベルの攻撃には、不正なアクセス ポイント、認証攻撃、Evil Twin アクセス ポイント、man-in-the-middle、Wi-Fi フィッシング、盗聴などがあります。これらの攻撃のほとんどは、OSI 参照モデルのレイヤ 2 に存在します。

認証、暗号化、セグメント化による適切なセキュリティ ソリューションを実装すれば、これらの広く知られている攻撃の多くは軽減できます。レイヤ 2 攻撃が発生したときは、レイヤ 2 セキュリティ モニタリング ソリューションを展開することもできます。

ところが、現在の Wireless Intrusion Detection System (WIDS; ワイヤレス侵入検知システム) ソリューションの大きな落とし穴は、レイヤ 1 に潜むセキュリティの脅威をこれまで検出できていないということです。

一般に、WIDS では 802.11 無線カードを使用しますが、このカードではレイヤ 1 の状況を把握する機能に制限があります。受信信号の強度やチャネル全体の Signal-to-Noise Ratio (SNR; SN 比) などのハイレベルなレイヤ 1 統計しかモニタリングできません。このように限られた機能では、詳細なスペクトル分析にはまったく不十分です。このため、モバイルまたはセンサーベースの WIDS ソリューションに含まれる 802.11 無線カードでは、レイヤ 2 のセキュリティ モニタリングとパフォーマンス分析しか行うことができません。この事実を踏まえたうえで、レイヤ 1 の適切なスペクトル分析とセキュリティ モニタリングを実行するために有効なツールは、本格的なスペクトル アナライザだけであることを理解する必要があります。

では、潜在的なセキュリティの脅威として存在するレイヤ 1 のリスクには具体的にどのようなものがあるのでしょうか。レイヤ 1 のセキュリティ リスクには、大きく分けて、検出不可能な不正アクセス ポイントと DoS 攻撃の 2 つがあります。これらについて、以下で説明します。

### 検出不可能な不正アクセス ポイント

ワイヤレス ネットワークで最も関心の高いセキュリティ リスクは、不正なアクセス ポイントのリスクです。不正な 802.11 デバイスは、多くの場合、802.3 イーサネット デー

タ ポートに接続されます。この接続によってどのような結果が生じるのかについては、接続を行った人自身ですら完全に理解しているとは限りません。問題は、不正デバイスがデータ ポートに接続されたことで 802.3 有線インフラストラクチャへの「入り口 (ポータル)」になったということです。

このことは、不正な無線デバイスに接続できる人であれば誰でも、ワイヤレス ポータル経由でネットワーク リソースを攻撃できることを意味します。WIDS ソリューションは、当初、不正なアクセス ポイントとデバイスを検出する目的で開発されました。このソリューションは、不正な Wi-Fi デバイスの検出に効果的であることが証明されているだけでなく、公表済みおよび未公表の数多くの終了方法によって不正デバイスを自動的に無効にできるように拡張されてきました。

問題は、WIDS/WIPS ソリューションのレイヤ 1 分析機能に制限があるため、特定の種類の不正アクセス ポイントを検出できないということです。WIDS/WIPS ソリューションに含まれる 802.11 無線カードは、それ以外の一般的な Wi-Fi 信号を認識するように設計されています。したがって、標準的な Wi-Fi プロトコルを使用する不正デバイスは、比較的すぐに検出されます (非標準的なセンター周波数で動作するなど、Wi-Fi を非標準的な方法で使用するデバイスは、簡単には検出されない可能性があります)。Wi-Fi 以外のプロトコルを使用するデバイスも検出されません。Wi-Fi 以外のプロトコルを使用する不正デバイスの例としては、Frequency Hopping Spread Spectrum (FHSS; 周波数ホッピング スペクトル拡散) 無線プロトコルを使用するものがあります。1997 ~ 1999 年の間に製造された旧式の 802.11 アクセス ポイントの多くは、802.11 FH と呼ばれる周波数ホッピング プロトコルを使用していました。

