事例研究

シスコゲスト無線ホットスポット

シスコ IT 事例研究 / 無線 LAN (WLAN) / ゲスト無線ホットスポット: 本事例研究は、シスコシステムズを訪れる顧客に利便性を提供するゲスト無線ホットスポットを導入する際に、既存の WLAN がどのように利用されたかを紹介するものです。シスコのグローバルネットワークは、世界屈指の大きさと複雑さを誇る最先端の企業環境です。シスコの顧客は、シスコ IT のこの分野での経験を参考に、同様の企業ニーズに応えることができます。

「シスコには既に無線インフラ環境があったので、展開は容易でした。レイヤ 2 ホットスポットソリューションの展開を正式決定した後に行ったのは、Cisco BBSM のインストール、ゲスト VLAN の設定、ファイアーウォール上の経路開設、ログインページと利用規定の作成だけです。それでサービスを始められたのです」—トニー＝ディエップ (Tony Diep)、無線ホットスポットのグローバルアーキテクチャおよびデザイン担当 IT プロジェクトマネージャ

課題

シスコシステムズでは、訪れた顧客があらゆる面で満足できるようなサービスの提供に努めており、その範囲も、エグゼクティブブリーフィングやテクニカルブリーフィングといったものから、PoC（概念検証）のデモや利便性といったことまで多岐に渡ります。とりわけ、Executive Briefing Center (EBC) や Technical Briefing Center (TBC) での何日も続く打ち合わせやトレーニング、会議などへ参加する顧客にとって、日常業務時と同等の利便性が提供されるかどうかは重要なポイントです。多くの顧客が望むのは、E メールやインターネット、VPN を利用した自社のネットワークへの接続環境です。Europe, Middle East, and Africa (EMEA) のエンタープライズ テクノロジー ソリューションのテクニカル プロジェクト マネージャであるサル＝ピアース (Sal Pearce) は、「EBC や TBC といった社外向けのエリアに、お客様用の無線インターネットアクセス環境はありませんでした。何度も要望があったにもかかわらずです」と言います。そこでシスコは、既存の無線インフラを利用し、訪問客へインターネット アクセスを提供することにしました。このゲスト無線ホットスポットサービスの提供範囲は、数週から数ヶ月の間インターネットへのアクセスを必要とする認定ベンダーや、社内で働く契約社員にも拡大されることになりました。それまでは、ベンダーがシスコに長期滞在する場合、ダイアルアップ接続を強いられることもあったのです。

社内では、DSL や有線ホットスポットサービスなどを利用し、訪問客にインターネット アクセスを提供している部署や部門もありました。しかしこれらは標準化されておらず、大きな負担となっていました。さらに、シスコの機密情報にはどの顧客もアクセスできないようにするという難題もありました。「ネットワーク全体のセキュリティ強度は、もっとも脆弱なリンクと同等になってしまうのです」無線ホットスポット グローバル アーキテクチャおよびデザイン担当 IT プロジェクトマネージャ、トニー＝ディエップ (Tony Diep) は言います。「どの企業もセキュリティを侵害されることのない、IT が管理する一貫したソリューションが必要なのです」

シスコは、ゲスト無線ホットスポット ソリューションの導入にあたり、セキュリティを最重要視したいくつかの基準を設けました。導入されるソリューションは、ゲスト トラフィックを、ゲスト VLAN 内を通すことでシスコの社内トラフィックと区別させるようなものでなければなりません。セキュリティ面でもうひとつ重要になるのは、シスコのネットワーク上に誰がいて、何をしているかを把握し、不審な動作があればそれを遮断し、ネットワークを保護できるようにすることです。これにはエンドツーエンドのユーザ認証が必要です。ただ、それにより利便性が低下しないことも重要です。導入されるソリューションは使い易く、シスコ IT や案内係、受付などに重いサポート負担がかからないものでなければなりません。さらに、シスコ IT では、社内の音声およびデータトラフィック用に既に導入されていた Cisco Aironet® 350 と 1200 無線アクセスポイントを使って、ゲスト

