Cisco Prime Infrastructure の概要

この章では、Cisco Unified Network Solution と Cisco Prime Infrastructure について説明します。ここで説明する内容は、次のとおりです。

Cisco Unified Network Solution

Cisco Unified Network Solution は、有線ネットワークと 802.11 無線ネットワークの両方のソリューションを企業やサービス プロバイダーに提供します。これによって大規模な有線および無線 LAN の展開および管理が簡素化され、他に類のないトップレベルのセキュリティ インフラストラクチャを構築できます。オペレーティング システムによって、すべてのクライアント データ、通信、およびシステム管理機能の管理、無線リソース管理（RRM）機能の実行、オペレーティング システムのセキュリティ ソリューションを使用したシステム全体のモビリティ ポリシーの管理、およびオペレーティング システムのセキュリティ フレームワークを使用したすべてのセキュリティ機能の調整が行われます。

Cisco Unified Network Solution は、Cisco Managed Switch、Cisco Unified Wireless Network Controller（以降、*コントローラ*）および関連付けられている Lightweight アクセス ポイントから構成されます。これらはオペレーティング システムで制御され、次のいずれかまたはすべてのオペレーティング システムのユーザ インターフェイスによって、すべて同時に管理されます。

- Cisco コントローラによってホスティングされ全機能を備えた HTTPS Web ユーザ インターフェイス。個々のコントローラを設定してモニタするときに使用できます。
- 全機能を備えたコマンドライン インターフェイス（CLI）。個々のコントローラの設定とモニタに使用できます。
- Prime Infrastructure は 1 つ以上のコントローラや関連アクセス ポイントの設定とモニタに使用できます。Prime Infrastructure には、大規模システムのモニタリングと制御に便利なツールが準備されています。定義済みの物理アプライアンスと特定の仮想配置で実行されます。
- 業界標準の SNMP V1、V2c、および V3 インターフェイスであれば、SNMP 準拠のサードパーティ製ネットワーク管理システムと併用できます。

Cisco Unified Network Solution は、クライアント データ サービス、クライアントのモニタリングと制御をサポートし、またすべての不正アクセス ポイントの検出、モニタリング、および封じ込めの各機能をサポートします。これによって、Lightweight アクセス ポイント、コントローラ、およびオプションの Prime Infrastructure を使用して、企業とサービス プロバイダーに無線サービスを用意します。

（注）　特に指定しない限り、コントローラに関する情報はすべての Cisco Unified Wireless Network Controller に適用されます。これには、Cisco 2000 および 2100 シリーズ Unified Wireless Network Controller、Cisco 4100 シリーズ Unified Wireless Network Controller、Cisco 4400 シリーズ Unified Wireless Network Controller、Cisco 5500 シリーズ ワイヤレス LAN コントローラ、Cisco Wireless Services Module（WiSM）内および Cisco 26/28/37/38*xx* シリーズ Integrated Services Router 内のコントローラが含まれますが、これらに限定されません。

Prime Infrastructure について

Prime Infrastructure を使用すると、1 つ以上のコントローラ、スイッチ、および関連するアクセス ポイントを設定し、モニタできます。Prime Infrastructure には、コントローラ レベルで使用されるのと同じ設定、パフォーマンス モニタリング、セキュリティ、障害管理、およびアカウンティングのオプションが含まれますが、複数のコントローラとその管理対象のアクセス ポイントをグラフィカルに表示するオプションも追加されています。

Prime Infrastructure は Linux 上でサービスとして動作するため、継続的に実行され、リブート後には実行が再開されます。

Cisco Prime Infrastructure ユーザ インターフェイスには、Chrome プラグイン リリースを備えた Mozilla Firefox 11.0 または 12.0、あるいは Internet Explorer 8 または 9、または Google Chrome 19.0 が必要です。バージョン 8 よりも前の Internet Explorer は推奨しません。ブラウザを実行するクライアントには、最小で 1 GB のメモリと 2 GHz のプロセッサが必要です。クライアント デバイスでは、CPU やメモリを大量に使用するアプリケーションを実行しないでください。