また、かつては HomeRF Working Group と呼ばれるモバイル ワイヤレス ベンダーのコンソーシアムも存在していました。これらのベンダーは、2.4 GHz 周波数範囲でも FHSS 伝送を使用する、非 802.11 アクセス ポイントを製造していました。802.11 FH および HomeRF デバイスはすでに販売が終了していますが、eBay や他のオークション業者などから非常に低い価格で広く入手できます。

Bluetooth 無線も 2.4 GHz 周波数範囲で FHSS 伝送を使用します。Bluetooth 無線はイーサネット接続も備えた多くのデバイス (ノート PC など) で使用されているので、潜在的なセキュリティの脅威と見なす必要があります。

### David Coleman 氏略歴

ワイヤレス セキュリティ / ネットワーキングのトレーナー兼コンサルタント。ワイヤレス ネットワーキング認定の業界標準として世界中で認められている CWNP のコースで教鞭をとるかたわら、個々のベンダー向けにカスタマイズした Wi-Fi トレーニングも行っています。これまで、ワイヤレス ネットワーキング管理、ワイヤレス セキュリティ、ワイヤレス フレーム分析の分野で世界中の IT 担当者を指導してきました。氏の運営する AirSpy Training 社 (www.airspy.com) は、企業トレーニングを専門とし、これまでに SpectraLink、Avaya、Dell Computers などの企業と共同で事業を展開しています。政府機関にも注力しており、各種法執行機関、米海兵隊、米陸軍、米海軍、その他の連邦および州政府機関の数多くのコンピュータ セキュリティ 担当者にトレーニングを提供しています。

## WI-FI ネットワークの保護

旧式の 802.11 FH と HomeRF、および Bluetooth 無線はすべて、攻撃者が不正デバイスとして利用でき、現在の WIDS/WIPS ソリューションによって検出されることもありません。事実、このような弱点があることから、悪意を持ってネットワークにオープンポートを設定しようとする者にとっては、非常に魅力のある手段となります。このような不正デバイスを検出および特定するために必要なツールがスペクトルアナライザです。

スペクトルアナライザは、周波数ホッピング無線を含む、あらゆる種類の非 Wi-Fi 無線デバイスを検出できます。実際、一部のアナライザは、デバイスの RF シグニチャを確認して、見つかった非 Wi-Fi 無線の種類を正確に特定できます。

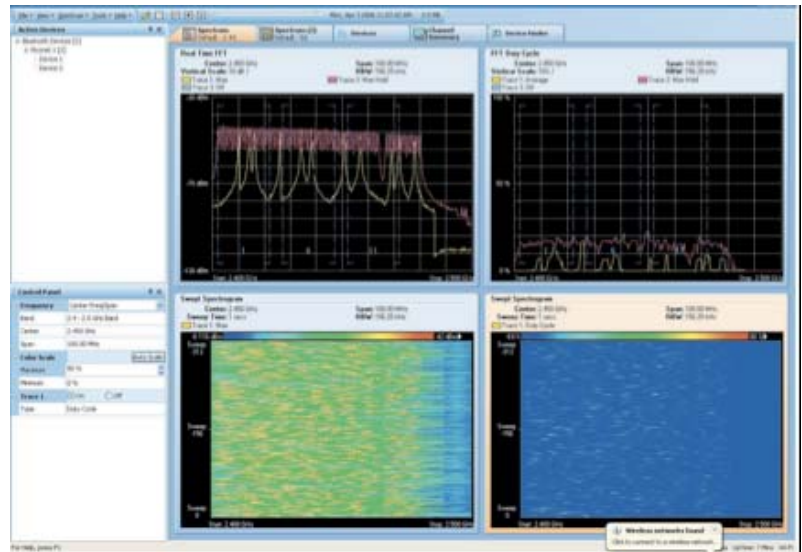
検出されない潜在的な不正デバイスのもう 1 つの例として、802.11 無線カードでサポートされていない周波数範囲で伝送するアクセスポイントがあります。802.11 無線カードは、免許不要の 2.4 GHz ISM 周波数帯または 5 GHz UNII 周波数帯で伝送を行います。非 802.11 ワイヤレスネットワーク機器の中には、免許不要の 902 ~ 928 MHz の ISM 周波数帯で動作するものがあります。802.11 無線カードは 900 MHz 周波数範囲をリッスンしないので、この種のデバイスを検出できるのは、900 MHz 周波数範囲をスイープするスペクトルアナライザだけになります。