無線ホットスポットを展開しようと考えていました。既存の装置上にゲスト VLAN を構築することで、ハードウェアコストは削減され、また、無線周波数干渉も最小限に抑えられるため、従業員は従来どおり、無線 LAN を使い続けることができます。

シスコのネットワーク保護のため、シスコのインフォメーションセキュリティ（InfoSec）グループは、ゲストトラフィックが流れるのは専用 VLAN 内のみとし、シスコのネットワークを通過させないと規定しました。

ソリューション

シスコ IT は、社内の既存の無線 LAN インフラ上に構築することで、インフラの追加購入の必要性を抑えたゲスト無線ホットスポットソリューションを策定しました。稼働中の無線ネットワークを使って訪問客にアクセスを提供することは、理論的には、ゲスト VLAN を追加できるようにアクセスポイントの設定を変更し、既存の社内データおよび音声用 VLAN を拡張すること、および Cisco Building Broadband Service Manager (BBSM) サーバを既存の LAN アーキテクチャへ追加することでした。「無線ゲスト ホットスポットは、大変理解しやすいソリューションです」とディエップは言います。

シスコ IT は、Cisco Service Selection Gateway (SSG/Subscriber Edge Service Manager) との比較検討の末、ディエップが「箱の中のホットスポット」と呼ぶ Cisco BBSM を採用しました。Cisco BBSM は最もコストがかからず、展開、設定が簡単です。サービスプロバイダ用に設計された Cisco SSG が Cisco IOS® ソフトウェアの一部であり、シスコのルータと UNIX サーバ上で動作するのに対し、Cisco BBSM は Windows 2000 サーバプラットフォーム上で動作します。

BBSM では、ユーザごとの認証を行います。訪問客は、受付票に記入し、受付や同伴社員からゲストユーザ ID と一定期間有効なパスワード受け取ります。全てのゲスト無線トラフィックはゲスト用に分離された VLAN を流れ、ポリシーに基づき最も近くの BBSM にルーティングされるため、シスコの社内ネットワークにアクセスすることはありません。BBSM はまた、ユーザが最初にログインする際、免責事項を表示し、サービスの利用に際してユーザには法的責任があり、シスコではサービスの提供によって被るいかなる損害も負わないことを確認させます。さらに、BBSM には、接続者と接続日時を含むアカウント情報が記録されるため、インターネット上で発生した問題行為がシスコのゲスト ホットスポットを通して行われたものであると判明した場合、司法権がその行動を追跡し、行為者を特定することに協力できるのです。

ゲスト無線ホットスポットの展開にあたり、シスコ IT は 2 段階のアプローチを採用しました。第 1 段階では、1 ヶ所のホットスポットにつき 1 台のサーバを必要とする Cisco BBSM の レイヤ 2 機能を使います。同時に、全世界の全てのシスコオフィスでゲスト無線ホットスポットを展開する準備として、第 2 段階では、シスコ IT とシスコのネットワーク管理テクノロジー グループが共同でレイヤ 3 機能を追加します。これにより、1 台の Cisco BBSM サーバで複数の地理的に分散したホットスポットをサポートすることが可能になります。