（注）　サードパーティ製ブラウザ拡張機能を有効にしないよう強く推奨します。Internet Explorer では、[Tools] > [Internet Options] を選択して、[Advanced] タブで [Enable third-party browser extensions] チェックボックスを選択解除することで、サードパーティのブラウザ拡張を無効にできます。

Prime Infrastructure を使用すると、コントローラの設定とモニタリングが簡単になり、データ入力ミスも減少します。Prime Infrastructure は業界標準の SNMP プロトコルを使用して、コントローラと通信します。

Prime Infrastructure には、Floor Plan editor も含まれており、以下を実行できます。

- ベクトル化されたビットマップ キャンパス、フロア図面、屋外領域地図にアクセスする。
- 壁の種類の追加や変更を行う。
- ベクトル ウォール形式マップをデータベースにインポートする。

（注）　ベクトル ファイルを使うことで、Cisco Prime Infrastructure RF 予測ツールはより正確な壁と窓の RF 減衰値に基づいた、より良い RF 予測を行えます。

Cisco Unified Network コンポーネント

Cisco Unified Network ソリューションは、ビジネスのための非常に高いレベルのネットワーク セキュリティと多用途性を実現します。Cisco Unified Network ソリューションでは、オフィス内でのモビリティ向上やオフィスの建物間の接続のための安全なワイヤレス ネットワークを提供して、ご使用のネットワークを強化できます。この項では、Cisco Unified Network ソリューションのさまざまなネットワーク コンポーネントについて説明します。次のトピックを扱います。

Cisco Prime Prime Infrastructure

Prime Infrastructure はネットワーク管理者に、RF 予測、ポリシー プロビジョニング、ネットワーク最適化、トラブルシューティング、ユーザ トラッキング、セキュリティ モニタリング、および有線 / 無線 LAN システム管理の統一ソリューションを提供します。堅固なグラフィカル インターフェイスで、有線 / 無線 LAN の展開や操作はシンプルでコスト効率の高いものになります。詳細なトレンド分析および分析レポートにより、Prime Infrastructure は現行のネットワーク操作に不可欠なものになります。

WLAN コントローラ

WLAN コントローラは、高い拡張性と柔軟性を備えたプラットフォームで、中大規模企業やキャンパス環境でのミッションクリティカルなワイヤレス通信のためのシステム全体のサービスを実現します。802.11n のパフォーマンスと最大限の拡張性を重点に設計された WLAN コントローラは、5000 アクセス ポイントから 250 アクセス ポイントまでを同時に管理する能力により強化された稼働時間、信頼性の高いストリーミング ビデオや有料レベルの音声品質を可能にする優れたパフォーマンス、そして要求が非常に高い環境での安定したモビリティ経験を実現する進んだディザスタ リカバリ性能を備えています。

Prime Infrastructure は Cisco ワイヤレス コントローラをサポートしており、これはネットワークの展開や操作、管理を簡素化することで Cisco Unified Network の全体的運用経費を削減するのに役立ちます。Prime Infrastructure では、次の WLAN コントローラがサポートされています。

- Cisco 2106 ワイヤレス LAN コントローラ
- Cisco 2500 シリーズ ワイヤレス コントローラ
- Cisco 4400 シリーズ ワイヤレス LAN コントローラ
- Cisco 5508 シリーズ ワイヤレス コントローラ
- Cisco Catalyst 6500 シリーズ スイッチ用 Cisco Wireless Services Module（WiSM）
- Cisco Catalyst 6500 シリーズ スイッチ用 Cisco Wireless Services Module 2（WiSM2）
- Cisco Flex 7500 シリーズ ワイヤレス コントローラ
- Cisco Flex 8500 シリーズ ワイヤレス コントローラ
- Cisco Grey Nicols ワイヤレス コントローラ
- Cisco 仮想ワイヤレス コントローラ

仮想 LAN コントローラ

Virtual Wireless LAN Controller は、業界標準の仮想化インフラストラクチャに準拠したハードウェアで実行できるソフトウェアです。Virtual Wireless LAN Controller には、ユーザが要件に基づいてハードウェアを選択できる柔軟性があります。

コントローラ設定ページを使用して Virtual Wireless LAN Controller のプロパティを表示または設定する場合、Prime Infrastructure では VWLC としてデバイス タイプの値が表示されます（[Configure] > [Controllers] > [IP address] > [Properties] > [Settings]）。