数多くの 802.11 不正デバイスを検出および防止するうえで、レイヤ 2 WIDS/WIPS ソリューションは今なお推奨されるソリューションです。ただし、常時稼働のスペクトル分析ソリューションを追加することによって、より広い範囲の不正デバイスを数多く検出できるようになります。

### レイヤ 1 DoS 攻撃

Wi-Fi セキュリティにとってきわめて厄介な問題が DoS 攻撃です。DoS 攻撃における攻撃者の目的は、セキュリティを突破したり、ネットワークからデータを盗んだりすることではなく、単にネットワークを使用できなくすることです。ミッションクリティカルなシステムにとって、これはセキュリ

図 1 動作中の Bluetooth デバイスのスペクトル分析ビューの例



ティ上の重大な懸念事項です。WLAN が停止した場合、WLAN を経由してアクセスされるアプリケーションやネットワークリソースは使用できなくなります。ワイヤレス VoIP 電話による通話は途切れ、データベースサーバとの通信は不能になり、インターネットゲートウェイへのワイヤレスアクセスは遮断されます。

多くの DoS 攻撃はレイヤ 2 に存在し、攻撃者が、802.11 管理フレームのレイヤ 2 ヘッダー内の情報を操作し、編集したフレームをパケットジェネレータのような機器を使用してワイヤレス環境に再伝送することによって、攻撃が発生します。

公表されているレイヤ 2 DoS 攻撃は数多く存在します。最も一般的なものは、認証取り消しまたはアソシエーション解除の管理フレームを操作することによって実行されます。現在のところ、レイヤ 2 DoS 攻撃を阻止することは簡単ではありませんが、検出することは簡単です。802.11w タスクグループでは、多くのレイヤ 2 DoS 攻撃を阻止するための方法を協議しています。この方法は、シスコの Unified Wireless 構想の下、Management Frame Protection (MFP; 管理フレーム保護) によって推進されています。

レイヤ 2 DoS 攻撃の発生元である無線カードは、ワイヤレス侵入検出システムによって検出および特定できます。ところが、ワイヤレスネットワークに対する DoS 攻撃は、RF 環境のレイヤ 1 でより簡単に行われる可能性

があります。レイヤ 1 DoS 攻撃は、無線周波数干渉の結果として発生します。802.11 WLAN 無線カードは、Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA; キャリア検知多重アクセス/衝突回避) と呼ばれるメディアアクセス方式を使用します。このメディアアクセス方式では、半二重無線メディアにおいて任意の時点で 1 つの無線カードからのみ伝送が行われることが保証されます。CSMA プロトコルの構成要素として Clear Channel Assessment (CCA; クリアチャンネルアセスメント) があります。CCA を簡単に説明すると、802.11 無線カードが伝送の前にリッスンすることです。

802.11 無線カードは、伝送を開始するとき、CCA を実行し、同じ周波数空間の現在の RF 伝送をリッスンします。RF メディアがクリアの場合、無線カードは伝送を行います。ただし、メディアがクリアでない場合 (事前定義されたエネルギーしきい値を超える RF 伝送が検知された場合)、802.11 無線カードは、指定された時間だけ待機し、もう一度 CCA を実行して、メディアがクリアであることを確認してから伝送します。CCA を何度実行しても RF 伝送が絶えず検知される場合は、信号がなくなるまで 802.11 伝送は完全に停止します。RF 信号の干渉によって 802.11 伝送が停止すれば、結果的に WLAN への DoS になります。では、レイヤ 1 DoS は何によってもたらされるのでしょうか。これは、意図的な干渉または意図的でない干渉の結果として発生します。