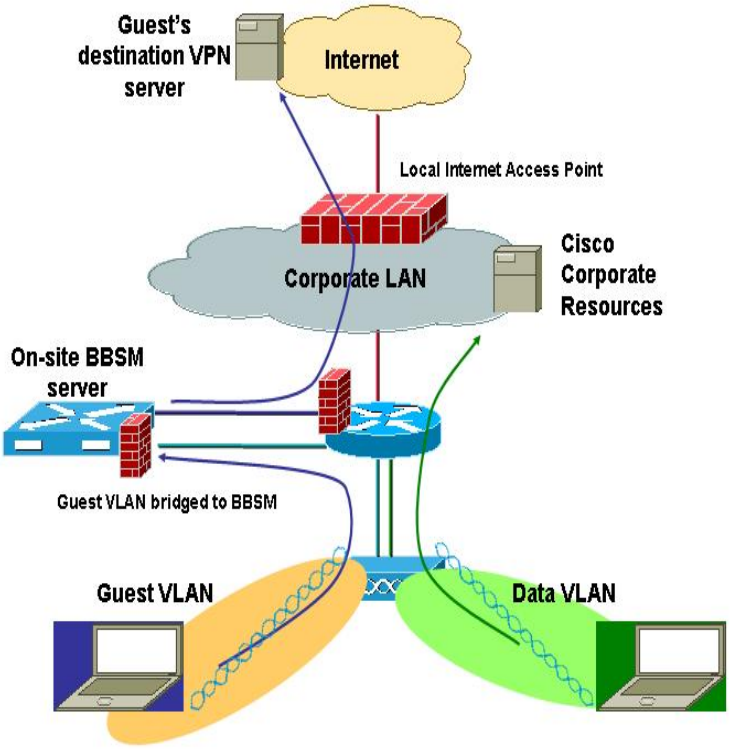
第 1 段階: レイヤ 2 BBSM ホットスポット

2003 年 9 月に完了した第 1 段階では、サンノゼ本社とロンドン、そしてアムステルダムの 3 ヶ所の EBC にゲスト無線ホットスポットが展開されました。Cisco BBSM サーバは、展開されたホットスポットと同一のサブネット内に設置されています。

Cisco BBSM サーバにはそれぞれ 2 つのインターフェイスがあります。このうち 1 つは Cisco Aironet 350 または 1200 無線アクセスポイントに接続されたスイッチに、もう 1 つはインターネットの非武装地帯（DMZ）内のコネクションを使ってインターネットにそれぞれ接続されます（図 1 参照）。アクセスポイントにつながっているインターフェイスの IP アドレスは、全てのゲストトラフィックでデフォルトゲートウェイになります。これにより、全てのゲスト インターネットトラフィックは Cisco BBSM に即座にルーティングされ、社内 LAN は完全に迂回することになります。これに対し、社内無線トラフィックは異なる VLAN 上にあり、独自の SSID を持つため、Cisco BBSM は全く通りません。

このモデルでは、Cisco BBSM はホットスポットのデフォルトゲートウェイであると同時に、DHCP を使った IP アドレス割り当てサーバおよびドメイン名サーバとしても機能します。