仮想 LAN コントローラでサポートされていない機能

- データ DTLS
- Cisco 600 シリーズ OfficeExtend アクセス ポイント
- ワイヤレス レート制限
- 内部 DHCP サーバ
- モビリティ / ゲスト アンカー
- マルチキャスト ユニキャスト モード
- PMIPv6
- コントローラのハイ アベイラビリティ
- 屋外メッシュ アクセス ポイント

（注） FlexConnect モードで屋外 AP がサポートされます。

アクセス ポイント

Prime Infrastructure は、業界最先端の性能を持つアクセス ポイントをサポートし、セキュアで信頼性の高い無線接続を屋内外両方の環境で実現します。Prime Infrastructure は、あらゆる業界や業態、トポロジーに特有のニーズを満たすためのさまざまなアクセス ポイントを幅広くサポートしています。

Prime Infrastructure は次のアクセス ポイントをサポートしています。

- Cisco Aironet 801、802、1040、1100、1130、1140、1200、1230、1240、1250、1260、1310、1500、1522、1524、1552、2600i、2600e、3500i、3500e、3500p、3600i、および 3600e シリーズ Lightweight アクセス ポイント。
- Cisco Aironet 1040、1100、1130、1141、1142、1200、1240、1250、1260、2600i、および 2600e 自律アクセス ポイント。
- Cisco 600 シリーズ OfficeExtend アクセス ポイント。
- Lightweight アクセス ポイント プロトコル（LWAPP）または Control and Provisioning of Wireless Access Points（CAPWAP）プロトコルが動作している Cisco Aironet アクセス ポイント。

組み込みアクセス ポイント

Prime Infrastructure は Cisco 800 シリーズ Integrated Services Router（ISR）上の統合アクセス ポイントである AP801 をサポートしています。このアクセス ポイントはルータの Cisco IOS イメージとは別の Cisco IOS ソフトウェア イメージを使用します。これは、ローカルで設定および管理される Autonomous アクセス ポイントとして動作することも、CAPWAP プロトコルまたは LWAPP プロトコルを使用して集中管理されるアクセス ポイントとして動作することもできます。AP801 には Autonomous Cisco IOS ソフトウェア リリースおよび統合モードのリカバリ イメージの両方が事前にロードされています。

コントローラで AP801 を使用する場合、ルータ上の特権 EXEC モードで **service-module wlan-ap 0 bootimage unified** コマンドを入力して、アクセス ポイント上の統合モードのリカバリ イメージを有効にする必要があります。

（注）　**service-module wlan-ap 0 bootimage unified** コマンドが動作しない場合は、ソフトウェア ライセンスが最新のものかどうかを確認してください。

リカバリ イメージを有効にした後、ルータ上で **service-module wlan-ap 0 reload** コマンドを入力し、アクセス ポイントのシャットダウンとリブートを行います。アクセス ポイントはリブート後にコントローラを検知し、完全な CAPWAP または LWAPP ソフトウェア リリースをコントローラからダウンロードして Lightweight アクセス ポイントとして動作します。

（注）　前述の CLI コマンドを使用するには、ルータが Cisco IOS Release 12.4(20)T 以降を実行している必要があります。問題が発生した場合、次の URL にある『Integrated Services Router configuration guide』の「Troubleshooting an Upgrade or Reverting the AP to Autonomous Mode」の項を参照してください。
http://www.cisco.com/en/US/docs/routers/access/800/860-880-890/software/configuration/guide/admin_ap.html

CAPWAP または LWAPP をサポートするには、ルータがアクティブ化されており、Cisco Advanced IP Services IOS のライセンス グレード イメージを保持している必要があります。ルータ上の Cisco IOS イメージをアップグレードするには、ライセンスが必要です。ライセンス情報については、次の URL を参照してください。

http://www.cisco.com/en/US/docs/routers/access/sw_activation/SA_on_ISR.html

AP801 が統合モードのリカバリ イメージと共にブートすると、コントローラと通信し、統合イメージと設定をコントローラからダウンロードするため、IP アドレスが必要です。ルータは DHCP サーバ機能、コントローラにアクセスするための DHCP プール、および DHCP プール設定におけるコントローラ IP アドレスのためのセットアップ オプション 43 を提供できます。このタスクを実行するには、次の設定を使用します。

```
ip dhcp pool pool_name
    network ip_address subnet_mask
    dns-server ip_address
    default-router ip_address
    option 43 hex controller_ip_address_in_hex
Example:
ip dhcp pool embedded-ap-pool
    network 209.165.200.224 255.255.255.224
    dns-server 209.165.200.225
    default-router 209.165.200.226
    option 43 hex f104.0a0a.0a0f /* single WLC IP address (209.165.201.0) in hex format */
```

