

## 解決すべき問題

多くの組織では、コンピューティング環境の柔軟性を高め、労働力の効率的なモバイル化を促進するために、ワイヤレスネットワークを展開しています。しかし、この柔軟性はクリティカルなアプリケーションのサービス品質（QoS）の低下につながる場合があります。音声やビデオのように遅延の影響を受けやすいアプリケーションについては、特に気を付ける必要があります。QoS テクノロジーを使用すると、ネットワーク インフラストラクチャは一定レベルのサービスをアプリケーションに提供し、アプリケーションはパフォーマンス要件を満たすことができます。QoS は、さまざまなトラフィック タイプを区別してネットワーク上のリソースを割り当てることができるので、クリティカルなアプリケーションは優先してネットワークを効率よく使うことができます。ネットワークの輻輳時、QoS によって管理されるトラフィックは、QoS が有効になっていないトラフィックに比べて大幅に高いパフォーマンスを維持します。

ワイヤレス ネットワークではユーザが移動することは避けられないので、重要なアプリケーションを優先して、適切な帯域幅を的確に割り当てることが困難な場合があります。ユーザはあるエリアから別のエリアへ自由に移動するので、それまで輻輳のなかったエリアにネットワークの輻輳が動的に発生します。

IEEE 802.11e 規格は、アクセス ポイントからクライアントへのダウンストリームのパフォーマンスなど、ワイヤレスに関連したいくつかの QoS の問題に対応しています。ただし、802.11e はノードやアプリケーションのタイプを区別しません。そのため、クライアントからアクセス ポイントへのアップストリーム接続において、遅延の影響を受けやすいトラフィックまたはクリティカルなトラフィックが、損失や遅延に対して脆弱になります。

802.11e はアプリケーション単位で QoS を提供しないので、金融や医療の情報などのクリティカルなアプリケーションのトラフィックが、それほどクリティカルでない電子メールや Web ブラウザのトラフィックと同じように処理されます。これによってワイヤレス ネットワークでの競合や輻輳が悪化し、アプリケーション全体のパフォーマンスが低下します。802.11e 規格のサブセットをサポートする Wi-Fi Multimedia (WFM) 対応デバイスはトラフィック タイプを分類できますが、それらの自己評価マーキングは不正なアプリケーションからの不適切な使用の可能性があるので、常に信頼できるとは限りません。パフォーマンスが低いためにユーザが重要なアプリケーションを実行できないとすれば、ワイヤレス展開によって得られるメリットは最小限または無効になってしまいます。

## ワイヤレス環境での Cisco Security Agent の利点

### Cisco Security Agent によるワイヤレス環境の最適化

Cisco<sup>®</sup> Security Agent は 802.11e および WMM テクノロジーの展開を強化します。具体的には、アップストリームトラフィックに QoS ポリシーを適用し、アプリケーション単位で Differentiated Services Code Point (DSCP) マーキングを設定および検証します（たとえば、金融トラフィックをミッションクリティカルとマークし、Web トラフィックをベストエフォートとマークします）。これらの DSCP マーキングは、送信されたパケットの IP ヘッダーに挿入され、ワイヤレスネットワークのアップストリームのデバイスがそれを使用してパケットを分類し、QoS サービスポリシーを適用してそのトラフィックに応じた優先順位を付けます。Cisco Security Agent を使用すると、クライアントに対して任意のレベルでこの優先順位付けを実行できます。つまり、プロトコルレベルまたは特定のプロトコルのポートレベル、さらに最も重要なのは、アプリケーションレベルでポートレベルかつプロトコルレ

ベルで実行できることです。そのため管理者は、どのトラフィックを優先するかを高度なレベルで制御できます。Cisco Security Agent は、QoS を前提に設計されたアプリケーションでない場合でも、すべてのアプリケーションに QoS を提供します。また、Cisco Security Agent により、組織は既存の WMM 非対応レガシー デバイスを使用し、アプリケーションフローをマーキングすることでクリティカルなアプリケーションの QoS を実現できます。

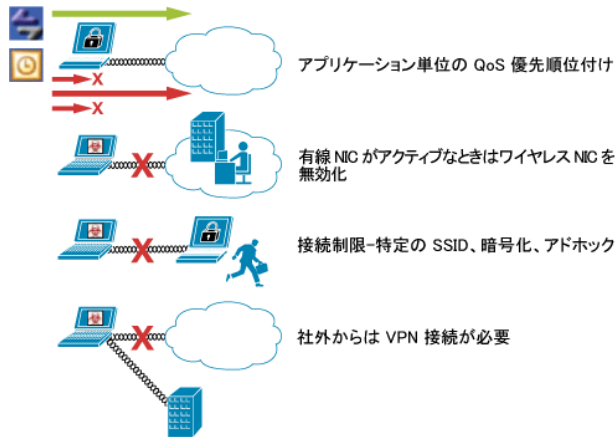
Cisco Security Agent は、Cisco Management Center for Cisco Security Agents にレポートするデスクトップおよびサーバに導入されたホストベースのエージェントで構成されます。Management Center はスタンドアロンアプリケーションとして動作し、すべての管理機能を中央集中方式で実行します。そのロールベースの Web ブラウザ アクセスによって、管理者がすべてのエンドポイントに適用する QoS ポリシーを一元化して作成または変更することが容易になります。