図 1 第 1 段階: シスコのゲスト無線ホットスポットの展開: レイヤ 2 設計



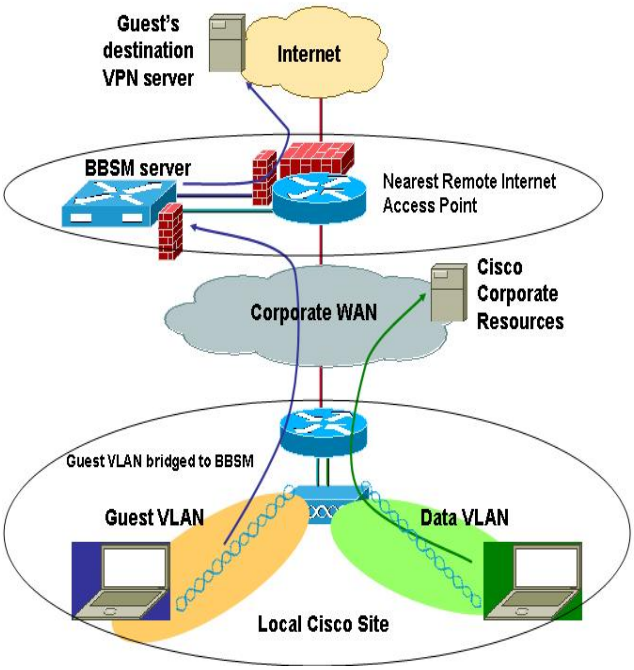
第 2 段階: レイヤ 3 BBSM ホットスポット

シスコ IT では、BBSM のレイヤ 3 機能を利用できるようにする無線ホットスポットの展開第 2 段階を現在も引き続き行っています。ここでのアーキテクチャは第 1 段階でのものと似ていますが、BBSM サーバと共に、GRE トンネルを構築するヘッドエンドルータも必要になります。BBSM サーバはシスコ IT のインターネット POP 内にある主要なインターネットアクセス拠点内に配備されます。「ゲストユーザはシスコのイントラネットへアクセスする必要はないので、BBSM とヘッドエンドトンネルルータをインターネットのもっとも近くに設置するのが理想的な設計となります」ディエップは語ります。「ホットスポットインフラを既存のネットワークインフラに統合することで、管理が容易になり、WAN を流れる不要なトラフィックを減らすこともできます」 世界各地の 250 を越すシスコの拠点にいるホットスポットユーザは、その場で無線ゲスト VLAN にログインし、WAN 内を（ほとんどのデータトラフィックにマーキングされるのと同じ規定のサービス品質で）もっとも近くのインターネット アクセスポイントにある BBSM サーバまでトンネリングされます。BBSM サーバは、SSL によって暗号化された必要な免責事項を記載したウェブページが表示させ、ユーザはそこで入構時に渡されたユーザ ID とパスワードを使って認証を受けることになります。ゲストトラフィックは異なる VLAN を流れるため、必要に応じてサービス品質（QOS）を設定することも可能です。

シスコ IT が 250 を越す拠点全てでこのサービスを展開するためにかけた費用が比較的小額だったのは、既存のネットワーク装置と帯域幅を利用したためです。この方式が取り入れられたのは、シスコの拠点でインターネットにアクセスする訪問客数が拠点内人口に占める割合は小さいはずで、各拠点からインターネット アクセスポイントまでの WAN 回線帯域幅を増強する必要はないと想定されているからです。訪問客には、（VPN クライアントに問題が発生する可能性を最小限に抑えるため、プライベートアドレスではなく）インターネット接続用にシスコに割り当てられているアドレスブロックの中から、ルーティング可能なグローバル IP アドレスが提供されます。新たに必要だったのは、シスコのグローバ

ルネットワーク内にある 8 ヶ所のインターネット アクセスポイントそれぞれに、稼動用とスタンバイ用の 1 対の BBSM サーバと、ゲスト GRE トンネルを終わらせる 1 台の Cisco 7206VXR だけです（注: このルータは、何らかの理由により DMZ ルータと分ける必要がある場合にのみ設置されます。シスコ IT では、ここにルータを設置することで、ホットスポットサービスとインターネットアクセスサービスと、役割を明確に分け、それぞれのサポートは IT 内の異なるグループが行います）。ホットスポットの優先度が高いエリアでは、さらにもう 1 台の Cisco 7206 ルータを冗長構成用に追加しました（図 2 参照）。

図 2 第 2 段階: シスコ ゲスト無線ホットスポットの展開: レイヤ 3 設計



セキュリティの確保

「既存の WLAN からゲストアクセス層を分けるのは比較的簡単です。問題なのは、セキュリティという点においてそれが正しくできるかどうかなのです」とディエップは言います。そこで、シスコ IT はシスコ InfoSec と緊密に連携して展開プランを作成しました。「私たちは、このビジネスニーズが妥当なものであることを InfoSec に納得してもらう必要がありました。InfoSec からは、DMZ 機器[1] に関するセキュリティガイドラインに従ってサーバとルータを堅牢なものにすることを求められました。特に、Cisco BBSM をインターネットアクセスポイント内の DMZ 上に設置することで、誰からもハッキングされないようにすることが求められました」さらに、シスコ InfoSec からは、ゲストトラフィックが社内のスイッチファブリックを流れないことも求められたため、シスコ IT ではシスコ拠点内の各ルータと BBSM に接続されたルータ間で GRE によるトンネリングを行うことで、ゲストトラフィックが社内ネットワークのどこにも漏れ出さないようにしました。