AP801 802.11n 無線は、Cisco Aironet 1250 シリーズ アクセス ポイントの 802.11n 無線よりも低い電力レベルをサポートします。AP801 は無線電力レベルを保持し、アクセス ポイントがコントローラに接続する場合に、これをコントローラに渡します。コントローラは与えられた値を使用してユーザ設定を制限します。

AP801 は、FlexConnect モードで使用できます。FlexConnect の詳細は、「FlexConnect の設定」（P.12-1）を参照してください。

（注）　AP801 の詳細は、次の URL にある Cisco 800 シリーズ ISR についてのマニュアルを参照してください。
http://www.cisco.com/en/US/products/hw/routers/ps380/tsd_products_support_series_home.html.

アクセス ポイント通信プロトコル

コントローラ ソフトウェア リリース 5.2 以降では、Cisco Lightweight アクセス ポイントは、IETF 標準 Control and Provisioning of Wireless Access Points Protocol（CAPWAP）を使用して、ネットワーク上のコントローラと他の Lightweight アクセス ポイントとの間の通信を行います。5.2 よりも前のコントローラ ソフトウェア リリースは、これらの通信に Lightweight Access Point Protocol（LWAPP; Lightweight アクセス ポイント プロトコル）を使用します。

CAPWAP は LWAPP に基づく標準の互換プロトコルであり、コントローラによる無線アクセス ポイントの集合の管理を可能にします。CAPWAP は、次のような理由により、コントローラ ソフトウェア リリース 5.2 で実装されています。

- LWAPP を使用するシスコ製品に、CAPWAP を使用する次世代シスコ製品へのアップグレード パスを提供するため。
- RFID リーダーおよび類似のデバイスを管理するため。
- コントローラにサードパーティのアクセス ポイントとの将来的な互換性を持たせるため。

LWAPP 対応のアクセス ポイントは CAPWAP と互換性があり、CAPWAP コントローラにシームレスに変換できます。たとえば、CAPWAP 使用時のコントローラ ディスカバリ プロセスおよびファームウェア ダウンロード プロセスは、LWAPP 使用時のものと同じです。例外として、レイヤ 2 の展開は CAPWAP ではサポートされません。

CAPWAP ソフトウェアのコントローラと LWAPP ソフトウェアのコントローラを組み合わせて配置することができます。CAPWAP を使用可能なソフトウェアでは、アクセス ポイントは CAPWAP を実行するコントローラでも LWAPP を実行するコントローラでも join できます。Cisco Aironet 1140 シリーズ アクセス ポイントは唯一の例外であり、CAPWAP のみをサポートするため、CAPWAP を実行するコントローラにのみ接続します。

（注）　WLC バージョン 7.0 以降が動作している CAPWAP コントローラだけに関連付けられた Cisco Aironet 1140 シリーズおよび 3500 シリーズ アクセス ポイント。

ここでは、次の内容について説明します。

- 「CAPWAP 使用のガイドラインと制限」（P.1-7）
- 「Cisco ワイヤレス LAN コントローラ AutoDiscovery」（P.1-7）
- 「コントローラ ディスカバリのプロセス」（P.1-7）

CAPWAP 使用のガイドラインと制限

- CAPWAP および LWAPP コントローラは同じモビリティ グループで使用できません。このため、CAPWAP コントローラと LWAPP コントローラとの間のクライアント モビリティはサポートされていません。
- LWAPP を使用するアクセス ポイントからのトラフィックのみ許可するようファイアウォールが設定されている場合は、ファイアウォールのルールを変更して CAPWAP を使用するアクセス ポイントからのトラフィックを許可する必要があります。
- CAPWAP ポートが有効であり、アクセス ポイントがコントローラに接続できないようにする可能性のある中間デバイスによりブロックされていないことを確認してください。
- CAPWAP が LWAPP と異なるポートを使用している場合は、ネットワーク内のアクセス コントロール リスト（ACL）を変更する必要があります。