図 2 信号ジェネレータ



**意図的な DoS**

意図的な DoS は、RF 信号ジェネレータ デバイスのような機器を保有している個人からの悪意のある攻撃とすることができます。信号ジェネレータには、2.4 GHz ISM 帯域と 5 GHz UNII 帯域の両方で伝送するものがあります。信号ジェネレータは、多くの場合、電力計を使用して同軸ケーブルの損失を計測するときの電源を提供するなど、正当なテストの目的で使用されます。

悪意のある個人が通常のアンテナを介して 1 ワット (+30 dBm) の信号を伝送するのを阻止するにはどうしたらよいでしょう。信号ジェネレータは電波妨害装置に改造されるようになってきており、これは、最大 100 mw (+20 dBm) で伝送する多くの 802.11 無線カードの性能を上回ります。高利得アンテナと信号ジェネレータを組み合わせると、より大きな放射電力を得て、DoS 攻撃の範囲を広げることが可能になります。単方向アンテナを使用すると、レイヤ 1 DoS 電波妨害攻撃を局所に集中させることができます。

図 3 電波妨害装置



電波妨害装置および信号ジェネレータは、狭帯域または広帯域に対応します。たとえば、2.4 GHz の狭帯域ジェネレータは、特定のチャンネルで DoS を発生させることができます。図 4 に、狭帯域電波妨害装置のスペクトルキャプチャを示します。



図 4 狭帯域電波妨害装置のスペクトルキャプチャの例

広帯域の電波妨害装置は、複数の周波数でノイズフロアを引き起こす信号を放出します。図 5 に、2.4 GHz の広帯域電波妨害装置のスペクトルキャプチャを示します。

図 5 広帯域電波妨害装置のスペクトルキャプチャの例



意図的なレイヤ 1 DoS 攻撃で使用できるもう一つのデバイスに、通常の 802.11 無線カードがあります。802.11 無線カードを「連続伝送」の状態に置くことができたらどうなるでしょう。その場合、無線カードはデータの送信や変調を実際には行いませんが、狭帯域の信号ジェネレータとまったく同じように一定の RF 信号を送信します。他の 802.11 無線カードはメディアにアクセスできません。CCA を実行するたびに、途切れることのないトランスミッタによってメディアが占有されているからです。オーストラリアにあるクイーンズランド大学の研究者達は、この攻撃が実現可能であることを突き止めました。このテストのため、802.11b 無線カードを製造する某大手チップセットメーカーが、無線カードを連続伝送の状態に置くソフトウェアユーティリティを開発しました。このユーティリティは、悪意のある目的にも利用でき、Queensland Attack (クイーンズランド攻撃) と広く呼ばれています。30 mW で連続伝送の状態にある 802.11b 無線カードは、1 ワットの電波妨害装置に比べれば、それほど脅威ではないかもしれませんが、しかし、そのようなカードが使用されている無線範囲内にある 802.11b/g カードはすべて影響を受けます。

# レイヤ 1 に潜むセキュリティの脅威

## 意図的でない DoS

悪意のある攻撃が行われなくても RF 干渉によって DoS が生じることはあるでしょうか。

もちろんあります。あらゆる種類のデバイスは、非常に混雑した 2.4 GHz ISM 帯域で伝送を行います。RF ビデオカメラ、ベビー モニタ、コードレス電話、電子レンジなどはすべて干渉源となる可能性があります。最初のサイト調査の主目的は、これらの干渉源を排除することです。しかし、ある従業員が社内ポリシーのことを忘れてしまい、最初のサイト調査が実施された後で、電波漏出の多い電子レンジや 2.4 GHz のコードレス電話などを使用したとしたらどうなるでしょう。一般の電子レンジは 800 ~ 1,000 ワットで動作します。電子レンジはシールドされていますが、時間の経過と共に電波漏出しやすくなる可能性があります。-40 dBm の受信信号は 1 ミリワットの約 1/10,000 であり、802.11 通信にとっては非常に強い信号と見なされます。1,000 ワットの電子レンジの電波漏出率が 0.0000001 % であったとしても、802.11 無線にとっては干渉源となります。図 6 に、電子レンジのスペクトルビューを示します。信号が広帯域のスペクトルでスイープし、約 50 % のデューティ サイクルで動作している点に注目してくださ