ゲスト無線アクセスを展開するのにもっとも安全な方法は、各拠点で社内ネットワークとは物理的に隔絶された回線を追加購入することです。ディエップはこれを「エアギャップ」と表現します。しかし、回線を追加することは費用やサポート負担の増大にもつながります。「Cisco BBSM

[1] www.cisco.com/application/pdf/en/us/guest/products/ps533/c1244/cdccont0900aecd80093fe0.pdf

や SSG ホットスポットソリューションは次善の策なのです」とディエップは言います。「強力なファイアーウォールとしての BBSM とポリシーベースのルーティングを組み合わせることで、セキュリティ面での安心感が得られたのです」

次に、シスコ IT はファイアーウォールを設定し、ゲストトラフィックがシスコのイントラネットを流れないようにしました。シスコでは、「一部を除き全てを拒否する」のではなく、「一部を除き全てを受け入れる」方式を採りました。この方式は、セキュリティの脆弱性が知られている場合（例えば、Blaster ワームや Nachi ワームに対して脆弱なポート 135 や 4444）を除き全てのトラフィックを受け入れるものです。もし「一部を除き全てを拒否する」方式を採用すると、IT ではクライアント VPN 用の個々の TCP ポート ID など、利用者の要件ごとに何度もファイアーウォールの設定を変更することになり、さらなるサポート間接費がかかります。訪問客がシスコの社内ネットワークへアクセスするのを防ぐのは、Cisco BBSM の外部インターフェイスが接続されている Cisco 7200 シリーズルータの発着信アクセスコントロールリスト (ACL) です。

さらに、Cisco Aironet 350 および 1200 アクセスポイントで無線暗号プロトコル (WEP) を有効にするかどうかと、「guestnet」SSID をブロードキャストするかどうかという 2 つのポリシーを定めることになりました。結局、シスコでは、端末とアクセスポイント間のトラフィックを暗号化する WEP を有効にしないことにしました。理由は、訪問客の利便性とサポート負担の回避です。「WEP をサポートすると、訪問客には、WEP が使えるように無線クライアントを設定し、26 文字の暗号キーを入力する必要が生じます」とディエップは語ります。「ですから訪問客には、VPN を使ってデータを暗号化するよう求めています」

また、SSID のブロードキャストに関しては、これを行うことにしました。SSID は、無線ネットワーク機器が無線接続を確立し、維持するための固有の識別子です。この決定にも訪問客の利便性が影響しました。もし SSID がブロードキャストされなければ、訪問客はハード側で無線クライアントのコードを設定し、SSID に関連付けなければなりません。「SSID をセキュリティ層の 1 つとみなしてはいけません。SSID を特定するためにネットワークスニッファーを使うことは簡単だからです」とディエップは念を押します。「セキュリティを確保するために、私たちはアクセスコードやファイアーウォール、VPN を利用します。また、さらなるユーザ保護のために Publicly Secure Packet Forwarding (PSPF) の導入も検討しています」 PSPF はシスコのアクセスポイントが持つ機能の 1 つで、クライアント間で通信ができないようにするものです。