Cisco ワイヤレス LAN コントローラ AutoDiscovery

コントローラの AutoDiscovery は、オペレータによって定義された Cisco WLAN ソリューション モビリティ グループ サブネットに限定されます。

Cisco ワイヤレス LAN コントローラの AutoDiscovery には、次のような特徴があります。

- オペレータは、IP アドレスによって単独のコントローラを検索できます。
- 指定した IP アドレス範囲内のネットワーク上にあるコントローラを検出します。
- コントローラ情報を Cisco Prime Infrastructure データベースに自動的に入力します。

（注） Class C アドレス範囲では、コントローラの AutoDiscovery に時間がかかる場合があります。Class B や Class A 範囲には大量のアドレスがあるため、Class B や Class A 全体を範囲とした AutoDiscovery は推奨しません。

アクセス ポイントがコントローラと関連付けられると、コントローラはただちにアクセス ポイント情報を Cisco Prime Infrastructure に送信し、アクセス ポイントは自動的にデータベースに追加されます。

アクセス ポイント情報が Cisco Prime Infrastructure データベースに登録された後、オペレータはアクセス ポイントを Cisco Prime Infrastructure ユーザ インターフェイス マップ上の適切なスポットに追加できます。

コントローラ ディスカバリのプロセス

CAPWAP 環境では、Lightweight アクセス ポイントが CAPWAP 検出方式によってコントローラを検出し、コントローラに CAPWAP 接続要求を送信します。これに対し、コントローラはアクセス ポイントに CAPWAP join response を返し、アクセス ポイントはコントローラに join できるようになります。アクセス ポイントがコントローラに join すると、コントローラによってアクセス ポイントの構成、ファームウェア、制御トランザクション、およびデータ トランザクションが管理されます。

Lightweight アクセス ポイントをネットワークでアクティブにするには、コントローラがそのアクセス ポイントを検出する必要があります。Lightweight アクセス ポイントでは、次のコントローラ ディスカバリのプロセスがサポートされています。

- Layer 3 CAPWAP または LWAPP ディスカバリ：アクセス ポイントとは異なるサブネット上で行われ、レイヤ 2 ディスカバリで使用される MAC アドレスではなく IP アドレスと UDP パケットが使用されます。

- Over-The-Air Provisioning（OTAP）：この機能は Cisco 4400 シリーズ コントローラでサポートされています。この機能がコントローラ上で有効にされると（コントローラの [General] ページ）、関連付けられたアクセス ポイントすべてはワイヤレス CAPWAP または LWAPP ネイバー メッセージを送信し、新しいアクセス ポイントはこれらのメッセージからコントローラの IP アドレスを受信します。この機能はデフォルトでは無効です。すべてのアクセス ポイントをインストールする際は、無効のままにしておいてください。
- ローカルに保存されているコントローラの IP アドレス ディスカバリ：アクセス ポイントがすでにコントローラにアソシエートされている場合、プライマリ、セカンダリおよびターシャリ コントローラの IP アドレスはアクセス ポイントの不揮発性メモリに保存されます。今後の展開用にアクセス ポイントにコントローラの IP アドレスを保存するこのプロセスは、「*アクセス ポイントのプライミング*」と呼ばれます。
- DHCP サーバの検出：この機能では、DHCP オプション 43 を使用してアクセス ポイントにコントローラの IP アドレスを割り当てます。Cisco スイッチでは、通常この機能に使用される DHCP サーバ オプションをサポートしています。
- DNS の検出：アクセス ポイントでは、ドメイン ネーム サーバ（DNS）を介してコントローラを検出できます。アクセス ポイントでこれを実行するには、CISCO-CAPWAP-CONTROLLER.*localdomain* または CISCO-LWAPP-CONTROLLER.*localdomain* への応答としてコントローラの IP アドレスを返すよう、DNS を設定する必要があります。ここで、*localdomain* はアクセス ポイント ドメイン名です。アクセス ポイントは、DHCP サーバから IP アドレスと DNS の情報を受信すると、DNS に接続して CISCO-CAPWAP-CONTROLLER.*localdomain* または CISCO-LWAPP-CONTROLLER.*localdomain* を解決します。DNS からコントローラの IP アドレスのリストを受信すると、アクセス ポイントはコントローラに discovery request を送信します。