い(マグネトロンがオン/オフが 60 Hz のサイクルで切り替わる場合)。図 7 に、アナログ ビデオ カメラのスペクトルビューを示します。信号が単一の周波数で動作し、100% のデューティ サイクルで伝送されている点に注目してください。5 GHz UNII の周波数で伝送を行う干渉デバイスはほとんど存在しませんが、それも時間の経過と共に変化します。5 GHz のスペクトル分析も必須の作業として捉える必要があります。

意図的でない干渉は連続的な DoS を発生させる可能性があります。サービスの中断は散発的であることがほとんどです。このサービス中断によって、データ アプリケーション用に使用される Wi-Fi ネットワークのパフォーマンスは影響を受けます。そればかりではなく、Wi-Fi ネットワーク内の VoIP 通信は完全に遮断される可能性があります。少なくとも、意図的でない干渉の結果、再伝送を行わなければならないようになります。最初のサイト調査では、このような干渉源を排除します。ただし、干渉デバイスが再出現することに備えて、スペクトル モニタリングを常時または定期的に行う必要があるでしょう。

図 6 電子レンジのスペクトル キャプチャの例

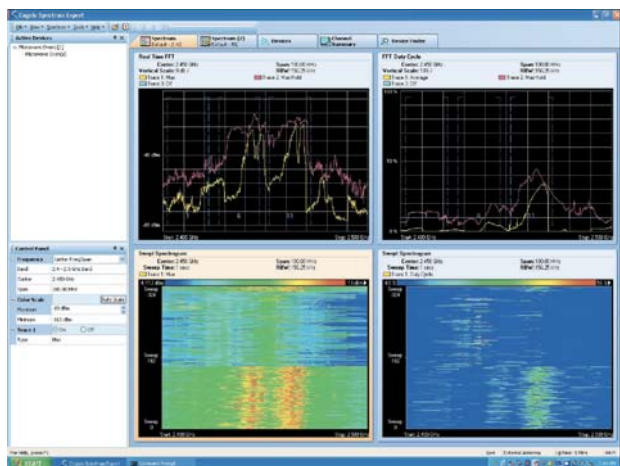
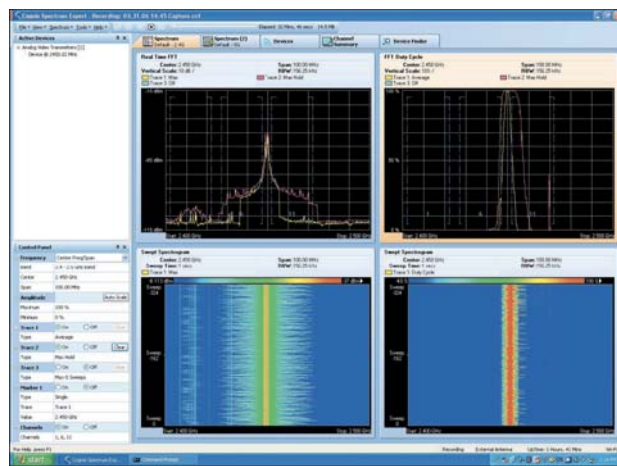