ユーザエクスペリエンス

ゲストネットワークを誰が利用でき、誰に監視能力を持たせるかを管理するために、特定の期間アクセスが可能になる固有のアクセスコードを提供します。レイヤ 2 の展開においては、アクセスコード管理者として、シスコの管理アシスタントが、制限アクセス権を使って Cisco BBSM インターフェイスにログインし、訪問客の名前と、招待したシスコスポンサーがリクエストした時間を入力し（例えば、ある週の月曜日から金曜日の午前 8 時から午後 5 時までなど）アクセスできるようにします。滞在中の訪問客には Cisco BBSM が生成した印刷も可能なアクセスコードが手渡されます。展開第 2 段階では、アクセスコードの生成をスポンサーが行うことで、管理層をなくすことが計画されています。スポンサーは、アクセスコードのデータを安全に BBSM に送信できる社内のウェブページを利用することになります。新しい機能ではまた、アクセスコードの一括リクエストの実現や、様々な管理ツールの提供も計画されています。レイヤ 3 の展開においては、アクセスコードを生成する中央ウェブページも重要で、これにより、異なる BBSM にログインせずに異なる場所へのアクセスコードが生成できるようになります。

ゲスト無線ホットスポットの利用は、訪問客がいつものようにブラウザを立ち上げることから始まります。訪問客がシスコの社内サイト外のウェブページを開こうとすると、追跡用フルネームの入力と、使用許諾への同意を行うログインページに自動的にジャンプします。訪問客は、続いて固有のアクセスコードの入力を求められます。BBSM による認証が終わると、訪問客はシスコの社内ネットワークにアクセスすることなくインターネットに接続できるようになります。伝送データは VPN クライアントを使用するまで暗号化されません。また、シスコ IT では Cisco NetFlow テクノロジーを利用してインターネット利用の履歴をとっており、法的理由により必要な場合は、データの読み出しも可能です。

こうして、訪問客は、ウェブ閲覧、E メール、リモートオフィスとの VPN セッションなど、完全に無制限に近い形でのインターネット接続が可能になります。シスコ IT では、ピアツーピア接続を規制し、トロイの木馬攻撃に使われることが知られているポートも許可しないことにしました。このソリューションでは、セッションが詳細に記録され、シスコ IT の法務部や法執行機関が必要とした場合、訪問客に提供された IP アドレスからアクセスコードや名前がわかるようになっています。ただし、トラフィックの内容は検出も記録も分析もされません。

セッションの詳細

訪問客が URL を入力した際、無線 PC から Cisco Aironet アクセスポイントまで、トラフィックは、拠点の WAN ルータを出発し、WAN を通り、インターネット DMZ 内の BBSM に接続されたルータから BBSM サーバへと流れていきます。

BBSM では、社内 BBSM ネットワークインターフェイスカード (NIC) にパケットを送信している PC の IP アドレスと MAC アドレスを検索し、その PC が認証されているかどうかを判別します。認証されている場合、トラフィックは既定のフィルタと合致するので、外部 BBSM NIC に送出されます。そうでない場合、BBSM はその PC をログインページに転送します。ここで表示される利用規定を訪問客が承認すると、BBSM はさらに認証ページに転送し、英数字 8 桁のアクセスコードの入力を求めます。その後、BBSM は入力されたアクセスコードが有効なものであるかを確認します。有効であればリクエストを www.cisco.com に転送します。その際、BBSM サーバの外部 NIC と BBSM デスクトップルータ間では、トラフィックが必ずゲストネットワークを流れるようにします。その方法は以下の通りです。

「PC から BBSM デスクトップルータとして機能する Cisco 2600 ルータ（デスクトップルータ用に Cisco 6500 を使用）へのトラフィックは全てレイヤ 2 を通ります」とシスコ IT のネットワークエンジニアであるパトリック＝ギルブレス (Patrick Gilbreath) は言います。「このため、ゲスト VLAN 内のゲストトラフィックは BBSM デスクトップルータへ向かう経路以外はとれず、シスコの社内ネットワークは保護されるのです」