Prime Infrastructure サービス

組織内の IT 部門には、増大する帯域幅や性能要求に応え、新しいモバイル デバイスの増加に対応しながら、同時にネットワーク アクセス、可用性、規制遵守を確保することが求められています。

シスコとパートナーは、IT スタッフによる Cisco Unified Network への移行をお手伝いします。これで、Wi-Fi 機能を持つ電話やタブレットといったさまざまなモバイル デバイスやリッチなメディア コンテンツに対応できる、セキュアで高性能な、有線と無線の統合ネットワーク管理が容易になります。

この項では、Prime Infrastructure が提供するサービスについて説明します。次のトピックを扱います。

- 「Cisco Context Aware Service ソリューション」（P.1-8）
- 「Cisco Identity Service Engine ソリューション」（P.1-9）
- 「Cisco Adaptive Wireless Intrusion Prevention Service」（P.1-10）

Cisco Context Aware Service ソリューション

Context Aware Service（CAS）は、Wi-Fi 802.11a/b/g/n ネットワークがアクティブな Wi-Fi デバイスを持つ人や物（ワイヤレス クライアントやアクティブ RFID タグ、端末からワイヤレス インフラストラクチャを通じて上流クライアントに送られる関連データなど）の位置を特定できるようにします。

Context Aware Service（CAS）を使用することで、モビリティ サービス エンジン（MSE）が Cisco アクセス ポイントからの位置や可用性といったコンテキスト情報を取得して、何千ものモバイル アセットやクライアントを同時にトラッキングすることが可能になります。

収集されたコンテキスト情報は、中央集中型 WLAN 管理プラットフォームである Prime Infrastructure のユーザ インターフェイスに GUI 形式で表示できます。Prime Infrastructure は MSE とのインターフェイスとなる管理システムで、MSE が提供するサービス用のユーザ インターフェイス（UI）を備えています。

MSE のインストールと初期設定が完了した後、MSE は複数の Cisco ワイヤレス LAN コントローラと通信して、オペレータが定義したコンテキスト情報を収集できます。その後、関連付けられた Prime Infrastructure を使用して各 MSE と通信し、選択したデータの送信や表示を行うことができます。

クライアント、スイッチ、不正アクセス ポイント、不正クライアント、モバイル ステーション、アクティブ RFID アセット タグの情報を収集するよう MSE を設定できます。

Context-Aware の位置情報サービスを使用すれば、管理者は 802.11 ベースのデバイスすべての位置を特定できます。デバイスの種類や状態を指定することも可能です。システムは、クライアント（関連付け済みや検証中など）、不正アクセス ポイント、不正クライアント、アクティブ タグをすべて識別し、位置を特定できます。詳しくは、『Context Aware Mobility Solution Deployment Guide』を参照してください。

（注）　1 つの MSE は 1 つの Prime Infrastructure でのみ管理できます。つまり、単一の MSE は複数の Prime Infrastructure では管理できませんが、単一の Prime Infrastructure で複数の MSE を管理することはできます。管理対象デバイスの数が 1 つの MSE の容量を超えた場合、複数の独立した MSE の配置が必要になります。

Cisco Identity Service Engine ソリューション

Cisco Identity Services Engine（ISE）は、次世代のアイデンティティおよびポリシー ベースのネットワーク アクセス プラットフォームで、企業はこれを利用して法令遵守の確保、インフラストラクチャ セキュリティの強化、サービス運営の簡素化が可能です。

Cisco ISE では、認証、許可、ポスチャ、ゲスト、プロファイリングについてのポリシーの作成と管理を 1 つのコンソールで行えます。さらに、ポリシー要素をサービス全体で再利用することが可能になったため、企業としてタスク数とオーバーヘッドを減らし、整合性を高めることが可能です。