図 7 アナログ セキュリティ カメラのスペクトル キャプチャの例



### Neil Diener 略歴

米国シスコシステムズ社 CTO(最高技術責任者)の技術リーダー。信頼性の高いコミュニケーション システムのアーキテクチャと設計の分野で 20 年以上の経験があります。シスコに移籍する前は、スペクトル分析のリーダー企業である Cognio 社の共同創業者兼 CTO を務めました。Motorola 社、Sun Microsystems 社、Xerox 社などの企業で重役ポストも歴任しています。MIT(マサチューセッツ工科大学)にて電気工学学士号、USC(南カリフォルニア大学)にてコンピュータ工学修士号を取得。

## モバイル型スペクトル分析と分散型スペクトルセキュリティ

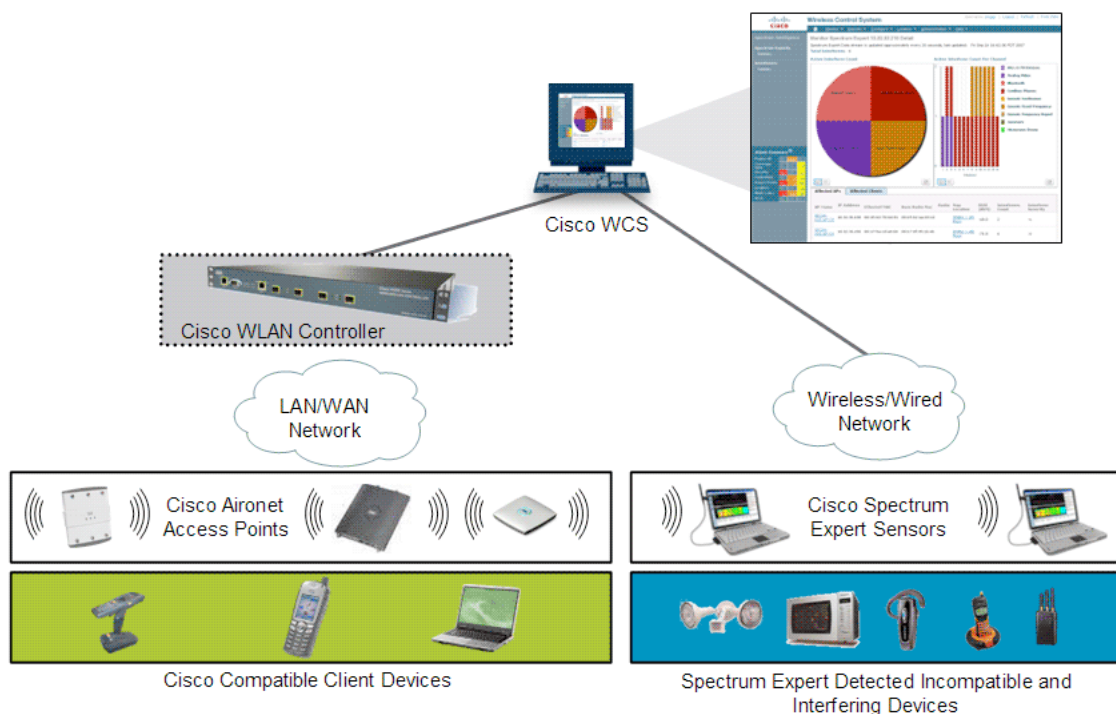
従来のスペクトルアナライザハードウェアは40,000ミドル以上に及ぶものもあり、多くの中堅・中小規模の企業にとっては法外な金額でした。しかし、シスコシステムズが手頃で使いやすいスペクトルインテリジェンス製品を導入したことによって、多くのサイト調査担当者がスペクトル分析を802.11サイト調査における必須事項として捉えるようになってきました。これらの製品は、独自仕様のPCカードハードウェアで動作する、低価格でソフトウェアベースのスペクトル分析ソリューションです。干渉の問題を最初に排除することでネットワークの継続的なサポートコストを削減できるので、製品への投資は最初のサイト調査の後に回収されます。また、WLAN担当者は、レイヤ1のセキュリティリスクに対する予防措置として、これらのスペクトル分析ソリューションを実装し始めています。