### ワイヤレス ポリシー制御

ワイヤレス展開戦略には、クリティカルなアプリケーションに QoS パフォーマンスを提供することに加え、セキュリティポリシーを含める必要があります。Cisco Security Agent は、ワイヤレスポリシー制御によってワイヤレス展開全体のセキュリティを強化し、ワイヤレスユーザによるリスクの高い動作を最小限に抑えます。ポリシーによって、ユーザが社外にいるときはワイヤレストラフィックへのVPN接続を要求するなど、ワイヤレス接続を特定のパラメータに制限できます。Cisco Security Agent のロケーションベースのポリシー制御は、ユーザがリモート状態の場合、機密ファイルやクリティカルアプリケーションへのアクセスを制限する機能によって、追加の保護レイヤを提供します。ワイヤレスネットワークと有線ネットワークのインターフェイス同時使用を回避でき、アドホックモードや特定のワイヤレス暗号化タイプ

の使用を制限できるので、セキュリティレベルが向上します。ワイヤレス ブロードバンド カードを区別し、必要な場合はカード タイプに基づいて使用を制限できます。これにより、企業が所有するノート PC での個人的なワイヤレス ブロードバンド カードの使用を防止します。

図 1 Cisco Security Agent のワイヤレス制御



## Cisco Security Agent とは

Cisco Security Agent は従来のエンドポイント セキュリティソリューションを超えるソリューションであり、悪意のある動作を特定して未然に防ぐことによって、企業のネットワークとアプリケーションの脅威となる既知および未知の潜在的セキュリティ リスクを排除します。Cisco Security Agent は動作を分析するため、このソリューションは運用コストを抑えると同時に堅牢な保護を実現します。

Cisco Security Agent はアプリケーションとカーネルの間に常駐し、基盤となるオペレーティングシステムの安定性とパフォーマンスへの影響を最小限に抑えながら、アプリケーションの可視性を最大化します。このソフトウェア独自の

アーキテクチャは、ファイル、ネットワーク、レジストリ ソースへのすべてのオペレーティング システム コール、およびメモリ ページ、共有ライブラリ モジュール、COM オブジェクトなどの動的なランタイム リソースへのすべてのオペレーティング システム コールを代行受信します。エージェントは独自のインテリジェンスを適用し、特定のアプリケーションまたはすべてのアプリケーションに対する不適切な動作または許容できない動作を定義したルールに基づいて、システム コールの動作の相関を行います。この相関と、それに続くアプリケーションの動作の分析によって、ソフトウェアは（セキュリティ スタッフの指示どおりに）新たな侵入を防ぐことができます。

アプリケーションが何らかの操作を実行しようとする時、Cisco Security Agent はその操作をアプリケーションのセキュリティ ポリシーに照らしてチェックし、操作の続行についてリアルタイムで許可または拒否の決定を下します。加えて、その要求をログに記録するか否かを判断します。Cisco Security Agent は、分散ファイアウォール、オペレーティングシステムのロックダウンと統合性の保証、悪意のあるモバイル コードからの防御、監査イベント収集機能を実装するセキュリティ ポリシーを組み合わせ、サーバおよびデスクトップ用のデフォルト ポリシーとして提供することで、公開企業システムのための多層防御による保護を実現します。

## Cisco Security Agent を選択する理由

ワイヤレス ネットワークによって柔軟性と自由度が大幅に向上しますが、同時に組織は、重要な資産や機密データを攻撃や悪用から守るため、ネットワークおよびデバイスを保護する方法について再検討する必要があります。Cisco Security Agent は、データのプライバシーを侵害する、悪意のある攻撃や従業員による不正使用の防止において、組織のワイヤレス セキュリティ ポリシー全体で重要な役割を果たします。

© 2008 Cisco Systems, Inc. All rights reserved.

Cisco、Cisco Systems、および Cisco Systems ロゴは、Cisco Systems, Inc. またはその関連会社の米国およびその他の一定の国における登録商標または商標です。本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。「パートナー」または「partner」という用語の使用は Cisco と他社との間のパートナーシップ関係を意味するものではありません。(0805R)

この資料に記載された仕様は予告なく変更する場合があります。