ゲストトラフィックがデスクトップルータに到達すると、ルートマップにより経路を変更されます。ルートマップは、ACL を利用して全トラフィックにネクストホップを指定し、BBSM デスクトップルータと BBSM DMZ ルータを結ぶ GRE トンネルインターフェイスへのネクストホップを指定します。ゲストネットワークは動的ルーティングプロトコルではアドバタイズされないため、このトンネルは、稼動ネットワークへ向かう静的ルートの 1 つを用い、両ルータ上に構築されます。「BBSM デスクトップルータと BBSM DMZ ルータ上にあるその他のルートは全て静的ルートです」とギルブレスは言います。静的ルートを使用することで、ネットワークを流れるトラフィックをしっかりと管理することができます。トラフィックはその後、社内ネットワーク内に構築された GRE トンネルを通り DMZ へ伝送されます。トラフィックはそこで、ACL を使ってゲストネットワークを照合する、もう 1 つのルートマップにより、BBSM の内部 NIC の IP アドレスへのネクストホップが指定されます。この時点で、全てのゲストトラフィックは、BBSM のフィルタを通過しインターネットへ続く外部 NIC に向かうか、認証のため経路変更されるかを待つことになります。戻ってきたトラフィックも出て行くトラフィックと同じ経路をたどります。

サポート

「このサービスのサポートレベルの設定にも問題がありました。従来、社内の稼動無線 LAN は解決までの期間が 2 日の Priority 4 (P4) に設定されていました」ディエップは言います。「ところが、クライアントと共に仕事をするアカウントマネージャからは、このサービスの機能停止は、収益に直接影響し、4 時間以内に解決すべきとされる P2 に値するという声が聞かれたのです」こうした状況の中、シスコ IT には、業務に直接影響しないサービスに保証される以上のリソースを消費することなく、停止時間を最小限に抑える適切なサポートを提供する必要が生じました。「最終的に、私たちはホットスポットサービスの優先度を 2 つの水準に分けました。EBC のホットスポットには、P2（解決時間 4 時間）を、その他のホットスポットには P3（解決時間 1 日）を設定したのです」とディエップは語ります。シスコ IT は、外部クライアントのラップトップの設定については免責されています。シスコ IT が保証するのはサービスを利用可能状態にすることで、ネットワークへのアクセス方法についてはスポンサーやオンラインヘルプなどがサポートします。

シスコ IT は機能停止時の対応を既存のサポート体制と同様に行います。シスコでは、Global Technical Response Center (GTRC) が社内のサポートに関する問い合わせ全てを受け付け、適切なサポートグループに転送しています。EBC で機能が停止した場合、GTRC は即時対応可能なエンジニアに連絡をします。他の場所で機能が停止した場合は、最適なサポートグループに転送します。

シスコ IT 内には、ネットワーキング、ホスティング、クライアントデスクトップなど、様々なグループがあります。BBSM は IT がサポートする中では特殊な機器です。その理由として、ウィンドウズサーバであること、ネットワークで使われること、エンドユーザの認証を行うこと、DMZ にアクセスするため稼動 LAN を通ることがあげられます。このサービスで使われている他の機器は全てネットワーク機器であるため、IT では、ネットワークチームがサービスを全面的に管理することで、サポートを簡素化しました。問題が発生した場合、ネットワークチームは IT 内の他のチーム（例えば、ウィンドウズやサーバに問題がある場合は、ホスティングチーム）や、BBSM 特有の問題が発生した場合は Cisco Technical Assistance Center と共同で問題に取り組みます。

成果

米国と EMEA の顧客は、ゲスト無線ホットスポットを大変歓迎しています。「大ヒットです」ピアースは言います。「お客様はこのサービスに非常に感銘を受けています。特にアクセスが簡単で高速な点に関して。お客様には、滞在中に届く E メールや重要な問題にも常に目を光らせておくことができると評判です。私たちは、お客様に対し、滞在中の生産性をできる限り確保しています」実際、このソリューションのエグゼクティブブリーフィングやテクニカルブリーフィングを聞き、Cisco BBSM やゲスト無線ネットワークを自社内にも展開した顧客もいるのです。