Cisco ISE はデバイス、インフラストラクチャ、サービスから情報を収集して、組織がさらにリッチなコンテキスト ポリシーをネットワーク全体に一元的に実施することを可能にします。ISE はネットワークに接続するクライアントやデバイスすべてをトラッキングし、接続したユーザ、デバイスのアイデンティティや位置、さらにエンドポイントの健全性についての一元的な情報源として動作します。

IP 接続可能なエンドポイント デバイスすべてを検出し、識別し、モニタする機能により、IT チームは社内ネットワーク上のユーザと「ヘッドレス」デバイス双方を十分に把握できます。

Cisco ISE は AAA、ポスチャ、プロファイリング、ゲストの管理機能を単一のアプライアンスに統合して動的なアクセス制御を実施します。Identity Services Engine は企業インフラストラクチャ全体に展開でき、802.1x 有線、無線、VPN ネットワークをサポートしています。

Prime Infrastructure は、ネットワーク上の有線クライアントとワイヤレス クライアントの両方を管理します。Cisco ISE を RADIUS サーバとしてクライアントの認証に使用する場合、Prime Infrastructure は Cisco ISE からクライアントについての追加情報を収集し、クライアント関連の情報すべてを Prime Infrastructure に提供して、単一のコンソールで表示可能にします。

ネットワーク内でポスチャ プロファイリングが実施されている場合、Prime Infrastructure は Cisco ISE との通信でクライアントのポスチャ データを取得し、クライアントの他の属性とともに表示します。Cisco ISE を使用してネットワーク内のクライアントやエンドポイントのプロファイリングを行う場合、Prime Infrastructure はプロファイルされたデータを収集して、クライアントの種類（iPhone、iPad、Android デバイス、その他のデバイス）を識別します。

Cisco ISE は Prime Infrastructure によるクライアント情報のモニタとトラブルシューティングを助け、クライアント関連の情報すべてを単一のコンソールに表示します。

Cisco Adaptive Wireless Intrusion Prevention Service

RF 環境に常時注意を払うことは、法的責任の最小化、ブランド イメージの維持、法的規制の遵守のために重要です。

Cisco Adaptive Wireless Intrusion Prevention System（IPS）は、ワイヤレス ネットワークの異常、不正アクセス、RF 攻撃に対するモニタリングと検出に特化した、先進のネットワーク セキュリティを提供します。Cisco Unified Network と統合されているため、オーバーレイ ソリューションを必要とせずに、ネットワーク全体を一元的に把握し、管理できます。

Cisco Adaptive Wireless Intrusion Prevention Service（wIPS）は、不正アクセス ポイント、不正クライアント、およびアドホック接続の検出と緩和、Over-the-Air ワイヤレス ハッキングおよび驚異の検出、セキュリティ脆弱性モニタリング、パフォーマンス モニタリングおよび自己最適化、脅威予防のためのネットワーク強化、高機能なワイヤレス セキュリティ管理およびレポート作成を行います。

Cisco wIPS は、協働して統合セキュリティ モニタリング ソリューションを実現する、次のコンポーネントで構成されています。

- wIPS ソフトウェア実行中のモビリティ サービス エンジン（MSE）: すべてのコントローラとそれらの各 wIPS モニタ モード アクセス ポイントからのアラーム集約の中央ポイント。アラーム情報とフォレンジック ファイルはアーカイブ目的でモビリティ サービス エンジンに保存されます。
- wIPS モニタ モード アクセス ポイント : 攻撃検出とフォレンジック（パケット キャプチャ）機能を備えた固定チャネル スキャンを提供します。
- ローカル モード アクセス ポイント : タイムスライス型不正スキャンに加え、ワイヤレス サービスをクライアントに提供します。
- ワイヤレス LAN コントローラ : wIPS モニタ モード アクセス ポイントから受信した攻撃情報をモビリティ サービス エンジンに転送し、設定パラメータをアクセス ポイントに配布します。
- Prime Infrastructure : モビリティ サービス エンジン上での wIPS サービス設定、コントローラへの wIPS 設定内容のプッシュ、wIPS モニタ モードのアクセス ポイント設定を行う、一元化された管理プラットフォームを管理者に提供します。Prime Infrastructure は、wIPS アラーム、フォレンジック、報告の表示や、攻撃百科事典へのアクセスにも使用されます。