スペクトル分析システムには、モバイル型と分散型の2つの形態があります。モバイル型スペクトル分析デバイスの例として、Cisco Spectrum Expertがあります。この製品は、CardBusカードとソフトウェアで構成され、ノートPCで動作してポータブルな測定システムを実現します。分散型スペクトル分析システムの例として、Cisco Spectrum Cardbus Sensorを備えたCisco Wireless Control System (WCS)があります。この分散型スペクトルインテリジェ

ンスは、スタティックまたはモバイルで展開される一連のPower-over-Ethernet (PoE) センサーで構成されます。これらのセンサーは、スペクトル測定を常時行い、そのデータをサーバに送信します。サーバでは、データをアーカイブおよび分析して、ユーザに提示します。モバイル型および分散型システムは、次に説明するとおり、それぞれの長所と利便性を備えています。

モバイル型システムは、サイト調査の場合など、インフラストラクチャを展開する前の段階で非常に役立ちます。また、フロアスペースをくまなく調査して、物理的に確認が難しい場所に建物の外部などから干渉が発生していないかどうかを確認するときにも使用できます。干渉源が検出されたら、干渉デバイスの場所を追跡することもできます。システムをトラッキングモードに設定すれば、「ガイガーカウンター」として使用して、電波の強いところや弱いところを探りながら干渉デバイスを特定できます。この追跡機能は、指向性アンテナと組み合わせることで、さらに拡張できます。セキュリティの観点から言うと、モバイル型のツールは、不正デバイスや電波妨害装置を検出するためのフロアスペースの定期的なスウィープの一環として使用できます。モバイル型システムは、本格的なセキュリティモニタリングソリューションというよりも、基本的に「スポットチェック」の用途に適しています。セキュリティレベルの高いデータを保有していない多くの企業にとっては、これだけでも十分でしょう。

図 8 Cisco Spectrum Intelligence の図



分散型スペクトル分析システムは、モバイル型よりも多くの機能を提供しますが、センサーのインフラストラクチャコストにより、価格も多少高めになります。分散型システムの主な利点は、週 7 日 24 時間体制で動作し、リモート管理できることです（複数の建物に分散している大企業にとっては重要）。常時稼働しているので、レイヤ 1 に関連するセキュリティの問題が発生した場合、それが断続的なものであっても、すべて検出されることが保証されます。ミッションクリティカルなアプリケーションや機密性の高いデータを展開している企業は、分散型システムの使用を検討する必要があります。

分散型システムの別の適用例として、「ノー ワイヤレスゾーン」の実装があります。これは、建物の中の安全なエリアを指し、情報のセキュリティを確保する目的でワイヤレス デバイスの使用が禁止されます。一例として、米国の政府施設内にある Segmented Compartmented Information Facility (SCIF; 分割コンパートメント情報施設) があります。これらの施設では WLAN IDS システムが導入されている所もありますが、Bluetooth やコードレス電話など、他の

ワイヤレス デバイスの使用を禁止するには、本格的なレイヤ 1 分析システムが必要です。また、ポケットベル、携帯電話、WiMax 無線などの WAN デバイスが使用されないように、他の帯域を監視することもできます。分散型システムは、セキュリティ監査の一環として必要なレポートを自動生成する際にも使用できます。

数多くの展開にとって、モバイル型と分散型のスペクトル分析ツールを用意しておくことは理にかなっています。モバイル型ツールは最初のサイト調査および確認しづらい場所の定期的なスウィープで使用します。分散型ツールは、スペクトル使用の週 7 日 24 時間体制でのモニタリングおよびアーカイブで使用します。分散型ツールによって干渉が検出され、その大まかなエリアが示されたら、今度はモバイル型ツールを使用して干渉デバイスの正確な場所を特定することもできます。モバイル型および分散型スペクトル分析ソリューションを組み合わせることで、完成度の高いエンタープライズ スペクトル セキュリティ ソリューションになります。