「社内に計画を発表して以来、ホットスポット導入のリクエストを受けない日はほとんどありません」とディエップは言います。「チームは、ホットスポットが広がり、みんなが使うようになっていくのを見て大変満足しています」

次のステップ

ゲスト無線ホットスポットは地域を限った展開に成功したため、シスコでは世界中のオフィスへの導入を始めています。無線ホットスポットの展開完了後、シスコ IT では、レイヤ 3 の BBSM テクノロジーを活用することで、特定エリアで有線イーサネット LAN セグメントのセキュリティを確保することを考えています。偶然でもスイッチへ接続されてしまうとシスコへ直接アクセスすることになるため、シスコオフィス内にあるセキュリティが確保されていないエリアの有線イーサネットポートはセキュリティ脅威となる可能性があります。「BBSM テクノロジーは無線でも有線でも使えるため、指定のユーザのみにアクセスを保証し、その他の接続は拒否できるすばらしい手法なのです」とディエップは語ります。

教訓

シスコは展開の過程で得た教訓や推奨プラクティスを編集することで、顧客が無線ホットスポットを導入しやすくしています。下記は編集された推奨プラクティスからの抜粋です。

- 「顧客に対し、ラップトップの設定方法とサービス利用に関して明確なガイドラインを提示すること」とピアースは言います。例えばシスコでは、手順書を作成し、ゲスト無線アクセスが提供されているロビーや会議室で配布しています。
- 社内の様々なグループとの調整を入念に行うこと。シスコ IT は法務、マーケティング、セキュリティグループとの調整を行いました。「私の役割は主に、各チームスがムーズに話し合いを行えるようにすることでした」とディエップは言います。ウィンドウズ 2000 サーバ上で動作するネットワークアクセスコントロール デバイスである Cisco BBSM は、その担当範囲もトランスポート・ネットワーキングチームとホスティングチームの両者にまたがっていました。最終的には、サーバのハードウェア部分をホスティングチームが、その他の部分は全てネットワーキンググループが担当することで合意しました。
- 計画の初期段階で IP アドレスの割り当て戦略を決めること。ネットワークアドレス変換 (NAT) アドレスも使用できますが、VPN クライアントによっては規制がかかります。ルーティング可能なアドレスでは常に十分なアドレス数があるとは限りません。

「私たちは、Cisco BBSM を購入したお客様にただ『これが設定方法です』というわけではありません」とピアースは言います。「私たち自身もホットスポットを取り巻く業務プロセスには気がかりがあります。サポート方法を理解しなければならなかったこと、お客様のニーズを見極め喜んでいただくこと、サービスについて教育をすることなどがその例です。私たちは教訓やベストプラクティスの共有がぜひとも必要だと思います。私たちが社内での展開に際して培ってきた豊富な知識を共有することで、お客様は思わぬ落とし穴から逃れることができるのです」

その他、各ビジネスソリューションに対する Cisco IT の事例研究は、
Cisco IT @ Work をご覧ください
http://www.cisco.com/jp (シスコシステムズ→Cisco IT@ Work)

付記

この文書に記載されている事例は、シスコが自社製品の展開によって得たものであり、この結果には様々な要因が関連していると考えられるため、同様の結果を別の事例で得られることを保証するものではありません。

この文書は、明示、黙示に関わらず、商品性の保証や特定用途への適合性を含む、いかなる保証をも与えるものではありません。

司法権によっては、明示、黙示に関わらず上記免責を認めない場合があります。その場合、この免責事項は適用されないことがあります。

シスコシステムズ株式会社

〒107-0052 東京都港区赤坂 2-14-27 国際新赤坂ビル東館
http://www.cisco.com/jp

お問合せ先（シスココンタクトセンター）
http://www.cisco.com/jp/service/contactcenter
0120-933-122（通話料無料）、03-6670-2992（携帯電話、PHS）
電話受付時間：平日 10:00～12:00 、13:00～17:00